UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

“PROPUESTA PARA EL MODELO DE ADMINISTRACIÓN DE LA RED INFORMÁTICA DE LA FACULTAD DE QUÍMICA DE LA UNAM”

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN TELECOMUNICACIONES

PRESENTA:

ARANDA PAREDES VÍCTOR MANUEL

DIRECTOR DE TESIS: MTRO. JAVIER JULIÁN ROBLES RIVAS
CODIRECTOR DE TESIS: DR. JAVIER GÓMEZ CASTELLANOS
MÉXICO DF. 2006

Dedicatoria

Para mis padres. Sin ellos todo mi esfuerzo hubiera sido en vano.

Agradecimientos

La realización de este trabajo no hubiera sido posible sin la existencia de la educación publica, por ello quiero dar las gracias a todos aquellos que de una u otra forma han dedicado parte de su tiempo a la preparación que en todos estos años he recibido.

Contenido

Resumen

Este trabajo presenta una alternativa de solución a las necesidades en la administración de la nueva infraestructura de red, implementada en la Facultad de Química de la UNAM. La solución implica el diseño y puesta en marcha de un modelo de administración, basado en modelos funcional estándar de la ITU y de la ISO. Estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes.

Inicia describiendo los problemas causados por la antigua red de datos y las generalidades del proyecto red, que la Facultad de Química ha presentado como solución a estos. El proyecto es el diseño de la infraestructura de red que pretende dar solución a todos los problemas de la antigua red de datos. El trabajo incluye información teórica, que es la base para el planteamiento del proyecto de red y del modelo de administración propuesto, con la descripción detallada del proyecto y requerimientos que debe satisfacer. Además de un análisis de la nueva infraestructura de red sobre la cual se implementara el modelo de administración aquí propuesto.

Finalmente se plantea un modelo de administración de red de datos, basado en una división departamental que sea útil a la Facultad de Química. Al mismo tiempo se establecen los objetivos y actividades de cada departamento y se finaliza con una propuesta del Staff técnico que realizara estas actividades. Incluye consideraciones a futuro de la red y del modelo de administración.

Abstract

This work presents an alternative of solution to the problems in the administration of the new infrastructure of network implemented in the Faculty of Chemistry of the UNAM. The solution implies the design and beginning of an administration model, based on a standard functional model of the ITU and the ISO. The model details the tasks and functions that must be executed in the process of network management.

This begins describing to the problems caused by the old data network and the majorities of the project that the Faculty of Chemistry has presented like solution. The project is the design of the infrastructure of data network that it tries to give solution to all the problems caused by the old data network. The work includes theoretical information, that it is the base for the exposition of the project of network and the proposed model of administration, along with the detailed description of the project and requirements that must satisfy. In addition to an analysis of the new infrastructure of network and the administration model implemented.

In the final part a model of network management of data considers, based on a departmental division that is useful to the Faculty of Chemistry. At the same time the objectives settle down and activities of each department and are finalized with a proposal of the technical Staff that made these activities. In order to finalize, the considerations to future become of the network and the model of administration.

CAPÍTULO 1

Descripción del trabajo de Investigación

1.1 OBJETIVO

Ofrecer un modelo de administración que de solución a las necesidades de configuración, operación y mantenimiento de la nueva red informática de la Facultad de Química de la UNAM basado en modelos funcionales estándar de administración de redes aceptados internacionalmente.

1.2 JUSTIFICACIÓN

La Facultad de Química necesita proveer la infraestructura de comunicaciones que de servicio a los alumnos, cuerpo docente, administrativo y de investigación que conforma toda su comunidad; en apoyo al desarrollo de sus actividades.

La Facultad de Química ha implementado un ambicioso proyecto de red informática, propuesto como solución a las necesidades de comunicación, que considera el suministro, instalación y certificación de un Sistema de Cableado Estructurado Estándar, basado en las normas EIA/TIA 568 y 569, así como los equipos activos basados en tecnología *Gigabit Ethernet* y la norma IEEE 802.3, que sean necesarios para la segmentación total de la red.

La realización del proyecto de integración de la red informática de la facultad de Química implica el diseño y puesta en marcha de un modelo de administración de la nueva infraestructura de comunicaciones. Este debe ser parte integrante de un modelo de soporte a tecnologías de información y comunicaciones de la Facultad de Química.

La propuesta para el modelo de administración de la nueva infraestructura de comunicaciones esta basada en la especialización que permita controlar principalmente los aspectos de configuración, operación, y mantenimiento, así como proporcionar autosuficiencia en la gestión de la infraestructura informática.

Todo con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos.

1.3 METODOLOGÍA Y ALCANCE

Para lograr implementar un modelo de administración de red de datos, en la Facultad de Química, basado en la especialización, se utilizará modelos funcionales estándar de la ITU-ISO. Estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes.

Esta propuesta plantea el seguimiento del estándar TMN (Telecommunications Management Network), modelo definido en la serie M.3000 de la ITU-T y del OSI-NM de ISO. Estos modelos presentan las áreas funcionales en la cual se divide la administración de redes y que se adaptarán para lograr un modelo de administración de red útil para la Facultad de Química.

Se establecerán los objetivos particulares de cada área, que en síntesis aseguran el eficiente y efectivo empleo de los recursos, La descripción de las tareas de cada área funcional, tendrá que seguir como meta el cumplimiento del objetivo planteado.

Además se establecerán las tareas y procedimientos de cada área y las herramientas para lograr el cumplimiento de estas, así como la relación que existente entre las áreas del modelo. Por ultimo se incluirá el perfil de especialización necesario para el personal que debe cubrir las tareas en estas áreas.

La utilización de este modelo, contempla que la red evoluciona, que los problemas cambian y que la forma de administrar debe ser adaptativa, y que para esto se necesita una estructura organizacional que al final permite adaptar este modelo a futuros cambios.

1.4 ACERCA DEL CONTENIDO DE LOS CAPITULOS

Este trabajo se divide en 5 apartados, desarrollados en forma de capítulos para conformar esta propuesta.

A continuación se describe en forma general el contenido de cada capitulo.

El análisis contextual:

Describe como opera la Facultad de Química de la UNAM, los problemas que presenta su actual red informática en infraestructura y administración, así como el proyecto de red creado para resolver estos problemas.

Los fundamentos teóricos:

Ahondara en los componentes de una computadora y el papel de las computadoras en un sistema de redes. Se empleara el método de “menor a mayor” para conocer un poco acerca de los sistemas de redes, comenzando por uno de los componentes más básicos de una red: la computadora.

Además se entenderá como las normas aseguran la compatibilidad e interoperabilidad entre diferentes tipos de tecnologías de red, las topologías de red existentes, los dispositivos de LAN básicos y la evolución de los dispositivos de red.

También sé detallará la capa de red como la responsable de la navegación de datos a través de la red y su función es la de encontrar la mejor ruta para moverse por dicha red. Se explicara el papel del enrutador en la realización de la función de *Internetworking* clave de la capa 3 del modelo de referencia OSI. Además, se explicara que es el direccionamiento IP y las mascaras de subred.

Para terminar se menciona cómo mantener la red y conseguir que funcione a un nivel aceptable. Además, cuándo es necesario ampliar o cambiar la configuración de la red para satisfacer la demanda cambiante. En este capítulo se explicará como administrar una red utilizando técnicas como la documentación, el control y la solución de problemas.

Análisis del caso:

En este capitulo, se verán los aspectos generales del proyecto de red, que se implementara como la solución a los problemas que presenta la antigua red informática de la Facultad de Química. Se incluye las especificaciones y requerimientos necesarios para su implementación; además de la distribución de los servicios de datos que en el próximo capitulo servirá como base en la configuración de la red.

La Propuesta del esquema de administración de red:

En este capítulo veremos una propuesta para la configuración de red y la metodología propuesta para su administración. Se establecerán las metas del modelo de administración y las tareas necesarias para conseguir el cumplimiento de estas metas. Al final se hacen las consideraciones a futuro de la infraestructura de red y del modelo de administración de red propuesto.

Conclusiones:

Integra las conclusiones del trabajo referentes a la infraestructura de red y al modelo de administración.

CAPÍTULO 2

Análisis contextual de la problemática

2.1 LA OPERACIÓN DE LA FACULTAD DE QUÍMICA

La Facultad de Química es la Institución de educación superior en Química más importante de México. Forma parte de la UNAM y tiene más de 85 años contribuyendo al progreso de México. Su comunidad esta formada por 1,200 Académicos y más de 5,000 estudiantes. Las instalaciones se localizan en la Ciudad Universitaria. Cuenta con 5 edificios con más de 75,000 metros cuadrados, 153 laboratorios, 71 salones y equipos con la tecnología más avanzada.[1]

La Facultad de Química realiza diferentes actividades, entre ellas se encuentran la docencia. Se imparten 5 carreras y participa en 6 posgrados universitarios. En Investigación, con más de 600 proyectos de investigación. En Difusión de la cultura y educación continua, con instalaciones especiales en Tacuba y CU para cursos de actualización.

La Figura 2.1 muestra un diagrama de como se encuentra organizada administrativamente la Facultad de Química.

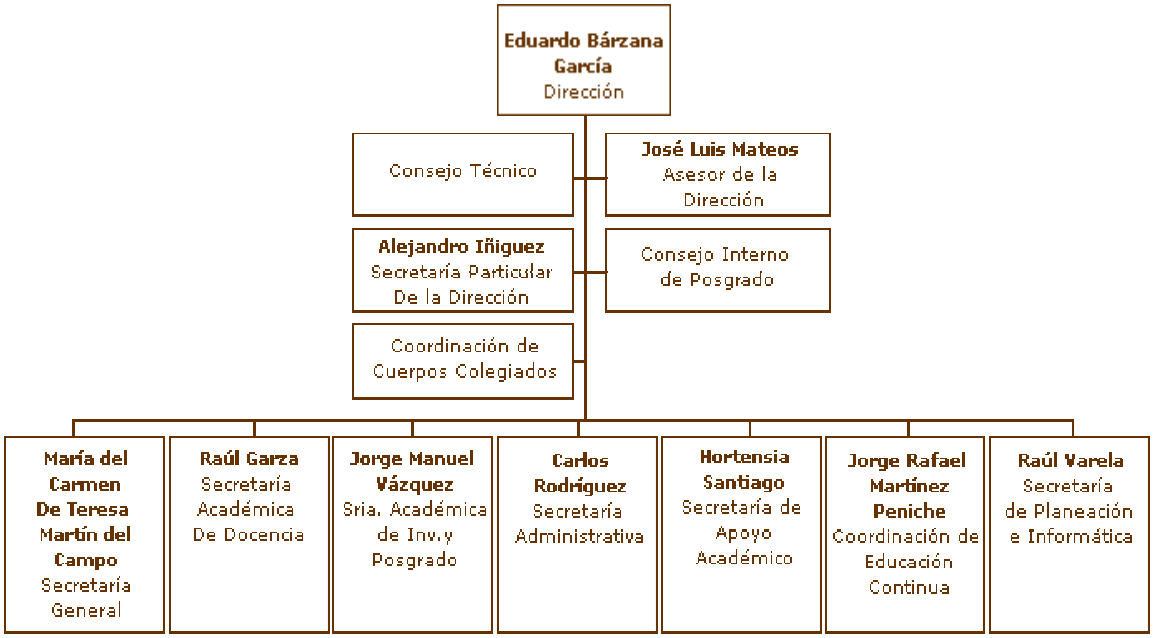

Figura 2.1. Organización básica de la Facultad

[1] http://www.fquim.unam.mx/

La Facultad está organizada por trece departamentos académicos y cada uno de los miembros del personal académico está adscrito a uno de estos departamentos.

- Departamento de Fisicoquímica.
- Departamento de Administración Industrial.
- Departamento de Biología.
- Departamento de Bioquímica.
- Departamento de Química Orgánica.
- Departamento de Química Inorgánica.
- Departamento de Física y Química Teórica.
- Departamento de Ingeniería Química.
- Departamento de Ingeniería Química Metalúrgica.
- Departamento de Química Analítica.
- Departamento de Alimentos y Biotecnología.
- Departamento de Farmacia.
- Departamento de Matemáticas.

2.2 LA ANTIGUA RED INFORMÁTICA

La antigua red informática de la Facultad de Química fue implementada aproximadamente hace 15 años, fue creada para ofrecer servicios de comunicación de voz y datos a los departamentos de administración, de personal y de investigación. Las tareas en ese entonces, no requerían de equipos con gran capacidad de procesamiento y por lo tanto la red no transportaba una gran cantidad de datos.

Con el paso del tiempo la comunidad de la Facultad comenzó a crecer, la cantidad de alumnos se incremento, hubo la necesidad de contratar más personal académico, los proyectos de investigación crecían constantemente, y los servicios que prestaba la Facultad se incrementaron al mismo tiempo. Con estos cambios fue necesario contar con mayor número de instalaciones, más salones y equipo.

Este crecimiento requirió de la creación de mayores y mejores procesos académicos y administrativos. La comunidad demandaban de mayores servicios administrativos, como el acceso a comprobantes de estudio, comprobantes de calificaciones, tramites escolares etc., además del acceso a equipos de cómputo y acceso a Internet. Los departamentos administrativos y académicos tenían ahora la misión de llevar el control de más alumnos y de proveer de mayores servicios a estos; así las computadoras comenzaron a tomar un papel importante dentro de todas las actividades de la Facultad.

Por lo anterior la red informática existente en ese momento no respondió a los cambios que en otros ámbitos experimento la Facultad, generándose un retraso tecnológico y una creciente complicación en su administración y mantenimiento

La infraestructura de red fue la primera parte de la red en resentir estos cambios. Algunos de los problemas eran la falta de una completa cobertura dentro de las instalaciones y el incremento de usuarios que requería de nuevos servicios de datos. Así los nuevos usuarios tuvieron que resolver la falta de servicios utilizando dispositivos de comunicación como Concentradores y Conmutadores, que lograban incrementar el número de servicios a costa de compartir una misma conexión de red y con esto compartir el ancho de banda disponible. La llegada de equipos más potentes, de aplicaciones más grandes y con mas funciones, el manejo de bases de datos más robustas, la comunicación cada vez mas necesaria de datos entre diferentes departamentos de la Facultad, la creación de nuevos servicios y el acceso a las nuevas tecnologías disponibles en Internet; requerían que la infraestructura de red fuera capaz de afrontar estos retos; pero la antigua red soportaría muy poco tiempo estos constantes cambios.

Los problemas en la administración de red eran evidentes; el personal encargado de crear la antigua infraestructura de red no contemplo la administración como parte integral de esta. No existió una estructura o diseño previo de administración y se aplicaron mínimos conceptos de forma lenta y en muchas ocasiones solo cuando esto era necesario. La falta de un inventario de los equipos de la red y el monitoreo de actividades, provocaba dificultades en la administración; sobre todo cuando surgía un problema en la red y era difícil detectar cual era el origen de tal suceso. La cantidad de usuarios que ingresaban a la red y las actividades que realizaban no eran auditadas, la falta software antivirus actualizados y de políticas de uso, ocasionaba grandes problemas de seguridad. La administración de direcciones IP y el uso no autorizado de estás

provocaba conflicto en los equipos y los servicios de la red. Por ultimo un centro de soporte técnico, que no contó con la metodología para la atención de casos y en consecuencia no conseguía atender todos los problemas.

Por lo anterior fue necesario proponer un nuevo proyecto de infraestructura de red que resolviera la problemática y un modelo de administración de red, que fuera parte integral al sistema de comunicaciones aceptado como solución.

2.3 EL PROYECTO DE INFRAESTRUCTURA Y EL MODELO DE ADMINISTRACIÓN DE RED

El proyecto que define la integración de la red informática de la Facultad de Química consiste en las especificaciones necesarias para la infraestructura de la red de datos que dará servicio a los diferentes niveles de los edificios que componen el conjunto de Postgrado de la Facultad de Química de la UNAM, ubicada en Cuidad Universitaria en México DF.

En este proyecto la red de datos ha sido diseñada partiendo de la existencia de las salas de equipo, clóset y gabinetes principales, los cuales cuentan con el suministro eléctrico necesario, y las correspondientes tierras físicas. Adicionalmente se cuenta con el enlace a Internet provisto por Red UNAM.

La implantación de la solución en su conjunto se sujetará al diseño y requerimientos técnicos especificados por la Facultad de Química, y serán provistos mediante el suministro, instalación, puesta en marcha, configuración y sintonización de los elementos que se establece la conforman.

La red de datos se fundamenta en el estándar ANSI/EIA/TIA 802.3[2] (Ethernet), lo que asegura la interoperabilidad de los equipos de comunicaciones; el cableado estructurado se fundamenta estrictamente bajo los estándares EIA/TIA 568-B y 569-A. Las adecuaciones de tipo físico y eléctrico se basan en los estándares EIA/TIA 606 y ETI/TIA 607.

La realización del proyecto de integración de red informática de la Facultad de Química implica el diseño y puesta en marcha de un modelo de administración de la nueva infraestructura de comunicaciones. Este debe ser parte integrante de un modelo de soporte a tecnologías de información y comunicaciones de la Facultad.

La propuesta para el modelo de administración de la nueva infraestructura de comunicaciones está basada en el seguimiento del estándar TMN (Telecommunications Management Network), que es un modelo definido en la serie M.3000 de la ITU-T[3] y del modelo OSI-NM de ISO[4]. El seguimiento de estos estándares asegura la autosuficiencia en la gestión de la infraestructura informática.

[2] http://www.anixter.com
[3] http://www.itu.int
[4] http://www.iso.org

CAPÍTULO 3

Fundamentos teóricos

3.1 INTRODUCCIÓN

En este capítulo, se explica cuales son los componentes de una computadora y el papel de las computadoras en un sistema de redes. Se empleara el método de “menor a mayor” para conocer acerca de los sistemas de redes, comenzando por uno de los componentes básico de una red: la computadora.

Para ayudar a comprender el papel que desempeñan las computadoras en los sistemas de redes, se puede tomar como referencia Internet. Pensemos en Internet como en un árbol y las computadoras como las hojas del árbol, las computadoras son los componentes que generan la información y la reciben de Internet. Las computadoras pueden funcionar sin Internet, pero Internet no puede existir sin las computadoras.

Con el avance constante de las redes se crearon implementaciones diferentes tanto en hardware y software para su construcción. Como resultado, muchas de ellas fueron incompatibles haciendo difícil el intercambio de información. Para resolver esto, la Organización Internacional de Normalización (OSI) investigó muchos esquemas de red que pudieran dar soluciona a tal incompatibilidad de implementaciones; como resultado en 1984 lanzaron el modelo OSI.

En este capitulo se entenderá como los estándares aseguran una gran compatibilidad e interoperabilidad entre diferentes tipos de tecnologías de red, las topologías de red existentes, los dispositivos de LAN básicos y la evolución de los dispositivos de red.

También se explicará que la capa de red es la responsable de la navegación de los datos a través de la red y que su función es la de encontrar la mejor ruta para moverse por dicha red. Se explicara el papel del enrutador en la realización de la función de *Internetworking* clave de la capa 3 del modelo de referencia OSI. Además, se aprenderá que es el direccionamiento IP y las mascaras de subred.

Finalmente conoceremos cómo mantener la red y conseguir que funcione a un nivel aceptable. Esto significa como solucionar los problemas cuando éstos se presenten. Además, cuándo es necesario ampliar o cambiar la configuración de la red para satisfacer la demanda cambiante. En este capítulo se aprenderá a administrar una red utilizando técnicas como la documentación, el control y la solución de problemas.

3.2 CONCEPTOS BÁSICOS DE REDES

FLUJO DE INFORMACIÓN EN UNA COMPUTADORA IDEAL

La Figura 3.1 muestra los componentes principales de una computadora ideal. Puede pensar en los componentes internos de una computadora como en una red de dispositivos, todos conectados al bus del sistema. En cierto modo, una computadora es una pequeña red informática.

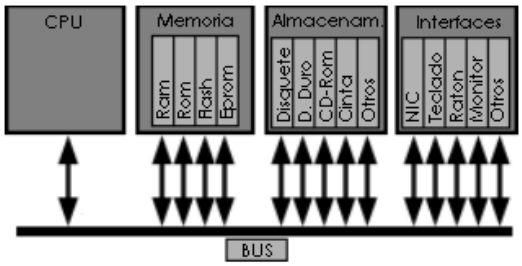

Figura 3.1 Todas las computadoras disponen de CPU, memoria, almacenamiento e interfaces.

TARJETAS DE INTERFAZ DE RED

Como se muestra en la Figura 3.2, una tarjeta de interfaz de red (NIC, Network Interface Card) es una placa de circuito impreso que proporciona capacidades de comunicación de red hacia y desde una computadora personal. También denominada adaptador de LAN, se conecta a la tarjeta principal y proporciona un puerto para conectarse a la red.

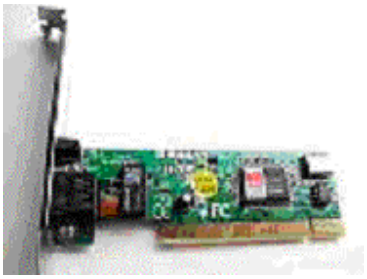

Figura 3.2. Una NIC proporciona un puerto para el acceso de la computadora a la red.

EL SOFTWARE DE LAS COMPUTADORAS

Ahora que se tiene una idea de qué conforma el hardware de las computadoras, necesitamos el segundo ingrediente (el *software*). El propósito del *software* es permitir interactuar con la computadora o el dispositivo de red para conseguir que haga lo que uno quiere. En esta sección, se hablara de los navegadores web (como Netscape e Internet Explorer) y los plug-ins.

Navegadores Web

Un navegador actúa en nombre de un usuario, contactando con un servidor web, solicitando información, recibiendo información y mostrando los resultados en una pantalla. Un navegador es un software que interpreta el lenguaje de marcado de hipertexto (HTML, HyperText Markup Language), que es el lenguaje empleado para codificar el contenido de las páginas web. HTML puede mostrar gráficos y reproducir sonidos, películas y otros archivos multimedia. Los hiperenlaces (comandos de programa que apuntan a otros lugares dentro de una computadora o en una red) conectan con otras páginas web y con archivos que pueden descargarse. Los dos navegadores más habituales son Netscape Communicator e Internet Explorer.

Los plug-ins

Existen también muchos tipos de archivos propietarios (es decir, cuyo formato es propiedad y está controlado por una empresa) que los navegadores web estándar no pueden mostrar. Para visualizar estos archivos, debe configurar su navegador para emplear aplicaciones plug-in. Estas aplicaciones trabajan conjuntamente con el navegador para ejecutar el programa requerido para visualizar esos archivos especiales. Algunos ejemplos son: Flash/Shockwave, QuickTime, RealAudio, RealPlayer.

REDES Y SISTEMAS DE REDES

Una red es un sistema intrínsecamente conectado de objetos o personas. Los propios sistemas nervioso y cardiovascular son redes. El diagrama de grupo de la Figura 3.3 muestra diversos tipos de redes; pero puede pensar en otras. Observe los siguientes agrupamientos:

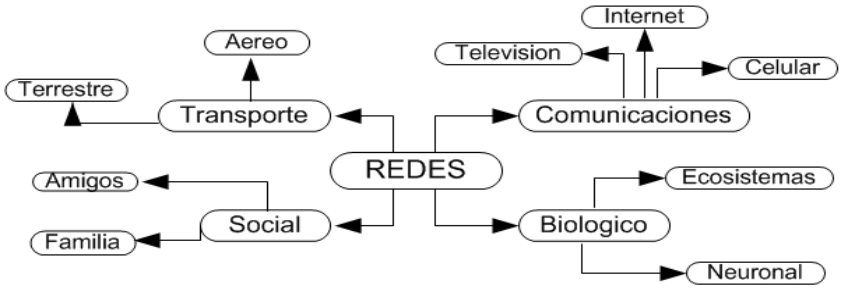

Figura 3.3. El término red se emplea de muchas formas, pero el resultado es similar, en todos los casos, al de una red de computadoras.

REDES DE DATOS

Las redes de datos aparecieron como resultado de las aplicaciones para computadoras *mainframe* que habían sido escritas para empresas. Sin embargo, en el momento en que estas aplicaciones fueron escritas, las empresas disponían de computadoras que eran dispositivos aislados, que operaban por sí mismos, independientemente de cualquier otra computadora. Por tanto, es evidente que no era una manera eficiente o económicamente efectiva de trabajar en las empresas. Así las empresas se dieron cuenta de cuánto dinero se podrían ahorrar y cuánto podrían aumentar la productividad empleando la tecnología de redes. Se comenzó a añadir redes y a extender las redes existentes casi tan rápidamente como aparecían las nuevas tecnologías y productos de red. Como resultado de esto, a comienzos de los 80 se vivió una tremenda expansión de las redes; sin embargo, el desarrollo inicial de las redes fue en cierto modo caótico.

A mediados de los 80, se detectaron ciertos problemas. Muchas de las tecnologías de red que habían aparecido habían sido creadas con diferentes implementaciones de *hardware* y *software*. En consecuencia, muchas de las nuevas tecnologías de red eran incompatibles entre sí. Todo esto hizo mucho más difícil que se comunicaran entre sí las redes que empleaban diferentes especificaciones. Sin embargo, las LAN, como posibilitaban la conexión de estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio, hicieron posible que las empresas emplearan la tecnología informática para comunicarse de forma eficiente y compartir elementos tales como los archivos o las impresoras.

A medida que el empleo de las computadoras crecía en la empresa, pronto fue obvio que incluso las LAN no eran suficientes. En un sistema LAN, cada departamento o compañía es una especie de isla electrónica. Era necesaria una forma de que la información se moviera eficiente y rápidamente, no sólo dentro de una compañía, sino de una empresa a otra. Entonces, la solución fue la conexión de las LAN mediante redes de área metropolitana MAN, (*Metropolitan-Area Networks*) y redes de área amplia WAN, (*Wide-Area Networks*). Debido a que las WAN permiten la conexión de usuarios de la red en zonas geográficas extensas, hicieron posible que las empresas se comunicaran con el resto a larga distancia.

SOLUCIONES PARA LOS SISTEMAS DE RED

Redes de área local:

Las redes de área local (LAN) están constituidas por computadoras, tarjetas de interfaz de red, medios de red, dispositivos de control del tráfico de la red y dispositivos periféricos. Las LAN permiten a las empresas que emplean tecnología informática compartir de forma eficiente elementos, tales como archivos e impresoras, y posibilitar las comunicaciones, como el correo electrónico. Unen entre sí datos, comunicaciones, computadoras y servidores de archivos. Las LAN están diseñadas para lo siguiente:

- Operar dentro de una zona geográfica limitada.
- Permitir a muchos usuarios acceder a medios de alto ancho de banda.
- Proporcionar conectividad de tiempo completo a los servicios locales.
- Conectar físicamente dispositivos adyacentes.

Redes de área amplia:

WAN es un acrónimo de *Wide Area Network* que en español significa “red de área amplia”. Un ejemplo de este tipo de redes sería la misma Internet o cualquier red en que no esté en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible). Opera en la capa física y de enlace del modelo de referencia OSI. A nivel de alcance, esta red abarca desde unos 100km (País) hasta llegar incluso a 1000km (Continente).

Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes. Las WAN están diseñadas para lo siguiente:

- Operar dentro de una zona geográfica amplia.
- Conectar físicamente dispositivos lejanos.
- Legar a sitios donde las LAN no llegan.
- Están basadas la mayoría de los casos en redes públicas.
- Utilizan elementos de conmutación

Entre algunas de las tecnologías WAN habituales se incluyen:

- Los módems analógicos.
- RDSI o ISDN (Red digital de servicios integrados, *Integrated Services Digital Network*)
- DSL (Línea de abonado digital. *Digital Subscriber Line*).
- Frame Relay.
- ATM (Modo de transferencia asincrona, *Asynchronous Transfer Mode*).
- Las series de portadora T (EEUU) y E (Europa): Tí, El, T3, E3, etc.
- SONET (Red óptica síncrona, *Synchronous Optical Network*): STS-1 (OC-1), STS-3 (OC-3), etc.

ANCHO DE BANDA DIGITAL

El ancho de banda es la medida de cuánta información puede fluir de un lugar a otro en una cantidad de tiempo dada. Bits por segundo es una unidad de ancho de banda. El ancho de banda es un elemento importante de las redes, aunque todavía puede resultar bastante abstracto y difícil de comprender. A continuación hay una analogía que pueden ayudarle a entender lo que es el ancho de banda.

El ancho de banda es como la anchura de una tubería, como se muestra en la Figura 3.4. Piense en la red de tuberías que proporciona agua a su hogar y que saca las aguas residuales del mismo. Estas tuberías tienen diferentes diámetros: la tubería de agua principal de la ciudad puede tener 2 metros de diámetro, mientras que la del grifo de la cocina puede tener 2 centímetros. La anchura de la tubería mide la capacidad de transportar agua de la tubería. En esta analogía, el agua es como la información, y la anchura de la tubería, como el ancho de banda. De hecho, muchos expertos en redes hablan en términos de "colocar tuberías más grandes" refiriéndose a un mayor ancho de banda (más capacidad de transportar información).

Figura 3.4. Cuanto mayor es la tubería, mayor es el promedio de fluido que puede pasar a través de ella.

3.3 MODELO DE REFERENCIA OSI

DESCRIPCIÓN DEL MODELO OSI

El modelo de referencia OSI[1] es la arquitectura de red actual más prominente. El objetivo de éste es el de desarrollar estándares para la interconexión de sistemas abiertos (*Open System Interconnection*, OSI)[2]. El término OSI es el nombre dado a un conjunto de estándares para las comunicaciones entre computadoras, terminales y redes. OSI es un modelo de 7 capas, donde cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI.

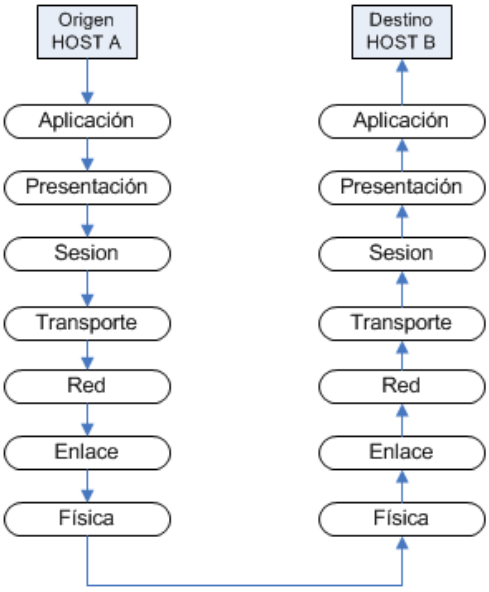

Figura 3.5. Capas del modelo de referencia OSI

CAPA DE APLICACIÓN

Relacionado con las funciones de más alto nivel que proporcionan soporte a las aplicaciones o actividades del sistema. Por ejemplo, control de transferencia de archivos, soporte al operador funciones de dialogo de alto nivel, actividades de bases de datos de alto nivel. Los tres primeros niveles proporcionan una variedad de servicios que son empleados en la sesión de los usuarios, a este subconjunto se le denomina subsistema de la sesión de servicios. Se definen una serie de aplicaciones para la comunicación entre distintos sistemas, las cuales gestionan:

- Transferencia de archivos (FTP).
- Intercambio de mensajes (correo electrónico).
- Login remoto (rlogin, telnet).
- Acceso a bases de datos, etc.

[1] http://www.iso.org
[2] http://www.fuac.edu.co/autonoma/servicios/estudiantes/tele/Osi/osi.html#aplica

CAPA DE PRESENTACIÓN.

Sus funciones están relacionadas con el conjunto de caracteres o códigos de datos que son usados, o la manera como van a ser presentados en pantalla o como van a ser impresos, cuando un conjunto de caracteres llega a una pantalla, se dan ciertas acciones para una presentación buena de la información. Esta capa también tiene que ver con el conjunto de caracteres que debe presentar una edición de datos, salto de línea, colocación de datos en columnas, adición de encabezados fijos para las columnas etc. En esta capa se realizan las siguientes funciones:

- Se da formato a la información para visualizarla o imprimirla.
- Se interpretan los códigos que estén en los datos (conversión de código).
- Se gestiona la encriptación de datos.
- Se realiza la compresión de datos.
- Establece una sintaxis y semántica de la información transmitida.
- Se define la estructura de los datos a transmitir (por ejemplo, define los campos de un registro: nombre, dirección, teléfono, etc.).
- Define el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc).
- Compresión de datos.
- Criptografía.

CAPA DE SESIÓN.

Estandariza el proceso de establecimiento y terminación de una sesión, si por algún motivo esta sesión falla este restaura la sesión sin perdida de datos o si esto no es posible termina la sesión de una manera ordenada chequeando y recuperando todas sus funciones. Establece las reglas o protocolos para el dialogo entre maquinas y así poder regular quien habla y por cuanto tiempo o si hablan en forma alterna es decir las reglas del dialogo que son acordadas. Provee mecanismos para organizar y estructurar diálogos entre procesos de aplicación. Actúa como un elemento moderador capaz de coordinar y controlar el intercambio de los datos. Controla la integridad y el flujo de los datos en ambos sentidos. Algunas de las funciones que realiza son las siguientes:

- Establecimiento de la conexión de sesión.
- Intercambio de datos.
- Liberación de la conexión de sesión.
- Sincronización de la sesión.
- Administración de la sesión.
- Permite a usuarios en diferentes máquinas establecer una sesión.
- Una sesión puede ser usada para efectuar un login a un sistema de tiempo compartido remoto, para transferir un archivo entre 2 máquinas, etc.
- Controla el diálogo (quién habla, cuándo, cuánto tiempo, half duplex o full duplex).
- Función de sincronización.

CAPA DE TRANSPORTE

Controla la interacción entre procesos usuarios, incluye controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones, controla el flujo de transacciones y direccionamiento de maquinas a procesos de usuario. Esta capa asegura que se reciban todos los datos y en el orden adecuado. Realiza un control de extremo a extremo. Algunas de las funciones realizadas son:

- Acepta los datos del nivel de sesión, fragmentándolos en unidades más pequeñas en caso necesario y los pasa al nivel de red.
- Multiplexaje.
- Regula el control de flujo del tráfico de extremo a extremo.
- Reconoce los paquetes duplicados.
- Establece conexiones punto a punto sin errores para el envío de mensajes.

- Permite multiplexar una conexión punto a punto entre diferentes procesos del usuario (puntos extremos de una conexión).
- Provee la función de difusión de mensajes (Broadcast) a múltiples destinos.

CAPA DE RED

Relaciona los circuitos virtuales, estos circuitos son imaginarios y aunque no existen Figuran e interactúan con los niveles mas altos y dan la impresión de existencia en este nivel están los procedimientos de interfaces estándar para el circuito virtual y los mecanismos complejos de operación están ocultos a los niveles mas altos de software tanto como sea posible. En esta capa se determina el establecimiento de la ruta.

- Esta capa mira las direcciones del paquete para determinar los métodos de conmutación y enrutamiento.
- Realiza control de congestión.
- Divide los mensajes de la capa de transporte en paquetes y los ensambla al final.
- Utiliza el nivel de enlace para el envío de paquetes: un paquete es encapsulado en una trama.
- Enrutamiento de paquetes.
- Envía los paquetes de nodo a nodo usando ya sea un circuito virtual o como Datagramas.

CAPA DE ENLACE DE DATOS

Este nivel se relaciona con el envío de bloque de datos sobre una comunicación física, determina el principio y el fin de un bloque de datos transmitido, detecta errores de transmisión, controla muchas maquinas que comparten un circuito físico para que sus transmisiones no sufran mezclas, envía un mensaje a una maquina entre varias.

- Detección y control de errores (mediante el empleo del CRC).
- Control de secuencia.
- Control de flujo.
- Control de enlace lógico.
- Control de acceso al medio.
- Sincronización de la trama.
- Estructura el flujo de bits bajo un formato predefinido llamado trama.
- Para formar una trama, el nivel de enlace agrega una secuencia especial de bits al principio y al final del flujo inicial de bits.
- Transfiere tramas de una forma confiable libre de errores (utiliza reconocimientos y retransmisión de tramas).
- Provee control de flujo.

CAPA FÍSICA.

Relaciona la agrupación de circuitos físicos a través de los cuales los bits son movidos y que encierran las características físicas, eléctricas funcionales y procedimientos, para el envío y recepción de bits.

- Define las características físicas (componentes y conectores mecánicos).
- Define las características eléctricas (niveles de tensión).
- Define las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmisión de flujo de bits a través del medio. No existe estructura alguna.
- Especifica cables, conectores y componentes de interfaz con el medio de transmisión.

3.4 MEDIOS DE TRANSMISIÓN.

DEFINICIÓN

Un medio de transmisión es el camino físico a través del cual se transmite la señal de información, cuando se establece una comunicación entre el emisor y el receptor**.**

CABLE COAXIAL

Es un tipo de cable[3] que consiste de un alambre central rodeado por una malla de alambre, separados ambos por un aislante. La malla está usualmente conectada a un sistema de tierras, y su función principal es minimizar la interferencia eléctrica y de radiofrecuencia.

Figura 3.6. Cable Coaxial

- Este cable, aunque es más caro que el par trenzado, se puede utilizar a más larga distancia, con velocidades de transmisión superiores, menos interferencias y permite conectar más estaciones de trabajo.
- Se suele utilizar para televisión, telefonía a larga distancia, redes de área local, conexión de periféricos a corta distancia, etc.
- Se utiliza para transmitir señales analógicas o digitales.
- Sus inconvenientes principales son: atenuación, ruido térmico, ruido de intermodulación.
- Para señales analógicas, se necesita un amplificador cada pocos kilómetros y para señales digitales un repetidor cada kilómetro.

CABLE PAR TRENZADO

El par trenzado[4] consiste en alambre de cobre ordinario que es enroscado para reducir la inducción electromagnética. Cada alambre tiene su propio aislante. Dado que es común el requerimiento de más de un par trenzado para comunicar dispositivos, es usual que muchos pares sean construidos dentro de un mismo cable. La implementación más común en redes de datos es la llamada UTP (*Unshield Twisted Pair*), que consiste de cuatro pares trenzados con una impedancia de 100 ohms. Otra implementación es la STP (*Shielded Twisted Pair*) de una impedancia de 150 ohms. Cuando son varios los pares que vienen en un solo cable, éstos son identificados por un código de color.

Existen categorías en el UTP. Cada categoría especifica unas características eléctricas para el cable: atenuación, capacidad de la línea e impedancia. Existen actualmente 8 categorías dentro del cable UTP:

- Categoría 1: Este tipo de cable esta especialmente diseñado para redes telefónicas, es el típico cable empleado para teléfonos por las compañías telefónicas. Alcanzan como máximo velocidades de hasta 4 Mbps.
- Categoría 2: De características idénticas al cable de categoría 1.

[3] http://iio.ens.uabc.mx/~jmilanez/escolar/redes/05010000.html
[4] http://www.prodigyweb.net.mx/fjrangelc/default_archivos/Page680.htm

- Categoría 3: Es utilizado en redes de ordenadores de hasta 16 Mbps. de velocidad y con un ancho de banda de hasta 16 Mhz.
- Categoría 4: Esta definido para redes de ordenadores tipo anillo como Token Ring con un ancho de banda de hasta 20 Mhz y con una velocidad de 20 Mbps.
- Categoría 5: Es un estándar dentro de las comunicaciones en redes LAN. Es capaz de soportar comunicaciones de hasta 100 Mbps. con un ancho de banda de hasta 100 Mhz. Este tipo de cable es de 8 hilos, es decir cuatro pares trenzados.
- Categoría 5e: Es una categoría 5 mejorada. Minimiza la atenuación y las interferencias. Esta categoría no tiene estandarizadas las normas aunque si esta diferenciada por los diferentes organismos.
- Categoría 6: No esta estandarizada aunque ya se está utilizando. Se definirán sus características para un ancho de banda de 250 Mhz.
- Categoría 7: No esta definida y mucho menos estandarizada. Se definirá para un ancho de banda de 600 Mhz. El gran inconveniente de esta categoría es el tipo de conector seleccionado que es un RJ-45 de 1 pines.

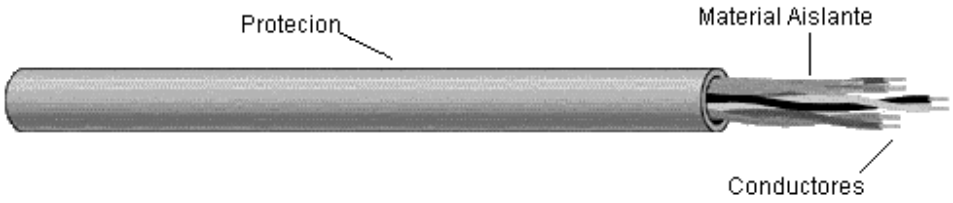

Figura 3.7. Cable Trenzado

- Es el medio guiado más barato y más usado.
- La utilización del trenzado tiende a disminuir la interferencia electromagnética.
- Este tipo de medio es el más utilizado debido a su bajo coste (se utiliza mucho en telefonía) pero su inconveniente principal es su poca velocidad de transmisión y su corta distancia de alcance.
- Con estos cables, se pueden transmitir señales analógicas o digitales.
- Es un medio muy susceptible a ruido y a interferencias. Para evitar estos problemas se suele trenzar el cable con distintos pasos de torsión y se suele recubrir con una malla externa para evitar las interferencias externas.

FIBRA ÓPTICA.

La fibra óptica[5] consiste de un material transparente que varía su nivel de refracción conforme se aleja de la misma. Esta variación de la refracción del rayo de luz es tal que el rayo que incide dentro de un cierto ángulo viajará por la misma sin pérdidas teóricas. Según los modos de implementación de la fibra óptica para la propagación de luz dentro de ellas, se tienen dos tipos: multi-modo y mono-modo. Para su uso y protección la fibra es cubierta por amortiguadores, aislantes, mallas y en ocasiones con gel.

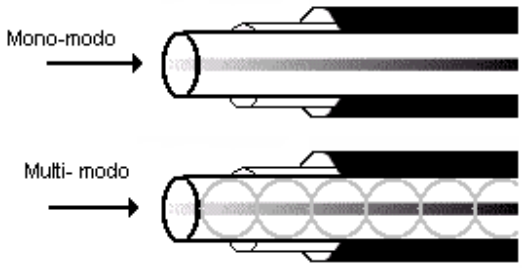

Figura 3.8. Fibra Óptica

[5] http://orbita.starmedia.com/ygalarza/Ciencia.html

- Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica
- El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo. Alrededor de este conglomerado está la cubierta (constituida de material plástico o similar) que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad, etc.
- Es un medio muy apropiado para largas distancias e incluso últimamente para LAN.
- Permite mayor ancho de banda que el cable coaxial.
- Menor tamaño, peso.
- Menor atenuación.
- Aislamiento electromagnético.
- Mayor separación entre repetidores.
- Su rango de frecuencias es todo el espectro visible y parte del infrarrojo.

ENLACES SATELITALES

Consiste en un haz de microondas colimado, es decir un haz con rayos paralelos, sobre el cual se modulan los datos y se transmite al satélite desde la superficie terrestre (Enlace). Este haz se recibe y retransmite a los destinos previamente determinados mediante un circuito a bordo del satélite denominado transponder, que consiste en la unión de un transmisor y un receptor. Cada satélite tiene muchos transpondedores, cada uno de los cuales cubre una banda de frecuencias determinada. Un canal de satélite representativo tiene un ancho de banda muy alto y puede enlazar centenas de datos con alta tasa de bits usando multiplexación.

- El satélite recibe las señales y las amplifica o retransmite en la dirección adecuada.
- Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario.
- Se suele utilizar este sistema para: Difusión de televisión, Transmisión telefónica a larga distancia. Redes privadas.
- El rango de frecuencias para la recepción del satélite debe ser diferente del rango al que este emite, para que no haya interferencias entre las señales que ascienden y las que descienden.
- Debido a que la señal tarda un pequeño intervalo de tiempo desde que sale del emisor en la Tierra hasta que es devuelta al receptor o receptores, ha de tenerse cuidado con el control de errores y de flujo de la señal.
- Las microondas son unidireccionales y las ondas de radio omnidireccionales.
- Las microondas son más sensibles a la atenuación producida por la lluvia.

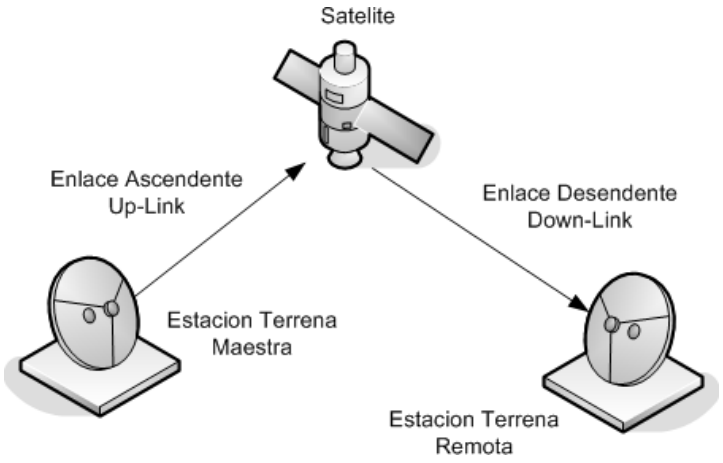

Figura 3.9. Enlace Satelital

MICROONDAS.

La transmisión de microondas se lleva a cabo en una escala de frecuencias comprendida entre los 2 y los 40 Ghz. Para este tipo de frecuencias es necesario que las antenas emisora y receptora no tengan obstáculos entre ellas, lo que obliga a utilizar antenas repetidoras cuyo espaciamiento está determinado por la distancia entre los extremos a comunicarse y por una zona elíptica que se debe mantener libre de obstáculos llamada zona de Fresnel en honor a su descubridor.

En la actualidad se están comercializando redes locales cuyas estaciones están enlazadas entre sí por ondas de radio, empleando una sección del espectro electromagnético como son las frecuencias de 18 Ghz, obteniéndose rendimientos superiores a los que ofrecen tecnologías que utilizan cables coaxiales para interconectar la red.

Se suelen utilizar en sustitución del cable coaxial o las fibras ópticas ya que se necesitan menos repetidores y amplificadores, aunque se necesitan antenas alineadas. Se usan para transmisión de televisión y voz. La principal causa de pérdidas es la atenuación debido a que las pérdidas aumentan con el cuadrado de la distancia (con cable coaxial y par trenzado son logarítmicas). La atenuación aumenta con las lluvias. Las interferencias es otro inconveniente de las microondas ya que al proliferar estos sistemas, pude haber más solapamientos de señales.

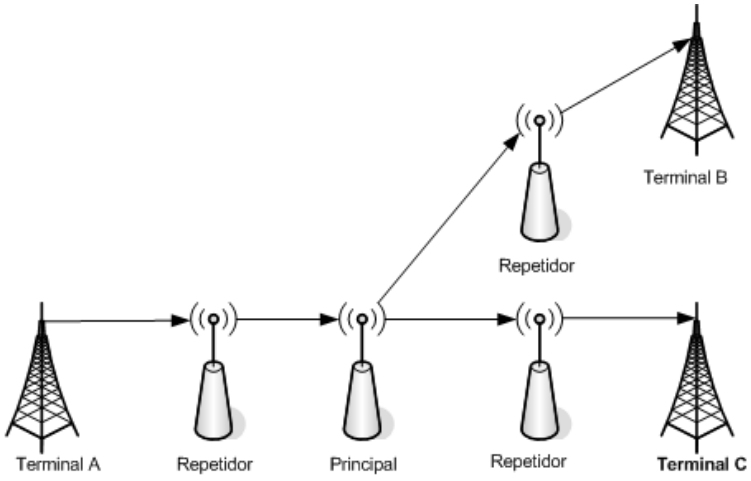

Figura 3.10. Enlace De Microondas

INFRARROJOS

Los emisores y receptores de infrarrojos deben estar alineados o bien estar en línea tras la posible reflexión de rayo en superficies como las paredes. En infrarrojos no existen problemas de seguridad ni de interferencias ya que estos rayos no pueden atravesar los objetos (paredes por ejemplo). Tampoco es necesario permiso para su utilización (en microondas y ondas de radio si es necesario un permiso para asignar una frecuencia de uso).

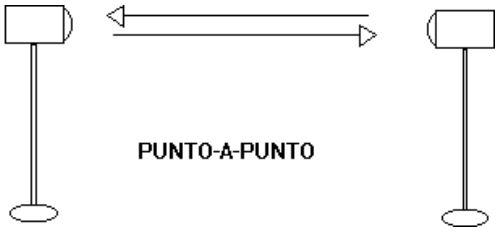

Figura 3.11 Comunicación infrarroja

3.5 REDES DE ÁREA LOCAL

INTRODUCCIÓN A LAS REDES DE ÁREA LOCAL

Aunque enviar datos a cada dispositivo de una red podría funcionar en una red relativamente pequeña, es fácil suponer que cuanto mayor sea la red, más tráfico tendrá. Esto puede ser un gran problema, porque sólo se puede enviar un paquete de datos por el cable cada vez. Si sólo hay un cable interconectado entre cada dispositivo de red, el flujo de datos de dicha red disminuirá considerablemente. Los dispositivos de red son productos que se emplean para conectar redes. Al igual que las redes de computación crecen en tamaño y complejidad, lo hacen también los dispositivos que se utilizan para conectarlas. Los dispositivos de red pueden controlar la cantidad de tráfico de una red y pueden acelerar su flujo de datos.

TOPOLOGÍA

La topología define la estructura de la red. Su definición contiene dos partes: la topología física, que es el diseño real del cableado (medios), y la topología lógica, que define cómo los equipos acceden a los medios. La topología física que se usa normalmente es en bus, en anillo, en estrella, en estrella extendida, jerárquica y en malla (véase la Figura 3.12).

Las topologías físicas que se utilizan con mayor frecuencia son:

- Bus: Emplea un único segmento, al que se conectan directamente todos los Equipos.
- Anillo: Conecta un equipo al siguiente, y el último equipo al primero. Así se crea un anillo físico de cable.
- Estrella: Conecta todos los cables a un punto central de concentración. Este punto normalmente es un concentrador o un conmutador.
- Estrella extendida: Emplea la topología en estrella. Enlaza estrellas individuales enlazando sus concentradores / conmutadores. Así, se extiende la longitud y el tamaño de la red.
- Jerárquica: Similar a la topología en estrella extendida, pero en lugar de enlazar los concentradores / conmutadores, cada sistema secundario, se enlaza a una computadora principal que controla el tráfico de la topología.
- Malla: Se emplea cuando no puede haber ninguna ruptura en la comunicación como, por ejemplo, en los sistemas de control de una central nuclear. Como puede observar en la Figura 3.12, con una topología en malla, cada equipo tiene sus propias conexiones con todos los demás equipos. Una malla parcial refleja el diseño de Internet, Que tiene varias rutas para una ubicación, aunque no dispone, de una conexión entre cada equipo y el resto de los equipos.

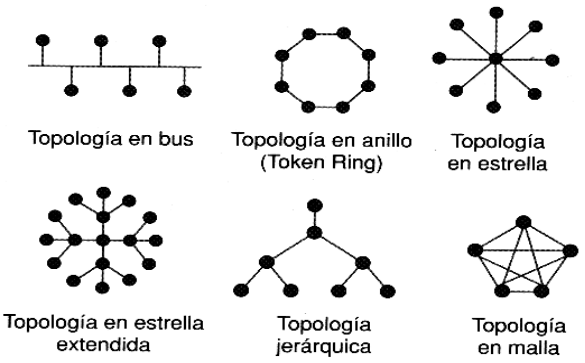

Figura 3.12 El diseño físico, que describe cómo se construye una LAN: se denomina topología.

MEDIOS UTILIZADOS EN LAS LAN

Los símbolos para los medios[6] son diferentes, como se puede ver en la Figura 3.13. Por ejemplo, el símbolo de Ethernet es normalmente una línea recta con líneas perpendiculares que se proyectan a partir de ella. El símbolo de una red Token Ring es un círculo con equipos conectados, y el símbolo de FDDI (*Fiber Distributed Data Interface*) son dos círculos concéntricos con dispositivos conectados.

Figura 3.13. El medio de red es el medio por el que viajan las señales de un dispositivo de red a otro.

Las funciones básicas del medio son transportar un flujo de información, en forma de bits, a través de la LAN. Otros medios de red, como las LAN inalámbricas (emplean la atmósfera o el espacio como medio de transporte),o las LAN cableadas, que encierran las señales de red en cables o fibras. Los medios de red se consideran componentes de Capa 1 de las LAN. Se pueden construir redes de computadoras con diferentes tipos de medios. Cada medio tiene sus ventajas e inconvenientes. Lo que puede ser una ventaja para un medio (costo del cable de categoría 5), puede ser un inconveniente para otro (costo de la fibra óptica). Algunas de las posibles ventajas o desventajas son:

- Costo.
- Facilidad de instalación.
- Longitud máxima del cable.

FUNCIONAMIENTO DE LA TOPOLOGÍA BUS

En una LAN, las estaciones de trabajo deben estar conectadas. Si en la LAN se incluye un servidor de archivos, también se conectará con las estaciones de trabajo. Los medios de red realizan esta conexión (véase la Figura 3.14).

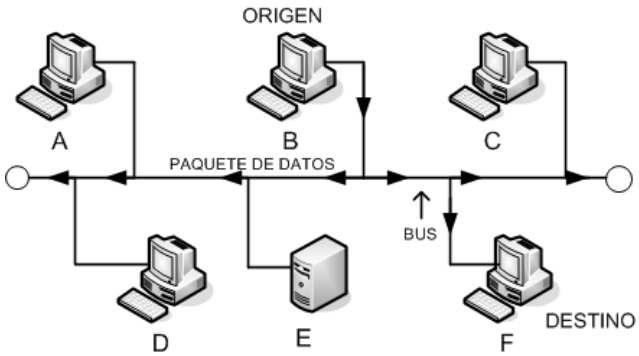

Figura 3.14 La topología bus es típica en las LAN Ethernet, como 10Base2 y 10Base5.

La topología bus es aquella en la que todos los dispositivos de la LAN se conectan a un medio de red lineal. A este medio de red lineal también se le conoce como línea troncal o bus. Cada dispositivo, como una estación de trabajo o un servidor, se conecta independientemente a un cable de bus mediante algún tipo de conexión.

[6] Cisco System, Inc. "Academia de Networking de Cisco System, Guía del primer año". 2 ed.. Pearson Education. S.A. Madrid 2002. Pag. 79

TRANSMISIÓN DE SEÑALES SOBRE LA TOPOLOGÍA BUS

Como se muestra en la Figura 3.14, las señales viajan en ambas direcciones desde el origen cuando se transmiten los datos sobre los medios de red en una topología en bus. Estas señales están disponibles para todos los dispositivos de la LAN. Cada dispositivo verifica los datos mientras pasan. Si la dirección MAC de destino que es transportada por los datos no coincide con la del dispositivo, éste ignorará los datos. Sin embargo, si coincide, el dispositivo copia los datos y los pasa al enlace de datos y a las capas de red del modelo de referencia OSI. Como puede ver en la Figura 3.15, cada extremo del cable tiene un terminador. Cuando una señal alcanza el extremo del bus, es absorbida por el terminador. Esto previene que las señales reboten y sean recibidas de nuevo en las estaciones de trabajo que estén conectadas al bus. Para asegurarse de que sólo un puesto de trabajo transmite cada vez, la topología en bus emplea la detección por colisión, de forma que, si más de un nodo intenta transmitir al mismo tiempo, se produce una colisión.

REPETIDORES

Como hemos mencionado en la sección "Medios", existen diferentes tipos de medios, y cada uno tiene sus ventajas y desventajas. Una de las desventajas del tipo de cable que se usa principalmente, el CAT5 UTP, es la longitud del mismo. La longitud máxima para un cable UTP en una red es de 100 metros. Si necesita extender la red más allá de este límite, deberá añadir un dispositivo a la red. Dicho dispositivo se llama repetidor[7]. Al igual que los medios de red, los repetidores son dispositivos de red que existen en la Capa 1, la capa física, del modelo de referencia OSI. El propósito del repetidor es regenerar y reenviar las señales de red a nivel de bits para hacer posible que éstas viajen largas distancias por los medios.

PASARELA

Una pasarela o *gateway* es un dispositivo, con frecuencia un ordenador, que realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Por ejemplo, un *gateway* de correo electrónico, o de mensajes, convierte mensajes entre dos diferentes protocolos de mensajes.

CONCENTRADORES

En general, el término concentrador[8] se emplea en lugar de repetidor cuando se refiere al dispositivo que sirve como centro de la red. Aunque un concentrador opera en una topología física en estrella, crea el mismo entorno de contención que un bus. Esto se debe a que cuando un dispositivo transmite, el resto de dispositivos le escuchan y la contención crea un bus lógico. Los concentradores se consideran dispositivos de capa 1 porque sólo regeneran la señal y la repiten en todos los puntos (conexiones de red).

PUENTES

Un puente[9] es un dispositivo de capa 2 diseñado para crear dos o más segmentos LAN, cada uno de ellos con un dominio de colisión separado. O sea, han sido creados para crear un ancho de banda más utilizable. El propósito de un puente es filtrar el tráfico de la LAN, para mantener el tráfico local, permitiendo la conectividad con otras partes (segmentos) de la LAN para el tráfico que se dirige allí. Se preguntará cómo diferencia el puente el tráfico local del que no lo es. La respuesta es la misma que da el servicio postal cuando se le hace la misma pregunta. Comprueban si la dirección es local. Cada dispositivo de red tiene una dirección MAC única en la NIC. El puente controla qué direcciones MAC tiene en cada lado, y toma sus decisiones basándose en la lista de direcciones MAC.

---

[7] Cisco System, Inc. “Academia de Networking de Cisco System, Guía del primer año”. 2 ed.. Pearson Education. S.A. Madrid 2002. Pag. 81
[8] Ídem. Psg. 83
[9] Ídem. Pag 87

Los puentes filtran el tráfico de red fijándose sólo en las direcciones MAC. Por tanto, pueden enviar rápidamente tráfico representando cualquier protocolo de capa de red. La Figura 3.15 muestra un ejemplo de cómo se utiliza un puente, muestra el símbolo del puente, que recuerda a un puente colgante. Tradicionalmente, el término puente hace referencia a un dispositivo que sólo tiene dos puertos. Sin embargo, también se pueden ver referencias a puentes con tres o más puertos.

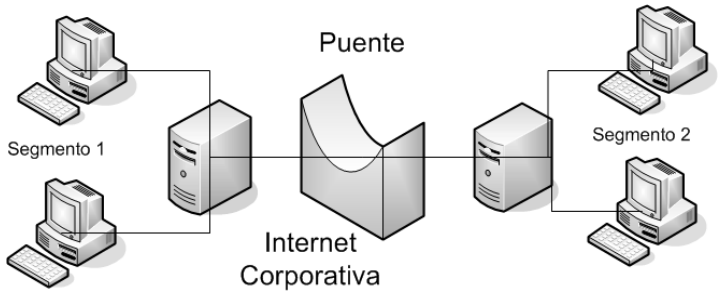

Figura 3.15. Los puentes operan en la capa 2, la capa de enlace de datos, del modelo de referencia OSI; no necesitan examinar la información de la capa superior.

CONMUTADORES DE DATOS

Un conmutador[10], es un dispositivo de capa 2. De hecho, al conmutador a veces se le llama puente multipuerto, igual que al concentrador se le llama repetidor multipuerto. Los Conmutadores toman decisiones basándose en las direcciones MAC y los concentradores, sencillamente, no toman decisiones. Gracias a las decisiones que toman los conmutadores, las LAN son mucho más eficientes. Lo consiguen "conmutando" los datos fuera del puerto al que el propio equipo está conectado. Por su parte, un concentrador envía los datos a todos sus puertos para que todos los equipos tengan que ver y procesar (aceptar o rechazar) todos los datos. La Figura 3.16 muestra el símbolo de un conmutador. Las flechas de la parte superior representan los datos de rutas separadas que puede haber en un conmutador, a diferencia de un concentrador, donde los datos fluyen en todas las rutas.

Figura 3.16. Los conmutadores de capa 2 son dispositivos que funcionan en la capa de enlace de datos del modelo OSI.

El propósito de un conmutador es concentrar la conectividad mientras crea una transmisión de datos más eficiente. Por ahora, piense que un conmutador es algo que combina la conectividad de un concentrador con la regulación del tráfico de un puente en cada puerto. Conmuta las tramas de los puertos entrantes (interfaces) a los puertos salientes mientras proporciona a cada puerto un ancho de banda completo (la velocidad de transmisión de datos en el *Backbone* de la red).

ENRUTADORES

El enrutador[11] es el principal dispositivo con el que se trabaja cuando se está en la capa de red OSI, también conocida como capa 3. Trabajar en la capa 3 permite al enrutador tomar decisiones basándose en las direcciones de red, al contrario de las direcciones MAC individuales de la capa 2. Los enrutadores también pueden conectar diferentes tecnologías de capa 2, como *Ethernet, Token Ring y FDDI*. Sin embargo, debido a su capacidad de enrutar paquetes en base a la información de la capa 3, los enrutadores se han convertido en el *Backbone* de Internet, ejecutando el protocolo IP.

[10] Cisco System, Inc. “Academia de Networking de Cisco System, Guía del primer año”. 2 ed.. Pearson Education. S.A. Madrid 2002. Pag. 90
[11] Ídem. Pag. 92

El propósito de un enrutador es examinar los paquetes entrantes (datos de la capa 3), elegir la mejor ruta para ellos a través de la red, y después, conmutarlos al mejor puerto de salida. Los enrutadores son el dispositivo regulador de tráfico más importante en las redes grandes. Permiten que cualquier tipo de computadora se comunique con otra en cualquier parte del mundo. Mientras ejecutan estas funciones básicas, también pueden efectuar muchas otras tareas. Los enrutadores usan un esquema de direcciones diferente al de la capa 3 para tomar las decisiones de envío. Utilizan direcciones de capa de red, también llamadas Protocolo Internet (IP), o direcciones lógicas, en lugar de las direcciones MAC. Los enrutadores equiparan la información de la Tabla de enrutamiento con las direcciones IP de destino de los datos, y envían los datos entrantes hacia la subred y el equipo correctos. Como las direcciones IP se implementan en el software y hacen referencia a la red en la que está ubicado el dispositivo, a veces las direcciones de capa 3 se llaman direcciones de protocolo o direcciones de red. Las direcciones físicas, o MAC, normalmente las asigna el fabricante de la NIC y están codificadas en el interior de dicha NIC. Por otro lado, las direcciones de capa de red, o direcciones IP, las asigna normalmente el administrador de la red.

El símbolo de un enrutador, mostrado en la Figura 3.17, sugiere sus dos propósitos principales: selección de rutas y conmutación de paquetes a la que sea mejor. Un enrutador puede tener muchos tipos diferentes de puertos de interfaz.

Figura 3.17. El símbolo del enrutador (observe las flechas entrantes y salientes).

SEGMENTOS DE RED

El término segmento tiene muchos significados en el mundo de las redes. La definición correcta depende de la situación en la que se emplee. Históricamente, un segmento identifica un medio de capa 1, que es la ruta común para la transmisión de datos en una LAN. Como hemos mencionado anteriormente en la sección "Medios de transmisión", existe una longitud máxima para la transmisión de datos en cada tipo de medio. Cada vez que se usa un dispositivo electrónico para aumentar la longitud, o para manipular datos en el medio, se crea un nuevo segmento físico (véase la Figura 3.18). Una segunda definición, usada actualmente, define un segmento como un dominio de colisión.

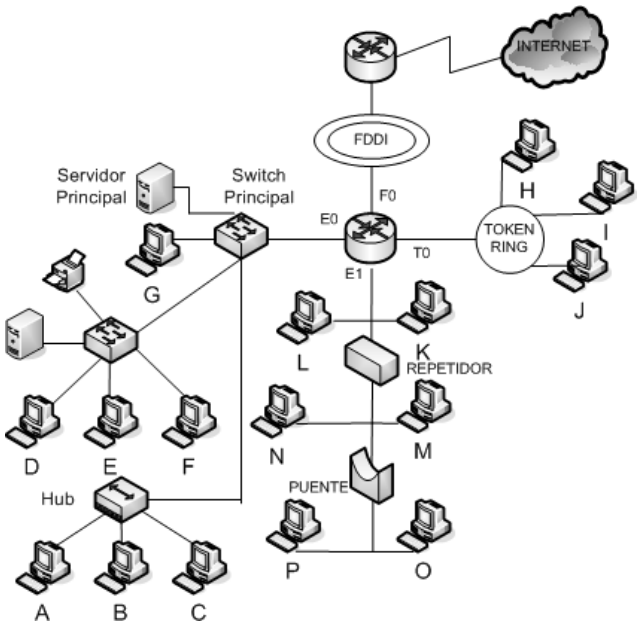

Figura 3.18. Una red puede estar compuesta por varios segmentos conectados por dispositivos de red.

3.6 ENRUTAMIENTO Y DIRECCIONAMIENTO.

IMPORTANCIA DE LA CAPA DE RED

La capa de red[12] es la responsable de la navegación de los datos a través de una red y su función es la de encontrar la mejor ruta para moverse por dicha red. Los dispositivos utilizan el esquema de direccionamiento de la capa de red para determinar el destino de los datos mientras éstos se mueven a través de la red. La capa de red define la forma de transportar el tráfico entre los dispositivos que no están conectados localmente. Se utilizan dos piezas de información para conseguir esto:

- Direcciones lógicas asociadas con las estaciones de origen y de destino.
- Rutas a través de la red para alcanzar los destinos deseados.

La capa de red mueve los datos a través de un grupo de redes (*Internetwork*). El esquema de direccionamiento de la capa de red es utilizado por los dispositivos para determinar el destino de los datos mientras se mueven a través de las redes. Como se muestra en la Figura 3.19, sin los servicios de la capa de red, el equipo B no podría determinar dónde está el equipo A.

Para determinar qué redes forman una *Internetwork* y dónde están los dispositivos en el contexto de esas redes, se utilizan esquemas lógicos de direccionamiento. Estos esquemas varían según el protocolo de capa de red que se utilice. Los protocolos que sí disponen de capa de red utilizan un esquema de direccionamiento jerárquico que permite direcciones únicas dentro de los límites de la red, además de un método para encontrar una ruta para que los datos viajen entre las redes. Las direcciones MAC utilizan un esquema de direccionamiento plano que hace difícil localizar los dispositivos en otras redes. El direccionamiento jerárquico, por otro lado, no sólo permite que la información fluya a través de una *Internetwork*, sino que también proporciona un medio eficiente de hacerlo.

Un requisito para llevar a cabo el *Internetworking* es tener una arquitectura de direcciones eficiente a la que estén adheridos todos los usuarios de esa *Internetwork*. Las arquitecturas de direcciones pueden tener formas distintas. Las direcciones de red siempre son numéricas, pero se pueden expresar en base 2 (binaria), base 10 (decimal), o incluso base 16 (hexadecimal). Las arquitecturas pueden ser altamente escalables o diseñadas para servir a pequeñas comunidades de usuarios.

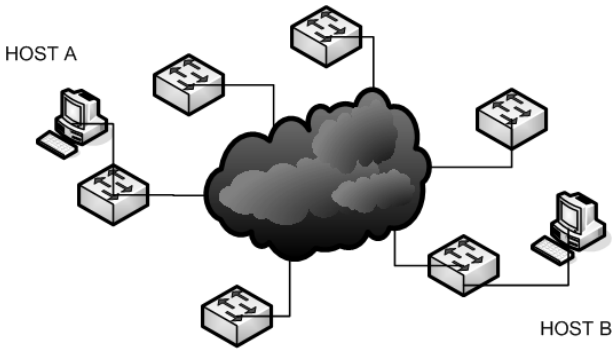

Figura 3.19 La única forma de que el equipo B alcance el equipo A es utilizando un esquema de direccionamiento.

[12] Cisco System, Inc. “Academia de Networking de Cisco System, Guía del primer año”. 2 ed.. Pearson Education. S.A. Madrid 2002. Pag. 347

SEGMENTACIÓN Y SISTEMAS AUTÓNOMOS

Hay dos factores principales que afectan a la escalabilidad de una red: el crecimiento de cada red y el crecimiento del número de redes. Cuando una LAN, MAN o WAN crece, puede que sea necesario, o conveniente, dividirla en partes más pequeñas, llamadas segmentos de red. Esto da como resultado que la red se convierta en un grupo de redes, que requieren cada una direcciones separadas.

Una analogía que le puede ayudar a entender la necesidad de segmentar una red es imaginar un sistema de autopistas y el número de vehículos que la utilizan, como se muestra en la Figura 3.20. A medida que aumenta la población en las zonas que rodean la autopista, las carreteras se cargan con demasiados vehículos. Las redes funcionan de la misma forma. A medida que las redes crecen, la cantidad de tráfico crece. Una solución es aumentar el ancho de banda; esto es análogo, o añadir carriles a la autopista. Otra solución puede ser utilizar dispositivos que segmenten la red y controlen el flujo de tráfico, de la misma forma que los semáforos controlan el flujo de vehículos en una calle.

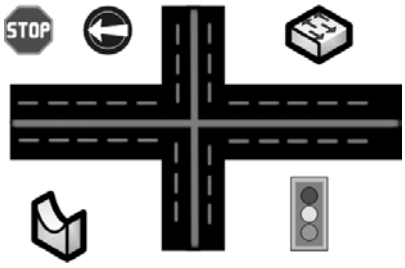

Figura 3.20. Los dispositivos de red controlan el flujo al igual que lo hacen los semáforos y la capa de red es la responsable de las decisiones relacionadas con la ruta a tomar.

DISPOSITIVOS DE RED DE CAPA 3 Y DETERMINACIÓN DE LA RUTA

Los enrutadores son dispositivos de *Internetworking* que funcionan en la capa de red del modelo OSI. Unen, o interconectan, segmentos de red, o redes enteras, como se muestra en la Figura 3.21 Pasan paquetes de datos entre redes basándose en la información de la capa 3.

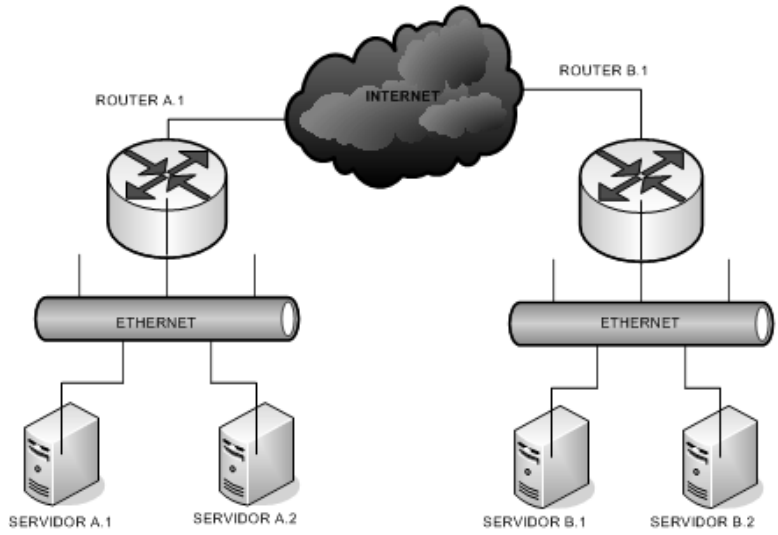

Figura 3.21 El direccionamiento único permite la comunicación entre estaciones finales

Los enrutadores toman decisiones lógicas teniendo en cuenta la mejor ruta para el envío de los datos en una *Internetwork*; estas decisiones se implementan enviando los paquetes a los puertos de salida y a los segmentos asociados apropiados. Los enrutadores toman los paquetes de los dispositivos de la LAN y, basándose en la información de la capa 3, los envían a través de la red.

La conexión de un enrutador a una LAN, o a una WAN, habitualmente se llama interfase, pero también se llama puerto. Cuando un enrutador es de enrutamiento IP, cada LAN o WAN a la que está conectado debe tener una única dirección IP de red, o de subred, asignada. La interfaz del enrutador debe tener una dirección IP de equipo válida para que la subred se conecte. En la mayoría de los casos, un enrutador sólo puede tener una conexión a cada subred individual.

La determinación de ruta sucede en la capa de red. Permite que un enrutador evalúe las rutas disponibles a un destino para establecer la mejor forma de gestionar un paquete. Los servicios de enrutamiento utilizan la información de la topología de red para evaluar las rutas de red (véase la Figura 3.22). La determinación de esta ruta es el proceso que desarrolla un enrutador para seleccionar el siguiente salto hacia el destino último de un paquete. Este proceso también se llama enrutamiento del paquete.

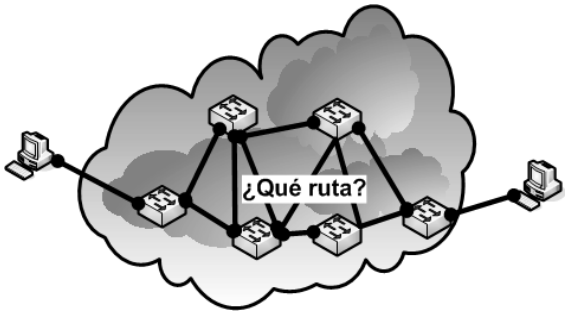

Figura 3.22. La función de determinación de ruta permite que un enrutador evalúe las rutas disponibles a un destino para gestionar lo mejor posible un paquete.

DIRECCIONAMIENTO DE LA CAPA DE RED

Una dirección de red ayuda al enrutador a identificar la ruta dentro de la nube de la red. El enrutador utiliza la dirección de red para identificar la red de destino de un paquete dentro de una *Internetwork*. Además de la dirección de red, los protocolos de red utilizan alguna forma de dirección de equipo, o nodo. Para algunos protocolos de capa de red, un administrador de red asigna direcciones de equipo de acuerdo a algún plan de direccionamiento de red predeterminado. Para otros, dicha asignación es parcial, o completamente dinámica (o automática). La Figura 3.23 muestra tres dispositivos en la Red 1 (dos equipos y un enrutador), cada uno con su propia dirección de equipo única (la Figura también muestra que el enrutador está conectado a otras dos redes, la 2 y la 3).

RED	EQUIPO
1	1, 2, 3
2	1
3	1

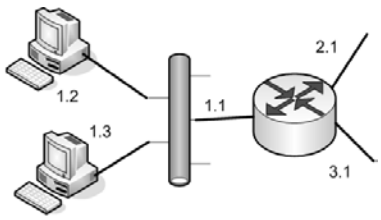

Figura 3.23. Una dirección de red se compone de una parte que corresponde a la red y una parte que corresponde al equipo.

Sin el direccionamiento de la capa de red, no puede tener lugar el enrutamiento. Los enrutadores necesitan direcciones de red para asegurar la correcta entrega de los paquetes. Sin una estructura de direccionamiento jerárquica, los paquetes no podrían viajar a través de una *Internetwork*.[13]

Una dirección IP se puede representar por un número binario de 32 bits escrito como cuatro octetos, como se muestra en la Tabla 3.1.

Octeto (8 bits)	Octeto (8 bits)	Octeto (8 bits)	Octeto (8 bits)
$2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$	$2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$	$2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$	$2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$
11000000	00000101	00100010	00001011
IGUAL			
192	5	34	11

Tabla 3.1 Las direcciones IP se pueden expresar como números binarios compuestos por unos y ceros.

Una empresa u organización puede recibir tres clases[14] de direcciones IP por parte del ARIN, RIPE NCC, APNIC, o el ISP de la organización (véase la Figura 3.24):

Clase A	**N**	**H**	**H**	**H**	De 0.0.0.0 a 127.255.255.255
Clase B	**N**	**N**	**N**	**H**	De 128.0.0.0 a 191.255.255.255
Clase C	**N**	**N**	**N**	**H**	De 192.0.0.0 a 223.255.255.255
Clase D	Para múltiples difusiones				De 224.0.0.0 a 239.255.255.255
Clase E	Para investigación				De 240.0.0.0 a 247.255.255.255

H	= Número de equipo asignado por el administrador de la red
N	= Número de red asignado por ARIN, RIPE NCC o APNIC

Tabla 3.2. El ARIN asigna las tres clases de direcciones IP.

FUNDAMENTOS DE SUBNETING

La jerarquía original de dos niveles de Internet suponía que cada sitio sólo tendría una red, por lo que sólo necesitaría una única conexión a Internet. Inicialmente, éstas eran suposiciones seguras. Sin embargo, con el tiempo, la computación en red maduró y se expandió. A medida que los sitios *web* comenzaron a desarrollar múltiples redes, se hizo obvio que se necesitaban algunos mecanismos para diferenciar entre las múltiples redes lógicas que estaban emergiendo como subconjuntos del segundo nivel de Internet. De no ser así, no podría haber una forma eficiente de enrutar datos a sistemas finales específicos en *webs* con múltiples redes.

Una respuesta a este problema fue dar a cada red lógica, o subred, su propio rango de direcciones IP. Por esto los administradores de redes necesitan a veces dividir las redes, especialmente las grandes, en otras más pequeñas. Estas divisiones se llaman *subnetworks* y proporcionan flexibilidad de direccionamiento. Habitualmente, las redes lógicas se conocen simplemente como subredes. El concepto de *subnetting* se basa en la necesidad de un tercer nivel en la jerarquía de direccionamiento de Internet.

En tales entornos de múltiples redes, cada subred se conectaba a Internet mediante un punto común: un enrutador (véase la Figura 3.24). Los detalles propios del entorno de la red interna son intrascendentes para Internet. Lo decisivo en una red privada es que sea capaz de enviar sus propios paquetes de datos. Por tanto, Internet sólo debe interesarse por cómo conectar con el enrutador de *gateway* de esa red. Dentro de la red privada, la parte de equipo de la dirección IP se puede subdividir para crear subredes.

[13] Cisco System, Inc. "Academia de Networking de Cisco System, Guía del primer año". 2 ed.. Pearson Education. S.A. Madrid 2002. Pag. 356
[14] Ídem. Pag. 359

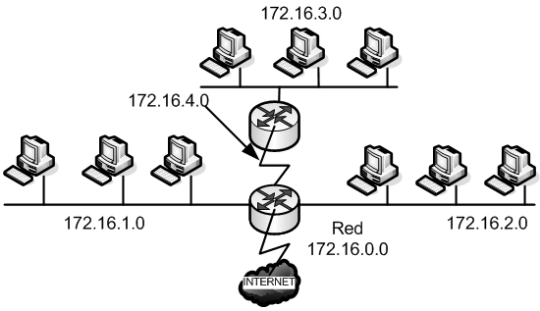

Figura 3.24. Cuatro subredes forman la red 172.16.0.0.

Las direcciones de subred incluyen la parte de red de clase A, B o C, además de un campo subred y un campo equipo, los cuales se crean a partir de la parte de equipo original para toda la red. La capacidad de decidir cómo dividir la parte de equipo original en estos nuevos campos proporciona flexibilidad de direccionamiento al administrador de la red. Para crear una dirección de subred, un administrador toma prestados bits de la parte de equipo original y los designa como el campo subred. El número mínimo de bits que se pueden tomar prestados es de dos.

La máscara de subred no es una dirección aunque determina qué parte de una dirección IP es el campo de red y cuál es el campo de equipo. Las máscaras de subred utilizan el mismo formato que las direcciones IP. En otras palabras, cada una tiene una longitud de 32 bits y se divide en cuatro octetos. Las máscaras de subred sólo tienen unos en su parte de red y de subred, y sólo ceros en la parte de equipo. Por defecto, si no se toman bits prestados, la máscara de subred para una red de clase B es 255.255.0.0. En caso contrario, si se tomaran prestados 8 bits, la máscara de subred para la misma red de clase B sería 255.255.255.0, como se muestra en las Figura 3.25. Sin embargo, como hay dos octetos en el campo equipo de una red de clase B, se pueden tomar prestados hasta 14 bits para crear subredes. Una red de clase C sólo tiene un octeto en el campo equipo. Por tanto, sólo se pueden tomar prestados hasta 6 bits en estas redes para crear subredes.

	Red		Equipo	
Dirección IP	172	16	0	0
	Red		Equipo	
Mascara de subred predeterminada	255	255	0	0
	Red		Subred	Equipo
Mascara de subred de 8 bits	255	255	255	0

Utilizar los bits de la parte de Equipo, empezando por la posición de bit de orden superior

Figura 3.25. Si toma prestados bits para una máscara de subred, utilice los de la parte de equipo empezando por la posición del bit de orden superior.

Por defecto, si no toma prestado ningún bit, la máscara de subred para una red de clase B sería 255.255.0.0, que es el equivalente decimal con puntos de todo unos en los 16 bits correspondientes al número de red de clase B y ceros en los otros 16 bits. Si se tomaran prestados 8 bits para el campo subred, la máscara de subred incluiría 8 bits a uno adicionales y sería 255.255.255.0. Por ejemplo, si la máscara de red 255.255.255.0 estuviera asociada con la dirección de clase B 130.5.2.144 (se han tomado prestados 8 bits para crear subredes), el enrutador sabría cómo enrutar este paquete a la subred 130.5.2.0 en lugar de sólo a la red 130.5.0.0 (véase la Figura 3.26).

	Red	Sub red	Equipo
130.5.0.0	10000010 00000101	00000000	00000000
255.255.255.0	11111111 11111111	11111111	00000000
	Prefijo de red extendido (máscara de subred)		

Figura 3.26. Ejemplo de máscara de subred.

Una de las decisiones que se deben tomar al crear subredes es determinar el número óptimo de subredes y equipos (véase la Figura 3.27).

Número de bits prestados	Número de subredes creadas	Número de equipos por subred	Número total de equipos	Porcentaje utilizado
2	2	62	124	49%
3	6	30	180	71%
4	14	14	196	77%
5	30	6	180	71%
6	62	2	124	49%

Figura 3.27. El número de direcciones IP perdidas en una red de clase C depende del número de bits que se toman prestados para el proceso de *subnetting*.

Cuando se crean subredes, se pierden bastantes direcciones potenciales. Por esta razón, los administradores de redes deben prestar mucha atención al porcentaje de direcciones que pierden al crear subredes.

DIRECCIONES PRIVADAS

Ciertas direcciones de cada clase de direcciones IP no se asignan. Estas direcciones se llaman direcciones privadas (véase la Figura 3.28). Las direcciones privadas pueden ser utilizadas por todos los equipos que empleen la conversión de direcciones de red (NAT, *Network Address Translation*) o un servidor Proxy para conectarse a Internet, o por equipos que no se conecten en absoluto a Internet.

Los siguientes rangos están disponibles para direccionamiento privado

10.0.0.8- 10.255.255.255

172.16.0.0-172.31.255.255

192.168.0.0 -192.168.255.255

Figura 3.28 Espacio de direcciones privado.

Las direcciones privadas se pueden utilizar junto con un servidor de conversión de direcciones de red (NAT). Se necesita un servidor NAT o un servidor Proxy para proporcionar conectividad a todos los equipos de una red que tenga relativamente pocas direcciones públicas disponibles. Por acuerdo, cualquier tráfico con una dirección de destino dentro de uno de los rangos de direcciones privadas no se enrutará en Internet.

3.7 PROYECTO ESTRUCTURADO DE CABLEADO.

ESTÁNDAR DE SISTEMAS DE CABLEADO ESTRUCTURADO. (EIA/TIA 568A).

A principios de 1985, las compañías representantes de las industrias de telecomunicaciones y computación se preocupaban por la falta de un estándar para sistemas de cableado de edificio de telecomunicaciones. La Asociación de la Industria de Comunicaciones Computacionales (CCIA) solicitó que la Asociación de Industrias Electrónicas (EIA) desarrollara este modelo necesario. En julio de 1991 se publicó la primera versión del estándar como EIA/TIA-568. En agosto del mismo año se publicó un Boletín de Sistemas Técnicos TSB-36 con especificaciones para grados mayores (Cat 4, Cat 5) de UTP. En agosto de 1992 el TSB-40 fue publicado, enfocándose a grados mayores de equipos conectores de UTP. En enero de 1994 el TSB-40 fue corregido por el TSB-40A que trataba, más detalladamente, sobre los cables de conexión provisional UTP y esclarecía los requerimientos de prueba de los conductores hembra modulares UTP. El modelo 568 fue corregido por el EIA/TIA 568-A. El TSB-36 y el TSB-40A fueron absorbidos en el contenido de este modelo revisado, junto con otras modificaciones.

Propósito del estándar EIA/TIA 568-A[15]:

- Establecer un cableado estándar genérico de telecomunicaciones que respaldará un ambiente multiproveedor.
- Permitir la planeación e instalación de un sistema de cableado estructurado para construcciones comerciales.
- Establecer un criterio de ejecución y técnico para varias configuraciones de sistemas de cableado.

Actualmente ISO está desarrollando un cableado estándar sobre una base internacional, con el titulo: Cableado Genérico para Cableado de Establecimientos Comerciales ISO/IEC11801

Campo del estándar EIA/TIA 568-A

El estándar especifica:

- Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente de oficina.
- Topología y distancias recomendadas.
- Parámetros de medios de comunicación que determinan el rendimiento.
- Disposiciones de conexión y sujeción para asegurarla interconexión.
- La vida productiva de los sistemas de telecomunicaciones por cable por más de 10 años.

Los seis subsistemas de un sistema de cableado estructurado

1. Entrada de construcción

La instalación de entrada del edificio da el punto en donde el cableado exterior entra en contacto con el cableado central interior del edificio. Los requerimientos físicos del contacto de le red son definidos en el Estándar EIA/TIA-569.

2. Sala de Equipo

Los aspectos de diseño de la sala de equipo se especifican en el estándar EIA/TIA-569. Las salas de equipo, generalmente alojan componentes de mayor complejidad que el clóset de telecomunicaciones. Cualquier o todas las funciones de un cuarto de telecomunicaciones pueden estar disponibles en una sala de equipo.

[15] Francisco Jose Molina Robles. " Redes de área local" Alfa Omega RA-MA, 2004. Pag. 441

3. Cableado Central

El cableado central provee la interconexión entre los cuartos de telecomunicaciones, salas de equipo e instalaciones de entrada. Consiste en los cables centrales, interconexiones intermedias y principales, terminaciones mecánicas y cables de parcheo o puentes, utilizados para interconexiones de central a central. Esto incluye;

- Conexión vertical entre pisos.
- Cables entre la sala de equipo y las instalaciones de entrada del cableado del edificio.
- Cableado entre edificios.

4. Cuarto de Telecomunicaciones

Un armario de telecomunicaciones es el área de un edificio que aloja el equipo del sistema de cableado de telecomunicaciones. Este incluye las terminaciones mecánicas y / o interconexiones para el sistema de cableado central y horizontal.

5. Cableado Horizontal

El sistema de cableado horizontal se extiende desde la toma de corriente de telecomunicaciones (información) del área de trabajo hasta el armario de telecomunicaciones y consiste en lo siguiente:

- Cableado Horizontal.
- Salida de Telecomunicaciones.
- Terminaciones de Cable.
- Interconexiones.

6. Área de Trabajo

Los componentes del área de trabajo se extienden desde la salida de información hasta el equipo de estación. El cableado del área de trabajo está diseñado de manera que sea sencillo el interconectarse, para que los cambios, aumentos y movimientos se puedan manejar fácilmente.

1. Entrada del Edificio.
2. Sala de Equipo.
3. Cableado Central.
4. Cuarto de Telecomunicaciones.
5. Cableado Horizontal.
6. Área de Trabajo.

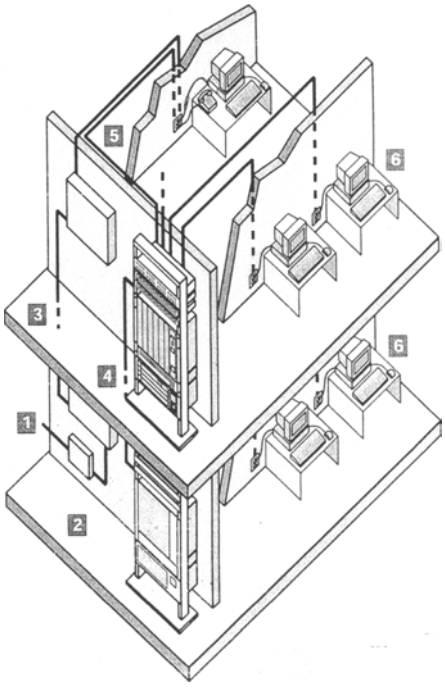

Figura.3.29 Los seis subsistemas de un sistema de cableado estructurado

ESTÁNDAR DE RUTAS Y ESPACIOS DE TELECOMUNICACIONES PARA EDIFICIOS COMERCIALES (EIA/TIA 569).

La propuesta de EIA/TIA-569[16]

Este estándar reconoce tres conceptos fundamentales relacionados con telecomunicaciones y edificios:

- Los edificios son dinámicos. Durante la existencia de un edificio, las remodelaciones son más la regla que la excepción. Este estándar reconoce, de manera positiva, que el cambio ocurre.
- Los sistemas de telecomunicaciones y de medios son dinámicos. Durante la existencia de un edificio, los equipos de telecomunicaciones cambian dramáticamente. Este estándar reconoce este hecho siendo tan independiente como sea posible de proveedores de equipo.
- Telecomunicaciones son más que datos y voz. Telecomunicaciones también incorpora otros sistemas tales como control ambiental, seguridad, audio, televisión, alarmas y sonido. De hecho, telecomunicaciones incorporan todos los sistemas de bajo voltaje que transportan información en los edificios.

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

ESTÁNDAR PARA LA INFRAESTRUCTURA DE TELECOMUNICACIONES (EIA/TIA 606).

La propuesta de EIA/TIA-607[17]

Las modernas construcciones requieren de una efectiva infraestructura de telecomunicaciones, que soporte la amplia variedad de servicios que depende de la electrónica para el transporte de información. La administración incluye documentación básica y temporalmente actualizaciones de esquemas, etiquetas y registros.

La administración puede ser complementada con documentos de registros, pero hoy en día se incrementa la complejidad de los ambientes de telecomunicaciones, la efectiva administración se debe aumenta con el uso de sistemas basados en computadoras.

Un edificio comercial tiene una expectativa de vida de al menos 50 años. Además, en un ambiente multi-usuario, continuos movimientos, agregados y cambios son inevitables. A la administración le toca el guardado de registros y el cada vez más necesario rol de la flexibilidad y dirección de frecuentes movimientos, agregados y cambios. Este estándar describe concientemente la administración del registro de cambios de elementos en las estructuras modernas de sistemas de cableado.

ESTÁNDAR DE TIERRAS FÍSICAS PARA TELECOMUNICACIONES (EIA/TIA 607).

La propuesta de ANSI/TIA/EIA-607[18]

Este estándar especifica un informe para las tierras e uniones en infraestructura de telecomunicaciones que será seguido para edificios comerciales.

El desarrollo en las comunicaciones de voz y datos y su convergencia lleva cada vez más a la compleja interacción de los sistemas en su funcionamiento y mantenimiento por el propio usuario. Estos sistemas requieren de una confiable referencia eléctrica, una buena tierra de referencia. Los accesorios para tierra deben estar muy cerca la pieza del conducto de hierro, por que no podrán satisfacer la referencia de tierra para la actividad de sistemas electrónicos sofisticados.

[16] Francisco Jose Molina Robles. “Redes de área local” Alfa Omega RA-MA, 2004. Pag. 441
[17] http://www.anixter.com
[18] http://www.anixter.com

3.8 ADMINISTRACIÓN DE REDES

LA PARTE ADMINISTRATIVA DE LA ADMINISTRACIÓN DE REDES

La visión de una red es importante. Una red es un conjunto de dispositivos que interactúan entre sí para proporcionar comunicación. Cuando un administrador de red examina una red, debe considerarla como una entidad completa, y no en sus partes individuales. En otras palabras, cada uno de los dispositivos de una red afecta a otros dispositivos y a la red en su conjunto. Como se muestra en la Figura 3.30, nada queda aislado cuando se conecte a una red, no hay nada aislado.

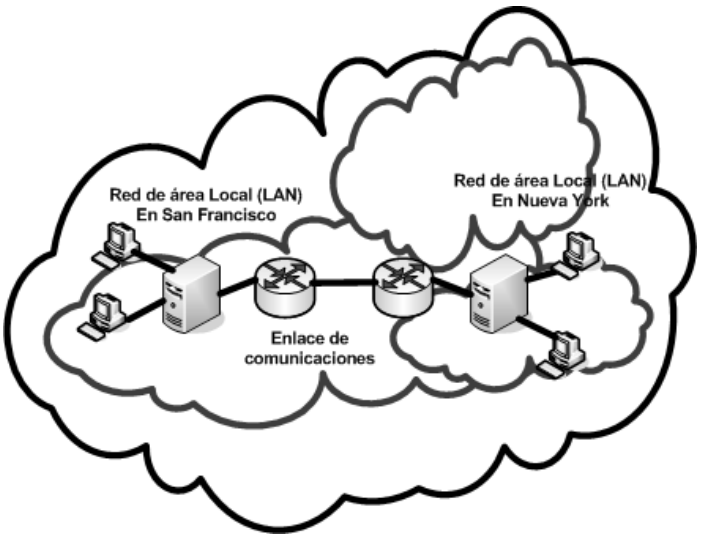

Figura 3.30 Configuración básica de una red.

Lo mismo se puede aplicar a un sistema de red. Si el servidor de red está configurado para funcionar con el protocolo IPX/SPX y los equipos no lo están, no podrán comunicarse. Además, si el sistema funciona bien y el administrador cambia los protocolos en una sola parte, el sistema dejará de funcionar. Un dispositivo afecta al modo de funcionamiento del otro. Otro ejemplo es que haya un servidor DNS ubicado en la dirección IP 192.150.11.123. Todos los Equipos están configurados para encontrar el servidor DNS en esta dirección IP. Si un técnico de redes cambia la dirección IP del servidor DNS sin cambiar los identificadores de equipo, los equipos ya no prestarán servicios DNS.

Lo más importante que hay que tener en cuenta al tratar con una red consiste en verla como una unidad, en vez de cómo un grupo de dispositivos individuales conectados. Esto también se aplica a las conexiones de área amplia que se usan cuando se conecta con Internet. Los cambios que se hagan en los enrutadores de la ubicación afectarán directamente a la eficiencia y fiabilidad de la comunicación a través de la totalidad del sistema.

CÓMO COMPRENDER Y ESTABLECER LOS LÍMITES DE LA RED

En una red de empresa, es importante que los miembros del personal de la red conozcan sus responsabilidades. ¿Es responsabilidad del personal diagnosticar los problemas de escritorio de un usuario o, sencillamente, la de determinar que un problema de usuario no tiene que ver con la comunicación? ¿Se extiende la responsabilidad del usuario únicamente el paramento del cableado horizontal, o también a la totalidad del NIC?

Estas definiciones son importantes para un departamento de redes, ya que afectan al trabajo de cada persona y al costo de los servicios de red de la empresa. Cuanto mayor sea la responsabilidad de un departamento de redes, mayor será el costo de los recursos. Cuando las responsabilidades estén divididas, una red podrá servir más eficientemente. La desventaja, obviamente, es que el costo de los recursos ha aumentado con el crecimiento y la ampliación.

La tarea del mantenimiento de la red puede abarcar todos los aspectos de la red, o se puede centrar a ciertos componentes. Estas responsabilidades tienen que ser definidas y exigidas sobre una base departamento a departamento. La clave para entender esta relación es que la acción de crear un área de responsabilidad muy grande puede limitar los recursos del departamento, pero la acción de hacerla muy pequeña puede ocasionar que sea complicado solucionar con eficacia los problemas de la red.

COSTOS DE UNA RED

La administración de una red abarca muchas responsabilidades, entre las cuales se incluyen el costo y el análisis. Esto implica la determinación no sólo del costo del diseño e implementación de la red, sino también el costo de mantenerla, actualizarla y controlarla. La determinación del costo de una instalación de red no es una tarea especialmente difícil para la mayoría de administradores de redes. Es posible establecer listas de equipamiento y costos; los costos laborales pueden ser calculados por medio de tarifas fijas. Desdichadamente, el costo de construir la red sólo es el comienzo.

Algunos de los demás factores económicos que hay que tener en cuenta son los siguientes:

- El crecimiento de la red con el transcurso del tiempo.
- La formación técnica y de usuario.
- Las reparaciones.
- El despliegue de *software*.

Estos factores económicos son mucho más difíciles de planificar que el costo de construir una red. El administrador de red debe ser capaz de ver las tendencias históricas y de crecimiento de la empresa para proyectar el costo de crecimiento de la red. Un administrador debe examinar el nuevo software y hardware para determinar si la empresa tiene que implementarlos (y cuándo), así como determinar qué formación de personal es necesaria para soportar estas nuevas tecnologías. También hay que añadir el costo del equipamiento de reserva para operaciones vitales al costo del mantenimiento de la red.

DOCUMENTACIÓN DE INFORMES DE ERROR

Una administración de red eficaz requiere una documentación detallada, por lo que cuando se presenten problemas, debe generarse un documento de errores. Este documento se utiliza para reunir la información básica necesaria para identificar y asignar un problema de red, y también proporciona una forma de hacer un seguimiento del progreso y solución final del problema. Los informes de problemas proporcionan una justificación a los administradores para contratar nuevo personal, adquirir nuevo equipo y proporcionar más formación. Esta documentación también proporciona soluciones a problemas recurrentes que ya se han resuelto.

CÓMO CONTROLAR LA RED

Aunque existen muchas razones para controlar la red, las dos razones principales son la de predecir los cambios para el crecimiento futuro y detectar los cambios inesperados en el estado de la red. Los inesperados podrían ser por ejemplo, el fallo de un enrutador o un conmutador, que un pirata estuviera tratando de acceder ilegalmente a la red, o un fallo en el enlace de comunicaciones. Si le falta la capacidad de controlar la red, un administrador sólo podrá reaccionar ante los problemas cuando éstos tengan lugar, en vez de prevenirlos.

CONTROL DE LA CONEXIÓN

Una de las formas más básicas de control de la conexión tiene lugar todos los días en una red. El proceso de inicio de sesión que los usuarios realizan en la red verifica que las conexiones están funcionando correctamente o que el departamento de redes pronto recibirá una llamada. Sin embargo, este no es el método ideal para el control de la conexión. Programas sencillos pueden permitir al administrador acceder a una lista de direcciones IP de equipo, de forma que se hagan *pings* periódicos a estas direcciones. Si se produce un problema en la conexión, el programa alertará al administrador con la salida del *ping*. Esta es una forma muy primitiva e ineficaz de controlar la red, pero es mejor que nada.

Otro aspecto de este tipo de control es que sólo determina que hay una interrupción en las comunicaciones entre la estación de control y el dispositivo de destino. El fallo podría ser un enrutador, conmutador o un segmento de red defectuosos. La prueba de los *pings* sólo indica que la conexión está caída; no indica dónde está el problema.

CONTROL DEL TRÁFICO

El control de tráfico es un método más sofisticado de control de redes. Busca el tráfico de paquetes en la red y genera informes basados en él. Programas como Microsoft Windows NT Network Monitor y Fluke's Network Analyzer constituyen ejemplos de este tipo de software.

Estos programas no sólo detectan los fallos del equipamiento, sino que determinan si un componente está sobrecargado o pobremente configurado La desventaja de este tipo de programas es que normalmente funciona en un solo segmento a la vez; Si es preciso reunir los datos de otros segmentos, el software de control deberá ser trasladado a ese segmento. Puede superar esto con el uso de agentes en los segmentos de red remotos (como se muestra en la Figura 3.31). El equipamiento, como los conmutadores y los enrutadores, puede generar y transmitir estadísticas de tráfico como parte de su sistema operativo. Así, ¿cómo se reúnen y organizan los datos en una ubicación central para que sean útiles a la administración de red? La respuesta es el Protocolo simple de administración de redes (SNMP).

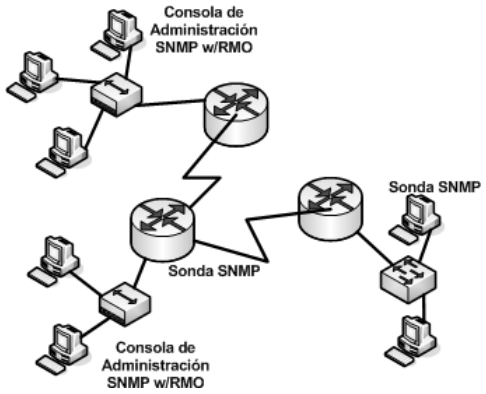

Figura 3.31 Diseño SNMP.

EL PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE REDES

El Protocolo simple de administración de redes (SNMP) es un protocolo que permite a la administración transmitir datos estadísticos por una red a una consola de administración central. SNMP es un componente de la arquitectura de administración de red, que consta de cuatro componentes principales:

- Estación de administración. La interfaz del administrador de red del sistema de red. Dispone de los programas necesarios para manipular los datos y controlar la red. La estación de administración también mantiene la Base de Información de Administración (MIB), que se extrae de los dispositivos sometidos a esta administración.

- Agente de administración. El componente que está en los dispositivos a administrar. Los puentes, los enrutadores, los concentradores y los conmutadores pueden contener agentes SNMP para permitirles ser controlados por la estación de administración.

- Base de información de administración (MIB): Está provista de una estructura de base de datos y reside en cada dispositivo que se administra. La base de datos contiene una serie de objetos, que son datos de recursos reunidos en el dispositivo administrado. Algunas de las categorías de la MIB incluyen los datos de interfaz de puerto, los datos TCP y los datos ICMP.

- Protocolo de administración de red: Se usa como SNMP. SNMP es un protocolo de capa de aplicación que está diseñado para comunicar datos entre la consola de administración y el a gente de administración. Dispone de tres opciones clave: la posibilidad de que la consola de administración recupere (*GET*) datos del agente, la posibilidad de poner (*PUT*) la consola de administración estableciendo valores de objeto en el agente, y la posibilidad de interceptar (*TRAP*) al agente, notificando a la consola de administración los eventos importantes.

Cuando se desarrolló SNMP, se diseñó para ser un sistema a corto plazo que posteriormente sería sustituido. Pero, al igual que TCP/IP, se ha convertido en uno de los estándares principales de las configuraciones de administración para Internet / intranet. Durante los últimos años, se han incorporado mejoras a SNMP con el fin de ampliar sus posibilidades de control y administración. Una de las principales mejoras a SNMP se denomina supervisión remota (RMON). Las extensiones RMON de SNMP le ofrecen la posibilidad de ver la red en su totalidad, en vez de ver los dispositivos individualmente considerados.

SUPERVISIÓN REMOTA

Las sondas reúnen datos remotos en RMON[19]. Una sonda tiene la misma función que un agente SNMP. Una sonda tiene opciones RMON, mientras que un agente no. Cuando se trabaja con RMON, al igual que con SNMP, una consola de administración central es el punto de recogida de datos. Existe una sonda RMON en cada uno de los segmentos de la red controlada. Estas sondas pueden ser equipos dedicados, residentes en un servidor, o bien pueden estar incluidas en un dispositivo de *Networking* estándar, como un enrutador o un conmutador. Estas sondas reúnen los datos especificados de cada segmento y los transmiten a la consola de administración. Las consolas de administración remota proporcionan dos ventajas principales a los procesos de administración de consola En primer lugar la capacidad de que haya más de un administrador de red en diferentes ubicaciones físicas controlando y administrando la misma red. En segundo lugar destaca el concepto de redundancia.

[19] Cisco System, Inc. “Academia de Networking de Cisco System, Guía del segundo año”. 2 ed.. Pearson Education. S.A. Madrid 2003. Pag. 413

La extensión RMON del protocolo SNMP crea nuevas categorías de datos. Estas categorías incorporan más ramas a la base de datos MIB. Cada una de las categorías principales se explica en la siguiente lista:

- El grupo de estadísticas de la Ethernet. Contiene las estadísticas reunidas en cada una de las subredes controladas. El otro tipo de referencia de datos es una Tabla de índices. La Tabla identifica cada dispositivo Ethernet controlado, lo que permite mantener los contadores individuales de cada dispositivo Ethernet.

- El grupo de control del historial. Contiene una Tabla de datos que registra muestras de contadores del grupo de estadísticas de la Ethernet durante un periodo de tiempo concreto. Estas muestras sientan las bases de la red y se pueden usar para compararlas con las bases originales con el fin de resolver problemas o actualizar las bases cuando cambie la red.

- El grupo de alarmas. Emplea límites especificados por el usuario, llamados umbrales. Si los contadores de datos que se están controlando traspasan los umbrales, se enviará un mensaje o una alarma a la persona concreta. Este es un componente a tener en cuenta en la solución de errores preventiva.

- El grupo de Equipos. Contiene contadores que se mantienen por cada equipo que se descubra en el segmento de subred. Algunas de las categorías de contador mantenidas son paquetes, octetos, errores y difusiones. Los tipos de contadores asociados a cada uno de los elementos anteriormente mencionados podrían ser, por ejemplo, el total de paquetes, los paquetes recibidos y los paquetes enviados, junto con muchos contadores específicos de un tipo de elemento.

- El grupo TOP N de equipos. Se emplea para preparar informes sobre un grupo de equipos que están en la parte más alta de una lista basada en un parámetro calculado. La mejor manera de describir este grupo es ejemplificándolo. Se podría generar un informe para los diez primeros equipos que generaran difusiones a lo largo del día. Otro informe podría generarse en la mayoría de paquetes transmitidos durante el día. Esta categoría supone una forma muy sencilla de determinar qué tipo de tráfico de datos ocupa más la subred seleccionada.

- El grupo de matrices. Registra la comunicación de datos entre dos equipos de una subred. Estos datos están almacenados en forma de matriz (una Tabla multidimensional). Uno de los informes que se pueden generar en esta categoría es el equipo que utiliza un servidor.

- El grupo de filtrado. Proporciona una forma de que una consola de administración pueda enseñar a una sonda RMON cómo reunir paquetes seleccionados de una interfaz específica de una subred concreta. Esta selección se basa en el uso de dos filtros, el filtro de datos y el de estado. El filtro de datos está diseñado para cotejar o no cotejar determinados patrones de datos, lo que permite la selección de esos datos concretos. El filtro de estado se basa en el tipo de paquete examinado, como un paquete CRC o un paquete válido. Estos filtros pueden combinarse utilizando “and” u “or” lógicos para crear condiciones muy complicadas. El grupo de filtrado permite al administrador de red examinar selectivamente los distintos tipos de paquetes con el fin de proporcionar un mejor análisis y solución de problemas.

- El grupo de captura da paquetes. Permite al administrador especificar un método para capturar paquetes que hayan sido seleccionados por el grupo de filtrado. Al capturar paquetes especificados, el administrador de red podrá examinar en detalle los paquetes que cumplan con el filtrado básico. El grupo de paquetes también especifica la cantidad de paquetes individuales capturados y el número total de paquetes capturados.

- El grupo de eventos. Contiene eventos generados por otros grupos de la base de datos MIB. Un ejemplo es un contador que exceda el umbral para ese contador especificado en el grupo de alarmas. Esta acción generaría un evento en el grupo de eventos. En base a este evento, se podría generar una acción, como la emisión de un mensaje de alerta a todos los que se enumeren en los parámetros del grupo de alarmas o la creación de una entrada registrada en la Tabla de eventos. Se genera un evento en todas las operaciones de comparación de las extensiones RMON de MIB.

Recuerde que RMON es una extensión del protocolo SNMP. Específicamente, esto significa que aunque RMON mejore las opciones de funcionamiento y control de SNMP, SNMP sigue siendo necesario para que RMON funcione en una red.

CÓMO SOLUCIONAR LOS PROBLEMAS DE LAS REDES

Los problemas siempre se presentan incluso cuando se controla la red, el equipamiento es fiable y los usuarios son cuidadosos. La prueba de fuego de un buen administrador de red es la capacidad de analizar, solucionar problemas y corregir problemas bajo la presión de un fallo de red que origine un tiempo de inactividad de la empresa.

La primera cuestión a la hora de solucionar los problemas de red consiste en usar el diario técnico y tornar notas. Esta acción puede definir un camino apropiado para diagnosticar un problema. Puede ser indicativo de lo que ya ha probado y el efecto que tuvo en el problema. Esto puede resultar extremadamente útil a la hora de solucionar cualquier problema, para que no se repitan los intentos de resolver el problema. Tomar notas también resulta útil si el problema se pasa a otro técnico, ya que evita que esa persona tenga que rehacer todo el trabajo. Es necesario incluir una copia de estas notas con la solución del problema cuando éste ya se haya solucionado. Esto sirve como referencia para problemas similares que se pudieran presentar.

Otro elemento esencial de la solución de problemas preventiva es el etiquetado. Etiquételo todo, incluyendo ambos extremos de un trazado de cable horizontal. Esta etiqueta no sólo debe incluir el número del cable, sino también dónde se encuentra el otro extremo y la utilización del cable. Junto con las etiquetas del cableado, el etiquetado de cada puerto de un concentrador, conmutador o enrutador por ubicación, finalidad y punto de conexión mejora mucho la flexibilidad a la hora de resolver los problemas. Por último, también se deberán etiquetar convenientemente todos los demás componentes que se unan a la red por ubicación y finalidad. Con este tipo de etiquetado, se podrán localizar todos los componentes, y su finalidad en la red se podrá definir con mucha más facilidad. Un correcto etiquetado, junto con la documentación de red creada en el momento de construcción y actualización de la red, proporcionará un cuadro completo de la red, así como de sus relaciones.

Otra cuestión importante es que la documentación sólo es útil si está actualizada. Todos los cambios que se hagan en la red deberán estar documentados con relación a los dispositivos o cables que se hayan cambiado y en la documentación impresa que se emplee para definir la red completa.

El primer paso a la hora de solucionar los problemas de red consiste en definir el problema. Esta definición puede ser una consolidación de muchas fuentes distintas. Uno de los orígenes puede ser un problema o un informe del servicio técnico, que identifica el problema inicialmente. Otra fuente podría ser una conversación telefónica con el usuario en la que se tratara el problema con el fin de reunir más información acerca de él. Las herramientas de control de redes pueden proporcionar una idea más completa acerca del problema específico a resolver. Otros usuarios y sus propias observaciones también suministrarán información. La evaluación de toda esta información ofrece un punto de partida mucho más claro para resolver el problema, en vez de trabajar a partir de cualquier otra fuente.

CAPÍTULO 4

Análisis del caso

4.1 INTRODUCCIÓN

La Facultad de Química requiere implementar servicios de datos para comunicar las instalaciones del conjunto de "Posgrado" ubicado en Ciudad Universitaria, mediante el suministro, instalación, configuración y sintonización de los elementos que integren el diseño propuesto como solución.

La propuesta de solución, considera el suministro, instalación y certificación de un Sistema de Cableado Estructurado Estándar según la normatividad EIA/TIA 568 y 569, así como los equipos activos basados en tecnología *Gigabit Ethernet* y la norma IEEE 802.3, que sean requeridos para la segmentación total de la red de datos.

En este capitulo, se verán los aspectos generales del proyecto de red[1], que se implementará como la solución a las necesidades que presenta la antigua red informática de la Facultad de Química. Se incluyen las especificaciones y requerimientos necesarios para su implementación; además de la distribución de los servicios de datos que en el próximo capitulo servirá como base en la configuración de la red.

4.2 DEFINICIÓN DEL PROYECTO

El proyecto que define la integración de la red informática de la Facultad de Química consiste en las especificaciones necesarias para la infraestructura de la red de datos que dará servicio a los diferentes niveles de los edificios que componen el conjunto Posgrado de la Facultad de Química de la UNAM, ubicada en Cuidad Universitaria en México DF.

En este proyecto la red de datos ha sido diseñada partiendo de la existencia de las salas de equipo, closet y gabinetes principales, los cuales cuentan con el suministro eléctrico necesario, y la correspondiente tierra física. Adicionalmente se cuenta con el enlace a Internet.

La implantación de la solución en su conjunto se sujetará al diseño y requerimientos técnicos especificados por la Facultad de Química, y serán provistos mediante el suministro, instalación, puesta en marcha, configuración y sintonización de los elementos que se establece la conforman.

La red de datos se fundamenta en el estándar ANSI/EIA/TIA 802.3 (*Ethernet*), lo que asegura la interoperabilidad de los equipos de comunicaciones; el cableado estructurado se fundamenta estrictamente bajo los estándares EIA/TIA 568-A 568-B y 569-A. Las adecuaciones de tipo físico y eléctrico se basan en los estándares EIA/TIA 606 y ETI/TIA 607.

[1] M. Julián Javier Robles Rivas. "Proyecto de Integración de la red Informática de la Facultad de Química. 2003

4.3 REQUERIMIENTO EN LOS SERVICIOS DE DATOS

El análisis previo al proyecto de red, requiero el análisis de los servicios necesarios de datos que aseguren el servicio a todos los usuarios para el cual esta proyectado el alcance de la red. La siguiente Tabla muestra la cantidad y la Figura la distribución de estos servicios.

SERVICIOS DE DATOS NECESARIOS
ZONA A 525
ZONA B 688

Tabla 4.1. Cantidad de servicios necesarios

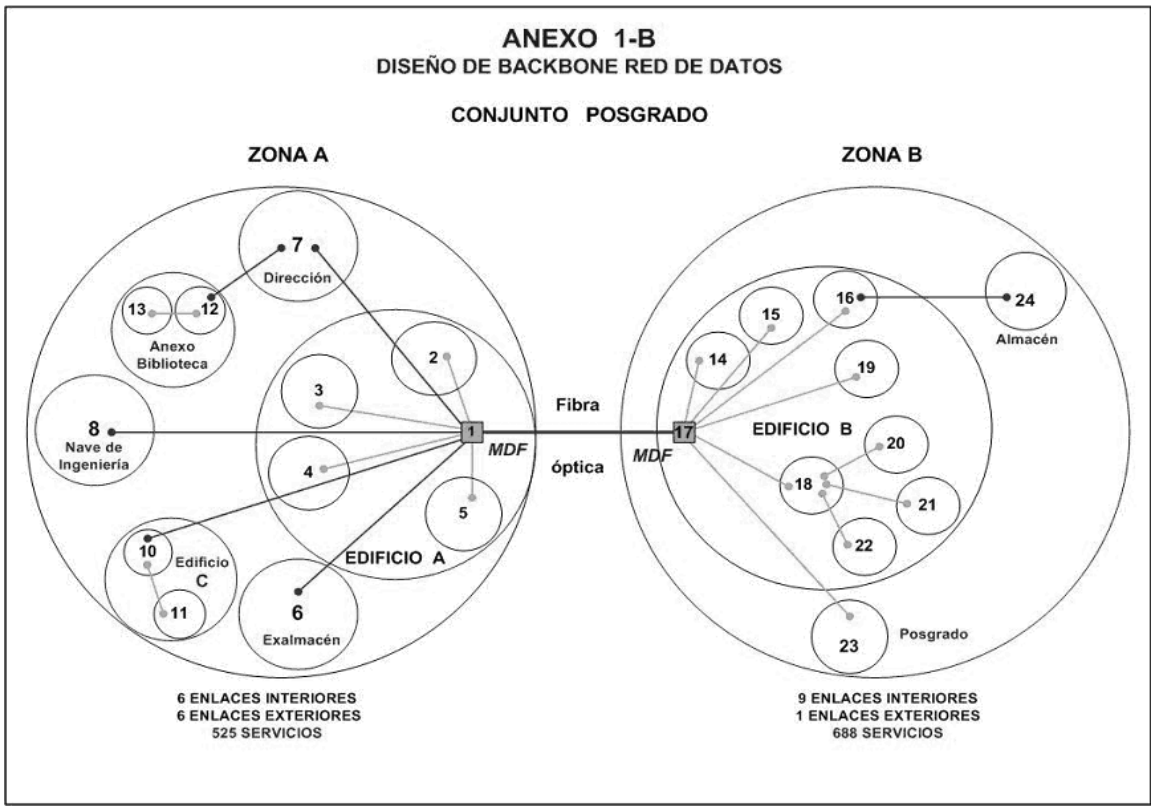

Figura 4.1. Distribución de los servicios de datos por áreas

DESCRIPCIÓN DE LOS SERVICIOS DE DATOS

El servicio de transmisión de datos permitirá la comunicación entre todos los equipos integrados a la red, con un esquema de direccionamiento y enrutamiento propio, independiente de su ubicación física, de la configuración de la red y equipos de conmutación de alto desempeño, y la de los cableados locales. Asimismo, permitirá la comunicación con la red de datos de la UNAM de forma directa.

4.4 ANÁLISIS DE LA INFRAESTRUCTURA DE RED

UBICACIÓN GENERAL DE LAS ÁREAS DE TRABAJO

La Facultad de Química cuenta con varios edificios dentro del Conjunto de Posgrado. Debido a la densidad de la demanda de los servicios de datos proyectados y de acuerdo a la distribución espacial de los edificios, se han definido para este conjunto dos zonas En este proyecto se han referido de la siguiente forma:

DENOMINACIÓN	ZONA	EDIFICIOS
Conjunto Postgrado	Zona A	• Edificio A. • Exalmacen • Dirección-Biblioteca. • Nave de Ingeniería. • Auditorios. • Edifico C. • Anexo de Biblioteca..
	Zona B	• Edificio B. • Postgrado • Almacén

Tabla 4.2. Zonas de distribución de los servicios de Datos

DISEÑO DE LA RED INFORMÁTICA DE LA FACULTAD DE QUÍMICA

Sistema de cableado estructurado

Estará integrado por todos los elementos físicos y mecánicos que forman los cableados para datos, en los seis subsistemas referidos en el estándar EIA/TIA 586-b:

1. De entrada al edificio.
2. Sala de equipo.
3. Cableado central (*Backbone*).
4. Closet de telecomunicaciones.
5. Cableado Horizontal.
6. Área de trabajo.

El cableado de datos permitirá la operación a velocidad *Gigabit Ethernet* en todos y cada uno de los servicios, por lo que todos los componentes serán del tipo CAT 6.

1. Sistema de entrada al edificio

En este proyecto esta conformado por la sala que alberga la acometida de RedUnam. Este se encuentra adecuado al estándar EIA/TIA 569

2. Sala de equipo

Los aspectos físicos del diseño de una sala de equipo se detallan en el estándar EIA/TIA-569. Estas salas alojan componentes de mayor complejidad a los encontrados en un closet de telecomunicaciones. Cualquier función de un cuarto de telecomunicaciones puede estar disponible en una sala de equipo. Este sistema está compuesto por el MDF del edificio A y el MDF del edificio B. Este se encuentra adecuado al estándar EIA/TIA 569

3. Cableado central

Este sistema provee la interconexión entre los clóset de telecomunicaciones, Salas de equipo y el Sistema de entrada al edificio. Consiste en los cables centrales, interconexiones principales e intermedias, terminaciones mecánicas y cables de parcheo o puentes, empleados para interconectar los MDF, CTP y CT.

Incluye:

Cableado de *Backbone*

Para el caso de enlaces entre edificios, las trayectorias considerarán en todo momento los sistemas de registros existentes en las instalaciones del conjunto, cuando las especificaciones técnicas lo permitan, a fin de realizar las menores adecuaciones en este sentido.

Backbone de datos

Estará formado por los equipos de conmutación de datos de alto desempeño y respectivos enlaces agregados de fibra óptica que unen de forma redundante los dos MDF del conjunto de Posgrado. La comunicación entre salas de equipo (MDF-MDF) se integrará mediante un *Backbone Gigabit Ethernet* Full *Duplex* redundante de fibra óptica.

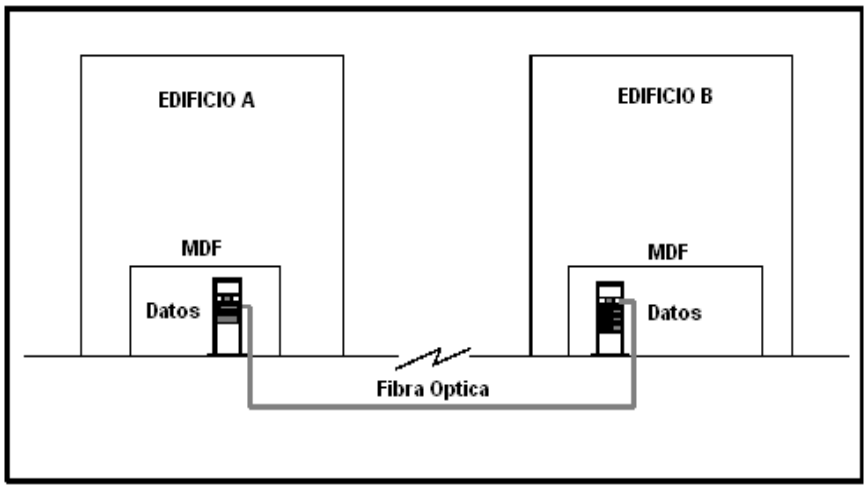

Figura 4.3. Representación del cableado central de datos (*Backbone*)

Cableado entre edificios (Red de comunicación de datos)

Datos

Esta Red está formada por los enlaces de fibra óptica que unen el *Backbone* con los equipos de conmutación en las acometidas de cada edificio, en una topología de estrella, con no más de dos niveles jerárquicos de interconexión desde el *Backbone*.

El enlace será de fibra óptica multimodo del tipo requerido y de tantos hilos como se requiera, y será conducido a través de la infraestructura definida.

El enlace de los MDF hacia las acometidas se los edificios, estará conectado en su totalidad a través de paneles de distribución de fibra óptica y ser montados en el rack correspondiente.

Cableado Vertical (entre pisos)

Este sistema permitirá unir equipo de conmutación principal de cada edifico con los equipos de comunicación departamentales.

Datos

Este cableado esta formado por los enlaces de fibra óptica que unen los CTP con los CT en topología de estrella, con no más de dos niveles jerárquicos de interconexión desde el *Backbone*.

La comunicación entre CTP y CT se realizará empleando fibra óptica para establecer un enlace vertical *Gigabit Ethernet Full Duplex*. El enlace será con fibra óptica multimodo interna de dos hilos, en el número que se requiera para cada CT, la cual será conducida a través de la infraestructura definida.

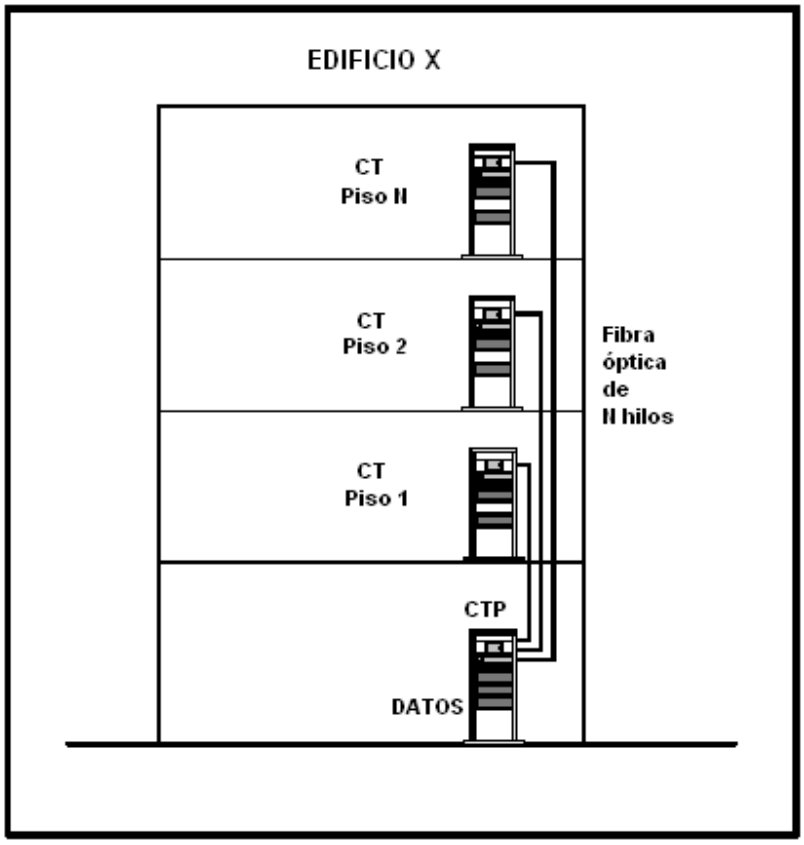

Figura 4.4. Representación del cableado vertical para datos.

4. Cableado horizontal

El sistema de cableado horizontal se extiende desde la salida de telecomunicaciones del área de trabajo, hasta el closet de telecomunicaciones del nivel correspondiente, y consiste en:

- Cableado horizontal.
- Salida de telecomunicaciones.
- Terminación de cables.
- Interconexiones.

Para el caso particular del presente proyecto la solución propuesta incluirá adicionalmente el suministro, instalación, puesta en marcha, configuración y sintonización de los equipos de conmutación locales que sean necesarios, así como el mantenimiento y adecuaciones necesarias para el equipo necesario.

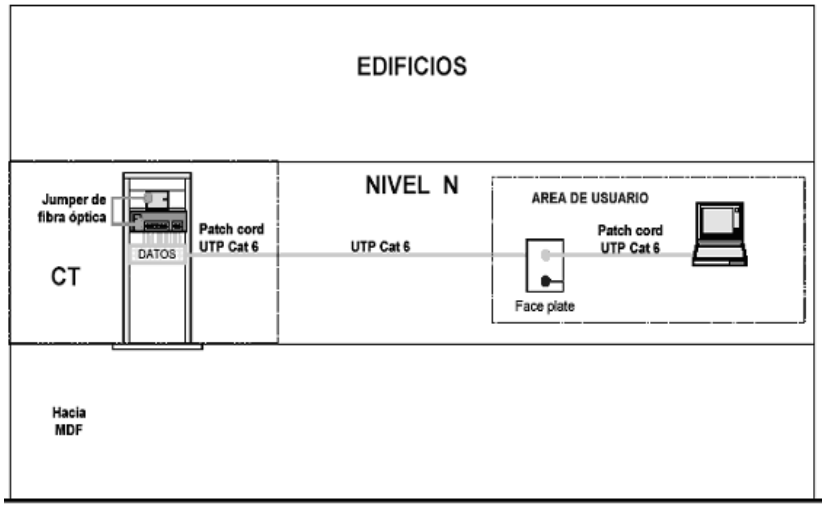

Figura 4.5 Representación del cableado horizontal para datos

5. Cableado del área de trabajo

El área de trabajo se compone de los elementos que van desde la salida de telecomunicaciones (*Face Plates*), hasta la estación de trabajo (DTE).

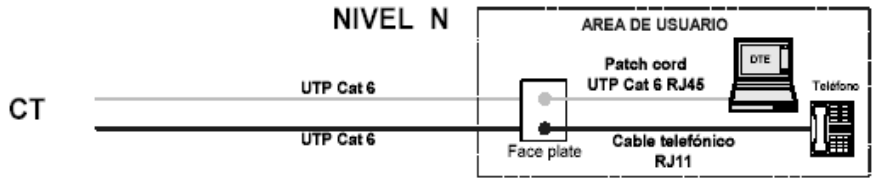

Figura 4.6. Representación del cableado en áreas de trabajo para datos.

6. Closet de telecomunicaciones

Son las áreas dentro de un edificio que alojan el equipo del sistema de cableado estructurado y / o equipos de comunicaciones. Incluirá las terminaciones mecánicas e interconexiones para el sistema de cableado central y horizontal. Dada la complejidad del cableado estructurado, el cableado se distribuirá en los MDF de los edificios A y B.

CAPÍTULO 5

Propuesta del esquema de Administración de red

5.1 INTRODUCCIÓN

En los anteriores capítulos hemos visto la problemática presente en la antigua red de la Facultad de Química, la necesidad del cambio de está para lograr satisfacer las necesidades informáticas de su comunidad, el proyecto presentado como solución a los problemas de la antigua red y los requerimientos y especificaciones para su implementación.

Pero el diseño y la implementación de la red son solo parte de la solución a todas las necesidades que genera la antigua red. Tenemos que saber cómo mantenerla y que funcione a un nivel aceptable. Esto significa que debemos saber como resolver los problemas cuando aparezcan. Además deberemos decidir cuando es necesario expandir o cambiar la configuración de red a fin de reunir las peticiones de modificación.

En este capítulo veremos una propuesta para la configuración de red y la metodología propuesta para su administración. Se establecerán las metas del modelo de administración y las tareas necesarias para conseguir el cumplimiento de estas.

5.2 CONFIGURACIÓN DE RED

INTRODUCCIÓN

En esta sección mostraremos la configuración básica de la nueva red para asegurar una entrega de datos segura. Se presenta el plan de direccionamiento y segmentación de la red y la configuración mínima de los dispositivos de comunicación para su implementación.

SEGMENTACIÓN Y DIRECCIONAMIENTO

Para realizar una eficiente segmentación y direccionamiento de todos los equipos de la red interna, será necesario utilizar una dirección IP privada, que al dividirla sea lo suficientemente grande para dar una dirección IP a todos los equipo que componen la red. Además se de realizar una segmentación, que logre subredes con dimensiones similares.

La segmentación se hará apoyándose en la división de la propia infraestructura de red. Esta infraestructura divide físicamente la red en varios closet de telecomunicaciones, cada closet con una distribución de equipos según su área y la zona donde se encuentra. La segmentación lógica de la red se hará al asignar un número de red por cada closet, ya que estos realizan una segmentación física con similar cantidad de servicios de datos. El direccionamiento deberá ser capaz de abarcar todos los equipos que componen cada subred.

El rango utilizado direcciones privadas será de clase C, esto para tener un margen aceptable de expansión en futuras expansiones de la red. Las direcciones privadas de clase C se muestran en la Tabla 5.1.

	De		Hasta	
Rango de direcciones privadas	192.168.0.0		192.168.255.255	
Mascara de clase C	255	255	255	0

Tabla 5.1. Rango de direcciones privadas clase C

Este rango de direcciones nos permite 254 direcciones IP para dar una dirección a cada equipo, esto por cada dirección red privada de clase C. Así se puede asignar una dirección de red privada de clase C a cada closet de telecomunicaciones, solo si cada closet no supera 254 servicios de datos. En la Tabla 5.2 se presenta la relación de cada closet con la cantidad de servicios de datos que maneja.

NO. DE CLOSET	EDIFICIO	DENOMINACIÓN DEL ÁREA	RED	SERVICIOS DE DATOS
1	A	LABORATORIO DE FÍSICA	1	44
2	A	LABORATORIO 1D	2	29
3	A	LABORATORIO 2D	3	31
4	A	LABORATORIO 3D	4	21
5	A	LABORATORIO 4D	5	34
6	EX ALMACÉN	FÍSICO QUÍMICA	6	29
7	DIR. BIBLIOTECA	DIRECCIÓN	7	58
8	NAVE INGENIERÍA	LABORATORIO	8	29
9	AUDITORIOS	ESTRADO A	9	2
10	C	CENTRO INFORMÁTICA	10	77
11	C	LABORATORIO 105	11	18
12	ANEXO BIBLIOTECA	BIBLIOTECA	12	43
13	ANEXO BIBLIOTECA	SALA DE CURSOS	13	110
14	B	SICA	14	169
15	B	MULTIMEDIA	15	112
16	B	USAI	16	5
17	B	LABORATORIO 101	17	41
18	B	SRIA. ADMINISTRATIVA.	18	65
19	B	LABORATORIO 102	19	13
20	B	LABORATORIO 209	20	25
21	B	LABORATORIO307	21	19
22	B	IDIOMAS	22	12
23	POSTGRADO	COMPUTO	23	224
24	POSTGRADO	ALMACÉN	24	3

Tabla 5.2. Relación de closet de telecomunicaciones
y la cantidad de servicios datos por closet.

La Tabla anterior nos muestra los clóset de telecomunicaciones, con su respectiva ubicación física y la cantidad de servicios de datos que maneja; además se incluye el número de red con que identificaremos a cada closet.

Para mostrar una representación grafica del comportamiento que presenta la densidad de servicios de datos por closet se presenta la Figura 5.1.

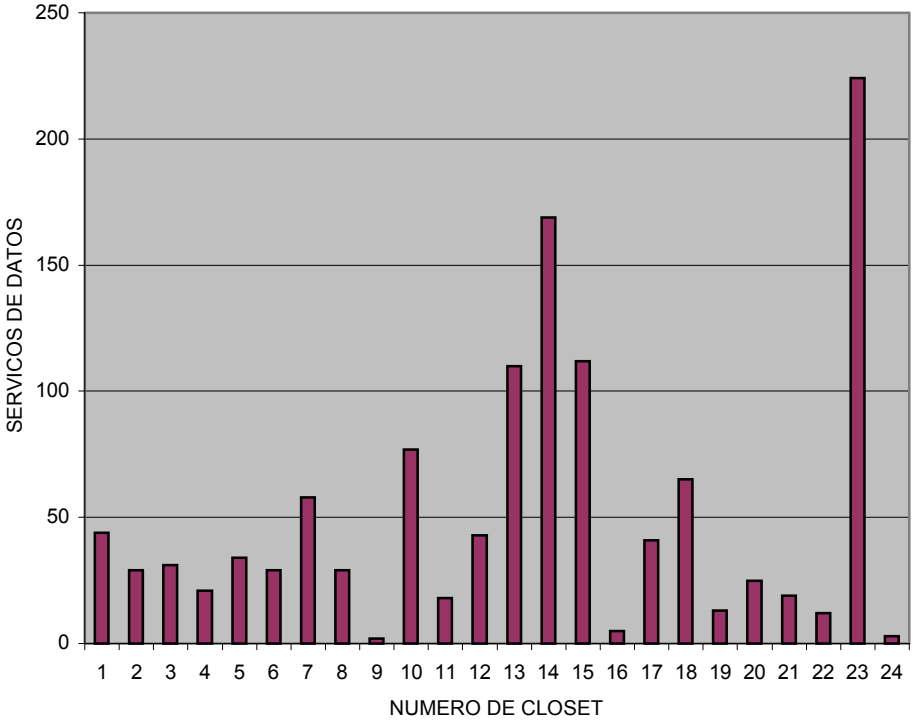

Figura 5.1. Servicios de datos por closet de telecomunicaciones

La grafica anterior nos muestra que hay un closet de telecomunicaciones que se acerca mucho a la cantidad límite de equipo a la que puede asignarle una dirección IP. El constante cambio en las redes puede ayudarnos a saber que, en un futuro, el número de equipo en este closet, pueda llegar a superar los 254 equipos que tenemos como limite.

Para solucionar esto podemos dar dos números de red para este closet. En este closet existen 5 conmutadores de 48 puertos cada uno, esto para poder dar servicios a los 224 equipos que se conectaran a este closet. Tomaremos tres conmutadores para asignar un número de red y a los restantes 2 conmutadores otro. Así los primeros 144 equipos del closet 23 pertenecerán a una red y los restantes 80 equipos estarán asignados a otra.

Para asignar una dirección IP a todos los equipos empezaremos por la red 192.168.1.0. La red 192.168.0.0 la ocuparemos para asignar direcciones a los enlaces y equipos en el *Backbone*.

El plan de direccionamiento propuesto, para la red interna, quedará como se muestra en la Tabla 5.3. En esta Tabla se incluye el closet con su número de red asignado y el rango de direcciones IP útiles en cada subred.

NUMERO DE CLOSET	NUMERO DE RED	EQUIPO		DIRECCIÓN DE BROADCAST
		DESDE	HASTA	
1	192.168.1.0	192.168.1.1	192.168.1.254	192.168.1.255
2	192.168.2.0	192.168.2.1	192.168.2.254	192.168.2.255
3	192.168.3.0	192.168.3.1	192.168.3.254	192.168.3.255
4	192.168.4.0	192.168.4.1	192.168.4.254	192.168.4.255
5	192.168.5.0	192.168.5.1	192.168.5.254	192.168.5.255
6	192.168.6.0	192.168.6.1	192.168.6.254	192.168.6.255
7	192.168.7.0	192.168.7.1	192.168.7.254	192.168.7.255
8	192.168.8.0	192.168.8.1	192.168.8.254	192.168.8.255
9	192.168.9.0	192.168.9.1	192.168.9.254	192.168.9.255
10	192.168.10.0	192.168.10.1	192.168.10.254	192.168.10.255
11	192.168.11.0	192.168.11.1	192.168.11.254	192.168.11.255
12	192.168.12.0	192.168.12.1	192.168.12.254	192.168.12.255
13	192.168.13.0	192.168.13.1	192.168.13.254	192.168.13.255
14	192.168.14.0	192.168.14.1	192.168.14.254	192.168.14.255
15	192.168.15.0	192.168.15.1	192.168.15.254	192.168.15.255
16	192.168.16.0	192.168.16.1	192.168.16.254	192.168.16.255
17	192.168.17.0	192.168.17.1	192.168.17.254	192.168.17.255
18	192.168.18.0	192.168.18.1	192.168.18.254	192.168.18.255
19	192.168.19.0	192.168.19.1	192.168.19.254	192.168.19.255
20	192.168.20.0	192.168.20.1	192.168.20.254	192.168.20.255
21	192.168.21.0	192.168.21.1	192.168.21.254	192.168.21.255
22	192.168.22.0	192.168.22.1	192.168.22.254	192.168.22.255
23	192.168.23.0	192.168.23.1	192.168.23.254	192.168.23.255
23	192.168.24.0	192.168.24.1	192.168.24.254	192.168.24.255
24	192.168.25.0	192.168.25.1	192.168.25.254	192.168.25.255

Tabla 5.3. Plan de Direccionamiento para la red interna.

De las subredes anteriores reservaremos las primeras 200 direcciones IP para direccionamiento de los equipos y las restantes 54 para impresoras, servidores o cualquier otro dispositivo que necesite una dirección IP para trabajar dentro de cada subred. La Tabla 5.4 muestra el rango de direcciones IP para los diferentes dispositivos que se conecten a cada closet.

	De	Hasta
Direcciones de equipo en cada subred	X.X.X.1	X.X.X.200
Direcciones de otros dispositivos en cada subred	X.X.X.201	X.X.X.254

Tabla 5.4 Direcciones IP para los diferentes dispositivos en la red

Las direcciones IP que habrá que reservar para los conmutadores con fines de administración, esto por que los sistemas de administración necesitan acceder a los equipos por medio de una dirección IP valida, serán tomadas de las primeras direcciones del “rango de direcciones de otros dispositivos para cada red”. Así las direcciones IP asignadas a cada conmutador se muestran en la Tabla 5.5.

CLOSET	CONMU-TADORES	RANGO IP		CLOSET	CONMU-TADORES	RANGO IP	
		DESDE	HASTA			DESDE	HASTA
1	1	192.168.1.201	192.168.1.201	14	4	192.168.14.201	192.168.14.204
2	1	192.168.2.201	192.168.2.201	15	3	192.168.15.201	192.168.15.203
3	1	192.168.3.201	192.168.3.201	16	1	192.168.16.201	192.168.16.201
4	1	192.168.4.201	192.168.4.201	17	1	192.168.17.201	192.168.17.201
5	1	192.168.5.201	192.168.5.201	18	2	192.168.18.201	192.168.18.202
6	1	192.168.6.201	192.168.6.201	19	1	192.168.19.201	192.168.19.201
7	2	192.168.7.201	192.168.7.202	20	1	192.168.20.201	192.168.20.201
8	1	192.168.8.201	192.168.8.201	21	1	192.168.21.201	192.168.21.201
9	-	-	-	22	1	192.168.22.201	192.168.22.201
10	2	192.168.10.201	192.168.10.202	23	3	192.168.23.201	192.168.23.203
11	1	192.168.11.201	192.168.11.201	23	2	192.168.24.201	192.168.24.202
12	1	192.168.12.201	192.168.12.201	24	1	192.168.25.201	192.168.25.201
13	3	192.168.13.201	192.168.13.203				

Tabla 5.5.Direcciones IP para los conmutadores

Para terminar el plan de direccionamiento se utilizara el número de red 192.168.0.0 para asignar una dirección IP a los enlaces del *Backbone*, y también para asignar direcciones IP a los servidores que den algún servicio a gran parte de la red. Los servidores serán conectados a un conmutador directamente conectado a los equipos de alto rendimiento con el fin de proporcionar servicios a la red de mayor velocidad. Las características del número de red utilizado se muestran en la Tabla 5.6.

TIPO	NUMERO DE RED	EQUIPO		DIRECCIÓN DE BROADCAST
		DESDE	HASTA	
BACKBONE	192.168.0.0	192.168.0.1	192.168.0.254	192.168.1.255

Tabla 5.6 Numero de red para las direcciones IP del *Backbone*.

Para asignar una dirección IP a los enlaces de fibra óptica entre los conmutadores de alto rendimiento tomaremos dos direcciones del rango de equipo disponibles para la red del *Backbone*. El enlace en el conmutador primario (closet 17) será 192.168.0.1 y la dirección del enlace en el conmutador secundario (closet 1) será 192.168.0.2. Lo anterior se resume en la Tabla 5.7

CONMUTADOR	CLOSET	DIRECCIÓN DEL ENLACE DE FIBRA ÓPTICA
1	17	192.168.0.1
2	1	192.168.0.2

Tabla 5.7 Direcciones IP para los enlaces de fibra óptica.

Para asignar una dirección IP a los servidores de la red, se utilizaran el rango de direcciones restantes de la dirección de red. Como se muestra en la Tabla 5.8

NUMERO DE RED	EQUIPO		DIRECCIÓN DE BROADCAST
	DESDE	HASTA	
192.168.0.0	192.168.0.3	192.168.0.254	192.168.0.255

Tabla 5.8 Direcciones IP para otros dispositivos en el *Backbone*.

ASIGNACIÓN DINÁMICA DE LOS PARÁMETROS DE RED CON DHCP

El uso de direcciones IP estáticas en redes, conlleva siempre inconvenientes de mantenimiento. Los nuevos nodos que se conecten a la red o los cambios vitales como servidores de nombres, *gateway*, etc. nos obligaran a configurar nuevamente todos los equipos que hacen uso de estos parámetros. Dado que cuanto más grande es la red es más difícil mantenerla de este modo. Para resolver este problema, en la red, se propone aplicara el Protocolo para Configuración Dinámica de Terminales, conocido como DHCP (*Dynamic Host Configuration Protocol*). Así la asignación de los parámetros de red para cada equipo, se realizara de forma automática con la ayuda de un servidor DHCP.

Antes de continuar hay que establecer que equipos actuarán como clientes DHCP, y cuales no; ya que los equipos que no actúen como clientes DHCP se les tendrá que asignar una IP fija, (como por ejemplo, el servidor DNS, o el servidor de autenticación). Las direcciones fijas deberán ser reservadas en el servidor DHCP, para evitar que este asigne estas direcciones a clientes DHCP y con esto provocar conflictos.

Para reservar un rango útil de direcciones IP dentro de cada red, utilizaremos la Tabla 5.3 de la sección anterior. Este rango de direcciones se ocupara para asignar direcciones dinámicas y fijas dentro de cada red. Los equipos actuarán como clientes DHCP y se les asignara una dirección dinámica; las impresoras, servidores y otros dispositivos como los conmutadores no serán clientes DHCP y se les asignara una dirección IP fija. Los rangos para direcciones dinámicas y fijas se establecen en la Tabla 5.4 de la sección anterior.

Para realizar la configuración e instalación del servidor DHCP podemos realizarlo de dos formas. La primera es utilizar un sistema operativo con licencia como podría ser Windows 2000 Server, esta opción requerirá el pago de una licencia, la del sistema operativo, además de la compra de una computadora donde se ejecutaran el *software*. La segunda opción, y en la que nos basaremos, incluye la utilización de un servidor Linux DHCP, que es un servidor basado en *software* libre y no requiere gastos en licencias de uso, lo único es contar con la computadora que cumpla los requerimientos para la ejecución del *software* de forma eficiente.

Al equipo que utilicemos como servidor DHCP, estará directamente conectado al segmento del Backbone, no será cliente DHCP, por lo tanto tendremos que asignarle los parámetros de red de forma manual. La Tabla 5.9 muestra los parámetros de red del equipo.

Dirección IP Fija	192.168.0.3
Mascara de Red	255.255.255.0

Tabla 5.9. Parámetros de red del servidor DHCP.

Configuración del servidor DHCP sobre Linux

La configuración del servidor DHCP[1] es sencilla, esta se realizara sobre Linux Red Hat 9, para otras versiones y distribuciones del Linux la configuración cambia muy poco. La distribución propuesta requiere que sea instalada sobre un equipo con las características que se presentan en la Tabla 5.10

	Mínimo	Modo Texto	Modo Grafico
CPU	Pentium	200 MHz clase Pentium o superior	Pentium II 400 MHz o superior
DISCO DURO	850 MB Mínimo		
MEMORIA	64 MB	64 MB	128 o superior

Tabla 5.10 Características del equipo para el servidor DHCP

[1] **¡Error! Vínculo no válido.**

Después de la instalación del sistema operativo en el equipo propuesto la instalación y configuración del servidor DHCP se resume en los puntos siguientes:

1. Instalación del paquete DHCP: En Red Hat el paquete se llama dhcp-x.y-z.i386.rpm (siendo x, y y z los números de versión), y viene en el CD del Sistema Operativo. Para instalarlo, basta con ejecutar rpm -ihv dhcp-x.y-z.i386.rpm, con lo que según el medio de instalación que se tenga configurado pedirá CD o se bajará de la red.

2. Configuración general: A continuación se incluye el fichero, de ejemplo, de configuración necesaria para que el servidor DHCP realice el direccionamiento que se ha mencionado anteriormente. Después se explica detalladamente el contenido del fichero:

   Fichero /etc/dhcpd.conf:

```
subnet 10.64.0.0 netmask 255.255.255.224 {

# --- default gateway

        option routers                  10.64.0.1;
        option subnet-mask              255.255.255.224;
        option domain-name-servers      10.64.0.1;
        range dynamic-bootp             10.64.0.2 10.64.0.30;
        default-lease-time              3600;
        max-lease-time                  7200;
}

subnet 172.16.0.0 netmask 255.255.0.0 {
}
```

   - El fichero esta compuesto de varias secciones "*subnet*", que es donde se configura cada una de las subredes a las que tiene acceso el servidor. Dentro de cada una de estas secciones, se configura la información que se enviará a los clientes DHCP que se pongan en comunicación con el servidor en dicha subred.
   - La línea "*option routers*" indica el enrutador por defecto que se indicará a los clientes que deben utilizar.
   - La línea "*option subnet-mask*" indica la máscara de red para los clientes.
   - Mediante la línea "*option domain-name-servers*" se informa a los clientes del (de los) servidor(es) DNS que pueden usar.
   - La línea "*range dynamic-bootp*" indica al servidor el rango de direcciones de dicha subred que se debe usar para asignación dinámica. En el caso del ejemplo, de la 2 a la 30, es decir, 29 direcciones.
   - Las líneas "*default-lease-time*" y "*max-lease-time*" definen los períodos por defecto y máximo que un cliente puede mantener su dirección sin necesidad de renovarla pidiéndola de nuevo. Cuando el servidor asigna una dirección a un cliente, le asigna también una caducidad, y una vez transcurrido dicho período el cliente debe renovar su asignación de dirección solicitándola de nuevo.

3. Configuración de los parámetros: Hay otros muchos parámetros que se pueden enviar a los clientes, como por ejemplo, los nombres de dominio Internet, las direcciones de los servidores WINS (para clientes Windows), servidores de impresión, rutas, y otros muchos. Para conocer todos los parámetros que el servidor DHCP permite configurar, se puede consultar el archivo de ayuda correspondiente a *dhcp-options*.

Para terminar de configurar nuestro servidor correctamente y se mantenga funcionando será necesario tener en cuenta los siguientes puntos:

- El servidor DHCP necesita tener configuradas todas las interfaces y subredes que encuentre en el equipo, incluso aunque no vaya a servir direcciones en ellas; en este último caso, no se definirán rangos en el fichero de configuración para dichas subredes. En caso de que falte alguna, el servidor no arrancará.
- Debido a esto, si cualquiera de las interfaces cambia (direccionamiento, nombre, etc.), será necesario reiniciar también el servidor DHCP para que active la nueva configuración.
- Como el servidor DHCP van a suministrar direcciones IP a múltiples subredes, debemos considerar que cualquier Enrutador conectando subredes deben actuar como un agente de relevo DHCP (DHCP *relay agent*). Si nuestros enrutadores no tienen activo el DHCP *relay agent* al menos un servidor DHCP será requerido en cada subred en la que existan clientes DHCP.
- El servidor DHCP debe estar configurado con una dirección IP estática, mascara de subred y *gateway* además del resto de parámetros del TCP/IP (es decir, no puede ser además un cliente DHCP).

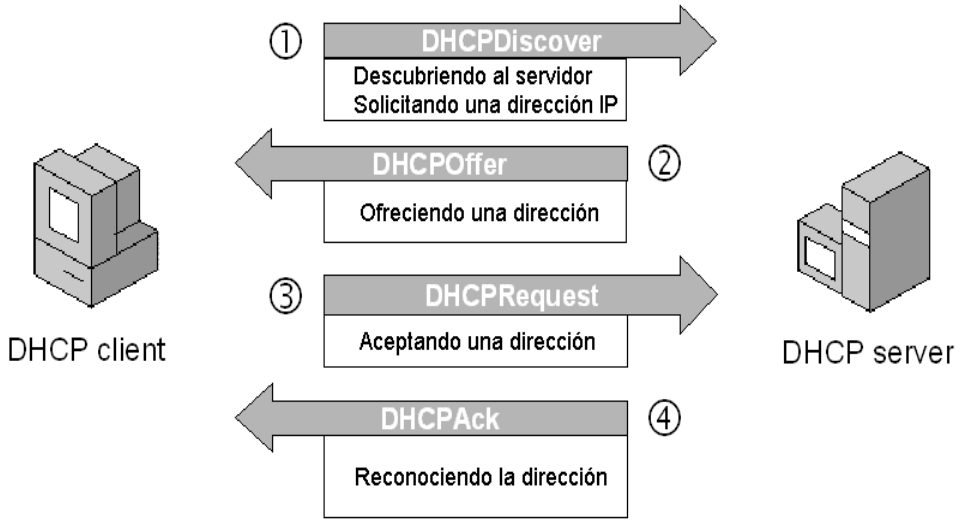

Figura 5.2. Proceso básico DHCP

AUTENTIFICACIÓN DE RED

Uno de los requerimientos primordiales de los sistemas informáticos que desempeñan tareas importantes son los mecanismos de seguridad, adecuados a la información que se intenta proteger. El conjunto de tales mecanismos ha de incluir al menos un sistema que permita identificar a las entidades (elementos activos del sistema, generalmente usuarios) que intentan acceder a los objetos (elementos pasivos, como archivos o capacidad de cómputo), mediante procesos tan simples como una contraseña o tan complejos como un dispositivo analizador de patrones retínales.

Los sistemas que habitualmente utilizamos los humanos para identificar a una persona, como el aspecto físico o la forma de hablar, son demasiado complejos para una computadora; el objetivo de los sistemas de identificación de usuarios no suele ser identificar a una persona, sino autenticar que esa persona sea quien dice ser realmente.

Es por eso que los servidores de control de acceso sean vuelto una obligación de seguridad en el uso de una red. Estos son la interfaz de mantenimiento para el acceso a una aplicación, actuando como una base de datos de información de cada usuario. Generalmente estos se comunican directamente con el equipo de acceso (Servidores de comunicaciones, enrutador, conmutador, etc.) usando protocolos estándar como lo es RADIUS.

RADIUS es un protocolo de control de acceso desarrollado por Livingston Enterprises y que la IETF ha recogido en los RFCs 2865 y 2866. Fue diseñado para autenticar usuarios y utiliza una arquitectura cliente / servidor. El servidor contiene información de los usuarios, almacenando sus contraseñas y sus perfiles, y el cliente es el encargado de pasar las peticiones de conexión de los usuarios al servidor para que éste las autentique y responda al cliente diciéndole si ese usuario está o no registrado.

El uso de un servidor de acceso, como RADIUS, ayuda a los administradores de red a implementar un medio sencillo y eficaz para agregar mecanismos de seguridad a la red. Entre mas usuarios tienen acceso a nuestra red, mucho más se incrementan los riesgos para mantenerla en un ambiente seguro. Dado que cuanto más grande es la red es más difícil mantenerla de este modo, para resolver este problema, como una propuesta en la red de la Facultad de Química, se aplicara el Protocolo RADIUS. La autentificación de usuarios con acceso a la red se realizara en forma automática con ayuda del servidor RADIUS, el usuario solo tendrá que proporcionar su nombre de usuario y contraseña.

Para realizar la configuración e instalación del servidor RADIUS podemos realizarlo de dos formas. La primera es utilizar un sistema operativo con licencia como podría ser Windows 2000 Server y un software con licencia para el servidor RADIUS, esta opción requerirá el pago de dos licencias, la del sistema operativo y la del software del servidor, además de la computadora donde se ejecutaran ambos software. La segunda opción, y en la que nos basaremos, incluye la utilización de un servidor Linux RADIUS, que es un servidor basado en software libre y no requiere gastos en licencias de software y el solo es necesario contar con la computadora que cumpla los requerimientos para la ejecución del *software* de forma eficiente.

El equipo que utilicemos como servidor RADIUS, estará directamente conectado al segmento del *Backbone*, no será cliente DHCP, por lo tanto tendremos que asignarle los parámetros de red de forma manual. La Tabla 5.11 muestra la configuración del equipo:

Dirección IP Fija	192.168.0.4
Mascara de Red	255.255.255.0

Tabla 5.11. Parámetros de red del servidor RADIUS

Configuración del servidor RADIUS sobre Linux

La configuración del servidor RADIUS[2] es sencilla, esta se realizara sobre Linux Red Hat 9, para otras versiones y distribuciones del Linux la configuración cambia muy poco. La distribución propuesta requiere que sea instalada sobre un equipo con las características que se presentan en la Tabla 5.10.

Después de la instalación del sistema operativo en el equipo propuesto la instalación y configuración del servidor RADIUS se resume en los puntos siguientes:

1. Instalación del servidor FreeRADIUS:

    a. Lo primero es conseguir el archivo comprimido con el código fuente de la aplicación, para ello lo podemos descargar desde aquí: http://www.freeradius.org/ Ese fichero contiene los archivos fuentes comprimidos y empaquetados.

    b. La instalación es sencilla, para esto tendremos que ejecutar desde la línea de comandos lo siguiente:

```
bash$ tar -zxvf freeradius.tar.gz
bash$ ./configure
bash$ make
bash# make install
```

2. Configuración General del servidor FreeRADIUS

    a. En este punto, el software base FreeRADIUS esta instalado. Antes de empezar, pensemos, que necesitaremos personalizar algunos archivos de configuración para que apunten a maquinas y redes especificas de nuestra configuración. La mayoría de estos archivos están localizados en el directorio /etc/raddb.

    b. Configurando el archivo "*clients*": Primero, echemos un vistazo al archivo /etc/raddb/clients. Este archivo contiene la lista de los equipos o enrutadores autorizados para bombardear al servidor FreeRADIUS con solicitudes de autentificación y la clave secreta que estos equipos o enrutadores usaran en sus solicitudes. Algunas entradas comunes están ya incluidas en este archivo, de las cuales uno puede eliminar o comentar las líneas que uno no necesite.

    Uno debe asegurarse que la clave secreta listada en el archivo "clients" es la misma que esta programada dentro del equipo de comunicaciones que será un cliente RADIUS. En nuestra red los conmutadores actuaran como clientes RADIUS y deberán ser programas para actuar como tales. La programación de los conmutadores, para actuar como clientes RADIUS la realizara el personal de la empresa que provea estos equipos, y tendrá que programar la misma clave secreta para que estos puedan hacer solicitudes de autentificación al servidor FreeRADIUS

    También se deberá añadir la dirección IP de estos equipos de comunicación. A continuación se muestra un ejemplo del archivo "*clients*".

```
# Client Name              Key
#----------------          ----------
#portmaster1.isp.com       testing123
#portmaster2.isp.com       testing123
#proxyradius.isp2.com      TheirKey
localequipo                testing123
192.168.1.100              testing123
tc-clt.hasselltech.net     oreilly
```

[2] http://www.freeradius.org

Aunque esto pueda parecer obvio, uno debe cambiar la clave secreta que viene por defecto en los archivos o en los ejemplos listados previamente. Cometer este error representa un riesgo de seguridad en la implementación de red.

c. Configurando el archivo "*users*": Este archivo contiene la información de seguridad y autentificación para cada usuario. FreeRADIUS permite varias modificaciones al estilo original del servidor RADIUS de tratar usuarios desconocidos en el archivo "*users*". En el pasado, si un usuario no fue configurado en el archivo "*users*", el servidor buscaría en el archivo "*password*" de UNIX, y entonces le negaría el acceso si este no tuviera una cuenta en la maquina. Había una sola entrada por defecto permitida. En contraste, FreeRADIUS permite múltiples entradas por defecto y puede encontrar una optima coincidencia para cada una de ellas. Permite espacios y símbolos en los atributos de nombre de usuario.

Para añadir un usuario al archivo "*users*" y probar la funcionalidad de este, se incluye un archivo "*users*" de ejemplo como el siguiente:

```
Steve       Auth-Type := Local, User-Password == "testing"
            Service-Type = Framed-User,
            Framed-Protocol = PPP,
            Framed-IP-Address = 172.16.3.33,
            Framed-IP-Netmask = 255.255.255.0,
            Framed-Routing = Broadcast-Listen,
            Framed-Filter-Id = "std.ppp",
            Framed-MTU = 1500,
            Framed-Compression = Van-Jacobsen-TCP-IP
DEFAULT     Service-Type == Framed-User
            Framed-IP-Address = 255.255.255.254,
            Framed-MTU = 576,
            Service-Type = Framed-User,
            Fall-Through = Yes
DEFAULT     Framed-Protocol == PPP
            Framed-Protocol = PPP,
            Framed-Compression = Van-Jacobson-TCP-IP
```

En este archivo podemos ver en la primera línea el "*username*" llamado "steve", este será el nombre de usuario en la red; en la misma línea podemos ver "*User-Password == "testing"*" que es la contraseña que el usuario necesitara para autentificarse y poder hacer uso de la red.

Este formato de entrada en el archivo "*users*" debe existir por cada usuario de la red y debe realizarse una copia para cada usuario nuevo que quiera hacer uso de los recursos de esta.

Las contraseñas pueden ser generadas con ayuda de software gratuito que se puede encontrar en Internet. Una copia de este tipo de software para generar las contraseñas puede encontrase en http://www.bordeline.com.ar/ y su nombre es "Generador de contraseñas 1.1". Los nombres de usuarios seguirán las reglas establecidas en "Políticas en la asignación de los datos de red".

d. Activar el servidor de RADIUS

Para inicializar RADIUS solo escriba /usr/local/bin/radiusd.

REDES DE ÁREA LOCAL VIRTUALES (VLANs)

En la configuración de red, todos los equipos, de un segmento, estarán conectados a un mismo conmutador. Por lo tanto comparten el mismo dominio de difusión, esto provoca que cualquier paquete de difusión enviado al segmento sea replicado en todos los puertos del conmutador. Este hecho hace que el rendimiento de la red baje considerablemente debido al uso del ancho de banda de dichos mensajes de información.

Esto no es considerable si todos los dispositivos que pertenecen al segmento usan la información de dichos mensajes de difusión, pero es muy habitual que dentro de una misma LAN (dominio de difusión) haya usuarios pertenecientes a distintos grupos de trabajo, por lo que la información de dichos mensajes de difusión sólo incumbe, la mayoría de las veces, a los dispositivos pertenecientes al mismo grupo de trabajo. Este hecho hace que a cada usuario le lleguen mensajes de otros grupos de trabajo que no le incumben, y lo que es peor: que el ancho de banda usado por dichos mensajes no puede ser utilizado por los usuarios de otro grupo de trabajo distinto. El problema anterior sólo ocurre en el ámbito de LAN, puesto que un enrutador es un dispositivo que aísla dominios de difusión, es decir, los mensajes de difusión de una LAN no son propagados más allá.

Para limitar los dominios de difusión en el ámbito de LAN se ha creado el concepto de VLAN[3]. La implementación de las VLAN se realiza en el ámbito de capa 2, por lo que pueden ser implementadas en un conmutador. El objetivo es que los dominios de difusión no se asignen por la pertenencia a una determinada red LAN, es decir, por su situación física dentro de la LAN, sino que éstos son definidos en función de en que puerto del conmutador está conectado a los dispositivos. La implementación de una VLAN se realiza asignado cada puerto del conmutador a una determinada VLAN, limitando la difusión de mensajes entre los dispositivos (puertos) que pertenecen a la misma VLAN.

En esta sección sé establecerá la configuración de cinco VLANs dentro de la red de la Facultad de Química. Estas VLANs realizarán una agrupación lógica de los usuarios, que entre otras ventajas, permitirán mayor administración en las cuentas de acceso y de los servicios a los cuales tienen derecho. La configuración de los conmutadores para el trabajo con VLAN, la realizara el personal de la empresa que provee los equipos de comunicación.

Cuando el usuario realice el proceso de autentificación con éxito, el conmutador al cual se conecta su equipo, deberá asignar el puerto de conexión a una VLAN. Esta asignación se realizará con un conjunto de procesos que realizan el servidor RADIUS y el conmutador de comunicaciones. Cuando el proceso de autentificación se inicia, el usuario ingresa el nombre de usuario y contraseña al sistema, el conmutador toma esta información y hace una solicitud de autentificación al servidor RADIUS, si el usuario es valido, el servidor regresa una respuesta afirmativa y envía información acerca de la cuenta del usuario, donde se incluye el identificador de VLAN a la cual se ha asignado su cuenta; el conmutador utilizara esta información para asignar el puerto de conexión del usuario a la VLAN que le corresponde.

Configuración de VLAN

Para iniciar se crearán cinco VLANs, que posteriormente podrán incrementarse según el grado de especialización que se requiera en la administración de usuarios. El primer grupo de usuarios asignados a una VLAN, son los administradores de red. Este grupo contará con todos los servicios disponibles en la de red. El segundo grupo corresponde a los Investigadores de la Facultad. Este grupo requiere la mayoría de servicios disponibles para realizar sus actividades, pero no contara con servicios exclusivos al grupo de administradores. El tercer grupo pertenece a los usuarios del tipo académico. Este grupo realiza actividades que solo requieren acceso a los sistemas administrativos, Internet y correo electrónico. El cuarto grupo corresponde al grupo de usuarios administrativos. Este grupo tiene los mismos privilegios que el grupo anterior, pero tendrá que modificarse en función de los servicios de red sobre los cuales se apoya para realizar su trabajo. El quinto grupo corresponde a los usuarios del tipo alumnos e invitados. Este grupo solo tiene acceso a Internet y correo electrónico. El último grupo corresponde a los dispositivos de red y solo debe permitirse los servicios necesarios para su buen funcionamiento y negar aquellos que pongan en riesgo su seguridad.

[3] 2.Cisco System, Inc. “Academia de Networking de Cisco System, Guía del segundo año”. Segunda edición. Pearson Education. S.A. Madrid 2003. Pag. 69

Las cuentas de usuario serán asignadas a las diferentes VLAN dependiendo del tipo de actividades, que los usuarios realicen dentro de la Facultad de Química. El personal del Centro de informática analizará la información del usuario y determinara a que VLAN será asignada su cuenta de acceso.

En función de las actividades de cada grupo y con ayuda de un método de seguridad muy útil en redes, que consiste en negar puertos TCP y UDP comúnmente vulnerables, y solo permitir aquellos que sean necesarios, se crearan el conjunto de servicios permitidos para cada VLAN. Ambos TCP y UDP usan números de puertos para pasar datos a las capas superiores. Los números de puertos ayudan a definir y a guardar todos los diferentes tipos de conversaciones que tienen lugar a través de la red. Cada protocolo de la capa de aplicación incluyendo FTP, Telnet, SMTP, DNS TFTP, SNMP y el protocolo de información de ruteo (RIP), tiene un número específico de puerto que identifica este y lo separa de otros protocolos.

En la Tabla 5.12 se listan los puertos negados para cada VLAN. Los puertos TCP/UDP negados son algunos de los puertos preasignados de mayor uso[4], que son usados por protocolos y aplicaciones que no son necesarios para el tipo de actividades de los usuarios que componen a las diferentes VLAN.

VLAN	NUMERO DE PUERTO NEGADO		
ADMINISTRADORES DE RED	NINGUNO		
INVESTIGADORES	snmp (161,162)	nntp (119)	ldap (389)
	bootp (67)	lpd (515)	finger (79)
	netbios (135-9,445)	bgp (179)	ntp (123)
	portmap (111)	nfs (2049)	syslog (514)
	imap (143)	rlogin (512-514)	socks (1080)
	time (37)	lockd (4045)	
ACADÉMICOS	telnet (23)	nntp (119)	rlogin (512-514)
	tftp (69)	lpd (515)	lockd (4045)
	snmp (161,162)	bgp (179)	ldap (389)
	klogind (543)	para juegos(2301-11)	pequeños(1-20)
	bootp (67)	tacacs (49)	finger (79)
	netbios (135-9,445)	Kerberos (88)	ntp (123)
	portmap (111)	nfs (2049)	syslog (514)
	dns (53)	news (144)	socks (1080)
	time (37)	ftp (21)	Rip (520)
ADMINISTRATIVOS	telnet (23)	nntp (119)	rlogin (512-514)
	tftp (69)	lpd (515)	lockd (4045)
	snmp (161,162)	bgp (179)	ldap (389)
	klogind (543)	para juegos(2301-11)	pequeños(1-20)
	bootp (67)	tacacs (49)	finger (79)
	netbios (135-9,445)	Kerberos (88)	ntp (123)
	portmap (111)	nfs (2049)	syslog (514)
	dns (53)	news (144)	socks (1080)
	time (37)	ftp (21)	Rip (520)
ALUMNOS E INVITADOS	telnet (23)	time (37)	rlogin (512-514)
	tftp (69)	nntp (119)	lockd (4045)
	snmp (161,162)	lpd (515)	ldap (389)
	irc (6667-6901)	bgp (179)	pop (109,110)
	klogind (543)	para juegos(2301-11)	Pequeños(1-20)
	bootp (67)	tacacs (49)	finger (79)
	netbios (135-9,445)	Kerberos (88)	ntp (123)
	portmap (111)	nfs (2049)	syslog (514)
	dns (53)	ssh (22)	socks (1080)
	smtp (25)	news (144)	Rip (520)
	imap (143)	ftp (21)	
DISPOSITIVOS DE RED	irc (6667-6901)	lpd (515)	lockd (4045)
	klogind (543)	bgp (179)	ldap (389)
	bootp (67)	para juego(2301-2311)	Pequeños(1-20)
	netbios (135-9,445)	nfs (2049)	finger (79)
	portmap (111)	ssh (22)	ntp (123)
	imap (143)	news (144)	syslog (514)
	time (37)	ftp (21)	socks (1080)
	nntp (119)	rlogin (512-514)	

Tabla. 5.12 Puertos negados para cada VLAN.

[4] http://www.iana.org/assignments/port-numbers

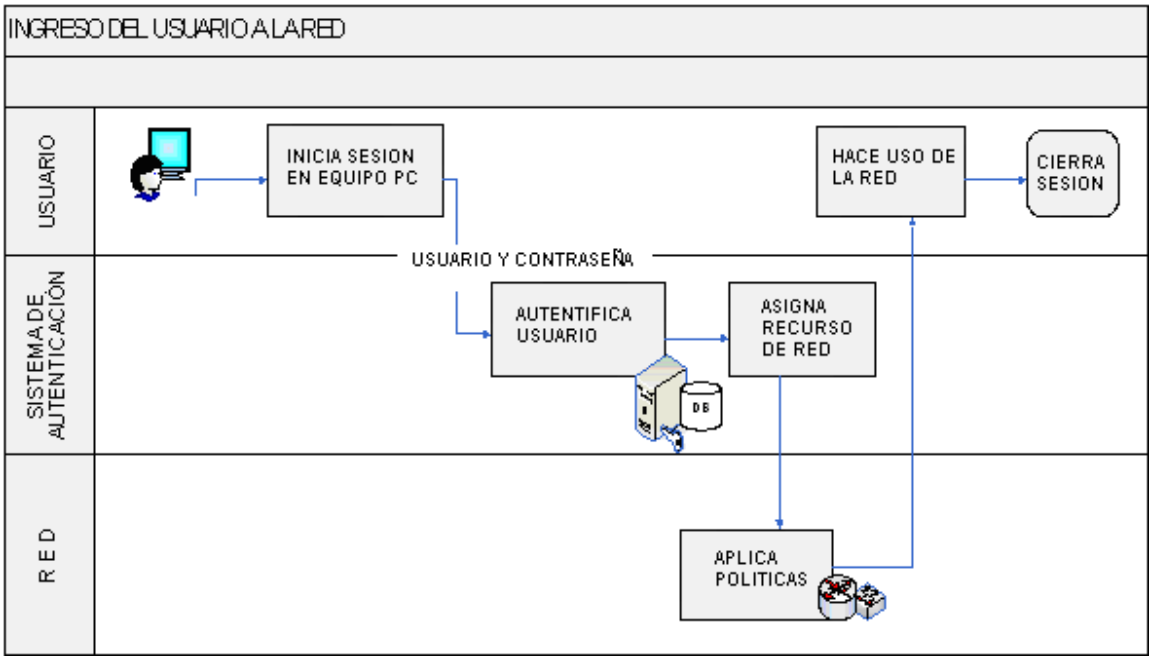

Figura 5.3. Proceso de Autentificación de usuarios

5.3 ESQUEMA DE ADMINISTRACIÓN

INTRODUCCIÓN

Aquí se presenta la descripción de la metodología utilizada en la administración de redes de datos basada en modelos funcional estándar de la ITU y de la ISO. Estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes.

Estos modelos presentan las áreas funcionales en la cual se divide la administración de redes. Esta propuesta realizará las modificaciones necesarias para adaptarlo a la administración de la red de la Facultad de Química. Se establecerán los objetivos particulares de cada área, que en síntesis aseguran el eficiente empleo de los recursos, que debe lograrse con el cumplimiento de los objetivos planteados para cada área en la que se subdivide este modelo.

La descripción de las tareas de cada área funcional, tendrá que seguir como meta el cumplimiento del objetivo planteado. El modelo original sé vera modificado en función de las necesidades de la Facultad de Química, pero en principio, este planteara la base a seguir para la integración de un modelo de administración basado en un estándar establecido por órganos internacionales.

MODELO FUNCIONAL PARA LA ADMINISTRACIÓN DE REDES

Nuestra propuesta plantea el seguimiento del estándar TMN (*Telecommunications Management Network*), que es un modelo definido en la serie M.3000 de la ITU-T y de OSI-NM (*OSI-Network Management*) de ISO.

Dentro de estos modelos se propone que la administración de redes se divida en 5 áreas funcionales:

- Administración de la configuración.
- Administración del rendimiento.
- Administración de fallas.
- Administración de la contabilidad.
- Administración de la seguridad.

Cada área cuenta con un objetivo en particular y las tareas asociadas para el cumplimiento de estos. La suma de todos estos objetivos tendrá que satisfacer en su totalidad el propósito general para el cual se ha planteado esta administración.

La Figura 5.4 muestra la división por áreas basada en los modelos planteados y las diferentes etapas que compone cada área.

MODELO FUNCIONAL

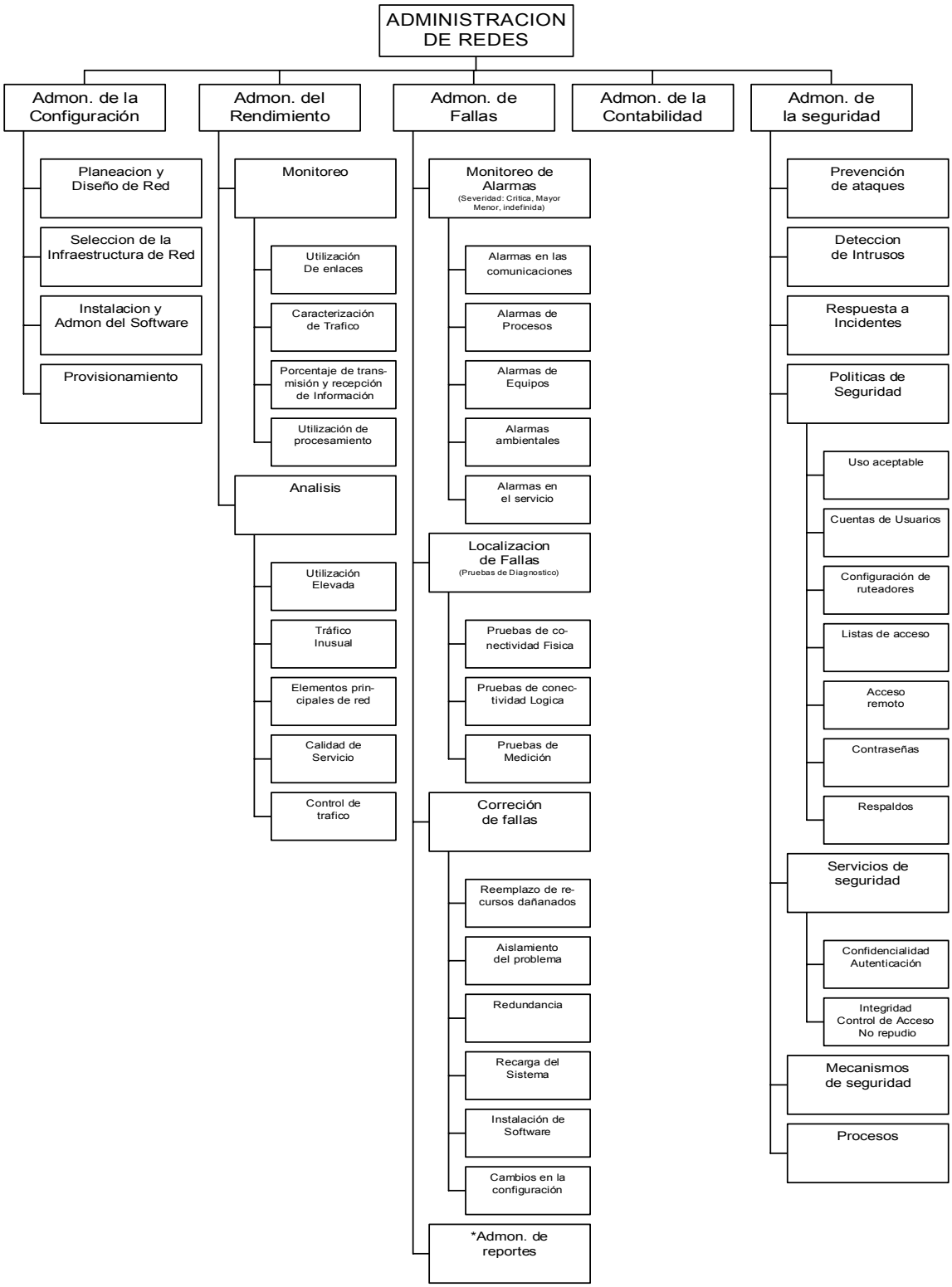

Figura 5.4 Áreas y etapas del Modelo Funcional

EL MODELO APLICADO A LA FACULTAD DE QUÍMICA

Para hacer aplicable el modelo a la Facultad de Química se propone la fusión de áreas del modelo estándar en tres departamentos que se encargaran en conjunto de la administración de la red.

Estos departamentos mantendrán varios de los objetivos planteados por el modelo; pero la división se reducirá a tres áreas y no a cinco como se contempla en el modelo estándar. Esta división se realiza para reducir el numero de personal necesario que realice las actividades y hacer aplicable el modelo en la nueva red. Las modificaciones proponen iniciar con un modelo básico de administración que posteriormente podrá ser ampliado al modelo completo dependiendo del grado de especialización de la administración que se desee por la Facultad de Química.

Se mantendrá fuera de esta propuesta las actividades del área de contabilidad, si los administradores de red consideran apropiado llevar la contabilidad de sus usuarios este modelo permite ser ampliado para incluir el área de contabilidad y todas actividades que esto conlleva.

El objetivo del área de contabilidad es realizar los cobros correspondientes a la utilización de los recursos de red. Entre sus tareas se encuentra obtener la información sobre la utilización de los recursos de red y calcular las cuotas de acuerdo a los recursos utilizados. La contabilidad se usa principalmente en sectores particulares donde se realiza un cobro por el uso de los recursos, como sucede con un proveedor de servicio de Internet (IPS por sus siglas en ingles).

La fusión de áreas busca integrar las actividades del modelo estándar, que mayor relación tienen, dentro de departamentos. Esta fusión permitirá establecer un modelo básico de administración, donde se incluirán las actividades de mayor relevancia agrupas en un menor número de departamento, que consigan satisfacer las tareas asociadas utilizando un menor número de recursos y de personal. Esta propuesta también incluirá un departamento con las actividades relacionada a la atención de los problemas de usuarios.

Cada departamento tendrá objetivos específicos y cumplirá tareas determinadas según las áreas del modelo que relaciona. Las áreas que relacionan cada departamento son

1. Administración del rendimiento y de seguridad en el departamento de Monitoreo y Seguridad
2. Administración de configuración y fallas en el departamento de Operación y Mantenimiento.
3. Atención a los problemas de usuarios en el departamento de Soporte Técnico.

Para mantener un nivel aceptable de servicio en la red, se requiere de un esquema de operación jerárquico; en el cuál tendremos al Centro de Informática, de la Facultad de Química, ubicado en el nivel más alto. Debajo de éste, se encontrara el Departamento de Operación y Mantenimiento, el Departamento de Monitoreo y Seguridad y el Departamento de Soporte Técnico.

La propuesta para la administración se plantea en la Figura 5.5.

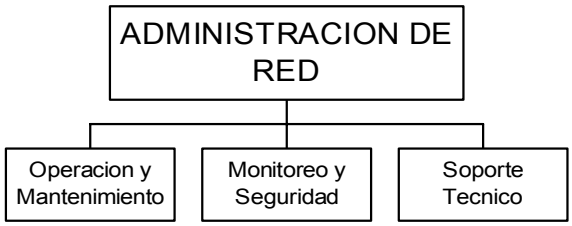

Figura 5.5. Departamentos del modelo de administración propuesto

EL CENTRO DE INFORMÁTICA.

El Centro de informática tendrá como función principal coordinar a los diferentes departamentos de esta administración. Realizará las actividades que aporten recursos a los departamentos, además de establecer los procedimientos y políticas, para la interacción entre ellos y la comunidad de la Facultad, todo para asegurar su adecuada organización y conjunción con la institución.

OBJETIVOS, TAREAS, PROCEDIMIENTOS Y POLÍTICAS

Los objetivos que este departamento debe cumplir son:

- Proporcionar servicios de información a los departamentos de esta administración.
- Establecer los procedimientos de interacción con la comunidad de la Facultad.
- Analizar y solucionar de eventos extraordinarios.

El Centro de Informática, contara con un conjunto de tareas, procedimientos y políticas establecidos, que serán las herramientas necesarias para el cumplimiento de sus objetivos. La administración de la red será responsabilidad completa de este Centro. A continuación se mencionan sus tareas.

- Documentación de red.
- Control de inventario de dispositivos de red.
- Administración de información de los usuarios de red.
- Realización de los mapas de red.
- Control de software autorizado.
- Atención a solicitud de información.
- Atención a solicitud de servicios.
- Solución de eventos extraordinarios.

Los procedimientos que se realizaran para el cumplimiento de estas tareas serán los siguientes

- Procedimiento de obtención de los datos de *hardware* y *software*.
- Procedimiento para la atención de las solicitudes de información.
- Procedimiento para la atención de las solicitudes de servicios.
- Reasignación de casos.

Las políticas a seguir en este departamento son las siguientes:

- Políticas en la asignación de los datos de red.
- Políticas de uso de *software* y equipos de cómputo.

DISEÑO DEL CENTRO.

Esta etapa consiste en establecer como se realizaran las tareas que anteriormente se definieron. La meta principal es dotar de los recursos de información que los departamentos necesitan para realizar sus actividades y atender las solicitudes de servicio que la comunidad de la Facultad realice.

Documentación de red

Auditoria de instalaciones

Una auditoria de instalaciones permite tener constancia de dónde está todo. Debe incluir el cableado, los puestos de trabajo, las impresoras y los dispositivos de comunicación (Conmutadores o Enrutadores). Resumiendo, debe proporcionar información detallada sobre la ubicación de todos los componentes de la red. Idealmente, toda esta información debería estar registrada en la versión de trabajo de un documento llamado diagrama de instalaciones, cuando se instaló la red o mejor conocido como “memoria Técnica”. Cuando se complete la auditoria, se podrá transferir la información registrada en los diagramas al conjunto de planos del edificio.

Esta documentación representara la memoria del Centro de informática. Ante todo deberá incluirse los siguientes componentes:

- Diagramas que indican el trazado de la distribución del cableado físico.
- El tipo de cable.
- La longitud de cada cable.
- El tipo de terminación de cada cable.
- La ubicación física de cada panel de parcheo.
- Un esquema de etiquetado para la identificación sencilla de cada cable.

Distribución de los closet de telecomunicaciones

Este documento contiene la distribución física y lógica del closet de telecomunicaciones principal y de todos los closet de distribución intermedios de la red. Incluye la distribución física del montaje de los equipos de telecomunicaciones en *racks*, así como la finalidad de cada equipo dentro de la red. También incluye la información del panel de parcheo que ayudara a identificar las terminaciones del cable, así como la identificación y los detalles de configuración de todo el equipo que se encuentra en cada closet.

Detalles de configuración de los dispositivos de red

Los detalles relativos a la configuración de los servidores que ofrecen servicio a la red (Servidor de autentificación, servidor de DHCP, etc.), tienen que ser registrados con ayuda de un formato de resguardo, como el que se incluye en la Figura 5.6. La información de estas hojas esta estandarizada y contiene aspectos como la marca y el modelo de la computadora, el numero de serie, unidades de disco flexible, unidades de disco duro, Unidad DVD / CD-ROM, tarjeta de sonido y red, cantidad de RAM y todos los demás detalles físicos del equipo. Esta información también incluye detalles sobre la configuración de los equipos como el IRQ el DMA y la configuración de la dirección de la memoria básica de las tarjetas periféricas.

Por ultimo este documento contiene información sobre la ubicación física, el usuario encargado del equipo y la identificación de la red (Dirección IP, dirección MAC, subred, etc.) acerca de la computadora.

HOJA DE CONFIGURACIÓN DE HARDWARE (Una hoja por equipo)					
Tipo de equipo					
Localización física					
Marca y modelo					
Numero de serie					
Numero de inventario					
UNIDADES DE ALMACENAMIENTO FIJOS Y REMOVIBLES					
Marca	Letra de la unidad	Capacidad	Interna / Externa	Slot de Conexión	
MEMORIA ACTUAL/ MÁXIMA					
Actual			Máxima		
TARJETAS DE RED					
Marca	Modelo	Tipo	IRQ	DMA	Dirección
Comentarios					

Figura 5.6 Hoja de configuración de hardware

Listado de *software*

También es necesario incluir junto con la hoja anterior el *software* estándar y especial que se usa en cada equipo de comunicación, servidor o impresora, con el fin de documentar los detalles de instalación de la configuración estándar de cada paquete de *software*. Esta lista incluye el sistema operativo y el *software* de aplicación.

Registro de mantenimiento

También resulta útil mantener una lista de todas las reparaciones que se hayan hecho en todo el equipamiento de red. Esto ayudara a predecir los posibles problemas futuros con el *hardware* y el *software* existentes. Se puede pensar en incorporar un servicio de *Help Desk* (ayuda de escritorio) que consiste en ayuda proporcionada por especialistas con gran conocimiento de *hardware* y *software*. Para brindan el soporte necesario en caso de fallas de los sistemas o dispositivos.

Inventario de dispositivos de red

Procedimiento de obtención de los datos de Hardware y software

El programa que se utilizara para obtener los datos de hardware y software de los equipos es “WinAudit”, que puede obtenerse en www.pxserver.com/WinAudit.htm, Este software realiza un completo inventario del sistema en unos pocos minutos. No requiere instalación; un doble clic basta para que el programa analice el equipo y muestre una completa lista de todo el *hardware* y *software* instalado. Este programa tiene un tamaño de 129 Kb y podrá ser transportado de maquina en maquina con un disquete de 3.5 pulgadas.

Para obtener los datos del inventario se seguirá los siguientes pasos:

1. Ejecutar el programa, dentro del equipo del que se desee obtener información de *hardware* y *software*.
2. En el menú “*View*” dar clic en “*Options*”. En esta pantalla dejamos seleccionadas solo las siguientes opciones.

    a) General Information.
    b) Installed software.
    c) Processor Details.
    d) Memory Information.

e) TCP/IP Settings.
f) Drive Information.

3. Damos clic en el botón "*Audit*" y se generara un archivo que contiene información sobre los programas instalados, periféricos, uso de memoria, modelo de procesador, configuración de red, etc.
4. El informe se guardara en formato de texto con el nombre del usuario encargado del equipo.
5. Para terminar de obtener los datos del equipo también será necesario obtener la siguiente información.

    a) Número de serie del monitor.
    b) Número de serie del CPU.
    c) Marca del equipo.
    d) Modelo del equipo.

    En los equipos de telecomunicaciones se debe obtenerlos siguientes datos

    a) El número de serie del equipo.
    b) Modelo y marca.
    c) Ubicación física.
    d) Área a la que otorga servicio.

6. Para completar la obtención de los datos para el inventario, es necesario obtener la información del usuario, al cual quedara asignado el equipo.

    Los datos que se deben obtener del usuario serán los siguientes:

    a) Nombre completo del usuario.
    b) Puesto de trabajo.
    c) Jefe inmediato superior.
    d) Extensión telefónica.
    e) Ubicación física.

Análisis y procesamiento de los datos.

Para que los usuarios tengan acceso a la nueva red, deberán estar asignados a una VLAN, esto con el fin de lograr mejorar la administración de los recursos y servicios, que se reflejara en una mejor calidad en beneficio de todos los usuarios de la red.

Con los datos obtenidos el personal del Centro de Informática analizara la información del usuario y determinara a que VLAN será asignada su cuenta de acceso. Generara las cuentas de acceso a la red y tendrá que asignar un nombre de usuario y contraseña únicos por cada usuario de la red. El nombre de usuario y contraseña, de cada cuenta, seguirán las reglas que se encuentran en las "Políticas en la asignación de los datos de red" en el Apéndice B.

Además deberá analizarse la información del *software* instalado en cada equipo. El Centro de informática debe realizar una lista que incluya los tipos de software que se emplean, el número de usuarios para cada aplicación y las peticiones de operatividad de cada una de ellas. Durante el inventario de software, puede asegurarse también que el número de usuarios de cada aplicación del software no sobrepase el número de licencias que posee el Centro.

Resguardo de información.

Los datos obtenidos en el inventario deben ser digitalizados, para lleva mayor control sobre estos y para generar los resguardos del equipo. La digitalización de estos datos estará a cargo del personal del Centro de Informática, y se recomienda utilizar una base de datos para su mejor administración. Se incluye un formato en el Apéndice A que puede ayudar en la digitalización inicial de estos datos.

El documento de resguardo será generado a partir de los datos del inventario y servirá para tener control de las personas a las cuales queda asignado cada equipo dentro de la red. El usuario deberá firmar este documento y se le entregara una copia impresa o digital de las políticas y procedimientos

para hacer uso de la red. Los documentos de resguardo deberán ser almacenados en un lugar seguro, y deberán ser actualizados cada vez que sea requerido. Se incluye una copia del documento de resguardo en el Apéndice A.

Generación de etiquetas

Las etiquetas tendrán el objetivo de tener una referencia del inventario en el mismo equipo; las cuales deberán ser ubicarlas en un lugar visible y accesible, para futuras consultas. El lugar idóneo para colocaran las etiquetas lo decidirá el personal del Centro de Informática.

Se recomienda ubicar las etiquetas en la parte frontal del monitor en la esquina superior derecha. Para el CPU se recomienda también, ubicarlas en la esquina superior derecha. En los equipos de comunicaciones se colocaran en la parte de mejor visibilidad. Como lo muestra la Figura 5.7.

Las etiquetas para el monitor, el CPU y los equipos de comunicación deberán contener la siguiente información:

a) Numero de inventario.
b) Tipo y modelo de equipo.
c) Nombre del responsable del equipo.

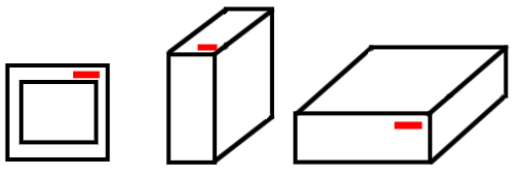

Figura 5.7. Esquema para la ubicación de las etiquetas del inventario.

Mapas de la red

Después de realizar los inventarios y la documentación de red, se debe utilizar la información obtenida para generar el mapa de la red, que es muy similar a un plano. Dicho mapa debe incluir la ubicación física y la disposición de todos los dispositivos conectados a la red y las aplicaciones con las que funcionan. También se deberían incluir las direcciones IP y MAC de cada dispositivo. Por último, el mapa de la red debería incluir las distancias de cada cable entre los nodos de la red. El mapa de la red completo debería guardarse cerca de la ubicación seleccionada para el uso de cada departamento.

Software autorizado.

En esta actividad se pretende analizar las necesidades de software para el uso interno de la Facultad de Química así como la cantidad de licencias de uso de este software.

El Centro de informática realizará la actualización constante de la base de datos del software autorizado, y actualizara el documento “Políticas de buen uso de equipos de computo y software”, donde se incluye una copia en el Apéndice B.

El Centro de informática, tendrá la tarea de informar a la comunidad los medios para solicitar la instalación de software nuevo o la instalación de una copia con licencia. Además promoverá el uso de software legal, dando a conocer las ventajas, que entre otras cosas cuenta con soporte técnico especializado por parte del proveedor e informando que el uso indebido del software genera responsabilidades legales tanto para la Facultad como para los responsables de sistemas..

Solicitud de información

En esta actividad se pretende, atender las solicitudes de información, como la consulta de información de los inventarios de red, información sobre los usuarios de red, documentación y mapas de red, etc., que necesitan los departamentos de esta administración para realizar sus actividades.

La información con que cuenta el Centro es útil para las actividades que realizan los departamentos de esta administración, es responsabilidad del Centro mantenerla actualizada y proporcionarla a los departamentos que la soliciten. Se deberá informar a cada departamento los medios para solicitar dicha información.

A continuación se describe el procedimiento para la solicitud de información.

Procedimiento para la atención de las solicitudes de información

El Centro de Informática deberá poner a disposición de los departamentos que componen la administración de la red el servicio que permitirá hacer consultas de información, las cuales deberán ser evaluadas en el menor plazo posible.

Recibiendo la solicitud será evaluada por personal del Centro de Informática y este deberá verificar a la brevedad posible el origen de la solicitud enviada, de ser valida; informar sí la información solicitada esta disponibles y la fecha de entrega de la misma.

Vías para presentar solicitudes

- En formato electrónico por correo electrónico. (Correo asignado por el Centro para este uso).
- En formato escrito personalmente (En las instalaciones del Centro de Informática).

Datos que se deben incluir para presentación de la solicitud:

a. Nombre y apellidos de la persona que solicita la información.
b. Departamento al que pertenece.
c. Los datos de envió de la información si esta es autorizada.
d. Teléfono.
e. Correo electrónico.
f. Tipo de información que necesita.

El formato que se incluye en la Figura 5.8 puede ayudar a llevar un mejor control de estas solicitudes. Para mejorar el trato de la solicitud se debe recomendar al solicitante detallar el tipo de información a solicitar: Describir de manera concisa la información solicitada.

SOLICITUD DE INFORMACIÓN	
Complete el contenido del siguiente formulario para recibir información puntual del Centro de Informática	
Nombre	
Apellidos	
Cargo	
Jefe inmediato	
Departamento	
Teléfono	
Extensión	
Correo electrónico	
Tipo de Información solicitada	

Figura 5.8. Formato para solicitar información al Centro de informática

Solicitud de servicios

En esta actividad se pretende, atender las solicitudes de servicios, realizadas por los usuarios de la red al Centro de informática. Los servicios que el Centro de Informática ofrecerá son:

- Alta y baja de un usuario dentro de la red.
- Instalación de software.
- Respaldo de información.

El Centro de Informática debe informar de los procedimientos necesarios para presentar las solicitudes. Los medios para presentar estas solicitudes son los siguientes:

- En formato electrónico por correo electrónico. (Correo asignado por el Centro para este uso).
- En formato escrito personalmente (En las instalaciones del Centro de Informática).

A continuación se describe el procedimiento para la solicitud de servicios.

Procedimiento para la atención de las solicitudes de servicios

Recibiendo la solicitud será evaluada por personal del Centro de Informática y este deberá verificar a la brevedad posible el origen de la solicitud enviada, de ser valida; informar la fecha de entrega del servicio. Posteriormente tendrá que ser enviada al departamento correspondiente para su aprovisionamiento.

Las solicitudes de alta y baja de usuarios y de respaldo de información serán asignadas al departamento de Monitoreo y Seguridad para su aprovisionamiento. Las solicitudes de instalación de *software* serán enviadas al departamento de Operación y Mantenimiento.

El formato de la Figura 5.9 es una propuesta para solicitar por medio de un documento escrito las solicitudes de servicio. Para mejorar el trato de la solicitud se debe recomendar al solicitante que informe claramente el tipo de servicio a solicitar. Describir de manera concisa el servicio solicitado.

SOLICITUD DE (_____)

Nombre de quien solicita el servicio: _____
Cargo:_____
Departamento: _____
Solicita que a:_____
Con cargo de:_____
Y Domicilio:_____
Le sea concedido (TIPO DE SERVICIO):_____
_____
como usuario dentro de la red de la Facultad de Química.

Razón por lo que se hace la solicitud:_____
_____
_____
Fecha: _____

Firma y sello del departamento

Figura 5.9. Formato para solicitar un servicio al Centro de informática

Solución de eventos extraordinarios.

Esta actividad pretende analizar y solucionar aquellos casos no contemplados dentro de las actividades de cada departamento. El Centro de informática tendrá la función de analizar los problemas que surjan en los departamentos de esta administración para los cuales, no se tienen actividades definidas para su solución.

Casos reasignados

Otra de las actividades que este departamento tendrá que realizar será la reasignación de casos. La reasignación de casos deberá realizarse cuando se presentan las siguientes situaciones:

- Inhabilidad de un departamento de continuar con la solución de un problema por motivos de alcance o de recursos.
- Falta de experiencia en la solución de un caso o por no pertenecer al tipo de casos que atiende cada departamento.

La reasignación de casos la realizará el personal del Centro de informática, después de evaluar toda la información del caso; para poder precisar que departamento o instancia tendrá que continuar con el caso.

STAFF TÉCNICO

Todas las actividades asociadas a este departamento serán realizadas y manejadas por el grupo de trabajo que actualmente conforma el Centro de Informática, y que tiene el control de la administración de la antigua red de la Facultad de Química.

DEPARTAMENTO DE MONITOREO Y SEGURIDAD

Cada departamento tendrá objetivos y tareas bien definidas, que en conjunto lograran el cumplimiento del objetivo general de administración. A continuación se establecen los objetivos, tareas, procedimientos y políticas del Departamento de Monitoreo y Seguridad. Este departamento realizara las funciones de dos de las áreas del modelo TMN, la administración del rendimiento y la administración de la seguridad. A continuación se definen los objetivos de este departamento.

OBJETIVOS, TAREAS, PROCEDIMIENTOS Y POLÍTICAS.

Los objetivos que este departamento debe cumplir son:

- Mantener en el nivel planeado el desempeño de la red.
- Monitorear y analizar el tráfico que circula por la red.
- Prevención de problemas futuros. Administración preactiva.
- Proporcionar servicios de seguridad a los elementos de red.
- Crear estrategias para la prevención y detección de ataques.
- Crear estrategias para la respuesta a incidentes.

El departamento de monitoreo y seguridad, contara con un conjunto de tareas, procedimientos y políticas establecidos, que serán las herramientas necesarias para el cumplimiento de sus objetivos. La atención a la red y la seguridad de esta se realizara en diferentes etapas, todas definidas, para asegurar el rendimiento optimo de la red. A continuación se definen las tareas de este departamento.

- Monitoreo
  - Recolección estadística de información referente al comportamiento de la red.
  - Utilización de enlaces.
  - Caracterización de tráfico.
  - Porcentajes de envío y recepción de información.
- Análisis
  - Utilización elevada.
  - Elementos principales de la red. Control de Trafico.
  - Errores elevados.
  - Rendimiento de red.
- Seguridad
  - Identificación de los activos de red.
  - Mecanismos de implementación.
  - Prevención y respuesta a incidentes.
  - Políticas de seguridad que sean consecuentes con la misión de Seguridad.

Los procedimientos que se realizarán para el cumplimiento de estas tareas serán los siguientes

- Análisis de la información para la toma de decisiones.
- Proceso de respuesta a incidentes.
- Procedimiento de alta y baja de cuentas de usuario.

Las políticas que este departamento debe hacer cumplir son:

- Políticas de uso de la red.
- Políticas de contraseñas.
- Políticas de respaldo.
- Procedimiento de altas y baja de usuarios.

DISEÑO DEL DEPARTAMENTO.

Consiste en establecer como se realizaran las tareas que anteriormente se definieron para este departamento.

El diseño de monitoreo estará orientado, a la extracción e interpretación de datos relacionados con el estado y el desempeño de los dispositivos conectados a la red. Mediante su correcta interpretación, y llevando un registro histórico de los acontecimientos que se van dando a lo largo del tiempo, así el personal de este departamento podrá determinar de manera más rápida el comportamiento de ciertos equipos e incluso, adelantarse y predecir el deterioro del nivel de servicio en alguna parte de la red.

La administración de los equipos de ruteo es una de las actividades de este departamento. Estos dispositivos son los encargados de dirigir la información de un lado a otro por la ruta más óptima. Una vez conectados a la infraestructura de la red, el personal de este departamento deberá mantener las configuraciones óptimas, de tal manera que puedan, seguir operando sin inconvenientes dentro de las modificaciones que se presentan con el tiempo dentro red.

Como ayuda a este departamento se utilizara el *software* que la Facultad ha adquirido, el "*EPICENTER*" de la marca *Extreme Networks*. Este software nos permite utilizar varias de sus herramientas para cumplir con las tareas de este departamento, tales como monitorear los equipos de comunicaciones, permitiéndonos monitorear estos dispositivos a través de un sistema visual que representa al dispositivo y nos permite configurarlo sin tener que dirigirse a la ubicación física del dispositivo, utilizando ya sea una sesión Telnet u otro programa. Con estas herramientas podemos monitorear el estado de los conmutadores así como modificar su configuración, esto claro solo para el personal autorizado.

El primer paso para utilizar el *EPICENTER* es ajustarlo a nuestras necesidades para esto utilizaremos el *Applet "Administration*" que sirve para definir las cuentas con las que trabajaremos al utilizar el *EPICENTER*

Ajustando el *EPICENTER*

Para iniciar sesión dentro del servidor *EPICENTER* y usar las utilidades de administración, se debe tener una cuenta de usuario y una contraseña. El personal de este departamento encargado del servidor puede crear y modificar cuentas de usuarios, contraseñas y permisos para cuentas, a través del *Applet "Administraction"*. Finalmente el *Applet "Administraction* nos permite modificar las propiedades que afectan el rendimiento y configuración del servidor *EPICENTER*.

Cuentas de usuario.

El administrador del servidor tendrá que realizar las acciones necesarias dentro de este *Applet* para que crear otras cuentas para ayudar a la gestión del servidor. Estas cuentas se detallan en la Tabla 5.13.

NOMBRE DE USUARIO	TIPO DE ACCESO	DESCRIPCIÓN
Admon	*Administrato*r	Puede crear y modificar cuentas dentro del servidor. Puede cambiar parámetro de dispositivos y también ver información y estadísticas
Manage	*Manager*	Puede cambiar parámetros de dispositivos y también ver información y estadísticas
Usuario	*Monitor*	Puede ver información y estadísticas

Tabla. 5.13 Cuentas de acceso del EPICENTER

El acceso, al servidor, con la cuenta "Admon" solo será necesario cuanto se creen o modifiquen cuentas de usuario. Para modificar los parámetros de los dispositivos y revisar la información estadística se utilizara la cuenta de "Manage". La cuenta de usuario será para visualizar las estadísticas y reportes de información.

Las contraseñas para cada cuenta creada, quedan a la elección del administrador, no se incluyen dentro de este trabajo, para evitar problemas de seguridad. Se recomienda cambiar las contraseñas de estas cuentas una vez al mes.

Usando el "INVENTORY MANAGER"

El "*Inventory Manager*" es un *Applet* que guarda una base de datos de todos los dispositivos de red administrados por el *EPICENTER*. Puede descubrir cualquier dispositivo que corra un agente compatible con MIB-2.

Provee una función automática para descubrir dispositivos dentro de la red. Esta característica puede descubrir dispositivos *Extreme* y dispositivos compatibles con MIB-2. También se pueden añadir dispositivos manualmente utilizando otras funciones del software.

Una vez que el dispositivo de red es reconocido en la base de datos del servidor, este puede ser asignado a un grupo especifico de dispositivos y configurarlo usando el "*Inventory Manager*" y otros *Applet* con que cuenta el software, también se pueden recibir alarmas acerca del dispositivo y se puede observar la topología jerárquica de los dispositivos que se conocen en la base de datos.

Grupos de dispositivos

Los dispositivos están organizados en uno o más "grupos de dispositivos". Un grupo de dispositivos es un conjunto de dispositivos de red que tienen características en común y que pueden ser administrados como un grupo. Un dispositivo puede pertenecer a uno y solo un grupo de dispositivos, todos los dispositivos al ser añadidos se incluyen a un grupo por defecto "Group Default", si uno no especifica otro.

Creación de los grupos de dispositivos

Para administrar los dispositivos de comunicaciones deberán ser añadidos a diferentes grupos. Estos grupos estarán formados por dispositivos que guardaran alguna característica en común. Se propone el siguiente conjunto de grupos, que tratan de organizar los equipos por estar la misma área de ubicación y similar cantidad de dispositivos por grupo. La Tabla 5.14 muestra esta propuesta.

GRUPO	NOMBRE	NUMERO DE DISPOSITIVOS (CONMUTADORES)	CLOSET DE UBICACIÓN DE LOS DISPOSITIVOS
1	POSTGRADO	5	23
2	EDIFICIO A	5	1,2,3,4,5
3	EDIFICIO B1	5	18,20,21,22
4	EDIFICIO B2	5	17,14
5	EDIFICIO B3	4	11,15,16,24
6	ANEXO BIBLIOTECA	4	13,12
7	EDIFICIO C	3	7
8	DIRECCIÓN	2	10,11
9	ALMACÉN INGENIERÍA	2	8,6,9

Tabla. 5.14. Grupo de dispositivos en el EPICENTER

Se muestra el nombre de los grupos que deberán ser creados dentro del *Applet "Inventory Manager*" y los dispositivos que serán agregados a cada grupo. Esta división tratara de asociar los dispositivos según su ubicación y cantidad de dispositivos, tratando de lograr grupos homogéneos lo más cercano posible. Esta configuración tendrá que ser hecha por el administrador del servidor.

Se puede utilizar el "*Gruping Manager*" para administrar estos grupos, crear grupos de dispositivos, puertos, usuarios, y VLAN, que pueden ser tratados como una sola entidad

Monitoreo

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos tales como la utilización de enlaces, caracterización del trafico, porcentaje de transmisión y recepción de información, etc. Para esta actividad se puede utilizar una de las herramientas del *EPICENTER* llamada "*Real-Time Statistics*".

Usando el "*Real-Time Statistics*"

El "*Real Time Statistics*" de *EPICENTER* nos permite visualizar una representación grafica de estadísticas de errores y utilización en tiempo real para dispositivos administrados. Los datos son tomados desde la base de información de administración (MIB) de la tabla "*EtherHistory*" del monitoreo remoto (RMON). Para esto se debe tener habilitado RMON para el dispositivo administrado.

Se pueden obtener datos para múltiples puertos de un dispositivo, una ranura de expansión, o dentro de un grupo de puertos y opcionalmente mostrar el conjunto de datos más relevantes (TOP N). También es posible configurarlo para que los datos sean actualizados en intervalos de tiempos definidos.

Se ocupara este *Applet* para realizar las siguientes actividades

- Monitorear el porcentaje de utilización para cada puerto utilizado dentro de todos los conmutadores.
- Monitorear el porcentaje de errores para cada puerto utilizado, dentro de todos los conmutadores.
- Monitorear el porcentaje de utilización del enlace de fibra óptica de cada conmutador.

Esta información debe ser almacenada agrupándola al conmutador al que pertenece.

Caracterización de tráfico

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

Analizadores de red

Un analizador de red, llamado también analizador de protocolo, es un dispositivo que rastrea la información estadística de una forma muy parecida al supervisor de red, pero con un nivel de servicio más sofisticado. De hecho, estos dispositivos son tan sofisticados e inteligentes que no sólo detectan e identifican problemas, como cuellos de botella, sino que también los solucionan.

Existe un analizador de red de la marca Fluke llamado "*Optiview Protocol Expert*". Este es un analizador y monitor de red en software que permite la caracterización del trafico, identificar degradación en la red, captura de paquetes, además de la decodificación en los siete niveles del modelo OSI, lo que facilita la identificación y la solución de los problemas más complicados en segmentos conmutados. Este software es propietario y necesita el pago de una licencia de uso para su implementación. Por otra parte existe otro analizador de red llamado "*Ethereal*" que es un software de licencia libre distribuido debajo la licencia GNU, que quiere decir que no requiere pagos de licencias para su distribución e implementación.

Para realizar la actividad de caracterización de trafico podemos utilizar uno de estos dos analizadores de red. Siguiendo el mismo rumbo de las propuestas hechas en los capítulos anteriores, de utilizar software libre para evitar gastos excesivos, utilizaremos Ethereal como analizador de red.

A continuación se presenta una guía corta de uso para el *Ethereal*, para conseguir una introducción básica del software y las características que ocuparemos para realizar las actividades de este departamento. Esta guía no intenta decir todo sobre el software y una vez que el personal de este departamento haya aprendido los fundamentos estos pueden continuar por sí solos.

Instalando el *Ethereal*

Ethereal y las utilidades que tienen asociadas son instaladas como parte del software ejecutable que se puede obtener en www.ethereal.com/distribution/win32/. Para mas detalles de la instalación pueden dirigirse a la página http://www.ethereal.com/.

Usando *Ethereal*

Para comenzar a familiarizarse con el uso del software seguiremos los siguientes pasos.

1. Para iniciar el programa, en Windows dar clic en el botón inicio, programas y *Ethereal*.
2. Seleccionar *Ethereal*. Aparecerá una pantalla como la que se muestra en la Figura. 5.10, *Ethereal* despliega una ventana que consiste en tres partes. En un inicio estos paneles están en blanco.

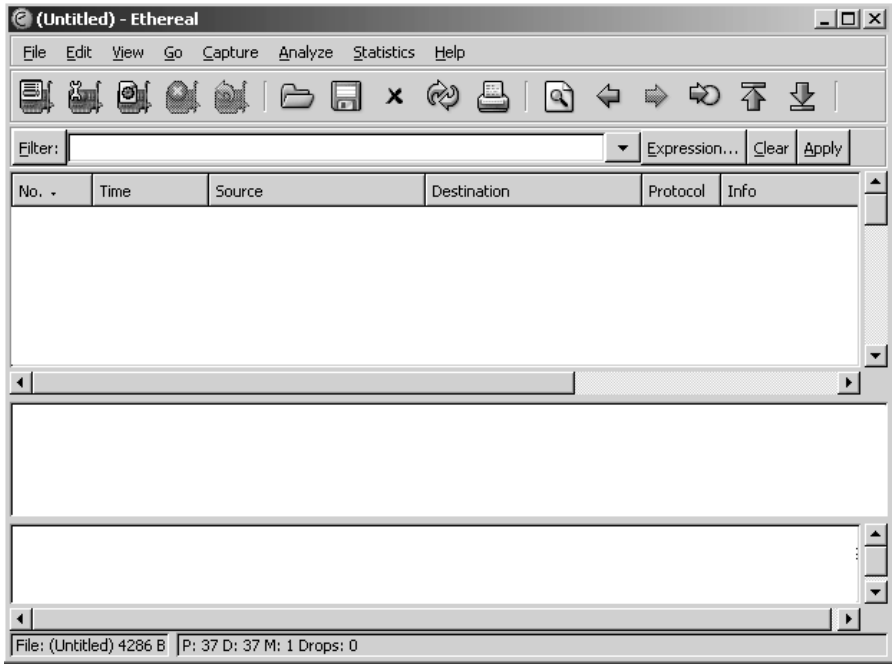

Figura 5.10 Ventana de inicio del Ethereal

Captura de paquetes

Para capturar paquete debemos abrir el menú "*Capture*" y dar clic en la opción "*Options*". Aparece una ventana como la que se que se muestra en la Figura 5.11.

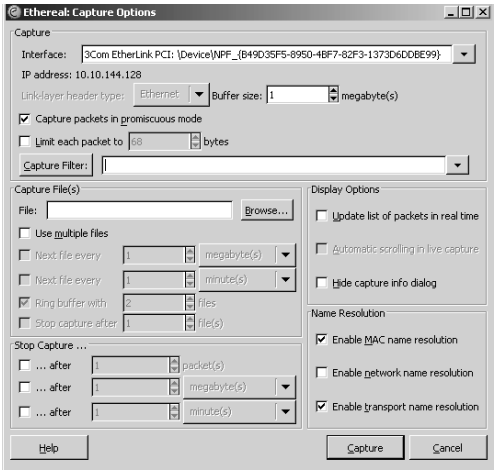

Figura .5.11 Opciones de captura del *Ethereal*.

Dentro de esta ventana tenemos varias opciones. Las opciones están agrupadas por funciones. La Tabla 5.15 muestra la agrupación y la descripción de estas funciones.

GRUPO	DESCRIPCIÓN
CAPTURE	Aquí se puede limitar el tamaño en bytes de los paquetes capturados, o solo capturar una parte de los paquetes. Esto es útil si se desea solamente la información de cabecera, y si uno quiere mantener archivos pequeños. La opción de "*Capture packets in promiscuous mode*" se utiliza para capturar todo lo que pasen por el segmento de red al que estemos conectados. Si uno desea ver los paquetes de entrada y de salida esta opción debe estar seleccionada. Además podemos establecer un filtro para los paquetes capturados.
CAPTURE FILES	Aquí podemos establecer el nombre del archivo donde se guardaran los paquetes capturados. Usar la opción "*ring bufer*" permite especificar el número de archivos a usar en la captura. En esta opción cuando un archivo esta lleno uno nuevo comienza a grabarse. Cuando el número específico de archivos están todos llenos la captura inicia nuevamente sobrescribiendo los archivos en la secuencia inicial. Esta función es útil si uno desea capturar continuamente pero no desea llenar el disco duro.
DISPLAY OPTION	Se usa para actualizar la lista en tiempo real.
CAPTURE LIMITS	Esta opción limita el número de paquetes que uno puede capturar. Aquí tres opciones, limitar el numero de paquetes, por una cantidad de espacio de disco, o por tiempo.
NAME RESOLUTION	Establece el nombre de resolución.

Tabla 5.15. Grupos de funciones de captura de Ethereal.

Cuando se ha establecido los parámetros que uno requiere podemos utilizar el botón "capture" para comenzar la captura. Todos los paquetes que circulen por el segmento de red al que estemos conectados, comenzaran a ser capturados. El proceso de captura se muestra en una ventana como la de la Figura 5.12.

La captura continuara hasta llegar al numero de paquetes que uno estableció o hasta que demos clic en el botón "*stop*".

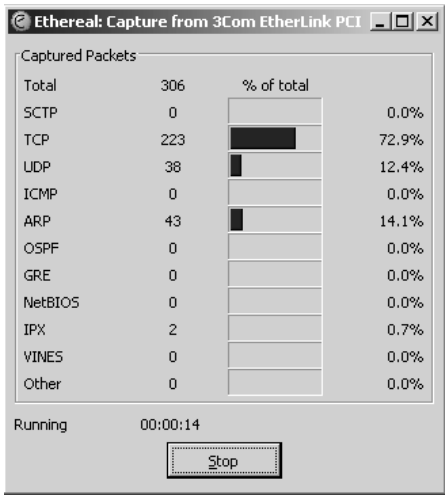

Figura 5.12 Ventana de captura de *Ethereal*.

Detenida la captura se mostrará una ventana con de los paquetes capturados, esta ventana incluye información como el número de paquete, el tiempo de captura, el origen y destino del paquete, el protocolo, etc. En la Figura 5.13 se muestra esta pantalla. En esta ventana uno puede explorarla hasta encontrar los tipos de paquetes buscados y dar clic en el para observar los detalles.

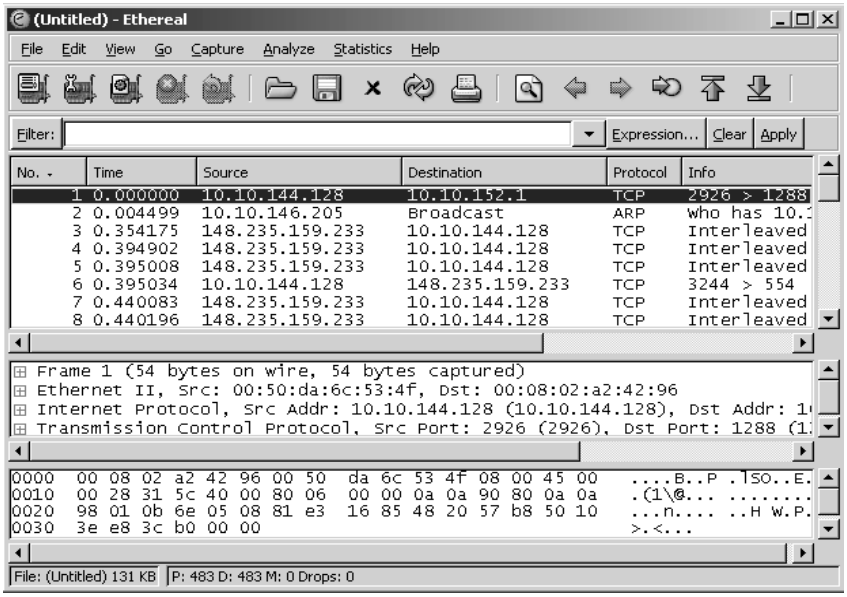

Figura 5.13. Información de captura de paquetes en *Ethereal*

Filtrado de paquetes

Ethereal puede realizar un filtrado de los paquetes capturados, esta opción es muy útil ya que puede crear filtros que clasifiquen todo el tipo de trafico generado en la red, por protocolo, dirección IP origen o destino, dirección MAC, trafico entre equipos, etc.

Para crear un filtro abrimos el menú "*Analize*" y damos clic en la opción "*display filters*" o con ayuda de la caja de dialogo que se encuentra debajo de los botones de la barra de herramientas.

Crear un filtro puede ser muy complejo, pero las buenas noticias son que uno no tiene que saber mucho sobre la sintaxis de filtros para hacer filtros útiles. La manera en gran medida más fácil de construir los filtros está en ayudarse en la estructura de los protocolos. Conociendo parte del protocolo podemos filtrarlos por sus características.

Si queremos escribir un filtro rápidamente para filtrar los paquetes de un protocolo en especifico, basta con escribir dentro de la caja de dialogo el nombre de protocolo a filtrar para filtrar todos los paquetes que coincidan con este protocolo. Lo mismo podemos hacerlo con una dirección MAC o IP. Podemos generar filtros más complejos con la ayuda de la sintaxis creada para estos filtros. Se puede obtener ayuda de esta sintaxis de filtros en la ayuda incluida en el propio programa.

Después de familiarizarse con este software, se utilizaran sus herramientas para caracterizar él tráfico que circula en la red. Para esto se realizaran las siguientes actividades.

1. Capturar el tráfico en cada segmento de red diariamente por un periodo de 10 minutos. Se debe procurar capturar el tráfico en las horas de mayor actividad en la red.
2. Crear un filtro para agrupar los paquetes capturados por protocolos.
3. Crear un filtro para agrupar los paquetes capturados por dirección MAC destino.
4. Crear un filtro para agrupar los paquetes capturados por dirección MAC origen.
5. Con esta información crear filtro del protocolo y servicios más utilizados dentro de la red.
6. Almacenar esta información, agrupada por segmento y hora de captura.

Análisis.

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

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

Utilización elevada.

Si se detecta que la utilización de un enlace o un puerto es muy alta, deberá tomarse la decisión de incrementar el ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso de debe informar el incidente para verificar la seguridad de red.

Cuando un puerto o un enlace se detecte con una utilización elevada (mas del 80% de su capacidad), durante un periodo largo, será necesario tomar una de las acciones descritas en el párrafo anterior.

Elementos principales de la red. Control de Trafico

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

Con esta información se realizará un reporte, para informar que elementos son los de mayor tráfico y que elementos han incrementado su tráfico misteriosamente y tomar las decisiones en seguridad que estos elementos requieran. Si las acciones tomadas no son suficientes, éstas se deben reforzar para que lo sean, es decir, se debe estar revisando y actualizando constantemente.

Errores elevados

Si existen elementos con una alta taza de errores puede deberse a una mala configuración del dispositivo o un daño en el *hardware*. Si esto sucede se informara al departamento de operación y mantenimiento encargado de las fallas de estos dispositivos.

Rendimiento de red

Las evaluaciones periódicas de la red para caracterizar el tráfico es una herramienta de prevención y mantenimiento importante que pueden ayudar a asegurar que la red continúa funcionando a un nivel aceptable. La primera evaluación del comportamiento se debe hacer después de que la red haya estado operativa durante un buen periodo de tiempo. Se debe basar en la información proporcionada por el monitoreo y por la información disponible del Centro de informática y otros departamentos. Después de completar esta información, se debe presentar los resultados de la evaluación bajo la forma de un informe de evaluación. Esto permitirá llevar un registro del funcionamiento de la red y si la red va a continuar funcionando como se espera. El propósito del informe de evaluación es revelar los puntos fuertes y débiles de la red, para que se puedan corregir si fuese necesario.

Por ejemplo, los registros que mantiene el analizador de red pueden indicar una tendencia hacia una velocidad de tráfico más lenta en ciertos segmentos de la red. Una auditoria actualizada del *hardware* y el *software* de la red puede revelar la adición de varios dispositivos de red nuevos que funcionan con aplicaciones que generan gran cantidad de tráfico en dichos segmentos. Cuando ambos conjuntos de datos se juntan y se presentan como un informe de evaluación, esta información puede ser utilizada como base para proponer cambios en la red y en su funcionamiento.

Es posible detectar situaciones anormales como el tráfico inusual dentro de la red. Con la ayuda de las estadísticas de los analizadores, podemos identificar el tráfico común que circula dentro de la red. El análisis constante de estas estadísticas mostrara si se mantiene ese mismo tráfico o existe otro que antes no era común dentro de la red. Esto en realidad, consiste en detectar comportamientos anómalos o cosas que se desvíen del comportamiento normal. Esta técnica es muy buena para detectar ataques que no habían sido considerados con anterioridad.

Seguridad

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

Para cada recurso en la red, este departamento aplicara los mecanismos para establecer permisos de utilización, así como monitorizar el uso que se hace de los recursos. Todas estas tareas, se basaran en las políticas de uso la red que se incluyen en el Apéndice B. Otro aspecto a considerar es el de la monitorización y registro de las actividades de los usuarios pudiendo denegar el acceso de los usuarios en función de que intenten realizar actividades para los que no tienen permiso. Esta

actividad podría ser utilizada posteriormente con la ayuda del departamento de Contabilidad y de los procedimientos de auditoria.

En este apartado se tratara de proponer un diseño de seguridad para atender las cuestiones asociadas con el incremento de los requisitos de seguridad y se abordaran los pasos necesarios para desarrollar las estrategias de seguridad y el cumplimiento de los objetivos de este departamento.

Identificación de los activos de red

Para poder realizar un buen diseño de seguridad, es necesario identificar perfectamente los activos de red que debemos proteger. Los activos de red se pueden dividir en dos, los físicos y los lógicos, Los activos físicos son los equipos, servidores, conmutadores y enrutadores y los lógicos, que son los servicios de red, como Web, correo electrónico, FTP, los sistemas operativos, las aplicaciones y los datos contenidos en los equipos. También será necesario saber el lugar físico donde se encuentran y quien esta a cargo de estos.

En la Tabla 5.16 se presenta la relación de activos que serán protegidos dentro del esquema de seguridad.

NO. DE CLOSET	DENOMINACIÓN DEL ÁREA	SERVICIOS DE DATOS	EQUIPOS ACTIVOS (CONMUTADORES)
1	LABORATORIO DE FÍSICA	44	1
2	LABORATORIO 1D	29	1
3	LABORATORIO 2D	31	1
4	LABORATORIO 3D	21	1
5	LABORATORIO 4D	34	1
6	FÍSICO QUÍMICA	29	1
7	DIRECCIÓN	58	2
8	LABORATORIO	29	1
9	ESTRADO A	2	-
10	CENTRO INFORMÁTICA	77	2
11	LABORATORIO 105	18	1
12	BIBLIOTECA	43	1
13	SALA DE CURSOS	110	3
14	SICA	169	4
15	MULTIMEDIA	112	3
16	USAI	5	1
17	LABORATORIO 101	41	1
18	SRIA. ADMITIVA	65	2
19	LABORATORIO 102	13	1
20	LABORATORIO 209	25	1
21	LABORATORIO 307	19	1
22	IDIOMAS	12	1
23	COMPUTO	224	5
24	ALMACEN	3	1

Tabla 5.16 Activos físicos a proteger por el área de seguridad

Los equipos asignados a los usuarios, así como los servidores de red serán también parte de los activos físicos que serán protegidos, su ubicación y el personal asignado a cada equipo, se encuentra en el inventario con el que cuenta el Centro de informática de la Facultad de Química, este departamento debe solicitar esta información para tener conocimiento de todos los equipos que este departamento protegerá en su plan de seguridad. Toda la información contenida en estos equipos y los servicios de red serán protegidos como los activos lógicos.

Mecanismos de implementación.

El primer paso será otorgar servicios de seguridad a los activos de la red, para esto existen mecanismos ya establecidos que proporcionan seguridad básica dentro de la red para asegura su continuo servicio. Estos mecanismos son:

- Mecanismos de Autentificación, Autorización, Auditoria.
- Administración de usuarios y contraseñas (Servidor RADIUS).
- Cifrado de datos.
- Filtros de paquetes.
- Políticas de Respaldo.
- *Firewall* y Detección de intrusos.
- Control de acceso físico.
- Respuesta a incidentes de seguridad.

Mecanismos de Autentificación, Autorización y Auditoria.

La autentificación de usuarios dentro de la red ya esta definida por completo dentro del esquema de configuración de la red, este proceso incluye un servidor de autentificación RADIUS donde los usuarios tendrán que autentificarse para hacer uso de la red. La autentificación se hace cuando el usuario ingresa un nombre de usuario y una contraseña que el servidor RADIUS tiene validados.

La autorización de usuarios dentro de la red también esta definido en el esquema de configuración de la red. Cada usuario al pertenecer a una VLAN tendrá diferentes servicios. La modificación de los servicios que otorga cada VLAN y el cambio de usuarios dentro de las VLAN deberá ejecutarlo el personal de este departamento.

La auditoria de usuarios quedara pendiente en este esquema, posteriormente podrá ser incluido para su implementación como parte de la administración de la red; pero esto ya dependerá de los avances y desarrollos que en seguridad se tengan dentro del futuro de la red.

Administración de cuentas de usuarios y contraseñas (Servidor RADIUS)

Para este tipo de actividades es indispensable tener un manual de procedimientos escrito y llevarlo a cabo al pie de la letra. De esta manera, cabría pensar que un manual de procedimientos es un paso adelante para poder llegar a la calidad deseada.

Procedimiento de alta y baja de cuentas de usuario

Cuando un nuevo elemento de la Facultad requiere una cuenta de acceso a la red, se deberán seguirse los siguientes pasos:

1. Deberá llenarse un formulario que contenga, al menos los siguientes datos:

    - Nombre y Apellido del usuario.
    - Puesto de trabajo.
    - Jefe inmediato superior que avale el pedido.
    - Descripción de los trabajos que debe realizar en el sistema.
    - Consentimiento de que sus actividades son susceptibles de ser auditadas en cualquier momento y de que conoce las políticas de uso (para lo cual, se le debe dar una copia de tales políticas que se incluyen en el apéndice B).
    - Asimismo, este formulario debe tener otros elementos que conciernen a la parte de ejecución del área encargada de dar de alta la cuenta, datos como:
        - Tipo de cuenta.
        - Fecha de caducidad.
        - Fecha de expiración.
        - Datos referentes a los permisos de acceso (por ejemplo, tipos de permisos a los diferentes directorios y / o archivos, VLAN).
        - Si tiene o no restricciones horarias para el uso de algunos recursos y / o para el ingreso al sistema.

2. El almacenamiento digital de datos estará a cargo del personal de este departamento, y deberá hacerse en una base de datos, puede ocuparse el gestor de bases de datos incluido en el paquete Office de Microsoft.

3. La asignación de la VLAN a la cual pertenecerá cada cuenta de usuario dependerá del trabajo que este realizara dentro de la red. Se deberá incluir la cuenta dentro de una VLAN que de soporte a las actividades para el éxito de su trabajo.

4. Se asignara un nombre de usuario y una contraseña a cada cuenta. Las políticas de nombres de usuario y contraseñas se incluyen dentro del apéndice B.

5. Se creara la entrada en los archivos de usuarios del servidor RADIUS incluyendo el nombre de usuario, la contraseña y la VLAN asignada.

6. Generar el documento informativo de los datos de la cuenta creada, se entregara una copia al usuario y otra se utilizara como resguardo.

Procedimiento de baja de cuenta de usuario

Este procedimiento es el que se lleva a cabo cuando se aleja un elemento de la Facultad o cuando alguien deja de trabajar por un determinado tiempo (licencia sin goce de sueldo, vacaciones, viajes prolongados, baja temporales etc.). Sobre la base de la explicación anterior hay, entonces, dos tipos de alejamientos: permanente y parcial.

Aquí, es necesario definir un circuito administrativo a seguir, y saber que todos los componentes del diseño de seguridad, debe estar fuertemente apoyado por la parte administrativa de la Facultad.

Un ejemplo de este circuito, podría ser: ante el alejamiento de un elemento de la Facultad, la sección encargada de la administración de los recursos humanos o el departamento de servicios escolares, debe informar en un formulario de “Alejamiento de personal”, todos los datos del individuo que ha dejado la organización, así como de la posición que éste ocupaba y el tipo de alejamiento (permanente o no). Una vez llegada la información al Centro de informática, este lo informara a este departamento, y se utilizara para dar de baja o inhabilitar la cuenta del usuario.

La definición de si se da de baja o se inhabilita es algo importante pues, si se da de baja, se deberían eliminar los archivos y directorios del usuario, mientras que si sólo se inhabilita, no pasa de esta acción. Si el alejamiento del individuo no era permanente, al volver a la organización, la sección que había informado anteriormente de la ausencia, debe comunicar su regreso, por medio de un formulario dando cuenta de tal hecho para volver a habilitar la cuenta al individuo.

Cifrado de Datos

El cifrado de datos, no estará aun presente dentro de esta red. El Centro de Informática y los encargados del departamento de seguridad determinaran la necesidad de la implementación del cifrado de datos ya que esto implica un análisis como lo es la reducción del rendimiento de la red debido a la implementación de estos mecanismos de seguridad.

El cifrado constituye una opción de seguridad muy útil, ya que proporciona la confidencialidad de datos. Cuando un usuario o el administrador de la red considera que han analizado los riesgos que atraería la revelación de ciertos datos dentro de la red, es una solución muy útil, aunque atrae como desventajas puntos de fallo, si es que todo el trafico debe pasar por un solo punto de cifrado y el consumo de energía de CPU y memoria en los equipos, enrutador y servidores. Por otra parte existen servicios donde no es necesario el cifrado de datos como lo es la navegación en Internet, el correo electrónico y la transferencia de archivos.

Filtros de Paquetes

Los Filtros de paquetes se pueden configurar en enrutadores y servidores para aceptar o denegar paquetes provenientes de direcciones o servicios concretos. Los filtros de paquetes incrementan los mecanismos de autentificación y autorización. Estos ayudaran a proteger los recursos de red del uso no autorizado, de la sustracción, de la destrucción y de los ataques de denegación de servicio.

Las normas de seguridad deben declarar si los filtros de paquetes implementan una de las siguientes formas:

- Denegar tipos específicos de paquetes y aceptar todo lo demás.
- Aceptar tipos específicos de paquetes y denegar todo lo demás.

La segunda es la norma que propondremos para esta red, que es más fácil de implementar y más segura, ya que el personal de este departamento no tiene que prevenir ataques futuros en los que se vayan a denegar paquetes; también es más fácil de probar, ya que es un conjunto finito de usos aceptados en la red.

Los filtros de paquetes se implementan con las listas de acceso dentro de los enrutadores y conmutadores, que les permite controlar si el tráfico de red es reenviado o bloqueado por sus interfaces. Entre los criterios típicos se puede incluir la dirección de origen del paquete, la dirección de destino del paquete o el protocolo de capa superior del paquete.

Un criterio de acceso consiste de una combinación de los siguientes campos:

- Dirección MAC de destino u origen.
- Identificador de VLAN.
- Tipo de servicio IP.
- Protocolo IP.
- Dirección IP de destino, origen o mascara de Red.
- Puerto de destino u origen de capa 4.
- Bits de inicio de sesión TCP.
- Puerto de egreso o ingreso.

Las listas de acceso podrán ser tan elaboradas como el personal de este departamento lo crea conveniente, el análisis del tráfico ayudara a crear listas de acceso más especializadas, pero en un principio este trabajo recomienda la creación de las siguientes listas de acceso:

1. Negar todos los paquetes que provengan de la VLAN “alumnos” a las restantes VLAN, ya que la VLAN “alumnos” no necesitaran tener acceso a los equipos de las otras VLAN.

2. Negar tráfico hacia equipos por medio de la dirección MAC para que estos no tengan acceso a equipos donde se desea mayor seguridad. Para esto haremos lo siguiente:

    - Crear una lista de acceso para el puerto donde se encuentran ubicado el servidor de RADIUS y permitir el acceso a solo a los equipos que necesitan comunicarse con este servidor.

    - Crear una lista de acceso para negar el acceso a las áreas de “Dirección” y “Secretaria Administrativa” permitiendo el tráfico solo de áreas permitidas. Los alumnos no deberían tener acceso a estas áreas.

Las listas de acceso deben ser avaluadas constantemente para evitar disminuir el rendimiento de la red y evitar problemas de comunicación entre equipos. Se recomienda evaluarlas una vez al mes, para adaptarlas a los cambios de comunicación de los equipos de la red.

Políticas de Respaldo

Aquí especificaremos qué información debe respaldarse, con qué periodicidad, qué medios de respaldo utilizar, cómo deberá ser restaurada la información, dónde deberán almacenarse los respaldos, etc. Los siguientes puntos deberán seguirse para todos los respaldos de información hechos por este departamento. Toda la información que sea necesaria para mantener el buen estado de la red y su correcto funcionamiento será respaldada por este departamento. Si algún departamento de esta Facultad solicita respaldo de su información el proceso de respaldo seguirá los lineamientos aquí mencionados.

- El personal de este departamento es el responsable de realizar respaldos de la información periódicamente.
- La información respaldada deberá ser almacenada en un lugar seguro y distante del sitio de trabajo.
- Deberá mantenerse siempre una versión reciente impresa de los archivos más importantes de cada sistema importante dentro de la red.
- En el momento en que la información respaldada deje de ser útil a la Facultad o departamento que solicito el respaldo, dicha información deberá ser borrada antes de deshacerse del medio.

A continuación se presentan las políticas para realizar los respaldos de información:

1. La información básica a respaldar por este departamento será la siguiente:

    a. Archivos de configuración del servidor RADIUS.
    b. Archivos de configuración del servidor DHCP.
    c. Imágenes de configuración de los conmutadores departamentales.

2. Cada treinta días deberá efectuarse un respaldo completo del sistema y cada día deberán ser respaldados todos los archivos que fueron modificados o creados. El ciclo de respaldos puede cambiar según las necesidades de la propia red.

3. Todos los respaldos deberán realizarse en medios extraíbles, como discos compactos o cintas magnéticas. Se etiquetaran adecuadamente, con los siguientes datos: Fecha de realización, tipo de respaldo, cantidad de discos del respaldo, tipo de información, sistema, versión y departamento al que pertenece.

4. La información será restaurada inmediatamente después que surja un problema por falta de información o si el sistema no puede ser recuperado.

5. Los respaldos se almacenaran en este departamento en un lugar seguro y solo accesible al personal de confianza, donde se deberá tener las copias de respaldo así como el informe de todos los datos del respaldo.

Los respaldos de información representan la fuente de recuperación principal dentro de los planes de contingencia, deben considerarse parte fundamental en los procesos de seguridad. La actividad constante y programada de respaldos de información asegura la recuperación, casi total, de las actividades afectadas antes pérdidas de información y eventos de seguridad que ponen en riesgo el buen funcionamiento de los sistemas de la red.

Firewall y detección de intrusos

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

Un sistema de detección de intrusos (IDS por sus siglas en ingles) es un programa usado para detectar accesos desautorizados a un equipo o a un servicio de red. Estos accesos pueden ser ataques de habilidosos programadores, usuarios, etc. o software que usa herramientas de forma automática.

El funcionamiento de un “Detector de intrusos” se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos o comportamientos sospechosos, como puede ser el barrido o escaneo de puertos, paquetes malformados, etc.

Normalmente esta herramienta se integra con un *Firewall*, El detector de intrusos es incapaz de detener los ataques por si solo "excepto los que están incluidos en un dispositivo de *Gateway* con funcionalidad de *Firewall*", pero al estar trabajando en conjunto con el *Firewall* se convierten en una herramienta muy poderosa ya que se une la inteligencia del Detector de Intrusos que no solo analiza que tipo de trafico, si no que también revisa el contenido y su comportamiento, y el poder de bloqueo del *Firewall*, este al ser el punto donde forzosamente deben pasar los paquetes, ahí pueden ser bloqueados sin problema alguno.

En el mercado existen diferentes versiones, de *hardware* y de *software* para implementar estas soluciones. En *software*, por mencionar algunos, esta el *Intrusion Detection* de *Computer Associates* y el *SNORT* de software libre. En *hardware* esta de *Symantec*, el *Security gateway*, entre otros.

La implementación de una solución de este tipo, requiere de un análisis de costo y beneficio. El Centro de informática debe evaluar las necesidades de un sistema de detección de intrusos, ya sea en *software* o en *hardware*. El resultado de esta evaluación debe basarse en los requerimientos actuales y futuros de la red, así como en el costo de la implementación de este tipo de sistemas.

Aquí se recomienda el sistema de detección de intrusos llamado “*SNORT*” por estar basado en software libre. Los equipos a proteger en un inicio deberán ser los servidores y los equipos de comunicaciones; la administración de este departamento deberán evaluar que otros dispositivos deberán ser protegidos.

Control de Acceso Físico

Es uno de los controles principales para restringir el acceso físico a los dispositivos (servidores, estaciones de trabajo y closets) Los componentes a menudo utilizados son:

- Asegurar el edificio.- Asegurar todas las puertas no esenciales para que el acceso desde fuera requiera una llave o una tarjeta.
- Cámaras de seguridad.- Un sistema de cámaras de seguridad que permita el monitoreo de las entradas al edificio puede ser un efectivo impedimento así como la evidencia registrada de quien traspasa ilegalmente.
- Guardias de Seguridad.- Los guardias de seguridad que validen la entrada de todos los empleados y otros visitantes.
- Candados de computadoras. Usar *hardware* especializado que restrinja el acceso a los teclados, monitores, controladores, etc.

Respuesta a incidentes de seguridad

Aún si la administración de la seguridad de la red tiene implementado procesos y herramientas para la detección de amenazas y vulnerabilidades, y adicionalmente posee una infraestructura y mecanismos de seguridad, los incidentes de seguridad podrían ocurrir. Un incidente de seguridad puede ser cualquier evento que compromete el ambiente de seguridad de la red.

Para evitar estas situaciones, este departamento debe emprender actitudes preactivas para asegurar que su ambiente está preparado para identificar eventos y mitigar los posibles daños en el menor tiempo posible, reduciendo el impacto del incidente y el costo de la investigación.

Proceso de respuesta a incidentes

Las respuestas a incidentes[5] comprenden un grupo de etapas que este departamento debe cumplir cuando un evento de seguridad ocurra. Un proceso de respuesta a incidentes ayudaría a manejar correcta y eficientemente un evento inusual determinado. Asimismo, el diseño de un proceso para el monitoreo y respuesta a incidentes podría ayudar a identificar la necesidad de recursos y asignación de roles y responsabilidades. La Figura 5.14 ilustra el proceso recomendado para el monitoreo y respuesta a incidentes de manera efectiva.

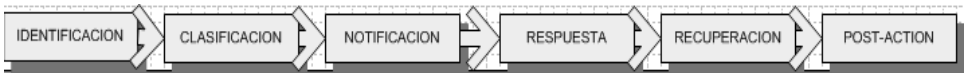

Figura 5.14. Proceso de respuesta a incidentes

Para un mayor entendimiento de cómo se interrelacionan cada una de las etapas del proceso de respuesta a incidentes, la Figura 5.15 muestra el flujo de acciones que ejecutaría el equipo de respuesta definido.

Identificación del incidente

Este departamento debe determinar si el incidente es un ataque real o una falsa alarma, y de ser un ataque real, debe identificar el tipo específico de ataque. Algunos tipos comunes de incidentes incluyen:

- Ataques a sitio de la red.
- Ataques de denegación de servicio.
- Escaneo de puertos (Scan por siglas en ingles).
- Escuchar tráfico (Sniffing por sus sigla en ingles).
- Ingeniería social.
- Acceso no autorizado.
- Infección de virus.

Categorizar el incidente por tipo, contribuye a hacer seguimiento y entender el riesgo al que se encuentra sometida la Facultad.

Clasificación del incidente

Durante el proceso de clasificación, se asigna un nivel de severidad al incidente, con la finalidad de controlar los recursos y el tiempo para afrontarlo. Para proveer un marco consistente para categorizar la severidad de los incidentes, la organización debe desarrollar una escala de calificación. A continuación se sugiere un esquema de clasificación:

- Nivel de Severidad 1: Crisis.
- Nivel de Severidad 2: Incidente Serio.
- Nivel de Severidad 3: Incidente.
- Nivel de Severidad 4: Evento.

En esta escala, el nivel superior (“Crisis”), es el más severo e indica que la Facultad está “corriendo peligro”. Por ejemplo, una situación bajo esta categoría sería un acceso no autorizado o borrado de la información almacenada en un servidor crítico. Durante una crisis, debe destinarse de manera total, todos los recursos y tiempo necesario para remediar el problema.

El segundo nivel (“Incidente Serio”), implica que el daño está ocurriendo a la Facultad, por lo que se requiere atención inmediata para prevenir que el incidente escale a un nivel de crisis. Por ejemplo, ha sido expuesta información de cuentas de usuario que puede ser utilizada para realizar un acceso no autorizado.

[5] http://pc-news.com/detalle.asp?sid=&id=11&Ida=1999

El tercer nivel (“Incidente”), es algo que debe ser resuelto, pero su nivel de urgencia es bajo. Por ejemplo, un detector de intrusos ha identificado un escaneo de la red interna de una compañía. En este caso, la organización experimenta poco o ningún daño, pero el incidente es un indicador claro que alguien o algo está intentando identificar sistemas o encontrar vulnerabilidades que explotar.

El cuarto nivel (“Evento”), es similar a un incidente, el cual debe ser resuelto, pero el grado de urgencia es menor. Por ejemplo, que una cuenta ha sido bloqueada después de múltiples intentos fallidos de acceso, esto podría significar que una persona no autorizada está intentando adivinar las contraseñas de usuarios para ganar acceso al sistema.

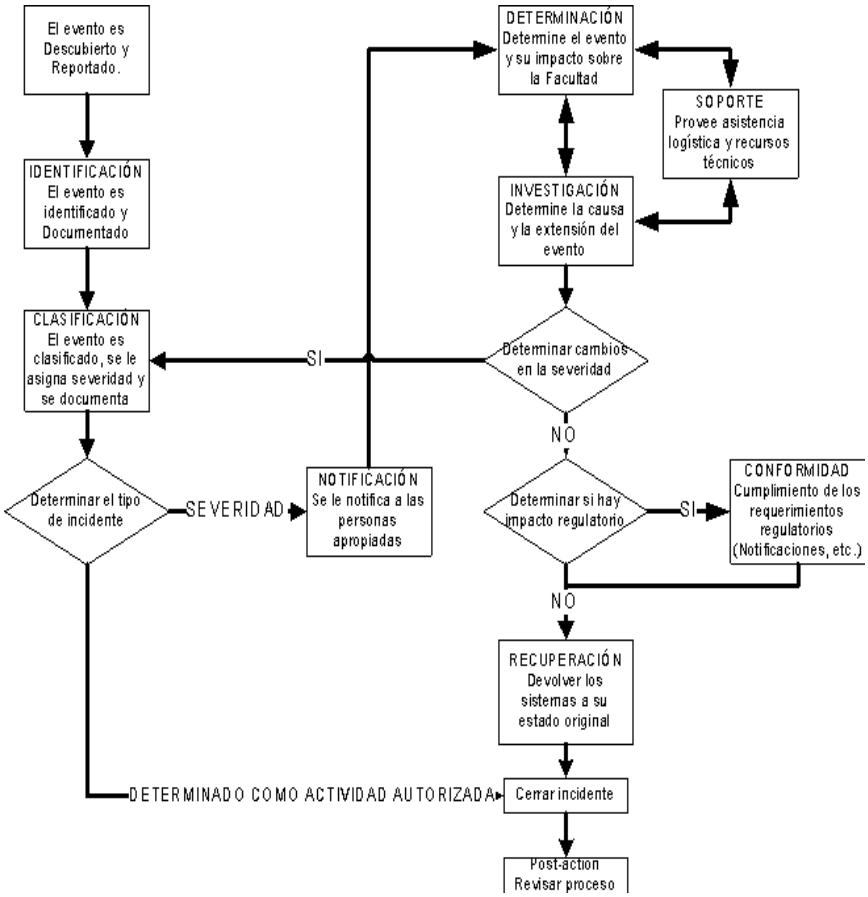

Figura 5.15. Diagrama de flujo de acciones a seguir por el equipo de respuesta a incidentes.

Notificación del incidente

Cuando un incidente ha sido identificado, el nivel de severidad determinará las personas apropiadas que deben ser notificadas de la ocurrencia de dicho incidente, con el fin de que realicen las acciones adecuadas de acuerdo con sus roles y responsabilidades.

Respuesta al incidente

El diseño de patrones de respuesta recomendados contribuye a realizar una evaluación del incidente y a coordinar las actividades de respuesta y el nivel de severidad asignado ayuda a establecer medidas apropiadas de investigación. La fase de respuesta puede ocurrir en paralelo con las etapas clasificación y notificación. Las tres áreas primarias en esta fase son: evaluación, investigación y soporte.

Evaluación. La evaluación comienza en el instante en que el incidente es identificado. Implica la recolección de todos los datos relevantes sobre el incidente por parte de los miembros del equipo de respuesta a incidentes y la determinación del impacto en las operaciones de la organización.

Los miembros relevantes del equipo de respuesta a incidentes deben planificar las acciones de restauración y cumplir con los requerimientos mínimos que se mencionan a continuación:

- Conexiones: Identificar todas las conexiones activas desde y hacia el activo comprometido.
- Registro: Registrar cualquier actividad observada, si la actividad del incidente se encuentra en progreso.
- Plan de recuperación de desastres: Determinar la necesidad de la activación de los planes de recuperación de desastres o plan de continuidad del negocio.
- Reemplazo: Determinar los recursos disponibles para reemplazar los activos afectados.
- Investigación. La investigación determina la causa y alcance del incidente. Identificar la causa contribuye a revelar las vulnerabilidades técnicas que permitieron el evento. Esta actividad ayuda a identificar todas las máquinas e información comprometida, modificada o eliminada, y cualquier información o lógica maliciosa almacenada durante el incidente que sea utilizada para comprometer el resto de los componentes de red.

El personal debe identificar cuáles máquinas fueron comprometidas, incluyendo la máquina directamente afectada por el intruso, las máquinas cuya información de cuentas y contraseñas pudieron ser capturadas y todas las máquinas que comparten el mismo segmento de red con la máquina comprometida. El personal encargo de la seguridad de la información asisten al personal de respuesta a incidentes identificando y adquiriendo evidencia sobre la naturaleza y causa del incidente, mientras los miembros del equipo de respuesta a incidentes documentan y mantienen informado al líder de su equipo sobre todos los pasos de la investigación.

De considerarse apropiado, el líder del equipo de respuesta a incidentes recolectará y documentará todos los registros necesarios para transferir la investigación a las autoridades que correspondan. En este sentido el líder del equipo debe contar con el apoyo institucional para hacer valer las políticas y reglamentos.

Soporte. El tiempo es un componente crucial durante un evento de respuesta a incidentes. Si el equipo de investigación no puede tener acceso inmediato a los sistemas y redes afectadas, este retraso podría incrementar el alcance y la severidad del incidente. El equipo de respuesta a incidentes debe apoyarse con los demás departamentos para que pueda proveer acceso a los recursos para sostener el esfuerzo de respuesta a incidentes.

Recuperación del incidente

El objetivo primordial de la etapa de recuperación es devolver a los equipos o dispositivos comprometidos a un estado seguro y operacional, de la manera más eficiente posible. La fase de recuperación le permite a los usuarios evaluar el daño ocurrido, la información que se ha perdido y cuál es el estatus del sistema posterior al ataque.

Todas las máquinas comprometidas requieren ser recuperadas. La recuperación debe estar a la par del nivel de compromiso. En caso de cuentas compartidas y contraseñas capturadas, que no fueron utilizadas para comprometer otros sistemas, un simple cambio de contraseñas podría ser toda la recuperación adecuada. Algunos incidentes pueden requerir la reconstrucción del sistema a partir de los medios de instalación.

El proceso de recuperación debe ocurrir fuera de línea siempre y cuando sea posible. Si la máquina es esencial para las operaciones, la organización debe considerar un reemplazo temporal mientras el equipo es reconstruido y asegurado. Si es necesario reconstruir varias máquinas, todas deben ser llevadas a un estado fuera de línea simultáneamente y luego ser reconectadas una vez aseguradas. Los miembros del equipo de recuperación de incidentes deben proveer instrucciones durante esta etapa, pero el personal encargado de la seguridad de la información debe realizar efectivamente la reconstrucción y aseguramiento de los sistemas.

Luego de haberse completado todas las evaluaciones y acciones de investigación, el líder del equipo de respuesta a incidentes debe proveer instrucciones al personal encargado de la seguridad de la información, responsables de la recuperación. Estos a su vez deben informarle sobre las acciones de recuperación que se llevan a cabo, para labores de seguimiento, evaluación y reflexión sobre el incidente.

Una actividad "*post-action*" es una reunión que se lleva a cabo una vez que se haya resuelto el incidente. El propósito de la reunión es discutir las lecciones aprendidas y las mejoras que pueden ser implementadas para resolver de mejor forma un evento similar en el futuro. Esta debe llevarse a cabo dentro de las dos semanas siguientes a la resolución de cada incidente de seguridad o ataque simulado.

Queda como responsabilidad del líder del equipo de respuesta a incidentes:

- Programar y liderar la reunión *post-action*.
- Documentar las lecciones aprendidas.
- Hacer seguimiento.
- Desarrollar el reporte final, el cual debe incluir las acciones tomadas.

La sesión "*post-action*" debe enfocarse en las acciones que funcionaron y las que no funcionaron durante el proceso de respuesta al incidente e incluir a todos los participantes que trabajaron en la resolución del incidente.

STAFF TÉCNICO.

Todas las actividades asociadas a este departamento serán realizadas por un grupo de trabajo, que cumplirá diversas características, además de compartir las actividades establecidas para este departamento.

Como propuesta inicial se recomienda que el equipo sea conformado por 6 integrantes, que cubrirán a todas las actividades de este departamento. Los elementos deberán tener experiencia y conocimiento en los puntos que se incluyen en la Tabla 5.17.

PERFIL DEL PERSONAL PARA EL DEPARTAMENTO DE MONITOREO Y SEGURIDAD
• Manejo de sistemas operativos a nivel administración (Windows todas las versiones, Novell o Linux).
• Experiencia en análisis de red.
• Experiencia en seguridad informática ajuste de sistemas y mecanismos de seguridad, detección de intrusos y similares.
• Experiencia en gestión de cuentas de usuarios.
• Conocimientos de seguridad Informática.
• Conocimientos de TCP/IP.

Tabla 5.17. Perfil del personal de Monitoreo y Seguridad

DEPARTAMENTO DE OPERACIÓN Y MANTENIMIENTO

A continuación se establecen los objetivos tareas, procedimientos y políticas del Departamento de Operación y Mantenimiento. Este departamento realizara las funciones de dos de las áreas del modelo TMN, la administración de configuración y la administración de fallas.

OBJETIVOS, TAREAS, PROCEDIMIENTOS Y POLÍTICAS.

Los objetivos que este departamento debe cumplir son:

- Satisfacer los requerimientos actuales y futuros de la red.
- Mantener un manejo adecuado de los recursos de *hardware* y *software*.
- Detectar y solucionar situaciones anormales en la red.

El departamento de operación y mantenimiento, contará con un conjunto de tareas, procedimientos y políticas establecidos, que serán las herramientas necesarias para el cumplimiento de sus objetivos. La operación de la red y el mantenimiento de esta se realizará en diferentes etapas, todas definidas para asegurar el rendimiento optimo de la red. A continuación se definen las tareas de este departamento.

- Planeación y diseño de la red.
- Selección de los recursos necesarios para mantener los sistemas y dispositivos en condiciones de operación.
- Instalación y Administración del *hardware* y *software*.
- Aprovisionamiento.
- Manejo de configuraciones en equipos.
- Monitoreo de alarmas.
- Localización de fallas.
- Pruebas de diagnóstico.
- Corrección de fallas de red.
- Administración de reportes.

Los procedimientos que se realizarán para el cumplimiento de estas tareas serán los siguientes

- Procedimiento de instalación de *Hardware*.
- Procedimiento de instalación de *Software*.
- Procedimiento de pruebas de diagnóstico.
- Procedimiento general de corrección de fallas.

Las políticas a seguir en este departamento son las siguientes:

- Políticas de respaldo de configuraciones.
- Políticas de seguimiento a reportes.

DISEÑO DEL DEPARTAMENTO.

Consiste en establecer como se realizarán las tareas que anteriormente se establecieron para este departamento.

Planeación Y Diseño De Red

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

El proceso de planeación y diseño de nuestra red contemplara varias etapas.

1. Reunir las necesidades de la red, las cuales pueden ser específicas o generales, tecnológicas, cuantitativas, etc. Algunas de las necesidades específicas y de índole tecnológica de la red pueden ser.

    - La necesidad de nuevas tecnologías (Voz sobre IP, MPLS, etc.).
    - Calidad de servicio (QoS).
    - Cantidad de nodos en un edificio.
    - Cantidad de Conmutadores necesarios para cubrir la demanda de nodos.
    - El número de usuarios.
    - Si la LAN se va a extender a varios edificios.
    - El medio de red actual.
    - Los conocimientos técnicos de los usuarios.
    - El nivel de tráfico de la red.
    - El nivel de seguridad.

    Este tipo de requerimientos solamente involucra una adecuación en el diseño de la red, no requiere de un rediseño completo, en el caso de alguna necesidad más general puede requerir de un cambio total en la red ya que en estos casos los cambios afectan a gran parte del diseño.

2. Diseñar la topología de la red, que de soporte a las nuevas tecnologías que satisfagan las necesidades de red.

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

4. Diseñar la distribución del tráfico mediante algún mecanismo de enrutamiento, estático o dinámico.

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

6. Este proceso debe realizarse periódicamente, cada dos meses como sugerencia, con la intención de detectar las cambiantes necesidades de la red y su pronta solución. Este proceso puede ser realizado con ayuda de encuestas a los usuarios de la red, así como también al resto de los departamentos que componen esta administración.

Selección de los recursos necesarios para mantener los sistemas y dispositivos operacionales.

Esta selección se debe realizar de acuerdo a las necesidades y la tecnología utilizada. Si alguna aplicación o dispositivo es utilizado dentro de la red, esta actividad deberá proveer los recursos necesarios para su adecuado y continuo funcionamiento. La selección de estos recursos se deberá enfocarse principalmente en siguientes puntos.

- Parches y actualizaciones para sistemas operativos de conmutadores y enrutadores.
- Actualización de controladores en impresoras, tarjetas de red, etc.
- Contratación de personal o capacitación del existente para la operación de nuevas tecnologías o dispositivos dentro de la red.
- Capacitación de los usuarios finales para manejo de equipo o software.

Esta actividad debe realizarse en periodos de poca o nula actividad dentro de la red para evitar problemas en el servicio a usuarios; como podría darse en la actualización del software de un conmutador o enrutador. Lo más recomendable es hacer un plan de pruebas previo al cual deben ser sujetas las actividades de mayor riesgo. El ciclo de esta actividad dependerá de las necesidades de la propia red.

Instalación y administración del *hardware* y *software*.

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

Instalación y administración de *hardware*

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

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

La tarea de administración del hardware es otra actividad esencial para el control del equipamiento y los costos asociados así como para asegurar que los usuarios disponen del equipamiento suficiente para cubrir sus necesidades.

Con ayuda de la información obtenida por el centro de Informática sobre el *hardware* existente de la red este departamento deberá realizar las siguientes actividades:

- Añadir información relativa a puestos de trabajo no instalados en red.
- Añadir información sobre otros aspectos como la localización física, condiciones en que se encuentra, etc.
- Establecimiento de parámetros de configuración en los ficheros de configuración del sistema operativo.
- Realizar el seguimiento de averías de los componentes de los equipos.
- Anotar información al inventario referente a los componentes que forman al equipo (tarjetas, discos, etc.).

Instalación y administración de *software*

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

- Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de *software*.
- Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

Las actividades relativas a la administración de *software* permiten al departamento determinar si las aplicaciones necesitadas por los usuarios se encuentran instaladas y donde están localizadas en la red, además permiten el seguimiento de número de licencias existentes y el cumplimiento de su uso en la red.

Las tareas que deben realizarse para esta actividad son las siguientes:

- Creación y mantenimiento del inventario de *software* instalado.
- Especificación y requerimiento del número de copias disponibles de los distintos paquetes.
- Seguimiento de la instalación no autorizada de *software* y de otros ficheros en prevención de introducción de virus.
- Autorización a los usuarios para la utilización de los paquetes de *software*.

La información que se suele extraer es la siguiente:

- Información general del paquete: fabricante, versión, número de licencias, etc.
- Disponibilidad: quién usa el *software*, quién lo puede usar, etc.
- Ficheros que componen el paquete.
- Información adicional establecida por el equipo de este departamento.

Esta actividad debe realizarse en periodos de poca o nula actividad dentro de la red para evitar problemas en el servicio a usuarios, cada dos meses como sugerencia, con la intención de detectar las cambiantes necesidades de software dentro de la red. Este proceso puede ser realizado con ayuda de encuestas a los usuarios de la red, así como también al resto de los departamentos que componen esta administración.

Aprovisionamiento

Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de *hardware* como de *software*, siempre se encuentren disponibles ante cualquier eventualidad. Algunos elementos de *hardware* más importantes como son: tarjetas procesadoras, fuentes de poder, módulos de repuesto, equipos para sustitución y un respaldo de cada uno de ellos.

Manejo de configuraciones en equipos.

Esta actividad se realiza para respaldar, almacenar y restaurar la configuración de los equipos de comunicaciones. Dentro del *software* de monitoreo adquirido por la Facultad de Química, el *EPICENTER*, existe una herramienta llamada "*Configuration Manager*", que puede ayudar en el éxito de esta actividad.

Usando el "*Configuration Manager*"

El "*Configuration Manager*" es un *Applet* que provee una interfase grafica para cargar y descargar archivos a y desde dispositivos administrados. También provee una estructura para almacenar archivos de configuración, para permitir el seguimiento de múltiples versiones. La actualización de archivos de configuración puede desempeñarse por demanda, o puede ser programado para ocurrir en tiempos regulares, una vez al día o una vez al mes.

Se ocupara este *Applet* para realizar las siguientes actividades

- Realizar copias de los archivos de configuración de todos los dispositivos administrados una vez por semana.
- Restablecer los archivos de configuración en los dispositivos cuanto se presente algún incidente no previsto y pierdan estos su configuración o cuando se reporte una alarma de mal funcionamiento de los dispositivos que haga necesario restablecer su antigua configuración.
- Mantener los dispositivos administrados con las imágenes de software más actuales.

Monitoreo de alarmas

Esta actividad se realiza para notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP. En este caso nosotros utilizaremos el *Applet* para monitoreo de alarmas que acompaña al *EPICENTER*.

Usando el "*Alarm System*"

El sistema *EPICENTER* de alarmas, provee detección de alarmas, errores y un operador de alarmas para los dispositivos monitoreados por el *EPICENTER*. Esto incluye a todos los dispositivos que el *EPICENTER* puede incluir en su base de inventarios.

El sistema de alarmas provee un conjunto predefinido de alarmas habilitadas, que inmediatamente generaran reportes, tales como autentificación o fallas en la conexión; problemas en dispositivos tales como fallas en las fuentes de poder o ventiladores, localización de problemas o dispositivos reiniciados. El sistema de alarmas también permite definir alarmas propias que reportaran errores bajo condiciones que uno especifique, tales como repetición de ocurrencias o valores de umbrales excedidos. También pueden especificar que acciones se deben tomarse cuando una alarma ocurre y es posible habilitar o deshabilitar alarmas.

La detección de errores esta basado en la captura de mensajes del protocolo SNMP. El sistema soporta MIB-2, el MIB privado de *Extreme Networks*, Monitoreo Remoto (RMON), mensajes y selección de mensajes de otras MIBs.

Por conveniencia el *Alarm System* provee un número de alarmas definidas. Estas alarmas son habilitadas por defecto y activadas tan pronto como el servidor *EPICENTER* esta activado. Este Incluye las siguientes alarmas:

- SNMP inalcanzable.
- Falla en la actualización de una configuración desde el sistema EPICENTER.
- Estado de actividad Fallido.
- Advertencia de dispositivo del *EPICENTER.*

Definiendo alarmas

Además de las alarmas ya predefinidas por el servidor, definiremos un conjunto más de alarmas que nos ayudaran a monitorear un mayor número de eventos dentro de la red. Las alarmas se muestran y se registran dentro del *Applet "Alarm Log Browser*", donde se especifican los datos de estas, como la hora en que se genero, la fecha el dispositivo que la disparo, entre otras cosas.

Las alarmas son generadas a partir de ciertos eventos, cuando un evento ocurre, puede definirse una alarma que nos alerte que el evento ha ocurrido dentro de la red. En las Tablas 5.18 y 5.19, se especifican los eventos SNMP y RMON, para los cuales se definirá una alarma.

Falla en la autentificación (*Authentication Failed*):	Este evento indica que una solicitud SMNP con una cadena invalidad fue recibida en el dispositivo.
Inicio Frió (*Cold Start*):	Este evento indica que un dispositivo fue reiniciado.
Umbral alto de utilización de CPU: (*CPU Utilization Rising Threshold*):	Este evento es generado cuando se supera un valor predefinido para la utilización del CPU (90% para nuestro modelo).
EDP Vecino removido (*EDP Neighbor Removed*):	Este evento es generado cuando un dispositivo no ha enviado una actualización de su existencia en su periodo configurado de tiempo.
Falla en el ventilador (*Fan Failed*):	Este evento indica que uno o más ventiladores en el interior de un dispositivo ha fallado.
Conexión Invalida (*Invalid Login*):	Este evento indica que un usuario intento conectarse al dispositivo pero su acceso fue rehusado por nombre o contraseña incorrectos. Este evento se activa después de tres intentos fallados de conexión.
Enlace Caído (*Link Down*):	Este evento indica que un puerto entro en inactividad desde un previo estado activo.
Enlace Activo (**Link Up**):	Este evento indica que un puerto entro en actividad desde un estado previo inactivo. Esta alarma se activara para todo todos puertos.
Sobrecalentamiento (*OverHeat)*:	Este evento indica que el sensor de temperatura de la tarjeta del dispositivo ha reportado una condición de sobre calentamiento.
Falla en fuente de poder (*Power Supply Failed*):	Este evento indica que una o más fuentes de poder han fallado.
Falla en la fuente redundante de poder (*Redundant Power Supply Failed*):	Este evento indica que la fuente redundante de poder esta indicando una condición de alarma.

Tabla 5.18. Eventos SNMP para definir alarmas

Eventos RMON

Porcentaje de utilización del CPU	Definida para cuando se supere el 90%
Porcentaje de utilización de puerto	Definida para cuando se supere el 80%
Temperatura	Cuando un dispositivo incremente en 50% su temperatura normal
Cambio de topología de red	Definida para cualquier cambio en la red

Tabla 5.19. Eventos RMON para definir alarmas

Debe existir una persona encargada para monitorear las alarmas de los dispositivos de red. Tendrá una cuanta de Tipo “monitor” dentro del sistema *EPICENTER* y realizara las siguientes funciones:

- Revisar las nuevas alarmas en el *Applet “Alarm System*”, una vez al día.
- Filtrar las alarmas de grado severo, para atenderlas inmediatamente.
- Informar al administrador del servidor la llegada de las alarmas de grado severo, realizando un reporte de alarma y enviarlo a la dirección de e-mail del personal de este departamento encargado de la atención a fallas.
- Si es posible resolver el problema vía *software*, el encargado será el administrador del servidor.

Localización de fallas

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

Pruebas de diagnóstico

Se deben verificar todas las conexiones de los cables del segmento donde se encuentra el equipo que esta fallando. Se recomienda comenzar con las conexiones del área de trabajo y seguir después hasta el closet de telecomunicaciones. Existen herramientas de diagnóstico, como el reflectómetro de dominio de tiempo que permiten localizar los defectos de un cable. Si piensa que el problema está en un puesto de trabajo, habrá que comprobar el conmutador del closet de telecomunicaciones, el cable, el conector y la memoria. Se debería emplear cualquier utilidad de diagnóstico de la tarjeta de interfaz de red del dispositivo para diagnosticar y resolver el problema.

Junto con los procesos arriba mencionados, existen herramientas de *software* que están a disposición para resolver los problemas de conectividad de red. Estas herramientas pueden ayudar en la solución de los problemas de las LAN, y son especialmente útiles en una solución de los problemas de las WAN. La localización de fallas se compone de pruebas de diagnostico de conectividad física y lógica así como pruebas de medición.

Las pruebas de conectividad lógica y las pruebas de medición pueden ser hechas con las herramientas que se describen a continuación, las pruebas de conectividad física, Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

Se examinarán los comandos que están a disposición de cualquier administrador de red en la mayoría de los paquetes de software. Entre estos comandos se incluye los comandos *Ping, Tracert, Telnet, Netstat, Arp* e *Ipconfig.*

Ping

Ping envía paquetes eco ICMP para verificar las conexiones de un equipo remoto. La salida de la Figura 5.16. Muestra si el *ping* tiene éxito o no. La salida, si tiene éxito muestra el número de paquetes a los que se ha respondido y el tiempo de retorno de eco.

```
C:\>ping 10.200.125.124

Haciendo ping a 10.200.125.124 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 10.200.125.124:
        Paquetes: enviados = 4, recibidos = 0, perdidos = 4 (100% perdidos),
Tiempos aproximados de recorrido redondo en milisegundos:
        mínimo = 0ms, máximo =  0ms, promedio =  0ms
```

```
C:\>ping 127.0.0.1

Haciendo ping a 127.0.0.1 con 32 bytes de datos:
Respuesta desde 127.0.0.1: bytes =32 tiempo<10ms TTL =128

Estadísticas de ping para 127.0.0.1:
        Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de recorrido redondo en milisegundos:
        mínimo = 0ms, máximo =  0ms, promedio =  0ms
```

Figura 5.16. Salida de ping.

Tracert

Tracert muestra la ruta que un paquete tomo para llegar a su destino. La salida de la Figura 5.17 muestra el comando trace.

```
C:\>tracert 65.208.80.242

Traza a la dirección ciscosys-gw1.customer.alter.net [65.208.80.242]
sobre un máximo de 30 saltos:

1        1 ms     1 ms     <10 ms   10.10.146.1
2        1 ms     <10 ms   <10 ms   192.168.1.74
3        87 ms    87 ms    87 ms    na.avantel.net.mx [207.249.167.114]
4        89 ms    89 m     88 ms    65.208.80.242

Traza completa.
```

```
C:\>tracert 65.208.80.243

Traza a 65.208.80.243 sobre caminos de 30 saltos como máximo.

1        <10 ms   <10 ms   <10 ms   10.10.146.2
2        <10 ms   <10 ms   <10 ms   customer-1.xertix.com [200.57.91.1]
3        *        *        *        Tiempo de espera agotado.
```

Figura.5.17. Salida de *tracert*.

Telnet

Es un programa de emulación de terminal que permite ejecutar comandos interactivos en el servidor *Telnet*. Hasta que se establece una conexión no pasa dato alguno; si la conexión se interrumpe, *Telnet* lo indicara. Esto es útil para probar los parámetros de configuración de inicio de sesión de un equipo remoto (véase la Figura 5.18).

```
-------------------------------------------------------------------------------
RS 3100 System Software, Version 9.4.0.6
Riverstone Networks, Inc., Copyright (c) 2000-2005. All rights reserved.
System started on 2005-09-12 14:53:11
-------------------------------------------------------------------------------

Press RETURN to activate console .

Username: noc
Password:
RIVERSTON>
```

Figura.5.18 Salida Telnet.

Arp

Arp recopila direcciones de hardware de los equipos locales y el *Gateway* determinado. Puede ver la Tabla *Arp* y comprobar si hay entradas invalidas o duplicadas (véase la Figura 5.19)

```
C:\>arp -a

Interfaz: 10.10.144.128 on Interface 0x1000003

Dirección IP Dirección física   Tipo
10.10.145          100-08-02-f7-2c-ce dinámico
10.10.146.2        00-08-02-a2-42-96  dinámico
```

Figura.5.19 Salida Arp.

Netstat

Netstat muestra estadísticas de protocolo y de las conexiones de red TCP/IP activas (véase la Figura 5.20).

```
C:\Documents and Settings>netstat -a

Conexiones activas

Proto  Dirección local        Dirección remota      Estado
TCP    varanda:epmap          varanda:0             LISTENING
TCP    varanda:microsoft-ds   varanda:0             LISTENING
TCP    varanda:3306           varanda:0             LISTENING
TCP    varanda:netbios-ssn    varanda:0             LISTENING
UDP    varanda:netbios-dgm    *:*
UDP    varanda:isakmp         *:*
```

```
C:\Documents and Settings>netstat -e
Estadísticas de interfaz
                           Recibidos             Enviados
    Bytes                  56692809              21861630
    Paquetes unicast       137529                130329
    Paquetes no unicast    93059                 486
    Descartados            0                     0
    Errores                0                     0
    Protocolos desconocidos                      1848
```

Figura.5.20 Salida *Netstat*.

Ipconfig

Esta utilidad muestran información de direccionamiento IP de los adaptadores de red locales o a una NIC especifica (Véase la Figura 5.21).

```
C:\>IPCONFIG

Configuración IP de Windows 2000

Ethernet adaptador Conexión de área local 2 Metro:

Sufijo DNS específico de la conexión. :
Dirección IP                          10.10.144.128
Máscara de subred                     255.255.252.0
Puerta de enlace predeterminada       10.10.146.1
```

Figura.5.21 Salida Ipconfig.

Para obtener más ayuda de estos comandos y conocer las todas las funciones que realizan se debe consultar la documentación que se incluye con el paquete de software que utilice.

Corrección de fallas.

Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En esta propuesta solo se mencionan las prácticas referentes a las fallas al nivel de la red.
El proceso de eliminación y la técnica “divide y vencerás” es uno de los métodos mas apropiados para la solución de problemas de red. Los siguientes escenarios explican la técnica.

El proceso de la técnica de eliminación

Imagínese que un usuario de su red llama al departamento de soporte técnico para notificar que su equipo no puede conectarse a Internet. El técnico rellena el formulario de informe de errores, y después de realizar las actividades para solucionar el problema, este departamento no consigue solucionarlo y lo envía al Centro de Informática, quien lo reasigna ahora a este departamento. Puede llamar y hablar con el usuario, quien le indicara que no ha hecho nada más que intentar conectarse a Internet. Realiza preguntas al usuario y este le informa que la computadora fue actualizada la noche anterior. La primera hipótesis es que los controladores de red de la computadora deben estar configurados de forma incorrecta. Se dirige a la maquina y comprueba la información de configuración de red de la computadora, realizando las siguientes actividades.

1. Hacerle un *ping* al servidor o al *Gateway* de esa subred. Si no se puede conectar pase al punto siguiente.
2. La solución siguiente consiste en comprobar si el cable de red del equipo esta convenientemente conectado.
3. Compruebe ambos extremos del cable y trate de hacer *ping* nuevamente al servidor.
4. A continuación hacer un *ping* a 127.0.0.1, que es la dirección de *Loopback* del equipo. Si ping es satisfactorio, se elimina el potencial problema entre la computadora, la configuración del controlador y la tarjeta NIC.
5. Para eliminar la posibilidad de un problema con el servidor o el *Gateway* de este segmento de red será necesario buscar otra computadora conectada a la red, y hacerle un *ping* a la dirección del servidor y si el resultado es satisfactorio. Esto elimina que el servidor, el *Backbone* y la conexión con el servidor plantee problemas.
6. Dirigirse al panel de parcheo y cambiae el puerto del equipo y trate de hacer un nuevo *ping* al servidor. Si la solución sigue sin funcionar. Esto acota la búsqueda al cable horizontal o al cable del equipo. Vuelva al panel de parcheo, coloque el cable nuevamente en el puerto original del conmutador, adquiera un nuevo cable de red para el equipo y vuelva a este ultimo.
7. Sustituya el cable de la estación de trabajo y trate de hacer un nuevo *ping* al servidor Si Esta vez tiene éxito, el problema a quedado resuelto.
8. Si no resuelve el problema después de verificar todos los elementos de red, puede ser necesario que contacte al especialista que realizo el cableado estructurado de su red o a los técnicos de sus equipos de telecomunicaciones.

Otros métodos igualmente recurridos, son los siguientes.

- Reemplazo de recursos dañados. Hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente.
- Aislamiento del problema. Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.
- Redundancia. Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.
- Recarga del sistema. Muchos sistemas se estabilizan si son reiniciados.
- Instalación de *software*. Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.
- Cambios en la configuración. También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

Administración de reportes

El ultimo paso consiste en documentar la solución del problema en el formulario de informe de errores para que pueda ser registrado como solventado.
Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido. Este es un medio para que los usuarios del servicio puedan conocer el estado actual de la falla que reportaron.

Creación de reportes

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

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

Seguimiento a reportes

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

Manejo de reportes

El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado, hacer cambios en los atributos del reporte, como lo es el teléfono de algún contacto, solicitar hora y fecha de la creación o finalización de un reporte, etc.

Finalización de reportes

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

STAFF TÉCNICO

Todas las actividades asociadas a este departamento serán realizadas por un grupo de trabajo, que cumplirá diversas características, además de compartir las actividades establecidas para este departamento.

Como propuesta inicial se recomienda que el equipo sea conformado por 3 integrantes, que realizaran todas las actividades de este departamento. Los elementos deberán tener experiencia y conocimiento en los puntos que se incluyen en la Tabla 5.20

PERFIL DEL PERSONAL PARA EL DEPARTAMENTO DE OPERACIÓN Y MANTENIMIENTO
• Manejo de sistemas operativos a nivel administración (Windows todas las versiones, Novell o Linux).
• Experiencia en instalación de *Hardware y software*
• Experiencia en monitoreo de alarmas
• Conocimiento de pruebas de diagnostico de red
• Experiencia en corrección de fallas en red
• Conocimiento de TCP/IP

Tabla.5.20 Perfil del personal de operación y mantenimiento.

DEPARTAMENTO DE SOPORTE TÉCNICO

A continuación se establecen los objetivos, tareas, procedimientos y políticas del Departamento de Soporte Técnico. Este departamento realizara las funciones necesarias para ofrecer asistencia técnica y solucionar los problemas de los usuarios de la red.

OBJETIVOS, TAREAS, PROCEDIMIENTOS Y POLÍTICAS.

Los objetivos que este departamento debe cumplir son:

- Proveer asistencia técnica de calidad para usuarios con productos de uso individual o designado.
- Resolver problemas que puedan surgir en un momento dado por causas fortuitas y que interrumpan las operaciones normales.

El departamento de soporte técnico, contara con un conjunto de tareas, procedimientos y políticas que serán las herramientas necesarias para el cumplimiento de sus objetivos. La atención a casos y el soporte técnico a usuarios se realizara en diferentes etapas, todas bien definidas y que deberán seguirse en el orden establecido para asegurar el éxito en la atención a casos y el seguimiento continuo de estos hasta su solución. A continuación se definen las tareas de este departamento.

- Atención a problemas de usuarios de la red.
- Corrección de fallas.
- Creación de reportes.

Los procedimientos que se realizarán para el cumplimiento de estas tareas serán los siguientes:

- Reporte de un caso al departamento.
- Asignación y registro del caso a un encargado de soporte técnico.
- Resolución del caso.
- Cerrando el caso.

Las políticas a seguir en este departamento son las siguientes:

- Prioridad de un caso.
- Políticas de buen uso de equipo y de software.

DISEÑO DEL DEPARTAMENTO

Consiste en establecer como se realizaran las tareas que anteriormente se definieron para este departamento.

Atención a problemas de usuarios

Dentro de este departamento, todos los usuarios de la red disponen de acceso a los servicios, a la documentación sobre problemas conocidos, procedimientos para corregir errores y manuales técnicos apropiados para el desarrollo de sus actividades.

Todo usuario registrado de la red, podrá recibir asistencia directa para problemas relacionados con la instalación y defectos de productos, incluidas caídas del sistema y errores provocados por el *software* autorizado por el Centro de Informática y la ayuda técnica que necesite. Este servicio es gratuito para los usuarios. Cuando surja un caso el usuario solo tendrá que comunicarse con este departamento a través de los números telefónicos asignados a este departamento y por Web utilizando el correo electrónico de soporte técnico. Este departamento debe dar a conocer los medios de contacto para atención de casos a todos los usuarios de la red.

La atención a los problemas de usuarios, se realizara con ayuda de los procedimientos “Reporte de un caso al departamento” y “Asignación y registro del caso a un encargado de soporte técnico”. Toda atención a un problema iniciara en el momento que un usuario se comunique al departamento solicitando un servicio. El personal que inicie la atención del caso deberá registrar el caso y seguir su desarrollo hasta el final, que será cuando el caso sea resuelto. Para casos extraordinarios, donde el departamento no sea capaz de resolver el caso, el Centro de Informática será el encargado de reasignar el caso al personal o departamento adecuado.

El departamento de soporte técnico es el encargo del generar las políticas de buen uso de equipo y de software. En el Apéndice B se incluye una propuesta de “Políticas de buen uso de equipo de cómputo y de software”.

Reporte de un caso al departamento

Cuando el usuario necesite reportar un caso al departamento de soporte, se le pedirá tenga a la mano la siguiente información para agilizar la solución a su problema. Se puede utilizar el “formato de caso” o *Checklist* proporcionado en el Apéndice A, para organizar la siguiente información.

- Número de cliente.
- Número de caso.
- Ingeniero de soporte.
- Fecha de apertura de caso.
- Producto y versión correspondiente que esta utilizando del software.
- Sistema operativo y versión.
- Equipo, sistema operativo y versión del equipo donde está corriendo el programa.
- Descripción del problema (Incluyendo número de errores, mensajes de error, circunstancias en las que el problema ocurrió).
- Cualquier información adicional que ayude a describir más el problema.

Una vez que el caso ha sido registrado se le asignará un número y a un encargado apropiado para resolverlo. El usuario debe anotar el número de caso en su *Checklist*. Este número es una referencia rápida a toda la información respecto a su pregunta.

El equipo de soporte técnico será el encargado de informar a los usuarios el procedimiento aquí descrito. Puede hacerse una circular haciéndola llegar a todos los usuarios de la red.

Asignación y registro del caso a un encargado de soporte técnico

Se tomara como un caso toda aquella pregunta o requerimiento de asistencia que el usuario interno hace al departamento de soporte técnico. Un caso es definido ya sea como una pregunta técnica o una instancia de un problema. Por ejemplo, si el usuario llama con preguntas relacionadas con Excel y otra con Visual Basic, lo manejara como dos casos diferentes. Cada caso recibirá un número de referencia, llamado número de caso, lo cual permitirá priorizar y darle seguimiento al problema eficientemente. Habrá que asegúrese, que el usuario, registre el número de caso cuando la persona que lo haya tomado le asigne, esto hará más fácil la comunicación entre ambos puntos de contacto.

Cuando el usuario llama a soporte técnico, primero se verifica la validez del usuario y se guardan todos los detalles del problema incluida la prioridad concertada. La respuesta de la primera llamada varía de acuerdo a la prioridad del caso y en el tipo de usuario.

Cada reporte de un caso tendrá que ser registrado, esta información deberá almacenarla el departamento de soporte técnico se recomienda utilizarse una base de datos para registrar los datos siguientes:

El número de cliente,	Este número hará referencia a los datos del usuario, nombre, puesto ubicación etc.
Tipo de usuario	Puede ser administrador, académico o administrativo
Número de caso,	Se asignara un número progresivo a cada caso reportado
Personal de soporte encargado,	Personal del departamento de soporte al cual quedo asignado el caso
Fecha de apertura del caso,	Fecha en la que se atendió al usuario y se realizo el registro del caso
Descripción del problema	Detalles ofrecidos por el usuario que reporto el caso, y observaciones del personal de soporte técnico.
Prioridad del caso	Se describe en las políticas pasa priorizar un caso. Apéndice B

Tabla.5.21 Datos para el registro para un caso en soporte técnico.

Algunas veces resolver el caso durante la primera llamada realizada o devuelta no es posible. Información adicional puede ser requerida, o la discusión inicial puede indicar que es otro el tipo de experiencia requerida ya sea para resolver el caso o verificar un defecto potencial del producto. Si esta experiencia diferente es requerida, el personal de soporte técnico transferirá el caso, al departamento correspondiente, a un ingeniero con el conocimiento apropiado y al usuario le informará del cambio.

Si el usuario tiene información adicional de su caso, puede actualizar su caso llamando al centro de soporte proporcionando el número de caso recibido asegurándose de que la información que está proporcionando quede asentada en el registro del caso.

Existe software especializado para el registro y gestión de casos. Estos programas pueden clasificar y dar prioridad a las solicitudes de servicio, organizan las solicitudes por fecha y por usuario, pueden crear un historial de servicio por equipo, crear inventarios de equipos y tomar control remotamente para solucionar problemas en los equipo de usuarios. En el mercado existen muchos programas de este tipo, uno de los mas completos y que puede utilizarse para ayudar a este departamento es “Track-it” de la marca “*Numera”* o “*Netretina Helpdesk*” de la marca “*Netretina*”.

Corrección de fallas

Después de terminada la actividad de atención a problemas de usuarios, donde involucra un proceso de interacción entre el usuario y el personal del departamento para obtener la mayor información relacionada con el problema, la siguiente actividad será corregir la falla. En esta etapa el departamento de soporte técnico atenderá el problema hasta su fin, esto quiere decir, cuando el caso sea resulto o el caso sea asignado a otro departamento para su atención. Esta actividad de realizara con ayuda del procedimiento llamado “Resolución del caso”.

Resolución del caso

Existen dos modalidades, para iniciar el proceso de resolución de un caso:

- Remoto. El soporte se ofrece vía telefónica o por Internet (correo electrónico o mensajero instantáneo), para resolver dudas de configuraciones, instalaciones de paquetería estándar y puesta en marcha de servicios.
- En sitio. Cuando se proporcionar mantenimiento preventivo y correctivo en el lugar de instalación de los equipos, también con dos opciones de servicio:
    - Mantenimiento preventivo. Servicio calendarizado para verificar la operación y actualizaciones, revisar las opciones de seguridad y mejora continua de la instalación. Esta opción necesita ser planeada por el departamento de soporte técnico.
    - Mantenimiento correctivo. Puesta en marcha por fallos imprevistos, verificación de configuraciones y verificación de la integridad del sistema.

Si en cualquier momento de la atención del caso el usuario no está satisfecho con el plan de acción efectuado hasta el momento este puede requerir el escalamiento de su caso. Los requerimientos de reescalar serán evaluados por el personal de soporte técnico y el responsable de la atención el caso. El departamento de soporte técnico será el responsable de proponerle otro plan de atención para la resolución del problema.

Creación de reportes

Para terminar con las tareas de este departamento, será necesario cerrar cada caso y documentar los pasos realizados en la solución encontrada. Esta actividad ayudara a tener un control de los casos atendidos y una referencia útil cuando se presenten casos parecidos. Esto se realizada con la ayuda el procedimiento “Cerrando el caso”.

Cerrando el caso

Un caso se considera cerrado cuando el usuario y el ingeniero o encargado de soporte acuerdan que una solución ha sido encontrada. Un caso puede ser cerrado por:

- La información y / o software proporcionada por el ingeniero o encargado de soporte ha resuelto su problema.
- El usuario puede considerar que el caso ya no es necesario.
- El usuario y el encargado de soporte acuerdan que su problema es resultado de un problema que no puede ser aislado.
- El caso ha sido asignado a otro departamento de atención.

Después de cerrar el caso se creara un reporte de este y se almacenara para sus consultas posteriores. La administración de estos reportes corre a cargo del mismo departamento.

EL STAFF TÉCNICO.

Todas las actividades asociadas a este departamento serán realizadas por un grupo de trabajo, que cumplirá diversas características, además de compartir las actividades establecidas para este departamento.

Como propuesta inicial se recomienda que el equipo sea conformado por 3 integrantes, que cubrirán a todos los problemas de los usuarios de red. Los elementos deberán tener experiencia y conocimiento en los puntos que se incluyen en la Tabla.5.22

PERFIL DEL ENCARGADO DE SOPORTE TÉCNICO
• Conocimiento de sistemas operativos (Windows todas las versiones, Novell o Linux).
• Manejo de herramientas Office, antivirus, correo electrónico, Exchange, Notes.
• Conocimiento de Aplicaciones administrativas.
• Experiencia en reparación de equipos.
• Experiencia en reparación de cableado de red.
• Experiencia en manejo y solución de problemas de conectividad en red y conexión a Internet.

Tabla.5.22 Perfil del personal de soporte técnico.

5.4 CONSIDERACIONES A FUTURO

Para finalizar esta propuesta, se hacen las consideraciones a futuro de la infraestructura de red y del modelo de administración.

El diseño de la infraestructura de red basado en estándares internacionales asegura la interoperabilidad de los sistemas y equipos que en un futuro se implementen sobre esta. Los cambios que la infraestructura sufra para adaptarse a las necesidades de la comunidad tendrán que seguir un plan de pruebas para su correcta implementación. Estas acciones garantizaran su funcionamiento por largo tiempo.

Los departamentos en que se dividen la administración de la infraestructura, deberán ejercer sus actividades de forma independientemente sin la necesidad del Centro de informática. El Centro de informática reorganizara sus funciones en forma de los departamentos sugeridos; esto será el primer paso para alcanzar la división que recomiendan los modelos. El personal que trabaja en el Centro de informática deberá incorporarse a estos departamentos, de acuerdo a su perfil. Todo siempre bajo la supervisión del titular de la Coordinación de Informática de la Facultad de Química.

Para el continuo funcionamiento de la red los servicios son parte fundamental, la falta de estos pondría en riesgo las actividades de los usuarios. Es recomendable tener los servicios de red dentro de un ambiente distribuido y redundante. Es recomendable utilizar servidores en estado de espera que aseguren la continuidad de los servicios ante la falla del los servidores principales. La redundancia de servidores y el respaldo de información permitirán elevar el nivel de disponibilidad, pero estas herramientas no impedirán que los sistemas fallen poniendo en riesgo las actividades de los usuarios. Será necesario diseñar planes de contingencia que contemplen un plan de acción para enfrentar los problemas que pueden afectar la continuidad de los servicios. Estos planes deben considerarse fundamentales en la recuperación de red cuando se ponga en riesgo la continuidad de su servicio. La importancia de contar con el apoyo institucional en la aplicación de estos, asegurara su pronta aplicación y beneficia el buen funcionamiento de la red en favor de las actividades de la comunidad de la Facultad.

La gestión de los recursos de red y de los usuarios puede especializarse si se utilizan un mayor número de grupos para su administración. Esto grupos pueden ser mas pequeños y mas especializados asignando recursos a los usuarios según el tipo de actividades que realicen. La administración de los recursos mejorara ya que solo tendrán acceso a ellos los usuarios que realmente los necesitan y no se desperdiciaran recursos de la red.

La administración de la contabilidad será un área a desarrollar en las ampliaciones de este modelo. Las actividades de esta área beneficiarían a la gestión de usuarios y a las actividades de seguridad. La contabilidad ayudara a conocer que recursos son los más utilizados en la red, que usuarios tienen acceso a estos y cuales deben ser considerados de mayor importancia en función del uso que se les da dentro de la red. La contabilidad llevara un registro de acceso a los recursos lo que aporta otra herramienta al área de seguridad en la protección de sistemas.

Existen prácticas consideradas “buenas” dentro de la administración de red y que pueden ser consideradas en beneficio de este modelo. La capacitación y especialización del personal debe ser una práctica constante que asegura el éxito de las tareas de los departamentos, La especialización del personal asegura el máximo rendimiento de las herramientas y sistemas que utilizan para su trabajo, lo que ayuda a sacar el máximo provecho de las inversiones. En consecuencia la inversión retorna al mejorar la eficiencia de las actividades, mejorando la calidad de los servicios que ofrece este personal a los usuarios de red.

CONCLUSIONES

Conclusiones

La comunidad de la Facultad de Química requería de una infraestructura de red que fuera capaz de satisfacer las necesidades de comunicación y que ofreciera un soporte confiable a las nuevas tecnologías de redes. Estas razones dieron origen a uno a los proyectos más ambiciosos: el diseño y construcción de la nueva infraestructura de red datos de la Facultad.

Pero un proyecto de tales magnitudes, no aseguraría la solución a todos los problemas sino forma parte de un modelo de soporte a tecnologías de información y comunicación, que ofrezca una solución completa a las necesidades de la antigua infraestructura y de la red de datos de la Facultad. La nueva infraestructura debe contar con un modelo de administración de red que mantenga en un alto nivel la calidad y disponibilidad de su servicio, y que asegurare el eficiente uso de la infraestructura creada. Esta es la razón principal del diseño del modelo de administración propuesto por este trabajo.

La propuesta que presento es un conjunto de objetivos, tareas y procedimientos que con ayuda de un proceso estandarizado en administración de redes y adaptado a las condiciones de funcionamiento de la Facultad de Química de la UNAM, representa una solución para administrar la infraestructura de red de datos que ha sido construida recientemente en esta institución.

Este trabajo propone utilizar un modelo basado en recomendaciones de órganos internacionales, que son utilizadas para administrar la infraestructura sobre las que descansan las redes de telecomunicaciones. La metodología, se basa en modelos con tareas bien definidas y complementarias, que se dividen en áreas para permitir su mejor entendimiento y facilitar su implementación y actualización. Este trabajo ha adaptado lo mejor posible estas recomendaciones y las mejores prácticas en la administración de redes, para lograr su acople al funcionamiento de la Facultad de Química.

Se han modificado tareas y procedimientos recomendados, para que se integren de forma sencilla a las actividades de la institución. Se agruparon actividades comunes para reducir el número de personal que recomiendan los modelos. Las políticas de red sufrieron modificaciones para evitar conflictos con la legislación universitaria. La propuesta se instauro sobre una estructura jerárquica, donde se mantuvo al Centro de Informática como el encargado de la nueva red; tratando de aprovechar la experiencia de este equipo de trabajo en beneficio del buen desempeño del modelo de administración. Finalmente se creo el departamento de soporte técnico para cubrir el área de atención de usuarios, que se no considera en los modelos que se utilizaron como guía.

Al cubrir estas necesidades se segura que el modelo se adaptara a las condiciones de funcionamiento de la Facultad de Química y en forma general a las condiciones de una institución de educación. Pero su completa adaptación se fundamenta en cumplir algunas condiciones. Primero, es necesario contratar mas personal para que realice las actividades asignadas a cada departamento. El personal debe estar capacitado y de preferencia contar con experiencia. Segundo, debe contarse con un plan de trabajo para migrar todos los equipos a la nueva red, tratando de afectar lo menos posible a los usuarios en el desarrollo de sus actividades. Tercero, el impacto que genera siempre un cambio debe minimizarse, creando un plan de actividades para que los usuarios conozcan la nueva metodología de trabajo de la red. Por ultimo, el personal que participara en la administración de la red, debe saber que este modelo debe actualizarse para seguir ofreciendo una solución a los cambios futuros de la red.

Seguir sus propuestas elevaran la calidad de los servicios que ofrece la red. Elimina la dependencia de ofrecer un servicio de calidad solo cuando lo realiza personal experto en el área. Establece la calidad de los servicios en función de la calidad del procedimiento que se utiliza y no del persona que lo realiza. Enfrenta problemas de la administración de redes agrupando actividades especificas y orientadas a cada área, para que estas se complementen y realicen un trabajo completo para solucionar problemas.

Es una solución económica, lo que es una ventaja para su aceptación. Solo propone invertir en los lugares donde es necesario, como la capacitación y ofrece soluciones que no genera gastos como lo es utilizar software libre. Eleva la disponibilidad de la red, al monitorear su rendimiento y conocer su estado actual, lo que permite en muchos casos adelantarse ante el deterioro del nivel de servicio en alguna parte de la red. Ofrece soluciones y estrategias para afrontar eventos que ponen en riesgo el buen funcionamiento. Eleva la seguridad, estableciendo políticas de uso y mecanismo para aseguran los recursos. Cuenta con las actividades para satisfacer las necesidades actuales y futuras de la red, además de su mantenimiento y las actividades de su operación.

Resumiendo este modelo sugiere la especialización y división de actividades para hacer más eficiente la operación y funcionamiento de la nueva red. Mejora la calidad de los servicios ofrecidos. Beneficia el desarrollo de las actividades de la Facultad, al mejorar los resultados en las tareas que se realizan con ayuda de la red de datos.

Finalmente, este modelo puede ser un ejemplo para comenzar la especialización y estandarización de otros procesos, buscando elevar el nivel de calidad de toda la Facultad. Es posible utilizarlo en otras instituciones, considerando las modificaciones necesarias. Este tipo de modelos debe considerarse un medio para mejorar la calidad de los proceso. Dentro de las facultades esto debería ser una actividad constante, que mejore la calidad de cada Facultad y por consecuencia el de toda la universidad.

APÉNDICE A

Documentos de apoyo

FORMATO DE CASO DE SOPORTE TÉCNICO

Checklist de Soporte Técnico
Para facilitar la solución a su problema y a tener registro de él, por favor llene
El siguiente checklist antes de llamar a su centro de Soporte Técnico.
• Número de cliente
• Número de caso
• Ingeniero de soporte
• Fecha de apertura de caso
• Producto y versión correspondiente que esta utilizando del software
• Sistema operativo y versión
• Máquina, sistema operativo y versión de la máquina donde
está corriendo el programa
•Descripción del problema (Incluyendo número de errores,
mensajes de error, circunstancias en las que el problema ocurrió)
•Cualquier información adicional que ayude a describir más el problema

DOCUMENTO DE RESGUARDO DE EQUIPOS

FACULTAD DE QUIMICA

UNAM

Ciudad, Provincia o Estado Código postal
Tel. Número de teléfono Fax Número de fax

INFORME DE RESGUARDO

Usuario

Nombre .....
Nº de Usuario .....
Ubicación .....
Puesto .....
Jefe .....
Telefono .....

Equipo de Computo

Sistema operativo ..... Nombre del equipo .....
Memoria RAM ..... Disco Duro .....
Tipo Procesador ..... CD-ROM .....
Vel. Procesador .....

Cuenta de Usuario

Tipo de Cuenta .....
Permisos .....

Notas

Se hace entrega de la siguiente informacion:

1. Politicas de uso de equipo de computo y software
2. Politicas de uso de la red de datos
3. Procedimiento para ingresar a la red
4. Procedimiento para reportar un caso a soporte tecnico

Consentimiento de que sus actividades son susceptibles de ser auditadas en cualquier momento esto para asegurar el buen uso de la red y garantizar el servicio a los demas usuarios de la red y de que conoce las normas de "buen uso de los recursos"

Firma del Usuario

Centro de Informatica

FORMATO PARA REGISTRO DE INVENTARIOS

Facultad de Química

FORMATO DE REGISTRO INVENTARIOS

NUMERO USUARIO	NOMBRE	PUESTO DE TRABAJO	JEFE	TELEFONO (ETX.)	UBICACIÓN FISICA	NUMERO SERIE MONITOR	NUMERO SERIE CPU	INVENTARIO MONITOR	INVENTARIO CPU	VLAN	CONTRASEÑA	FECHA DE EXPIRACION
1	ARANDA PAREDES VICTOR	ACADEMICO	ROBLES JAVIER	123	SICA	123456789_0	098765432_1	MON_0001	CPU_0001		timar888	01-Ene-05
2								MON_0002	CPU_0002		cresa146	01-Ene-05
3								MON_0003	CPU_0003		moro070	01-Ene-05
4								MON_0004	CPU_0004		goton888	01-Ene-05
5								MON_0005	CPU_0005		usura763	01-Ene-05
6								MON_0006	CPU_0006		diador354	01-Ene-05
7								MON_0007	CPU_0007		cocal076	01-Ene-05
8								MON_0008	CPU_0008		timar888	01-Ene-05
9								MON_0009	CPU_0009		cresa146	01-Ene-05
10								MON_0010	CPU_0010		moro070	01-Ene-05
11								MON_0011	CPU_0011		goton888	01-Ene-05
12								MON_0012	CPU_0012		usura763	01-Ene-05
13								MON_0013	CPU_0013		diador354	01-Ene-05
14								MON_0014	CPU_0014		cocal076	01-Ene-05
15								MON_0015	CPU_0015		timar888	01-Ene-05

APÉNDICE B

Políticas sugeridas

POLÍTICAS EN LA ASIGNACIÓN DE LOS DATOS DE RED

ASIGNACIÓN DE NOMBRES DE EQUIPOS

La asignación de los nombres de los equipos de la red seguirá el siguiente formato, esto con el fin de lograr homogeneidad en la asignación de estos nombres y así lograr búsquedas más rápidas de los equipos dentro de la red.

El nombre de Equipo constara de dos partes:

a) Primera letra del primer nombre del usuario, al cual esta asignado el equipo.
b) Todo el apellido paterno.

Nota: Si existe mas de dos maquinas asignadas a un usuario, agregar al final números progresivos comenzando por el número uno. Se escribirán los nombres sin ningún signo de puntuación.

Ejemplo: USUARIO: Roberto Aranda Paredes
NOMBRE DE EQUIPO 1: raranda
NOMBRE DE EQUIPO 2: raranda1

ASIGNACIÓN DE GRUPO DE TRABAJO

El grupo de trabajo al cual será asignado cada equipo dependerá del área funcional a la que pertenezca, así tenemos los siguientes grupos de trabajo.

ZONA	EDIFICIO	NIVEL	DENOMINACIÓN DEL ÁREA	GRUPO DE TRABAJO
1	A	PB	LABORATORIO DE FÍSICA	LABORATORIO_DE_FÍSICA
2	A	1	LABORATORIO 1D	LABORATORIO_1D
3	A	2	LABORATORIO 2D	LABORATORIO_2D
4	A	3	LABORATORIO 3D	LABORATORIO_3D
5	A	4	LABORATORIO 4D	LABORATORIO_4D
6	EXALMACEN	PB	FÍSICO QUÍMICA	FISICO_QUIMICA
7	DIRECCIÓN BIBLIOTECA	PB	DIRECCIÓN	DIRECCIÓN
8	NAVE DE INGENIERÍA	PB	LABORATORIO	LABORATORIO
9	AUDITORIOS	PB	ESTRADO A	ESTRADO_A
10	C	PB	CENTRO INFORMÁTICA	CENTRO _ INFORMÁTICA
11	C	1	LABORATORIO 105	LABORATORIO_105
12	ANEXO BIBLIOTECA	PB,1	BIBLIOTECA	BIBLIOTECA
13	ANEXO BIBLIOTECA	2	SALA DE CURSOS	SALA_DE_CURSOS
14	B	SÓTANO	SICA	SICA
15	B	PB	MULTIMEDIA	MULTIMEDIA

16	B	PB	USAI	USAI
17	B	1	LABORATORIO 101	LABORATORIO_101
18	B	1	SRIA. ADMITIVA.	SRIA_ADMITIVA
19	B	2	LABORATORIO 201	LABORATORIO_201
20	B	2	LABORATORIO 209	LABORATORIO_209
21	B	3	LABORATORIO 307	LABORATORIO_307
22	B	4	IDIOMAS	IDIOMAS
23	POSTGRADO	PB	CÓMPUTO	CÓMPUTO
24	ALMACÉN	PB	ALMACÉN	ALMACÉN

ASIGNACIÓN DE CONTRASEÑAS Y NOMBRE DE USUARIO PARA USO DE LOS RECURSOS DE RED

Contraseña

Las contraseñas deben cumplir las siguientes características.

1. La cantidad de caracteres mínimo que debe tener será de 8.
2. No tiene que tener relación directa con las características del usuario, tales como la fecha de nacimiento, apelativos, nombres de familiares, etc.
3. Debe constar de caracteres alfanuméricos, mayúsculas, minúsculas, números y símbolos de puntuación.
4. La generación de estas contraseñas correrá a cargo del personal del Centro de Informática.

Nota: Una vez que al usuario se le ha asignado una contraseña, se le debe correr un "programa crackeador" para tener idea de cuán segura es, sobre la base del tiempo que tarda en romper la palabra.

Nombre de Usuarios

El Nombre de usuario estará compuesto por dos partes:

1. Primera letra del primer nombre del usuario, al cual esta asignado el equipo.
2. Todo el apellido paterno.

Nota: Si existe mas de dos maquinas asignadas a un usuario, agregar al final números progresivos comenzando por el número uno. Se escribirán los nombres sin ningún signo de puntuación.

Ejemplo: USUARIO: Roberto Aranda Paredes
NOMBRE DE EQUIPO 1: raranda
NOMBRE DE EQUIPO 2: raranda1

ASIGNACIÓN DE LA DIRECCIÓN DE CORREO ELECTRÓNICO

La asignación de la dirección de correo electrónico seguirá el siguiente formato, esto con el fin de lograr homogeneidad en la asignación y así lograr búsquedas más rápidas cuando se busca un equipo.

La dirección de correo electrónico constara de dos partes:

a) Primer nombre del usuario, al cual esta asignado el equipo.
b) Todo el apellido paterno.

Nota: Separar estas dos partes con un punto, no utilizar signos de puntuación y letras mayúsculas.

EJEMPLO USUARIO: Roberto Aranda Paredes
CORREO ELECTRÓNICO: roberto.aranda@dominio

POLÍTICAS DE USO DE LA RED DE LA FACULTAD DE QUÍMICA

INTRODUCCIÓN

Las siguientes políticas servirán como referencia, y en ningún momento pretenden constituirse como normas absolutas. Todos aquellos actos que se consideren como violaciones a las normatividades vigentes (Reglamento de la Universidad, y / o cualquier otra disposición debidamente establecida en el ámbito jurídico), y que no se mencionen expresamente en este documento, no están permitidas.
Al utilizar la red de esta Facultad, se espera que el usuario (Estudiante, Docente, Administrativo) use los servicios con respeto, cortesía y responsabilidad, en procura de no vulnerar los derechos de los demás usuarios de la Red.

Se incorporan aquí los lineamientos y las políticas del Centro de Informática. Se espera que por parte de los usuarios se tenga conocimiento básico de cómo funciona una red e Internet, los tipos de uso generalmente aceptados y los tipos de uso que se evitan.

Toda persona que utilice los servicios que ofrece la red de esta Facultad deberá aceptar el reglamento vigente sobre su uso. El desconocimiento del mismo no exonera de las responsabilidades asignadas.

Las autoridades académicas y administrativas, y en particular el Centro de Informática, deberían publicar y difundir estas políticas de uso para y entre los usuarios de los bienes y recursos informáticos provistos a través de la red.

Los casos no previstos por el presente reglamento serán resueltos por el Centro de Informática, y si la situación lo amerita serán a canalizados a las instancias correspondientes.

DEFINICIÓN DE TÉRMINOS

Red de datos:

Red de datos es el nombre dado al conjunto de instalaciones y recursos informáticos de la Facultad de Química de la UNAM, en particular aquel provisto por el Centro de Informática. También hacen parte de ella la infraestructura de telecomunicaciones, y los servicios teleinformáticos prestados por otras dependencias de la sede, y que se encuentren bajo la supervisión del Centro de Informática.

Usuario:

Se entiende por usuario de la red, todo ente que reciba o provea información a través de la Red de datos; en particular, caben bajo esta denominación, las dependencias académico-administrativas, y las personas que tengan alguna vinculación académica o laboral con la Facultad y cumplan con los requerimientos de acceso a la Red. Las presentes políticas serán aplicadas a todos los usuarios.

Servicio:

Se entiende por servicio, los aplicativos y / o conjunto de programas (software) que apoyan la labor académica y administrativa del que hacer cotidiano de los usuarios que requieren y / o proveen información a través de la Red de datos.

Cuenta:

Mecanismo de identificación asignado a un usuario. Dicho mecanismo será único e intransferible, vigente durante el tiempo de vinculación del usuario con la Red, y sujeto a las restricciones definidas por el Centro de Informática, o la autoridad competente.

Recurso:

Cualquier insumo involucrado en la prestación de los servicios asociados a la red de datos.

PERSONAL AUTORIZADO

Están autorizados a utilizar los servicios de la Red de datos, todo el personal docente, el personal administrativo, los estudiantes (activos, becarios y egresados) de la Facultad de Química. La clasificación de usuarios es la siguiente:

a) Administradores.
b) Investigadores.
c) Académicos.
d) Administrativos.
e) Alumnos.
f) Invitados

USO DE LOS SERVICIOS EN LA RED DE DATOS

I. De la cuenta de usuario

Para hacer uso de cualquiera de los servicios de la Red de datos, el usuario deberá tener una cuenta cuya asignación estará regida por los siguientes criterios:

1. Si se es un usuario docente de planta, administrativo de planta, o un estudiante activo de pre o post grado, una vez se ingrese por primera vez a la Facultad de Química, de manera automática.

2. Si se es un usuario externo: Ésta se solicitará mediante comunicación escrita, dirigida al Centro de Informática. Dicha comunicación deberá detallar documento de identidad, dependencia y tipo de vinculación del potencial usuario con la Facultad. La entrega de la solicitud no garantiza la apertura de la cuenta, sino que ésta será analizada por el coordinador del Centro de Informática. La vigencia de la misma estará determinada por el tiempo estimado de vinculación del usuario con la Facultad.

3. Los procedimientos de notificación de la asignación de la cuenta de usuario serán los siguientes:

    a. Para los usuarios docentes, administrativos y externos, se hará cuando se haga entrega de la copia de resguardo del equipo de computo que tiene asignado.
    b. Para los usuarios estudiantes, su cuenta estará asignada por los centros de computo donde utilice los recursos de red.

    Nota: En caso de extravío de la información de la cuenta, el usuario deberá dirigirse personalmente a las instalaciones del Centro de Cómputo con documento de identidad, para el procedimiento de recuperación de la misma.

II. De los recursos

La infraestructura de la Red de datos se utilizará únicamente para desarrollos académicos, de investigación, técnicos y administrativos de la Institución. Así mismos los recursos de la Red de datos solo podrán ser usados de acuerdo con lo previsto por las normas de manejo de bienes de la universidad, las políticas presentadas en este documento, y todas las demás normativas asociadas a las mismas.

Se prohíben, salvo autorización y supervisión expresa del Centro de Informática, la intervención física de los usuarios sobre tos recursos de la Red de datos (Cables, enlaces, equipos activos y / o pasivos) y el acceso a los centros de cableado de los edificios.

Los recursos asociados a la Red de datos sólo podrán utilizarse para propósitos legales. Cuando se provea el acceso a recursos externos a la Red de datos, aplicaran las normativas definidas por la fuente de dichos recursos externos.

III. Usos inaceptables

- Envío de material ofensivo, o de contenidos difamatorios.
- Transmisión de información de terceros sin previa autorización de la autoridad competente o dueños de los derechos.

- Distribución no autorizada o copia de software sin licencia.
- Acoso informático y / o electrónico a cualquier miembro usuario de la red.
- Difusión de información de carácter comercial o cualquier otra forma que represente un lucro para la persona que lo origina, o la procura.
- Envío de mensajes bromas(Falsas alarmas asociadas a virus o fallos de seguridad).
- Difusión de contenidos asedados a proselitismo político, religioso o racial.
- Difusión de contenidos que infrinjan o de alguna manera no tengan claro el cumplimiento de las normas vigentes sobre derechos de autor y propiedad intelectual.
- Difusión de material obsceno o que incite a la violencia.
- Publicación y recepción de contenidos comerciales y / o personales en cuentas de usuario asignadas a dependencias de la Facultad.
- Cualquier tipo de uso catalogado como infracción informática (hacking, cracking, snooping, probing, entre otros.)

IV. Cesión de privilegios

Ningún usuario de la Red de datos está facultado para conceder acceso a los servidos y / o recursos de la red a terceros.

Todos los usuarios con recursos de la Red de datos bajo su responsabilidad, sólo harán uso de los mismos en beneficio institucional, deberán velar por la protección física de los bienes, y acogerse a las presentes políticas y normativas asociadas a las mismas. También será responsabilidad de este personal brindar acceso al personal previamente autorizado por el Centro de Informática para dar soporte o hacer labores de inventario sobre los bienes correspondientes.

V. Labores de arbitramento

El Centro de Informática, será único arbitro en cuanto a qué constituye una violación de lo dispuesto en el numeral IV.

VII Seguridad del Sistema y de la Red

Se prohíbe cualquier tipo de acción o comportamiento que vaya en contra de la seguridad física y / o lógica de los recursos asociados a la red de datos. Dichos comportamientos podrán acarrear sanciones institucionales, civiles y / o penales, y no se encuentran limitados a los siguientes:

- Acceso, uso, puesta a prueba, o exploración no autorizada de los servidores, dispositivos o aplicaciones comprometidas en la prestación de los servidos de la Red de datos.
- Bombardeo de correo (uso de mail bombers), inundación de tráfico (TCP Syn Flooding), intentos de denegación de servicio y / o difusión de virus, troyanos o cualquier otro tipo de software malicioso a usuarios, redes y / o servidores de la red de datos, o de cualquier otra red de Internet.
- Realizar cualquier tipo de suplantación mediante información falsa a nivel de direcciones MAC, encabezado IP o TCP, y / o encabezados a nivel de datos de protocolos de aplicación.
- Activación, sin previa autorización, de programas que consuman de manera no controlada tiempo de procesamiento en servidores institucionales.
- Cambios en las configuraciones de hardware o software de la red, que puedan ocasionar inestabilidad o caídas en el rendimiento de la Red, o de otros recursos comprometidos en la prestación de servicios a través de la misma.

Todos los usuarios de la red deberán acogerse a las políticas de seguridad establecidas y difundidas por el Centro de Informática de esta Facultad.

VIII. De los derechos y responsabilidades de los usuarios de la Red

Derechos:

- Los usuarios internos pueden utilizar los recursos de la red con las limitantes consignadas en el punto de usos inaceptables.
- Los usuarios dispondrán de pleno acceso a los recursos de la red, de acuerdo a lo consignado en el presente documento y en las normativas asociadas a este.
- A los usuarios externos se les faculta a utilizar únicamente los recursos que se les asigne por parte del Centro de Informática y / o el proyecto al cual estén inscritos.
- Los usuarios gozan de la privacidad de su información, con la salvedad de aquellos casos en que se detecten acciones que pongan en riesgo la seguridad de la Red de datos o de cualquier otra red.
- Los usuarios podrán acceder a la Internet, cobijados bajo las políticas implementadas mediante firewall y proxy diseñadas por el Centro Informática para brindar seguridad a la red de datos y hacer un buen uso del ancho de banda.

Responsabilidades:

- Se considera que el correo electrónico es una comunicación directa y confidencial entre el emisor y el receptor o receptores, y no debe ser vista o reproducida por nadie más que ellos.
- En el correo electrónico el usuario deberá acatar indeclinablemente las normas dictadas para el uso de éste servicio en las disposiciones aquí expuestas.
- El usuario velará por asegurar que sus archivos cuenten con las protecciones para escritura, lectura y ejecución adecuadas.
- El usuario debe asegurarse de acatar las disposiciones dictadas en las políticas de seguridad con referencia a éste tipo de protección, y que el software y medios que se introduzcan en la red de datos no contengan virus.
- Cualquier cambio en el hardware de red de una estación de trabajo deberá ser notificado al Centro de Informática en un lapso no mayor a 4 horas después de efectuado dicho cambio.
- Los usuarios deben asegurarse de acatar las disposiciones dictadas en términos de garantizar que no se introduzcan en la red contenidos infectados de virus o software malicioso.
- Los usuarios no deben alterar o corromper información ajena.
- Es responsabilidad del usuario realizar el respaldo de su información.
- Será responsabilidad del usuario informarse sobre los detalles de los tipos de licencia, cobertura, transferibilidad y certificación mediante solicitud al Centro de Cómputo de la Sede.
- Los envíos masivos de correo electrónico ("broadcasts") ó que incluyan a todos los usuarios de la red, sólo podrán ser transmitidos si son autorizados por el Centro de informática.
- Los correos masivos y la utilización de las listas de correo se regirán por las normas establecidazas para dicho fin.
- La información enviada a través del correo electrónico será responsabilidad exclusiva del emisor.

IX De las restricciones de uso

Dadas las limitantes que existen en lo que tiene que ver con la cantidad de recursos informáticos disponibles en la Facultad, se formularán algunas restricciones asociadas a los mismos, sin prejuicio de las que puedan surgir como parte de las necesidades de servicio.

Restricciones asociadas a las estaciones de trabajo y periféricos.

- Las computadoras asignados directamente a los usuarios en las dependencias administrativas y entes académicos, podrán ser utilizados libremente por cualquier usuario de la red, de acuerdo a lo dispuesto por el reglamento de uso.
- El uso de las máquinas conectadas a la red y que estén asignadas a proyectos específicos estará regulado por los responsables del proyecto en conjunto con la Facultad que haga las veces de gestora y / o coordinadora del mismo.

Restricciones asociadas al acceso a los servicios.

- Los usuarios podrán utilizar libremente los servicios de red (Internet, archivos, antivirus, etc.).Sin embargo en caso de ser necesario el Centro de Informática podrá proponer restricciones de acceso a ciertos servicios, en procura de mejorar el rendimiento de la red.

- En atención a la disponibilidad de direccionamiento público, sólo se entregaran direcciones de ésta red a los servidores de Internet y a las estaciones de administración de la red.
- El tiempo de conexión a la red de datos y los servicios que esta ofrece no tendrán ningún costo para los miembros de la comunidad.
- No está autorizado el montaje de servidores, que por sus funcionalidades puedan comprometer el buen funcionamiento y la seguridad de la red. Para su instalación deberá mediar una comunicación dirigida a la jefatura del Centro de Informática, a partir de lo cual se realizará el análisis de factibilidad de la misma.
- Los servicios de red remotos (vía telefónica) sólo se ofrecerán a los usuarios docentes y administrativos. Se prohíbe el uso de cuentas asociadas a dependencias para el acceso a dichos servidos.
- La reubicación de equipos de red, inicialización de servidores, cambio de parámetros en configuración en equipos activos de la red, y la instalación y modificación de redes físicas al interior de la Red de datos serán competencia y responsabilidad exclusiva del personal de Centro de Informática de la Facultad; La instalación de nuevos equipos con conexión a la Red de datos deberá ser notificada previamente al Centro de Cómputo.
- La instalación de paquetes y programas en los servidores generales de la red se llevara a cabo por el personal del Centro de Informática y en el caso de servidores fuera del Centro de Informática por el administrador del sistema particular bajo la supervisión del personal de ésta oficina.
- El uso de los paquetes de licencia adquiridos por la Facultad será libre para cualquier usuario de la red, para todos casos se recomienda informarse acerca del uso, vigencias y restricciones de los mismos con la Unidad de Soporte Técnico del Centro de Informática.

Si existe alguna duda favor de comunicarse al Centro de Cómputo, donde se te informará más acerca de cualquiera de los puntos aquí descritos.

POLÍTICAS DE BUEN USO DE EQUIPOS DE CÓMPUTO Y SOFTWARE

Objetivo:

Normar el uso del software y equipos de cómputo PCS y Macintosh dentro de la Facultad de Química.

Políticas Generales

1. Los lineamientos que se establecen en este procedimiento, son de carácter obligatorio y general para todos los empleados de la Facultad de Química de la UNAM que tengan a su cargo equipos de cómputo PCS y Macintosh, así como para todos los usuarios de las mismas.
2. Los equipos de Computo propiedad de la Facultad de Química son asignados por (.....) por medio de Centro de informática, con el fin de que realicen las actividades propias de su función dentro de la institución, por lo cual, deben mantener cuidado con el equipo asignado.
3. Es obligatorio para los empleados y usuarios de la Facultad de Química, el acatar las disposiciones que se emitan para regular la utilización y buen manejo de los equipos y sistemas de computo que La Facultad de Química asigna a cada usuario.
4. Se considera de carácter institucional el siguiente software:

   Para equipos personales

   a) Hoja de Calculo: Nombre
   b) Procesador de texto: Nombre
   c) Paquetes de presentaciones: Nombre
   d) Agenda electrónica: Nombre
   e) Reportador y manejador de bases de datos: Nombre
   f) Bases de Datos: Nombre
   g) Correo electrónico: Nombre
   h) Software para desarrollo de aplicaciones: Nombre
   i) Antivirus: Nombre
   j) La adquisición de cualquier software distinto a los anteriores deberá ser previamente autorizado por el Centro de Informática

Para equipos Macintosh

k) Hoja de Calculo: Nombre
l) Procesador de texto: Nombre
m) Paquetes de presentaciones: Nombre
n) Agenda electrónica: Nombre
o) Reportador y manejador de bases de datos: Nombre
p) Bases de Datos: Nombre
q) Correo electrónico: Nombre
r) Software para desarrollo de aplicaciones: Nombre
s) Antivirus: Nombre
t) La adquisición de cualquier software distinto a los anteriores deberá ser previamente autorizado por el Centro de Informática

5. Todo software que se utilice en los equipos de computo propiedad de la Facultad de Química que no sea algunos de los señalados en el punto anterior será considerado como software sin licencia, salvo los casos en que haya autorización por escrito del Centro de Informática para la adquisición de cualquier otro producto que requiera ser utilizado para las funciones del área en especifico.
6. En caso de tener instalados en un equipo de cómputo propiedad de la Facultad de Química, software distinto al institucional, el empleado o alumno que tenga en su equipo este tipo de paquetería, se hará responsable único de su uso. No deberá instalarse ningún software particular, sin tener la autorización expresa del centro de informática, y queda prohibido instalar software proveniente de Internet (Freeware, Shareware) en los sistemas de computo de la institución, a pesar de que el mismo sea para uso de la institución.
7. El centro de Informática es la única facultada para autorizar la instalación de software adicional al institucional.
8. En caso de requerir algún software en especial favor de ponerse en contacto con el Centro de Informática, explicando los motivos para un software diferente, a los señalados en el punto 4.
9. Aquellos usuarios de los equipos que tengan software sin licencia, deberán justificar al Centro de Informática su procedencia y en su caso la licencia correspondiente; en caso de no justificar su procedencia y / o Licencia se eliminara el software y se registrara el incidente.
10. La Institución se reserva la facultad de realizar en cualquier momento auditorias al equipo de computo asignado a los empleados y funcionarios de la institución; si en la auditoria practicada a los equipos se detecta que existe paquetería distinta a la permitida por la institución y no es justificable la procedencia de esta, se procederá al formateo del disco duro para la desinstalación del Software y a la elaboración de un informe en el que se exponga la situación a fin de que se tomen las medidas pertinentes.
11. El Centro de Informática tiene la facultad de realizar Auditorias Internas en el momento que así lo requiera a cualquier equipo asignado a algún empleado o funcionario debiendo estos últimos facilitar el acceso a dicho equipo para ser auditado.
12. Queda estrictamente prohibido el uso de Juegos, Pornografía, Protectores de Pantalla, dentro de los equipos de cómputo; la persona que sea sorprendida con este tipo de paquetería se hará acreedor a las sanciones establecidas.

PRIORIDAD DE UN CASO DE SOPORTE TÉCNICO

Las prioridades de los casos están asignadas basadas en la urgencia del problema y el impacto en la actividad. La prioridad del caso determina el tiempo de respuesta inicial efectuado. El usuario tendrá que explicar el impacto que el caso tiene en su proyecto de tal forma que el soporte técnico pueda ajustar lo mejor posible el problema. La prioridad incluso beneficiara para que la carga de trabajo en soporte técnico sea más adecuada para todos los usuarios que solicitan de él.

Prioridad 1

El software no es operacional y no hay alternativa de solución posible, o una alternativa existe pero es inaceptable por el impacto a su actividad. El desarrollo o la producción está detenida o el problema esta causando un impacto en la posibilidad de seguir desarrollando.

Prioridad 2

El software es operacional, pero su funcionalidad está seriamente afectada. Puede existir una alternativa de solución, pero el implementarla se lleva tiempo y puede afectar adversamente el ciclo de vida de su proyecto.

Prioridad 3 (default)

El software está operando, pero el desarrollo o la producción están siendo impactadas. El desarrollo o la producción pueden continuar por un monto razonable de tiempo antes de que el problema se vuelva crítico. Una alternativa de solución está disponible y es aceptable.

Prioridad 4

El software es operable, pero le gustaría sugerir alguna funcionalidad o simplemente usted tiene una pregunta sobre el funcionamiento del software que no esté documentada.

GLOSARIO DE TÉRMINOS

Glosario de términos

ANSI: American Nacional Standards Institute.

APPLET: Pequeña aplicación escrita en Java la cual se difunde a través de la red en orden de ejecutarse en el navegador cliente

AREA DE TRABAJO: Espacio físico que ocupa el personal de un departamento Funcional.

ARP: Son las siglas en inglés de Address Resolution Protocol (Protocolo de resolución de direcciones). Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

BACKBONE: Conjunto de equipos de comunicaciones centrales (core) de las redes de cada conjunto, y enlaces de fibra óptica que los une (cableado dorsal).

BROADCAST: En castellano "difusiones", se producen cuando una fuente envía datos a todos los dispositivos de una red.

CABLEADO CENTRAL: Enlaces de fibra óptica que une equipos de comunicaciones de Backbone

CABLEADO HORIZONTAL: Cableado estructurado de un edificio por nivel.

CABLEADO VERTICAL: Conjunto de enlaces entre el CTP y CPI de un edificio

CONJUNTO POSGRADO: Conjunto de instalaciones formado por la Zona A y la Zona B.

CONMUTADOR: Un conmutador (en c es un dispositivo de interconexión de redes de Equipo que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconection*). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los datagramas en la red.

CPU: Se llama CPU (siglas de Central Processing Unit) o Unidad Central de Proceso (UCP) a la unidad donde se ejecutan las instrucciones de los programas y se controla el funcionamiento de los distintos componentes del ordenador. Suele estar integrada en un chip denominado microprocesador.

CT: Closet o gabinete de comunicaciones de un edificio.

CTP: Closet o gabinete de comunicaciones principal de un edificio.

DATAGRAMA: Entidad de datos autocontenida e independiente que transporta información suficiente para ser encaminada desde su ordenador de origen a su ordenador de destino sin tener que depender de que se haya producido anteriormente tráfico alguno entre ambos y la red de transporte.

DHCP: (Dynamic Equipo ConFiguration Protocol.) Protocolo para la conFiguración automática de los parámetros de red de los equipos. La información se almacena en un servidor DHCP al que los equipos, al encenderse, solicitan los parámetros de conFiguración.

DIRECCIÓN IP: Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

DMA: El Acceso directo a memoria (DMA, del inglés Direct Memory Access) permite a cierto tipo de componentes de ordenador acceder a la memoria del sistema para leer y / o escribir independientemente de la CPU principal. Muchos sistemas hardware utilizan DMA, incluyendo controladores de unidades de disco, tarjetas gráficas, y tarjetas de sonido.

DNS: (Sistema de Nombres de Dominio) El DNS un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("equipos") basándose en los nombres de estos.

DTE: Data Terminal Equipment (computadora, estación de trabajo o equipo periférico).

EIA: Electronic Industries Alliance.

EQUIPO: (sistema central) Ordenador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP.

FIREWALL: Combinación de hardware y software la cual separa una red de área local (LAN) en dos o mas partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

FRAME RELAY: Frame Relay se define, oficialmente, como un servicio portador RDSI de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para velocidades de hasta 2,048 Mbps, aunque nada le impide superarlas. Trabaja en capa 2 del modelo OSI. Es utilizado para conectar distintas LANs entre si de una manera rápida y eficiente.

FTP: Protocolo de transferencia de archivos. Por medio del Protocolo de transferencia de archivos se pueden enviar o recibir archivos entre el cliente y el Equipo.

GATEWAY: Hoy se utiliza el término "Enrutador" (direccionador) en lugar de la definición original de "gateway". Actualmente Gateway es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero operativas diferentes.

GNU GPL: La GNU GPL (General Public License o licencia pública general) es una licencia creada por la Free Software Foundation y orientada principalmente a los términos de distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre.

HTTP: HTTP es un protocolo con la ligereza y velocidad necesaria para distribuir y manejar sistemas de información de varios medios. Es un protocolo genérico orientado al objeto, que puede ser usado para muchas tareas como servidor de nombres y sistemas distribuidos orientados al objeto, por extensión de los comandos, o métodos usados. Una característica de HTTP es la independencia en la visualización y representación de los datos, permitiendo a los sistemas ser construidos independientemente del desarrollo de nuevos avances en la representación de los datos. HTTP ha sido usado por los servidores World Wide Web desde su inicio en 1993.

IDF: CTP que alberga el equipo de conmutación principal de un edificio.

IEEE: Institute of Electrical & Electronic Engineers.

ICMP: El Protocolo de Control de Mensajes de Internet (ICMP por sus siglas en inglés) es uno de los protocolos centrales de la suite de protocolos de Internet. Es usado principalmente por los Sistemas operativos de las computadoras en una red para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible ó que un Enrutador ó Equipo no puede ser localizado.

IDS: IDS son las siglas para el sistema de detección de intrusos (Intrusion Detection System) por sus siglas en ingles

Internetworking: El arte y la ciencia de conectar redes individuales de área local (LAN) para crear una red de área amplia (WANs).Internetworking puede ser extremadamente complejo por que generalmente involucra la conectividad entre redes que usan diferentes protocolos.

IPCONFIG: Muestra los valores actuales de la conFiguración de la red TCP/IP y actualiza la conFiguración de DHCP (Protocolo de conFiguración dinámica de Equipo) y DNS (Sistema de nombres de dominio). Si se utiliza sin parámetros, ipconfig muestra las direcciones IPv6 o la dirección IPv4, la máscara de subred y la puerta de enlace predeterminada de todos los adaptadores.

IRQ: Interrupción (también conocida como interrupción hardware) es una señal recibida por el procesador de un ordenador, indicando que debe "interrumpir" el curso de ejecución actual y pasar a ejecutar código específico para tratar esta situación.

ISO: La Organización Internacional de Normalización (ISO) es una organización internacional no gubernamental, compuesta por representantes de los Organismos de Normalización (ONs) nacionales, que produce Normas Internacionales industriales y comerciales

ISP: Internet Service Provider Organización que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas o por líneas conmutadas. Es una entidad, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas físicas y/o jurídicas, les ofrece una serie de servicios (hospedaje de páginas web, consultoría de diseño e implantación de webs e Intranets, etc.).

IETF: El IETF (Internet Engineering Task Force, en castellano Grupo de Trabajo en Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad.

ITU: ITU, International Telecommunication Union (en español Unión Internacional de Telecomunicaciones, UIT) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas Administraciones y Empresas Operadoras.

LAN: (Red de Area Local) Red de datos para dar servicio a un área geográfica máxima de unos pocos kilómetros cuadrados, por lo cual pueden optimizarse los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps.

LOOPBACK: El dispositivo de red loopback es un interfaz de red virtual que siempre representa al propio dispositivo independientemente de la dirección IP que se le haya asignado. El valor en IPv4 es 127.0.0.1.

LINUX: Versión de libre distribución del sistema operativo UNIX; fue desarrollada por Linus Torvald

MAC: En redes de computadoras Media Access Control address cuyo acrónimo es MAC es un identificador físico -un número, único en el mundo, de 48 bits- almacenado en fábrica dentro de una tarjeta de red o una interfase usada para asignar globalmente direcciones únicas en algunos modelos OSI (capa 2) y en la capa física del conjunto de protocolos de Internet. Las direcciones MAC son asignadas por el IEEE y son utilizadas en varias tecnologías

MAINFRAME: Los ordenadores centrales o mainframes son ordenadores grandes, potentes y caros usados principalmente por grandes compañías para el procesamiento de grandes cantidades de datos, por ejemplo, el procesamiento de transacciones bancarias. El término apareció a principios de los setenta con la introducción de ordenadores más pequeños como la serie DEC PDP, que fueron conocidos como mini ordenadores, por lo que los usuarios acuñaron el término ordenador central para describir a los tipos de ordenadores más grandes y antiguos.

MDF: CTP que alberga equipo de comunicaciones del Backbone.

MIB: Abreviación para “Management Information Base” por sus siglas en ingles, Es una base de datos de objetos que pueden ser monitoreados por un sistema de administración de red. Tanto SNMP como RMON usan un formato estándar de MIB que permiten a cualquier herramienta SNMP o RMON monitorear cualquier dispositivo definido en MIB.

MODEM: Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una red digital de servicios integrados (ISDN), mediante unos procesos denominados modulación (para transmitir información) y desmodulación (para recibir información).

MPLS: MPLS (siglas de Multiprotocol Label Conmutadoring) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

NAS: Del inglés Network Access Servers (Servidores de acceso a la red). Estos servidores pueden conectar un módem a un circuito telefónico y proporcionar acceso de datos a Internet. En el futuro, los mismos *gateways* combinarán servicios VoIP y servicios de acceso a la red.

NAT: NAT ("Network Address Translation"): NAT es el método por el cual se traduce la dirección de un nodo en Red a otra dirección.

NETSTAT: Es una herramienta de línea de comandos que muestra un listado de las conexiones activas de un ordenador, tanto entrantes como salientes. Existen versiones tanto en sistemas Unix como en sistemas Windows

Networking: Término utilizado para referirse a las redes de telecomunicaciones en general.

NIC: Abreviado como NIC se refiere a “Network interface card” (por sus siglas en ingles), una tarjeta de expansión, que uno inserta en la computadora para poder estar conectado a una red.

OSI: Interconexión de Sistemas Abiertos (Open Systems Interconnect). Es el protocolo en el que se apoya Internet. Establece la manera como se realiza la comunicación entre dos computadoras a través de siete capas: Física, Datos, Red, Transporte, Sesión, Presentación y Aplicación.

PING: Packet Internet Groper. Sin lugar a dudas en una red el comando que más se puede llegar a utilizar es ping. Este comando se utiliza para comprobar si una determinada interfaz de red, de nuestra computadora o de otra, se encuentra activa. Su función más habitual es simplemente verificar si una máquina está encendida. Lo que se está haciendo en realidad es mandar paquetes del tipo ``echo request'', y para los que se devuelven son del tipo ``echo reply''.

PROXY: En el contexto de las ciencias de la computación, el término proxy (en inglés apoderado o delegado) hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual de esa representación es la de permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

QOS: La QoS (Quality of Service, Calidad de Servicio) garantiza que se transmitirá cierta cantidad de datos en un tiempo dado (throughput).

RADIUS: RADIUS (acrónimo en inglés de Remote Access Dial-In User Server). Es un protocolo de autentificación, autorización y accounting para aplicaciones de acceso a la red o movilidad IP.

RAM: Random Access Memory (memoria de acceso aleatorio). Por lo general el término RAM es comprendido generalmente como la memoria volátil (los datos e instrucciones se borran al apagarse la PC) que puede ser escrita y leída. La memoria del equipo permite almacenar datos de entrada, instrucciones de los programas que se están ejecutando en ese momento, los datos resultados del procesamiento y los datos que se preparan para la salida.

RFC: Serie de documentos iniciada en 1967 la cual describe el conjunto de protocolos de Internet y experimentos similares.

RIP: Son las siglas de Routing Information Protocol (Protocolo de información de encaminamiento). Es un protocolo de pasarela interior o IGP (Internet Gateway Protocol) utilizado por los Enrutadores, aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

ENRUTADOR: Dispositivo que distribuye tráfico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y Tablas de direccionamiento.

SCRIPT: Secuencia de comandos que se le dan a un módem con el propósito de configurarlo (velocidad, compresión de datos, etc.) o para realizar tareas específicas (llamar al proveedor, colgar, etc.). A veces es necesario modificar un script o cadena de inicio la cual establece las condiciones iniciales del módem (por ejemplo cambiar ATDT que establece una línea telefónica por tonos a ATDP que indica una línea telefónica por pulsos, etc.).

SMTP: Protocolo Simple de Transferencia de Correo. Es definido en STD 10, RFC 821, y se usa para la transferencia de correo electrónico entre computadoras. Es un protocolo de servidor a servidor, de forma que para poder leer los mensajes se deben utilizar otros protocolos.

SNIFFING: Es la técnica de capturar todos los paquetes que pasan por una red.

SNMP: Acrónimo de Simple Network Management Protocol. Protocolo estándar para la administración de red en Internet. Prácticamente todos los sistemas operativos, Enrutadores, Conmutadores, módems cable o ADSL módem, firewalls, etc. se ofrecen con este servicio.

SNORT: Es un sniffer de paquetes y un detector de intrusos. Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Así mismo existen herramientas de terceros para mostrar reportes en tiempo real (ACID) o para convertirlo en un Sistema Detector y Preventor de Intrusos.

TIA: Telecomunications Industry Association.

TCP: (Transmission Control Protocol) Protocolo de Control de Transmisión. Forma de comunicación básica de Internet la cual hace posible que cualquier tipo de información (mensajes, gráficos o audio) viaje en forma de paquetes sin que estos se pierdan y siguiendo cualquier ruta posible.

TELNET: Servicio de Internet con el cual un usuario se puede conectar de forma remota a otra computadora, como si se hiciera desde un terminal local, usualmente por el puerto 23. Es preferible usar otros programas más actualizados como ssh2, ya que Telnet tiene vulnerabilidades.

TMN: El término TMN es introducido por el ITU como la abreviatura para “Telecommunications Management Network” por sus siglas en ingles que significa administración de redes de telecomunicaciones. El concepto de un TMN esta definido por la recomendación M.3010. TMN tiene una relación fuerte con la administración OSI, y define un número de conceptos que tengan importancia para la administración de Internet.

TRACERT: Tracert es una utilidad, que se usa para seguir la ruta o camino que se toma en la red utilizando el protocolo TCP/IP. Lo hace enviando paquetes que van variando para así determinarla.

UDP: Protocolo de Datagramas de Usuario. Protocolo que no pide confirmación de la validez de los paquetes enviados por la computadora emisora. Este protocolo es actualmente usado para la transmisión de sonido y vídeo a través de Internet. El UDP está diseñado para satisfacer necesidades concretas de ancho de banda y como no reenvía los datos perdidos, es ideal para el tráfico de voz digitalizada debido a que un paquete perdido no afecta la calidad del sonido.

UNIX: Sistema operativo especializado en capacidades de multiusuario y multitarea. Fue la base inicial de Internet.

VLAN: Es el acrónimo de Virtual Local Area Network o Virtual LAN.

WEB SITE: Conjunto de páginas web que comparten un mismo tema e intención y que generalmente se encuentra en un sólo servidor. Punto de la red con una dirección única y al que pueden acceder los usuarios para obtener información.

BIBLIOGRAFÍA

Bibliografía

EDITORIAL

1. Cisco System, Inc. “Academia de Networking de Cisco System, Guía del primer año”. Segunda edición. Pearson Education. S.A. Madrid 2002.
2. Cisco System, Inc. “Academia de Networking de Cisco System, Guía del segundo año”. Segunda edición. Pearson Education. S.A. Madrid 2003.
3. Masahiko Matsushita: "Telecommunication Management Network", Vol. 3, NTT Review, 1991
4. CCITT Blue Book: "Recommendation M.30, Principles for a Telecommunications Management Network", Vol 4, 1989.
5. Francisco Jose Molina Robles. “Redes de área local” Alfa Omega RA-MA, 2004.
6. M. Julián Javier Robles Rivas. “Proyecto de Integración de la red Informática de la Facultad de Química. 2003
7. Christopher Negus. “La Biblia de Red Hat Linux 9. Anaya Multimedia, Febrero 2004.

ELECTRÓNICA

1. Facultad de Química. Sitio Web de la Facultad de Química.
   http://www.fquim.unam.mx/sitio/
2. Centro de operación de Red UNAM. Administración de redes TMN como metodología.
   http:www.noc.unam.mx/tech-docs/tmn-unam2.ppt
3. SimpleWeb.Introdution to TMN.
   http://www.simpleweb.org/tutorials/tmn/
4. International Comunication Union. Telecommunication Management Network (TMN).
   http://www.itu.int
5. Internacional organization for Standardization. OSI-MN.
   http://www.iso.org
6. Asociación técnicos de informática. Glosario de términos en Internet.
   http://www.ati.es/novatica/glosario/buscador/buscador_gloint.html
7. Sitio web para los entusiastas de la informática y las redes de computadoras. Arquitectura de administración OSI.
   http://www.arcesio.net/osinm/osinmfuncion.html
8. 3COM. Network Troubleshooting Overview.
   http://support.3com.com/infodeli/tools/netmgt/tncsunix/product/091500/c1ovrvw.htm
9. FreeRadius.
   http://www.freeradius.org/
10. El Centro de Tesis, Documentos, Publicaciones y Recursos Educativos más amplio de la Red. Diseño de una red LAN.
    http://www.monografias.com/trabajos12/redlan/redlan.shtml
11. Ingenieros en Informática. Administración de redes.
    http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/cap10.php
12. Ethereal.
    http://www.ethereal.com/
13. Seguridad en Unix y redes. Sistema de detección de intrusos.
    http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node280.html
14. Glosario de Términos informativos.
    http://www.geocities.com/Athens/2693/glosario.html

15. Pc-news. Monitoreo y respuesta a incidentes de seguridad.
http://pc-news.com/detalle.asp?sid=&id=11&Ida=1999
16. Fundamentos de informática, telecomunicaciones y redes. Modelo de referencia OSI.
http://www.fuac.edu.co/autonoma/servicios/estudiantes/tele/Osi/osi.html#aplica
17. The Internet Engineering Task Force. RADIUS Accounting.
18. http://www.ietf.org/rfc/rfc2866.txt
19. Red Hat. Red hat linux 9.
http://www.redhat.com/
20. Cisco. IP Subnet Calculation & Design Online Documentation.
http://www.cisco.com/techtools/ip_addr_help.html#Purpose%20&%20Scope
21. Anixter. Estándares para redes
http://www.anixter.com
22. Fibra óptica
http://orbita.starmedia.com/ygalarza/Ciencia.html
23. Cable coaxial
http://iio.ens.uabc.mx/~jmilanez/escolar/redes/05010000.html
24. Par Trenzado
http://www.prodigyweb.net.mx/fjrangelc/default_archivos/Page680.htm
25. Puertos TCP y UDP
http://www.iana.org/assignments/port-numbers

ÍNDICE DE FIGURAS

Índice de figuras

ÍNDICE DE TABLAS

Índice de tablas