UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CREACIÓN DEL MANUAL DE PRÁCTICAS PARA EL LABORATORIO DE ADMINISTRACIÓN DE REDES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

MACÍAS RÍOS MARÍA EUGENIA

MEDINA ORTEGA KAREN CRISTINA

DIRECTORA DE TESIS:
M. C. MA. JAQUELINA LÓPEZ BARRIENTOS

Ciudad Universitaria, México D.F. 2006.

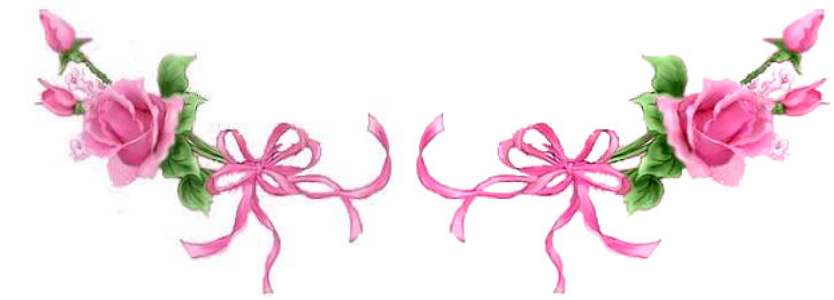
Agradecimientos

Siempre es complicado dar las gracias con el corazón en las manos, pero estamos seguras que en esta ocasión, es la oportunidad idónea para recordar que siempre hay alguien junto a nosotras y que habrá gente alrededor a quien les importe, nuestras acciones por lo que agradecemos a todas esas personas, que nos han visto crecer, que han seguido nuestras vidas muy de cerca, a nuestras familias por el apoyo moral y el amor que día a día nos demuestran, a los amigos que hemos logrado a lo largo de nuestras vidas y a las personas que ya no vemos, a las personas que seguimos conociendo y a las personas que en nuestra búsqueda, por un crecimiento espiritual nos faltan por conocer.

Con todo nuestro cariño y compartiendo el alma, nos resta por decir que dedicamos esta tesis a todas aquellas personas que en nuestro corazón tienen ya un lugar.

Gracias

Karen *Maru*



A Dios por darme la oportunidad de vivir y conocer a las personas exactas, en el momento preciso en mi vida.

A mis padres: Cristina Ortega y Pedro Medina Salazar, por estar conmigo.

A mis hermanas: Denisse, Priscila, Lúlu y Pedro, por ser las personas que inyectan vida a mi vida.

A mi madrina Lidia, por su tolerancia, paciencia y disposición de escucharme en todo momento.

A la familia de Maru y obviamente a Maru, por su enorme apoyo, paciencia y tolerancia para que este trabajo pudiera concluirse.

A todos mis amig@s por la amistad que me han brindado, a Eric por estar conmigo y brindarme su apoyo y por recorrer conmigo experiencias inolvidables, por haber compartido tristezas, alegrías y sobre todo gracias por apoyarme en los momentos difíciles.

A la profesora M. C. Ma. Jaquelina López Barrientos por su paciencia y dedicación, motivación y amistad y a todas aquellas personas que han sido una guía en mi formación, a la Facultad de Ingeniería y a la UNAM, por ser mi segunda casa.

Karen

A Dios por las bendiciones, por darme la oportunidad de la vida y las personas que están a mi lado.

A mis padres: Magdalena Ríos y Arturo Macías, por que siempre me han apoyado en todo momento, por brindarme su amor, amistad y cariño. No existen palabras para expresar cuanto los admiro y los quiero, en verdad muchas gracias por confiar en mí.

A mis hermanas: Nadia, Lucia y Adria, por compartir tantos momentos alegres y tristes, por su apoyo, consejos y dedicación, gracias.

A Karen por ser una gran persona y por compartir este gran reto, gracias por apoyarme amiga.

A todos mis amig@s por la amistad que me han brindado, por recorrer conmigo experiencias inolvidables, por haber compartido tristezas, alegrías y sobre todo gracias por apoyarme en los momentos difíciles.

Al M. I. Rigel Gámez Leal por su apoyo, amistad, comprensión e impulso, a todos los integrantes del CAALFI, por su apoyo y comprensión.

A la profesora M. C. Ma. Jaquelina López Barrientos por su paciencia, tolerancia, dedicación, motivación y amistad y a todas aquellas personas que han sido una guía en mi formación, a la Facultad de Ingeniería y a la UNAM.

Maru

INTRODUCCIÓN

Actualmente la Ingeniería en Computación tiene enorme presencia en el mundo, con ello las redes de datos, ya que la información de las empresas, organizaciones gubernamentales y educativas, entre otras; se transporta, almacena, genera, procesa y mantiene a través de esta tecnología, siendo así uno de los campos más importantes y excitantes de nuestro tiempo.

El área de las comunicaciones en general, y específicamente las redes de datos han experimentado en las últimas décadas un impulso extraordinario. Una de las razones de este hecho se debe a la elevada aceptación y penetración, que este tipo de tecnología ha encontrado en nuestra sociedad. De manera que, hoy en día, no es concebible la existencia de un centro empresarial, investigador o administrativo en el que no se haga uso de sistemas de comunicación para el manejo y administración de información.

Una red consta de muchas piezas complejas de hardware y software que interactúan entre sí; desde enlaces, puentes, routers, hosts y otros dispositivos que constituyen los componentes físicos de la red, hasta los diversos protocolos que los coordinan y controlan. La administración de la red, implica la planificación, organización, integración, dirección y el control de tales elementos de comunicación, para garantizar un adecuado nivel de servicio, de acuerdo a un costo determinado. Entre los objetivos principales de la administración de redes, encontramos el de mejorar su disponibilidad y el rendimiento de los elementos del sistema, así como incrementar su efectividad.

Por lo anterior es necesario que el administrador de red, cumpla con los siguientes puntos en la realización de sus actividades:

- Planificación, el administrador debe considerar desde el inicio, la infraestructura del sistema de la que depende la vida futura de la red, así como las políticas y ética que rigen el cómputo.
- Organización, el administrador implementará los modelos de la administración de redes para su óptimo desempeño y utilizará modelos para administración de los protocolos utilizados en las redes de datos.
- Integración, el administrador debe ser capaz de implementar las tecnologías actuales e integrarlas como soluciones para el adecuado funcionamiento de las redes.
- Dirección, el administrador debe contar con las habilidades directivas que le permitan interactuar con el equipo de trabajo, teniendo la capacidad de conjuntar esfuerzos en beneficio de la red.
- Control, el administrador debe optimizar las prestaciones de los elementos que componen la red, a través del monitoreo continuo del sistema global, manejando estándares para la medición, ejecución, acciones preventivas y correctivas.

Así, los administradores deben asegurar la planificación de la seguridad de la red para que ésta proporcione servicio continuo, diseñando de acuerdo con el nivel de rendimiento requerido en la empresa u organización e implementando nuevas funciones a medida que crecen las demandas en ella.

Es indispensable que las nuevas generaciones de Ingeniería en Computación adquieran los conocimientos y habilidades prácticas que les permitan planificar, organizar, integrar, dirigir y controlar de manera eficiente la tecnología asociada a la información en este ámbito, esto es, la Administración de Redes.

Por ello actualmente, la Facultad de Ingeniería preocupada por mantener actualizados los conocimientos de sus egresados, lleva a cabo la integración de una asignatura (Administración de Redes) en el nuevo plan de estudios, con la finalidad de cubrir estas necesidades y por lo que el presente trabajo de tesis está enfocado a desarrollar una propuesta de prácticas de laboratorio, así como el material teórico que sustente dicho conocimiento y que sirva de base para que los alumnos adquieran las habilidades necesarias de la Administración de Redes.

El objetivo principal de esta tesis, es desarrollar una propuesta del manual de prácticas del Laboratorio de Administración de Redes, que permita a los estudiantes de Ingeniería en Computación, adquirir las habilidades necesarias para desenvolverse con éxito profesional.

Para llevar a cabo el objetivo y con base en el programa de la asignatura Administración de Redes, esta tesis está compuesta por cinco capítulos.

Capítulo uno, *Planeación*, abarca los cimientos teóricos que un administrador de redes debe conocer para llevar a cabo la planeación de la red, identificando los elementos que la conforman, comprendiendo los objetivos del diseño, llevando a cabo el análisis de requerimientos de hardware y software, tomando en cuenta el direccionamiento lógico, así como elaborando las políticas de cómputo, con ética profesional.

Para este capítulo, cuyo objetivo es conocer e identificar los elementos que conforman una red de datos, así como las políticas y ética que rigen sobre el cómputo, se han propuesto tres prácticas:

- Práctica 1, Configuración básica de redes.
- Práctica 2A, Manejo de dispositivos de interconectividad, hub y switch.
- Práctica 2B, Manejo de dispositivos de interconectividad, routers.

Capítulo dos, *Organización*, se describen los modelos de administración de red: TMN, TOM y eTOM, que un administrador de redes puede aplicar a la red para obtener un óptimo desempeño; de la misma forma se presentan los protocolos de administración de red como SNMP, CMIP y CORBA.

Para este capítulo, cuyo objetivo es aplicar los modelos de administración de redes para su óptimo desempeño, se han propuesto tres prácticas:

- Práctica 3, Administración con SNMP.
- Práctica 4, Modelado de procesos de negocio con eTOM.
- Práctica 5, Introducción a la programación CORBA.

Capítulo tres, *Integración*, se presentan las tecnologías actuales que pueden ser aplicadas a las redes e integrar soluciones para su adecuado funcionamiento. Se analizan las tecnologías en telecomunicaciones, telefonía, comunicaciones inalámbricas, Internet2, videoconferencia y se estudia la metodología para la evaluación de proyectos de cómputo.

Para este capítulo, cuyo objetivo es conocer las tecnologías actuales e integrar soluciones para el adecuado funcionamiento de las redes que se están implantando, se han propuesto cuatro prácticas:

- Práctica 6, Configuración de VoIP.
- Práctica 7A, Comunicaciones inalámbricas, red tipo infraestructura.

- Práctica 7B, Comunicaciones inalámbricas, servidor DHCP.
- Práctica 8, Videoconferencia.

Capítulo cuatro, *Dirección*, se muestran las habilidades que debe poseer un directivo de las tecnologías de las telecomunicaciones, que le permitan manejar los conflictos que se presentan en la organización, con el fin de que los equipos sean más efectivos.

Para este capítulo, cuyo objetivo es conocer e identificar el perfil y las habilidades que deberá poseer un directivo de las tecnologías de las telecomunicaciones, se ha propuesto una práctica:

- Práctica 9, Manejo de conflictos.

Capítulo cinco, *Control*, el administrador debe llevar a cabo el control de la red, por medio de mecanismos de seguridad, monitoreando la red, manejando las listas de acceso, implementando auditorías informáticas y considerando que se debe contar con un plan de contingencia en caso de desastres.

Para este capítulo, cuyo objetivo es conocer, identificar y aplicar técnicas que le permitan diseñar, implantar y manejar de forma adecuada la red diseñada a fin de medir y obtener los resultados del desempeño esperados, de acuerdo a los objetivos planteados desde la planeación, se han propuesto cuatro prácticas:

- Práctica 10A, Mecanismos de seguridad, firma digital.
- Práctica 10B, Mecanismos de seguridad, certificados digitales.
- Práctica 10C, Mecanismos de seguridad, firewall.
- Práctica 11, Monitoreo de la red.

Finalmente se presentan las prácticas propuestas, donde se aprecia que el número de prácticas destinadas a cada tema corresponde en parte proporcional, al número de horas destinadas al mismo, según el plan de estudio de la asignatura; por último se exponen las conclusiones del presente trabajo de tesis.

Capítulo 1

PLANEACIÓN

INTRODUCCIÓN

Las computadoras aportan una mayor velocidad, precisión y fiabilidad al proceso de negocio. Por consiguiente, ahorran tiempo, dinero y mejoran la calidad de los servicios y productos que se ofrecen a los clientes. Las redes añaden un valor incluso mayor que estas ventajas fundamentales, haciendo que las computadoras (y otras tecnologías) trabajen rápida y fácilmente entre sí, también permiten conectar a la organización a Internet y puede aportar numerosos beneficios adicionales como videoconferencia, multimedia, transferencia de archivos de video, datos, voz y archivos gráficos a gran velocidad, servicios de información de negocio en línea, etc.

Por ello, la planeación de la red, indica al administrador los puntos que debe considerar desde el inicio, la infraestructura del sistema de la que depende la vida futura de la red, así como las políticas y ética que rigen el cómputo.

En este primer capítulo se muestran los objetivos del diseño de la red, ¿por qué construir una red?, ¿cuáles son los beneficios?, ¿cuál es la metodología en el diseño de una red?, el análisis de los requerimientos de software y hardware, así como el direccionamiento lógico.

Analizaremos el diseño de las políticas de cómputo y la ética informática, puntos que nos permiten tener una planeación óptima de la red, considerando la funcionalidad, la escalabilidad, la adaptabilidad y manejabilidad, dependiendo del tipo de organización.

1.1 Objetivos del diseño en las redes

Las redes se encuentran en todos los lugares: si se emplea una tarjeta de crédito o débito, para realizar llamadas telefónicas, o bien si se usa una computadora para acceder a Internet. Estos escenarios, son entornos complejos que implican la existencia de múltiples medios, protocolos e interconexiones con redes externas.

Las organizaciones han visto incrementada drásticamente su productividad, gracias a la inversión en redes más robustas, dicho incremento no se consigue únicamente comprando equipos de red. Se requiere de profesionales preparados para planificar, diseñar, instalar, desplegar, configurar, operar, mantener y resolver los problemas de las redes actuales. Es en este, ámbito donde los administradores de redes garantizan la planificación de la seguridad de la red y su funcionamiento continuo.

Las redes bien diseñadas y cuidadosamente instaladas pueden reducir los problemas asociados al crecimiento de un entorno de trabajo en red en desarrollo.

El diseño, la construcción y el mantenimiento de una red pueden, resultar una tarea complicada a pesar de las mejoras en el rendimiento de los equipos y las posibilidades de los medios.

Entre las principales actividades con las que se debe comprometer una red de computadoras se encuentran:

a. La información debe entregarse de manera confiable sin ningún daño en los datos, al mismo tiempo que debe ser consistente.
b. Las computadoras que integran la red, deben ser capaces de identificarse entre sí a lo largo de misma red.
c. Debe existir una forma estándar de nombrar e identificar las partes de una red.

Las aplicaciones que existen sobre las redes, pueden ser tan sencillas, como la transferencia de un archivo de una máquina a otra, o tan complejas como un sistema de transferencia financiero, en el que la información se trasmite a través de pulsos eléctricos mediante fibra óptica. Independientemente de la aplicación, el objetivo fundamental de la red, consiste en asegurar que los datos sean compartidos de una manera eficiente, rápida, confiable y precisa.

El diseño de una red, implica más que la simple conexión de computadoras. Para diseñar redes fiables, administrables y escalables se deben considerar cada una de las características de los componentes que la integran.

El primer paso en el diseño de una red, consiste en establecer y documentar los objetivos, los cuales requieren ser específicos de cada organización. Se pueden establecer ciertos requisitos que a continuación se enlistan, para el diseño de una red, en esta primera etapa:

a. Funcionalidad, esto significa que la red debe permitir a los usuarios satisfacer sus necesidades, proporcionando conectividad de usuario a usuario y de usuario a aplicación, con velocidad y fiabilidad razonables.
b. Escalabilidad, la red puede crecer, esto es, debe ser capaz de ser modificable en su tamaño, sin necesidad de alterar el diseño original.
c. Adaptabilidad, las redes deben construirse con la idea del cambio, por lo que no debe contar con elementos que la limiten en la implantación de nueva tecnología.

d. Manejabilidad, garantizar la estabilidad de operación, es un objetivo de las redes para facilitar el control de las mismas.

¿POR QUÉ CONSTRUIR UNA RED?

Sin importar cuál sea el tipo de red, todas tienen los siguientes objetivos en común:

1. Las redes incrementan la eficiencia.
2. Ayudan a estandarizar políticas, procedimientos y prácticas entre los usuarios.
3. Reúnen diversas ideas y problemáticas en un foro común, donde se pueden tratar de una forma global, en lugar de hacerlo de manera local.
4. Aseguran que la información sea redundante, en un momento dado.

En conclusión, si se tiene la necesidad de comunicarse, compartir información o aplicaciones y no se desea ir de una máquina a otra llevando y trayendo discos, la conectividad de redes ofrece una gran cantidad de beneficios.

1.1.1 Beneficios de la red

Las computadoras aportan una mayor velocidad, precisión y fiabilidad al proceso de la organización. Por consiguiente, ahorran tiempo y dinero, mejorando la calidad de los servicios y productos que se ofrecen a los usuarios. Las redes añaden un valor incluso mayor que estas ventajas fundamentales, haciendo que las computadoras (y otras tecnologías) trabajen rápida y fácilmente entre sí. Por ello, para seguir siendo competitivo en el actual entorno en cualquier organización, una red eficaz es una necesidad crítica, y entre los principales beneficios encontramos.

a. Compartir de manera eficiente los recursos, esto incluye:
    1. Dispositivos de salida, como impresoras.
    2. Dispositivos de entrada como escáneres.
    3. Dispositivos de almacenamiento como CD-ROM, unidades ZIP, JAZ.
    4. Módems y conexiones a Internet.
b. Aplicaciones compartidas, el compartir datos y aplicaciones, es una razón importante de la conectividad de redes y puede ser tan simple como utilizar una copia de Microsoft Word almacenada en otra unidad de usuario o bien tan compleja como una aplicación groupware que rutea datos de usuario a usuarios de acuerdo a un conjunto de reglas preestablecidas. Ejemplos de este punto son los calendarios de grupos, listas de correos, etc.
c. Administración centralizada, una vez que las computadoras están en red, existen herramientas que permiten la administración conjunta de los equipos, sin tener que considerar el caso individual de cada máquina, por ejemplo: el software Systems Management Server de Microsoft, Saber LAN Manager de McAfee, TME10 de Tivoli y Norton Administrador para Redes de Symantec, entre otros.

    Este grupo de utilerías le permiten al administrador reunir y estandarizar configuraciones de computadoras de toda una red y en el mejor de los casos instalar software en las computadoras de los usuarios sin tener que abandonar el escritorio.

1.1.2 Desventajas de no estar en red

Entre las principales desventajas que encontramos al no tener nuestros equipos conectados en red tenemos:

a. Compartir recursos de forma ineficiente.
b. Al no estar en red, no se pueden compartir ni aplicaciones ni hardware.
c. Aplicaciones de software no compartidas, la única forma de compartir es a través de medios extraíbles, sin embargo este método no es muy eficiente, además se requiere del software adecuado para ver las aplicaciones.
d. Recursos de impresión no compartidos, existe un método de conectar las impresoras a equipos que no están en red, esto es a través de interruptores que pueden dañar los elementos electrónicos de una impresora.
e. Recursos de Internet no compartidos, no hay conexiones comunes, por lo que entonces no hay una salida compartida a Internet.
f. Datos de baja velocidad.
g. Administración no centralizada de datos, al no estar en red, no existe una configuración estándar de acceso, ni del sistema, se requiere un tratamiento individual para cada equipo, lo cual constituye una pérdida de tiempo, trabajo y dinero.
h. Costo, la conectividad de red, reduce gastos que son sumamente elevados en la computación.

1.1.3 Metodología de diseño de redes

Para que las redes cumplan con sus objetivos, deben estar diseñadas e implementadas, en función de una serie planificada de pasos sistemáticos, entre los que se incluyen:

1. Conocer los requisitos y expectativas de los usuarios.
2. Analizar los requisitos de la red.
3. Documentar e implementar las redes lógicas y físicas.

A. Conocer los requisitos y expectativas de los usuarios

El primer paso consiste en reunir información acerca de la estructura de la organización, en la que se implantará la red. Entre los puntos más importantes están:

a. Antecedentes de la organización y su estado actual.
b. El crecimiento esperado.
c. Las normas de funcionamiento.
d. Procedimientos de administración.
e. Sistemas y procedimientos de oficina.
f. Opiniones y necesidades de los usuarios que utilizarán la red.

Algunas preguntas de referencia pueden ser:

- ¿Quién va a usar la red?

- ¿Qué nivel de conocimientos tiene el usuario?
- ¿Cuáles son sus opiniones acerca de las computadoras y sus aplicaciones?

Las respuestas a estas preguntas, permiten determinar el nivel de formación necesario y el número de personas a las que deberá dar cobertura la red.

Este primer proceso permite clarificar e identificar los problemas existentes, de la misma manera es necesario verificar si existen normas documentadas, datos de carácter vital, operaciones clave para el negocio, además de los protocolos permitidos en la red o tipo de hosts requeridos.

Este primer encuentro consiste en una plática con el usuario, donde se abordan todos los puntos anteriores, tratando de identificar los recursos y limitaciones de la organización.

La documentación de todos los aspectos anteriores permite prevenir costos y desarrollar un presupuesto adecuado.

B. Analizar las necesidades que cubrirá la red

Esta etapa consiste en analizar a los usuarios obtenidos en el punto anterior en conjunto con los requerimientos de la red, teniendo presente que una red debe ser capaz de proporcionar información adecuada en tiempos.

En este apartado se debe tratar de encontrar respuestas a las siguientes preguntas:

- ¿Qué aplicaciones se van a implementar?
- ¿A qué redes nuevas se va a acceder?
- ¿Cuáles son los criterios de éxito?
- ¿Qué nivel de fiabilidad deben tener las redes?

C. Documentar e implementar las redes lógicas y físicas

Posteriormente al análisis de los requisitos es fundamental, definir una topología que cubra las expectativas planteadas, una de éstas, es la arquitectura ethernet, definida en el estándar 802.3 de la IEEE, Instituto de Ingenieros en Electrónica y Electricidad (Institute of Electrical and Electronics Engineers).

Es vital determinar la carga de tráfico de una red, antes de desarrollar la estructura y adquirir el hardware, esto es determinar el tamaño de los paquetes o tamaño de los archivos en bytes por segundo que hay que transmitir sobre la red.

En ocasiones existen transferencias de archivos de grandes tamaños, lo cual ocasiona congestión en ciertos puntos como:

- Acceso a Internet.
- Las computadoras que cargan software de un sitio remoto.
- Transmisiones de video e imágenes.
- Acceso a bases de datos centrales.
- Servidores de archivos de los departamentos.

Para estimar esta carga de tráfico, es indispensable considerar los puntos críticos de actividad.

¿CÓMO DISEÑAR LA TOPOLOGÍA DE CAPA 1?

Los elementos fundamentales del diseño de una red, se pueden dividir en tres categorías simples, basadas en el modelo de referencia OSI: la capa de red, la capa de enlace y la capa física.

La capa física controla la forma en que se transmiten los datos entre el nodo de origen y el de destino, por lo tanto el tipo de medio y la topología elegida ayudarán a determinar la cantidad de datos que pueden viajar por la red, así como la rapidez con la que lo hagan.

El cableado físico, es el componente más importante en la construcción de las redes. Dentro del diseño se debe considerar el tipo de cable utilizado, regularmente cable coaxial, UTP o fibra óptica; así como la estructura general del cableado.

Es indispensable considerar las limitaciones relativas a las distancias, así como la evaluación de los puntos fuertes y débiles de cada una de las topologías, pues el funcionamiento de una buena red requiere de cimientos fuertes.

En esta línea, es necesario realizar auditorías de cableado, para identificar las áreas que requieren actualizaciones y recableados.

El cable de fibra óptica, debido a sus características debe ser utilizado en el backbone y el cable UTP categoría 6 en los trazados horizontales.

1.2 Análisis de requerimientos de hardware

1.2.1 Introducción

Las redes se componen de dos partes fundamentales: la red física y la red lógica.

La red física incluye el cableado, las tarjetas de red, las computadoras y todo el equipo de comunicación que se emplea para la transmisión de datos. Se considera como la parte visible.

La red lógica, consiste en la disposición lógica de estos componentes físicos, se consideran como las reglas que permiten a los dispositivos físicos trabajar en conjunto, por ejemplo: los protocolos de red, los servicios del Directorio de Netware de Novell, el método de Microsoft denominado Dominio, etc.

1.2.2 Componentes de red

Los diseñadores de redes deben considerar algunos componentes vitales de la red, como los mostrados en la siguiente lista:

a. Computadoras, también conocidas como estaciones de trabajo o terminales, son los equipos donde los usuarios trabajan.

b. Servidores, computadoras que comparten recursos como archivos, impresoras, comunicaciones o bien aplicaciones, (como procesadores de datos) con otros equipos. Los servidores no funcionan como estaciones de trabajo, ejecutan sistemas operativos especializados como NetWare, Windows NT, Unix y Linux. Hoy en día cada

servidor está dedicado a una función en específico como el correo electrónico o la de compartir archivos, etc.

Los servidores pueden clasificarse en dos tipos, cuya diferencia estriba en los servicios que proporcionan:

1. Servidores de empresa, este servidor da cobertura a todos los usuarios de la red ofreciendo servicios, como el correo electrónico o el DNS, Sistema de Nombres de Dominio (Domain Name System), indispensables dentro de una organización.

   El servidor de empresa debe estar colocado dentro del MDF, Armario de Distribución Principal (Main, Distribution, Facility), de manera que el tráfico de los servidores de empresa únicamente tiene que viajar en esta área y no ser transmitido por otras redes.

2. Servidores de grupo de trabajo, este tipo se servidor da cobertura, a un conjunto específico de usuarios, prestando servicios como el procesamiento de datos, compartir archivos y otros, necesarios únicamente para un sector de público determinado.

   Los servidores de grupo de trabajo, deben estar colocados dentro del IDF, Armarios de Distribución Intermedia (Intermediate Distribution Facilities), los cuales están próximos a los usuarios que acceden a las aplicaciones de estos servidores. De esta forma el tráfico de los servidores de grupo únicamente tiene que viajar por la infraestructura de la red hasta ese IDF, sin afectar a los usuarios de otro segmento de red. Ejemplos de servidores de grupos de trabajo son: servidores de ingeniería, servidores de departamentos, servidores de aplicaciones, etc.

c. Impresoras de red, se consideran como herramientas conectadas a la red de tal forma que más de un usuario pueda imprimir en ella.

d. Hub, dispositivo que proporciona a la red, un punto de conexión para todos los componentes.

e. Routers, dispositivo de interconexión de redes de computadoras que opera en la capa de red del modelo OSI, su función principal es la de interconectar segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red. Toman decisiones lógicas, con respecto a la mejor ruta para el envío de datos y posteriormente dirigen los paquetes hacia el segmento y puerto de salida adecuados.

f. Puentes, son equipos que enlazan dos redes, actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Únicamente el tráfico de una red que va dirigido a la otra cruza el dispositivo, permitiendo a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones.

g. Alambrado y cableado, el cableado debe cumplir con estándares establecidos como por ejemplo: el EIA/TIA 568, EIA/TIA 569 y EIA/TIA 606 para que la red funcione. Una red es tan eficaz como el cableado subyacente.

h. Tarjetas de red, una NIC, Tarjeta de Interfaz de Red (Network Interface Card) es una placa de circuito impreso que proporciona capacidades de comunicaciones de red hacia y desde una computadora personal. Se denominan también adaptadores de LAN, se conectan a la placa madre y proporcionan un puerto para conectarse a la red.

   Esta tarjeta puede ser diseñada como una tarjeta Ethernet, como una tarjeta Token Ring o como una tarjeta FDDI, es decir una Interfaz de Datos Distribuidos por Fibra Óptica (Fiber Distributed Data Interface).

Una NIC, se comunica a la red empleando una conexión serie y con la computadora a través de una conexión en paralelo.

Una tarjeta de interfaz de red, requiere de al menos tres aspectos para trabajar correctamente:

1. IRQ, Línea de Petición de Interrupción (Interrupted Request) es una señal que informa a la CPU, Unidad Central de Procesamiento (Central Processing Unit) que ha ocurrido un evento que requiere de su atención. Las IRQ, se envían sobre una línea de hardware al microprocesador, de manera similar a cuando se presiona una tecla en el teclado, la CPU debe llevar el caracter del teclado a la RAM.
2. Dirección de entrada y salida, una dirección de entrada y salida es una posición de memoria empleada para introducir o recuperar datos de una computadora mediante un dispositivo auxiliar.
3. Dirección de memoria.

i. Switch, dispositivo de interconexión que opera en la capa 2 del modelo OSI, es decir, interconecta dos o más segmentos de red, funcionando de manera similar a los puentes, pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

j. Rack, bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones, son un armazón metálico con un ancho normalizado de 19 pulgadas. El armazón cuenta con guías horizontales donde puede apoyarse el equipamiento, así como puntos de anclaje para los tornillos que fijan dicho equipamiento al armazón. La distancia entre cada guía horizontal o "estante" también está normalizada y se denomina altura o simplemente por la letra U. Todos los equipos deben adaptar su altura a un múltiplo de dicha unidad.

1.3 Análisis de requerimientos de software

La red lógica es lo que los usuarios observan, cuando se encuentran laborando, en sus escritorios. Son colecciones de recursos como el espacio en disco duro, impresoras, aplicaciones a las que una computadora no tendría acceso si no estuviera conectada a una red. La red lógica no es física, es el resultado de la organización física.

La red lógica incluye por ejemplo: los protocolos de red (formas especiales para comunicarse entre las computadoras), los servicios especiales como el NetWare de Novell (también conocidos como Servicios del Directorio, cuyo objetivo es organizar las computadoras e impresoras en red), herramientas de monitoreo, entre otras.

Un gran número de servicios relacionados con las redes y paquetes de software caen en el área lógica de una red. El software tiene como propósito interactuar con la computadora o el dispositivo de red, por lo que es necesario realizar un análisis minucioso de las necesidades del usuario. Entre las principales aplicaciones de software que podemos encontrar en las redes destacan:

a. Navegadores, un navegador es un software que interpreta HTML, Lenguaje de Marcado de Hipertexto (HypertText Markup Language) empleado para codificar el contenido de las páginas Web, permite mostrar gráficos y reproducir sonidos, películas y otros archivos multimedia. Esta herramienta actúa en nombre de un usuario realizando algunas de estas actividades:
   - Contactando con un servidor Web.

- Solicitando información.
- Recibiendo información.
- Mostrando resultados en pantalla.

b. Plug-ins, existen un gran número de archivos propietarios, es decir, su formato es controlado por una empresa, de manera que los navegadores Web estándar no los pueden interpretar y se requiere configurarlos.

   Los plug-ins, son aplicaciones que trabajan en conjunto con el navegador para ejecutar el programa requerido en la visualización de esos archivos propietarios.

   Entre los plug-ins propietarios encontramos:

   - Flash/Shockwave, reproduce archivos multimedia: texto, gráficos, video, animación y sonido integrado, realizados con programas como Macromedia Authorware, Director y Flash.
   - QuickTime, reproduce películas y sonidos almacenados en el formato RealAudio.
   - RealPlayer G2, reproduce archivos de películas con alta resolución almacenados en formato Real Player.
   - RealAudio, reproduce archivos de películas almacenados en el formato RealAudio.

c. Aplicaciones ofimáticas, los equipos de cómputo también se emplean para realizar tareas administrativas, para lo cual requieren aplicaciones ofimáticas que incluyen software de cálculo, procesamiento de texto, gestión de bases de datos, para presentaciones y un administrador de información personal que incluye un programa de correo electrónico.

d. Antivirus, software cuyo objetivo es mantener estable el equipo de cómputo, ante los virus informáticos. La elección de un antivirus requiere el análisis de características como:

   - Capacidad de detección y desinfección, esto es la facultad para detectar una gran cantidad de código malicioso dentro de los equipos de cómputo.
   - Heurística, capacidad de detectar virus desconocidos a través de sondeos del sistema en busca de síntomas de infección, como pueden ser fechas extrañas en archivos, programas residentes en memoria, configuración extraña del sistema.
   - Velocidad, se refiere a la cantidad de tiempo utilizada para escanear los datos.
   - Actualización, capacidad de mantener bases víricas o librerías actualizadas para tener el antídoto a los virus más recientes, servicios de atención, es decir el servicio técnico en línea.

   Entre los principales ejemplos de antivirus actuales encontramos:

   - F- Secure.
   - Panda Software.
   - Symantec Norton Antivirus.
   - Anyware AntivirusMcAfee Virus Scan.

e. Software de administración, el software para la administración de la información, está compuesto de una base de datos compleja, con una computadora propietaria que permite que un administrador de red, observe y modifique las configuraciones de las estaciones de trabajo de los usuarios.

La mayor parte del software de administración requiere que cada sistema tenga un agente, que es la parte del software que interactúa con la base de datos administrativa y debe estar instalado en la estación de trabajo, a veces los agentes pueden instalarse automáticamente a medida que el usuario ingresa a la red.

Los administradores de red que instalan y utilizan de manera rigurosa el software de administración de la configuración, tienen un mejor control de las estaciones de trabajo de sus usuarios. Es posible obtener un inventario de la red de manera rápida e instalar y actualizar software para muchos usuarios simultáneamente, de igual forma es posible instalar alarmas que registren un acceso no autorizado, lo cual ayuda a tener un control sobre el robo de hardware y la instalación de software no autorizado por el usuario.

1.4 Análisis de direccionamiento lógico

1.4.1 Modelo de referencia OSI

Los modelos de red emplean capas para simplificar las funciones de trabajo en red. La separación de estas funciones, se denomina estructuración en capas, de esta manera un modelo estructurado en capas sirve para entender e implementar las comunicaciones entre computadoras.

Al emplear capas, el modelo de referencia OSI simplifica las tareas que necesitan llevar a cabo dos computadoras para comunicarse entre sí. Cada capa se centra en unas funciones específicas, permitiendo así al diseñador de redes elegir los dispositivos de red y las funciones de trabajo en red más apropiados para cada capa.

Esta división de las funciones de trabajo en red, incluyen las siguientes ventajas:

a. Las capas dividen los aspectos del funcionamiento de las redes en elementos menos complejos.
b. Las capas definen interfases estándar para la compatibilidad plug-and-play.
c. Las capas permiten a los ingenieros concentrar sus esfuerzos de diseño y desarrollo en funciones modulares.
d. Promueven la simetría de las funciones modulares.
e. Impiden que los cambios en un área afecten a otras áreas de forma que cada una de ellas, pueda desarrollarse independientemente.
f. Finalmente las capas dividen la complejidad del trabajo en red, en operaciones separadas fáciles de aprender.

Las capas del modelo OSI, Interconexión de Sistemas Abiertos (Open Systems Interconnection) fueron creadas por la ISO, Organización Internacional de Estándares (International Organization for Standarization) en 1974 con el propósito de abrir la comunicación entre diferentes sistemas sin recurrir a cambios a la lógica y fundamentos del hardware y software. El modelo de referencia OSI no es un protocolo, es un modelo para entender el diseño de una arquitectura de red que sea flexible, robusta e interoperable.

El modelo OSI está conformado en 7 capas, las cuales se observan en la Tabla No. 1.1.

Capa	Nombre
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Física

Tabla No. 1.1 Modelo OSI

1. Capa física, se ocupa de la transmisión de bits a través de un canal de comunicación, así como la definición de las características del mismo canal. Regula aspectos de la comunicación como el tipo de señal: analógica o digital, el esquema de codificación, sincronización de los bits, tipo de modulación, tipo de enlace: punto-punto o punto-multipunto, el modo de comunicación (duplex, half-duplex o simplex), la tasa de bits (número de bits por segundo), la topología empleada y en general, todas las cuestiones eléctricas, mecánicas, señalización y de procedimiento en la interfaz física (cables, conectores, enchufes,) entre los dispositivos que se comunican.

2. Capa de enlace de datos, ensambla los bits de la capa física en grupos de tramas (protocolos de red) y asegura su correcto envío. También es la encargada de la verificación de errores de la capa física, así en caso de que ocurra un error en los bits la capa de enlace en el receptor se encarga de avisarle al transmisor que efectúe una re-transmisión, por lo tanto la capa de enlace se encarga también del control de flujo de los datos.

   La capa de enlace de datos se divide en dos subcapas:

   - LLC, Control del Enlace Lógico (Logical Link Control) define como los datos son transferidos sobre el cable y provee servicios de enlace de datos a las capas superiores.
   - MAC, Control de Acceso al Medio (Medium Access Control) establece quien puede usar la red cuando múltiples dispositivos están intentando acceder simultáneamente, ejemplos de MAC son las técnicas: token passing, Ethernet CSMA/CD, etc.

3. Capa de red, es la responsable del envío fuente a destino de los paquetes, es decir, se asegura que cada paquete llegue desde su punto inicial hasta su punto final.

   Si dos sistemas están conectados en el mismo enlace, no existe la necesidad de la capa de red. Sin embargo, si dos sistemas están en diferentes redes (enlaces) será necesaria una capa de red para culminar la entrega fuente a destino del paquete.

   Las responsabilidades específicas de la capa de red incluyen:

   a. Direccionamiento lógico, el direccionamiento físico implementado en la capa de enlace de datos manipula el problema del direccionamiento localmente, pero si un paquete pasa de la frontera de la red, se necesita otro sistema de direccionamiento para ayudar a distinguir los sistemas fuente y destino. La capa de red agrega un encabezado al paquete que llega de la capa superior, que entre otras cosas, incluye la dirección lógica del origen y del destino.

   b. Enrutamiento, cuando redes independientes o enlaces son conectados juntos para crear una interred (por ejemplo una red de redes como Internet) o una red

grande, los dispositivos llamados routers, enrutan los paquetes a su destino final. Una de las funciones de la capa de red es la de proveer este mecanismo.

4. Capa de transporte, es la responsable del envío fuente a destino (extremo-extremo) del mensaje entero. Mientras que la capa de red supervisa el envío extremo-extremo de paquetes individuales, no reconoce cualquier relación entre esos paquetes. Trata a cada uno independientemente, sin embargo cada pieza pertenece a un mensaje separado. Por otro lado, la capa de transporte, asegura que el mensaje completo arribe intacto y en orden, supervisando el control de flujo y control de error al nivel de la fuente-destino.

   Las funciones que realiza la capa de transporte consisten en: asegurar un servicio confiable y el romper el mensaje (de la capa de sesión) en pequeños paquetes, además de asignar un número de secuencia y enviarlos.

5. Capa de sesión, los servicios proveídos por las primeras tres capas (física, enlace de datos y red) no son suficientes para algunos procesos. La capa de sesión es controladora de diálogos de la red. Establece, mantiene y sincroniza la interacción entre los sistemas.

6. Capa de presentación, se encarga de la sintaxis y la semántica de la información intercambiada entre dos sistemas. Dentro de las tareas específicas se encuentran: la traducción de códigos, la cifrado y la compresión.

7. Capa de aplicación, permite al usuario acceder a la red. Provee de las interfases de usuario y soporte para servicios tales como correo electrónico, transferencia de archivos, administración de bases de datos compartidas y otros tipos de servicios distribuidos.

1.4.2 TCP/IP vs. OSI

La suite de protocolos de TCP/IP está compuesta de 4 capas que no corresponden exactamente a las capas del modelo OSI, ver Tabla No. 1.2.

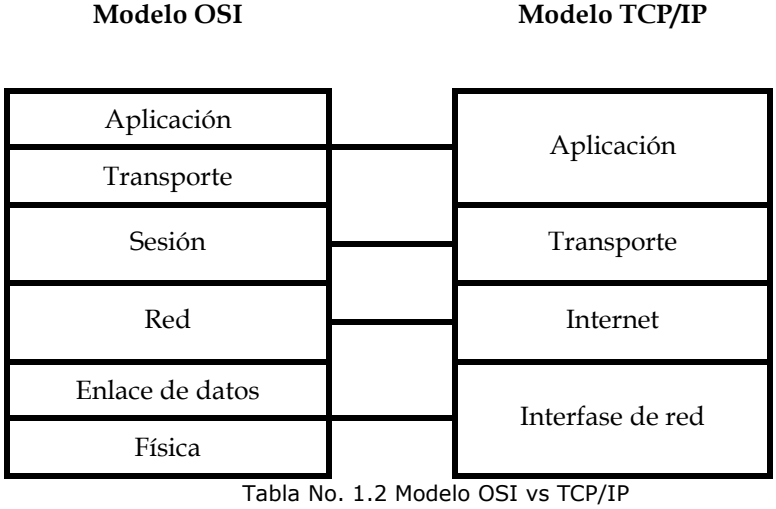


Tabla No. 1.2 Modelo OSI vs TCP/IP

a. Capa de interfase de red, comprende la capa física y de enlace de datos del modelo OSI, se centra en el envío de datos hacia otros dispositivos. Se debe conocer la parte física de la red para formatear los datos correctamente y conocer sus desventajas y requerimientos.

b. Capa de internet, abarca la capa de red del modelo OSI, proporcionando la funcionalidad para las comunicaciones entre redes a través de routers. Para realizar esto la capa de Internet depende del protocolo IP, Protocolo de Internet (Internet Protocol), el protocolo más importante de la suite TCP/IP.

c. Capa de transporte, esta capa es responsable de las comunicaciones extremo-extremo de la red, utiliza dos protocolos para realizar esta tarea: TCP, Protocolo de Control de Transmisión (Transmission Control Protocol) y UDP, Protocolo de Datagrama de Usuario (User Datagram Protocol).

d. Capa de aplicación, esta capa incluye todas las aplicaciones que hacen uso de la capa de transporte para enviar y recibir datos tales como RSH, Shell Remoto (Remote Shell); REXEC, Ejecución Remota (Remote Execute); TELNET, Emulación de Terminal (Terminal Emulation); FTP, Protocolo de Transferencia de Archivos (File Transfer Protocol), rlogin, DNS; NFS, Sistema de Archivos de Red (Network File System), etc.

1.4.3 Direccionamiento lógico

Se lleva a cabo en la capa de Internet del TCP/IP, la cual es responsable de las funciones de conmutación y enrutamiento de la información (direccionamiento lógico), proporcionando los procedimientos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario conocer la topología de la red (forma en que están interconectados los nodos), con objeto de determinar la ruta más adecuada.

Las principales funciones que se llevan a cabo, consisten en dividir los mensajes, conocer la topología de la red en caso de que las máquinas no se encuentren en la misma red, encaminar la información, enviar los paquetes y ensamblar los paquetes en el host destino.

A. Direcciones MAC

Toda NIC independientemente del medio que utilice (cable, aire, microondas, etc.), dispone de un identificador llamado dirección MAC, el cual opera en la capa de enlace de datos del modelo OSI y es exclusivo para cada NIC.

Esta dirección MAC, está formada por 48 bits, de los cuales los 24 primeros identifican al fabricante y los 24 siguientes son el número de serie/referencia que el fabricante le ha asignado a la NIC.

Por ello se supone que no existen dos NIC con la misma MAC, o no deben de existir, aunque en el mercado existen tarjetas de red a las cuales se le pueden cambiar la MAC.

La forma de representar la dirección MAC es en hexadecimal por ejemplo, la siguiente dirección MAC se puede representar de esta forma: 3A-F5-CD-98-33-B1, o bien sin separadores: 3AF5CD-9833B1, siendo la primera opción, la forma más común de representación.

En toda trama de información que circula por una red, independientemente del medio sobre el que se transporte, habrá sido encapsulada en la capa de enlace de datos, con una MAC destino y una MAC origen, lo que permite que esta trama llegue al dispositivo con la MAC destino coincidente.

B. Direcciones IP

En el entorno TCP/IP, las estaciones finales se comunican con los servidores, los hosts u otras estaciones finales. Esto se produce por que cada uno de los nodos que utiliza el paquete de protocolos TCP/IP posee una dirección lógica de 32 bits única, conocida como dirección IP. Además en un entorno TCP/IP, cada red se ve como una dirección única. IP es la base para el enrutamiento de los datagramas, da una identificación global y única de los elementos de la red.

Algunas características del direccionamiento IP son:

a. El tráfico es enrutado a través de la red basado en una dirección, en vez de un nombre.
b. Cada compañía ubicada en la red es vista como una red única con una dirección única.
c. Para escoger la ruta se basa en su ubicación.
d. La ubicación es representada por una dirección.
e. Cada dirección tiene dos partes para la identificación de la red:
    1. Network ID que identifica a la red.
    2. Host ID que identifica al nodo, siendo única en la red y utilizada para diferenciar al nivel de red de la capa OSI y TCP/IP.

Los servidores, switches, routers y las computadoras, entre otros, son ejemplos de hosts, y por tanto deben ser direccionados. En otras palabras, todo equipo que necesite enviar y recibir datagramas o paquetes IP, se debe diferenciar con una dirección de host y debe ser ubicado en un segmento de red IP.

Pero a la vez la dirección está dividida en 4 octetos (grupos de ocho bits), representados por un número decimal de 0 a 255, separados por un punto.

Ejemplo:
Dirección IP: 192. 168. 1. 1

Network ID Host ID

B.1 Clases de direcciones

Las clases de direcciones sirven para definir los bits de la dirección IP que se van a destinar para red y host de acuerdo a las cantidades requeridas por cada uno. Las direcciones IP son usadas para asignar networks ID´s, a las organizaciones y también son utilizadas para establecer la dirección de los Host ID.

Los tipos de clases de direcciones IP se muestran en la Tabla No. 1.3, así como algunas de sus características.

B.2 Enrutamiento

La capa de Internet del modelo TCP/IP, debe relacionar y hacer de interfaz con varias capas inferiores. Los routers deben ser capaces de manipular paquetes encapsulados en distintas tramas de nivel inferior, sin cambiar el direccionamiento de la capa 3.

La determinación de la ruta, es la decisión de qué ruta debería tomar el tráfico para atravesar la nube de redes. Para que la comunicación de la ruta sea verdaderamente práctica, una red debe presentar coherentemente las rutas disponibles entre los routers. Cada router cuenta con una dirección de subred, ésta puede ser utilizada en el proceso de enrutamiento. Por lo tanto las direcciones IP deben transportar información, que luego puede ser utilizada por parte de un proceso de enrutamiento.

C. Funcionamiento de un switch

Un switch es un dispositivo de trabajo en red situado en la capa de enlace de datos del modelo de referencia OSI. En esta capa además se encuentran las NIC que pueden ser inalámbricas y los puentes.

Los switches toman decisiones basándose en las direcciones MAC, así hacen que la LAN sea mucho más eficiente, mediante la conmutación de datos, sólo desde el puerto al cual está conectado el host correspondiente.

El propósito del switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. El switch es la conectividad y la regulación de tráfico en cada puerto pues conmuta paquetes desde los puertos (las interfases) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total.
Básicamente un switch es un administrador inteligente del ancho de banda, ver Figura 1.1.

Figura 1.1 Switch 3Com

D. Funcionamiento de un router

Los routers, ver Figura 1.2, retransmiten un paquete de un enlace de datos a otro. Para ello lleva a cabo dos funciones básicas:

a. Una función de determinación de ruta, que permite al router seleccionar la interfaz apropiada para reenviar un paquete.

b. Una función de conmutación, que permite al router aceptar un paquete en una interfaz y reenviarlo a una segunda interfaz.

Figura 1.2 Router Cisco

Clase de IP	# de Host (# Redes)	Notación	Submáscara de default	Network ID	Host ID	Rango de valores	Observaciones
A	6777214 (12	w.x.y.z	255.0.0.0	w.0.0.0	x.y.z	1-126 *	Están reservadas para las redes grandes. Son privadas, no son de dominio público.
B	65534	w.x.y.z	255.255.0.0	w.x.0.0	y.z	128-191	Esta clase es una de las más utilizadas para Internet, están reservadas para las redes de tamaño medio. Son privadas, no son de dominio público.
C	254	w.x.y.z	255.255.255.0	w.x.y.0	z	192-223	Están reservadas para las redes locales pequeñas. Son privadas, no son de dominio público.
D	Multicasting	w.x.y.z	-	No disponibl	-	224-239	Para servicios de difusión múltiple de datos
E	ara futuro us	w.x.y.z	-	No disponibl	-	240-255	Direcciones experimentales para uso Futuro.
*** El network 127.0.0.0 es reservada para pruebas de conectividad**							

Tabla No. 1.3 Clasificación de las direcciones IP

1.5 Diseño de políticas de cómputo

El diseño de las políticas de cómputo debe tener en cuenta los objetivos de proporcionar un buen servicio y un adecuado manejo de los equipos existentes en la organización.

Debemos contar con un servicio de cómputo integral y eficiente para las empresas, organizaciones gubernamentales o educativas; por ello se deben considerar todos los aspectos que proporcionen un servicio de calidad.

Al diseñar las políticas de cómputo debemos tener en cuenta los siguientes puntos:

De lo general:

- Se tiene que definir quiénes pueden hacer uso de los equipos de cómputo, es decir, que personal de la empresa, alumnos de la institución educativa, trabajadores, etc.
- Los horarios en que se les permitirá el uso.
- Los requisitos que deben cumplir: pertenecer a la empresa, estar inscritos en la institución, contar con alguna identificación.
- Si cuentan con permiso de instalar programas ajenos a los permitidos.
- Establecer los límites de responsabilidad sobre la información que se almacena en los discos duros.
- Dejar muy claro que, queda estrictamente prohibido inspeccionar, copiar y almacenar software que viole la ley de derechos de autor.
- El usuario que requiera conectar equipos personales a la red o periféricos a las computadoras, deberá contar con la autorización del responsable.

De los derechos:

- Hacer uso de los servicios de cómputo proporcionados.
- Respaldar información en su cuenta personalizada y/o unidades magnéticas extraíbles.
- Recibir el reglamento y una capacitación del mismo en la fecha y horario establecido por el responsable.

De las obligaciones:

- Presentar su credencial de identificación.
- Cerrar su sesión como usuario de la red.
- Vacunar sus discos.
- Apagar el equipo de cómputo, limpiar y acomodar su área de trabajo al término de su sesión.

De las restricciones:

- Introducir alimentos, bebidas, fumar y tirar basura.
- Introducir cualquier tipo de arma o estupefaciente.
- Introducir cualquier equipo ajeno a la organización.
- Transferir la cuenta asignada.

- Modificar los parámetros de configuración de hardware y software instalado.
- Mover el equipo de cómputo, mobiliario y cambiar los cables de conexión a la red.
- Conectarse a equipos no autorizados.
- Realizar trabajos con fines de lucro.
- Utilizar cualquier tipo de juego.
- Utilizar la infraestructura de la organización, empresa e institución para lanzar virus.
- Utilizar la infraestructura de la organización, empresa e institución para realizar ataques internos o externos.
- Acceder a información que pueda dañar la imagen: faltas a la moral y a las buenas costumbres.
- Ingresar a las áreas exclusivas del personal del área cómputo.

De las sanciones:

Las sanciones a que están sujetos los usuarios por incumplimiento de sus obligaciones e incurrir en las restricciones señaladas:

- Llamada de atención de manera verbal o escrita.
- Suspensión temporal de los servicios del centro de cómputo.
- Suspensión definitiva de los servicios del centro de cómputo.
- Reposición o pago de los bienes extraviados, destruidos o deteriorados.

1.6. Ética informática

La ética es la teoría o ciencia del comportamiento moral de los hombres en la sociedad, es decir, es la ciencia de una forma específica de conducta humana.

Para comprender más afondo lo que la ética es, requerimos retomar las raíces de los vocablos moral y ética.

La palabra moral procede del latín mos o mores, "costumbre" o "costumbres", en el sentido de un conjunto de normas o reglas adquiridas por hábito. La moral tiene que ver así con el comportamiento adquirido, o modo de ser conquistado por el hombre.

La palabra ética proviene del griego ethos, que significa análogamente "modo de pensar" o "caracter" en cuanto a forma de vida también adquirida o conquistada por el hombre.

La tecnología de información permite que grandes cantidades de datos estén al alcance de las empresas, organizaciones gubernamentales, educativas y de sus empleados. Aunque este acceso supone beneficios, la verdad es que también crea un enorme potencial para su mala utilización.

Para lograr una verdadera ética informática, tenemos que establecer que la ética informática no sólo toca un aspecto puramente moral, sino un compromiso con la profesión, que conlleva honestidad, compañerismo, confidencialidad, derechos, obligaciones, lealtad y responsabilidad, entre otros valores y actitudes.

En la Facultad de Ingeniería se han publicado las políticas en cómputo, por el subcomité de administradores de red, las cuales se detallan en el Anexo 1A.

1.6.1 Código de ética

Los seres humanos no sólo debemos tener presentes todos los conceptos y principios que involucran los términos ética y moral, pues es muy importante que al hablar de profesionistas y hombres de ciencia también tengamos presente el elemento ético, ya que es un componente inseparable de la actuación profesional, pues no debemos olvidar que toda profesión no es únicamente un modo de ganarse la vida y realizarse personalmente, sino que también tiene un fin social que consiste en servir adecuadamente a cada una de las necesidades que la sociedad debe satisfacer y posibilitar el bien común.

Por lo anterior es muy recomendable contar con un código de ética en cada profesión, que permita poner de manifiesto una serie de cualidades morales (honestidad intelectual, desinterés personal, decisión en la defensa de la verdad y en la crítica de la falsedad, etc.) cuya profesión asegure una mejor realización del objetivo fundamental (la búsqueda de la verdad) que preside la actividad de cada profesionista. Por ello, cada Universidad no sólo debe enseñar cómo ejercer una profesión, sino también debe inculcar en los estudiantes un patrimonio de valores, es decir una formación ética, que oriente al futuro profesionista a ejercer una profesión de forma adecuada.

El código de ética profesional es aplicable a toda persona que tenga una profesión asociada con la informática, la computación o los sistemas computacionales, sin importar la índole de su actividad o la especialidad que cultive tanto en el ejercicio independiente o cuando actúe como funcionario o empleado de instituciones públicas o privadas.

Por tal motivo se presentan un conjunto de códigos de ética en el Anexo 1A. Los códigos que se detallan en este anexo son el Código de Ética Profesional del Ingeniero Mexicano, el Código de Ética y Ejercicio Profesional de Ingeniería de Software de la IEEE, en particular el Código de Ética Universitario de la UNAM, Código de ética para la Facultad de Ingeniería en el ámbito informático, así como el Código de Ética Docente del Personal Académico de la Facultad de Ingeniería.

Capítulo 2

ORGANIZACIÓN

INTRODUCCIÓN

En el mundo actual, en donde la informática gira entorno al concepto de red, el trabajo de los administradores, es muy complejo. Su misión consiste en mantener en funcionamiento cada dispositivo que conforma la red.

Tradicionalmente la administración, ha partido de soluciones propietarias y cerradas, con un ámbito de acción limitado a una empresa o institución.

La evolución tecnológica ha permitido la entrada de múltiples fabricantes, generando que las redes actuales sean entornos heterogéneos, que requieren sistemas de administración que implementen estándares abiertos, con el objetivo de compatibilizar protocolos de información.

Dentro de las habilidades del administrador de redes, no sólo se incluyen las de análisis, diseño e implantación de redes, si no también aquéllas relacionadas con el correcto funcionamiento de la misma. Debe conocer cómo resolver los problemas cuando se presentan, decidir cuándo es necesario expandir o cambiar la configuración de la red, a fin de reunir las peticiones de modificación, entre otras más.

Cuando una red ya está trabajando, se deben realizar una serie de mecanismos documentados, para tener conocimiento de cómo se comporta la red, a través de sistemas de administración de redes, que satisfacen las expectativas de los usuarios, que consideran a la red como un entorno fiable, seguro, rápido y operativo.

Un sistema de administración de red tiene por objetivos:

- Administración de usuarios y software.
- Seguridad.
- Administración de fallos y rendimiento.
- Planificación.

La administración de una red, no se debe dejar a un lado en el diseño de un sistema de información ya que las ventajas se ven reflejadas en todos los niveles.

2.1 Modelo básico de administración de redes

2.1.1 Introducción a los modelos de administración de redes

Conforme la red crece, se convierte en un recurso vital que requiere ser administrado con eficiencia. Administrar una red significa definir la mejor topología para un adecuado comportamiento, con base en los objetivos de la organización y a las tecnologías disponibles, además de tener conocimiento y control sobre los eventos que permitan realizar proyecciones en el futuro.

El administrador de redes, debe dominar los aspectos que permitan definir una red de manera tal que ésta sea:

- Extensible, debe permitir su crecimiento de acuerdo a nuevos requerimientos.
- Transparente, no causar dificultades a los usuarios.
- Eficiente, conforme crece debe mantener una calidad en la transmisión de datos.
- Confiable, los datos transmitidos deben ser los esperados.

Dentro de las principales tareas de un administrador de redes, se encuentran:

- El monitoreo de la disponibilidad de la red.
- Mejorar la automatización.
- Vigilar el tiempo de respuesta.
- Seguridad.
- Redireccionar el tráfico.
- Contar con la capacidad de restablecimiento.
- Registrar usuarios.

Algunas actividades detrás de la administración de las redes incluyen:

- Controlar los medios corporativos, para que éstos ofrezcan un correcto rendimiento.
- Control de la complejidad, controlar tanto los componentes, como el número de usuarios, interfases, protocolos, proveedores, para no perder la pista de la red.
- Mejorar el servicio, los usuarios esperan mejores servicios aunque la red crezca.
- Balanceo de distintas necesidades, los usuarios deben contar con diversas aplicaciones para un nivel de soporte en específico, con especial interés en las áreas de rendimiento, disponibilidad y seguridad.
- Reducción de tiempos muertos, es importante considerar una alta disponibilidad de los recursos gracias al propio diseño redundante.
- Control de costos, vigilar y controlar la utilización de los recursos para que los usuarios estén satisfechos sin la necesidad de incrementar costos.

La interacción entre el administrador y el dispositivo administrado, añade tráfico a la red, por lo que es necesario que cuando estos elementos se incorporen, se cuenten con estrategias de monitoreo que aumenten el rendimiento de la red, considerando que los dispositivos administrados deben contar con la capacidad de responder a las peticiones del administrador, sin tener que descuidar sus funciones.

Para cumplir con tales objetivos, se requieren de estructuras normalizadas, como la que se muestra en la Figura 2.1, que permitan la administración de elementos heterogéneos de múltiples proveedores.

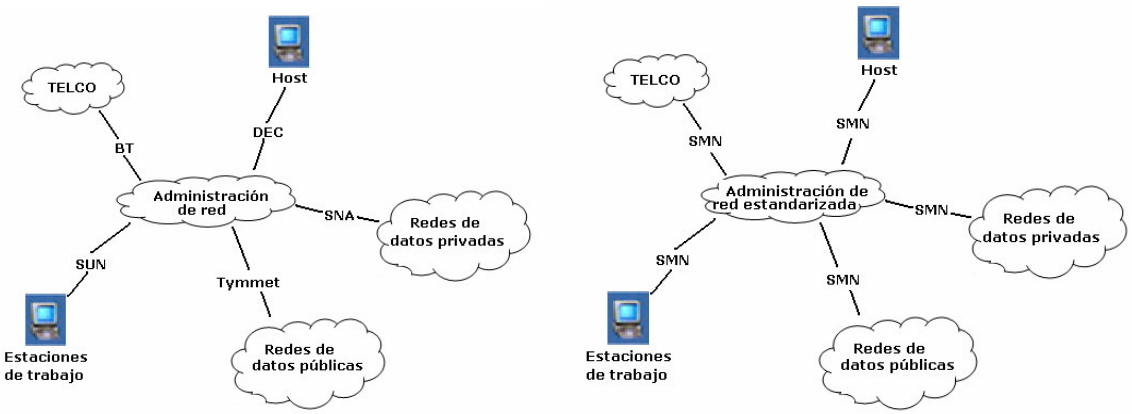


Figura 2.1 Arquitecturas normalizadas

La administración de redes se subdivide en administración de redes informáticas y administración de redes de telecomunicaciones, como se muestra en la Figura 2.2.

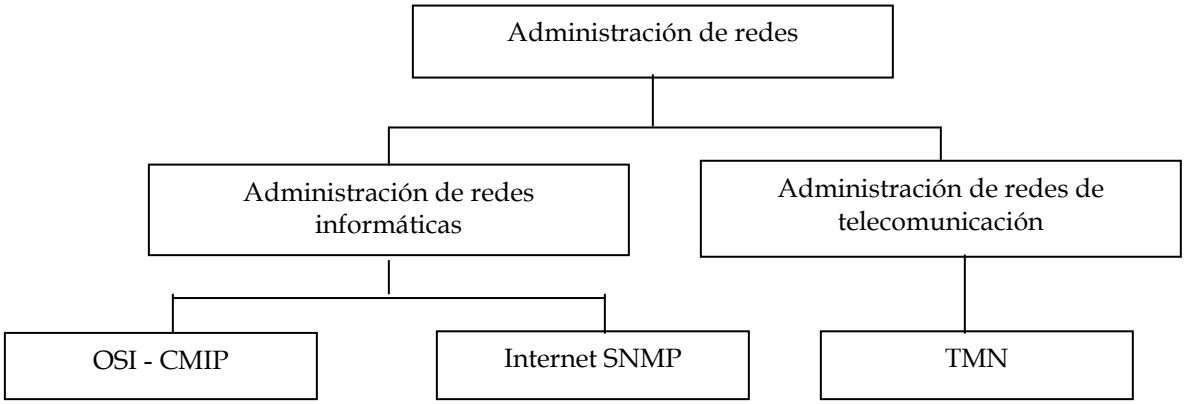


Figura 2.2 Administración de redes

Desafortunadamente la realidad, es que la administración de redes, suele verse como un costo adicional más que como una inversión a través de la cual, la organización podrá disminuir el gasto innecesario de capital y el control de costos de operación.

2.1.2 Arquitectura de administración de redes

La administración de red requiere de la habilidad para supervisar, comprobar, sondear, configurar y controlar los componentes hardware y software de una red. Dado que los dispositivos de red son distribuidos, el administrador debe ser capaz de recopilar datos, para la supervisión de entidades remotas, así como realizar cambios sobre ellas, para controlarlas. Para llevar a cabo actividades como las anteriores, se requiere de una arquitectura de sistemas de administración de redes, que se compone de los siguientes elementos:

a. Entidad administradora, aplicación con control humano que se ejecuta en una estación centralizada de administración de red, en el NOC, Centro de Operaciones de Red (Network Operations Center) este es el lugar donde se realiza la actividad de la

administración de la red, controla la recolección, procesamiento, análisis y/o visualización de la información de administración. En el NOC, se inician las acciones que controlan el comportamiento de la red y donde el administrador de red interactúa con los dispositivos que la conforman.

b. Dispositivo administrado, es una parte del equipamiento de la red, incluido el software, que reside en la red administrada. Un dispositivo administrado puede ser un host, un router, un switch, un puente, un hub, una impresora o un módem. En el dispositivo hay diversos objetos administrados, por ejemplo: el hardware como una tarjeta de interfaz de red y el conjunto de parámetros de configuración de los dispositivos hardware y software.

c. Base de información de administración, lugar donde se almacenan los datos referentes a los objetos administrados.

d. Agente de administración de red, proceso residente que se ejecuta en cada dispositivo administrado y que se comunica con la entidad administradora, realizando acciones locales bajo el control de los comandos de la entidad administradora.

e. Protocolo de administración de red, éste se ejecuta entre la entidad administradora y el dispositivo administrado permitiendo a la entidad administradora consultar el estado de los dispositivos e indirectamente realizar acciones en dichos dispositivos a través de los agentes.

Los agentes utilizan el protocolo de administración de red, para informar a la entidad administradora de eventos excepcionales, por ejemplo: el fallo de componentes o la trasgresión de los umbrales de rendimiento.

El protocolo de administración no controla por sí mismo, proporciona una herramienta con la que el administrador de red puede supervisar, comprobar, sondear, configurar, analizar, evaluar y controlar la red.

La anterior infraestructura, ver Figura 2.3 es la base de la implementación de diferentes modelos de administración de red.

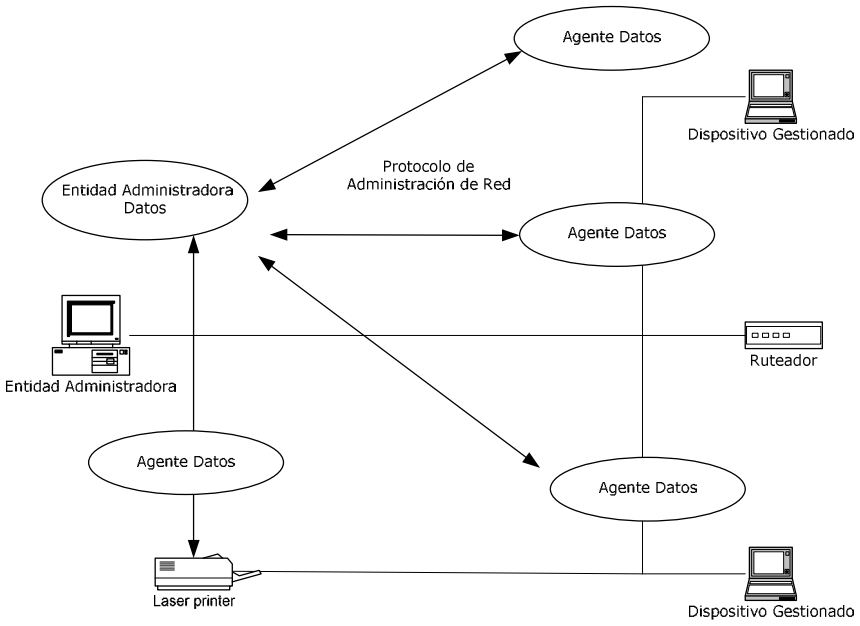


Figura 2.3 Infraestructura de administración de redes

2.1.3 Modelos de administración de redes, OSI

La ISO, creó un comité para generar un modelo para la administración de una red, éste se compone de 4 submodelos, planteados en la Figura 2.4, con el propósito de tener un entorno de trabajo estructurado.

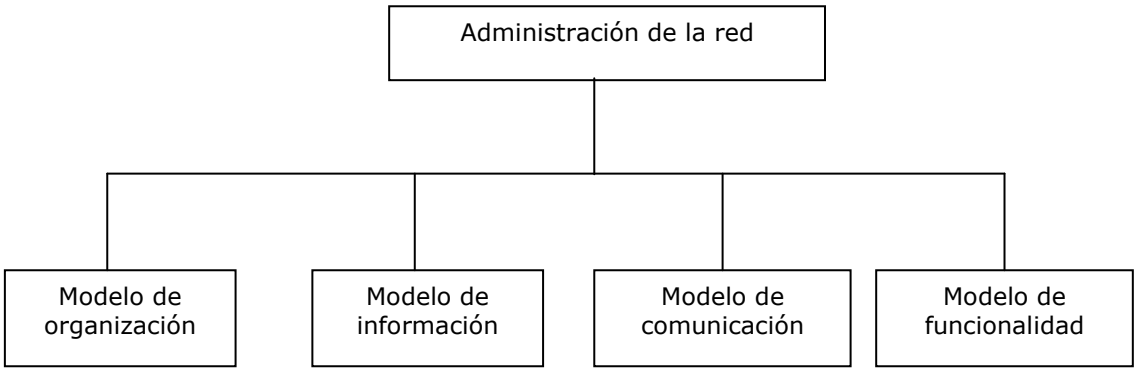


Figura 2.4 Modelo de administración de redes, propuesto por OSI

a. Modelo de organización, encargado de la descripción de los componentes de la administración de la red, esto es: el administrador, el agente, etc., junto con sus relaciones. La forma en como estos componentes interactúan da lugar a diferentes arquitecturas. Parte de una estructura de red dividida en dominios de administración. La división del entorno se realiza a partir de dos aspectos principales: políticas y funciones, por ejemplo: dominios con una misma política de seguridad u otras políticas como dominios geográficos, tecnológicos, etc.

b. Modelo de información, encargado de la estructura y el almacenamiento de la información de administración de los objetos de la red, la cual se almacena en una base de datos llamada MIB, Base de Información de Administración (Management Information Base). El estándar de la industria se centra en la SMI, Estructura de la Información de Administración (Structure Management Information) para definir sintaxis y semántica de la información que se almacena en la MIB.

c. Modelo de comunicación, encargado de verificar la forma en que se comunican los datos de administración entre el agente y el proceso administrador. Abarca los protocolos de transporte y aplicación junto con los comandos y respuestas.

d. Modelo de funcionalidad, el cual direcciona las aplicaciones de administración de red, que se encuentran en el NMS, Sistema de Administración de la Red (Network Management System). Este modelo es visto desde arriba hacia abajo, dividido en cuatro subcapas y es reconocido como el estándar, por lo que es de gran aceptación entre los distintos fabricantes, al ser una forma útil de describir los requerimientos de cualquier sistema de administración de red. Incluye las cinco áreas en las que se divide la administración de redes, también denominadas FCAPS:

   - Fallo (Fault).
   - Configuración (Configuration).
   - Contabilidad (Accounting).
   - Rendimiento (Performance).
   - Seguridad (Security).

Para permitir la interoperabilidad entre las distintas plataformas de redes, los estándares de administración de redes, han obligado a los fabricantes de los dispositivos de red a adaptarse a ellos.

2.2 Modelo de administración de redes de telecomunicaciones, TMN

2.2.1 Introducción al modelo de administración TMN

Las redes y servicios de telecomunicaciones surgen para cubrir la necesidad de transportar información entre varias localidades, separadas físicamente. Por ello, la infraestructura necesaria para prestar estos servicios, se encuentra distribuida en un espacio geográfico que puede abarcar miles de kilómetros. Por lo anterior, es vital disponer de sistemas de soporte que ayuden a realizar todas las actividades de administración de las redes y servicios.

Una red de telecomunicaciones se compone de equipos físicos, que incluyen su software asociado, el cual se encarga de las funciones que constituyen elementos lógicos, éstos sirven para elaborar las capas de la red de transmisión. De manera que una red de telecomunicaciones se puede representar por medio de 3 capas lógicas:

a. Capa de equipos, engloba el equipamiento físico y su software, que constituyen una entidad en la red, que cumplen funciones lógicas.
b. Capa de transmisión de red, ofrece el soporte de transmisión para la información, se constituye a partir de los elementos lógicos proporcionados por las entidades de red.
c. Capa de servicios, ofrece servicios de enlace punto a punto permanentes o conmutados, así como una transmisión por circuito o por datagrama (paquete). Estos servicios son los que el operador vende a sus clientes.

Para administrar los elementos físicos y lógicos de una red de telecomunicaciones, se definió el TMN, Red de Administración de Telecomunicaciones (Telecommunication Management Network) que proporciona el marco modular en el que las operaciones, las aplicaciones informáticas y los equipos se comunican de forma segura y normalizada.

El desarrollo de TMN, se vio motivado por las siguientes razones:

a. Creciente heterogeneidad en la tecnología para la construcción de redes de telecomunicación.
b. Coexistencia de redes analógicos-digitales.
c. Posibilidad de introducir nuevos servicios de alta calidad.

2.2.2 Modelo de administración TMN

Estándar definido en la serie M.300 de la ITU-T, Unión Internacional de Telecomunicaciones (International Telecommunication Union) que presenta un conjunto de requisitos arquitecturales, que deben cumplir las redes de administración de telecomunicaciones.

Esta norma busca la interconexión de diferentes sistemas y equipos, permitiendo el intercambio de información de administración, a través de diferentes interfases normalizadas.

Las empresas telefónicas adoptan el modelo de comunicaciones TMN, como una manera de estructurar lógicamente el soporte a sus actividades.

TMN, tiene la ventaja de separar la administración de toda una red en diferentes capas, para facilitar la administración de redes, desde lo más básico (administración de dispositivos de red en la parte inferior) hasta lo más complejo (estrategias de negocio en la parte superior). Sin embargo presenta el problema de que no integra los diferentes procesos de instalación, control y facturación de nuevos servicios.

A. Estructura general de TMN

El modelo TMN se basa en el modelo OSI, de esta manera se definen 4 arquitecturas que lo conforman y las cuales se definen a continuación:

a. Arquitectura funcional, define los bloques funcionales de una TMN y sus puntos de referencia, estos bloques representan funciones apropiadas requeridas por TMN y que son ejecutadas por elementos de la arquitectura física de TMN.

   El estándar M.3010, define 5 tipos de bloques funcionales que se muestran en la Figura 2.5.

   - WFS, Estación de Trabajo (Workstation Function) define las funciones de interacción con el usuario.
   - QAF, Bloque de Función de Adaptación (Q Adaptor Function) define funciones que permiten incorporar a la red de administración TMN, entidades.
   - NEF, Bloque de Función de Elemento de Red (Network Element Function) incluye funciones de los equipos de red a administrar.
   - OSF, Bloque de Función de Sistemas de Operación (Operations Systems Functions) procesa la información de administración para monitorear, coordinar y controlar la red de telecomunicaciones.
   - MF, Bloque de Función de Mediación (Mediation Function) establece las funciones de mediación entre OSF's y NEF's, que preparan la información de administración para que satisfaga los requisitos de ambos. Las funciones de medición pueden implicar: filtrado, almacenamiento, adaptación, condensado, etc.

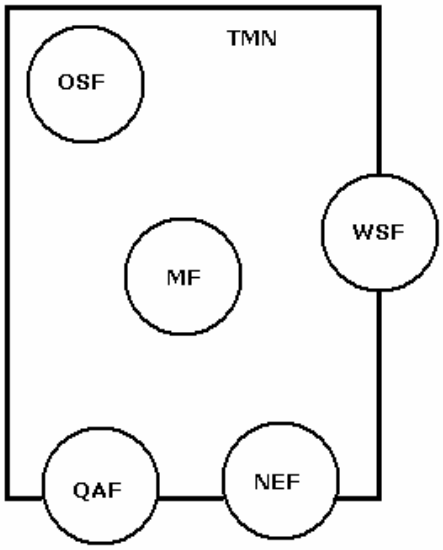


Figura 2.5 Bloques funcionales de la arquitectura funcional

b. Arquitectura de la información, la información de administración se modela con base en objetos administrados.

Un recurso puede ser representado por varios objetos, cada uno proporcionando una perspectiva diferente.

b.1 Objetos administrados, se definen como abstracciones de los recursos físicos o lógicos a ser administrados, con el fin de monitorear la red y prevenir anomalías en su operación, ver Figura 2.6. Un objeto administrado se caracteriza por:

- Atributos que posee.
- Operaciones que se efectúan sobre él.
- Comportamiento que presenta.
- Notificaciones que emite.

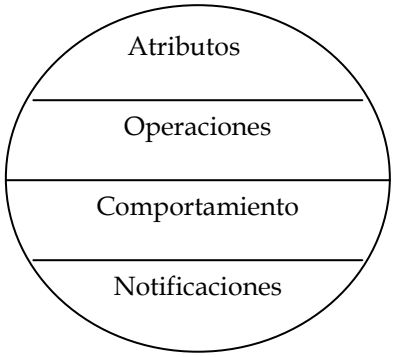


Figura 2.6 Estructura de un objeto administrado en TMN

Un objeto administrado no corresponde a un elemento de red, representa uno de los componentes importantes de un elemento de red, por ejemplo: la unidad de control de un circuito o un recurso lógico como el estado de un elemento físico de la red. Cada objeto administrado tiene un nombre único, cuya condición cambia en función del tiempo.

El objeto administrado es una visión parcial del recurso, donde sólo se muestran los aspectos de interés para el sistema de administración.

b.2 GDMO, Guías para la Definición de Objetos de Administración (Guidelines for the Definition of Management), la definición de objetos administrados se realiza a través del estándar X.7222 que proporciona la sintaxis con la que se especifican las MIB's de los equipos TMN.

b.3 Modelo administrador-agente, el modelo TMN identifica claramente dos papeles dentro de los procesos de administración:

- Administrador, que inicia las operaciones de administración y recibe notificaciones del agente.
- Agente, mantiene los objetos administrados asociados, respondiendo a las operaciones iniciadas por el administrador emitiendo las correspondientes notificaciones.

En este modelo el administrador, no se comunica directamente con los recursos administrados, sino a través de otra aplicación llamada agente, que es la que tiene la responsabilidad directa sobre ellos, como se muestra en la Figura 2.7.

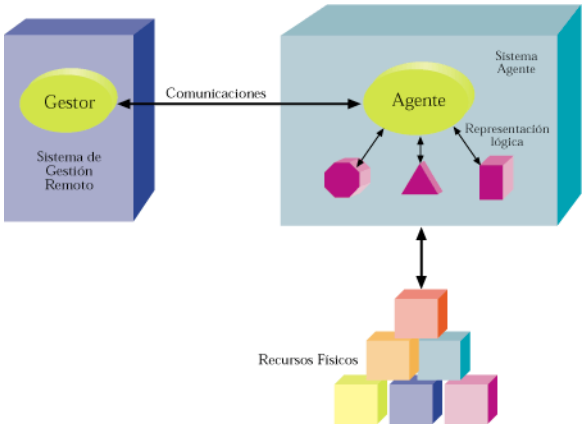


Figura 2.7 Modelo administrador-agente en TMN

b.4 MIB, Base de Información de Administración (Management Information Base) consiste en una base de datos relacional, que contiene información de los datos pertenecientes a los objetos administrados. Cada uno de los agentes tiene su propia MIB, que satisface la sintaxis de SMI. La MIB forma la base común de conocimiento entre el sistema y los agentes de administración.

El sistema de administración realiza operaciones sobre los objetos administrados representados en la MIB y el agente se encarga de traducir estas operaciones en acciones sobre los recursos físicos de la red.

b.5 Protocolos en TMN, el administrador y el agente se comunican a través de protocolos "Q", estándares construidos de acuerdo al modelo OSI. Los componentes de un protocolo Q son:

- Interfase de aplicación, con una estructura comando respuesta. Los elementos esenciales de la interfase de aplicación TMN son similares a la administración OSI/CMIP e incluyen: CMISE, ROSE, SMASE, ACESE y FTAM.
- Protocolo de aplicación, séptima capa del modelo OSI.
- Protocolo de soporte.
- Protocolo de red.

c. Arquitectura física, describe los elementos físicos de un sistema de administración de red TMN, definiendo reglas para sus relaciones. El estándar M.3010, define los siguientes elementos físicos en donde se implementan las funciones de administración:

- OS, Sistema de Operaciones (Operations System).
- WS, Estación de Trabajo (Workstation).
- NE, Elemento de Red (Network Element).
- DCN, Red de Comunicación de Datos (Data Comunication Network).
- MD, Dispositivo de Mediación (Mediation Device).
- QA, Adaptador Q (Q Adaptador).

c.1 Interfases, los bloques físicos se interconectan entre sí, mediante interfases estándares, que son implementaciones de un punto de referencia que liga dos bloques funcionales físicamente separados. Para nombrar a los puntos de referencia, se usa una notación en letras mayúsculas.

d. Arquitectura lógica en capas, las áreas de administración TMN siguen el modelo FCPAS de la organización OSI, como se muestra a continuación:

- Administración de fallos.
- Administración de configuración.
- Administración de factibilidad.
- Administración de prestaciones.
- Administración de seguridad.

Estas funciones se pueden estructurar lógicamente en capas que corresponden a diferentes niveles de abstracción, los cuales se representan generalmente a través de una pirámide, ilustrada en la Figura 2.8.

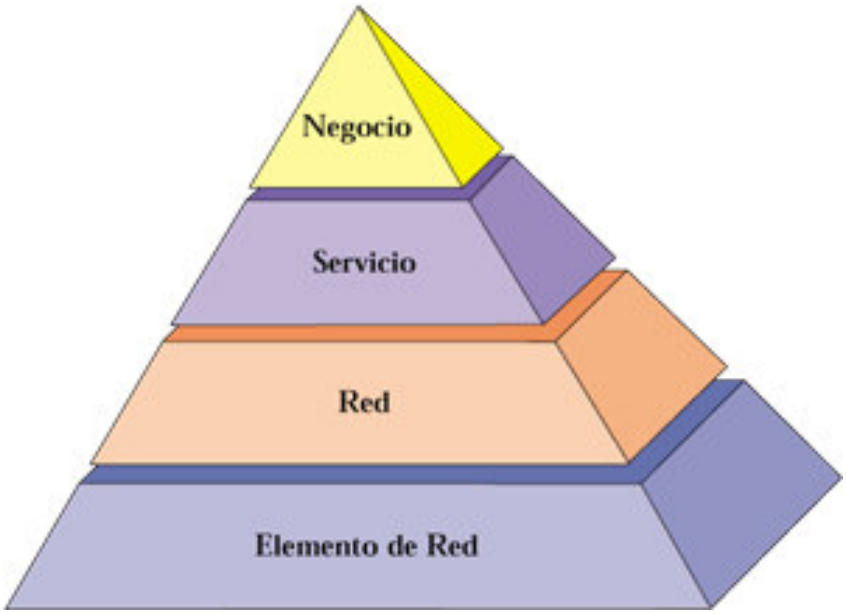


Figura 2.8 Niveles de administración en TMN

d.1 Nivel de administración de elemento de red, capa de red más baja que incluye funciones propias de los elementos individuales, controla y coordina un subconjunto de elementos de red. Se encarga de todos los aspectos relacionados con switches, sistemas de transmisión, etc., considerados como elementos aislados. Incluye las funciones que proporcionan información en formato TMN del equipo de red, así como las funciones de adaptación para proporcionar interfases TMN a elementos de red no TMN.

d.2 Nivel de administración de elementos, distingue elementos individuales, administrando un conjunto de ellos. Ofrece una vista consolidada del dominio de administración, hacia un nivel de red.

d.3 Nivel de administración de red, consolida las vistas parciales de los EMS, Sistemas Administradores de Elementos (Element Management System). No da una visión interna de los elementos, controla y coordina la visión de la red de los elementos individuales. Proporciona, elimina o modifica las capacidades de la red para dar soporte a los servicios al cliente. Interactúa con la administración de servicios en temas de prestaciones, utilización, etc. Es responsable del transporte de la información entre dos extremos y de asegurar que ésta se realiza de forma correcta. Cualquier error o problema que se detecte en este nivel y que afecte a

los servicios que se prestan a los usuarios, debe ser notificado hacia el nivel de gestión de servicio.

d.4 Nivel de administración de servicios, administra de manera integrada los servicios que ofrece la red, incluye aspectos contractuales de los servicios a clientes, se considera como una interfaz con el cliente. En este nivel se administran las peticiones de servicio, los QoS, Calidad de Servicio (Quality of Service).

d.5 Nivel de administración de negocios o comercial, es el nivel más alto que incluye las estrategias de negocios que definen las acciones para conseguir el retorno de la inversión, considerando la responsabilidad global sobre la administración de la organización. Considera la toma de decisiones estratégicas, políticas e inversiones, por ejemplo la interfaz entre el sistema de contabilidad del patrimonio de la organización y el sistema de inventario.

2.3 Modelo TOM y eTOM

La industria de las telecomunicaciones está transformándose, de la conmutación de circuitos a la conmutación de paquetes. El cambio en el paradigma de la tecnología, combinado a la necesidad de los proveedores de servicios de telecomunicaciones, de contar con procesos automatizados bien definidos, han motivado la creación de modelos de negocios, que les permitan mantenerse estables, en un mercado altamente competitivo.

Una de las iniciativas del TMF, Foro de Administración de Telecomunicaciones (TeleManagement Forum) es la definición y desarrollo de un modelo de procesos de negocios que permite la reingeniería de procesos dentro de las empresas SP, Proveedoras de Servicios de Telecomunicaciones (Service Provider).

El modelo inicial TOM, Mapa de Operaciones de Telecomunicaciones (Telecom Operations Map) proporciona una estructura de referencia para las operaciones y administración en las compañías de telecomunicaciones. Su objetivo era la unificación de los procesos, resaltando las entradas, salidas y actividades requeridas para la administración de las operaciones, además proporciona la definición de una terminología común, que facilita las negociaciones entre clientes y proveedores.

El TMF decidió expandir el modelo TOM a la estructura actual eTOM, debido a dos motivos principales:

a. La necesidad de contar con un modelo que representara el funcionamiento completo de los procesos de una organización SP.

b. El modelo TOM, no proporcionó bastante impacto en la administración de los procesos de negocios, despertando la necesidad de procesos integrados, sin incrementar el grado de complejidad en las relaciones de los proveedores de servicios.

El diagrama que representa los componentes fundamentales del modelo TOM, se muestra en la Figura 2.9.

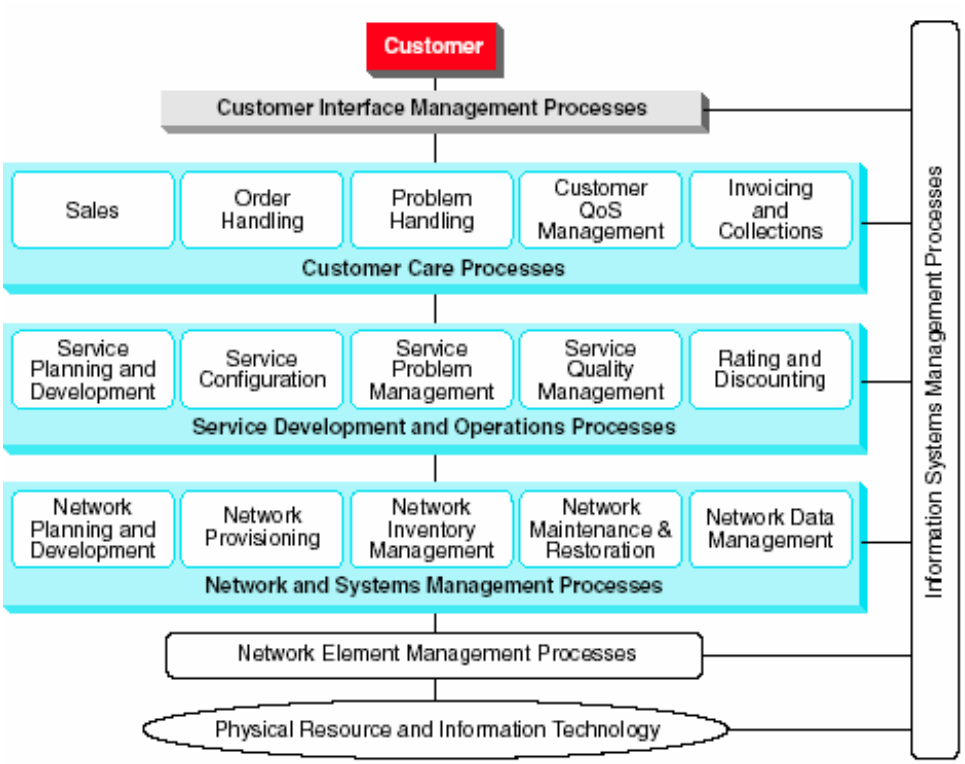


Figura 2.9 Modelo TOM, Mapa de Operaciones de Telecomunicaciones

El desarrollo de eTOM, engloba los procesos de operaciones considerados en TOM, dentro de una estructura de procesos de negocios comprensibles, que incluyen la totalidad de la empresa.

El eTOM, es un modelo de procesos de negocio, una estructura generalizada que describe todos los procesos requeridos por un SP, analizándolos en diferentes niveles de detalle. Para estas empresas, sirve como un punto de partida para el control de procesos y provee de un marco de referencia para la reingeniería de procesos, de acuerdo a las necesidades, relaciones internas, alianzas y acuerdos de trabajo. eTOM resalta las funciones requeridas, entradas y salidas.

El propósito de eTOM es proporcionar una visión que permita competir exitosamente a través de la implementación de la administración de procesos de negocios. eTOM se convierte en una herramienta útil para planificadores, administradores y estrategas; haciendo énfasis en una estructura, componentes de proceso, interacciones de los mismos, roles y responsabilidades; proporcionando un conjunto de requerimientos para la solución de sistemas, arquitecturas, tecnologías e implementación.

eTOM comienza con la descripción general de la empresa y define los procesos de negocios en una serie de agrupaciones, empleando una jerarquización, en la descomposición para estructurarlos y así obtener los procesos de negocios más detallados. La descomposición de procesos, incluye la administración de las relaciones con los clientes, las relaciones existentes desde el marketing hasta la facturación, el servicio de soporte después de las ventas, entre otros. El modelo eTOM a nivel conceptual se muestra en la Figura 2.10.

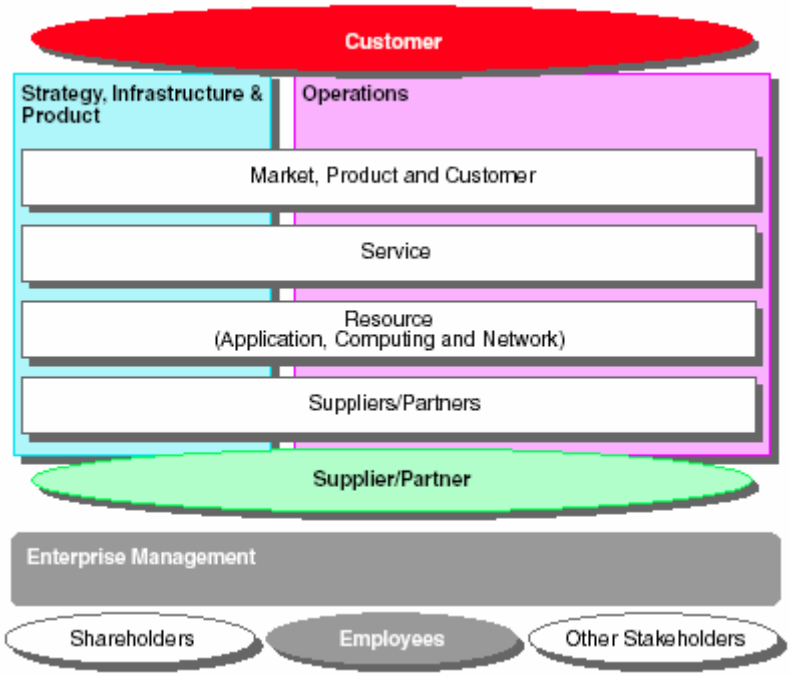


Figura 2.10 Modelo eTOM, nivel conceptual

Los niveles conceptuales de eTOM, son vistos en tres áreas de procesos, las cuales se describen a continuación.

1. Operaciones, el área de procesos de operaciones es el corazón de eTOM, incluye todos los procesos de operaciones que soportan las aplicaciones de los clientes y su administración. Por ejemplo: aquellas operaciones que se establecen directamente con el cliente. La vista de operaciones en el modelo eTOM, incluye la administración de ventas y el manejo de relaciones socio-proveedores.
2. Estrategia, Infraestructura y Productos, esta área incluye procesos que desarrollan estrategias, construcción de infraestructura, desarrollo y administración de productos, así como la administración de la cadena de proveedores. En el modelo eTOM, la infraestructura se refiere al ajuste de las tecnologías de la información y recursos que dan sostén a los productos y servicios que la organización ofrece. Ejemplos de estos procesos son: los procesos incluidos en CRM, Administración de Relaciones con los Clientes (Customer Relationships Management).
3. Administración de la empresa, es un área que incluye procesos básicos de negocios, requeridos para el correcto funcionamiento de una empresa. Dichos procesos están enfocados sobre el nivel empresarial, objetivos y propósitos, teniendo relación con la mayoría de los otros procesos dentro de la empresa, como el área de operaciones, estrategia, infraestructura y productos. Ejemplos de estos procesos son: la administración financiera, la administración de recursos humanos, etc.

En la actualidad, la administración de redes se incluye en el modelo eTOM, donde los procesos de soporte de operación, activación de servicios, aprovisionamiento y facturación, permiten tener un control total de la infraestructura de la red, desde la relación con el cliente o usuario final, hasta su facturación o direccionamiento de costos a diferentes departamentos (procesos agrupados en forma vertical) y desde el control de dispositivos hasta el manejo de negocios (procesos agrupados en su forma horizontal).

2.3.1 Niveles de eTOM

eTOM, es descompuesto bajo un nivel conceptual en un conjunto de procesos agrupados, que proveen de un primer nivel de detalle, en el cual la organización es vista en su totalidad. Existe una división de los procesos de acuerdo a la forma en como se realizan en:

a. Agrupación horizontal de procesos, representan una vista de los procesos funcionales relacionados dentro de los negocios, como los que se incluyen en la administración de la cadena de suministro.

b. Agrupación vertical de procesos, representan una vista punto a punto de los procesos dentro de una empresa, como por ejemplo los flujos de facturación hacia los clientes.

Las tres áreas del modelo eTOM (Operaciones, Estrategia, Producto e Infraestructura y Administración de la Empresa) incluyen esta estructura bidimensional tal como se muestra en la Figura 2.11.

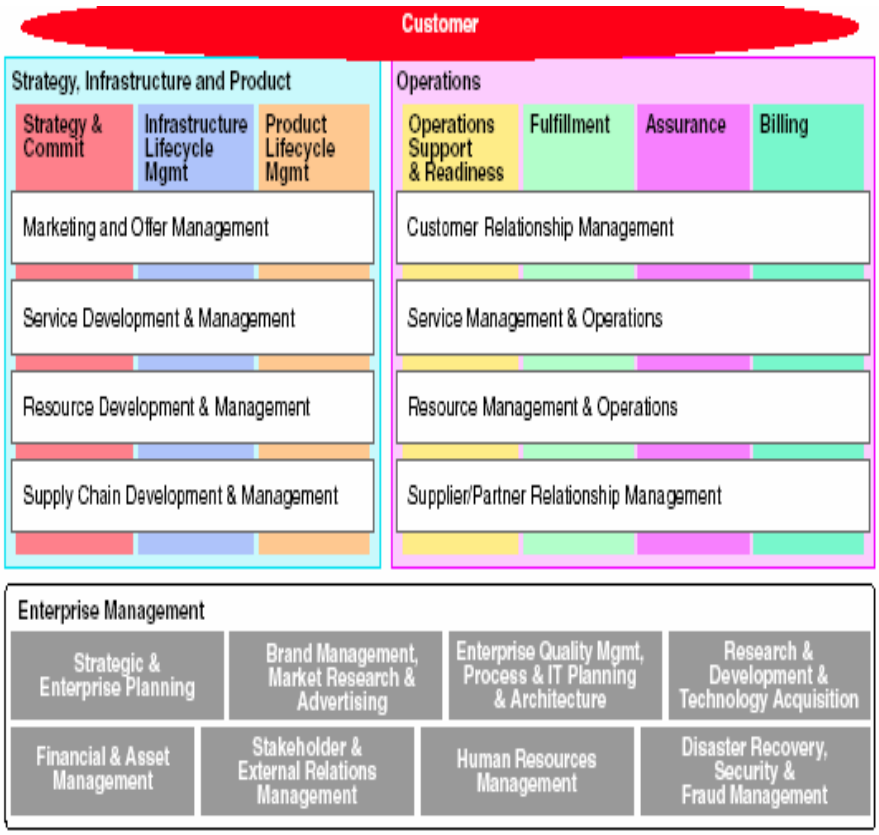


Figura 2.11 Modelo eTOM

A. Área de operaciones

OPS, Área de Procesos de Operaciones, incluye todos los procesos de operación que soportan la administración y están definidos en la Figura 2.12.

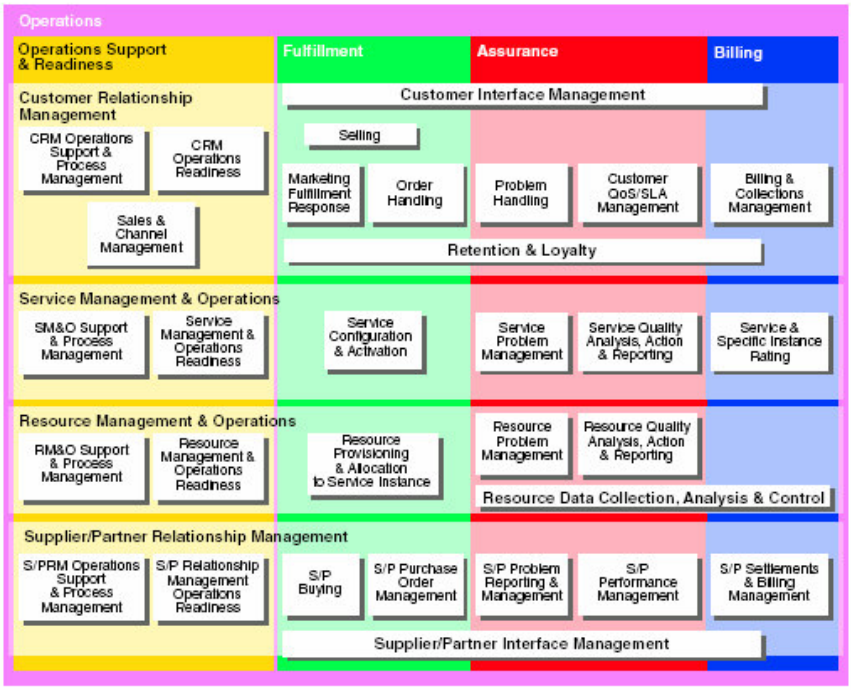


Figura 2.12 Área de operaciones

Los procesos contenidos en el área de operaciones se agrupan verticalmente en dos áreas:

1. FAB, Activación, Aprovisionamiento y Facturación (Fulfillment, Assurance, Billing) se consideran como el núcleo del área de operaciones, algunas ocasiones son referencias a los procesos de operaciones del cliente, sirviendo de interfases con el soporte al cliente. Son los procesos que tienen mayor prioridad dentro de una empresa.

   a. Activación de Servicios (Fulfillment), este conjunto de procesos es responsable de proveer los productos solicitados a los clientes, de una manera oportuna y correcta. Lo anterior se traduce en la satisfacción, ya sea de una necesidad personal, de un negocio de un cliente, a través de soluciones desarrolladas con productos específicos de la empresa.

   b. Aprovisionamiento (Assurance), estos procesos son responsables de la ejecución de estrategias activas, proactivas y reactivas que aseguren los servicios proporcionados a los clientes, con niveles de desempeño QoS. Para lo anterior se requiere de un monitoreo continuo del estado de los recursos, el cual permite detectar posibles fallas, a través de la recolección de datos y su análisis, evitando que el cliente sufra la falta del servicio.

   c. Facturación (Billing), conjunto de procesos responsable de la generación de facturas oportunas y exactas. Abarca los procesos de facturación a los clientes, seguimiento y recolección de sus pagos, atención de inquietudes por parte de los clientes, investigaciones de estado de las facturas, soporte para procesos de prepago de servicios y es responsable de resolver cualquier problema de facturación de una manera oportuna, sin dejar de lado la satisfacción del cliente.

2. OSR, Soporte de Operaciones y Disponibilidad (Operations, Support and Readiness) incluye aquellas actividades necesarias para asegurar que los procesos de operaciones de los clientes, puedan responder a las necesidades de los mismos, en

un tiempo y costo solicitado, incluyendo su satisfacción en cuanto a la entrega y el soporte.

La estructura horizontal en el área de operaciones incluye 4 grupos funcionales que dan soporte a los procesos del FAB, así como a la administración de operaciones, que soportan los servicios ofrecidos a los clientes, recursos y relaciones entre proveedores-socios. La estructura horizontal se compone de las siguientes áreas:

1. CRM, Administración de las Relaciones con el Cliente (Customer Relationship Management) este conjunto de procesos considera el conocimiento fundamental de las necesidades de los clientes e incluye todas las funcionalidades necesarias para la adquisición, extensión y mantenimiento de las relaciones con un cliente. Este bloque se enfoca al servicio al cliente y el soporte que se le da, ya sea telefónico, Web o centro de servicio, así como a la recopilación de la información de los clientes, con el objetivo de personalizar e integrar los servicios al cliente, además de identificar las oportunidades para incrementar el valor del cliente en la empresa.
2. SM&O, Administración de Servicios y Operaciones (Service Management & Operations) este conjunto de procesos centra su atención en el conocimiento de todos los aspectos que implican los servicios, tales como la conectividad, acceso, contenido, etc. Considera todas las funcionalidades necesarias para la administración y operación de las comunicaciones y servicios de información indispensables para dar soporte a los servicios ofrecidos al cliente. La atención se centra en la entrega y administración de servicios.
3. RM&O, Administración de Recursos y Operaciones (Resource Management & Operations) este conjunto de procesos mantiene información de los recursos como las aplicaciones, infraestructura de red y cómputo; siendo responsable de la administración de los mismos (redes, sistemas de tecnología de información, servidores, routers, etc.), todos ellos requeridos para entregar y proporcionar el soporte de servicios al cliente.
4. S/RPM, Administración de las Relaciones Proveedores–Socios (Supplier/Partner Relationship Management) este conjunto de aplicaciones es el núcleo de los procesos de operaciones. Incluir este bloque dentro de la estructura de eTOM, es una de las claves que diferencian al modelo de su antecesor, el modelo TOM. Su existencia permite una interfaz directa con el ciclo de vida correspondiente, operaciones punto a punto con los clientes o procesos funcionales con los proveedores y socios.

B. Área de procesos de estrategia, infraestructura y producto

SIP, Área de Procesos de Estrategia, Infraestructura y Producto (Strategy, Infraestructure & Product Area) contiene los procesos contenidos en la Figura 2.13.

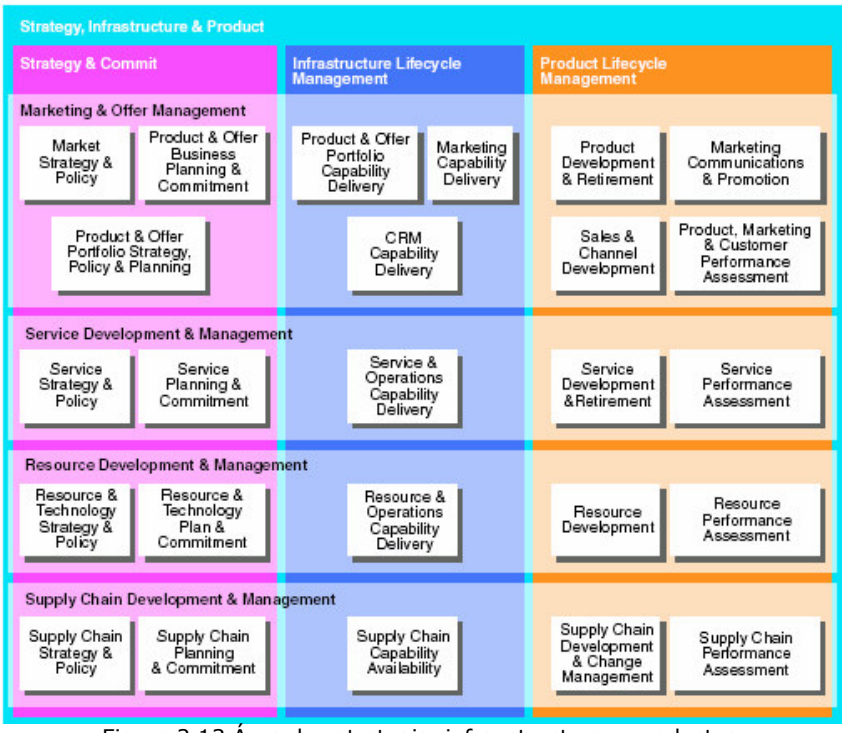


Figura 2.13 Área de estrategia, infraestructura y productos

El grupo de procesos verticales del SIP, abarca el conjunto de procesos de estrategia y entrega junto con los dos ciclos de vida de administración de procesos, todos ellos mostrados como un árbol vertical de procesos punto a punto. El grupo de procesos verticales se compone de las siguientes áreas:

1. Estrategia y entrega, estos procesos tienen por objetivo la generación de estrategias de negocios específicas, así como su aplicación dentro de los negocios. Abarca todos los niveles de operación, desde el mercado, clientes y productos, pasando por los servicios y recursos, así como la inclusión de proveedores y servicios.
2. Administración del ciclo de vida de la infraestructura, la administración de estos procesos, incluye el control y soporte para la provisión de productos a los clientes. Su atención se enfoca en el conocimiento de las expectativas de los clientes, así como las ofertas de productos, la infraestructura que soporta las funciones de operación y los productos, proveedores y socios involucrados en las ofertas de la empresa, hacia los clientes. Define, planea e implementa la infraestructura necesaria, aplicaciones de cómputo y redes.
3. Administración del ciclo de vida de los productos, este bloque es responsable de la definición, planeación, diseño e implementación de todos los productos que ofrece la empresa. Analiza los márgenes de beneficios y pérdidas de los productos, para proporcionar al cliente una satisfacción con entregas de calidad, así como el desarrollo de nuevos productos para el mercado.

La agrupación de los procesos horizontales correspondientes a su comportamiento funcional, se divide en 4 áreas que interactúan con el área de operaciones, incluyen funcionalidades necesarias para la definición de estrategias de desarrollo, administración de la elaboración de los productos, servicios y recursos. Las áreas que integran las capas horizontales se muestran a continuación:

1. Administración del mercado y de la oferta (Marketing & Offer Management), este grupo de procesos está enfocado al conocimiento del desarrollo y realización de los procesos de negocio centrales. Para un ICSP, Proveedor de Servicios de Comunicación e Información (Information Communication Service Provider) abarca funciones para el desarrollo de nuevos productos, administración de los productos existentes e implementación de estrategias de mercado.
2. Administración y desarrollo de servicios, esta área se centra en la planeación, desarrollo y entrega de servicios, al área de operaciones. Incluye las funciones necesarias para la definición de estrategias para la creación y diseño de servicios, administración y evaluación de los servicios actuales ofrecidos, así como el desarrollo de capacidades que permitan conocer futuras demandas de servicios.
3. Administración y desarrollo de recursos, este grupo de procesos se centra en la planeación, desarrollo y entrega de los recursos necesarios para el soporte de servicios y productos, al área de operaciones. Incluye funcionalidades necesarias para la definición de estrategias de desarrollo de la red de trabajo y otros recursos físicos y lógicos, así como la introducción a nuevas tecnologías, redes internas de trabajo, administración y aseguramiento de los recursos existentes.
4. Administración y desarrollo de cadenas de proveedores, conjunto de procesos cuyo objetivo principal son las relaciones o interacciones requeridas en la organización con los socios y proveedores, así como todos aquéllos involucrados en el mantenimiento de las cadenas de proveedores. Aseguran que los mejores proveedores y socios sean seleccionados como parte de la empresa.

C. Área de procesos de administración de la empresa

Esta área incluye el conocimiento de las acciones en los diferentes niveles de la empresa, así como sus necesidades y considera toda la administración de procesos de negocios, necesarios para dar el soporte al resto de la empresa, no siendo específicamente del domino de las telecomunicaciones, como se observa en la Figura 2.14.

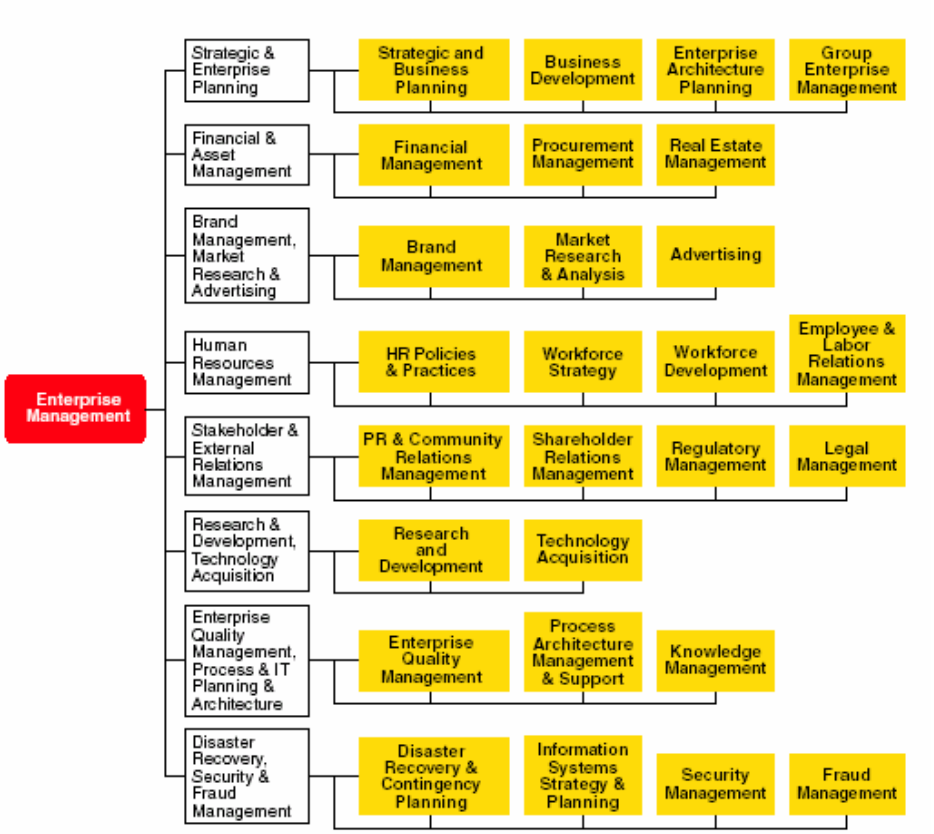


Figura 2.14 Administración de la empresa

2.3.2 Aplicaciones de eTOM

En la industria de las telecomunicaciones, eTOM puede ser utilizado como:

a. Una herramienta de análisis de procesos que permita la evaluación y desarrollo de nuevos procesos.

b. Una herramienta de análisis de costos de la realización, de cada uno de los procesos individuales dentro de una organización.

c. Principales SP, de EU emplean eTOM para aclarar la implicación en los procesos de nuevos proyectos bajo evaluación.

d. Principales SP, de Europa, usan eTOM como un proceso neutral para arbitrar disputas entre unidades internas de la organización.

e. Principales SP, de Australia, aplican eTOM como proceso estándar de la industria para el desarrollo de sus propios negocios.

f. Principales SP, de Asia-Pacífico se han convertido en referencia de administración, cuando han aplicado eTOM en los procesos de mejoramiento.

2.3.3 Ventajas de emplear eTOM

Dentro de las principales ventajas de utilizar eTOM, encontramos:

a. Hace posible una estructura estándar, terminología y un esquema de clasificación para describir los procesos de negocios y su construcción en bloques.

b. Provee una disciplina para ser aplicada.

c. Proporciona las bases para entender y administrar diferentes aplicaciones de la tecnología de la información, en términos de los requerimientos de los procesos de negocios.

d. El empleo del modelo eTOM, permite consistencia y alta calidad en los flujos de proceso punto a punto, que también pueden ser creados con oportunidades y realización de mejoras.

e. Usar eTOM, dentro de la industria de las telecomunicaciones incrementa la posibilidad de que las aplicaciones sean realmente integradas a un costo menor.

f. eTOM, posiciona a las empresas SP, de telecomunicaciones dentro de un contexto global de negocios, que les permite encontrar la interacción entre los procesos de negocios y las relaciones entre los elementos que intervienen.

g. eTOM, provee de la definición de terminología común, referentes a los procesos, subprocesos y las actividades realizadas en cada una. La terminología en común, facilita los procesos de negociación entre los clientes y proveedores de servicios.

h. eTOM, está definido de una forma general, de manera que es independiente a la organización, tecnología y servicio.

i. eTOM, representa un consenso de la industria de las telecomunicaciones para los SP, que proporciona posiciones armonizadas a través de escenas globales, basándose en contribuciones de los miembros, debiéndose ser ajustado o ampliado en las organizaciones individuales.

j. eTOM, es un marco de trabajo para definir procesos, que suministra una perspectiva orientada a negocio.

k. eTOM proporciona un acelerado retorno de inversión de los gastos de capital, a través del control de los costos de operación, calidad de servicio y administración de los anchos de banda, que se relacionan con necesidades como rápido desarrollo, automatización, escalabilidad y manejo de activos.

2.3.4 Áreas de trabajo de eTOM

Actualmente los miembros del TMF, se encuentran trabajando en las siguientes líneas de eTOM:

- eTOM como modelo para servicios de nueva generación, tecnología y aplicaciones.
- TRIP, Procesos de Integración de Recursos (eTOM Tecnhonology Resource Integration Processes).
- Administración de la fuerza de trabajo.
- Procesos de facturación.
- Articulación de trabajos.
- Recuperación de desastres.
- Administración de fraude y seguridad.

2.4 Protocolos de administración de redes

2.4.1 Introducción a los protocolos de administración

Los fabricantes proporcionan una serie de herramientas software, para la administración de las redes, las cuales están diseñadas para supervisar los nodos, los niveles de tráfico, vigilar los cuellos de botella, seguir la pista del software y recopilar la información de diagnóstico.

Las funciones que deben proveer los diversos productos de red para su administración, se clasifican de la siguiente manera:

a. Información del estado de la red.
b. Generación de alarmas entre fallas.
c. Modificación de parámetros de la red.

Existe un inconveniente en la última función, que es la alta dependencia del proveedor y cabe la posibilidad de ser incompatible con productos de terceros.

Estas aplicaciones requieren de un medio de comunicación común, que les permita interactuar sin problemas, de manera que existe la necesidad de crear protocolos de administración normalizados, ver Figura 2.15.

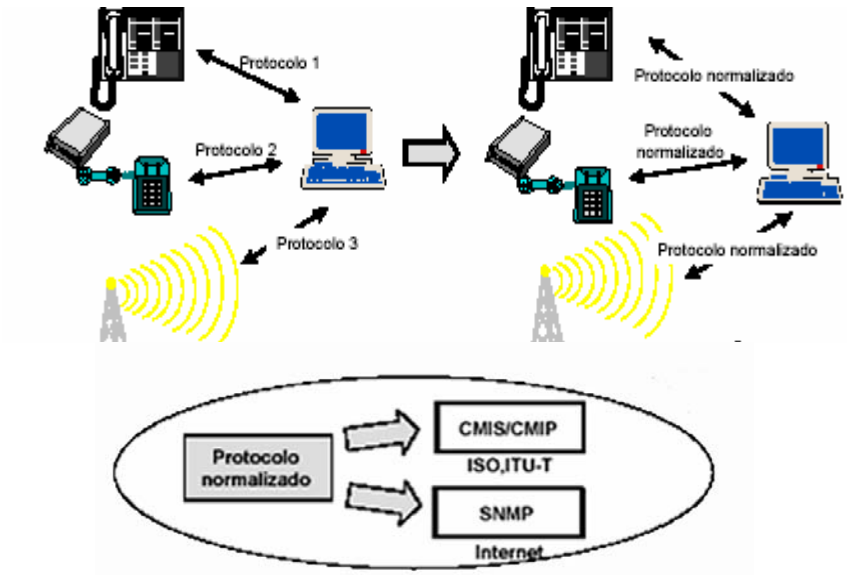


Figura 2.15 Protocolos normalizados de administración de red

Para evitar incompatibilidades, la ISO desarrolló dos estándares para la administración de redes: CMIS y CMIP, que se ubican en la capa de aplicación del modelo OSI. En el contexto de los productos de administración de red, CMIP se encarga de recolectar la información de las capas inferiores e informa a CMIS.

En el ámbito TCP/IP se desarrolló un estándar que provee una funcionalidad similar a CMIP, sencillo y popular: SNMP.

En entornos locales se utiliza SNMP y a nivel de red de área amplia, se hace uso del protocolo CMIP.

CORBA, desarrollado por el OMG, Grupo de Administración de Objetos (Object Management Group) es un protocolo que ofrece interoperabilidad y portabilidad entre diferentes lenguajes de programación, plataformas de hardware y sistemas operativos. Su uso está basado en la integración de sistemas de administración de servicios de telecomunicaciones.

2.4.2 Protocolo de Información de Administración Común, CMIP

A. Introducción a CMIP

CMIP, Protocolo de Información de Administración Común (Common Management Information Protocol) desarrollado por la ISO, ofrece un mecanismo de transporte en la forma de servicio pregunta-respuesta para las 7 capas del modelo OSI.

CMIP, es considerada como una arquitectura de administración de red, que provee de mecanismos de intercambio de información, entre un administrador y elementos remotos de red, cuyo funcionamiento está basado en los servicios CMIS. Desarrollado por el Comité Consultivo Internacional de Telegrafía y Telefonía, es un protocolo similar a SNMP, sólo que con beneficios adicionales, los cuales a su vez lo hacen un protocolo complejo, que no es muy utilizado. Dentro de las ventajas que tiene en relación con SNMP, es su manejo de seguridad integrado desde su diseño, junto con la capacidad de activar tareas cuando suceden problemas en el dispositivo administrado. Este protocolo no se basa únicamente en preguntas y respuestas, si no también en la activación de tareas.

Los sistemas de administración de red, basados en CMIP son utilizados en la administración de:

- Redes de Área Local, LAN.
- Redes Corporativas y Privadas de Área Amplia.
- Redes Nacionales e Internacionales.

B. Características del protocolo CMIP

Entre las principales características del protocolo CMIP encontramos:

- Se basa en el paradigma administrador-agente y una base de información.
- CMIS/CMIP requiere de gran cantidad de memoria y capacidad de CPU.
- Genera cabeceras complicadas en los mensajes de los protocolos.
- Las especificaciones son difíciles de realizar y tediosas de implementar en aplicaciones.
- La comunicación con los agentes está orientada a conexión.
- La estructura de funcionamiento es distribuida.
- Permite una jerarquía de sistemas de operación.
- El protocolo asegura que los mensajes lleguen a su destino.

Con lo anterior se tiene una administración dirigida por eventos, lo cual significa que el agente notifica al administrador de sucesos, la información concerniente a los recursos administrados. El agente es responsable de monitorear los recursos.

CMIP, presenta la ventaja de que existe menor gestión de tráfico con su consecuente desventaja de tener agentes más complejos.

C. Objetos administrados en OSI

La información de administración, representa los recursos físicos y lógicos de una red, definiéndose como una entidad intermedia entre el objeto real y el protocolo de comunicación utilizado, por ejemplo los switches, las estaciones de trabajo, etc.

D. Servicios empleados por CMIP

CMIS, los servicios proporcionados por la arquitectura de administración OSI, se denominan CMIS, Servicios Comunes de Información de Administración (Common Management Information Services) que definen su implementación en el protocolo CMIP y son invocados mediante un conjunto de primitivas relacionadas con uno o varios objetos de la MIB.

a.1 Primitivas CMIS/CMIP, las estructuras de información que implementan los servicios de un nivel, reciben el nombre de primitivas. CMIS/CMIP hacen uso de las siguientes primitivas:

- M-GET, obtiene información sobre los valores de los atributos de un objeto administrable.
- M-SET, modifica la información contenida en un objeto administrable.
- M-ACTION, invoca una operación sobre un objeto administrado.
- M-CREATE, crea la representación de una instancia de un objeto administrado de una clase determinada.
- M-DELETE, elimina la representación de una instancia de un objeto administrado.
- M-CANCEL-GET, cancela una petición M-GET previa. La cancelación se puede deber a un excesivo consumo de tiempo por parte de un servicio GET.
- M-EVENT-REPORT, notifica un evento, como puede ser una notificación de alarma entre elementos de red y este servicio puede ser o no confirmado.
- Las operaciones CMIS/CMIP se pueden originar tanto en administradores como en agentes.

E. Protocolos de aplicación en CMIP

Para comunicarse entre sí, dos entidades de aplicación (administrador-agente) requieren de las UDPA, Unidades de Datos de Protocolo de Aplicación (Application Protocol Data Units). CMIP, se compone de los siguientes protocolos OSI:

a. ACSE, Elemento de Servicio de Control de Asociación (Association Control Service Element) protocolo que establece y libera asociaciones entre entidades de aplicación. El establecimiento lo puede realizar el agente o el administrador y durante el proceso se intercambian los títulos de la entidad de aplicación para identificarse, junto a los nombres de contexto de aplicación. ACSE, es utilizado directamente por el usuario de la administración y proporciona los siguientes servicios:

- A-ASSOCIATE, servicio confirmado requerido para iniciar la asociación entre entidades de aplicación.
- A-RELEASE, servicio confirmado implementado para liberar una asociación entre entidades de aplicación sin pérdida de información.
- A-ABORT, servicio no confirmado que causa la liberación anormal de una asociación con una posible pérdida de información.

- A-P-ABORT, servicio iniciado por el proveedor que indica la liberación anormal de la asociación del servicio de presentación con posible pérdida de información.

b. ROSE, Elemento de Servicio para Operación Remota (Remote Operation Service Element) protocolo encargado de las llamadas de procedimientos remotos, permite la invocación de una operación en un sistema remoto, de la siguiente manera: el administrador solicita una operación remota, el agente lo intenta ejecutar y devuelve el resultado del intento.

   Servicios que proporciona ROSE a CMISE:

   - RO-INVOKE, servicio no confirmado usado por un usuario de ROSE, para invocar que una operación sea realizado por un ROSE remoto.
   - RO-RESULT, servicio no confirmado que un ROSE invocado usa para contestar a una previa indicación RO-INVOKE, en el caso de que se haya realizado con éxito.
   - RO-ERROR, servicio no confirmado que es usado por un usuario de ROSE invocado para contestar a una previa indicación RO-INVOKE, en el caso de que haya fracasado.
   - RO-REJECT, servicio no confirmado utilizado por un usuario de ROSE para rechazar una petición.

c. CMISE, Elemento Común de Servicios de Información de Administración (Common Management Information Service) protocolo que proporciona los servicios básicos de administración para reportar eventos, manipular datos de administración y generar requerimientos. CMISE, hace uso de los servicios proporcionados por ACSE y ROSE, como se muestra en la Figura 2.16.

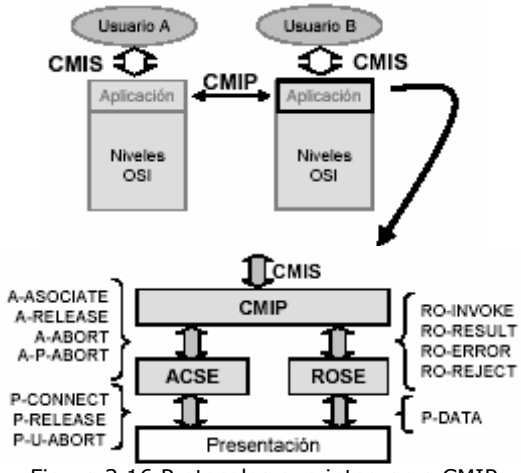


Figura 2.16 Protocolos que integran a CMIP

F. Servicios ofrecidos por CMIP

A través de CMISE, el protocolo CMIP proporciona tres tipos de servicios, mostrados en la Figura 2.17 y descritos a continuación:

a. Manejo de datos, utilizado por el administrador para solicitar y alterar información de los recursos del agente.

b. Informe de sucesos, empleado por el agente para informar al administrador.

c. Control directo, empleado por el administrador para la ejecución de diversas acciones en el agente.

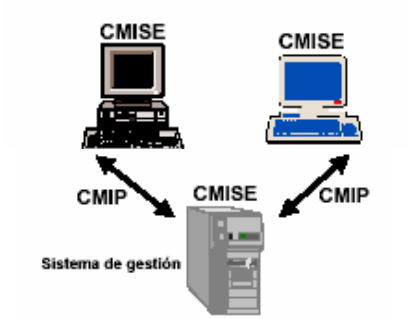


Figura 2.17 Funcionamiento de CMIP

2.4.3 Protocolo Simple de Administración de Red, SNMP

A. Introducción a SNMP

SNMP, Protocolo Simple de Administración de Red (Simple Network Management Protocol) es un estándar de administración de redes basado en el conjunto de protocolos TCP/IP, que permite la consulta a los diferentes elementos que constituyen la red.

Definido por la comunidad EITF, Fuerza de Tareas de Ingenieros de Internet (Internet Engineering Task Force) tiene sus orígenes en SGMP, Protocolo Sencillo de Supervisión de Pasarela (Simple Gateway Monotoring Protocol) y actualmente es la herramienta de administración de redes más implementada por los fabricantes.

SNMP ha evolucionado de SNMPv1, SNMP v2 hasta la versión actual SNMP v3 y permite a los administradores de red:

a. Supervisar la operación de la red.
b. Configurar equipos.
c. Encontrar y resolver fallos.
d. Analizar prestaciones de los equipos.
e. Acceder a la información de productos de diferentes fabricantes de una misma manera, desarrollando una herramienta común de monitoreo.

Hoy en día, SNMP es el protocolo de administración de red más ampliamente usado y desarrollado.

B. Entorno de administración en Internet

SNMP, es el protocolo empleado para la administración de redes basadas en TCP/IP como lo es Internet, siendo ésta la configuración de redes más extendida.

El entorno de trabajo del protocolo SNMP se basa en cuatro componentes:

a. SMI, Estructura de Administración de la Información: RFC1155, lenguaje de definición de datos, que especifica los tipos de datos, un modelo de objetos y reglas para escribir y comprobar la información de administración. Los objetos MIB se especifican a partir de este lenguaje.

b. Administración de la Base de Información, MIB: RFC1156, RFC 1213, incluye la definición de los objetos de red, conocida como objetos MIB. La información de administración, se representa como un conjunto de objetos que conforman un almacenamiento de información virtual, conocido como Base de Información de Administración. Un objeto MIB, puede ser un contador (por ejemplo el número de datagramas IP que han sido eliminados en el router debido a los errores en la cabecera del datagrama IP o bien el número de errores de detección de la portadora en una tarjeta de interfaz ethernet). Los objetos MIB definen la información de administración que mantiene un dispositivo y aquéllos que están relacionados, se recogen en un módulo MIB.

c. Protocolo Simple de Administración de Redes, SNMP: RFC 1157, medio de comunicación para transmitir información y comandos entre la entidad administradora y un agente que se ejecuta en un dispositivo de red en representación de dicha entidad.

d. Capacidad de seguridad y administración de objetos.

C. Funcionamiento de SNMP

SNMP, opera en el nivel de la capa de aplicación, utilizando el protocolo de transporte TCP/IP. Define una comunicación cliente-servidor, éste último se encuentra en cada equipo que se desea administrar (host, router, etc.) y el cliente en la estación de monitoreo, ver Figura 2.18.

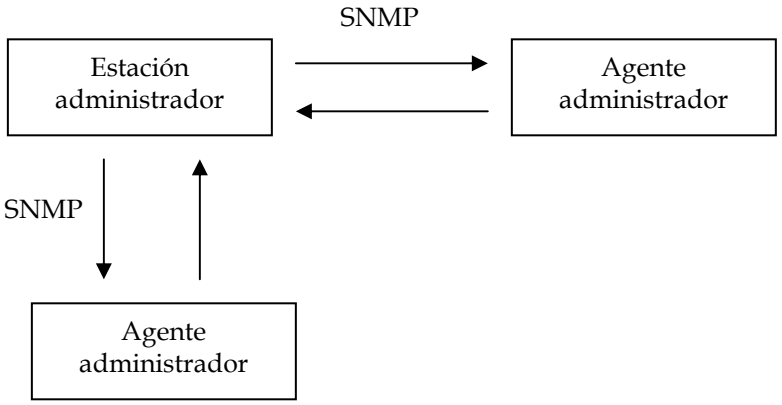


Figura 2.18 Arquitectura administrador-agente SNMP

La filosofía de comunicación de SNMP está basada en los principios de obtener y almacenar. La administración se realiza a nivel de IP, por lo que es posible controlar los dispositivos que estén conectados en cualquier red accesible desde Internet y no únicamente equipos locales.

El protocolo SNMP, obtiene la información de la red a través de un método denominado colección MIB. Esto significa que se desplaza de un dispositivo de red a otro, preguntando sobre su estado. Después se copia la información del estado de cada dispositivo, además de la MIB local de cada uno de ellos.

I. Modelo organizativo de SNMP

El modelo organizativo de la administración de redes basado en SNMP, se compone de los siguientes elementos, ver Figura 2.19:

- Entidad administradora.

- Administración de agente.
- Base de información de administración.
- Protocolo de administración de red.
- Estructura de la información de administración.
- Seguridad y la administración.

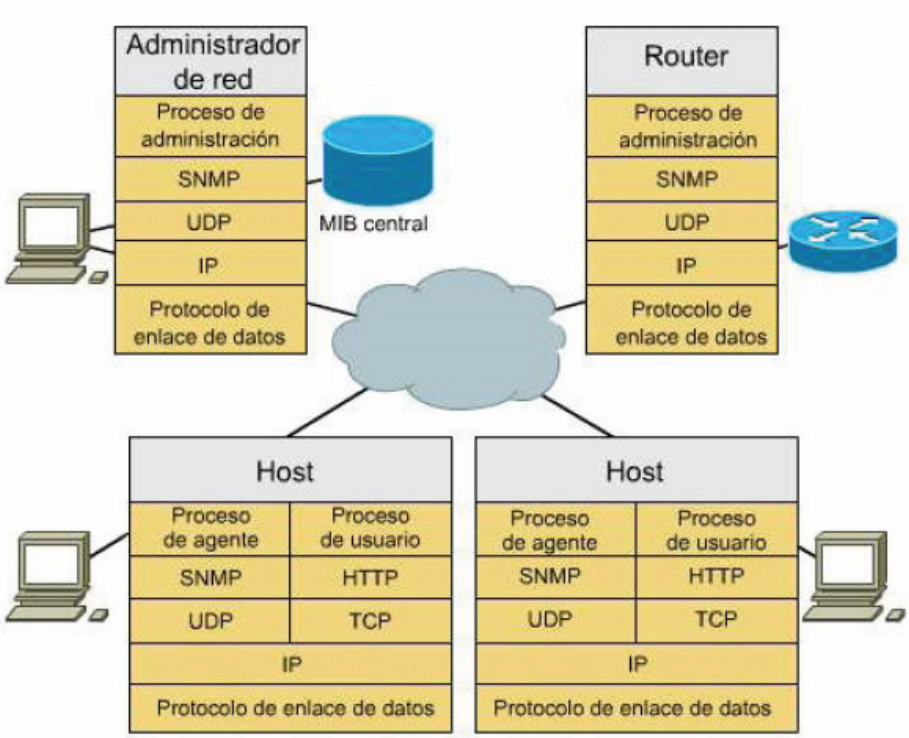


Figura 2.19 Componentes de la arquitectura SNMP

a. NMS, Entidad Administradora (Network Management System) es responsable de solicitar información al agente, a través de solicitudes basadas en peticiones específicas. El administrador registra, procesa y analiza la información recuperada de varias formas genéricas, mostrándola a través una utilidad gráfica.

   El NMS, se encuentra en una estación de trabajo o nodo que ejecuta un sistema operativo común y corriente, dispone de una cantidad de RAM suficiente que le permite almacenar todas las aplicaciones de administración que se están ejecutando al mismo tiempo, sin embargo también se puede implementar en diversos sistemas. Incluye una colección de software llamado NMA, Aplicación de Administración de Red (Network Management Station) que incorpora una interfaz gráfica de usuario para permitir a los administradores autorizados controlar la red. Este NMS, responde a los comandos del usuario y a los emitidos para dirigir a los agentes a lo largo de la red, lleva a cabo el monitoreo recuperando los valores desde la MIB y puede hacer que se realice una acción en un agente o cambiar la configuración de otro, ver Figura 2.20. A menudo a la entidad administradora, se le denomina como Administrador SNMP.

   Las aplicaciones de administración de red, confían en el sistema operativo y su arquitectura de comunicación. Entre los NMA más reconocidos encontramos:

   1. CiscoWorks2000, herramienta que emplea utilidades como: la administración de recursos, topología de servicios, etc.

2. Hp Open View, software organizado en mapas o ventanas con determinados símbolos. Por defecto, la primera vez que arranca, descubre todos los elementos con dirección IP a los que tiene acceso desde la máquina donde administra. Una vez descubiertos, los inserta en el mapa Internet, donde los conecta según la información que obtiene a partir de los nodos de direcciones IP, tablas de ruteo, etc.
3. SNMPc, plataforma de administración de red para Microsoft Windows 98 y NT, creada para monitorear y administrar redes de pequeño y mediano tamaño, así como también para ser utilizada como herramienta de configuración de hubs, switches y routers. Cuenta con programas de aplicación para representación gráfica de dispositivos y manejo detallado de MIBs privadas.

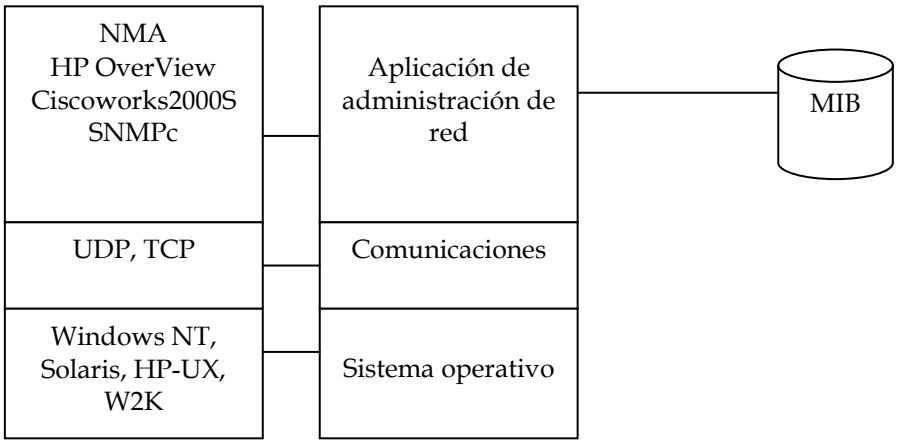


Figura 2.20 Esquema de una estación de administración

b. Administración de agente, los agentes de administración son procesos que se ejecutan en cada nodo de la red, como los hosts, routers, puentes y hubs, los cuales deben estar equipados con SNMP para poder ser administrados. Representa a la parte del servidor en la medida que tiene la información que se desea administrar y espera los comandos por parte del cliente (entidad administradora).

   Todos los datos del agente, ver Figura 2.21, se almacenan en su MIB y entre las principales funciones que un agente puede controlar encontramos:

   - Número y estado de sus circuitos virtuales.
   - Número de ciertos tipos de mensajes de error recibidos.
   - Número de bytes y paquetes entrantes y salientes del dispositivo.
   - Longitud máxima de la cola de salida, para routers y otros dispositivos de interconectividad.
   - Mensajes de difusión enviados y recibidos.
   - Interfases de red que han caído y las que se han activado.

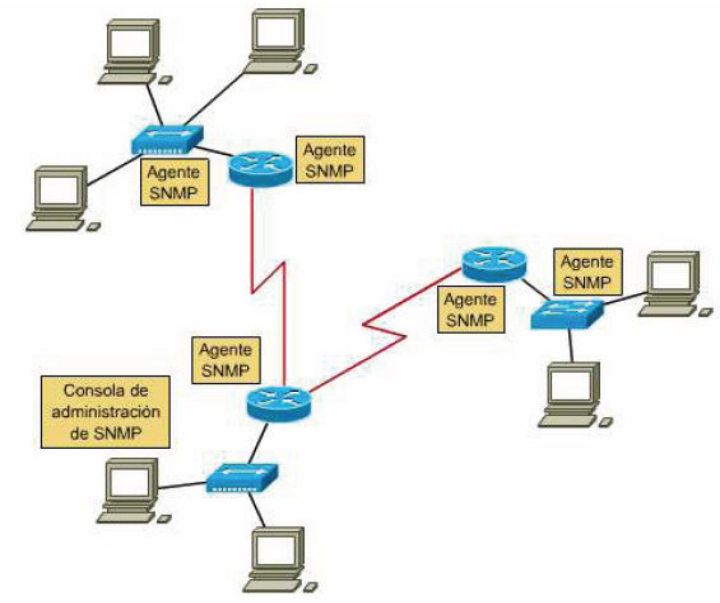


Figura 2.21 Agentes SNMP

Los agentes responden a las peticiones de información y demandan acciones desde el NMS a través del sondeo (cuando la entidad administradora solicita información del objeto administrado con una frecuencia determinada) y pueden facilitar información importante a través de interrupciones, las cuales pueden ser convencionales (cuando el objeto administrado avisa de un suceso a través de notificaciones) o interrupciones modificadas (que son la combinación de sondeos e interrupciones convencionales).

c. Bases de administración de información, se emplean para almacenar información estructurada sobre los elementos que integran la red y sus atributos. La estructura de almacenamiento se encuentra definida en el SMI, la cual define los tipos de datos que pueden utilizarse para almacenar un objeto, cómo deben nombrarse dichos objetos y cómo deben codificarse para su transmisión sobre la red.

   Actualmente existen tres diferentes tipos de éstas:

   1. MIB estándares.
   2. MIB experimentales, consideradas como las MIB en fase de desarrollo por los grupos de trabajo de Internet.
   3. MIB privadas, corresponden a las MIB's de productos específicos, incorporan la información de los diversos fabricantes de equipos y añaden funcionalidad a las MIB estándar. Regularmente los fabricantes las hacen públicas poniéndolas accesibles en Internet.

   Todos los valores almacenados en la MIB, son consultados y/o actualizados por una entidad administradora, enviando mensajes SNMP al agente que se está ejecutando en un dispositivo administrado en representación de la entidad administradora.

d. Protocolo de administración de red, existen dos formas de comunicación entre los agentes y las entidades administradoras:

   - Modo petición–respuesta, es el uso más común de SNMP, donde la entidad administradora envía una petición a un agente que la recibe, realizando una acción y enviando una respuesta a tal petición. La solicitud es empleada para consulta (obtener) o modificar (establecer) los valores de los objetos MIB, asociados con el dispositivo administrado.

- Modo de notificaciones, en este modo de operación, el agente envía un mensaje no solicitado denominado mensaje trampa, a una entidad administradora. Dichos mensajes se utilizan para notificar una situación excepcional que da lugar a cambios en los valores de los objetos MIB.

Un protocolo de administración de la capa de transporte es el encargado de efectuar la comunicación entre el administrador y el agente, mediante un intercambio de mensajes que ejecutan las operaciones de administración.

De acuerdo a los dos modos de operación de SNMP, es posible clasificar a los mensajes en tres grupos:

- Lectura, se presenta cuando el administrador recupera instancias de objetos administrados de un agente, le permite obtener el estado del dispositivo administrado a través de mecanismos de sondeo o polling. Ejemplos de esta clasificación de mensajes son las primitivas: Get, GetNext, GetBulk.
- Escritura, cuando el administrador crea o modifica las instancias de objetos administrados en un agente, permitiendo actuar sobre el dispositivo administrado, se tienen los mensajes de tipo escritura. Ejemplo de esta clasificación es el mensaje Set.
- Notificaciones, el agente informa a un administrador de la ocurrencia de una situación anómala a través de este tipo de mensajes. Ejemplos de esta clasificación son las primitivas: TRAP, SMPV2-TRAP.

En la Tabla No. 2.1 se presenta un resumen de los siete mensajes utilizados en SNMP, también denominados genéricamente como PDU, Unidades de Datos de Protocolo (Protocol Data Unit).

Tipo PDU de SNMP	Emisor-Receptor	Descripción
GetRequest	Administrador a Agente	Obtiene el valor de una o más instancias de objetos MIB.
GetNextRequest	Administrador a Agente	Obtiene el valor de la siguiente instancia de objeto MIB en una lista o tabla
GetBulkRequest	Administrador a Agente	Obtiene valores en n bloque grande de datos.
InformRequest	Administrador a Agente	Informa a la entidad administradora remota de los valores MIB remotos a su acceso.
SetRequest	Administrador a Agente	Establece valores de una o más instancias de objetos MIB.
Response	Agente a Administrador o Administrador a Agente	Generado en respuesta a: GetRequest GetNextRequest GetBulkRequest SetRequest InformRequest
SNMPv2-Trap	Agente a Administrador	Informa al administrador de un evento excepcional

Tabla No. 2.1 Mensajes utilizados en SNMP

El modelo organizativo basado en SNMP, es un modelo de dos capas que asume que todos los dispositivos de la red son administrables a través de SNMP, regularmente esto no es el caso, pues existen elementos que cuentan con su propia interfaz de administración, para estas situaciones, es necesario un modelo organizativo de tres niveles, donde un administrador de red que requiera obtener información o controlar este nodo propietario, se comunica con un agente proxy, el cual traduce la petición a una forma que se adecue al sistema destinatario y use cualquier protocolo de administración propietario para comunicarse con el sistema, las respuestas pasan nuevamente por el proxy y éste las traduce en mensajes SNMP que devuelve posteriormente al administrador.

D. Protocolo de Datagrama de Usuario, UDP

Las UDP empleadas en SNMP, pueden ser transmitidas por medio de diferentes protocolos de transporte, sin embargo son típicamente transportadas en un datagrama UDP, Protocolo de Datagrama de Usuario (User Datagram Protocol).

UDP, es un protocolo de transporte no fiable que no garantiza que una petición o respuesta sean recibidas por el destino.

E. Configuración y rendimiento de una red administrada por el protocolo SNMP

Para que el NMS se comunique con los dispositivos, éstos deben tener activado el SNMP. Analizar la configuración y el rendimiento en la administración, requiere la determinación de las dimensiones de algunos parámetros como lo son:

a. Número de estaciones de trabajo.
b. Número de redes.
c. Número de segmentos.
d. Número de nodos.
e. Número de interfases.
f. Número de routers.
g. Número de nodos administrados.

Con base en esta información es posible calcular la carga de administración, que es equivalente al número de nodos más el número de interfases administradas para cada nodo, de esta forma considerando el número de redes y segmentos se determina finalmente el número de objetos a administrar.

El NMS utilizado para sostener el sistema de administración, debe cubrir las funcionalidades de monitoreo y de descubrimiento básicas (Discover) junto con las funcionalidades de presentación (Display), además de detección de eventos de acción y de recolección de datos. Las anteriores funciones requieren de espacio en memoria estándar, memoria swap, espacio de disco y potencia de cálculo.

2.4.4 Comparación entre los protocolos CMIP y SNMP

El protocolo CMIP, no es tan implementado como el SNMP, sobre todo en las nuevas instalaciones, debido a que las arquitecturas de administración con protocolo CMIP de diferentes fabricantes, presentan información que es propietaria, generando incompatibilidad.

En cuanto a modelo de datos de instrumentación, el protocolo SNMP se representa a través de variables, tablas, traps, etc., mientras que CMIP utiliza un modelo de objetos extendido.

Respecto a la identificación de nombres de datos administrados, SNMP hace uso de un árbol de directorio estático y CMIP hace uso de un árbol de directorios dinámico.

En relación con la representación de datos uniforme, SNMP utiliza un número mínimo de tipos de datos ASN1 mientras que CMIP hace uso de un rango extendido de tipos ASN1.

En el soporte de transporte de primitivas query/responses de administración, SNMP utiliza datagramas con la máxima independencia de la elección de transporte, mientras que CMIP utiliza conexiones con fuerte dependencia del estándar OSI.

A nivel funcional el protocolo CMIP obtiene mayor rendimiento de los mensajes enviados, ya que reduce la señalización respecto al protocolo SNMP.

En seguridad, el protocolo CMIP es mucho más seguro que el SNMP.

A nivel operacional, el protocolo CMIP se basa en una arquitectura jerárquicamente distribuida, lo que permite que el número de objetos supervisados sea mayor que en el protocolo SNMP, que al ser de tipo centralizado viene limitado por la capacidad tecnológica de las plataformas de administración.

El costo de procesado y de la misma aplicación es más elevado en una plataforma CMIP.

El soporte por parte del fabricante, es mucho mayor al protocolo SNMP, debido a que es utilizado por la mayoría de los clientes y existe una multitud de productos comerciales.

El protocolo CMIP, permite más extensiones, es escalable, permite la herencia de atributos y es más flexible que el protocolo SNMP.

CMIP, creado y estandarizado para el monitoreo y control de redes heterogéneas corrige los errores de SNMP.

En SNMP los dispositivos de la red no tienen que ser inteligentes para informar cuando suceda un problema. Las preguntas de SNMP se encargan de esta tarea. En las grandes redes, que tienen conectados muchos dispositivos y recursos, la técnica de preguntas SNMP puede ser una desventaja, por que contribuye a un mayor tráfico en la red, haciéndola más lenta.

Entre las principales ventajas de SNMP, podemos encontrar las siguientes:

a. Es un protocolo abierto, estándar del mercado.
b. Es simple y fácil de utilizar.
c. Modelo útil para el acceso a datos de la administración de la red.
d. Acceso y organización eficientes de los datos administración.
e. Independencia del entorno de comunicaciones.
f. Capacidades generales de monitoreo y control.

Entre las principales desventajas se pueden considerar las siguientes:

a. Limitaciones en el mecanismo de obtención de información.

b. Falta de obtención selectiva de información.

c. No dispone de controles de administración.

d. Limitaciones de las capacidades de modelado de datos: MIB estática, correlación de datos difícil, modelado de sistemas complejos.

2.4.5 Arquitectura de Intermediación de Petición de Objetos Comunes, CORBA

A. Introducción a la administración distribuida

El sector de las telecomunicaciones enfrenta trascendentales cambios debido a factores como la tecnología, la desregulación de los mercados y exigencias de los clientes. Uno de los aspectos más relevantes es la administración de los servicios que este sector ofrece, lo cual no resulta sencillo considerando que la administración de una red compuesta por equipos y sistemas de tecnologías, proviene de diversos proveedores e incluye diversas plataformas y protocolos.

La creciente complejidad y heterogeneidad de las redes modernas de telecomunicaciones, está generando la necesidad de buscar mecanismos simples y uniformes para administrarlas.

A través del surgimiento de modelos abiertos de computación distribuida como CORBA, algunos esfuerzos de esta búsqueda, se han orientado hacia el establecimiento de éste, como modelo común para la administración de redes.

Un factor relevante en el éxito de CORBA, consiste en la estrategia de transición entre el estado actual, con una gran difusión de sistemas administrador basados en protocolos SNMP y CMIP a el modelo CORBA.

CORBA, se utiliza como mecanismo de computación distribuida más proveedor de servicios del dominio de las telecomunicaciones. Esta arquitectura facilita la programación en redes heterogéneas, permitiendo crear aplicaciones distribuidas que interactúan como si hubiesen sido implementadas en un mismo lenguaje de programación y sobre una misma computadora. Además de la integración de sistemas OSS, Sistemas Abiertos de Soporte (Open System Services) de diferentes proveedores para su interoperabilidad.

Los servicios de la plataforma CORBA, ofrecen un dominio común de administración que abstrae los protocolos requeridos por los objetos administrados.

B. Funciones principales de CORBA

Dentro de las principales funciones que tiene CORBA, se encuentran tareas habituales en sistemas distribuidos como lo son:

- Registro, localización y activación de objetos.
- Administración de errores.
- Multiplexación y desmultiplexación de invocaciones.

C. Conceptos fundamentales

CORBA, Arquitectura de Intermediación de Petición de Objetos Comunes (Common Object Request Broker Architecture) es un conjunto de especificaciones estándares, neutrales al lenguaje y a la plataforma que sirve para construir aplicaciones de objetos distribuidos.

Las aplicaciones CORBA están diseñadas para estar aisladas, de los detalles del código de comunicaciones, facilitando la invocación de métodos remotos bajo un paradigma orientado a objetos.

CORBA, está definido y controlado por el OMG, Grupo de Administración de Objetos (Object Management Group) que define las APIs, Interfaz de Programación de Aplicaciones (Application Programming Interface), el protocolo de comunicaciones y los mecanismos necesarios para permitir la interoperabilidad entre diferentes aplicaciones escritas en diferentes lenguajes y ejecutadas en diferentes plataformas, lo que es fundamental en computación distribuida.

En un sentido general CORBA "envuelve" el código escrito en otro lenguaje, en un paquete que contiene información adicional sobre las capacidades del código que contiene y sobre cómo llamar a sus métodos. Los objetos que resultan pueden entonces ser invocados desde otro programa (u objeto CORBA) desde la red. En este sentido CORBA se puede considerar como un formato de documentación legible por la máquina, similar a un archivo de cabeceras pero con más información.

A continuación se describen los componentes de la arquitectura CORBA:

1. IDL, Lenguaje de Definición de la Interfaz CORBA (Interface Definition Language) utilizado para especificar las interfases con los servicios que los objetos ofrecerán, éste proporciona un mecanismo neutral al lenguaje que permite definir interfases de objetos distribuidos.

   CORBA puede especificar a partir de este IDL, la interfaz a un lenguaje determinado, describiendo cómo los tipos de dato CORBA deben ser utilizados en las implementaciones del cliente y del servidor. Existen implementaciones estándar basadas en Ada, C, C++, Smalltalk, Java, Perl, TCL y Python.

   Al compilar una interfaz en IDL, se genera un código para el cliente y el servidor (el implementador del objeto). El código del cliente sirve para poder realizar las llamadas a métodos remotos. Es el conocido como stub, el cual incluye un proxy (representante) del objeto remoto en el lado del cliente. El código generado para el servidor consiste en unos skeletons (esqueletos) en el que el desarrollador tiene que implementar los métodos del objeto. CORBA es más que una especificación multiplataforma, también define servicios habitualmente necesarios como: seguridad y transacciones.

2. ORB, Intermediario de Petición de Objetos (Object Request Broker) es el núcleo de CORBA que administra la transferencia de mensajes desde un programa hacia un objeto localizado en un servidor en una red remota, escondiendo al programador la complejidad de las comunicaciones en las redes.

   Un ORB, permite crear objetos cuyas operaciones pueden ser invocadas por programas cliente, localizados en cualquier parte de la red. El programa que contiene instancias de objetos CORBA, es a menudo conocido como un servidor. El cliente únicamente requiere conocer la definición IDL de un objeto CORBA, para invocar sus operaciones, sin importar el lenguaje de programación utilizado en su

implementación, su localización en la red o el sistema operativo sobre el que se ejecuta.

En el nivel inferior, las especificaciones CORBA que tratan con el ORB, definen exactamente cómo los clientes distribuidos pueden utilizar remotamente los servicios de servidores distribuidos, de un modo independiente del lenguaje y de la plataforma. Describen de igual forma el protocolo de comunicaciones subyacente en el que se produce la utilización de ese servicio.

El ORB, no es el único componente de la plataforma CORBA, sólo que provee los mecanismos para la interacción entre los objetos y la arquitectura que se construye sobre él, es conocida como OMA.

3. DII, Interfaz de Invocación Dinámica (Dynamic Invocation Interface) es una interfaz que permite la construcción dinámica de invocaciones para un determinado objeto. Una invocación dinámica se compone de una referencia al objeto, una operación y una lista de parámetros, todos estos datos obtenidos del IR.
4. IR, Repositorio de Interfases (Interface Repository) es un servicio que ofrece objetos persistentes que representan la información IDL de las interfases disponibles en CORBA de una forma accesible en tiempo de ejecución.

D. Arquitectura de Administración de Objetos, OMA

La arquitectura OMA, Arquitectura de Administración de Objetos (Object Management Architecture) hace posible el desarrollo de aplicaciones utilizando componentes software que ofrecen servicios estándar sobre interfases estándar.

OMA, define cuatro tipos de componentes:

1. Servicios Comunes de Objetos, CORBAservices, independientes de dominio, útiles para muchos programas distribuidos (localización de objetos por nombre o por características, transacciones, notificación de sucesos, etc.). Podemos mencionar al menos dos tipos de estos servicios:
   a. Servicios de Objetos Comunes CORBAservice, definen los servicios CORBA, en los que confían las aplicaciones basadas en CORBA, como el de proporcionar nombres de objetos legibles a las asignaciones de referencias de objeto y consultar objetos por medio de algunos criterios de búsqueda.
   b. Servicio de Seguridad de CORBA, es un componente OMG-CORBAservice, que está relacionado con la seguridad de objetos distribuidos en las aplicaciones basadas en CORBA, definido para funcionar principalmente sobre el nivel ORB, permite la interoperabilidad y la seguridad mejorada.

      Al usar componentes que implementan esta especificación, las aplicaciones obtienen la ventaja de la protección de la seguridad basada en estándares, incluyendo la autenticidad, el no repudio, la autorización, la auditoría, la integridad y la confidencialidad.
2. Facilidades Comunes, CORBAfacilities, para aplicaciones de usuarios finales (Distributed Document Component Facility).
3. Interfases de Dominio, CORBAdomains, para dominios específicos (telecomunicaciones).
4. Aplicaciones, para aplicaciones específicas no normalizadas.

E. Implementación de aplicaciones con CORBA

El primer paso en el desarrollo de una aplicación CORBA, es la definición de las interfases de los objetos usando el IDL. A partir de esta definición y mediante un compilador IDL se genera el código stub, el cual captura las invocaciones del cliente a las operaciones del servidor y del esqueleto, que invoca las operaciones del servidor y recoge sus resultados.

Cuando un programa cliente invoca una operación de un objeto CORBA, lo hace a través del stub que intercepta la llamada y la entrega al ORB, éste la redirecciona a través de la red hacia el servidor donde reside el objeto CORBA, donde utiliza el esqueleto para invocar la operación requerida y recibir los resultados, que son finalmente entregados al cliente a través del stub.

Los ORB, se comunican entre sí mediante un protocolo estándar denominado IIOP, Protocolo Inter-ORB (Internet Inter-ORB Protocol).

Capítulo 3

INTEGRACIÓN

INTRODUCCIÓN

Integrar tecnologías actuales para un adecuado funcionamiento de las redes, es un punto clave que un administrador de redes debe conocer. Por ello en este capítulo se estudian las tecnologías de telecomunicaciones, telefonía, comunicaciones inalámbricas, Internet2, videoconferencia y evaluación de proyectos.

Los avances de la tecnología de telecomunicaciones se producen día a día, por lo tanto es importante contar con sistemas de multiplexación y de transmisión de señales digitales. Los sistemas PDH, SDH y DWDM permiten una mayor velocidad de transmisión.

La tecnología de telefonía se lleva a cabo por medio del sistema de señalización No. 7. VoIP permite conexiones telefónicas por medio de Internet. Para implementar esta tecnología es necesario conocer los servicios integrados proporcionados por como ISDN y xDSL para la transmisión de datos, voz y video.

Hoy en día las comunicaciones inalámbricas han tenido un gran auge, para integrar esta tecnología es necesario conocer las características y funcionamiento de las redes Wi-Fi y WiMAX, las cuales se basan en los estándares IEEE 802.11 y 802.16.

Las redes GSM ofrecen un servicio de transmisión de datos, éstas se basan en la conmutación de circuitos y en un canal de comunicación que está ocupado por un usuario. Las redes GPRS ofrecen integración de las técnicas de transmisión por paquetes, que permiten acceder a los servicios de Internet, con una mayor velocidad gracias a la utilización de múltiples canales que se atribuyen a un usuario o se comparten con varios. En las comunicaciones móviles son necesarias las técnicas de multiacceso para compartir los recursos radioeléctricos de la interfaz de radio por parte de un conjunto de usuarios, para ello es necesario conocer las técnicas TDMA Y CDMA.

Internet2 se creó como una red alternativa al Internet comercial, para permitir el intercambio y colaboración de investigación y educación entre diversas instituciones educativas. En México el CUDI es el organismo que maneja el proyecto de la red Internet2 que impulsa el desarrollo de aplicaciones, fomentando la colaboración en proyectos de investigación y educación entre sus miembros.

Videoconferencia es un sistema de comunicación diseñado para enlazar uno o varios usuarios a distancia y hace posible la interacción de datos, video y audio con usuarios de cualquier parte del mundo, esta tecnología se basa en los estándares H.320 y H.323.

La evaluación de un proyecto tiene por objetivo conocer su rentabilidad económica y social, de tal manera que se asegure resolver una necesidad humana en forma eficiente, segura y rentable. La metodología de evaluación de proyectos para áreas de cómputo, se centra en el estudio del mercado o cuantificación de las necesidades del servicio, el estudio técnico, el análisis económico y la evaluación económica.

3.1 Tecnología de telecomunicaciones

Los servicios demandados en la actualidad son muy diferentes a los que existían cuando muchas redes de fibra óptica fueron construidas, los cambios en las redes de telecomunicaciones, la convergencia de sus tecnologías y de la informática aunado a múltiples factores, han modificado entre otros muchos aspectos las redes de datos y transporte de telecomunicaciones, que dan servicio ya sea a celulares, redes de fibra óptica, de cobre, aplicaciones de voz y video; motivando la necesidad de mayor capacidad y ancho de banda.

3.1.1 Jerarquía Digital Plesiócrona, PDH

PDH, Jerarquía Digital Plesiócrona (Plesiochronous Digital Hierarchy) arquitectura de multiplexación y de transmisión de señales digitales entre elementos de redes cuyas señales de reloj de muestreo no están sincronizadas con exactitud.

El término *plesiócrono* se deriva del griego *plesio*, cercano y *chronos*, tiempo y se refiere al hecho de que las redes PDH funcionan en un estado donde las diferentes partes de la red están casi, pero no completamente sincronizadas. La tecnología PDH, permite la transmisión de flujos de datos que, nominalmente están funcionando a la misma velocidad de bits por segundo, pero permitiendo una cierta variación alrededor de la velocidad nominal.

PDH es una tecnología usada en telecomunicaciones, para transportar grandes cantidades de información mediante equipos digitales de transmisión, que funcionan sobre fibra óptica, cable coaxial o radio de microondas. También simplifica la planificación de la red haciéndola más fácil de administrar y totalmente compatible con los estándares de la industria.

En la Tabla No. 3.1 se muestran los distintos niveles de multiplexación PDH utilizados en Norteamérica (Estados Unidos y Canadá), Europa y Japón. En México se utiliza la denominación norteamericana.

Nivel	Norteamérica		Europa		Japón
	Mbps	Denominación	Mbps	Denominación	Mbps
1	1,544	T1	2,048	E1	1,544
2	6,312	T2	8,448	E2	6,312
3	44,736	T3	34,368	E3	32,064
4	274,176	T4	139,264	E4	97,728

Tabla No. 3.1 Niveles de multiplexación PDH

La denominación norteamericana, japonesa y europea de sistemas PDH, difieren ligeramente en sus detalles de trabajo, pero los principios de funcionamiento son los mismos, por ello en el Anexo 3.A se describe únicamente la denominación europea.

A. Administración de redes PDH

Se pueden diferenciar al menos 3 etapas de desarrollo, de los sistemas de supervisión de redes digitales:

1. Transmisión de alarmas, consiste en un sistema de multiplexación de alarmas sobre una trama de datos de baja velocidad (hasta 300 bps). Se trata de una operación unidireccional desde las estaciones remotas hacia un concentrador de alarmas. Estos sistemas actuaron hasta la década de los '80.

2. Sistema de telesupervisión, dedicado, permite el diálogo entre las estaciones remotas con una estación master. Permite efectuar la transmisión de alarmas, telecontroles, medidas a distancia y evaluación de la tasa de error BER. La velocidad necesaria para el protocolo de comunicación es relativamente más elevada, en el orden de 1200 bps. Estos sistemas comenzaron con la red digital PDH y se instalan hasta mediados de la década de los '90.
3. Red de administración de telecomunicaciones, permite, además de las funciones anteriormente mencionadas, el almacenamiento de datos y la reconfiguración de la red. Lo interesante de esta red TMN es que se encuentra normalizada por el ITU-T para compatibilidad entre distintos productores, permitiendo la supervisión no sólo de equipos de transmisión sino cualquier otro tipo de equipos. La velocidad de comunicación es más alta debido al incremento de la complejidad en el protocolo de comunicación. Pueden distinguirse 2 etapas, en la primera (1992) como sistema de gestión dedicado a SDH y en la segunda (a partir de 1994) como TMN.

Los equipos PDH están siendo actualmente reemplazados por equipos de tecnología SDH en la mayoría de las redes de telecomunicación, debido a las mayores capacidades de transmisión de estos y a sus mejores condiciones para la operación y mantenimiento centralizado.

3.1.2 Jerarquía Digital Síncrona, SDH

SDH, Jerarquía Digital Síncrona (Synchronous Digital Hierarchy) arquitectura de multiplexación y de transmisión de señales digitales entre elementos de redes cuyas señales de reloj de muestreo son sincronizadas con exactitud.

La unidad de transmisión básica de SDH es el STM-1, Módulo de Transporte Síncrono (Synchronous Transport Module Level 1) con una velocidad de transferencia de 155 Mbps. La descripción de la estructura del STM se muestra en el Anexo 3.B.

SDH permite el transporte de muchos tipos de tráfico tales como voz, video, multimedia y paquetes de datos como los que genera IP. Su papel es, esencialmente administrar la utilización de la infraestructura de fibra, esto significa administrar el ancho de banda eficientemente mientras porta varios tipos de tráfico, detectar fallos y recuperar de ellos la transmisión de forma transparente para las capas superiores.

Las principales características del sistema de red de transporte SDH son: multiplexación digital, fibra óptica, esquemas de protección, sincronización, topologías en anillo y administración de red.

A. Administración de redes SDH

La arquitectura típica del sistema de administración para las redes síncronas contiene los siguientes componentes:

- NE, Elemento de la Red (Network Element) en una red SDH el multiplexor, el equipo terminal de la línea o repetidor, los circuitos de conexión cruzada (Cross-Connect), el equipo de radio enlace y la fuente de sincronismo, son los elementos de la red, los cuales poseen hacia el exterior la interfaz F y Q que permiten la conexión con el sistema de reoperaciones (esta constituido por una o más estaciones de trabajo). La interfaz F admite la conexión de una PC como sistema de administración local.

- Adaptador de interfaz Q, permite adaptar un elemento de la red, NE ya existente a la TMN que se introduce. Los elementos de red SDH ya disponen de interfases F y Q.
- Elemento de medición, permite la conexión entre el elemento de la red y el sistema de operaciones mediante un canal de operación de datos normalizados.
- Sistema de operaciones, se trata de componentes informáticos para el proceso y presentación de la información.

Las funciones de la red administrada se estructuran en 5 niveles, es decir, cada nivel se administra en estratos diferentes, de acuerdo con ITU-T M.3010:

1. BML, Capa de Administración del Sistema (Business Management Layer), para los modelos de largo plazo, planes de servicio y tarifas.
2. SML, Capa de Administración de Servicios (Service Management Layer), para la administración de órdenes de servicio.
3. NML, Capa de Administración de la Red (Network Management Layer), para la administración de alarmas, tráfico, ejecución y configuración de la red.
4. EML, Capa de Administración del Elemento de Red (Element Management Layer), para la administración de alarmas, tráfico, ejecución y configuración de la equipo.
5. NEL, Administración Local del Elemento de Red (Network Element Layer), para las funciones locales de la administración.

3.1.3 Ventajas y desventajas: SDH respecto a PDH

Algunas de estas ventajas son:

- El proceso de multiplexación es mucho más directo. La utilización de punteros permite una localización sencilla y rápida de las señales tributarias de la información.
- El procesamiento de la señal se lleva a cabo a nivel de STM-1. Las señales de velocidades superiores son síncronas entre sí y están en fase por ser generadas localmente por cada nodo de la red.
- Las tramas tributarias de las señales de línea pueden ser subdivididas para acomodar cargas plesiócronas, tráfico ATM o unidades de menor orden. Esto supone mezclar tráfico de distinto tipo dando lugar a redes flexibles.
- Compatibilidad eléctrica y óptica entre los equipos de los distintos suministradores, gracias a los estándares internacionales sobre interfases eléctricos y ópticos.

En cuanto a las desventajas tenemos que:

- Algunas redes PDH actuales presentan ya cierta flexibilidad, pero no son compatibles con SDH.
- Necesidad de sincronismo entre los nodos de la red SDH, se requiere que todos los servicios trabajen bajo una misma referencia de temporización.
- El principio de compatibilidad ha estado por encima de la optimización de ancho de banda. El número de bytes destinados a la cabecera de sección es muy grande, lo que nos lleva a perder eficiencia.

3.1.4 División de Longitud de Onda Densa, DWDM

La tecnología DWDM, División de Longitud de Onda Densa (Dense Wavelenght Division Mutiplexing) permite multiplexar las longitudes de onda que pasan por la fibra óptica. Es una técnica usada para incrementar la capacidad de transmisión de una fibra óptica, esto se logra transmitiendo múltiples señales en diferentes longitudes de onda a través de una sola fibra. Cada señal obtiene una única longitud de onda, o color en el espectro de colores de la luz. Después todas las señales son transmitidas juntas y combinadas como una sola señal. Esto quiere decir, que en un mismo filamento, es posible trasmitir datos, voz y video mediante múltiples formatos y protocolos ver Figura 3.1.

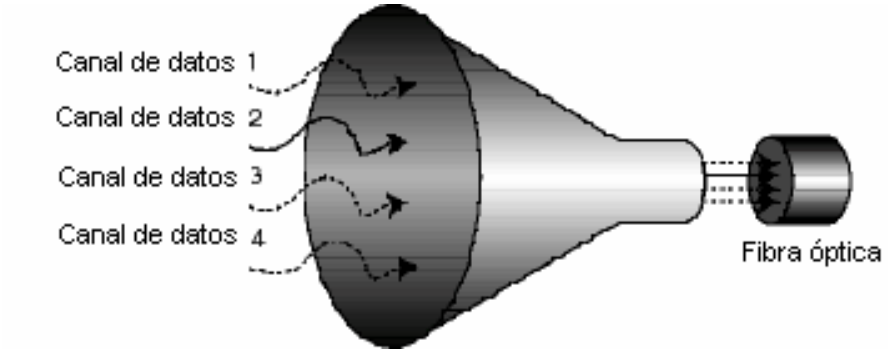


Figura 3.1 Filamento de fibra óptica con tecnología DWDM

"Con el actual trazado y tecnología de iluminación, la fibra permite el traspaso de una tecnología. Es decir, se requiere un filamento para interconectar telefonía, otra para red de datos, otra para protocolo Ethernet, etc. La tecnología DWDM es una tecnología soñada desde hace muchos años, pues admite todo tipo de señales y protocolos en forma simultánea, lo que significa un ahorro importante en la capacidad de la fibra óptica instalada"

A. Ventajas de DWDM

Actualmente, DWDM no es vista solamente como una técnica para ampliar la capacidad de una red de fibra óptica, sino más bien, como una tecnología robusta en el "backbone" de redes multiservicios y redes de acceso móvil, que permite satisfacer el crecimiento en volumen y complejidad que presentan los servicios de telecomunicaciones. Las principales ventajas que ofrece DWDM se enlistan a continuación:

- Aumenta dramáticamente la capacidad de un punto a otro de la red de fibra óptica, lo cual es considerado la aplicación clásica de DWDM. Esto se debe principalmente a la posibilidad de transmitir varias señales dentro de una sola y a las altas tasas de transmisión que soporta.
- Permite transportar cualquier formato de transmisión en cada canal óptico. Así, sin necesidad de utilizar una estructura común para la transmisión de señales, es posible utilizar diferentes longitudes de onda para enviar información síncrona o asíncrona, analógica o digital, a través de la misma fibra.
- Permite utilizar la longitud de onda como una nueva dimensión, además del tiempo y el espacio, en el diseño de redes de comunicación.

3.2 Tecnología de telefonía

3.2.1 Sistema de Señalización No. 7, SS7

Toda llamada telefónica requiere de un sistema de señalización para que ésta sea establecida y mantenida. El envío del número telefónico, el tono de llamada o de ocupado y la información del número del que se llama, son algunos ejemplos de señalización. La señalización, por lo tanto, permite el intercambio de información entre los componentes de una red telefónica para permitir la provisión y el mantenimiento de dicho servicio. Implementar servicios de voz sobre IP en redes de cable, requiere el conocimiento del Sistema de Señalización No. 7, para garantizar la compatibilidad con la red telefónica tradicional.

En México, la organización PU-RDSI, Parte de Usuario de la Red Digital de Servicios Integrados, especifica el modelo de señalización para las redes telefónicas y la norma que la define hace referencia al Plan Técnico Fundamental de Señalización como "Parte de Usuario para Servicios Integrados-México" denominado PAUSI-MX.

SS7, es el estándar de la tecnología conocida como CCS, Señalización de Canal Común (Common Channel Signaling) que consiste en el uso de un canal diferente al canal de voz, destinado únicamente a la señalización. Esta separación permite que, por un lado, se tenga un canal que lleve la conversación y, por otro, un canal que contenga la señalización, de manera que ambos se lleven a cabo de manera independiente. Por este motivo, SS7 es un sistema de señalización fuera de banda que se caracteriza por la transmisión de paquetes de datos a alta velocidad y por la posibilidad de permitir la señalización entre diferentes elementos de la red, entre los cuales no se tiene una comunicación directa.

SS7, permite que algunos de los nodos de la red puedan analizar las señales y, con base en éstas, llevar a cabo alguna acción determinada, gracias a esto ofrece importantes servicios para el usuario final, entre los que destacan el identificador de llamadas, los números gratuitos 01-800 y características de portabilidad del número telefónico, permitiendo que la señalización se lleve a cabo en todo momento, aún cuando no existan llamadas establecidas. Lo anterior pudiera ser útil para activar funciones especiales mediante algún código, sin la necesidad de establecer propiamente una llamada telefónica.

En el SS7 se define una arquitectura y un modelo de capas, éste último es similar en muchos aspectos al modelo de referencia OSI.

La arquitectura de red SS7, consiste en un conjunto interconectado de elementos que intercambian mensajes para llevar a cabo funciones de señalización, para mayores detalles consultar el Anexo 3.C.

3.2.2 Voz sobre el Protocolo de Internet, VoIP

VoIP, Voz sobre el Protocolo Internet (Voice Over IP) es una tecnología de comunicación telefónica que ofrece conexiones a Internet de banda ancha, permitiendo la transmisión de la voz a través de redes IP en forma de paquetes de datos. VoIP permite la integración de todos los servicios (datos, voz y video) sobre un sólo canal, mediante el uso de Internet de banda ancha.

Los elementos principales de una red corporativa de voz, son los sistemas de conmutación, a los que hay que añadir los elementos de transmisión, de supervisión y los propios equipos

de usuarios. Como elementos de conmutación existen varios tipos de dispositivos que pueden desempeñar esta función:

- KTS, Sistemas multilínea (Key Telephone System).
- PBX, Central Privada de Intercambio (Private Brand eXchange).
- Centrex, Oficina Central de Intercambio de Servicio (Central Office Exchange Service).

El soporte de una llamada telefónica sobre una red de paquetes, que en la mayoría de los casos es una red IP consta de dos fases:

1. Establecimiento de la llamada, esto es el equivalente a la obtención de tono de invitación a marcar, la marcación de número destino, la obtención de timbre de llamada o de la señal de ocupado y el descolgado del receptor para contestar la llamada.
2. La propia conversación.

En cualquiera de estas dos fases, es necesaria una serie de estándares que regulen y permitan la interconexión de equipos de distintos fabricantes, como los protocolos de señalización y los protocolos de transporte.

A. Protocolos de señalización

Los protocolos de señalización tienen como objetivo el establecimiento de las llamadas, y son básicamente el corazón de la voz sobre paquetes, distinguiéndola de otros tipos de servicios. Las funciones que realizan son:

1. Localización de usuarios, si un usuario A se desea comunicar con un usuario B, en primer lugar A necesita descubrir la localización actual de B en la red, con el fin de que la petición del establecimiento de sesión pueda establecerse.
2. Establecimiento de sesión, el protocolo de señalización permite al usuario llamado aceptar la llamada, rechazarla o desviarla a otra persona, buzón de voz o página Web.
3. Negociación de la sesión, la sesión multimedia que se esta estableciendo puede comprender diferentes tipos de flujo de información (audio, video, etc). Cada uno de estos flujos puede utilizar algoritmos de compresión de audio y video diferentes, dado que puede tener lugar en diferentes puertos y direcciones unicast o multicast. El proceso de negociación permite a las partes implicadas acordar un conjunto de parámetros de inicialización.
4. Administración de los participantes en la llamada, es posible añadir y/o eliminar miembros de una sesión ya establecida.
5. Otras funciones, como transferir una llamada o el colgar dicha llamada, requiere la conmutación entre los dos extremos.

Para cumplir con todos estos requisitos, existen fundamentalmente tres protocolos:

- H.323, fue concebido para comunicaciones multimedia en redes de área local, pero se ha extendido a la VoIP, proporciona control de llamadas, funciones de conferencia, administración de llamadas, capacidad de negociación de parámetros y otros servicios complementarios.

- SIP, Protocolo para Inicio de Sesión (Session Initiation Protocol) ha sido diseñado para soportar el control de llamadas y la negociación de sesiones de forma distribuida.
- MGCP, Protocolo de Control de Pasarela de Medios (Media Gateway Control Protocol) se trata de un control de protocolo que permite a un controlador central la monitoreo de eventos que ocurren en los teléfonos IP y en las pasarelas, les impone el envío de información a direcciones específicas.

B. Protocolos de transporte

Los protocolos de transporte tienen como objetivo asegurar la comunicación de voz; para el establecimiento de una red para transportar contenidos multimedia bajo demanda de las aplicaciones que la utilizan, no es tarea trivial. Podemos contar con al menos, tres dificultades:

1. Mayores requerimientos de ancho de banda.
2. La mayoría de las aplicaciones multimedia requieren el tráfico en tiempo real.
3. Secuencia de carácter crítico en la generación de los datos multimedia.

Para solucionar estos problemas, se crearon los protocolos de transporte, cuya misión es trasladar la información útil del origen al destino, cumpliendo con los requerimientos exigidos por las aplicaciones multimedia en general y por la voz en particular.

Los protocolos de transporte más empleados en la integración de voz y de datos son:

a. RTP, Protocolo de Transporte en Tiempo Real (Real Time Transport Protocol).

   Las funciones que realiza el RTP son:

   - Fragmentación, cada paquete tiene el número de secuencia empleado para la detección de pérdida durante el reensamblado del mensaje en recepción.
   - Sincronización intermedia, los paquetes del mismo flujo pueden sufrir retardos diferentes, dando lugar a la aparición del jitter. Para compensarlo, las aplicaciones emplean buffers que utilizan las marcas temporales, proporcionadas por el RTP para medir jitter.
   - Identificación del tipo de carga, en una red de paquetes, tanto las condiciones de la red como la perdida de paquetes y el retardo los mismos varían e incluso de la misma llamada.
   - Indicación de trama, las señales de audio y video se envían en unidades lógicas denominadas tramas. Es necesario indicar al receptor el principio y el final de cada una de las tramas, a fin de que pueda sincronizarse con niveles superiores, para lo que emplea un bit de marca.
   - Indicación de fuente, en una sesión multicast existen varios usuarios participantes y debe haber algún modo de poder identificar al usuario que generó un determinado paquete. Esta es la misión del campo SSRC, Fuente de Sincronización (Synchronization Source)

b. RTCP, Protocolo de Control en Tiempo Real (Real Time Control Protocol).

   Las funciones que realiza el RTCP son:

- Realimentación sobre la QoS, los receptores de una sesión emplean RTCP para informar al emisor sobre la calidad de su recepción. Esta información incluye el número de paquetes perdidos, jitter y el RTT, Tiempo Aproximado de Viaje (Round Trip Time) y puede ser empleada por la fuente en aplicaciones adaptativas que ajustan la codificación y otros parámetros en función de la información de retroalimentación.
- Sincronización intermedia, para mejorar el nivel de flexibilidad, el audio y el video que suele transportarse en flujos diferentes que deben sincronizarse en el receptor. Esta capacidad de sincronización es proporcionada por el RTCP incluso en el caso de que los flujos procedan de fuerzas distintas.
- Identificación, los paquetes RTCP contienen información e identificación de cada participante de la sesión, tal como la dirección de correo electrónico, el número de teléfono o el nombre completo de dicho participante, esto permite a todos los participantes conocer la identidad del resto.
- Control de la sesión, RTCP permite a un participante indicar que deja la sesión (envío de paquetes BYE) así como el intercambio de mensajes cortos entre participantes

C. Funcionamiento de VoIP

La operación básica de VoIP se ilustra en la Figura 3.2 y consiste fundamentalmente:

a. Digitalizar la voz en el extremo que emite.
b. Compactar la voz digitalizada.
c. Transmitirla como un conjunto de paquetes de datos por IP.
d. Recibir los paquetes en el otro extremo de la comunicación.
e. Descompactarlos.
f. Reproducirlos para ser escuchados.

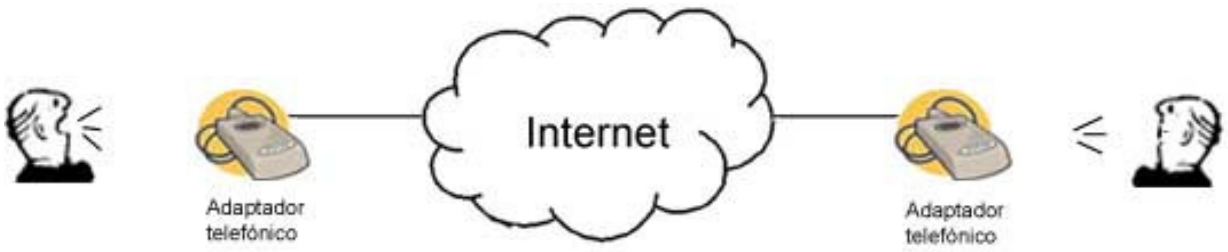


Figura 3.2 Esquema general de VoIP

D. Clases de comunicación de VoIP

Podemos definir dos clases de comunicación VoIP como se describe a continuación:

a. La comunicación IP-IP (Todo en Internet), se logra cuando todos los elementos en comunicación están conectados a Internet, como se representa en la Figura 3.3.

Figura 3.3 Comunicación IP-IP

Lograr una comunicación IP-IP tiene la ventaja de que los elementos principales que inciden sobre el rendimiento y la calidad del servicio están en manos del proveedor del mismo. La desventaja es obviamente que no todas las personas o entidades con las que se desea comunicar cuentan con los elementos para hacerlo, iniciando con una conexión de banda ancha a Internet.

b. La comunicación IP-PSTN, Protocolo de Internet–Red de Servicios de Telefonía Pública (Internet Protocol-Public Service Telephon Network) es decir, entre Internet y la red telefónica. Se tiene cuando alguno de los elementos en comunicación no está conectado a Internet, sino a una red telefónica, como se representa en la Figura 3.4.

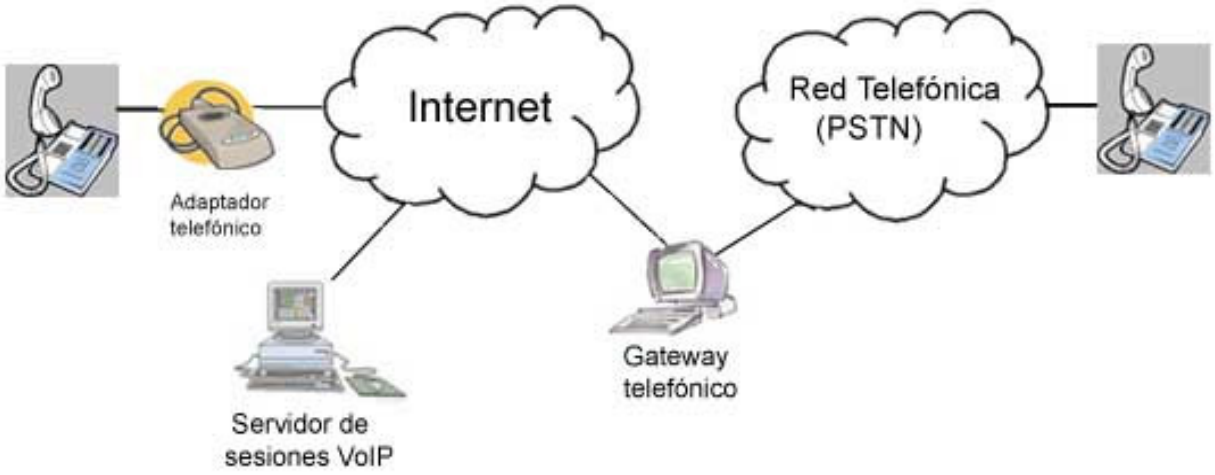


Figura 3.4 Comunicación IP-PSTN

La ventaja de una comunicación IP-PSTN es que puede establecer comunicación con aparatos telefónicos o de fax convencionales, a través de servicios proporcionados por compañías telefónicas a nivel mundial, pero el salto de Internet a la red telefónica introduce elementos fuera del control del proveedor del servicio de VoIP, que en ocasiones van en detrimento de la calidad.

Para hacer o recibir llamadas de VoIP, se requiere de un teléfono convencional de marcado por tonos (no de disco) y de un adaptador ver la Figura 3.5.

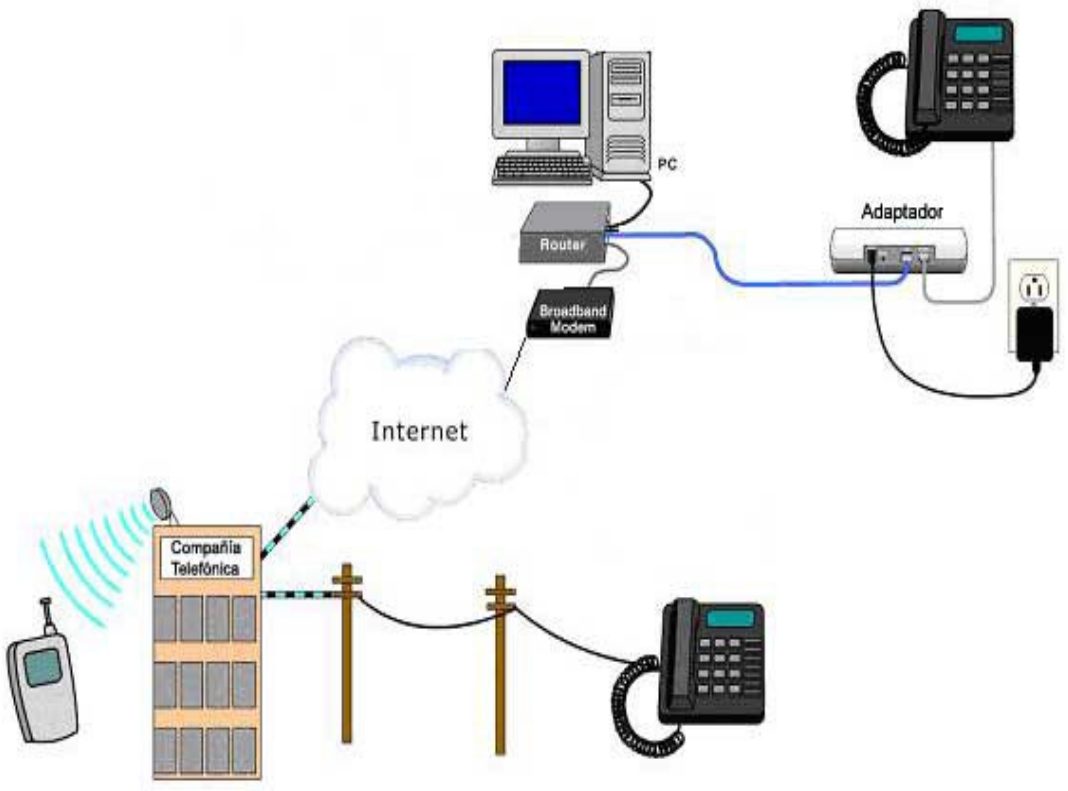


Figura 3.5 Componentes para envío y recepción de llamadas mediante VoIP

Para hacer una llamada se marca de manera semejante a como se hace desde un teléfono convencional, solo que la llamada no es atendida por una compañía telefónica, sino por un servidor conectado en Internet que la procesa y enruta de manera apropiada.

Si la llamada está dirigida a otro aparato de voz por IP, la conexión se hace por Internet. Si la llamada está dirigida a un teléfono convencional, la conexión se termina a través de una compañía telefónica.

3.2.3 ISDN y xDSL

3.2.3.1 Red Digital de Servicios Integrados, ISDN

ISDN, Red Digital de Servicios Integrados (Integrated Services Digital Network) es una tecnología que utiliza la línea telefónica existente para transmitir voz, datos y video simultáneamente. La velocidad de transmisión de esta tecnología es superior a los módems regulares y no es necesario instalar ningún cableado adicional. El servicio ISDN brinda la capacidad de dos líneas de 64Kbps (una para voz y otra para datos o la combinación de ambas, para un total de 128Kbps en servicio de Internet) y uno de 16Kbps para señalización.

Se cuentan con dos tipos de líneas ISDN:

1. Acceso básico, este recurso lo utilizan particularmente pequeñas y medianas empresas, ya que es posible conectarse con varios equipos terminales. Una conexión de acceso básico cuenta con un dispositivo terminador de red de dos canales, facilitando así la utilización de dos equipos o enlaces simultáneos.

2. Acceso primario, este recurso permite la utilización de hasta 30 canales y lo emplean esencialmente las medianas o grandes empresas con grandes servidores para acceso remoto, fax.

Beneficios que proporciona ISDN:

- Mayor velocidad de acceso a Internet (64 Kbps a 128 Kbps).
- Mayor calidad de voz entre usuarios que disponen de ISDN.
- Mayor robustez, seguridad y disponibilidad de las líneas telefónicas.
- Posibilidad para realizar videoconferencias nacionales e internacionales en sala o desde una computadora.

Aplicaciones que proporciona ISDN:

- Servicio de videoconferencia nacional e internacional.
- Servicio de voz y de transmisión de datos.
- Servicio de backups de IPL, Carga Inicial de Programas (Initial Program Load).
- Acceso a Internet de mayor velocidad.

3.2.3.2 Línea Digital de Abonado, xDSL

El término Línea Digital de Abonado (Digital Subscriber Line) denominado a veces xDSL, agrupa varias tecnologías relacionadas que proporcionan un servicio WAN similar a ISDN, pero a velocidades mayores.

DSL utiliza los cables de telefonía estándar para la transmisión de datos desde el domicilio de un usuario al PoP, Punto de Presencia (Point of Presence) de una compañía telefónica por medio de una conexión privada punto a punto. A partir de ahí las señales viajan por el equipo de conmutación estándar de la compañía telefónica, hasta otra conexión DSL en el destino. La distancia entre el sitio y el PoP está limitada, a mayor tasa de transmisión menor distancia operativa.

El hardware necesario para una conexión DSL, en cualquiera de sus modalidades, es una línea telefónica y un módem DSL en ambos extremos del enlace. Para los servicios que proporcionan transmisión simultánea de datos y voz, se requiere un divisor de línea denominado splitter, que separa las frecuencias inferiores utilizadas por el tráfico de voz y las frecuencias superiores utilizadas por el servicio DSL. Los componentes se muestran en la Figura 3.6.

Figura 3.6 Componentes de la tecnología DSL

Las velocidades de transmisión de los servicios DSL varían y algunos de ellos tienen funcionamiento asimétrico, esto significa que tienen velocidades diferentes de subida y de bajada. Esta variación se debe a que el manojo de cables del PoP es más susceptible a un tipo de interferencia denominada diafonía del extremo cercano.

Las comunicaciones telefónicas utilizan una pequeña cantidad del ancho de banda que proporciona el cable tradicional. DSL utiliza frecuencias por encima del ancho de banda de telefonía estándar (300 a 3200 Hz) y métodos de codificación de señal avanzados para transmitir datos a mayor velocidad.

Algunos servicios DSL emplean frecuencias fuera del rango de las comunicaciones de voz estándar, por lo que la línea se utiliza para tráfico normal de voz al mismo tiempo que transmite datos digitales.

Los diversos servicios DSL, disponen de abreviaturas con la primera letra diferente por lo que a veces se les denomina, xDSL, con la "x" actuando como comodín, los servicios y sus propiedades se muestran en la Tabla No. 3.2.

Nombre de la tecnología	Concepto	Velocidad de bajada	Velocidad de subida	Distancia máxima
IDSL	ISDN DSL	144 Kbps	144 Kbps	5.5 km
HDSL	High-Data Rate DSL	1,544 Mbps	1,544 Mbps	3.6-4.6 km
SDSL	Symetric DSL	1,544 Mbps	1,544 Mbps	3km
ADSL	Asymetric DSL	1544-8444 Mbps	640 Kbps-1544 Mbps	3-5.5km
RADSL	Rate Adaptive DSL	1544-8448 Mbps	640 Kbps-1544 Mbps	3-5.5km
VDSL	Very-High DSL	12.96-51.84 Mbps	1.6-2.3 Mbps	300-1400m

Tabla No. 3.2 Tecnologías xDSL

a. IDSL, Línea Digital de Abonado por ISDN, los circuitos de IDSL llevan los datos, no voz. Se aplica principalmente como acceso a Internet, Intranet, acceso remoto a LAN, telefonía IP, videoconferencia, etc.

b. HDSL, Línea Digital de Abonado de Alta Velocidad (High Data-Rate DSL) es la más antigua de las variantes de xDSL. Se usa para transmisión digital de banda ancha dentro de instalaciones de empresas y compañías telefónicas que requieren dos cables entrelazados y que usan líneas T1. La principal característica de HDSL es que es simétrica; está disponible una cantidad igual de ancho de banda en ambas direcciones. Por esta razón, su máxima tasa de transferencia de datos es menor que la de ADSL. Esta tecnología esta sustituyendo a T1 y E1 para conexiones a Internet e interconexiones de LAN.

c. SDSL, Línea Digital de Abonado Simétrica (Symmetric Digital Subscriber Line) cuenta con la posibilidad de la transmisión de voz simultánea. Esta tecnología esta sustituyendo a T1 y E1 para conexiones a Internet, interconexiones de LAN.

d. ADSL, Línea Digital de Abonado Asimétrica (Asymmetrical Digital Subscriber Line) útil para la transmisión de video bajo demanda, voz sobre IP, redes privadas virtuales, acceso a Internet/Intranet, acceso remoto a LAN.

e. RADSL, Línea Digital de Abonado de Tasa Adaptable (Rate Adaptive Digital Subscriber Line) la velocidad de transmisión se ajusta de manera dinámica según la longitud del enlace y la calidad de la señal. Existe la posibilidad de transmitir voz simultánea.

f. VDSL, Línea Digital de Abonado de Muy Alta Velocidad (Very-High-Speed Digital Subscriber Line) probablemente será una tecnología con preferencia de uso en aplicaciones con mayor ancho de banda, como manejo de imágenes médicas, video en tiempo real o televisión de alta definición.

Cabe mencionar que DSL utiliza conexiones permanentes, no dispone de servicio de marcación, ningún número asignado a las conexiones y ningún procedimiento de establecimiento de sesión. La conexión está continuamente activada y es privada. Como solución de acceso a Internet ha crecido por su precio relativamente bajo y su elevada velocidad de transmisión. Las compañías telefónicas implementan HDSL para sus propias líneas, pues pueden realizar las mismas funciones que la infraestructura T1 y E1 convencional, sin requerir un cable con condiciones especiales y con la mitad de repetidores a lo largo del recorrido de la conexión. Para los usuarios domésticos ADSL, se comercializa como solución de acceso a Internet.

3.3 Comunicaciones inalámbricas

En sus inicios, las aplicaciones de las redes inalámbricas fueron confinadas a industrias y grandes almacenes. Hoy en día las WLAN, Redes Inalámbricas de Área Local (Wireless Local Area Network), son instaladas en Universidades, oficinas, hogares y hasta en espacios públicos. Las WLAN se componen de computadoras portátiles o de escritorio que se conectan a dispositivos fijos llamados AP, Puntos de Acceso (Access Points) vía señales de radio o infrarrojo.

Las implementaciones de las WLAN abarcan todas las modalidades posibles, desde las PAN, Red de Área Personal (Personal Area Networks); MAN, Red de Área Metropolitana (Metropolitan Area Network); hasta las WAN, Red de Área Amplia (Wide Area Networks).

La PAN es una red inalámbrica de corto alcance, generalmente para uso en interiores a pocos metros. Mientras que las redes inalámbricas tipo WAN y MAN consisten de torres y antenas que transmiten ondas de radio o usan tecnología de microondas para conectar redes de área local, utilizando enlaces punto-punto y punto-multipunto. Otra característica importante de los productos WLAN es la interoperatibilidad. Gracias al desarrollo de estándares, pueden mezclarse dispositivos inalámbricos de diversos fabricantes haciendo un acceso más directo y transparente con la tecnología.

3.3.1 Estándares IEEE 802.11 y 802.16

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso de la IEEE, y la ETSI, Instituto Europeo de Estándares de Telecomunicaciones (European Telecommunications Standards Institute). Una vez aceptados se convierten en la base de los fabricantes para desarrollar sus productos.

3.3.1.1 Estándar IEEE 802.11

IEEE 802.11 es un estándar de comunicaciones que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando las normas de funcionamiento en una WLAN, que emplea ondas de radio en la banda de 2.4 GHz y 5 GHz.

El estándar cumple con los siguientes requisitos:

- Admite estaciones fijas, portátiles o móviles dentro de un área local.
- Proporciona conectividad inalámbrica.

Los dos niveles que aplica el estándar son:

A. Nivel físico

El nivel físico definido en el estándar 802.11 establece dos posibles topologías y tres tipos de medios inalámbricos, que funcionan a cuatro velocidades posibles.

El bloque constructivo fundamental de una LAN inalámbrica es el BSS, Conjunto de Servicios Básicos (Basic Services Set), el cual es un área geográfica en la que las estaciones inalámbricas se pueden comunicar. La configuración y el área BSS dependen del tipo de medio inalámbrico que se use y de la naturaleza del entorno.

El estándar define dos tipos de topologías red inalámbrica:

- La topología ad hoc, en donde los dispositivos de la red dentro de BSS son móviles o portátiles, es decir inalámbricos, esta limitada a un máximo de 10 dispositivos, ver Figura 3.7.

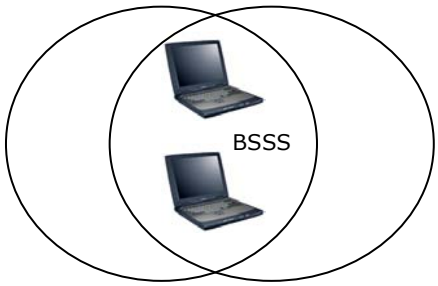


Figura 3.7. Topología ad hoc

- La topología de infraestructura, consta de al menos un AP, Punto de Acceso (Access Point) inalámbrico, que es un dispositivo autónomo o bien un equipo que incluye un dispositivo inalámbrico y que puede estar o no conectado a un red fija estándar por medio de un cable o por dos o más estaciones inalámbricas, ver Figura 3.8.

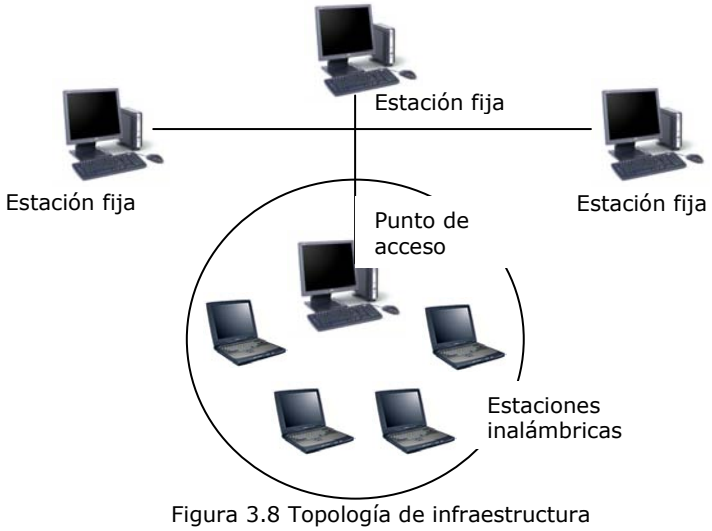


Figura 3.8 Topología de infraestructura

El estándar define tres medios de nivel físico, dos que usan señales de RF, Radiofrecuencia (Radio Frequency) y uno que usa señales de infrarrojos, los cuales utilizan el mismo nivel de acceso al medio, estos medios del nivel físico se describen a continuación:

- FHSS, Espectro Extendido de Salto de Frecuencia (Frecuency Hopping Spread Spectrum) banda de frecuencia de 2.4 GHz, ancho de banda de 83 MHz, es decir entre 2400 y 2483 GHz, usa un código o algoritmo predeterminado para imponer cambios de frecuencia continuamente, en incrementos discretos, sobre una amplia banda de frecuencias. La implementación exige 79 canales de 1MHz esto es para el emisor y receptor y define una velocidad de 1Mbps, con una velocidad opcional de 2Mbps.
- DSSS, Espectro Extendido de Secuencia Directa (Direct Sequence Spread Sprectrum), banda de frecuencia de 2.4 GHz, ancho de banda de 83 MHz, es decir entre 2400 y 2483 GHz, utiliza un código digital chip o código por chip, que tiene una velocidad de bit más alta que la señal de datos, soporta velocidades de transmisión de 1 Mbps y 2 Mbps.
- Infrarrojos, usan frecuencias en el intervalo 850 a 950 nanómetros, soportan una velocidad de transmisión de 1 Mbps y una velocidad operacional de 2 Mbps, con un alcance de 10 m a 20 m.

En el estándar se definen las tramas de nivel físico que tienen su propio formato y existen tres tipos:

1. Trama del espectro extendido de salto de frecuencia.
2. Trama de espectro extendido de secuencia directa.
3. Trama de infrarrojos.

B. Nivel de enlace de datos

El estándar define la funcionalidad del subnivel MAC, Control de Acceso al Medio (Medium Access Control), que consiste en un servicio del transporte no orientado a conexión que lleva los datos LLC, Control de Enlace Lógico (Logical Link Control) a un destino de la red en forma de MSDU, Unidades de Datos de Servicio MAC (MAC Service Data Unit). Este servicio se define por un formato de trama y un mecanismo de control de acceso al medio.

El estándar define tres tipos básicos de trama del nivel MAC:

- Tramas de datos, utilizadas para transmitir datos de los niveles superiores entre estaciones.
- Tramas de control, utilizadas para regular el acceso al medio de la red y para reconocer las tramas de datos transmitidas.
- Tramas de administración, utilizadas para intercambiar información de administración de la red para realizar funciones de red, como asociación y autenticación.

A partir del nivel de red hacia arriba, los sistemas pueden emplear cualquier conjunto de protocolos, como el TCP/IP o IPX.

Además de este documento existen tres suplementos llamados IEEE 802.11a, 802.11b y 802.11g, los cuales no son documentos utilizables de modo aislado y cuyos cambios deben aplicarse al estándar original. A continuación se muestran la evolución que ha tenido el estándar 802.11, ver Tabla No. 3.3.

	802.11			802.11a	802.11b	802.11g
	FHSS	**DSSS**	**INFRARROJOS**			
Frecuencia	2.4 GHz	2.4 GHz	850 y 950 nanómetros	5 GHz	2.4 GHz	2.4 GHz
Ancho de Banda	83 MHz 2400 y 2483 GHz	83 MHz 2400 y 2483 GHz	3 a $15x10^{14}$Hz	2400 GHz	83 MHz 2400 y 2483 GHz	83 MHz 2400 y 2483 GHz
Velocidad de transmisión	1 a 2 Mbps	1 a 2 Mbps	1 a 2 Mbps	54 Mbps	5.5 y 11 Mbps	22 y 54 Mbps
Alcance	-	-	-	50 m	100 m	mayor que
Medio Físico	-	-	-	OFDM	DSSS	DSSS y OFDM

Tabla No. 3.3 Versiones del estándar IEEE 802.11 para redes inalámbricas

a. WLAN 802.11a, Wi-Fi 5, en julio de 1999 se aprobó el estándar 802.11a, que con una QAM-64, Modulación de Amplitud en Cuadratura (Quadrature Amplitude Modulation) y la codificación OFDM, Modulación por División Ortogonal de Frecuencia (Orthogonal Frequency Division Multiplexing) alcanza una velocidad de hasta 54 Mbps en la banda de 5 GHz, menos congestionada, con un alcance limitado a 50 m.

b. WLAN 802.11b, Wi-Fi, en el año 1999, se aprobó el estándar 802.11b, con una velocidad de transmisión de 5.5 y de 11 Mbps y un alcance de 100m, que al igual que Bluetooth y Home RF, también emplea la banda de ISM, Industrial, Científica y Médica (Industrial, Scientific and Medical) de 2.4 GHz, pero en lugar de una simple modulación de radio digital y FH, Salto de Frecuencia (Frequency Hopping), utiliza una la modulación lineal compleja como DSSS. Permite mayor velocidad, pero presenta una menor seguridad.

c. WLAN 802.11g, Wi-Fi, en el año 2003 se aprobó el estándar 802.11g, con una velocidad de 22 Mbps o hasta incluso 54 Mbps, emplea la banda de 2.4 GHz.

Existen otras actualizaciones al estándar, algunas actualmente se están trabajando y desarrollando por grupos de trabajo, una muestra de estas son:

- WLAN 802.1x, proporciona un mecanismo para autenticar equipos que se conectan a un punto de acceso inalámbricos, típicamente a través de un servidor RADIUS, Servicio de Autenticación Remota de Usuarios por Marcación (Remote Authentication Dial-In User Service) este estándar emergente no es práctico para redes pequeñas pero es ideal para grandes organizaciones, ya que tiene uno o más servidores de autenticación. Este estándar se aplica tanto en redes cableadas convencionales como a las redes inalámbricas.
- WLAN 801.11i, es el sucesor del WEP, está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP, Protocolo de Llaves Íntegras, Seguras-Temporales (Temporary Keys Integrity Protocolo) y AES, Estándar de Cifrado Avanzado (Advance Encription Standar).
- WLAN 802.11e, está dirigido a los requerimientos de calidad de servicio para todas las interfases IEEE WLAN de radio.

- WLAN 802.11f, define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
- WLAN 802.11h, define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.

3.3.1.2 Estándar IEEE 802.16

IEEE 802.16 denominado WiMAX, Interoperabilidad Mundial para Acceso por Microondas (Worldwide Interoperability for Microwave Access) presenta algunas de las características:

- Radio de acción hasta de 50 km.
- Gran ancho de banda: una sola estación de base puede admitir de manera simultánea más de 60 empresas con conectividad tipo T1/E1 o cientos de hogares con conexión tipo DSL.
- Es independiente de protocolos, puede transportar: IP, Ethernet, ATM.
- Transmite otros servicios agregados como: VoIP, datos y video.
- Compatible con las antenas de telefonía de tercera generación (denominadas "antenas inteligentes"), que gracias a la emisión de un haz acotado apuntan constantemente al receptor aún en movimiento.

El principal componente es una antena colocada en una torre con una cobertura de hasta 7500 km^2. El segundo elemento es el receptor WiMAX, que puede ir desde una caja colocada en el techo de la casa, hasta algo tan pequeño como una tarjeta PCMCIA en una computadora portátil.

Una antena WiMAX estará conectada al ISP, Proveedor de Servicios de Internet (Internet Service Provider) por medio de fibra óptica o cable con gran ancho de banda (30 Mbps o más) y esa misma antena, en el modelo de la telefonía celular, podrá ser el punto de acceso a la red tanto de usuarios móviles como de otras antenas funcionando como repetidoras, sin conexión por cable alguno. De esta forma, la tecnología WiMAX permite enlazar zonas rurales o de difícil acceso, donde las compañías de telecomunicaciones no han colocado cables por el costo de instalación o mantenimiento.

Parte fundamental de la cobertura, estabilidad e impacto de las redes MAN apoyadas en WiMAX, radica en la frecuencia de transmisión. Existiendo dos alternativas:

1. Cuando el equipo del usuario se encuentre en una zona con varios obstáculos (edificios, árboles, cerros, etc.) se usará una baja frecuencia, en el orden de los 2 a 11 GHz. Estas frecuencias son menos susceptibles a la pérdida del enlace por algún objeto que se interponga entre la antena WiMAX y el dispositivo del usuario. El precio por pagar para mantener la conectividad, es que el ancho de banda también será inferior a los 54 Mbps.
2. Si existe línea de vista, es decir, cero obstáculos entre la antena WiMAX y el equipo del usuario, se podrá optar por una mayor frecuencia, hasta 66 GHz, con el considerable incremento en el ancho de banda. La norma 802.16 establece un tope de 70 Mbps.

A partir de las variaciones en el uso de frecuencias, es claro determinar que equipos de mayor capacidad, como es el caso de los routers, preferentemente estarán asociados a una conexión de alta frecuencia con las antenas WiMAX y los equipos de mayor movilidad, como

las computadoras portátiles, seguirán asociándose a redes WiFi o WiMAX en menores frecuencias y anchos de banda.

Una de las aplicaciones de WiMAX podría ser utilizada para ampliar los servicios de telecomunicaciones a nivel gubernamental, empresarial e institucional. Una Universidad podrá proporcionar acceso a la red en todo su campus con una sola antena, a la suficiente altura y ubicación. Los gobiernos pueden respaldar los actuales esquemas de comunicación de datos por medios inalámbricos, usando celdas WiMAX ubicadas de manera estratégica en zonas de acceso controlado.

En el ámbito social, la combinación de WiFi, WiMAX y la telefonía VoIP permitirá el despliegue de más líneas de telecomunicaciones hacia zonas apartadas, con ancho de banda suficiente para la integración de servicios multimedia: voz, video y datos.

3.3.2 TDMA y CDMA

En comunicaciones móviles son necesarias las técnicas de multiacceso, para compartir los recursos radioeléctricos de la interfaz de radio, por parte de un conjunto de usuarios. Se denomina canal físico, a la facilidad concedida a un usuario mediante la cual éste puede acceder al sistema. Las técnicas de multiacceso son procedimientos de asignación de canales físicos a las estaciones. En general, están asociadas con los métodos de modulación utilizados y con la naturaleza (analógica o digital) de la información a transmitir.

A. Acceso Múltiple por División del Tiempo, TDMA

En la técnica TDMA, Acceso Múltiple por División del Tiempo (Time Division Multiplex Access) se asigna a los usuarios una misma frecuencia durante breves intervalos de tiempo, de forma periódica, de manera que los usuarios efectúan transmisiones simultáneas pero discontinuas, en esa frecuencia portadora mediante ráfagas o paquetes de información.

El sistema dispone de mecanismos de direccionamiento y sincronización de forma que cada receptor extrae del flujo de señal únicamente las ráfagas destinadas al mismo e ignora las demás.

En TDMA la transmisión se organiza en tramas, una trama es una sucesión de intervalos, cada uno de los cuales se asigna a una terminal. El tiempo en el cual el terminal efectúa su acceso y en el que dispone de todo el recurso del ancho de banda del sistema radioeléctrico, es la duración del intervalo. Toda terminal transmite en un tiempo, la información de tráfico recopilada durante una trama más otras señales auxiliares, en un proceso de almacenamiento y envío. La información se transmite en forma de un tren de bits llamados ráfaga (burst). Por su propia naturaleza TDMA únicamente es posible con señales digitales de origen o analógicas digitalizadas.

TDMA es una tecnología inalámbrica de segunda generación que brinda servicios de alta calidad de voz y datos de circuito conmutado en las bandas más usadas del espectro, también se conoce como ANSI-136 o IS-136, por las normas que definen sus características.

La técnica TDMA ofrece las siguientes características:

- Complejidad del acceso, requiere de estricta sincronización temporal para evitar colisiones de ráfagas.
- Simplificación de las estaciones base multicanales, el transceptor proporciona N canales.

- Limitación en el tamaño de la trama.
- Retardo en la comunicación, como la transmisión es discontinua, la información es discontinua, por lo cual debe de acumularse en una memoria para su posterior lectura y presentación de forma continua.
- Elevada versatilidad, puede acumularse los intervalos de los usuarios.
- Necesidad de digitalización de la información.
- Transmisiones de banda ancha, afectada por perturbaciones generadas en el medio radioeléctrico que deben contrarrestarse.
- Facilidad de la señalización asociada a una comunicación que puede insertarse en campos de bits dentro de la ráfaga o en intervalos específicos dentro de la tramas sin alterar la estructura de TDMA.
- Idoneidad para media/alta capacidad de tráfico derivada de su buen rendimiento espectral.
- Posibilidad de transmisión dúplex con una sola frecuencia (dúplex temporal).

B. Acceso Múltiple por División de Código, CDMA

La técnica CDMA, Acceso Múltiple por División de Código (Code Division Multiplex Access) otorga a cada canal la totalidad del volumen espectral disponible; todo el ancho de banda, durante todo el tiempo y en toda la zona de cobertura de forma que permite la transmisión simultánea de varias comunicaciones, que emplean todos los mismos recursos a la vez. La separación entre ellas se realiza asignándoles distintos códigos digitales.

La técnica CDMA utiliza la llamada modulación de SS, Espectro Ensanchado (Spread Spectrum) que consiste en la manipulación de la señal digital a transmitir de banda ancha, por otra señal digital de banda ancha llamada código de ensanchamiento o código de dirección. La señal resultante tiene un gran ancho de banda y se denomina ensanchada. Si se multiplica está señal por la señal de código se produce el efecto contrario de compresión.

La técnica CDMA ofrece una amplia capacidad de canales y tiene las siguientes características básicas:

- Requiere que las señales a transmitir y los códigos de dirección sean digitales.
- Es una técnica intrínsecamente de banda ancha.
- Ofrece gran capacidad de tráfico.
- Debido a la gran anchura de banda, los receptores CDMA poseen gran resolución temporal, ya que extraen los ecos de la señal debido a la propagación multitrayecto.
- Requiere estricta sincronización y control de potencia de las transmisiones. Las señales han de llegar a las estaciones con potencias similares para que se pueda efectuar su separación.
- Únicamente se requiere de un transceptor físico en la estación base para sustentar múltiples canales.
- La tecnología a utilizar en CDMA es muy compleja y requiere una elevada integración para conseguir terminales livianos y de reducido tamaño.

- En entornos continuos puede utilizarse las mismas frecuencias, lo cual mejora la calidad del traspaso de comunicaciones de una BS, Estación Base (Bases Station) a otra continua.

3.3.3 GSM y GPRS

La principal característica de la telefonía móvil digital, es que la voz y toda la información se convierte en una sucesión de unos y ceros antes de ser transmitida, protegiendo la información y evitando que pueda ser interceptada por terceras personas.

Los sistemas analógicos transmitían y recibían la información de la misma manera que una estación de radio, de modo que cualquier persona con un receptor de radio puede interceptar la comunicación. Los teléfonos digitales codifican en formato digital tanto la voz y los datos que sólo el teléfono al que estamos llamando puede volver a decodificar.

Las redes GSM ofrecen un servicio de transmisión de datos, éstas se basan en la conmutación de circuitos y en un canal de comunicación que está ocupado por un usuario. Por tal razón el ETSI recomienda la integración de las técnicas de transmisión por paquetes denominadas GPRS, que permiten acceder a los servicios de Internet con una mayor velocidad gracias a la utilización de múltiples canales que se atribuyen a un usuario o se comparten con varios.

3.3.3.1 Sistema Global para Comunicaciones Móviles, GSM

En 1982, un consorcio de países europeos creó GSM, Grupo Especial Móvil (Groupe Special Mobile) para desarrollar una tecnología celular que proporcionará roaming internacional imperceptible al usuario y soporte para servicios avanzados no disponibles en las redes analógicas. El ETSI se hizo cargo del proyecto en 1989 y completó la primera serie de especificaciones técnicas. La primera red GSM fue lanzada en 1991, y fue seguida por varias más el año siguiente. Al adoptarse la tecnología en países no europeos, se hizo evidente que GSM sería una tecnología global y no europea; así fue como la sigla GSM comenzó a significar Sistema Global para Comunicaciones Móviles (Global System For Mobile Comunications), con una velocidad máxima de 9.6 Kbps.

GSM es un sistema de comunicación basado en el uso de células digitales, que se desarrolló para crear un sistema para celulares único, que sirviese de estándar para Europa y que fuese compatible con los servicios existentes y futuros sobre ISDN.

El número de servicios que se han ido desarrollando sobre GSM han evolucionando con el paso del tiempo, los servicios que se van incorporando a GSM se llevan a cabo por el MoU, Memorando de Entendimiento (Memorando of Understanding) que viene a ser como un subgrupo encargado de estos temas, el MoU ha definido tres tipos de categorías de servicios que pueden ofrecerse sobre una red GSM y se describen a continuación:

- Teleservicios, que engloba a los servicios básicos de telefonía, como las llamadas de emergencia; SMS, Servicio de Mensajes Cortos (Short Messaging Services); Servicios de fax y Voz.
- Servicios portadores, que son los usados para la transmisión y recepción síncrona y asíncrona de datos.
- Servicios complementarios, como la llamada en espera, la llamada múltiple e identificación de llamada.

La tecnología GSM esta basado en dos principios y su arquitectura, las cuales se muestran a continuación:

A. Los sistemas celulares

Los sistemas celulares se basan en la división del área de cobertura de un operador en lo que se denomina células, éstas se caracterizan por su tamaño que está determinado por la potencia del transmisor, la cual debe ser lo más baja posible a fin de poder reutilizar el mayor número de frecuencias para obtener un mayor número de usuarios que pueden hacer uso del sistema, ya que cada uno puede usar una frecuencia sin interferir en la de otro usuario. La distancia que debe existir entre dos células debe ser lo suficientemente grande como para que no se produzca interferencia entre ellas; también existen determinados canales que se reservan para labores de señalización y control de toda la red.

Las células se unen a otras mediante cable, o bien a través radio enlaces, así como con la red telefónica fija.

El siguiente nivel de organización que existe en GSM es el de cluster, que no es más que un conjunto de células agrupadas entre sí, estos clusters suelen agrupar conjuntos de 4, 7, 12 ó 21 células distintas que se distribuyen por toda el área de cobertura del operador.

B. Tipos de células

En GSM se distinguen cuatro tipos diferentes de células:

- Macrocélulas (Macrocells), son células de gran tamaño utilizadas en áreas de terreno muy grandes y donde la distancia entre áreas pobladas es muy distante entre sí.
- Microcélulas (Microcells), se utilizan en áreas donde hay una gran densidad de población.
- Células selectivas (Selectived Cells), célula con un alcance y un radio de acción determinado.
- Células Sombrilla (Umbrella Cells), células que utilizan un elevado número de células de tamaño pequeño y continuamente se están produciendo cambios (hand-over) del terminal de una célula a otra para evitar que suceda esto lo que se hace es agrupar conjuntos de microcélulas de modo que aumente la potencia de la nueva célula formada y así poder reducir el número de hand-over que se producen.

C. Arquitectura de una red GSM

Todas las redes GSM se pueden dividir en cuatro partes fundamentales:

1. MS, Estación Móvil (Mobile Station), consta a su vez de dos elementos básicos, por un lado el terminal o equipo móvil y por otro lado el SIM, Módulo de Identidad de Abonado (Subscriber Identity Module).
    - Los terminales (teléfonos celulares) se diferencian entre unos y otros en la potencia que tienen que va desde los 2 watts hasta los 20 watts(generalmente instalados en vehículos).
    - El SIM es una pequeña tarjeta inteligente que sirve para identificar las características de la terminal, permite al usuario acceder a todos los servicios que haya disponibles por su operador, la ventaja es que proporcionan movilidad al usuario ya que puede cambiar de terminal y llevarse consigo el SIM. Una vez que

se introduce el PIN, Número de Identidad Personal (Personal Identity Number) en el terminal, éste va a ponerse a buscar redes GSM que estén disponibles y va a tratar de validarse en ellas, una vez que la red (generalmente con la que se tiene contrato) ha validado el terminal, el teléfono queda registrado en la célula que lo ha validado.

2. BSS, Subsistema de Estación Base (Base Station Subsystem), sirve para conectar a las estaciones móviles con los NSS, además se encargan de la transmisión y recepción; consta de dos elementos:
   - BTS, Estación Radio Base (Base Transceiver Station) consta de transceivers y antenas usadas en cada célula de la red y que suelen estar situadas en el centro de la célula, generalmente su potencia de transmisión determinan el tamaño de la célula, ver Figura 3.9.
   - BSC, Controlador de Estación de Base (Base Station Controller) se utiliza como controlador de los BTS y tienen como funciones principales las de estar al cargo de los hand-overs, los saltos de frecuencia (Frequency Hopping) y los controles de las frecuencias de radio de los BTS.

Figura 3.9 Estación Radio Base

3. NSS, Subsistema de Conmutación y Red (Network and Switching Subsystem), este sistema se encarga de administrar las comunicaciones que se realizan entre los diferentes usuarios de la red, para poder hacer este trabajo la NSS se divide en siete sistemas diferentes, cada uno con una misión dentro de la red:
   - MSC, Conmutador de Red GSM (Mobile Switching Center) es el componente central del NSS y se encarga de realizar las labores de conmutación dentro de la red, así como de proporcionar conexión con otras redes.
   - GMSC, Centro de Conmutación de Movilidad de Entrada (Gateway Mobile Switching Center) dispositivo traductor que sirve de mediador entre las redes de telefonía fijas y la red GSM.
   - HLR, Registro de Abonados Locales (Home Location Registrer) es una base de datos que contiene información sobre los usuarios conectados a un determinado MSC. Entre la información que almacena el HLR tenemos fundamentalmente la

localización del usuario y los servicios a los que tiene acceso. El HRL funciona en unión con el VLR.

- VLR, Registro de Localización de Visitantes (Visitor Location Registrer) contiene toda la información necesaria sobre un usuario para que pueda acceder a los servicios de red. Forma parte del HLR con quien comparte funcionalidad.
- AUC, Centro de Autentificación (Authentication Center) proporciona los parámetros necesarios para la autenticación de usuarios dentro de la red; también se encarga de soportar funciones de cifrado.
- EIR, Registro de Identificación de Equipos (Equipment Identy Registrer) se utiliza para proporcionar seguridad en las redes GSM pero a nivel de equipos válidos. La EIR contiene una base de datos con todos los terminales que son válidos para ser usados en la red. Esta base de datos contiene los IMEI, Identidad Internacional de Equipos Móviles (International Mobile Equipment Identity) de cada terminal, de manera que si un determinado móvil trata de hacer uso de la red y su IMEI no se encuentra localizado en la base de datos del EIR no puede hacer uso de la red.
- GIWU, Unidad de Trabajo de GSM (GSM Interworking Unit) sirve como interfaz de comunicación entre diferentes redes para transferencia de datos.

4. OSS, Subsistemas de Soporte y Operación (Operation and Support Subsystem), se conectan a diferentes NSS y BSC para controlar y monitorear toda la red GSM. La tendencia actual en estos sistemas es que, dado que el número de BSS se está incrementando se pretende delegar funciones que actualmente se encarga de hacerlas el subsistema OSS en los BTS de modo que se reduzcan los costos de mantenimiento del sistema.

En GSM hay dos aspectos que forman parte del funcionamiento normal cuando se viaja, el primero es el roaming que se produce cuando se valida dentro de la red GSM y el terminal no es capaz de encontrar la red del cual sé es cliente y consiste en la utilización de la red que se encuentra disponible. El segundo aspecto es el hand-over, que consiste en la transición que se produce cuando pasamos del rango de acción de una célula al rango de acción de otra, es responsable de mantener el servicio de manera constante y de que las transiciones entre una célula y otra sean lo suficientemente pequeñas como para pasar desapercibidas por los usuarios.

3.3.3.2 Servicio de Radiotransmisión de Paquetes Generales, GPRS

GPRS, Servicio de Radiotransmisión de Paquetes Generales (General Packet Radio Service) es una nueva tecnología basada en las redes GSM, que permite acceder a los servicios de Internet con una velocidad de alcance de hasta los 115 Kbps, gracias a que utiliza múltiples canales de radio.

Los servicios móviles para Internet o Intranet que se encuentran disponibles son: la oficina móvil (remote access) o conexión remota a la red de la empresa, el correo electrónico, el acceso a Internet, el comercio electrónico, los servicios de información localizados, la telemetría entre otros.

El nodo de soporte GSN, Nodo de Soporte de Entrada (Gateway Support Node) del GPRS es el elemento principal de la infraestructura. Este routerr puede proporcionar la conexión y el trabajo con otras redes de datos, puede administrar la movilidad de los usuarios a través de los registros del GPRS y es capaz de entregar los paquetes de datos a las estaciones móviles, independientemente de su posición. Físicamente el GSN puede estar integrado en el

MSC o puede ser un elemento separado de la red, basado en la arquitectura de los routers de las redes de datos. Los paquetes de datos del usuario pasan directamente entre el GSN y el BSS, gracias a la señalización que acontece entre GSN y el MSC.

A. Arquitectura de la red

Para la realización de un servicio de datos por paquetes en la red celular GSM se pueden seguir dos inicializaciones diferentes:

- Inicialización de sistema integrado, procura que toda la infraestructura necesaria para el soporte del servicio sea añadida a la red GSM.
- Inicialización de sistema separado procura el añadido de la funcionalidad necesaria para el soporte del GPRS a las entidades que componen la infraestructura de la red GSM.

En realidad, también la inicialización de sistema integrado requiere la introducción de nuevas entidades, garantizando, desde el punto de vista económico, un impacto menos vistoso sobre los costos necesarios para la implementación del servicio.

Las entidades que tienen que ser añadidas, desde el punto de vista de la integración del servicio GPRS en la red GSM, son:

- GSN, Nodo de Soporte de Entrada (Gateway Support Node) que constituyen los nodos de soporte del servicio GPRS.

  Los nodos GSN pueden verse como entidades en las que está localizada gran parte de las funciones necesarias para soportar el GPRS. En el GPRS PLMN, Red Pública Móvil de GSM (Public Land Mobile Network), generalmente hay más nodos GSN y la infraestructura que los conecta, denominada backbone network (ruta de enlace), permite el ruteo de los paquetes transmitidos por los usuarios de la red o dirigidos a éstos. En relación con la localización de la estación móvil genérica GPRS, se usan los HSN Nodo de Asistencia de Soporte (Home Support Node) y el VSN Nodo de Soporte Visitado (Visited Support Node).

  a. HSN, es el nodo de la backbone network al que llegan los paquetes dirigidos al móvil con base al valor de su dirección de la red; además, cuando el móvil es localizado en el área administrada por otro nodo de la ruta de enlace, el HSN vuelve a mandar hacia ese nodo los paquetes destinados al móvil.

  b. VSN, es el nodo de la backbone network en cuya área se encuentra normalmente el móvil.

  c. Backbone network, puede ser una red pública de datos de paquetes, lo que permite limitar los costos de realización o bien una red de datos de paquetes dedicada y optimizada para el soporte del servicio. La primera solución determina, con respecto a la segunda, mayores retrasos de transmisión cuando los paquetes se intercambian entre usuarios de GPRS PLMN y usuarios de otra red, mientras que la segunda presenta unos costos de realización más elevados.

     A la backbone network también están conectadas las entidades de trabajo, que garantizan la interconexión de la GPRS PLMN a otras redes de datos como, por ejemplo, la red Internet, las redes PSPDN, Red de Datos de Paquetes Públicos (Public Switched Packet Data Network), las redes privadas de paquetes y otras.

Las principales funciones desempeñadas por estas entidades son: la conversión de los protocolos y el mapeo de las direcciones de red de las entidades envueltas en la comunicación de datos.

- GPRS register, las funciones llevadas a cabo por un GPRS register son esencialmente las de memorizar información relativa al servicio GPRS, en particular cada GPRS register contiene:

  a. Información necesaria para el ruteo de los paquetes dirigidos a un móvil GPRS, por ejemplo, la dirección de red del móvil para un determinado protocolo de red y el tipo de protocolo de red a cuya dirección se refiere.

  b. Información relativa al perfil de suscripción del abonado, por ejemplo, las características de la calidad del servicio solicitada por el usuario QoS, Calidad del Servicio (Quality of Service).

B. Topología del servicio

El servicio GPRS pone a disposición de sus usuarios dos topologías de servicio diferentes:

a. PTP, Punto a Punto (Point To Point) el PTP es aquel en el que el usuario envía uno o más paquetes a un único destinatario; en relación a las modalidades con las que la conexión punto a punto es administrada, se pueden localizar dos clases de servicios punto a punto:

   - CLNS, Servicio Sin Conexión Punto-Punto (Connection Less Point To Point Services) un servicio PTP CLNS es aquel en el que dos paquetes sucesivos son independientes entre ellos; por tanto, es como si cada uno de los paquetes formáse parte de una comunicación en sí misma. Un servicio con esta característica se define como un servicio de datagrama y puede ser útil para soportar aplicaciones bursty de tipo no interactivo.

   - CONS, Servicio de Conexión Orientado Punto-Punto (Connection Oriented Point To Point Services) un servicio PTP CONS establece una relación lógica entre la fuente y el destinatario de los paquetes, relación que permanece activa durante el tiempo total de la conexión; el servicio es, por lo tanto, un circuito virtual, es decir, en la fase de set-up de la conexión se establece un recorrido para el ruteo de los paquetes, con la diferencia de que, respecto a una conexión por conmutación del circuito, los recursos físicos se liberan en cuanto el paquete genérico se ha transmitido, manteniendo la conexión lógica. Las aplicaciones que se adaptan bien a un servicio bearer (portador) de este tipo son aquellas interactivas o transnacionales, en las que se mantiene un diálogo continuo entre las dos entidades en comunicación.

b. PTM, Punto a Multipunto (Point To Multipoint) los servicios PTM, al contrario que los servicios PTP, implican a más de un usuario destinatario y el envío de los paquetes se ejecuta con base en la ubicación geográfica. Obviamente el servicio bearer PTM no puede implicar como usuarios destinatarios de paquetes a los usuarios de las redes interconectadas a la GPRS PLMN, sino sólo a usuarios de móviles.

3.4 Internet2

El término Internet2 se asocia como nombre genérico para identificar a las NREN, Redes Nacionales Avanzadas Educativas y de Investigación, (National Research and Education Network) que tuvieron su origen en los Estados Unidos, cuando se creó una red alternativa al Internet comercial, para permitir el intercambio y colaboración de investigación y educación entre diversas instituciones educativas.

En ese sentido, el término Internet2 es, en realidad, el nombre del consorcio de las 206 Universidades, empresas y organismos gubernamentales asociados para el desarrollo, operación y utilización de esta red académica en Estados Unidos; no obstante, por el rico intercambio existente en la colaboración de proyectos, el concepto de las redes académicas y de investigación rebasa la frontera americana y diversos países alrededor del mundo inician la construcción de este tipo de redes.

Su desarrollo abre las puertas a aplicaciones que usan transferencia masiva de datos, video en tiempo real, investigación y colaboración remota; de igual forma, permite impulsar la creación de nuevas herramientas para la educación superior y la investigación.

3.4.1 Red Internet2

La red de Internet2 está compuesta por redes principales o backbones en Estados Unidos, a los cuales se conectan los llamados gigaPoPs (un gigaPoP es una red regional, con ancho de banda del orden de los gigabits por segundo conectada a Internet2) y backbones internacionales los cuales a su vez se conectan a gigaPoPs o nodos en particular tales como Universidades. Por ejemplo en Estados Unidos el MIT, la Universidad de Boston y la Universidad de Harvard conforman el gigaPoP llamado BOS.

En la Figura 3.10 se puede visualizar que actualmente existen dos grandes backbones en Estados Unidos (aunque hoy en día el backbone Abilene es mucho mayor en ancho de banda, 2.4 Gbps), de los cuales se distribuyen enlaces hacia backbones en otros países. Uno de estos backbones internacionales es REUNA, Red Universitaria Nacional.

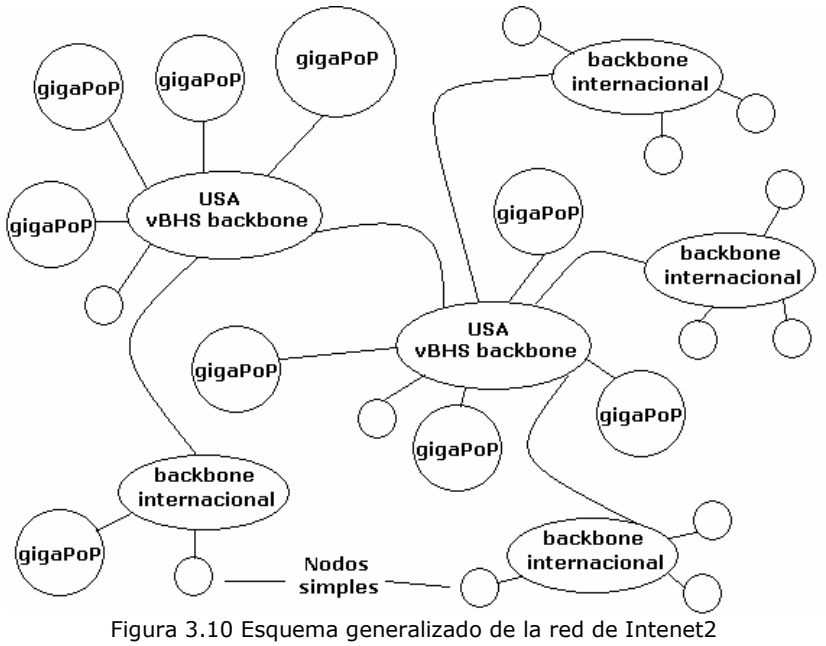


Figura 3.10 Esquema generalizado de la red de Intenet2

La conexión a Internet2 no requiere nuevo equipamiento ni nuevas conexiones por el lado de los usuarios de las respectivas Universidades conectadas a Internet2. Los backbones son los responsables de encaminar el flujo de datos por Internet2 o Internet comercial según corresponda.

3.4.2 Internet2 en México

La CUDI, Corporación Universitaria para el Desarrollo de Internet es una asociación civil integrada por las Universidades del país, de carácter privado, sin fines de lucro, que fue fundada en abril de 1999. Su misión es promover y coordinar el desarrollo de una red de telecomunicaciones de la más avanzada tecnología y amplia capacidad, enfocada al desarrollo científico y educativo en México.

CUDI es el organismo que maneja el proyecto de la red Internet2 en México e impulsa el desarrollo de aplicaciones que utilicen esta red, fomentando la colaboración en proyectos de investigación y educación entre sus miembros.

La construcción de la red Internet2 en México, se basó en la voluntad de las Universidades líderes del país de absorber, a prorrata, el costo de instalar y operar la red y su interconexión a las redes universitarias de alta velocidad en Estados Unidos y Canadá.

Apoyándose en este compromiso, Teléfonos de México y Avantel han aportado sin costo a la red CUDI 8,000 km de red dorsal de alta capacidad. A cambio de esta donación se ha establecido que la red tiene que transmitir exclusivamente tráfico de carácter educativo o de investigación.

Actualmente la membresía de CUDI se integra por las principales Universidades y centros de investigación del país. Adicionalmente, forman parte de la membresía de CUDI, empresas que apoyan la investigación y educación en el país, donde la UNAM es miembro fundador del CUDI en México.

La administración de CUDI recae en su Consejo Directivo, que es el órgano de gobierno conformado por una Asamblea de miembros del manejo de la Asociación Civil. Su presidencia rota anualmente entre los Asociados Académicos de la organización.

En la actualidad la red de CUDI cuenta con una infraestructura de más de 8,000 km de enlaces de alta capacidad que operan a una velocidad de 155 Mbps, ver Figura 3.11. Esta red dorsal abarca todo el territorio nacional, cuenta además con tres enlaces de la misma velocidad que permiten la interconexión con las principales redes académicas de Estados Unidos y del resto del mundo. A través de estos enlaces es posible tener acceso a más de 45 redes similares de Europa, Asia, Oceanía y América Latina que interconectan a más de 3,000 Universidades y Centros de Investigación.

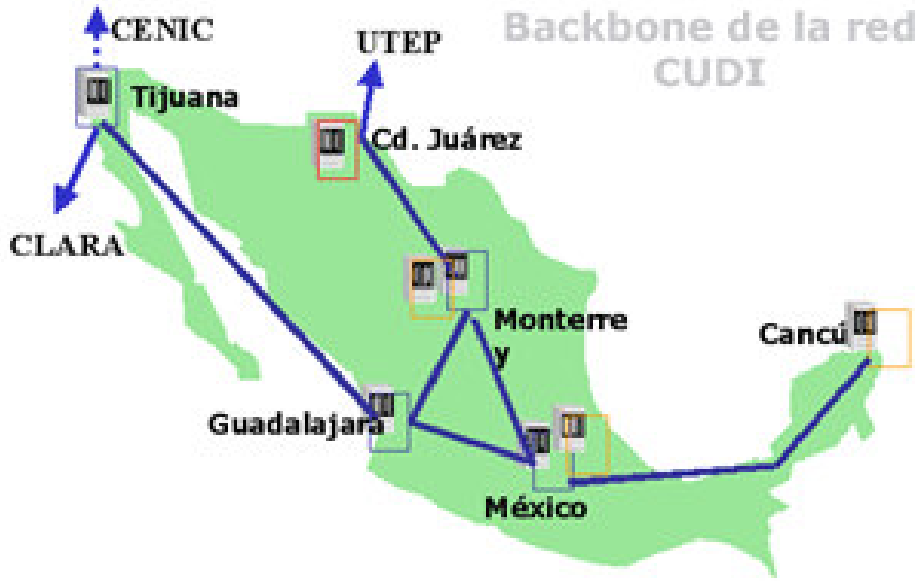


Figura 3.11 Esquema de la red CUDI

La red CUDI maneja los protocolos más avanzados en redes de telecomunicaciones como son QoS, Multicast, IPv6, H.323, MPLS, Multiprotocolo de Switcheo por Etiquetas (MultiProtocol Label Switching) y HDTV, Televisión de Alta Definición (High Definition Television). La red cuenta con su propio centro de operación NOC, Centro de Operaciones de Red (Network Operation Center), lo que permite que en la red corran aplicaciones críticas en todas las ramas de la ciencia.

En el país ya se están manejando aplicaciones en materias como Educación a Distancia, Bibliotecas Digitales, Telecomunicaciones Avanzadas, Salud, Telemedicina, Investigaciones Genéticas y Biológicas, Física de Alta Energía, Realidad Virtual, Astronomía, Ciencias de la Tierra, Redes de Supercómputo, Robótica y Colaboratorios. Las Universidades y centros de investigación mexicanos están llevando a cabo actividades en estas ramas en colaboración con instituciones avanzadas de todo el mundo.

3.4.3 Internet2 y CLARA

CLARA, Cooperación LatinoAmericana de Redes Avanzadas, es una red regional de telecomunicaciones de la más alta tecnología que interconecta a las redes académicas avanzadas nacionales de América Latina y a éstas con sus pares en Europa y el mundo.

El 1 de septiembre de 2004, RedCLARA comenzó a proveer conectividad directa a una velocidad de 155 Mbps, en una topología de anillo, enlazando a las redes de investigación y educación nacionales de Argentina, Brasil, Chile, Panamá y México, conectándolas con GÉANT a una velocidad de 622 Mbps, mediante un enlace entre São Paulo, Brasil y Madrid, España; ver Figura 3.12, donde se muestra la topología troncal de la Red CLARA.

El NOC, Centro de Operaciones de Red CLARA es provisto por CUDI y administra la operación diaria de la red, ubicándose en la Ciudad de México.

Es responsabilidad del NOC la administración, el control, el monitoreo y la operación diaria de todas las infraestructuras físicas y lógicas que conforman la red troncal de RedCLARA. El trabajo del NOC persigue asegurar altos niveles de rendimiento y de operación de la red además de sus interconexiones.

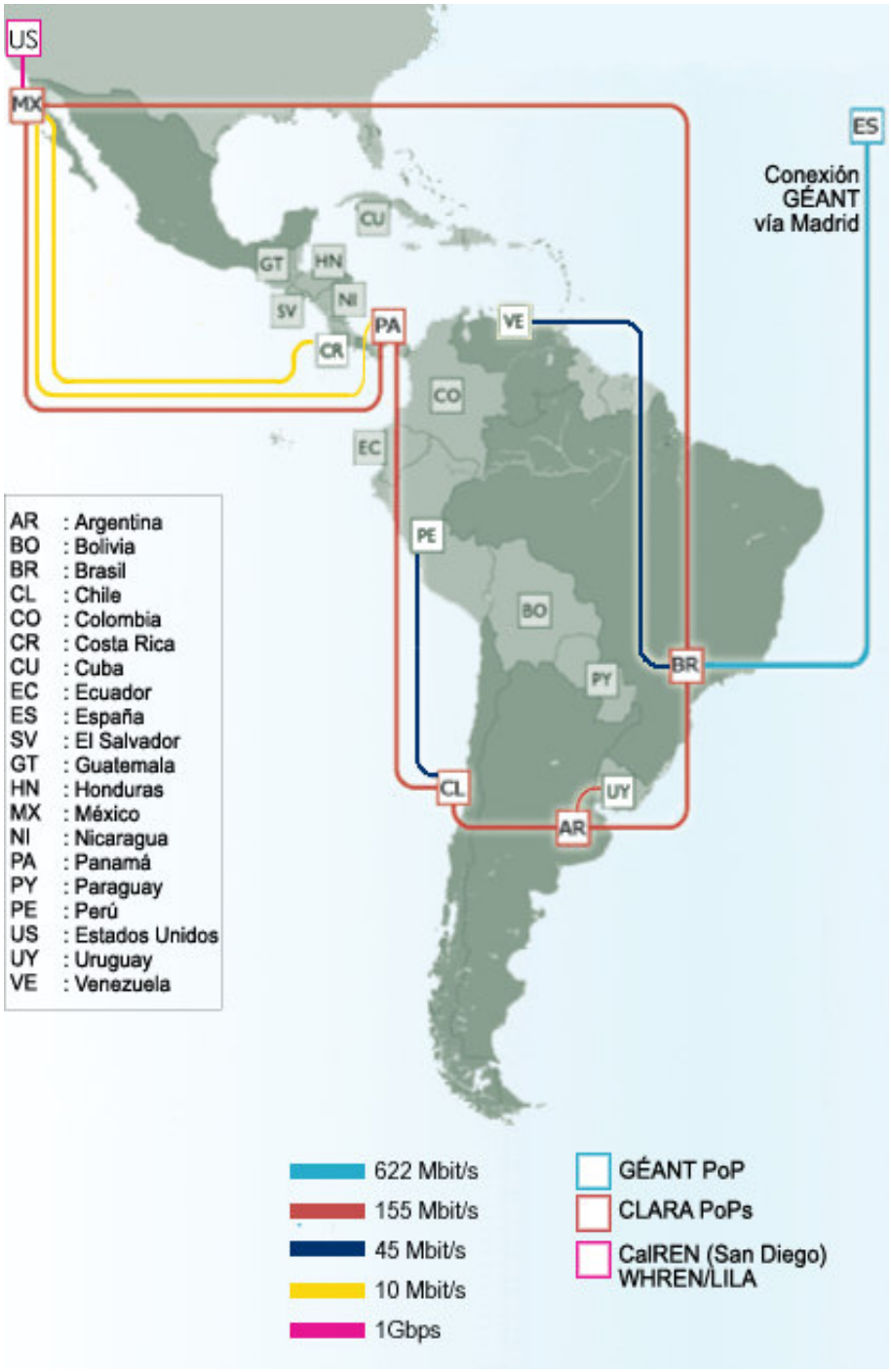


Figura 3.12 Mapa de la topología de la RedCLARA

El NOC, al igual que el NEG, Grupo de Ingeniería de la Red (Network Engineer Group) de CLARA, depende del Comité Técnico de CLARA, cuyo propósito es el de mantener a CLARA en la frontera de los servicios avanzados de redes IP. Este objetivo debe lograrlo mediante la coordinación del NOC y el NEG. Además, el Comité Técnico debe proveer la mejor información y el más alto flujo de comunicaciones entre los grupos, protegiendo aquellos asuntos técnicos y políticos de los miembros de CLARA.

3.5 Videoconferencia

La videoconferencia es un sistema digital de telecomunicaciones que permite mantener reuniones colectivas entre varias personas, que se encuentran en lugares distantes. Esta comunicación se realiza en tiempo real, vía telefónica y se transmite tanto video como el sonido, en ambos sentidos, lo que podríamos llamar una reunión virtual. Los interlocutores se ven y se hablan como si estuvieran en la misma sala de reuniones, a la vez que se pueden intercambiar datos, fax, información gráfica, video, diapositivas, etc.

La mayoría de los sistemas de videoconferencia utilizan el video digital comprimido, para la transmisión de video por medio de las redes de transmisión de datos de alta capacidad como la ISDN.

Las videoconferencias a menudo se transmiten por medio de líneas del teléfono especializadas como T1/E1. Estas líneas trabajan a altas velocidades y son muy eficaces para esta tecnología, pero se alquilan por medio de circuitos especiales y tienen un costo de mantenimiento mensual relativamente alto. Por otro lado, los costos de comunicación se calculan en función de la distancia y en el tiempo de comunicación. Los sistemas de videoconferencia pueden operar a distintas velocidades de transmisión de datos, es decir a varios fragmentos de capacidad de líneas E1. Un sistema de videoconferencia también puede compartir una línea E1 con la transmisión de otro tipo de datos digitales como son transmisiones de Internet o transferencias de archivos.

La videoconferencia normalmente es usada para conectar dos sitios remotos empleando sofisticada tecnología de computadoras.

3.5.1 Equipo para videoconferencia

Para poder llevar a cabo una transmisión de videoconferencia se requiere del siguiente equipo:

- CODEC, COdificador/DECodificador también denominado COmpresor/DECompresor, este dispositivo convierte las señales de video y audio en señales digitales, es considerado el corazón del sistema de videoconferencia. El codec toma las señales analógicas, las comprime y digitaliza transmitiendo las señales a través de las líneas de teléfonos digitales, ver Figura 3.13.

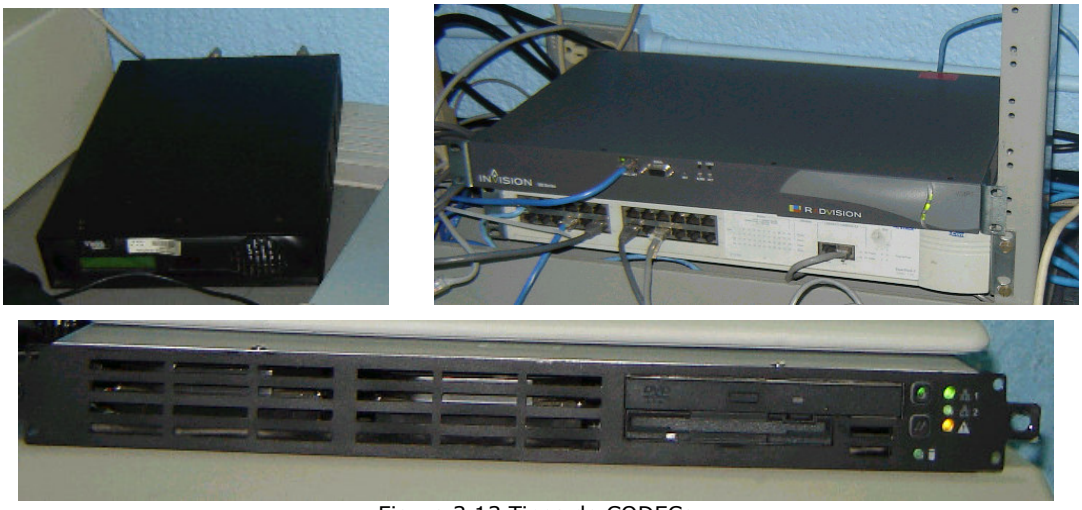


Figura 3.13 Tipos de CODECs

- CODECS para integración, equipos profesionales de videoconferencia con múltiples conexiones de entrada y salida posibles para instalar en salas de grandes dimensiones con cualquier proyector, pantalla, kit de control o demás accesorios audiovisuales profesionales.
- Dispositivo de control, puede ser: una tableta de control, teclado, ratón, pantalla sensible al tacto o control remoto. Este dispositivo controla el CODEC y el equipo periférico del sistema, ver Figura 3.14.

Figura 3.14 Dispositivos de control

- Cámara robótica, es la cámara incluida en cualquier equipo, ésta es manejada a través de la tableta de control, ver Figura 3.15.

Figura 3.15 Cámara robótica

- Micrófonos, captan el audio que se envía al otro sitio, ver Figura 3.16.

Figura 3.16 Micrófonos

- Monitores, en ellos se puede observar a los participantes del sitio local y de los sitios remotos, así como gráficas, fotografías, diapositivas, videos, etc., ver Figura 3.17.

Figura 3.17 Monitores, izquierda monitor local, derecha monitor remoto

- Videoteléfonos, equipos compactos para uso individual, compuestos por CODEC con teclado, auricular telefónico, cámara fija y pantalla LCD. Aportan máxima simplicidad de instalación y uso, ver Figura 3.18.

Figura 3.18 Videoteléfono

- MCU, Unidad de Multiconferencia, es un equipo específico que permite conectar simultáneamente más de dos puntos, para que establezcan reuniones de videoconferencia multipunto (permite hasta más de 50 puntos simultáneos), ver Figura 3.19.

Figura 3.19 Unidad de multiconferencia

- Kits de Pc o laptop, conjuntos para uso individual, preparados para integrarse en la PC o laptop; compuestos de tarjeta códec-capturadora, cámara desktop fija, auricular telefónico y software.
- Software del sistema de videoconferencia, es el programa que permite la acción conjunta de los elementos que integran al sistema de videoconferencia.

  ISABEL, GnomeMeeting y Microsoft NetMeeting son ejemplos de software configurable de audio, video y datos, que permiten crear escenarios de colaboración adaptados a las necesidades de usuarios.

  1. ISABEL, es un software para videoconferencias multipunto avanzado, con un rango de velocidad de 128 Kbps a 10 Mbps, para PC basado en dos conceptos:
     - Servicio, la aplicación adapta su funcionamiento y control a las necesidades del servicio concreto de telereunión, teleclase o teleconferencia.
     - Modo de interacción, cada presentación en pantalla enfatiza en lo que es importante en cada momento.

     ISABEL utiliza TCP/UDP sobre IP, por lo que puede usar múltiple tecnologías de acceso: ethernet, ATM, ISDL, ADSL, FR, satélite.
  2. GnomeMeeting, es un cliente H.323 diseñado para el entorno GNOME, cuenta con un entorno gráfico configurable, el cual hace más ameno su uso, permite la búsqueda de usuarios mediante un motor de búsqueda, guiado por distintos criterios, así como conocer todas las acciones llevadas a cabo por el usuario a lo largo del uso del programa.
  3. NetMeeting, es un software para conferencia que posibilita la comunicación y colaboración en tiempo real mediante Internet o una Intranet. NetMeeting es compatible con los estándares de comunicación para audio, video y conferencia de datos. Los usuarios de NetMeeting pueden comunicarse y colaborar con usuarios de otros productos basados en estándares compatibles. Pueden comunicarse por módem, una línea ISDL o una LAN mediante el protocolo TCP/IP.
- DCU, Dispositivo de comunicación, al que llega la señal digital desde el CODEC y la envía por el canal de transmisión (microondas, fibra óptica, etc.) lo que permite enviar y recibir la señal a los sitios remotos, ver Figura 3.20.

Figura 3.20 Dispositivos de comunicación

- Canal de transmisión, todo sistema de videoconferencia requiere de un canal para transmitir la señal de audio y video a otro sitio, éste puede ser: cable coaxial, microondas, fibra óptica, satélite, ver Figura 3.21.

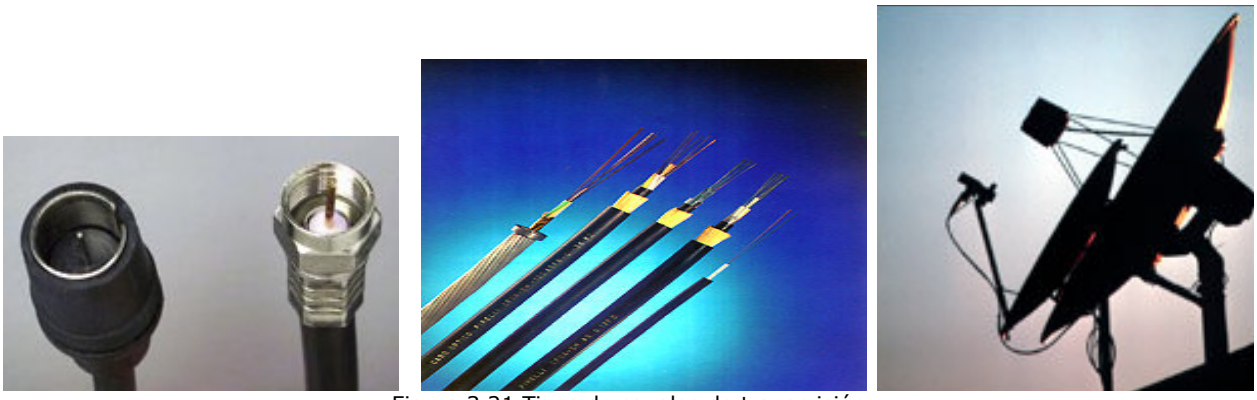


Figura 3.21 Tipos de canales de transmisión

- Espacio, es el área especialmente acondicionada tanto en acústica e iluminación para alojar el equipo y realizar las sesiones. El nivel de confort de la sala mejora la calidad del encuentro, ver Figura 3.22.

Figura 3.22 Sala de la red de videoconferencia de DGSCA, UNAM

- Personal calificado, es indispensable que cada sitio, cuente con al menos una persona que posea los conocimientos necesarios de telecomunicaciones y operación técnica del equipo.

3.5.2 Tipos de conexiones

En cuanto a la conexión existen básicamente 2 modelos:

- Videoconferencia punto a punto, es cuando la videoconferencia se va a realizar entre dos únicos terminales de videoconferencia. Previamente se establece la llamada telefónica mediante el número ISDL. Es decir, un equipo de videoconferencia hace la llamada a través del número ISDL al otro equipo y se inicia la comunicación.

- Videoconferencia multipunto, en este modelo la videoconferencia va a ser entre más de 2 terminales. Es necesario que, un equipo que sea capaz de hacer la unión entre todos los terminales que participarán en la multivideoconferencia (equipo conmutador de video de puertos ISDL). Este equipo, a partir de ahora puente de videoconferencia, se encargará de recibir la señal de todos los equipos de videoconferencia y de distribuir todas estas señales a todos los equipos, con el fin de que todos puedan participar al mismo tiempo en dicho evento.

¿CÓMO FUNCIONA EL SISTEMA DE VIDEOCONFERENCIA?

Las señales proporcionadas por las cámaras, los micrófonos y equipos periféricos son enviadas al CODEC, dentro de éste se realiza un proceso complejo, el cual resumimos en tres etapas:

1. El CODEC convierte las señales de audio y video a un código de computadora, a esto se le conoce como digitalizar. La información es reducida en pequeños paquetes de datos binarios (0 ó 1). De esta forma se transmiten datos requiriendo menos espacio en el canal de comunicación, ver Figura 3.23.

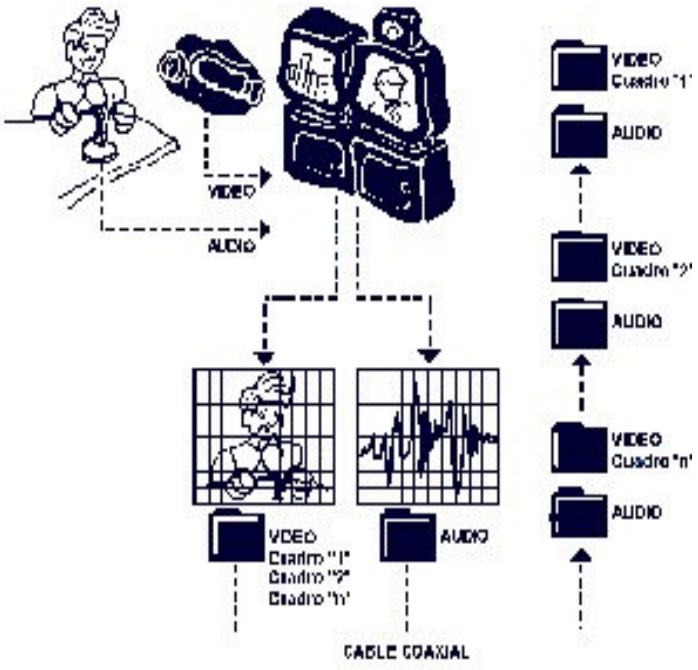


Figura 3.23 Diagrama del transmisión del CODEC

2. Los datos son enviados a otro dispositivo de comunicación, el cual los transmite al sitio remoto por un canal de transmisión (cable coaxial, fibra óptica, microondas o satélite) por el que viajará, ver Figura 3.24.

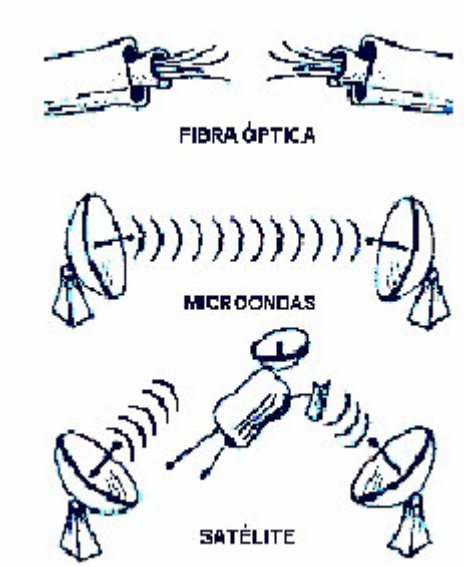


Figura 3.24 Diagrama de transmisión de los datos

3. A través del canal, el otro sitio recibe los datos por medio del dispositivo de comunicación, el cual lo entrega al CODEC que se encarga de descifrar y decodificar a señales de audio y video, las que envía a los monitores para que sean vistas y escuchadas por las personas que asisten al evento, ver Figura 3.25.

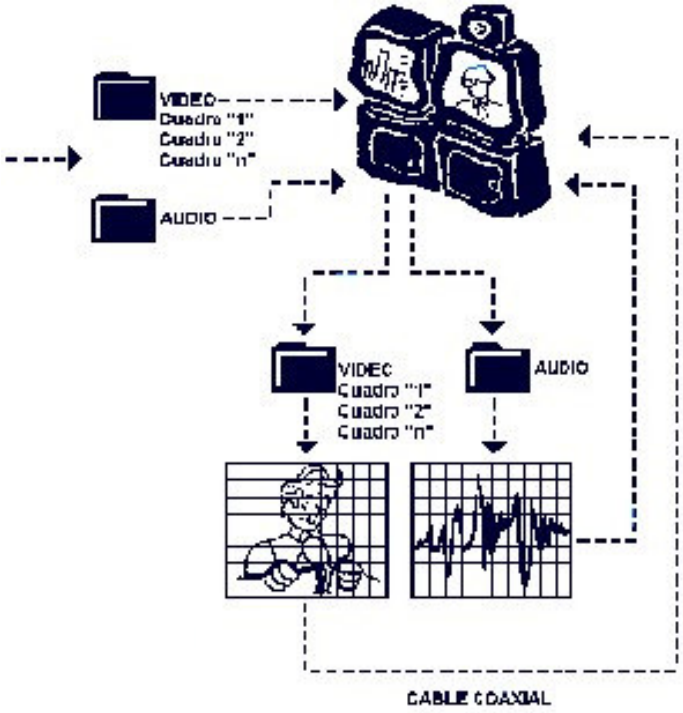


Figura 3.25 Diagrama del recepción del CODEC

3.5.3 Protocolos de videoconferencia

La ITU trabaja en una serie de estándares para lograr la interoperabilidad de los programas para videoconferencia. Estos son:

- H.320 diseñado para enlaces ISDN, se ha ido adaptando para usarse en la tecnología WAN. El estándar recoge todos los subestandares tales como H.261 (video), G.7XX (audio), H.320 (control) y T.120 (datos) y transmite a 128 Kbps.

  Una versión de H.320 está diseñada para multipunto, la MCU permite 3 o más terminales para compartir información de audio y video. Una simple red multipunto debe ser considerada como una conferencia punto a punto excepto porque 2 o más terminales están presentes.

- H.323 estándar que define videoconferencias basadas en LAN y permite una interoperabilidad entre los diferentes vendedores; también define videoconferencias usando líneas de viejos sistemas telefónicos.

  Estándar que especifica los componentes, protocolos y procedimientos que proporcionan servicios de comunicación multimedia (audio, video y datos en tiempo real) sobre redes de paquetes no orientadas a la conexión y que no garanticen calidad de servicio.

  H.323, especifica cuatro tipos de componentes: terminales, pasarela, gatekeepers y unidades de control multipunto, que conjuntamente proporcionan un servicio de comunicación multimedia punto a punto o punto multipunto.

- H.324 trabaja sobre líneas telefónicas regulares a velocidades de 28.8 Kbps ó 56 Kbps, puede dar 5 ó 7 cuadros por segundo, la transmisión de imágenes es de muy baja calidad, similar a una secuencia de fotos, una detrás de otra.

  El estándar H.324 para transmisión de videoconferencia define una metodología para su transporte a través de la red telefónica ó lo que se conoce como POTS, Red Telefónica de Sistemas Convencionales (Plain Old Telephone Systems), describe terminales para comunicaciones multimedia trabajando a bajas velocidades, utilizando módems V.34. Estos terminales pueden transmitir voz, datos y video en cualquier combinación en tiempo real, está diseñado para optimizar la calidad de la transmisión de videoconferencia sobre los enlaces de baja velocidad asociados con los POTS, estas bajas velocidades de transmisión sumadas a la naturaleza impredecible del medio de transmisión, restringe este tipo de videoconferencia a unos pocos cuadros por segundo.

  Sin embargo, se espera que el estándar H.324 tenga cierta aceptación entre el mercado de consumidores. Primero, porque este tipo de videoconferencia está orientada a aplicaciones recreativas, donde no se requiere de una elevada calidad y en segundo lugar debido a la facilidad de implementación donde sólo se requiere de una PC equipada con un módem y utilizar la red telefónica convencional.

3.5.4 Administración de la red de videoconferencia

DGSCA, Dirección General de Servicios de Cómputo Académico de la UNAM, tiene a su cargo la administración de las tres redes de videoconferencia a través del VNOC, Centro de Operaciones de Videoconferencia, ver Figuras 3.26 y 3.27.

- RVUNAM, Red de Videoconferencia de la UNAM, establecida en 1993.
- RNVE, Red Nacional de Videoconferencia para la Educación, establecida en 1997.
- RVCUDI, Red de Videoconferencia CUDI, establecida en 2001.

En el Anexo 3.D se encuentran las especificaciones para los enlaces por ISDN, por enlace dedicado y por redes conmutadas por paquetes (IP).

Las salas de videoconferencia de México, se ubican en diversas dependencias de la UNAM e instituciones educativas y son administradas desde el VNOC. El sistema de administración de videoconferencia en DGSCA, sirve para concentrar las salas y los sistemas de videoconferencia, además de ser un centro convertidor de protocolos.

Todos los dispositivos deben estar bajo ciertos estándares como el H.320 para ISDN y enlaces dedicados; el H.323 para video sobre IP.

Entre los principales objetivos del VNOC se pueden encontrar:

1. Conectar diferentes sitios, donde cada uno puede responder a diferentes protocolos.
2. Convertir protocolos.
3. Organizar conferencias multipunto y punto.
4. Además de los enlaces de conectividad, tiene que considerar la administración de la logística a través de:
    a. Agendas de Salas de Videoconferencia.
    b. Aplicación de uso, que existen 3 diferentes clases de acuerdo al tipo de red de videoconferencia a la que pertenezcan.

La administración de las redes de videoconferencias se hace mediante un modelo de dos capas.

1. Capa de conectividad, incluye dispositivos de conectividad, su mantenimiento, configuración, programación, así como prueba de equipo y funcionalidad. Trabaja sobre conexiones físicas de la red.
2. Capa de logística, incluye la organización de la videoconferencia, utilizado para ello un sistema de reservación de videoconferencias. El sistema recibe las solicitudes y las programa en un calendario, definiendo si la sala está ocupada o es desconocida, evitando el empalme de las actividades, para las solicitudes de videoconferencias se emplean formatos escritos que evitan cualquier contratiempo.

    La solicitud de videoconferencia se realiza mediante correo electrónico donde se obtienes aprobaciones o rechazos.

Se cuentan con políticas que permiten encausar o ubicar ciertas solicitudes dependiendo del tipo de red de videoconferencia. El VNOC permite desarrollar proyectos relativos a las videoconferencias, proporcionar capacitación, servicios a las salas de videoconferencia entre otros.

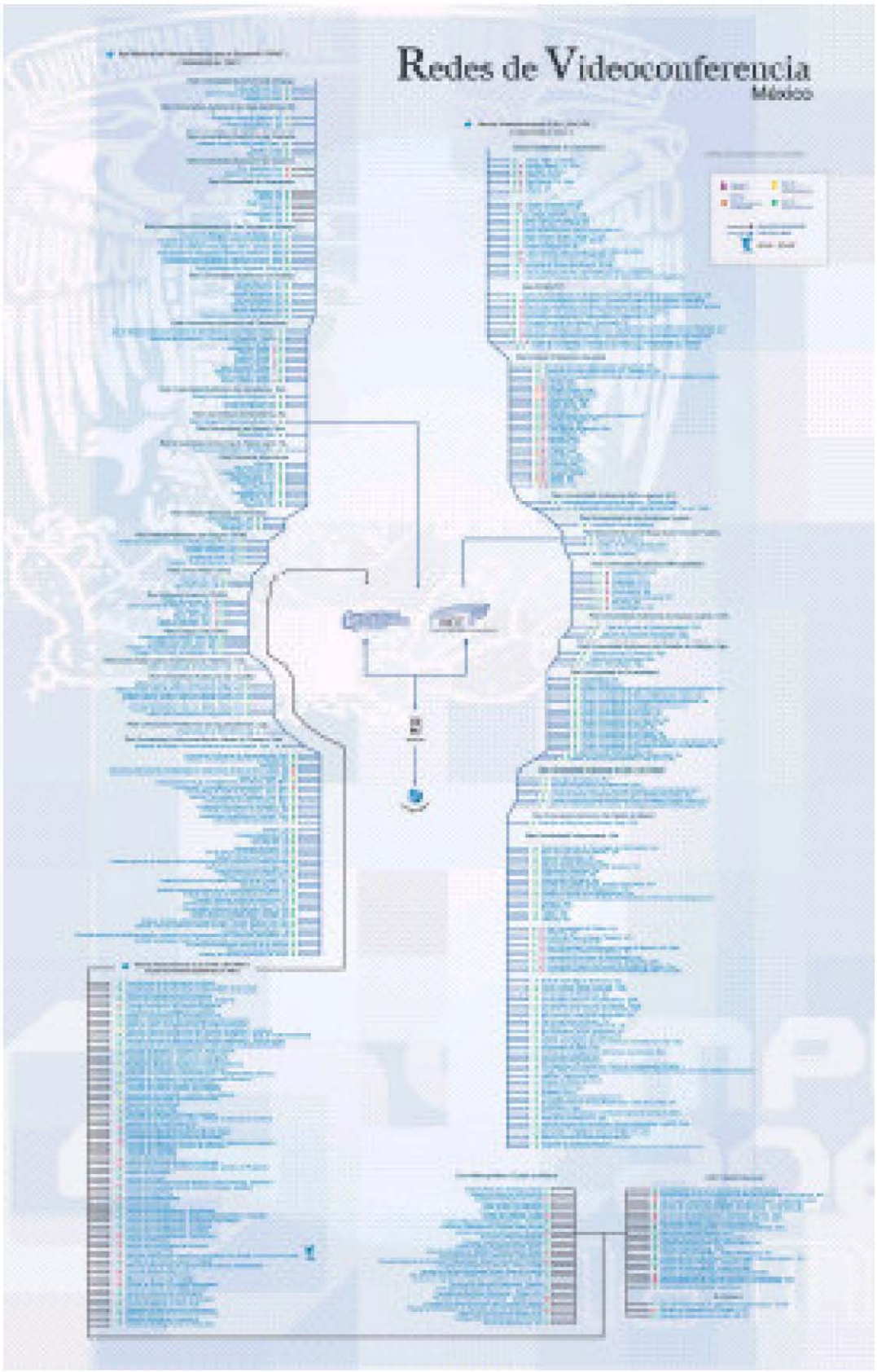


Figura 3.26 Redes de videoconferencia en México

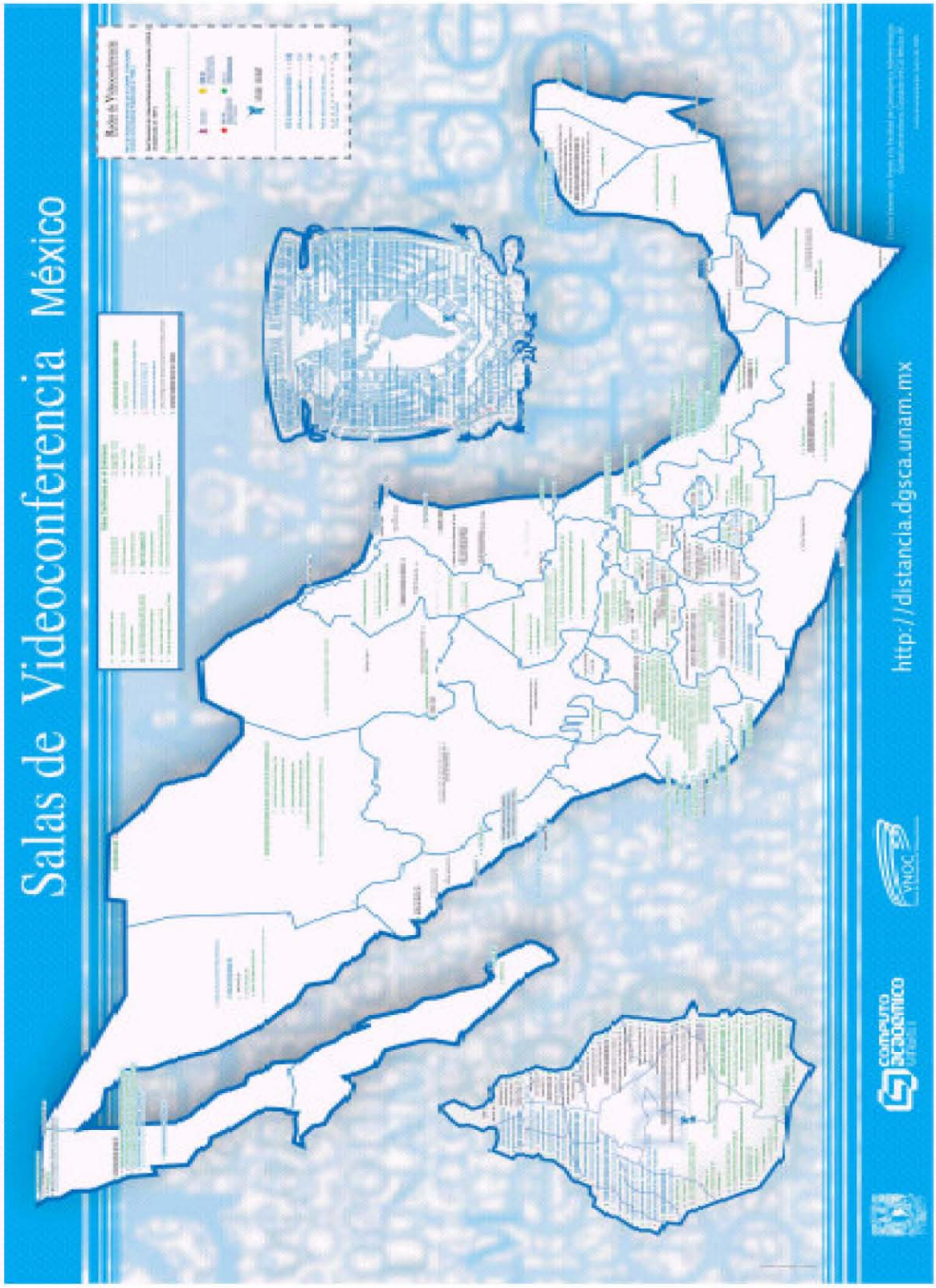


Figura 3.27 Salas de videoconferencias en México

3.6 Evaluación de proyectos

Un proyecto, es la búsqueda de una solución inteligente al planteamiento de un problema tendente a resolver. La evaluación de un proyecto tiene por objetivo conocer su rentabilidad económica y social, de tal manera que se asegure resolver una necesidad humana en forma eficiente, segura y rentable.

La metodología de evaluación de proyectos para centros de cómputo, es una adaptación del método tradicional. Desde que la ONU la desarrolló en 1950, esta metodología ha mantenido cuatro etapas:

1. Estudio del mercado o cuantificación de las necesidades del servicio.
2. Estudio técnico.
3. Análisis económico.
4. Evaluación económica.

Cada una de estas etapas tiene ciertas adaptaciones cuando se aplica a centros de cómputo.

Antes de iniciar el proceso de evaluación de proyectos, es necesario realizar:

1. Introducción, la cual debe contener una breve reseña histórica del desarrollo y los usos del producto, además de precisar cuáles son los factores relevantes que influyen directamente en su consumo.
2. Antecedentes y marco de desarrollo, el estudio debe estar situado en las condiciones económicas y sociales, aclarando básicamente por que se pensó en emprenderlo, a qué personas o entidades beneficiará; qué problema específico resolverá y los objetivos de estudio.
3. Un estudio de factibilidad, cuyos objetivos generales siempre serán los siguientes:
   a. Demostrar que existe suficiente demanda del servicio de procesamiento electrónico de datos, para justificar la instalación de la red.
   b. Demostrar que se dominan los aspectos tecnológicos de la operación de la red.
   c. Demostrar que la inversión de la red es económicamente rentable o que la alternativa seleccionada es la óptima desde el punto de vista económico.

Después de concluir el estudio de evaluación de proyecto, es necesario incluir un apartado de conclusiones generales, donde se exponga abierta y francamente, cuáles son las bases cuantitativas que orillan a tomar la decisión de inversión en el proyecto estudiado.

3.6.1 Estudio del mercado

A. Cuantificación de las necesidades

Nos referimos a la cuantificación de las necesidades del servicio, como los servicios que se desean prestar. El servicio lo otorgan varios dispositivos, de manera que cada uno de ellos debe definirse con claridad. Estos dispositivos son:

- Estaciones de trabajo, en donde deben definirse la memoria actual y expansible, la memoria caché, la capacidad de disco duro, el sistema operativo a utilizar, el tipo de monitor.

- Servidor, en donde deben definirse tipo y número de ranuras exclusivas para discos y para dispositivos de almacenamiento, el tipo de software administrador, la memoria RAM actual y expansible.
- Impresoras en donde deben definirse el número de páginas que imprime por minuto, tipo de interfase y tipo de impresora (láser, matriz de punto, inyección de tinta).
- Discos, en donde deben definirse la capacidad deseada formateado y sin formatear, tasa media de transferencia en Mbps, tiempo promedio de búsqueda en milisegundos y tiempo promedio de acceso.

Las características mencionadas pueden ampliarse o reducirse, dependiendo del uso de la red.

La cuantificación de la demanda del servicio es el primer paso, que se basa en las necesidades del usuario. La operación de una red tiene las siguientes necesidades:

- Almacenar datos y crear bases de datos.
- Almacenar software y herramientas manipuladoras de datos.
- Permitir acceso de usuarios a los dispositivos de entrada/salida.
- Comunicación, administración y control de software.
- Compartir recursos (memorias, impresoras, etc.).
- Arquitectura abierta, etc.

Con base en esta información se puede medir la demanda del servicio, mediante al menos tres formas:

a. Relacionar cada uno de los servicios que ofrece la red con el tiempo, se efectúa un análisis de regresión entre cada uno de los factores (capacidad de horas de trabajo de CPU, total de líneas impresas por unidad de tiempo, promedio de pistas o tracks utilizadas, número de usuarios) con el tiempo. Se pronostica el comportamiento de cada uno de ellos a determinado número de años.

b. Efectuar una regresión múltiple, asignando los Mb demandados como una dependiente de otras, como puede ser la cantidad de usuarios, el tiempo de respuesta, el número de terminales y el tiempo en años.

c. Métodos cualitativos, éstos se utilizan cuando no existen datos cuantificados de la demanda o es muy difícil obtenerlos. Los métodos cualitativos son dos básicamente:
    - Método Delfos.
    - Método de encuestas.

B. Cuantificación de la oferta

La oferta es la capacidad de servicio disponible actualmente para procesar datos en la empresa o institución. Para cuantificar la oferta de cualquier tipo de red, sólo hay que verificar la capacidad con que se cuenta.

C. Balance demanda-oferta

Este paso consiste en la comparación de la oferta y la demanda, nos permite pronosticar que sucederá en el futuro con la red, proporcionando información que nos llevará a tomar la mayoría de las determinaciones que se hagan a lo largo del estudio de factibilidad, como el tamaño de los equipos para adquirir, la inversión necesaria, etc.

D. Análisis de los costos actuales o precios del servicio

Su objetivo es determinar el ingreso monetario en cierto periodo, pero no siempre es aplicable este paso, ya que en las redes no existen ingresos. Se tiene que tomar en cuenta que si se trata se una empresa de servicios de telecomunicaciones, si se debe determinar este punto.

E. Mecanismo de adopción del nuevo sistema de red

Donde debe desarrollarse un programa de capacitación con base en las necesidades propias de la entidad.

3.6.2 Estudio técnico

El estudio técnico se compone de diez etapas, las cuales se describen a continuación:

1. La localización de las instalaciones y riesgo de daños, es muy importante considerar el lugar físico donde se instalarán. El lugar físico donde estarán ubicados cada uno de los componentes tiene relación con el riesgo de daño a las instalaciones. La seguridad en informática es la protección de los recursos, con que cuenta el área como lo son:

   a. Recursos humanos: personal de informática, usuarios, staff.

   b. Instalaciones y equipo: hardware (CPU, consola de operación), dispositivos de almacenamiento (discos, cintas), dispositivos de entrada/salida (impresoras, terminales), equipo especial (controladores, servidores), equipo de respaldo (archivos y documentos), edificio (pisos, instalaciones eléctricas, cristales), equipo de comunicación (módem, multiplexores, cables).

   c. Datos: software (sistema operativo, utilerías, paquetes), administrativos (documentos, procedimiento), registros y estadística (de personal, financieros, de ventas).

   La localización de las instalaciones, determina la ubicación física y los sistemas de protección de las instalaciones, del equipo y parte de protección contra recursos humanos. El método que se utiliza para llevar a cabo esta fase, es el de puntos ponderados.

   Los pasos a desarrollar en el método de puntos ponderados son:

   a. Hacer un listado de los factores que se consideran relevantes para la localización. En un estudio de vialidad para centros de cómputo se supone que ya existen uno o varios edificios y lo que se desea es determinar un sitio preciso, dentro de(los) edificio(s), donde se instalará la red. De esta manera, los factores que se pueden enlistar para localizar la red y prevenirla del riesgo son:

      - Área independiente de otras, que cuentan con demasiado tránsito, presencia de personal ajeno a la empresa o ambos aspectos.
      - Área con facilidades para instalar aire acondicionado.

- Área libre de riesgo de inundación, que no sea el sótano ni lugares atravesados en el piso o el techo, por instalaciones hidráulicas.
- Área construida con materiales no flamables.
- Área de baja temperatura, es decir, que ninguna parte del área esté expuesta tan directamente a la luz solar, pues esto haría que la temperatura se elevara en verano.
- Área en la que sea fácil de controlar el acceso, pero que a la vez sea de rápida evacuación en caso de siniestro.
- Área que no este construida con paredes de cristal. Los centros de de cómputo no son salas de exhibición.

b. Asignar un peso a cada factor según la importancia que tenga para la organización.

c. Determinar las áreas dentro del edificio que son alternativas para la instalación de la red y calificar cada una de ellas.

d. Obtener la calificación ponderada y seleccionar el sitio con mayor calificación.

El método de puntos ponderados, es para instalar el equipo de cómputo y no hay que confundir la localización de éste con la asignación de terminales a los distintos usuarios. Para esta asignación se sigue en mismo método, pero los factores a considerar son lo siguientes:

a. Necesidad de tener una terminal personal en la oficina.

b. Utilización de red: solo para consulta de datos, para consulta de datos y toma de decisiones o para cargar datos.

c. Tiempo de uso aproximado al día del servicio de cómputo.

d. Nivel de puesto que ocupa.

e. Utilización de otros servicios de la red: impresión, correo electrónico, etc.

f. Si se puede compartir la red con otros usuarios.

g. Con cuántos usuarios cercanos puede compartir la red.

Con base en las respuestas que proporcionen todos estos solicitantes de una terminal, se asignará un peso a cada respuesta y una calificación a la misma. Se obtiene la calificación ponderada y se asignan tantas terminales como presupuesto disponible exista en la organización. Este método es desde luego, para determinar la localización física de las terminales.

2. Tamaño óptimo de las instalaciones, se define como la capacidad máxima de operación de los equipos en cada una de sus características.
3. La descripción de la operación de la red, en esta parte se debe resolver el problema de construcción y operación de la red. Para construir una red hay que considerar cinco puntos básicos.

   a. Seleccionar la topología y el equipo físico (hardware).

   b. Instalar el equipo físico y el sistema operativo de la red.

   c. Configurar el sistema y cargar las aplicaciones.

   d. Crear el entorno del usuario.

e. Establecer una administración de la red.

4. Los componentes de la red, entre los que se encuentran: servidores, estaciones de trabajo, esquemas de acceso, tarjetas de red, sistemas operativos de las estaciones de trabajo, los recursos compartidos, la comunicación con otros sistemas, los puentes, las puertas de enlace (gateways).
5. Topología de la red, se tiene que determinar, qué tipo de topología se implementará, ya sea bus, estrella, anillo, ad hoc o infraestructura.
6. Sistema de protección de software, de datos y de recursos humanos.
7. Instalación y configuración de la red, en donde se toma en cuenta, la estructura de la red, tipos y opciones de cable y el modelo de administración.
8. Sistema de seguridad para la instalación física de los equipos.
9. Elección de paquetería.
10. Administración de la red.

3.6.3 Análisis económico

El estudio económico tiene como objetivo, determinar cual es el monto de los recursos económicos necesarios para la realización del proyecto de red, por eso es necesario tener en cuenta los siguientes aspectos, los cuales se tienen que desarrollar para poder llevar a cabo este estudio:

1. Determinación de los costos totales, los costos se agrupan como costos totales de prestación de servicio.
2. Inversión inicial, comprende la adquisición de todos los activos fijos o tangibles y diferidos o intangibles, necesarios para iniciar las operaciones de la red.
3. Depreciación y amortización, toman sentido determinarlos cuando se pagan impuestos; si el objetivo de la red es vender información se debe considerar este punto, pero si hablamos del gobierno ya sea en las secretarías, instituciones educativas o cualquier otra entidad exenta de dicho pago, no es necesario llevar a cabo este punto.
4. Capital de trabajo, si se perciben ingresos por la inversión en la red se deben determinar, pero si la inversión es sólo para apoyar las labores administrativas de la organización, ya sea pública o privada y la inversión no genera ingreso alguno por sí misma, debe omitirse este cálculo.
5. Punto de equilibrio, pasa lo mismo que para el apartado anterior. Aquí el punto de equilibrio es la cantidad de información que debe venderse a determinado precio unitario, para que estos ingresos sean iguales a los costos incurridos en generar información.
6. Balance general, se presenta el mismo caso que el punto 4.
7. Financiamiento de la inversión, en inversiones del gobierno no se considera un financiamiento, en cuanto a organizaciones privadas puede o no existir financiamiento.
8. Estado de resultado, se presenta el mismo caso que el punto 4.
9. Determinación del TMAR, Tasa Mínima Aceptable de Rendimiento.

3.6.4 Evaluación económica

El objetivo de este estudio, es la toma de decisión entre al menos dos alternativas posibles y que un tomador racional de decisiones, seleccione aquella alternativa que, habiendo cumplido con todas las necesidades tecnológicas de operación tenga el menor costo. Este estudio se lleva a cabo con los siguientes puntos:

1. Se obtendrá el valor presente neto y la TIR, Tasa Interna de Rendimiento, tomando en cuenta el rendimiento esperado por el inversionista.
2. Con base en los resultados obtenidos, se analizará el rendimiento de la inversión y sus riesgos para así tomar una decisión sobre bases firmes.
3. Presentar el punto de equilibrio y los estados financieros mencionados anteriormente.

Capítulo 4

DIRECCIÓN

INTRODUCCIÓN

La actualidad laboral se caracteriza por una división de trabajo, donde se asigna a cada persona una serie de tareas concretas y simplificadas. La actividad organizativa y su adecuación en cada momento de acuerdo a las características y circunstancias, es una de las tareas que corresponden a la Dirección, quien en todo momento establece las directrices para la planeación, estructuración, aprobación y desarrollo de proyectos, asignados a los colaboradores del área.

Los administradores de redes, deben contar con la habilidad de combinar el trabajo de los individuos y grupos, que utilizando los medios disponibles, proporcione los mejores resultados en el desempeño del área. De acuerdo a lo anterior, el carácter y capacidad del administrador son de vital importancia, pues de él dependen la autoridad, las decisiones y en gran parte, el clima en que han de desenvolverse las relaciones humanas.

El liderazgo es un aspecto importante de la función directiva. La capacidad de dirigir eficazmente, es una de las claves para cumplir los objetivos comunes. La clave, consiste en la definición clara de un rol y en un grado de discreción o autoridad, capaz de respaldar las acciones.

El liderazgo y la motivación se encuentran íntimamente vinculados, ya que al entender la motivación, se puede apreciar mejor lo que las personas desean y la razón por la que actúan de una manera determinada. Los líderes actúan para ayudar a un grupo a alcanzar objetivos, a través de la máxima aplicación de sus capacidades.

Un buen administrador, no se para detrás de un grupo para empujar e instigar, se coloca al frente, facilitando el progreso e inspirando al grupo para lograr los objetivos de la organización.

Uno de los dispositivos más usados de la organización al cual el líder debe dirigir, es el comité de trabajo, conocido como fuerza de área, área de trabajo, equipo de trabajo, comisión, etc. Su esencia es la misma, un grupo de personas a las cuales se les asigna una misión.

Las personas representan diversos papeles dentro de los grupos: algunos buscan información, otros la proporcionan; algunos propician la participación, otros son seguidores; algunos intentan coordinar esfuerzos, otros adoptan actitudes agresivas.

Algunos especialistas establecen 4 etapas de desarrollo para los grupos: la formación, el conflicto, la normatividad y el desempeño. En la etapa de conflicto, el administrador debe manejar la situación de manera que pueda resolver el problema, con ayuda de herramientas diseñadas para ello. La comunicación, entonces juega un papel importante.

Aunque la comunicación se aplica a todas las fases de la administración, es particularmente importante en la función de dirección. La comunicación es el proceso de transferencia de información de un emisor a un receptor, el cual debe entender el mensaje para que el ciclo se cumpla. Para verificar la efectividad de la comunicación, una persona debe contar con la retroalimentación. Nunca se puede estar seguro de que un mensaje ha sido codificado, transmitido, decodificado y entendido efectivamente, hasta que éste no sea confirmado.

4.1 Dirección general

La dirección es la esencia misma de la administración, a fin de emitir una definición tenemos cuatro posturas:

1. Robert B. Buchele, afirma que comprende la influencia interpersonal de la administración, a través de la cual logra que sus subordinados obtengan los objetivos de la organización mediante la supervisión, la comunicación y la motivación.
2. Buró K. Scanlan, ratifica que consiste en coordinar el esfuerzo común de los subordinados, para alcanzar las metas de la organización.
3. Leonard J. Kazmier, afirma que es la guía y la supervisión de los esfuerzos de los subordinados, para alcanzar las metas de la organización.
4. Joel J. Lerner y H.A. Baker, aseguran que consiste en dirigir las operaciones mediante la cooperación del esfuerzo de los subordinados a través de la motivación y la supervisión.

Con base en las cuatro anteriores posturas, podemos definir a la dirección como: la ejecución de los planes de acuerdo con la estructura organizacional, mediante la guía de los esfuerzos del grupo social a través de la motivación, la comunicación y la supervisión.

La administración es el proceso de planear, organizar, integrar, dirigir y controlar los esfuerzos de los miembros de la organización y aplicar los demás recursos de ella para alcanzar las metas establecidas.

En la dirección general, se debe tener en cuenta el proceso administrativo para poder llevar a cabo sus objetivos.

Un proceso es una forma sistemática de hacer las cosas y en conjunto con la definición de administración dada anteriormente, el proceso de administración se refiere a planear y organizar la estructura de las organizaciones, en las cuales se ejecutan la dirección y el control para darle seguimiento a los procesos administrativos.

4.1.1 Proceso administrativo

Es más fácil comprender algo tan complejo como la administración, si se describe como una serie de partes o funciones individuales que integran un proceso total. El proceso administrativo es una simplificación del mundo real, usado para presentar relaciones complejas en términos fáciles de entender, ver la Figura 4.1.

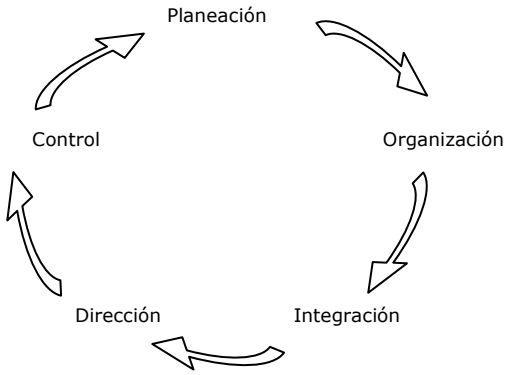


Figura 4.1 Diagrama del proceso administrativo

A. Etapas del proceso administrativo

1. Mecánica, es la fase donde se realiza la estructura principal de la orgamización e incluye las siguientes fases:
   a. Planeación.
   b. Organización.
2. Dinámica, fase donde se realiza la ejecución con eficiencia y eficacia de la organización e incluye estas fases:
   a. Integración.
   b. Dirección.
   c. Control.

La Figura 4.2 muestra el cuadro esquemático del proceso administrativo, que nos permite identificar las etapas en que se divide, las fases con que cuenta y los elementos que cada una de ellas incluye.

B. Fases y elementos del proceso administrativo

1. Planeación, implica que los administradores piensen, a través de sus objetivos con anticipación, que sus acciones se basen en algún método, plan o lógica, más que una mera suposición. Los planes dan a la organización sus objetivos y fijan el mejor procedimiento para obtenerlos. La planeación consiste en seleccionar misiones y objetivos, así como las acciones necesarias para cumplirlos, requiriendo por lo tanto de la toma de decisiones, esto es de la elección de cursos de acción futura a partir de diversas alternativas. Existen varios tipos de planes, los cuales van desde los propósitos y objetivos generales, hasta las acciones más detalladas por emprender.

   I. Elementos

   - Propósitos o misiones, se identifica la función o tarea básica de una empresa o institución o de una parte de esta.
   - Objetivos o metas, son los fines que se persiguen por medio de una actividad de una u otra índole.
   - Estrategias, es la determinación de los objetivos básicos a largo plazo de una organización, la adopción de los recursos de acción y la asignación de recursos necesarios para su cumplimiento.
   - Políticas, son enunciados o criterios generales que orientan o encausan el pensamiento en la toma de decisiones.
   - Procedimientos, son planes por medio de los cuales se establece un método para el manejo de actividades futuras.
   - Reglas, se exponen acciones o prohibiciones específicas, no sujetas a discrecionalidad de cada persona.
   - Programas, son un conjunto de metas, políticas, procedimientos, reglas, asignaciones de tareas, pasos a seguir, recursos por emplear y otros elementos necesarios para llevar a cabo un curso de acción dado.
   - Presupuestos, es la formulación de resultados esperados expresada en términos numéricos.

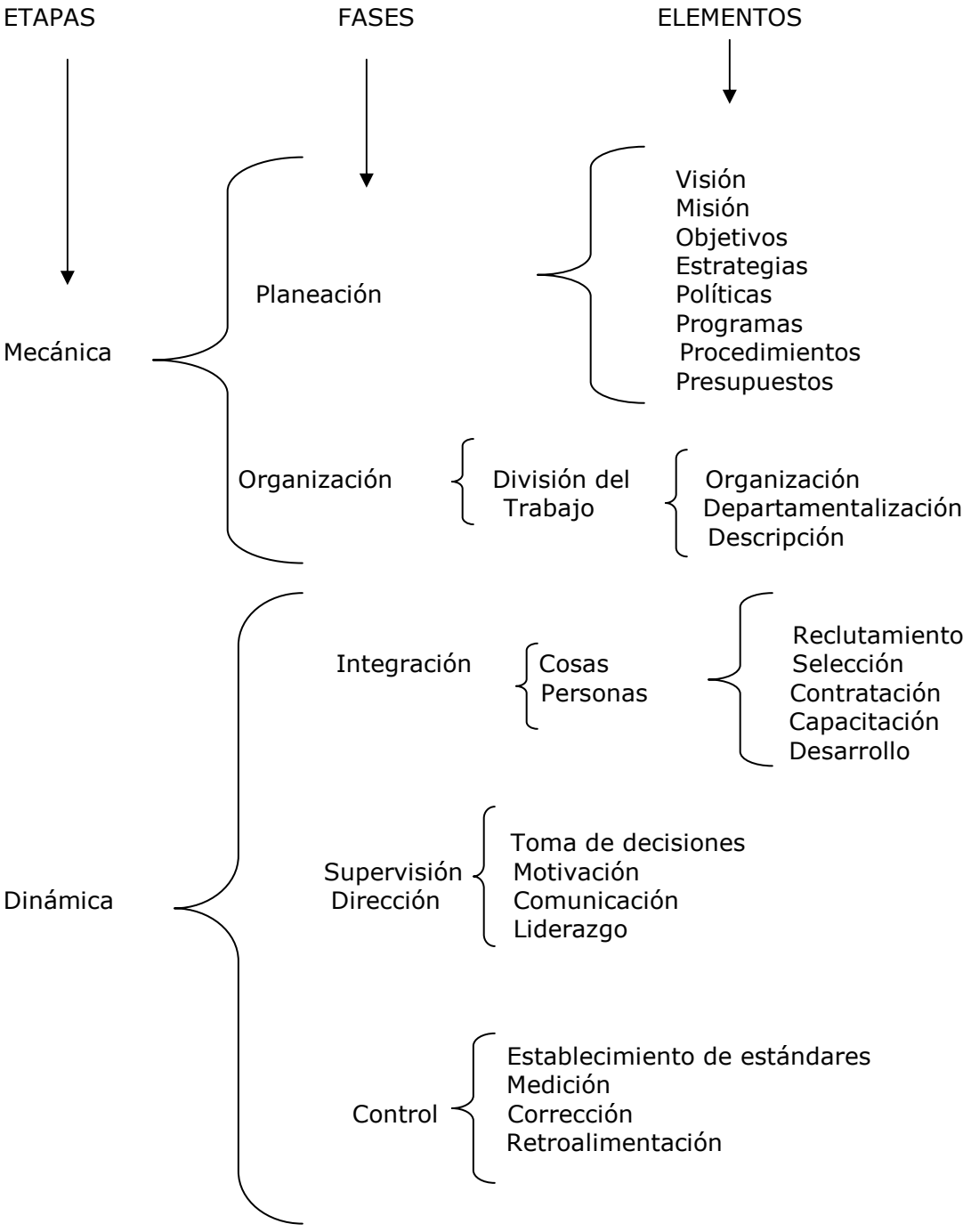


Figura 4.2 Cuadro esquemático del proceso administrativo

2. Organización, es el proceso de disponer y destinar el trabajo, la autoridad y los recursos entre los miembros de una organización, en una forma tal que pueda lograr los objetivos de la misma de manera eficiente. Los administradores deben adecuar la estructura de la organización con sus objetivos y recursos, un proceso que se denomina diseño organizacional. Es la parte de la administración que supone el establecimiento de una estructura intencionada de los papeles que los individuos deberán desempeñar en una organización. La estructura es intencionada, en el

sentido de que debe garantizar la asignación de todas las tareas necesarias, para el cumplimiento de las metas, asignación que debe hacerse a las personas mejor capacitadas para realizar estas tareas.

I. Elementos

- Funciones
  - La identificación y la clasificación de las actividades requeridas.
  - La agrupación de las actividades necesarias para el cumplimiento de los objetivos.
  - La asignación de cada grupo de actividades a un administrador dotado de la autoridad (delegación) necesaria para supervisarlo.
  - La estipulación de coordinación horizontal (en un mismo o similar nivel organizacional) y vertical (entre las oficinas generales, una división y un departamento) en la estructura organizacional.
- Jerarquías
  - Fijar la autoridad y la responsabilidad correspondiente a cada nivel que existe dentro de una organización.
- Puestos
  - Las obligaciones y requisitos que tienen en concreto cada unidad de trabajo susceptible de ser desempeñada por una persona.

3. Integración, consiste en los procedimientos para dotar al organismo social de todos aquellos elementos, tanto humanos como materiales, que la mecánica administrativa señala como necesarios para su más eficaz funcionamiento, escogiéndolos, introduciéndolos, articulándolos y buscando su mejor desarrollo. Aunque la integración comprende cosas y personas lógicamente son importantes las personas y, sobre todo, los elementos administrativos o de mando.

   Consiste en ocupar y mantener los puestos de la estructura organizacional. Esto se realiza mediante la identificación de los requerimientos de fuerza de trabajo, el inventario de las personas disponibles y el reclutamiento, selección, contratación, ascenso, evaluación, planeación de carrera, compensación y capacitación o desarrollo, tanto de candidatos como de empleados en funciones, a fin de que puedan cumplir eficaz y eficientemente sus tareas.

   I. Elementos

   - Selección, es el proceso para elegir entre varios candidatos, dentro o fuera de la organización a la persona más indicada para ocupar un puesto en ese mismo momento o en el futuro.
   - Introducción, la mejor manera para lograr que los nuevos elementos se articulen lo más óptima y rápidamente que sea posible al organismo social.
   - Desarrollo, es un método sistemático integrado y planeado que se realiza a través de la capacitación, el adiestramiento y la formación del personal para elevar la eficacia de grupos de personas y de la organización o de una unidad organizacional importante.

4. Dirección, es impulsar, coordinar y vigilar las acciones de cada miembro y grupo de un organismo social, con el fin de que el conjunto de todas ellas realice del modo más eficaz los planes señalados.

Es el hecho de influir en los individuos para que contribuyan a favor del cumplimiento de las metas organizacionales y grupales; por lo tanto, tiene que ver fundamentalmente con el aspecto interpersonal de la administración.

I. Elementos

- Autoridad y mando, es el principio del que deriva toda la administración y por lo mismo, su elemento principal, es la dirección o liderazgo, arte o proceso de influir en las personas.
- Comunicación, es la transferencia de información de un emisor a un receptor, el cual debe estar en condiciones de comprenderla.
- Delegación, es la forma técnica para comunicar a los subordinados la facultad de decidir sin perder el control de lo que se ejecuta.
- Supervisión, es revisar si las cosas se están haciendo tal y como se habían planeado y ordenado.

5. Control, consiste en el establecimiento de sistemas que permitan medir los resultados actuales y pasados, en relación con los esperados, con el fin de saber si se ha obtenido lo que se esperaba, a fin de corregir y mejorar. El control permite formular nuevos planes, a través de la medición y corrección del desempeño individual y organizacional, para garantizar que los hechos se apeguen a los planes. Implica la detección de desviaciones respecto a las normas y la contribución de la corrección de estas. En pocas palabras el control facilita el cumplimiento de los planes. Las actividades del control suelen relacionarse con la medición de los logros.

   I. Elementos

   - Establecimiento de normas, criterios de desempeño, para que los administradores puedan recibir señales de cómo marchan las cosas.
   - Medición del desempeño, debe realizarse idealmente con fundamento en la previsión, a fin de que las desviaciones puedan detectarse antes de que ocurran y evitarse mediante las acciones apropiadas.
   - Corrección de las variaciones respecto de normas y planes, es el punto de control que puede concebirse como parte del sistema total de administración y ponerse en relación con las demás funciones administrativas.

En la dirección general se lleva se a cabo todo el proceso administrativo para el cumplimiento de objetivos de la organización.

4.2 Habilidades directivas del administrador de redes

Un administrador de red sirve a los usuarios, crea espacios de comunicación, atiende sugerencias, mantiene las herramientas y el espacio requerido por cada usuario, a tiempo y de buena forma, mantiene el hardware y el software de la computadoras y las redes a su cargo, mantiene documentación que describe la red, el hardware y el software que administra, respeta la privacidad de los usuarios y promueve el buen uso de los recursos. Por estos motivos y tomando en cuenta las actividades del administrador, enunciamos las siguientes habilidades con las que debe contar para realizar con éxito sus funciones.

4.2.1 Comunicación

La comunicación es un medio por el cual la dirección, dentro de una organización debe de saber como satisfacer sus objetivos.

En la comunicación hay tres elementos básicos: el emisor, el mensaje y el receptor. Existe la comunicación de manera escrita y oral, así como la formal, aquella que la organización establece oficialmente para transmitir o recibir mensajes y la informal aquella al margen de los canales oficiales.

Existen problemas para tener una comunicación adecuada y estos pueden ser causados por factores como la filtración, el lenguaje y el ruido.

En la dirección, la comunicación es una parte muy importante, por que es el medio a través del cual se tiene un contacto con los empleados, para poder brindarles la información adecuada y así lograr en conjunto los objetivos de la organización.

4.2.2 Motivación

Motivación se define como la voluntad para hacer un gran esfuerzo por alcanzar las metas de la organización, condicionado por la capacidad del esfuerzo para satisfacer alguna necesidad personal.

La motivación se aplica a una amplia serie de impulsos, deseos, necesidades, anhelos y fuerzas similares. Decir que los directivos motivan a sus subordinados, es decir que realizan cosas con las que esperan satisfacer esos impulsos y deseos e inducir a los subordinados a actuar de determinada manera.

MC. Clelland afirma que las personas se motivan principalmente por tres factores:

1. La motivación a la realización, consiste en lograr metas con miras a obtener un beneficio de ellas.
2. La motivación por la afiliación, se orienta a establecer contactos cercanos con las personas.
3. La motivación al poder, se caracteriza por el deseo de influir sobre los demás.

La motivación puede o no ser afectada dentro de una organización por características como las siguientes:

- Aspectos individuales: intereses y objetivos.
- Aspectos del trabajo: lo que desempeñan.
- Aspectos del sistema de trabajo: el ambiente laboral.

A. Aplicación de factores de motivación en la organización

Con base en diferentes investigaciones, se ha demostrado que la aplicación de los siguientes factores conducen al cumplimiento de los objetivos de la organización.

- Hacer interesante el trabajo.
- Relacionar las recompensas con el rendimiento.
- Proporcionar recompensas que sean valoradas.
- Satisfacción personal.
- Reconocimiento formal.
- Alentar a la participación y colaboración.

- Ofrecer retroalimentación.
- Tratar a los empleados como personas.

4.2.3 Liderazgo

Liderazgo es lograr que las cosas se hagan, cuando hay un objetivo que alcanzar o una tarea por cumplir y se necesita más que una persona para hacerlo; tratar de estimular e incitar a los individuos y equipos a dar lo mejor de ellos mismos, para alcanzar un resultado deseado.

Características del líder:

a. El líder debe tener el carácter miembro, es decir, debe pertenecer al grupo que encabeza, compartiendo con los demás miembros los patrones culturales y significados que ahí existen.

b. La primera significación del líder no resulta por sus rasgos individuales únicos, universales (estatura alta, baja, aspectos, voz, etc.).

c. Cada grupo considera líder al que sobresalga en algo que le interesa, o más brillante, o mejor organizador, el que posee más tacto, el que sea más agresivo o más bondadoso.

d. Cada grupo elabora su prototipo ideal y por lo tanto no puede haber un ideal único para todos los grupos. El líder debe organizar, vigilar, dirigir o simplemente motivar al grupo a determinadas acciones según sea la necesidad que se tenga.

e. Por último, otra exigencia que se presenta al líder, es la de tener la oportunidad de ocupar ese rol en el grupo, si no se presenta dicha posibilidad, nunca podrá demostrar su capacidad de líder.

4.2.4 Disciplina

La disciplina es la capacidad de actuar ordenada y perseverantemente, para conseguir un bien. Exige un orden y unos lineamientos para poder lograr más rápidamente los objetivos deseados, soportando las molestias que esto ocasiona. La principal necesidad para adquirir este valor es la autoexigencia, es decir, la capacidad de pedirnos a nosotros mismos un esfuerzo "extra" para ir haciendo las cosas de la mejor manera. El que se sabe exigir a sí mismo se hace comprensivo con los demás y aprende a trabajar y a darle sentido a todo lo que hace. La disciplina es indispensable para optar con persistencia por el mejor de los caminos; es decir, por el que va a dictar una conciencia bien formada que sabe reconocer los deberes propios y se pone en marcha para actuar.

4.2.5 Relaciones

Las relaciones humanas son las encauzadas a crear y mantener entre los individuos relaciones cordiales, vínculos amistosos, basados en ciertas reglas aceptadas por todos y fundamentalmente, en el reconocimiento y respeto de la personalidad humana.

4.3 Cómo lograr que los equipos de trabajo sean efectivos

4.3.1 Trabajo en equipo

El trabajo en equipo se concibe como una estrategia que destaca fortalezas y debilidades propias, así como oportunidades y amenazas a las que debemos enfrentarnos en nuestra práctica cotidiana, ayudando a las organizaciones a alcanzar los objetivos deseados.

La creatividad necesaria es fácil de lograr procurando los máximos niveles de participación, promoviendo el interés en las tareas, en las metas que se persiguen y en la forma de lograrlo.

Las razones más frecuentes para trabajar en equipo están relacionadas con factores que cubren diferentes tipos de necesidades, como lo son:

1. Seguridad, laborar en equipo disminuye la inseguridad de "estar solo". El individuo duda menos de sí mismo y resiste mejor las amenazas, gracias a la interacción con otros que le proporcionan confianza.
2. Estatus, los integrantes de un equipo considerado importante por los demás, derivan en reconocimiento y posición.
3. Autoestima, los equipos pueden hacer que las personas sientan que valen, promoviendo su desarrollo.
4. Afiliación, los equipos satisfacen las necesidades de amistad, relaciones sociales, apoyo y afecto.
5. Poder, objetivos que no son posibles de alcanzar individualmente, son posibles gracias a la acción conjunta de otros miembros del equipo.
6. Obtención de metas, una actividad particular, requiere el trabajo de varias personas. Un equipo reúne talentos, conocimientos y fuerzas para concluir un trabajo.

Los equipos desempeñan diversas funciones para sus integrantes, por ejemplo: existen comités permanentes de ejecutivos que se reúnen periódicamente, grupos de trabajos creados para analizar diferentes problemas, equipos temporales de proyectos que se reúnen para detectar y resolver problemas específicos.

Un equipo se convierte en un mecanismo por medio del cual sus miembros pueden resolver problemas o tareas, tomando decisiones grupales. Existen ventajas importantes para trabajar en equipo, entre las que destacan las siguientes:

1. Información y conocimiento completo.
2. Aumento de la diversidad de puntos de vista, que genera un ambiente heterogéneo que da pie a enfoques amplios con mayores alternativas.
3. Mayor aceptación de una solución, por parte de los integrantes de un grupo.

De la misma manera es posible resaltar algunas desventajas de este mecanismo, como se muestra a continuación:

1. Lentitud, se requiere tiempo para laborar en equipo.
2. Presiones de conformismo, existen presiones sociales como el deseo que tienen los miembros de ser aceptados y considerados como elementos positivos, lo cual genera estancamiento en la controversia y genera conformismo.

3. Dominio de uno o algunos de los miembros en el equipo.
4. Responsabilidad dispersa.

La evidencia obtenida de las investigaciones revela que los equipos alcanzan mejores resultados que los individuos. Las decisiones individuales se caracterizan por su rapidez, sin embargo un equipo fomenta la creatividad y cooperación.

4.3.2 Características de los equipos de trabajo

Las cualidades personales y profesionales, son atributos de los integrantes en particular de un equipo de trabajo. Entre estas características podemos destacar:

1. El nivel del conocimiento global del equipo.
2. Capacidad de aportar y sugerir ideas.
3. Capacidad de escuchar, dialogar y debatir.
4. Predisposición a los acuerdos.
5. Vinculación y compromiso en la organización.
6. Capacidad de ejercer el liderazgo.
7. Credibilidad personal y profesional.

Regularmente los equipos de trabajo se ven influenciados por dos fenómenos que pueden llegar a mermar su funcionamiento:

a. Pensamiento del equipo, se refiere a las normas y descripción de situaciones donde las presiones del grupo para lograr el conformismo impiden al equipo juzgar con espíritu crítico las opiniones originales, poco populares o minoritarias. Los miembros se ajustan a las suposiciones, sin expresar inquietudes, generando una ilusión de unanimidad. El pensamiento del equipo es un efecto natural, de deseo de alcanzar un consenso y acuerdo, pero puede causar un efecto destructivo sobre el desempeño del equipo de trabajo.
b. Tendencia inicial del equipo, indica que al discutir una serie de alternativas y llegar a una solución, los miembros del equipo suelen exagerar las posiciones iniciales y generar situaciones que impidan enfrentar un riesgo en la toma de decisiones innovadoras.

4.3.3 Métodos para el buen funcionamiento de un equipo de trabajo

El administrador de redes, debe estar al pendiente de las actividades, la satisfacción laboral, la comunicación y otras variables de los equipos de trabajo. Para ello se requiere contar con el conocimiento que nos permita solucionar y mejorar algunas situaciones que impiden el correcto funcionamiento del área.

A. Satisfacción laboral

Estrechamente ligada al desempeño y al ambiente de una organización, la satisfacción laboral, se considera como un factor determinante que permite que un integrante del equipo realice su labor con calidad y eficiencia.

B. Comunicación

El proceso de intercambio de mensajes, está ligado a factores como la percepción, la motivación, los roles y las normas; determinando la eficacia con la que se transmite el significado del mensaje.

La comunicación perfecta es inalcanzable, sin embargo se puede buscar una comunicación eficaz que incluye percepciones de confianza, exactitud, deseo de interacción, receptividad y claridad en el lenguaje.

Una comunicación deficiente es la causa de conflictos interpersonales que inhiben el buen desempeño de un equipo. El proceso comunicativo representa un incremento de mensajes, donde el factor humano genera distorsión que altera el resultado. Se dice que la comunicación es perfecta cuando una idea o pensamiento es transmitido de modo que la imagen mental percibida por el receptor coincide con la del emisor, sin embargo la mayoría de las veces no es posible alcanzarla.

La comunicación realiza 4 funciones básicas dentro de un equipo:

a. Control, la comunicación sirve para controlar el comportamiento de los integrantes de un equipo debido a que las organizaciones poseen jerarquías de autoridad y normas formales que requieren ser aceptadas.
b. Motivación, la comunicación propicia la motivación al esclarecer a los trabajadores lo que debe hacerse, la eficiencia con la que se están llevando a cabo las actividades y las medidas para mejorar el desempeño además de la fijación de metas, la retroalimentación unido al reforzamiento de la conducta deseada, estimulan la motivación.
c. Expresión de emociones, el trabajo en equipo constituye la principal fuente de interacción social, la comunicación dentro de él, es un mecanismo indispensable, para externar frustración y sentimientos de satisfacción, de manera que permita la expresión emocional de las necesidades sociales.
d. Expresión de información, proporciona la información que necesitan los individuos y equipos para tomar decisiones al transmitir los datos, con los cuales se podrán identificar y evaluar las diferentes alternativas de solución.

Para que los equipos de trabajo desempeñen un buen rendimiento, es preciso que conserven alguna clase de control sobre sus miembros, que estimule su desempeño y que los motive a tomar decisiones.

Existen condiciones que afectan la transmisión de un mensaje en el proceso de comunicación, éstas suelen agruparse en 4 grupos:

a. Habilidades, entre las cuales se requieren para una eficacia global en la comunicación: el habla, la lectura y la capacidad de escuchar y razonar.
b. Actitudes, las cuales influyen en el comportamiento y por consecuencia en la comunicación.
c. Conocimientos, el conocimiento en algunas áreas del saber limita la capacidad comunicativa, debido a que no podemos comunicar algo que no sabemos y si el conocimiento es vasto quizás el receptor no entenderá el mensaje.

d. Sistemas socioculturales, las creencias y valores del individuo forman parte de su cultura que influye en su percepción, en el proceso de la comunicación.

Nuestro sistema sociocultural, nivel de conocimientos, actitudes y habilidades influyen en la capacidad de recibir y enviar un mensaje. Para que estos factores no alteren nuestro proceso comunicativo, existe un elemento llamado retroalimentación, que permite comprobar la eficacia con que se ha transmitido el mensaje, al determinar que se ha logrado la comprensión del mismo.

Además de las deformaciones propias del proceso comunicativo existen otras barreras que la obstaculizan y que es necesario que un administrador de redes conozca para poder enfrentarlas, éstas se describen a continuación:

1. Filtración, denota manipulación de la información por quien envía el mensaje, con el objeto de que sea vista más favorablemente por el receptor. La información que llega a los niveles superiores es condensada y sintetizada por los subordinados para no exceder en detalles de la información. La filtración pretende decir lo que el jefe quiere escuchar, con la consecuente pérdida de objetividad.
2. Emociones, el estado de ánimo del receptor en el momento en el que le llega un mensaje, incidirá en la interpretación que de él haga. Un mismo mensaje recibido cuando se está enojado o preocupado será interpretado en forma diferente cuando el estado de ánimo es alto o neutral. Las emociones extremas como el gozo y la depresión, fácilmente obstaculizan una buena comunicación. En estos casos estamos propensos a dejarnos llevar por la emoción, más que por el pensamiento racional y objetivo.
3. Lenguaje, las palabras significan cosas diferentes, para cada persona. El significado de la palabra no está en ella, si no en nosotros mismos y éste depende de la edad, la escolaridad y el sistema cultural de la persona.

Dentro de los equipos de trabajo también se encuentra la presencia de los rumores, forma de comunicación informal que despierta el interés de una gran mayoría, ante circunstancias ambiguas. Los principales propósitos de los rumores, son la interpretación de información escasa o fragmentada y servir de vehículo para organizar a los miembros de un equipo.

El rumor forma parte integral de la red de comunicación de cualquier equipo de trabajo y debe ser utilizado para identificar las cuestiones confusas que otros juzguen importantes, siendo considerado como excelente elemento de retroalimentación que no puede ser eliminado. Es posible manejar los rumores reduciendo sus efectos negativos, siguiendo una serie de recomendaciones como las que se listan a continuación:

- Anunciar un horario para tomar decisiones importantes.
- Explicar las decisiones y conductas que parecieran incongruentes o secretas.
- Dar a conocer riesgos positivos o negativos de las decisiones actuales y de los planes futuros.

Para transmitir un mensaje no sólo se requieren palabras, se consideran aspectos físicos como: una sonrisa, un fruncimiento de ceño, un movimiento provocativo del cuerpo, elementos que transmiten un significado adicional.

Todo movimiento corporal tiene un significado, con el cual externamos nuestro estado de ánimo, por ejemplo: un levantamiento de ceja expresa incredulidad, un frotamiento de nariz indica un estado de desconcierto, las manos en la frente indican aislamiento o reflexión, un

levantamiento de hombros es un gesto de indiferencia, cerramos un ojo para denotar complicidad, etc.

Aunque la interpretación del lenguaje corporal no sea universal, esta enriquece y a menudo complica la comunicación verbal.

De la misma manera los tonos de voz, son partícipes en el proceso de comunicación: un tono suave y sereno produce un significado distinto del de una entonación áspera y con énfasis fuerte en la última palabra.

Las expresiones faciales junto con las entonaciones, demuestran una serie de actitudes personales que fortalecen el proceso de comunicación.

Cada palabra, acción, silencio u omisión transmite un significado. La gente creará sus propios mensajes ante las señales que recibe de otros y esta interpretación es uno de los determinantes en la satisfacción o insatisfacción en ella.

C. Técnicas para el trabajo en equipo

Para lograr que el equipo funcione es posible que el administrador recurra a técnicas que permitan aminorar los problemas de interacción, en la búsqueda de mejores soluciones. Entre las principales encontramos:

1. Lluvia de ideas, su objetivo es superar las presiones de conformismo en el equipo, que retardan las alternativas creativas. Esto se logra mediante un proceso generador de ideas. El procedimiento para aplicar esta técnica, incluye una sesión entre 6 y 12 personas sentadas alrededor de una mesa. El líder del equipo plantea el problema con claridad de manera que los integrantes lo entiendan, solicita la expresión con toda libertad de todas las alternativas pensadas durante un determinado tiempo, en el que no se admiten críticas. Al término de este intercambio, las opiniones se analizan y discuten.
2. Grupo nominal, limita la discusión interpersonal durante el proceso de la toma de decisiones. Para realizarla, los miembros del equipo están físicamente presentes, se formula el problema y se siguen los siguientes pasos:
   a. Los participantes se reúnen en equipos, pero antes de iniciar la discusión, cada uno escribe sus ideas referentes al problema.
   b. Posteriormente cada participante expone una de sus ideas, resaltando sus características y anotándola en un pizarrón. El procedimiento se repite para todos los participantes.
   c. El grupo discute la claridad de las ideas y las evalúa.
   d. Cada miembro clasifica las ideas en silencio. La decisión final se toma a partir de la idea que logra la clasificación global más elevada.

   La principal ventaja de la técnica del grupo nominal es que permite al grupo reunirse formalmente pero sin limitar el pensamiento, llegando a una solución viable.
3. Técnica Delphi, técnica compleja y lenta que no requiere la presencia física de los participantes e incluye los siguientes pasos:
   a. Identificación del problema, para solicitar a los miembros del equipo soluciones mediante una serie de cuestionarios diseñados.
   b. Cada miembro completa el primer cuestionario en forma anónima e independiente.

c. Los resultados del primer cuestionario se recopilan, se transcriben y reproducen en una oficina central.

d. Cada miembro recibe una copia de los resultados.

e. Después de analizar los resultados se pide de nuevo la opinión, lo que da origen a nuevas soluciones o modificaciones en la postura inicial.

Los pasos d y e, se repiten hasta lograr un consenso.

La Tabla No. 4.1 muestra un análisis de las ventajas y desventajas de las técnicas anteriores.

Criterio de eficacia	Tormenta de ideas	Nominal	Delphi
Número de ideas	Moderado	Alto	Alto
Calidad de las ideas	Moderado	Alta	Alta
Presión social	Baja	Moderada	Baja
Tiempos/costos	Bajo	Bajo	Alto
Orientación a las tareas	Alta	Alta	Alta
Posibilidad de conflicto interpersonal	Baja	Moderada	Alta
Sensación de logro	Alta	Alta	Moderada
Compromiso con la solución	No aplicable	Moderado	Bajo
Aumento de la cohesión del grupo	Alto	Moderado	Bajo

Tabla No. 4.1 Análisis comparativo de las técnicas de trabajo en equipo

4.4 Habilidades para el manejo de conflictos

Definimos al conflicto como un proceso que se inicia cuando una parte percibe que otra ha afectado de manera negativa o que está a punto de afectar, alguno de sus intereses.

Los conflictos interpersonales e intergrupales se presentan en todas las organizaciones y son parte de las relaciones sociales, ejemplos de ellos se dan entre individuos de un mismo grupo, una persona y su jefe, entre uno o más departamentos de una organización, entre el sindicato y la administración, etc.

El conflicto puede generar consecuencias positivas o negativas, centrando el objetivo en saber como manejarlo de manera que se puedan obtener los mejores beneficios y minimizar los aspectos adversos.

Los efectos negativos del conflicto se deben a factores como la ruptura de la comunicación, la coherencia y la cooperación. Regularmente los individuos que se encuentran involucrados en ellos, presentan tensión nerviosa, frustración y ansiedad, que hacen que su desempeño no sea óptimo.

A pesar de los efectos negativos del conflicto, se puede considerar un cambio necesario en la organización, siendo fuente de motivación para desarrollar métodos inventivos y de progreso continuo.

4.4.1 Corrientes del pensamiento del conflicto

En la Tabla No. 4.2 se resumen las corrientes del pensamiento que analizan el conflicto junto a sus principales características.

Corriente	Características
Tradicional	Afirma que el conflicto se debe evitar, pues es un indicador de un mal funcionamiento y resulta negativo y violento.
Relaciones humanas	Afirma que el conflicto, es un resultado normal e inevitable de cualquier grupo y no son malos, si no que se pueden considerar como una fuerza positiva que determina el rendimiento del grupo.
Interactiva	Propone que los conflictos son imprescindibles para un desempeño eficiente en una organización, promoviendo que los líderes conserven un grado mínimo constante de conflicto, que haga de la organización un elemento viable, auto-crítico y creativo.

Tabla No. 4.2 Corrientes del pensamiento sobre el conflicto

La corriente interactiva, propone la existencia de dos tipos de conflictos:

1. Conflictos funcionales, refuerzan las metas del grupo y mejoran su rendimiento, a través de fomentar el interés, la curiosidad, el entorno de evaluación de uno mismo y el cambio.
2. Conflictos disfuncionales, los cuales entorpecen el rendimiento del grupo.

4.4.2 Etapas del proceso del conflicto

Los administradores de redes interactúan con su personal y diariamente se enfrentan a conflictos, por lo que es de vital importancia conocer a detalle el proceso del conflicto, el cual se resume en la Figura 4.3.

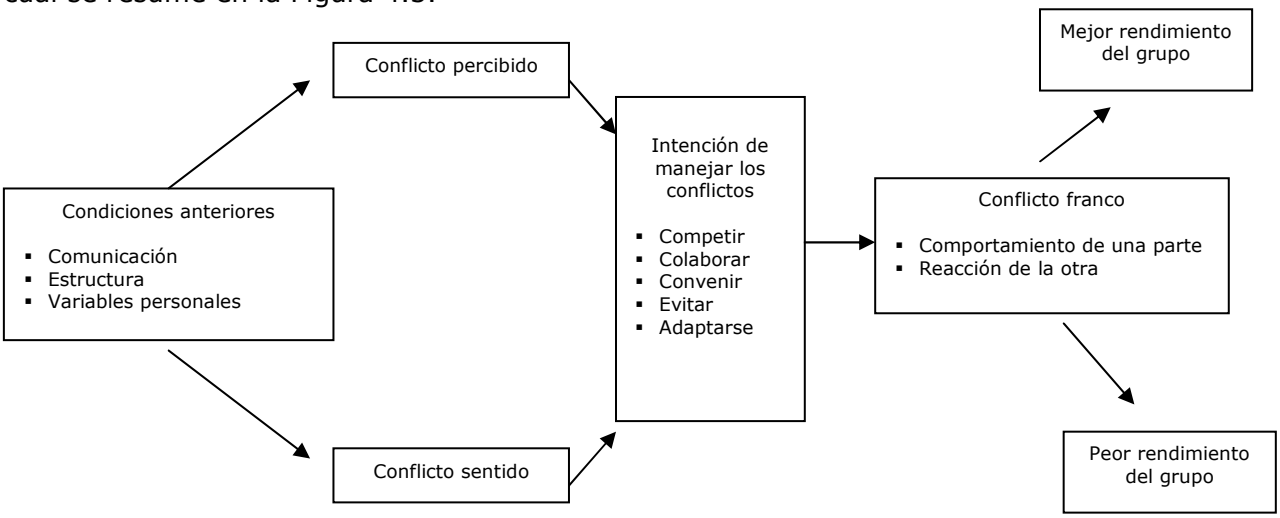


Figura 4.3 Etapas del proceso del conflicto

El proceso del conflicto se compone de 5 etapas:

1. Posible oposición o incompatibilidad, se da en presencia de condiciones que favorecen al conflicto las cuales se clasifican en 3 grupos:
   a. Comunicación, engloba malos entendidos y ruido en los canales de comunicación que retrasan la colaboración.
   b. Estructura, incluye el tamaño, grado de especialización en las actividades asignadas a los miembros, claridad de la jurisdicción, estilos de liderazgo, interdependencia, sistemas de premios, etc.

c. Variables de personalidad, incluye el sistema de valores personales que propicia las diferencias individuales.

2. Conocimiento y personalización, es el punto donde se definen las cuestiones del conflicto y se delinea la serie de posibles arreglos. Se resalta la importancia de las emociones que generan en ocasiones, percepciones negativas o bien el sentimiento positivo que permite soluciones innovadoras.

3. Intenciones, se consideran las decisiones sobre como actuar de una forma determinada, intervienen las percepciones, las emociones y sus conductas. Ofrecen lineamientos a seguir en una situación de conflicto. Considerando dos parámetros: la disposición a cooperar y la reafirmación (necesidad de satisfacer sus propios intereses), se identifican 5 intenciones para manejar conflictos, que se muestran en la Tabla No. 4.3.

Intención	Característica
Competidor	En busca de la satisfacción de los propios intereses independientemente del impacto que produzca en las otras partes del conflicto.
Colaborador	Situación donde las partes de un conflicto desean satisfacer plenamente los intereses de ambas partes.
Evasivo	Se observa el deseo de retirarse de un conflicto o acabarlo, tratando de ignorarlo y evitando a las personas con quienes no se está de acuerdo.
Acomodático	Implica la disposición de una de las partes para colocar los intereses de la otra parte por encima de los propios, con objeto de conservar la relación.
Conciliación	Situación donde las partes en conflicto están dispuestas a ceder algo.

Tabla No. 4.3 Intenciones para resolver el conflicto

Una persona puede elegir una o más de las intenciones anteriores, para manejar un conflicto, con base a una combinación de sus características intelectuales y personalidad.

4. Conducta, es la etapa en el que el conflicto se vuelve visible, incluye afirmaciones, actos y reacciones de las partes en conflicto. Se considera como un proceso dinámico de interacción donde son aplicadas las técnicas para la administración del conflicto, descritas más adelante.

5. Resultados, son la consecuencia de las acciones tomadas y son clasificadas en dos tipos:

   a. Resultados funcionales, en este caso el conflicto produce una mejoría en el rendimiento del grupo, se ha comprobado que genera dinamicidad.

   b. Resultados disfuncionales, entorpecen el rendimiento del grupo a través del rompimiento de vínculos de comunicación que conducen a la destrucción del grupo.

4.4.3 Estrategias de administración del conflicto

La administración del conflicto, significa el mantenimiento de un nivel de conflicto que resulta óptimo para la supervivencia y efectividad de la organización. Este nivel puede elevarse o disminuirse alterando las condiciones de la organización.

Existen diferentes estrategias de respuesta para administrar un conflicto, que se clasifican en:

1. Intentos de evasión, que incluyen actitudes de abandono y allanamiento que impiden la confrontación del conflicto, en este grupo podemos encontrar las siguientes tácticas:

   - Allanamiento y acomodo, genera una situación en el que la parte dominante se vuelve opresiva y la parte sometida se vuelve menos resistente.
   - Retiro y abandono, reacción que implica cuando cualquier parte o ambos se retira. Esta solución es benéfica cuando sus actividades no son interdependientes, en el caso contrario donde se requiere coordinación, no existe una solución.
   - Tácticas de allanamiento y conciliación, consisten en que las partes ignoren sus diferencias y traten de ceder mediante acciones que expresen un deseo de cooperación y relación armoniosa con la otra parte, a través de ofrecimientos de reconocimiento y declaraciones de respeto, acciones que eviten hacer acusaciones, amenazas o agresiones hacia la otra parte y un compromiso de reforzamiento y declaraciones conciliatorias de la otra parte.

     El allanamiento puede ser un enfoque adecuado, para evitar la hostilidad y ruptura de relaciones de trabajo, mientras el origen del conflicto no esté relacionado con la ejecución de la tarea. Por el contrario este método no será efectivo si se utiliza para evitar la confrontación de desacuerdos acerca de problemas de coordinación y ejecución mutuos.

2. Confrontación, que ofrece soluciones para enfrentar un conflicto, entre las tácticas principales encontramos:

   - Persuasión, constituye un método para enfrentar el conflicto tratando de convencer a la parte contraria de cambiar de posición. Algunas acciones dentro de éste incluyen: proporcionar evidencia por medio de hechos concretos que respalden la postura, desacreditar la información que apoye la posición del oponente señalando los errores en el razonamiento, señalar las maneras que sus proposiciones beneficiarán a la otra parte. El éxito de estas acciones depende de la credibilidad de la persona que los hace, junto a la disposición de la parte contraria para considerar dichos argumentos. Las técnicas de persuasión más efectivas son aquéllas que no amenazan el ego de la parte contraria.
   - Tácticas de coerción y presión, este método consiste en forzar a la otra parte en ceder, debido a las diferencias en la autoridad. Se conforma por acciones como:

     a. Amenazas, es la advertencia explícita o implícita de que una acción en perjuicio de la otra parte, será tomada a menos que se cumpla con ciertas demandas. Estas acciones son creíbles, de acuerdo a la capacidad de realización de quien las hace.

     b. Secuencias de castigo, acciones agresivas para castigar si es necesario, aplicando una pequeña cantidad de poder de coerción, para mostrar lo que ocurrirá si no se cumplen con las demandas.

     c. Compromisos posicionales, es la declaración de una de las partes involucradas de que no cederá más y que la otra parte deberá hacerlo en vista de las consecuencias de un estancamiento. En esta clasificación encontramos las demandas no negociables y los ofrecimientos de tómalo o déjalo.

     d. Coaliciones, táctica común que busca un aliado con el poder o influencia suficientes para asegurarle una ventaja decisiva sobre la parte opositora. No es la mejor manera de resolver el conflicto, debido a que crea resentimiento en la parte débil, quien puede sabotear las pretensiones.

- Tácticas de negociación orientadas al intercambio, la negociación es el proceso de intercambio de concesiones hasta que se logra un compromiso. El objetivo de cada parte es obtener los máximos beneficios en las circunstancias sin depender de lo que reciba la otra parte. Entre las acciones que implican estas tácticas, encontramos:

  a. Proponer un mediador.

  b. Sugerir un intercambio de posibles soluciones.

  Este método no resulta efectivo en el caso de conflictos en los que predomina la desconfianza y la falta de disposición.

- Solución integral de problemas, su objetivo implica encontrar un arreglo que reconcilie a través de la integración las necesidades de ambas partes, definiendo al conflicto como un problema mutuo, donde las partes implicadas cooperan en la búsqueda de una solución satisfactoria para ambas. Existe un intercambio de información abierto y honesto de los hechos, necesidades y sentimientos. Cada participante pretende entender el conflicto desde el punto de vista de la otra parte y descubrir las necesidades que deben ser solucionadas en el arreglo. El éxito de este camino recae en la cooperación y creatividad de ambas partes.

En la Figura 4.4 se muestran las tácticas de resolución de conflictos, donde claramente se observa que:

1. La coerción o dominación refleja un deseo de satisfacer sólo los intereses personales.
2. El acomodo refleja un deseo de satisfacer sólo los intereses de la otra parte.
3. El abandono o allanamiento refleja poco deseo de satisfacer los intereses competitivos de cualquiera de las partes.
4. La solución integral refleja un fuerte deseo de satisfacer los intereses de ambas partes.
5. La negociación o compromiso refleja un deseo moderado de satisfacer los intereses de ambas partes.
6. La persuasión es un intermedio entre la coerción y la negociación.

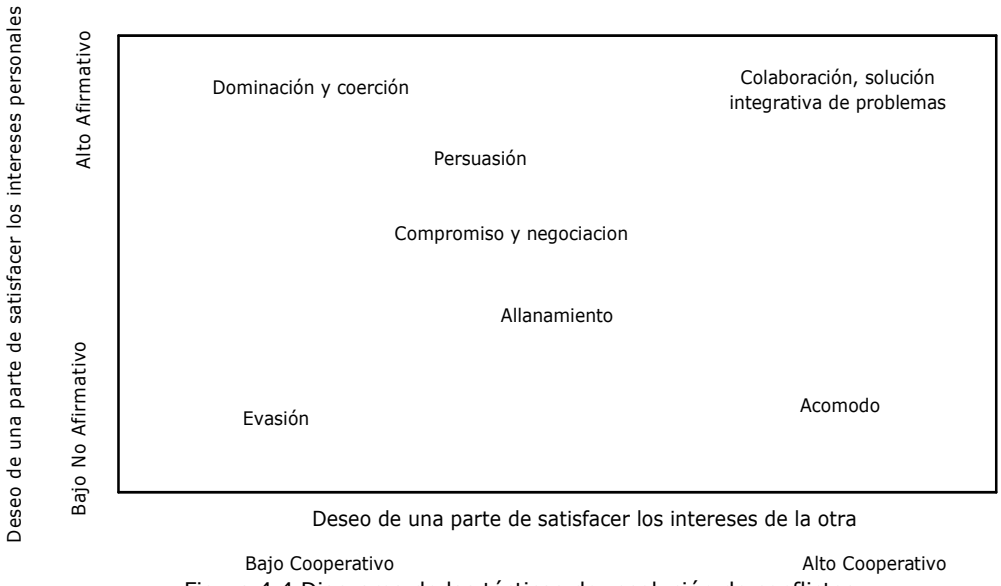


Figura 4.4 Diagrama de las tácticas de resolución de conflictos

A. Intervención de terceros

Los conflictos se agravan cuando existe una orientación de ganar-perder, debido a que existen pocas intenciones para alcanzar un común acuerdo. Siendo la única forma de resolverlos a través de una intervención externa. Los principales tipos de intervenciones de terceros son:

1. Arbitraje, procedimiento en que un tercero con autoridad, escucha a las partes en conflicto, funcionando como un juez en la determinación de un arreglo que obliga a ambas partes. Este sistema es una manera ordenada de arreglar las disputas y es preferible a usar la agresión mutua.

   Un árbitro puede ser efectivo, en la determinación de un arreglo justo, si está bien informado. El arbitraje se utiliza comúnmente para resolver disputas entre dos individuos o departamentos de una organización, por lo general el árbitro es el superior común con la autoridad de implantar un reglamento y vigilar su cumplimiento. El arbitraje será aceptable cuando ambas partes lo consideren como imparcial y objetivo.

2. Mediación, implica la participación de un tercero neutral que facilita la solución continua del conflicto, recurriendo al razonamiento y convencimiento sugiriendo nuevas alternativas. A diferencia del árbitro, el mediador no tiene autoridad directa sobre las partes opositoras y sus recomendaciones no son coercitivas. Sin embargo, restablece la comunicación que ha quedado interrumpida y propicia el intercambio de concesiones específicas. Un mediador facilita la solución integral de problemas, pues ayuda a reunir y aclarar la información cuando ésta es ambigua. El éxito del mediador dependerá de su poder de persuasión, prestigio y comprensión de las posiciones contrarias, siendo efectiva cuando el grado del conflicto es moderado.

3. Proceso de consulta entre las partes, difiere del arbitraje y la mediación, en su objetivo que consiste en mejorar la relación entre las partes y desarrollar su capacidad para resolver conflictos por sí mismos en el futuro.

   El consultor del proceso, no tiene el poder del arbitraje y no trata de mediar respecto a las propuestas existentes. Su labor consiste en utilizar técnicas diseñadas para aumentar la conciencia de cada una de las partes respecto a percepciones distorsionadas y conducta no funcional, que interfiere con la resolución del conflicto. Resulta una guía hacia el uso del descubrimiento de los hechos, sin dar soluciones específicas, propiciando las buenas relaciones a largo plazo y dando percepciones unidas a nuevas actitudes positivas. Entre las principales acciones que realiza un consultor del proceso se encuentran:

   a. Regulación de la localización, oportunidad y duración de las confrontaciones para asegurar una motivación positiva para resolver el conflicto.

   b. Animar a las partes en conflicto a diagnosticar las razones del problema.

   c. Impulsar la utilización de procesos de solución de problemas y desanimar las reacciones no productivas como amenazas, acusaciones y comentarios negativos.

   d. Facilitar la precisión de la comunicación, resumiendo la posición de cada parte.

4. Conciliación, un conciliador es un tercero en el que se tiene confianza y que ofrece un vínculo de comunicación informal entre las partes en conflicto. Regularmente se emplea en conflictos internacionales, laborales, familiares y comunitarios, aunque su papel llega a traslaparse con la mediación.

La solución del conflicto puede ser inhibida por los errores y limitaciones normales del proceso humano de juicio, cuando el conflicto comprende muchas premisas con resultados auditivamente diferentes.

B. Consejos para administrar el conflicto

De acuerdo a un gran número de investigaciones se ha encontrado que para lograr una estabilidad en una organización, es indispensable poner en práctica las técnicas de administración de conflictos, tomando los siguientes puntos como importantes:

1. Arbitrar directamente, cuando las partes son incapaces de resolver los conflictos de manera constructiva, el administrador común a ambas partes interviene en la solución.
2. Establecer reglas y procedimientos que permitan solucionar los conflictos.
3. Reducir la interdependencia, puede evitar conflictos, cuando se alteran aspectos de la organización formal. El método de reducir fricción entre las partes interdependientes, consiste en crear amortiguadores como el rediseño de puestos en el área.
4. Reasignar recursos, cuando el conflicto se produce por la competencia de recursos escasos.
5. Modificar el programa para la premiación, cuando la organización provoca el conflicto a través de la competencia, más que la cooperación es necesario modificar la planificación de premios.
6. Modificar los patrones de comunicación que regularmente son restringidos y distorsionados durante el conflicto, para proporcionar a las partes involucradas información más significativa y confiable.
7. Aumentar las habilidades para la superación del conflicto, los representantes de cada parte en conflicto deben contar con las habilidades interpersonales necesarias, para generar soluciones productivas.
8. Cuando el administrador toma una posición rígida, fomenta una actitud rígida como respuesta, cuando se fomenta una cooperación regularmente se origina una respuesta cooperativa.
9. Experiencia, los administradores que desarrollan habilidades para escuchar mejor, formular preguntas y aprender a abordar con argumentos directos, son menos ofensivos y evitan el uso de palabras y frases que irritan al opositor, generando un ambiente franco de confianza, necesario para tener un arreglo integrador.

Capítulo 5

CONTROL

INTRODUCCIÓN

La función administrativa del control es la medida y la corrección del desempeño, para garantizar que se lleven a cabo los objetivos de la organización y los planes diseñados para lograrlo. Sin objetivos y planes, el control es imposible, ya que el desempeño debe ser medido con base en algunos criterios establecidos.

Las técnicas y los sistemas de control son esencialmente los mismos para el dinero, los procedimientos de oficina, el ánimo, la calidad de servicio de una red, etc. El proceso básico de control, en donde sea que se implemente y se cual sea su objetivo, implica tres pasos:

1. Establecimiento de parámetros, que son criterios de desempeño, puntos elegidos en un programa total de planeación.
2. Medición del desempeño de dichos parámetros
3. Corrección de todo aquello que se desvíe de parámetros y planes.

El control de la red es un proceso continuo importante, que el administrador de red debe realizar, considerando para ello los siguientes puntos:

a. Seguridad de la red, considerada como un proceso continuo construido alrededor de las políticas de seguridad, eje del funcionamiento del sistema. Implica probar la efectividad de los esquemas de seguridad de acuerdo con cierta normatividad como el ISO17799, Criterios Comunes, etc.
b. Monitoreo de la red, esta acción implica mantener una supervisión continua de la red, estando alerta de todos los fenómenos que suceden en ella.
c. Control de acceso a la red, permitir quien puede usar y acceder a ciertos recursos de la red, genera un esquema de seguridad que puede disminuir ataques.
d. Auditorías informáticas a la red, revisar constantemente el funcionamiento de la red, conforme a las normas es vital.
e. Plan de contingencia en caso de desastres, permite reanudar la actividad en caso de un desastre que deje inoperante la red por un espacio de tiempo.

El control administrativo es esencialmente el mismo proceso básico de control que el que se encuentra en los sistemas físicos, biológicos y sociales. Muchos sistemas se autocontrolan a través de la retroalimentación, que muestra las desviaciones de los parámetros e inicia los cambios.

Los administradores de redes, miden el desempeño real de la red, comparan estas mediciones con los parámetros e identifican y analizan las desviaciones. Pero para realizar correcciones necesarias, deben desarrollarse programas correctivos y efectuarse con la finalidad de lograr el desempeño deseado.

5.1 Seguridad en redes

Al principio de su existencia, las redes de computadoras fueron usadas generalmente para el envío de correo electrónico y para compartir recursos, regularmente impresoras, en organizaciones de mediano a gran tamaño. En estas condiciones la seguridad carecía prácticamente de importancia y no fue objeto de atención. Sin embargo, en la actualidad millones de personas usan redes para transacciones bancarias, compras, etc. y la seguridad aparece como un problema potencial de grandes proporciones. Los problemas de seguridad de las redes pueden dividirse de forma general en cuatro áreas interrelacionadas:

- El secreto, encargado de mantener la información fuera de las manos de usuarios no autorizados.
- La validación de identificación, encargada de determinar la identidad de la persona-computadora con la que se está comunicando.
- El no repudio, encargado de asegurar la "firma" de los mensajes, de igual forma que se firma en un papel una petición de compra-venta entre organizaciones.
- El control de integridad, encargado de asegurar que el mensaje recibido fue el enviado por la otra parte y no un mensaje manipulado por un tercero.

El concepto de seguridad se refiere a todo tipo de precauciones y protecciones que se llevan a cabo, para evitar cualquier acción que comprometa a la información. La seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en esquemas, políticas de seguridad y herramientas de seguridad.

5.1.1 Esquemas de seguridad en red

Hay una amplia gama de tecnologías de seguridad que proporcionan soluciones para proteger el acceso a una red y los mecanismos de transporte de datos de la infraestructura de la misma. Las tecnologías se pueden utilizar de modo distinto a la hora de solucionar los problemas relacionados con la identidad del usuario o dispositivo, la integridad de los datos y la confidencialidad de los mismos.

A. Elementos de una arquitectura de seguridad

De manera general una arquitectura de seguridad debe incluir los siguientes elementos:

- Identidad, este elemento abarca la autenticación (que responde a la pregunta ¿quién es usted y dónde está?) y la autorización (que responde a la pregunta ¿a qué se le permite acceder?).
- Integridad, abarca la seguridad de los dispositivos de la infraestructura de la red: acceso físico a una computadora (o router, switch o firewall), acceso lógico (hace referencia a los mecanismos de identidad, es decir la autenticación y la autorización) y la seguridad del perímetro.
- Confidencialidad, garantiza la privacidad de la comunicación de los datos entre el remitente y el destinatario de la información.
- Disponibilidad, garantiza que todos los recursos vitales son accesibles.
- Auditoría, es necesario verificar y controlar las políticas de seguridad de la infraestructura de la red corporativa.

B. La seguridad de la red como un proceso continuo

La seguridad de la red debe ser un proceso continuo construido alrededor de las normas de seguridad. Unas políticas de seguridad continuas son más efectivas, porque promueven la prueba y la reaplicación de las medidas de seguridad actualizadas. Este proceso de seguridad se representa mediante el círculo de seguridad presentado en la Figura 5.1.

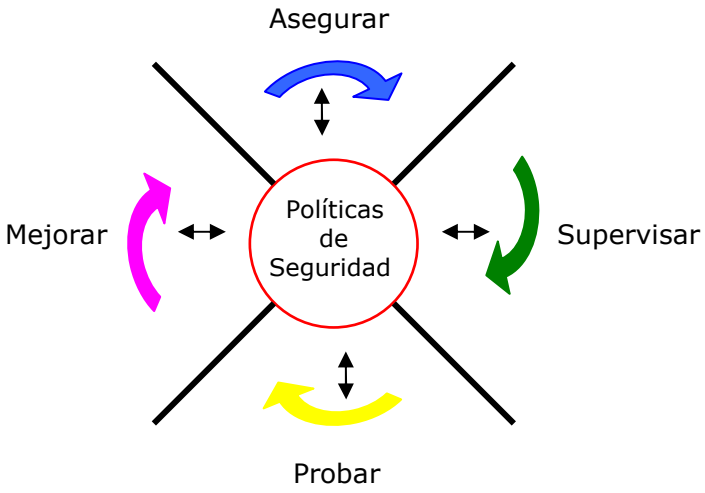


Figura 5.1 La seguridad en la red como un proceso continuo se construye alrededor de las políticas de seguridad

Para comenzar este proceso continuo conocido como círculo de seguridad, es preciso crear unas políticas de seguridad que permitan la aplicación de las medidas oportunas, para mayor detalle sobre las políticas de seguridad consultar la sección 5.1.4.

Las políticas de seguridad precisan la realización de las siguientes tareas:

- Identificar los objetivos de seguridad de la organización.
- Documentar los recursos que se van a proteger.
- Identificar la infraestructura de la red con planos e inventarios actualizados.

Tras desarrollar las políticas de seguridad, éstas se transforman en el eje sobre el que se basan los siguientes cuatro pasos del círculo de seguridad:

1. Asegurar el sistema, es necesario implementar los dispositivos de seguridad (cortafuegos, sistemas de autenticación de identificación, cifradores, etc.), con la intención de prevenir los accesos no autorizados a los sistemas de red.
2. Supervisar la red para comprobar violaciones y ataques contra las normas de seguridad de la organización. Las violaciones pueden producirse dentro del perímetro de seguridad de la red, por un empleado descontento o desde fuera de la red, por un hacker. La supervisión de la red mediante un sistema de detección de intrusos, puede asegurar que los dispositivos de seguridad del paso 1 han sido configurados correctamente.
3. Probar la efectividad de los esquemas de seguridad en un lugar. Utilizar un escáner de seguridad para identificar la postura de la red, respecto a los procedimientos de defensa que forman el eje del círculo de seguridad.

4. Mejorar la seguridad corporativa, supone recopilar y analizar información de las fases de prueba y supervisión para mejorar la seguridad.

Las fases de asegurar, supervisar, probar y mejorar se deben repetir continuamente, incorporando las versiones actualizadas de la política de seguridad de la organización.

C. Criterios Comunes

A finales de 1998 fue aprobado el esquema de evaluación de seguridad llamado CCITSF, Criterios Comunes para la Evaluación de Seguridad de Tecnología de la Información (Common Criteria for Information Technology Security) mejor conocido como CC, Criterios Comunes (Common Criteria).

Los CC son una norma internacional para evaluar la seguridad de los productos de la IT, Tecnología de la Información (Information Technology) basada en los criterios europeos, norteamericanos y canadienses existentes para la evaluación de la seguridad de la IT, por ello los resultados obtenidos al realizar una evaluación siguiendo los CC, son reconocidos internacionalmente. Además tiene por objetivo principal, el proporcionar protección a la información.

En la evaluación de las propiedades de seguridad de los productos de la IT, existen tres grupos que tienen interés general en la misma: los consumidores, los desarrolladores y los evaluadores.

Bajo los CC, las clases de productos son evaluadas basándose en los puntos de los PP, Perfiles de Protección que especifican los requerimientos funcionales de seguridad. Los PP deben ser desarrollados para aplicarse a los sistemas operativos, cortafuegos, tarjetas inteligentes y otros productos que se esperan que cuenten con requerimientos de seguridad.

Los perfiles de protección y las metas de seguridad, son elementos esenciales de la estructura de los CC:

- Un PP, Perfiles de Protección (Protection of Profiles) es un requerimiento que define un problema de seguridad general de un consumidor o grupo de consumidores. Establece: esto es lo que se necesita.
- Una ST, Meta de Seguridad (Security of Target) es una especificación que define una solución general de un desarrollador para un problema de seguridad. Establece: esto es lo que se ha construido o se construirá en el futuro.

A continuación se observa la Tabla No. 5.1 que generaliza las tres partes de los CC para los consumidores, los desarrolladores y los evaluadores.

	CONSUMIDORES	DESARROLLADORES	EVALUADORES
Definición	Para los consumidores son una forma de definir los requerimientos de seguridad IT, son los productos IT: • Hardware. • Software. • Firmware.	Para los desarrolladores son una forma de describir las facultades o capacidades de seguridad de IT de cada uno de sus productos IT de manera específica.	Para los evaluadores son una herramienta para medir el grado de confianza que se pueda tener en la seguridad de un producto
Parte I	Se utiliza para conocer antecedentes y propósitos de referencia, proporciona estructura y gu.ía de PPs.	Se utiliza para conocer antecedentes y como referencia para el desarrollo de requerimientos y formulación de especificaciones de seguridad para TOE, Objeto de Evaluación (Target of Evaluation).	Se utiliza para conocer antecedentes y propósitos de referencia, proporciona estructura y guía para PPs y STs.
Parte II Requerimientos funcionales	Se utiliza como guía y como referencia cuando es necesaria la formulación de informes de requerimientos para funciones de seguridad.	Se utiliza como referencia donde es necesaria la interpretación de informes de requerimientos funcionales y la formulación de especificaciones funcionales para TOEs	Se utiliza como informe obligatorio de criterio de evaluación donde es necesaria, se determina si un TOE efectivamente reúne las funciones de seguridad exigidas.
Partes III Requerimientos de garantía	Se utiliza como guía cuando es necesaria la determinación de los niveles requeridos de garantía.	Se utiliza como referencia donde es necesaria la interpretación de informes de requerimientos de seguridad y la determinación de aproximaciones de garantía de los TOEs.	Se utiliza como informe obligatorio del criterio de evaluación, donde se determinan las garantías de las TOEs y donde se lleva a cabo la evaluación de PPs y STs

Tabla No. 5.1 Elementos que integran los Criterios Comunes

D. OCTAVE

OCTAVE, Tratamiento Crítico Operacional, de Activos y Evaluación de las Vulnerabilidades (The Operationally Critical Threat, Asset and Vulnerability Evaluation). Metodología que utiliza un acercamiento de tres partes para ayudar a guiar a una organización a través del proceso de identificar y dirigir problemas de seguridad, ver Figura 5.2:

1. Construir perfiles con base en las amenazas.
2. Identificar vulnerabilidades en la infraestructura.
3. Desarrollar estrategias de seguridad y planes.

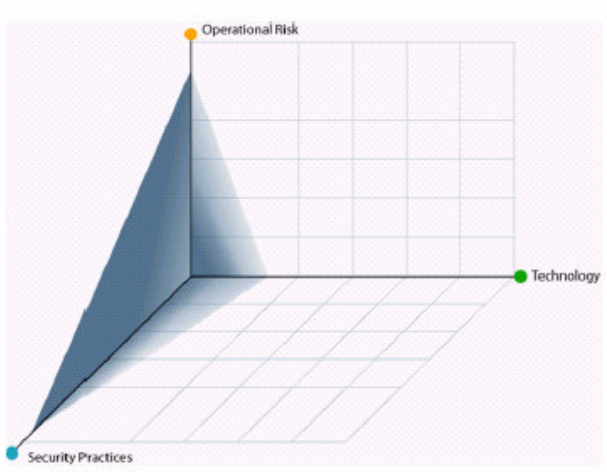


Figura 5.2 Balance de los tres aspectos de OCTAVE

El método OCTAVE se desarrolla en tres fases, que se conforman por varios pasos, para analizar los aspectos organizacionales y tecnológicos con el fin de obtener una visión de las necesidades requeridas en cuanto a seguridad. Cada fase se desarrolla de la siguiente forma, ver Figura 5.3.

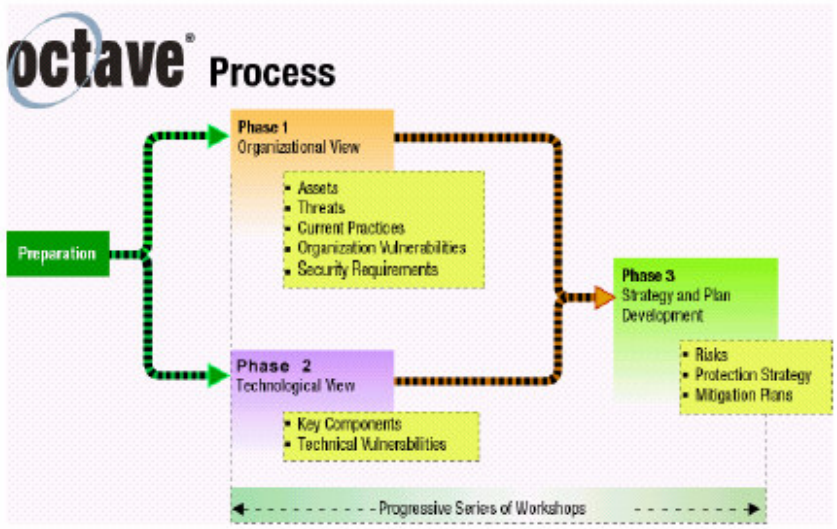


Figura 5.3 Diagrama de Octave

- Fase 1, implica desarrollar una lista de elementos a proteger y ataques que los afectan. En esta fase se determinan qué recursos o elementos son los más importantes, qué es lo que se hace actualmente para protegerlos y cómo pueden ser amenazados.
- Fase 2, incluye la identificación de los puntos vulnerables en la infraestructura. A través de esta fase se conocerán cuales son los puntos vulnerables, en cuanto a la infraestructura actual que puedan permitir acciones no autorizadas, a los elementos que se desean proteger.
- Fase 3, consiste en el desarrollo de planes y estrategias de seguridad. En esta fase se analizarán los riesgos que pueden afectar a los elementos críticos y se decidirá cómo protegerlos de dichos riesgos.

5.1.2 Normatividad ISO 17799

La normatividad ISO 17799, es un código de buenas prácticas para la administración de la seguridad informática, su origen se encuentra en el BS7799, (código de buenas prácticas para la administración de la seguridad de la información) propuesto en 1995 por el British Standard Institute, gracias a un grupo dedicado a la seguridad de la información, el CCSC–DTI, Centro Comercial de Seguridad en Cómputo del Departamento Británico de Comercio e Industria (Commercial Center of Security in Calculation of the British Department of Commerce and Industry) cuya tarea principal era la de brindar ayuda a los vendedores de productos de seguridad IT, mediante el establecimiento de un conjunto de criterios de evaluación de seguridad reconocidos internacionalmente.

Algunas organizaciones utilizaron el estándar BS7799, otras tantas expresaron la necesidad de un estándar común. Por tal demanda, se da el lanzamiento en diciembre del año 2000 y teniendo por nombre ISO/IEC 17799:2000, el único estándar de alto nivel dedicado al manejo de la seguridad de la información en un campo manejado por "Principios" y "Buenas Prácticas".

La ISO 17799, define la seguridad de información como la conservación de la confiabilidad, la integridad, la disponibilidad y la autenticidad, por lo tanto la seguridad de la información se logra implementando un conjunto de controles, los cuales pueden ser políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software. Estos controles necesitan ser establecidos para asegurar que se alcancen los objetivos específicos de seguridad de la organización.

A. Tipos de controles

El estándar ISO 17799 establece una clasificación de controles de acuerdo a sus objetivos en particular:

a. Basados sobre requerimientos legislativos, los cuales incluyen:
   - Protección de datos y privacidad de información personal.
   - Guardado de registros organizacionales.
   - Derechos de propiedad intelectual

b. Los considerados a ser la mejor práctica para la seguridad de la información e incluyen:
   - Información sobre la documentación de las políticas de seguridad.
   - Distribución de responsabilidades en la seguridad de la información.
   - Educación y entrenamiento en seguridad de la información.
   - Reporte de incidentes de seguridad.
   - Dirección de continuidad de negocios

B. Las diez áreas de control

La meta de la seguridad de la información, es proteger este recurso de manera oportuna y conveniente de un rango muy amplio de vulnerabilidades, de tal manera que se asegure la continuidad de la organización, se minimicen los daños y se maximicen las ganancias de las inversiones y las oportunidades de negocio. Por lo anterior, se han establecido diez áreas de control, las cuales se detallan a continuación:

1. Política de seguridad, se necesita una política que refleje las expectativas de la organización en materia de seguridad, a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación en curso.
2. Organización de la seguridad, sugiere diseñar una estructura de administración, dentro de la organización que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.
3. Control y clasificación de los recursos de información, implica un inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurarse que se brinde un nivel adecuado de protección.
4. Seguridad del personal, establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. Se debe tener e implementar un plan para reportar los incidentes.
5. Seguridad física y ambiental, responde a la necesidad de proteger las áreas, el equipo y los controles generales.
6. Manejo de las comunicaciones y las operaciones, implica conservar la integridad y disponibilidad del procesamiento y la comunicación de la información protegiéndola en las redes e infraestructura de soporte.
7. Control de acceso, establece la importancia de monitorear, controlar el acceso a la red y a los recursos de aplicación, para protegerlos contra los abusos internos e intrusos externos.
8. Desarrollo y mantenimiento de los sistemas, este punto recalca que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.
9. Manejo de la continuidad de la organización, aconseja estar preparado para contrarrestar las interrupciones en las actividades de la organización y para proteger sus procesos importantes en caso de una falla grave o desastre.
10. Cumplimiento, imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO 17799 concuerda con otros requisitos jurídicos, como la Directiva de la Unión Europea que concierne a la privacidad, la HIPAA, Ley de Responsabilidad y Transferibilidad del Seguro Médico (Health Insurance Portability and Accountability Act) y el GLBA, la ley de Modernización de Servicios Financieros (Gramm-Leach-Billey). Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoría del sistema, a fin de garantizar que las organizaciones obtengan el máximo beneficio.

5.1.3 Identificación de amenazas y tipos de ataques

Una amenaza es todo aquello que intenta destruir o pretende destruir. Entre los factores que dan lugar a una amenaza, se encuentran los desastres naturales, las fallas por software y hardware, los códigos maliciosos y el factor humano. Por lo anterior es posible afirmar que un ataque es la actuación de una amenaza.

A. Identificación de amenazas

Se suelen dividir las amenazas que existen sobre los sistemas informáticos en tres grandes grupos, en función del ámbito o la forma en que se pueden producir:

a. Desastres del entorno, dentro de este grupo se incluyen todos los posibles problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Por ejemplo, se han de tener en cuenta desastres naturales (terremotos, inundaciones, etc.), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico y peligros relacionados con operadores, programadores o usuarios del sistema.

b. Amenazas en el sistema, bajo esta denominación se contemplan todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad, etc.

c. Amenazas en la red, cada día es menos común que una máquina trabaje aislada de todas las demás; se tiende a comunicar equipos mediante redes locales, intranets o la propia Internet, esta interconexión acarrea nuevas y peligrosas amenazas a la seguridad de los equipos, peligros que hasta el momento de la conexión no se suelen tener en cuenta. Por ejemplo, es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red, a proteger una red local del resto de Internet o a instalar sistemas de autenticación de usuarios remotos, que necesitan acceder a ciertos recursos internos de la organización (como por ejemplo un investigador que se conecta desde su casa a través de un módem).

Hay que considerar hacer los respaldos de la información, contar con una sede alterna, llevar a cabo simulacros, contar con un plan de contingencia. Y también es muy importante saber como responder ante una amenaza.

B. Clasificación general de las amenazas

La Figura 5.4 muestra, el flujo normal de la información el cual no debe presentar ningún tipo de obstáculo, para que la información llegue al destinatario. Este flujo de información se encuentra bajo cuatro posibles amenazas:

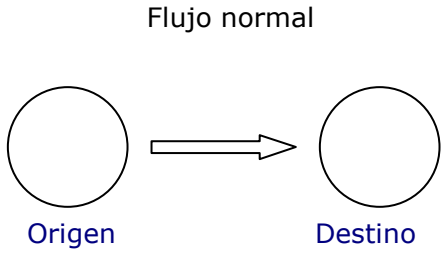


Figura 5.4 Diagrama del flujo normal de la información

1. Interrupción, es decir un recurso del sistema es destruido, interrumpido o se vuelve no disponible, amenaza que ataca la disponibilidad ver Figura 5.5.

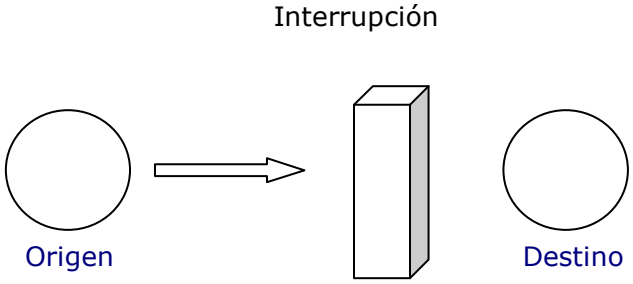


Figura 5.5 Diagrama de la amenaza de interrupción

2. Intercepción, una identidad no autorizada logra acceder a un recurso y ver o tomar la información, amenaza que ataca la confiabilidad ver Figura 5.6.

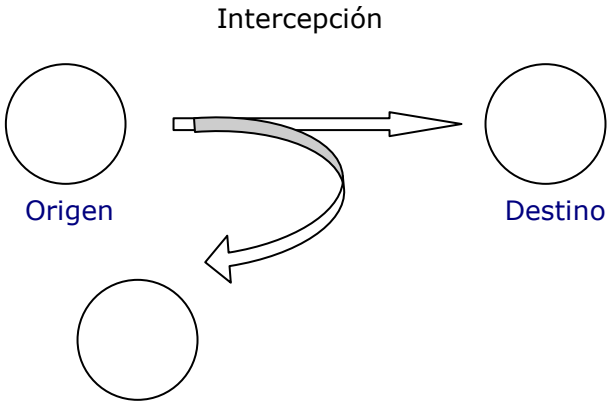


Figura 5.6 Diagrama de la amenaza de intercepción

3. Modificación, es cuando una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipular la información, amenaza que ataca la integridad ver Figura 5.7.

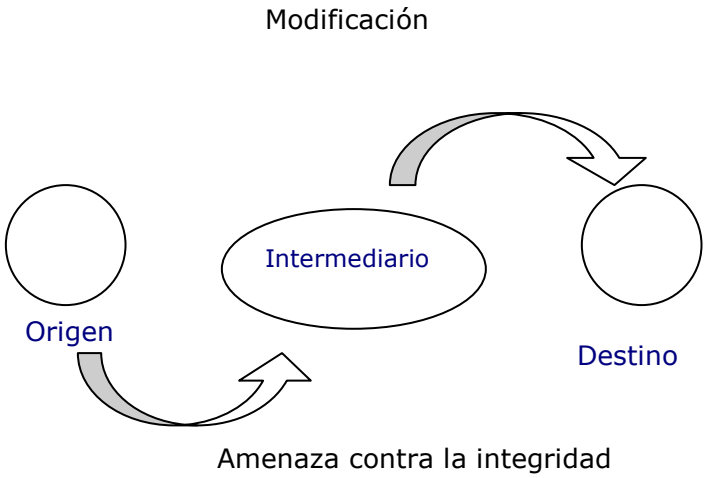


Figura 5.7 Diagrama de la amenaza de modificación

4. Suplantación, es cuando una entidad no autorizada inserta información falsa en el sistema, amenaza que ataca la autenticidad ver Figura 5.8.

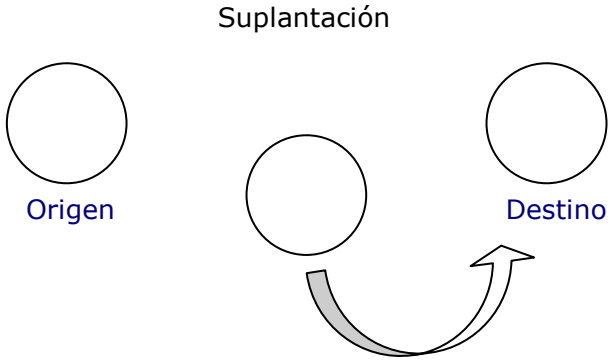


Figura 5.8 Diagrama de la amenaza de suplantación

C. Tipos de ataques

Como ya mencionamos anteriormente el ataque es la actuación de la amenaza; pero ¿por qué elementos se lleva a cabo?, esto se lleva a cabo ya sea por motivación, por capacidad o por oportunidad.

A diferencia de lo que muchos creen, el mayor número de ataques en las diferentes redes se llevan a cabo por personas de la misma organización: administradores resentidos, vengativos o por empleados y en menor porcentaje, pero no por eso menos peligrosos, son aquellos ataques realizados por curiosidad o para probar sus capacidades.

Las etapas de un ataque son: la preparación, la activación y la ejecución. Es posible definir dos tipos de ataques:

1. Pasivo, debido a que el atacante no altera la información, es decir, no nos percatamos de lo que está pasando. Cualquier ataque pasivo tiene los siguientes objetivos:
   a. Intercepción de datos, consiste en el conocimiento de la información cuando existe una liberación de los contenidos del mensaje.
   b. Análisis del tráfico, consiste en la observación de todo el tráfico que pasa por la red.
2. Activo, debido a que implican algún tipo de modificación del flujo de los datos transmitidos o la creación de un falso flujo de datos; siempre nos damos cuenta de lo que está pasando. Entre las principales actividades que caracterizan a este ataque encontramos:
   a. Enmascaramiento o suplantación de identidad, en este caso el intruso se hace pasar por una entidad diferente.
   b. Réplica o reactuación, uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado debido a que se realiza una retransmisión subsecuente.

c. Modificación de mensajes, una porción del mensaje legítimo es alterado, o los mismos mensajes son retardados o reordenados, esto provoca un efecto no autorizado.

d. Degradación fraudulenta del servicio, este tipo de acción impide o inhibe el uso normal o la administración de recursos informáticos y de comunicaciones.

5.1.4 Políticas de seguridad en redes

Para lograr un efectivo control sobre todos los componentes que conforman la red y asegurar que su conectividad a otras no sea frágil, es necesario establecer con exactitud qué recursos de la red y servicios se desean proteger de manera que se esté preparado para conectar la red con el resto del mundo. Esto implica el estudio y definición de los aspectos necesarios para la planeación de la seguridad de la red, análisis de riesgos, identificación de recursos, amenazas, uso de la red, responsabilidades, planes de acción y contingencia.

Una política de seguridad es un conjunto de leyes, reglas y prácticas que regulan cómo una organización maneja, protege y distribuye información sensitiva. Este documento se convierte en el primer paso para construir barreras de protección efectivas.

Por medio de las políticas de seguridad será posible definir los derechos y obligaciones del personal, además de establecer las sanciones que se aplicarán en caso de que éstas no sean respetadas.

A. Elementos de una política de seguridad

¿Qué debe contener una política de seguridad?, a continuación se definen algunos de los puntos que deben ser considerados en el diseño de una política de seguridad:

a. Explicaciones, es importante que la política sea explícita y comprensible por que es la base para tomar ciertas decisiones.

b. Las responsabilidades de todos, una política establece expectativas y responsabilidades entre el administrador de red, los usuarios y la gerencia; permite a todos saber qué esperar el uno del otro.

c. Lenguaje común, es importante hacer una política comprensible y precisa.

d. Autoridad para la aplicación, cuando no se sigue la política se debe hacer algo para solucionarlo. Alguien debe ser responsable de que esas soluciones ocurran, la política debe especificar quien será esa persona y el rango general de sanciones.

   La política debe especificar quién va a decidir y dar indicaciones sobre la clase de sanciones que se pueden imponer. No debe especificar con exactitud qué pasará cuando algo suceda; es una política, no una sentencia obligatoria de ley.

e. Previsión para revisiones, no se debe establecer una política una vez y olvidarse de ella para siempre. Las necesidades de una organización cambiarán con el tiempo y las políticas antes adecuadas pueden volverse demasiado estrictas o demasiado flexibles. Por tal motivo las políticas de seguridad se deben revisar y cambiar periódicamente.

f. Análisis de temas de seguridad específicos, los siguientes temas se deben considerar para escribir una política:

   - ¿A quién se le permite tener una cuenta en la red? ¿Existen cuentas para invitados? ¿Qué hacer con respecto a personal externo a la organización?

- ¿Pueden compartirse las cuentas entre varias personas? ¿Qué pasa si una secretaria usa la cuenta de un ejecutivo para procesar el correo electrónico de esa persona? ¿Qué hay de los proyectos en común? ¿Qué hay de los miembros de la familia? ¿Se comparte una cuenta, si se permite que alguien tome prestada por un momento una ventana en su máquina?
- ¿Cuándo pierde la gente el derecho de tener una cuenta, qué hacer al respecto? ¿Qué pasa si la gente se va o se le niega el acceso?
- ¿Quién puede instalar módems para entrar a la red? ¿Es correcto que otras personas instalen módems para hacer llamadas externas? ¿Hay algo especial acerca de las líneas PPP, SLIP, ISDN?
- ¿Qué debe hacer la gente antes de conectar una computadora a la red principal?
- ¿Qué tan seguras deben ser las computadoras antes de obtener servicios de máquinas, que se mantienen en forma centralizada?
- ¿Qué tan seguras deben ser las computadoras para conectarse a una red sin protección con acceso a Internet?
- ¿Cómo se protegerá la información financiera?
- ¿Cómo se protegerá la información confidencial sobre la gente?
- ¿Qué tienen que hacer los usuarios para protegerse a sí mismos y a la red? ¿Qué clase de contraseñas deben tener y cuándo deben cambiarlas?
- ¿Qué puede hacer la gente en Internet? ¿Pueden transferir archivos ejecutables al azar y ejecutarlos?
- ¿Qué precauciones se debe tomar contra los virus de las computadoras personales?
- ¿Quién puede conectar su sitio con redes externas y qué es una red externa? ¿Es correcto que un administrador de proyecto conecte su sitio a otro sitio específico? ¿Qué pasa si establece una segunda conexión a Internet?
- ¿Cómo se van asegurar las computadoras caseras? ¿Cómo van a tener acceso seguro a su red?
- ¿Qué información de la organización se considera confidencial? ¿Cómo será protegida? ¿Puede enviarse información fuera del sitio por medio del correo electrónico?
- Si tiene sitios remotos, ¿cómo se va a asegurar el acceso hacia su red principal?

Algunos aspectos que no debe contener una política de seguridad se detallan a continuación:

a. Detalles técnico, la política de seguridad debe describir qué intenta proteger y por qué, no debe describir detalles del cómo. Es mucho más útil tener un documento que describe "qué" y "por qué" en términos que todas las personas de la organización puedan entenderlo.

b. Los problemas de alguien más, la política de cada organización es diferente. Organizaciones distintas tienen preocupaciones distintas, apremios distintos, usuarios distintos y capacidades distintas; todo esto lleva a políticas distintas. Más aún, la política de una organización puede cambiar con el tiempo, conforme esta crece y cambia. No hay que dar por hecho que se deben de hacer las cosas como siempre se han hecho o que se pueden pedir prestadas las políticas de alguien más y simplemente cambiarle los nombres.

5.1.5 Mecanismos y herramientas de seguridad

Los mecanismos de seguridad son técnicas que se utilizan para implementar un servicio, es decir, están diseñados para detectar, prevenir o recobrarse de un ataque de seguridad debido a que implementan varios servicios básicos de seguridad o combinaciones de estos.

Los mecanismos básicos, pueden agruparse de varias formas para proporcionar varios servicios de seguridad, los cuales poseen tres componentes diferentes:

a. Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
b. Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado y generación de números aleatorios.
c. Un conjunto de procedimientos, que definen como se usarán los algoritmos, quién envía qué, a quién y cuándo.

No existe un único mecanismo capaz de proveer todos los servicios, sin embargo, la mayoría de ellos hace uso de técnicas criptográficas basadas en el cifrado de la información. Los mecanismos pueden ser clasificados como preventivos, detectivos y recuperables.

A. Tipos de mecanismos de seguridad

Los mecanismos de seguridad pueden clasificarse en dos categorías:

1. Mecanismos de seguridad generalizados, se relacionan con los niveles y manejo de seguridad requeridos. Se aplican a los sistemas para cumplir la política general de seguridad de la organización, ver Tabla No. 5.2.

	Mecanismos
a.	Funcionalidad de confianza
b.	Etiquetas de seguridad
c.	Detección de eventos
d.	Rastreo de auditoría de seguridad
e.	Recuperación de seguridad

Tabla No. 5.2 Mecanismos de seguridad generalizados

A continuación se explican cada uno de ellos:

a. Funcionalidad de confianza, se puede utilizar bien para extender los otros mecanismos de seguridad o para establecer su efectividad. Cualquier tipo de funcionalidad que proporcione directamente mecanismos de seguridad o el acceso a los mismos debe ser de confianza.
b. Etiquetas de seguridad, están asociados a los recursos del sistema. A menudo es necesario que los datos de tránsito lleven una etiqueta de seguridad apropiada. Un nivel de seguridad puede implicar datos adicionales que se asocian a los datos transmitidos o puede ser implícito.
c. Detección de eventos, relevante para la seguridad se utiliza para detectar violaciones aparentes de la seguridad.
d. Seguimiento de auditorías de seguridad, que consiste en la revisión y examen independiente de los registros y las actividades del sistema para probar la

operatividad de los controles, asegurar el cumplimiento de las políticas y procedimientos operacionales establecidos y recomendar los cambios adecuados en el control, políticas y procedimientos.

e. Recuperación de seguridad, trata con solicitudes de mecanismos como administradores de eventos y funciones de administración, realiza acciones de recuperación resultado de la aplicación de una serie de reglas.

2. Mecanismos de seguridad específicos, los mecanismos de seguridad específicos, definen la implementación de los servicios concretos, ver Tabla No. 5.3.

	Mecanismos
a.	Cifrado
b.	Firma digital
c.	Control de acceso
d.	Integridad de los datos
e.	Intercambio de autenticación
f.	Tráfico de relleno
g.	Control de encaminamiento
h.	Certificación

Tabla No. 5.3 Mecanismos de seguridad específicos

A continuación se explican cada uno de ellos:

a. Cifrado, se utiliza para proteger la confidencialidad de las unidades de los datos y la información del flujo de tráfico o para dar soporte y complementar otros mecanismos de seguridad.

b. Firma digital, se utiliza para proporcionar una analogía electrónica a la firma manuscrita en documentos electrónicos. La firma digital se puede definir como un conjunto de datos (como códigos o claves criptográficas privadas) que se añaden a una unidad de datos de modo que protejan a ésta contra cualquier falsificación, permitiendo al receptor comprobar el origen y la integridad de los datos. Para ello se cifra la unidad de datos junto con algún componente secreto del firmante y se obtiene un valor de control ligado al resultado cifrado.

c. Control de acceso, se utiliza para autenticar las capacidades de una entidad para acceder a un recurso dado, se puede llevar a cabo en el origen o en un punto intermedio y se encarga de asegurar que el emisor está autorizado a comunicarse con el receptor o a usar los recursos de comunicación, soporta el servicio de control de acceso y está ligado a la autenticación y confianza.

d. Integridad de datos, asegura que los datos no sean alterados o destruidos. Este mecanismo trata con la integridad de una unidad o campo de datos simples y la integridad de una secuencia de unidades o campos de datos.

e. Intercambio de autenticación, se utiliza para verificar la supuesta identidad de los usuarios. En la ITU X.509 (ITU, 1987) se dice que un mecanismo de intercambio de autenticación es fuerte si se basa en el uso de técnicas criptográficas para proteger los mensajes que se van a intercambiar.

f. Tráfico de relleno, se utiliza para la protección contra ataques de análisis de tráfico. Mediante la generación de ejercicios de comunicación no autenticada, unidades de datos y datos ilegítimos. El objetivo no es revelar si los datos que se están transmitiendo representan y codifican realmente información. En

consecuencia estos mecanismos únicamente serán efectivos si son protegidos por un servicio de confidencialidad de datos.

g. Control de ruteo, se puede utilizar para la selección dinámica o preestablecida de rutas específicas para la transmisión de los datos. Los sistemas de comunicaciones que detectan de forma persistente ataques activos o pasivos, pueden indicar al proveedor de servicio de la red, que desean establecer una conexión por una ruta diferente.

h. Certificación, se puede emplear para asegurarse de ciertas propiedades de los datos que se comunican entre dos o más entidades, como su integridad, origen, tiempo o destino. La certificación la realiza una tercera entidad de confianza, que es la que da testimonio de la autenticidad.

5.2 Monitoreo de la red

Definimos monitoreo, al proceso continuo de recolección y análisis de datos cualitativos y cuantitativos, con base en los objetivos planteados en las políticas de seguridad. El objetivo del monitoreo es descubrir las fortalezas y/o debilidades para establecer líneas de acción, permitiendo brindar correcciones y reorientaciones en las técnicas de ejecución. Entre las principales actividades que se incluyen dentro del monitoreo de las redes, se encuentran las dedicadas al desarrollo de tareas de supervisión, capaces de controlar resultados de operaciones diversas, así como programas que permitan la observación de variables seleccionadas.

Existen dos razones primordiales para monitorear la red:

1. Predecir los cambios para el crecimiento futuro apoyado en un historial de comportamiento de la red.
2. Detectar los cambios inesperados en el estado de la red.

La detección oportuna de fallas y la predicción de cambios son actividades que permiten proporcionar un buen servicio a los usuarios. De ahí la importancia de contar con un esquema capaz de notificarnos las fallas en la red, a través de su comportamiento.

5.2.1 Enfoques del monitoreo de la red

Existen dos enfoques principales para abordar el proceso de monitoreo, aunque diferentes son complementarios.

A. Enfoque activo

El monitoreo con enfoque activo, se realiza inyectando paquetes de prueba en la red o enviando paquetes a determinadas aplicaciones, midiendo sus tiempos de respuesta; éste es empleado para medir fundamentalmente el desempeño de la red.

Entre las principales técnicas de monitoreo activo encontramos:

a. Basadas en ICMP, el protocolo ICMP permite diagnosticar problemas en la red, detectando retardos, pérdidas de paquetes, así como la disponibilidad de hosts y redes.

b. Basadas en TCP, permiten el análisis de la tasa de transferencia, así como el diagnóstico de problemas a nivel aplicación.

c. Basadas en UCP, son herramientas que analizan el RTT, Tiempo Aproximado de Viaje (Round Trip Times) esto es, el tiempo que tarda un bit en desplazarse desde un extremo a otro del medio y nuevamente en regresar, además de los paquetes perdidos en un sentido.

B. Enfoque pasivo

Se basa en la obtención de datos a partir de la recolección y análisis del tráfico que circula por la red, para lo cual se emplean diferentes herramientas como lo son sniffers, routers, computadoras con software de análisis de tráfico, además de dispositivos que soporten protocolos de administración como SNMP, RMON, etc. Este enfoque no agrega tráfico a la red como lo hace el enfoque activo, es utilizado para caracterizar el tráfico en la red y para contabilizar su uso.

Entre las principales técnicas de monitoreo pasivo encontramos:

1. Solicitudes remotas, esta técnica se realiza a través de SNMP o bien mediante otros métodos de acceso. SNMP, obtiene estadísticas sobre el uso del ancho de banda en los dispositivos de red, para lo cual requiere el acceso a ellos, de la misma manera genera paquetes denominados traps que indican que un evento inusual se ha presentado. Otros métodos incluyen acceso a dispositivos mediante scripts realizados en perl u otro lenguaje, cuyo objetivo es obtener información del dispositivo a monitorear.
2. Captura de tráfico, esta técnica se puede implementar a través de dos formas: mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura o bien mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. La técnica de captura de tráfico es empleada para contabilizar el tráfico que circula por la red.
3. Análisis de tráfico y flujos, técnica empleada para caracterizar el tráfico de la red, esto es identificar el tipo de aplicaciones que son más utilizadas. Se implementa haciendo uso de agentes que envían información mediante RMON o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por diferentes criterios: aplicación, direcciones IP origen y destino, puertos origen y destino, etc.

   El objetivo es la identificación del tipo de tráfico de la red, considerando que un flujo es un conjunto de paquetes con las siguientes características:

   - Misma dirección IP origen y destino.
   - Mismo puerto TCP origen y destino.
   - Mismo tipo de aplicación.

   Los flujos se pueden obtener a través de routers o mediante dispositivos capaces de capturar tráfico y transformarlo en flujos. Regularmente esta técnica es empleada para tareas de facturación.

5.2.2 División del área de monitoreo de la red

El proceso de monitoreo de una red, puede a su vez ser dividido en los siguientes subprocesos:

a. Monitoreo de la conexión, una de las formas básicas de monitorear la conexión es a través del inicio de sesión que los usuarios realizan para conectarse a la red. Existen programas sencillos que son herramientas prácticas para el administrador, de manera que pueda realizar ping constantes a los diferentes elementos de la red y detectar fallos.

b. Monitoreo del tráfico, es un método sofisticado para controlar el estado de la red, busca el flujo de paquetes en la red y genera informes basados en dicho estado. Programas como Microsoft Windows Network Monitor, Ethereal y Agilent constituyen ejemplos de herramientas que analizan el tráfico en una red. El software analizador de tráfico, no sólo detecta fallos, si no que determina si un componente está sobrecargado con una configuración deficiente, su desventaja radica en que normalmente funcionan en un segmento de la red.

c. Monitoreo remoto, se realiza mediante sondas que recogen información y la trasladan a una consola central. Existe una sonda en cada uno de los segmentos de la red monitoriada que pueden ser host dedicados, dispositivos de red, etc.

   Las principales consolas de administración remota proporcionan dos ventajas en los procesos de red:

   1. La capacidad de que haya más de un administrador de la red, en diferentes ubicaciones físicas monitoreando y administrando la misma red.
   2. La redundancia de tener dos o más consolas de administración significa que si una consola falla, la otra podrá seguir usándose para monitorear la red.

d. Monitoreo de aplicaciones, supervisa la operación de las aplicaciones para controlar el adecuado uso de licencias, además de determinar el número de clientes que acceden simultáneamente a una aplicación utilizando opciones de bloqueo.

5.2.3 Esquemas de monitoreo

Para establecer un esquema de monitoreo, existe un modelo que permite identificar los elementos necesarios, para obtener las cifras que proporcionan información acerca del rendimiento de la red, además de verificar si se encuentra de acuerdo a los requerimientos. Este modelo identifica el proceso de determinación de métricas:

1. Formulación de métricas de servicio, esta etapa se divide a su vez, en cuatro fases, que se muestran en la Figura 5.9.

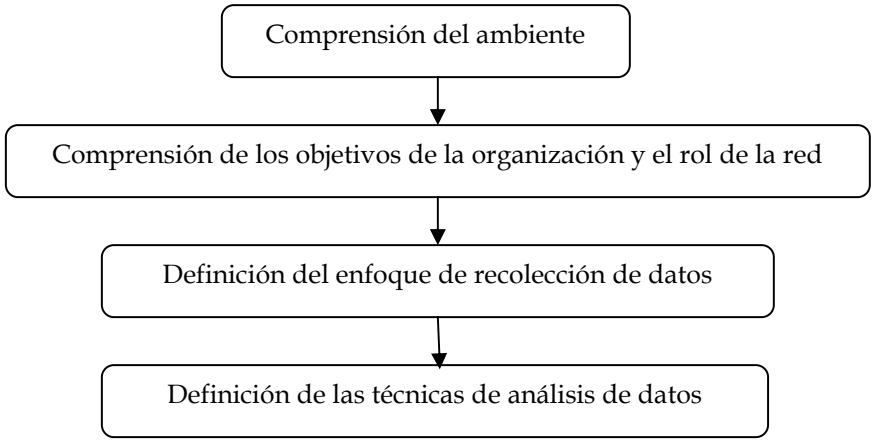


Figura 5.9 Fases del monitoreo de una red

a. Comprensión del ambiente, es la etapa de descubrimiento, donde el objetivo es el conocimiento del estado actual de la red, no requiere de métricas e incluye entrevistas a usuarios, análisis de planes de adquisición relacionados con servidores o redes y el análisis de diagramas de red.

b. Comprensión de los objetivos de la organización y el rol de la red, esta fase implica la definición de la estrategia para la administración de la red, mediante la formulación de lineamientos de tecnologías recomendadas y clasificación de proveedores.

c. Definición del enfoque de recolección de datos, esta etapa desarrolla una estrategia, para reunir los datos de acuerdo a los lineamientos establecidos, bajo la definición de tres criterios claves: ¿cuándo y dónde es deseable reunir la información de la red? y ¿qué información se debe reunir? A su vez suele dividirse en 4 fases mostradas en la Figura 5.10.

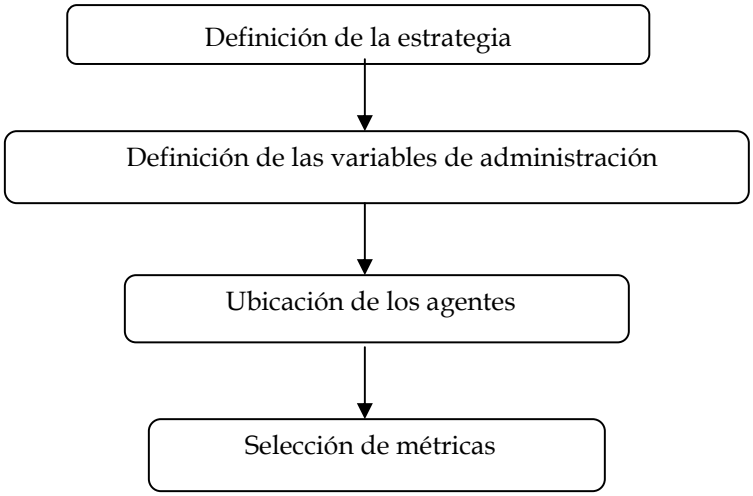


Figura 5.10 Fases de la recolección de datos

c.1 Definición de estrategias, se refiere a las diversas alternativas para la recolección de datos, entre las que resaltan:

- Periodos pico, la planificación se efectúa con base al peor rendimiento ubicando el peor caso, cuando exista un problema de red, durante un periodo pico. Su desventaja recae en la complejidad de obtener un conjunto amplio de datos que representan un estado de la red.
- Periodos pico y no pico, incluye información tanto en periodos pico como no pico, de manera que es representativa del uso de la red. Obtiene una mejor imagen acerca de los patrones de red.

c.2 Definición de variables de administración, la definición de tales variables, requiere de una delimitación y depende de las diferentes aplicaciones, por ejemplo en un servidor Web, será necesario monitorear el tiempo que no está en funcionamiento, tiempo requerido para mantenimiento, tipos de acceso, etc. La Tabla No. 5.4, presenta algunos ejemplos de variables de monitoreo.

Variables de monitoreo
Utilización de ancho de banda
Consumo de CPU
Consumo de memoria
Estado físico de las conexiones
Tipo de tráfico
Alarmas
Tiempo de funcionamiento
Porcentaje de utilización
Memoria de caché existente
Número de conexiones activas
Bloqueo de registros
Estado de transacciones
Situación de discos
Número de archivos abiertos
Tipos de paquetes enviados

Tabla No. 5.4 Variables de monitoreo

Los dispositivos a ser monitoreados pueden ser divididos en tres grupos:

i. Dispositivos de interconexión, abarcan elementos de red activos como routers, switches, firewall, hubs, host, etc.

ii. Servidores, en este grupo se encuentran los servidores de correo, servidores de Web, servidores de bases de datos, etc.

iii. Red de administración, ubicamos en este rubro a los equipos de monitoreo, logs y de configuración.

c.3 Ubicación de los agentes, este paso incluye la determinación del lugar donde serán ubicados los agentes de monitoreo para reunir los datos sobre las variables de monitoreo, para lo cual existen dos alternativas:

i. Agentes residentes, dispositivos físicos que se encuentran en la red y que cuentan con mecanismos de recolección de datos, por ejemplo: switches, routers, hub, etc.

ii. Agentes dedicados, equipos dedicados cuya única función en la red, es recolectar datos.

c.4 Selección de métricas, posteriormente a la identificación de las variables de monitoreo y a la ubicación de agentes, es necesario delimitar cómo se va a medir, esto a través del uso de métricas. La definición de métricas permite establecer patrones de comportamiento para los dispositivos que serán monitoreados. Existen diferentes tipos de métricas de acuerdo a los elementos a monitorear y en la siguiente lista se describen las principales:

- Métricas de tráfico de entrada y salida.
- Métricas de empleo de procesador y memoria.
- Métricas de estado de interfases.
- Métricas de conexiones lógicas.
- Métricas de retardo.
- Métricas de aplicaciones específicas.

A cada una de las métricas, se les asigna un valor promedio el cual identifica su patrón de comportamiento. Para facilitar la selección de las métricas a emplear se deben agrupar en un conjunto las alternativas para recolectar datos que provean información común.

Establecido qué se va a monitorear y cómo se va a medir, se requieren de mecanismos que permitan estar atentos al comportamiento de la red. El siguiente paso es la definición de alarmas. Las alarmas son consideradas como eventos con comportamiento inusual, existen diferentes tipos y las más comunes son aquéllas que reportan, cuando el estado operacional de un dispositivo o servicio cambia. Los otros tipos de alarmas se basan en patrones previamente definidos en las métricas, a estos valores máximos se les conoce como umbrales (threshold). Cuando estos patrones son superados se producen alarmas, pues se considera un comportamiento fuera del patrón. Entre las principales alarmas encontramos:

- Alarmas de procesamiento.
- Alarmas de conectividad.
- Alarmas ambientales.
- Alarmas de utilización.
- Alarmas de disponibilidad.

d. Definición de las técnicas de análisis de datos.

5.2.4 Análisis del desempeño de la red bajo diferentes condiciones

A. Número de estaciones

Los elementos fundamentales de una red son la topología, los medios de transmisión, la disposición de los equipos y la técnica de control de acceso al medio. En su conjunto determinan el costo, la capacidad de la red, además del tipo de datos que serán transmitidos, la velocidad y la eficiencia de las comunicaciones e incluso la clase de las aplicaciones que soportará la red.

El conjunto de nodos que comparten un medio físico forman un dominio de colisión, ya que sus tramas son susceptibles de colisionar entre sí. Al aumentar el número de estaciones que pertenecen al mismo dominio de colisión aumenta la congestión de la red, debido a que el ancho de banda es compartido entre todas. Por ejemplo: el protocolo CSMA/CD, se degrada demasiado al aumentar el número de estaciones.

Algunas soluciones a la degradación provocada por dominios de colisión grandes son:

- Aumento de la velocidad de transmisión, sin embargo esta acción puede crear repercusiones en el tipo de señalización o el tamaño de la trama.
- Segmentar la red, mejorando el rendimiento de la red.

Para realizar un análisis del rendimiento de una red, debemos considerar las diferentes topologías que se tienen, para analizar la manera que afecta el número de estaciones, al ancho de banda de la red. La Tabla No. 5.5 muestra una valoración cualitativa de las diversas topologías. Para un mayor detalle de cada uno de ellas es posible consultar el Anexo 5.E.

Topología	Estrella	Bus	Árbol	Anillo
Complejidad	Baja	Baja	Media	Alta
Vulnerabilidad	Alta	Alta	Media	Alta
Administración de averías	Buena	Limitada	Media	Buena
Capacidad de expansión	Alta	Alta	Alta	Alta
Costo	Alto	Bajo	Bajo	Alto

Tabla No. 5.5 Valoración cualitativa de topologías

La elección del medio de transmisión se determina por una serie de factores restringidos por la topología, además de las siguientes consideraciones:

- Capacidad, debe soportar el tráfico de red esperado.
- Fiabilidad, satisfaciendo los requisitos de disponibilidad.
- Tipos de datos soportados, ajustados a la aplicación.
- Alcance del entorno, proporcionando un servicio a la gama de entornos requeridos.

Una topología en bus se implementa la mayoría de las veces con un cable coaxial en banda base, para el caso de los sistemas ethernet. Una topología en estrella puede ser instalada con fibra óptica o bien cable de par trenzado, siendo más complicado trabajarlo con cable coaxial. Una topología en estrella se aprovecha de la disposición natural del cableado de los edificios, esto generalmente resulta mejor para distancias cortas y puede ofrecer velocidades elevadas a un número pequeño de dispositivos.

La Tabla No. 5.6 presenta una valoración cualitativa de las características de diversos cables.

Tipo de cable	Ancho de banda	Longitud	Fiabilidad de la resistencia	Seguridad	Complejidad de la instalación	Costo
Par Trenzado	Moderado	Pequeña	Moderado	Baja	Sencilla	Bajo
Coaxial	Grande	Moderada	Alta	Moderada	Moderada	Moderado
Fibra óptica	Muy grande	Muy alta	Muy Alta	Alta	Complejo	Alto

Tabla No. 5.6 Valoración cualitativa de los medios de transmisión

B. Intensidad de tráfico

El monitoreo del tráfico de red en términos de volumen, es empleado para estudios de capacidad, planeación y rendimiento. En ocasiones es imprescindible para entender el tipo de tráfico que fluye a través de la red de comunicaciones, en el caso de que se produzcan inesperados incrementos en el tráfico. El analizar el flujo de paquetes, conforme al protocolo por ejemplo IP, ARP, RARP, IPX permite hacer comparaciones con análisis anteriores y definir las causas de los congestionamientos.

El analizador de tráfico observa dentro de los paquetes ethernet y los desenvuelve para analizar el tipo de protocolo que circula por la red, permitiendo mostrar la utilización que se está haciendo del ancho de banda, entre las direcciones origen y destino del protocolo. Para mayor control es posible la definición de perfiles que son monitoreados de forma independiente con diferentes valores de umbrales para la administración de alarmas. En la Figura 5.11, se tiene una vista de un analizador comercial que presenta una serie de estadísticas con respecto a los protocolos ICMP, UDP y TCP.

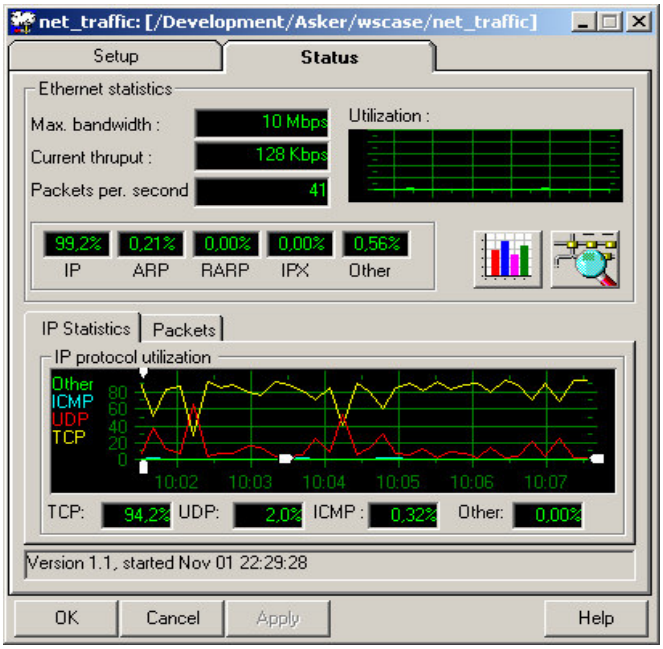


Figura 5.11 Estadísticas proporcionadas por un analizador de tráfico

a. Funcionamiento de un analizador de tráfico, el analizador de tráfico, captura los paquetes de datos que viajan por una red, para posteriormente decodificar el protocolo y generar estadísticas.

b. Ventajas de los analizadores de tráfico, el analizador de tráfico, se vuelve una utilidad imprescindible para el diagnóstico, resolución de problemas de red y su optimización, debido a que proporcionan una visión definida de la actividad de la red, mostrando con precisión los cuellos de botellas, malas configuraciones de protocolos, entre otros detalles.

   El administrador de redes emplea la información reunida por los analizadores de tráfico para efectuar un análisis de las operaciones de base y tendencias de manera que el rendimiento pueda ser optimizado.

c. Aplicaciones de los analizadores de tráfico, es posible determinar el ancho de banda de la red, que está utilizando un usuario o una aplicación, por ejemplo si se observa

que el host del usuario genera una cantidad desproporcionada de tráfico http, se puede concluir que está gastando mucho tiempo explorando la Web.

Algunos analizadores de tráfico además de capturar paquetes, los generan para simular condiciones de tráfico a niveles precisos, verificando el nivel operacional de la red o bien para probar la carga de un equipo.

d. Software analizador de tráfico, los analizadores de tráfico se diferencian entre sí por su soporte a los diversos protocolos, para decodificar de forma correcta los paquetes. Por ejemplo puede admitir soporte ethernet y probablemente Token Ring en el nivel de enlace de datos, pero si una red utiliza FDDI o ATM, se requerirá de un analizador más complejo y costoso.

Actualmente encontramos varias opciones de software libre que analizan el tráfico de una red:

a. Ntop, analizador de tráfico de red, de uso extendido en las plataformas Linux, que informa del uso de la red de manera similar al comando top de UNIX, diseñado por Luca Deri de la Universidad de Pisa, se basa en el programa pcapture, ver Figura 5.12.

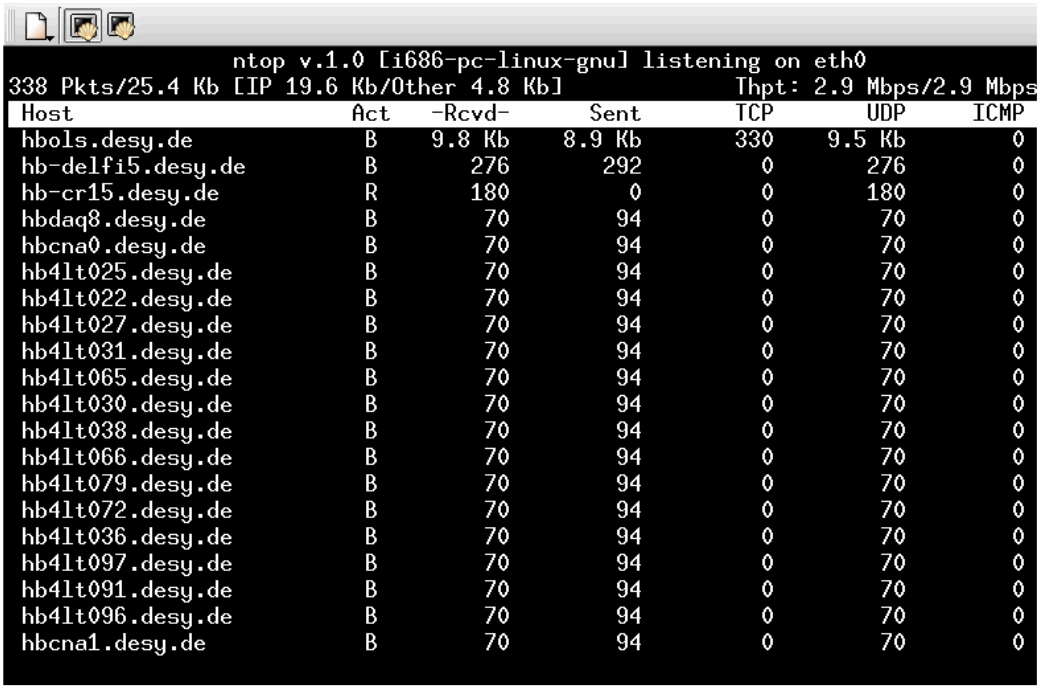


Figura 5.12 Analizador de tráfico Ntop

El software Ntop se ejecuta en dos modos diferentes:

- Modo interactivo, que permite que los resultados del programa se muestren en tiempo real en una ventana de terminal.
- Soporte Web, permite que la salida del programa sea supervisada por múltiples usuarios locales o remotos mediante un explorador Web.

C. Análisis de paquetes

El análisis de paquetes se realiza por medio de los analizadores de red, también denominados analizadores de protocolos, rastreadores, husmeadores de paquetes o sniffers, siendo una herramienta que permite capturar el tráfico que viaja por la red, dando

oportunidad de analizar sus propiedades, decodificar y mostrar el contenido de los paquetes. Para cada paquete el software muestra la información encontrada en cada campo de cada cabecera de protocolo, así como los datos de aplicación originales que van en la carga útil del paquete.

Los analizadores de paquetes, proporcionan estadísticas sobre el tráfico que circula por la red, así como el número de paquetes que usan un protocolo determinado y la cantidad de tráfico originado por cada sistema en la red, siendo de vital importancia en el proceso de aprendizaje del comportamiento de los protocolos.

a. Funcionamiento de un analizador de paquetes

El analizador de paquetes funciona conmutando la tarjeta de red de un equipo, configurada en modo promiscuo. La tarjeta examina las direcciones destino de la cabecera del protocolo en el nivel de enlace de datos de cada paquete que llega al equipo y si el paquete no va dirigido a ese equipo, lo descarta, evitando que el CPU tenga que analizar miles de paquetes extraños, cuando la tarjeta se configura en modo promiscuo, acepta todos los paquetes que llegan a la red, sin importar la dirección y los dirige al software analizador de red, para ser procesados, permitiendo al sistema analizar no sólo el tráfico generado si no también el intercambiado por los otros sistemas de red. Una vez que la aplicación captura el tráfico de la red, almacena los paquetes completos en un buffer al que se puede acceder durante la etapa de análisis.

Es posible aplicar filtros para limitar los tipos de datos que captura el analizador de red, controlando el flujo de la información. La mayoría de los analizadores de red cuenta con dos tipos de filtros:

1. Filtros de captura, limita los paquetes que el analizador guarda en el buffer.
2. Filtros de muestra, limita los paquetes capturados que se muestran en pantalla.

Existen diversas formas de aplicar los filtros, por ejemplo:

1. Si se desea monitorear el comportamiento de un host, se crea un filtro que capture únicamente paquetes generados por esa máquina.
2. Si se requiere monitorear el comportamiento de un determinado protocolo, se diseña un filtro con las características de análisis de un mismo protocolo.
3. Monitorear el comportamiento de determinados paquetes que incluyan ciertos caracteres ASCII o hexadecimales.

Si se combinan las anteriores posibilidades utilizando operadores booleanos como AND y OR, se tienen filtros muy específicos que presentan la información requerida.

b. Ventajas de los analizadores de paquetes

El análisis de paquetes es imprescindible para un administrador de red, cuando su fin es el monitoreo, sin embargo también puede ser utilizado por personal no autorizado que puede provocar daños.

5.2.5 Elección de las herramientas de monitoreo

Existen un sin número de herramientas para realizar el monitoreo de la red, tanto comerciales como de software libre. La elección depende de factores humanos, económicos

y de infraestructura (perfil de conocimiento de los administradores, recursos económicos y equipo de cómputo disponible).

Entre las principales herramientas podemos describir brevemente algunas de ellas.

A. Agilent

Solución para el monitoreo de redes, emplea herramientas de base de datos para almacenar la información de los dispositivos y aprovechar sus funcionalidades de graficación, proporcionando un esquema de obtención rápido de datos remotos, manejo de plantillas avanzadas, ofrece servicio de alarmas mediante manejo de umbrales; todo por medio de una consola de administración fácil de configurar, ver Figura 5.13.

Figura 5.13 Analizador de tráfico Agilent

B. NetSNMP

Conjunto de aplicaciones cuyo objetivo es obtener información vía SNMP, de los equipos de interconexión, provee de manejo de traps para la notificación de eventos y soporta la versión 3 de SNMP que incluye mecanismos de seguridad como confidencialidad y autenticación.

C. Nagios

Aplicación para el monitoreo de servicios, host, etc., que pertenecen a una red, muestra el estado operacional de todos los servicios y hosts en un ambiente Web, envía notificaciones mediante correo electrónico cuando el estado operacional cambia.

D. TcpView

Programa en Windows que muestra detalladamente los puertos TCP y UDP del sistema que están habilitados. Provee de un subconjunto de herramientas similares al netstat. Cuando inicia TCPView, numera todos los puertos activos TCP y UDP, resolviendo su dirección a nombres de dominio.

5.3 Manejo de accesos: listas de acceso y herramientas de seguridad

Los administradores de redes, deben ser capaces de denegar el acceso no deseado a la red, a la vez que permitir el acceso sí deseado. Aunque las herramientas de seguridad (como contraseñas, equipos callback y dispositivos físicos de seguridad) son útiles, a menudo carecen de la flexibilidad del filtrado básico del tráfico y de los controles específicos que prefieren la mayoría de los administradores. Por ejemplo, un administrador de redes puede permitir que los usuarios accedan a Internet, pero impedir que los usuarios externos hagan telnet dentro de la red.

Los routers proporcionan capacidades básicas de filtrado, como el bloqueo de tráfico de Internet, mediante las ACL, Listas de Control de Acceso (Access Control List). Una ACL es una colección secuencial de condiciones de sentencias de permisos o denegación, que se aplican a direcciones o a los protocolos de la capa superior. Estas condiciones de las listas de acceso, se utilizan para implementar las reglas de filtración de paquetes.
Es importante configurar correctamente las ACL y saber donde colocarlas dentro de la red. Las ACL sirven para muchas tareas, entre sus funciones más básicas están: el filtrado

interno de los paquetes, la protección de la red interna del acceso de Internet ilegal y la restricción del acceso a los puertos del terminal virtual.

5.3.1 Panorámica de las ACL

Las ACL son listas de instrucciones que se aplican a la interfaz del router. Estas listas le indican qué tipo de paquetes aceptar y cuáles denegar. La aceptación y la denegación se basa en ciertas especificaciones, como la dirección de origen, la dirección destino y el número de puerto.

Al aplicar la ACL a una interfaz del router es posible administrar el tráfico y revisar los paquetes. Todo tráfico que pasa por la interfaz se compara con ciertas condiciones de las ACL. Es posible crear listas de acceso, para todos los protocolos de red enrutados, con el objetivo de filtrar los paquetes que pasan por el router, para controlar el acceso a la red o a la subred.

5.3.2 Razones para crear ACL

Hay muchas razones para crear listas de acceso. Por ejemplo, se pueden utilizar para lo siguiente:

- Limitar el tráfico de la red e incrementar su rendimiento.
- Controlar el flujo de tráfico.
- Proporcionar un nivel básico de seguridad para el acceso a la red.
- Decidir que tipo de tráfico es enviado o bloqueado en la interfaz del router.

5.3.3 Tipos de listas de acceso

El número utilizado para identificar una lista concreta debe ser seleccionado de un rango numérico acorde con el uso concreto de la lista. En la Tabla No. 5.7 vemos los principales tipos de listas disponibles. En este apartado nos centraremos especialmente en las listas IP, en sus formas estándar y extendida.

Protocolo	Tipo	Rango	Filtra por
IP	Estándar	1-99 y 1300-1999	el origen
IP	Extendidas	100-199 y 2000-2699	el origen, destino, protocolo, puerto.
Ethernet	Código (Type)	200-299	el tipo de código ethernet
DECnet	Protocol Suite	300-399	el origen
Appletalk	Protocol Suite	600-699	el origen
Ethernet	Direcciones	700-799	la dirección MAC
IPX	Estándar	800-899	el origen
IPX	Extendida	900-999	el origen, destino, protocolo, puerto
IPX	SAP	1000-1099	tipo de aplicación (SAP, Service Access Point)

Tabla No. 5.7 Tipos de listas de acceso y sus rangos numéricos

Los routers Cisco tienen tres tipos de listas de acceso:

- Listas de acceso estándar, que tienen una sola dirección origen de los paquetes para las operaciones coincidentes.
- Listas de acceso extendida, permiten filtrar el tráfico en función del origen, destino, protocolo, puerto y otros parámetros. Utiliza dos direcciones con información opcional

del tipo de protocolo para las operaciones coincidentes. Permiten filtrar el tráfico de interfaz con base en las direcciones IP de origen y la información del protocolo.

- Listas de acceso con nombre, permiten identificar los filtros utilizados de una forma más descriptiva, terminan con la limitación artificial que imponen los rangos numéricos y ofrece nuevas posibilidades de configuración, como el filtrado dinámico, también permite eliminar entradas concretas sin la necesidad de borrarlas por completo y volver a configurar (aunque no podrá cambiar el orden de la lista).

5.3.4 Especificación de condiciones

Las condiciones de las listas de acceso permiten identificar las direcciones de origen y destino de los paquetes. Junto con las direcciones se especifican máscaras que permiten identificar la parte de la dirección que debe coincidir exactamente y la parte que puede ser ignorada.

Las máscaras de las listas de acceso son distintas a las máscaras de red y subred utilizadas para configurar interfases o rutas estáticas. Concretamente los ceros de las máscaras significan que el bit correspondiente de la dirección es relevante, mientras que los unos significan que el bit correspondiente de la dirección no debe ser tomando en cuenta a la hora de decidir si la condición se cumple. A las máscaras de las listas de acceso se les denomina wildcard mask o máscaras comodín.

Por ejemplo, la dirección IP 10.10.10.0 con una máscara de lista de acceso semejante a 0.0.0.255, ver Tabla No. 5.8, al pasar a binario la dirección y la máscara podemos ver qué parte de la dirección será tenida en cuenta a la hora de determinar si un paquete concreto cumple la condición.

	Decimal	Binario
Dirección	10.10.10.0	00001010.00001010.00001010.00000000
Máscara	0.0.0.255	00000000.00000000.00000000.11111111

Tabla No. 5.8 Direcciones y máscaras comodín

Esta condición selecciona las direcciones que comprenden desde la 10.10.10.0 hasta la 10.10.10.255 o dicho de otra forma las direcciones de la forma 10.10.10.x. Por ejemplo la dirección 10.10.9.7 no cumple la condición (el tercer byte de la dirección es distinto en la dirección y en la condición, este tercer byte es relevante, tal como indica los ceros de la máscara para este tercer octeto) pero la dirección 10.10.10.254 si cumple las condiciones especificadas por la condición del ejemplo.

La máscara inversa de las listas de acceso, también puede ser determinada sustrayendo la máscara normal de la máscara 255.255.255.255. En el ejemplo, la máscara comodín para la red 10.10.10.255 con una máscara normal 255.255.255.0 sería 255.255.255.255 - 255.255.255.0 (normal) = 0.0.0.255 (inversa, comodín).

5.4 Auditoría informática

El cómputo es una herramienta clave dentro de la administración integral de una organización. A finales del siglo XX, los sistemas de tecnologías se conformaron como elementos claves dentro de las organizaciones, ya que respaldan la toma de decisiones, generando un alto grado de dependencia, así como una elevada inversión en ellas. Debido a su importancia, existe la auditoría informática.

Con frecuencia el término auditoría es incorrectamente empleado como sinónimo de detección de errores y fallas, perdiendo su objetivo central: la evaluación continúa de la eficacia y eficiencia de una organización.

Los sistemas de tecnología de información deben ser sometidos a controles de calidad, ya que las computadoras y centros de procesamiento de datos, son blancos de espionaje, terrorismo y delincuencia.

5.4.1 Objetivos

La auditoría informática se considera como un proceso continuo y evolutivo, que a través de técnicas y procedimientos aplicados en una organización por personal independiente a la operación de la misma, evalúa la función de la tecnología de la información y su aportación al cumplimiento de los objetivos de la organización, para mejorar el nivel de apoyo al cumplimiento.

Entre las principales funciones de la auditoría informática encontramos:

- Vigilar y evaluar a través de dictámenes.
- Evaluar costos, seguridad, riesgos informáticos, etc.
- Operar bajo el plan auditor.
- Utilizar metodologías de evaluación del tipo cualitativo con la característica de las pruebas de auditoría.
- Establecer planes como ciclos completos.

5.4.2 Beneficios

Entre los principales beneficios de la auditoría informática, encontramos:

- Mejoramiento de la imagen pública.
- Generar confianza en los usuarios en cuestiones relacionadas con la seguridad y control de servicios de TI.
- Optimizar las relaciones internas y el clima de trabajo.
- Disminuye costos debido a los reprocesos, rechazos, reclamos, etc.
- Realiza un control de la inversión en un entorno de TI.
- Genera un balance de los riesgos de TI.
- Mejora la capacidad de toma de decisiones, haciendo éstas más rápidas y de menor riesgo, al contar con información precisa.
- Mejora la calidad de los servicios debido al incremento de la capacidad de adaptación dinámica del mercado.

5.4.3 Áreas de la auditoría informática

Existen diferentes áreas de la auditoría informática, las cuales se muestran en la siguiente lista:

- Auditoría física.
- Auditoría de seguridad.
- Auditoría de desarrollo.

- Auditoría de mantenimiento.
- Auditoría de explotación.
- Auditoría ofimática.
- Auditoría de calidad.
- Auditoría de redes.
- Auditoría de dirección.

5.4.4 Metodología

Las fases que incluyen a la auditoría informática son similares a la auditoría tradicional y se compone de las siguientes etapas:

1. Planeación, etapa cuyo propósito es entender y obtener los procesos de negocio, incluye la concentración de objetivos, la delimitación del área que cubrirá, las personas de la organización que se involucrarán en el proceso de auditoría, el establecimiento del plan de trabajo.

   El plan de trabajo debe incluir los siguientes puntos: definición de tareas, calendario de actividades, resultados parciales, presupuesto, equipo auditor necesario, etc.

2. Desarrollo de la auditoría, requiere la realización de entrevistas, cuestionarios, observaciones de las situaciones y procedimientos deficientes.
3. Análisis y evaluación, su objetivo es determinar la probable efectividad y eficiencia del control interno. También es conocida como la etapa de diagnóstico, pues implica la meditación sin contacto con la organización auditada, considerando la experiencia del equipo auditor, para la definición de los puntos débiles y fuertes, así como los riesgos eventuales y tipos de solución.
4. Pruebas, existe una clasificación de las pruebas realizadas en:

   a. Pruebas de cumplimiento, aquellas realizadas para verificar la efectividad de los procedimientos de control.

   b. Pruebas sustantivas, aquellas que se implementan para verificar los procesos de trabajo.

5. Resultados, se informan los resultados de la auditoría, con el fin de reportar las sugerencias correspondientes a las mejoras encontradas, argumentando y documentando de forma suficiente, para evitar que sean rechazadas. El desarrollo del plan de mejoras debe incluir un resumen de las deficiencias encontradas, recogiendo las recomendaciones encaminadas a resolver esos puntos débiles, mediante medidas a corto plazo (mejoras en plazo, calidad, planificación o formación), medidas a medio plazo (mayor necesidad de recursos, optimización de programas, documentación y aspectos de diseño) y medidas a largo plazo (cambios en políticas, medios y estructuras del servicio).
6. Seguimiento, realizado para evaluar el nivel de cumplimiento e impacto en las recomendaciones hechas.

5.4.5 Criterios

Es preciso supervisar continuamente los controles internos informáticos, para asegurarse de que el sistema funciona de acuerdo a lo planeado, considerando factores de cambio externos e internos.

A. Controles en la informática distribuida y redes

Las políticas y procedimientos de control en informática, son los elementos que al ser ejecutados de manera formal y oportuna garantizan que las funciones y servicios relacionados con la informática, se lleven a cabo con eficiencia para el apoyo estratégico, táctico y operativo que requiere la organización.

Tanto las políticas como procedimientos de control mínimos, que deben existir en el área de redes, se describen en la Tabla No. 5.1 del Anexo 5.A, las cuales sirven como referencia al auditor, adecuando dichas listas a las condiciones particulares de la organización.

B. Requisitos para la auditoría informática

- Debe seguir una metodología preestablecida.
- Se realizará en una fecha precisa y fija.
- Será personal extraño al servicio de la informática, quien la realizará.

5.4.6 Planeación de la auditoría: propósito y alcance

El personal encargado de realizar la auditoría informática, debe generar un plan que justifique su trabajo, durante cierto periodo. Cada proyecto de auditoría, respalda los objetivos y tiene un alcance que satisface a tres áreas principalmente:

1. Alta dirección, mediante la verificación y aseguramiento del cumplimiento de políticas inherentes a la TI.
2. Auditoría, apoya la definición, implantación y seguimiento de políticas, controles y procedimientos de auditoría, colaborando en la elaboración de planes de capacitación.
3. Informática, define, implanta y da seguimiento a las políticas, controles, procedimientos y estándares relativos a la administración de la informática, la evaluación y adquisición de nuevas tecnologías y servicios.

Los siguientes puntos definen las características claves de todo plan de auditoría que aseguran un apoyo eficiente y permanente.

- Creación de un comité de control y seguimiento integrado por la alta dirección y responsables directos de la auditoría.
- Análisis de proyectos de negocios, de informática y auditoría, de manera conjunta que permitan obtener el impacto que tienen entre sí.
- Establecer fechas de reuniones formales e informales para dar seguimiento a los planes de compromiso conjunto.
- El plan de auditoría informática, suele ser subdivido en 4 procesos de planeación:

  1. Proceso de planeación de negocios.
  2. Proceso de planeación de informática.
  3. Proceso de planeación de auditoría.
  4. Proceso de planeación de auditoría informática.

  Cada uno de los puntos anteriores se describe en el Anexo 5.B.

5.4.7 Seguimiento y reportes

El reporte de auditoría informática, es el medio formal para comunicar y establecer el alcance, objetivos, periodo de cobertura y extensión del trabajo de auditoría realizado, identificando la organización, las necesidades de las partes interesadas y cualquier restricción acerca de su distribución, además de incluir resultados, conclusiones y recomendaciones.

Existen normas que definen el contenido y formato del reporte, las cuales consideran que el estilo del reporte debe ser el apropiado para las partes interesadas y puede estar en forma escrita, oral o electrónica. Un reporte escrito debe identificar la organización auditada e incluir un título, una firma y una fecha, siendo objetivo, claro, conciso, constructivo y oportuno.

A continuación se explican brevemente los elementos que integran un reporte de auditoría informática:

1. Identificación del informe, el título del informe deberá resaltarse con objeto de distinguirlo de otros informes.
2. Identificación del cliente, deberá identificarse a los destinatarios y a las personas que efectúen el encargo.
3. Identificación de la entidad informática auditada.
4. Establecimiento de objetivos, el reporte debe incluir una especificación de los objetivos de la auditoría para identificar las razones de su realización. Si, en la opinión del auditor, algún objetivo de auditoría establecido en el reporte no fue satisfecho, éste debe notificarse en el reporte, además de una declaración del alcance de la auditoría que describa la naturaleza, el tiempo y extensión del trabajo realizado. La declaración del alcance debe identificar el área funcional de auditoría, el periodo de auditoría cubierto, los sistemas de información, aplicaciones o ambiente de auditoría revisado, de igual forma debe identificar las circunstancias de la limitación del alcance cuando, las pruebas y los procedimientos apropiados para conocer las normas no han sido suficientes o cuando las restricciones en el trabajo de auditoría han sido impuestas por el auditado.
5. Restricciones en la distribución, el reporte identifica al auditado e indica la fecha de emisión de éste, declarando cualquier restricción que haya para su distribución.
6. Normativa aplicada y excepciones, identificación de las normas legales y profesionales utilizadas, así como las excepciones significativas de uso y el posible impacto en los resultados de la auditoría.
7. Alcance de la auditoría, concretar la naturaleza y extensión del trabajo realizado, identificando el área organizativa, el periodo, etc.
8. Hallazgos reportados, el documento describe un hallazgo significativo mediante aclaraciones de las condiciones, causas y efectos del estado además del criterio organizacional, profesional y gubernamental empleado para su identificación. Resalta los estándares organizacionales, profesionales y/o gubernamentales o los códigos utilizados, por ejemplo: estándares ISACA, para la auditoría de sistemas de información, etc.
9. Conclusiones, informe corto de opinión, el reporte expresa una conclusión considerada como la evaluación del auditor del área que está siendo auditada, siendo éste quien detalle los objetivos específicos de auditoría, las recomendaciones para acciones correctivas, etc. El informe debe contener uno de los siguientes tipos de opinión:

a. Opinión favorable, ésta es considerada sin salvedades o limpia y es el resultado del trabajo realizado sin limitaciones de alcance y sin incertidumbre, con base en la normativa legal y profesional.

b. Opinión con salvedades, incluye el reiterar la opinión favorable al respecto de las salvedades cuando sean significativas, en relación con los objetivos de la auditoría, describiéndose con precisión la naturaleza y razones de las mismas.

c. Opinión desfavorable, se aplica en el caso de identificación de irregularidades, incumplimiento de la normativa legal y profesional que afecten significativamente a los objetivos de auditoría informática.

d. Opinión denegada, esta acción puede tener su origen en las limitaciones al alcance de la auditoría, incertidumbres significativas de un modo tal que impidan al auditor formarse una opinión, irregularidades o incumplimiento de normativas legales y profesionales.

10. Actividades de seguimiento, implica la descripción de requerimientos de una respuesta, considerando las acciones.

11. Fecha del informe, el tiempo es un elemento indispensable para conocer la magnitud del trabajo y aplicaciones. Conviene precisar las fechas de inicio y conclusión del trabajo de campo, el cierre de ejercicio, se realiza un informe de auditoria informática como herramienta de apoyo a la auditoría de cuentas.

12. Identificación y firma del auditor, la identificación resulta un elemento esencial, tanto si es individual como si forma parte de una sociedad de auditoría.

5.4.8 Auditoría de redes

La auditoría en redes pretende asegurar una función formal de la administración de la red, a través de la existencia de procedimientos y controles, que permitan detectar el grado de confianza, satisfacción y desempeño que brindan a la organización. Para lo anterior, se requieren de parámetros de medición del desempeño de la red (gráficas, estadísticas, etc.), evaluación de controles y otros.

Entre las principales actividades que se realizan para auditar esta área encontramos:

1. Comparación de proyectos con la planeación de la auditoría.
2. Concertar citas con el personal que debe ser entrevistado.
3. Revisión del formulario correspondiente, así como su actualización de acuerdo a las necesidades de la organización.
4. Efectuar las entrevistas y visitas necesarias.
5. Elaboración de un borrador con conclusiones y recomendaciones principales.
6. Clasificación y almacenado de la información de soporte en dispositivos de almacenamiento seguro.
7. Elaboración formal de conclusiones y recomendaciones finales.

A menudo la auditoría de redes, se divide en el análisis de 3 módulos:

1. Administración, en la Tabla No. 5.6 del Anexo 5.C, se detallan las principales funciones que se realizan durante la primera etapa de la auditoría de redes.
2. Instalación, las siguientes son algunas de las preguntas que pueden servir como referencia para aplicar una auditoría en el área de redes.

- ¿Existen procedimientos que aseguren la oportuna y adecuada instalación de componentes que conforman la red?
- ¿Existen formatos que permitan identificar las actividades que se llevan a cabo?
- ¿Existe la documentación necesaria para cuando se instalan los componentes de la red (hardware, software, procedimientos, etc.)?
- ¿Existen procedimientos definidos para la compra de software que asegura su adquisición legal?
- ¿Existe un responsable de las actividades de seguridad y control para garantizar el uso adecuado y protección de software?

3. Operación y seguridad, durante esta etapa de la auditoría de la red es necesario verificar la existencia de:
   - Manuales de operación de la red, que contemplen aspectos de seguridad.
   - Personal responsable de administrar la red.
   - Capacitación del personal para realizar actividades de administración de operación y seguridad.
   - Estándares de desempeño que involucran parámetros de tiempos de respuesta, tráfico (volúmenes de información, velocidad), interrupciones, tiempo de recuperación de la red, equipos interconectados.

5.4.9 Estándares de la auditoría informática

Existe un estándar internacional conocido como COBIT, Objetivos de Control para la Información y Tecnología Relacionada (Control Objectives for Information and Related Technology) este sirve como guía para la buena práctica de la auditoría informática y contempla procesos típicos agrupados en 4 dominios:

1. Planificación y organización.
2. Adquisición e implementación.
3. Distribución y soporte.
4. Monitoreo.

Los procesos requieren ser evaluados de manera continua para verificar su calidad y su eficiencia en cuanto a requerimientos de control, para una mayor descripción de cada una de las etapas anteriores se puede acudir al Anexo 5.D.

5.5 Plan de contingencias informático

La reanudación de la actividad de un desastre puede ser una de las actuaciones más desafiantes con las que un administrador de redes profesional debe enfrentarse.

No existe ninguna manera para proteger completamente los datos y los sistemas contra todo tipo de amenazas ambientales a gran escala, que puedan arrasar edificios enteros; es prudente reflexionar sobre lo que sucedería en el caso de que tal desastre se presentará y la organización se encuentre sin ningún tipo de acceso a la red del lugar de trabajo. Por lo tanto, el plan de contingencia es el proceso de determinar qué hacer si la catástrofe se abate sobre la organización, siendo necesario recuperar la red y los sistemas.

Uno de los problemas asociados al plan de contingencia para redes, es saber por dónde empezar. Establecer un proceso de comunicaciones después de un desastre, requiere práctica y análisis para tener aptitudes y poder realizarlo con un alto nivel de experiencia.

Probablemente, llevó años diseñar y construir la actual red, de repente, será necesario reconstruirla en unos días. Esto requerirá toda la pericia disponible para que sea un éxito.

El objetivo del proceso de generar un plan de contingencia, es producir un documento denominado Plan de Contingencia, el cual proporciona la cohesión que permite al grupo de recuperación, actuar como un equipo, al adjuntar a cada miembro una lista concreta de responsabilidades y procedimientos a seguir.

Un plan de contingencia debe contar con las siguientes características:

1. Un plan debe ser práctico, un plan difícil de ejecutarse de forma rutinaria terminaría dejando de hacerse de forma rutinaria. Un plan que no es práctico es peor que no tenerlo. Es necesario realizar un plan que se adapte a la forma en la que trabaja realmente la gente y no la forma como debería de trabajar.
2. Un plan debe ser examinado de forma constante, analizando las estrategias, las amenazas y su eficacia. Al menos deben revisarse dos veces al año con la dirección de la organización.
3. Un plan debe ser probado, es indispensable verificarlo para encontrar errores y depurarlos.

5.5.1 Disponibilidad de los datos

La preparación ante un desastre comienza asegurándose que se tienen los datos a recuperar. La realización de copias de seguridad fiables debería ser un requisito previo del plan de contingencia, de no ser así, se está malgastando el tiempo pensado que es posible recuperar algo, por lo tanto no se considera en el plan. Estas son algunas de las cosas que se deben hacer antes de que ocurra un desastre:

- Realizar copias de seguridad todos los días y verificar su finalización.
- Almacenar y renovar regularmente los medios de almacenamiento de copias de seguridad en una localización externa, para asegurar la recuperación en el caso de un desastre en la instalación principal, esto nos cerciora la disponibilidad del acceso a los datos en una emergencia.
- Familiarizarse con la recuperación de datos a través del sistema de copias de seguridad, es decir, sería mucho mejor conocer de antemano las limitaciones del sistema de copias de seguridad que encontrarlas cuando ya es demasiado tarde.

5.5.2 Metodología para el plan de contingencia

Una vez controlado los aspectos de las copias de seguridad y almacenamiento de datos, es el momento de reflexionar sobre lo que se necesitará cuando suceda un desastre. Existe una metodología general que puede emplearse para formalizar el proceso dentro de la organización.

A. Análisis de riesgos

En esta fase, la preocupación está relacionada con tres simples preguntas:

1. ¿Qué está bajo riesgo?

Para responder a esta cuestión, se necesita incorporar todos los componentes de la red susceptibles a ser dañados, dando lugar a la pérdida de conexiones, computadoras o datos. Un diagrama de la arquitectura de todos los componentes del sistema de red, facilitará la realización de un inventario de los elementos que pueden necesitar ser sustituidos tras un

desastre. No hay que olvidar que también el software necesita ser reemplazado y que todos los productos del software relevantes han de ser identificados.

Uno de los aspectos menos agradables a tener en cuenta y que a menudo se pasa por alto, es que las personas esenciales se vean afectadas por el desastre y sea necesario recurrir a otras para realizar sus labores. Una formación diversificada en los sistemas dentro de la organización, puede ayudar a reducir el impacto de la indisponibilidad de uno de los colaboradores. Al menos, los manuales de aplicaciones más importantes para la organización, deberán encontrarse disponibles en una localización externa.

2. ¿Qué puede ir mal?

La respuesta a tal cuestión varía desde lo evidente hasta lo imposible. Las clases más obvias de los desastres, son los desastres naturales que conllevan tormentas de todo tipo a los acontecimientos geológicos como terremotos o volcanes. Las inundaciones pueden ocurrir en casi cualquier lugar; los incendios constituyen uno de los peores desastres posibles y no debemos pasar por alto los ataques terroristas y otros actos deliberados de destrucción, cometidos por personas que pueden devastar sistemas e instalaciones. Consideraremos todos los ataques que puedan amenazar la red.

3. ¿Cuál es la probabilidad de que suceda?

Para responder a esta cuestión, se requiere de ciertas consideraciones presupuestarias. Ello puede ayudar a asumir distintos escenarios de presupuesto, para comprender cuales son los costos de compromiso para diferentes niveles de protección y preparación. Se puede estar expuesto a ciertas amenazas cuya protección no está al alcance del presupuesto, pero, al menos, sé es consciente de su existencia y por lo tanto, es posible mejorar el plan en un futuro.

B. Valoración de los riesgos

La valoración de los riesgos es el proceso de determinar el costo para la organización, de experimentar un desastre que afecte a su actividad. La preocupación principal es comprender la cantidad de pérdida financiera que puede provocar la interrupción de los servicios de red.

Los costos de un desastre pueden clasificarse de la siguiente forma:

- Costos reales de reemplazar el equipo informático.
- Costos de producción.
- Costos por negocio perdido.
- Costos de reputación.

C. Asignación de prioridades a las aplicaciones

Después de que acontezca el desastre y se inicie la recuperación de los sistemas, deben conocerse las aplicaciones a recuperar en primer lugar. Esto implica la necesidad de determinar por anticipado cuáles son las aplicaciones fundamentales de la organización.

Es indispensable que la dirección ayude a determinar el orden en que los sistemas serán recuperados. Es de esperar que esa información sea aceptada de buen agrado por todos los jefes de las diferentes áreas. Independientemente de ello, el plan de contingencia debería

incluir la lista de los sistemas y su prioridad. Esta sección del plan deberá estar firmada por la dirección para minimizar los desacuerdos.

Una vez conocido lo que se va a restaurar, deberá disponerse de todo lo necesario para la disponibilidad de tales aplicaciones. Un sistema de aplicación en una red está compuesta por los sistemas de servidores, donde las aplicaciones almacenan los datos; de los sistemas de estaciones de trabajo que los procesan; las impresoras o fax empleados para E/S; la red que interconecta todo y el software de las aplicaciones.

D. Establecimiento de los requerimientos de recuperación

La clave de este proceso es definir un periodo de tiempo aceptable y viable para lograr que la red esté de nuevo activa. Es muy importante conceder una cantidad de tiempo adecuada y no realizar estimaciones poco realistas sobre las propias posibilidades. El término para este tiempo es RTO, Tiempo de Recuperación Objetivo (Recovery Time Objetive). EL RTO definido debe ser verificado para comprobar que es realista y factible, no sólo por uno mismo, sino por el resto de la organización, que puede ser requerido para realizar el trabajo.

La dirección de la organización debería colaborar íntimamente con el personal de la administración de la red para determinar el RTO de las aplicaciones. Aplicaciones diferentes tendrán RTO diferentes.

Es necesario asegurarse de que se dispone de tiempo para recuperar los medios de almacenamiento, localizados en la instalación de almacenamiento exterior y para adquirir los sistemas necesarios. Deberá conocerse por anticipado cómo realizar las órdenes de compra de los equipos cuando la organización se encuentra en un estado de total desorganización.

E. Elaboración de la documentación

Crear un documento que mucha gente pueda tener como referencia es la cruz del plan de contingencia. Implicará un esfuerzo significativo para algunas personas, pero ayudará a aprender cosas sobre el sistema y puede que algún día salve a la organización. La documentación requiere que se tomen en cuenta los siguientes aspectos:

a. El compromiso de la dirección, que debe apoyar la iniciativa para que sea un éxito. Uno de los problemas del plan de contingencia en un entorno de comunicaciones, es que la tecnología de redes cambia tan rápidamente que resulta difícil permanecer al día.
b. Contenido del plan de contingencia, el cual debe contemplar las cinco áreas siguientes:
    1. Listas de notificación, números de teléfonos, mapas y direcciones.
    2. Prioridades, responsabilidades, relaciones y procedimientos.
    3. Información sobre adquisiciones y compras.
    4. Diagramas de red.
    5. Sistemas, configuraciones y copias de seguridad.

F. Verificación e implementación del plan

Una vez redactado el plan, hay que probarlo, pues hay que estar seguros de que funcionará. Para ello, se debe ser escéptico sobre el propio trabajo, de manera que pueda uno probarse a sí mismo que funciona.

Han de efectuarse las pruebas para encontrar problemas y subsanarlos antes de que el plan de contingencia tenga que entrar en operación. Si existen errores en la información, tomar nota de ellos y corregir el plan. Es recomendable hacer la comprobación del plan por partes.

G. Distribución y mantenimiento del plan

Por último, cuando se disponga de un plan definitivo ya verificado, es de vital importancia distribuirlo a las personas que necesitan tenerlo, además de contar con un control de las versiones del plan, de manera que no exista confusión con múltiples versiones. También es necesario asegurar la disponibilidad de copias extra del plan, para depósito en la instalación exterior o en cualquier otro lugar de trabajo.

El mantenimiento del plan es un proceso sencillo. Se comienza con una revisión del plan existente y se examina en su totalidad, realizando cambios a cualquier información que pueda haber variado. En ese instante, se debe volver a evaluar los sistemas de aplicación y determinar cuales son los más importantes para la organización. Las modificaciones a esta parte del plan causarán modificaciones consecutivas a los procedimientos de recuperación.

Un buen plan de contingencia comienza con el compromiso de la dirección general, aceptando el hecho de que se trata de un proceso continuo.

MANUAL DE PRÁCTICAS

MANUAL DE PRÁCTICAS

De acuerdo al temario de la asignatura de Administración de Redes, se llevo a cabo un análisis con respecto a las horas que se tienen contempladas para cada uno de los temas, éste se ve reflejado en el diagrama al final de esta sección.

Para el primer capítulo, *Planeación*, cuyo objetivo es conocer e identificar los elementos que conforman una red de datos, así como las políticas y ética que rigen sobre el cómputo, se tienen contempladas 7.5 horas en la teoría al semestre, conforme a lo anterior se han propuesto tres prácticas:

- Práctica 1, Configuración básica de redes.

  Objetivos de aprendizaje:

  - El alumno conocerá e identificará elementos que conforman una red de datos, así como las políticas y ética que rigen sobre el cómputo.
  - El alumno adquirirá la capacidad del manejo de los comandos adecuados para la configuración del hardware, protocolos y software asociado a las redes locales de computadoras en los sistemas operativos Linux y Windows.

- Práctica 2A, Manejo de dispositivos de interconectividad, hub y switch.

  Objetivos de aprendizaje:

  - El alumno conocerá, profundizará en el conocimiento e identificará los elementos que conforman una red de datos, además de investigar las políticas y ética que las rigen.
  - El alumno desarrollará las habilidades necesarias que le permitan la manipulación de equipos de interconexión como lo son los hubs y switches.
  - El alumno analizará el comportamiento de valores cuantitativos de una red, como lo son: el retardo, el número de colisiones, etc., mediante herramientas de simulación de redes como OPNET IT GURU Academic.

- Práctica 2B, Manejo de dispositivos de interconectividad, router.

  Objetivos de aprendizaje:

  - El alumno desarrollará las habilidades necesarias que le permitan la manipulación de equipos de interconexión de capa de red, como lo son los routers.
  - El alumno analizará el comportamiento de las tablas de ruteo estáticas, dentro de una red de área local, mediante una herramienta de simulación de redes: RouterSim CCNA v3.0 de Cisco.

Para el segundo capítulo, *Organización,* cuyo objetivo es aplicar los modelos de administración de redes para su óptimo desempeño, se tienen contempladas 10.5 horas en la teoría al semestre y se han propuesto tres prácticas:

- Práctica 3, Administración con SNMP.

  Objetivos de aprendizaje:

  - El alumno analizará y explorará el significado y utilidad de los diferentes objetos de la MIB-II, consultando los valores a un agente SNMP con ayuda del software MG-SOFT MIB Browser.

- El alumno aprenderá a través de la interfaz de línea de comando, a configurar el protocolo de mantenimiento SNMP, en routers Cisco.
- El alumno aprenderá a crear una ACL, Lista de Control de Acceso (Access Control List) sencilla para configurar el protocolo de mantenimiento SNMP.

- Práctica 4, Modelado de procesos de negocio con eTOM.

  Objetivos de aprendizaje:

  - El alumno adquirirá los conocimientos básicos de la metodología de procesos de negocios eTOM, como fundamento para la administración de una organización proveedora de TI.
  - El alumno aprenderá a diseñar un modelo de proceso de negocio y ejecutará una simulación del mismo, empleando un software de modelado denominado Savvivon Process Modeler.

- Práctica 5, Introducción a la programación CORBA.

  Objetivos de aprendizaje:

  - El alumno conocerá e identificará los elementos que constituyen la programación de redes distribuidas.
  - El alumno construirá una aplicación sencilla con CORBA, de manera que se familiarice con los pasos básicos necesarios para construir una aplicación y desarrolle la habilidad de explicar el código fuente.

Para el tercer capítulo, *Integración*, cuyo objetivo es conocer las tecnologías actuales e integrar soluciones para el adecuado funcionamiento de las redes que se están implantando, se tienen contempladas 10.5 horas en la teoría al semestre y se han propuesto cuatro prácticas:

- Práctica 6, Configuración de VoIP.

  Objetivos de aprendizaje:

  - El alumno adquirirá los conocimientos básicos acerca de VoIP, como medio de comunicación, así como lo protocolos de señalización y transmisión para poder llevar a cabo una llamada telefónica por medio de redes IP.
  - El alumno aprenderá a configurar un conmutador de VoIP, empleando el software Asterisk para el PBX y X-lite Softphone, para establecer una llamada VoIP.

- Práctica 7A, Comunicaciones inalámbricas, red tipo infraestructura.

  Objetivos de aprendizaje:

  - El alumno aprenderá a configurar una red inalámbrica tipo infraestructura vía Web.
  - El alumno adquirirá la habilidad, para habilitar en el access point un sistema de filtrado basado en MAC (a veces llamado también filtrado por hardware), que únicamente permita el acceso a la red a tarjetas de red concretas, identificadas por su MAC.

- Práctica 7B, Comunicaciones inalámbricas, servidor DHCP.

  Objetivos de aprendizaje:

  - El alumno analizará las características y los elementos que conforman un servidor DHCP.

  - El alumno instalará y configurará los parámetros de un servidor DHCP, en una computadora con sistema operativo Linux.

- Práctica 8, Videoconferencia.

  Objetivos de aprendizaje:

  - El alumno examinará los estándares y elementos que conforman un sistema de videoconferencia.
  - El alumno conocerá y aprenderá como se lleva a cabo una videoconferencia en la sala de Videoconferencia del Centro de Docencia de la Facultad de Ingeniería de la UNAM.

Para el cuarto capítulo, *Dirección*, cuyo objetivo es conocer e identificar el perfil y las habilidades que deberá poseer un directivo de las tecnologías de las telecomunicaciones, se tienen contempladas 4.5 horas en la teoría al semestre y se ha propuesto una práctica:

- Práctica 9, Manejo de conflictos.

  Objetivos de aprendizaje:

  - El alumno definirá el concepto de conflicto, identificando las razones que lo provocan y la forma en que las personas lo manejan. De la misma manera reconocerá técnicas para la evasión y resolución de conflictos.
  - El alumno adquirirá la habilidad para aplicar estrategias de supervisión que minimicen el conflicto y mejoren las relaciones humanas que favorecen el buen funcionamiento del área.
  - El alumno realizará un análisis comparativo entre dos tipos de liderazgos, resaltando características, ventajas y desventajas.

Para el quinto capítulo, cuyo objetivo es conocer, identificar y aplicar técnicas que le permitan diseñar, implantar y manejar de forma adecuada la red diseñada, a fin de medir y obtener los resultados del desempeño esperados, de acuerdo a los objetivos planteados desde la planeación, se tienen contempladas 15 horas en teoría, por lo cual se han propuesto cuatro prácticas:

- Práctica 10A, Mecanismos de seguridad, firma digital.

  Objetivos de aprendizaje:

  - El alumno se familiarizará con herramientas básicas relacionadas con la seguridad en la red, las cuales podrán ser estudiadas a profundidad en subsecuentes asignaturas.
  - El alumno será capaz de realizar una aplicación que permita el proceso de firmado de un documento a través de la infraestructura de claves asimétricas, en el lenguaje orientado a objetos, Java.

- Práctica 10B, Mecanismos de seguridad, certificados digitales.

  Objetivos de aprendizaje:

  - El alumno identificará los diversos tipos de certificados, así como su importancia dentro de los esquemas de seguridad en las redes.
  - El alumno se familiarizará con una herramienta de software libre que permite la administración de certificados digitales, OpenSSL.

- Práctica 10C, Mecanismos de seguridad, firewall.

Objetivos de aprendizaje:

- El alumno adquirirá las habilidades necesarias que le permitan implementar un mecanismo de seguridad específico, como el firewall.
- El alumno, analizará el comportamiento de una red bajo condiciones de seguridad específicas, de acuerdo a estadísticas obtenidas.

- Práctica 11, Monitoreo de la red.

  Objetivo de aprendizaje:

  - El alumno empleará una herramienta de análisis de protocolos, que le permita monitorear el comportamiento de la red del Laboratorio de Redes de Datos y Seguridad.
  - El alumno obtendrá reportes de diversos parámetros de la red, analizando los resultados y generando diagnósticos de comportamiento de la red.

El presente manual de prácticas, se encuentra contenido en el disco anexo a este trabajo.

DIAGRAMA DE GANT

Planeación de las prácticas del Laboratorio de Administración de Redes

	Tema 1	Tema 2	Tema 3	Tema 4	Tema 5
Horas	7.5	10.5	10.5	4.5	15

Semana del semestre	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Teórica Hrs. 48	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5	1.5 1.5
Avances	7.5															
			10.5													
							10.5									
											4.5					
												15				

Semanas del semestre	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Práctica Hrs 28*		2	2	2	2	2	2	2	2	2	2	2	2	2	2	
No. Semanas			1	2	3	4	5	6	7	8	9	10	11	12	13	
***Presentación**																
No. de práctica			1	2A	2B											
No. de práctica						3	4	5								
No. de práctica									6	7A	8					
No. de práctica												9				
No. de práctica													10A	10B	11	
Prácticas adicionales										7B				10C		

Nota: Nos referimos a los temas como capítulos en la tesis.

Práctica 1	**Configuración Básica de Redes**
Práctica 2A	**Manejo de dispositivos de interconectividad, hub, switch**
Práctica 2B	**Manejo de dispositivos de interconectividad, routers**
Práctica 3	**Administración con SNMP**
Práctica 4	**Modelado de los procesos de negocios con eTOM**
Práctica 5	**Introducción a Corba**
Práctica 6	**Voz IP**
Practica 7A	**Comunicaciones Inalambricas, red tipo infraestructura**
Practica 7B	**Comunicaciones Inalambricas, servidor DHCP**
Práctica 8	**Videoconferencias**
Práctica 9	**Manejo de conflictos**
Práctica 10A	**Mecanismos de Seguridad Parte, Firma digital**
Práctica 10B	**Mecanismos de Seguridad Parte, Certificados digitales**
Práctica 10C	**Mecanismos de Seguridad Parte, Firewall**
Práctica 11	**Monitoreo de la Red**

CONCLUSIONES

CONCLUSIONES

Este proyecto de tesis nos ha permitido introducirnos en nuevos campos de conocimiento, desde las áreas administrativas y de psicología, hasta áreas especializadas como la seguridad en redes y las nuevas tecnologías de telecomunicaciones.

El objetivo primordial fue el desarrollo de un manual de prácticas para el Laboratorio de Administración de Redes, para lo cual realizamos una investigación teórica de los temas considerados en el temario aprobado para la nueva asignatura y que actualmente también forma parte del manual de prácticas.

Para llevar a cabo el objetivo y con base en el programa de la asignatura Administración de Redes, esta tesis está compuesta por cinco capítulos, a continuación se describen brevemente las prácticas propuestas.

Capítulo uno, *Planeación*, abarca los cimientos teóricos que un administrador de redes debe conocer para llevar a cabo la planeación de la red, identificando los elementos que la conforman, comprendiendo los objetivos del diseño, llevando a cabo el análisis de requerimientos de hardware y software, tomando en cuenta el direccionamiento lógico, así como elaborando las políticas de cómputo, con ética profesional.

Para este capítulo, cuyo objetivo es conocer e identificar los elementos que conforman una red de datos, así como las políticas y ética que rigen sobre el cómputo, se han propuesto tres prácticas:

- Práctica 1, Configuración básica de redes.
- Práctica 2A, Manejo de dispositivos de interconectividad, hub y switch.
- Práctica 2B, Manejo de dispositivos de interconectividad, routers.

Capítulo dos, *Organización*, se describen los modelos de administración de red: TMN, TOM y eTOM, que un administrador de redes puede aplicar a la red para obtener un óptimo desempeño; de la misma forma se presentan los protocolos de administración de red como SNMP, CMIP y CORBA.

Para este capítulo, cuyo objetivo es aplicar los modelos de administración de redes para su óptimo desempeño, se han propuesto tres prácticas:

- Práctica 3, Administración con SNMP.
- Práctica 4, Modelado de procesos de negocio con eTOM.
- Práctica 5, Introducción a la programación CORBA.

Capítulo tres, *Integración*, se presentan las tecnologías actuales que pueden ser aplicadas a las redes e integrar soluciones para su adecuado funcionamiento. Se analizan las tecnologías en telecomunicaciones, telefonía, comunicaciones inalámbricas, Internet2, videoconferencia y se estudia la metodología para la evaluación de proyectos de cómputo.

Para este capítulo, cuyo objetivo es conocer las tecnologías actuales e integrar soluciones para el adecuado funcionamiento de las redes que se están implantando, se han propuesto cuatro prácticas:

- Práctica 6, Configuración de VoIP.
- Práctica 7A, Comunicaciones inalámbricas, red tipo infraestructura.

- Práctica 7B, Comunicaciones inalámbricas, servidor DHCP.
- Práctica 8, Videoconferencia.

Capítulo cuatro, *Dirección*, se muestran las habilidades que debe poseer un directivo de las tecnologías de las telecomunicaciones, que le permitan manejar los conflictos que se presentan en la organización, con el fin de que los equipos sean más efectivos.

Para este capítulo, cuyo objetivo es conocer e identificar el perfil y las habilidades que deberá poseer un directivo de las tecnologías de las telecomunicaciones, se ha propuesto una práctica:

- Práctica 9, Manejo de conflictos.

Capítulo cinco, *Control*, el administrador debe llevar a cabo el control de la red, por medio de mecanismos de seguridad, monitoreando la red, manejando las listas de acceso, implementando auditorías informáticas y considerando que se debe contar con un plan de contingencia en caso de desastres.

Para este capítulo, cuyo objetivo es conocer, identificar y aplicar técnicas que le permitan diseñar, implantar y manejar de forma adecuada la red diseñada a fin de medir y obtener los resultados del desempeño esperados, de acuerdo a los objetivos planteados desde la planeación, se han propuesto cuatro prácticas:

- Práctica 10A, Mecanismos de seguridad, firma digital.
- Práctica 10B, Mecanismos de seguridad, certificados digitales.
- Práctica 10C, Mecanismos de seguridad, firewall.
- Práctica 11, Monitoreo de la red.

El formato de las prácticas del laboratorio, se basó en el manual de las prácticas desarrolladas para la asignatura de Redes de Datos. Esta estructura se conforma de los siguientes puntos:

1. Objetivo de aprendizaje, donde se describen las metas que se desean alcanzar después de la realización de la práctica.
2. Conceptos teóricos, breve introducción sobre el tema, de manera que el estudiante pueda ubicarse en el contexto de desarrollo.
3. Equipo y material necesario, descripción del material necesario para desarrollar la práctica.
4. Desarrollo, implica las actividades secuenciales en que se divide la práctica.
5. Conclusiones, en este punto el alumno expresa lo aprendido en la realización de la práctica.
6. Cuestionario previo, preguntas concretas que sirven como antecedentes a la práctica.

Cabe mencionar que la mayoría de las prácticas, ya han sido probadas con estudiantes de la carrera de Ingeniería en Computación, de la propia Facultad, que ya contaban con conocimientos teóricos básicos de redes de datos. Estas pruebas, nos han permitido recibir retroalimentación, que ha dado lugar a la reestructuración de algunos puntos de las prácticas, definiendo de forma más clara los tiempos, la redacción y los objetivos. Las pruebas se han realizado en el Laboratorio de Redes de Datos y Seguridad, coordinado por la profesora M.C. Ma. Jaquelina López Barrientos.

Se presentan las prácticas propuestas en el CD adjunto a la tesis, siendo posible apreciar que el número de prácticas destinadas a cada tema, corresponde en parte proporcional, al número de horas destinadas al mismo, según el plan de estudio de la asignatura.

Para enriquecer el contenido de las prácticas, buscando que éstas sean actuales y objetivas, visitamos a diferentes profesionales en las áreas de administración de redes en DGSCA, donde se ubica el NOC, Centro de Operación de Red de la UNAM, teniendo la oportunidad de entrevistar al responsable del centro, quien nos compartió su experiencia. De la misma forma, conversamos con el administrador de la red CUDI, quien se encuentra laborando en la misma dependencia, desarrollando actividades de administración de la red Internet2. En esta misma línea de acción, nos entrevistamos con el administrador de RVUNAM, quien nos mostró el equipo moderno de videoconferencia, que le permite a este centro administrar toda la red de videoconferencia, no sólo en la UNAM, si no a nivel nacional. En el área de telecomunicaciones, platicamos con el responsable, quien nos asesoró acerca de la implementación de VoIP sobre una red local.

Con estos acontecimientos, reforzamos y comprobamos el hecho de que la UNAM, es una institución que cuenta con tecnología de punta, que le permite consolidarse como la máxima casa de estudios en nuestro país.

En la Facultad de Ingeniería, concertamos diferentes entrevistas con cada uno de los profesores que imparten la asignatura de Redes de Computadoras. En primera instancia, el Ing. Alejandro Velázquez Mena, administrador de la red de la División de Ingeniería Eléctrica, nos mostró información acerca de los parámetros de red que se monitorean y que pueden ser consultados, vía Web por cualquier usuario, de la misma manera nos explicó la estructura de la red de la división, a la cual pertenece nuestro Laboratorio de Redes de Datos y Seguridad. En la entrevista con el M. C. Marco Antonio Vigueras Villaseñor, platicamos acerca del modelo de administración eTOM y nos proporcionó fuentes bibliográficas que profundizan sobre el tema. En el encuentro con el Ing. Noé Cruz Marín, administrador de la red de Servicios de Cómputo Académico de la Facultad, resaltamos la importancia de contar con un manual de laboratorio de prácticas, que refuerce el conocimiento teórico aprendido en las aulas.

La Facultad, cuenta con una sala de videoconferencia funcionando en el Centro de Docencia, ubicada en el anexo de la misma. Concertamos varias entrevistas con el responsable de la sala, el Ing. Alejandro Navarrete, quien amablemente nos mostró el equipo que se tiene y nos explicó su funcionamiento. En una de las entrevistas, tuvimos la oportunidad de platicar con el Ing. Miguel Mejía, responsable del centro, con el objetivo de plantear la posibilidad de realizar una práctica, consistente en la visita al centro. Esta propuesta tuvo éxito y el Centro de Docencia, está en la mejor disposición de participar en la formación académica de los alumnos.

A través de una página de Internet, pudimos contactar al Director General de BPMC Group, empresa encargada de proporcionar servicios enfocados al modelado de procesos de negocios. En entrevista con él, platicamos acerca del funcionamiento de la metodología eTOM, en casos reales de empresas. Abarcamos temas desde su historia, hasta su aplicación más extensa con ayuda del software Casewise.

Estas entrevistas, contribuyeron al mejor desarrollo y contenido de las prácticas, ya que nos permitieron ampliar nuestro panorama sobre las tecnologías, los esquemas y las metodologías que en la actualidad se aplican en las organizaciones, para tener una red funcionando adecuadamente.

El software empleado en el desarrollo de las prácticas, tiene diferentes orígenes:

a. OPNET IT GURU Academic, en su versión académica la cual puede ser instalada sin problemas de licencias, al menos por un año, que es cuando se requiere de una actualización, está disponible para descargarse de la página:

   http://www.opnet.com/services/university/itguru_academic_edition.html

b. RouterSim CCNA, un simulador de redes donado por una empresa dedicada a impartir cursos de certificación, actualmente se encuentra instalada en el Laboratorio.

c. MG-SOFT MIB Browser, versión gratuita disponible de la red, de la página:

   http://www.mg-soft.si/mgMibBrowserPE.html

d. Casewise, versión proporcionada por el Director General de BMPC Group.

e. Savvion Process Modeler Business Manager, versión descargada de la red, de la página:

   http://www.savvion.com/forms1/process_modeler.php

f. Java 5, versión actualizada del ambiente de desarrollo de java disponible en la página de Sun:

   http://java.sun.com/j2se/1.5.0/download.jsp

g. OpenSSL, software libre descargado de la red de la página:

   http://www.openssl.org/

h. Asterisk@Home, servidor de VoIP desarrollado bajo la licencia de software libre, descargada de la página:

   http://www.asterisk.org/

i. X-lite Softphone, herramienta libre para establecer llamadas vía IP a través del un servidor de VoIP, descargado de la página:

   http://www.counterpath.com/

j. 3Com Network Supervisor, software de administración de red incluido en el switch 3Com instalado en el Laboratorio de Redes de Datos y Seguridad.

k. Agilent, analizador de protocolos de redes obtenido mediante una donación. Actualmente se cuenta con un número específico de licencias.

En este sentido, en esta propuesta de prácticas se pretende incorporar algunas otras, a fin de enriquecer el manual y que el alumno tenga la oportunidad de realizarlas, en clase o bien como actividades extracurriculares, para adquirir un mayor conocimiento. Conforme a lo anterior, se han planteado las prácticas 7B y 10C.

INFRAESTRUCTURA

A continuación se presenta una lista de dispositivos que conforman la infraestructura necesaria, para implementar las prácticas de Administración de Redes de manera óptima.

5 piezas	Hub Ethernet 10BaseT o FastEthernet (4 -8) puertos, Mini Hub ANSEL.
11 piezas	Tarjeta inalámbrica, PCI Card, MSI PC11B2.
8 piezas	Access Point Wireless 11b, AP11B.
11 piezas	Diadema Multimedia (audífonos y micrófono).
2 piezas	Router Cisco (4 puertos).
4 piezas	Switch 3Com1317300.

ANEXOS

ANEXOS

El presente anexo, está contenido en el disco adjunto a este trabajo.

GLOSARIO

GLOSARIO

10BASE2:
También denominado conectividad con cable coaxial, su longitud máxima de segmento es de 185 metros.

10BASE5:
Denominado thicknet o AUI, Interfaz de Unidad de Conexión. Son redes intermedias entre 10Base2 y 10 BaseT. La longitud máxima del segmento es de 500 metros.

100BASE-T:
Trabaja sobre dos de los cuatro pares de alambre de par trenzado sin blindaje, su longitud máxima de un segmento desde el dispositivo concentrador hasta la estación de trabajo es de 100 metros.

100BASE-T, Fast Ethernet
Los datos viajan a 100 megabits por segundo a través de dos pares de alambre de cobre de par trenzado sin blindaje, la longitud máxima del cable entre el dispositivo concentrador y la estación de trabajo es de 20 metros.

100BASE-FX:
Equivale a la red Fast-Ethernet que opera a través de fibras ópticas, debido a que la fibra óptica no tiene limitaciones en cuanto a distancias no existe una longitud máxima de cable.

100BASE-T4:
Similar a la red 100BASE-T que opera a través de 4 pares de alambre de par trenzado sin blindaje, tiene una longitud máxima de cable de 20 metros entre el dispositivo concentrador y la estación de trabajo.

ANCHO DE BANDA:
Es el término utilizado para indicar la cantidad de datos que pueden transmitir los dispositivos como por ejemplo las tarjetas de red o los módems. Se utiliza como unidad los Kbps o Mbps.

APLICACIONES GROUPWARE:
Aplicación de software que permite a las personas utilizar computadoras en red, para trabajar en conjunto.

ATM:
Topología más reciente que permite tanto la transmisión de voz como de datos a través de cable o fibra, por medio de celdas de 53 bytes, que incluyen una gran cantidad de identificadores como la Calidad de Servicio, entre otros. Ofrece una velocidad de ruteo sumamente alta desde 25 hasta 622 Mbps.

ARP:
Protocolo de resolución de direcciones (Address Resolution Protocol**),** determina las direcciones de la capa de enlace de datos de las direcciones IP conocidas.

ASCII:
Código Americano Estándar para el Intercambio de Información, forma en el que las computadoras convierten caracteres, números y otros símbolos en 1’s ó 0’s.

BACKUP:
Es una línea auxiliar que mantiene el flujo normal de las operaciones que realiza el cliente a través de la línea inalámbrica ante alguna avería.

BACKUPS DE IPL:
Respaldo del programa de carga inicial.

BER:
Tasa de Error Bit (Bit Error Rate) el cual establece la probabilidad de que un bit registre error en la transmisión debido a interferencia o desvanecimientos en el canal inalámbrico.

BURSTY:

Paquetes de datos informáticos que se transmiten por ráfagas cortas y de forma continúa.

CAN:

Red de área de campus, es muy similar a una MAN pues opera a la velocidad de todas las LAN's que la componen. Regularmente se encuentran en un área local limitada, cuando esto sucede se utilizan dispositivos como los puentes o repetidores para enlazar los componentes de la red.

CEPT:

Conferencia Europea de Administraciones de Correos y Telecomunicaciones (*Conférence européenne des administrations des postes et des télécommunications*) es un organismo internacional que agrupa a las entidades responsables en la administración pública de cada país europeo de las políticas y la regulación de las comunicaciones, tanto postales como de telecomunicaciones.

CONMUTACIÓN:

Técnica que consiste en convertir datos en paquetes, considerado como el desarrollo más importante para la conectividad de redes.

COLISIÓN:

Circunstancia que se da, cuando más de una computadora intenta transmitir paquetes al mismo tiempo. Las computadoras involucradas detectan la colisión, detienen la transmisión y esperan un tiempo aleatorio para iniciar la retransmisión.

CONEXIONES DE INTERNET:

Existen al menos 3 tipos de conexiones a Internet:

a. Acceso telefónico, también conocida como dial-up es la forma como la mayoría de los usuarios se conectan a Internet, regularmente no son caras ni eficientes.
b. Conexiones dedicadas, utilizan líneas telefónicas a 56 Kbps son un poco más rápidas.
c. Conexiones troncales, ejemplos de ellas son las T1's, E1's y T3's, se puede transitar sobre ellas a una velocidad mucho más rápida.

CSMA/CD:

Acceso Múltiple de Percepción de Portadora con Detección de Colisiones.

DATAGRAMAS:

Pequeños paquetes de longitud fija, en los que se dividen los datos a transmitir.

DOMINIO DE COLISIÓN:

Segmento compartido por las computadoras en una topología lógica ethernet. Grupo de computadoras que comparte un cable para comunicarse entre ellas, cada computadora escucha a las demás y puede transmitir cuando ninguna de las otras lo está haciendo.

EMPAQUETADO:

Mecanismo que permite convertir una cantidad grande de datos en porciones más pequeñas de datos.

ETHERNET:

Surge en 1973, basado en el estándar de IEEE llamado 802.3 CSMA/CD, solucionando problemas de interconectividad entre equipos de cómputo.

EXTRANET:

Son en esencia, intranets que utilizan a Internet como vehículos para interactuar con otras personas proporcionando valores de seguridad, etc.

FAMILIA ETHERNET:

Ethernet es un término ampliamente utilizado para describir la topología lógica que utiliza CSMA/CD y las topologías físicas sobre las que operan las redes CSMA/CD. Los miembros principales de estas familias son: 10Base2, 10Base5, 10BaseT, 100Base-T, 100Base-Fx, 100BaseT4.

GROUPWARE:

Programa informático colaborativo, se refiere a los programas informáticos que integran el trabajo en un sólo proyecto con muchos usuarios concurrentes que se encuentran en diversas áreas.

HCC:

Conexión Cruzada Horizontal.

ICMP:

Protocolo de mensajes de Control en Internet (Internet Control Message Protocol) ofrece opciones de control y mensajería.

INTERNET:

Es una serie de redes privadas de computadoras (LAN, MAN, WAN), conectadas entre sí. Cada red privada individual pertenece a una organización, que es responsable de las computadoras en su área de influencia. Las redes privadas individuales se conectan a través de routers, que deciden que datos se quedan dentro de la red local y cuáles salen hacia otras redes.

INTRANET:

Se presenta cuando se ha creado una LAN, MAN y WAN, que cumple con los estándares de Internet.

JITTER:

Jitter es el ruido de fase con componentes frecuenciales sobre 10 Hz. El ruido de fase hace más difícil recuperar la temporización transportada por la señal, y hace que la velocidad de bit de la señal de entrada varíe, modificando el flujo de datos real dentro de la NE.

MODO DE TRANSFERENCIA ASÍNCRONO (ATM):

Tecnología de conmutación y multiplexión, de alta velocidad, orientada a conexión que usa celdas de 53 bytes (cabecera de 5 bytes y tributaria de 48 bytes) para transmitir diferentes tipos de tráfico simultáneo, incluyendo voz, video y datos.

MULTIPLEXOR:

Dispositivo que permite a dos o más señales ser transmitidas simultáneamente en una única portadora o canal.

MULTIPLEXIÓN DIGITAL:

Este término fue introducido hace 20 años y permitió que las señales de comunicaciones analógicas sean portadas en formato digital sobre la red. El tráfico digital puede ser portado mucho más eficientemente y permite el monitoreo de errores, para propósitos de calidad.

NOVELL:

Sistema operativo líder en redes, que permite la conectividad creando sistemas distribuidos.

OFDM:

Modulación por División Ortogonal de Frecuencia (Orthogonal Frequency Division Multiplexing) es muy eficiente en ambientes dispersos en el tiempo, como oficinas, donde las señales de radio son reflejadas desde muchos puntos, esto es que la señal llega a diferentes tiempos de propagación antes de que llegue al receptor.

OFIMÁTICA:

(Acrón, de oficina e infor *mática*) Automatización, mediante sistemas electrónicos, de las telecomunicaciones y procesos administrativos en las oficinas.

ORGANIZACIONES DE ESTANDARIZACIÓN EN AUDITORÍA INFORMÁTICA:

La auditoría informática se desarrolla en función de normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional.

PPP:

Protocolo Punto a Punto (Point to Point Protocol) es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

PROCESAMIENTO POR LOTES:

Es la forma como se interactuaba con la computadora hace 30 ó 40 años, en el que el operador de consola programaba una serie de actividades para una hora específica de la noche, comúnmente se presentaba en ambientes mainframes.

PROTOCOLO DE RED:

Conjunto de reglas para el envío y recepción de datos a través de una red. Manejan la conversión de datos desde las aplicaciones a la topología lógica.

PU-RDSI:

Parte de Usuario de la Red Digital de Servicios Integrados, establece el sistema de señalización no. 7 como el protocolo para proporcionar las funciones de señalización necesarias para sustentar servicios en una red digital de servicios integrados.

RARP:

Protocolo de Resolución Inversa de Direcciones (Reverse Address Resolution Protocol) determina las direcciones de red cuando se conocen las direcciones de la capa de enlaces de datos.

RED VERTEBRAL DE INTERNET:

Conjunto de líneas telefónicas utilizadas por las empresas telefónicas para la transmisión de grandes volúmenes de datos a velocidades de 155 y 622 Mbps, estrictamente son los únicos elementos que pertenecen a Internet.

REPETIDOR:

Dispositivo que permite que los elementos de una red, se comuniquen de una manera eficiente. Este amplifica y limpia las señales digitales y las envía a su destino.

RFC:

Documentos en los que se describen detalladamente los estándares que predominan, en la creación de software para Internet. También son conocidos con el nombre de Solicitudes de Comentarios.

RTT:

Tiempo de Viaje Redondo (Roed Trip Time) tiempo estimado de viaje de ida y vuelta.

SISTEMA DE RED:

Un sistema de red, tiene su base en la topología física, el siguiente nivel es la topología lógica y más arriba tiene los protocolos de red.

SLIP:

Protocolo de Línea Serial de Internet (Serial Line Internet Protocol) es una forma simple para encapsular datagramas IP sobre líneas sincrónicas. Este sistema se hizo famoso en los años 80 y principios de los 90 cuando las conexiones domiciliarias a Internet por medio de módems no superaban los 2400 bps.

SNEAKERNET:

Término acuñado para aquellas computadoras que no estaban en red y que requerían de compartir un archivo mediante el proceso de copiado en disco flexible y transferirlo a la computadora destino.

SOFTWARE DE AUDITORÍA INFORMÁTICA:

Consiste en programas de computadora empleados por el auditor como parte de sus actividades de auditoría en el proceso de recolección de datos, pueden pertenecer a paquetes escritos para un propósito en específico o bien ser programas de utilería o de administración de sistema.

SONET:

Synchronous Optical Network, es un estándar para el transporte de telecomunicaciones en redes de fibra óptica.

SPLITTER:

Como su nombre lo indica, los divisores de señal o splitters separan la señal en dos o más ramas para entregarla a dos o más dispositivos. Los splitter están diseñados para trabajar con un rango de frecuencia determinado; por ejemplo, para dividir la señal después del decodificador hay que utilizar un splitter pasivo que tenga un rango de frecuencia de 5 a 900 MHz para que no se presenten pérdidas de señal.

SUMAS DE VERIFICACIÓN:

Número que devuelve una computadora al recibir un paquete enviado, de 1's y 0's.

T1:

Regularmente son conocidas con este nombre las líneas telefónicas troncales de compañías que operan a velocidades de hasta 1.5 Mbps.

TAN:

Redes de área muy pequeña, término acuñada a aquellas redes en donde se tienen conectadas únicamente dos o tres equipos, que regularmente se instalan en casas o en otro lugar donde no sean negocios.

TERMINAL VIRTUAL:

Sección de un equipo que será empleado como si fuese una sola terminal y para permitir el ingreso del usuario válido éste debe cumplir con ciertas características (según la política de seguridad) y para ello se hace uso de listas de control de acceso donde se verifica la autenticidad del usuario

TOKEN-RING:

Basado en el estándar creado por IBM y la IEEE 802.5, como una mejora al 802.3 (CSMA/CD). Trabaja de forma diferente a ethernet, tiene un paquete especial denominado token, el cual viaja a través de toda la red, cuando una computadora desea transmitir espera al token, lo toma y transmite, terminado el proceso libera al token a la siguiente estación de trabajo en línea y así sucesivamente, es decir cada nodo espera su turno para transmitir.

TOPOLOGÍAS:

Término que se define como la disposición de una red, ésta puede ser lógica o física.

TOPOLOGÍAS LÓGICAS:

Establece las reglas mediante las cuales se llevará a cabo la comunicación, por ejemplo Ethernet, Token-Ring, FDDI, ATM.

TRAMA:

Grupo de bits enviados en serie sobre un canal de comunicaciones. Unidad lógica de transmisión enviada entre entidades en la capa de datos que contiene su propia información de control para direccionamiento y control de errores.

TRANSCEPTOR:

Es un dispositivo que realiza, dentro de una misma caja o chasis, funciones tanto de transmisión como de recepción, utilizando componentes de circuito comunes para ambas funciones. Dado que determinados elementos se utilizan tanto para la transmisión como para la recepción, la comunicación que provee un transceptor solo puede ser semipuplex, lo que significa que pueden enviarse señales entre dos terminales en ambos sentidos, pero no simultáneamente.

TRIBUTARIA:

Señal de velocidad más baja de entrada a un multiplexor para la combinación (multiplexación) con otras señales de baja velocidad para formar un agregado de mayor velocidad.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

1. Guía del Segundo Año, Academia de Networking de Cisco Systems CCNA 3 y 4
   Ed. Pearson Educación. Madrid, España. 2004.

2. Diseño de Seguridad en Redes.
   Merike, Kaeo.
   Ed. Pearson Educación. Madrid, España. 2003.

3. Sistema de Autenticación para Seguridad en Redes.
   Rolf Oppliger.
   Ed. Rama. Madrid, España. 1998.

4. Evaluación de Proyectos.
   Gabriel Baca Urbina.
   Ed. Mc Graw Hill. 4ª.ed. México. 2004.

5. Administración de Red Hat Linux.
   Thomas Schenk et al.
   Ed. Pearson Educación, Madrid España. 2001.

6. Auditoría Informática, un enfoque práctico.
   Mario G. Piattini, Emilio del Peso.
   Ed. Ra-Ma . 2ª. ed. Madrid España, 2001.

7. Optical Networking.
   Robert Elsenpeter.
   Ed. Mc Graw Hill. California, Estados Unidos. 2002.

8. Entér@te.
   Importancia de la Auditoría informática
   Nubia Fernández Grajales
   Año 4. Número 43 Suplemento mensual.
   27 de octubre 2005.

9. Auditoría en Informática.
   Enrique Hernández Hernández.
   CECSA.2ª ed. Grupo Patria Cultural. México 2000.

10. Comunicaciones y Redes de Computadores.
    William Stallings.
    Pearson Prentice Hall. 7ª ed. España, 2004.

11. Seguridad en Unix, Sistemas Abiertos e Internet.
    Ribagorda Garnacho. Ed. Parainfor. España. 1996.

12. Redes para procesos distribuidos.
    Jesús García Tomás. Ed. Alfaomega. 2ª ed. España 2001

13. Network Simulatios Experiments Manual.
    Larry L. Peterson, Bruce S. Davie.
    Ed. Morgan Kaufmann, 3a. ed. E.U. 2003.

14. Elementos de administración, un enfoque internacional.
Harold Coontz, Heinz Weihrich.
Ed. Mc GrawHill, 6a ed. México. 2002.

15. WI-FI, Cómo construir una red inalámbrica.
José Antonio Carballar.
Ed. Alfaomega-Rama. Madrid, España. 2004.

16. Manual de telecomunicaciones.
José Manual Huidobro Moya.
Ed. Alfaomega-Rama. Madrid, España. 2004.

17. Manual de administración de Linux.
Steve Shah.
Ed. Mc GrawHill. Madrid, España. 2001.

18. Cisco Catalyst LAN Switching.
Rossi, Louis R., Rossi Louis D.
Ed. Mc GrawHill.

19. Seguridad en Java.
Jaime Jaorsky, Paul J. Perrone.
Ed. Prentice Hall. Madrid, España 2001.

21. Guía de Seguridad e Integridad de Datos LAN Times

MESOGRAFÍA

MESOGRAFÍA

1. http://es.nimsoft.com/environments/traffic-analyzer.shtml
2. http://andercheran.aiind.upv.es/toni/personal/campusti.pdf
3. http://www.symantec.com/region/mx/enterprisesecurity/content/expert/LAM_3857.html
4. http://es.tldp.org/Articulos-periodisticos/jfs/security1/seguridad1.html
5. http://www.iana.org/assignments/port-numbers
6. http://es.wikipedia.org/wiki/Groupware
7. http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node336.html
8. http://www.enterate.unam.mx/
9. http://es.wikipedia.org/wiki/Jerarqu%C3%ADa_Digital_Plesi%C3%B3crona
10. http://www.diveo.net.mx/html/glosario.html
11. http://es.wikipedia.org/wiki/Jerarqu%C3%ADa_Digital_S%C3%ADncrona
12. http://www.mailxmail.com/curso/informatica/sdh/capitulo1.htm
13. http://www.cofetel.gob.mx/wb2/COFETEL/COFE_Normas_listado_
14. http://www.cinit.org.mx/articulo.php?idArticulo=7
15. http://www.ericsson.com.mx/technology/xDSL.shtml
16. http://es.wikipedia.org/wiki/STM-1
17. http://www.opnet.com/services/university/itguru_academic_edition.html
18. http://www.mg-soft.si/mgMibBrowserPE.html
19. http://www.savvion.com/forms1/process_modeler.php
20. http://java.sun.com/j2se/1.5.0/download.jsp
21. http://www.openssl.org/
22. http://www.asterisk.org/
23. http://www.counterpath.com/
24. http://bulma.net/body.phtml?nIdNoticia=1429
25. http://www.gwolf.org/seguridad/pki/node14.html
26. http://bulma.net/body.phtml?nIdNoticia=2234
27. http://es.wikipedia.org/wiki/GSM
28. http://www.pello.info/filez/firewall/iptables.html
29. http://www.flukenetworks.com/cuatrorazones
30. http://www.gestiopolis.com/recursos/checking/reprueba17.asp
31. http://www.psicojack.com/psicometricos.html
32. http://www.seguridaddigital.info/index.php?option=com_content&task=view&id=37&Itemid=26
33. http://www.ilustrados.com/publicaciones/EpyVZVZFEldlaHrEBX.php

34. http://tr.eltiempo.terra.com.co/blogs/home/contenidoblog.php?blog=8674749171
35. http://gsyc.escet.urjc.es/docencia/asignaturas/tsai/transpas/node5.html
36. http://www.certisur.com/support/serverid/faq/index.html

Salas de Videoconferencia México

Salas Certificadas en el Extranjero.

- NASA Johnson Space Center. TX US
- NASA Langley Space Center. VA US
- Purdue University. IN US
- Red Teleinformática Académica (RETINA). BS ARG
- Red Universitaria Nacional (REUNA) CL
- University of Texas. San Antonio. TX US
- Dirección de Tecnología y Comunicaciones, El Salvador
- Boston University. MA US
- DePaul University. IL US
- Fundación CIENTEC. SJ CR
- Mayo Clinic Scottsdale AR US
- Museo del Agua. MURCIA ES
- NASA Goddard Space Flight Center. MD US
- Universidad Francisco Gavidia. Dirección de Tecnología y Comunicaciones
- Collage Station. Tx, EUA
- Houston. TX, EUA
- Dallas. Tx, EUA
- San Antonio. TX, EUA
- México, DF.
- Austin. TX, EUA
- Centro Nacional de Alta Tecnología (CENAT) - Costa Rica
- Texas A&M University
- Escuela Permanente de Extensión en San Antonio. TX US
- Escuela de Extensión en Chicago IL.US
- Escuela de Extensión en Canadá QB.CA
- Instituto Tecnológico Centro Americano Departamento de informática, El Salvador
- Universidad Pedagógica Nacional de el Salvador

Redes de Videoconferencia

Red de Videoconferencia de la UNAM [RVUNAM]
Ciudad Universitaria[Establecida en 1993]

Red Nacional de Videoconferencia para la Educación [RNVE]
[Establecida en 1997]

Red de Videoconferencia CUDI [RVCUDI]
[Establecida en 2001]

- Internet 2
- Sala de videoconferencia en Mantenimiento
- Sala de videoconferencia en Proyecto
- Sala de videoconferencia

UPLINK EDUSAT

RED de Videoconferencia RVUNAM	108
RED de Videoconferencia RNVE	131
RED de Videoconferencia RVCUDI	152
RED de Videoconferencia Extranjera	27
TOTAL DE SALAS	418

El colegio de la frontera norte, BC
Tijuana telemática, BC.
IPN Tijuana, BC.
IPN Centro de Investigación y Desarrollo de Tecnología Digital, B.C.
Sala principal Mexicali , BC.
Ensenada dirección general, BC.
Centro de Investigación Científica y Educación Superior de Ensenada Sala Principal
Centro de Investigación Científica y Educación Superior de Ensenada-Telemática
Centro de Investigación Científica y Educación Superior de Ensenada-Dirección General
Centro de Ciencias de la Materia Condensada - Ensenada, BC.
Instituto de Astronomía San, Pedro Martir, BC.
CIBNOR, B.C.S
IPN La Paz, BCS.
Instituto de Geología, Estación Regional Noreste, Son
Centro de Ciencias Físicas, Son
EDUCADIS, Son
IPN Hermosillo, Son.
Instituto Tecnológico de Sonora, Son.
Centro de Investigación en Alimentación y Desarrollo, Son.
IPN Ciudad Juárez, Chih.
Universidad Autónoma de ciudad de Juárez Sala de Control de Videoconferencia, Chih
Universidad Autónoma de Chihuahua, Chih.
Sala de Control de Videoconferencia, Chih.
Instituto de Ciencias Biomédicas, Chih.
Instituto de Ingeniería y Tecnología, Chih.
Coordinación General de Tecnologías de la Información, Chih
Centro de Investigación en Materiales Avanzados A.C. Sala de Videoconferencia, Chi.
Universidad Autónoma de la Laguna Auditorio, Torreón Coah
Monclova, Coah.
Universidad Autónoma de la Laguna, Torreon Coah
Infotaca Central Unidad Saltillo,Coah.
Sala Principal de Videoconferencia, NL.
Universidad de Monterrey, NL.
IPN Monterrey, NL.
Red Biblioteca Central. Monterrey, NL.
Dirección General de Informática. NL
Hospital Universitario. Monterrey, NL.
Programa Universitario de Salud,NL.
ITESM. Monterrey, NL.
Instituto de Estudios Superiores de Tamps
IEST. Vicerrectoría Académica Educación a Distancia, Tamps.
Dir. de Telecomunicaciones. Centro de Excelencia Ciudad Victoria, Tamps.
Nuevo Laredo, Tamps.
Reynosa, Tamps.
Reynosa Rmx, Tamps.
Matamoros, Tamps.
Valle Hermoso, Tamps.
San Fernando, Tamps.
Jiménez, Tamps.
Estación Manuel, Tamps.
Mante, Tamps.
IPN Tampico, Tamps
Pemex Tampico, Tamp.
Campus los Mochis, Sin.
Rectoría los Mochis, Sin.
Campus Guasave, Sin.
Campus Guamuchil, Sin.
Campus Culiacán, Sin.
IPN Culiacán, Sin.
Universidad Autónoma de Sinaloa,Sin.
Instituto Tecnológico de Occidente, Sin
Red Universidad de Occidente, Sinaloa
Instituto de Ciencias del Mar y Limnología. Campus Mazatlán, Sin
Campus Mazatlán, Sin.
Universidad Juárez del Estado de Durango, Dgo
Escuela de Matemáticas
Centro Universitario de Cómputo. Zac
Unidad de Idiomas. Zac
Escuela Preparatoria de Matehuala, SLP.
El Colegio de San Luis A.C. SLP.
Facultad de Medicina, SLP.
Instituto Potosino de Investigación Científica y Tecnológica,SLP.
Centro de Información de Ciencias Sociales y Administrativas, SLP.
Centro de Información de Ciencia, Tecnología y Diseño Matehuala, SLP.
Unidad Académica Multidisciplinaria Zona Huasteca Ciudad Valles, SLP.
Unidad Académica Multidisciplinaria Zona Media,Río Verde, SLP.
IPN Guadalajara, Jal.
Guadalajara, Jal.
Dpto de Info,Ags
UAA,Ags.
Universidad Autónoma de Guadalajara, Jal.
Centro Universitario de Ciencias Económico Administrativas, Jal.
Centro Universitario de Arte, Arquitectura y Diseño, Jal.
Centro Universitario de Ciencias Exactas e Ingeniería, Jal.
Edificio Cultural y Administrativo. Piso 5 Y 6, Jal.
Centro Universitario de la Costa Sur Jal.
Edificio Cultural y Administrativo. planta baja, Jal
Centro Universitario de Ciencias Biológicas y Agropecuarias, Jal.
Centro Universitario de Ciencias Sociales y Humanidades, Jal.
Centro Universitario de los Valles, Jal.
Centro Universitario de la Ciénega, Jal.
Instituto Thomas Jefferson, Jal
León, Gto.
Centro de Investigación en Matemáticas GTO
Instituto de Ciencias Agrícolas Irapuato, Gto
Irapuato, Gto.
Salamanca, Gto.
Pemex Salamanca, Gto
Dpto.de Telecomunicaciones y Cómputo Salamanca
Celaya, Gto.
Preparatoria Oficial de Guanajuato
I.T. L.Dirección de Sistemas León Gto
Universidad del Bajío, Gto.
IPN San Miguel de Allende, Gto.
Guanajuato, Gto.
Silao, Gto.
CIDA,DTS.Gto
IPN Querétaro, Qro.
CIDETEQ.S.C. Qro.
INJ, Qro.
CIATEQ A.C. Qro
ITESM , Qro.
Colegio Carol Baur, Qro.
Centro de Geociencias
CIDI Qro.
Campus Tlahuelilpan, Hgo.
U. A. Q., Qro.
U. A. C., Hgo.
Pemex Tula, Hgo.
Facultad de Trabajo Social. Campus Poza Rica, Ver
Pemex Poza Rica, Ver.
Colegio de Notarios de Xalapa A.C. Ver
IPN Xalapa, Ver.
Instituto de Ecología A.C. Ver.
Centro de Investigación y Asistencia en Tecnología y Diseño del Edo de Jal.
Puerto Vallarta, Jal.
Centro Universitario de los Altos, Jal.
Centro Universitario del Sur, Jal.
Colegio Carol Baur, Guadalajara, Jal.
Centro Universitario de la Costa, Jal.
Centro Universitario del Norte, Jal.
Universidad La Salle Guadalajara, Jal.
Red Universidad de Colima, Col.
Programa de Videoconferencia, Col
Instituto de Astronomía, Mich.
Coordinación de Educación a Distancia. Edificio Q., Mich.
Facultad de Biología. Edificio R, Morelia. Mich.
Centro de Cómputo Universitario. Edificio N,Morelia, Mich.
El Colegio de Michoacán A.C.Departamento de Cómputo. Mich
Morelia, Mich. IPN
CREFAL Pátzcuaro, Mich.
Coordinación de Educación a Distancia,Uruapan, Mich.
Centro de Cómputo Universitario. Sala 2 Zamora, Mich.
Centro de Radioastronomía y Astrofísica. Morelia, Mich.
Centro de Investigaciones en Ecosistemas.Morelia, Mich.
Instituto de Matemáticas. Unidad Morelia
Colegio de Postgraduados, Edo Mex.
ITESM Toluca, Edo. Mex.
Colegio Carol Baur, Edo. Mex.
I.T. J.Kinder Garden Edo Mex.
I.N.I.N. Edo. Mex.
U.A.E.M Edo. Mex.
U. T. N. Edo. Mex.
U. V. E. Edo. Mex.
I. T. E., Edo. Mex.
I.T. J.High School Edo Mex.
ITESM, Edo. Mex.
UAT, Tlax.
C.A.T.E.D., Sala 1, Tlaxcala
IPN,Puebla, Pue.
INAOE, Pue.
U. P.A.E.P, Pue.
Facultad de Medicina
Centro de Tecnología Educativa
Edificio Carolino
Universidad de las Américas
IIEC. Mor.
U.A.E.M. Mor.
C.I.C.S.
C.R.I.M., Mor.
C.I.F.N., Mor.
INB.P. Mor.
C.C.F., Mor.
GT.Mor.
DGCA, Chilpancingo, Gro.
FCA, Acapulco, Gro.
IPN Oaxaca, Oax.
Universidad Autónoma Benito Juárez de Oaxaca
Dirección de Redes, Telecomunicaciones e Informática, Oax.
Centro Cultural Santo Domingo, Oax.
Universidad Pedagógica Nacional Unidad 201 - Oax
Centro de Investigación Científica de Yucatán A.C.Departamento de Cómputo
Sede Académica de Ciencias Sociales y Humanidades, Yuc.
Edificio Central. Teatro Felipe Carrillo Puerto, Yuc.
Centro De Investigaciones Regionales, Yuc.
Edificio Central. Sala Audiovisual Dr. Eduardo Urzáiz, Yuc.
Edificio Central. Auditorio Manuel Cepeda Peraza, Yuc.
Facultad de Medicina. Sala Dr. Maximiliano Carrillo, Yuc.
Facultad De Medicina. Sala Lic. Benito Juárez, Yuc.
IPN Mérida, Yuc.
IPN Campeche, Camp.
Universidad Autónoma de Campeche, Camp.
IPN Campech, Q. Roo.
Instituto Ciencias del Mar , Puerto Morelos, Q. Roo.
Universidad Autónoma de Quintana Roo, Q. Roo.
Pemex Ciudad del Carmen, Camp.
Pemex Dos Bocas, Tab.
Centro de Cómputo Universitario, Tab.
Pemex Villahermosa, Tab.
Pemex Coatzacoalcos, Ver.
Mmatitlán, Ver.
USIBI Coatzacoalcos, Ver.
El Colegio de la Frontera Sur. Centro de Investigación.Chiapas
San Cristobal de las Casas, Chis.
Tuxtla Gutiérrez, Chis.
IPN Tuxtla Gutiérrez, Chis.
Tapachula, Chis.
Dirección General de Investigaciones, Ver
Pemex Veracruz, Ver.
Dirección General de Tecnología de Información. Ver
Sala "Gonzalo Aguirre Beltrán" Ver
Sala de Autoconocer, Ver
Sala de Juntas Rectoría. Ver
Sala de Videoconferencia USBI Veracruz. Ver
Vicerrectoría Veracruz, Ver.
Enseñanza Distribuida. Dirección de Extensión de Servicios Tecnológicos, Ver
Laboratorio Nacional de Informática Avanzada IANVA A.C.Ver
Vicerrectoría Orizabar, Ver
Diseño.- Guillermo Vázquez

UNAM
COMPUTO academico Unam
VNOC Centro de Operaciones de Videoconferencia

http://distancia.dgsca.unam.mx

Circuito Exterior s/n frente a la Facultad de Contaduría y Administración
Ciudad Universitaria, Coyoacán 04510 México DF.

Fecha de actualización: Enero del 2005

Redes de Videoconferencia
México

Fecha de actualización: Enero del 2005

Internet 2 · Sala de videoconferencia en Mantenimiento · Sala de videoconferencia en Proyecto · Sala de videoconferencia

ENLACES DEDICADOS
CONEXI'N ISDN
UPLINK EDUSAT

Red Nacional de Videoconferencia para la Educación [RNVE]
[Establecida en 1997]

Red Universidad Autónoma de Chiapas.
- Tuxtla Gutiérrez, Chis.
- San Cristobal de las Casas, Chis.
- Tapachula, Chis.

Red Universidad Autónoma de Baja California, BC.
- Ensenada dirección general, BC.
- Sala principal Mexicali , BC.
- Tijuana telemática, BC.

Red Universidad Autónoma de Coahuila.
- Infoteca Central Unidad Saltillo,Coah.
- Torreón, Coah.
- Monclova, Coah.

Red Universidad Autónoma de Guerrero.
- FCA. Acapulco, Gro.
- DGCA. Chilpancingo, Gro.

Red Universidad de Guanajuato.
- Irapuato, Gto.
- Celaya, Gto.
- Salamanca, Gto.
- León, Gto.
- Guanajuato, Gto.
- Silao, Gto.

Red Universidad Michoacana de San Nicolas de Hidalgo.
- Facultad de Biología. Edificio R, Morelia. Mich.
- Centro de Cómputo Universitario. Edificio N,Morelia, Mich.
- Centro de Cómputo Universitario. Sala 2 Zamora, Mich.
- Coordinación de Educación a Distancia. Edificio Q , Mich.
- Coordinación de Educación a Distancia,Uruapan, Mich.
- Red Universidad de Occidente. Sinaloa

Red Universidad Autónoma de Sinaloa.
- Campus Mazatlán, Sin.
- Campus Culiacán, Sin.
- Rectoría los Mochis, Sin.
- Campus Guasave, Sin.
- Campus Guamuchil, Sin.
- Campus los Mochis, Sin.
- Universidad Autónoma de Sinaloa,Sin.

Red Universidad Autónoma de Tamaulipas
- Dir. de Telecomunicaciones. Centro de Excelencia Ciudad Victoria, Tamps.
- Vicerrectoría Académica - Educación a Distancia, Tamps.
- Reynosa, Tamps.
- Matamoros, Tamps.
- Mante, Tamps.
- Tampico, Tamps.
- Jiménez, Tamps.
- Valle Hermoso, Tamps.
- Estación Manuel, Tamps.
- San Fernando, Tamps.
- Nuevo Laredo, Tamps.

Red Universidad Autónoma de Zacatecas, Zac.
- Centro Universitario de Cómputo. Zac
- Unidad de Idiomas. Zac

Red Universidad de Monterrey, NL.
- Sala Principal de Videoconferencia, NL.

Red Universidad de Sonora, Son.
- EDUCADIS, Son

Red Universidad Autónoma de Nuevo León, NL.
- Programa Universitario de Salud,NL.

Red Petróleos Mexicanos
- Tula, Hgo.
- Villahermosa, Tab.
- Ciudad del Carmen, Yuc.
- Torre Ejecutiva, D.F.
- Reynosa, Tamps.
- Poza Rica, Ver.
- Coatzacoalcos, Ver.
- Tampico, Tamp.
- Dos Bocas, Tab.
- Veracruz, Ver.

Red Instituto Mexicano del Petróleo
- Ciudad de México, DF.
- Salamanca, Gto.
- Minatitlán, Ver.

Red Instituto Mexicano del Seguro Social.
- Unidad de Investigación Centro Médico Siglo XXI. DF.
- Hospital Tlatelolco, DF.
- Hospital la Raza, DF.
- Hospital Gabriel Mancera, DF.

Red Universidad Latina
- Cuernavaca, Mor.
- Campus Sur, DF.
- Campus Centro, DF.

Red Videoconferencia ITESM.
- ITESM. Monterrey, NL.
- Campus Estado de México, Edo. Mex.
- Cd. México, DF.
- Toluca, Edo. Mex.
- Campus Querétaro, Qro.

Red Colegio Carol Baur
- Plantel Misiones Colegio Carol Baur
- Colegio Carol Baur, Edo. Mex.
- Plantel Juriquilla Colegio Carol Baur, Qro.
- Colegio Carol Baur, Guadalajara, Jal.

Red Universidad Juárez Autónoma de Tabasco, Tab.
- Centro de Cómputo Universitario, Tab.

Red Universidad Autónoma de Yucatán
- Edificio Central. Teatro Felipe Carrillo Puerto, Yuc.
- Edificio Central. Sala Audiovisual Dr. Eduardo Urzéiz, Yuc.
- Edificio Central. Auditorio Manuel Cepeda Peraza, Yuc.
- Facultad de Médicina. Sala Dr. Maximiliano Canto, Yuc.
- Facultad De Medicina. Sala Lic. Benito Juárez, Yuc.
- Centro De Investigaciones Regionales, Yuc.

Red Universidad Politécnica de Aguascalientes, Ags.
- Departamento de Informática, Ags

Red Universidad Autónoma Benito Juárez de Oaxaca, Oax.
- Dirección de Redes, Telecomunicaciones e Informática, Oax.

- Universidad Autónoma de Aguascalientes, Ags.
- Instituto Tecnológico Autónomo de México, DF.
- UNITEC, DF.
- Asociación Nacional de Universidades e Instituciones de Educación Superior, DF
- Casa de Francia, DF.
- Instituto Nacional de Investigaciones Nucleares, Edo. Mex.
- Universidad Tecnológica Netzahualcóyotl, Edo. Mex.
- Universidad del Valle de Ecatepec, Edo. Mex.
- Instituto Tecnológico de Ecatepec, Edo. Mex.
- Universidad Autónoma Chapingo, Hgo.
- Universidad Autónoma de Querétaro, Qro.
- Instituto Tecnológico de Occidente, Sin
- Universidad Autónoma de Tlaxcala, Tlax.
- Universidad Iberoamericana, DF.

- ISSSTE, DF
- Hospital Médica Sur, DF
- Hospital ABC, DF
- Secretaría de Salud, DF
- Centro Nacional de Rehabilitación, DF
- Instituto Nacional de Nutrición, DF
- Instituto Nacional de Salud Pública Departamento de Educación a Distancia. Mor
- Instituto Nacional de Cancerología, DF
- Instituto Nacional de Pediatría, DF
- Instituto Nacional de Psiquiatría
- Instituto Nacional de Psquiatría "Ramón de la Fuente" .D.F
- Sanatorio Español, DF
- Instituto Latinoamericano de la Comunicación Educativa, DF
- Instituto Nacional de Antropología e Historia, DF
- Consejo Nacional contra las Adicciones, DF
- Universidad Juárez del Estado de Durango, Dgo
- Universidad Autónoma de Quintana Roo, Q. Roo
- Centro Nacional de Metrología, CENAM. Qro
- Instituto Thomas Jefferson,High School Thomas Jefferson Edo Mex
- Instituto Thomas Jefferson,Kinder Garden Thomas Jefferson Edo Mex
- Instituto Thomas Jefferson, Jal
- Escuela Nacional de Bibliotecología y Archivonomía Departamento de Desarrollo Informático. DF
- Instituto Tecnológico Centro Americano Dpto. de Informática, El Salvador
- Universidad Pedagógica Nacional de el Salvador
- Escuela de Matemáticas.Dgo
- Instituto de Estudios Superiores de Tamps.

Red de Videoconferencia de la UNAM [RVUNAM]
Ciudad Universitaria[Establecida en 1993]

- Coordinación de Humanidades Auditorio
- Coordinación de Humanidades Auditorio Mario de la Cueva
- Centro de Enseñanza para Extranjeros.
- Centro de Enseñanza para Extranjeros, Auditorio.
- Consejo Académico de Ciencias Biológicas
- Coordinación de Investigación Científica
- DGSCA. Observatorio de Visualización Ixtli
- DGSCA. Subdirección de Tecnología para la Educación
- DGSCA. Centro de Operaciones de Videoconferencia
- Dirección General de Servicios de Cómputo Académico - Auditorio
- Dirección General de Servicios de Cómputo Académico - Aula de Videoconferencia
- Direcciín General de Servicios de Cómputo Académico - Sala de juntas
- Coordinación de Universidad Abierta y Educación a Distancia (CUAED)
- Facultad de Medicina. Auditorio Dr. Raul Fournier
- Facultad de Medicina. Edificio de Investigación
- Facultad de Medicina Auditorio Fernando Ocaranza
- Facultad de Medicina Veterinaria y Zootécnia
- Facultad de Contaduría y Administración - Auditorio Pérez del Toro.
- Facultad de Contaduría. División de Educación Continua
- Facultad de Contaduría y Administración
- Facultad de Derecho División de Posgrado.
- Facultad de de Filosofía y Letras - Aula Magna.
- Facultad de Ciencias Conjunto Amoxcalli.
- Facultad de Odontología
- Facultad de Economía
- Facultad de Ciencias Políticas y Sociales
- Facultad de de Filosofía y Letras - División de Educación Continua
- Facultad de Química Edificio D.
- Facultad de Ingeniería Auditorio Barros Sierra
- Facultad de Ingeniería. Centro de Docencia
- Facultad de Ingeniería. División de Ingeniería Mecánica e Industrial
- Facultad de Ingeniería. División de Posgrado
- Facultad de Psicología
- Instituto de Astronomía
- Instituto de Ciencias del Mar y Limnología.
- Instituto de Ciencias del Mar y Limnología. Division de Posgrado
- Instituto de Ecología
- Instituto de Física
- Instituto de Fisiología Celular Biofísica y Neurociencias. Auditorio 2
- Instituto de Fisiología Celular. Edificio Principal, Auditorio
- Instituto de Geofísica
- Instituto de Matemáticas
- Instituto de Química
- Instituto de Investigaciones Biomédicas
- Instituto de Investigaciones Matemáticas Aplicadas y Sistemas
- Instituto de Investigaciones Filológicas Aula Magna.
- Instituto de Investigaciones Filológicas
- Instituto de Investigaciones Jurídicas
- Instituto de Investigaciones Económicas
- Instituto de Biología
- Instituto de Investigaciones Sociales
- Instituto de Ingeniería
- Dirección General de Televisión Universitaria TV, UNAM
- Unidad de Seminarios, Ignacio Chávez
- Dirección General de Divulgación de la Ciencia, UNIVERSUM
- Torre de Rectoría,Piso 3 y 6
- Dirección General de Personal
- Oficina de Apoyo al Consejo Universitario
- Escuela Nacional de Trabajo Social
- Centro de Ciencias de la Atmósfera
- Oficina de Apoyo al Consejo Universitario
- Consejo Académico de Área. Sala 1
- Defensoría de los Derechos Universitarios
- Biblioteca Conjuta de la Ciencia de la Tierra
- Dirección General de Proveeduría
- Instituto de Investigaciones en Materiales

COMPUTO academico unam

VNOC
Centro de Operaciones de Videoconferencia

Webcast

INTERNET

Red de Videoconferencia CUDI [RVCUDI]
[Establecida en 2001]

Salas Certificadas en el Extranjero.
- Texas A&M University
- Collage Station. Tx, EUA
- Houston. Tx, EUA
- Dallas. Tx, EUA
- San Antonio. Tx, EUA
- México, DF.
- Austin. Tx, EUA
- Boston University. MA US
- DePaul University. IL US
- Fundación CIENTEC. SJ CR
- Mayo Clinic Scottsdale AR US
- Museo del Agua. MURCIA ES
- NASA Goddard Space Flight Center. MD US
- NASA Johnson Space Center. TX US
- NASA Langley Space Center. VA US
- Purdue University. IN US
- Red Teleinformática Académica (RETINA). BS ARG
- Red Universitaria Nacional (REUNA) CL
- University of Texas. San Antonio. TX US
- Centro Nacional de Alta Tecnología (CENAT) - Costa Rica
- Universidad Francisco Gavidia, Dirección de Tecnología y Comunicaciones

Red CONACYT.
- Centro de Investigación en Materiales Avanzados A.C. Sala de Videoconferencia, Chi.
- Centro de Investigación Científica y Educación Superior de Ensenada-Telemática
- Centro de Investigación Científica y Educación Superior de Ensenada-Dirección General
- Corporación Universitaria para el Desarrollo de Internet Cudi A.C.
- Centro de Investigación en Alimentación y Desarrollo, Son.
- Consejo Nacional de Ciencia y Tecnología, DF.
- Centro de Investigaciones en óptica Ac. Departamento de Teleinformática y Sistemas, Gto
- Centro de Investigación Científica y Educación Superior de Ensenada Sala Principal
- Centro de Investigación Científica de Yucatán A.C.Departamento de Cómputo
- Centro de Investigación y Asistencia en Tecnología y Diseño del Edo de Jal.

Red Instituto Politécnico Nacional
- Dirección de Informática Auditorio Zacatenco, DF.
- Dirección de Informática Estudio VC, Zacatenco, DF.
- Centro de Investigación y Estudios Avanzados Dpto. de Matemática Educativa
- Tijuana, BC
- La Paz, BCS.
- Ciudad Juárez, Chih.
- Tuxtla Gutiérrez, Chis.
- Campeche, Camp.
- Santo Tom·s, DF.
- Iztacalco, DF.
- Coordinación de Educación a Distancia, DF.
- Centro Inteligente, DF.
- Zacatenco, DF.
- San Miguel de Allende, Gto.
- Guadalajara, Jal.
- Morelia, Mich.
- Monterrey, NL.
- Oaxaca, Oax.
- Puebla, Pue.
- Querétaro, Qro.
- Cancún, Q. Roo.
- Culiacán, Sin.
- Hermosillo, Son.
- Tampico, Tamps
- Jalapa, Ver.
- Mérida, Yuc.

Red Universidad Autónoma de la Laguna, A.C.
- Universidad Autónoma de la Laguna, Torreon Coah
- Universidad Autónoma de la Laguna Auditorio, Torreon Coah

Red Universidad de las Américas Puebla.
- Universidad de las Américas

Red Benemérita Universidad Autónoma de Puebla.
- Facultad de Medicina
- Centro de Tecnología Educativa
- Edificio Carolino

Red Universidad Autónoma Metropolitana
- Azcapotzalco II, DF.
- Iztapalapa I, DF.
- Iztapalapa II, DF.
- Xochimilco I, DF.
- Xochimilco II, DF.
- Casa primera imprenta, DF.
- Rectoría, DF.
- Azcapotzalco I, DF.

Red Universidad Autónoma de Ciudad Juárez, Chih
- Sala de Control de Videoconferencia, Chih.
- Instituto de Ciencias Biomédicas Chih·
- Instituto de Ingeniería y Tecnología Chih

Red Universidad Autónoma del Estado de Hidalgo, Hgo.
- Campus Virtual -Tulancingo, Hgo.
- Campus Virtual-Actopan, Hgo.
- Campus Tlahuelilpan, Hgo.

Red Universidad de Guadalajara.
- Guadalajara, Jal.
- Puerto Vallarta, Jal.
- Centro Universitario de Ciencias Económico Administrativas, Jal.
- Centro Universitario de Arte, Arquitectura y Diseño, Jal.
- Centro Universitario de Ciencias Exactas e Ingeniería, Jal.
- Centro Universitario de Ciencias de la Salud, Jal.
- Centro Universitario de los Altos, Jal.
- Centro Universitario de la Costa, Jal.
- Centro Universitario de la Costa Sur Jal.
- Centro Universitario de los Lagos, Jal.
- Centro Universitario del Norte, Jal.
- Centro Universitario de los Valles, Jal.
- Centro Universitario de la Ciénega, Jal.
- Centro Universitario de Ciencias Biológicas y Agropecuarias, Jal.
- Centro Universitario de Ciencias Sociales y Humanidades, Jal.
- Centro Universitario del Sur, Jal.
- Edificio Cultural y Administrativo. planta baja, Jal
- Edificio Cultural y Administrativo. Piso 5 Y 6, Jal.

Red Universidad Autónoma de San Luis Potosí
- Facultad de Medicina, SLP.
- Escuela Preparatoria de Matehuala, SLP.
- Centro de Información de Ciencias Sociales y Administrativas, SLP.
- Unidad Académica Multidisciplinaria Zona Media,Río Verde, SLP.
- Unidad Académica Multidisciplinaria Zona Huasteca Ciudad Valles, SLP.
- Centro de Información de Ciencia, Tecnología y Diseño Matehuala, SLP.

Red Universidad Autónoma del Estado de México
- Dirección de Servicios de Cómputo. Sala 1,2,3.

Red Universidad Veracruzana. Ver
- Dirección General de Tecnología de Información. Ver
- Sala "Gonzalo Aguirre Beltrán". Ver
- Sala de Autoacceso. Ver
- Sala de Juntas Rectoría. Ver
- Sala de Videoconferencia USBI Veracruz. Ver
- Vicerrectoría Veracruz, Ver
- USBI Coatzacoalcos, Ver
- Vicerrectoría Orizabar, Ver
- Facultad de Trabajo Social. Campus Poza Rica, Ver
- Colegio de Notarios de Xalapa A.C., Ver
- Dirección General de Investigaciones, Ver
- Enseñanza Distribuida. Dirección de Extensión de Servicios Tecnológicos, Ver
- Veracruz, Ver.
- Minatitlán, Ver
- Tuxpan, Ver.
- Córdoba, Ver.
- Red Universidad de Colima, Col.
- INFOTEC, DF.
- Centro de Cultura Digital TELMEX, DF.
- Universidad La Salle, DF.
- Red Universidad Autónomadel Estado de Mexico Edo Mex
- Universidad La Salle Guadalajara, Jal.
- Universidad Autónoma de Guadalajara Jal
- Universidad Autónoma del Estado de Morelos, Mor.
- Universidad Popular Autónoma del Estado de Puebla Pue
- Laboratorio Nacional de Informatica Avanzada IANIA ,A.C.Ver
- Instituto Tecnológico de Sonora, Son.
- Centro Cultural Santo Domingo, Oax.
- Universidad de Monterrey, NL.
- Universidad Autónoma de Chihuahua, Chih.
- Universidad Autónoma de Campeche, Camp.
- Suprema Corte de Justicia de la Nación, DF.
- Red Comisión Federal de Electricidad, DF.
- Red Universidad Anáhuac, D.F
- Universidad Pedagógica Nacional, DF.
- Red Biblioteca Central. Monterrey, NL.
- Hospital Universitario. Monterrey, NL.
- Instituto Tecnológico de Le·n, Dirección de Sistemas León Gto
- Universidad del Bajío, Gto.
- Instituto de Investigaciones Eléctricas. Cuernavaca, Mor.
- Universidad Panamericana
- El Colegio de la Frontera Sur. Centro de Investigación.Chiapas
- Texas A&M University Campus Ciudad de México Representación de Texas A&M University, DF.
- CREFAL Pátzcuaro, Mich.
- Colegio de México A.C. D.F
- CIDETEQ S.C. Qro
- CIBNOR. B.C.S
- El Colegio Nacional Aula Mayor. D.F
- El Colegio Nacional Fondo Reservado - Sala de Juntas, DF.
- CIATEQ A.C.. Qro
- El Colegio de Michoacán A.C.Departamento de Cómputo. Mich
- Instituto de Ecología A.C. Ver.
- Instituto Nacional de Astrofísica, Optica y electrónica INAOE. Pue
- Universidad Pedagógica Nacional Unidad. 201.Oax
- Sala de Control de Videoconferencia.Chih
- Dirección de Teleinformática.Mor
- Instituto Latinoamericano de la Comunicación Educativa.Auditorio Virtual.DF

Zona Metropolitana Ciudad de México
- Instituto Mexicano del Seguro Social
- Academia Nacional de Medicina
- Academia Mexicana de Cirugía
- Casa de las Humanidades
- Casa Universitaria del Libro
- Centro de Extensión Coapa
- Centro Educativo Multidisciplinario - Polanco
- Centro de Extensión en Cómputo Mascarones
- Centro Nacional de Educación Química
- Fundación Roberto Medellín
- Escuela Nacional de Artes Plásticas
- ENAP, Antigua Academia de San Carlos
- Escuela Nacional de Estudios Profesionales Aragón
- Escuela Nacional de Enfermería y Obstetricia
- Escuela Nacional de Estudios Profesionales Aragón, Educación Continua
- Facultad de Estudios Superiores, FES- Acatlán
- Facultad de Estudios Superiores Acatlán. Área de Docencia
- Facultad de Ingeniería. División de Educación Continua. DF.
- Facultad de Estudios Superiores - Iztacala
- Facultad de Estudios Superiores - Cuautl·n C.1
- Facultad de Estudios Superiores - Cuautl·n C.4
- Facultad de Estudios Superiores - Zaragoza C.2
- Facultad de Derecho División de Educación Continua
- Programa Universitario de Estudios sobre la Ciudad (PUEC)
- Palacio de la Escuela de Medicina. DF
- Antigua Escuela Nacional de Economía
- Centro de Geociencias. Qro

RED UNAM Nacional
- Coordinación General de Tecnologías de la Información
- Centro Regional de Investigaciones Multidisciplinarias. Cuernavaca, Mor.
- Centro de Investigación sobre Fijación de Nitrógeno. Cuernavaca, Mor
- Centro de Ciencias de la Materia Condensada - Ensenada, BC.
- Centro de Alta Tecnologia en Educacion a Distancia, Sala 1, Tlaxcala
- Centro de Radioastronomía y Astrofísica. Morelia, Mich.
- Centro de Ciencias Física. Cuernavaca, Mor.
- Centro de Investigaciones en Ecosistemas.Morelia, Mich
- Centro de Ciencias Físicas, Son
- Ciencias Genómicas Cuernavaca, Mor.
- Instituto de Astronomía San, Pedro Martir, BC.
- Instituto de Astronomía, Mich.
- Instituto Ciencias del Mar - Puerto Morelos, Q. Roo.
- Instituto de Ciencias del Mar Y Limnología. Campus Mazatl·n. Sin
- Instituto de Neurobiología. Juriquilla, Qro.
- Instituto de Matemáticas. Unidad Morelia
- Instituto de Geología. Estación Regional Noreste
- Sede Académica de Ciencias Sociales y Humanidades, Yuc.
- Licenciatura en Ciencias Genómicas

Extranjero
- Escuela Permanente de Extensión en San Antonio. TX US
- Escuela de Extensión en Chicago IL US
- Escuela de Extensión en Canad· QB CA

ANEXOS

1. A. Código de ética

POLÍTICAS DE SEGURIDAD EN CÓMPUTO PARA LA FACULTAD DE INGENIERÍA
SUBCOMITÉ DE ADMINISTRADORES DE RED

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."

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."

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.
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 , 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 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.

CÓDIGO DE ÉTICA PROFESIONAL DEL INGENIERO MEXICANO

El Código de Ética Profesional del Ingeniero Mexicano se publicó el 1 de julio de 1983, y firmó como testigo el C. Licenciado Miguel de la Madrid Hurtado, Presidente constitucional de los Estados Unidos Mexicanos, el cual se transcribe a continuación:

- El ingeniero reconoce que el mayor mérito es el trabajo, por lo que ejercerá su profesión comprometido con el servicio a la sociedad mexicana atendiendo al bienestar y progreso de la mayoría.
- Al transformar la naturaleza en beneficio de la humanidad, el ingeniero debe acrecentar su conciencia de que el mundo es la morada del hombre y de que su interés por el universo es una garantía de la superación de su espíritu y del conocimiento de la realidad para hacerla más justa y feliz.
- El ingeniero debe rechazar los trabajos que tengan como fin atentar contra el interés general; de esta manera evitará situaciones que impliquen peligros o constituyan una amenaza contra el medio ambiente, la vida, la salud y demás derechos del ser humano.
- Es un deber ineludible del ingeniero sostener el prestigio de la profesión y velar por su cabal ejercicio; asimismo, mantener una conducta profesional cimentada en la capacidad, la honradez, fortaleza, la templanza, la magnanimidad, la modestia, la franqueza y la justicia, con la conciencia de subordinar el bienestar individual al bien social.
- El ingeniero debe procurar el perfeccionamiento constante de conocimientos, en particular de su profesión, divulgar su saber, compartir su experiencia, proveer oportunidades para la formación y la capacitación de los trabajadores, brindar reconocimiento, apoyo moral y material a la institución educativa en donde realizó sus estudios; de esta manera revertirá a la sociedad las oportunidades que ha recibido.
- Es responsabilidad del ingeniero que su trabajo se realice con eficiencia y apoyo a las disposiciones legales. En particular, velará por el cumplimiento de las normas de protección a los trabajadores establecidas en la legislación laboral mexicana.
- En el ejercicio de su profesión, el ingeniero debe cumplir con diligencia los compromisos que haya asumido y desempeñará con dedicación y lealtad los trabajos que se le asignen, evitando anteponer su interés personal en la atención de asuntos que se le encomienden, o coludirse para ejercer competencia desleal en perjuicio de quien reciba sus servicios.
- Observará una conducta decorosa, tratando con respeto, diligencia, imparcialidad y rectitud a las personas con las que tenga relación, particularmente a sus colaboradores, absteniéndose de incurrir en desviaciones y abusos de autoridad y de disponer o autorizar a un subordinado conductas ilícitas, así como de favorecer indebidamente a terceros.
- Debe salvaguardarlos intereses de la institución o persona para la que trabaje y hacer buen uso de los recursos que se le hayan asignado para el desempeño de sus labores.
- Cumplirá con eficiencia las disposiciones que en ejercicio de sus atribuciones le dictaminen sus superiores jerárquicos, respetará y hará respetar su posición y trabajo; si discrepara de sus superiores tendrá la obligación de manifestar ante ellos las razones de su discrepancia.

El ingeniero tendrá como norma crear y promover la tecnología nacional; pondrá especial cuidado en vigilar que la transferencia tecnológica se adapte a nuestras condiciones conforme al marco legal establecido. Se obliga a guardar secreto profesional de los datos confidenciales que conozca en el ejercicio de su profesión, salvo que le sean requeridos por autoridad competente.

CODIGO DE ETICA Y EJERCICIO PROFESIONAL DE INGENIERIA DE SOFTWARE

(Versión 5.2) según es recomendado por el

Grupo de Trabajo Conjunto del IEEE-CS/ACM en Ética y Ejercicio Profesional de Ingeniería de Software

PREAMBULO

Las computadoras juegan un papel central y creciente en el comercio, la industria, el gobierno, la medicina, la educación, el entretenimiento y la sociedad en general. Los Ingenieros de Software son aquellos que contribuyen, mediante participación directa o mediante la enseñanza, al análisis, especificación, diseño, desarrollo, certificación, mantenimiento y prueba de sistemas de software. Debido a sus roles en el desarrollo de sistemas de software, los ingenieros de software tienen grandes oportunidades para hacerlo o causar daño. Para asegurar, tanto como sea posible, que sus esfuerzos serán utilizados por siempre, los ingenieros de software tienen que comprometerse ellos mismo en hacer la ingeniería de software una profesión respetable y beneficiosa. De acuerdo con este compromiso, los ingenieros de software deberán apegarse al siguiente Código de Ética y Ejercicio Profesional.

El Código contiene ocho Principios relacionados al comportamiento y a las decisiones tomadas por ingenieros de software profesionales, incluyendo practicantes, educadores, gerentes, supervisores y creadores de políticas, así como también aprendices y estudiantes de la profesión. Los Principios identifican las relaciones éticamente responsables en las cuales individuos, grupos, y organizaciones participan y las obligaciones principales con estas relaciones. Las Cláusulas de cada Principio son ilustraciones de algunas de las obligaciones incluidas en estas relaciones. Estas obligaciones están basadas en la humanidad del Ingeniero de Software, con especial atención sobre las personas afectadas por el trabajo de los ingenieros de software, y los únicos elementos del ejercicio de la Ingeniería de Software. El Código prescribe éstas como obligaciones de cualquiera que pretenda ser o aspire a Ingeniero de Software.

Este no pretende que las partes individuales del Código sean utilizadas de manera aislada para justificar errores de omisión o intención. La lista de Principios y Cláusulas no es exhaustiva. Las Cláusulas no deben ser leídas separando lo aceptable de lo inaceptable en la conducta profesional en todas las situaciones prácticas. El Código no es un simple algoritmo ético que genera decisiones éticas. En algunas situaciones los estándares pueden entrar en contradicción entre sí o con otros estándares de otras fuentes. Estas situaciones requieren que el Ingeniero de Software utilice su juicio ético para actuar de una forma en la que sea más consistente con el espíritu del Código de Ética y Ejercicio Profesional según las circunstancias.

Las contradicciones éticas pueden ser atacadas mediante la consideración ponderada de principios fundamentales, en lugar de confiar ciegamente en regulaciones detalladas. Estos Principios deben influenciar ingenieros de software para considerar ampliamente a quien es afectado por sus trabajos; examinar si ellos y sus colegas están tratando a otros seres humanos con el debido respeto; analizar como el menos apoderado será afectado por sus decisiones; y considerar si sus actuaciones serán juzgadas digna del trabajo profesional ideal como ingeniero. En todos estos juicios la preocupación por la salud, seguridad y el bienestar del público es elemental.

El dinámico y demandante contexto de la ingeniería de software requiere un código que sea adaptable y aplicable a nuevas situaciones a medida que ocurran. Sin embargo, aún en esta generalidad, el Código provee soporte a ingenieros de software y gerentes de ingenieros de software que necesiten tomar una acción positiva en un caso específico mediante la documentación de la postura ética de la profesión. El Código provee un fundamento ético al que individuos dentro de equipos y el equipo como un todo pueden apelar. El Código ayuda a definir aquellas acciones que son éticamente improcedentes demandar de un ingeniero de software o equipos de ingenieros de software.

El Código no es simplemente para arbitrar la naturaleza de actos cuestionables; éste también tiene una importante función educacional. Como este Código manifiesta el consenso de la profesión en aspectos éticos, esto es una intención de educar tanto al público como a los profesionales aspirantes acerca de las obligaciones éticas de todos los ingenieros de software.

- PRINCIPIOS

Principio 1. PÚBLICO

Los Ingenieros de Software deberán actuar consistentemente con el interés público. En particular, los ingenieros de software deberán, según sea apropiado:

1.1 Aceptar completa responsabilidad por su trabajo propio.

1.2 Moderar los intereses del ingeniero de software, el empleador, el cliente y los usuarios con el bien público.

1.3 Aprobar software solo si tienen una creencia fundamentada de que es seguro, satisface las especificaciones, pasa las pruebas apropiadas, y no disminuye la calidad de vida, disminuye privacidad o daña el ambiente. El efecto final del trabajo deberá ser para el bien público.

1.4 Notificar a las personas o autoridades pertinentes sobre cualquier peligro actual o potencial al usuario, el público, o el ambiente, que ellos razonablemente consideren está asociado con el software o los documentos relacionados.

1.5 Cooperar en los esfuerzos por corregir problemas de alta preocupación pública causada por el software, su instalación, mantenimiento, soporte o documentación.

1.6 Ser justo y evitar el fiasco en todas las declaraciones, particularmente las públicas, pertinentes a documentos, métodos y herramientas relacionados al software.

1.7 Considerar aspectos de incapacidad física, asignación de recursos, desventaja económica u otros factores que puedan disminuir el acceso a los beneficios del software.

1.8 Estar dispuesto a oficios profesionales voluntarios a buenas causas y contribuir con la educación pública concerniente a la disciplina.

Principio 2. CLIENTE Y EMPLEADOR

Los Ingenieros de Software deberán actuar de tal manera que esté dentro de los mejores intereses de su cliente y su empleador, consistente con el interés público. En particular, los ingenieros de software deberán, según sea apropiado:

2.1 Proveer servicio en las áreas de competencia, siendo honesto y franco sobre las limitaciones de su experiencia y educación.

2.2 No utilizar software que conscientemente haya sido obtenido o retenido ilegal o antiéticamente.

2.3 Utilizar la propiedad del cliente o empleador sólo del modo apropiadamente autorizado, y con el conocimiento y consentimiento del cliente o empleador.

2.4 Asegurar que cualquier documento sobre el que ellos se basen haya sido aprobado, y cuando lo amerite, por alguien autorizado.

2.5 Mantener en privado cualquier información confidencial obtenida en su trabajo profesional, donde dicha confidencialidad sea consistente con el interés público y consistente con la ley.

2.6 Identificar, documentar, recolectar evidencia y reportar al cliente o empleador oportunamente si, en su opinión, un proyecto está camino a fracasar, evidencia estar muy caro, viola la ley de propiedad intelectual, o si por el contrario va a resultar problemático.

2.7 Identificar, documentar, y reportar al empleador o cliente aspectos significantes de interés social, en el software o documentos relacionados, de los cuales ellos estén conscientes.

2.8 No aceptar trabajo exterior perjudicial al trabajo que ellos realizan para su empleador principal.

2.9 No promover interés adverso a su empleador o cliente, a menos que un asunto ético mayor esté siendo comprometido; en ese caso, informar al empleador u otra autoridad apropiada sobre el asunto ético.

Principio 3. PRODUCTO

Los ingenieros de software deberán asegurar que sus productos y modificaciones relacionadas cumplen con los más altos estándares profesionales. En particular, los ingenieros de software deberán, según sea apropiado:

3.1 Esforzarse por alta calidad, costo aceptable y cronograma razonable, asegurando que los aspectos significantes estén claros y sean aceptados por el empleador y el cliente, y estén disponibles para consideración del usuario y el público.

3.2 Asegurar metas y objetivos apropiados y alcanzables para cualquier proyecto en los que trabajen o propongan.

3.3 Identificar, definir y trabajar aspectos éticos, económicos, culturales, legales y ambientales relacionados a proyectos de trabajo.

3.4 Asegurar que ellos están calificados para cualquier proyecto en el cual trabajen o le propongan trabajar mediante una combinación apropiada de educación y entrenamiento, y experiencia.

3.5 Asegurar que sea utilizado un método apropiado para cualquier proyecto en que trabajen o le propongan trabajar.

3.6 Trabajar para seguir estándares profesionales, cuando estén disponibles, que sean más apropiados para la tarea a mano, salvo aquellas que hayan sido justificadas ética o técnicamente.

3.7 Esforzarse por comprender completamente las especificaciones del software en el que trabajan.

3.8 Asegurar que las especificaciones del software en el que trabajan hayan sido bien documentadas, satisfacen los requerimientos del usuario y tienen la debida aprobación.

3.9 Asegurar estimados cuantitativos realistas de costo, cronograma, personal, calidad y resultados en cualquier proyecto en que trabajen o le propongan trabajar y dar un juicio de valor indefinido de estos estimados.

3.10 Asegurar prueba, depuración, y revisión apropiada del software y documentos relacionados en los que trabajan.

3.11 Asegurar una documentación adecuada, incluyendo problemas significantes descubiertos y soluciones adoptadas, para cualquier proyecto en el que trabajen.

3.12 Trabajar para desarrollar software y documentos relacionados que respeten la privacidad de aquellos que serán afectados por ese software.

3.13 Ser cuidadoso de utilizar sólo datos precisos resultantes de medios legales y éticos, y utilizarlos sólo de las maneras autorizadas apropiadamente.

3.14 Mantener la integridad de los datos, siendo perceptivo de ocurrencias obsoletas o deficientes.

3.15 Tratar todas las formas de mantenimiento de software con el mismo profesionalismo de desarrollo nuevo.

Principio 4. JUICIO

Los ingenieros de software deben mantener integridad e independencia en su juicio de valor profesional. En particular, los ingenieros de software deben, según sea apropiado:

4.1 Atemperar todo juicio técnico por la necesidad de soportar y mantener valores humanos.

4.2 Solo avalar documentos ya sean preparados bajo su supervisión o dentro de sus áreas de competencia y con los cuales ellos estén de acuerdo.

4.3 Mantener objetividad profesional con respecto a cualquier software o documentos relacionados que se les haya pedido evaluar.

4.4 No ocuparse en prácticas financieras engañosas como soborno, doble facturación, u otra práctica financiera impropia.

4.5 Notifique a todas las partes involucradas aquellos conflictos de intereses que no puedan ser evitados o evadidos razonablemente.

4.6 Rehusar participar, como miembros o asesores, en organismo privado, gubernamental o profesional interesado en aspectos relativos a software, en el cual ellos, sus empleados o sus clientes tengan potenciales conflictos de intereses sin revelar.

Principio 5. GERENCIA

Los gerentes y líderes de ingeniería de software deberán apegarse y promover un enfoque ético de la gerencia de desarrollo y mantenimiento de software. En particular, aquellos manejando o liderando ingenieros de software deberán, según sea apropiado:

5.1 Asegurar buena gerencia de cualquier proyecto en que ellos trabajen, incluyendo procedimientos efectivos para la promoción de calidad y reducción de riesgo.

5.2 Asegurar que los ingenieros de software estén informados de los estándares antes de apoyarse en ellos.

5.3 Asegurar que los ingenieros de software conozcan las políticas y procedimientos del empleador para proteger claves, archivos e información que sea confidencial al empleador o confidencial a otros.

5.4 Asignar trabajo sólo después de tomar en cuenta contribuciones apropiadas de educación y experiencia templadas con un deseo de fomentar esa educación y experiencia.

5.5 Asegurar estimados cuantitativos realistas de costo, calendario, personal, calidad y resultados de cualquier proyecto en el que trabajen o propongan trabajar, y dar un juicio de valor indefinido de estos estimados.

5.6 Atraer ingenieros de software potenciales sólo mediante la descripción exacta y completa de las condiciones de trabajo.

5.7 Ofrecer remuneración justa y exacta.

5.8 No impedir injustamente que alguien tome una posición para la cual esa persona es apropiadamente calificada.

5.9 Asegurar que haya un contrato justo concerniente a la propiedad de cualquier software, procesos, investigación, escritos, u otra propiedad intelectual a la que haya contribuido un ingeniero de software.

5.10 Proveer un debido proceso en cargos de audiencia de violación de una política del empleador o de este código.

5.11 No pedir a un ingeniero de software hacer algo en desacuerdo con este Código.

5.12 No sancionar a nadie por expresar preocupaciones éticas acerca de un proyecto.

Principio 6. PROFESION

Los ingenieros de software deben fomentar la integridad y reputación de la profesión de acuerdo con el interés público. En particular, los ingenieros de software deben, según sea apropiado:

6.1 Ayudar a desarrollar un ambiente organizacional favorable para actuar éticamente.

6.2 Promover el conocimiento público de la ingeniería de software.

6.3 Expandir el conocimiento de la ingeniería de software mediante la participación apropiada en organizaciones profesionales, encuentros y publicaciones.

6.4 Soportar, como miembros de una profesión, a otros ingenieros de software tratando de seguir este Código.

6.5 No promover su interés propio a costo de la profesión, cliente o empleador.

6.6 Obedecer todas las leyes que rigen su trabajo, a menos que, en circunstanciasexcepcionales, dicho obedecimiento sea inconsistente con el interés público.

6.7 Ser preciso en plantear las características del software en el que trabajan, evitando no sólo afirmaciones falsas sino también afirmaciones que pudieran razonablemente estar supuestas a ser especulativas, vacuas, engañosas, confusas, o dudosas.

6.8 Tomar responsabilidad para detectar, corregir, y reportar errores en software y documentos asociados en los que trabajen.

6.9 Asegurar que clientes, empleadores, y supervisores conozcan el compromiso del ingeniero de software con este Código de ética, y las subsecuentes derivaciones de dicho compromiso.

6.10 Evitar asociaciones con negocios y organizaciones que entren en conflicto con este código.

6.11 Reconocer que las violaciones a este Código son inconsistentes con ser un ingeniero de software profesional.

6.12 Expresar preocupación a las personas involucradas cuando sean detectadas violaciones significativas a este Código a menos que sea imposible, anti-productivo, o peligroso.

6.13 Reportar violaciones significativas de este Código a las autoridades competentes cuando esté claro que el asesoramiento a las personas involucradas en estas violaciones significativas sea imposible, anti-productivo o peligroso.

Principio 7. COLEGAS

Los ingenieros de software deberán ser justos y comprensivos con sus colegas. En particular, los ingenieros de software deberán, según sea apropiado:

7.1 Animar a los colegas a apegarse a este Código.

7.2 Asistir a los colegas en el desarrollo profesional.

7.3 Dar crédito completo al trabajo de otros y abstenerse a tomar crédito inmerecido.

7.4 Revisar el trabajo de otros de una manera objetiva, cándida, y apropiadamente documentada.

7.5 Dar una audiencia justa a las opiniones, inquietudes, o quejas de un colega.

7.6 Asistir a los colegas en estar completamente al tanto de prácticas actuales de estándares de trabajo incluyendo políticas y procedimientos para protección de claves, archivos y otra información confidencial, y medidas de seguridad en general.

7.7 No intervenir injustamente en la profesión de ningún colega; Sin embargo, por interés del empleador, el cliente o el beneficio público se puede coaccionar a ingenieros de software, en buena fe, para cuestionar la competencia de un colega.

7.8 En situaciones fuera de sus propias áreas de competencia, pedir opiniones de otros profesionales que tengan competencia en esa área.

Principio 8. INTERES PROPIO

Los Ingenieros de Software deberán participar en el aprendizaje de por vida del ejercicio de su profesión y deberán promover un enfoque ético para el ejercicio de la misma. En particular, los ingenieros de software deberán continuamente esforzarse en:

8.1 Promover su conocimiento de desarrollo en el análisis, especificación, diseño, desarrollo, mantenimiento y prueba de software y documentos relacionados, junto con la gerencia del proceso de desarrollo.

8.2 Mejorar su habilidad de crear software de calidad, seguro, confiable, y útil a un costo y un tiempo razonable.

8.3 Mejorar su habilidad de producir documentación precisa, informativa y bien escrita.

8.4 Mejorar su entendimiento del software y documentos relacionados con los que trabajan y del ambiente en que utilizarán.

8.5 Mejorar su conocimiento concerniente a estándares y a la ley gobernante del software y documentos en los que trabajan.

8.6 Mejorar su conocimiento de este Código, su interpretación, y su aplicación en su trabajo.

8.7 No dar tratamiento injusto a nadie debido a cualquier prejuicio irrelevante.

8.8 No influenciar a otros para emprender cualquier acción que involucre una violación de este Código.

8.9 Reconocer que violaciones personales de este Código no van acordes con ser un ingeniero de software profesional.

Este Código fue desarrollado por el comité conjunto IEEE-CS/ACM en Etica y Ejercicio Profesional de Ingeniería de Software (SEEPP):

Comité Ejecutivo: Donald Gotterbarn (Presidente), Keith Miller and Simon Rogerson;

Miembros: Steve Barber, Peter Barnes, Ilene Burnstein, Michael Davis, Amr El-Kadi, N. Ben Fairweather, Milton Fulghum, N. Jayaram, Tom Jewett, Mark Kanko, Ernie Kallman, Duncan Langford, Joyce Currie Little, Ed Mechler, Manuel J. Norman, Douglas Phillips, Peter Ron Prinzivalli, Patrick Sullivan, John Weckert, Vivian Weil, S. Weisband and Laurie Honour Werth.

Traducido y adaptado al español por:
Ing. Melvin Pérez Chair
IEEE Computer Chapter

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:
   - Interesarse en el bienestar común y aplicar sus conocimientos profesionales para beneficio de la institución así como de sus integrantes.
   - Desarrollar sus deberes con honestidad e imparcialidad y servir con dedicación a sus superiores, sus empleados y a la comunidad universitaria general.
   - 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.
   - 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 recurso 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 INGENIERÍA EN EL ÁMBITO INFORMÁTICO

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 éstos 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.

CÓDIGO DE ÉTICA DOCENTE DEL PERSONAL ACADÉMICO DE LA FACULTAD DE INGENIERÍA, UNAM

1. Conocer con amplitud y profundidad el campo académico, científico y práctico de la asignatura que enseño, y preparar, debidamente actualizado, cada tema que exponga.
2. Transmitir con precisión, claridad y sencillez, dentro del grado de profundidad que se requiera, el curso que imparto.
3. Asistir a clase siempre, puntualmente y trabajar sistemáticamente y hacer trabajar a los estudiantes de la misma manera.
4. Motivar, estimular y mostrar interés por el aprendizaje significativo de los estudiantes y evaluar a conciencia y con justicia el grado de aprendizaje de los alumnos.
5. Aceptar observaciones, opiniones y críticas de los estudiantes, sin menoscabar mi papel de gula y educador.
6. Fomentar en los estudiantes el interés por la Ciencia y la Innovación Tecnológica, y también por las Ciencias Sociales y Humanidades que les permitan adquirir una conciencia social que los impulse a conocer la situación política, económica, social y cultural del país, con un sentido de participación y compromiso.
7. Las relaciones con mis Colegas deberán estar sustentadas en los principios de lealtad, mutuo respeto, consideración justa, solidaridad y en la promoción permanente de oportunidades para mejorar el desarrollo profesional.
8. Contribuir, en forma comprometida, con la calidad de mi labor educativa, al prestigio y eficiencia de nuestra Facultad.
9. Promover y mantener el cuidado de las propiedades física e intelectuales de la Universidad, para asegurar un ambiente propicio para el mejoramiento continuo del proceso enseñanza-aprendizaje.
10. Ser ejemplo de integridad personal y académica, de responsabilidad y tolerancia, respetuoso de las Normas y Reglamentos, y de la dignidad de nuestra Profesión, y llevar consigo la obligación de servir a los estudiantes, a la Universidad y a la Sociedad con absoluto convencimiento.

Para finalizar, seria imposible plasmar en este trabajo. de tesis cada uno de los códigos de ética que existen en México, debido a que cada Institución cuenta con su propio código, por lo cual nos dimos a la tarea de mostrar los principales códigos de ética que nos afectan directamente a los ingenieros de la facultad de Ingeniería.

Es necesario que como ingenieros nos tomemos un tiempo para analizar cada uno de estos códigos, debido a que nos dan una idea precisa de cómo nos debemos de guiar en nuestra vida profesional independientemente del puesto que desempeñemos en la Industria.

Si logramos captar las ideas principales de los códigos presentados anteriormente, podemos estar seguros de que nuestra actitud ante los distintos trabajos que nos enfrentemos los sabremos sacar de la mejor forma posible, sin temor a pensar en haber cometido una falla en la toma de decisiones.

3. A Niveles de multiplexación PDH

La versión americana, japonesa y europea de sistemas PDH, difieren ligeramente en sus detalles de trabajo, pero los principios de funcionamiento son los mismos, por ello a continuación se describe solo la versión europea:

La velocidad básica de transferencia de información, o primer nivel jerárquico, es un flujo de datos de 2,048 Mbps (generalmente conocido de forma abreviada por "2 megas").

Para transmisiones de voz, este flujo se divide en 30 canales de 64 kbps (abreviado como "64K") más otros 2 canales de 64 kbps utilizados para señalización y sincronización. De forma alternativa es posible también utilizar el flujo completo de 2 megas para usos no vocales, tales como la transmisión de datos.

La velocidad del flujo de datos 2 megas es controlada por un reloj en el equipo que la genera. A esta velocidad se le permite una variación, alrededor de la velocidad exacta de 2,048 Mbps, de +/- 50 partes por millón. Esto significa que dos flujos diferentes de 2 megas pueden estar (y probablemente lo están) funcionando a velocidades ligeramente diferentes uno de otro.

Al fin de poder transportar múltiples flujos de 2 megas de un lugar a otro, estos son combinados, o multiplexados en grupos de cuatro en un equipo multiplexor. La multiplexación se lleva a cabo tomando un bit del flujo 1, seguido por un bit del flujo 2, luego otro del 3 y finalmente otro del 4. El multiplexor además añade bits adicionales a fin de permitir al desmultiplexor del extremo distante descodificar qué bits pertenecen a cada flujo de 2 megas y así reconstituir los flujos originales. Estos bit adicionales son, por un lado, los denominados *bits de justificación* o de *relleno* y por otro una combinación fija de unos y ceros que es la denominada palabra de alineamiento de trama que se transmite cada vez que se completa el proceso de transmisión de los 30+2 canales de los 4 flujos de 2 megas, que es lo que constituye una trama del orden superior (8 megas).

La necesidad de los bits de relleno o justificación es que como cada uno de los flujos de 2 megas no está funcionando necesariamente a la misma velocidad que los demás, es necesario hacer algunas compensaciones. Para ello el multiplexor asume que los cuatro flujos están trabajando a la máxima velocidad permitida, lo que conlleva que, a menos que realmente esté sucediendo esto, en algún momento el multiplexor buscará el próximo bit, pero este no llegará, por ser la velocidad del flujo inferior a la máxima. En este caso el multiplexor señalizará (mediante los bits de justificación) al desmultiplexor que falta un bit. Esto permite al multiplexor reconstruir correctamente los flujos originales de los cuatro 2 megas y a sus velocidades plesiócronas correctas.

La velocidad del flujo resultante del proceso antes descrito es de 8,448 Mbps (8 megas) que corresponde al segundo nivel jerárquico.

Por procedimientos similares se llega a los niveles tercero, constituido por 4 flujos de 8 megas y una velocidad de 34,368 Mbps (34 megas) y cuarto, formado por 4 flujos de 34 megas y una velocidad de 139,264 Mbps (140 megas).

De la misma forma, mediante la multiplexación de 4 flujos de 140 megas, se forma un flujo de 565 Mbits, pero su estructura y proceso de multiplexación, al contrario de lo que sucede con los cuatro niveles precedentes, no ha sido normalizado por los organismos de

normalización especializados UIT y CEPT, por lo que los flujos generados por los equipos de un fabricante pueden ser, y de hecho lo son, incompatibles con los de otro fabricante, lo que obliga a que el enlace completo de 565 Mbps esté constituido con terminales del mismo fabricante.

La velocidad de 565 Mbps es la típica de los sistemas de transmisión por fibra óptica, aunque en el pasado se ha utilizado, aunque con escaso éxito por sus estrictos requerimientos, sobre cables coaxiales.

3. B Estructura de la trama STM-1 de SDH

Las tramas contienen información de cada uno de los componentes de la red, *trayecto*, *línea* y *sección*, además de la información de usuario. Los datos son encapsulados en contenedores específicos para cada tipo de señal tributaria.

A estos contenedores se les añade una información adicional denominada *tara de trayecto* (Path overhead), que son bytes utilizados con fines de mantenimiento de la red, dando lugar a la formación de los denominados contenedores virtuales (VC). El resultado de la multiplexación es una trama formada por 9 filas de 270 octetos cada fila (270 columnas de 9 octetos). La transmisión se realiza bit a bit en el sentido de izquierda a derecha y de arriba abajo. La trama se transmite a razón de 8000 veces por segundo (cada trama se transmite en 125 μs). Por lo tanto el régimen binario (Rb) para cada uno de los niveles es:

STM-1=8000*(270octetos*8bits*9filas)=155Mbps.

STM-4=4*8000*(270octetos*8bits*9filas)=622Mbps.

STM-16=16*8000*(270octetos*8bits*9filas)=2.5Gbps.

De las 270 columnas que forman la trama STM-1 las 9 primeras forman la denominada tara (Overhead), independiente de la tara de trayecto de los contenedores virtuales antes mencionados, mientras que las 261 restantes constituyen la carga útil (Payload).

En la tara están contenidos bytes para alineamiento de trama, control de errores, canales de operación y mantenimiento de la red y los punteros, que indican el comienzo del primer octeto de cada contenedor virtual.

3. C La arquitectura de red SS7, Sistema de Señalización No. 7

La arquitectura SS7 distingue tres diferentes puntos de señalización: puntos de conmutación de señal (SSPs), puntos de transferencia de señal (STPs) y puntos de control de señal (SCPs). En la arquitectura norteamericana de señalización se han asignado ciertos símbolos para denotar cada una de estas entidades de la red telefónica. La simbología se ilustra en la siguiente figura 3.C1.

Figura 3.C1. Elementos de señalización de red

Los puntos de conmutación de señal representan conmutadores telefónicos equipados con características SS7 y enlaces terminales de señalización. Son éstos los que originan, terminan o conmutan las llamadas. Los puntos de transferencia de señal son parte fundamental de la arquitectura SS7, pues representan los conmutadores de paquetes de la red; son los encargados de recibir y dirigir los mensajes de señalización hacia el destinatario correcto, por lo que llevan a cabo funciones de ruteo. Cuando el STP recibe un mensaje procedente de un SSP, el STP verifica el destino del mensaje y de no ser para él, elige, a partir de sus tablas de ruteo, el punto destinatario de señalización y el enlace a través del cual se enviará el mensaje a este nodo. Los puntos de control de señalización son entidades de la red que ofrecen una lógica complementaria, utilizada para ofrecer servicios adicionales. Básicamente, se trata de bases de datos que proveen características avanzadas como, por ejemplo, servicios a números gratuitos 1-800. Para poder utilizar estos servicios, el SSP envía un mensaje al SCP solicitando instrucciones. Por tal motivo, los conmutadores deben ofrecer cierta funcionalidad que les permita interactuar con el SCP y por esto, en la literatura también se conoce a los SSPs como puntos de conmutación de servicios. Los STPs y SCPs son normalmente implementados en pares, y aunque no se ubican en el mismo lugar, operan en forma redundante.

Para que la arquitectura SS7 sea robusta, la red deberá diseñarse de tal forma que ofrezca un alto grado de redundancia. De esta forma, cualquier problema que pudiera surgir en alguno de los nodos o en alguno de los enlaces, no provocaría una catástrofe en la red y, en consecuencia, se logra una arquitectura confiable y veloz. La figura 3.C2 muestra un sencillo ejemplo de la disposición de los elementos de la red SS7 y la manera en que estos elementos forman dos redes interconectadas. Será importante enfatizar ciertas características a las que se hace referencia en el mismo esquema:

- Los STPs W y X llevan a cabo las mismas funciones y, por lo tanto, son parte de la redundancia de la arquitectura. Lo mismo sucede para el par de STPs Y y Z.

- Cada SSP cuenta con dos enlaces, uno a cada STP. La señalización SS7 al resto del mundo se envía a través de cualquiera de estos enlaces, por lo que se observa aún más redundancia.

- Los STPs que forman un par entre sí, se unen mediante un enlace.

- Dos pares de STPs siempre se encuentran interconectados entre sí.
- Al igual que los STPs, los SCPs se implementan en pares. Sin embargo, no existe un enlace que una los puntos de control que forman un par.
- Siempre existe una señalización indirecta asociada a los elementos de ambas redes interconectadas.

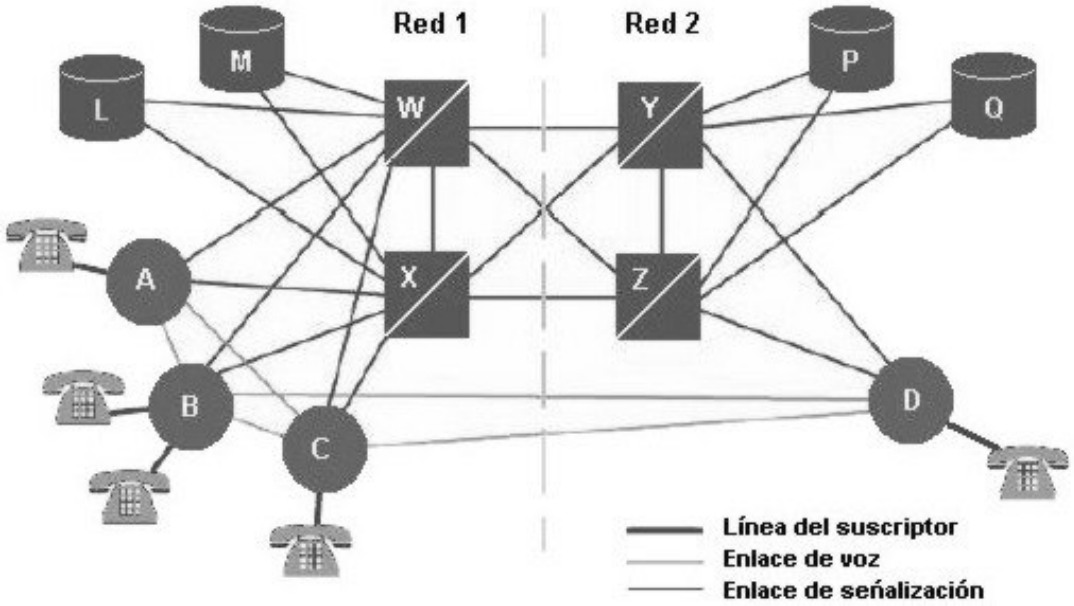


Figura 3.C2. Arquitectura SS7

A partir de la figura anterior se observan dos diferentes tipos de enlace: los enlaces de voz y los enlaces de señalización. Los enlaces de señalización son similares en cuanto a que se trata de líneas bidireccionales que utilizan las mismas capas más bajas del protocolo, pero difieren de acuerdo a su uso en la red telefónica. Básicamente se tienen enlaces A, B, C, D, E y F, aunque existe una categoría que integra los enlaces B y D, conocidos como enlaces B/D. Los enlaces A utilizan esta letra para denotar el "acceso" y unen puntos terminales de señalización, es decir, un STP con un SSP o con un SCP. Ejemplos de este tipo de enlaces son los formados por los nodos AX, AW o PY. Un SSP o SCP que desea comunicarse con su STP puede establecer la señalización a través de cualquiera de sus enlaces tipo A.

Los enlaces B, D y B/D se utilizan para interconectar dos pares de STPs y su función consiste en llevar los mensajes de señalización más allá del área descrita por su red. Los enlaces B toman su nombre a partir del término en inglés "bridge", que traducido al español se refiere al "puente" que se forma entre dos STPs que no forman un par. Ejemplos de estos enlaces son los que unen los nodos WY y WZ. La letra D en este otro tipo de enlaces denota que éstos son "diagonales" y su función consiste en interconectar pares de STPs a diferentes niveles jerárquicos. Sin embargo, debido a que no existe una jerarquía asociada bien definida, los enlaces B y D suelen considerarse dentro de la categoría B/D. Los enlaces C unen los dos STPs que forman un par y se utilizan para garantizar la confiabilidad de la arquitectura, en el caso en que uno o más enlaces de otro tipo no se encuentren disponibles. La letra C se refiere a un enlace "cruzado" y como ejemplo tenemos el enlace WX.

Así como los enlaces A conectan un SSP con su STP local correspondiente, existe otro tipo de enlace que es opcional y cuya función es unir un SSP con el STP de otra red para ofrecer

un respaldo en la conectividad. A estos enlaces se les conoce como "extendidos", motivo por el cual se les ha asignado la letra E. Estos enlaces no se muestran en la figura 3.C2.

Finalmente, se tienen los enlaces F cuya función es unir dos SSPs, normalmente de la misma red, permitiendo únicamente una señalización asociada. La letra utilizada para designar este tipo de enlaces denota una unión "fully associated", es decir, "completamente asociada". El enlace entre los nodos AB es un ejemplo de esta clase de uniones.

Como ya hemos visto, la arquitectura de red SS7 consiste en un conjunto interconectado de elementos que intercambian mensajes para llevar a cabo funciones de señalización. El protocolo SS7, que en realidad no es uno solo, sino una agrupación de ellos, fue diseñado para facilitar dichas funciones y para mantener la red sobre la cual se ofrecen estos servicios. Al igual que muchos otros protocolos recientes, SS7 se encuentra dividido en capas y presenta similitudes con el modelo OSI. La figura 3 muestra cuáles son las capas que integran el modelo SS7.

3. D Especificaciones para los enlaces por ISDN, por enlace dedicado y por redes

Pruebas con Gatekeeper en RVCUDI

El procedimiento que se describe a continuación tiene por objetivo faciltar a los miembros de la Red de Videoconferencia de la Corporación Universitaria para el Desarrollo de Internet (RVCUDI) la generación de pruebas de conectividad por IP/H.323 así como optimizar los planes de marcación con E.164.

IMPORTANTE: Este esquema de pruebas de conectividad sólo está disponible para sitios que estén registrados en la RVCUDI. El VNOC y los administradores de gatekeepers regionales y locales se reservan el derecho de dar de baja cualquier sitio no autorizado.

Conceptos fundamentales

Sistema Terminal: Equipo de videoconferencia (CODEC). Último nivel de registro en el esquema de marcación E.164. Puede registrarse ante un gatekeeper local (su identificador E.164 será entonces de cuatro dígitos), a la ausencia de éste ante un gatekeeper regional (su identificador E.164 será entonces de siete u ocho dígitos, dependiendo de que el gatekeeper regional administre un prefijo de zona - código de área de 2 o tres dígitos) y a la ausencia de éste ante el gatekeeper del VNOC RVCUDI (su identificador E.164 será entonces de 10 dígitos).

Gatekeeper Local: Sistema de administración de llamadas H.323 y definición de zonas asociado a una institución exclusivamente. Puede registrar sistemas terminales dentro de la institución, registrarse a si mismo como dependiente de un gatekeeper regional y validarse ante los gatekeepers dentro de esa región, conformando una vecindad de gatekeepers. Ante la ausencia de un gatekeeper regional se registrará ante el gatekeeper VNOC RVCUDI. Su prefijo de zona puede ser de tres a cuatro dígitos (equivalentes a los dígitos de la marcación telefónica convencional hacia la institución - esto al registrarse ante un gatekeeper regional) o de 6 dígitos (el código de área y los dígitos de marcación a la institución - esto al registrarse directamente con el gatekeeper VNOC RVCUDI por la ausencia de un gatekeeper regional).

Gatekeeper Regional: Sistema de administración de llamadas H.323 y definición de zonas asociado a una región que puede comprender una o más instituciones. Puede registrar sistemas terminales y gatekeepers locales y registrarse a si mismo como dependiente del gatekeeper VNOC RVCUDI. Así también puede validarse ante otros gatekeepers regionales conformando vecindad de gatekeepers. Su prefijo de zona puede ser de dos a tres dígitos (equivalentes a los dígitos del código de área telefónico convencional).

Gatekeeper VNOC RVCUDI: Sistema de administración de llamadas H.323 y definición de zonas en la Red de Videoconferencia CUDI a nivel nacional que comprende sistemas terminales, gatekeepers locales y gatekeepers regionales. Puede validarse ante otros gatekeepers nacionales conformando vecindad de gatekeepers nacionales para facilitar la marcación y servicios H.323 a nivel mundial. Su prefijo de zona es de dos dígitos: 52, correspondientes al código de país asignado a México en la telefonía convencional. La dirección IP del gatekeeper VNOC RVCUDI es la 132.248.120.10 y el código de servicio disponible para pruebas es el 60.

Requisitos técnicos para equipos terminales:

1. Sistema de videoconferencia compatible con la norma H.323 V2.0 o superior (No están autorizados sistemas personales del tipo NetMeeting o Messenger).
2. Conexión a Internet 2 con al menos 384Kbps garantizados.
3. Dirección IPv4 pública y homologada (No están autorizadas IP detrás de NAT).

Requisitos técnicos para gatekeepers regionales y locales:

1. Gatekeeper compatible con la norma H.323 V2.0 o superior.
2. Conexión a Internet 2 con al menos 384Kbps garantizados.
3. Dirección IPv4 pública y homologada (No están autorizadas IP detrás de NAT).

Registró se sistemas terminales:

1. Identificar si existe un gatekeeper local o regional. En caso de no existir uno u otro, en las opciones de configuración del sistema terminal, registrar la dirección IP del Gatekeeper VNOC RVCUDI: 132.248.120.10
2. Establecer un identificador E.164 (númerico):
   - Para sistemas dentro de la Ciudad de México y Zona Metropolitana. El identificador E.164 deberá incluir el Código de Área (55), los cuatro dígitos iniciales de la marcación telefónica a la institución y cuatro dígitos progresivos para los sistemas de videoconferencia (iniciando con 0000). El Identificador E.164 constará en total de 10 dígitos.

     Ejemplo: El primer sistema registrado en la UNAM tendrá el siguiente Identificador E.164: 5556220000, donde 55 es el código de área de la Ciudad de México, 5622 los dígitos para marcación a números telefónicos en la UNAM y 0000 los dígitos correspondientes al primer sistema de VC con ID E.164.

   - Para sistemas fuera de la Ciudad de México y Zona Metropolitana.

     a. Registro con un Gatekeeper Local. Si ya existe un gatekeeper local asociado a un gatekeeper regional o al gatekeeper del VNOC RVCUDI el sistema terminal se deberá registrar con ese gatekeeper local y su identificador E.164 deberá constar solamente de cuatro dígitos progresivos para los sistemas de videoconferencia (asignando 0000 para el primer sistema, 0001 para el segundo, etc).

     b. Registro con un Gatekeeper Regional. Si ya existe un gatekeeper regional pero no uno local, el sistema terminal se deberá registrar con ese gatekeeper regional y su identificador E.164 deberá constar de tres a cuatro dígitos, correspondientes a los dígitos iniciales de la marcación telefónica convencional a la institución a la que pertenece más cuatro dígitos progresivos para los sistemas de videoconferencia (asignando 0000 para el primer sistema, 0001 para el segundo, etc). El identificador E.164 será entonces de siete u ocho dígitos, en función de la longitud del prefijo de zona - código de área que administre el gatekeeper regional (tres o dos dígitos respectivamente).

     c. Registro con el gatekeeper VNOC RVCUDI. Si no existe un gatekeeper local o regional se podrá dar de alta en el Gatekeeper del VNOC RVCUDI y su identificador E.164 deberá incluir el Código de Área (dos a tres dígitos) los tres o cuatro dígitos iniciales de la marcación telefónica a la institución y cuatro dígitos progresivos para los sistemas de videoconferencia (iniciando con 0000). El Identificador E.164 constará en total de 10 dítgitos.

IMPORTANTE: Por el momento no existen gatekeepers regionales. Conforme se vaya realizando el registro de gatekeepers regionales en el gatekeeper del VNOC RVCUDI se listarán en este sitio web.

3. Guardar los cambios de configuración y, preferentemente, reiniciar el sistema terminal.
4. Revisar que el sistema esté registrado en el gatekeeper. Algunos sistemas lo indican en la primera pantalla de la interfaz, otros requieren del acceso a la configuración de gatekeeper para revisar el adecuado registro.

Registro de gatekeeper local:

1. Identificar la existencia de un gatekeeper regional. A la ausencia de éste, en las opciones de configuración del gatekeeper, registrar la dirección IP del Gatekeeper VNOC RVCUDI: 132.248.120.10 como gatekeeper maestro.
2. Asignar como prefijo de zona H.323 (equivalente a código de área) el correspondiente a la marcación telefónica local. Este será el prefijo que administrará el gatekeeper local y será heredado en los identificadores E.164 a todos los sistemas que se registren en el gatekeeper local. Podrá tener una extensión de tres a cuatro dígitos si el registro es con un gatekeeper regional o de seis dígitos si el registro es con el gatekeeper VNOC RVCUDI.
3. Guardar la configuración y, preferentemente, reiniciar el sistema.
4. Revisar que el gatekeeper local ha sido reconocido por el gatekeeper regional o el gatekeeper VNOC RVCUDI. En caso de error revisar que no exista otro gatekeeper local ya registrado con el mismo prefijo de zona o código de área.

Registró de gatekeeper regional en el gatekeeper de VNOC RVCUDI:

1. En las opciones de configuración del gatekeeper, registrar la dirección IP del Gatekeeper VNOC RVCUDI: 132.248.120.10 como gatekeeper maestro.
2. Asignar como prefijo de zona H.323 (equivalente a código de área) el correspondiente a la marcación telefónica local. Este será el prefijo que administrará el gatekeeper regional y será heredado en los identificadores E.164 a todos los sistemas que se registren en el gatekeeper regional. Podrá tener una extensión de dos a tres dígitos.
3. Guardar la configuración y, preferentemente, reiniciar el sistema.
4. Revisar que el gatekeeper regional ha sido reconocido por el gatekeeper VNOC RVCUDI. En caso de error revisar que no exista otro gatekeeper regional ya registrado con el mismo prefijo de zona o código de área.

Marcación:

1. Local Punto a Punto.

   Para pruebas de marcación hacia sistemas de videoconferencia H.323 dentro de la misma zona (registrados en el mismo gatekeeper local) basta con marcar al número de extensión del sistema (4 dígitos).

2. Local Multipunto.

En caso de que el gatekeeper local tenga definidos servicios de multipuntos, se deberá marcar el código de servicio correspondiente por parte de cada uno de los sitios que participarán en la prueba multipunto. Por ejemplo: si el código 60 corresponde a una videoconferencia multipunto de hasta 4 sitios a 384Kbps con presencia continua, cada sitio deberá marcar exclusivamente el código 60 para acceder a la conferencia multipunto. Se consultará con el administrador del gatekeeper local los códigos de servicio válidos en esa zona H.323.

3. Regional Punto a Punto.

   Para pruebas de marcación hacia sistemas de videoconferencia H.323 dentro de la misma región (registrados en el mismo gatekeeper regional) basta con marcar al número de terminal que deberá constar de los tres o cuatro dígitos de marcación telefónica convencional más la extensión del sistema (4 dígitos), esto es: un total de siete u ocho dígitos. Por ejemplo: para marcar a un sistema dentro de la misma región con número de institución 8885 y extensión H.323 0001 se digitará 88850001, sin necesidad de anteponer el código de área.

4. Regional Multipunto.

   En caso de que el gatekeeper regional tenga definidos servicios de multipuntos, se deberá marcar el código de servicio correspondiente por parte de cada uno de los sitios que participarán en la prueba multipunto. Por ejemplo: si el prefijo de zona - código de área del gatekeeper regional es 81 y el código 60 corresponde a una videoconferencia multipunto de hasta 4 sitios a 384Kbps con presencia continua cada sitio deberá marcar exclusivamente el 8160 para acceder a la conferencia multipunto dentro de la misma región. Se deberá consultar con el administrador del gatekeeper regional los códigos de servicio válidos en esa zona H.323.

5. Nacional Punto a Punto.

   Para pruebas de marcación hacia sistemas de videoconferencia H.323 dentro del mismo país (registrados en el gatekeeper VNOC RVCUDI) basta con marcar al número de terminal que deberá constar del código de área - prefijo de zona más los tres o cuatro dígitos de marcación telefónica convencional más la extensión del sistema (4 dígitos), esto es: invariablemente un total de 10 dígitos. Por ejemplo: para marcar a un sistema en la RVCUDI con código de área 99, número de institución 8885 y extensión H.323 0001 se digitará 9988850001, sin necesidad de anteponer el código de país.

6. Nacional Multipunto.

   El gatekeeper VNOC RVCUDI tiene disponible para efecto de pruebas el código de servicio 60. Si un sitio ya registrado en alguno de los niveles de gatekeepers marca el código 5260 accederá de inmediato a una conferencia multipunto de hasta 4 sitios a 384Kbps, 30 cuadros por segundo y H.263 en protocolo de video. Los demás sitios que deseen participar en la prueba deberán estar validados en la estructura de gatekeepers y marcar el mismo código. Una vez finalizadas las pruebas del esquema de marcación E.164 se darán a conocer los códigos de servicio para otras configuraciones y capacidades.

NOTA: Si no hay otros sitios en RVCUDI realizando pruebas con el servicio 60, el sitio que esté ingresando al servicio recibirá su propia imagen (loop de video) sin retorno de audio.

Dudas o comentarios: Fabián Romo (VNOC RVUNAM RNVE RVCUDI)

Especificaciones Técnicas: Conexión H.320 por ISDN

A continuación de definen los requisitos técnicos para conexiones por norma H.320 hacia la Red UNAM de videoconferencia (RVUNAM), la Red Nacional de Videoconferencia para la Educación (RNVE) y la Red de Videoconferencia CUDI (RVCUDI) a través de enlaces ISDN.

Última actualización: 4/08/2003

Enlaces digitales:

- Tipo de enlace: Euro ISDN o National ISDN-1.
- Ancho de banda mínimo: 1BRI (128 kbps).
- Ancho de banda estándar: 3BRI (384 kbps).
- Ancho de banda máximo: 1PRI (2.048 Mbps).
- Agregación de canales: Bonding 1.

NOTA: No se aceptan enlaces con números no homologados

Equipo de comunicación:

- NT1 con interfaz U/ST para conexión al sistema de videoconferencia.
- Cables RJ45 para ISDN

Equipo de videoconferencia.

CODEC que cumpla con el estándar H.320 de la ITU-T:

- Algoritmos de compresión de video: H.261 y H.263.
- Algoritmos de compresión de audio: G.711a, G.711u, G.722 y G.723
- Algoritmos de comunicaciones: H.221.

Equipo adicional:

- Monitores y/o proyectores.
- Micrófonos de mesa e inalámbricos.
- Videocasettera VHS.
- Reproductor de DVD Multiregión.
- Mezcladora de audio de 4 canales (opcional).
- Amplificador de audio (opcional).

Especificaciones Técnicas:
Conexión H.320 por enlace dedicado

A continuación de definen los requisitos técnicos para conexiones por norma H.320 hacia la Red UNAM de videoconferencia (RVUNAM), la Red Nacional de Videoconferencia para la Educación (RNVE) y la Red de Videoconferencia CUDI (RVCUDI)

Última actualización: 4/08/2003

Enlaces digitales:

- Tipo de enlace: Digital estándar europeo (E1 o E0's).
- Punta A: Sitio solicitante.
- Punta B: Zona Cultural, Ciudad Universitaria. México D,F.
- Ancho de banda mínimo: 2E0´s (128 kbps).
- Ancho de banda estándar: 6E0´s (384 kbps).
- Ancho de banda máximo: 1E1 (2.048 Mbps).

NOTA: No se aceptan enlaces del tipo DS0

Equipo de comunicación:

- En el sitio solicitante, si el enlace se proporciona por cable coaxial:
  - 1 FCD-E1(convertidor de interfaz).
  - 1 cable V.35 macho a RS-449 macho.
- Si el enlace se proporciona por fibra óptica:
  - 1 FOM-40 (módem de fibra óptica).
  - 1 cable V.35 macho a RS-449 macho.
- En el Centro de Operaciones de Videoconferencia (VNOC) de la UNAM:
  - 2 FCD-E1 (convertidor de interfaz).
  - 2 FOM-40 (módem de fibra óptica).
  - 1 cable V.35 macho a RS-449 macho.
  - 1 puerto de unidad multipunto.

En el caso de enlaces compartidos (videoconferencia, datos y/o voz) agregar un FCD –24 en el sitio solicitante y un FCD – 24 en la VNOC UNAM, para todos los escenarios descritos.

Equipo de videoconferencia:

CODEC que cumpla con el estándar H.320 de la ITU-T:

- Algoritmos de compresión de video: H.261 y H.263.
- Algoritmos de compresión de audio: G.711a, G.711u, G.722 y G.723
- Algoritmos de comunicaciones: H.221.

Equipo adicional:

- Monitores y/o proyectores.
- Micrófonos de mesa e inalámbricos.
- Videocasettera VHS.
- Reproductor de DVD Multiregión.
- Mezcladora de audio de 4 canales (opcional).
- Amplificador de audio (opcional).

Especificaciones Técnicas:
Conexión H.323 en redes conmutadas por paquetes (IP)

A continuación de definen los requisitos técnicos para conexiones por norma H.323 hacia la Red UNAM de videoconferencia (RVUNAM), la Red Nacional de Videoconferencia para la Educación (RNVE) y la Red de Videoconferencia CUDI (RVCUDI) a través de redes conmutadas por paquetes (IP), como Internet e Internet2.

Última actualización: 4/08/2003

Enlace

- Red conmutada por paquetes (IP), Internet o Internet 2.
- Ancho de banda mínimo: 64 kbps.
- Ancho de banda estándar: 384 kbps.
- Ancho de banda máximo: 2.048 Mbps.
- Calidad de Servicio: Requerida. Precedencia 1.

NOTA: No se garantiza la conexión con direcciones IP no homologadas o detrás de un NAT (Network Address Translation)

Comunicaciones

- TCP/IP. IPv4 e IPv6.
- Cableado estrucurado Categoría 5 o superior-
- Red local conmutada (switch) a 100 Mbps.
- Registro en un gatekeeper de la RVUNAM, RNVE o RVCUDI. Asignación de extensión y zona de marcación.

Equipo de videoconferencia:

CODEC que cumpla con el estándar H.323 de la ITU-T:

- Algoritmos de compresión de video: H.261, H.263 y H.264.
- Algoritmos de compresión de audio: G.711a, G.711u, G.722 , G.723a, G.723b y G.728.
- Algoritmos de comunicaciones: Sobre TCP/IP.

NOTA: No se garantiza la calidad de la conexión si algún sitio dentro de la conferencia usa funciones no estándares, como DuoVideo, Presencia Continua, el Anexo D del H.261 para envío de diapositivas y SpeedMatching.

Equipo adicional:

- Monitores y/o proyectores.
- Micrófonos de mesa e inalámbricos.
- Videocasettera VHS.

- Reproductor de DVD Multiregión (opcional)
- Mezcladora de audio de 4 canales (opcional).
- Amplificador de audio (opcional).

5. A Procedimientos de control del área de redes

Tanto las políticas como procedimientos de control mínimos, que deben existir en el área de redes, se describen en la Tabla No. 5.1.

Área de Revisión: Redes	**Comentarios**
1. Justificación formal de la instalación de una red de comunicación.	Procedimiento Obligatorio
2. Planeación formal de las etapas de implantación de la red.	Procedimiento Obligatorio
3. Documento que indique cómo administrar y operar la red.	Procedimiento Obligatorio
4. Presencia de un responsable directo de la administración de la red.	Procedimiento Obligatorio
5. Existencia de elementos que justifiquen el software y sistemas que se implantarán en la red local.	Procedimiento Obligatorio
6. Instalación exclusiva de software original (legalizada en la red).	Procedimiento Obligatorio
7. Existirá una definición formal de usuarios que tendrán acceso a la red.	Procedimiento Obligatorio
8. Procedimientos de respaldo de la información manejada en la red local.	Procedimiento Obligatorio
9. Procedimientos que no permitan accesos no autorizados a la red local.	Procedimiento Obligatorio
10. Procedimientos de respaldo de datos y equipo de cómputo de la red local.	Procedimiento Obligatorio
11. Políticas que limiten el uso de la red local por perfil de usuario.	Procedimiento Obligatorio
12. Procedimientos de uso de la red local, entrada, operación y salida.	Procedimiento Obligatorio
13. Procedimientos de seguridad al conectarse con otras redes.	Procedimiento Obligatorio
14. Planes de implantación, conversión y pruebas de aceptación para la red.	Procedimiento Obligatorio
15. Existencia de un grupo de control de red.	Procedimiento Obligatorio
16. Procedimientos que definan las medidas de seguridad en la red.	Procedimiento Obligatorio
17. Existencia de un inventario de los activos de la red.	Procedimiento Obligatorio
18. Métodos de monitoreo de la red, para medir su eficiencia.	Procedimiento Obligatorio
19. Políticas de recuperación e inicio.	Procedimiento Obligatorio
20. Políticas de adquisición y uso del equipo	Procedimiento Obligatorio

Tabla No. 5.1 Políticas y procedimientos de control en redes

La Tabla No. 5.2 presenta una lista de verificación de políticas y procedimientos para el área de telecomunicaciones.

Área de Revisión: Telecomunicaciones	Comentarios
1. Justificación formal de la instalación de una red de comunicación.	Procedimiento Obligatorio
2. Planeación formal de las etapas de implantación de la red.	Procedimiento Obligatorio
3. Documento que indique cómo administrar y operar la red (routers, módems, medios de transmisión, accesos, etc.)	Procedimiento Obligatorio
4. Presencia de un responsable directo de la administración de la red.	Procedimiento Obligatorio
5. Existencia de elementos que justifiquen el software y sistemas que se implantarán en la red local.	Procedimiento Obligatorio
6. Debe haber datos que justifiquen la integración de un equipo de red.	Procedimiento Obligatorio
7. Procedimientos de integración a la red de equipos autorizados por el administrador.	Procedimiento Obligatorio
8. Procedimientos de definición de usuarios con acceso a la red.	Procedimiento Obligatorio
9. Políticas de seguridad para los datos manejados en la red.	Procedimiento Obligatorio
10. Procedimientos de respaldo de datos y equipo de la red.	Procedimiento Obligatorio
11. Políticas que limiten el uso de la red por perfil de usuario.	Procedimiento Obligatorio
12. Procedimientos de uso de la red entrada, operación y salida.	Procedimiento Obligatorio
13. Procedimientos de seguridad al conectarse con otras redes.	Procedimiento Obligatorio
14. Procedimiento de respaldo de la tecnología de la red.	Procedimiento Obligatorio
15. Políticas que apoyan el mantenimiento y reemplazo de la red.	Procedimiento Obligatorio

Tabla No. 5.2 Políticas y procedimientos de control en telecomunicaciones

5. B Procesos del plan de auditoría

1. Proceso de planeación de negocios, determina las estrategias y cursos de acción del negocio, mediante entrevistas y análisis detallados de cada proceso básico de la organización, entre los ejemplos de procesos básicos encontramos:
   - Auditoría, finanzas, administración, ventas y compras en una empresa.
   - Recursos humanos, producción y administración de la manufactura.
2. Proceso de planeación en informática, define el conjunto de proyectos relacionados con la función de informática en tiempos de corto, mediano y largo plazo. Cada proyecto debe estar orientado a cubrir los objetivos definidos en el plan de negocios.

   La Tabla No.5.3 muestra las tareas básicas del proceso de planeación en informática así como los responsables de ejecución.

Actividad	Responsable de Ejecución	Responsable de Seguimiento	Comentarios
Determinación de áreas apoyadas por informática, basados en el plan de negocios	Coordinador o supervisor de planeación informática	Director o gerente de informática	Las áreas de oportunidad relativas al negocio así como los proyectos específicos solicitados o recomendados por asesores externos, emanan del plan de negocio.
Elaboración del plan de informática	Coordinador o supervisor de planeación informática	Director o gerente de informática	Es importante que la función responsable de ejecutar cada proyecto se involucre en esta tarea, por ejemplo el área de comunicaciones, el área de desarrollo, etc.
Presentación del plan a la alta dirección	Director o gerente de informática	Alta dirección del negocio	Antes de presentar el documento se verifica que exista un análisis costo/beneficio de cada proyecto, así como las fechas de terminación.
Ejecución del plan de auditoría	Funciones de informática: Desarrollo, Investigación, Comunicaciones, Soporte a Usuarios, etc.	Gerente o supervisores de cada área	

Tabla No. 5.3 Tareas básicas del proceso de planeación en informática

3. Proceso de planeación de la auditoría, define el conjunto de proyectos de evaluación y verificación de políticas, controles y procedimientos pertenecientes a todas las áreas con el objetivo de asegurar un buen manejo y administración de los recursos de la organización.

   La Tabla No. 5.4 muestra las tareas básicas del proceso de planeación en informática así como los responsables de ejecución.

Actividad	Responsable de Ejecución	Responsable de Seguimiento
Determinación de las áreas por auditar en el negocio	Coordinador o supervisor de auditoría	Director o gerente de auditoría
Elaboración del plan de auditoría	Coordinador o supervisor de auditoría	Director o gerente de auditoría
Presentación del plan a la alta dirección	Director o gerente de informática	Alta dirección del negocio
Ejecución del plan de auditoría	Supervisor o auditores externos o internos	Gerente o supervisores de cada área

Tabla No. 5.4 Tareas básicas del proceso de planeación en auditoría

   El proceso de planeación de la auditoría informática, depende del diagnóstico previo que realice el auditor en informática sobre la situación existente en la organización, en cuanto a las diferentes áreas de la informática, considerando las prioridades de la alta dirección.

4. Proceso de la auditoría informática, incluye la definición y formalización de proyectos abarcando actividades desarrolladas por el auditor informático cuyo objetivo principal, es el aseguramiento de la calidad y control de los elementos que se encuentran relacionados con los recursos de la informática.

   La Tabla No. 5.5 presenta una descripción breve de las actividades desempeñadas en esta etapa.

Actividad	Responsable de Ejecución	Responsable de Seguimiento
Determinación de las áreas por auditar en el negocio	Coordinador o supervisor de auditoría informática	Director o gerente de auditoría en informática
Elaboración del plan de auditoría en informática	Coordinador o supervisor de auditoría en informática	Director o gerente de auditoría
Presentación del plan a la alta dirección	Director o gerente de informática	Alta dirección del negocio
Ejecución del plan de auditoría en informática	Supervisor o auditores externos o internos	Gerente o supervisores de cada área

Tabla No. 5.5 Tareas básicas del proceso de planeación en auditoría informática

5. C Actividades dentro del proceso de planeación en la auditoría de redes

La Tabla No. 5.6 presenta las actividades realizadas durante el proceso de planeación en la auditoría de redes.

Etapa	Funciones	Actividades Detalladas
Planeación	Implica la definición de un plan formal que contempla:	
	Evaluación del hardware actual	• Análisis y evaluación de la red actual. Análisis y diagnóstico del número de computadoras y periféricos.
	Evaluación del software actual	• Análisis y diagnóstico del software instalado en la red o computadoras: graficadores, procesadores de texto, hojas electrónicas, etc. • Lenguajes de programación, sistemas operativos, etc. • Licencias, copias "piratas", versiones, número de usuarios. • Software por legalizar.
	Estudio para justificar la instalación o reemplazo de la red	• Hardware requerido: computadores, periféricos, etc. • Configuración de la red: distribución física, interfases, etc. • Software requerido: aspectos legales, paquetes de cómputo, lenguajes de programación, sistemas operativos, etc. • Evaluación costo-beneficio • Procedimientos e capacitación, seguridad, mantenimiento, operación, monitoreo, etc.

Tabla No. 5.6 Actividades realizadas durante la planeación de una auditoría de redes

5. D Estándares de la auditoría informática

1. Planificación y organización, permite identificar la forma en que la tecnología contribuye al cumplimiento de los objetivos institucionales, así como el establecimiento de una organización e infraestructura tecnológica adecuada.
2. Adquisición e implementación, incluye la identificación, desarrollo y adquisición de soluciones adecuadas, así como su implementación. Cubre los cambios y el mantenimiento realizado a los sistemas existentes.
3. Distribución y soporte, corresponde a la entrega de los servicios requeridos, desde las tradicionales operaciones sobre seguridad y continuidad, hasta la capacitación, así como el soporte necesario.
4. Monitoreo, los procesos requieren ser evaluados de manera continua para verificar su calidad y suficiencia en cuanto a requerimientos de control.

5. E Diferentes topologías de red

a. Topología en bus y anillo

En las topologías en bus y anillo se comparte un medio multipunto debido a que todas las estaciones se encuentran directamente conectadas a través de interfases físicas apropiadas, conocidas como tomas de conexión, a un medio de transmisión lineal o bus.

En una topología en bus, el funcionamiento full-duplex entre la estación y la toma de conexión permite la transmisión y recepción de datos por medio del bus. Una transmisión desde cualquier estación se propaga a través del medio en ambos sentidos y es recibida por el resto de las estaciones, en cada extremo del bus existe un terminador que absorbe las señales eliminándolas del bus. Una ventaja de esta topología es la modularidad y adaptabilidad, pues resulta sencillo añadir o retirar estaciones de red.

En la topología de árbol, se tiene una generalización de la topología en bus, el medio de transmisión es un cable ramificado sin bucles cerrados, comenzando en una raíz.

En la topología anillo, la red consta de un conjunto de repetidores unidos por enlaces punto a punto formando un bucle cerrado. Cada estación se conecta a la red mediante un repetidor transmitiendo los datos hacia la red a través de él, en forma de tramas que circulan por el anillo pasando por las demás estaciones, de modo que la estación de destino reconoce su dirección y copia la trama, mientras ésta la atraviesa, en una memoria temporal local. La trama continúa circulando hasta que alcanza de nuevo la estación origen donde es eliminada del medio. Debido a que el anillo es compartido por varias estaciones se necesita una técnica de control de acceso al medio para determinar cuando puede insertar tramas cada estación.

Una topología en anillo puede ser usada para proporcionar enlaces de muy alta velocidad sobre distancias largas, debido a que un anillo puede proporcionar potencialmente mejor rendimiento que cualquier otra topología. Sin embargo una desventaja es que el fallo de un solo enlace o de un repetidor puede inutilizar la red entera.

b. Topología en estrella

En esta topología cada estación está directamente conectada a un nodo central común, generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción. Existen dos alternativas para el funcionamiento del nodo central:

1. Modo difusión, la transmisión de una trama por parte de una estación se retransmite sobre todos los enlaces de salida del nodo central. En este caso, aunque la disposición física es una estrella, lógicamente funciona como un bus: una transmisión desde cualquier estación es recibida por el resto de estaciones y únicamente puede transmitir una estación en un instante de tiempo dado. En este modo, el dispositivo central recibe el nombre de concentrador o hub.
2. Modo de conmutación de tramas, en este el modo, el nodo central funciona como dispositivo de conmutación de tramas. Una trama entrante se almacena temporalmente en el nodo y se retransmite sobre un enlace de salida hacia la estación destino.

c. Elección de la topología

La elección de la topología depende de diversos factores entre los que se encuentran la fiabilidad de la misma, la capacidad de expansión y sobre todo el rendimiento. Esta elección forma parte del proceso global de diseño de una red, por lo que debe llevarse a cabo con la elección del medio de transmisión, la disposición del cableado y la técnica de control de acceso.

6. A Organizaciones de estandarización

En la industria de las comunicaciones se aceptó la necesidad de los estándares, para definir las características físicas, eléctricas y de procedimiento de los equipos de comunicación. Este punto de vista, no era compartido por la industria de las computadoras.

Los fabricantes de equipos de comunicación comprendieron que sus equipos debían interconectarse y comunicarse con equipos desarrollados por terceros, mientras que los fabricantes de computadoras han intentado monopolizar a sus usuarios.

La existencia de diferentes computadoras y la proliferación del procesamiento distribuido, han desencadenados una situación insostenible. Las computadoras de diferentes fabricantes deben comunicarse entre sí, sin necesidad de que los clientes tengan que desarrollar o adquirir software para adaptar protocolos de uso específico.

Como consecuencia la normalización se está imponiendo en todas las áreas tecnológicas.

Existen una serie de ventajas y desventajas del proceso de estandarización. Entre las principales ventajas resaltan:

- La existencia de un estándar para un software o equipo dado asegura potencialmente un gran mercado, lo que estimula la producción masiva y en algunos casos el uso de integración a gran escala o integración a muy gran escala, reduciendo los costos.
- Un estándar permite que los productos de diferentes fabricantes se comuniquen, dotando al comprador de flexibilidad en la selección y uso de equipos.

Entre las principales desventajas tenemos:

- Los estándares tienden a estancar a la tecnología. Mientras son revisados y adaptados, es posible desarrollar otras técnicas más eficientes.
- Existen una gran cantidad de estándares para la misma función lo que llega a provocar conflicto entre ellos.

Las organizaciones más importantes que se encargan de desarrollar las normalizaciones son:

1. Asociación de Internet

La ISOC, Asociación Internet (Internet Society) es una asociación profesional conformada por más de 150 organizaciones y 6000 miembros individuales de más de 100 países. Lidera el planteamiento de las cuestiones que afectan al futuro de Internet, a la vez que es el organismo en torno al cual se organizan los grupos responsables de la normalización en Internet. A ésta pertenecen, entre otros los siguientes comités:

- IAB, Comité de Arquitectura de Internet (Internet Arquitectura Board)
- IETF, Comité de Ingeniería de Internet (Internet Engineering Task Force)

La ISOC, desarrolla los RFC y normas en Internet.

2. IEEE 802

Comité para las Normas 802 LAN/MAN de IEEE, Instituto de Ingenieros Eléctricos Electrónicos, (Institute of Electrical and Electronics Engineers). Desarrolla los estándares para las redes de área local y redes de área metropolitana. Los estándares más utilizados son los correspondientes a la familia Ethernet, token ring, LAN inalámbricas, interconexión con puentes y LAN virtuales con puentes.

3. Forum ATM

El Forum ATM, es una organización internacional sin ánimo de lucro cuyo objetivo es la promoción de los productos y servicios de ATM, Modelo de Transferencia Asíncrona (Asynchronous Transfer Mode), mediante especificaciones interoperativas rápidamente convergentes. El Forum promueve la cooperación industrial.

4. ISO

La ISO, Organización Internacional de Estandarización (Internacional Organization for Standardization) es una federación mundial de organismos nacionales de normalización de más de 140 países. Es una organización no gubernamental que promueve el desarrollo de la normalización y actividades relacionadas con la intención de facilitar el intercambio internacional de bienes y servicios, unido al desarrollo de la cooperación en los ámbitos intelectual, científico, tecnológico y económico. El trabajo ISO consiste en el establecimiento de acuerdos internacionales que se publican como Normas Internaciones.

5. TMForum

Organización integrada por más de 400 miembros (proveedores, integradores, etc.) cuyo objetivo primordial se centra en la definición de estándares que permitan la administración y automatización de los procesos de negocios.

6. ETSI

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 1
Configuración Básica de Redes

1.- Objetivo de aprendizaje

El alumno conocerá e identificará elementos que conforman una red de computadoras, así como las políticas y ética que rigen sobre el cómputo.

El alumno adquirirá la capacidad del manejo de los comandos adecuados para la configuración del hardware, protocolos y software asociado a las redes locales de computadoras en los sistemas operativos Linux y Windows.

2.- Conceptos teóricos

Una red de computadoras es un sistema de interconexión entre equipos que permite compartir recursos e información, para lo cual es necesario contar no sólo con las computadoras, si no con tarjetas de red, cables de conexión, dispositivos periféricos y el software conveniente.

Inicialmente la instalación de una red se realiza con el objetivo de compartir dispositivos e información, pero a medida que crece permite el enlace entre personas mediante diversas aplicaciones como el correo electrónico, mensajes instantáneos, etc.

Las redes se clasifican de acuerdo a su alcance geográfico en LAN, MAN y WAN. Una red de área local está formada por computadoras, periféricos y los elementos de conexión de los mismos.

Las computadoras pueden desarrollar dos funciones: como servidores o estaciones de trabajo. Los elementos de conexión son los cables, tarjetas de red y los dispositivos de interconectividad como los hubs.

Dentro de los cables de conexión se tienen: el cable UTP que consiste en dos hilos trenzados en forma independiente y recubiertos de una capa aislante, y se considera de fácil instalación; el cable STP consistente en dos hilos trenzados en forma independiente y recubiertos de una malla metálica, ofrece una protección contra las interferencias externas; el cable coaxial, hilo de cobre envuelto en una malla trenzada, separados por una material aislante; y finalmente la fibra óptica, formada por un núcleo de material transparente fino cuyo funcionamiento se basa en la transmisión de las refracciones de luz.

En la actualidad, en el mundo de los sistemas de cableado estructurado existen diferentes tipos de servicios, por ejemplo: voz, datos, video, monitoreo, control de dispositivos, etc., los cuales pueden transmitirse sobre un mismo tipo de cable. El estándar más conocido de cableado estructurado está definido por la EIA/TIA, y específicamente sobre cable de par trenzado UTP de categoría 5 y 5e, estos estándares son: EIA/TIA 568A y EIA/TIA 568B.

Los dispositivos de interconexión proporcionan la capacidad de extender la distancia de cobertura de una LAN, interconectar redes distantes o distintas y acceder a recursos centralizados. De la misma manera reducen los dominios de colisión y mejoran el rendimiento de las redes.

3.- Equipo y material necesario

3.1 Material que debe traer el alumno

- 2 cables de conexión directa configuración T568-B UTP, categoría 5e.
- 2 cables de conexión directa configuración T568-A UTP, categoría 5e.
- 1 cables de conexión cruzada.

3.2 Equipo del Laboratorio

- 2 PC's Pentium con una NIC Ethernet 10/100 Mbps instalada en cada una de ellas.
- Un hub Ethernet 10BaseT o FastEthernet (4 -8) puertos.
- Un switch Ethernet 10BaseT o FastEthernet(24 puertos).
- Flexómetro.

4.- Desarrollo

4.1 Sistema Operativo Windows XP

4.1.1 Conexión punto a punto

Esta primera parte, consiste en crear una red LAN Ethernet entre dos computadoras sin un dispositivo intermedio. Además de las conexiones físicas (capas de enlace de datos y física), será necesario realizar la configuración del protocolo TCP/IP de modo que exista comunicación.

No es necesario un hub o ningún otro dispositivo de red para la interconexión, en esta primera etapa.

Es indispensable iniciar la práctica con todos los dispositivos apagados y el cableado desconectado.

a. Conexión física de las estaciones de trabajo

Realice la conexión entre las dos estaciones de trabajo, mediante un cable cruzado de categoría 5e, desarrollado en la primera práctica del Laboratorio de Redes Datos, conectando los dos extremos del cable a cada NIC, ver Figura 1.1.

Figura 1.1 Conexión punto a punto

Investigue las características del cable empleado en este punto y complete la Tabla No. 1.1, con la información obtenida de acuerdo a los criterios especificados.

Características		Normas aplicables	Aplicaciones
Calibre			
Tipo de aislamiento			
Tipo de ensamble			
Tipo de cubierta			
Conductor			
Diámetro exterior			
Desempeño			
Impedancia			

Tabla No. 1.1 Características de cable UTP

Investigue la estructura de un cable UTP y dibuje un diagrama que muestre los componentes principales.

b. Verificación de la conexión física

Encienda las computadoras, eligiendo como sistema operativo Windows XP. Para verificar las conexiones de las mismas, asegúrese de que estén encendidas las luces de enlace de ambas NIC, ver Figura 1.2.

Figura 1.2 Tarjeta de red

Inicie sesión con la cuenta de Administrador, proporcionada por su profesor de Laboratorio.

c. Configuración de la IP

Seleccione el menú Inicio>Panel de Control>Conexiones de red, ver Figuras 1.3 y 1.4.

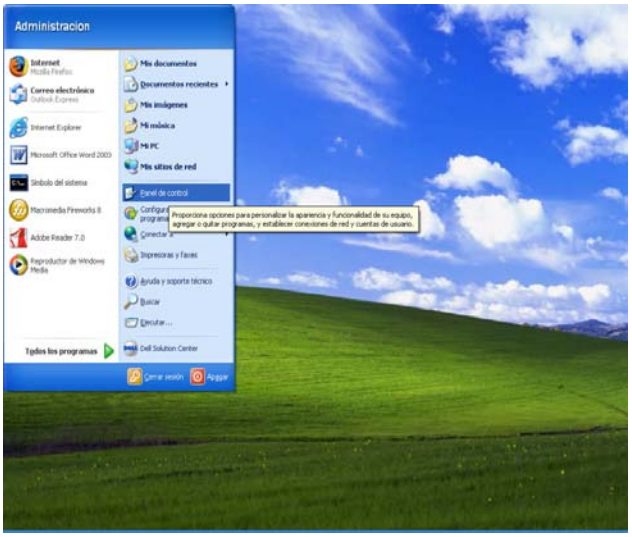


Figura 1.3 Panel de control

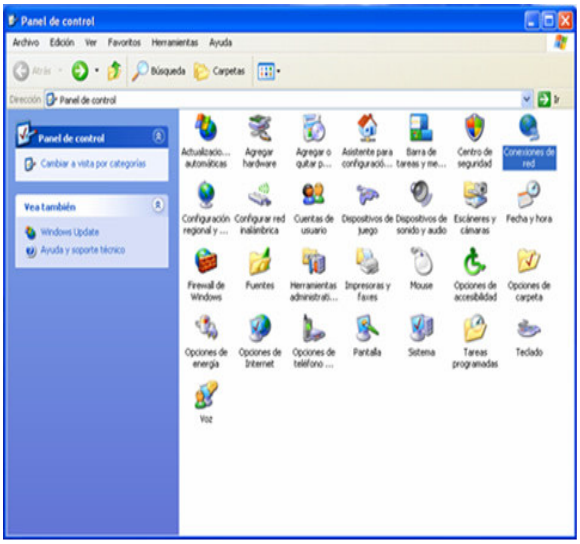


Figura 1.4 Conexión de red

En esta opción es posible configurar tanto las conexiones de red inalámbricas como las de red de área local, ver Figura 1.5.

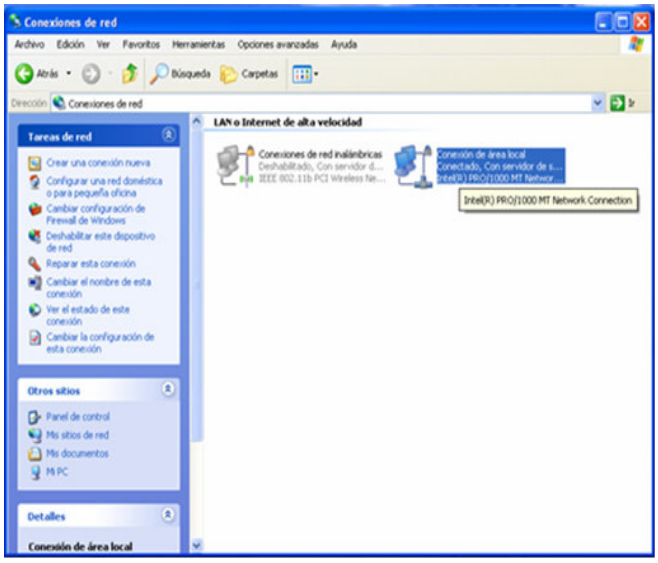


Figura 1.5 Configuración de red inalámbricas y red de área local

Haga doble clic sobre el icono de Conexión de área local, y observe la ventana del Estado de Conexión de área local, ver Figura 1.6.

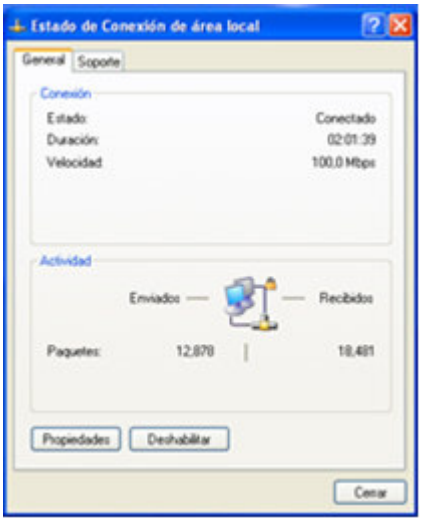


Figura 1.6 Estado de conexión de área local

Dentro de esa ventana, existen dos pestañas: General y Soporte. Elija la pestaña de Soporte, ver Figura 1.7, esta ventana muestra la configuración actual del protocolo TCP/IP. Anote la configuración IP existente en la Tabla No. 1.2, para poder restaurarla al final de la práctica, tanto para el host A como para el host B. Para obtener los datos correspondientes a los servidores DNS, haga clic en el botón Detalles, ver Figura 1.8.

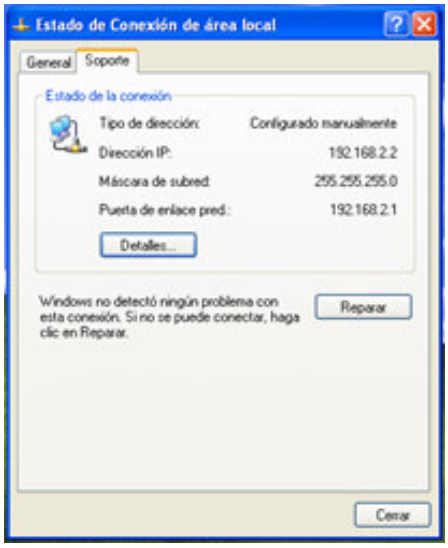


Figura 1.7 Pestaña Soporte

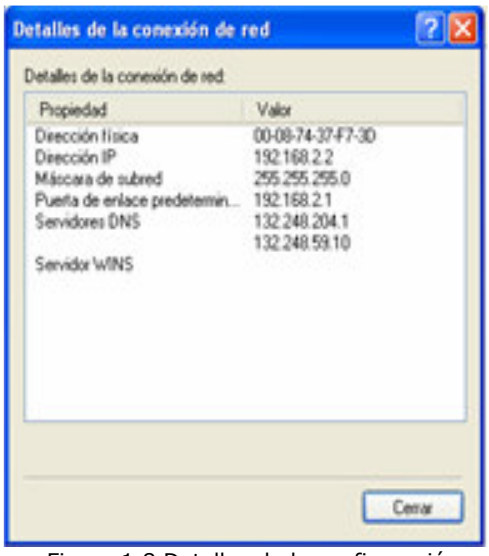


Figura 1.8 Detalles de la configuración

Parámetros de configuración	Host A	Host B
Dirección IP		
Máscara de subred		
Puerta de enlace predeterminada		
Servidor DNS preferido		
Servidor DNS alternativo		

Tabla No. 1.2 Configuración de la IP en host A y en host B

Acceda a la ventana de configuración IP, mediante la selección del menú Inicio>Panel de Control>Conexiones de red. Haga clic en el icono de Conexiones de área local, en ese momento se muestra el menú Tareas de Red, de éste elija la opción Cambiar la configuración de esta conexión, ver Figura 1.9.

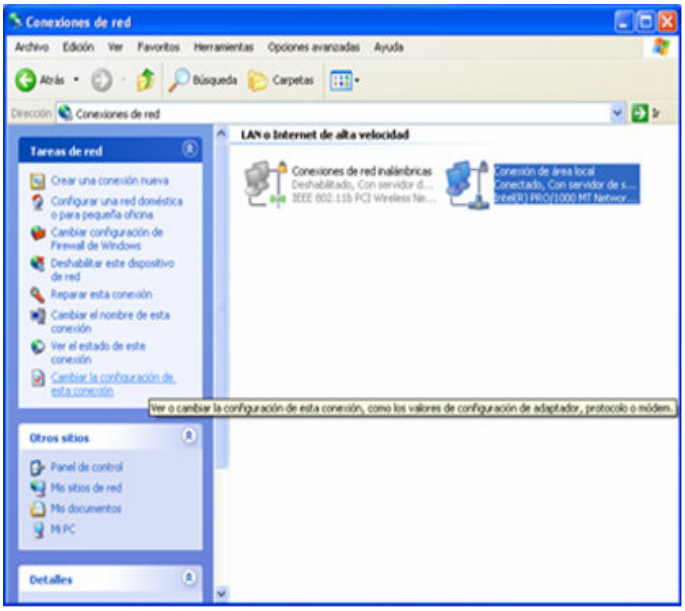


Figura 1.9 Cambiar la configuración de esta conexión

Enseguida observe la ventana de Propiedades de Conexión de área local, seleccione el elemento de conexión Protocolo de Internet TCP/IP y haga clic en Propiedades, ver Figura 1.10.

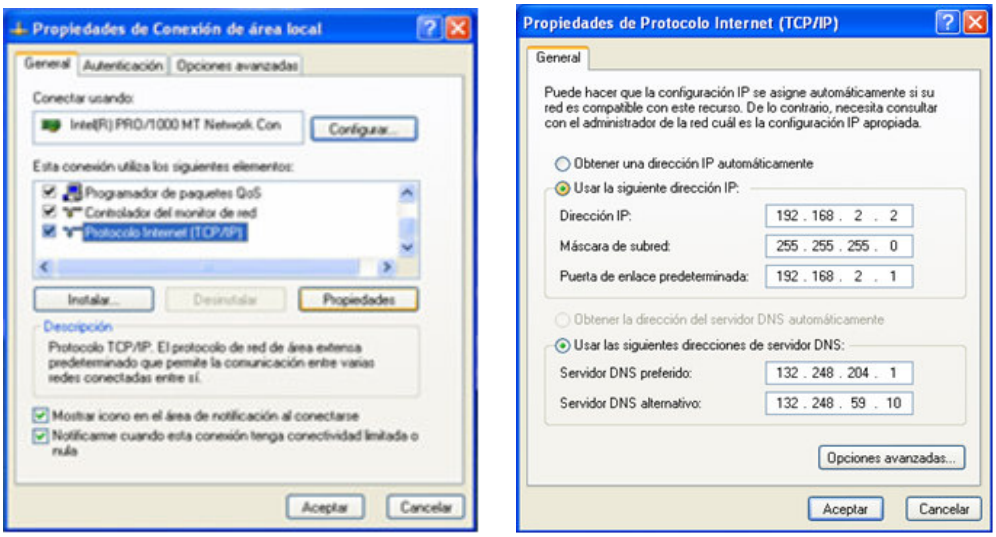


Figura 1.10 Propiedades de Protocolo Internet TCP/IP

De acuerdo a la información de la Tabla No. 1.3 asigne la dirección IP, máscara de subred e indique la puerta de enlace predeterminada a cada uno de los host.

Computadora	Dirección IP	Máscara de subred	Puerta de enlace predeterminado
A	192.168.1.1	255.255.255.0	
B	192.168.1.2	255.255.255.0	

Tabla No. 1.3 Configuración de la IP

Haga clic en el botón Aceptar y cierre la ventana de Propiedades de Conexión de área local.

En este caso no es necesaria la dirección IP de la puerta de enlace predeterminado, ¿por qué?

_____
_____
_____

d. Verificación de la comunicación

En el momento de aceptar los cambios en las propiedades TCP/IP de ambas computadoras, se muestra un menú de Detalles, el cual indica que la Conexión de área local está ahora activa, ver Figura 1.11.

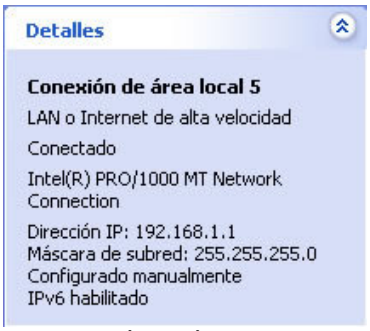


Figura 1.11 Conexión de área local punto a punto

Anote la información proporcionada por el menú Detalles e indique la velocidad de la conexión realizada.

_____
_____
_____

Utilice el menú Inicio>Todos los programas>Accesorios>Símbolo del Sistema y abra la línea de comandos MS-DOS, ver Figura 1.12.

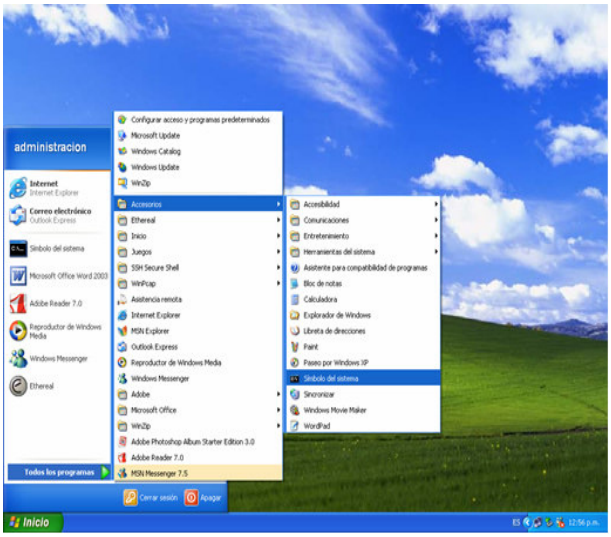


Figura 1.12 Símbolo de sistema en Windows

Pruebe la conectividad entre las estaciones de trabajo haciendo ping a la dirección IP de la otra computadora, como se muestra en la Tabla No. 1.4.

Computadora A	Computadora B
C:> ping 192.168.1.2	C:> ping 192.168.1.1

Tabla No. 1.4 Verificando conectividad

Explique cada una de las líneas resultantes de ejecutar el comando anterior.

_____
_____
_____

e. Confirmación de la configuración

Ejecute el comando ipconfig desde la línea de comandos de MS-DOS y anote el resultado en las siguientes líneas.

_____
_____
_____

f. Restablecimiento de la conexión

Restablezca la configuración IP original de las computadoras con ayuda de la Tabla No. 1.2 y los pasos definidos en el apartado Configuración de la IP. Desconecte los equipos y guarde los cables.

4.1.2 Conexión a un hub

Los hubs son dispositivos que permiten interconectar cables de manera que simulan el comportamiento de un bus en común. Se puede considerar como un repetidor multipuerto, pues toma la señal que entra por un puerto y la repite en todos los demás. Un hub sirve para segmentar la red pero no crea nuevos dominios de colisión.

Entre las principales ventajas de contar con un hub encontramos:

- En estándares como IEEE 802.3 y 803.5 permiten la interconexión de dispositivos mediante cables pares a un punto central, facilitando la incorporación de dispositivos a la red.
- Permite la implementación de la topología en estrella extendida, facilitando la extensión de la red.

Los hubs son los dispositivos más utilizados para la implementación de redes LAN, siendo la base de instalaciones de cableado estructurado. Es posible encontrar hubs inteligentes, pues incluyen su propio procesador y memoria, pudiendo ser programables para administrar el tráfico de red.

Un hub Ethernet funciona de la siguiente manera: recibe la señal por un puerto a través del par de transmisión 3 y 6 del cable, la regenera, sincroniza y reenvía por todos los pares de recepción: par 1 y 2 del cable, al resto de los puertos.

Este segundo punto de la práctica, consiste en crear una red LAN Ethernet con dos computadoras y un dispositivo de la capa 1, ver Figura 1.13.

Figura 1.13 Conexión a través de un dispositivo de capa física

a. Conexión física de las estaciones de trabajo

Realice la conexión física entre las dos estaciones de trabajo y el hub, mediante un cable recto de categoría 5e, conectando uno de los extremos del cable a la NIC y el otro a un puerto del hub.

b. Verificación de la conexión física

Para verificar las conexiones de las computadoras, asegúrese de que estén encendidas las luces de enlace de ambas NIC, ver Figura 1.14.

Figura 1.14 Verificando conexión con NIC

c. Configuración de la IP

Realice los pasos indicados en el apartado 4.1.1.c, Configuración de la IP a partir de la Figura 1.9, Cambiar la configuración de la conexión.

d. Verificación de la comunicación

En el momento de aceptar los cambios en las propiedades TCP/IP de ambas computadoras, se muestra un menú de Detalles, el cual indica que la Conexión de área local está activa, ver Figura 1.15.

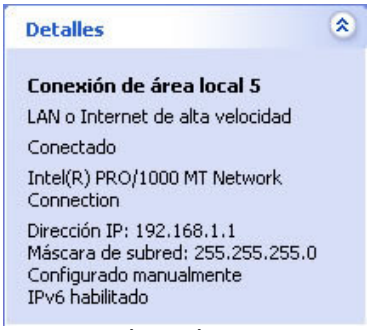


Figura 1.15 Conexión de área local mediante hub

Indique la velocidad de la conexión y pruebe la conectividad entre las estaciones de trabajo mediante la Tabla No. 1.4.

Los resultados obtenidos deben ser similares a los mostrados en la Figura 1.16. En caso contrario verifique las conexiones entre las computadoras y las propiedades de conexión TCP/IP.

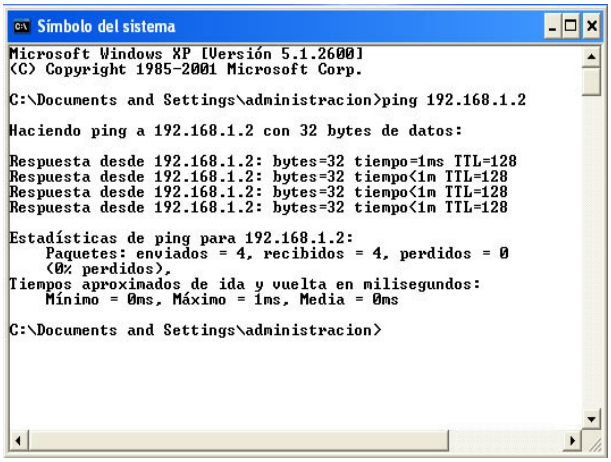


Figura 1.16 Realizando ping a 192.168.1.2

e. Restablecimiento de la configuración

Restablezca la configuración IP original de las computadoras con ayuda de la Tabla No. 1.2 y los pasos definidos en el apartado Configuración de la IP. Desconecte los equipos y guarde los cables.

4.1.3 Conexión a un switch

Esta tercera parte, consiste en analizar las características del cableado estructurado implementado en la red LAN Ethernet del Laboratorio de Redes. Se analizará la trayectoria que sigue el cable desde un nodo a través de la canaleta, hasta llegar al rack, donde es distribuido por el panel de parcheo y enlazado con cables patch cord al switch.

Además de las conexiones físicas también es indispensable configurar las computadoras con la configuración de red IP de modo que exista comunicación.

a. Conexión física de las estaciones de trabajo

Realice un diagrama del cableado estructurado del Laboratorio, indicando la ubicación de los equipos dentro del espacio geográfico, remarcando las conexiones con los jack y como el cable UTP viaja a través de las canaletas hasta llegar al rack. El diagrama debe presentar las longitudes así como el nombre específico de los hosts que integran a la red.

¿Cuál es el objetivo de utilizar un rack, en la conexión de redes de computadoras?

_____
_____
_____

Defina en qué consiste un panel de parcheo y sus principales ventajas.

_____
_____
_____

El diagrama de red se debe presentar en el informe de la práctica, elaborado con el software adecuado de manera que sea entendible y permita la documentación de la red.

El panel de parcheo consiste en un bloque de tomas, la cantidad de las cuales corresponde a la cantidad de puertos, es decir un bloque de 24 tomas es un panel para 24 puertos, ver Figura 1.17.

Figura 1.17 Panel de parcheo

Indique en el siguiente diagrama que muestra una sección de la parte frontal del panel de parcheo del Laboratorio de Redes, cada una de sus características, ver Figura 1.18.

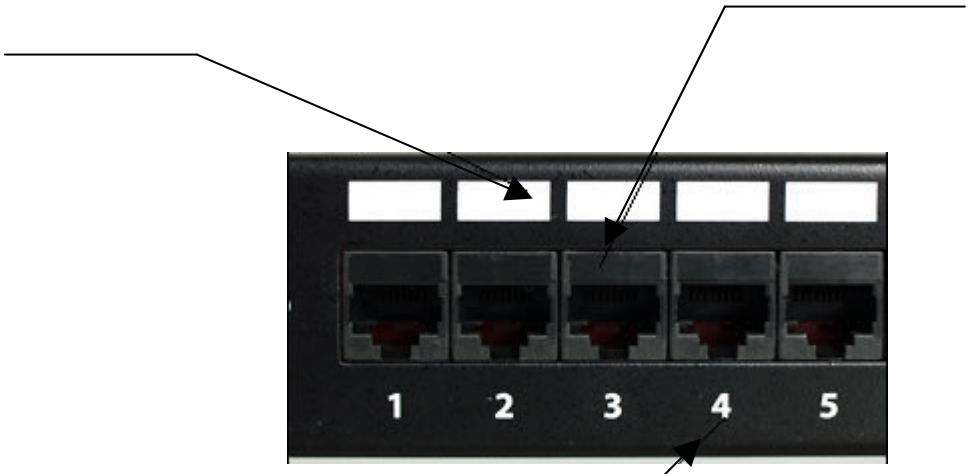


Figura 1.18 Una sección frontal del panel de parcheo

Indique los componentes de la parte trasera del panel de parcheo y su funcionamiento, tal como se muestra en la Figura 1.19.

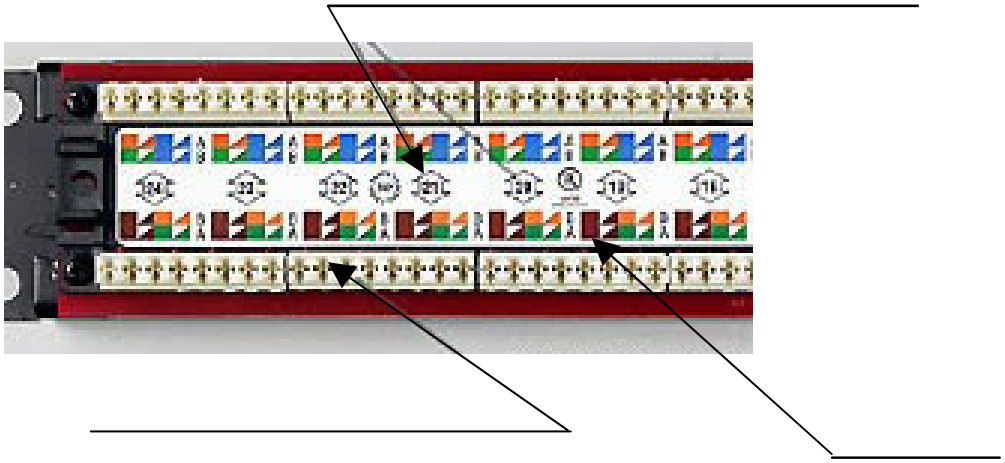


Figura 1.19 Vista trasera del panel de parcheo de la categoría 6

Indique cuál es el principal medio de conmutación con el panel de parcheo

_____
_____
_____

Identifique la topología de red implementada en el Laboratorio y documente las ventajas y desventajas de la misma.

_____
_____
_____

El Laboratorio cuenta con un dispositivo central de conexiones, el switch, investigue el modelo y las características de administración que ofrece.

_____
_____
_____

La conexión centralizada de los nodos facilita su administración con ayuda del diagrama de red, realice la conexión física del host a cargo de su equipo de trabajo en el switch, ver Figura 1.20.

Figura 1.20 Switch 3COM C17300 SuperStack 4226T implementado en el Laboratorio de Redes

Para verificar las conexiones de las computadoras, asegúrese de que estén encendidas las luces de enlace de las NIC.

b. Configuración de la IP

Configure la dirección IP al equipo del Laboratorio asignado conforme a la Tabla No. 1.5.

Computadora	Dirección IP	Máscara de subred	Puerta de enlace predeterminado
1	192.168.1.1	255.255.255.0	No es necesario
2	192.168.1.2	255.255.255.0	No es necesario
3	192.168.1.3	255.255.255.0	No es necesario
4	192.168.1.4	255.255.255.0	No es necesario
5	192.168.1.5	255.255.255.0	No es necesario
6	192.168.1.6	255.255.255.0	No es necesario
7	192.168.1.7	255.255.255.0	No es necesario
8	192.168.1.8	255.255.255.0	No es necesario
9	192.168.1.9	255.255.255.0	No es necesario
10	192.168.1.10	255.255.255.0	No es necesario

Tabla No. 1.5 Configuración de la IP

c. Verificación de la comunicación

Utilice el menú Inicio>Todos los programas>Accesorios>Símbolo del sistema, para abrir la línea de comandos MS-DOS, ver Figura 1.12.

Pruebe la conectividad entre las estaciones de trabajo haciendo ping a la dirección IP de la otra computadora, de acuerdo a la Tabla No. 1.6.

Host	C:> ping dirección
1	192.168.1.2
2	192.168.1.3
3	192.168.1.4
4	192.168.1.5
5	192.168.1.6
6	192.168.1.7
7	192.168.1.8
8	192.168.1.9
9	192.168.1.10
10	192.168.1.1

Tabla No. 1.6 Direcciones IP de las máquinas

e. Confirmación de la configuración

Ejecute el comando ipconfig desde la línea de comandos de MS-DOS y anote el resultado en la siguientes líneas

_____

_____

_____

f. Restablecimiento de la configuración

Restablezca la configuración IP original de las computadoras, desconecte los equipos y guarde los cables.

4.2 Sistema Operativo Linux

4.2.1 Conexión punto a punto

El sistema operativo Linux, es la base de muchos servidores en la red, conocer sus características de comportamiento, así como la manera de resolver problemas de configuración de red, es vital para los administradores.

Este punto de la práctica tiene por objetivo conectar dos computadoras directamente, creando una red, empleando el cable cruzado (crossover) en el sistema Fedora Core, ver Figura 1.21.

Figura 1.21 Conexión punto a punto

Es indispensable iniciar la práctica con todos los dispositivos encendidos, en la sesión de root y el cableado desconectado.

Nota: Cualquier cambio que se realice a la configuración del equipo será responsabilidad de los alumnos asignados al equipo.

Conecte físicamente las tarjetas de red, mediante el cable crossover.

Verifique que las luces de las tarjetas de red estén parpadeando, lo cual indica que sí existe comunicación entre los host, ver Figura 1.22.

Figura 1.22 Tarjeta de red

Es necesario conocer los nombres e IP asociadas de las computadoras involucradas (nombre_computadora1 y su IP asociada, nombre_computadora2 y su IP asociada), información que se proporciona en la Tabla No. 1.7.

Computadora	Dirección IP	Máscara de subred	Puerta de enlace predeterminado
A	192.168.1.1	255.255.255.0	No es necesario
B	192.168.1.2	255.255.255.0	No es necesario

Tabla No. 1.7 Configuración de la IP

Obtenga la información acerca de la configuración actual de la computadora mediante el siguiente comando, ver Figura 1.23.

[root@localhost root]# ifconfig eth0

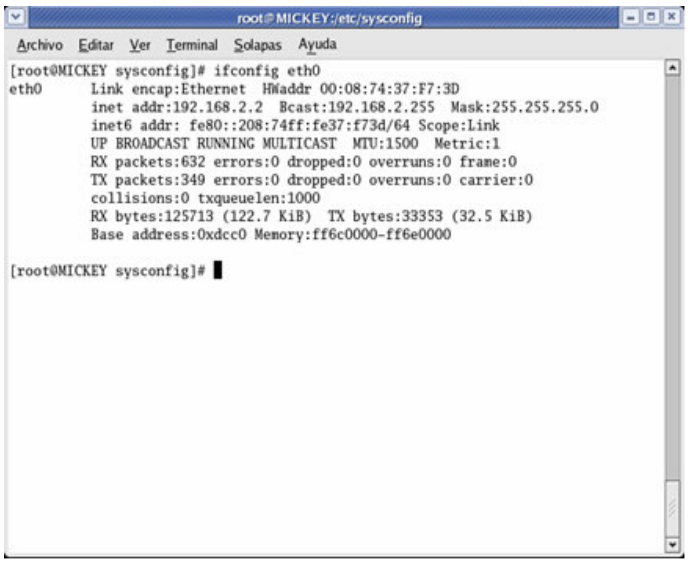


Figura 1.23 Configuración de la tarjeta eth0

Con la información obtenida del comando anterior complete los campos correspondientes en la Tabla No. 1.8. Conforme transcurre la práctica podrá llenar los otros campos.

Parámetros de configuración	Host A	Host B
Dirección IP		
Máscara de subred		
Broadcast		
Gateway		
DNS 1		
DNS 2		

Tabla No. 1.8 Configuración de parámetros iniciales de la IP en host A y en host B

a. Configuración de la tarjeta de red

Una vez detectada la tarjeta por el sistema operativo es necesario configurarla. La configuración se realizará mediante edición de archivos de configuración.

Visualice el archivo /etc/sysconfig/network-scripts/ifcfg-eth0 mediante el comando vi y obtenga la dirección del gateway actualmente configurado, ésta última colóquela en la Tabla No. 1.8, ver Figura 1.24.

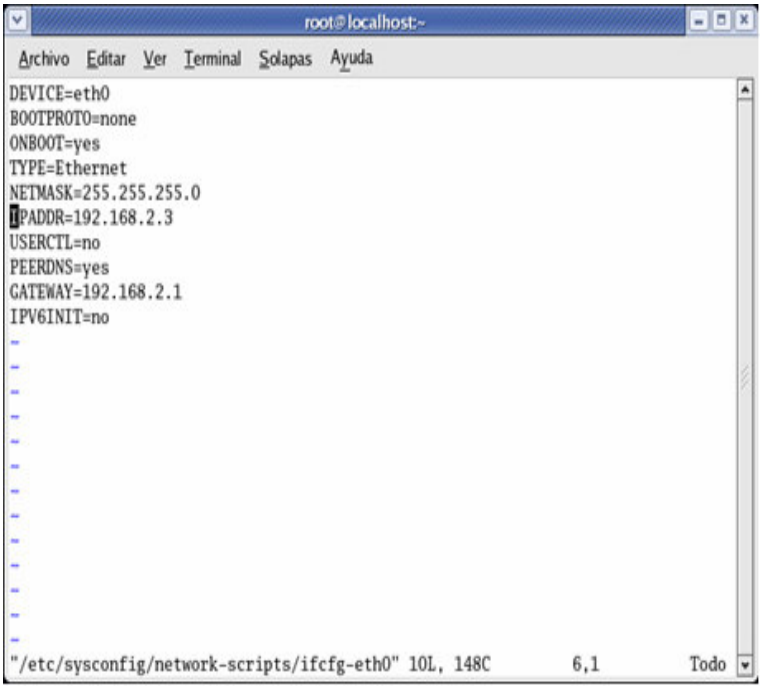


Figura 1.24 Salida del comando vi en /etc/sysconfig/network-scripts/ifcfg-eth0

Realice un respaldo del archivo /etc/sysconfig/network-scripts/ifcfg-eth0 mediante el siguiente comando.

[root@localhost root]# cp /etc/sysconfig/network-scripts/ifcfg-eth0 /etc/sysconfig/network-scripts/ifcfg-eth0Respaldo.txt

Edite el archivo /etc/sysconfig/network-scripts/ifcfg-eth0 con la siguiente información a través de la siguiente instrucción, ver Figura 1.25:

[root@localhost root]# vi /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
IPADDR=192.168.1.1
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255

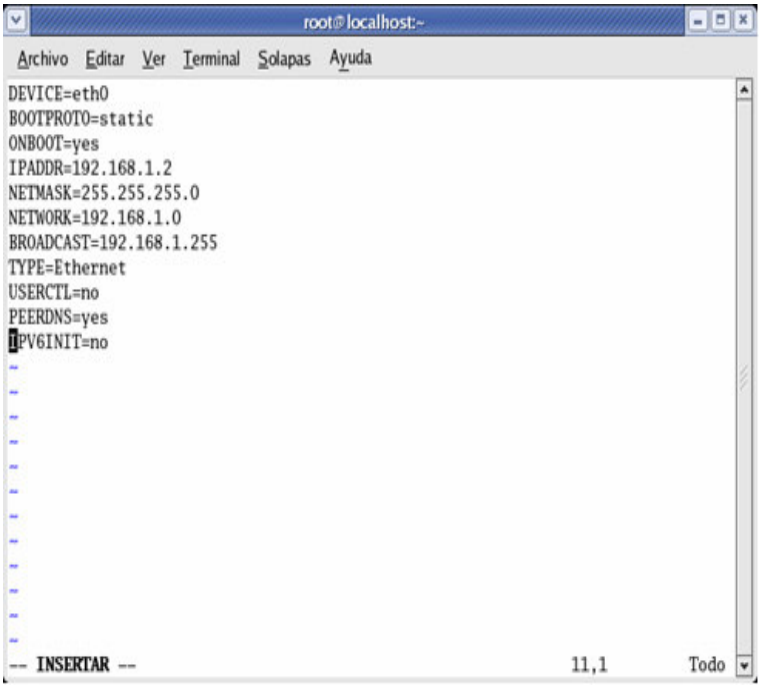


Figura 1.25 Modificando el archivo /etc/sysconfig/network

Si no existe el archivo, es necesario crearlo, con la siguiente instrucción:

[root@localhost root]# vi /etc/sysconfig/network-scripts/ifcfg-eth0

Investigue qué información se especifica en el archivo /etc/sysconfig/network.

_____
_____
_____

Verifique que el anterior archivo únicamente incluya las siguientes instrucciones, ver Figura 1.26.

NETWORKING=yes
HOSTNAME=

[root@localhost root]# vi /etc/sysconfig/network

El archivo /etc/resolv.conf indica los DNS actualmente configurados, ver Figura 1.27.

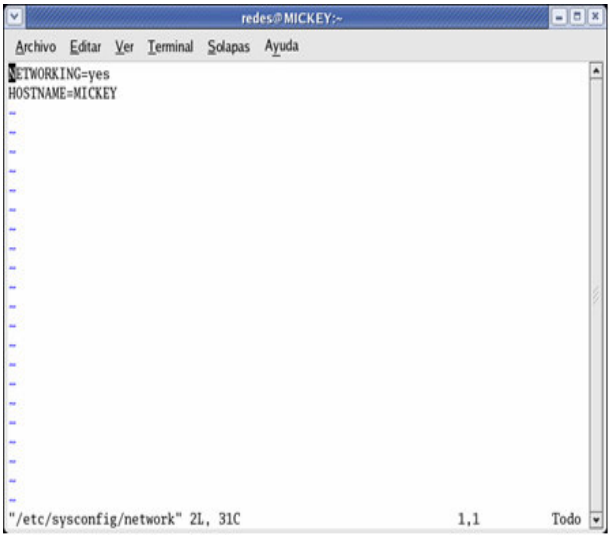


Figura 1.26 Archivo /etc/sysconfig/network

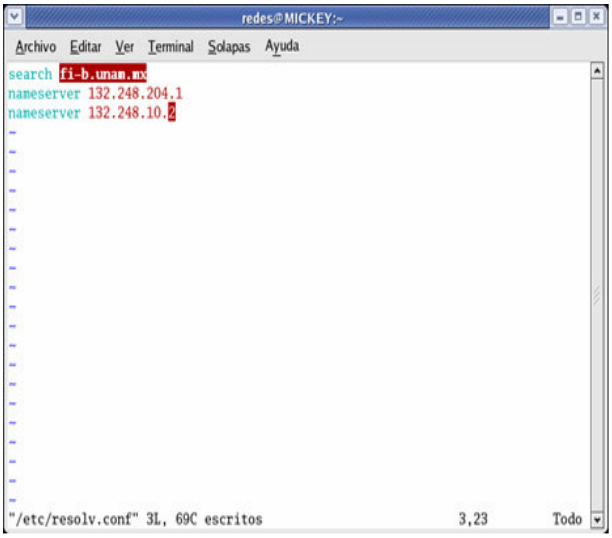


Figura 1.27 Archivo /etc/resolv.conf

Coloque las direcciones de los DNS configurados inicialmente en la Tabla No. 1.8, tabla de parámetros iniciales de configuración de red.

Realice un respaldo del archivo /etc/resolv.conf mediante el siguiente comando:

[root@localhost root]# cp /etc/resolv.conf /etc/resolv.confRespaldo.txt

Verifique que el contenido del archivo /etc/resolv.conf cuente con la siguiente información mediante el comando vi.

[root@localhost root]# vi /etc/resolv.conf

Search fi-b.unam.mx
nameserver 132.248.204.1
nameserver 132.248.10.2

Investigue si la edición del archivo que contiene los DNS, es necesaria para el objetivo de este punto, justificando su respuesta.

_____
_____
_____

Para que los archivos modificados de configuración tengan efecto, es necesario reiniciar el servicio de red del equipo, mediante los siguientes comandos.

[root@localhost root]# /etc/init.d/network stop

[root@localhost root]# /etc/init.d/network start

b. Verificación de la conectividad

Ejecute el comando ping al nodo adjunto con el objetivo de verificar la conectividad.

[root@localhost root]# ping 192.168.1.1, en el caso del host A

[root@localhost root]# ping 192.168.1.2, en el caso del host B

Los resultados deben ser similares a los mostrados en la Figura 1.28.

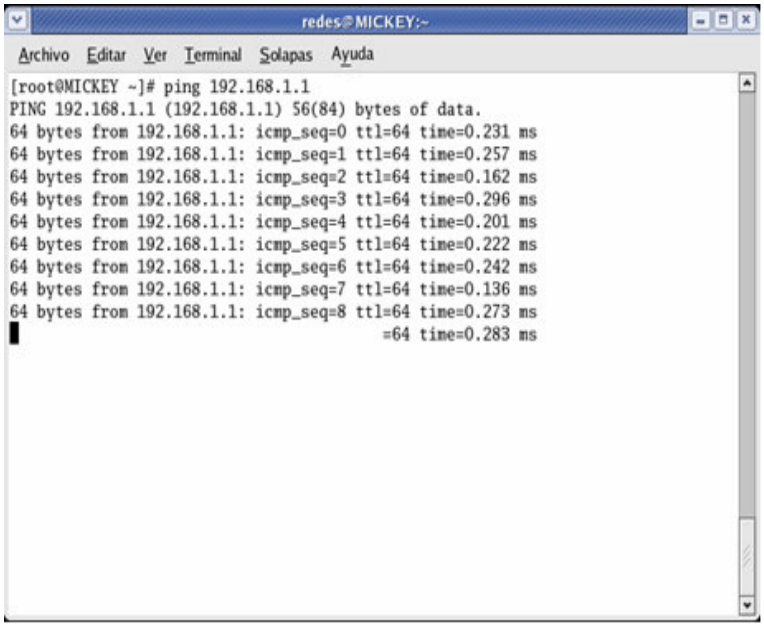


Figura 1.28 Ping a 192.168.1.1

Nota: Para detener el comando ping únicamente presione las teclas Ctrl.+C.

Investigue 5 opciones importantes de la herramienta ping, para probar la conectividad en las redes y defina su importancia para la administración de las redes.

_____
_____
_____

Investigue en qué consiste el parámetro de configuración de interfases de redes, denominado MTU.

_____
_____
_____

c. Restablecimiento de la conexión

Para restablecer la configuración de red, únicamente restaure los archivos originales, mediante los siguientes comandos, ver Figuras 1.29 y 1.31.

[root@localhost root]# mv /etc/resolv.confRespaldo.txt /etc/resolv.conf

[root@localhost root]# mv /etc/sysconfig/network-scripts/ifcfg-eth0Respaldo.txt etc/sysconfig/network-scripts/ifcfg-eth0

Responda afirmativamente a la pregunta de sobrescribir los archivos.

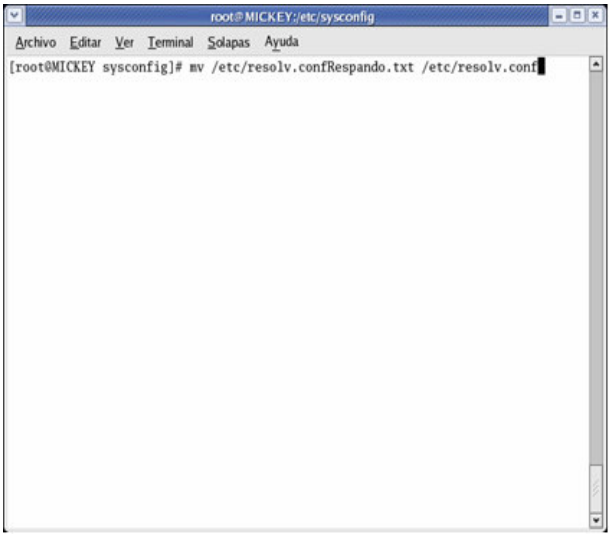


Figura 1.29 Restableciendo los DNS

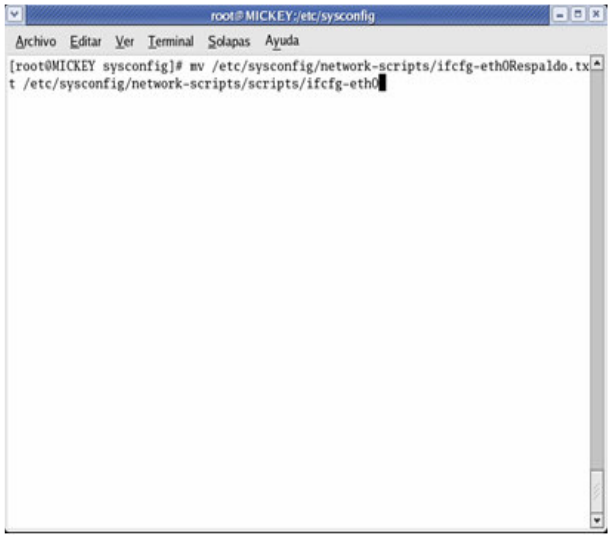


Figura 1.30 Restableciendo la configuración eth0

Para que los archivos modificados de configuración sean reestablecidos es necesario reiniciar el servicio de red del equipo, mediante los siguientes comandos, ver Figuras 1.31 y 1.32.

[root@localhost root]# /etc/init.d/network stop

[root@localhost root]# /etc/init.d/network start

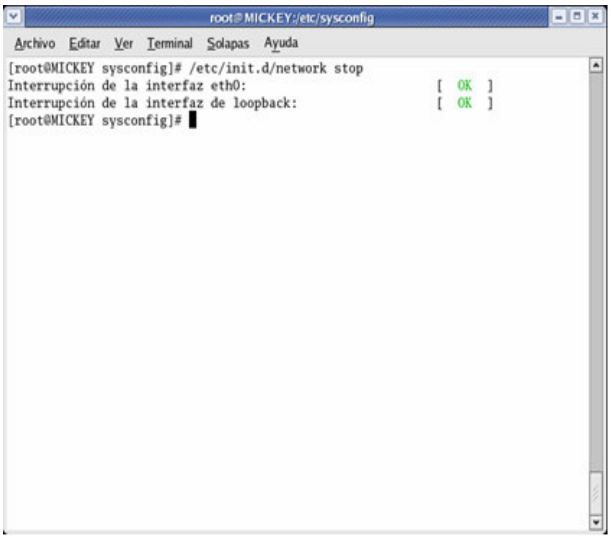


Figura 1.31 Deteniendo el servicio de red

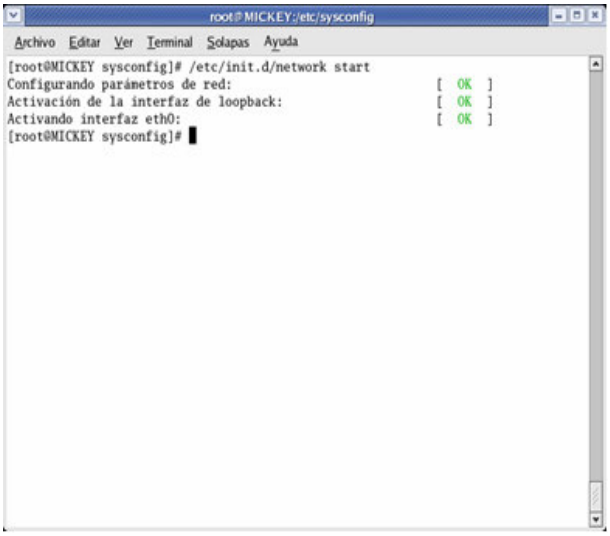


Figura 1.32 Levantando el servicio de red

Todos los scripts de inicio y fin de servicios se ubican en /etc/init.d. Las tareas del proceso init implican la comprobación del sistema de archivo, su montado, arranque de demonios de servicios, administración de redes, etc.

d. Verificación de la configuración inicial

Verifique que la configuración de red coincida con la especificada en la Tabla No. 1.8., a través de los comandos estudiados.

4.2.1 Conexión a un hub

Los hub o concentradores son dispositivos que permiten centralizar el cableado de una red, cuentan con varias puertos y requieren una conexión a la red eléctrica por medio de un transformador de 12V. Son la base de la topología estrella. Hay que tener en cuenta las siguientes características:

- El número de puertos, los hay con 5, 8, 16, 32 o más.
- La velocidad, principalmente es de 10Mb, de 100Mb, y los que son 10/100Mb a la vez. También los hay de 1000Mb.

Nota Profesor: Se recomienda utilizar un hub para 2 equipos de cómputo, de manera que se observen de mejor manera los resultados. Para adaptarse al material con que se cuenta en el laboratorio se propone al menos 2 hub, uno por cada 4 máquinas.

a. Verificación de la conexión física

Conecte 4 computadoras con el cable UTP de conexión directa al dispositivo central denominado hub y éste a su vez a la corriente eléctrica. No es necesario conectar el hub a un nodo de la red, ¿por qué?

_____
_____
_____

b. Configuración de la IP

Anote la configuración IP existente de cada una de las máquinas, en la Tabla No. 1.9, para poder restaurarla al final de la práctica, mediante el comando ifconfig y hostname.

[root@localhost root]# ifconfig –a

	Host A	**Host B**	**Host C**	**Host D**
Dirección IP				
Máscara de subred				
Nombre				

Tabla No. 1.9 Configuración de la IP

La configuración del protocolo TCP/IP para los sistemas Linux, es posible realizarla a través de la interfaz gráfica proporcionada por Fedora y mediante línea de comando.

En el menú Aplicaciones, ubicado en la barra de Herramientas, despliegue el submenú Herramientas del sistema >Asistente de configuración de Internet, ver Figura 1.33.

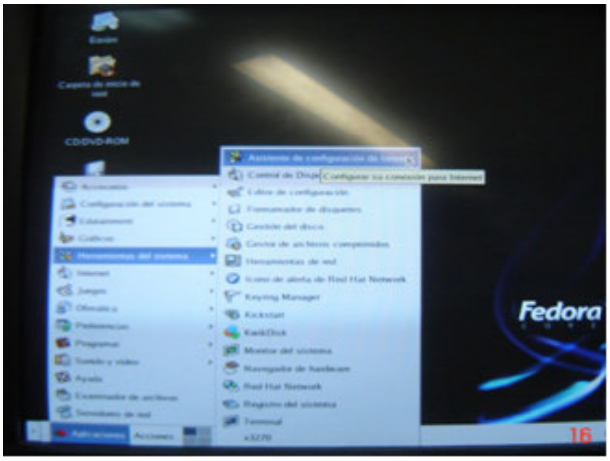


Figura 1.33 Menú Herramientas y Aplicaciones

El asistente solicita que seleccione el tipo de dispositivo a configurar. Elija la opción Conexión Ethernet y haga clic en Adelante, ver Figura 1.34. El asistente permite seleccionar la tarjeta que se desea configurar, por default reconoce la que está instalada en la computadora, en este caso Intel Corp. 82540EMGigabyteEthernetController (eth0), ver Figura 1.35 y haga clic en Adelante.

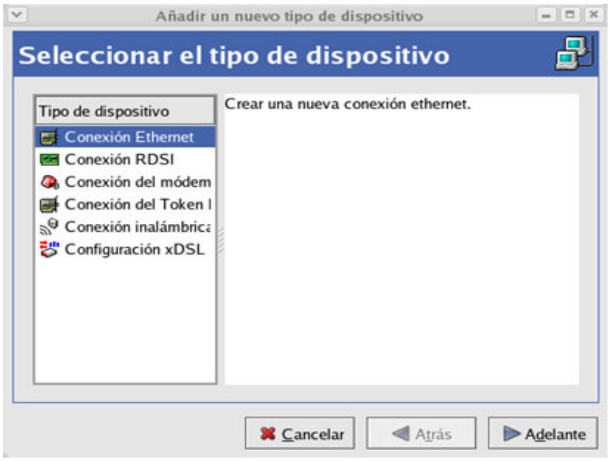


Figura 1.34 Selección del tipo de conexión

Figura 1.35 Selección de dispositivo

El asistente muestra la configuración de las opciones de red, verifique que la opción Configurar las direcciones IP de manera estática se encuentre activado, ver Figura 1.36. En el área de la configuración de la dirección IP manual, introduzca los datos indicados en la Tabla No. 1.10 de acuerdo a la computadora asignada.

Computadora	Dirección IP	Máscara de subred	Dirección de puerta de enlace
A	192.168.1.1	255.255.255.0	No es necesario
B	192.168.1.2	255.255.255.0	No es necesario
C	192.168.1.3	255.255.255.0	No es necesario
D	192.168.1.4	255.255.255.0	No es necesario

Tabla No. 1.10 Configuración de IP para host A y host B

La siguiente pantalla confirma la información introducida, haga clic en Aplicar, ver Figura 1.37.

Figura 1.36 Configuración de las opciones de red

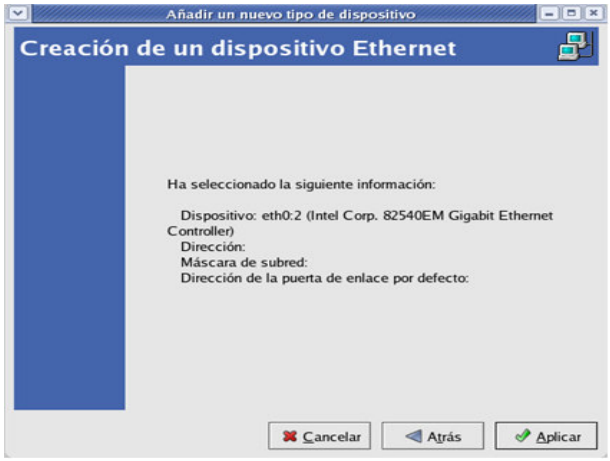


Figura 1.37 Creación de un dispositivo de red

Observe la ventana de Configuración de Red, haga clic en la pestaña de Dispositivos donde se muestra una lista de las configuraciones del dispositivo. Esta lista presenta activa la configuración anterior, seleccione la casilla de perfil y la configuración, y posteriormente elija la opción Desactivar, ver Figura 1.38.

Una ventana de aviso, pregunta si guarda los cambios. Haga clic en Sí, ver Figura 1.39.

Figura 1.38 Activar configuración anterior

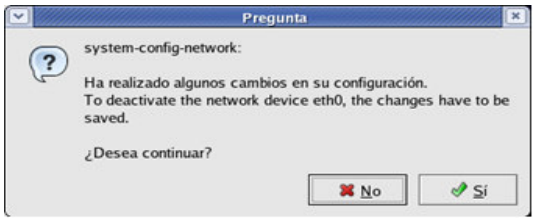


Figura 1.39 Desactivar configuración anterior

La siguiente ventana informa que los cambios han sido guardados. Haga clic en Aceptar, e inmediatamente observe una ventana de aviso de cambios, ver Figura 1.40. De esa manera la configuración anterior se muestra Desactivada, ver Figura 1.41.

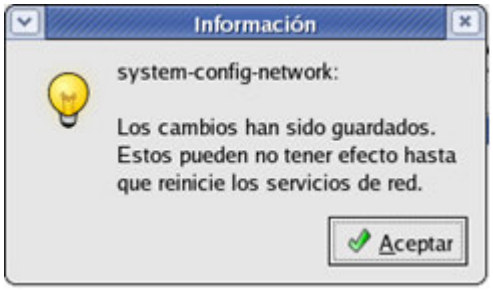


Figura 1.40 Cambios guardados

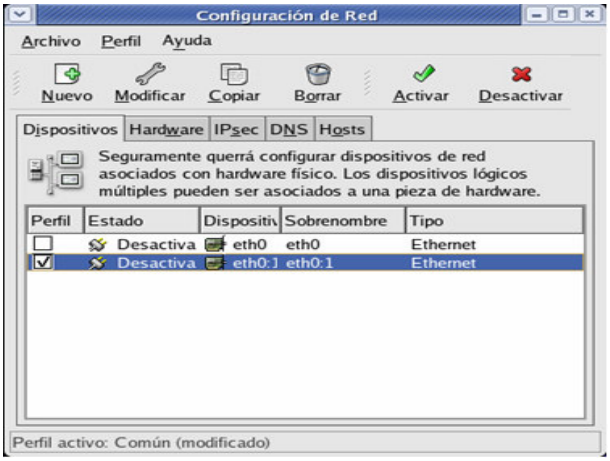


Figura 1.41 Configuración anterior desactivada

Para activar la configuración realizada, seleccione la casilla debajo de la columna perfil y la nueva configuración y haga clic en la opción Activar del Menú.

Se presenta una ventana informando los cambios, presione Sí y después Aceptar en las dos ventanas siguientes, ver Figura 1.42.

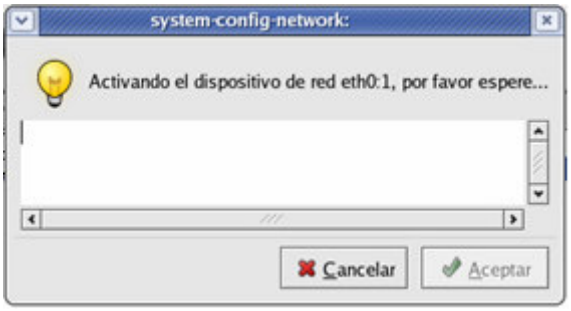


Figura 1.42 Ventana de confirmación de system-config-network

Cierre la ventana de Configuración. Para verificar la configuración de la IP, ejecute el comando ifconfig en una consola de shell, ver Figura 1.43.

[root@localhost root]# ifconfig

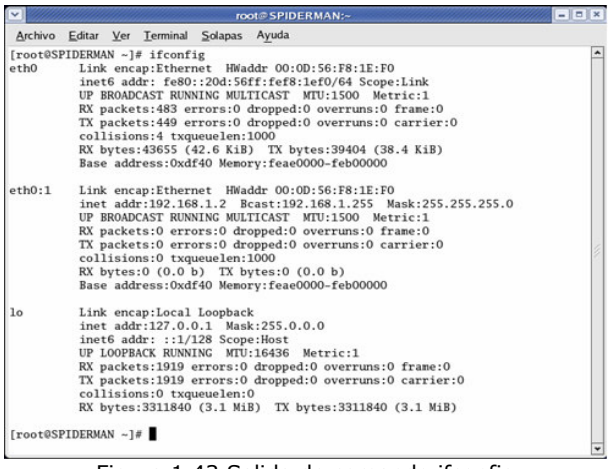


Figura 1.43 Salida de comando ifconfig

Identifique la información concerniente a la nueva configuración mediante el comando anterior y explique cada una de las líneas.

_____
_____
_____

Observe que todos los indicadores del hub están encendidos, ver Figura 1.44.

Figura 1.44 Indicadores del hub encendidos

e. Verificación de la conectividad

Verifique la conectividad entre los hosts conectados a través del hub. Ejecute el siguiente comando, ver Figuras 1.45 y 1.46.

[root@localhost root]# ping 192.168.1.4 , en el caso del host A

[root@localhost root]# ping 192.168.1.3, en el caso del host B

[root@localhost root]# ping 192.168.1.2, en el caso del host C

[root@localhost root]# ping 192.168.1.1, en el caso del host D

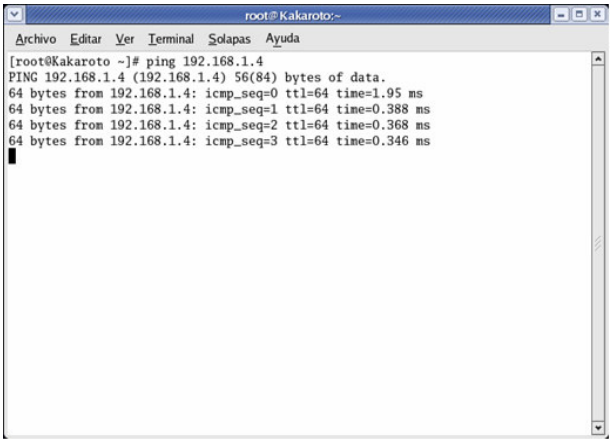


Figura 1.45 Ping a la computadora 192.168.1.4

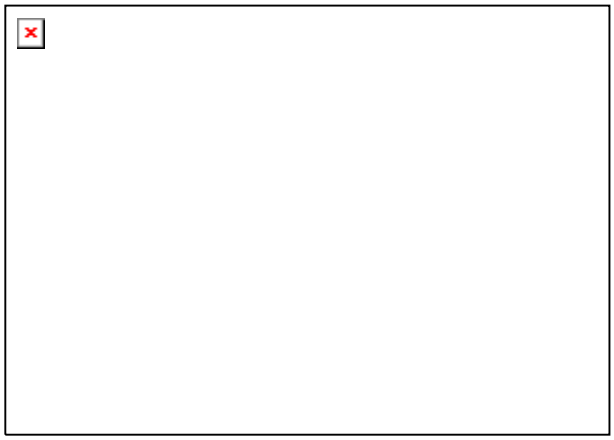


Figura 1.46 Ping a la computadora 192.168.1.3

f. Restableciendo la configuración

Cierre las terminales de shell para poder restablecer la conexión inicial. Inicie el menú Aplicaciones>Herramientas del Sistema>Control de Dispositivos de Red. Esta ventana permite controlar los dispositivos de red, muestra las interfases de red configuradas en el

perfil activo. Haga clic en el botón Configurar, ver Figura 1.47. Se observa la ventana de Configuración de red, ver Figura 1.48.

Figura 1.47 Control de dispositivos de red

Figura 1.48 Configuración de red

Seleccione el dispositivo activo desactivando la casilla de perfil y haga clic en la opción Borrar, ver Figura 1.49.

El asistente pregunta si se desea borrar la configuración del dispositivo, ver Figura 1.50 haga clic en Sí.

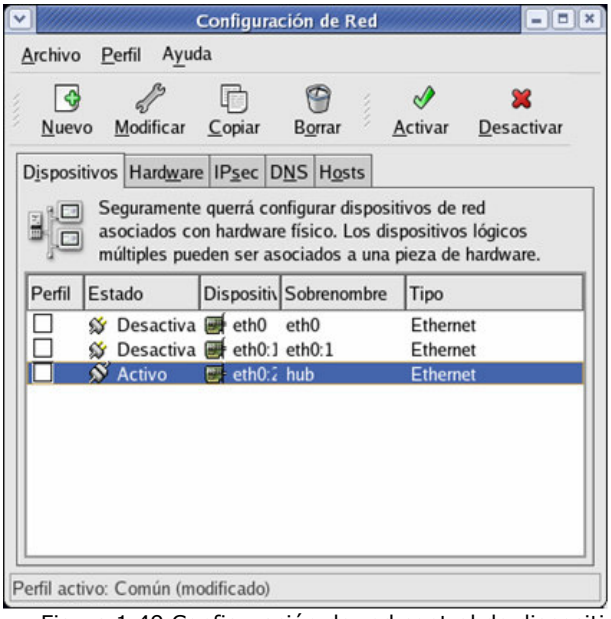


Figura 1.49 Configuración de red control de dispositivos de red

Figura 1.50 Confirmación de la acción

Se muestra la ventana de Configuración de red, seleccione el dispositivo con la configuración inicial de la práctica. Active la casilla de verificación de la columna perfil y elija Activar, ver Figura 1.51.

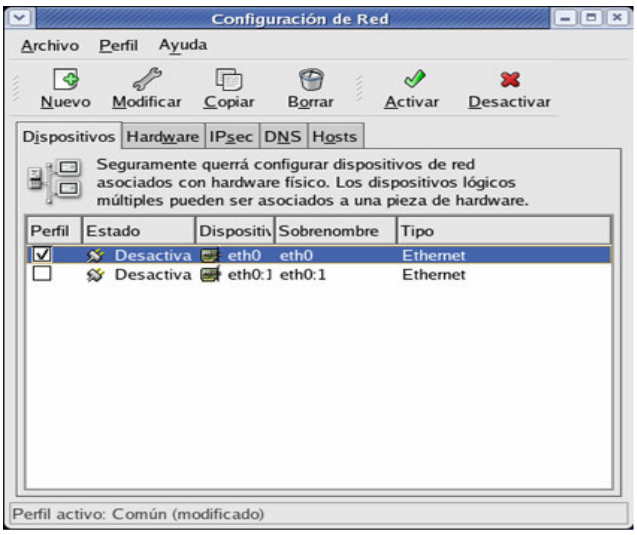


Figura 1.51 Configuración de red

Las ventanas de confirmación preguntan si se desea continuar, haga clic en Sí y después en Aceptar.

Cierre la ventana de Configuración de red. Verifique la configuración inicial de la IP, ejecutando el comando ifconfig en una consola, ver Figura 1.52.

[root@localhost root]# ifconfig

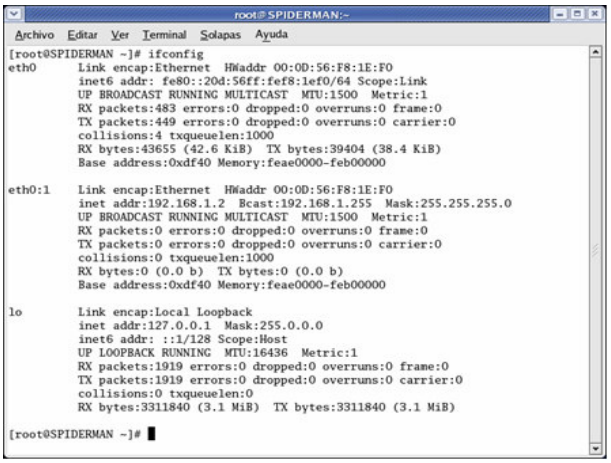


Figura 1.52 Salida de comando ifconfig

4.2.1 Conexión a un switch

Un administrador de redes debe saber configurar los servicios de red en línea de comando, debido a que existen ocasiones en las que no es posible levantar el GUI o bien la administración requiere hacerse remotamente. La herramienta necesaria para realizar la administración por línea de comandos de una tarjeta de red, es ifconfig.

Nota Profesor: Los cables de red y las computadoras estarán desconectados tanto del nodo como del panel de parcheo.

a. Configuración de la tarjeta de red

Conecte el cable de la roseta a la NIC de la computadora asignada, identifique el nodo y conecte su cable correspondiente del panel de parcheo al puerto indicado del switch.

Además de las conexiones físicas también hay que configurar las computadoras con la configuración de red IP de modo que exista comunicación.

Abra una terminal de línea de comando, mediante el menú Aplicaciones>Herramientas del Sistema>Terminal.

Teclee el comando ifconfig para obtener la información de la dirección actual y colóquela en la Tabla No. 1.11 para poderla restaurarla al final de la práctica.

[root@localhost root]# ifconfig

	Host A
Dirección IP	
Máscara de subred	
MAC	

Tabla No. 1.11 Configuración inicial de IP

Configure la tarjeta de red, mediante la herramienta ifconfig, ejecute el comando con la dirección IP de acuerdo a la Tabla No. 1.5, ver Figura 1.53.

[root@localhost root]# ifconfig eth0 192.168.1.X netmask 255.255.255.0

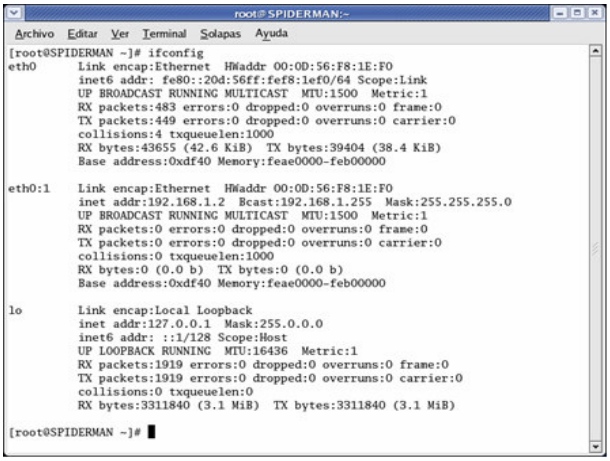


Figura 1.53 Salida del comando ifconfig

b. Verificación de la configuración de la tarjeta

Verifique la configuración del dispositivo de red eth0 a través del comando ifconfig eth0. Observe que la tarjeta tenga la dirección IP configurada.

c. Verificación de la conectividad

Pruebe la conectividad entre las estaciones de trabajo haciendo ping a la dirección IP de la otra computadora, conforme a la Tabla No. 1.6.

Reinicie el equipo con el comando reboot y verifique la configuración de la tarjeta de red.

Explique que sucede con la configuración y fundamente si justificación.

_____
_____
_____

Investigue al menos 5 opciones importantes de la herramienta ifconfig para configurar redes y defina su importancia para la administración de las redes.

_____
_____
_____

5. Conclusiones

6. Cuestionario Previo 1

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 2 Parte A
Manejo de Dispositivos de Interconectividad, hub y switch

1.- Objetivo de aprendizaje

El alumno conocerá, profundizará en el conocimiento e identificará los elementos que conforman una red de computadoras, además de investigar las políticas y ética que las rigen.

El alumno desarrollará las habilidades necesarias que le permitan la manipulación de equipos de interconexión como lo son los hubs y switches.

El alumno analizará el comportamiento de valores cuantitativos de una red como lo son: el retardo, el número de colisiones, etc., mediante herramientas de simulación de redes como OPNET IT GURU Academic.

2.- Conceptos teóricos

Para un administrador de red, resulta necesario e indispensable conocer los equipos, mecanismos y técnicas para extender las capacidades de las redes que están bajo su cargo. En algunas ocasiones es necesario extender físicamente una red, para añadir nuevas estaciones así como para interconectarla a una LAN con localización geográfica distinta. De igual forma, es conveniente planear el crecimiento de una LAN en términos de ancho de banda, para hacer frente a necesidades de comunicación actuales.

La extensión de las capacidades de una red, se logra mediante dispositivos hardware definidos para cada uno de los tipos de redes, en el caso de las LAN encontramos los hubs, switches, repetidores, puentes, access point; para las redes MAN, tenemos repetidores, canalizadores, módems analógicos, modéms cable; en el caso de las redes WAN, encontramos routers, multicanalizadores, módems satelitales, etc.

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- 1 cable módem nulo estándar o matricial.
- PC's Pentium con una NIC Ethernet 10/100 Mbps instalada en cada una de ellas.
- Un hub Ethernet 10BaseT o FastEthernet (4 -8) puertos.
- Un switch Ethernet 10BaseT o FastEthernet (24 puertos).
- Software Académico de Simulación de Redes, OPTNET IT GURU Academia.
- Software de Simulación RouterSim CCNA 3.0.
- Software de emulación de terminal Microsoft Hyperterminal.

4.- Desarrollo

4.1 Hub

El hub es un dispositivo activo que actúa como elemento central. Cada estación se conecta al hub, mediante dos enlaces: transmisión y recepción. El hub actúa como un repetidor: cuando transmite una única estación, el hub replica la señal en la línea de salida hacia cada host conectado. Regularmente el enlace consiste en dos pares trenzados no apantallados. Dada la alta velocidad y baja calidad de transmisión del par trenzado no apantallado, la longitud de un enlace está limitada a un entorno de 100m. Como alternativa se puede usar un enlace de fibra óptica en cuyo caso la longitud máxima es del orden de 500m.

Varios niveles de hub, se pueden colocar en cascada formando una configuración jerárquica, teniendo un hub raíz denominado HHUB, Encabezado Hub (Header Hub) y uno o más hubs intermedios denominados IHUB, Hub Intermedios (Intermediate Hub). Esta estructura se adecua bien a edificios cableados donde regularmente existe un armario de interconexiones en cada planta del edificio.

Existen hubs pasivos y activos, los primeros sólo interconectan dispositivos mientras que los segundos además regeneran la señal recibida, como si fuera un repetidor de ahí la denominación de repetidor multipuerto.

4.1.1 Introducción

Indique cada uno de los componentes en el siguiente diagrama de la vista frontal del hub, anteriormente implementado en el Laboratorio de Redes, ver Figura 2.1.

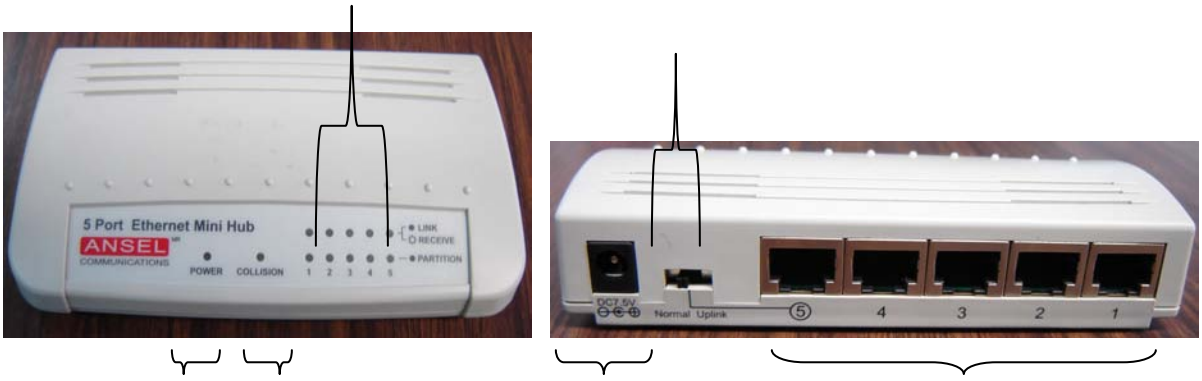


Figura 2.1 Diagrama del Hub 5 Puertos Ethernet Mini Hub ANSEL

Mencione el significado de cada uno de los indicadores del hub 5 Puertos Ethernet Mini Hub ANSEL.

_____
_____
_____

Describa paso a paso el funcionamiento interno del hub

_____
_____
_____

Nota: Un hub funciona a la velocidad del dispositivo más lento de la red, debido a que no tiene la capacidad de almacenar nada. Por lo tanto si un nodo que emite a 100Mb le transmite a otro de 10Mb no se aprovechará de manera adecuada el ancho banda.

4.1.2 Análisis del rendimiento de un hub

El hub extiende la funcionalidad de la red para que el cableado pueda ser extendido a mayor distancia, por eso su nombre de repetidor. El problema es que el hub transmite los broadcast a todos los puertos que contenga, esto es, si contiene 8 puertos todos los nodos que estén conectados recibirán la misma información, siendo innecesario y excesivo.

OPNET IT GURU Academic, es un entorno virtual de red capaz de modelar el comportamiento de todo tipo de red, incluyendo los elementos como routers, switches, hubs, protocolos, etc. Este software de simulación resulta básico para estudiantes y administradores de redes, ya que permite el diagnóstico de problemas y previsión del comportamiento de las redes en futuras ampliaciones, ver Figura 2.2.

Figura 2.2 OPNET IT GURU Academic

Investigue 3 valores cuantitativos considerados en el análisis del rendimiento de una red.

_____
_____
_____

4.1.2.1 Creación de un nuevo proyecto

Para la creación de la red a analizar, realice los siguientes pasos:

1. Seleccione menú>Inicio >Todos los programas>OPNET IT GURU Academic> OPNET IT GURU Academic, haga clic en botón *I have read this SOFTWARE AGREEMENT and I understand and accept the terms and conditions described herein* ver Figura 2.2.
2. Seleccione File>New y elija del menú desplegable Project. Haga clic en OK, ver Figura 2.3.
3. Se presenta una ventana, que solicita el nombre del proyecto y el nombre del escenario, ver Figura 2.4. En el campo de Project Name, introduzca el siguiente nombre: iniciales_LAN y para el campo Scenario Name: Hub, haga clic en OK.

Figura 2.3 Menú nuevo proyecto

Figura 2.4 Nombrando proyecto y escenario

Hasta este punto, se ha creado el proyecto y el nombre del primer escenario.

4.1.2.2 Creación de la red

1. Se inicia el asistente de configuración rápida. En la elección Topology elija Create Empty Scenario y haga clic en Next, ver Figura 2.5.
2. Seleccione la escala de red, como Office y haga clic en Next, ver Figura 2.6.

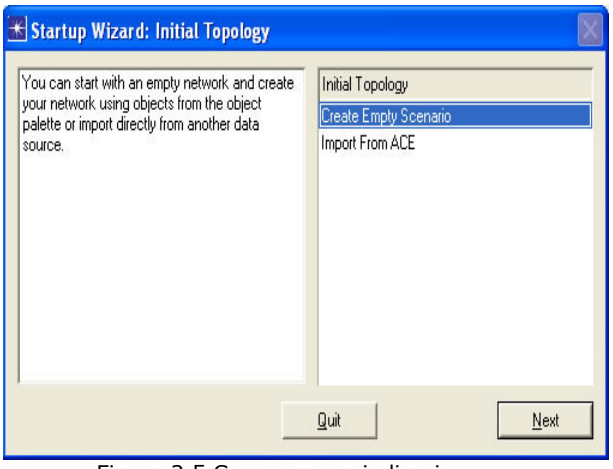


Figura 2.5 Crear escenario limpio

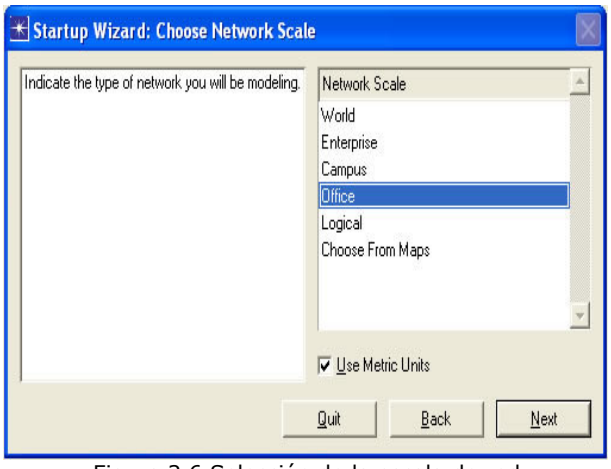


Figura 2.6 Selección de la escala de red

3. En la siguiente pantalla se solicitan las medidas de la escala de red seleccionada. Introduzca los valores para X e Y = 100m y haga clic en Next, ver Figura 2.7.
4. La siguiente ventana solicita que seleccione la Tecnología de Red, para esta simulación únicamente haga clic en Next, ver Figura 2.8.

Figura 2.7 Selección de las medidas de la oficina

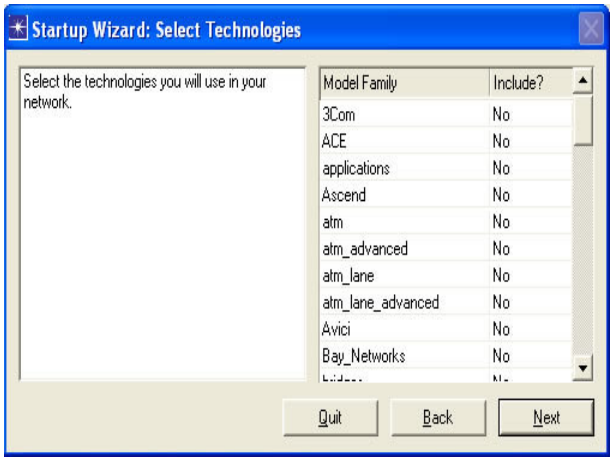


Figura 2.8 Selección de la tecnología

5. Revise los valores introducidos anteriormente y haga clic en OK, ver Figura 2.9.
6. El programa muestra el área de trabajo y una paleta de objetos, ver Figura 2.10. Cierre la paleta de objetos y seleccione del menú Topology, la opción Rapid Configuration.

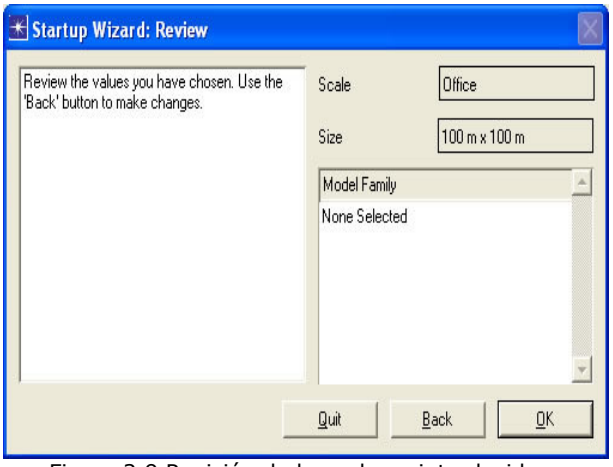


Figura 2.9 Revisión de los valores introducidos

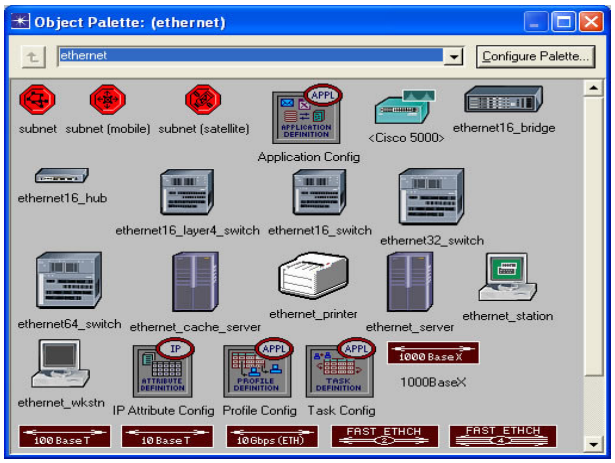


Figura 2.10 Paleta de Objetos

7. Seleccione la opción Star del menú de Rapid Configuration y haga clic en OK, ver Figura 2.11.
8. Haga clic en el botón Select Models. Active la opción Model List y seleccione ethernet. Haga clic en OK, ver Figura 2.12.

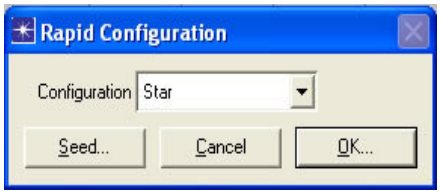


Figura 2.11 Selección de la topología en estrella

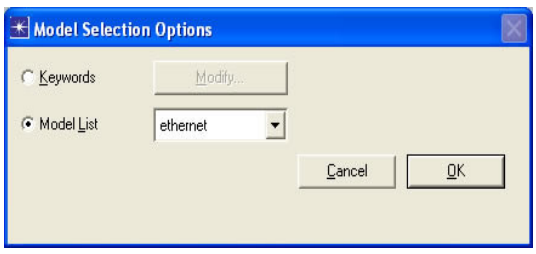


Figura 2.12 Selección de la opción Model List

9. Se muestra un asistente de Configuración Rápida, introduzca los valores descritos en la Tabla No. 2.1, para cada uno de los campos y haga clic en OK, Figura 2.13.

Características	Valores
Center Node Model	ethernet16_hub
Periphery Node Model	ethernet_station
Link Model	10BaseT
Number	16
X	50
Y	50
Radios	42

Tabla No. 2.1 Valores para la configuración de la red

El resultado de la topología creada debe ser similar a la Figura 2.14.

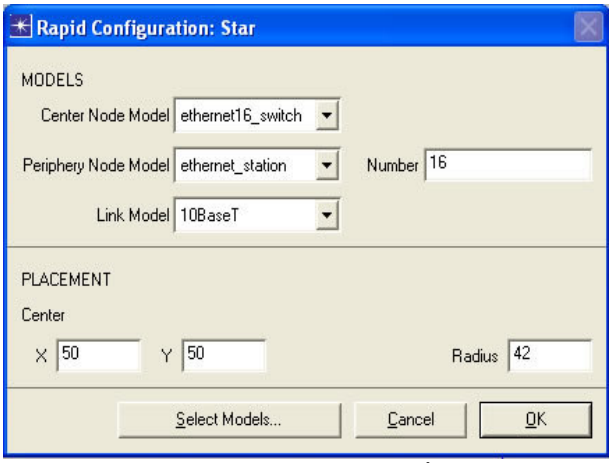


Figura 2.13 Valores de la configuración en estrella

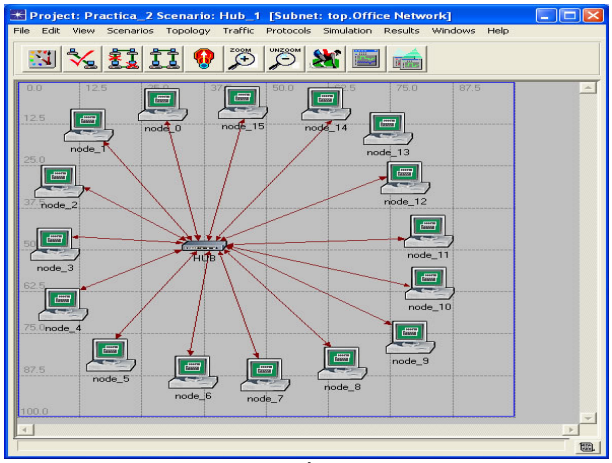


Figura 2.14 Topología estrella resultante

Indique cuál es el significado de Ethernet 16 y 10 Base T

_____

_____

_____

4.2.1.3 Configuración de los nodos de la red

Esta sección tiene como fin configurar el tráfico generado por las estaciones de trabajo en la red anterior.

1. Cambie el nombre del node_16 a Hub1, de la siguiente forma: con el botón derecho del ratón sobre el node_16, seleccione Edit Attributes_name = Hub1, haga clic en OK.
2. Obtenga el menú contextual de uno de los nodos de la red y seleccione la opción Select Similar Nodes. De esta forma todos los nodos estarán seleccionados, ver Figura 2.15.
3. Seleccione nuevamente el menú contextual, haciendo clic derecho sobre cualquiera de las estaciones y seleccione la opción Edit Atributes, ver Figura 2.16.

4. Active la opción Apply Changes to Selected Objects, de esta manera no habrá necesidad de configurar cada uno de los nodos individualmente, ver Figura 2.17.

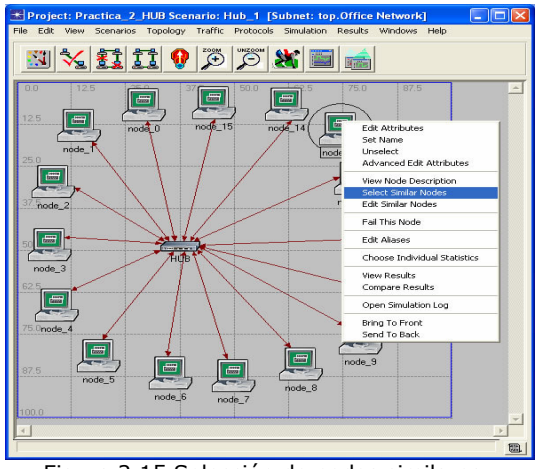


Figura 2.15 Selección de nodos similares

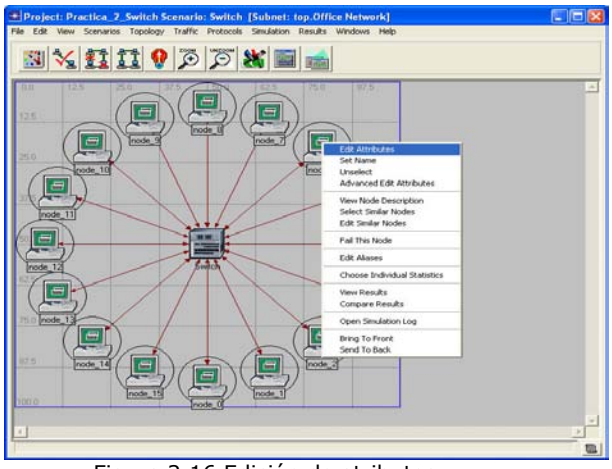


Figura 2.16 Edición de atributos

5. Expanda los atributos Traffic Generation Parameters y Packet Generation Arguments e introduzca los valores de acuerdo a la Tabla No. 2.2. Haga clic en OK, ver Figura 2.17.

	Características	Valores
Traffic Generation Parametres	**ON State Time (seconds)**	Exponential(100.0)
	OFF State Time (seconds)	Exponential(0.0)
Packet Generations Arguments	**Interarrivel Time (seconds)**	Exponential(0.02)
	Packet Size(bytes)	Constant (1500)

Tabla No. 2.2 Valores para la configuración de la red

6. Guarde el provecto a través del método abreviado Ctrl +S.

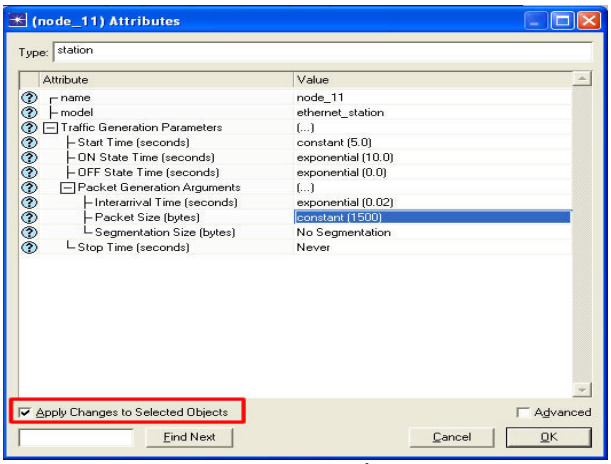


Figura 2.17 Generando el tráfico en los nodos

4.1.2.4 Elección de estadísticas

En esta sección configurará las estadísticas calculadas durante la simulación.

1. Haga clic derecho sobre cualquier punto del área de trabajo, que no sea un nodo o un enlace y seleccione la opción Choose Individual Statistics, ver Figura 2.18.
2. Active las siguientes estadísticas en el cuadro de diálogo Choose Results y haga clic en OK, ver Figura 2.19:

    - Global Statistics> Ethernet> Delay(sec).
    - Global Statistics> Traffic Sink> Trafficc Received(packets/sec).
    - Global Statistics> Traffic Source> Traffic Sent(packets/sec).
    - Node Statistics> Ethernet> Collision Count.

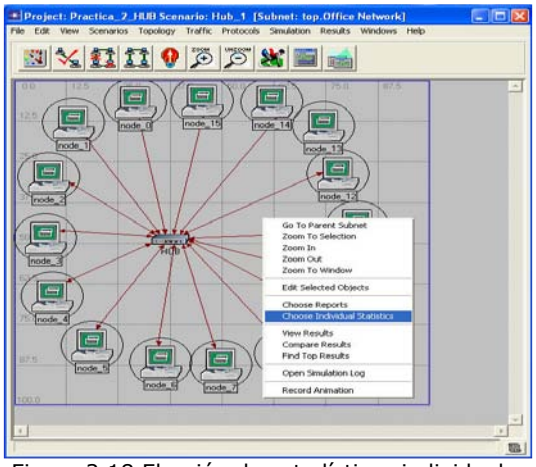


Figura 2.18 Elección de estadísticas individuales

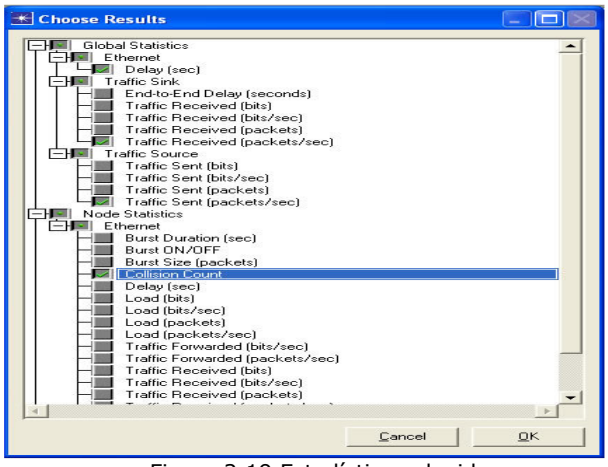


Figura 2.19 Estadísticas elegidas

Investigue en qué consiste la estadística Ethernet Delay, Traffic Received, Traffic Sent y Colision Count.

_____

_____

_____

4.1.2.5 Configuración de la simulación

Esta sección tiene como objetivo configurar los parámetros de duración de la simulación.

1. Haga clic en el botón Configure/Run Simulation, ver Figura 2.20.
2. Seleccione en el campo Duration el valor de 2 minutos y haga clic en Run, para ejecutar la simulación ver Figura 2.21.

Figura 2.20 Botón de configuración de simulación

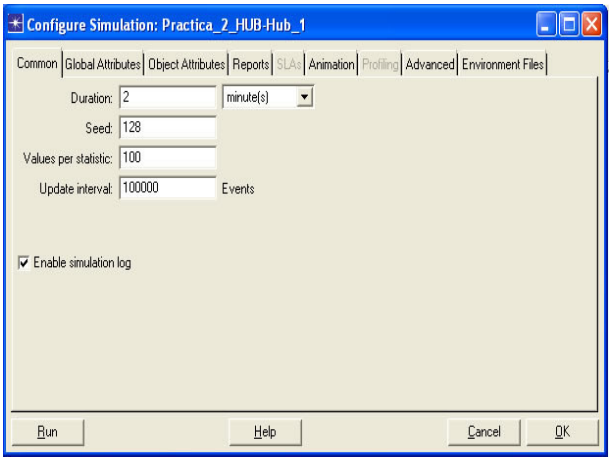


Figura 2.21 Elección de 2 minutos

3. Una vez que haya terminado la simulación haga clic en el botón Close del cuadro de diálogo de simulación.
4. Haga clic derecho sobre un punto en el área de trabajo y seleccione View Results.
5. Del cuadro de diálogo de View Results seleccione Global Statistics>Ethernet>Delay(sec) .
6. Repita el paso 5 seleccionando Global Statistics>Traffic Sink>Traffic Received(packets/sec).
7. Repita el paso 5 seleccionando Global Statistics>Traffic Source>Traffic Sent(packets/sec).

4.1.2.6 Análisis de resultados

Analice la gráfica de la Figura 2.22 que representa el retardo del hub e indique su importancia para un administrador de redes.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

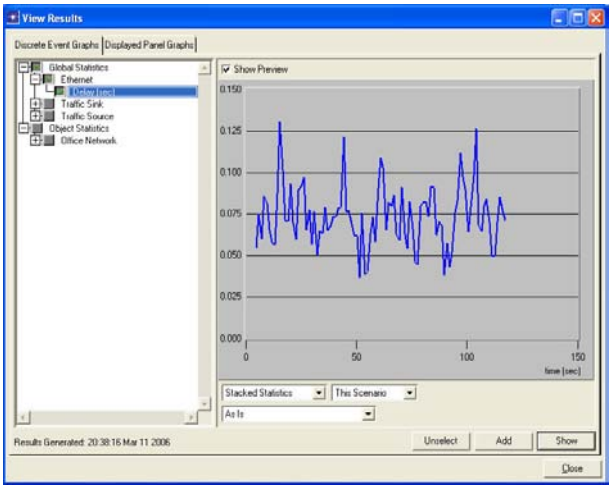


Figura 2.22 Estadística del retardo

Analice la estadística del tráfico recibido de la Figura 2.23 e indique la importancia de ésta, para un administrador de redes.

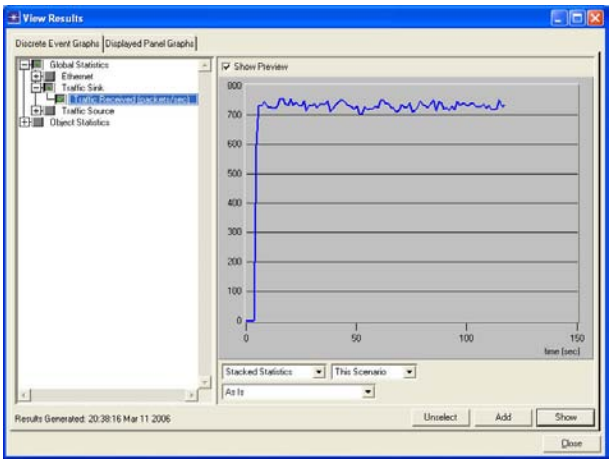


Figura 2.23 Estadística del tráfico recibido

Nota: Minimice los la simulación.

4.2 Switch

Un switch es un dispositivo hardware que incluye componentes similares a una computadora personal: CPU, RAM y un IOS, Sistema Operativo de Red (Internetworking Operating System). Puede ser administrado de la misma forma que un router o bien mediante una consola conectada a un puerto ya sea por Telnet o bien vía FTP.

Estos dispositivos de interconexión corresponden a la capa de enlace de datos, regularmente son implementados para preservar el ancho de banda de la red al utilizar la segmentación, ya que reenvían paquetes a un segmento en particular, utilizando el direccionamiento de hardware MAC.

Los switches pueden ser clasificados de acuerdo a la técnica que emplean, para el reenvío de los paquetes al segmento apropiado en:

- store-and-forward, en esta técnica los switches procesan completamente el paquete incluyendo el campo del algoritmo CRC y la determinación del direccionamiento del paquete. Esto requiere el almacenamiento temporal del paquete antes de ser enviado al segmento apropiado. Su principal ventaja es la eliminación del número de paquetes dañados que son enviados a la red.
- cut-through, esta técnica implementada por los switches hace que sean más rápidos, debido a que envían los paquetes tan pronto la dirección MAC es leída.

El switch implementado en el Laboratorio utiliza la primera técnica: store and forward.

4.2.1 Introducción y comandos básicos

Indique los componentes de la vista frontal del switch implementado en el Laboratorio de Redes, ver Figura 2.24.

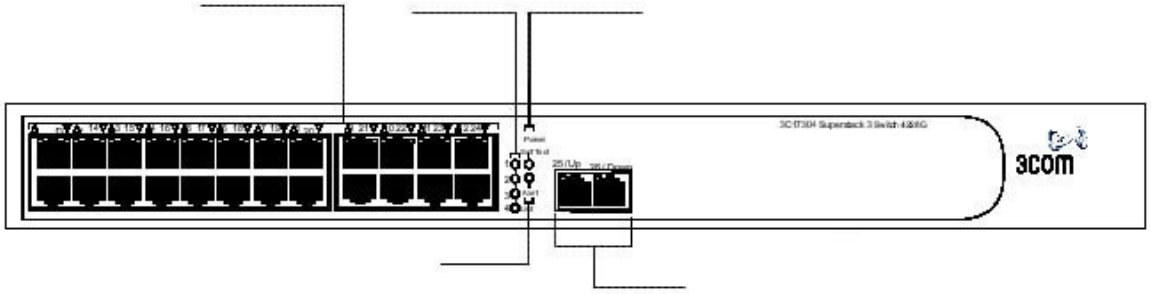


Figura 2.24 Vista frontal del switch 3COM 3C17300 Superstack 3Switch 4226T

Investigue el significado de los leds del switch 3COM 3C17300 Superstack 3Switch 4226T.

Indique los componentes de la vista posterior del switch implementado en el Laboratorio de Redes, ver Figura 2.25.

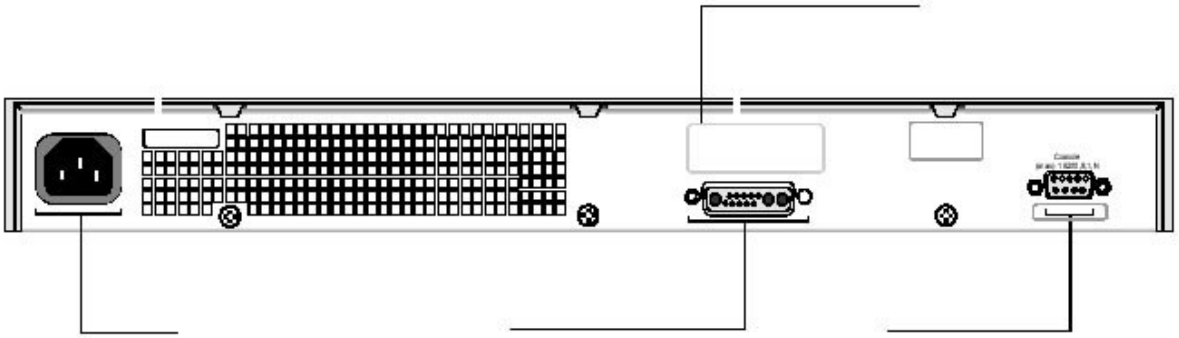


Figura 2.25 Vista posterior del switch 3COM 3C17300 Superstack 3Switch 4226T

Cuando un switch no conoce la dirección MAC de destino, envía la trama por todos sus puertos, al igual que un hub, a esta acción se le como flooding, inundación.

¿A qué se le denomina segmento de red?

Para cambiar y supervisar el funcionamiento de un switch es necesario acceder al software de administración que reside en él. El objetivo de administrar un switch es mejorar su rendimiento y por ende el rendimiento global de la red.

El proceso de configuración del switch se inicia cuando se enciende, la información de IP se configura de forma automática. Si se desea configurar manualmente la información de la IP,

es necesario indicar como establecer la conexión con el switch, ésta puede ser de dos formas:

a. Conexión a un puerto del panel frontal, lo cual implica la conexión de una estación de trabajo mediante un cable Ethernet a un puerto del panel frontal del switch.
b. Conexión al puerto de consola, radica en la conexión de una estación de trabajo mediante un cable módem nulo al puerto de consola.

4.2.1 Administración vía Web

El objetivo de este punto es la configuración manual de la dirección IP del switch accediendo a él a través de la conexión Web.

Este método resulta muy intuitivo ya que muestra en una página Web una representación gráfica del panel de puertos del switch, indicando aquéllos que se encuentran conectados y activos, también es posible solicitar que se muestren los que están operando en modo full dúplex o con control de flujo.

En la misma página inicial se indica el tiempo de operación del equipo en días, horas, minutos y segundos; así como una liga para iniciar una sesión Telnet. Al hacer clic sobre cualquiera de los puertos representados se ingresa a las opciones de configuración donde, a su vez, se puede introducir un nombre para cada puerto. Asimismo es posible habilitar o desactivar la administración de puertos individuales, al igual que la auto-negociación.

¿Por qué no se recomienda utilizar una sesión Telnet?

_____
_____
_____

Nota Profesor: Esta parte de la práctica se realiza en un equipo cercano al switch.

1. Compruebe que un extremo del cable Ethernet esté conectado a la NIC de la estación de trabajo y el otro extremo a uno de los puertos del panel frontal del switch, ver Figura 2.26.

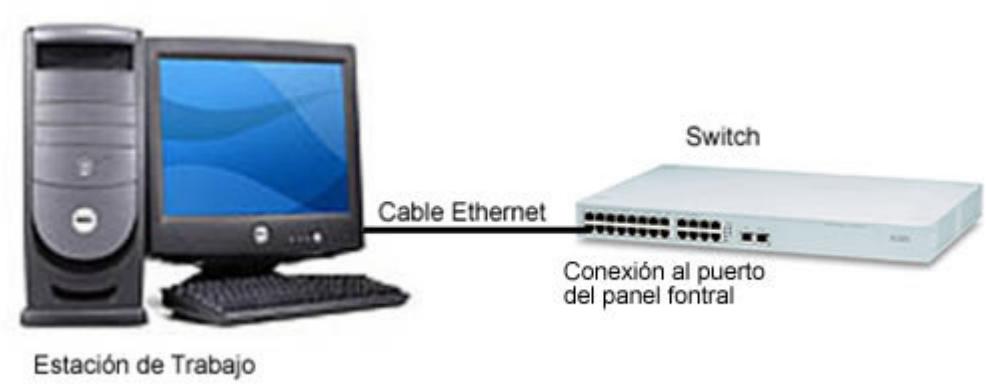


Figura 2.26 Conexión de una estación de trabajo al switch mediante un puerto del panel frontal

Nota Profesor: El switch tiene que estar desconectado al iniciar la práctica y los cables desconectados del panel de parcheo.

2. Encienda el switch, esta operación tiene una duración de un minuto aproximadamente, ver Figuras 2.27 y 2.28.

Figura 2.27 Encendido del switch

Figura 2.28 Proceso de testeo del switch

Describa el proceso de inicialización de un switch.

_____

_____

_____

3. Abra un navegador Web como Internet Explorer y escriba la dirección 192.168.2.123 en el campo del URL, esta es la dirección que se asignó al switch para poder ser administrado, ver Figura 2.29

Figura 2.29 Solicitud de usuario y contraseña

4. En los campos de usuario y contraseña escriba ***admin***, como nombre de usuario y haga clic en la tecla Enter en el indicador de contraseña. Estos campos son los predeterminados en la configuración inicial.

En este momento las páginas Getting Started permiten consultar información básica de la configuración del switch, ver Figura 2.30.

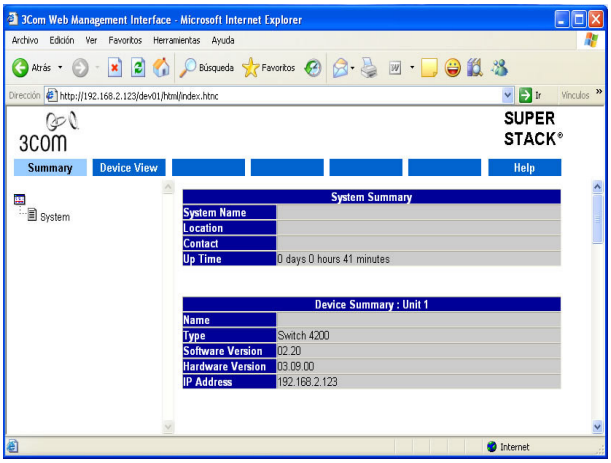


Figura 2.30 Configuración básica del switch

5. Seleccione el botón del menú Device View y se muestra un menú del lado izquierdo en forma jerárquica. Expanda la opción System y haga clic en Getting Started, ver Figura 2.31.

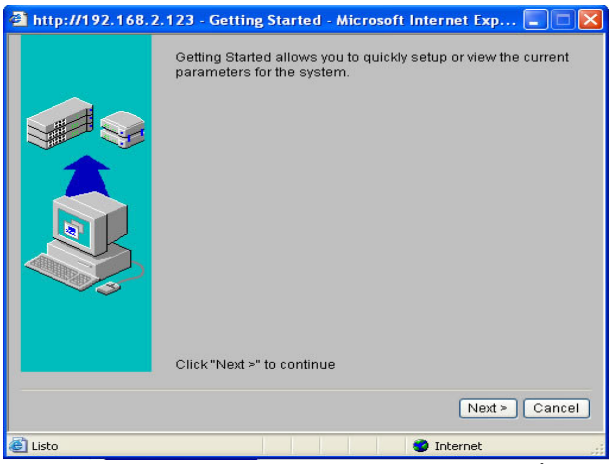


Figura 2.31 Asistente de inicio de configuración

Nota: Los cambios en la configuración del switch sólo pueden hacerse desde un navegador a la vez.

6. Haga clic en el botón Next y el asistente solicita un nombre, ubicación y contacto del sistema. Introduzca los siguientes valores: Switch_GRUPO, Laboratorio de Redes_GRUPO y Nombre del Administrador del Laboratorio de Redes_GRUPO. Haga clic en Next, ver Figura 2.32.

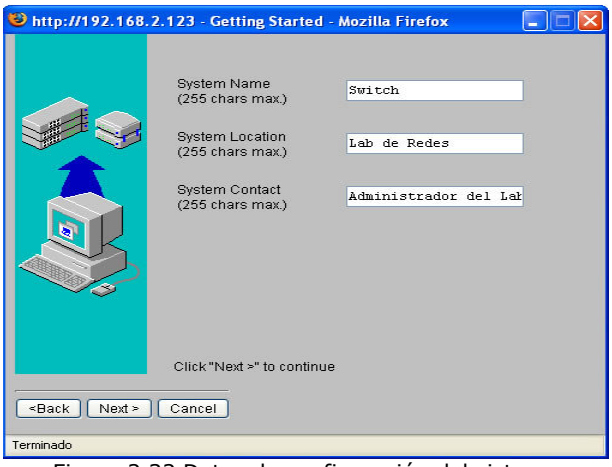


Figura 2.32 Datos de configuración del sistema

7. Seleccione la opción de configuración de IP Manual y haga clic en Next, ver Figura 2.33.

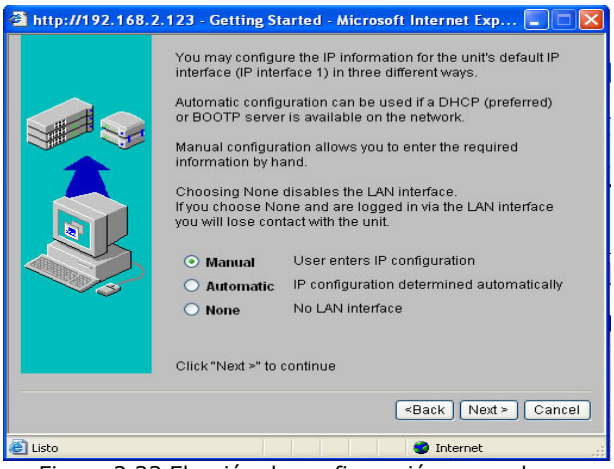


Figura 2.33 Elección de configuración manual

8. Anote la configuración de IP existente en la Tabla No. 2.3 para restaurarla al final de esta parte de la práctica.

	Valores
Dirección IP	
Máscara de subred	
Puerta de enlace predeterminada	

Tabla No. 2.3 Configuración actual del switch

9. Escriba la siguiente dirección IP, máscara de subred y puerta de enlace predeterminada que utilizará el switch cuando esté conectado a la red, ver Figura 2.34. Haga clic en Next.

	Valores
Dirección IP	**192.168.2.125**
Máscara de Subred	**255.255.255.0**
Puerta de enlace predeterminada	**192.168.2.1**

Tabla No. 2.4 Nueva configuración del switch

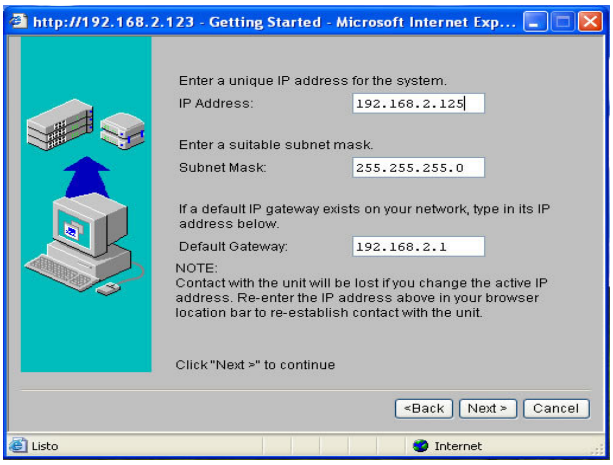


Figura 2.34 Configuración manual

10. El asistente solicita un password para el usuario de administración del switch, introduzca en el campo New Password: ***redadmin.*** y confirme el nuevo password. Haga clic en Next, ver Figura 2.35.

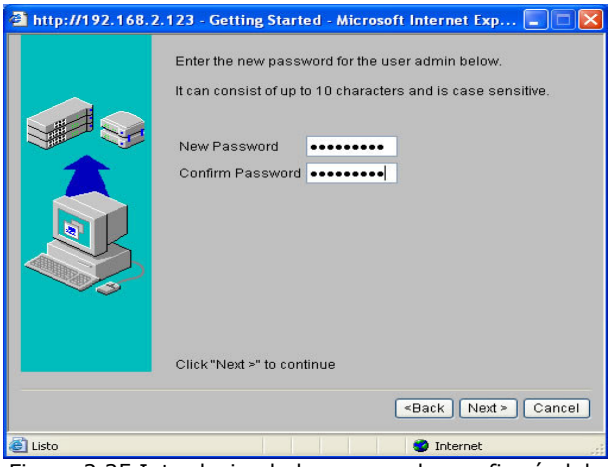


Figura 2.35 Introduciendo la password y confirmándolo

11. La siguiente ventana muestra un resumen de la información introducida, hasta este punto se ha completado la configuración inicial del switch preparado para que en la Práctica 3 se configure el método de administración seleccionado. Haga clic en Finish, ver Figura 2.36.

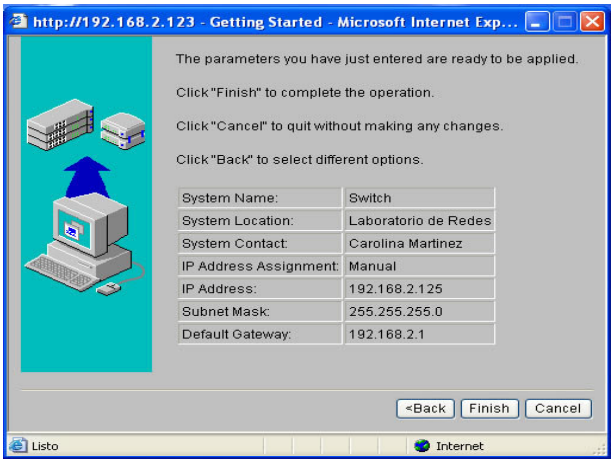


Figura 2.36 Ventana de resumen final

12. Introduzca nueva dirección IP en un navegador, es necesario introducir nuevamente el usuario y el password ahora configurado para confirmar los cambios. Observe la página Getting Started con los cambios realizados, ver Figura 2.37.

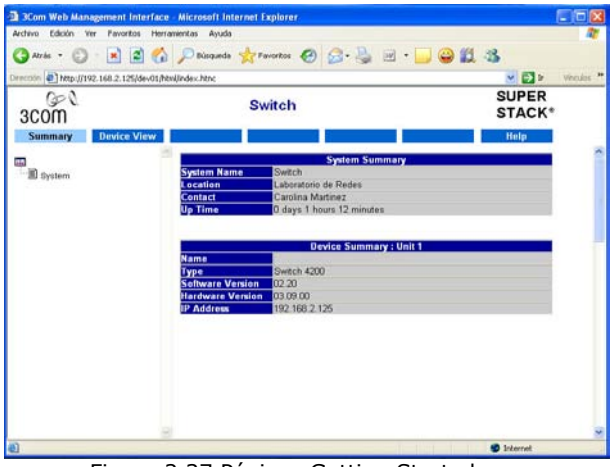


Figura 2.37 Páginas Getting Started

13. Repita los pasos anteriores para restablecer la configuración inicial del switch con ayuda de la Tabla No. 2.3.

4.2.3 Administración vía consola

Para configurar manualmente la dirección IP del switch es posible establecer una conexión al puerto consola, mientras el switch no está en línea o mientras el switch está conectado a la red mediante un cable de módem nulo estándar, ver Figura 2.38.

Figura 2.38 Configuración de IP mediante la consola del switch

1. Conecte un extremo del cable al conector macho del puerto de consola del switch, ver Figuras 2.39 y 2.40.

Figura 2.39 Cable módem nulo estándar

Figura 2.40 Conexión de los cables

2. Sujete los tornillos del cable para evitar que se afloje.
3. Conecte el otro extremo del cable a uno de los puertos serie también conocidos como puertos COM de la estación de trabajo, ver Figura 2.41.

Figura 2.41 Puerto serie de la estación de trabajo

4. Abra el software de emulación de terminal mediante el menú Inicio>Todos los Programas>Accesorios>Comunicaciones>Hyper Terminal.

5. En la ventana descripción de la conexión escriba en el campo nombre Switch y elija el icono que lo representará. Haga clic en Aceptar, ver Figura 2.42.

6. En la siguiente ventana elija la opción conectar usando el puerto COM1 y haga clic en Aceptar. Configure los valores del puerto COM al que se conecto el cable, de acuerdo a la Tabla No. 2.5. Haga clic en Aplicar y posteriormente en el botón Aceptar.

Figura 2.42 Hyper Terminal

Opciones	Valor
Bits por segundo:	19,200
Bits de Datos:	8
Paridad:	Ninguno
Bits de parada:	1
Control de Flujo:	Ninguno

Tabla No. 2.5 Configuración del software de emulación de terminal

7. Se muestra una terminal conectada al switch. Presione la tecla Enter y se mostrará un prompt solicitando el login, introduzca admin y presione Enter en el campo de password. Observe el menú de opciones del switch, ver Figura 2.43.

```
Menu options: --------------3Com SuperStack 3 Switch 4200---------------

 bridge             - Administer bridge-wide parameters
 logout             - Logout of the Command Line Interface
 physicalInterface  - Administer physical interfaces
 protocol           - Administer protocols
 security           - Administer security
 system             - Administer system-level functions
 trafficManagement  - Administer traffic management

Type  ? for help
---------------------------------------- (1)--------------------------
```

Figura 2.43 Menú del switch 3Com SuperStack 3 Switch 4200

Navegue a través del menú principal y anote 5 opciones del mismo.

_____
_____
_____

8. Introduzca la opción Getting Started en el prompt, en ese momento se pregunta el tipo de configuración a realizar la cual puede ser auto, manual y none. Introduzca la opción manual.
9. Ingrese la nueva configuración de dirección IP, máscara de subred y puerta de enlace de acuerdo a la Tabla No. 2.4, ver Figura 2.44.

```
---------------------------------------- (1)--------------------------
Select menu option: gettingStarted

IMPORTANT NOTES
Changes made will only be applied at the end of this dialogue.
To return to the top level menu or abort an action, press the [Esc] key.

Hitting return without entering a new value when prompted will
select the value displayed within the brackets '[]'.

IP ADDRESS DET
Select an IP address assignment method [current method shown].
auto - automatically allocate IP address using DHCP/BootP
manual - manually enter IP address
none - IP address not required

Enter your selection (auto,manual,none)[manual]: manual
Enter IP address           [192.168.2.123  ]: 192.168.2.125
Enter subnet mask          [255.255.255.0  ]: 255.255.255.0
Enter default gateway      [192.168.2.1    ]: 192.168.2.1
```

Figura 2.44 Configuración del switch

10. Introduzca el nombre del sistema: Switch_GRUPO, en ubicación: Lab de Redes_GRUPO y el contacto: Administrador Lab_GRUPO, ver Figura 2.45.

```
SYSTEM DETAILS
Enter system name     []: Switch
Enter system location []: Lab de Redes
Enter system contact  []: Administrador del Lab
```

Figura 2.45 Configuración de parámetros del switch

11. Se muestra una recomendación del uso de contraseñas. Conteste afirmativamente a la pregunta de la asignación del password.
12. Introduzca el password para el usuario admin: **redadmin.** y confirme el password.

13. Introduzca el password para el usuario manager: **redadmin2.** y confirme el password.
14. Introduzca el password para el usuario monitor: **redadmin3.** y confirme el password.

Investigue la diferencia entre los usuarios admin, manager y monitor.

_____
_____
_____

15. Se muestra el menú de configuración avanzada, preguntando si se desea realizar la configuración avanzada con SNMP. Responda no a lo anterior.
16. Se presenta el resumen de los parámetros configurados y se pregunta si se desean aplicar. Responda sí a lo anterior, ver Figura 2.46.

```
SUMMARY
The parameters you have just entered are ready to be applied:

IP address assignment method:  Manual
IP address:                    192.168.2.125
Subnet mask:                   255.255.255.0
Default gateway:               192.168.2.1
System name:                   Switch
System location:               Lab de Redes
System contact:                Administrador del Lab

WARNING: A change of IP address details will cause loss of management
communication with the device.
You will need to re-establish contact with the device after the new


Do you wish to apply parameters? (yes,no)[no]: yes

Select menu option:
```

Figura 2.46 Resumen de la configuración

17. Restaure la configuración inicial de acuerdo a los valores proporcionados por la Tabla No. 2.3.
18. Finalmente salga con el comando ***logout***
19. Salga de la terminal desde el menú Archivo>Salir. Responda afirmativamente a la pregunta Desconectar ahora. Responda no a la pregunta de ¿Desea guardar la conexión con el nombre Switch?

Nota: Para restaurar la configuración de los password únicamente introduzca Enter.

20. Desconecte el cable de los equipos.

Algunos switches tienen comandos similares a los routers, este apartado tiene por objetivo conocer algunos comandos básicos de los switches Cisco.

1. Inicie el simulador RouterSim CCNA a través del menú Inicio>Todos los programas>RouterSim CCNA.
2. Haga clic en el botón Continue.
3. Haga clic en el botón Net Visualizer y arrastre un switch 1900 al área de trabajo.
4. Haga doble clic sobre éste y observe la línea de consola.

Anote las opciones que presenta el menú de interfaz de usuario.

_____
_____
_____

5. Navegue entre las opciones del menú.
6. Cierre el simulador.

4.2.4 Análisis del rendimiento de un switch

El objetivo de este apartado es analizar el rendimiento del switch para posteriormente hacer comparaciones con el rendimiento del hub, estudiado en el punto anterior.

4.2.4.1 Creación de un nuevo proyecto

Para la creación de la red a analizar, realice los siguientes pasos:

1. Cierre las estadísticas de la anterior simulación.
2. Seleccione File>New> y elija del menú desplegable Project. Haga clic en OK, ver Figura 2.3.
3. Se presenta una ventana, que solicita el nombre del proyecto y el nombre del escenario, ver Figura 2.4. En el campo de Project Name, introduzca el siguiente nombre: iniciales_LAN2 y para el campo Scenario Name: Switch.

4.2.4.2 Creación de la red

1. Se inicia el asistente de configuración rápida. En la elección Topology elija Create Empty Scenario y haga clic en Next, ver Figura 2.5.
2. Seleccione la escala de red, como Office y haga clic en Next, ver Figura 2.6.
3. En la siguiente pantalla se solicitan las medidas de la escala de red seleccionada. Introduzca los valores para X e Y = 100m y haga clic en Next, ver Figura 2.7.
4. La siguiente ventana solicita que seleccione la Tecnología de Red, para esta simulación únicamente haga clic en Next, ver Figura 2.8.
5. Revise los valores introducidos anteriormente y haga clic en OK, ver Figura 2.9.
6. El programa muestra el área de trabajo y una paleta de objetos, ver Figura 2.10. Cierre la paleta de objetos y seleccione del menú Topology, la opción Rapid Configuration.
7. Seleccione la opción Star del menú de Rápida Configuración y haga clic en OK, ver Figura 2.11.
8. Haga clic sobe el botón Select Models, active la opción Model List y seleccione ethernet. Haga clic en OK, ver Figura 2.12.

9 Se muestra un asistente de Configuración Rápida, introduzca los valores descritos en la Tabla No. 2.6, para cada uno de los campos y haga clic en Ok, Figura 2.47.

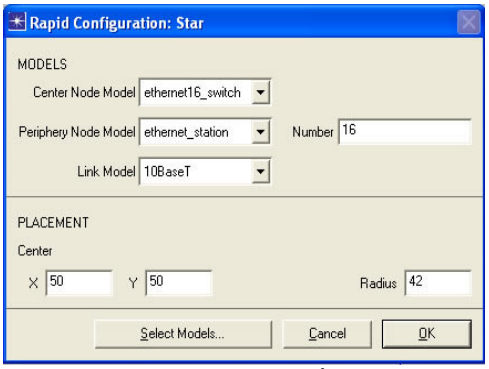


Figura 2.47 Configuración del switch

Características	Valores
Center Node Model	Ethernet16_Switch
Periphery Node Model	ethernet_station
Link Model	10BaseT
Number	16
X	50
Y	50
Radios	42

Tabla No. 2.6 Valores para la configuración de la red

4.2.4.3 Configuración de los nodos de la red

Repita los pasos realizados en la sección 4.1.2.3, para configurar los nodos que integran la red del switch, ver Figura 2.48. Cambiando el nombre de node_16 a Switch1.

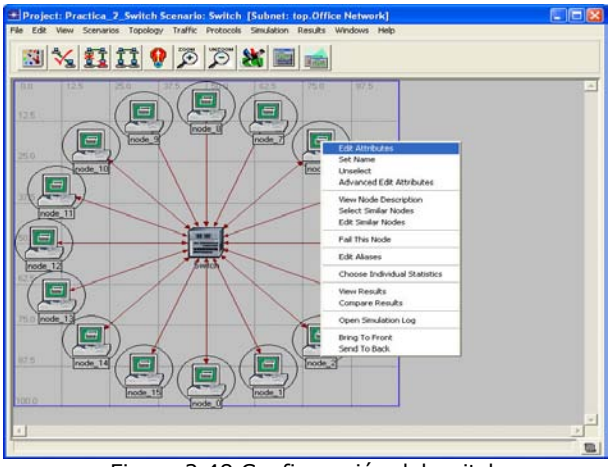


Figura 2.48 Configuración del switch

4.2.4.4 Elección de estadística

Repita los pasos realizados en la sección 4.1.2.4, para configurar los nodos que integran la red del switch.

4.2.4.5 Configuración de la simulación

Repita los pasos realizados en la sección 4.1.2.5, para configurar los nodos que integran la red del switch.

4.2.4.6 Análisis de resultados

Analice la gráfica de la Figura 2.49 que representa el tráfico recibido por el switch e indique su importancia para un administrador de redes.

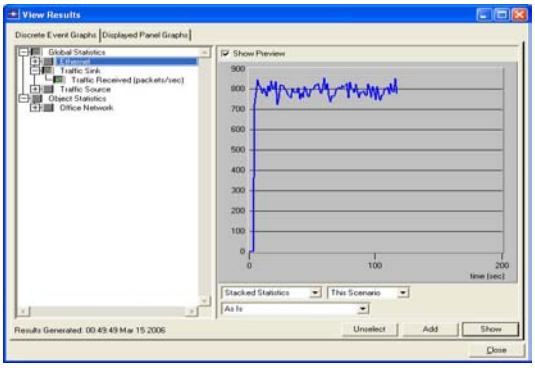


Figura 2.49 Tráfico recibido por el switch

Analice la gráfica de la Figura 2.50 que representa el tráfico enviado por el switch e indique su importancia para un administrador de redes.

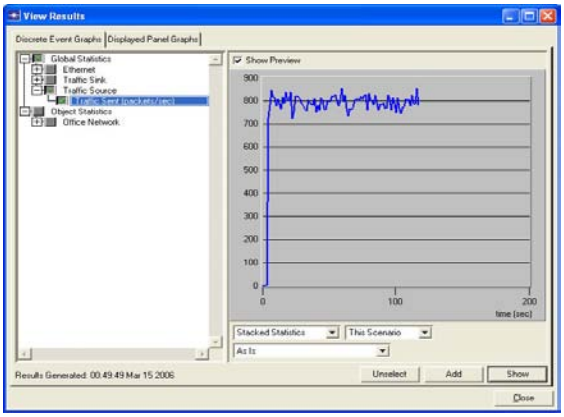


Figura 2.50 Tráfico enviado por el switch

Analice la gráfica de la Figura 2.51 que representa el retardo dentro del switch e indique su importancia para un administrador de redes.

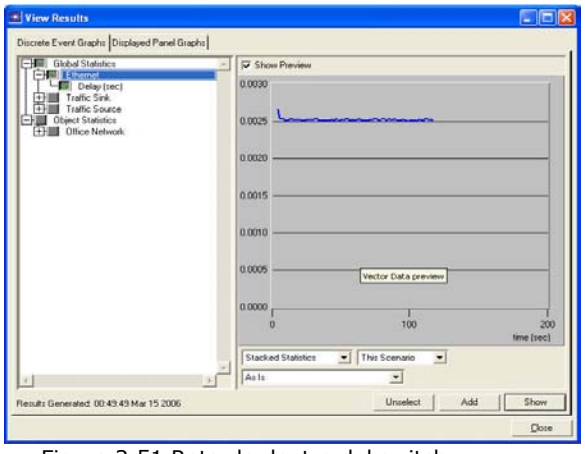


Figura 2.51 Retardo dentro del switch

Mencione la diferencia existente entre el hub y el switch

5.- Conclusiones y comentarios

6.- Cuestionario Previo

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 2 Parte B
Manejo de Dispositivos de Interconectividad

1.- Objetivo de aprendizaje

El alumno desarrollará las habilidades necesarias que le permitan la manipulación de equipos de interconexión como lo son los routers.

El alumno analizará el comportamiento de las tablas de ruteo estáticas dentro de una red de área local, mediante una herramienta de simulación de redes: RouterSim CCNA v3.0 de Cisco.

2.- Conceptos teóricos

Un protocolo de ruteo es aquel que se encarga de encontrar la ruta más corta para que los paquetes de información accedan a su destino lo más pronto posible, basándose en las tablas de ruteo que cada uno maneja y para lo cual intercambian información entre routers dentro de un AS, Sistema Autónomo (Autonomous System) que les permite actualizar continuamente dichas tablas de ruteo.

Existe una clasificación de los protocolos de ruteo en internos y externos: IGP y EGP. Los IGP, Protocolos de Ruteo Interior (Interior Routing Protocols) proporcionan un punto de decisión sobre qué ruta hay que tomar para llegar al destino basándose en información de distancia, tráfico y estado de rutas, entre los más importantes se encuentran: RIP, Protocolo de Información de Ruteo (Routing Information Protocol) y OSPF, Primera Ruta Más Corta (Open Short Path First), ver Figura 2.1.

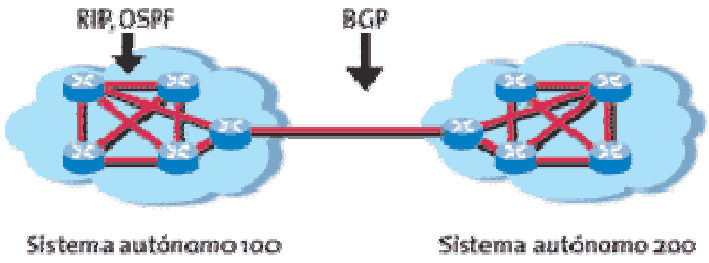


Figura 2.1 Relación entre protocolos de ruteo externo e interno

Los routers se comunican constantemente entre sí para informarse de las rutas bloqueadas, de las máquinas intermedias saturadas o caídas, etc. La habilidad de los routers, de tomar decisiones de hacia donde deben ser dirigidos los paquetes, la consiguen almacenando en su interior una tabla especial llamada tabla de ruteo. La lista de rutas que se almacena en una tabla de ruteo identifica cada entrada con una red o host destino. Periódicamente, cada router envía una copia de su tabla ruteo a cualquier otro router que pueda alcanzar directamente y así se actualizan. De esta manera cuando un paquete llega a un router, éste analiza su tabla de ruteo si en ésta existe una referencia a la dirección IP de la máquina destino, también lo estará el puerto por el que es accesible, de manera que por ahí se envía el paquete. En el caso de no encontrar ninguna referencia en la tabla, el router manda una petición de respuesta por todos los puertos, preguntando en cual de ellos se encuentra la máquina destino y una vez obtenido el puerto de acceso ingresa la tupla IP/Puerto en su tabla de ruteo, con lo que los nuevos paquetes para esa máquina serán enviados directamente.

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- PC's Pentium con una NIC Ethernet 10/100 Mbps instalada en cada una de ellas.
- Software de Simulación Cisco, RouterSim CCNA v 3.0.

4.- Desarrollo

4.1 Router

El router es un dispositivo hardware, o bien un software corriendo sobre una computadora, encargado principalmente de tomar decisiones de paquetes de acuerdo a las tablas de ruteo almacenadas. Normalmente un router cuenta con al menos 2 interfases de red, como pueden ser seriales o ethernet y puertos de consola auxiliar.

En el caso de los routers Cisco, son dispositivos hardware con un sistema operativo propietario llamado IOS, Sistema Operativo de Red (Internetworking Operating System) que además de su función fundamental, es capaz de hacer filtrado de paquetes, firewalling, traducción de direcciones, priorización de tráfico, etc.

Cuando un router identifica la dirección IP de un paquete, determina cual es el camino que debe seguir, decidiendo si envía el paquete de información por cable o por satélite, dependiendo de la lejanía.

Es posible clasificar a los routers en:

- Routers estáticos, los cuales no determinan rutas por lo que es necesario configurar la tabla de ruteo, especificando las rutas potenciales para los paquetes.
- Routers dinámicos, que tienen la capacidad de determinar rutas y encontrar la más óptima de acuerdo a la información de los paquetes y de otros routers.

4.1.1 Introducción y comandos básicos

Este punto de la práctica tiene por objetivo conocer los comandos básicos de un router Cisco, empleando el simulador RouterSim CCNA, éste es una herramienta que permite el diseño, construcción y configuración directa de routers, switches y hosts.

4.1.1.1 Modos básicos de un router

Los routers funcionan con tres modos básicos:

a. Modo de usuario, en este modo se entra por defecto, permite pocas opciones, principalmente las relacionadas con estadísticas.
b. Modo privilegiado, entramos en éste mediante el comando ***enable*** y es similar a un root en un sistema operativo Linux.
c. Modo de configuración, entramos en él mediante el comando ***configure terminal*** y permite modificar la configuración del router.

1. Inicie el simulador RouterSim CCNA a través del menú Inicio>Todos los programas>RouterSim CCNA, ver Figura 2.2.
2. Seleccione la opción Continue e inmediatamente se cargarán los elementos necesarios para realizar las simulaciones.
3. Haga clic en el botón Net Visualizer y tendrá un área de trabajo en la que colocará los dispositivos a estudiar, ver Figura 2.3.

Figura 2.2 Simulador de RouterSim CCNA

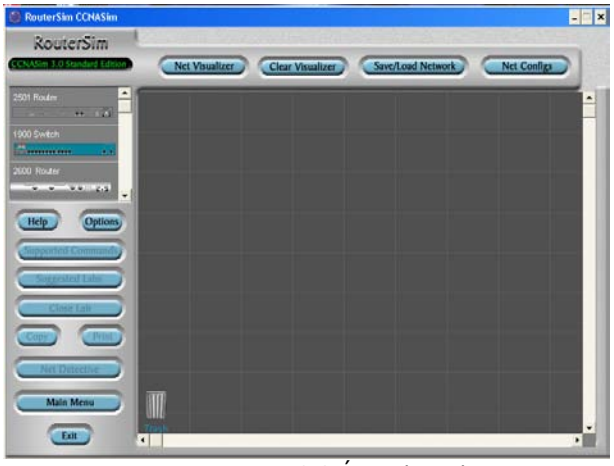


Figura 2.3 Área de trabajo

Para tener disponible una terminal CLI, Interfaz de Línea de Comandos, donde introducir las instrucciones necesarias, debe hacer doble clic sobre el router a analizar, ver Figuras 2.4 y 2.5. Al presionar Enter se tiene disponible el prompt en modo usuario, regularmente utilizado para conocer el estado del router.

Con el objeto de cambiar al modo privilegiado, debe teclear el comando ***enable***, recuerde observar el prompt ahora finalizado con el símbolo #.

Router>*enable*

Router#

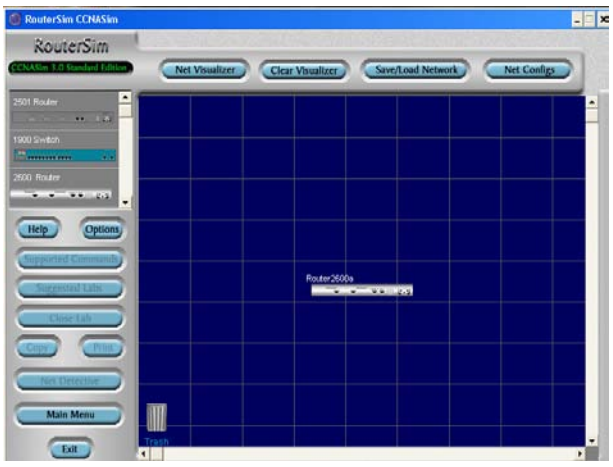


Figura 2.4 Área de trabajo con un router 2600a

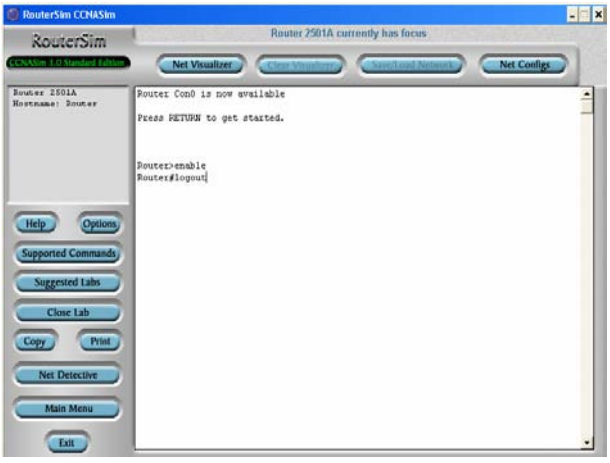


Figura 2.5 Línea de comando del router

Para salir del modo privilegiado es necesario desactivar la opción, tecleando el comando ***disable.*** Observe el prompt nuevamente con el símbolo > que identifica el modo usuario.

Router#*disable*

Router>

Para salir de la terminal ejecute el comando ***logout*** o ***exit***, de la siguiente manera:

Router>logout

Router con0 es now available.

Press RETURN to get started.

Nota: Siempre verifique el prompt antes de realizar algún cambio a la configuración de un router.

Investigue los componentes de un router.

_____
_____
_____

4.1.1.2 Proceso de configuración

Es importante conocer los diferentes tipos de prompt que existen en los routers para comprender su configuración. Para entrar en el modo de configuración de un dispositivo Cisco, es posible ejecutar cualquiera de las tres siguientes instrucciones en modo privilegiado:

a. configure terminal.
b. config t.
c. config.

El prompt del router en el modo configuración se obtiene tecleando el comando ***configure terminal***, en el modo privilegiado. Indique cada uno de los componentes del nuevo formato del prompt en las siguientes líneas, de acuerdo a la Figura 2.6.

_____
_____
_____

Dentro del modo configuración es posible manipular las interfases de un router. Para realizar cambios sobre dichas interfases, es necesario teclear el comando ***interface*** en modo configuración. Si no se conocen las opciones de la instrucción, la ayuda se obtiene a partir del comando ***interface ?***, ver Figura 2.7.

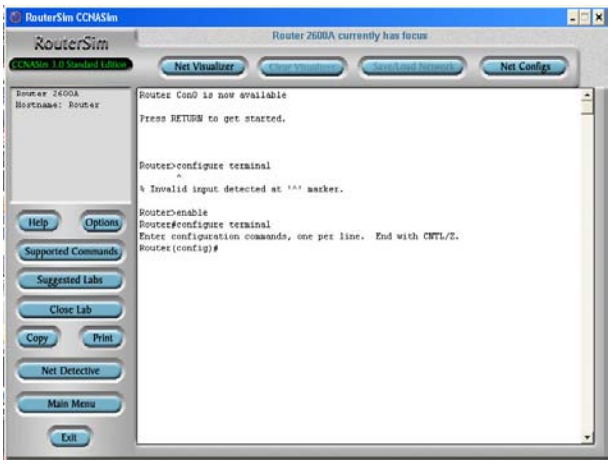


Figura 2.6 Prompt de configuración del router

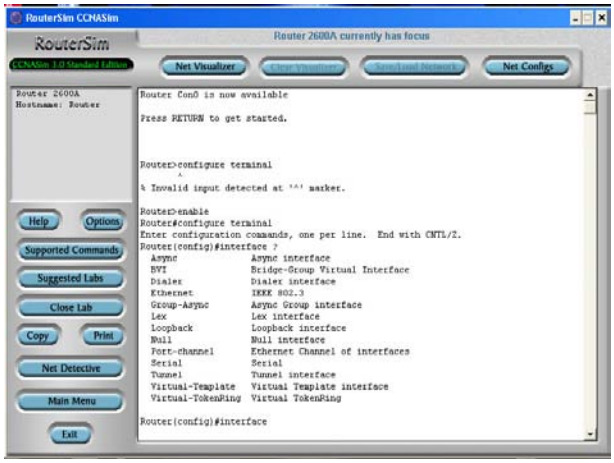


Figura 2.7 Ayuda del comando interface

Las contraseñas son las llaves del sistema, por lo que deben ser lo más seguras posibles para evitar inicios de sesión no autorizados, siendo éste el primer paso hacia problemas de seguridad mayores. El uso de contraseñas lo suficientemente fuertes como para amortizar un ataque, es un paso decisivo y a la vez sencillo que ahorra problemas en el futuro. Para cambiar la contraseña del modo privilegiado, debe ejecutar la siguiente instrucción en la CLI en modo configuración, de esta manera cuando vuelva a iniciar el modo privilegiado, el router solicitará una contraseña.

Router(config)*# enable secret todd*

Router(config)*# enable password cisco*

Para probar la nueva contraseña, es necesario salir del modo configuración, tecleando el comando ***exit,*** hasta salir del modo privilegiado.

Al iniciar sesión en el router presionando la tecla Enter y cambiando a modo privilegiado con el comando ***enable,*** el router solicita una contraseña, el siguiente paso será introducir la palabra todd y observar el prompt, ver Figuras 2.8 y 2.9.

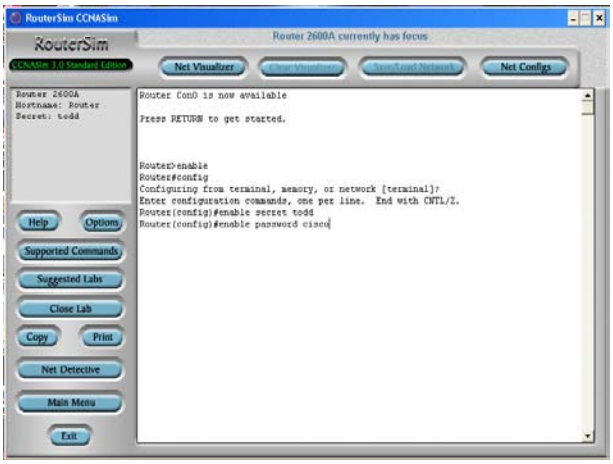


Figura 2.8 Cambiando la contraseña del router

Figura 2.9 Introduciendo la contraseña

Investigue el funcionamiento de la instrucción ***enable password cisco.***

_____
_____
_____

4.1.1.3 Obteniendo información de los routers

Los routers son dispositivos inteligentes ya que construyen las tablas de ruteo y mediante algoritmos determinan la mejor ruta posible para una transmisión en particular.

El comando ***show version***, provee de información básica acerca del hardware, así como la versión del software, los nombres y archivos de configuración, además de las imágenes de booteo.

Router>*show version*

El comando ***show running-config*** o ***show startup-config***, dentro del modo privilegiado, muestra la configuración del dispositivo cisco actual. La versión corta del comando anterior es ***sh run.***

Investigue las formas de acceso a un router Cisco.

_____
_____
_____

4.1.1.4 Configuración de interfases

La configuración de las interfases de un router, es el proceso más importante, debido a que sin ellas, el router es inservible, motivo por el cual su configuración debe estar activa a la hora de comunicarse con otros dispositivos.

La instrucción ***interface ?*** en la línea de comando, en modo configuración, muestra las opciones de los parámetros, dependiendo del dispositivo conectado.

Introducir el comando ***interface fastEthernet ?*** proporciona una salida que muestra las etiquetas de las interfases de red soportadas por el router.

Router(config)#*interface fastEthernet ?*
<0-1> Fast Ethernet interface number

Para configurar la interfase es necesario elegir una, mediante la siguiente instrucción:

Router(config)#*int fastEthernet 0?*

En algunas ocasiones es necesario elegir la interface que será configurada, mediante la opción mostrada en la siguiente instrucción:

Router(config)#*int fastEthernet 0/0*

Investigue que diferencia existe entre el comando ***interface fastEthernet 0/0*** e ***int fastEthernet 0/0***.

_____
_____
_____

4.1.1.5 Configuración de IP en las interfases

Para configurar la IP en una interfaz de red de un router, se utiliza el comando ***ip address***, desde el modo configuración, de la siguiente manera:

Router (config)#*int e0*

Router (config-if)#*ip address 172.16.10.2 255.255.255.0*

Router (config-if)#*no shut*

Investigue para qué se emplea el comando ***no shut*** en los routers Cisco.

_____
_____
_____

4.1.1.6 Configuración del hostname de un router

Es posible asignar un nombre a un router, el cual no afecta su funcionamiento ni comportamiento dentro de las redes, esto mediante la instrucción ***hostname***, en el modo configuración.

Router#*config t*

Router(config)#*hostname LabRx*

LabRx(config)#

El comando ***hostname*** tiene efecto inmediatamente después de dar Enter en la interfaz de línea de comando y es útil para identificar a los routers dentro de las redes.

4.1.1.7 Verificando la configuración del router

Existen diversas utilidades empleadas para verificar la configuración del router, tales como:

1. ping.
2. traceroute.
3. telnet.
4. show interface.

En el punto 4.1.2.2 Verificación de las tablas de ruteo, hará uso de la herramienta ping.

4.1.2 Configuración de un router

El objetivo de este punto es crear una configuración de routers de diferentes modelos que se comuniquen entre sí, a través de la configuración manual de sus tablas de ruteo.

1. Haga clic en el botón Net Visualizer, para obtener el área de trabajo.

2. Haga clic en el router 2501 y colóquelo en el espacio de trabajo. Repita este paso hasta obtener en el área de trabajo 5 routers 2501.
3. Haga clic en el router 2600 y colóquelo en el área de trabajo.
4. Haga las conexiones indicadas en la Tabla No. 2.1 para obtener un conjunto de routers interconectados, tal como se muestra en la Figura 2.10, haciendo clic derecho en el router inicial, seleccionando el puerto a conectar, indicando el tipo de conexión que para el caso de estudio es DTE, seleccionando el router final y haciendo clic en éste último para finalizar la conexión.

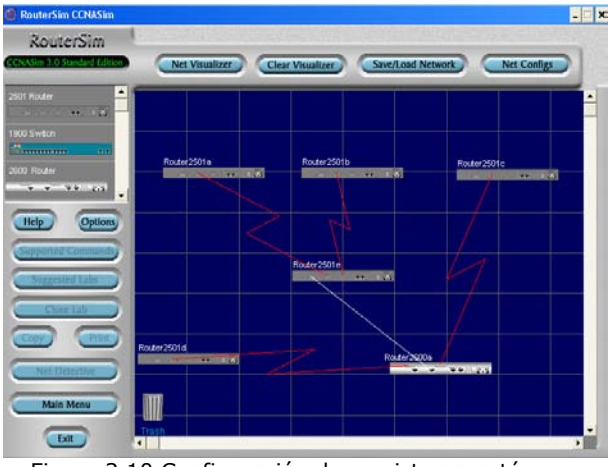


Figura 2.10 Configuración de un sistema autónomo

Router Inicial	Conexión	al	Router Final	Conexión
Router2501a	Puerto Serial 0 **S0**	→	Router2501e	Puerto Serial 0 **S0**
Router2501b	Puerto Serial 0 **S0**	→	Router2501e	Puerto Serial 1 **S1**
Router2501c	Puerto Serial 0 **S0**	→	Router2600a	Puerto Serial 0/0 **S0/0**
Router2501d	Puerto Serial 0 **S0**	→	Router2600a	Puerto Serial 0/1 **S0/1**
Router2501e	Puerto Ethernet **E0**	→	Router2600a	Puerto FastEthernet **F0/0**

Tabla No. 2.1 Tabla de conexiones de routers

Indique el cable empleado para realizar la conexión entre el puerto Ethernet de un router a un puerto fastEthernet de otro router.

_____
_____
_____

Nota: Es importante elegir la opción **DTE** cuando se hacen las conexiones entre routers.

5. Haga una conexión al router 2501a, haciendo doble clic sobre él. Presione la tecla Enter y asigne el nombre, password, descripción de interfases, banners y direcciones IP a cada interfase de acuerdo a las siguientes instrucciones, comentando la acción realizada por cada comando en su reporte final.

```
Router>enable
Router# config t
Router (config)# hostname 2501A
```

```
2501A (config)# enable secret todd
2501A (config)#line console 0
2501A (config-line)#login
2501A (config-line)#password todd
2501A (config-line)#line aux 0
2501A (config-line)#login
2501A (config-line)#password todd
2501A (config-line)#line vty 0 4
2501A (config-line)#login
2501A (config-line)#password todd
2501A (config-line)#interface ethernet0
2501A (config-if)#ip address 172.16.60.1  255.255.255.0
2501A (config-if)#description connection to LAN 60
2501A (config-if)#no shutdown
2501A (config-line)#interface serial0
2501A (config-if)#ip address 172.16.20.2  255.255.255.0
2501A (config-if)#description connection to 2501E
2501A (config-if)#no shutdown
2501A (config-if)#exit
2501A (config)#banner motd #
Este es el router 2501A
#
2501A (config)#exit
2501A#copy run star
```

6. Presione la tecla Enter para aceptar los cambios en el archivo startup-config y presione nuevamente Enter para sobrescribir la configuración.

7. Observe los cambios realizados en la configuración de los routers en la ventana superior izquierda.

8. Haga clic en el botón Net Visualizer.

9. Haga clic en el botón Save/Load Network, guarde el proyecto con la estructura iniciales_Routers, en C:\. El simulador pregunta si desea limpiar el escenario, haga clic en el botón No, de lo contrario se borrarán todas las configuraciones realizadas.

Investigue la función de la instrucción ***line aux 0***.

_____
_____
_____

10. Haga una conexión al router 2501b, haciendo doble clic sobre él. Presione la tecla Enter y asigne el nombre, password, descripción de interfases, banners y direcciones IP a cada interfase, de acuerdo a las siguientes instrucciones:

```
Router>enable
Router# config t
Router (config)# hostname 2501B
2501B (config)# enable secret todd
2501B (config)#line console 0
2501B (config-line)#login
2501B (config-line)#password todd
2501B (config-line)#line aux 0
```

```
2501B (config-line)#login
2501B (config-line)#password todd
2501B (config-line)#line vty 0 4
2501B (config-line)#login
2501B (config-line)#password todd
2501B (config-line)#interface ethernet0
2501B (config-if)#ip address 172.16.70.1  255.255.255.0
2501B (config-if)#description connection to LAN 70
2501B (config-if)#no shutdown
2501B (config-line)#interface serial0
2501B (config-if)#ip address 172.16.30.2  255.255.255.0
2501B (config-if)#description connection to 2501E
2501B (config-if)#no shutdown
2501B (config-if)#exit
2501B (config)#banner motd #
Este es el router 2501B
#
2501B (config)#exit
2501B#copy run star
```

11. Presione la tecla Enter para aceptar los cambios en el archivo startup-config y presione nuevamente Enter para sobrescribir la configuración.

12. Observe los cambios realizados en la configuración de los routers en la ventana superior izquierda.

13. Haga clic en el botón Net Visualizer.

14. Haga clic en el botón Save/Load Network, guarde el proyecto con la estructura iniciales_Routers, en C:\. El simulador pregunta si desea limpiar el escenario, haga clic en el botón No, de lo contrario se borrarán todas las configuraciones realizadas.

Investigue la función de la instrucción ***line vty 0 4.***

_____
_____
_____

15. Haga una conexión al router 2501c, haciendo doble clic sobre él. Presione la tecla Enter y asigne el nombre, password, descripción de interfases, banners y direcciones IP a cada interfase de acuerdo a las siguientes instrucciones:

```
Router>enable
Router# config t
Router (config)# hostname 2501C
2501C (config)# enable secret todd
2501C (config)#line console 0
2501C (config-line)#login
2501C (config-line)#password todd
2501C (config-line)#line aux 0
2501C (config-line)#login
2501C (config-line)#password todd
2501C (config-line)#line vty 0 4
2501C (config-line)#login
2501C (config-line)#password todd
```

```
2501C (config-line)#interface ethernet0
2501C (config-if)#ip address 172.16.80.1  255.255.255.0
2501C (config-if)#description connection to LAN 80
2501C (config-if)#no shutdown
2501C (config-line)#interface serial0
2501C (config-if)#ip address 172.16.40.2  255.255.255.0
2501C (config-if)#description connection to 2600A
2501C (config-if)#no shutdown
2501C (config-if)#exit
2501C (config)#banner motd #
Este es el router 2501C
#
2501C (config)#exit
2501C#copy run star
```

16. Presione la tecla Enter para aceptar los cambios en el archivo startup-config y presione nuevamente Enter para sobrescribir la configuración.

17. Observe los cambios realizados en la configuración de los routers en la ventana superior izquierda.

18. Haga clic en el botón Net Visualizer.

19. Haga clic en el botón Save/Load Network, guarde el proyecto con la estructura iniciales_Routers, en C:\. El simulador pregunta si desea limpiar el escenario, haga clic en el botón No, de lo contrario se borrarán todas las configuraciones realizadas.

Investigue la función de la instrucción ***banner motd #Este es el router 2501C#***

_____
_____
_____

20. Haga una conexión al router 2501d, haciendo doble clic sobre él. Presione la tecla Enter y asigne el nombre, password, descripción de interfases, banners y direcciones IP a cada interfase de acuerdo a las siguientes instrucciones:

```
Router>enable
Router# config t
Router (config)# hostname 2501D
2501D (config)# enable secret todd
2501D (config)#line console 0
2501D (config-line)#login
2501D (config-line)#password todd
2501D (config-line)#line aux 0
2501D (config-line)#login
2501D (config-line)#password todd
2501D (config-line)#line vty 0 4
2501D (config-line)#login
2501D (config-line)#password todd
2501D (config-line)#interface ethernet0
2501D (config-if)#ip address 172.16.90.1  255.255.255.0
2501D (config-if)#description connection to LAN 90
2501D (config-if)#no shutdown
2501D (config-line)#interface serial0
```

```
2501D (config-if)#ip address 172.16.50.2  255.255.255.0
2501D (config-if)#description connection to 2600A
2501D (config-if)#no shutdown
2501D (config-if)#exit
2501D (config)#banner motd #
Este es el router 2501D
#
2501D (config)#exit
2501D# copy run star
```

21. Presione la tecla Enter para aceptar los cambios en el archivo startup-config y presione nuevamente Enter para sobrescribir la configuración.

22. Observe los cambios realizados en la configuración de los routers en la ventana superior izquierda.

23. Haga clic en el botón Net Visualizer.

24. Haga clic en el botón Save/Load Network, guarde el proyecto con la estructura iniciales_Routers, en C:\. El simulador pregunta si desea limpiar el escenario, haga clic en el botón No, de lo contrario se borrarán todas las configuraciones realizadas.

Investigue la función de la instrucción ***copy run star.***

_____
_____
_____

25. Haga una conexión al router 2501e, haciendo doble clic sobre él. Presione la tecla Enter y asigne el nombre, password, descripción de interfases, banners y direcciones IP a cada interfase de acuerdo a las siguientes instrucciones:

```
Router>enable
Router# config t
Router (config)# hostname 2501E
2501E (config)# enable secret todd
2501E (config)#line console 0
2501E (config-line)#login
2501E (config-line)#password todd
2501E (config-line)#line aux 0
2501E (config-line)#login
2501E (config-line)#password todd
2501E (config-line)#line vty 0 4
2501E (config-line)#login
2501E (config-line)#password todd
2501E (config-line)#interface ethernet0
2501E (config-if)#ip address 172.16.10.1  255.255.255.0
2501E (config-if)#description connection to backbone
2501E (config-if)#no shutdown
2501E (config-line)#interface serial0
2501E (config-if)#ip address 172.16.20.1  255.255.255.0
2501E (config-if)#description connection to 2501A
2501E (config-if)#clock rate 64000
2501E (config-if)#no shutdown
```

```
2501E (config-line)#interface serial1
2501E (config-if)#ip address 172.16.30.1  255.255.255.0
2501E (config-if)#description connection to 2501B
2501E (config-if)#clock rate 64000
2501E (config-if)#no shutdown
2501E (config-if)#exit
2501E (config)#banner motd #
Este es el router 2501E
#
2501E (config)#exit
2501E# copy run star
```

26. Presione la tecla Enter para aceptar los cambios en el archivo startup-config y presione nuevamente Enter para sobrescribir la configuración.

27. Observe los cambios realizados en la configuración de los routers en la ventana superior izquierda.

28. Haga clic en el botón Net Visualizer.

29. Haga clic en el botón Save/Load Network, guarde el proyecto con la estructura iniciales_Routers, en C:\. El simulador pregunta si desea limpiar el escenario, haga clic en el botón No, de lo contrario se borrarán todas las configuraciones realizadas.

Investigue la función de la instrucción ***clock rate 64000.***

_____
_____
_____

30. Haga una conexión al router 2600a, haciendo doble clic sobre él. Presione la tecla Enter y asigne el nombre, password, descripción de interfases, banners y direcciones IP a cada interfase, de acuerdo a las siguientes instrucciones:

```
Router>enable
Router# config t
Router (config)# hostname 2600A
2600A (config)# enable secret todd
2600A (config)#line console 0
2600A (config-line)#login
2600A (config-line)#password todd
2600A (config-line)#line aux 0
2600A (config-line)#login
2600A (config-line)#password todd
2600A (config-line)#line vty 0 4
2600A (config-line)#login
2600A (config-line)#password todd
2600A (config-line)#interface f0/0
2600A (config-if)#ip address 172.16.10.2  255.255.255.0
2600A (config-if)#description connection to backbone
2600A (config-if)#no shutdown
2600A (config-line)#interface serial0/0
2600A (config-if)#ip address 172.16.40.1 255.255.255.0
2600A (config-if)#description connection to 2501C
2600A (config-if)#clock rate 64000
```

```
2600A (config-if)#no shutdown
2600A (config-line)#interface serial0/1
2600A (config-if)#ip address 172.16.50.1  255.255.255.0
2600A (config-if)#description connection to 2501D
2600A (config-if)#clock rate 64000
2600A (config-if)#no shutdown
2600A (config-if)#exit
2600A (config)#banner motd #
Este es el router 2600A
#
2600A (config)#exit
2600A# copy run star
```

31. Presione la tecla Enter para aceptar los cambios en el archivo startup-config y presione nuevamente Enter para sobrescribir la configuración.

32. Observe los cambios realizados en la configuración de los routers en la ventana superior izquierda.

33. Haga clic en el botón Net Visualizer.

34. Haga clic en el botón Save/Load Network, el simulador pregunta si desea limpiar el escenario, haga clic en el botón No.

Investigue la función de la instrucción ***description connection X.***

_____
_____
_____

35. Entender como se configuran los routers es indispensable para los administradores de redes. Verifique las conexiones realizadas mediante los siguientes comandos en cada unos de los routers desde el 2501A hasta el 2501E, terminando con el router 2600A. Anote la salida de los comandos anteriores en la Tabla No. 2.2.

```
2501A# show running-config
2501A# show ip route

2501B# show running-config
2501B# show ip route

2501C# show running-config
2501C# show ip route

2501D# show running-config
2501D# show ip route

2501E# show running-config
2501E# show ip route

2600A# show running-config
2600A# show ip route
```

	Subredes	Ethernet0	Serial0	Serial1	FastEthernet
2501A					
2501B					
2501C					
2501D					
2501E					
2600A					

Tabla No. 2.2 Tablas de ruteo estáticas

Explique la salida de las instrucciones ***show ip route.***

_____
_____
_____

4.1.2.1 Creación de la tabla de ruteo

El objetivo de este punto es configurar las tablas de ruteo manualmente, esto es crear tablas de ruteo estáticas en cada router que permitan la comunicación en toda la red.

Nota: El ruteo no funciona hasta que todos los routers tengan ya configuradas sus tablas de ruteo estáticas.

1. Abra la CLI del router 2501A, el cual está conectado a las redes 172.16.20 y 172.16.60.0 de manera que debe configurar una ruta estática para todas las redes que no están directamente conectadas. Teclee las siguientes instrucciones en modo configuración:

```
2501A#config t
2501A(config)# ip route 172.16.10.0 255.255.255.0 172.16.20.1
2501A(config)# ip route 172.16.30.0 255.255.255.0 172.16.20.1
2501A(config)# ip route 172.16.40.0 255.255.255.0 172.16.20.1
2501A(config)# ip route 172.16.50.0 255.255.255.0 172.16.20.1
2501A(config)# ip route 172.16.70.0 255.255.255.0 172.16.20.1
2501A(config)# ip route 172.16.80.0 255.255.255.0 172.16.20.1
2501A(config)# ip route 172.16.90.0 255.255.255.0 172.16.20.1
2501A(config)#exit
2501A#copy run start
```

2. Haga clic en el botón Save/Load Network, el simulador pregunta si desea limpiar el escenario, haga clic en el botón No.

Nota: La puerta de enlace está definida en el router 2501E con la dirección 172.16.20.1.

3. Abra la CLI del router 2501B, el cual está conectado a las redes 172.16.30 y 172.16.70.0 de manera que debe configurar una ruta estática para todas las redes que no están directamente conectadas. Teclee las siguientes instrucciones en modo configuración:

```
2501B#config t
2501B(config)# ip route 172.16.10.0 255.255.255.0 172.16.30.1
2501B(config)# ip route 172.16.20.0 255.255.255.0 172.16.30.1
2501B(config)# ip route 172.16.40.0 255.255.255.0 172.16.30.1
2501B(config)# ip route 172.16.50.0 255.255.255.0 172.16.30.1
```

```
2501B(config)# ip route 172.16.60.0 255.255.255.0 172.16.30.1
2501B(config)# ip route 172.16.80.0 255.255.255.0 172.16.30.1
2501B(config)# ip route 172.16.90.0 255.255.255.0 172.16.30.1
2501B(config)#exit
2501B#copy run start
```

4. Haga clic en el botón Save/Load Network, el simulador pregunta si desea limpiar el escenario, haga clic en el botón No.

Indique, para este router que dirección IP corresponde a la puerta de enlace.

_____
_____
_____

5. Abra la CLI del router 2501C, el cual está conectado a las redes 172.16.40 y 172.16.80.0 de manera que debe configurar una ruta estática para todas las redes que no están directamente conectadas. Teclee las siguientes instrucciones en modo configuración:

```
2501C#config t
2501C(config)# ip route 172.16.10.0 255.255.255.0 172.16.40.1
2501C(config)# ip route 172.16.20.0 255.255.255.0 172.16.40.1
2501C(config)# ip route 172.16.30.0 255.255.255.0 172.16.40.1
2501C(config)# ip route 172.16.50.0 255.255.255.0 172.16.40.1
2501C(config)# ip route 172.16.60.0 255.255.255.0 172.16.40.1
2501C(config)# ip route 172.16.70.0 255.255.255.0 172.16.40.1
2501C(config)# ip route 172.16.90.0 255.255.255.0 172.16.40.1
2501C(config)#exit
2501C#copy run start
```

6. Haga clic en el botón Save/Load Network, el simulador pregunta si desea limpiar el escenario, haga clic en el botón No.

Indique, para este router que dirección IP corresponde a la puerta de enlace.

_____
_____
_____

7. Abra la CLI del router 2501D, el cual está conectado a las redes 172.16.50.0 y 172.16.90.0 de manera que debe configurar una ruta estática para todas las redes que no están directamente conectadas. Teclee las siguientes instrucciones en modo configuración:

```
2501D#config t
2501D(config)# ip route 172.16.10.0 255.255.255.0 172.16.50.1
2501D(config)# ip route 172.16.20.0 255.255.255.0 172.16.50.1
2501D(config)# ip route 172.16.30.0 255.255.255.0 172.16.50.1
2501D(config)# ip route 172.16.40.0 255.255.255.0 172.16.50.1
2501D(config)# ip route 172.16.60.0 255.255.255.0 172.16.50.1
2501D(config)# ip route 172.16.70.0 255.255.255.0 172.16.50.1
2501D(config)# ip route 172.16.80.0 255.255.255.0 172.16.50.1
2501D(config)#exit
2501D#copy run start
```

8. Haga clic en el botón Save/Load Network, el simulador pregunta si desea limpiar el escenario, haga clic en el botón No.

Indique, para este router que dirección IP corresponde a la puerta de enlace.

_____
_____
_____

9. Abra la CLI del router 2501E, el cual está conectado a las redes 172.16.10.0, 172.16.20.0 y 172.16.30.0 de manera que debe configurar una ruta estática para todas las redes que no están directamente conectadas. Teclee las siguientes instrucciones en modo configuración:

```
2501E#config t
2501E(config)# ip route 172.16.40.0 255.255.255.0 172.16.10.2
2501E(config)# ip route 172.16.50.0 255.255.255.0 172.16.10.2
2501E(config)# ip route 172.16.60.0 255.255.255.0 172.16.20.2
2501E(config)# ip route 172.16.70.0 255.255.255.0 172.16.30.2
2501E(config)# ip route 172.16.80.0 255.255.255.0 172.16.10.2
2501E(config)# ip route 172.16.90.0 255.255.255.0 172.16.10.2
2501E(config)#exit
2501E#copy run start
```

10. Haga clic en el botón Save/Load Network, el simulador pregunta si desea limpiar el escenario, haga clic en el botón No.

Indique, para este router que direcciones IP corresponden a las puertas de enlace.

_____
_____
_____

11. Abra la CLI del router 2600A, el cual está conectado a las redes 172.16.10.0, 172.16.20.0, 172.16.40.0 y 172.16.50.0 de manera que debe configurar una ruta estática para todas las redes que no están directamente conectadas. Teclee las siguientes instrucciones en modo configuración:

```
2600A#config t
2600A(config)# ip route 172.16.20.0 255.255.255.0 172.16.10.1
2600A(config)# ip route 172.16.30.0 255.255.255.0 172.16.10.1
2600A(config)# ip route 172.16.60.0 255.255.255.0 172.16.10.1
2600A(config)# ip route 172.16.70.0 255.255.255.0 172.16.10.1
2600A(config)# ip route 172.16.80.0 255.255.255.0 172.16.40.2
2600A(config)# ip route 172.16.90.0 255.255.255.0 172.16.50.2
2600A(config)#exit
2600A#copy run start
```

12. Haga clic en el botón Save/Load Network, el simulador pregunta si desea limpiar el escenario, haga clic en el botón No.

Indique, para este router que direcciones IP corresponden a las puertas de enlace.

_____
_____
_____

4.1.2.2 Verificación de las tablas de ruteo

El objetivo de este apartado es la comprobación de las tablas de ruteo configuradas en el punto anterior, para lo cual se emplea el comando ***show ip route.*** Verifique los resultados de las siguientes instrucciones para cada uno de los routers.

1. Abra la CLI del router 2501A y use el comando show ip route para verificar la tabla de ruteo.

2501A# show ip route

2. Abra la CLI del router 2501B y use el comando show ip route para verificar la tabla de ruteo.

2501B# show ip route

3. Abra la CLI del router 2501C y use el comando show ip route para verificar la tabla de ruteo.

2501C# show ip route

4. Abra la CLI del router 2501D y use el comando show ip route para verificar la tabla de ruteo.

2501D# show ip route

5. Abra la CLI del router 2501E y use el comando show ip route para verificar la tabla de ruteo.

2501E# show ip route

6. Abra la CLI del router 2600A y use el comando show ip route para verificar la tabla de ruteo.

2600A# show ip route

Indique cuál es la salida del comando anterior para cada router.

_____
_____
_____

7. Una vez comprobadas las tablas de ruteo en todos los routers, verifique la conectividad entre los mismos mediante las siguientes instrucciones, ver Figuras 2.11 y 2.12.

2501A#ping 172.16.10.2
2501A#ping 172.16.20.1
2501A#ping 172.16.30.2
2501A#ping 172.16.40.2
2501A#ping 172.16.50.2
2501A#ping 172.16.60.1
2501A#ping 172.16.70.1
2501A#ping 172.16.80.1
2501A#ping 172.16.90.1

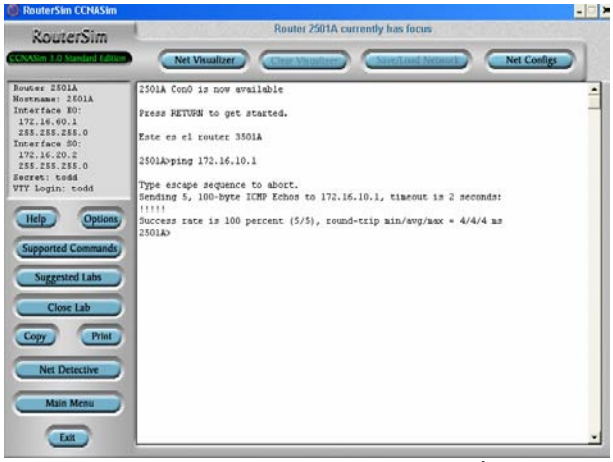


Figura 2.11 Ping realizado con éxito

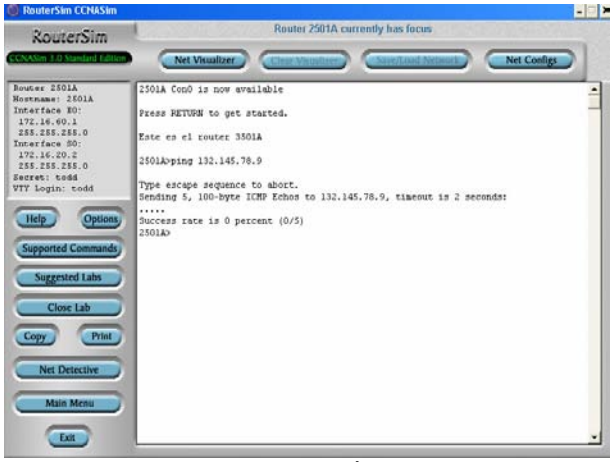


Figura 2.12 Ping realizado sin éxito

Explique la salida del comando ping cuando éste resulta ser exitoso.

_____

_____

_____

8. En el reporte final debe entregar el diagrama que represente la conectividad entre los routers, indicado las direcciones IP de las interfases configuradas, las puertas de enlaces y el nombre de los routers.

4.1.3 Eliminando las configuraciones existentes

Para finalizar es necesario dejar el espacio de trabajo sin ninguna configuración. Para lo anterior realice los siguientes pasos:

1. Elimine su archivo de C:\.
2. Regrese al área de trabajo, haciendo clic en el botón Net Visualizer y haga clic en el botón Save/Load.
3. Elija la opción afirmativa a si desea limpiar el área de trabajo. Esa acción dejará el área de trabajo sin configuración, para ser utilizada por el siguiente grupo.

5.-Conclusiones

6.-Cuestionario Previo 2B

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 3
Administración con SNMP

1.- Objetivo de aprendizaje

El alumno analizará y explorará el significado y utilidad de los diferentes objetos de la MIB-II, consultando los valores a un agente SNMP con ayuda del software MG-SOFT MIB Browser.

El alumno aprenderá a través de la interfaz de línea de comando, a configurar el protocolo de mantenimiento SNMP, en routers Cisco.

El alumno aprenderá a crear una ACL, Lista de Control de Acceso (Access Control List) sencilla para configurar el protocolo de mantenimiento SNMP.

2.- Conceptos teóricos

SNMP, Protocolo Simple de Administración (Simple Network Manager) es un protocolo del nivel de aplicación que proporciona una estructura de mensajes para el intercambio de información entre administradores y agentes SNMP, es decir proporciona un entorno de trabajo estandarizado y un lenguaje común empleado para el monitoreo y administración de dispositivos de la red. El protocolo SNMP se conforma de 3 elementos:

a. Un administrador SNMP, sistema empleado para controlar la actividad de los componentes de la red mediante SNMP, regularmente denominado NMS, Sistema de Administración de Red (Network Management System).
b. Un agente SNMP, es el componente software dentro del dispositivo administrado que mantiene los datos del mismo e informa al administrador acerca de ellos, cuando se requiere. Contiene variables de la MIB cuyos valores pueden ser solicitados o modificados por el administrador SNMP, mediante operaciones get y set.
c. Una MIB, es una colección de objetos de información de administración, residente en el dispositivo administrado. Sus colecciones de objetos están definidos como módulos escritos en un lenguaje especial.

El protocolo funciona de la siguiente manera: el administrador puede leer un valor de un agente o almacenar un valor en dicho agente, éste último obtiene los datos de la MIB, donde se almacenan los parámetros del dispositivo y datos del funcionamiento de la red. El agente responde a las solicitudes de los administradores y les puede enviar notificaciones no solicitadas, en forma de informes o interrupciones (traps) para dar a conocer las condiciones de la red.

Existen 6 operaciones básicas que se realizan entre administradores y agentes SNMP, las cuales se resumen en la Tabla No. 3.1.

Operación	Funcionamiento
get-request	Solicita el valor de una variable específica.
get-next-request	Solicita el valor de una variable sin conocer su nombre, se emplea en búsqueda secuencial en tablas.
get-bulk-request	Solicita bloques grandes de datos, por ejemplo varias filas de una tabla.
get-response	Es la respuesta a una petición get-request, get-next-request o set-request.
inform-request	Permite la comunicación entre administradores SNMP.
trap	Se refiere a los mensajes no solicitados enviados por los agentes al administrador SNMP si ocurre algún evento inesperado.

Tabla No. 3.1 Operaciones básicas entre agentes y administradores SNMP

Nota: El protocolo SNMP funciona de acuerdo al modelo cliente/servidor, donde el proceso servidor se ejecuta en los agentes y permanece escuchando las peticiones por parte del administrador SNMP.

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- PC's Pentium con una NIC Ethernet 10/100 Mbps instalada en cada una de ellas.
- Switch 3COM Ethernet 10BaseT o FastEthernet (24 puertos).
- Routers Cisco 2507.
- Software de análisis de MIB, MG-SOFT MIB Browser.
- 2 cables de consola de router RJ45-Serial.

4.- Desarrollo

4.1 Analizando la estructura de las MIB

El esquema de nombres únicos para cada objeto administrado se basa en la sintaxis de la SMI, Estructura de Administración de la Información (Structure of Management Information). La definición de objetos y su significado se almacena en la MIB, Base de Información de Administración (Management Information Base).

La estructura de la SMI y MIB se definen de acuerdo al estándar ASN.1, Notación de Sintaxis Abstracta Uno (Abstract Syntax Notation One).

SNMP, emplea un espacio de nombres jerárquico que constituye un árbol, cuya raíz se conecta a un conjunto de nodos etiquetados, donde cada una de tales etiquetas se compone de una breve descripción y un entero. El OID, Identificador de Objetos (Object Id) es el nombre de un nodo compuesto por la secuencia de enteros de las etiquetas de cada nodo, desde la raíz hasta el nodo en cuestión.

4.1.1 Explorando la herramienta

La MIB-II define 10 grupos cada uno con funciones específicas y son:

a. *system*, grupo que provee información general sobre el sistema administrado, conformado por 7 objetos escalares. Contiene información sobre la entidad, como hardware y software del sistema así como su versión, el tiempo desde la última iniciación, la persona de contacto, la localización física, entre otros.

b. *interfaces*, permite proporcionar información acerca de su descripción, tipo, máxima longitud de octetos de PDU, valor estimado de la tasa de transferencia, estado de la interfaz (up1-down2, testing3), su dirección física, errores en paquetes, cantidades de octetos entrantes y salientes.

c. *at*, comprende las relaciones entre direcciones IP y direcciones específicas de la red que deben soportar, como la tabla ARP, que relaciona direcciones IP con direcciones físicas de la red LAN.

d. *ip*, almacena información propia de la capa IP, como el número de datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc. También contiene información de variables de control, que permiten que aplicaciones remotas puedan ajustar el TTL, Tiempo de Vida (Time To Live) y manipular las tablas de ruteo de IP.

e. *icmp*, este grupo describe las siguientes estadísticas: número de mensajes ICMP recibidos, número de mensajes ICMP (destino inalcanzable) recibidos, número de mensajes ICMP (tiempo excedido) recibidos, número de mensajes ICMP (desbordamiento del emisor) recibidos, número de mensajes ICMP no enviados debido a problemas en ICMP.

f. *tcp*, este grupo incluye información propia del protocolo TCP, como estadísticas del número de segmentos transmitidos y recibidos, información de conexiones activas como dirección IP, puerto o estado actual.

g. *udp,* este grupo describe la siguiente información: número de datagramas UDP entregados a usuarios UDP, número de datagramas UDP recibidos para los que no existía aplicación en el puerto de destino, número de datagramas UDP recibidos que no se pudieron entregar y el número de datagramas UDP enviados por la entidad.

h. *egp*, este grupo describe las siguientes estadísticas: número de mensajes EGP recibidos sin error, número de mensajes EGP con error, número de mensajes EGP generados localmente, la dirección IP del vecino de esta entrada EGP, el estado EGP del sistema local con respecto a la entrada EGP vecino.

i. *transmisión*, proporciona información específica de cada medio de transmisión, es decir, este grupo soporta múltiples tipos de medios de comunicación, como cable coaxial, cable UTP, cable de fibra óptica y sistemas TI/EI.

j. s*nmp*, incluye estadísticas sobre tráfico de red SNMP, el número de paquetes recibidos, el número de peticiones SNMP con nombres erróneos de comunidad, entre otros.

1. Inicie la herramienta MG-SOFT MIB Browser a través de menú Inicio>Todos los programas> MG-SOFT MIB Browser, ver Figura 3.1. Observe que la dirección del agente remoto SNMP es la IP de la máquina.

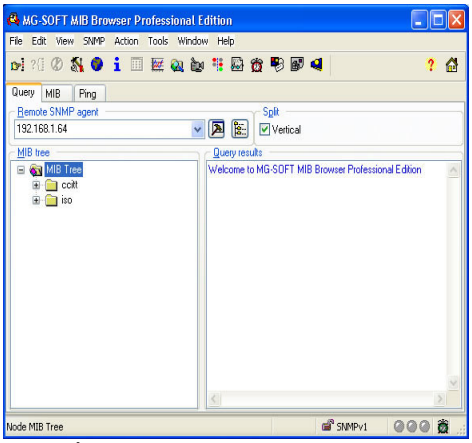


Figura 3.1 Menú inicial de la herramienta analizadora de MIB

2. Expanda la jerarquía desde la carpeta iso hasta llegar a mib-2 y observe los 10 grupos explicados anteriormente, ver Figura 3.2.

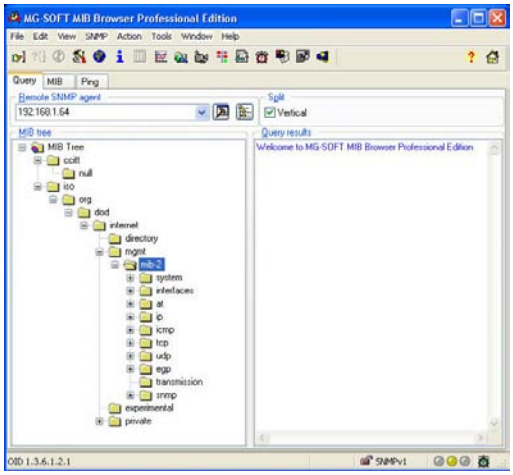


Figura 3.2 Grupos funcionales que integran a la mib-2

3. Expanda el nodo system y anote los parámetros de administración definidos en ese grupo.

_____

_____

_____

4. Para observar las propiedades de cada uno de los parámetros administrables seleccione la hoja final, obtenga el menú contextual y seleccione la opción Properties, ver Figuras 3.3 y 3.4.

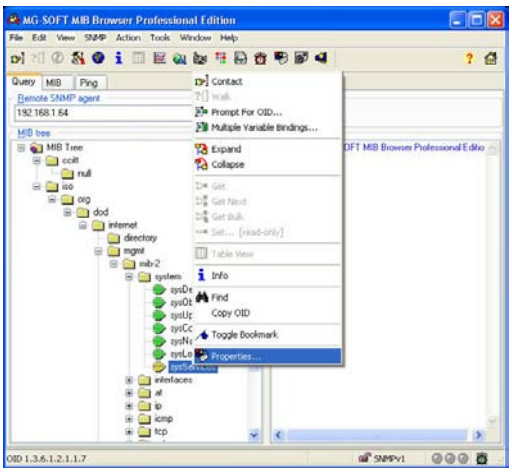


Figura 3.3 Propiedades de un nodo final

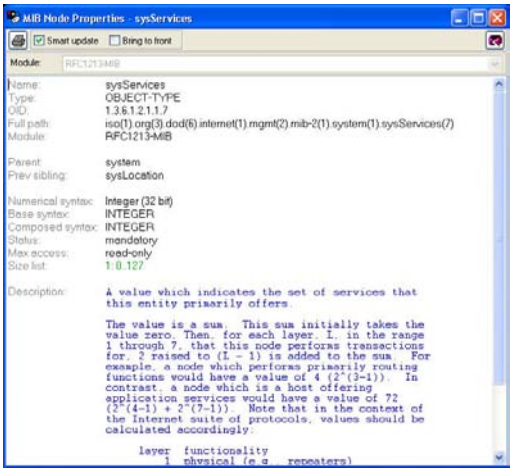


Figura 3.4 Opción Properties de un objeto

Investigue la información que proporciona este grupo al administrador de redes.

_____

_____

_____

En la Figura 3.5 anote el nombre de los diferentes componentes de la MIB.

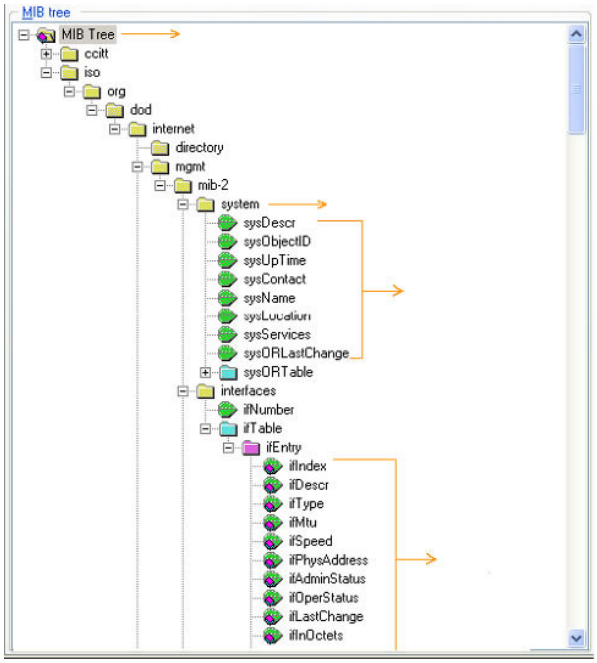


Figura 3.5 Diagrama de los componentes de la MIB

A. Contactando al agente remoto SNMP

Inicie la comunicación con el agente remoto SNMP, de la siguiente manera:

1. En el espacio de trabajo de MIB Browser, haga clic en la pestaña de Query.
2. En el campo del Remote SNMP agent, introduzca la dirección de IP del switch, 192.168.2.123, que corresponde al agente remoto SNMP.

3. Haga clic en el botón Contact Remote SNMP Agent, de la barra de herramientas o bien seleccione la opción Contact del menú SNMP.
4. Al establecer la comunicación con el agente SNMP a través de MIB Browser, el resultado se mostrará en el panel Query Results, ver Figura 3.6.

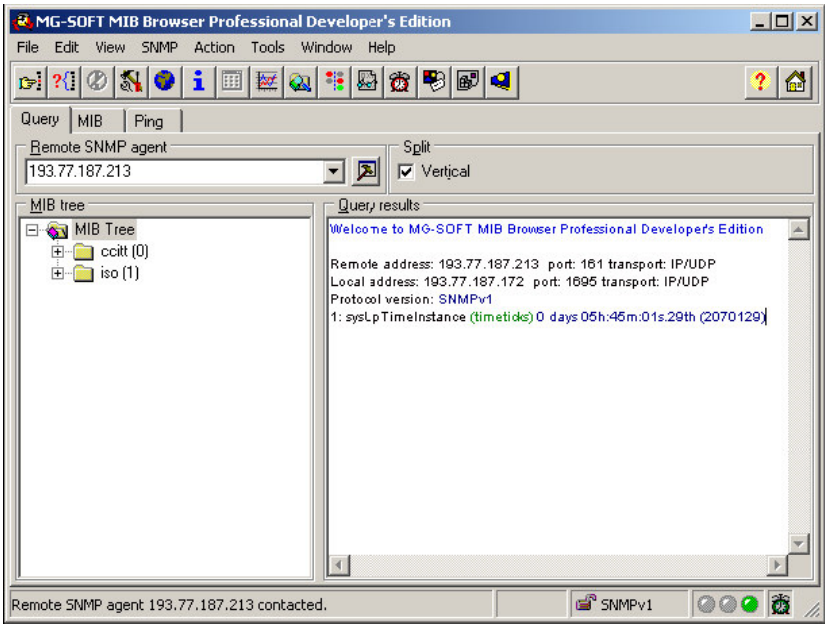


Figura 3.6 Estableciendo comunicación con el agente remoto SNMP

4.1.2 Interactuando con el agente SNMP (versión LINUX)

En este apartado de la práctica podrá configurar del SNMP, la instancia GetBulk del GetNext requests que busca las propiedades de los objetos específicos en el árbol de la MIB, de los agentes SNMP.

Nota: Sólo las versiones SNMPv2c y SNMPv3 soportan la operación del comando GetBulk.

Para mostrar el funcionamiento de la operación del SNMP, GetBulk es necesario tener comunicación con el agente remoto de SNMP.

1. Establezca la comunicación con el agente remoto de SNMP.
2. Para configurar la operación de GetBulk de SNMP en el MIB Browser, abra el cuadro de diálogo de las preferencias del protocolo SNMP, haciendo clic en el menú View y elija SNMP Protocol Preferences.
3. Se muestra un cuadro de diálogo SNMP Protocol Preferences y seleccione SNMPv2c o SNMPv3, ver Figura 3.7.

Figura 3.7 Cuadro de diálogo de SNMP Protocol Preferences

4. En el apartado de Get-Bulk settings, verifique que este seleccionado la opción Use Get-Bulk.
5. En el campo Non repeaters introduzca el número de repeticiones de las variables obligatorias, en nuestro caso cero y en el campo Max repetitions, introduzca el número máximo de objetos que regresan las variables obligatorias del GetBulk del SNMP, para este punto el valor es de 10.

Indique el procedimiento para consultar los valores de las instancias del grupo interfaces.

_____

_____

_____

4.1.3 Especificando parámetros del protocolo SNMP

En este apartado de la práctica aprenderá a especificar los parámetros que usa el protocolo SNMP del MIB Browser, para comunicarse con el agente remoto SNMP.

Nota: Es importante que se especifiquen correctamente los parámetros del protocolo SNMP del MIB Browser, para que exista comunicación con el agente remoto SNMP.

1. Para especificar las preferencias del protocolo SNMP, seleccione del menú View > SNMP Protocol Preferences o haga clic en el botón SNMP Protocol Preferences de la barra de herramientas.
2. A continuación se abrirá una ventana de diálogo, ver Figura 3.8.

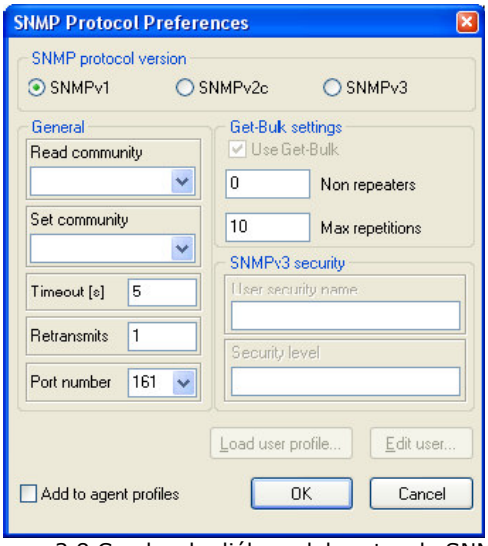


Figura 3.8 Cuadro de diálogo del protocolo SNMP

3. Puede elegir la versión del protocolo que esté utilizando ya sea SNMPv1, SNPMv2c o SNMPv3, del cuadro de diálogo.
4. Dependiendo del protocolo a utilizar, se deben configurar específicamente los parámetros.

B. Especificando parámetros del protocolo SNMPv1

Para usar el protocolo SNMPv1, se tienen que especificar los parámetros de la siguiente manera:

1. Seleccione la opción SNMPv1, del área de SNMP Protocol Version, ver Figura 3.9.

Figura 3.9 Elección del protocolo SNMPv1

2. En el apartado de General, se muestra una lista desplegable de Read community, hay que especificar el nombre de la cadena de lectura. Este parámetro permite utilizar únicamente las primitivas: SNMP GetNext y SNMP GetBulk requests. Verifique que se encuentre seleccionado la opción por default, public.

3. Después se muestra la lista desplegable de Set community, hay que especificar el nombre de la cadena de lectura. Este parámetro permite utilizar únicamente la primitiva Set requests. Verifique que se encuentre seleccionado la opción por default, private.
4. Introduzca en el campo Timeout, el tiempo en segundos que tiene que esperar la herramienta para volver a realizar una petición, 5 segundos.
5. Introduzca en el campo Retransmits, el número de retransmisiones que debe hacer el SNMP requests, 1 una vez.
6. Verifique en el menú desplegable Port number, el número de puerto que utiliza el agente remoto SNMP. Por default el número de puerto que muestra el agente SNMP es el 161.
7. Verifique que esté seleccionado la opción Add to agent profiles del cuadro de diálogo del SNMP Protocol Preferences, para salvar los cambios efectuados para el agente remoto.
8. Haga clic en el botón OK del cuadro de diálogo para aplicar los cambios.

4.1.4 Creación de un perfil de agente SNMP

Un perfil de agente, almacena la configuración referente a dispositivos específicos. Para crear un perfil de agente:

1. Seleccione el menú View> SNMP Agent Profiles o bien haga clic sobre el botón SNMP Agent Profiles.
2. Se presenta una ventana que contiene una estructura jerárquica compuesta de iconos que representan a carpetas de distintos agentes.
3. Obtenga el menú contextual de la carpeta SNMP Agent Profiles y seleccione la opción New Folder, ver Figura 3.10.

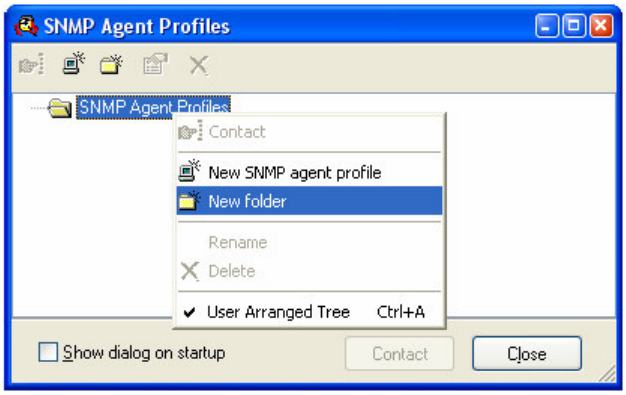


Figura 3. 10 Creación de un nuevo perfil de agente

4. Una nueva carpeta con el nombre por default, se muestra debajo de la carpeta anteriormente seleccionada, cambie el nombre por LabRedes. Obtenga el menú contextual de esta última carpeta y seleccione la opción New SNMP Agent o haga clic sobre el botón New SNMP Agent de la barra de herramientas, ver Figura 3.11.

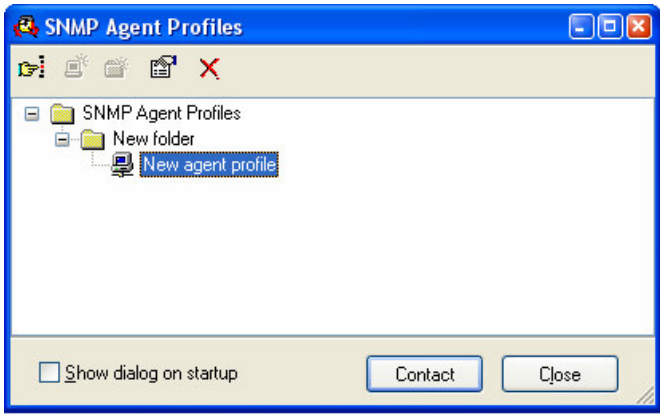


Figura 3. 11 Icono del nuevo agente creado

5. En la venta de SNMP Agent Profiles, cambie el nombre a switch. Obtenga el menú contextual de este agente, seleccione la opción Properties y establezca los valores de la Tabla No. 3.2, ver Figura 3.12.

General	
Name	switch 3com
Agent address	192.168.2.123
Port number	161
Protocol	SNMPv1
SNMPv1	
Read community	Public
Set community	Private
Retransmits	
Timeout (s)	5
Retransmits	4

Tabla No. 3.2 Configuración del perfil del agente

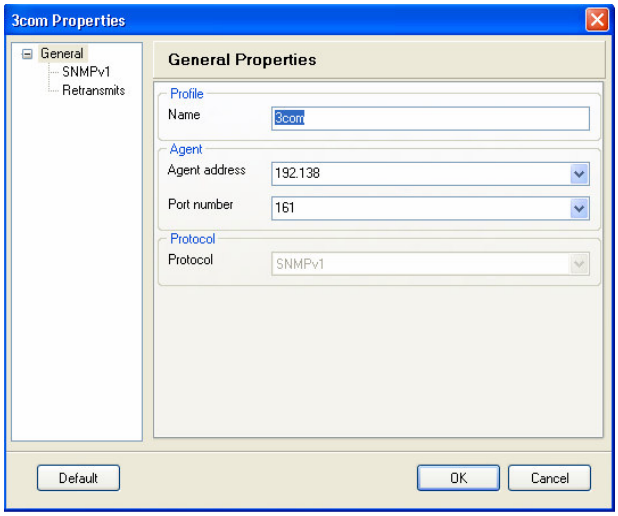


Figura 3.12 Propiedades de un agente

4.1.5 Descubrimiento de los agentes SNMP en la red

El objetivo de este apartado es realizar un descubrimiento en la red, de todos los agentes SNMP, que se encuentran activos, a través de la ventana Remote SNMP Agent Discovery.

1. Seleccione la opción Tools>Discover Agents, ver Figura 3.13.
2. Introduzca el rango de direcciones IP de la red a analizar, para nuestro caso será desde la dirección 192.168.2.100 a la 192.168.2.124, ver Figura 3.14.
3. Verifique que las propiedades de configuración del protocolo SNMP sean las correctas.
4. Haga clic en el botón Contacto y observe la barra de estado, ver Figura 3.15.

Figura 3.13Opción Discover Agents

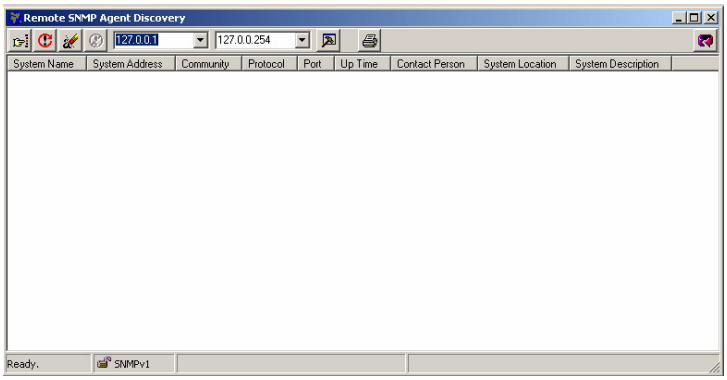


Figura 3.14 Rango de direcciones IP

MG-SOFT MIB Browser permite monitorear y administrar cualquier dispositivo SNMP sobre la red, éstos pueden ser servidores de base de datos, módems, impresoras, routers, switches, etc., empleando el estándar SNMPv1, SNMPv2c y SNMPv3.

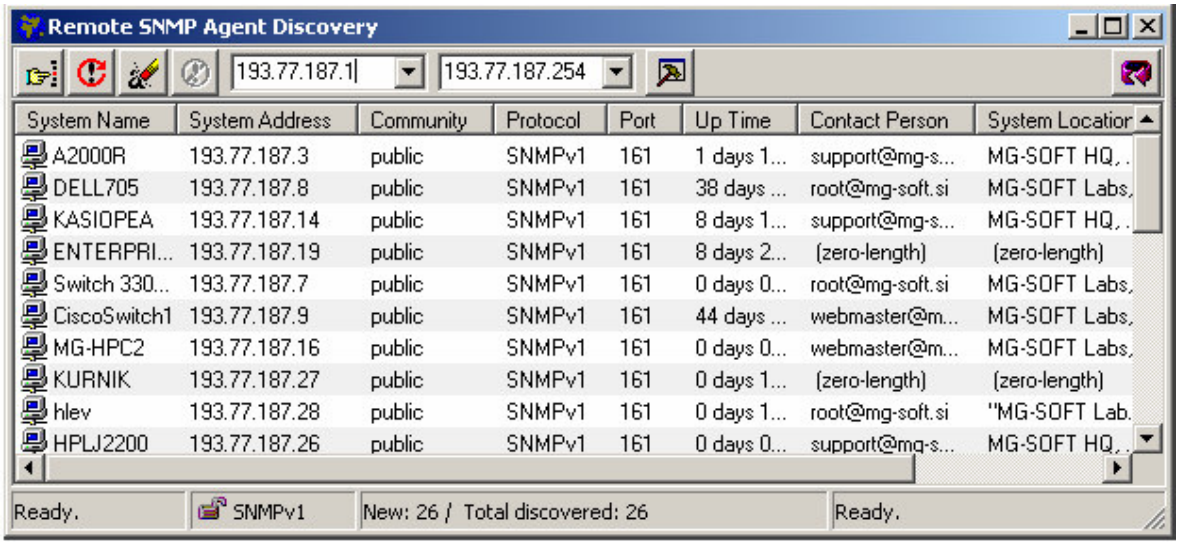


Figura 3.15 Dispositivos SNMPv1 encontrados en la red

La ventana muestra todos los agentes SNMP activos dentro del rango de direcciones, indique las características de cada uno de ellos.

_____

_____

_____

4.1.6 Monitoreando los agentes SNMP en la red

El objetivo de esta sección es aprender a manipular la información proporcionada por las ventanas de monitoreo continuo de los agentes SNMP.

1. En la ventana principal, cambie a la pestaña de Query.

2. En la lista desplegable Remote SNMP Agent, especifique la dirección IP del agente SNMP correspondiente al switch 3COM empleado en el Laboratorio.
3. Si requiere ajustar los parámetros del protocolo SNMP, haga clic en el icono de SNMP Protocols Preferences.
4. Expanda el árbol de la MIB, hasta llegar al nodo system, del cual obtendrá información.
5. En el menú principal, seleccione la opción Tools>Info Windows, ver Figura 3.16.

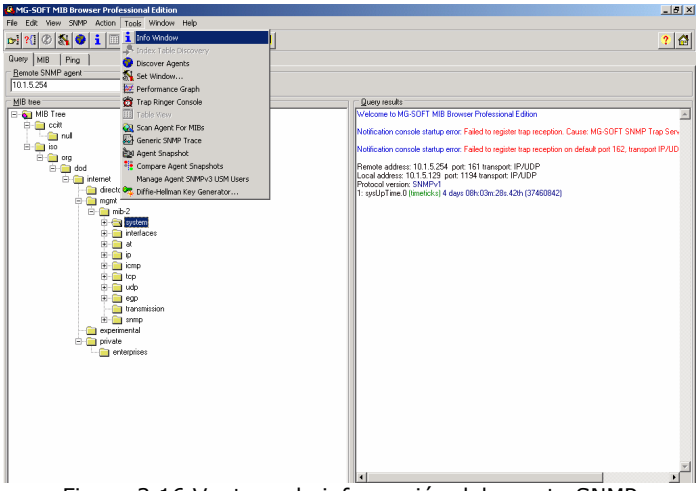


Figura 3.16 Ventana de información del agente SNMP

6. El explorador de la MIB, abrirá una ventana de información que proporciona una serie de instancias de objetos con sus nombres, sintaxis y valores actuales, ver Figura 3.17.

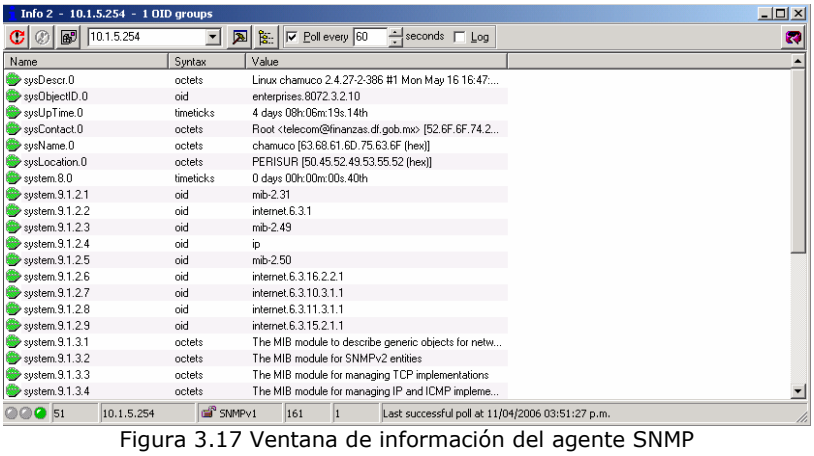


Figura 3.17 Ventana de información del agente SNMP

Investigue a qué se le conoce como notificaciones SNMP.

_____

_____

_____

Investigue a qué se le conoce como traps SNMP.

_____

_____

_____

Investigue a qué se le conoce como peticiones de informe SNMP.

_____
_____
_____

De acuerdo a lo analizado con ayuda de la herramienta, investigue el puerto que utiliza el agente SNMP para escuchar las peticiones del administrador y así mismo el número de puerto empleado, por el agente para responder a tales peticiones.

_____
_____
_____

Investigue al menos 3 aplicaciones que implementen SNMP para la administración de redes.

_____
_____
_____

4.2 Configuración SNMP en los routers Cisco

El protocolo SNMP se usa para la administración remota de dispositivos IP, como los routers. Por defecto existen dos nombres de comunidades que se usan por convenio: public con permisos de sólo lectura y private con permisos de lectura y escritura.

Al ser conocidos los nombres de las comunidades SNMP, son empleados por programas maliciosos para explotar vulnerabilidades, por lo que cambiar el nombre por defecto de las comunidades SNMP evita la mayoría de los problemas de ataques remotos contra routers Cisco.

4.2.1 Verificando el soporte de SNMP

Para configurar el soporte SNMP, es necesario iniciar en primera instancia una sesión remota de administración.

El método principal para la configuración, monitoreo y mantenimiento de equipos Cisco, es la interfaz de línea de comando. El acceso a esta interfaz se realiza normalmente a través del puerto consola de los routers. El cable que permite esta conexión puede ser de diferentes tipos: uno muy común es aquél que en un extremo cuenta con un conector RJ45, el cual no implica que sea una interfaz Ethernet, en el otro extremo tiene un conector serie para una estación de trabajo. Este cable será el que utilizará en esta práctica, ver Figura 3.18.

Figura 3.18 Cable de conexión al router

Nota Profesor: En este caso como el Laboratorio de Redes, cuenta con dos equipos routers 2507 Cisco y la conexión a ellos únicamente se puede realizar con una sesión Hyper Terminal por cada uno, se recomienda conformar dos equipos de trabajo.

1. Conecte el cable de consola al router en su extremo RJ45 en el puerto consola, ver Figura 3.19.

Figura 3.19 Conexión al puerto consola del router con el extremo RJ45

2. Conecte el cable de consola del router en su extremo serial en el puerto serie de la estación de trabajo, ver Figura 3.20.

Figura 3.20 Conexión al puerto serie de la estación de trabajo

3. Inicie una sesión Hyper Terminal, a través del menú Inicio>Todos los programas>Accesorios>Comunicaciones>Hyper Terminal. Configure los valores de la Tabla No. 3.3 en la nueva conexión.

Nombre de la conexión	Router
Conectar usando	COM1
Bits por segundo	9600
Bits de datos	8
Paridad	Ninguno
Bits de parada	1
Control de flujo	Ninguno

Tabla No. 3. 3 Configuración de la sesión Hyper Terminal

4. En pantalla se observa un prompt parpadeando. Presione la tecla Enter y observe el prompt ya estudiado en la práctica anterior del router, ver Figura 3.21.

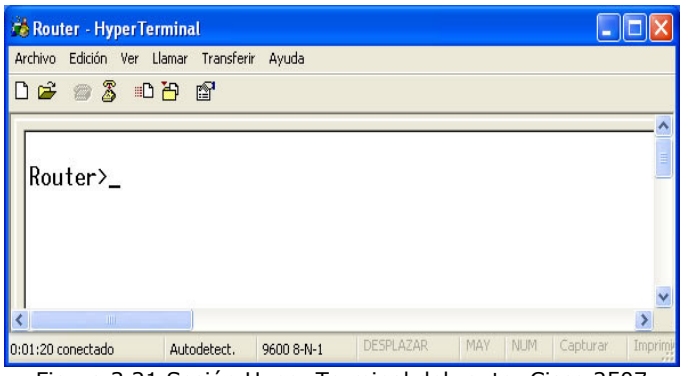


Figura 3.21 Sesión Hyper Terminal del router Cisco 2507

5. Pase al modo privilegiado y teclee el siguiente comando, ver Figura 3.22.

Router>enable
Router#show snmp

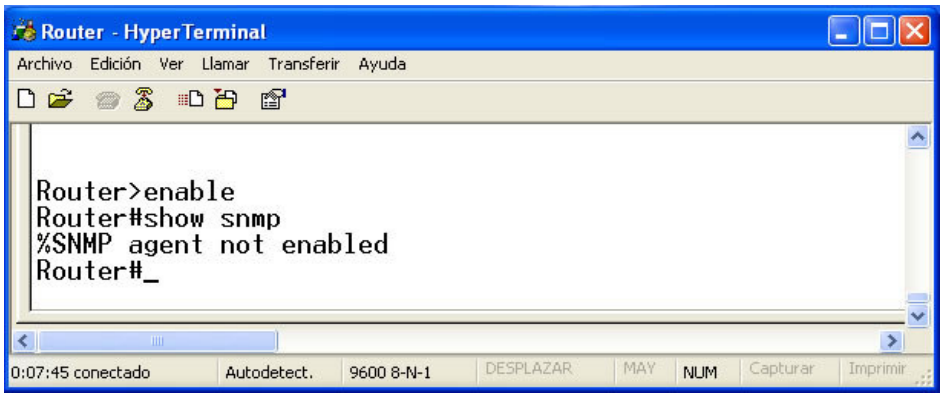


Figura 3.22 Agente no activado

6. Ejecute el siguiente comando, que permite extraer la configuración actual y las líneas que incluyan la palabra snmp.

Router# show running-config | include snmp

Si el soporte a SNMP está activo se presentan dos líneas similares a la Figura 3.x, las cuales indican que hay una comunidad de lectura y otra de escritura, configuradas.

snmp-server community public RO
snmp-server community private RW

Si no se desea el soporte para SNMP, en el router se requiere deshabilitarlo por razones de seguridad, en nuestro caso lo haremos para comenzar con una configuración sin soporte a SNMP.

7. Borre las comunidades establecidas a través de los siguientes comandos:

Router(config)# no snmp-server community public RO
Router(config)# no snmp-server community private RW

8. Deshabilite las interrupciones

Router(config)# no snmp-server enable traps

9. Deshabilite la posibilidad de apagar el router mediante mensajes SNMP.

Router(config)# no snmp-server system-shutdown

10. Deshabilite el servicio SNMP.

Router(config)# no snmp-server

Nota: No existen comandos específicos para habilitar SNMP en el router. SNMP se habilita con el primer comando del tipo ***snmp-server*** que se introduzca en el prompt.

4.2.2 Activando soporte del protocolo SNMP

Para configurar el soporte SNMP dentro de un router Cisco, realice los siguientes pasos:

1. Pase a modo de configuración global.

Router# configure terminal
Router(config)#

2. Cree el control de acceso para una comunidad SNMP. Es necesario introducir un nombre de comunidad para definir la relación entre el administrador SNMP y el agente SNMP. Esta comunidad actúa como una palabra clave para regular el acceso al agente que se haya en el router. Es posible especificar algunas características adicionales, como pueden ser:

    a. Una vista de la MIB, la cual define el subconjunto de objetos de la MIB accesibles para la comunidad dada.
    b. Permiso de lectura y escritura o de sólo lectura para los objetos de la MIB accesibles.
    c. Una ACL, con direcciones IP de los administradores SNMP a los que se permite acceder al agente empleando el nombre de comunidad especificado.

Router(config)# snmp-server community comaccess ro 4

Investigue la sintaxis del commando ***snmp-server community***.

_____
_____
_____

Nota: Es indispensable contar una interfaz ethernet del router, previamente configurada con una dirección IP.

3. Habilite la comunidad a través de la siguiente instrucción:

Router(config)# no snmp-server community *nombre_comunidad*

4. Cree la vista llamada mib2 que contiene todos los objetos dentro del subárbol mib-2.

Router(config)# snmp-server view mib2 1.3.6.1.2.1 included

Router(config)# snmp-server view mib2 mib-2 included
Router(config)# snmp-server view mib2 MIB-II included

5. Pruebe los siguientes comandos en el router y responda las preguntas.

Router(config)# snmp-server view phred system included

Describa el funcionamiento de la instrucción ***snmp-server view phred system included.***

_____
_____
_____

Router(config)# snmp-server view phred cisco included

_____
_____
_____

Nota: Si no se especifican los parámetros opcionales, se facilita acceso de sólo lectura a toda la MIB y a todos los hosts, a la vista por defecto denominada everything.

4.2.3 Configuración de las comunidades en el router

El objetivo de este punto es preparar al router para que acepte peticiones SNMP de lectura y escritura sobre toda la MIB, únicamente desde una estación en concreto, la estación administradora y peticiones de lectura desde cualquier máquina, pero limitadas sobre el grupo system de la MIB.

1. Inicie una conexión al router a través del puerto consola y cambie al modo configuración global.

Router> enable
configure terminal
Router(config)#

2. Se permitirá el acceso total de lectura y escritura desde una dirección IP que será la de la máquina conectada al puerto consola del router. De manera que será necesario crear una lista de acceso que sólo incluya esa estación, cuya dirección IP 192.168.2.3 a través del siguiente comando.

Router(config)# access-list 10 permit host 192.168.2.3
Router(config)# access-list 10 deny any

Investigue el funcionamiento de las instrucciones anteriores.

_____
_____
_____

3. El acceso de lectura se podrá realizar desde cualquier estación pero sólo al grupo system de la MIB, de manera que es necesario definir la vista correspondiente con el nombre de público.

Router(config)# snmp-server view publico system included

4. Cree dos comunidades una de sólo lectura: ro y otra de lectura-escritura: rw. La primera tendrá el nombre de comunidad 's0l0le0' y la segunda se llamará 'le0escrib0'.

Router(config)# snmp-server community s0l0le0 view publico ro
Router(comfit)# snmp-server community le0escrib0 rw 10

Nota: Elegir nombres de comunidad que no sean obvios resulta beneficioso para evitar que usuarios malintencionados intenten ingresar.

Hasta este punto el router está preparado para recibir y atender peticiones SNMPv1 de lectura sobre el grupo system de cualquier host y las peticiones de lectura y escritura sobre toda la MIB únicamente desde la estación configurada en la ACL, siempre y cuando ésta especifique el nombre de la comunidad 'le0escrib0'.

4.2.4 Verificación de la configuración en el router

El objetivo de este apartado es verificar que el acceso a la MIB del router se realiza tal y como se ha configurado, para lo cual utilizará el software de navegación MIB, analizado en el inicio de la práctica.

1. Muestre el estado y configuración del agente SNMP a través del siguiente comando, ver Figura 3.23.

Router> show snmp

Figura 3.23 Salida del comando SNMP

Investigue el funcionamiento de la instrucción ***show snmp.***

_____
_____
_____

2. En este punto verificará la existencia de dos agentes SNMP en la red, conforme al software MG-SOFT MIB Browser. Inicie el navegador a través del menú Inicio>Todos los programas> MG-SOFT MIB Browser >MIB-Browser.
3. Cambie las propiedades del protocolo SNMPv1, de acuerdo a las cadenas de comunidad configuradas en el router Cisco, ver Figura 3.24.

Figura 3.24 Cambiando los valores de configuración de SNMPv1

4. Haga clic en el botón de descubrimiento de agentes de SNMP y observe la existencia de dos agentes.

Describa los datos presentados en este mapa de agentes SNMP.

_____

_____

_____

5. Contacte al agente a través de la dirección IP asignada a la interfaz ethernet0 del router y observe el resultado de la conexión.
6. Haga una consulta de todos los valores obtenidos en las hojas del grupo system del grupo de la MIB-II del router, ver Figura 3.25.

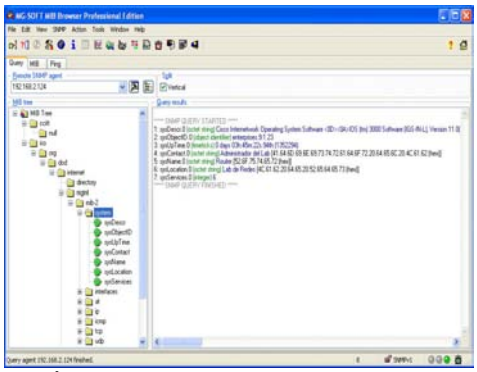


Figura 3.25 Visualización de la MIB del agente residente en el router Cisco 2507

5.-Conclusiones

Revise los objetivos iniciales de la práctica y anote sus resultados a continuación.

_____
_____
_____
_____

6.-Cuestionario Previo 3

ADMINISTRACIÓN DE REDES

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 4
Modelado de Procesos de Negocios con eTOM

1.- Objetivo de aprendizaje

El alumno adquirirá los conocimientos básicos de la metodología de procesos de negocios, eTOM, como fundamento para la administración de una organización proveedora de TI.

El alumno aprenderá a diseñar un modelo de proceso de negocio y ejecutará una simulación del mismo, empleando un software de modelado, denominado Savvivon Process Modeler.

2.- Conceptos teóricos

Actualmente las necesidades de la industria de las telecomunicaciones, incluyen el incremento de ingresos, la utilización de la red y la mejora continua de la eficiencia del personal. Las organizaciones dedicadas a las TI, Tecnologías de la Información (Information Technologys) requieren identificar los servicios, acordar los niveles de calidad, verificar acuerdos, enlazar la infraestructura con los servicios críticos, dar soporte a los usuarios, manejar los cambios para reducir riesgos y entregar el servicio de acuerdo a los niveles prometidos. Para llevar a cabo estas actividades, existen diferentes metodologías que permiten una eficiente administración de todas las tareas realizadas, por una organización en el ramo de las telecomunicaciones, ver Figura 4.1.

Figura 4.1 Estructura dentro de una organización TI

La misión principal de una organización proveedora de TI, es proporcionar una infraestructura técnica necesaria para ejecutar de forma satisfactoria los procesos de negocio. Por lo anterior, las metodologías surgen de la necesidad de proveer estrategias enfocadas al negocio, permitiendo: definir, implantar y mantener en forma integrada la administración de servicios de negocios, además de proporcionar un conjunto de directrices para la organización de servicios, definición de procesos requeridos para la identificación y manejo de niveles de calidad del servicio al cliente, junto con los recursos y el costo

requerido para lograrlo, finalmente se logra a una relación estrecha entre las TI y el desarrollo del negocio.

Existen diversas metodologías para cumplir con los objetivos anteriores, ver Figura 4.2, entre las que destacan:

a. COBIT, Objetivos de Control para Tecnología de Información Relacionadas (Control Objectives for Information and Related Technology) su misión consiste en investigar, desarrollar, publicar y promover un conjunto actualizado e internacional de objetivos de control de TI. Incluye controles de métricas de TI robustos, sin embargo no considera el flujo de los procesos, siendo débil en seguridad.

b. ITIL, Librería de Infraestructura de Tecnologías de Información (Information Technology Infrastructure Library) presenta un robusto modelado en los procesos de TI, propone el establecimiento de estándares que ayuden al control, operación y administración de los recursos, pero se encuentra limitado en seguridad y desarrollo de sistemas.

c. ISO 9000, consiste en un conjunto de cuatro normas relacionadas entre sí, genéricas, no específicas que permiten ser usadas en cualquier actividad, ya sea industrial o de servicios, promueven la adopción de un enfoque basado en procesos cuando se desarrolla, implementa y mejora la eficacia de un Sistema de Gestión de Calidad, para aumentar la satisfacción del cliente mediante el cumplimiento de los requisitos.

d. ISO 17799 es un código de buenas prácticas para la administración de la seguridad informática que proporciona controles sumamente robustos de seguridad, pero no especifica el flujo de procesos.

e. CMM, Modelo de Capacidad de Madurez (Capability Maturity Model) es una metodología integrada por cuatro categorías de proceso: Proceso de Ingeniería, Proceso de Administración de Proyectos, Procesos de Soporte para la Organización y Procesos de Administración de Procesos.

f. eTOM, Mapa de Operaciones de Telecomunicaciones (Telecom Operating Map) es un marco de operaciones que debe formar parte del modelo de negocios de la empresa. Implica un conjunto de grandes áreas de procesos que cubren en su totalidad, el funcionamiento de la organización.

g. Six Sigma, metodología de calidad aplicada para ofrecer un mejor producto o servicio a un costo más bajo, consistente en elaborar una serie de pasos para el control de calidad y optimización de procesos industriales. Define dos niveles: el operacional y gerencial.

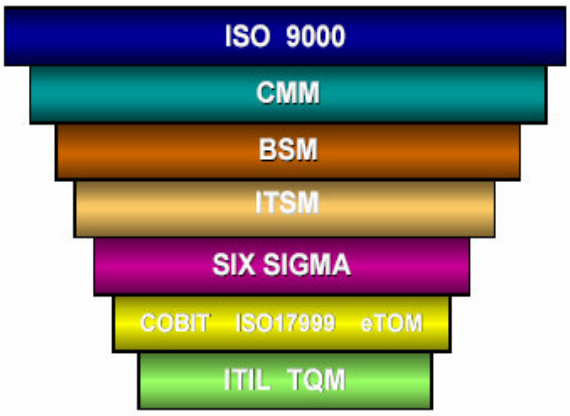


Figura 4.2 Metodologías para la administración de procesos de negocios

Anteriormente el administrador de red requería conocer la infraestructura desde un punto de vista meramente técnico, sin necesidad de preocuparse por el manejo y los costos de los activos. Mantener esta visión no funciona en la actualidad, ya que para contar con una red de comunicaciones eficiente, que implique bajos costos y cubra las expectativas de los usuarios, el administrador requiere no sólo conocer el área técnica, sino también el uso de herramientas de administración y finanzas, de ahí la importancia de esta práctica.

Inicialmente se trabajaba con el estándar TMN, Administración de Redes de Telecomunicaciones (Telecom Network Management) para controlar el proceso de administración de las comunicaciones. Este modelo separa la administración en diferentes capas, sin embargo presenta el problema de que no integra los servicios de instalación, control y facturación.

En la actualidad el modelo eTOM, respaldado por la organización TMNForum, presenta los distintos procesos que se recomiendan abarcar en la totalidad del negocio de cada organización, adaptándose a las necesidades actuales. Las áreas principales de éste incluyen:

a. Área de Procesos Operacionales, es el corazón del eTOM, donde se incluyen todos aquellos procesos que soportan las operaciones y su administración.
b. Área de Procesos de Estrategia, Infraestructura y Producto, la cual incluye todos los procesos necesarios para desarrollar estrategias, construir infraestructuras, desarrollo y administración de productos que administran la cadena de proveedores y/o socios de negocios.
c. Área de Procesos de la Administración Corporativa, incluye los procesos básicos para operar cualquier tipo de negocio, están enfocados en los niveles de procesos corporativos, en las metas y objetivos. Incluyen interfaces con casi todos los procesos de la organización, ya sean procesos operacionales, sobre productos o infraestructura.
d. Áreas de Procesos Funcionales de Soporte, se consideran cuatro áreas de procesos funcionales que se representan en niveles horizontales:
    - Nivel de Mercado, Producto y Clientes, incluye procesos que involucran las ventas, la administración de canales de ventas, mercadeo de productos y ofertas, así como la administración de las relaciones con los clientes, el manejo de órdenes y problemas, la administración de los acuerdos de servicio y la facturación.
    - Nivel de Servicios, abarca aquellos procesos que involucran el desarrollo de servicios y su configuración, la administración de los problemas de servicios y el análisis de la calidad del mismo, además del control de la tarifa de precios.
    - Nivel de los Recursos, implica aquellos procesos que involucran el desarrollo y la administración de la infraestructura de la organización, relacionada con los productos y servicios, o los necesarios para soportar la corporación en su totalidad.
    - Nivel de Proveedores-Socios de Negocio abarca, como su nombre lo dice, todos aquellos procesos que conciernen la interacción con proveedores-socios de la organización, tanto en la definición de la cadena de proveedores que se requiere para poder administrar un producto y su infraestructura, así como aquellos procesos que soportan las interfaces operacionales del SP, Proveedor de Servicios (Service Provider) con sus proveedores-socios de negocio.

Investigue en qué consiste el área de Procesos Operacionales dentro de eTOM.

_____
_____
_____

Investigue en que consiste el área de Procesos de Estrategia, Infraestructura y Productos dentro de eTOM.

_____
_____
_____

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- Software de modelado de procesos de negocios, Savvion Process Modeler Business Manager 6.0.

4.- Desarrollo

La competitividad dentro del área de las telecomunicaciones, ha causado que los clientes de los SP, demanden precios bajos y alta calidad, obligando a los SP a buscar continuamente mejoras en sus procesos internos. Todos los SP, cuentan con un conjunto básico de procesos de negocios que definen, implementan, realizan y mantienen los servicios que proporcionan. El éxito de un SP, radica en su capacidad de administración del ciclo de vida de estos procesos.

BPM, Administrador de Procesos de Negocio (Business Process Manager) es un software que permite a los SP, administrar el ciclo de vida de los procesos de negocio que los integran a través de su análisis, diseño, integración, implementación y optimización.

Process Modeler es una herramienta que permite diseñar plantillas para procesos de negocios básicos y almacenarlos o recuperarlos desde el Savvion Process Repository Process Modeler, éste último no será analizado en clase.

4.1 Diseño del modelo del proceso de negocio

La herramienta software, permite modelar un proceso de negocio de un SP, para lo cual es necesario seguir una metodología que incluye la descripción de:

a. Requerimientos del proceso de negocio.
b. Definición del flujo del proceso de negocio.
c. Creación del modelo del proceso de negocio.
d. Definición de los actores.
e. Asignación de las tareas.
f. Simulación del flujo del modelo del proceso de negocio.

4.1.1 Requerimientos del proceso de negocio

En esta fase se estudia el objetivo del proceso, tratando de descomponerlo en diversos pasos. Analice el siguiente caso:

> "Un SP, proporciona soporte a sus clientes ya sea vía telefónica o mediante visitas de personal calificado. Para hacer valida la garantía de un servicio, el cliente requiere realizar una solicitud del servicio, a la que se conoce como solicitud de orden de servicio.
>
> La solicitud de orden de servicio, es tomada por personal del área de atención al cliente, que verifica que su garantía sea efectiva. En caso de que ésta no sea válida, el cliente recibe una notificación por parte del área de soporte al cliente, de lo contrario se asigna la orden al área de consulta de servicio, donde se hace una revisión de la orden de servicio y el personal de la misma decide, si en primera instancia se requiere una visita o con una llamada telefónica es suficiente.
>
> El soporte vía telefónica a los clientes, está a cargo del área de servicio técnico. El personal de dicha área contacta al cliente para dar seguimiento a la orden de servicio. Si el problema es solucionado, se termina el proceso. En caso contrario se turna la solicitud de orden de servicio nuevamente al área de consulta de servicio, con el objetivo de programar una visita, de la misma forma en la que desde un principio se decide dar soporte a través de la visita.
>
> La programación de las visitas a los clientes, hace uso de un subproceso conocido como Despachador de Servicio, que organiza las citas con los clientes. Este subproceso verifica si se hace valida una extensión de la garantía de los servicios. En caso de que la respuesta sea afirmativa, se notifica al sistema financiero para proceder la solución, en caso de que la respuesta sea negativa se da por concluido la orden de solicitud de servicio."

De acuerdo a la problemática anterior, identifique el objetivo del proceso de negocio a modelar.

_____
_____
_____

Identifique las áreas involucradas en el proceso de negocio anterior.

1._____
2._____
3._____
4._____

Identifique el subproceso y sistema involucrados en el proceso de negocio anterior.

1. _____
2. _____

4.1.2 Definición del flujo del proceso de negocio

El objetivo de esta etapa es definir la secuencia del flujo de los diferentes pasos del proceso del negocio, relacionando cada paso con una actividad.

Para el ejemplo, identifique claramente las 5 actividades mostradas en la Tabla No. 4.1. Indique el personal encargado de realizarlas y observe el tiempo promedio de ejecución.

Actividades	Personal	Tiempo
Consulta técnica con el cliente vía telefónica.		30 minutos
Revisión de la orden de servicio.		8 hrs.
Notificación al cliente.		2 días
Programación de citas.		4 hrs.
Validación de la garantía.		4 hrs.

Tabla No. 4.1 Actividades realizadas con tiempos estimados

Construya un diagrama de flujo que indique la secuencia de las actividades anteriores.

4.1.3 Creación del modelo del proceso de negocio

Empleando el flujo de los procesos del negocio, cree el modelo del proceso de negocio, con ayuda de la herramienta de modelado y siguiendo los siguiente pasos.

1. Inicie el programa a través del menú Inicio>Todos los programas>Savvion > Process Modeler 6.0 SP2 > Launch Savvion Process Modeler, ver Figura 4.3

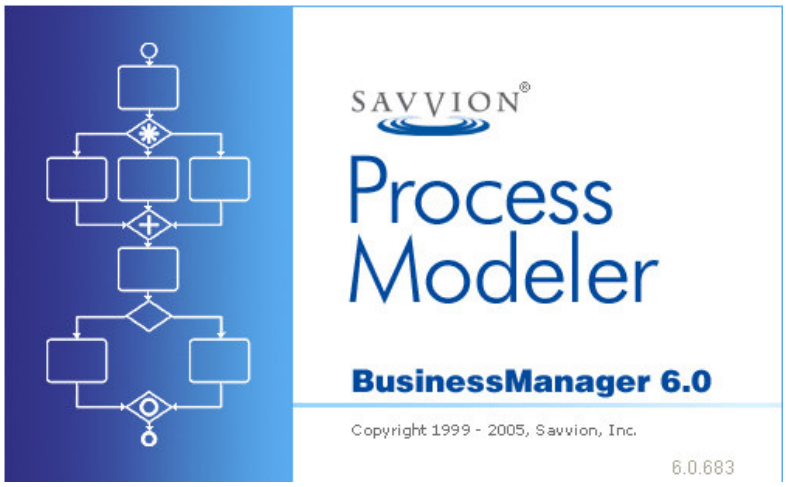


Figura 4.3 Process Modeler Bussiness Manager

2. El área de trabajo, se conforma por diversos elementos, ver Figura 4.4.

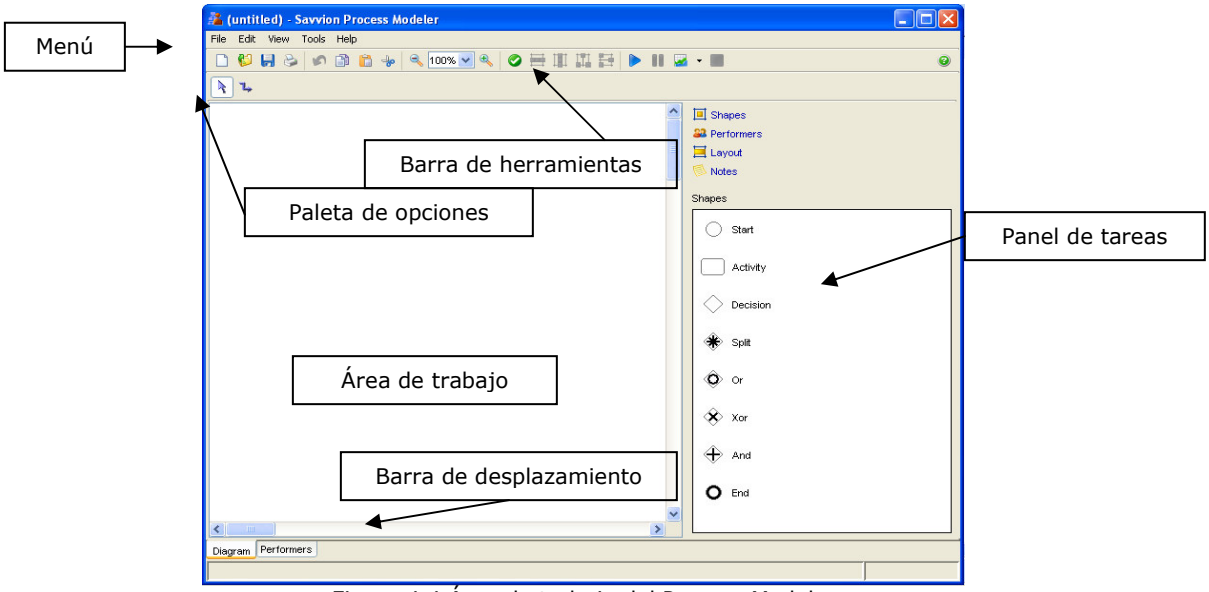


Figura 4.4 Área de trabajo del Process Modeler

3. Abra un nuevo proyecto a través del menú File>New. Se inicia un asistente, coloque el nombre de ProcesoOS_iniciales, en el campo ApplicationName, haga clic en Next ver Figura 4.5.

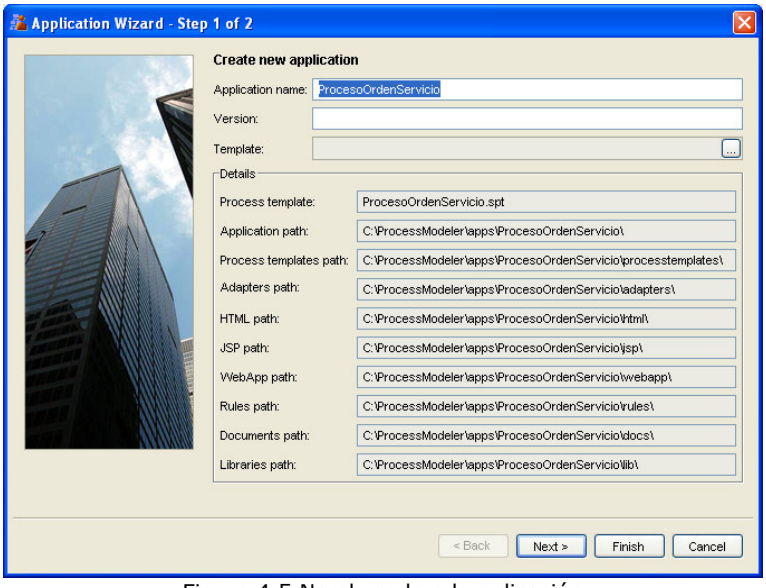


Figura 4.5 Nombrando a la aplicación

4. Introduzca una breve descripción del modelo de proceso de negocio en el campo correspondiente y el autor. Para elegir la duración del proceso haga clic en el botón derecho que aparece en la casilla de duration, se muestra una ventana e ingrese el valor de 3 días, haga clic en OK y por último, haga clic en Finish, ver Figura 4.6

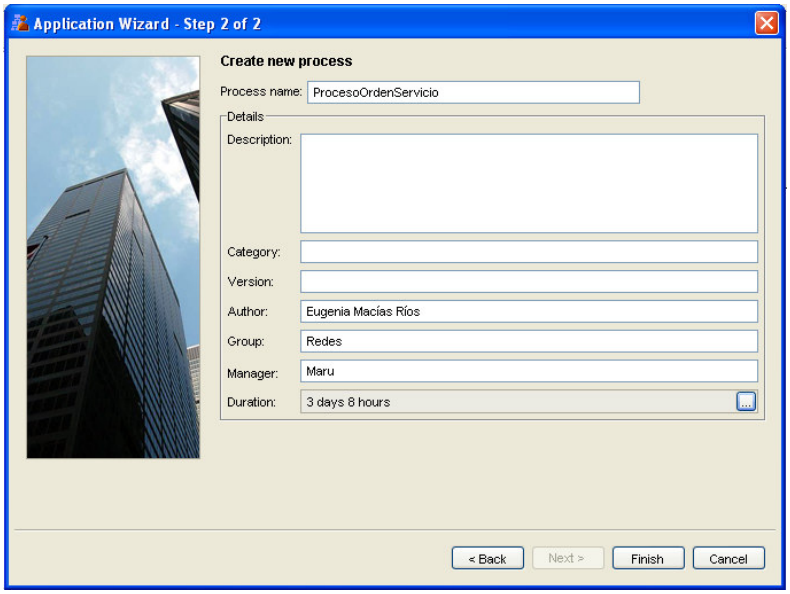


Figura 4.6 Agregando una descripción al modelo del proceso de negocio

5. Seleccione y arrastre la forma Star al área de trabajo, del panel de tareas en la clasificación Shapes. Todo proceso de negocio debe comenzar con una forma de este tipo.
6. Seleccione y arrastre 5 objetos Activity del panel de tareas, bajo la clasificación de Shapes, al área de trabajo.

7. Seleccione y arrastre 4 objetos Decision del panel de tareas, bajo la clasificación de Shapes, al área de trabajo, haga clic derecho sobre el objeto y elija properties para cada decisión introduzca un nombre, de acuerdo a los datos de la Tabla No. 4.2.

Decisión	Nombre
Decision 1	Garantía
Decision 2	Visita
Decision 3	Requiere Visita
Decision 4	Extensión de Garantía

Tabla No. 4.2 Nombres de las decisiones

8. Seleccione y arrastre 2 objetos Or del panel de tareas, bajo la clasificación de Shapes, al área de trabajo.
9. Seleccione y arrastre 3 objetos End del panel de tareas, bajo la clasificación de Shapes, al área de trabajo.
10. Cree el subproceso empleado en el modelado del proceso de negocio de la orden de servicio. Haga clic en el panel de tareas, elija la carpeta Performers, haga clic derecho y seleccione la opción Add, en el campo Sub-process introduzca el nombre de Despachador de Servicios y haga clic en OK, ver Figura 4.7. Observe el subproceso creada en el panel de tareas.

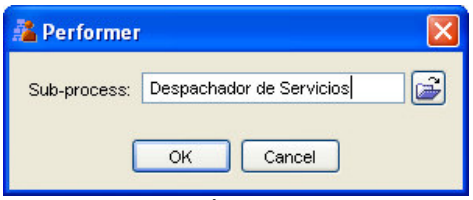


Figura 4.7 Creación del subproceso

11. Cree un objeto del tipo Adapter que representará el sistema financiero identificado en el modelo. Haga clic en la carpeta Adapters del panel de tareas de tareas, haga clic derecho y seleccione la opción Add del menú contextual. Introduzca los datos de la Tabla No. 4.3, ver Figura 4.8.

Campo	Valor
Class	ProcesoOS_iniciales.adapters.FinanceContracts
Method	notify

Tabla No. 4.3 Valores del objeto Adapter creado

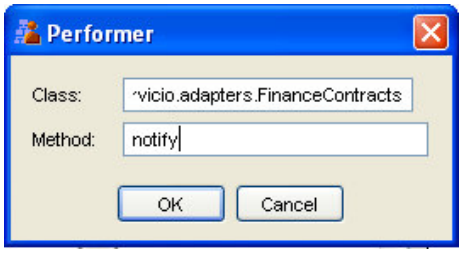


Figura 4.8 Valores del objeto Adapter creado

12. Arrastre los objetos Adapter y el subproceso creado al área de trabajo. Realice las conexiones entre los objetos con la herramienta conector que se encuentra en la paleta de opciones, de manera que tenga una configuración similar ala Figura 4.9.

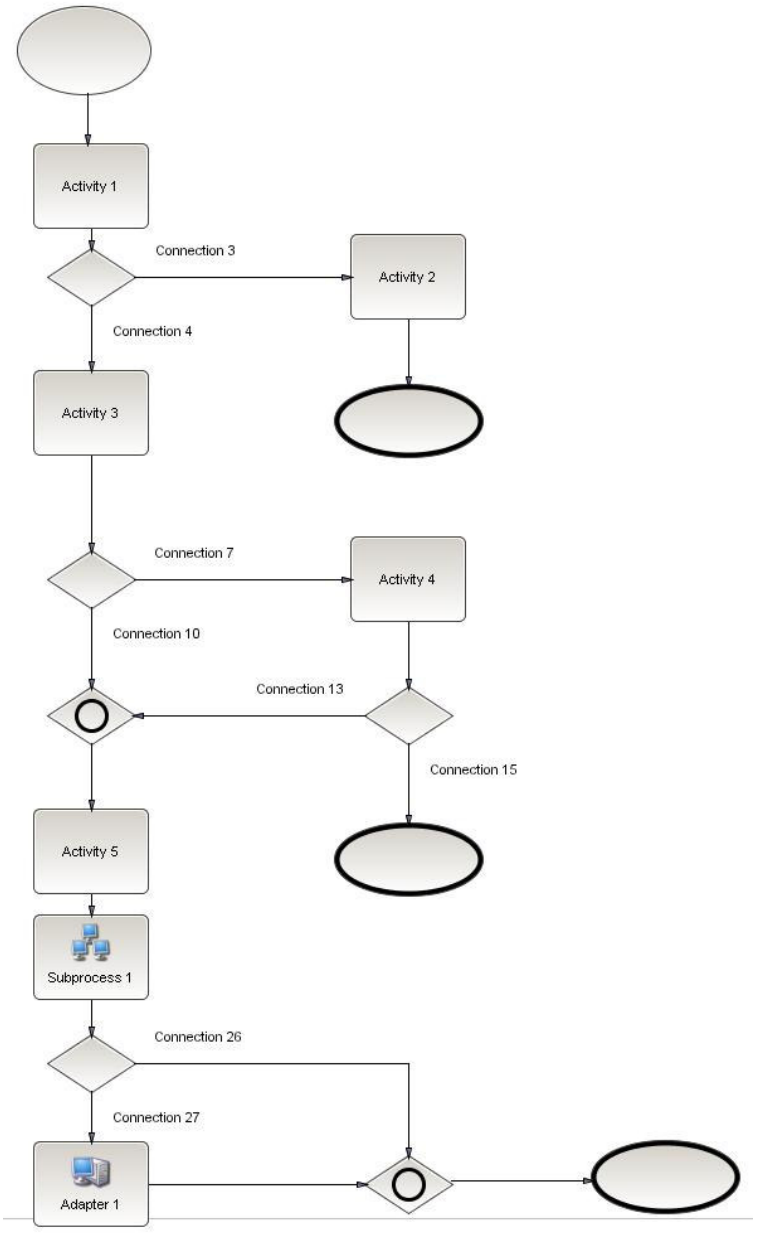


Figura 4.9 Primera configuración del modelo de procesos de negocio

4.1.4 Definición de actores

Cada tarea a realizar, es asignada al personal específico de un área, es decir a un actor. En este punto crearemos cada uno de los actores implicados en el actual proceso de negocio.

1. Seleccione la opción Performers del panel de tareas.

2. Despliegue la carpeta Users, obtenga el menú contextual sobre el usuario @Creator haciendo clic derecho y elija la opción Add.
3. Se presenta el cuadro de diálogo de Performer, introduzca los datos de la Tabla No. 4.4, para crear los 4 grupos de personas que intervienen en el proceso de solicitud de orden de servicio, ver Figuras 4.10.y 4.11

Actores del proceso de negocio				
General				
Name	Atención al cliente	Soporte al cliente	Consultores Servicio	Servicio Tecnico
Type	Group user	Group user	Group user	Group user
Select	Any of the group member	Any of the group member	Any of the group member	Any of the group member
Simulación				
Scenario	default	default	default	default
Group size	4	5	4	3

Tabla No. 4.4 Configuración de actores del proceso de negocio

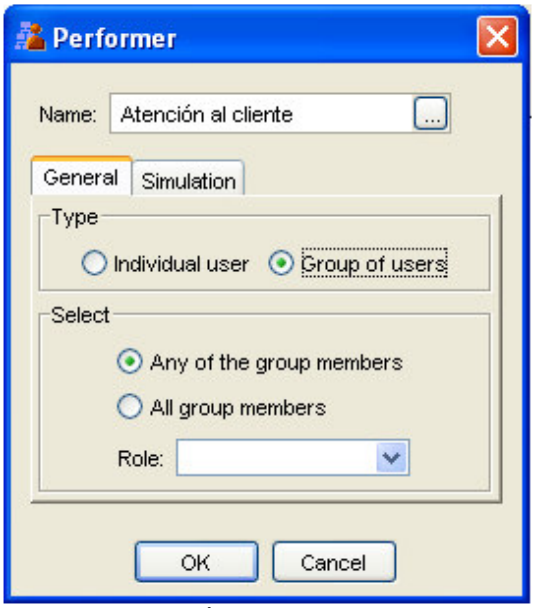


Figura 4.10 Configuración de actor en General

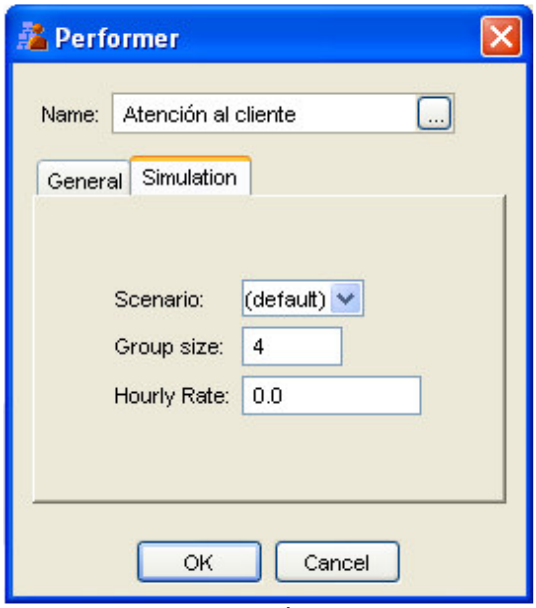


Figura 4.11 Configuración de actor en la Simulación

4.1.5 Asignación de las tareas

Definidas las etapas del proceso y sus actores, es necesario asignar las propiedades de cada actividad.

1. Seleccione el objeto Star con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo introduzca los valores de la Tabla No. 4.5. Haga clic en OK.

Name	Inicio de la orden de servicio
Label	Inicio de la orden de servicio
Description	Breve descripción de la etapa

Tabla No. 4.5 Configuración del objeto Star

2. Seleccione el objeto Activity1 con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo introduzca el nombre Validación de garantía. Haga clic en OK. Arrastre hacia esta actividad al grupo de usuarios de Atención al cliente.
3. Seleccione el objeto decisión Garantía con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo seleccione cada uno de los conectores y haga clic en el botón Modify. Asigne los valores de la Tabla No. 4.6 a cada uno de los conectores. Haga clic en OK.

Enlace 1	
Name	Garantía inválida
Probability	50%
Enlace 2	
Name	Garantía válida
Probability	50%

Tabla No. 4.6 Configuración del objeto Decision1

4. Seleccione el objeto Activity2 con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo introduzca el nombre Notificación al cliente. Haga clic en OK. Arrastre hacia esta actividad al grupo de usuarios de Soporte al cliente.
5. Seleccione el objeto Activity3 con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo introduzca el nombre Revisión de orden de servicio. Haga clic en OK. Arrastre hacia esta actividad al grupo de usuarios de Consulta de servicio.
6. Seleccione el objeto decisión Visita con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo seleccione cada uno de los conectores y haga clic en el botón Modify. Asigne los valores de la Tabla No. 4.7 a cada uno de los conectores. Haga clic en OK.

Enlace 1	
Name	No visita
Probability	60%
Enlace 2	
Name	Requiere visita
Probability	40%

Tabla No. 4.7 Configuración del objeto Decision2

7. Seleccione el objeto Activity4 con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo introduzca el nombre Atención experta al cliente. Haga clic en OK. Arrastre hacia esta actividad al grupo de usuarios de Soporte técnico.
8. Seleccione el objeto decisión Requiere Visita con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo seleccione cada uno de los conectores y haga clic en el botón Modify. Asigne los valores de la Tabla No. 4.8 a cada uno de los conectores. Haga clic en OK.

Enlace 1	
Name	Requiere visita
Probability	30%
Enlace 2	
Name	No requiere visita
Probability	70%

Tabla No. 4.8 Configuración del objeto Decision3

9. Seleccione el objeto Activity5 con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo introduzca el nombre Programación de citas. Haga clic en OK. Arrastre hacia esta actividad al grupo de usuarios de Consulta de servicio.
10. Seleccione el objeto Despachador de servicio con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo introduzca los valores de la Tabla No. 4.9. Haga clic en OK.

Name	Despachador de servicios
Label	Despachador de servicios
Description	Proceso encargado de verificar lo referente a la situación del servicio al cliente.
Duración	5 días

Tabla No. 4.9 Configuración del objeto despachador de servicio

11. Seleccione el objeto decisión Extensión de Garantía con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo seleccione cada uno de los conectores y haga clic en el botón Modify. Asigne los valores de la Tabla No. 4.10 a cada uno de los conectores. Haga clic en OK.

Enlace 1	
Name	No requiere extensión de garantía
Probability	65%
Enlace 2	
Name	Requeire extensión de garantía
Probability	35%

Tabla No. 4.10 Configuración del objeto Decision3

12. Seleccione el objeto Adapter con la herramienta puntero, obtenga el menú contextual y seleccione la opción Properties. En el cuadro de diálogo introduzca los valores de la Tabla No. 4.11. Haga clic en OK.

Name	Contratos de notificaciones financiera
Label	Contratos de notificaciones financiera
Description	El sistema financiero es contactado para el proceso de extensión de garantía.
Duración	Ninguna

Tabla No. 4.11 Configuración del objeto Decision3

La configuración final, del modelo del proceso de negocio, debe ser similar a la Figura 4.12.

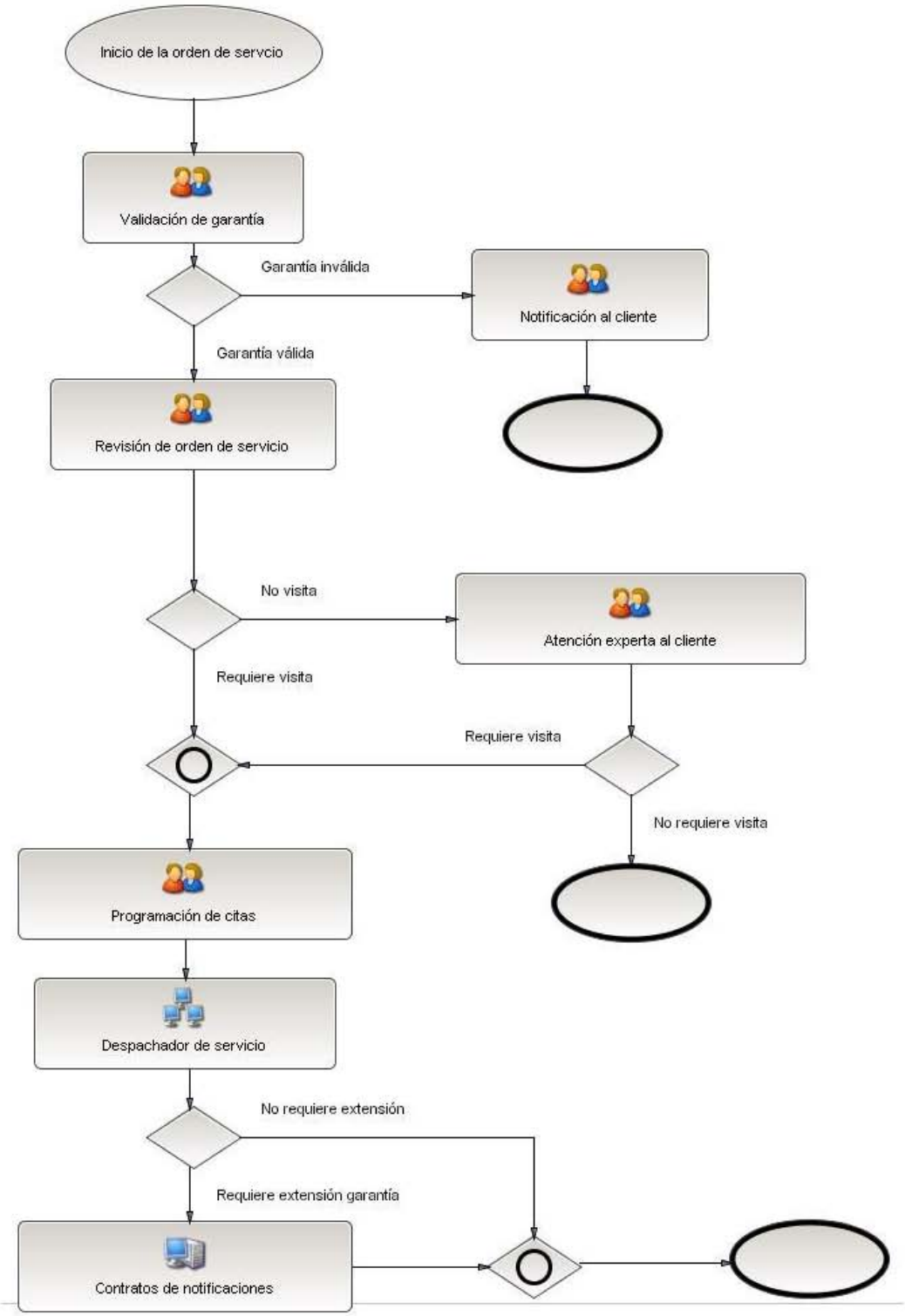


Figura 4.12 Configuración final del modelo de procesos de negocio

4.1.6 Simulación del flujo del modelo del proceso de negocio

Es posible simular el flujo de procesos antes de implementarlos para analizar cuellos de botellas o alguna deficiencia. La opción de simulación dentro de Process Modeler, requiere que cada paso del proceso de negocio, sea configurado en cuestión de tiempo de realización. En este apartado configurará los tiempos estimados para realizar cada uno de los pasos que integran el modelo del proceso de negocio.

1. Seleccione la actividad Validación de garantía, obtenga el menú contextual. En la pestaña General, en el campo duración haga clic sobre los puntos suspensivos e introduzca 4 horas como valor. Elija la pestaña de Simulación e introduzca el valor de la duración como 4 horas, ver Figura 4.13.

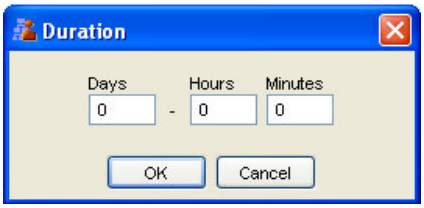


Figura 4.13 Duración de la actividad

2. Seleccione la actividad Notificación al cliente, obtenga el menú contextual. En la pestaña General, en el campo duración haga clic sobre los puntos suspensivos e introduzca 2 días como valor. Elija la pestaña de Simulación e introduzca el valor de la duración como 2 días.

3. Seleccione la actividad Revisión de la orden de servicio, obtenga el menú contextual. En la pestaña General, en el campo duración haga clic sobre los puntos suspensivos e introduzca 8 horas como valor. Elija la pestaña de Simulación e introduzca el valor de la duración de 8 horas.

4. Seleccione la actividad Atención experta al cliente, obtenga el menú contextual. En la pestaña General, en el campo duración haga clic sobre los puntos suspensivos e introduzca 30 minutos como valor. Elija la pestaña de Simulación e introduzca el valor de la duración de 30 minutos y tipo de distribución normal con desviación estándar de 15 minutos, en la opción Randomize duration using.

5. Seleccione la actividad Programación de citas, obtenga el menú contextual. En la pestaña General, en el campo duración haga clic sobre los puntos suspensivos e introduzca 4 horas como valor. Elija la pestaña de Simulación e introduzca el valor de la duración de 4 horas.

6. Verifique la estructura correcta del diagrama con la tecla de función F7. Si el diagrama es correcto haga clic en OK, en caso contrario verifique los conectores.

7. Ejecute la simulación, eligiendo la opción del menú Tools>Start Simulation. El cuadro de diálogo muestra que se probara el modelo del proceso de negocio con 10 instancias separadas por un intervalo de tiempo de 10 minutos. Haga clic en OK, ver Figura 4.14.

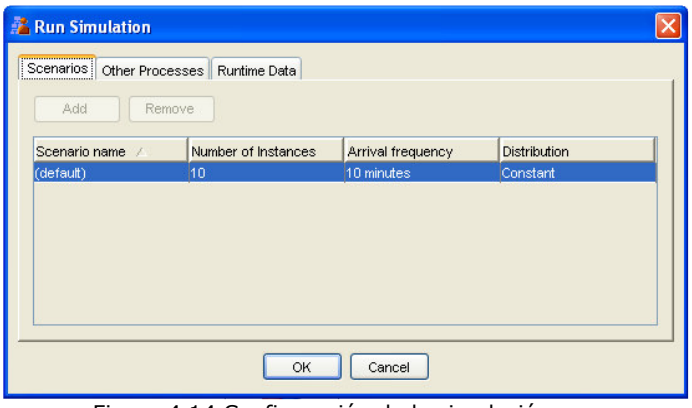


Figura 4.14 Configuración de la simulación

Observe la barra de generación de instancias y anote sus comentarios.

_____
_____
_____

Anote el valor del tiempo simulado.

_____

Anote los cuellos de botella detectados y proponga una posible solución.

_____
_____
_____

Complete el diagrama de la Figura 4.15, el cual representa las diferentes áreas de operación del modelo ETOM.

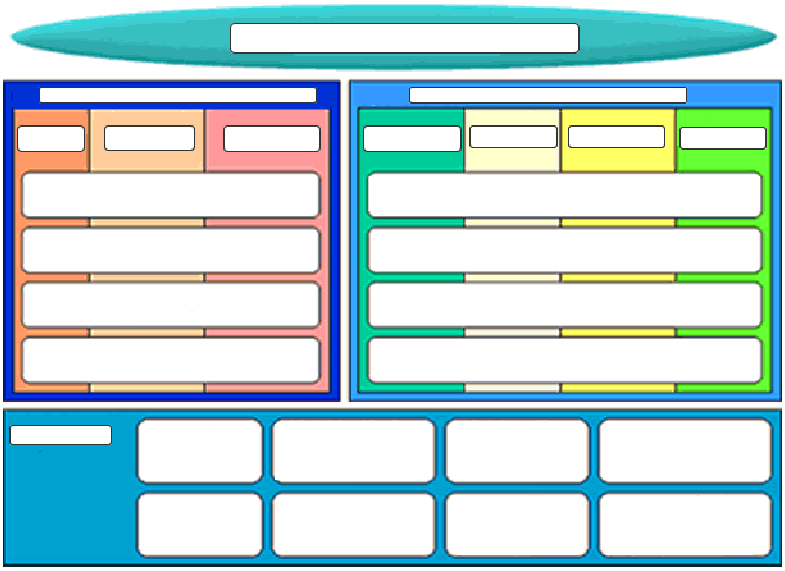


Figura 4.14 eTOM, (Telecom Operating Map) componentes principales

5.-Conclusiones

6.- Cuestionario Previo 4

1. Describa las principales ventajas de contar con una metodología de modelado.
2. Liste al menos 5 actividades de un administrador de red.
3. Investigue 3 beneficios medibles que se obtienen al contar con una administración apoyada en el modelo eTOM.

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 5
Introducción a la programación CORBA

1.- Objetivo de aprendizaje

El alumno conocerá e identificará los elementos que constituyen la programación distribuida sobre redes heterogéneas.

El alumno construirá una aplicación sencilla con CORBA, de manera que se familiarice con los pasos básicos necesarios para construir una aplicación mínima y cuente con la habilidad de explicar el código fuente.

2.- Conceptos teóricos

CORBA, es una herramienta que facilita el desarrollo de aplicaciones distribuidas en entornos heterogéneos, esto es donde existen diferentes sistemas operativos (Unix, Windows, MacOS, OS/2), diversos protocolos (TCP/IP, IPx), diferentes lenguajes de programación (Java, C, C++).

CORBA, define la infraestructura para la arquitectura OMA, Arquitectura de Administración de Objetos (Object Management Architecture), especificando los estándares necesarios para la invocación de métodos sobre objetos en entornos heterogéneos.

CORBA permite invocar métodos de objetos que residen en diferentes máquinas en entornos heterogéneos, esto significa que los objetos pueden estar desarrollados en diversos lenguajes y que los equipos pueden tener distinto hardware y sistema operativo, además de que los protocolos de comunicación suelen no ser semejantes. Ante estas circunstancias CORBA propicia el desarrollo de aplicaciones distribuidas.

CORBA hace uso de 3 conceptos básicos:

a. stub, representante local del objeto remoto encargado de la comunicación con el objeto remoto.
b. skeleton, encargado de la comunicación con el cliente.
c. cliente-servidor, encargados de las interacciones del tipo cliente-servidor.

CORBA hace una separación entre interfaz e implementación. La interfaz define un contrato, haciendo uso de las IDL, Lenguaje de Definición de Interfaz (Interface Definition Language), para posteriormente hacer un mapeo de ese contrato a distintos lenguajes de programación.

Las aplicaciones distribuidas se caracterizan: por su ejecución coordinada en diferentes máquinas comunicadas y alta complejidad en sus etapas de desarrollo debido a factores de administración de comunicaciones. CORBA abstrae estos detalles y hace la distribución de la aplicación un proceso menos complejo y costoso ya que organiza los servicios que se encuentran en la red a través de las interfaces IDL, siendo independientes de la plataforma y lenguaje de desarrollo.

CORBA ha llegado a ser incluido dentro de los clientes de Netscape y se pretende que llegue a sustituir al protocolo HTTP con IIOP, en el futuro.

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- Software de desarrollo de aplicaciones C++

4.- Desarrollo

La aplicación ha desarrollar consiste en un servidor que implementa un único objeto y un cliente que accede a ese objeto.

4.1 Escritura y compilación de una definición de IDL

El primer paso en cualquier aplicación CORBA es la definición de sus interfaces en IDL. CORBA separa claramente la interfaz de objetos de la implementación de los mismos. Las interfaces se definen utilizando el lenguaje IDL cuyas principales características son: su alto nivel de abstracción y sintaxis similar a C++. Para la implementación de los objetos se puede utilizar cualquier lenguaje de programación que proporcione un enlace con el lenguaje IDL. La implementación de CORBA es la que esconde al usuario de la arquitectura, toda la complejidad que pueda existir en un entorno.

Nota: Para que un lenguaje de programación se pueda implementar desde CORBA se debe tener definida la forma de enlazarse con el IDL.

A partir de la interfaz se generan de manera automática y para un lenguaje en concreto el código que enlaza a este objeto con CORBA, para posteriormente dentro del código de los clientes invocar una operación sobre el objeto.

4.2 Escritura y compilación de un servidor

El servidor crea los objetos remotos y hace accesibles sus referencias esperando que los clientes invoquen a dichos objetos o a sus métodos.

4.3 Escritura y compilación de un cliente

El cliente obtiene la referencia de uno o más objetos remotos en el servidor e invoca a sus métodos.

El cliente requiere la referencia del objeto remoto IOR, el tipo del objeto y el nombre de la operación que desea invocar. La invocación se realiza empleando el stub generado a partir del IDL y usando la invocación dinámica a través de DII, Interfaz de Invocación Dinámica (Dynamic Invocation Interface).

Investigue en qué consiste el ORB de CORBA

_____
_____
_____

4.4 Ejecución de la aplicación

Investigue la metodología de desarrollo para aplicaciones CORBA.

_____
_____
_____

Describe el funcionamiento de CORBA

_____
_____
_____

Investigue los pasos de desarrollo de una aplicación CORBA.

_____
_____
_____

5.-Conclusiones

6.-Cuestionario previo 5

1. Define qué es un entorno heterogéneo.
2. Explica en qué consiste el modelo TMN.
3. Describe las áreas fundamentales del modelo TMN.
4. Define que es CORBA.

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 6
Configuración de VoIP

1.- Objetivo de aprendizaje

El alumno adquirirá los conocimientos básicos acerca de VoIP como medio de comunicación, así como lo protocolos de señalización y transmisión para poder llevar a cabo una llamada telefónica por medio de redes IP.

El alumno aprenderá a configurar un conmutador de VoIP, empleando el software Asterisk para el PBX versión 1.2.7.1 y X-lite Softphone, para establecer una llamada VoIP.

2.- Conceptos teóricos

Los elementos principales de una red corporativa de voz, son los sistemas de conmutación, a los que hay que añadir los elementos de transmisión, de supervisión y los propios equipos de usuarios. Como elementos de conmutación existen varios tipos de dispositivos que pueden desempeñar esta función:

- KTS, Sistemas multilínea (Key Telephone System).
- PBX, Central Privada de Intercambio (Private Brand eXchange).
- Centrex, Oficina Central de Intercambio de Servicio (Central Office Exchange Service).

En esta práctica utilizará la conmutación por PBX, que es un sistema de telefonía que interconecta las extensiones telefónicas internas, con las troncales telefónicas; además usa métodos de conmutación digitales que pueden soportar la instalación de teléfonos y líneas tanto analógicas como digitales.

Otro de los elementos que empleará es el teléfono, que es un dispositivo de comunicación diseñado para transmitir señales eléctricas, desde su concepción original ha sufrido cambios y mejoras tanto en los métodos, como en los estándares y sistemas de explotación de la red.

Un softphone (combinación de Software y de Telephone) es un software que hace una simulación de teléfono convencional por computadora, permite usar la computadora para hacer llamadas a otros softphones o a otros teléfonos convencionales usando un VSP, Proveedor de Servicios de VoIP (VoIP Service Provider).

Asterisk, es una PBX completa diseñada en software que funciona en Linux y proporciona todas las características de una PBX. Trabaja con VoIP en varios protocolos (SIP, H323) e interactúa con casi todo el equipo estándar basado en telefonía IP.

El funcionamiento de VoIP, Voz sobre el Protocolo Internet (Voice Over Internet Protocol) consiste en la conversión de las señales de voz estándar en paquetes de datos comprimidos, que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. La evolución de la transmisión conmutada por circuitos basada en paquetes, toma el tráfico de la red pública telefónica y lo coloca en redes IP bien aprovisionadas. Las señales de voz se encapsulan en paquetes IP, que pueden transportarse como IP nativo o como IP por Ethernet, Frame Relay, ATM o SONET.

La operación básica de VoIP consiste fundamentalmente:

1) Digitalizar la voz en el extremo que emite.
2) Compactar la voz digitalizada.
3) Transmitirla como un conjunto de paquetes de datos por IP.
4) Recibir los paquetes en el otro extremo de la comunicación.
5) Descompactarlos.
6) Reproducirlos para ser escuchados.

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- Diademas con micrófono y audífonos.
- Servidor de VoIP Asterisk versión 1.2.7.1.
- Software X-lite softphone.

4.- Desarrollo

La convergencia de las redes de voz y de datos, han tenido como consecuencia profundos cambios en el desarrollo y la implementación de soluciones corporativas para la pequeña y mediana empresa fundamentalmente. Es por ello que un administrador de redes debe tener la capacidad de llevar a cabo la integración total de los servicios de comunicación.

4.1 Estándares de VoIP

En esta parte de la práctica aprenderá que para poder llevar a cabo una llamada telefónica a través de Internet, son necesarios los protocolos de señalización y transporte.

El soporte de una llamada telefónica sobre una red de paquetes, que en la mayoría de los casos es una red IP consta de dos fases:

1. Establecimiento de la llamada, esto es el equivalente a la obtención de tono de invitación a marcar, la marcación de número destino, la obtención de timbre de llamada o de la señal de ocupado y el descolgado del receptor para contestar la llamada.
2. La propia conversación.

En cualquiera de estas dos fases, es necesaria una serie de estándares que regulen y permitan la interconexión de equipos de distintos fabricantes, como los protocolos de señalización y los protocolos de transporte.

A qué se refieren lo protocolos de señalización.

_____
_____
_____

A qué se refieren lo protocolos de transporte.

_____
_____
_____

4.1.1 Protocolos de señalización

Los protocolos de señalización tiene como objetivo el establecimiento de las llamadas, y son básicamente el corazón de la voz sobre paquetes, distinguiéndola de otros tipos de servicios. Las funciones que realizan son:

1. Localización de usuarios, si un usuario A se desea comunicar con un usuario B, en primer lugar A necesita descubrir la localización actual de B en la red, con el fin de que la petición del establecimiento de sesión pueda establecerse.
2. Establecimiento de sesión, el protocolo de señalización permite al usuario llamado aceptar la llamada, rechazarla o desviarla a otra persona, buzón de voz o página Web.
3. Negociación de la sesión, la sesión multimedia que se esta estableciendo puede comprender diferentes tipos de flujo de información (audio, video, etc). Cada uno de estos flujos puede utilizar algoritmos de compresión de audio y video diferentes, dado que puede tener lugar en diferentes puertos y direcciones unicast o multicast. El proceso de negociación permite a las partes implicadas acordar un conjunto de parámetros de inicialización.
4. Administración de los participantes en la llamada, es posible añadir y/o eliminar miembros de una sesión ya establecida.
5. Otras funciones, como transferir una llamada o el colgar dicha llamada, requiere la conmutación entre los dos extremos.

Para cumplir con todos estos requisitos, existen fundamentalmente tres protocolos:

- H.323, fue concebido para comunicaciones multimedia en redes de área local, pero se ha extendido a la VoIP, proporciona control de llamadas, funciones de conferencia, administración de llamadas, capacidad de negociación de parámetros y otros servicios complementarios.
- SIP, Protocolo para Inicio de Sesión (Session Initiation Protocol), ha sido diseñado para soportar el control de llamadas y la negociación de sesiones de forma distribuida.
- MGCP, Protocolo de Control de Pasarela de Medios (Media Gateway Control Protocol), se trata de un control de protocolo que permite a un controlador central la monitorización de eventos que ocurren en los teléfonos IP y en las pasarelas, les impone el envío de información a direcciones específicas.

Complete la Tabla No. 6.1 con las características de los protocolos de señalización que se muestran.

Característica	H.323	SIP	MGCP
Organismo de estantarización			
Arquitectura			
Versión Actual			
Responsable del control de llamadas			
Puntos finales			
Señalización			
Soporte multimedia			
DTMF-relay			
Fax-relay			
Servicios suplementarios			

Tabla No. 6.1 Características de los protocolos de señalización

4.1.2 Protocolos de transporte

Los protocolos de transporte tienen como objetivo es asegurar la comunicación de voz; para el establecimiento de una red para transportar contenidos multimedia bajo demanda de las aplicaciones que la utilizan no es tarea trivial. Podemos contar con al menos, tres dificultades, que son:

1. Mayores requerimientos de ancho de banda.
2. La mayoría de las aplicaciones multimedia requieren el tráfico en tiempo real.
3. Secuencia de carácter crítico en la generación de los datos multimedia.

Para solucionar estos problemas, se crearon los protocolos de transporte, cuya misión es trasladar la información útil del origen al destino, cumpliendo con los requerimientos exigidos por las aplicaciones multimedia en general y por la voz en particular. Los protocolos de transporte más empleados en la integración de voz y de datos son RTP, Protocolo de Transporte en Tiempo Real (Real Time Transport Protocol) y el RTCP Protocolo de Control en Tiempo Real (Real Time Control Protocol).

Mencione cinco funciones que realice el RTP.

_____
_____
_____

Mencione cuatro funciones que realice el RTCP.

_____
_____
_____

4.2 Asterisk

La solución de telefonía basada en Asterisk, ofrece las funciones propias de las centralitas clásicas y además características avanzadas, logrando trabajar tanto con sistemas de telefonía estándar tradicionales como con sistemas de VoIP.

Asterisk está dotado con características que sólo ofrecen los grandes sistemas PBX propietarios como buzón de voz, conferencia de voz, llamadas en espera y registros de llamada detalladas. Para funcionar con VoIP no necesita de ningún hardware adicional, para interconectar con la telefonía tradicional requiere de tarjetas especiales de muy bajo costo (tarjetas FXO, FXS)

4.2.1 Instalación del servidor VoIP

Para la instalación del servidor de VoIP, se requiere de una PC que sea destinada para funcionar como conmutador telefónico. A esta PC le será cargado una versión de la distribución Linux CentOS que incluye Asterisk@home, ver Figura 6.1.

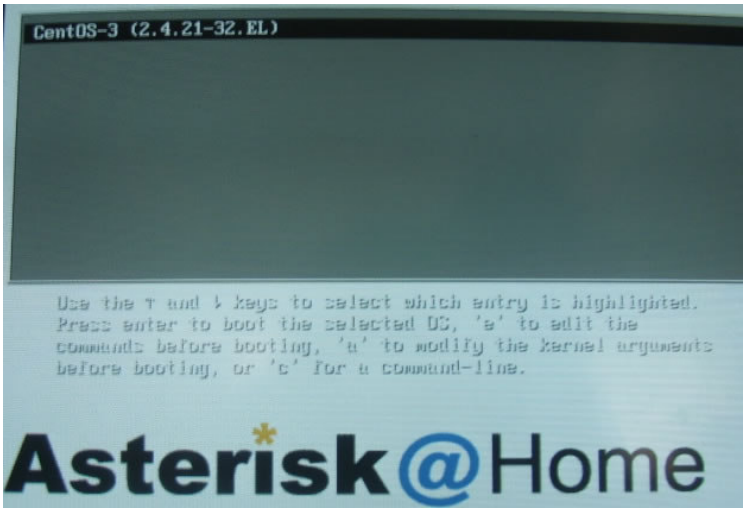


Figura 6.1 interfaz de la aplicación CenOS

Nota: Hay que tener en cuenta que Asterisk@home no es únicamente la aplicación como tal; la instalación nos borrará sin previo aviso todas las particiones que se encuentren en el equipo eliminado los datos.

Ya que se tiene instalado el sistema operativo y una vez reiniciado el equipo, el sistema estará ocupado compilando las aplicaciones. Trascurridos entre 30 y 45 minutos y tras un segundo reinicio, aparecerá el login del equipo para que el administrador se valide, ver Figura 6.2.

```
Welcome to Asterisk@Home
--------------------------------------------------
For access to the Asterisk@Home Web GUI use this URL
http://
For help on Asterisk@Home commands you can use from this
command shell type help-aah.
[root@asterisk1 root]#
```

Figura 6.2 Vista por primera ves del servidor VoIP, Asterisk@home

El sistema viene con un usuario por defecto ***root*** y una contraseña también por defecto ***password***, así que será necesario cambiarla mediante el comando ***passwd*** desde la línea de comandos.

A continuación se tendrá que ejecutar la aplicación ***netconfig***, para configurar los parámetros de la tarjeta de red (IP, máscara, DNS, gateway), el equipo se tendrá que reiniciar para que los cambios sean efectivos.

Una vez arrancado el servidor, aparecerá de nuevo el mismo mensaje de bienvenida, pero esta vez con la dirección Web a la que se llamará para ejecutar la administración del servidor, ver Figura 6.3.

Figura 6.3 Vista por primera ves del servidor VoIP, Asterisk@home

Hasta este punto se tiene ya instalado completamente el servidor, ahora será necesario configurar la herramienta vía Web.

4.2.2 Configuración vía Web

El objetivo de este punto es la configuración manual del servidor de VoIP accediendo a él a través de la conexión Web.

1. Abra un navegador Web como Internet Explorer y escriba la dirección 192.168.2.3 en el campo del URL, esta es la dirección que se asignó al servidor para poder ser administrado, ver Figura 6.4.

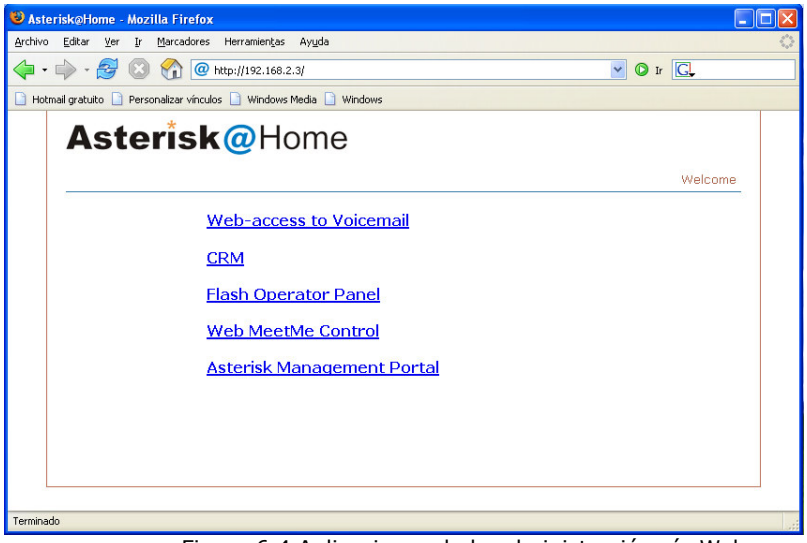


Figura 6.4 Aplicaciones de la administración vía Web

2. El navegador nos muestra la ventana de bienvenida a Asterisk@home, podrá entrar a los Web-access to Voicemail (acceso al correo de voz vía Web), CRM Administración de la Relación con el Cliente (Customer Relationship Management), Flash Operador Panel (Panel del operador Flash), navegue por estos menús.

¿Qué servicios proporciona el menú Web-access to Voicemail?

_____
_____
_____

¿Qué permite la opción CRM?

_____
_____
_____

¿Qué permite la opción Flash Operador Panel?

_____
_____
_____

3. Para los menús Web MeetMe Control y Asterisk Management Portal (Portal de administración de Asterisk), es necesario entrar como administrador, haga clic en el menú Asterisk Management Portal, coloque en los campos de usuario y contraseña, ***maint*** como nombre de usuario y ***password*** como contraseña. Estos campos son los predeterminados en la configuración inicial ver Figura 6.5.

Figura 6.5 Solicitud de usuario y contraseña

4. Una vez validados se tiene acceso a una serie de aplicaciones de administración: AMP, VoiceMail, CMR, Flash Panel, Web MeetMe Control y AMP. El objetivo de esta práctica se centra en el estudio del AMP (Asterisk Management Portal).

Nota: Dentro de esta aplicación es posible administrar el servidor en todos sus aspectos, incluso editando vía texto los ficheros de configuración.

5. Ingrese al menú Asterisk Management Portal, posteriormente arriba a la derecha, observe el menú SETUP haga clic en él, del lado izquierdo el elemento Extensions. A través de un sencillo formulario Web, podrá dar de alta y modificar las cuentas de usuario y extensiones de teléfono, ver Figuras 6.6a y 6.6b.

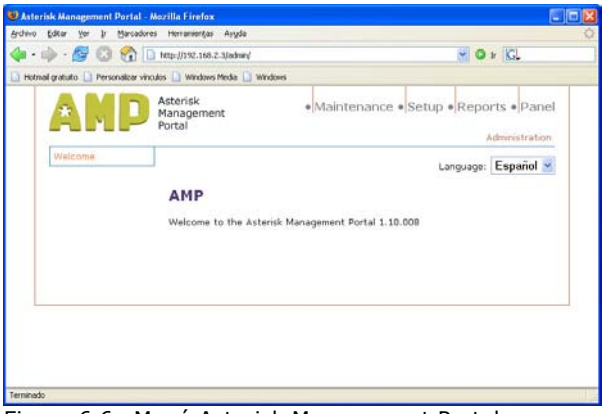


Figura 6.6a Menú Asterisk Management Portal

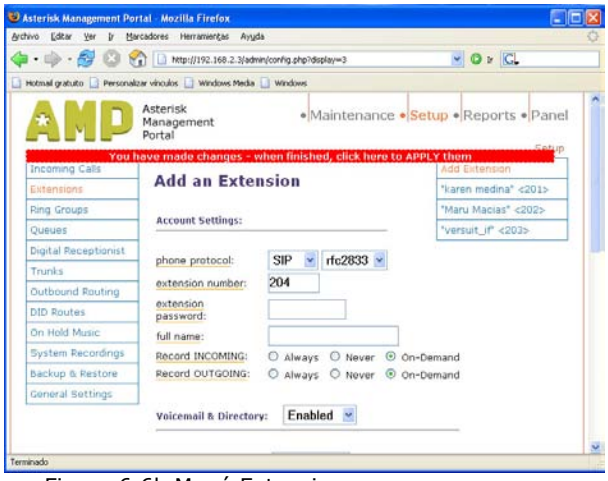


Figura 6.6b Menú Extensions

6. En este punto se dará de alta como usuario. Llene el formato de acuerdo a la Tabla No. 6.2

Características	Valores
Phone protocolo	SIP, RFC2833
Extension number	20*
Extensión password	inicianesnum
Full name	Primer nombre + Primer apellido

Tabla No. 6.2 Valores de configuración para los usuarios

Nota al Profesor: El número de extensión será consecutivo, así que se debe respetar el número que aparezca, se tiene que registrar uno por uno e ir actualizando la ventana del navegador, para que no de dupliquen las cuentas.

4.3 Softphone

Un softphone es típicamente parte de un entorno VoIP y puede estar basado en el estándar SIP/H.323 o basarse en un protocolo propietario.

Los softphone son parte del grupo tecnológico CTI, Integración Computadora-Telefonía (Computer Telephony Integrated). Hay varios tipos de softphones, algunos son a través de VoIP, otros funcionan utilizando teléfonos USB y algunos están implementados completamente en software que se comunica con las PBX a través de una Red de Área Local usando TCP/IP para controlar y marcar a través del teléfono físico. Comúnmente esto se hace a través de un entorno de centro de llamadas para comunicarse desde un directorio de clientes o para recibir llamadas, donde la información del cliente emerge en la pantalla de la computadora cuando el teléfono suena, dando a los agentes del centro de llamadas un volumen de información sobre quien está llamando, como recibirlo y dirigirse a él o ella.

4.3.1 Instalación softphone X-Lite

El X-Lite es un software muy amigable y robusto que permite realizar llamadas por Internet a través de un servidor de VoIP.

En esta parte de la práctica aprenderá a configurar un softphone, para poder establecer una llamada telefónica.

Nota Profesor: Se debe contar con una carpeta en C:/ con el nombre VoIP, en la que se encuentre el ejecutable del softphone –X-lite Setup

1. Abra un explorador de Windows a través del menú Inicio>Todos los programas>Accesorios>Explorador Windows, una vez abierta la ventana haga clic en C:/, localice y abra la carpeta VoIP, haga clic dos veces sobre –X-lite Setup, a continuación haga clic en el botón Next para continuar con la instalación.
2. Verifique que esté seleccionada la opción ***i accept the agreement*** y después haga clic en el botón Next.
3. Posteriormente el asistente le informa sobre la versión que se va instalar, para continuar haga clic en el botón Next; a continuación le preguntará donde desea instalar la aplicación, dejará la ubicación por default, por lo tanto haga clic en Next.
4. Nuevamente haga clic en Next, y verifique que sólo este seleccionada la casilla de Create a desktop icon y haga clic en Next.
5. Haga clic en el botón Install, espere unos segundos y para completar la instalación haga clic en Finish.

4.3.2 Configuración softphone X-Lite

Este punto de la práctica aprenderá la configuración del softphone, para poder establecer una llamada.

1. Para iniciar la configuración del programa X-lite, haga doble clic en el icono creado en el escritorio.
2. En el siguiente diagrama se muestran los elementos de softphone, para que se familiarice con la herramienta, ver Figura 6.7.

Figura6.7 Elementos de softphone X-Lite

3. A continuación se mostrará en el escritorio el softphone y el menú para poder configurar la herramienta, ver Figura 6.8

Figura 6.8 Softphone y el menú listo para configurar

4. Haga clic derecho sobre el softhope y elija del menú desplegable la opción Audio Tuning Wizard…, ver Figura 6.9, posteriormente aparecerá la ventana de Audio Tuning Wizard para poder configurar el audio y micrófono.

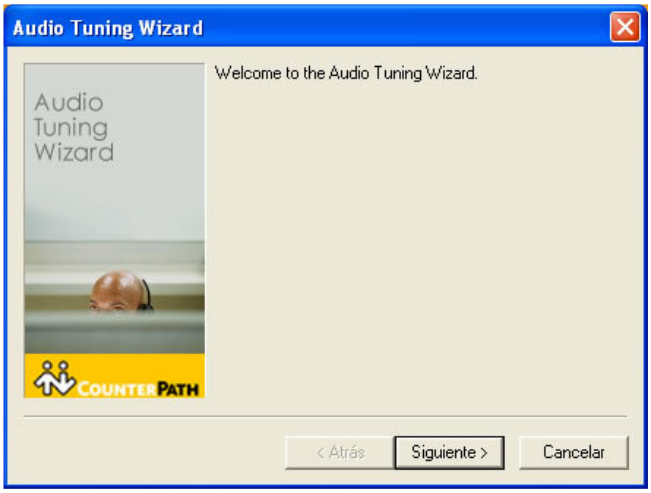


Figura 6.9 Ventana de bienvenida al Audio Tuning Wizard

5. Conecte la Diadema (audífonos y micrófono) a la computadora verificando que estén conectados correctamente en su logar correspondiente.
6. Haga clic en *Siguiente* para configurar la aplicación, seleccione el tipo de micrófono que se va a utilizar y haga clic en siguiente.
7. En la siguientes dos ventanas debe ajustar el volumen de los audifonos y la intensidad del micrófono, una vez realizado esto haga clic en *Siguiente* en cada ventana respectivamente, a continuación calibré el micrófono y posteriormente haga clic en *Siguiente*.
8. Elija la opción Cable / DSL / LAN y haga clic en *Siguiente*, para finalizar con la configuración del Audio Tuning Wizard haga clic en Finalizar.

Nota: Con el Audio Tuning Wizard se han configurados automáticamente las opciones Speaker Audio device, Mic Audio device e Ring Audio Device del menú System Settings, que posteriormente serán analizados.

9. Configure el softphone a la red, de acuerdo a los parámetros que se muestran en la Tabla No. 6.3, ver Figura 6.10, en el menú de Network.

Nota: Este menú se encuentra en Main Menu> System Settings> Network

Figura 6.10 Menú Network configurado

Características	Valores
Auto_Detect_IP:	Yes
Listen_on_IP	en blanco
Use X-NAT to Choose SIP/RTP Ports	Never
Listen SIP Port	5060
Listen RTP Port	8000
NAT Firewall IP	en blanco
Out Bound SIP Proxy	en blanco
Force Firewall Type	(do not force firewall type)
Primary STUN Server	en blanco
Secondary STUN Server	en blanco
Primary DNS Server	132.248.204.1 (o bien la dirección LAN, en presencia de LAN con DNS interno)
Secondary DNS Server	132.248.10.2 (o bien la dirección LAN, en presencia de LAN con DNS secundario interno)
Provider DNS Server	

Tabla No. 6.3 Valores que deben configurase en el menú Network

10. Realizado el punto anterior haga clic en BACK, a continuación seleccione SIP Proxy haciendo clic en SELEC, posteriormente haga clic dos veces en [Default], para poder configurar los parámetros siga la Tabla No.6.4, ver Figuras 6.11a y 6.11b.

Figura 6.11a Configurando parámetros SIP proxy a

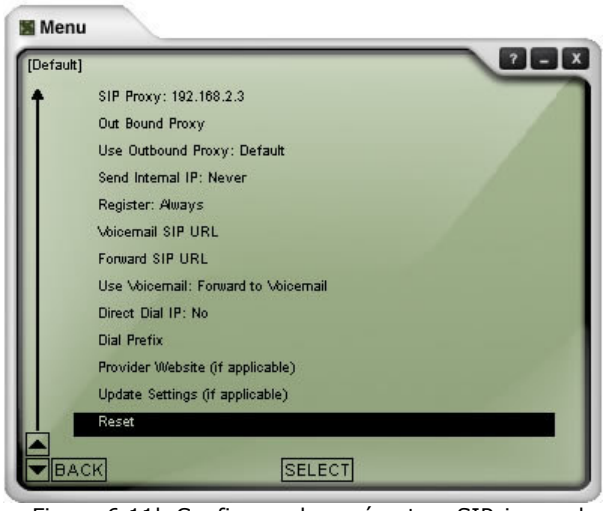


Figura 6.11b Configurando parámetros SIPsiproxy b

Características	Valores
Enabled :	Yes
Display Name	Primer nombre + Primer apellido
Username	Numero asignado por el administrador (201)
Authorization User	Numero asignado por el administrador (201)
Password	Password registrado en la configuración Vía Web
Domain/Realm	192.168.2.3
SIP Proxy	192.168.2.3
Out Bound Proxy	en blanco
Use Out Bound Proxy	defaul
Send Internal IP	Never
Register	Always
Voicemail SIP URL	en blanco
Forward SIP URL	en blanco
Use Voicemail	Forward to Voicemail
Direct Dial IP	no
Dial Prefix	en blanco
Provider WebSite	n/a (if applicable)
Update Settings	n/a (if applicable)

Tabla No. 6.4 Valores que deben configurase en el menú SIP Proxy> [Default]

11. Haga dos veces clic en BACK, para regresar al menú System Settings.

Como se observa, este menú muestra otras opciones, los parámetros X-Tunnel, X-Cipher e X-Vox son soportados por X-PRO. Los últimos menús Speaker Audio device, Mic Audio device e Ring Audio Device se configuran automáticamente durante el ***Audio Tuning Wizard***.

Investigue a que sé refiere X-PRO.

_____

_____

_____

12. Ahora regrese al Main Menú, haciendo clic en BACK.
13. A continuación haga clic en opción SELEC en Advanced System Setting, posteriormente a SIP Settings, en este punto sólo configurará dos parámetros de acuerdo a la Tabla No. 6.5, los demás los dejará con los valores predeterminados, ver Figura 6.12.

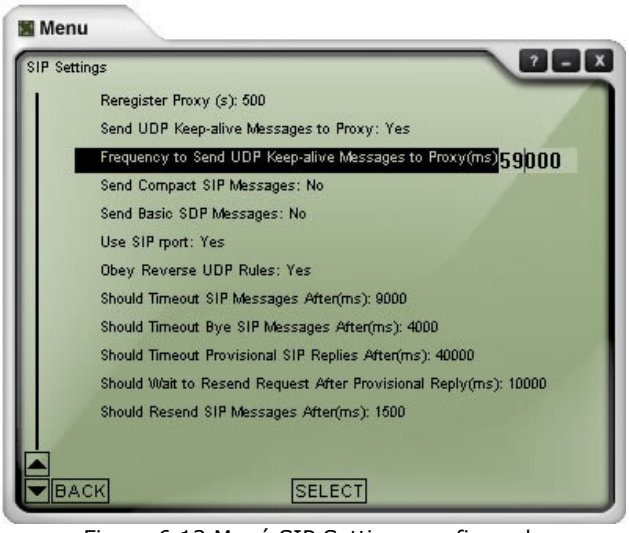


Figura 6.12 Menú SIP Settings configurado

Características	Valores
Reregister Proxy (s)	500
Frequency to send UDP message...	59000

Tabla No. 6.5 Valores que deben configurase en el menú SIP Settings

4.4 Estableciendo la llamada

Para poder establecer la llamada deberá seguir los siguientes pasos:

1. Como primer paso deberá elegir la línea por la cual desea hacer la llamada, para nuestro primer caso elegiremos la línea 1.
2. Marque el número de la computadora que se le ha asignado de acuerdo a la Tabla No. 6.6. y a complete la tabla.

Nota: Pida el número de extensión de la máquina que se le asigno a su compañero de laboratorio, ubicado en esa computadora.

Computadora No.	No. De extensión		Computadora No.	No. De extensión
1		→	6	
2		→	7	
3		→	8	
4		→	9	
5		→	10	

Tabla No. 6.6 Asignación para establecer la llamada

3. Haga clic en el botón llamar y converse la persona.

¿Pudo establecer la llamada?

_____
_____
_____

4. Cuelgue haciendo clic en el botón colgar.
5. Ahora, vuelva ha marcar a cualquier otra extensión por la línea 1, espere a que le contesten y pase a la línea 2 y marque a número de extensión que se le asigno en la Tabla No. 6.6.

¿Que fue ocurrió con la llamada que tiene en la línea 1?

_____
_____
_____

5.-Conclusiones

¿Que ventajas ofrece la tecnología de voz sobre IP?

_____
_____
_____
_____
_____

Mencione al menos 5 aplicaciones de la VoIP.

_____
_____
_____
_____
_____

6.- Cuestionario Previo

1. ¿Qué es el SS7?
2. ¿Qué es la técnica de conmutación de circuitos?
3. ¿Qué es la técnica conmutación de paquetes?

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 7 Parte A
Comunicaciones Inalámbricas: red tipo infraestructura

1.- Objetivo de aprendizaje

El alumno aprenderá a configurar una red inalámbrica tipo infraestructura vía Web, aprenderá a utilizar esta herramienta.

El alumno aprenderá a habilitar en el access point un sistema de filtrado basado en MAC (a veces llamado también filtrado por hardware), que solo permitirá el acceso a la red a tarjetas de red concretos, identificados con su MAC.

2.- Conceptos teóricos

En sus inicios, las aplicaciones de las redes inalámbricas fueron confinadas a industrias y grandes almacenes. Hoy en día, las WLAN Redes Inalámbricas de Área Local (Wireless Local Area Network), son instaladas en Universidades, oficinas, hogares y hasta en espacios públicos. Las WLAN se componen de computadoras portátiles o de escritorio (terminales) que se conectan a dispositivos fijos llamados AP vía señales de radio o infrarrojo.

Las estaciones de trabajo se comunican entre sí gracias a que utilizan la misma banda de frecuencias e internamente tienen instalados el mismo conjunto de protocolos, las redes Wi-Fi utilizan el estándar de comunicaciones IEEE 802.11.

IEEE 802.11 define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando las normas de funcionamiento en una WLAN, que emplea ondas de radio en la banda de 2.4 GHz y 5 GHz.

A. Nivel Físico

El nivel físico definido en el estándar 802.11 establece dos posibles topologías y tres tipos de medios inalámbricos, que funcionan a cuatro velocidades posibles.

El bloque constructivo fundamental de una LAN inalámbrica es el BSS, Conjunto de Servicios Básicos (Baste Serve Set), el cual es un área geográfica en la que las estaciones inalámbricas se pueden comunicar. La configuración y el área BSS dependen del tipo de medio inalámbrico que se use y de la naturaleza del entorno.

El estándar define dos tipos de topologías red inalámbrica:

- La topología ad hoc. Todos los dispositivos de la red dentro de BSS son móviles o portátiles, es decir inalámbricos.
- La topología de infraestructura. Consta de al menos un AP inalámbrico que puede estar conectado a una red fija estándar por medio de un cable y por dos o más estaciones inalámbricas.

B. Nivel de Enlace de Datos

El estándar define la funcionalidad del subnivel MAC, Control de Acceso al Medio (Medium Access Control), que consiste en un servicio del transporte no orientado a conexión que lleva los datos LLC, Control de Enlace Lógico (Logical Link Control) a un destino de la red en

forma de MSDU, Unidades de Datos de Servicio MAC. Este servicio se define por un formato de trama y un mecanismo de control de acceso al medio.

El estándar define tres tipos básicos de trama del nivel MAC:

- Tramas de datos, utilizadas para transmitir datos de los niveles superiores entre estaciones.
- Tramas de control, utilizadas para regular el acceso al medio de la red y para reconocer las tramas de datos transmitidas.
- Tramas de administración, utilizadas para intercambiar información de administración de la red para realizar funciones de red, como asociación y autenticación.

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- 2 Computadoras
- 2 Tarjeta de Red Inalámbrica
- 2 Tarjetas inalámbricas
- 2 Access point

4.- Desarrollo

4.1 Configuración vía Web del access point

AP, Puntos de Access Points (Access Points), es una estación base utilizada para administrar las comunicaciones entre los distintos terminales, funcionan de manera autónoma, sin necesidad de ser conectados directamente a ninguna computadora.

El AP no sólo es el medio de interconexión de todos los terminales inalámbricos, sino que también es el puente de interconexión con la red fija e Internet.

Nota Profesor: Para realizar esta práctica se deben tener instaladas y configuradas al menos dos tarjetas de red inalámbricas (Práctica 1).

Indique los componentes del access point implementado en el Laboratorio de Redes, ver Figura 7.1.

Figura 7.2 Vista del access Point MSI Gíreles 11b Accees Point AP11B

Analicé los indicadores de luz de access point, que información nos proporcionan.

_____
_____
_____

En este punto de la practica realizará la configuración vía Web, este método resulta intuitivo y grafico para la administración del access point.

1. Abra un navegador Web como Internet Explorer y escriba la dirección 192.168.2.*** en el campo del URL, esta es la dirección que se asignó al access point para poder ser administrado, ver Figura 7.3

Figura 7.3 Solicitud de usuario y contraseña

2. En los campos de usuario y contraseña escriba ***admin***, como nombre de usuario y pulse la tecla Enter en el indicador de contraseña. Estos campos son los predeterminados en la configuración inicial.

Nota: El segmento de red ha utilizar es el que ya esta configurado en el laboratorio (192.168.2.0 con mascara 255.255.255.0).

Vamos a configurar uno de los access point, este tiene por default una IP para acceder a su configuración, así que se debe de entrar a esta dirección IP (esta IP puede ser la que se muestra en la figura 7.4 y cambiarla por una del segmento de red correspondiente.

Default Parameters

IP Address	192.168.1.254
Password	admin
Subnet Mask	255.255.255.0
SSID	AP11B
Channel	7
Encryption	Off
DHCP Client	Disable

Figura 7.4 Configuración por default del Access Point.

Para cambiar esta configuración se debe acceder a la IP por default desde un navegador para poder cambiar esta configuración, esta IP se debe de teclear en la parte de dirección, como lo muestra la Figura 7.5.

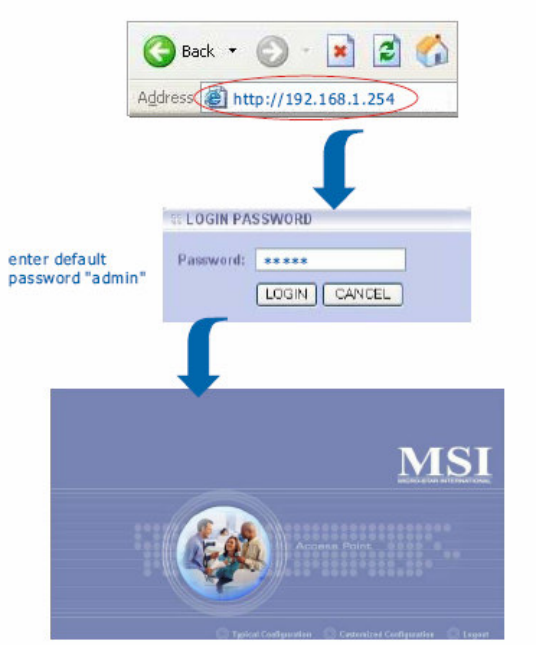


Figura 7.5 Configuración del Access Point.

A continuación se debe de configurar la IP, la mascara de red y la puerta de enlace, como se muestra en la Figura 7.6 Que para nuestro segmento de red pueden ser los valores siguientes:

Dirección de Red: 192.168.2.254
Mascara de Red: 255.255.255.0
Puerta de Enlace (Geteway): 192.168.2.1

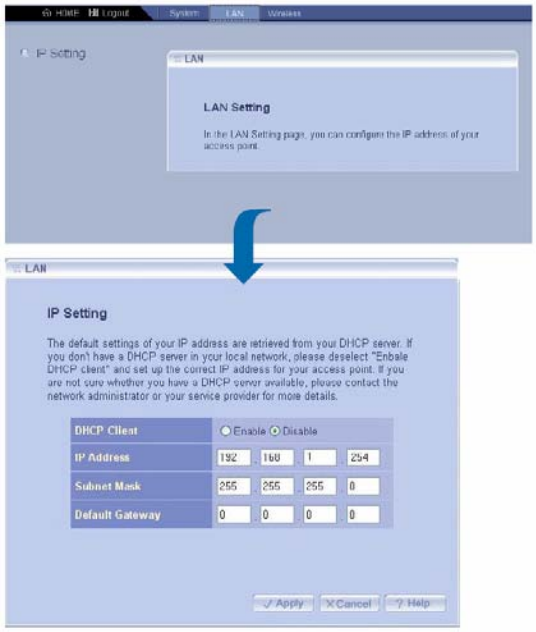


Figura 7.6 Configuración de IP del Access Point.

¿Qué pasa si el access point tiene una dirección IP fuera del segmento de red del laboratorio?

_____

_____

_____

Después de teclear estos valores dar ***Apply*** en la ventana actual y probar la conexión a red. Como lo muestra la Figura 7.7.

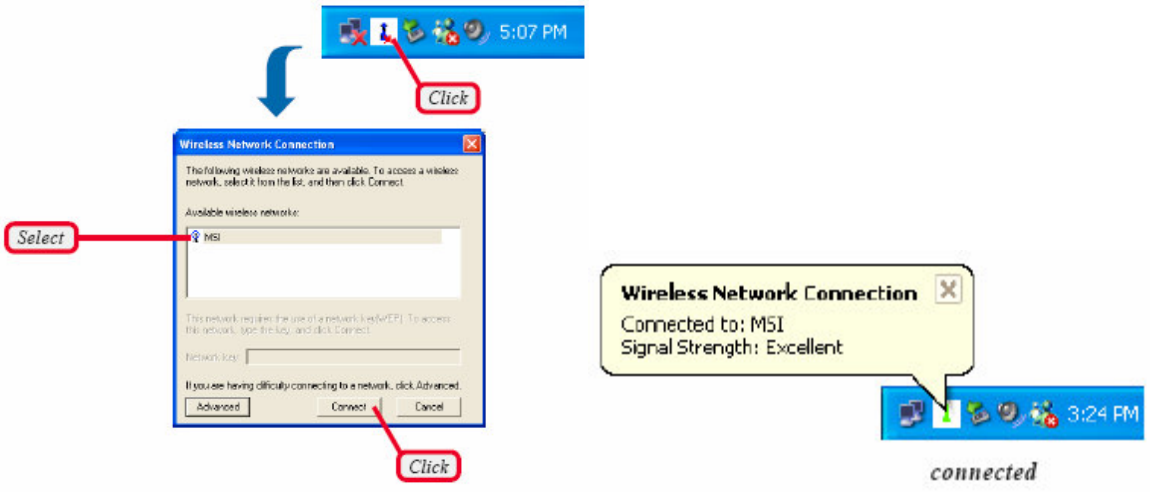


Figura 7.7 Conexión Red Inalámbrica.

4.2 Filtrado por MAC

En la mayoría de los casos no necesitaras conocer/utilizar el dato de la dirección física de tu adaptador de red, ni para configurar la conexión a internet, ni para montar tu red doméstica.

El caso mas usual en el que puedes necesitar conocer el dato de la dirección MAC es si configuras una red WIFI y habilitas en el punto de acceso un sistema de filtrado basado en MAC (a veces llamado también filtrado por hardware), que solo permitirá el acceso a la red a adaptadores de red concretos, identificados con su MAC. Todos los adaptadores de red inalámbricos tienen una dirección MAC única.

Es muy recomendable utilizar el filtrado por MAC con la cifrado WPA, ya que hay cientos programas que pueden falsificar las direcciones MAC, además de que los usuarios suelen intercambiar sus adaptadores de red WI-FI.

¿Qué es el cifrado WPA y WEP?

_____
_____
_____

Nota: Para poder realizar esta práctica hay que tener instaladas al menos dos tarjetas de red inalámbrica en computadoras diferentes para que a una de ellas no se le permita el acceso al access point.

La MAC address es un número único asignado a cada tarjeta de red; en cuanto identifica dispositivos de red, es también conocida como la dirección física.

¿Qué comando se puede utilizar para determinar la dirección MAC de la tarjeta en Windows y en Linux?

Windows _____
Linux _____

4.2.2 Ingresando al sistema de administración

Una vez hecho el paso 1 se tiene que acceder al access point desde un navegador empleando su dirección IP asignada (por ejemplo: 192.168.2.254), como se ve en la Figura 7.8. Una vez que se accedió al access point ir a la parte de Wireless, como lo muestra la figura 7.9

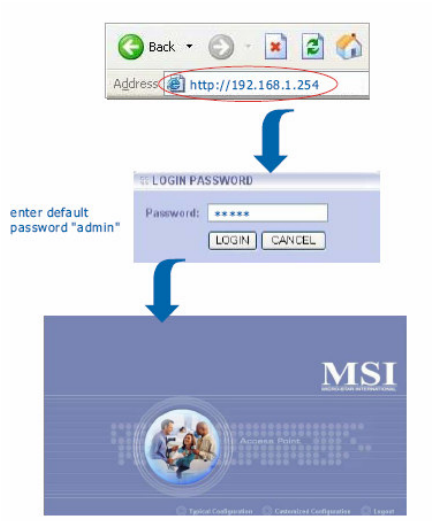


Figura 7.8 Acceso al Access Point.

Figura 7.9 Sección Wireless del Access Point.

4.2.3 Control de Asociación

1. Obtenga la dirección MAC de las tarjetas de red inalámbricas, a partir de

Ir a la subsección de Association Control, como lo muestra la Figura 7.10. Y en esta parte teclear la dirección MAC identificada en el paso 1 de la tarjeta de red que se quiere negar el acceso al access point.

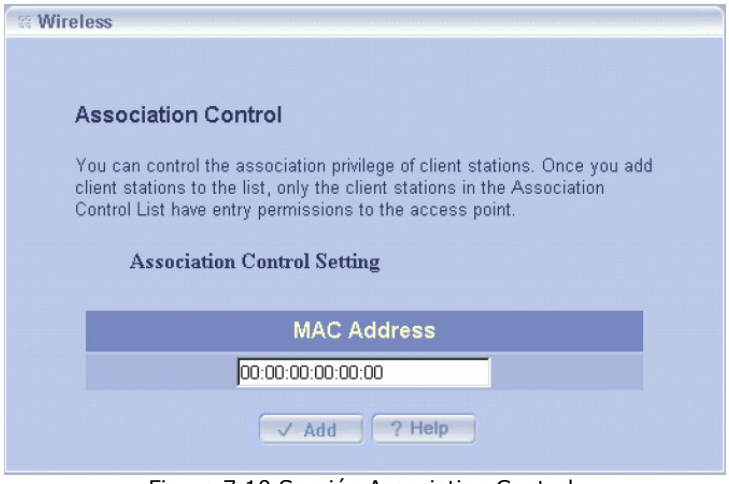


Figura 7.10 Sección Association Control.

4.2.4 Comprobación de denegación

Probar que en realidad la tarjeta de red seleccionada ya no tiene acceso al access point, haciendo un *ping* a la dirección IP de la puerta de enlace (por ejemplo: 192.168.2.1, como se muestra en la Figura 7.11. Además al intentar conectarse al access point marcara un error como el de la Figura 7.12.

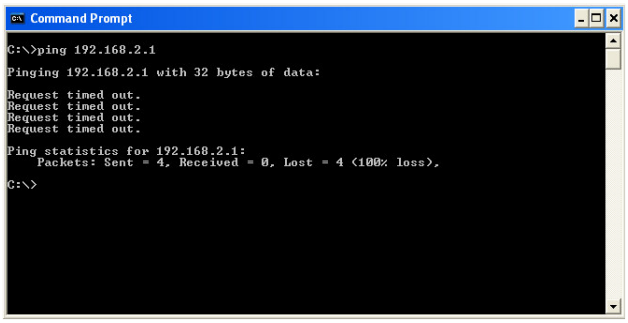


Figura 7.11 Comprobación de la Tarjeta de Red.

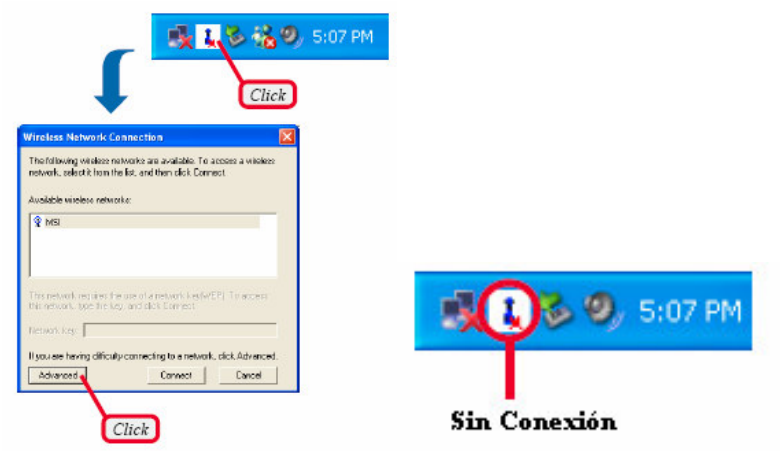


Figura 7.12 Error cuando no esta conectada a la red

5.-Conclusiones

¿Es útil una red inalámbrica infraestructura?
¿En que casos es preferible montar una red inalámbrica infraestructura?
¿Cuál es el alcance de este tipo de redes?
¿En qué casos es útil filtrar por MAC?
Si filtramos por MAC, ¿esta nuestra red completamente segura? Explique su respuesta.

6.- Cuestionario Previo

1. ¿Cuál es la definición de una tarjeta de red inalámbrica?
2. ¿Qué es una red inalámbrica infraestructura?
3. ¿Qué es un access point?
4. ¿Cuál es la definición de la dirección MAC (***Me****dia* ***A****ccess* ***C****ontrol address*)?
5. ¿Qué es ARP (Address Resolution Protocol)?

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 7 Parte B
Comunicaciones Inalámbricas; servidor DHCP (adicional)

1.- Objetivo de aprendizaje

El alumno analizará las características y los elementos que conforman un servidor DHCP.

El alumno instalará y configurará los parámetros un servidor DHCP, en una computadora con Sistema Operativo Linux.

2.- Conceptos teóricos

3.- Equipo y material necesario

3.1 Material que debe traer el alumno

3.2 Equipo del Laboratorio

1 Access Point
2 Tarjetas de Red Inalámbrica

Red del laboratorio
1 Computadora con sistema operativo Windows, con Ethereal instalado
1 Computadora con sistema operativo Linux, con Ntop instalado

4.- Desarrollo

4.1 Servidor DHCP

Un servidor DHCP (Dynamic Host Configuration Protocol) se utiliza para asignar direcciones IP a las computadoras de los usuarios cuando éstas arrancan.

Sin DHCP, cada dirección IP debe configurarse manualmente en cada ordenador y, si el ordenador se mueve a otro lugar en otra parte de la red, se debe de configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si el ordenador es conectado en un lugar diferente de la red.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- **Asignación manual**: donde la asignación se basa en una tabla con direcciones MAC (pares de direcciones IP ingresados manualmente por el administrador). Sólo las computadoras con una dirección MAC que figure en dicha tabla recibirá el IP que le asigna dicha tabla.

- **Asignación automática**: donde una dirección de IP libre obtenida de un rango determinado por el administrador se le asigna permanentemente a la computadora que la requiere.
- **Asignación dinámica**: el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

Algunas implementaciones de DHCP pueden actualizar el DNS asociado con los servidores para reflejar las nuevas direcciones IP mediante el protocolo de actualización de DNS establecido en RFC 2136 (Inglés).

El DHCP es una alternativa a otros protocolos de gestión de direcciones IP de red, como el BOOTP (*Bootstrap Protocol*). DHCP es un protocolo más avanzado, pero ambos son los usados normalmente.

Cuando el DHCP es incapaz de asignar una dirección IP, se utiliza un proceso llamado "Automatic Private Internet Protocol Addressing".

4.1.1 Anatomía del protocolo DHCP

DHCP usa los mismos puertos asignados por el IANA (*Autoridad de Números Asignados en Internet* según siglas en inglés) en BOOTP: 67/udp para las computadoras servidor y 68/udp para las computadoras cliente.

DHCP Discover

La computadora cliente emite peticiones masivamente en la subred local para encontrar un servidor disponible, mediante un paquete de broadcast. El router puede ser configurado para redireccionar los paquetes DHCP a un servidor DHCP en una subred diferente. La implementación cliente crea un paquete UDP (*Protocolo de Datagramas de Usuario* según siglas en inglés) con destino 255.255.255.255 y requiere también su última dirección IP conocida, aunque esto no es necesario y puede llegar a ser ignorado por el servidor.

DHCP Offer

El servidor determina la configuración basándose en la dirección del soporte físico de la computadora cliente especificada en el registro CHADDRvbnv. El servidor especifica la dirección IP en el registro YIADDR. Como la cual se ha dado en los demás parametros.

DHCP Request

El cliente selecciona la configuración de los paquetes recibidos de *DHCP Offer*. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor.

DHCP Acknowledge

El servidor confirma el pedido y lo publica masivamente en la subred. Se espera que el cliente configure su interface de red con las opciones que se les otorgo.

DHCP Inform

El cliente envía una petición al servidor de DHCP: para solicitar más información que la que el servidor ha enviado con el DHCPACK original; o para repetir los datos para un uso particular - por ejemplo, los browsers usan *DHCP Inform* para obtener la configuración de los proxies a través de WPAD. Dichas peticiones no hacen que el servidor de DHCP refresque el tiempo de vencimiento de IP en su base de datos

DHCP Release

El cliente envía una petición al servidor de DHCP para liberar DHCP y los el cliente desconfigura su dirección IP. Como los clientes generalmente no saben cuándo los usuarios pueden desconectarles de la red, el protocolo no define el envío del *DHCP Release* como obligatorio.

4.1.1.1 Parámetros confugurables

Un servidor DHCP puede proveer de una configuración opcional a la computadora cliente. Dichas opciones están definidas enRFC 2132 (Inglés)

Lista de opciones configurables:

- Dirección del servidor DNS
- Nombre DNS
- Puerta de enlace de la dirección IP
- Dirección de Publicación Masiva (*broadcast address*)
- Máscara de subred
- Tiempo máximo de espera del ARP (*Protocolo de Resolución de Direcciones* según siglas en inglés)
- MTU (*Unidad de Transferencia Máxima* según siglas en inglés) para la interfaz
- Servidores NIS (*Servicio de Información de Red* según siglas en inglés)
- Dominios NIS
- Servidores NTP (*Protocolo de Tiempo de Red* según siglas en inglés))
- Servidor SMTP
- Servidor TFTP
- Nombre del servidor WINS

4.1.2 Instalación y configuración del servidor DHCP

En este paso llevaremos a cabo la instalación y configuración del servidor DHCP. Para ello debemos descargar el paquete DHCP rpm, (usamos rpms porque nuestro servidor tiene Red Hat y éste usa paquetes rpm) esto se podrá hacer del servidor del laboratorio.
Para instalarlo teclear lo siguiente:

rpm –ivh "nombre del paquete"

¿Para que nos sirven las opciones ivh en el comando rpm?

_____
_____
_____

Ya que tenemos instalado el paquete, el siguiente paso es la configuración, el archivo de configuración es el que se llama dhcpd.conf, que se encuentra en el directorio /etc.

A continuación se listaran y explicaran algunos de los parámetros que se pueden configurar en este archivo.

- authoritative;
- one-lease-per-client on;
- server-identifier ppfm.atenea.dom;
- default-lease-time 604800;
- max-lease-time 604800;
- option subnet-mask 255.255.255.0;
- option broadcast-address 192.168.2.255;
- option routers 192.168.2.254;
- option domain-name-servers 192.168.1.10;
- option domain-name "seguridad.unam.mx";
- ddns-domainname "seguridad.unam.mx ";
- ddns-update-style ad-hoc;
- ddns-updates on;
- option netbios-name-servers 192.168.2.10;

- subnet x.x.x.x netmask y.y.y.y {
  range a.a.a.a b.b.b.b;
  }

authoritative; Supone que la configuración correcta para la red es la definida en el servidor DHCP y tratará de reasignar datos a los clientes mal configurados. Este parámetro puede ser global o asignado a una declaración de subred. Los cambios realizados en el servidor marcado como authoritative tienen una rápida propagación en la subred ya que se reconfigura cualquier cliente con la antigua configuración.

authoritative; tiene el significado opuesto al anterior parámetro.

one-lease-per-client on; cuando esta opción está en "on" y un cliente solicita una asignación, el servidor libera automáticamente cualquier otra asignación que tenga ese cliente. Se supone que si el cliente hace una solicitud es porque ha olvidado que tuviera alguna, es decir tiene un solo interfaz de red. Si no se da esta situación en los clientes hay que usar este parámetro con precaución.

server-identifier 192.168.2.1; este parámetro identifica el nodo que alberga el servicio DHCP. Sólo se deber usar cuando el nodo tenga más de una dirección IP asignada al interfaz.

default-lease-time 604800; indica el tiempo de asignación en segundos.

max-lease-time 604800; indica el tiempo máximo de asignación en segundos.

ddns-updates on; activa la actualización DNS con los valores asignados mediante DHCP.

ddns-domainname "seguridad.unam.mx"; indica el dominio en el que se actualizan los DNS

ddns-update-style interim; esta línea indica el método de actualización DNS automática con los valores de la IP asignados por DHCP. Más adelante veremos como hay que modificar las zonas en el archivo /etc/named.conf para permitir la actualización.

option subnet-mask 255.255.255.0; definimos la máscara general de red que vamos a utilizar.

option broadcast-address 192.168.1.255; definimos la dirección de difusión de la red.

option routers 192.168.2.1; definimos el gatewaye de la red.

option domain-name-servers 192.168.2.10; definimos la dirección del servidor DNS de la red.

option domain-name "atenea.dom"; definimos el nombre del dominio DNS que se añade a los nombres de host.

option netbios-name-servers 192.168.2.10; definimos la dirección del servidor WINS para NetBios.

Y por último definimos la red en la que queremos hacer asignaciones y los rangos de direcciones que puede asignar el servidor DHCP.

subnet _____
range _____

Iniciar el demonio de DHCP y hacer pruebas de que en realidad esta asignando IPs dentro del segmento especificado.

¿Cómo se pueden realizar estas pruebas?

_____
_____
_____

5.-Conclusiones

¿Por qué es útil un servidor DHCP?
¿Cuándo debemos utilizar un servidor DHCP?

6.Cuestionario Previo

¿Para que sirve un servidor DHCP?

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 8
Videoconferencia

1.- Objetivo de aprendizaje

El alumno examinará los estándares y elementos que conformar un sistema de videoconferencia.

El alumno conocerá y aprenderá como se lleva a cabo un sistema de videoconferencia en la sala de Videoconferencia del Centro de Docencia de la Facultad de Ingeniería de la UNAM.

2.- Conceptos teóricos

La videoconferencia es un sistema digital de telecomunicaciones que permite mantener reuniones colectivas entre varias personas que se encuentran en lugares distantes. Esta comunicación se realiza en tiempo real, vía telefónica y se transmite tanto vídeo como el sonido, en ambos sentidos, lo que podríamos llamar una reunión virtual. Los interlocutores se ven y se hablan como si estuvieran en la misma sala de reuniones, a la vez que se pueden intercambiar datos, fax, información gráfica, vídeo, diapositivas, etc.

La mayoría de los sistemas de Videoconferencia utilizan el vídeo digital comprimido para la transmisión de vídeo por medio de las redes de transmisión de datos de alta capacidad como la ISDN.

Videoconferencias, a menudo se transmiten por medio de líneas del teléfono especializadas como T-1/E1. Estas líneas trabajan a altas velocidades y son muy eficaces para esta tecnología, pero se alquilan por medio de circuitos especiales y tienen un costo de mantenimiento mensual relativamente alto. Por otro lado, los costos de comunicación se calculan en función de la distancia y en el tiempo de comunicación. Los sistemas de Videoconferencia pueden operar a distintas velocidades de transmisión de datos, es decir a varios fragmentos de capacidad de líneas E-1. Un sistema de Videoconferencia también puede compartir una línea E-1 con la transmisión de otro tipo de datos digitales como son transmisiones de Internet o transferencias de archivos.

La Videoconferencia normalmente es usada para conectar dos sitios remotos empleando sofisticada tecnología de computadoras.

3.- Equipo y material necesario

3.1 Material que debe traer el alumno

3.2 Equipo del Laboratorio

4.- Desarrollo

4.1.- El centro de docencia y la sala de videoconferencias

Esta práctica se realizar en el centro de docencia donde los alumnos podrán observar como se lleva acabo el sistema de videoconferencia. Analizando el equipo que se necesita, bajo que protocolos funciona.

4.2.- Estándares de Videoconferencia

La ITU trabaja en una serie de estándares para lograr la interoperabilidad de los programas para videoconferencia. Estos son:

- H.320 diseñado para enlaces ISDN, se ha ido adaptando para usarse en la tecnología WAN. El estándar recoge todos los subestandares tales como H.261 (vídeo), G.7XX (audio), H.320 (control) y T.120 (datos) y transmite 128 Kbps.

  Una versión de H.320 está diseñada para multipunto, la MCU permite 3 o más terminales para compartir información de audio y vídeo. Una simple red multipunto debe ser considerada como una conferencia punto a punto excepto porque 2 o más terminales están presentes.

- H.323 estándar que define videoconferencias basadas en LAN y permite una interoperabilidad entre los diferentes vendedores; también define videoconferencias usando líneas de viejos sistemas telefónicos.

  Estándar totalmente compatibles de aplicaciones de redes multimedia pueden expandirse a través de los múltiples "carriers backbone" (Redes privadas LAN/WAN e Internet) y viajar a través de muchos dispositivos hechos por diferentes vendedores, permite a estos seguir los mismos lineamientos para el desarrollo de equipos, software de red y software de aplicaciones para facilitar o eliminar los problemas de incompatibilidad encontrados hoy en día en las redes de múltiples vendedores incluyendo Internet.

  H.323, soporta diversos protocolos para una variedad de aplicaciones multimedia para una correcta transmisión de audio, vídeo y datos a través de múltiples ambientes de red.

- H.324 trabaja sobre líneas telefónicas regulares a velocidades de 28.8 Kbps ó 33.6 Kbps puede dar 5 ó 7 cuadros/se, la transmisión de imágenes es de muy baja calidad, simular a fotos una detrás de otra.

5.- Conclusiones

6.- Cuestionario Previo 8

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 9
Manejo de conflictos en el área de redes

1.- Objetivo de aprendizaje

El alumno definirá el concepto de conflicto, identificando las razones que lo provocan y la forma en que las personas lo manejan. De la misma manera reconocerá técnicas para la evasión y resolución de conflictos.

El alumno adquirirá la habilidad para aplicar estrategias de supervisión, que minimicen el conflicto y mejoren las relaciones humanas que favorecen el buen funcionamiento del área.

2.- Conceptos teóricos

En 1923 el investigador Charles E. Mayo, completó un estudio en el que se respalda la tesis, que sostiene que el trabajo individual no es el que genera los mejores frutos, pues el ser humano requiere de satisfacciones en la labor que desarrolla tanto individual como grupalmente.

En el mundo tecnológico en que nos desenvolvemos, las cosas deben ser administradas para obtener los objetivos propuestos.

El conflicto se inicia cuando individuos o grupos no obtienen lo que necesitan, buscando su interés propio. Los conflictos son inevitables, se desarrollan al entrar en contacto con personas, trabajos y el individuo mismo. Sin embargo deben minimizarse y resolverse a través de estrategias.

El conflicto se considera destructivo cuando, controla toda la atención, divide las personas y reduce la cooperación, aumenta las diferencias para finalmente conducir a un comportamiento destructivo.

El conflicto se puede considerar constructivo, cuando da lugar a la clarificación de problemas y controversias, generando soluciones basadas en una comunicación auténtica que permite desarrollar entendimiento y destrezas.

3.- Equipo y material necesario

4.- Desarrollo

1. Analice el siguiente caso real, dentro del área de administración de redes en una empresa proveedora de servicios de tecnología de información.

Eric Humbolt, administrador del área de redes, en una organización dedicada a proveer de servicios de telecomunicaciones, dedica su tiempo intentando que su equipo de trabajo sea capaz de desenvolverse en las reuniones de trabajo, sin que la tensión alcance límites insoportables, con el objetivo de contar con un equipo conjuntado, con una persona proveniente de cada división y desarrollar un plan integral, que tenga como meta, el realineamiento estratégico de la empresa, su puesta en marcha y buen funcionamiento, en un lapso de 6 meses.

Seis de los altos directivos involucrados, parecían estar decididos a dar un cambio drástico a la empresa, pero el séptimo daba la sensación de estar igualmente determinado a sabotear

el proceso. Ya habían tenido lugar 3 reuniones y Eric, no había conseguido que todos los participantes se pusieran de acuerdo en ninguno de los asuntos tratados.

Randy Louderback, administrador de bases de datos, regularmente dominaba la discusión del grupo o bien pasaba de todo y empezaba a tamborilear con su pluma sobre la mesa en señal de aburrimiento. Este individuo, que sometía al grupo con su personalidad y fuerte relación con el gerente general de la empresa, era capaz de retener información vital para el debate en el grupo y en otras ocasiones intervenía para denigrar fríamente las opiniones de cualquiera de los presentes. En la primera reunión realizada hacía un mes, insinuó lo que en ese momento pareció un chiste, que él no estaba hecho para trabajar en equipo con otros, a través del siguiente comentario:"Los líderes, dirigen; los gregarios…bueno mejor callémonos", mientras las pronunciaba esbozando una sonrisa plena de encanto y el resto del grupo había reído a carcajadas la gracia.

La empresa tenía problemas, no muy graves, pero sí lo bastante como para requerir por parte del área de dirección, un reposicionamiento estratégico.

Eric, preparó una estructura y directrices para los debates en grupo, las discrepancias y las tomas de decisiones, con la intención de proponérselas al grupo de directivos, para que realizarán su aportación antes de empezar a trabajar juntos. En un principio, previó ciertas discrepancias con algunos directivos, temores que resultaron infundados. A pesar de sus planificaciones, siempre hubo quien desbarato el proceso.

La tercera reunión, que había tenido lugar la semana anterior, se terminó en un caos completo. Se había decidido presentar una serie de propuestas por cada uno de los directivos, exposición que se desarrolló sin problemas hasta que tocó el turno a Randy, nuestro integrante conflictivo.

Finalmente en la cuarta reunión, todo el equipo estaba dentro de la sala, excepto Randy. Después de 10 minutos de conversaciones superficiales, Eric podía observar en cada una de las caras, la frustración reflejada en todos ellos, así que decidió que el tema de esa reunión sería la conducta de Randy para tratarlo abiertamente y tomar una decisión. Sin embargo, justo en el momento en que empezaba, éste entró pausadamente en la sala sonriendo y diciendo: "Lo siento, chicos", mientras sostenía una taza de café, como si ésta fuese la explicación suficiente para justificar su retraso. Eric, afirmó: "Randy, me alegro de que estés aquí, por que pienso que hoy debemos hablar del grupo". Randy interrumpió e hizo un comentario sarcástico, que provocó la salida de más de un integrante del equipo, la sala quedo en silencio.

2. Identifique la fuente del conflicto.

_____
_____
_____

3. Investigue las consecuencias en una organización, causadas por un conflicto como el anterior.

_____
_____
_____

4. Enumere al menos 5 actitudes de una persona conflictiva.

_____
_____
_____

Existen algunas técnicas para evadir o resolver conflictos, las cuales implican los siguientes pasos:

- Reconocimiento del conflicto.
- Establecimiento de metas.
- Establecimiento de comunicación frecuente.
- Comunicaciones de preocupaciones.
- Espíritu creativo.
- Discusión de las diferencias abiertamente.

Entre algunos puntos claves que deben considerarse a la hora de resolver conflictos encontramos:

- Se debe negociar antes de cerrar el trato.
- No debe ser intransigente: ser justo, ofrecer más respeto por la parte opositora que por lo que se está negociando.
- No negocie en estado de ira.
- Nunca piense que una negociación es insignificante.
- La técnica de la negociación debe llevar a un acuerdo inteligente, no a la confrontación.
- Una negociación efectiva no debe dejar resentimientos.
- Debe ser perdurable.
- En la negociación se debe privilegiar el bien común, dejando de lado el ego.

5. Investigue al menos 3 razones que den lugar a los conflictos.

_____
_____
_____

6. Investigue al menos 3 indicadores de la existencia de un conflicto.

_____
_____
_____

7. ¿Por qué no funciona este equipo de trabajo? Analice su respuesta y discuta en grupos de 3 personas, las coincidencias y diferencias.

_____
_____
_____

4.1 Capacidad para la resolución de conflicto

1. Indique la frecuencia con que emplea las siguientes tácticas para resolver conflictos, marcando con un círculo entorno al número que considere más adecuando.

		Rara Vez			**Siempre**	
		1	*2*	*3*	*4*	*5*
1	Negocia con sus compañeros para llegar aun compromiso.					
2	Trata de satisfacer las expectativas de sus compañeros.					
3	Trata de investigar un tema con sus compañeros para encontrar una solución aceptable para todos.					
4	Es firme cuando persigue su lado del tema.					
5	Trata de evitar que lo ubiquen en una posición difícil y trata de guardarse su conflicto ante sus compañeros.					
6	Define su solución del problema.					
7	Intercambia información exacta con sus compañeros para resolver juntos el problema.					
8	Evita analizar abiertamente sus diferencias con compañeros.					
9	Se adapta con facilidad a los deseos de sus compañeros.					
10	Trata de exponer todas sus preocupaciones que los problemas encuentren la mejor solución posible.					
11	Propone un terreno intermedio para romper los empates.					
12	Sigue las sugerencias de sus compañeros.					
13	Trata de callarse los desacuerdos con compañeros para evitar resentimientos.					
14	Argumenta su caso con compañeros de trabajo para demostrar los méritos de su posición.					

4.2 Casos prácticos de liderazgo

El objetivo de este punto es analizar los tipos de liderazgos empleados por 2 personajes de la industria informática.

1. Examine los siguientes casos reales de dos personajes que han dado lugar a dos fuertes empresas informáticas: Apple y Microsoft. Posteriormente responda las preguntas.

Dos hombres han dirigido la revolución de las computadoras personales. Sin embargo, la forma en que cada uno de estos hombres enfrento su propia búsqueda, ha sido distinta. Steve Jobs y Bill Gates, han cambiado la forma en la que el mundo hace negocios, pero la historia de sus liderazgos requiere ser estudiada.

Bill Gates

Bill Gates empezó a desarrollar sus habilidades, relativas a las computadoras, con su amigo de la infancia, Paul Allen, en Lakeside School, Seatle. A los 14 años, los dos constituyeron su primera compañía de computadoras. Al terminar la preparatoria Allen y Gates partieron hacia Boston.

Gates, fue aceptado en Harvard y Allen empezó a trabajar en Honeywell. Después de pasar solamente dos años en Harvard, Gates y Allen abandonaron Boston, para desarrollar, en Albuquerque, un lenguaje de computadora que sirviera a la nueva computadora personal

Altair 8080. Este lenguaje se convertiría en BASIC, cimiento de Microsoft, la cual fue creada como una sociedad en 1975.

Después de 5 años en Nuevo México, Microsoft fue trasladada a Bellevue, Washintong, en 1980, con BASIC y otros dos lenguajes de programación (COBOL y FORTRAN) en su arsenal. Posteriormente en ese mismo año, IBM empezó a desarrollar su primera PC y tuvo necesidad de un sistema operativo. Microsoft desarrolló el MS-DOS (Microsoft Disk Operating System) para IBM, mientras otras compañías creaban sistemas que competirían con Microsoft. La determinación y persuasión de Gates, en relación con el desarrollo de programas para MS-DOS, hizo de este sistema operativo la plataforma estándar de IBM.

Conforme Microsoft se volvió más exitoso Gates se dio cuenta de que necesitaba ayuda para su administración. Su entusiasmo, visión y trabajo arduo fueron la fuerza motriz detrás del crecimiento de la compañía, pero él reconoció la necesidad de una administración profesional. Gates introdujo a otro de sus amigos de Harvard, Steve Ballmer, quien había trabajado para Proter & Gamble, después de graduarse de Harvard y en ese entonces cursaba la maestría de Administración de Empresas en Standford. La persuasión de Gates, logró que Ballmer abandonara la escuela y se uniera a Microsoft. A lo largo de los años, Ballmer se ha convertido en un activo indispensable tanto para Gates, como para Microsoft.

En 1983, Gates siguió mostrando su inteligencia, al contratar a Jon Shriley, quien ordenó y modernizó la estructura de la organización, mientras Ballmer servía como consejero y portavoz de Gates. Microsoft continuó creciendo y prosperando en los 90, convirtiendo a Gates en el hombre más rico del mundo.

Microsoft domina tanto el mercado del sistema operativo, con su aplicación Windows, como el mercado del software de oficina, Microsoft Office.

Gates reconoció que su papel era ser el visionario la compañía y que necesitaba administradores profesionales, para dirigirla. Gates combinó su determinación y pasión inexorables con un equipo administrativo bien estructurado, para hacer de Microsoft el gigante que el día de hoy es.

Steve Jobs

El otro visionario, Steve Jobs y su amigo Steve Wosniak iniciaron en 1976 Apple Computer, en el garage de Jobs, en Los Altos, California. En contraste con Bill Gates, Jobs y Wosniak eran expertos en hardware e iniciaron una visión para una computadora personal que fuera económica y fácil de utilizar.

Cuando Microsoft ofreció BASIC a Apple, Jobs inmediatamente descartó la idea afirmando que él y Wosniak crearían su propia vesión de bASI en un fin de semana. Éste era el perfil típico de Jobs: firme y casi maniaco, en ocasiones.

Finalmente, Jobs aceptó BASIC de Microsoft, mientras trataba de consolidar su propia visión, es decir, el desarrollo de una interfaz más amigable y fácil de utilizar para una PC.

Muchos ven a Jobs como el anti-Gates. Jobs es un precursor y creador, en contraste con Gates, quien es más un individuo con el potencial de consolidar parámetros industriales.

El objetivo de Jobs, era cambiar al mundo con sus computadoras. Por otra parte era muy exigente con sus empleados. Jobs era distinto a Gates, Allen y Wosniak. No era un programador de computadoras dotado, si no la persona que vendía la idea de la

computadora personal al público. Jobs tomó la decisión de cambiar la dirección de Apple para desarrollar Macintosh, utilizando una GUI, Interfaz Gráfica de Usuario (Graphic Interface User), que introdujo al mundo el Mouse y los iconos en pantalla. Jobs forzó la gente a escoger entre el sistema operativo Microsoft-IBM Dos y su GUI Macintosh OS.

En un principio, Jobs fue el visionario que cambió el mundo de las computadoras y Apple empequeñeció a Microsoft. Con todo este éxito, había un problema mayor gestándose en Apple: Steve Jobs tenía una confianza excesiva y no vio que Gates y Microsoft constituían una seria amenaza para Apple.

Poco tiempo después de la aparición de la computadora Macintosh, Jobs pidió a Microsoft desarrollar un software para el sistema operativo Mac. Gates así lo hizo y procedió a lanzar un proyecto que copiara y mejorara la interfaz del usuario Apple. El resultado de esta empresa fue la aplicación Windows de Microsoft.

La actitud arrogante de Jobs, así como su carencia de habilidades administrativas, lo convirtió en una amenaza para el éxito de Apple. Nunca se preocupó por desarrollar presupuestos y se ha criticado su relación con los empleados. Wosniak abandonó Apple después de la aparición de Macintosh, debido a las diferencias con Jobs.

En 1985, John Scully, director general de Pepsi Cola sustituyó a Steve Job como presidente y director general de Apple Computer.

La década de los 90 vio a Microsoft y Apple tomar muy distintas direcciones. Microsoft se convirtió en una de las compañías más lucrativas del mundo. Jobs fundó NEXT, una empresa fabricante de computadoras y PIXAR, la empresa de animación que ha producido Toy Store y A Bug's Life.

Microsoft y Apple, al final del siglo

Apple tomó una dirección opuesta, el anticuado sistema operativo y la caída en la participación del mercado condujeron, a una disminución del desarrollo para el software en Mac. En 1998 Jobs regresó a Apple, como director general interino. Su visión, una vez más resulto en la innovador iMac. El diseño era clásico de Jobs. Ahora ha desarrollado una computadora simple, elegante y compatible con Internet, para agregar algo de emoción al mercado de las computadoras. Jobs también ha cambiado como administrador y líder. Ha madurado y solicita a su grupo de asesores profesionales consejos e ideas. Aunque es el director general interino, Jobs ha vendido todas menos una de sus acciones. Larry Ellison, director general de Oracle y miembro de la junta directiva de Apple, atribuye la Jobs, en cuanto a la dirección de Apple, al siguiente hecho:

> "Si bien posee sólo una acción de Apple, Jobs claramente es dueño del producto y la idea de la compañía. Mac es una expresión de su creatividad y Apple, como un todo, es una expresión de Steve. Ésta es la razón por la que a pesar de la palabra interino, en su título, permanecerá en Apple durante largo tiempo."

Con el éxito del sistema operativo Windows, la seria de aplicaciones Office y el software Internet Explorer, Microsoft se ha convertido en una palabra familiar. Bill Gates ha sido aclamado como genio de los negocios. El hecho de que los competidores de Microsoft, la prensa y el Departamento de Justicia de Estados Unidos hayan llamado a Microsoft un monopolio, refuerza la determinación de éxito en Gates.

Finalmente, muchas personas creen que esto conducirá a una batalla renovada entre Gates y Jobs.

2. ¿Cómo difieren Bill Gates y Steve Jobs en su estilo de liderazgo?

_____
_____
_____

3. Compare y contraste las prácticas administrativas de Gates y Jobs.

_____
_____
_____

4. ¿Cuál es su opinión sobre el futuro de Microsoft y Apple Computers?

_____
_____
_____

5. Para usted, ¿cuál es la esencia del liderazgo?

_____
_____
_____

6. Si usted fuera elegido para ser líder de grupo en un proyecto de clase, ¿qué conducta adoptaría con aquéllos elementos conflictos del grupo? ¿por qué?

_____
_____
_____

7. Haga una interpretación del siguiente párrafo y dé un ejemplo práctico de su aplicación:

"En una organización no se puede gobernar a los hombres, sino dirigir hacia unos objetivos a hombres que se gobiernan a sí mismos."

Sthephan Cambien

_____
_____
_____

5.- Conclusiones

6.- Cuestionario previo 9

1. Investigue el concepto de liderazgo.
2. Investigue al menos 3 características importantes de un jefe.
3. Investigue al menos 5 tipos de conflictos en el ámbito laboral
4. Investigue una clasificación de los jefes.

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 10 Parte A
Mecanismos de Seguridad, Firma Digital

1.- Objetivo de aprendizaje

El alumno se familiarizará con herramientas básicas relacionadas con la seguridad en la red, las cuales podrán ser estudiadas a profundidad en subsecuentes materias.

El alumno será capaz de realizar una aplicación que permita el proceso de firmado de un documento a través de la infraestructura de llaves asimétricas, en el lenguaje orientado a objetos, Java.

2.- Conceptos teóricos

En diversas organizaciones, tanto públicas como comerciales, Internet se ha convertido en un foro principal para hacer negocios, sirviendo como medio principal para la publicidad, el marketing, las ventas y la atención al cliente. Ha permitido que las empresas crezcan y a las grandes corporaciones, expandir su dominio.

Junto a las oportunidades que ofrece Internet se encuentran los riesgos importantes. Los servidores Web pueden ser sustituidos y a veces, las páginas Web han sido desconfiguradas. Los datos privados de los consumidores podrían ser revelados. Las transacciones financieras pueden ser falsificadas. Los cortafuegos de las empresas pueden ser infringidos y las redes de la empresa saboteadas. Todos estos escenarios, con llevan a un uso seguro de Internet.

La comunicación segura dentro de una red, debe cumplir con las siguientes características: confidencialidad, autenticación, integridad del mensaje, disponibilidad y control de acceso. Las 3 primeras características se han considerado componentes claves de una red segura, sin embargo se han añado en las últimas décadas, la necesidad de mantener la red operando.

El concepto de firma digital fue introducido por Diffie y Hellman en 1976, siendo un bloque de caracteres que acompaña a un documento acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad).

El proceso de firmado digital se inicia cuando el autor de un documento utiliza su clave secreta dentro del esquema de cifrado asimétrico, a la que sólo él tiene acceso, esto impide que pueda negar su autoría (revocación o no repudio). De esta forma el autor es vinculado al documento de la firma. El software del autor, aplica un algoritmo hash sobre el texto a firmar, obteniendo un extracto de longitud fija y absolutamente especifico del mensaje. Un cambio mínimo en el mensaje, dará lugar a una cadena hash distinta. El extracto tiene una longitud de 128 a 160 bits, dependiendo del algoritmo utilizado, entre los que se encuentran: MD5 o SHA-1. El algoritmo más utilizado en el proceso de encriptación asimétrica, es el RSA.

La validez de la firma es probada por cualquier persona que disponga de la clave pública del autor.

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- JSDK 1.5, instalado en las computadoras del Laboratorio.

4.- Desarrollo

La aplicación Java a realizar, se compone de dos programas, el primero hará el firmado del documento y el segundo verificará la firma de dicho documento. El programa que realiza el primer procedimiento debe cumplir con los siguientes requerimientos:

- Solicitar mediante la entrada estándar, el nombre del archivo que contiene la información a firmar (Archivo A).
- La salida del programa que firma el documento, deben ser dos archivos, el primero contendrá la llave pública generada y el segundo la firma del documento (Archivo B, Archivo C).
- El programa que recibe el Archivo A, debe generar internamente el par de claves.

El programa que realiza el segundo procedimiento debe cumplir con los siguientes requerimientos:

- Solicitar mediante la entrada estándar, el nombre del archivo que contiene la clave pública generada en el primer punto, además del nombre del archivo que contiene la información firmada (Archivo B, Archivo C).
- Indicar mediante una cadena si la firma es correcta.

4.1 Firma Digital

Nota Profesor: La realización de esta práctica requiere de conocimientos básicos de programación orientada a objetos.

Una firma digital, es un bloque de caracteres que se anexa a un documento con el fin de acreditar quién es su autor, se basa en la criptografía de clave pública, donde quién firma el mensaje lo cifra con su clave privada de forma que puede ser descifrado por todo aquel que posea la clave pública, correspondiente a la clave privada empleada para firmar el mensaje.

Nota: La firma digital no hace cifrado de mensajes, únicamente garantiza el origen.

Investigue el objetivo de la firma digital.

_____
_____
_____

El cifrado de un mensaje con la clave privada consume un tiempo elevado de proceso, por lo que resulta imprescindible contar con un texto más corto que el mensaje original, éste es obtenido mediante una función hash y comúnmente denominado huella digital o fingerprint. Si el mensaje original se altera, también varía la huella digital y lo que se cifra con la clave privada no es el mensaje original, si no la huella digital, el resultado se añade al documento a transmitir.

Investigue los 2 algoritmos hash, más utilizados en la actualidad.

_____
_____
_____

4.1.1 Criptografía

4.1.1.1 Criptografía de clave privada

La criptografía tradicional también denominada de clave secreta, se basa en que tanto emisor como receptor, cuentan con una misma clave, que es empleada por el primero para cifrar el mensaje, dando lugar a un mensaje ilegible, el segundo utiliza la misma clave de cifrado para descifrar y obtener el mensaje original.

Investigue la principal desventaja de la criptografía tradicional.

_____
_____
_____

4.1.1.2 Criptografía de clave pública

En este tipo de cifrado, el emisor y receptor cuentan con claves distintas. La clave pública es aquella que todo el mundo conoce, y que puede ser empleada por cualquiera para cifrar mensajes. La clave privada es aquella que únicamente conoce quien envía el mensaje y es capaz de descifrar los mensajes generados por la clave pública.

Investigue el algoritmo de cifrado más comúnmente utilizado por este tipo de cifrado.

_____
_____
_____

Una de las principales ventajas de la criptografía asimétrica es la simplificación de la administración de claves al permitir que varias personas utilicen un par de claves, únicamente existe un problema: ¿cómo distribuir una clave pública de forma que el usuario pueda encontrarla y saber que es válida?

4.1.2 Firma de un documento

El programa que genera las claves para firmar un documento, hará uso del API de Seguridad del JSDK 1.5.

1. Verifique la existencia de la herramienta JSDK 1.5 en el equipo asignado, accediendo en la línea de comando mediante el menú Inicio>Ejecutar>command.
2. Ejecute el comando java –version, en la línea de comando y observe el resultado, ver Figura 10.1.

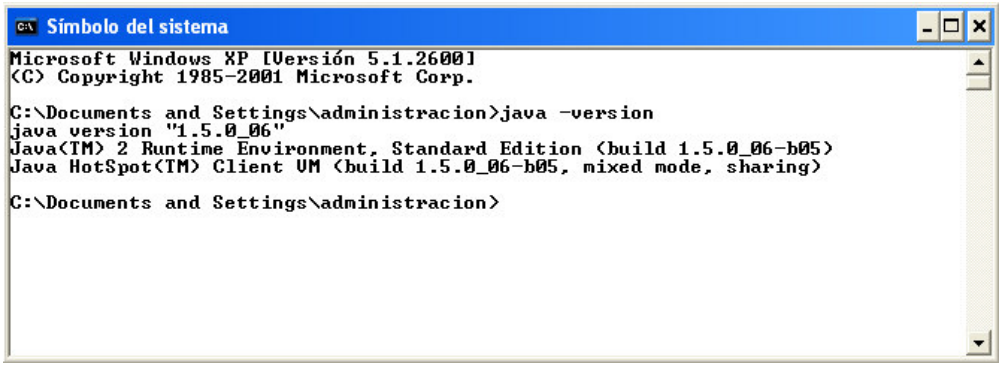


Figura 10.1 Version de java disponible

3. Cree una carpeta en C:\ con el nombre de Practica10a_INICIALES, de manera que sea donde almacene los archivos generados.
4. Abra la aplicación bloc de notas, a través de menú Inicio>Todos los programas>Accesorios>Bloc de notas. Teclee el siguiente código, el cual es la estructura inicial del programa, ver Figura 10.2. Guarde el archivo con el nombre de GeneraFirmaINICIALES.java.

```
import java.io.*;
import java.security.*;

class GeneraFirmaINICALES
{
    public static void main (String [] args)
    {
            /*Verificando el numero de argumentos de entrada*/
            if (args.length!=1)
            {
             System.out.println ("Sintaxis del programa es: java GeneraFirmaINICIALES archivoaFirmar");
            }
            else    try
                    {
                            /*En este bloque se debe colocar el código faltante*/
                    }
            catch (Exception e)
                    {
                    System.out.println("El error es " + e) ;
                    }
    }
}
```

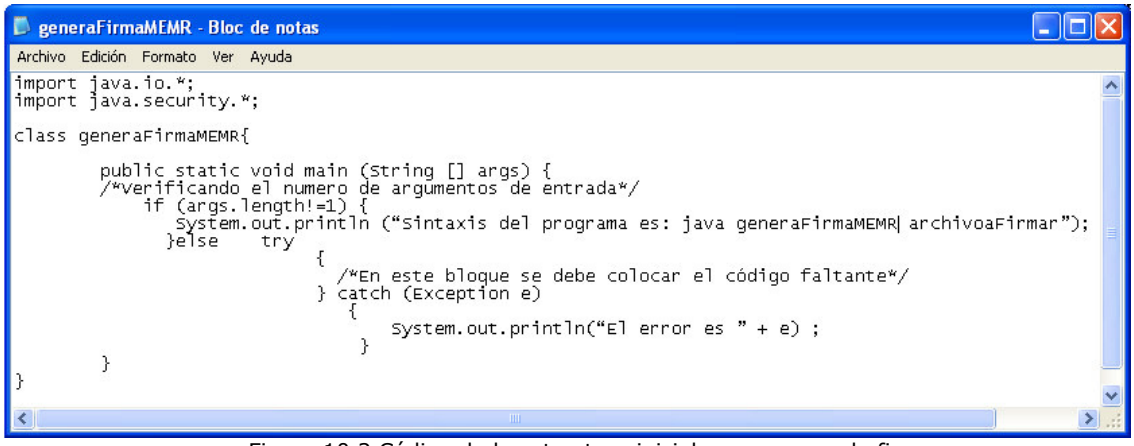


Figura 10.2 Código de la estructura inicial para generar la firma

El programa importa el paquete java.security.*; ya que ahí se encuentran las clases necesarias para generar las claves y firmar un documento. De la misma manera se importa el paquete java.io.*; por que en ese paquete se encuentran las clases necesarias para manipular los archivos de entrada.

Investigue el uso de las sentencias try y catch dentro del lenguaje java.

_____
_____
_____

Nota: Inserte las siguientes líneas del código en el programa debajo de la línea /*En este bloque se debe colocar el código faltante*/

5. Para generar una firma digital, se requiere una clave privada que inicie el proceso. La clase KeyPairGenerator permite esa funcionalidad mediante el siguiente código:

   KeyPairGenerator genClave=KeyPairGenerator.getInstance("RSA");

6. Inicie el objeto genClave através del método initialize, el cual tiene dos argumentos:

   a. Tamaño de clave, el cual es de 1024 bits.

   b. La fuente aleatoria, en el caso de la práctica haremos uso de la clase Secure Random.

SecureRandom aleatorio=SecureRandom.getInstance("SHA1PRNG","SUN");
genClave.initialize(1024, aleatorio);

El objeto SecureRandom, pretende aleatorizar el estado interno del propio generador utilizando el algoritmo de generación de números pseudoaleatorios llamado SHA1PRNG.

7. El siguiente paso es la generación del par de claves para almacenarlas en objetos del tipo PrivateKey y PublicKey, mediante el siguiente código:

KeyPair pardeClaves= genClave.generateKeyPair();
PrivateKey privada=pardeClaves.getPrivate();
PublicKey publica=pardeClaves.getPublic();

Investigue el funcionamiento del método ***getPrivate y getPublic***.

_____
_____
_____

Nota: Guarde los cambios efectuados en el código

8. El paso final de esta primera aplicación es el firmado de los datos, ya que se han creado la llave pública y privada. Cree un archivo de nombre datosaFirmar.txt con una nueva ventana de la aplicación de bloc de notas y guarde el archivo en la carpeta creada, con el siguiente contenido:

"Pensar en seguridad se vuelve necesario una vez que permitimos que nuestros recursos computacionales entren en contacto con el resto del mundo. Un puerto de comunicación abierto casi siempre está expuesto a ataques externos o a abusos; es necesario tomar medidas de seguridad para evitar el mal uso de los recursos. "

Nota: Guarde los cambios efectuados en el código.

9. Una firma digital se crea o bien se verifica usando una instancia de la clase Signature, mediante el siguiente código:

Signature firma=Signature.getInstance ("MD5withRSA");

10. Antes de que el objeto Signatura sea usado para firmar o verificar datos, requiere ser inicializado, el cual requiere de la clave privada.

firma.initSign(privada);

11. Antes de firmar, es necesario suministrar al objeto "firma" los datos a firmar, los cuales se almacenan dentro de un archivo. Las siguientes líneas abren el archivo, su contenido lo guardan en un buffer y posteriormente se lo hacen llegar al objeto "firma".

```
FileInputStream archivo=new FileInputStream(args[0]);
BufferedInputStream buferEntrada=new BufferedInputStream(archivo);
byte[] buffer=new byte[1024];
int longitud;

while (buferEntrada.available() !=0)
      {
       longitud =buferEntrada.read(buffer);
       firma.update(buffer, 0, longitud);
      }
buferEntrada.close();
```

12. Finalmente, una vez que se han suministrado los datos al objeto "firma", se genera la firma digital de los datos.

byte[] firmaReal=firma.sign();

13. Generada la firma es necesario enviarla a un archivo de la misma manera que la clave pública, para el proceso de verificado de firma digital.

```
                    /*Guardando los datos firmados en un archivo*/
FileOutputStream archivoFirma=new FileOutputStream("firmaINICIALES.txt");
archivoFirma.write(firmaReal);
archivoFirma.close();

                    /*Guardando la llave pública en un archivo*/
byte[] llave=publica.getEncoded();
FileOutputStream clavePublica=new
FileOutputStrem("llavePublicaINICIALES.txt");
clavePublica.write(llave);
clavePublica.close();
```

El método getEncoded obtiene los bytes codificados de la clave pública y luego se envían a un archivo.

Nota: Guarde los cambios efectuados en el código.

14. Debe ubicarse en el directorio C:\Practica10Ainiciales, para compilar el programa mediante la instrucción ***javac GeneraFirmaINICALES.java***, en la línea de comando de MS-DOS y observe el resultado.
15. Ejecute el programa, con la instrucción ***java GeneraFirmaINICALES datosaFirmar.txt*** y observe en su directorio de trabajo, la creación de los archivos esperados.

4.1.3 Verificación de la firma de un documento

La verificación de la firma de un documento, implica que quien recibe el mensaje, en primer lugar aplica la función hash a el documento recibido, descifra la huella digital cifrada y compara ésta con la obtenido al procesar el documento, si son iguales el documento no ha sido alterado y efectivamente ha sido enviado por quien firma.

En la Figura 10.3, describa el funcionamiento del proceso de firma digital, si la llave privada del usuario es P14%$369.? , la llave pública del usuario es P89/*.%*-:), el texto en claro es "keytool da soporte a los certificados en java", la huella digital cifrada es "03heabcdrere5HEabc".

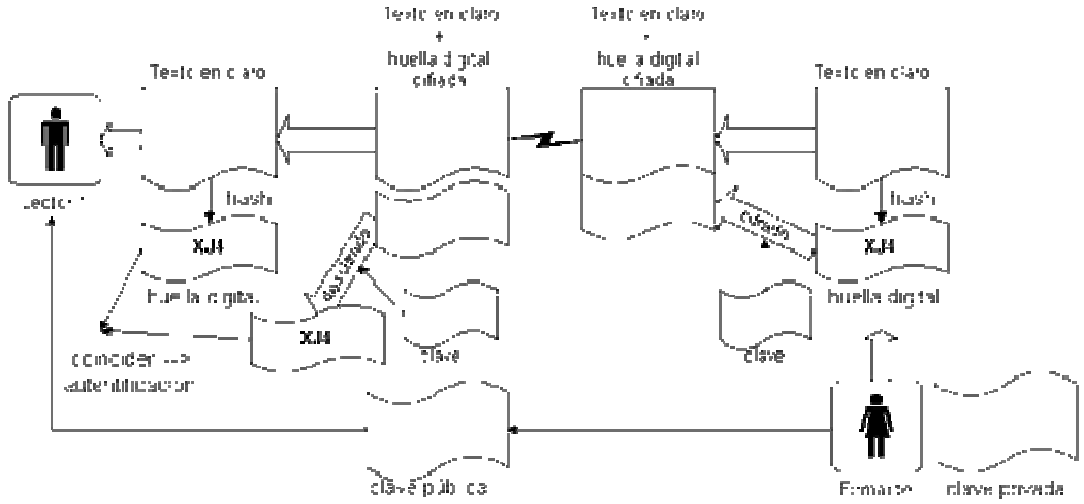


Figura 10.3 Proceso de la firma digital de un documento

De acuerdo al diagrama anterior, indique los argumentos que debe recibir el programa que verifica la firma digital de un documento.

_____
_____
_____

1. Abra la aplicación bloc de notas, a través de menú Inicio>Todos los programas>Accesorios>Bloc de notas. Teclee el siguiente código, el cual es la estructura inicial del programa. Guarde el archivo con el nombre de VerificaFirmaINICIALES.java.

Nota: No olvide guardar el archivo VerificaFirmaINICIALES.java en la misma carpeta C:\Practica10INICIALES.

```
import java.io.*;
import java.security.*;
import java.security.spec.*;

class VerificaFirmaINICIALES
{
    public static void main (String [] args)
    {
            /*Verificando el numero de argumentos de entrada*/
    if (args.length!=3)
            {
                    System.out.println
                     ("Sintaxis del programa es: java VerificaFirmaINICIALES
archivoaFirmarINICIALES.TXT llavepublicaINICIALES.TXT firmaArchivo");
            }
        else    try
            {
                    /*En este bloque se debe colocar el código faltante*/
            }
        catch (Exception e)
            {
                    System.err.println ("El erros es de "+ e.toString() );
```

```
            }
        }
    }
```

El programa importa el paquete java.security.spec, ya que éste contiene la clase X509EncodedKeySpec.

Nota: Inserte las siguientes líneas del código en el programa debajo de la línea /*En este bloque se debe colocar el código faltante*/

2. El primer paso consiste en importar los bytes codificados de la clave pública del archivo que lo contiene y convertirlos en un objeto del tipo PublicKey, mediante el siguiente código:

   FileInputStream llavepublica=new FileInputStream (args[0]);
   byte[] llave=new byte[llavepublica.available()];
   llavepublica.read(llave);
   llavepublica.close();

El arreglo de bytes llave, contiene los bytes codificados de la clave pública.

3. El siguiente paso consiste en obtener el valor de la llave pública, para lo cual hacemos uso de una clase KeyFactory, que proporciona conversión entre claves opacas (del tipo Key) y especificaciones de claves, que son representaciones transparentes del material de la clave. Primero es necesario una especificación de clave, mediante el estándar X.509, con el siguiente código:

   X509EncodedKeySpec pubKeySpec=new X509EncodedKeySpec(llave);

Investigue el contenido básico del estándar X.509.

_____
_____
_____

4. Se requiere de un objeto KeyFactory para realizar la conversión, éste debe trabajar con claves RSA.

   KeyFactory keyFactory = KeyFactory. getInstance("RSA");

5. Empleando el objeto keyFactory se genera un objeto PublicKey de la siguiente manera:

   PublicKey pubKey=keyFactory.generatePublic(pubKeySpec);

6. El siguiente paso consiste en intruducir los bytes firmados desde el archivo, especificado en el segundo argumento de la línea de comandos:

   FileInputStream archivoFirmado=new FileInputStream(args[1]);
   byte[] firmaVerificada=new byte[archivoFirmado.available()];
   archivoFirmado.read(firmaVerificada);
   archivoFirmado.close();

Hasta este punto el arreglo de bytes firmaVerificada contiene los bytes de la firma de documento.

7. Una firma se verifica usando una instancia de la clase Signature, definiendo los algoritmos utilizados en el proceso de la firma del documento:

   Signature firma=Signature.getInstance ("MD5withRSA");

8. Inicialice el objeto Signature con el método verificar, que recibe como argumentos la llave pública:

   firma.initVerify(pubKey);

9. Suministre al objeto firma los datos para los cuales se generó la firma, éstos se encuentran en el archivo original.

```
FileInputStream datos=new FileInputStream(args[2]);
BufferedInputStream buferEntrada=new BufferedInputStream(datos);
byte[] buffer=new byte[1024];
int longitud;

while (buferEntrada.available() !=0)
        {
         longitud= buferEntrada.read(buffer);
        firma.update(buffer,0,longitud);
        }
buferEntrada.close();
```

10. El proceso de verificación de la firma, permite reportar el resultado.

```
boolean verifica=firma.verify(firmaVerificada);

System.out.println ("Verificación de la firma  " +verifica);
```

Nota: Guarde los cambios efectuados en el código.

11. Compile el programa mediante la instrucción ***javac VerificaFirmaINICALES.java***, en la línea de comando de MS-DOS y observe el resultado.
12. Ejecute el programa, con la instrucción ***java VerificaFirmaINICALES llavepublicaINICIALES.txt firmaINICIALES.txt datosaFirmar.txt*** y observe el resultado.
13. Modifique el archivo llavePublica.txt en el bloc de notas, ejecute nuevamente el programa con la instrucción ***java VerificaFirmaINICALES llavepublicaINICIALES.txt firmaINICIALES.txt datosaFirmar.txt*** y observe el resultado.

Investigue el error obtenido en el punto anterior.

_____
_____
_____

Nota: Ejecute nuevamente la instrucción ***java GeneraFirmaINICALES datosaFirmar.txt***, para restablecer la llave publica

14. Modifique el archivo datosaFirmar.txt en el bloc de notas, ejecute nuevamente el programa con la instrucción java VerificaFirmaINICALES llavePublica firma datosaFirmar.txt y observe el resultado.

Defina el escenario que representa el punto anterior.

_____
_____
_____

5.-Conclusiones

6.-Cuestionario Previo 10a

1. Investigue el significado de las siglas MAC
2. Investigue en qué consisten las funciones hash y mencione al menos 3 ejemplos.
3. Investigue en qué consisten los algoritmos de clave pública
4. Mencione al menos 3 algoritmos de cifrado simétrico o de criptografía tradicional.

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 10 Parte B
Mecanismos de Seguridad, Certificados Digitales

1.- Objetivo de aprendizaje

El alumno identificará los diversos tipos de certificados, así como su importancia dentro de los esquemas de seguridad en las redes.

El alumno se familiarizará con una herramienta de software libre que permite la administración de certificados digitales, OpenSSL.

2.- Conceptos teóricos

El panorama de las telecomunicaciones de datos se ha visto afectado por un gran cambio en los últimos años del siglo XXI. Las innovaciones y cambios tecnológicos suceden con gran velocidad a medida que se perfeccionan y se depuran las ideas y técnicas que han permitido la unión entre la informática, la electrónica y las comunicaciones.

En las transacciones comunes los retos de identificación, autentificación y privacidad son resueltos con marcas físicas, tales como las firmas digitales. En las transacciones electrónicas, el equivalente a un sello tiene que ser codificado en información. El verificar que el sello se encuentra presente y no ha sido alterado, es la forma en la que, el que recibe la información puede confirmar la identidad del que lo envió y de esta manera se asegura que el mensaje no ha sido alterado ni modificado en el camino. Para crear un equivalente electrónico a la seguridad física, se usa la llamada criptografía.

Un certificado digital es un documento electrónico, mediante el cual un tercero confiable (una autoridad de certificación) garantiza la relación entre la identidad de un sujeto o entidad y su clave pública.

Existen varios formatos de certificado digital, los más comúnmente empleados se rigen por el estándar UIT-T X.509v3. El certificado contiene usualmente el nombre de la entidad certificada, un número serial, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- PC con sistema operativo Linux, Fedora Core2.

4.- Desarrollo

4.1. Certificado digital

Un certificado permite obtener la clave pública de otra entidad ya sea una persona o institución. Se considera como una declaración firmada digitalmente por una entidad indicando que la clave pública de otra persona tiene un valor específico.

Existen diferentes clases de certificados de acuerdo a su utilidad:

a. Certificados de Servidor, aportan a un sitio Web la característica de seguridad para poder intercambiar información como: números de cuenta, contraseñas, etc.
b. Certificados para WAP, permiten a los sitios Web la realización de transacciones seguras con sus usuarios móviles. Los certificados WAP permiten mantener conexiones seguras basadas en encriptación y autenticación con dispositivos de telefonía móvil.
c. Certificados personales, otorgan seguridad a los correos móviles basados en el estándar S/MIME, asegurando que el receptor designado sea el lector del mensaje.
d. Certificados para firmar código, permiten a los administradores o desarrolladores de software, firmar su código para la distribución segura entre sus clientes.
e. Certificados para IPSec-VPN, son los elementos necesarios para que la empresa aproveche las cualidades y ventajas del uso de las VPN, Redes Virtuales Privadas (Virtual Network Private).

4.1.1 Instalación de OpenSSL

OpenSSL, es una herramienta de software libre desarrollado por los miembros de la comunidad OpenSource, que permite la creación y administración de certificados digitales, además de contar con librerías relacionadas con la criptografía, útiles para proporcionar funciones criptográficas, como OpenSSH y navegadores Web (https). Este paquete es importante para cualquiera que esté planeando implementar un cierto nivel de seguridad en una máquina Linux.

Nota Profesor: Los equipos deben estar encendidos previamente sin iniciar sesión en Fedora.

1. Inicie sesión dentro del sistema operativo, ingresando la cuenta de redes con su correspondiente contraseña.
2. Abra una terminal de shell para instalar la herramienta.
3. Cree una carpeta llamada openssl, bajo el directorio /opt/.
4. Cambie de directorio a /opt/openssl, mediante el comando cd /opt/openssl.
5. Copie el archivo **openssl-0.9.x.tar.gz** ubicado en el directorio /home/redes/. de la máquina 192.168.2.3, mediante el comando scp al directorio actual.

[redes@localhost openssl]#scp estudiante@192.168.2.3:/home/redes/openssl-0.9.x.tar.gz .

6. Ejecute los siguientes comandos.

[redes@localhost openssl]#tar xvzf openssl-0.9.x.tar.gz

[redes@localhost openssl]#cd openssl-0.9.x

[redes@localhost openssl]# ./config

Donde x, corresponde a la versión más reciente descargada de la página Web http://www.openssl.org.

Nota: El script ./config permite la configuración de la herramienta, verificando la existencia de las dependencias existentes en el sistema.

7. Si el sistema no marca ningún error, ejecute la siguiente instrucción:

[redes@localhost openssl]# make

Nota: Make, es una herramienta de generación o automatización de código usada en sistemas operativos del tipo Linux/Unix, por defecto lee las instrucciones para generar el programa o para su instalación.

8. Nuevamente si no existe ningún error ejecute el siguiente comando:

[redes@localhost openssl]# make test

Nota: Make test, es un script que permite verificar que la aplicación fue bien compilada.

9. Cambie de usuario a root e instale el software a través del siguiente comando:

[redes@localhost openssl]# su -

[root@localhost openssl]#password:

[root@localhost openssl]# make install

Nota: Make install, es un script que instala la aplicación en los directorios destino.

El archivo de configuración de OpenSSL está en /usr/local/ssl/openssl.cnf, para el desarrollo de esta practica se empleará la configuración por default.

10. Verifique la instalación del programa mediante el comando ***whereis.***

[root@localhost openSSLiniciales]# whereis openssl

Investigue que información proporciona el comando anterior y anote su salida.

_____
_____
_____

Investigue la ruta del archivo de configuración openssl.cnf

_____
_____
_____

Nota: El directorio de instalación por default es /usr/local/ssl, donde se encuentran los binarios base del programa en la carpeta bin/ además de diferentes scripts para manejar una autoridad certificadora en misc/.

4.1.2 Comandos básicos en OpenSSL

El objetivo de este punto es conocer los comandos básicos de OpenSSL, para construir una infraestructura de clave pública.

1. Abra una terminal de shell, cree una carpeta con el nombre de OpenSSL_iniciales, el directorio home del usuario redes.

[root@localhost openSSLiniciales]#mkdir /home/redes/OpenSSLiniciales

2. Cambie de directorio a /home/redes/OpenSSLiniciales, el cual será el directorio de trabajo.

[root@localhost openSSLiniciales]#cd /home/redes/OpenSSLiniciales

3. Ejecute los siguientes comandos:

[root@localhost openSSLiniciales]#openssl version

Anote la versión instalada en el equipo asignado.

_____
_____
_____

4. Aplique las siguientes funciones hash al archivo de configuración de openssl y anote el resultado en las siguientes líneas.

[root@localhost openSSLiniciales]#openssl md5 /usr/share/ssl/openssl.cnf

Anote el resultado de la función md5 del archivo /usr/share/ssl/openssl.cnf

_____
_____
_____

[root@localhost openSSLiniciales]#openssl sha1 /usr/share/ssl/openssl.cnf

Anote el resultado de la función sha1 del archivo /usr/share/ssl/openssl.cnf

_____
_____
_____

[root@localhost openSSLiniciales]#openssl sha1 –out hash.txt /usr/share/ssl/openssl.cnf

Investigue la diferencia que existe entre el comando ejecutado y el anterior.

_____
_____
_____

OpenSSL cuenta con librerías que permiten el cifrado de archivos, con diferentes algoritmos.

5. Cree un archivo con nombre entrada.txt y teclee algunos datos para que posteriormente aplique los siguientes comandos:

[root@localhost openSSLiniciales]#openssl enc –des3 –salt –in entrada.txt –out cifra_a.bin –pass pass:iniciales

Investigue el funcionamiento del comando anterior.

_____
_____
_____

[root@localhost openSSLiniciales]#openssl enc –des-ede3-cbc –d –in cifra_a.bin –out descrifradoa3des.txt

Investigue el funcionamiento del comando anterior.

_____
_____
_____

4.1.3 Creación de una AC, Autoridad Certificadora

Una AC, Autoridad Certificadora (Certification Authority) es una organización confiable que recibe solicitudes de certificados de entidades, las valida, genera certificados y mantiene la información de su estado.

Entre las principales tareas de una AC, encontramos:

a. Admisión de certificados.
b. Autenticación del sujeto.
c. Generación de certificados.
d. Distribución de certificados.
e. Anulación de certificados.
f. Almacenes de datos.

Los certificados digitales proporcionan un mecanismo criptográfico para implementar la autenticación, siendo seguro y escalable para distribuir claves públicas en comunidades grandes.

Investigue que es una CPS, Declaración de Prácticas de Certificación (Certification Practice Statement) dentro de una AC.

_____
_____
_____

Investigue el procedimiento para obtener un certificado digital.

_____
_____
_____

Para crear un certificado digital en primera instancia se debe realizar una solicitud de certificado a una AC, que respalde la información del certificado solicitado. Algunas AC reconocidas son VerigSign, Visa, etc., éstas previo pago devuelven certificados firmados por

ellas. Para sustituir a dichas AC se creará una propia, para firmar los certificados que se generen.

1. Estando, en el directorio de trabajo teclee el siguiente comando, ver Figura 11.1.

[root@localhost openSSLiniciales]#openssl req −x509 −newkey rsa:2048 −keyout cakey.pem −days 3650 −out cacert.pem

```
[root@localhost OpenSSLmokc]# openssl req -x509 -newkey rsa:2048 -keyout cakey.pem -days 3650 -out cacert.pem
Generating a 2048 bit RSA private key
...+++
.............................................+++
writing new private key to 'cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:LabRedes
Organization Name (eg, company) [My Company Ltd]:UNAM
Organizational Unit Name (eg, section) []:FI
Common Name (eg, your name or your server's hostname) []:karen medina
Email Address []:kacrism@gmail.com
You have new mail in /var/spool/mail/root
[root@localhost OpenSSLmokc]# ls
cacert.pem  cakey.pem
[root@localhost OpenSSLmokc]#
```

Figura 11.1Creación de la Autoridad Certificadora

El comando anterior crea una AC para certificados X509 con algoritmo de encriptación RSA de 2048bytes. La opción –keyout permite que la clave privada de la AC se almacene en el archivo cakey.pem y la clave pública –out en el cacert.pem.

Investigue la función del parámetro –days.

_____
_____
_____

El formato de certificados X.509, es un estándar del ITU-T, (Internacional Telecommunication Union-Telecommunication Standarization Sector) y el ISO/IEC (Internacional Standards Organization-International Electrotechnical Commission), publicado en 1988.

Investigue los elementos del formato de un certificado X.509 v3.

_____
_____
_____

2. Seguidamente se solicita una frase password para la AC, introduzca la palabra: **.r3d3s.** y confirme la frase.
3. En el país introduzca el código identificador MX.
4. El siguiente campo solicita el estado o provincia, introduzca Distrito Federal.

5. En el nombre de la localización que solicita introduzca LabRedes.
6. En el nombre de la organización, introduzca UNAM.
7. En la unidad organizacional introduzca FI.
8. En el campo del nombre común, introduzca su primer nombre y apellido.
9. Finalmente proporcione su correo electrónico.

Hasta este punto se ha creado la AC, que validará los certificados que se generen durante la práctica.

10. Verifique que los archivos que contienen el certificado de la AC y su clave se han creado, en el directorio actual, a través de los siguientes comandos:

[root@localhost openSSLiniciales]$ cat cakey.pem

[root@localhost openSSLiniciales]$ cat cacert.pem

Investigue en qué consiste el formato .pem.

_____
_____
_____

4.1.4 Petición y generación de certificados

Es posible obtener un certificado digital a través de dos formas:

a. Petición on-line, en este tipo regularmente se solicitan certificados personales, para lo cual se requiere de llenar un formulario, enviar alguna documentación y esperar el certificado firmado por la AC.
b. Petición postal, resulta óptimo para la obtención de certificados de servidor, siendo una combinación ya que el CSR, Solicitud de Firma de Certificado (Certificate Sign Request) se envía por correo y la documentación se hace llegar por correo.

Un CSR es un archivo que incluye la información necesaria para solicitar un certificado digital.

El objetivo de este punto es generar un CSR, después de crear la AC en el punto anterior.

1. El primer paso para la generación de un certificado digital, es la creación de la clave privada del mismo. Teclee el siguiente comando, que crea una clave privada con un algoritmo de cifrado RSA de 2048 y se almacena en el archivo priv.pem, con la opción –passout pass: en la cual le indicará la frase privada para la clave privada, ver Figura 11.2.

[root@localhost openSSLiniciales]$ openssl genrsa –des3 –out priv.pem –passout pass:iniciales 2048

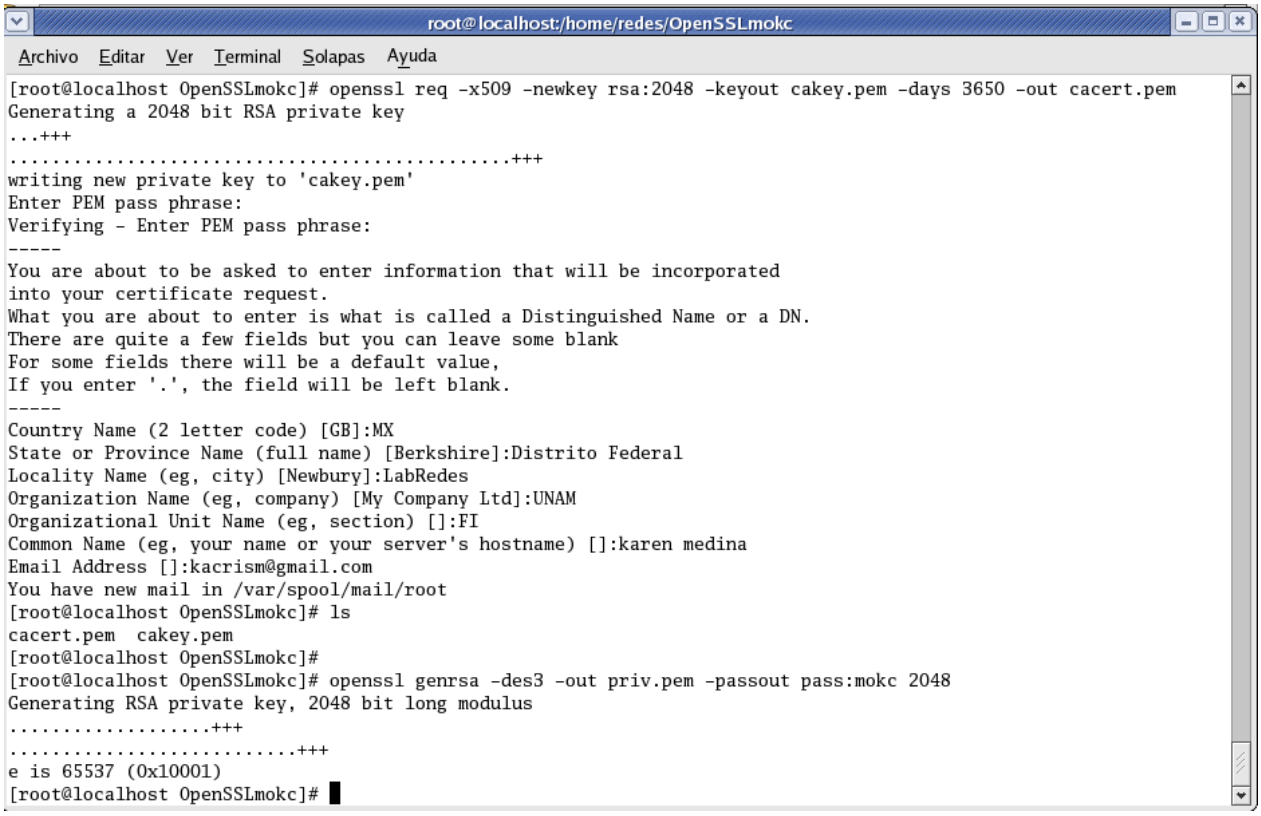


Figura 11.2 Creación de la clave privada del certificado

Investigue la sintaxis del comando ***openssl genrsa.***

_____
_____
_____

2. Verifique que el archivo priv.pem se haya creado en su home e identifique en su contenido los encabezados.

[root@localhost openSSLiniciales]$ cat priv.pem

3. El segundo paso es realizar una CSR, donde se define el propietario del mismo. El siguiente comando hace una petición con el parámetro subj en donde especificamos a quien pertenece el certificado dentro de las comillas separadas por la /. Así mismo, se indica la clave privada que será utilizada con el certificado además de la frase password.

[root@localhost openSSLiniciales]$ openssl req –new –subj "/DC=fi-b.unam.mx/OU=LabRedes/CN=fi-b" –key priv.pem –passin pass:iniciales –out peticion.pem

Investigue los argumentos del parámetro subj.

_____
_____
_____

Indique el nombre del archivo de salida de este comando y el parámetro que lo genera.

_____
_____
_____

4. Verifique que el archivo peticion.pem se haya creado en su home.

[root@localhost openSSLiniciales]$ls

4.1.5 Firma del certificado digital

Los certificados permiten que un individuo demuestre que es, quien dice ser, ya que está en posesión de la clave secreta asociada a su certificado y únicamente son útiles si existe una AC que los valide, pues si uno mismo se certifica no hay garantía de que la identidad que se muestra sea auténtica.
Un administrador de redes debe ser capaz de verificar que un AC ha emitido un certificado y detectar si un certificado no es válido. Para evitar la falsificación de certificados, la entidad certificadora después de autenticar la identidad del sujeto, firma digitalmente el certificado.

1. El tercer paso es la emisión del certificado. Para definir las características de un certificado digital openssl, cuenta con el archivo de configuración openssl.conf ubicado en la carpeta /etc/ssl/ o bien se puede hacer un archivo de configuración. Abra el editor vi y escriba las siguientes líneas, posteriormente guarde el archivo con el nombre de config1.txt, en el mismo directorio de trabajo.

basicConstraints = critical,CA:FALSE
extendedKeyUsage = serverAuth

Investigue el funcionamiento de las líneas anteriores.

_____
_____
_____

2. Contando con el archivo de configuración, teclee el siguiente comando que genera el certificado firmado por la AC, ya creada.

[root@localhost openSSLiniciales]$ openssl x509 –CA cacert.pem –CAkey cakey.pem –req –in peticion.pem –days 3650 –extfile config1.txt -sha1 –CAcreateserial –out servidorcert.pem

Investigue el funcionamiento del comando anterior.

_____
_____
_____

3. La aplicación solicita el password de la AC que firma el certificado, introduzca el password configurado inicialmente (**.r3d3s.**)., ver Figura 11.3.

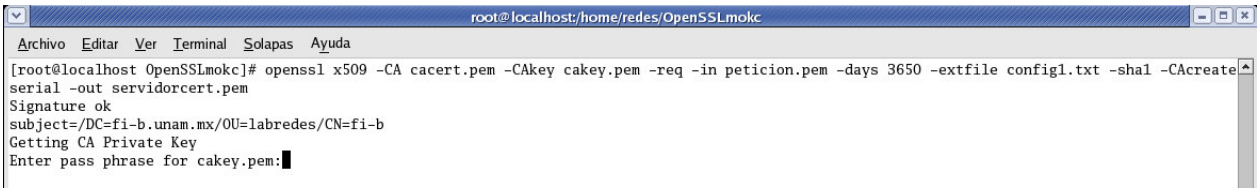


Figura 11.3 Solicitud de la frase pasword

4. Observe el resultado, el cual debe ser similar a la Figura 11.4

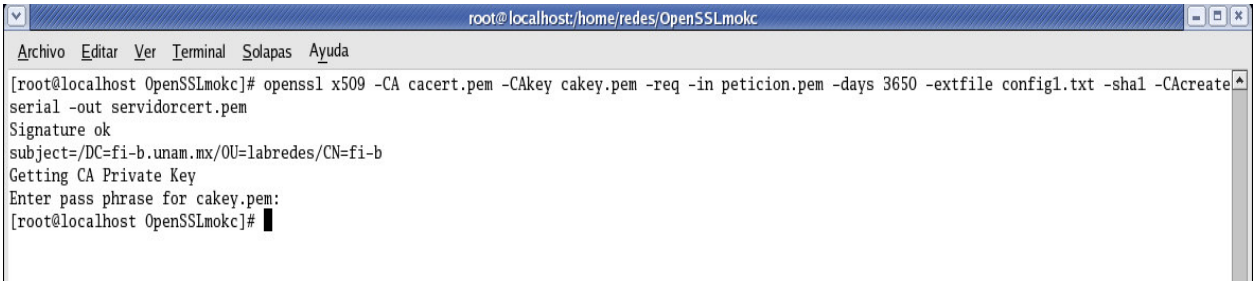


Figura 11.4 Confirmación de la firma del certificado

5. Verifique que el certificado se haya creado y analice su contenido, ver Figura 11.5.

[root@localhost openSSLiniciales]$ ls

[root@localhost openSSLiniciales]$ cat servidorcert.pem

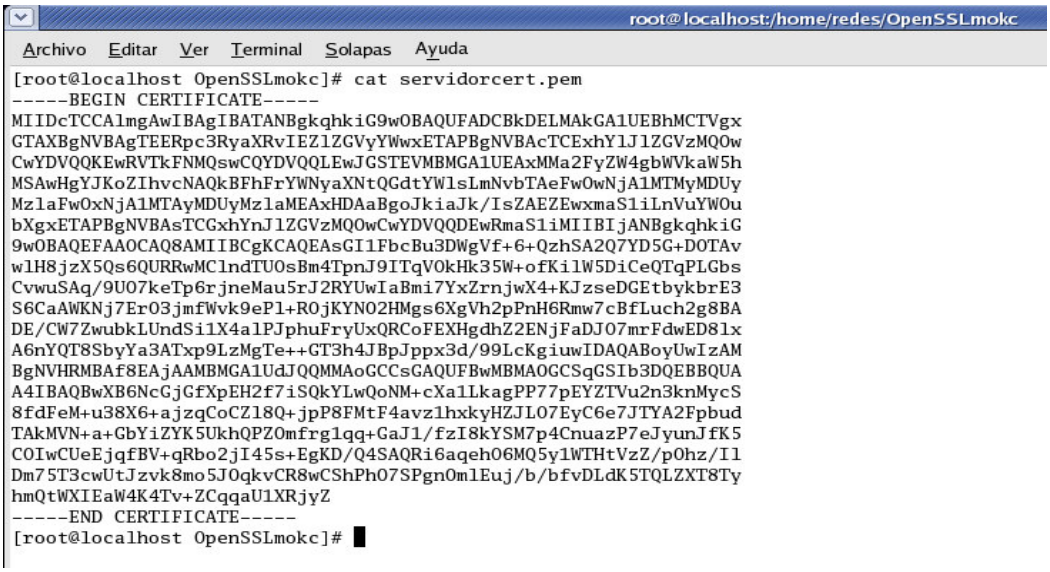


Figura 11.5 Contenido del certificado creado

Hasta este punto se ha creado un certificado que puede ser empleado para implementar un servidor que permita dar soporte a sitios Web certificados bajo SSL, Capa de Socket Seguros (Secure Socket Layer) en servidores Apache, por ejemplo.

6. Ejecute el siguiente comando que permite obtener información sobre el certificado recién creado, ver Figura 11.6.

[root@localhost openSSLiniciales]$ openssl x509 –in servidorcert.pem –text –noout

Figura 11.6 Información del certificado creado

Indique la información proporcionada por el comando anterior.

_____
_____
_____

4.1.6 CRL, Listas de Anulación de Certificados

Los certificados tienen un periodo de validez, durante el cual la AC, debe mantener la información de las entidades. Entre los datos más importantes que deben ser actualizados, se encuentra el estado de anulación del certificado, el cual indica que el periodo de validez ha terminado antes de tiempo y el sistema que lo emplee no debe confiar en él.

Investigue al menos 3 razones para indicar que un certificado ya no es válido.

_____
_____
_____

Las CRL, Listas de Anulación de Certificados (Certification Revocation List) son un mecanismo a través del cual la AC, da a conocer y distribuye la información acerca de los certificados anulados a las aplicaciones que los emplean. Estas estructuras de datos

firmadas por la AC, contienen su fecha y hora de publicación, el nombre de la entidad certificadora y los números de series de los certificados anulados que aún no han expirado.

Un administrador de redes, debe obtener la última CRL de la entidad que firma el certificado que emplean sus aplicaciones y verificar que los números de series de sus certificados no estén incluidos en tal lista.

Investigue 2 métodos de actualización de CRL.

_____
_____
_____

El objetivo de este punto es manipular el archivo de configuración de OpenSSL así como los comandos que permiten revocar certificados y generar listas de revocaciones.

1. Modifique el archivo de configuración openssl.cnf ubicado en /usr/share/ssl/openssl.cnf, comentando el campo dir y colocando el directorio actual en su lugar, de la siguiente manera:

```
#dir=./demoCA
dir=.
```

2. Cree un archivo de nombre index.txt en el directorio de trabajo.

[root@localhost openSSLiniciales]$touch index.txt

3. Revoque el certificado creado, mediante el siguiente comando ver Figura 11.7.

[root@localhost openSSLiniciales]$ openssl ca –keyfile cakey.pem –cert cacert.pem -revoke servidorcert.pem

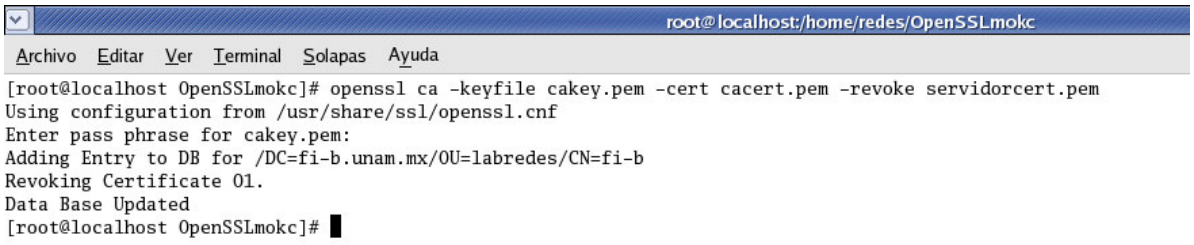


Figura 11.7 Revocando un certificado

Esta operación no modifica el certificado, simplemente actualiza el contenido del archivo de la base de datos, index.txt.

Describa el contenido de dicho archivo.

_____
_____
_____

Nota: La revocación de un certificado no es conocida hasta la publicación de la CRL.

4. Genere una CRL a través del siguiente comando, introduciendo la frase password de la clave privada de la AC, (**.r3d3s.**). ver Figura 11.8.

[root@localhost openSSLiniciales]$ openssl ca –gencrl –keyfile cakey.pem –cert cacert.pem –out ejemplo.crl

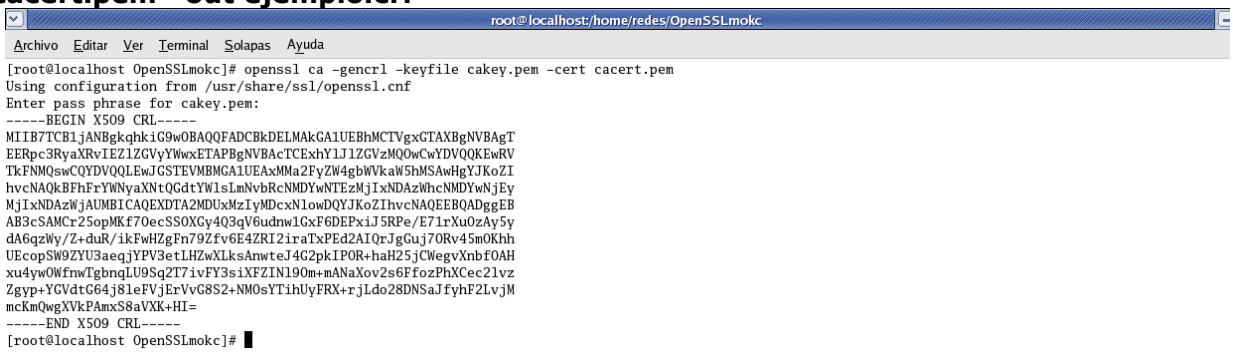


Figura 11.8 Creación de una CRL, Lista de Revocación de Certificados

5. Analice el contenido del archivo creado en el punto anterior.

[root@localhost openSSLiniciales]$ cat ejemplo.crl

6. Para obtener información acerca de la lista de revocación de certificados, ejecute el siguiente comando y observe que la salida debe ser similar a la Figura 11.9.

[root@localhost openSSLiniciales]$ openssl crl –in ejemplo.crl –text –noout

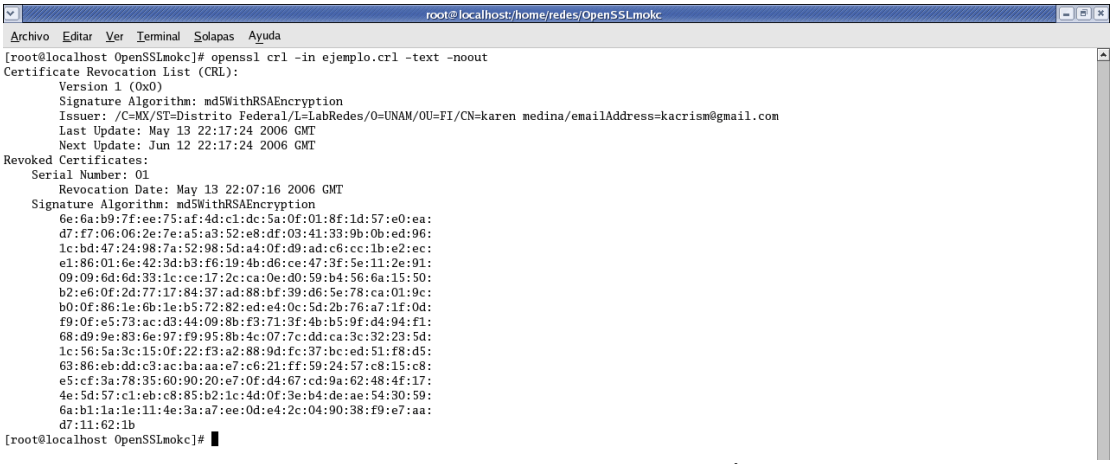


Figura 11.9 Contenido una CRL, Lista de Revocación de Certificados

Anote la salida del comando anterior, excepto la información en codificación hexadecimal.

_____

_____

_____

El comando anterior busca en la base de datos de la AC, los certificados revocados, generando una lista con los números de serie.

Las listas de revocación deben ser publicadas para que sean consultadas por lo usuario, por ejemplo en un servidor http. El sitio http://pki.cica.es/crl/ permite consultar una lista de certificados revocados por esa AC, ver Figura 11.10.

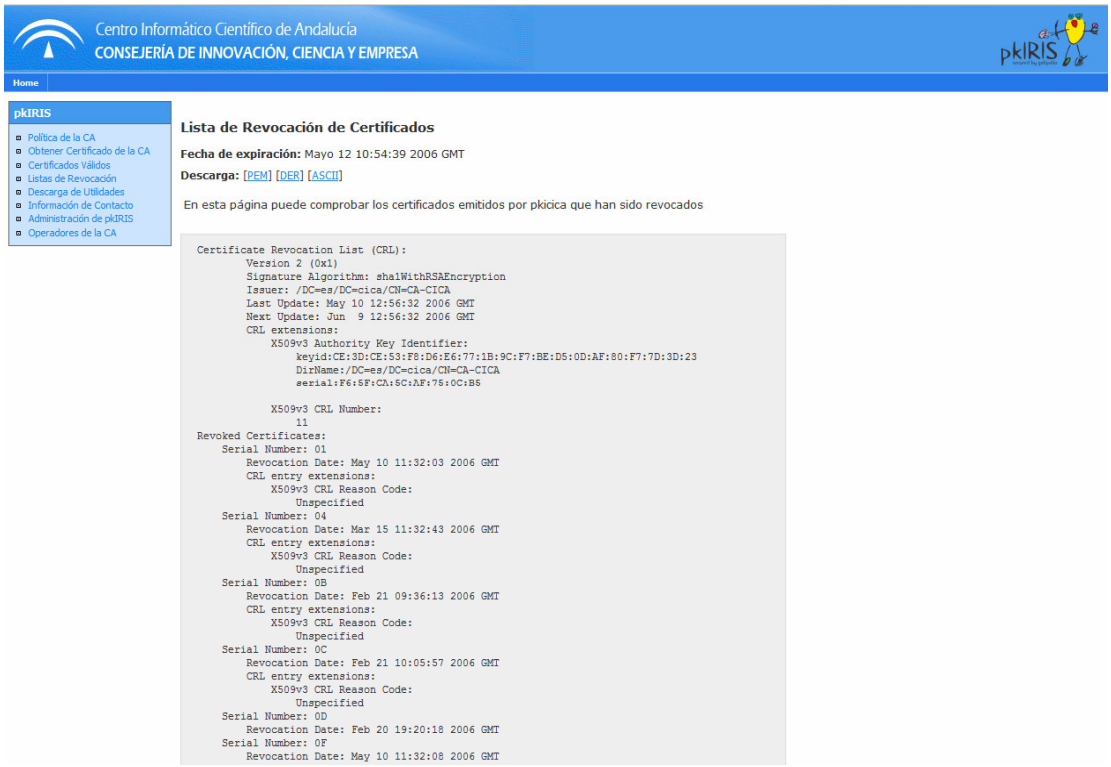


Figura 11.10 CRL, Lista de revocación de certificados publicada en la Web

4.1.7 Exportación de certificados digitales

Windows permite el uso de los certificados para firmarse con diversos servicios como el correo electrónico, para lo cual es necesario exportar el certificado a formato PCKS12.

1. Ejecute el siguiente comando que permite la exportación del archivo de un formato.pem a un formato entendible para Windows.

[root@localhost openSSLiniciales]$ openssl pkcs12 –export –in servidorcert.pem -inkey priv.pem –certfile cacert.pem –out certificado.p12

Nota: Los valores de las frases password que openssl requiere, se refieren a la clave privada del certificado **(iniciales)** y una clave que Windows pedirá para exportar e importar el certificado respectivamente **(redes)**.

5.-Conclusiones

_____
_____
_____
_____
_____
_____

6.-Cuestionario previo 10 B

1. Investigue en al menos 3 aplicaciones de los certificados digitales.
2. Investigue en qué consiste el proceso de importación de certificados.
3. Investigue al menos 2 herramientas adicionales que permitan la administración de certificados.
4. Describa brevemente el funcionamiento básico de un certificado digital.
5. Investigue en qué consiste el estándar ISO 17799.

ADMINISTRACIÓN DE REDES DE COMPUTADORAS

PRÁCTICA 11
Auditoria de una Red

1.- Objetivo de aprendizaje

El alumno se familiarizará con herramientas básicas relacionadas con la seguridad en la red, que generan controles que permiten la evaluación continúa de la eficacia y eficiencia de la red de una organización, objetivos básicos de la auditoría en redes.

2.- Conceptos teóricos

El cómputo es una herramienta clave dentro de la administración integral de una organización. A finales del siglo XX, los sistemas de tecnologías se conformaron como elementos claves dentro de las organizaciones, ya que respaldan la toma de decisiones, generando un alto grado de dependencia, así como una elevada inversión en ellas. Debido a su importancia, existe la auditoría informática.

Con frecuencia el término auditoría es incorrectamente empleado como sinónimo de detección de errores y fallas, perdiendo su objetivo central: la evaluación continúa de la eficacia y eficiencia de una organización.

Los sistemas de tecnología de información deben ser sometidos a controles de calidad, ya que las computadoras y centros de procesamiento de datos, son blancos de espionaje, terrorismo y delincuencia

La auditoría informática se considera como un proceso continuo y evolutivo, que a través de técnicas y procedimientos aplicados en una organización por personal independiente a la operación de la misma, evalúa la función de la tecnología de la información y su aportación al cumplimiento de los objetivos de la organización, para mejorar el nivel de apoyo al cumplimiento.

Las fases que incluyen a la auditoría informática son similares a la auditoría tradicional y se compone de las siguientes etapas:

1. Planeación, etapa cuyo propósito es entender y obtener los procesos de negocio, incluye la concentración de objetivos, la delimitación del área que cubrirá, las personas de la organización que se involucrarán en el proceso de auditoría, el establecimiento del plan de trabajo.

   El plan de trabajo debe incluir los siguientes puntos: definición de tareas, calendario de actividades, resultados parciales, presupuesto, equipo auditor necesario, etc.

2. Desarrollo de la auditoria, requiere la realización de entrevistas, cuestionarios, observaciones de las situaciones y procedimientos deficientes.

3. Análisis y evaluación, su objetivo es determinar la probable efectividad y eficiencia del control interno. También es conocida como la etapa de diagnóstico, pues implica la meditación sin contacto con la organización auditada, considerando la experiencia del equipo auditor, para la definición de los puntos débiles y fuertes, así como los riesgos eventuales y tipos de solución.

4. Pruebas, existe una clasificación de las pruebas realizadas en:

   a. Pruebas de cumplimiento, aquellas realizadas para verificar la efectividad de los procedimientos de control.

b. Pruebas sustantivas, aquellas que se implementan para verificar los procesos de trabajo.

5. Resultados, se informan los resultados de la auditoría, con el fin de reportar las sugerencias correspondientes a las mejoras encontradas, argumentando y documentando de forma suficiente, para evitar que sean rechazadas. El desarrollo del plan de mejoras debe incluir un resumen de las deficiencias encontradas, recogiendo las recomendaciones encaminadas a resolver esos puntos débiles, mediante medidas a corto plazo (mejoras en plazo, calidad, planificación o formación), medidas a medio plazo (mayor necesidad de recursos, optimización de programas, documentación y aspectos de diseño) y medidas a largo plazo (cambios en políticas, medios y estructuras del servicio).
6. Seguimiento, realizado para evaluar el nivel de cumplimiento e impacto en las recomendaciones hechas.

3.- Equipo y material necesario

4.- Desarrollo

A menudo la auditoría de redes, se divide en el análisis de 3 módulos:

1. Administración.
2. Instalación.
3. Operación y seguridad.

4.1 Administración

Investigue si en el Laboratorio de Redes de Datos y Seguridad existe la definición formal de un plan, que implique la definición de los siguientes procedimientos:

a. Evaluación del hardware actual.
b. Evaluación del software actual.
c. Estudio para justificar la instalación o reemplazo de la red.

_____
_____
_____

Investigue el organigrama del Laboratorio de Redes de Datos y Seguridad.

_____
_____
_____

4.2 Instalación

Conteste las siguientes preguntas que sirven como referencia para aplicar una auditoría en este módulo del área de redes. Si la respuesta es negativa, proponga una solución, de lo contrario, anexe el documento indicado en su reporte final.

¿Existen procedimientos que aseguren la oportuna y adecuada instalación de componentes que conforman la red?

_____
_____
_____

¿Existen formatos que permitan identificar las actividades que se llevan a cabo?

_____
_____
_____

¿Existe la documentación necesaria para cuando se instalan los componentes de la red (hardware, software, procedimientos, etc.)?

_____
_____
_____

¿Existen procedimientos definidos para la compra de software que asegura su adquisición legal?

_____
_____
_____

¿Existe un responsable de las actividades de seguridad y control para garantizar el uso adecuado y protección de software?

_____
_____
_____

4.3 Operación y seguridad

Durante esta etapa de la auditoría de la red, es necesario verificar la existencia de:

- Manuales de operación de la red, que contemplen aspectos de seguridad.
- Personal responsable de administrar la red.
- Capacitación del personal para realizar actividades de administración de operación y seguridad.
- Estándares de desempeño que involucran parámetros de tiempos de respuesta, trafico, etc.

Este punto de la práctica, tiene por objetivo obtener las diferentes estadísticas que le permiten generar un análisis del comportamiento de los siguientes parámetros, con la herramienta de administración 3·COM Network Supervisor.

A. Tiempo de respuesta.

B. Volúmenes de información.

C. Tiempo de recuperación de la red.

D. Interrupciones.

1. Inicie la herramienta de supervisión de redes, mediante el menú Inicio>Todos los programas>3ComNetworkSupervisor.
2. Inicie el asistente de reconocimiento de red, eligiendo la opción Local subset, ver Figura 11.1. El resultado de este análisis de red, es un mapa con todos los dispositivos que integran a la red.

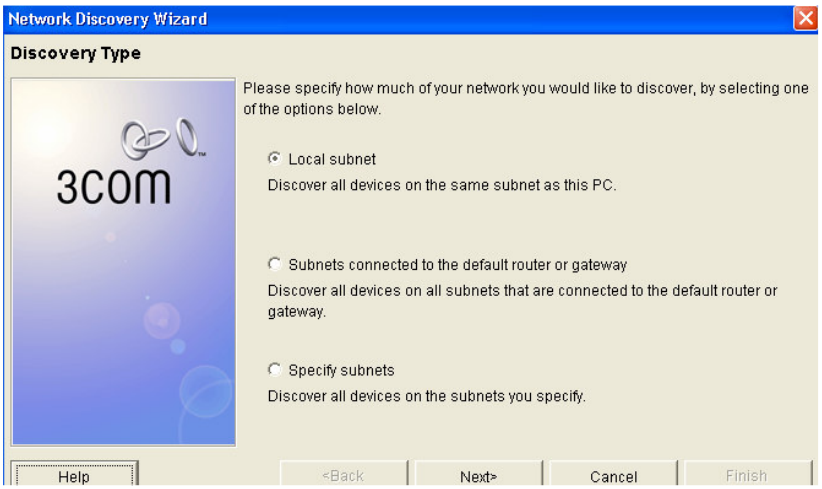


Figura 11.1 Reconocimiento de la red

3. Inicie el monitoreo del dispositivo activo central de la red, haciendo doble clic sobre él. Observe la barra de tráfico e interprete el resultado que muestra.
4. Cuando se hace un monitoreo de una variable y ésta sobresale del parámetro establecido, se producen los eventos, ver Figura 11.2. Explique el estado actual de la red.

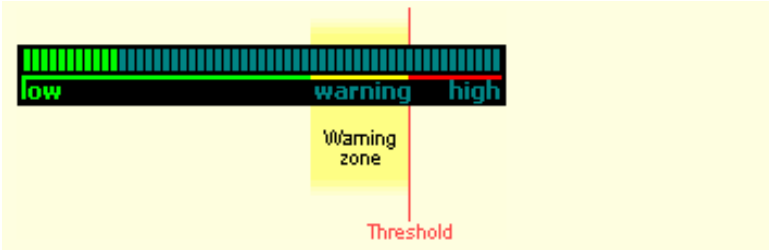


Figura 11.2 Evento en una actividad de monitoreo

Investigue los eventos que pueden ser analizados con esta herramienta de monitoreo.

_____
_____
_____

5. En todas las redes, hay dispositivos importantes y enlaces claves de quien depende la operación de la red, si éstos fallan pueden causar problemas a los usuarios de la red. Por tal razón es necesario configurar las alertas. La auditoría del tercer módulo, verifica la existencia de dicha configuración.

Investigue el concepto de alerta en el área de administración de redes.

_____
_____
_____

6. Configure una notificación hacia el correo del administrador que le notifique un valor fuera de rango para el tráfico TCP que circula por la red. Anote en las siguientes líneas el procedimiento realizado.

_____
_____
_____

7. Genere un reporte del comportamiento de la red, a través del menú principal, seleccione la opción Reports desde el menú Tools. En el cuadro de diálogo de Reports, el panel de generación de reportes es desplegado permitiendo elegir entre el tipo de reporte que se desea crear. Seleccione la primera opción y haga clic en el botón Generate.
8. Genere un inventario de la red, en el menú principal seleccione la opción Reports del menú Tools. Del cuadro de diálogo Reports, el panel de reportes generados es desplegado, permitiendo seleccionar el tipo de reporte que se desea crear. Seleccione de la lista de tipos de reporte, la opción Inventory y haga clic en Generate Reporte, para finalmente obtener una lista de todos los dispositivos sobre el mapa de la red.

Indique cada uno de los campos especificados en el inventario obtenido de la red.

_____
_____
_____

9. Obtenga un reporte que identifique los puertos disponibles de la red y permita la expansión de la capacidad de red. Lo anterior se obtiene generando un reporte de Capacidad. Seleccione la opción Reports, del menú Tools. Del cuadro de diálogo Reports, el panel de Reportes Generados, permite la elección del tipo de reporte que se desea crear para los dispositivos y enlaces de la red, seleccione de la lista de tipos de reportes, la opción Capacity y haga clic en el botón Generar Reporte.

Indique las características principales de este reporte y la ventaja de contar con él.

_____
_____
_____

10. Genere un reporte de conexiones, a través de menú Reports de la opción Tools. Seleccione Topology de la lista de tipos de reportes que se desean generar y haga clic en Generate Report. Observe los resultados.

Indique las características principales de este reporte y la ventaja de contar con él.

_____
_____
_____

11. Obtenga un reporte que muestra las configuraciones actuales de los equipos que integran a la red, a través de la elección Misconfigurations and Optimizations del menú Tools>Reports.

Analice la información que proporciona el reporte anterior y explique su importancia dentro del proceso de auditoría.

_____
_____
_____

12. Genere un reporte personalizado, que muestre información de los parámetros más significativos para una administrador de redes.

4.4 Reporte y seguimiento

De acuerdo a los reportes obtenidos y entrevistas, presente un reporte final en el que indique las áreas con debilidades, la propuesta y su conclusión final. El reporte debe cubrir con las siguientes especificaciones:

1. Identificación del informe, el título del informe, debe resaltarse.
2. Identificación del cliente.
3. Identificación de la entidad informática auditada.
4. Establecimiento de objetivos, que identifiquen las razones de su realización.
5. Restricciones en la distribución.
6. Alcance de la auditoría.
7. Hallazgos reportados.
8. Conclusiones, informe corto de opinión considerada como la evaluación del editor del área que ha sido auditada.
9. Actividades de seguimiento, implica la descripción de requerimientos de una respuesta, considerando las acciones.
10. Fecha del informe.
11. Identificación y firma del auditor.

5.-Conclusiones

6.-Cuestionario previo 11

1. Investigue en qué consisten los estándares ISACA.
2. Mencione 5 áreas dentro de la auditoría informática.
3. Investigue las etapas de la auditoría informática.
4. Investigue cuál es el objetivo de los controles en la informática.
5. Investigue los objetivos de la auditoría en redes.