13

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

INTEGRACIÓN DE SISTEMAS PARA LA ADMINISTRACIÓN DE LA RED NACIONAL DE CÓMPUTO DEL INSTITUTO FEDERAL ELECTORAL

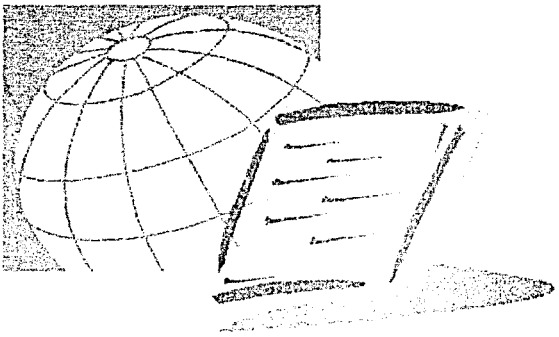
T E S I S
QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN
P R E S E N T A N :

CATALINA BERISTAIN GARZA
VERÓNICA GUTIÉRREZ PULIDO
ALEJANDRO PEREA MEJÍA
JORGE HUMBERTO TORRES ANTUÑANO

Director: M.I. Juan Carlos Roa Beiza

Cd. Universitaria, 2002

PAGINACIÓN DISCONTINUA



A mis padres, **Catalina Garza y Ricardo Beristain**, quienes me han heredado el tesoro más valioso que puede dársele a un hijo, su amor y comprensión, que sin estimar esfuerzo alguno han sacrificado gran parte de su vida en formarme y educarme. Para quien la ilusión de su existencia ha sido verme convertida en una mujer de provecho, nunca podré pagar todos sus desvelos ni con las riquezas más grandes del mundo. A los seres universalmente más queridos. Gracias.

A mis hermanos, **Lydia y Ricardo Beristain**, por su apoyo, motivación y contagiarme de su energía para lograr una superación día a día, pero sobre todo por creer en mi.

A **Lorena González** por su gran chispa, motivación y cariño.

A mis abuelos, **Hortensia Garza y Juan Martínez**, por su interés en mi superación personal y profesional, así como su invaluable apoyo en la culminación de mis estudios profesionales.

A mis compañeros de estudios y amigos, **César Sánchez, Arturo Ávila, Maite Martínez, Estela Monroy, Leticia Martínez, Verónica Gutiérrez**... por compartir conmigo su gran conocimiento, paciencia, pero principalmente su Amistad. Gracias por formar parte de mí.

A **Edgar García y Jorge Torres** por su gran apoyo, paciencia, cariño y alimentar en mí el espíritu de superación. Gracias por su invaluable Amistad.

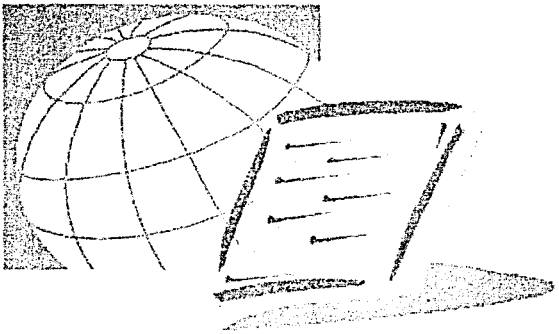
A todos aquellos que han formado parte en mi desarrollo personal y profesional, que no enlisto sus nombres, pero que indudablemente han sido parte importante en mi vida. Gracias.

A mi Alma Mater, **La Universidad Nacional Autónoma de México**, por abrirme las puertas del conocimiento y por iniciarme en la camino de la vida profesional.

Al **Instituto Federal Electoral y compañeros de trabajo** por el apoyo y facilidades en el desarrollo de esté trabajo de tesis.

Pero principalmente **a Dios**, por permitir que todo esto sea posible.

Catalina Beristain Garza



Primero que nada agradezco **a Dios** por haberme permitido llegar a donde me encuentro y por haberme dado la fuerza necesaria para salir adelante cuando la he requerido.

También les doy las gracias **a mis padres** por haberme brindado su apoyo incondicional en todo momento, por haber respetado mis decisiones y por el gran esfuerzo para darme una buena educación e inculcarme los principios morales que ahora tengo.

A mi hermana, que aunque no siempre estás de acuerdo conmigo, siempre estás ahí, compartiendo buenos y malos momentos.

A mis tíos y a mi abuelita, que siempre que lo he necesitado me han brindado su ayuda y que me han sabido aconsejar; también les agradezco esos momentos de convivencia, que aunque por la distancia no se den muy seguido, disfruto mucho.

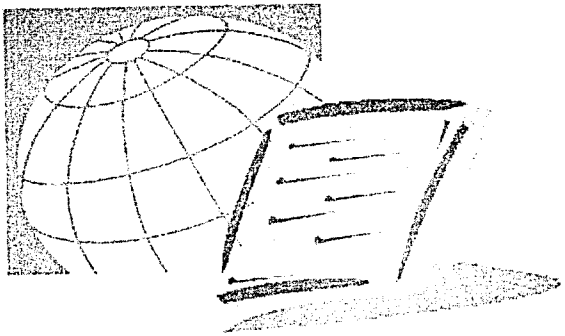
A Lety, por haberle dado el último toque a este trabajo de tesis, por la presión que ejerciste para que finalizaramos este trabajo, por tu comprensión y amistad incondicional.

A Maite, muchas gracias amiga por siempre estar presente, por la confianza que me has brindado y por todos los momentos que hemos pasado juntas.

A las Instituciones donde cursé mis estudios, primaria «John F. Kennedy», secundaria y preparatoria «Instituto Rudyard Kipling» y a la Facultad de Ingeniería por haberme brindado los conocimientos adquiridos y parte de la educación con la que cuento.

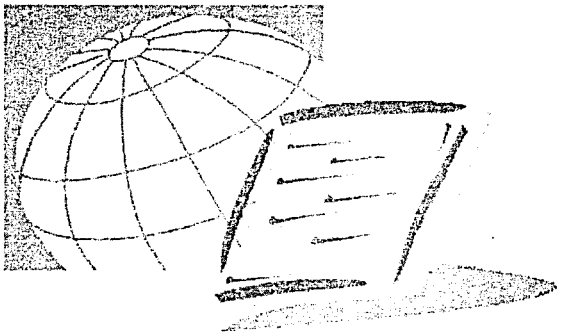
Finalmente a todas aquellas personas que no mencioné y que de una u otra manera contribuyeron con este logro.

Verónica Gutiérrez Pulido



Mil gracias a todas las personas que me han entendido y que a pesar de todo, me siguen brindando su amistad incondicional. Un agradecimiento especial a mi familia, que siempre ha apoyado mis decisiones.

Alejandro Perea Mejía



A mis padres, Perla Leticia Antuñano Ceniceros y Humberto Torres Sánchez

Con incalculable admiración y cariño, por su apoyo incondicional, por su preocupación infinita hacia mi persona, su esfuerzo incansable, por su cariño irremplazable, por sus estímulos y confianza, por sus consejos, por la formación que me han dado y porque con ellos, he logrado alcanzar ésta y todas las metas que me he propuesto. A ellos ... porque son únicos y porque me siento orgulloso de ser su hijo.

A mis queridos hermanos, Arturo y Rodrigo Alfonso

Porque han puesto en mi su confianza y su cariño, factores que me han impulsado a mejorar día a día en el ámbito familiar y laboral.

A toda mi familia, en especial a mi tía Mercedes Torres Sánchez y a mi abuela María de los Ángeles Ceniceros Cervantes.

Con respeto y cariño, porque incondicionalmente siempre me han brindado parte de su tiempo y esfuerzo.

A mis amigos, en especial a Catalina Beristain Garza y a Ma. Leticia Martínez Barrón

Principalmente, por su gran afecto y su sincera amistad; han estado a mi lado en toda circunstancia.

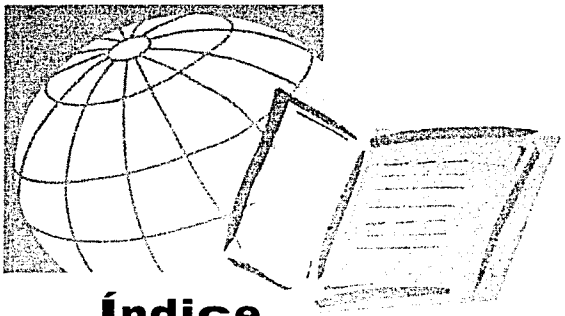
A mis compañeros de tesis, por sus enormes contribuciones y por haberme dado la oportunidad de participar con ellos.

A mis compañeros de trabajo, en especial a René Miranda Jaimes y a César Ledesma Ugalde

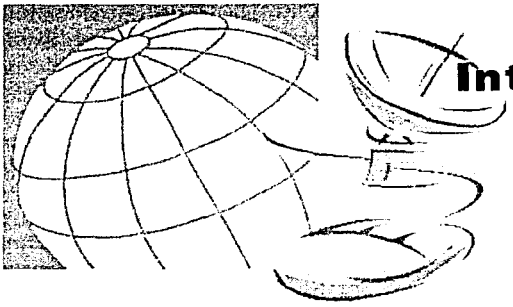
Por su compañerismo, por su confianza, por su trabajo y por su apoyo; piezas claves en el desarrollo profesional de mi persona.

A la Universidad Nacional Autónoma de México, en especial a la Facultad de Ingeniería, por ser mi segunda casa y brindarme las herramientas esenciales para desarrollarme en el ámbito en el cual hoy me desenvuelvo; y a la Dirección General de Servicios de Cómputo Académico, por abrirme sus puertas y darme la oportunidad de haber obtenido gran parte de la experiencia profesional con que hoy cuento.

UN SINCERO AGRADECIMIENTO A TODOS
Jorge Humberto Torres Antuñano



Índice



Introducción

El Instituto Federal Electoral cuenta con una red nacional de cómputo (RedIFE) que inició su operación a principios del año 2000. La red interconecta actualmente a las Oficinas Centrales y órganos desconcentrados en todo el país, sumando más de 350 nodos.

Actualmente la infraestructura de cómputo y comunicaciones instalada soporta diversos servicios, indispensables para el desarrollo de las actividades propias del Instituto; que van desde el correo electrónico, hasta los sistemas de información para los procesos electorales federales: Selección de Funcionarios de Casilla (Insaculación), Sistema de Información de la Jornada Electoral (SIJE), Programa de Resultados Electorales Preliminares (PREP) y otros.

Adicionalmente, se encuentra en proceso de análisis y desarrollo la actualización y modernización tecnológica de sistemas de carácter crítico, tanto para la operación interna del Instituto como para el servicio que se brinda al público en general.

Estos sistemas son:

- Sistema para la administración de los recursos del Instituto: administración de bienes, administración de servicios y administración de recursos humanos.

- Sistema para la transmisión en línea de datos del ciudadano desde los módulos de credencialización (foto digital, firma digital, huella digital, datos para la credencial).

Estos sistemas operarán en línea para la captura y consulta de información, haciendo uso intensivo de la infraestructura de la red nacional de informática.

De esta forma surge la necesidad de optimizar las funciones operativas de administración de la red y por tanto el objetivo del presente trabajo será integrar los sistemas que sean necesarios y así poder ofrecer a los usuarios de RedIFE un servicio de red eficiente y de calidad.

El sistema de administración deberá contar con herramientas que permitan el monitoreo continuo de los servicios, servidores, equipos de comunicaciones y enlaces; la detección automática y el correcto seguimiento de fallas; deberá tener la capacidad de hacer análisis del desempeño de la red y sus componentes, y la correspondiente automatización de procesos operativos. En él, se deberán ver reflejadas las necesidades de interacción entre las diversas áreas de operación y atención a usuarios.

El sistema deberá implementar los mecanismos para la detección, registro y seguimiento de posibles fallas, tanto de forma manual como automática; así como para el registro de parámetros operacionales de desempeño para la generación de reportes y estadísticas para la toma de decisiones.

La operación diaria del Instituto Federal Electoral, así como las actividades que se llevan a cabo, tienen un esquema de carácter centralizado; por lo cual los órganos desconcentrados dependen de las decisiones iniciales originadas desde las Oficinas Centrales.

El sistema de administración de red requerido, deberá incorporar y/o integrar las herramientas necesarias para llevar a cabo las tareas de monitoreo y seguimiento de problemas en la red de forma automatizada y sistemática. Esto ayudará en la toma de decisiones y la adecuada planeación del crecimiento de la red.

Los resultados esperados al finalizar este proyecto son:

1. Alta disponibilidad y alto desempeño de los servicios de red.
2. Detección automática de fallas y atención proactiva.
3. Rapidez y eficiencia en la solución de problemas.
4. Mejoramiento del manejo de los recursos.
5. Ofrecimiento de servicios de calidad.
6. Planeación de requerimientos futuros.
7. Automatización de procesos.
8. Generación de reportes para la toma de decisiones.

Consideramos que existen varias formas para resolver un problema y que probablemente la forma en que se organiza la información es importante durante el proceso de solución y desgloce del mismo. Por tanto, sentimos que una breve explicación de nuestra forma particular de resolver el problema sería importante exponerla en este momento.

Como el lector podrá percibir, en el **capítulo 1** se expone la problemática desde un punto de vista histórico y hasta cierto punto evolutivo. Aquí exponemos la forma en que, hasta antes del comienzo de la implementación de la solución, las tareas operativas de la red se llevaban a cabo. Se describe, también, cuáles son las entidades que intervienen en un proceso electoral, cual es su papel y cómo utilizan la infraestructura de comunicaciones para llevar a cabo sus tareas diarias.

Posteriormente en el apartado **1.2** se explica cuales son los equipos y las tecnologías utilizadas dentro de la infraestructura de comunicaciones de RedIFE y se indica cual es su papel dentro de la red y la forma en que se relaciona cada uno de ellos para brindar, en su conjunto, un servicio a las personas que laboran en el Instituto.

Finalmente en el apartado **1.3** se explican de manera puntual cuáles son los servicios que ofrece dicha infraestructura, tales servicios van desde el acceso a Internet y el correo electrónico hasta los servicios de bases de datos utilizados durante las jornadas electorales.

En el **capítulo 2**, se explican las tecnologías de comunicación utilizadas en RedIFE. El lector encontrará este capítulo muy informativo, ya que si no estuviera directamente relacionado con las tecnologías de información aquí encontrará una breve explicación de aquellas que se utilizan en RedIFE y que comúnmente se utilizan en muchas otras más redes de informática.

Este capítulo nos ayuda por un lado a comprender y delimitar el problema al que nos enfrentamos y también a darnos una idea clara de que tan complejo puede ser ofrecer los servicios informáticos en una organización como la del Instituto. Los temas que se cubren van desde la forma en que muchos sistemas trabajan en la actualidad, la arquitectura cliente-servidor, hasta la forma en que se transporta la información a través del cableado de la red de cómputo utilizando el protocolo TCP/IP.

Se expone también en el apartado **2.7.2** cómo es que actualmente se administran las redes de cómputo, lo cual nos hará intuir cuales son las posibles soluciones que se pueden adoptar para resolver el problema.

En el **capítulo 3**, entramos de lleno al proceso de solución, en donde utilizamos toda la información expuesta en los dos capítulos anteriores. Por un lado recordando la operación actual de la red, exponiendo las necesidades tanto actuales como futuras de los usuarios de la red.

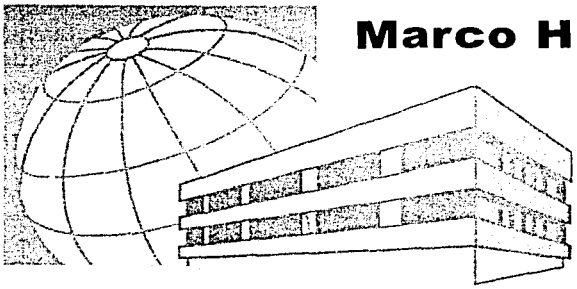
Luego en el los **apartados 3.5 y 3.6** respectivamente, exponemos las posibles soluciones y justificamos la que consideramos la solución más viable para el Instituto. Así mismo, al final del capítulo se expone de manera breve cuáles son los sistemas que se utilizarán y la forma en que estos trabajarán de manera integrada.

Para finalizar, el **capítulo 4** expone la forma en que se darán los flujos de trabajo entre las áreas de operación, con el uso da la nueva integración de sistemas para la administración de la red nacional de computo del Instituto Federal Electoral.

Consideramos que para su mejor entendimiento, debemos sugerir al lector detenerse a leer los dos primeros capítulos y entender bien las tecnologías utilizadas. Como hemos mencionado antes, el capítulo 2 nos da las bases necesarias, pero si no fuese suficiente, al final del trabajo se presenta bibliografía complementaria que el lector podrá consultar según sus necesidades.

Creemos conveniente mencionar que este trabajo de tesis contiene tecnicismos en inglés, los cuales tienen la traducción que encontramos más apropiada, entre paréntesis, la primera vez que aparecen.

CAPÍTULO I



Marco Histórico

1.1 FUNCIONES DEL INSTITUTO FEDERAL ELECTORAL

El Instituto Federal Electoral (IFE) es un organismo público autónomo, responsable de cumplir con la función estatal de organizar las elecciones federales, es decir, las relacionadas con la elección del Presidente de los Estados Unidos Mexicanos (cada 6 años) y de los diputados y senadores que integran el Congreso de la Unión (cada 3 años).

1.1.1 Antecedentes

Una vez constituido formalmente, el IFE empezó a funcionar el 11 de octubre de 1990 como resultado de una serie de reformas a la Constitución Política aprobadas en 1989 y de la expedición de una nueva legislación reglamentaria en materia electoral, el Código Federal de Instituciones y Procedimientos Electorales (COFIPE), en agosto de 1990. Antes de las reformas de 1989, la organización de las elecciones federales era función del Registro Federal Electoral, organismo que dependía directamente de la Secretaría de Gobernación.

Desde la fecha de creación del Instituto Federal Electoral la normatividad constitucional y legal en la materia ha experimentado tres importantes procesos de reforma: 1993, 1994 y 1996, que han impactado de manera significativa la integración y atributos del organismo depositario de la autoridad electobçl.

Entre los principales cambios e innovaciones, resultado de estos procesos de reforma, destacan los siguientes:

• La reforma de 1993 facultó a los órganos del Instituto Federal Electoral para la declaración de validez y la expedición de constancias para la elección de diputados y senadores así como para establecer topes a los gastos de campaña de las elecciones.

• La reforma de 1994 incrementó el peso e influencia de los consejeros ciudadanos en la composición y procesos de toma de decisiones de los órganos de dirección, confiriéndoles la mayoría de los votos, y amplió las atribuciones de los órganos de dirección a nivel estatal y distrital.

• La reforma de 1996 reforzó la autonomía e independencia del Instituto Federal Electoral al desligar, por completo, al Poder Ejecutivo de su integración y reservar el voto dentro de los órganos de dirección, exclusivamente a los consejeros ciudadanos.

1.1.2 Objetivos y actividades

El Instituto Federal Electoral está dotado de personalidad jurídica y patrimonio propios, es independiente en sus decisiones y funcionamiento del gobierno federal. En su integración participan el Poder Legislativo de la Unión, los partidos políticos nacionales y los ciudadanos.

Para el desempeño de sus actividades, el Instituto cuenta con un cuerpo de funcionarios integrados en un Servicio Profesional Electoral, a través del cual se da un seguimiento exhaustivo a las trayectorias laborales y se impulsa el desarrollo de los funcionarios en el marco de los procesos electorales. Con el fin de elevar el desempeño del Instituto y el personal en su conjunto.

A diferencia de los organismos electorales anteriores, que sólo funcionaban durante los procesos electorales (aproximadamente 1 año), del Instituto Federal Electoral se constituye como una institución de carácter permanente.

El Instituto Federal Electoral tiene su sede central en el Distrito Federal y se organiza bajo un esquema desconcentrado que le permite ejercer sus funciones en todo el territorio nacional.

De manera expresa y precisa, el ordenamiento legal dispone que la organización y funcionamiento del Instituto Federal Electoral apunte al cumplimiento de los siguientes fines:

- Contribuir al desarrollo de la vida democrática.
- Preservar el fortalecimiento del régimen de partidos políticos.
- Integrar el Registro Federal de Electores.
- Asegurar a los ciudadanos el ejercicio de sus derechos político electorales y vigilar el cumplimiento de sus obligaciones.
- Garantizar la celebración periódica y pacífica de las elecciones para renovar a los integrantes de los Poderes Legislativo y Ejecutivo de la Unión.
- Velar por la autenticidad y efectividad del sufragio.
- Llevar a cabo la promoción del voto y coadyuvar a la difusión de la cultura democrática.

Para alcanzar las metas establecidas, el Instituto Federal Electoral tiene a su cargo en forma integral y directa todas las actividades relacionadas con la preparación, organización y conducción de los procesos electorales, así como aquellas que resultan consecuentes con los fines que la ley le fija. Entre sus actividades fundamentales se pueden mencionar las siguientes:

- Capacitación en procesos electorales y educación cívica.
- Establecimiento y revisión continua de la geografía electoral.
- Derechos y prerrogativas de los partidos y agrupaciones políticas.
- Mantenimiento del padrón y listas de electores.
- Diseño, impresión y distribución de materiales electorales.
- Preparación de la jornada electoral.
- Cómputo de resultados.
- Declaración de validez y otorgamiento de constancias en la elección de diputados y senadores.
- Regulación de la observación electoral y de las encuestas y sondeos de opinión.

1.1.3 Estructura orgánica

En la conformación y funcionamiento del Instituto se distinguen y delimitan claramente las atribuciones de cuatro tipos de órganos: Órganos de Dirección, Órganos Ejecutivos, Órganos Técnicos y Órganos de Vigilancia.

Atendiendo al principio de desconcentración en que se sustenta la organización y funcionamiento del Instituto, estos órganos están representados a nivel central y delegacional (una delegación en cada una de las 32 entidades federativas y una subdelegación en cada uno de los 300 distritos uninominales). En la figura 1.1.3.1 se muestra la estructura orgánica del Instituto.

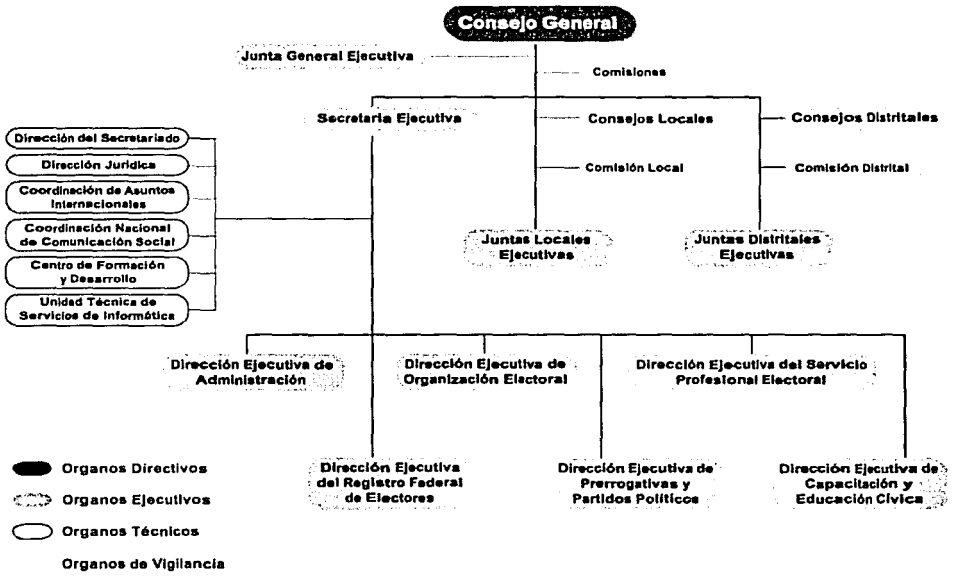


Figura 1.1.3.1 Estructura orgánica del Instituto Federal Electoral

1.1.4 Órganos de Dirección

- **Centrales.**

Consejo General.

Es el encargado de dirigir las actividades del Instituto, mediante la supervisión de la integración y el adecuado funcionamiento de los demás órganos en función de las políticas y programas aprobados de forma anual, así como también dictar las modalidades pertinentes para el óptimo aprovechamiento de los recursos de acuerdo a los informes anuales.

El Consejo General se integra por: Comisiones, Consejeros Electorales, Consejeros del Poder Legislativo y Consejeros de los Representantes de Partidos políticos.

Presidencia del Consejo.

Es un órgano central de carácter unipersonal que tiene a su cargo: presidir el Consejo; proponer al Consejo el nombramiento y remoción de los titulares de las Unidades Técnicas; presentar al Consejo el anteproyecto de presupuesto del año siguiente para su aprobación y remitirlo al titular del Poder Ejecutivo; designar a los encargados de despacho en caso de ausencia y convocar la realización de las sesiones de Consejo y de las reuniones de la Junta General Ejecutiva.

- **Delegacionales.**

Consejos Locales.

Son órganos delegacionales constituidos en cada una de las entidades federativas, que se instalan y sesionan durante los procesos electorales exclusivamente. Dentro de las atribuciones que les confiere la ley, los Consejos Locales tienen que velar por la observancia de las disposiciones del COFIPE a nivel local, así como el crear comisiones locales y vigilar el desempeño y funcionamiento de las vocalías de la Junta Local.

Los Consejos Locales están integrados por: el Presidente del Consejo Local, Comisiones Locales, Consejeros Electorales Locales y Representantes de los Partidos Políticos ante el Consejo Local.

Consejos Distritales.

Son órganos subdelegacionales constituidos en cada uno de los 300 distritos electorales, que se instalan y sesionan durante los procesos electorales exclusivamente. Dentro de las atribuciones que les confiere la ley, los Consejos Locales tienen que velar por la observancia de las disposiciones del COFIPE a nivel distrital, así como el crear comisiones distritales y vigilar el desempeño y funcionamiento de las vocalías de la Junta Distrital.

Los Consejos Distritales están integrados por: el Presidente del Consejo Distirtal, Comisiones Distritales, Consejeros Electorales Distritales y Representantes de los Partidos Políticos ante el Consejo Distrital.

Mesas Directivas de Casilla.

Son órganos que se instalan únicamente durante la jornada electoral y sus atribuciones son: instalar y clausurar la casilla en los términos del

COFIPE, recibir la votación, efectuar el escrutinio y cómputo de la votación, permanecer en la casilla durante toda la jornada y conducirse con respeto hacia los votantes y con estricto apego a la normatividad electoral.

Están integradas por: Funcionarios de casilla seleccionados mediante el proceso de insaculación y representantes de los partidos políticos acreditados.

1.1.5 Órganos Ejecutivos

- **Centrales.**

Junta General Ejecutiva.

Es un órgano ejecutivo de naturaleza colegiada que se integra de conformidad con lo que establece el artículo 85 del COFIPE. Sus atribuciones son: cumplir y ejecutar los acuerdos del Consejo; coordinar y supervisar la ejecución de las políticas y programas generales y específicos del Instituto; dictar los lineamientos necesarios para la adecuada ejecución de los acuerdos y resoluciones del Consejo y coordinar las actividades de las Direcciones Ejecutivas.

Secretaría Ejecutiva.

Es un órgano de carácter unipersonal, encargado de conducir la administración y supervisar el desarrollo adecuado de las actividades de los órganos ejecutivos y técnicos del Instituto, así como fungir como el representante legal del mismo. Su titular es el Secretario Ejecutivo.

Direcciones Ejecutivas:

Registro Federal de Electores (DERFE). Esta Dirección Ejecutiva tiene las siguientes atribuciones a su cargo: formar el catálogo general de electores; aplicar la técnica censal total en el territorio del país para formar el catálogo general de electores; aplicar la técnica censal en forma parcial en el ámbito territorial que determine la Junta General Ejecutiva; formar el padrón electoral; expedir la credencial para votar; revisar y actualizar anualmente el padrón electoral; establecer con las autoridades federales, estatales y municipales la coordinación necesaria, a fin de obtener la información sobre fallecimientos de los ciudadanos, o sobre pérdida, suspensión u obtención de ciudadanía; proporcionar a los órganos competentes del Instituto y a los partidos

políticos nacionales, las listas nominales de electores; formular, con base en los estudios que realice, el proyecto de división del territorio nacional en 300 distritos electorales uninominales, así como de las cinco circunscripciones plurinominales; mantener actualizada la cartografía electoral del país y asegurar que las comisiones de vigilancia nacional, estatales y distritales se integren, sesionen y funcionen de acuerdo al COFIPE.

Prerrogativas y Partidos Políticos (DEPyPP). Esta Dirección Ejecutiva tiene las siguientes atribuciones a su cargo: conocer de las notificaciones que formulen los organizaciones que pretendan constituirse como partidos políticos nacionales o como agrupaciones políticas y realizar las actividades pertinentes; recibir las solicitudes de registro de las organizaciones de ciudadanos que hayan cumplido los requisitos establecidos en el COFIPE para constituirse como partido político o agrupación política e integrar el expediente respectivo a someter a consideración del Consejo General; inscribir en el libro respectivo el registro de partidos y agrupaciones políticas, así como los convenios de fusión, frentes, coaliciones y acuerdos de participación; ministrar a los partidos políticos nacionales y a las agrupaciones políticas el financiamiento público al que tienen derecho; llevar a cabo los trámites necesarios para que los partidos políticos puedan disponer de las franquicias postales y telegráficas que les corresponden; apoyar las gestiones de los partidos políticos y las agrupaciones políticas para hacer efectivas las prerrogativas que tienen conferidas en materia fiscal; realizar las actividades para que los partidos políticos ejerzan sus prerrogativas y puedan acceder a la contratación de tiempos en radio y televisión; presidir la comisión de radiodifusión; llevar el libro de registro de integrantes de los órganos directivos de los partidos políticos y de sus representantes acreditados ante los órganos del Instituto a nivel nacional, local y distrital, así como el de los dirigentes de las agrupaciones políticas y llevar los libros de registro de candidatos a los puestos de elección popular.

Organización Electoral (DEOE). Esta Dirección Ejecutiva tiene las siguientes atribuciones a su cargo: apoyar la integración, instalación y funcionamiento de las Juntas Locales y Distritales Ejecutivas; elaborar los formatos de la documentación electoral, para someterlos a la aprobación del Consejo General; proveer lo necesario para la impresión y distribución de la documentación electoral autorizada; recabar de los Consejos Locales y de los Consejos Distritales, copias de las actas de sus sesiones y demás documentos relacionados con el proceso electoral y recabar la documentación necesaria e integrar los

expedientes a fin de que el Consejo General efectúe los cómputos que debe realizar; llevar la estadística de las elecciones federales.

Servicio Profesional Electoral (DESPE). Esta Dirección Ejecutiva tiene las siguientes atribuciones a su cargo: formular el anteproyecto de Estatuto que regirá a los integrantes del Servicio Profesional Electoral y llevar a cabo los programas de reclutamiento, selección, formación y desarrollo del personal profesional.

Capacitación Electoral y Educación Cívica (DECEyEC). Esta Dirección Ejecutiva tiene las siguientes atribuciones a su cargo: elaborar y proponer los programas de educación cívica y capacitación electoral que desarrollen las Juntas Locales y Distritales Ejecutivas; coordinar y vigilar el cumplimiento de los programas a que se refiere el inciso anterior; preparar el material didáctico y los instructivos electorales; orientar a los ciudadanos para el ejercicio de sus derechos y cumplimiento de sus obligaciones político-electorales y llevar a cabo las acciones necesarias para exhortar a los ciudadanos que no hubiesen cumplido con las obligaciones establecidas en el COFIPE, en particular las relativas a inscribirse en el Registro Federal de Electores y las de voto, a que lo hagan.

Administración (DEA). Esta Dirección Ejecutiva tiene las siguientes atribuciones a su cargo: aplicar las políticas, normas y procedimientos para la administración de los recursos financieros y materiales del Instituto; organizar, dirigir y controlar la administración de los recursos materiales y financieros, así como la prestación de los servicios generales en el Instituto; formular el anteproyecto anual del presupuesto del Instituto; establecer y operar los sistemas administrativos para el ejercicio y control presupuestales; elaborar el proyecto de manual de organización y catálogo de cargos y puestos del Instituto y someterlo a la aprobación a la Junta General Ejecutiva; atender las necesidades administrativas de los órganos del Instituto y presentar al Consejo General un informe anual respecto del ejercicio presupuestal del Instituto.

- **Delegacionales.**

Juntas Locales y Distritales Ejecutivas.

Son órganos colegiados de carácter permanente, encargados de aplicar los programas y políticas del Instituto en el ámbito territorial de cada una de las entidades federativas, tanto a nivel estatal como a nivel distrital.

Están integradas por las siguientes áreas: la Vocalía Ejecutiva, la Vocalía del Secretariado, la Vocalía del Registro Federal de Electores, la Vocalía de Capacitación Electoral y Educación Cívica y la Vocalía de Organización Electoral.

Vocales Ejecutivos Locales y Distritales.

Las atribuciones que les confiere el reglamento a los vocales ejecutivos es el de presidir el Consejo Local o Distrital, según corresponda y tener a su cargo la coordinación de las actividades de las Juntas Ejecutivas.

1.1.6 Órganos Técnicos

- **Centrales.**

Direcciones o Unidades Técnicas:

Coordinación Nacional de Comunicación Social (CNCS). Tiene las siguientes atribuciones a su cargo: implementar la estrategia de comunicación social necesaria, para difundir las actividades y funciones que desarrolla el Instituto, mediante políticas y programas aprobados; lleva a cabo un monitoreo continuo de los medios de comunicación, impresos y electrónicos sobre información relacionada con las actividades y funciones que desarrolla el Instituto. La CNCS es la representante ante los medios de comunicación para cualquier actividad o necesidad relacionada con ellos.

Coordinación de Asuntos Internacionales (CAI). Tiene las siguientes atribuciones a su cargo: ser la representante del Instituto a nivel internacional; promover el conocimiento y la adecuada valoración de la organización de los procesos electorales federales en México y coordinar las acciones de intercambio informativo, cooperación, asesoría y asistencia técnica en las que participe el Instituto a nivel internacional.

Contraloría Interna (CI). Ejerce sus atribuciones de manera autónoma respecto de cualquier órgano ejecutivo del Instituto, quedando supeditada al Consejo General. Su actividad principal es la de ejercer el Programa Anual de Auditoría Interna del Instituto.

Unidad Técnica de Servicios de Informática (UTSI, también llamada UNICOM). Tiene las siguientes atribuciones a su cargo: aplicar normas y reglamentos que deban regir el desarrollo, operación y mantenimiento de la infraestructura informática y de comunicaciones del Instituto;

realizar estudios, análisis, diseños, desarrollos, implementaciones, mantenimientos y expansiones para la infraestructura informática de cómputo y telecomunicaciones que las distintas áreas del Instituto le soliciten; desarrollar, administrar y mantener la red nacional de informática del Instituto, para interconenctar a los órganos directivos y ejecutivos centrales con los órganos locales y distritales; colaborar en la automatización permanente de los procesos administrativos y operativos del Instituto mediante la utilización de sistemas informáticos y comunicaciones; e implementar el sistema para el Programa de Resultados Electorales Preliminares.

Dirección Jurídica (DJ). Tiene las siguientes atribuciones a su cargo: coadyuvar con el Secretario Ejecutivo en el ejercicio de la representación legal del Instituto; preparar proyectos de reglamentos interiores y demás dispositivos jurídicos necesarios para el buen funcionamiento del Instituto y brindar toda la asesoría jurídica a los demás órganos para el correcto desempeño de sus actividades.

Dirección del Secretariado (DS). Tiene las siguientes atribuciones a su cargo: supervisar y verificar que las disposiciones legales, normas, políticas, criterios, lineamientos y metodología aprobada para la coordinación, gestión y control de recursos, se cumplan correctamente; y apoyar al Secretario Ejecutivo en el seguimiento y control de todos los asuntos y actividades a su cargo.

Centro de Formación y Desarrollo (CFD). Tiene las siguientes atribuciones a su cargo: diseñar exámenes para los procedimientos de reclutamiento y selección propios del Servicio Profesional Electoral del Instituto, así como para el personal de la rama administrativa; diseñar e impartir cursos de formación, capacitación y actualización para los aspirantes, miembros provisionales y miembros titulares del Servicio Profesional Electoral, así como el llevar a cabo la evaluación periódica de los integrantes; y proponer y llevar a cabo análisis, estudios e investigaciones para el desarrollo institucional de los órganos del Instituto y de éste en su conjunto.

Comité Nacional de Seguimiento y Evaluación. Este comité tiene la atribución de vigilar el desarrollo de los programas a nivel institucional y llevar a cabo la evaluación de los mismos; está integrado de acuerdo a los estatutos del COFIPE.

1.1.7 Órganos de Vigilancia

Centrales.

Comisión Nacional de Vigilancia. Es el órgano encargado de coadyuvar en que los trabajos relativos al Padrón Electoral se cumplan cabalmente.

Comisión de Radiodifusión. Se encarga de vigilar que las transmisiones de radio y televisión previstas en el COFIPE se realicen conforme al plan de medios que elabora la Dirección Ejecutiva de Prerrogativas y Partidos Políticos.

Delegacionales.

Comisiones Locales y Distritales de Vigilancia. Estas comisiones se integran por un Presidente (Vocal del Registro Federal de Electores), un Representante Propietario y un suplente por cada Partido Político Nacional y un Secretario designado por su Presidente. Sus atribuciones básicas son un reflejo de la Comisión Nacional de Vigilancia a nivel estatal y distrital.

1.2 INFRAESTRUCTURA DE CÓMPUTO Y COMUNICACIONES DE LA RED NACIONAL DE INFORMÁTICA DEL INSTITUTO

La infraestructura de la red de cómputo y comunicaciones del Instituto Federal Electoral surgió con la necesidad de contar con sistemas de comunicaciones que enlacen a todas sus áreas para garantizar un correcto flujo e intercambio de información. Dentro de la estructura del Instituto, la Dirección Ejecutiva del Registro Federal de Electores, anteriormente Registro Nacional de Electores, tuvo la necesidad de instalar un sistema de comunicaciones que comprendiera una red privada de datos, así como una red de voz para poder llevar a cabo una de sus funciones principales, la cual consiste en el mantenimiento del Padrón de Electores.

En la figura 1.2.1, se puede apreciar que la red para el mantenimiento del padrón electoral consiste en cuatro nodos principales que integran el backbone (red dorsal), estos nodos corresponden a la Cd. de México, Guadalajara, Monterrey y Puebla, los cuales se comunican entre sí a través de la tecnología **ATM** (Asynchronous Transfer Mode – Modo de Transferencia Asíncrona). A su vez estos se comunican con los nodos remotos por medio de **Frame Relay** (tecnología para redes WAN basada en conmutación de circuitos). Los enlaces utilizados para la interconexión de los nodos son proporcionados por **TELMEX** (Teléfonos de México).

Asimismo, la topología mostrada en la misma figura, es una estrella compuesta; en cuanto al intercambio de información, se comporta como una estrella, ya que el nodo de la Cd. De México, es el único que cuenta con los privilegios de tener acceso a los demás sitios. Los usuarios de cada una de las redes locales no tienen acceso a cualquiera de las otras redes, a excepción del mencionado, por razones de seguridad y confidencialidad de los datos.

Topología de la Red General del Sistema Integral de Comunicaciones del IFE

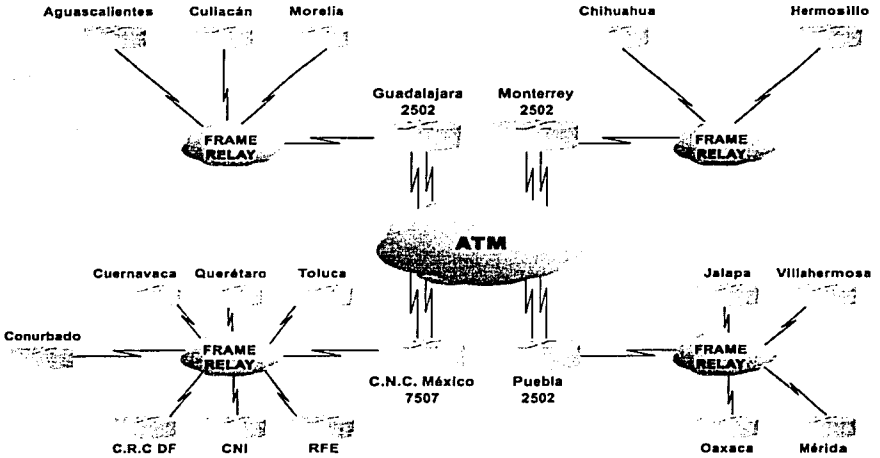


Figura 1.2.1 Red de comunicaciones para el mantenimiento del Padrón Electoral.

Las redes locales de los sitios remotos utilizan la arquitectura **Token Ring**. El acceso a estas redes se hace mediante enlaces seriales dedicados en **Frame Relay**. Se cuenta con enlaces de respaldo mediante líneas conmutadas y acceso vía módem al Centro Nacional de Cómputo (CNC), ubicado en la Cd. de México, mediante un servidor de acceso. Este equipo tiene la capacidad de atender simultáneamente a los 18 Centros Regionales de Cómputo (CRCs) que se encuentran en diferentes estados dentro de la República Mexicana.

De esta manera la DERFE es la primer área dentro del Instituto que lleva a cabo la instalación de una infraestructura de cómputo y comunicaciones para la automatización y realización de sus actividades y funciones.

Posteriormente durante el Proceso Electoral de 1997 se instaló en el Instituto una red de cómputo (ver figura 1.2.2), autónoma e independiente de la red para el mantenimiento del padrón electoral, que permitió llevar a cabo el sistema del Programa de Resultados Preliminares (PREP), que tuvo a su cargo la difusión inmediata de los resultados de la elección ante el Consejo General del Instituto, los Partidos Políticos Nacionales y la ciudadanía en general.

Para el correcto desarrollo del PREP, fue necesario diseñar un sistema de informática para recabar, capturar, validar y difundir la información. El desarrollo de la solución tecnológica para la realización de las elecciones de 1997 integra el uso de diferentes herramientas y equipo. Dentro de los sistemas, se necesitó de un manejador de bases de datos robusto, capaz de atender al número de transacciones esperadas; un monitor de transacciones capaz de garantizar la integridad de los datos, su incorporación a la base, así como la replicación entre centros y balanceo de cargas entre ellos; un conjunto de servicios y programas de extracción capaces de realizar todas las actividades de validación y autenticación de los datos, su incorporación a las tablas diseñadas para tal efecto, realizar las sumas correspondientes para cada tipo de votación y por último, realizar una extracción rápida y eficiente de datos; sistemas de transporte de la información entre centros; sistema global de difusión de resultados, el cual cuenta con los componentes necesarios para la generación de páginas HTML, gráficas dinámicas, reportes, generación de pantallas para el sistema de difusión dentro de las instalaciones del IFE y finalmente, el transporte de la información a sitios externos autorizados para la difusión de resultados en Internet.

Para los comicios se instalaron alrededor de 110,000 casillas distribuidas en el Distrito Federal y el interior de la República. Las actas generadas en cada casilla se concentraron en 300 nodos distritales, Centros de Acopio de Datos (CEDATs), para su captura y transmisión. Todos estos datos llegaron a un servidor de acceso comunicándose a través del protocolo de comunicaciones X.25 al centro de procesamiento, Centro Nacional de Recepción de Resultados Electorales Preliminares (CENARREP), ubicado en las oficinas centrales del IFE. Para mantener una confiabilidad y disponibilidad de todo el sistema se instaló un CENARREP alterno, ubicado en las instalaciones del World Trade Center (WTC). Conforme llegaba la información del conteo de las casillas, el CENARREP realizaba el conteo global para su publicación. La difusión de los resultados al interior del IFE se hizo mediante una Intranet y la difusión al público en general se hizo a través de Internet.

Se requirieron diversos servicios para comunicar a los CEDATs con los CENARREPs y los diferentes nodos que conformaron la red del PREP. La transferencia de datos entre el CEDAT y el CENARREP se llevó a cabo mediante módems. En cada CEDAT existían cinco líneas telefónicas: dos líneas dedicadas a la conexión vía módem por medio de las controladoras de las terminales punto de venta (**POS, Point of Sale**), una línea para la conexión a Internet; y las dos restantes, para voz.

Diagrama General Red PREP

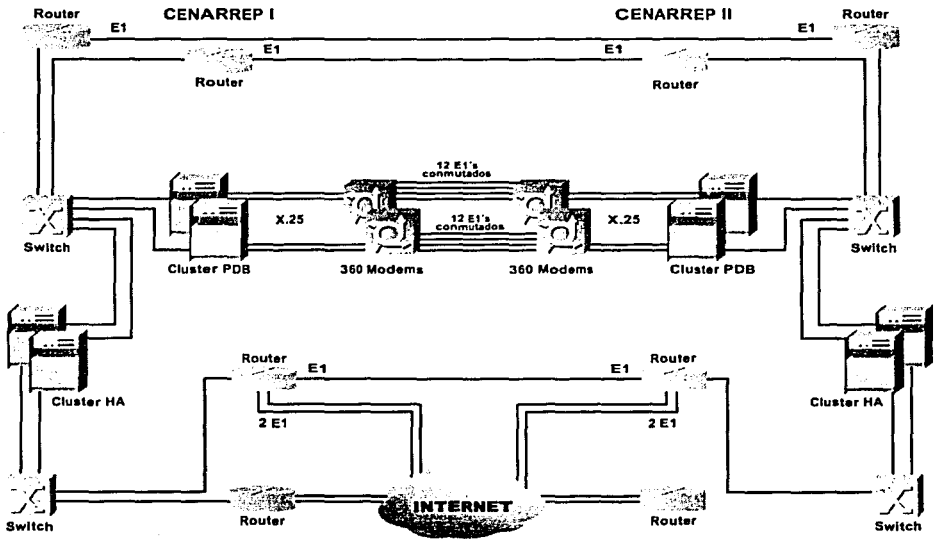


Figura 1.2.2 Diagrama General del Sistema de Cómputo y Comunicaciones para el PREP97.

En diseño original contemplaba la conexión de todos los centros distritales a un solo centro de cómputo y utilizar una aplicación que haría la replicación hacia el otro centro convirtiéndolo en un espejo. Para lograr una mayor rapidez, se decidió que, en las horas pico, operaran simultáneamente los equipos de respaldo conectados al CENARREP 2. Aprovechando que el diseño original lo permitía, la mitad de los CEDATs se conectaron al CENARREP 1 y la otra mitad de los CEDATs se conectaron al CENARREP 2, por lo que de un esquema simple de replicación se pasó a un esquema de procesamiento distribuido.

Los enlaces conmutados (líneas telefónicas) fueron proporcionadas e instaladas por TELMEX.

La consulta de los resultados del PREP en las Juntas Distritales y Locales Ejecutivas fue mediante una cuenta de acceso vía módem a un proveedor de servicios de Internet (**Internet Service Provider, ISP**), y en los CENARREPs se instalaron dos enlaces dedicados con dos proveedores de servicios de Internet diferentes.

Con la finalidad de contar con una infraestructura de redes lo bastante confiable, segura, y con un buen rendimiento, además de proyectar su utilización para los próximos años, se implantó una red de cómputo en las oficinas centrales ubicadas en el Conjunto Tlalpan de la Cd. de México mediante la instalación de cableado estructurado y la puesta en operación de servicios en Internet, que atendían a las necesidades iniciales del PREP. Esto permitió al Instituto aprovechar las ventajas de TCP/IP y brindar nuevos servicios tanto al personal como al público en general. En esas fechas el Instituto no contaba con un área específica encargada de ofrecer el soporte técnico a los usuarios, ni a la infraestructura de cómputo y comunicaciones instalada, por lo que al finalizar la jornada electoral de ese año, parte del personal que laboró en el PREP quedó a cargo de esas actividades.

En ese momento, los usuarios de la infraestructura instalada contaban principalmente con el servicio de Internet, más que servicios de uso interno del Instituto. Paulatinamente se fueron organizando, desarrollando y ofreciendo diversos servicios internos. Estos permitían la comunicación entre las diferentes áreas del Instituto, así como eliminar algunos gastos en papelería debido a la disminución de envío de faxes, impresión de boletines, etc.

Dada la problemática de que el Instituto contara con sistemas informáticos de cómputo y de comunicaciones para el adecuado ejercicio de sus funciones en el territorio nacional, surgió una iniciativa de crear la Unidad Técnica de Servicios de Informática, la cual tiene como funciones: realizar estudios, análisis, diseños, desarrollos, implementaciones, mantenimiento y expansiones para la infraestructura informática.

En la figura 1.2.3 se muestra la interconexión entre los edificios del conjunto Tlalpan: Edificio A, Edificio B, Edificio C y Edificio D. Actualmente cada edificio cuenta con un sistema de distribución de cableado estructurado (**Distribution Facility, DF**). En el caso de los edificios B, C y D, el sistema es de tipo "intermedio" (**Intermediate Distribution Facility, IDF**). Los equipos activos de los IDFs se conectan directamente a los equipos del sistema de distribución "principal" (**Main Distribution Facility, MDF**) por medio de la fibra óptica.

Actualmente los equipos activos que proporcionan el servicio de red a los usuarios son principalmente switches de capa 2, que hacen uso de las tecnologías Ethernet, FastEthernet y GigabitEthernet. Los equipos situados en el MDF se encargan de hacer las funciones de ruteo de paquetes y de la definición de las redes virtuales (**Virtual Local Area Networks, VLANs**) para la adecuada segmentación del tráfico de los grupos de usuarios del conjunto Tlalpan.

En un inicio los equipos que proporcionaban el servicio de red en cada uno de los edificios eran principalmente concentradores, interconectados a un switch encargado de hacer una segmentación simple del tráfico. La única tecnología utilizada era Ethernet. En la figura 1.2.3 se puede observar la interconexión de los concentradores mencionados antes de ser sustituidos por los switches.

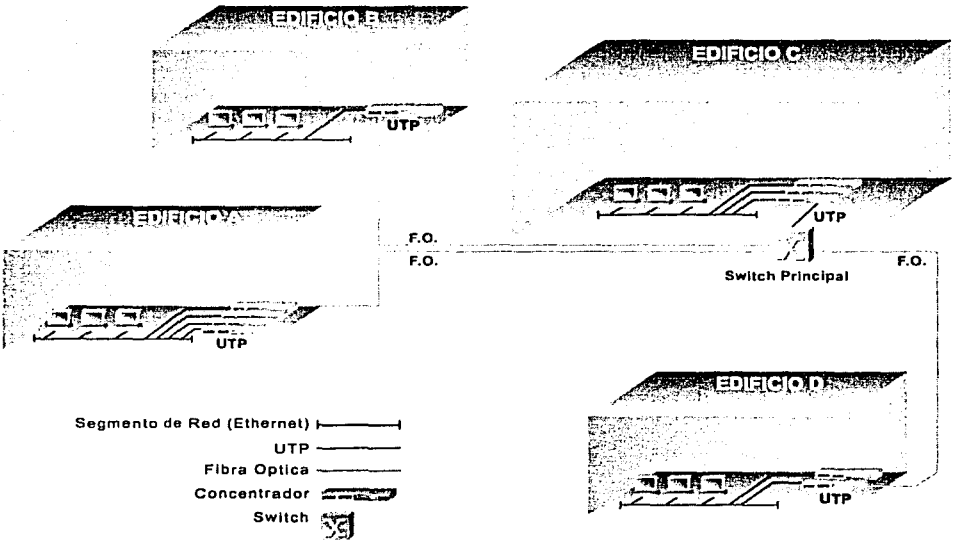


Figura 1.2.3 Diagrama de Interconexión del Conjunto Tlalpan a finales de 1999.

Es importante mencionar que cuando se instaló la red local del Conjunto Tlalpan en 1997, se adquirió un bloque de direcciones IP homologadas ante la instancia correspondiente (ARIN, American Registry for Internet Numbers), así como un sistema autónomo, necesarios para que el IFE contará con el servicio de acceso a Internet y los usuarios de la red de redes tuvieran acceso a la información disponible a través de la página WWW del Instituto.

En el año de 1999 la red del Instituto creció de manera considerable extendiéndose a otras oficinas en el área metropolitana y a los órganos desconcentrados en toda la República Mexicana (ver tabla 1.2.1)

Oficinas Centrales y Órganos Desconcentrados conectados a RedIFE	Tipo de Enlace
Centro de Formación y Desarrollo	DS0 (64 Kbps)
Inmueble de la DERFE	DS0 (128 Kbps)
Conjunto Zafiro (DEA, DESPE y Contraloría)	E1 (1984 Kbps)
300 Juntas Distritales Ejecutivas	DS0 (64 Kbps) CIR = 32 Kbps
32 Juntas Locales Ejecutivas	DS0 (128 Kbps) CIR = 64 Kbps

Tabla 1.2.1 Oficinas Centrales y Órganos Desconcentrados conectados a RedIFE.

Para llevar a cabo tal extensión de la red fue necesario cambiar el esquema de direccionamiento y seguridad, con el fin de brindar confiabilidad y confidencialidad de la información exclusiva para el manejo interno del Instituto, así como asegurar la integridad de las diferentes bases de datos asociados a los sistemas de la Intranet. Para tal objetivo, se implementaron tecnologías como **NAT (Network Address Translation)**, Traducción o mapeo de direcciones IP, **DHCP (Dynamic Host Configuration Protocol)**, Protocolo de configuración dinámica de hosts y *Proxie Servers*; fue necesario asignar nuevas direcciones IP (direcciones especiales para redes privadas) a los equipos ya conectados. De esta manera, solo los servicios de carácter público quedaron disponibles al usuario de Internet, mientras que los servicios de Intranet solo pueden ser usados por personal del IFE. En la figura 1.2.4 se puede observar este nuevo esquema de operación de la red implementado a inicios de 1999.

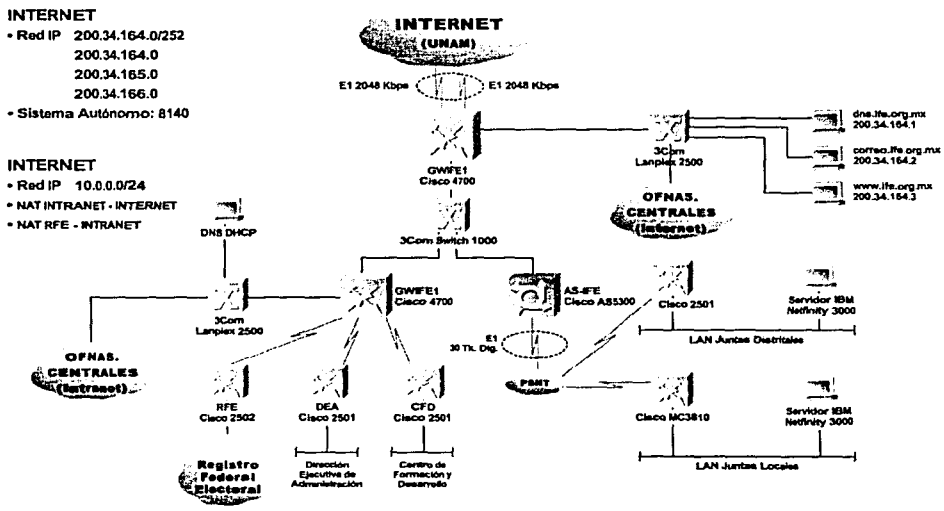


Figura 1.2.4 Diagrama de interconexión de RedIFE a Internet.

Al incorporar a las 300 Juntas Distritales Ejecutivas y 32 Juntas Locales Ejecutivas, se procuró homogeneizar los dispositivos que se utilizarían en cada una de las redes locales a instalar, esto para obtener las mayores funcionalidades que nos ofrecieran los dispositivos.

El equipo activo que se instaló en cada una de las oficinas sedes de las Juntas Ejecutivas es el siguiente:

- PC IBM Netfinity 3000 (Servidor LINUX RedHat 5.2)
- Ruteador Cisco
- Juntas Distritales: Cisco 2501
- Juntas Locales: Cisco MC3810
- Concentrador(es) 3Com
- Juntas Distritales: SuperStack II PSHUB40 (12 puertos)
- Juntas Locales: SuperStack II PSHUB40 (12 y/o 24 puertos)
- Módem de respaldo (3Com USRobotics 56k Voice Fax Modem Pro)
- UPS

En la figura 1.2.5 se muestra el diagrama general de la red local de una Junta Ejecutiva. Como se puede observar, el ruteador es el equipo activo que sirve

para interconectar la red local de la Junta con las Oficinas Centrales del Instituto a través de enlace digital a nivel WAN y un enlace de respaldo mediante una línea conmutada, para ello la necesidad de un módem externo.

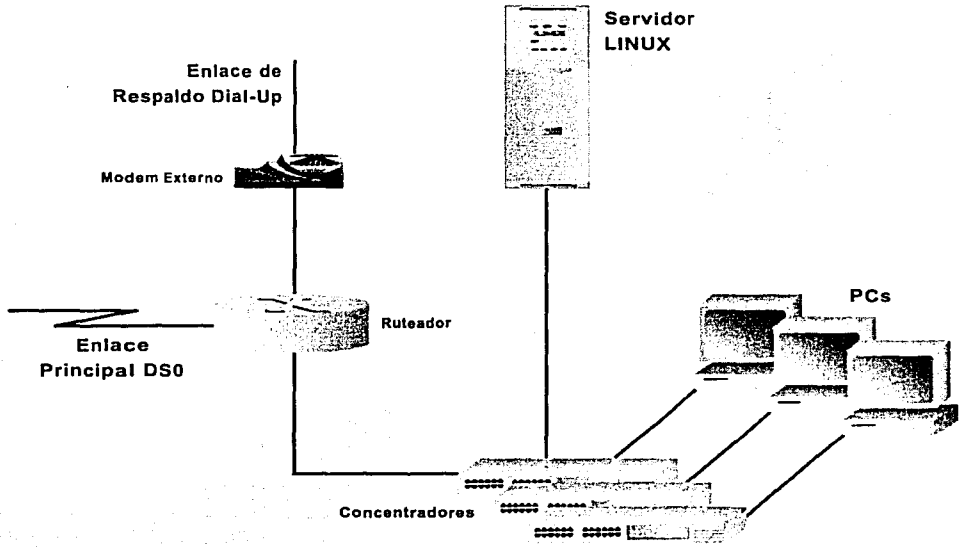


Figura 1.2.5 Diagrama de interconexión de los equipos de una Junta Ejecutiva

El personal que labora en las Juntas Ejecutivas no tiene conocimientos básicos o avanzados en el manejo de equipos de cómputo y comunicaciones para datos. Por tal motivo, la forma en que se interconectan los equipos de las redes locales de las Juntas Ejecutivas está diseñada para proporcionar al personal encargado de su operación en las Oficinas Centrales, los mecanismos necesarios para tener acceso a los equipos críticos (servidor, ruteador y concentrador) por más de una vía. En la figura 1.2.6 se puede observar que la interconexión de la línea telefónica permite utilizar los módems para tener acceso a las consolas de los equipos si por alguna razón se presenta alguna falla en el enlace digital.

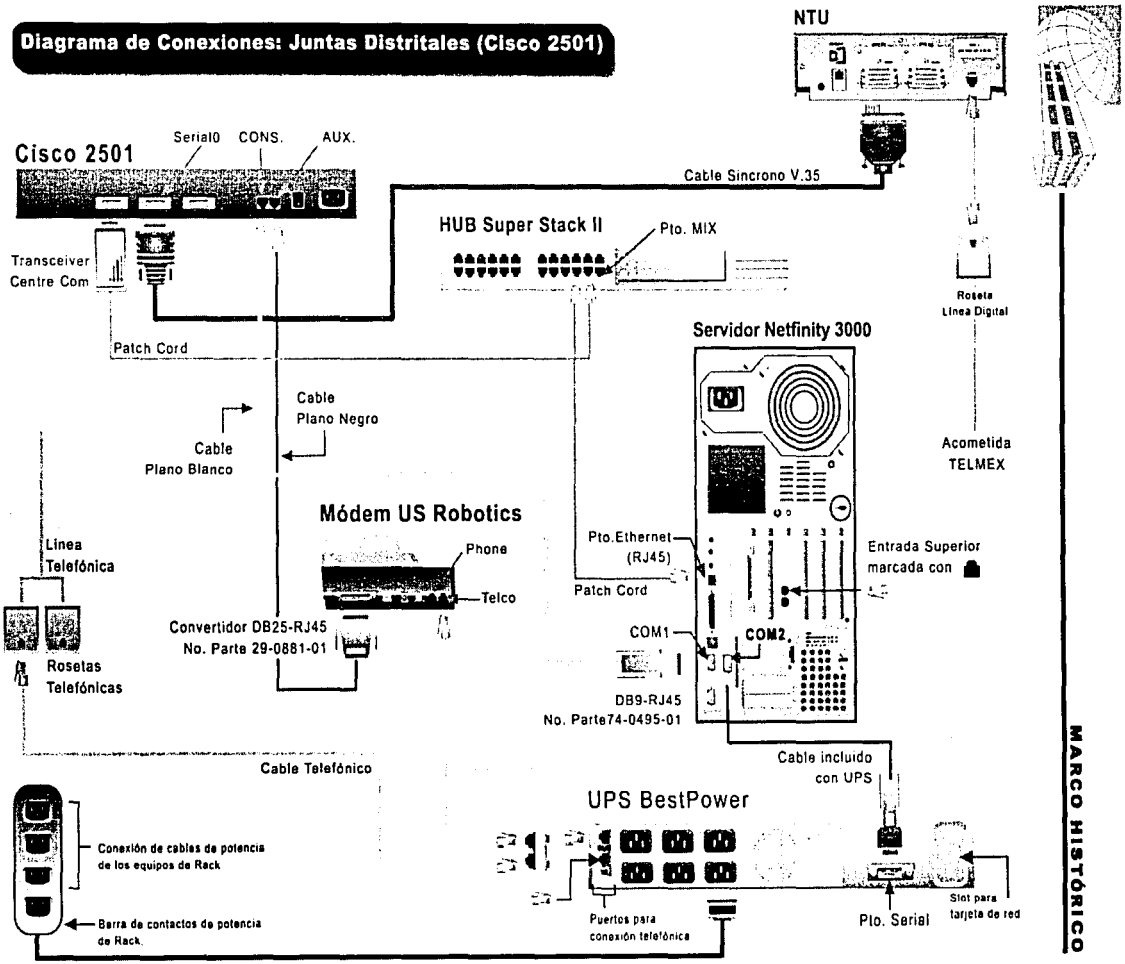


Figura 1.2.6 Esquema completo de Interconexión de los equipos en una Junta Distrital Ejecutiva.

Toda la infraestructura de red del IFE está diseñada para proporcionar al usuario dos características fundamentales: disponibilidad y confiabilidad. Los usuarios de las Juntas Ejecutivas dependen en gran medida de la organización de tipo centralizada del Instituto. En base a esta premisa, se consideró la necesidad de implementar el esquema de respaldo que se observa en la figura mencionada en el párrafo anterior.

En la figura 1.2.7 se muestra el diagrama de interconexión de la red nacional de informática con que cuenta actualmente el Instituto. En ella se puede observar los equipos de carácter crítico dentro de toda la red, desde los servidores principales hasta las redes locales de las Juntas Ejecutivas:

- Los ruteadores y equipos de red local son en su mayoría de la marca Cisco.
- Los enlaces metropolitanos son punto a punto y van desde DS0s a 64 Kbps hasta E1s con velocidades de 2048 Kbps
- Los enlaces digitales (principales) con las 332 Juntas Ejecutivas se basan en la tecnología Frame-Relay. Se interconectan en forma de estrella a equipos en Oficinas Centrales y se tiene redundancia en toda la infraestructura del proveedor: UNINET. En 324 Juntas Ejecutivas se tiene un DS0 local mediante cable de cobre desde la Central Local de TELMEX hasta el inmueble del Instituto; en las restantes 8, por problemas de ubicación geográfica, solo es posible tener el enlace mediante microondas satelitales.
- Los enlaces conmutados (respaldo) con las 332 Juntas Ejecutivas dependen de líneas conmutadas y un servidor de acceso (Cisco AS5300) con 60 módems y 60 troncales digitales.
- El servidor de acceso también permite brindar el servicio de acceso vía módem a usuarios del Instituto que requieren utilizar los servicios de RedIFE (Internet e Intranet) fuera de las instalaciones del Instituto.
- En las redes locales de las Oficinas Centrales se cuenta con switches de capa 2 y capa 3 de alto desempeño, que permiten brindar el servicio de red de forma directa a las computadoras personales y servidores mediante conexiones Ethernet, FastEthernet y GigabitEthernet.
- Los servidores y bases de datos Centrales están soportados por equipos SUN Ultra Enterprise 3000 y 3500, con sistema operativo Solaris. En algunos casos se utilizan servidores con sistema operativo LINUX.
- Los servidores y bases de datos para el mantenimiento del Sistema del Padrón Electoral están soportados por equipos de la marca IBM con sistema operativo AIX y manejadores de bases de datos Oracle.
- Los equipos de comunicaciones de la red para el mantenimiento del Sistema del Padrón Electoral son principalmente ruteadores Cisco y Switches WAN de la misma marca.

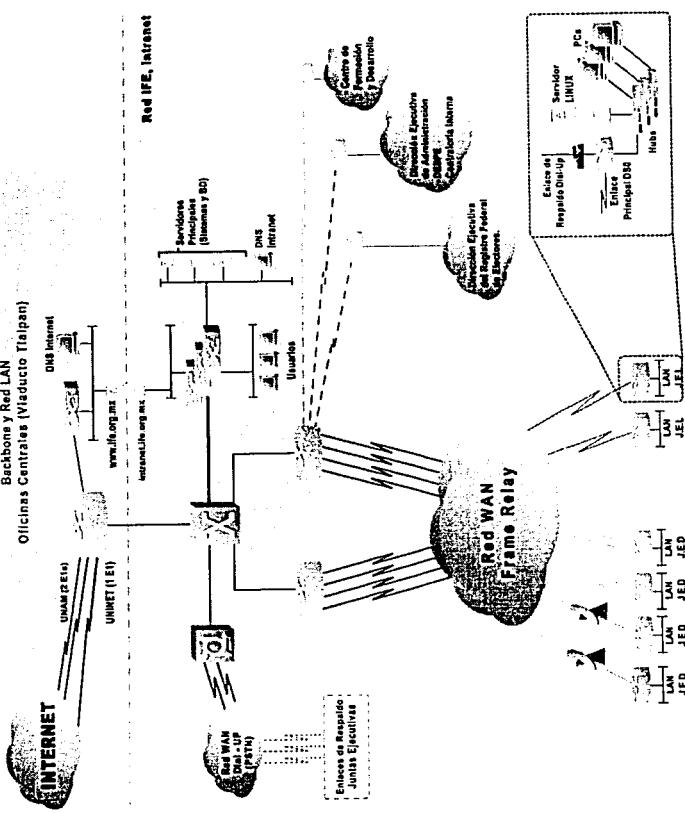


Figura1.2.7 Infraestructura de la Red Nacional de Informática del IFE.

1.3 SERVICIOS PROPORCIONADOS A TRAVÉS DE LA RED NACIONAL DE INFORMÁTICA DEL INSTITUTO

El Instituto Federal Electoral proporciona una serie de servicios, algunos de ellos de manera permanente y algunos otros únicamente durante el proceso electoral. Dentro de los servicios permanentes se encuentran los siguientes:

1.3.1 Servicios de Internet

Aproximadamente el 60% del personal del Instituto tiene acceso a estos servicios, al igual que a los servicios de Intranet. A continuación se describe cada uno de ellos.

Correo Electrónico. Este se encuentra distribuido, se tiene un servidor Unix en cada Junta Ejecutiva, que alberga las cuentas del personal de cada una de ellas, lo que les permite enviar y recibir correo de Internet e Intranet, este último sobre todo para comunicarse entre la Junta Local y sus Juntas Distritales. Y otro en Oficinas Centrales con las cuentas del personal de dichas oficinas, permitiéndoles de igual forma mantenerse en comunicación dentro y fuera de la redIFE mediante este servicio.

Para proporcionar un servicio eficiente y seguro el acceso se realiza a través del web, https://correo.ife.org.mx, el cual utiliza una herramienta que hace que los datos viajen de manera encriptada. Aunque la mayoría de los usuarios utilizan el web, también se tiene acceso mediante los protocolos **Post Office Protocol (POP, Protocolo de Oficina Postal)** e **Internet Message Access Protocol (IMAP, Protocolo de Acceso de Mensajes en Internet.**

World Wide Web (WWW, Red mundial de datos). El Instituto cuenta con una página de web que sin lugar a dudas, es el servicio más demandado por los ciudadanos durante el proceso electoral, la dirección para accesar es http://www.ife.org.mx, en donde se encuentra información acerca de la ubicación de los módulos de registro para obtener la credencial de elector, de las funciones del Instituto, estructura orgánica, partidos políticos, resultados electorales, distritos electorales, calendario electoral, legislación, comunicados de prensa, Registro Federal de Electores, etc.

Acceso vía módem. Recientemente se implantó este servicio para uso exclusivo del personal del Instituto, se proporciona a través del servidor de acceso que se utiliza para la comunicación de respaldo a las Juntas

Ejecutivas,que como se había mencionado anteriormente, cuenta con 60 módems que están respondiendo a las peticiones de los usuarios. Inicialmente se está proporcionando este servicio a los altos funcionarios, se planea ir ofreciéndolo por niveles, y de ser posible poder ofrecerlo a todo el personal con la debida autorización de su jefe superior; esto dependerá del uso que se le dé y de la capacidad del equipo de acceso.

A cada usuario se le asigna una cuenta y un **password** (contraseña), que se autentica con el protocolo **Terminal Access Controler Access Control System** (TACACS, Sistema de Control de Acceso / Controlador de Acceso de Terminales).

1.3.2 Servicios de Intranet

A estos servicios se tiene acceso únicamente desde RedIFE; no es posible tener acceso desde ningún lugar de Internet, ya que contienen información confidencial.

WWW. Se cuenta también con una página de Intranet con información del Consejo General, de la Junta General Ejecutiva, Secretaría Ejecutiva, Dirección Ejecutiva del Registro Federal Electoral, Dirección Ejecutiva de Capacitación Electoral y Educación Cívica, Dirección Ejecutiva de Organización Electoral, Dirección Ejecutiva de Administración, Dirección Ejecutiva del Servicio Profesional Electoral y Dirección Ejecutiva de Prerrogativas y Partidos Políticos, así como un directorio de correos electrónicos del personal del Instituto.

Adicionalmente cada Junta Ejecutiva tiene su propia página que contiene ligas a las páginas de Internet e Intranet antes mencionadas, y a los servicios y sistemas de acceso local; así como a la página de correo; información acerca del proceso electoral; manuales de los sistemas y del correo electrónico; estadísticas del padrón electoral y la lista nominal. Se le da mantenimiento a la información desde oficinas centrales, para lo que es necesaria la transferencia de archivos a través de la red, y sobre todo, permite el acceso a éste desde cualquier parte de redIFE.

Compartir recursos. Entre ellos, permite compartir archivos entre el personal y dispositivos de *hardware* a través de la red interna, como son impresoras y scanners.

Audio y video. Este es otro de los servicios recientes, por el momento solo las sesiones de consejo se pueden ver y escuchar mediante la red. Este servicio se planea crecer para incrementar y agilizar la comunicación entre el personal del Instituto.

1.3.3 Sistema de Actualización del Padrón

Mantenimiento del sistema de actualización del Padrón Electoral. Actualmente hay una gran cantidad de módulos para obtener y actualizar las credenciales de elector, estos no se encuentran conectados a red, por lo que hay personas que se encargan de llevar los datos para las credenciales a alguno de los 17 centros de acopio, una vez que están listas, se llevan al módulo correspondiente, este proceso se lleva 34 días aproximadamente.

Se pretende agilizar esto, instalando los módulos en las Juntas Distritales Ejecutivas, además de tener algunos semifijos y móviles, y que todos cuenten con conexión a red para que la fotografía, huella y firma digitalizados así como los datos del ciudadano sean enviados automáticamente al centro de acopio que le corresponde.

1.3.4 Uso de Sistemas en Red

Para el adecuado funcionamiento y control de las actividades desarrolladas por el Instituto, se desarrollaron una serie de sistemas que se ejecutan exclusivamente a través del servicio web.

Hay dos tipos de sistemas, los que son de uso permanente y los que funcionan únicamente durante el proceso electoral.

- **Sistemas de uso permanente**

- Administración de recursos. La Dirección de Informática Administrativa (DIA) con apoyo en el sistema SIAR (Sistema de Información de Administración de Recursos) lleva el control de recursos materiales, costos, nómina, etc., este sistema utiliza un manejador de bases de datos llamado Clipper, y los datos viajan a través de una red novell. Se pretende que estos viajen por la red del Instituto y sean administrados con un sistema más robusto.

- Sesiones de Consejo y Junta Ejecutiva. Este tiene la finalidad de que las Juntas Ejecutivas realicen la integración de bases de datos de las sesiones que lleve acabo cada consejo electoral, registrando a los

consejeros acreditados y a los representantes de cada partido político para participar en el consejo, en la fecha establecida y con información correcta; generando durante el proceso reportes de avances en los catálogos de registros de consejeros, así como la formación de los mismos por parte de las Juntas Distritales de cada estado. Con este sistema se busca dar seguimiento correcto y puntual a las actividades propias de las Vocalías de Organización Electoral Locales y Distritales de las 32 entidades federativas en la integración de las casillas en el Proceso Electoral.

- **Sistemas que se utilizan únicamente durante el proceso electoral**

- **Observadores Electorales.** Tiene como finalidad que las Juntas Ejecutivas realicen la integración de bases de datos de las organizaciones civiles y personas (nacionales o extranjeras) que deseen fungir como observadores del proceso electoral.

Con este se busca dar seguimiento correcto y puntual a las actividades propias de las Vocalías de Organización Electoral Ejecutivas Locales y Distritales de las 32 entidades federativas en la integración de identificación y acreditación de los ciudadanos que fungirán como observadores.

Para esto es necesario que la Juntas Ejecutivas capturen durante el proceso de Acreditación de Observadores Electorales en los Consejos Locales y Distritales, la información que manejan y reportan a Oficinas Centrales; a fin de llevar un control eficiente.

La información se concentra en servidores locales ubicados en cada una de las Juntas para después centralizarse en un servidor en Oficinas Centrales donde se almacena en una base de datos.

Se cuenta con otro sistema que proporciona a los Consejeros una fuente de consulta sobre los trabajos que se realizan en las Juntas Distritales y Locales Ejecutivas en el proceso de Acreditación de Observadores Electorales en los Consejos Distritales. Esto con el fin de llevar un control oportuno y eficiente.

Así mismo, facilitará el reporte de esta información a Oficinas Centrales toda vez que el sistema permite la generación automática de archivos y reportes predefinidos.

• **Registro de Candidatos. Este consta de dos versiones.**

- **Versión para Juntas Distritales.** Permite a las Juntas Distritales Ejecutivas, capturar la información requerida durante el proceso de registro de candidatos que soliciten los partidos políticos ante el Consejo Distrital, a fin de elaborar las listas que se presentarán ante el citado órgano colegiado de dirección, para su respectiva aprobación.

- **Versión para Oficinas Centrales.** Permite a la Dirección Ejecutiva de Prerrogativas y Partidos Políticos capturar la información requerida durante el proceso de registro de candidatos que soliciten los partidos políticos o las coaliciones ante el Consejo General, a fin de elaborar las listas que se presentan ante el citado órgano colegiado de dirección, para su respectiva aprobación.

• **Funcionarios de Casilla. Consta de dos versiones.**

- **Versión para Juntas Ejecutivas.** Su objetivo es facilitar y simplificar la captura y procesamiento de la información relativa a la notificación, capacitación, acreditación y designación de los ciudadanos que integran las mesas directivas de casilla, en la fecha establecida y con la información correcta; generando durante el proceso de selección mediante la primera insaculación, reportes diarios de ciudadanos notificados y capacitados; los listados de ciudadanos acreditados para participar en la segunda insaculación y el de funcionarios de casilla; así como los nombramientos, encartes (listado definitivo de las mesas directivas de casilla) y sustituciones.Cada distrito electoral tiene como responsable del sistema a los Vocales Distritales de Capacitación Electoral y Educación Cívica así como un capturista que vacía la información en la base de datos.

Consta de dos etapas que se llevan a cabo en una fecha en particular cada una, la cual se publica en el COFIPE:

Primera Insaculación. Es la selección del 10% (mínimo 50) de los ciudadanos que integran las listas nominales de electores. Almacena la lista nominal, lleva acabo el proceso de selección de ciudadanos, imprime las cartas de notificación a los ciudadanos insaculados, genera reportes del resultado de ésta y el listado de ciudadanos insaculados.

Segunda Insaculación. Se seleccionan los funcionarios de casilla del total de ciudadanos acreditados sobre la base de una letra previamente seleccionada y de ahí los que tengan mayor escolaridad serán elegidos para los distintos cargos de la mesa directiva de cada casilla.

Versión para Oficinas Centrales. Mediante éste se lleva el control de información referente a los funcionarios de casillas por cada una de las juntas distritales, locales y un concentrado nacional. Cabe hacer mención que este sistema solo es de consulta tanto nacional como estatal, por lo que su función es la de mostrar la información generada en todo el país por el sistema de Funcionarios de Casillas Distritales.

• Ubicación de casillas. Consta de dos versiones.

- Versión para Juntas Ejecutivas. Este sistema tiene como propósito apoyar a las Juntas Distritales Ejecutivas en los trabajos de registro y sistematización de información para la integración de las propuestas de Ubicación de Casillas, las visitas de examinación a los lugares propuestos, la aprobación de éstos, los medios de comunicación y transporte para acceder a las casillas, los materiales que requieren para su acondicionamiento y las rutas electorales, entre otros aspectos.

Así mismo, facilitará el reporte de esta información a Oficinas Centrales toda vez que el Sistema permite la generación automática de reportes predefinidos.

- Versión para Oficinas Centrales. Mediante este sistema es posible llevar a cabo el control de información referente a la ubicación de casillas por cada una de las Juntas Distritales, Locales y un concentrado nacional. Cabe mencionar que este sistema solo es de consulta, tanto nacional como estatal, por lo que su función es mostrar la información generada en todo el país por el sistema de Ubicación de Casillas Distritales.

• Representantes de Partidos Políticos.

Tiene la finalidad de que las Juntas Locales y Distritales realicen la integración de bases de datos, registrando a las personas acreditadas para fungir como representantes de cada partido político en la jornada electoral ante los funcionarios de casilla y se les permita observar el desarrollo de las votaciones, en la fecha establecida y con información correcta; generando durante el proceso reportes de avances en los catálogos de registros por parte de las Juntas Distritales de cada estado.

Con éste se busca dar seguimiento correcto y puntual a las actividades propias de las Vocalías de Organización Electoral Locales y Distritales de las 32 entidades federativas en la integración de la casilla en el Proceso Electoral.

• **Materiales y Productos Electorales. Se tienen dos versiones.**

- **Versión para Juntas Locales y Distritales.** Tiene el propósito de llevar el registro de la recepción de la documentación y los materiales electorales enviados por las Juntas Locales a los Consejos Distritales y que son necesarios para la instalación de casillas. Así mismo el Sistema permite registrar el envío de los paquetes electorales que deben ser entregados a los Presidentes de las Mesas Directivas de Casilla en vista a las elecciones que se estén llevando a cabo; generando durante el proceso reportes de avances en las recepciones y envíos por parte de las Juntas Locales de cada estado a sus diferentes Juntas Distritales.

Con este sistema se buscó dar seguimiento correcto y puntual a las actividades propias de las Vocalías de Organización Electoral Locales y Distritales de las 32 entidades federativas en la integración de la casilla en el Proceso Electoral.

- **Versión para Oficinas Centrales.** Por medio de éste, se lleva el control de información referente a la entrega de materiales y productos electorales que se utilizan en la jornada electoral por cada una de las juntas distritales, locales y un concentrado nacional. Cabe mencionar que este sistema solo es de consulta, tanto nacional como estatal, por lo que su función es mostrar la información generada en todo el país del sistema de materiales y productos electorales Distritales y Locales.

• **Sistema de Información de la Jornada Electoral.**

En este se captura la información sobre la instalación de casillas, los ciudadanos que fungen como Presidente, Secretario y Escrutadores en éstas, así como la presencia de los representantes de los partidos políticos ante las propias casillas que los Asistentes Electorales reporten a sus respectivos supervisores en las Juntas Distritales Ejecutivas al hacer los recorridos de su ruta electoral durante el desarrollo de la Jornada Electoral.

Así mismo, se captura la información de los reportes sobre los incidentes que llegaran a suscitarse durante la Jornada Electoral, que los Asistentes Electorales comunicarán a los encargados en los Consejos Distritales. De esta forma, el sistema permite mantener informados con oportunidad a los Consejos Locales, al Consejo General y a las diferentes áreas de Oficinas Centrales sobre los aspectos que se han referido del desarrollo de la Jornada Electoral.

Con éste se busca dar seguimiento correcto y puntual a las actividades propias de la Dirección de Organización Electoral de las 32 entidades federativas.

- **Cómputos.**

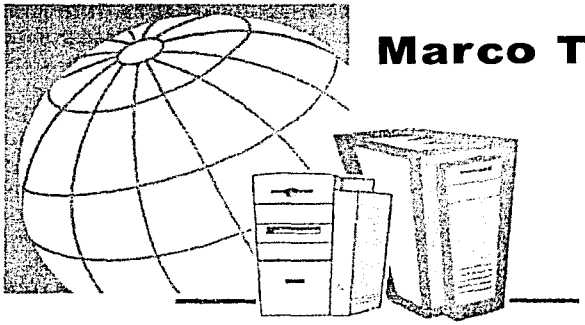
Tiene la finalidad de que las Juntas Locales y Distritales, así como Oficinas Centrales realicen los cómputos de los votos recopilados en las juntas de toda la república en donde se lleve acabo la elección de los candidatos aspirantes a los puestos de Presidente de la República, Senadores y Diputados; integrados en los catálogos de registros de cada elección.

Con éste se busca dar seguimiento correcto y puntual a las actividades propias de la Dirección de Organización Electoral de las 32 entidades federativas en la información de las candidaturas en el Proceso Electoral.

Estos son los sistemas que funcionaron en las últimas elecciones federales, sin embargo se está planeando crear algunos otros sistemas que automaticen más este proceso. Para lo cual es necesario contar con una infraestructura lo suficientemente robusta y con una buena administración para poder proporcionar estos servicios eficientemente a las áreas pertinentes.

Actualmente la administración de la red se realiza con apoyo en programas sencillos e independientes desarrollados por personal del área de comunicaciones, además de algunas tareas que se realizan de forma manual a falta de las herramientas de *software* necesarias. Es por ello el desarrollo de este trabajo.

CAPITULO II



Marco Teórico

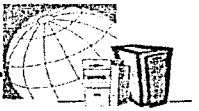
2.1 ARQUITECTURA CLIENTE-SERVIDOR

2.1.1. Definiciones

El término cliente-servidor fue utilizado por primera vez en la década de los ochentas haciendo referencia a las **PCs** (Computadoras Personales) dentro de una red. La arquitectura del *software* (La parte conceptual de la computación, los programas) cliente-servidor se refiere a una infraestructura modular versátil, basada en mensajes que pretende mejorar la flexibilidad, interoperabilidad y escalabilidad del esquema tradicional que es centralizado en la computación de tiempo compartido utilizado en las *mainframes*.

Hoy en día el término cliente-servidor tiene un significado muy específico que no tiene nada que ver con el *hardware* (La parte de la computación que es tangible). Aún así, algunas personas probablemente todavía siguen asociando el término cliente con la máquina (computadora) que tienen en su escritorio y el término servidor con alguna otra, a la cual estén conectados.

El punto clave para entender el concepto de cliente-servidor se encuentra en el aceptar que es un concepto lógico. El cliente y el servidor no necesariamente deben residir en *hardware* diferente. La tecnología del cliente-servidor es un modelo para la interacción entre procesos de *software* que se ejecutan de manera concurrente. Es importante entender que la relación entre el cliente y el servidor es una relación de comando o control. En cualquier intercambio el cliente inicia la petición y el servidor responde a ésta de la manera adecuada. El servidor jamás puede iniciar la conversación con el cliente. La interacción entre el cliente y el servidor es cooperativa, un intercambio transaccional en el cual el cliente es proactivo y el servidor es reactivo.



En términos generales un cliente puede definirse como el que hace las peticiones de servicio y el servidor como aquel quien es el proveedor de servicios.

En una máquina en particular pueden existir ambos procesos, el cliente y el servidor, dependiendo de la configuración de *software* que se esté utilizando. Aún más relevante resulta el hecho de que en la misma máquina se pueden estar ejecutando procesos paralelos y diferentes en donde alguno de ellos esta sirviendo a peticiones de clientes (servidor) y otro que esta requiriendo los servicios de algún otro proceso (cliente).

Bajo un esquema ideal para ambos procesos, cliente y servidor, resulta indiferente el hecho de que corran en la misma máquina o en máquinas diferentes. Algunos procesos de intercomunicación o protocolos de red pueden no soportar que el cliente y el servidor corran en el mismo sistema. Sin embargo, esa es una restricción del protocolo y no una característica de la arquitectura cliente-servidor. Desde una perspectiva teórica, la capacidad del *hardware* tampoco importa, la simplicidad del modelo es lo que lo hace tan poderoso.

De acuerdo a la definición de la arquitectura cliente-servidor es fácil distinguir sus componentes separándolos de la siguiente manera:

- **Cliente.** El cliente actúa como el punto de entrada para el usuario. Para ser cliente, una estación de trabajo debe tener la capacidad de poder hacer las peticiones de recursos que necesitará. En el modelo cliente-servidor, el cliente utiliza los servicios que son provistos por uno o más servidores. Es la parte proactiva de la relación ya que emite las peticiones y recibe las respuestas. Un cliente es una entidad dedicada a un usuario ya que comienza a funcionar cuando un cliente comienza su sesión y termina cuando el usuario decide finalizarla. Como se había comentado anteriormente una estación de trabajo puede operar como cliente mientras esté sirviendo también como servidor para otros procesos. Un buen ejemplo puede mencionarse en los ambientes de las **LANs** (Redes de Área Local) en donde una estación esté ejecutando procesos cliente para algún usuario y a la vez esté corriendo el proceso de servidor de impresión que responde a las peticiones de otros usuarios. En caso de los procesos distribuidos tanto los tipos de máquinas como los protocolos de comunicación resultan ser transparentes para el usuario, generándose así la ilusión de que la aplicación completa se está ejecutando de manera local sin necesidad de otros procesos, máquinas o redes.

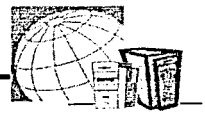
• **Servidor.** Un servidor realiza operaciones específicas para cualquier otro proceso que está requiriendo de sus servicios. El proceso del servidor es reactivo debido a que se activa basándose en las peticiones de los clientes. Se debe mantener siempre en ejecución y provee servicios a muchos clientes. El servidor ejecuta las transacciones requeridas y no interactúa con ningún otro servidor. La actividad fundamental de un servidor es soportar múltiples y simultáneas peticiones de los clientes. De esta manera, el servidor deberá ser capaz de soportar ***multitasking*** (Multitarea) y poder también hacer uso de la memoria compartida.

• **Red.** La esencia de la arquitectura cliente-servidor es la conectividad en un ambiente en donde convivan múltiples productos de múltiples fabricantes. Una red conecta estaciones de trabajo con recursos comunes y es un sistema dentro del cual se transmite la información. Las redes pueden clasificarse desde diferentes perspectivas. De acuerdo a su extensión geográfica, de acuerdo a las aplicaciones que se corren sobre ellas, de acuerdo a su topología, etc. Para la arquitectura cliente-servidor, el tipo de red sobre la cual se transmite la información no importa, siempre y cuando exista una comunicación entre las estaciones de trabajo que están ejecutando procesos clientes y/o servidores.

• **Aplicaciones.** El *software* es lo que une a los anteriores tres componentes y los hace funcionar a manera de sistema. La característica que distingue a la tecnología cliente-servidor de otras es que cuenta con capacidades cooperativas de procesamiento, que dividen de forma física el procesamiento que se realiza en el cliente y el que se realiza en el servidor, mientras que presentan una única representación lógica hacia el usuario.

2.1.2 Características

Un sistema cliente-servidor es aquel en el cual uno o más clientes y uno o más servidores, utilizando un sistema operativo y procesos de intercomunicación, forman un sistema compuesto permitiendo que se lleve a cabo la computación distribuida, el análisis y la presentación de resultados. Los clientes pueden correr en sistemas operativos heterogéneos y diferentes tipos de redes para hacer sus peticiones hacia los servidores. El servidor tiene control sobre los datos; sin embargo, algunos clientes pueden contener datos privados que residen en la estación de trabajo en donde se están ejecutando. Las características más notables de esta arquitectura incluyen al hecho de poder separar de manera lógica los procesos del cliente y los del



servidor, la habilidad de cambiar un servidor sin afectar a los clientes y la habilidad de cambiar un cliente sin afectar al servidor o a otros clientes. Otras características de la arquitectura cliente-servidor son las que a continuación se mencionan.

- El servidor es pasivo. Él no inicia las conversaciones con los clientes, aunque puede actuar como cliente para otros servicios.
- Espera y acepta peticiones.
- Presenta una interfaz abstracta y definida al cliente.
- Mantiene la independencia en la localización y la transparencia de la interfaz del cliente.

El cliente es una entidad que realiza peticiones de información. Sus funciones típicas son:

- Despliega la interfaz de usuario.
- Realiza tareas básicas de edición de datos de entrada.
- Construye las peticiones para ser enviadas al servidor.
- Se comunica con el servidor.
- Amolda las respuestas del servidor para su presentación.

La arquitectura cliente-servidor no es dependiente del *hardware*, ni es considerada como un solo producto. Cualquier cambio de configuración en *hardware/software* en el servidor debe ser transparente para el cliente.

2.1.3 Tipos de arquitecturas cliente-servidor

La mayoría de los programas de aplicación a su vez cuentan con 3 capas principalmente. La capa superior es la de presentación, que provee los medios para la interacción entre el humano y la máquina, es la interfaz del usuario. La capa de presentación se ocupa de la entrada del teclado, **mouse** (ratón) u otros dispositivos y la forma en que se despliega la información en el monitor del usuario. La capa intermedia está formada por la lógica de la aplicación o la lógica de la tarea, es decir la funcionalidad que le da su carácter al programa. La lógica de la aplicación es regularmente llamada así porque contiene las reglas que regirán la forma de comportamiento de cierto programa. Las reglas van a ser diferentes para un sistema de manejo de inventarios comparado con un sistema de administración de redes de datos, por ejemplo. La capa inferior provee servicios generalizados que necesitan las capas superiores, incluyendo servicios de transferencia de archivos, servicios de impresión, servicios de comunicación y tal vez más importante aún, servicios de bases de datos.

Por simplicidad, enfocaremos nuestro estudio hacia aquellos programas que necesitan de los servidores de bases de datos.

El número de capas en una arquitectura cliente-servidor se determina de acuerdo a qué tan ajustadas u holgadas estén las 3 capas en su nivel de integración.

Aplicaciones *one-tier* (de una capa)

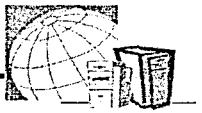
Una aplicación *one-tier* es aquella en la cual las 3 capas de la aplicación están plenamente integradas. En particular, la capa de presentación tiene información detallada de la estructura de la base de datos. La capa de aplicación esta comúnmente entrelazada con la capa de presentación y la de servicios. Las tres capas, incluyendo el motor de la base de datos, casi siempre se están ejecutando en la misma computadora.

Las aplicaciones *one-tier* son fáciles de diseñar y programar, especialmente hoy con todas las herramientas de programación que existen en el mercado. Es también posible crear aplicaciones multiusuario *one-tier* corriendo la aplicación en múltiples PCs y haciendo que éstas compartan una misma base de datos. La base de datos puede ser almacenada ya sea en una de las PCs o dentro de un servidor de archivos. Hay que hacer notar que cada PC que corre la aplicación tiene su propia copia del motor de la base de datos; solo los datos son compartidos, no así la lógica propia de la base de datos.

Las aplicaciones *one-tier* funcionan bien hasta que el número de usuarios se incrementa considerablemente. El problema es que todo el trabajo de las bases de datos se realiza en el cliente. Por ejemplo, si el programa necesita listar todos los clientes que tengan el apellido Rodríguez, toda la información –índices y registros- necesarios para resolver ese **query** (petición de base de datos) debe ser transferida sobre la red. Para algunos *querys* complejos, una cantidad considerable de datos tiene que ser examinada, incluso puede ser que se tenga que examinar todo el contenido de la base de datos. En un nivel más técnico, es difícil manejar motores de bases de datos de manera independiente y asegurarse de que no se vaya a presentar un conflicto cuando dos clientes traten de acceder o modificar el mismo registro.

Aplicaciones *two-tier* (de dos capas)

La solución a los problemas técnicos y de **performance** (desempeño) asociados a las aplicaciones *one-tier* multiusuario son las aplicaciones de arquitectura *two-tier*. Este tipo de aplicaciones son escritas de manera muy similar a las *one-tier*, con la excepción de que el motor de la base de datos no corre en el cliente, sino en el servidor que es el que contiene también la base



de datos. Existe aquí un método que comunica la capa lógica de la aplicación y los servicios de la base de datos.

Hoy en día, el método más utilizado es el **Structured *Query* Language SQL** (Lenguaje estructurado de peticiones), un lenguaje que puede encapsular complejos *querys* en sentencias relativamente compactas. La sentencia de SQL es enviada al servidor de bases de datos, el cual realiza el trabajo de forma local y regresa al cliente solo la información relevante (la respuesta). En las aplicaciones *two-tier*, solo los servicios de bases de datos están separados. La presentación y la lógica de la aplicación permanecen muy entrelazadas y ambas continúan teniendo información específica del diseño de la base de datos.

Las aplicaciones *two-tier* son un poco más complejas de programar comparadas con las *one-tier*, sin embargo muchas de las herramientas de desarrollo vienen equipadas con un gran soporte en sus ambientes de desarrollo para ofrecernos una forma rápida de programación. Estas herramientas son tan buenas que las aplicaciones *two-tier* pueden ser programadas casi tan rápido como las *one-tier*. La única desventaja es el costo. La mayoría de ellas proveen motores de bases de datos que sólo pueden manejar diseños *one-tier* (tal como el «Jet engine», usado en Access y Visual Basic), pero las aplicaciones *two-tier* requieren de productos de bases de datos separados tales como Oracle, IBM DB2, Sybase o Microsoft SQL Server.

Aplicaciones *three-tier* (de tres capas)

Las aplicaciones *three-tier* separan todas las capas de la aplicación en secciones independientes. En diseños *three-tier*, la lógica de la aplicación se convierte en un servicio y ese servicio puede correr en una máquina diferente. A esto se le llama comúnmente **application server** o simplemente ***app server*** (Servidor de aplicación).

En muchas ocasiones el *app server* corre en la misma máquina física de la base de datos. Sin embargo la ventaja principal es que el *app server* puede ser colocado en donde más convenga de acuerdo a los servicios que va a proporcionar. Por ejemplo, si estamos hablando de un sistema de ventas regionales, algunas regiones pueden tener muchos vendedores compartiendo un solo *app server* que está corriendo en una máquina dedicada. Sin embargo algún vendedor en una región remota puede correr tanto el cliente como el *app server* en su propia PC. No importa como estén configurados el cliente y el *app server*, todos los *app servers* pueden recibir servicios de bases de datos desde un sitio centralizado que puede ser incluso un mainframe. Y tampoco importa como sean distribuidos, todos los usuarios operarán la

aplicación de la misma manera desde cualquier cliente. La localización del *app server* y de la base de datos son irrelevantes para el usuario.

En las aplicaciones *three-tier*, la capa de presentación usualmente no tiene conocimiento del diseño de la base de datos. En lugar de esto, la capa de presentación se comunica con su *app server* utilizando una estrategia predefinida de mensajes.

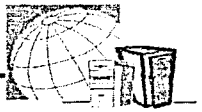
La mejor forma de entender esto es pensar en el «Web». Nuestro **browser** (navegador de Internet) no sabe absolutamente nada acerca de la estructura de la base de datos de «amazon.com», por ejemplo, pero de cualquier forma uno es capaz de interactuar con la base de datos cuando se está ordenando un libro. Este es el resultado de un protocolo bien definido de Internet que le permite al cliente (el browser) comunicarse con el *app server* (Web server). Aquí también se puede ordenar un libro desde cualquier PC, no solamente desde una en específico, lo único que necesitamos es un browser que pueda interpretar la programación de las páginas de web con las que se va a interactuar (en este caso, páginas con formas a llenar).

Las aplicaciones *three-tier* son más difíciles de construir. El mayor obstáculo es que los ambientes de desarrollo de aplicaciones no están diseñados para desarrollar diseños *three-tier* como lo están para diseños *two-tier*. Como resultado, se requiere escribir más código a mano al estar desarrollando aplicaciones *three-tier*. Estas aplicaciones también son difíciles de diseñar, porque son más abstractas que las *two-tier*. Los desarrolladores de *software* están apenas sacando versiones que puedan soportar diseños *three-tier* o ***n-tier*** (de n capas), pero hasta el momento el desarrollo de éstas no es del todo maduro.

Un punto de interés es que en diseños *three-tier* existe una relación entre el *app server* y el servidor de base de datos. En otras palabras, aunque el cliente en un diseño *three-tier* no tiene conocimiento del diseño de la base de datos, el *app server* sí.

El término *n-tier* es un término de moda. La verdad es que los diseños cuentan con un máximo de 3 capas; *n-tier* se refiere al hecho de que el *app server* puede solicitar servicios de muchos otros servicios, y esos servicios pueden a su vez necesitar de otros servicios para responder de manera apropiada a la solicitud original del cliente. Esto se puede comparar con la programación anidada de subrutinas en un programa.

Middleware es un término que a menudo es usado para describir la lógica de la aplicación que existe en el *app server*. Desgraciadamente, el mismo término también es utilizado para describir servicios genéricos. Por ejemplo, para



comunicarse, los diseños *three-tier* necesitarán un sistema definido de mensajes. Este es el verdadero *middleware* en el sentido de que funciona entre, o a la mitad, de las tres capas. Durante este estudio la definición de *middleware* será precisamente la que se describió en el ejemplo.

Por otro lado, si existe muy poca lógica de la aplicación o bien ninguna en el cliente, significando esto que se trata exclusivamente de la capa de presentación entonces se dice que se trata de un **thin-client** (cliente delgado). Si el cliente conoce mucho de la lógica de la aplicación, entonces se dice que es un **fat-client** (cliente gordo). El mejor ejemplo de un *thin-client* es nuestro web browser. Es tan delgado que puede conectarse hacia aplicaciones completamente diferentes de las cuales no conoce absolutamente nada y solo sabe como hacer la representación gráfica de los resultados.

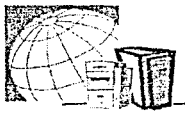
2.1.4 Paradigmas de comunicación

Las arquitecturas cliente-servidor proveen el **framework** (estructura) necesario que permite a muchas tecnologías incorporar diferentes aplicaciones. Los clientes y los servidores típicamente se comunican entre sí utilizando alguno de los siguientes paradigmas:

- **Remote Procedure Call RPC (Llamada de procedimiento remoto).** En este paradigma, el cliente invoca a un procedimiento remoto (el proceso servidor), el procedimiento remoto se ejecuta y envía de regreso la respuesta al cliente. El procedimiento remoto puede ser tan simple como regresar la hora del día o tan complejo como regresar todos los compradores del área de Monterrey que cuentan con un buen historial crediticio y son además varones. Cada par de petición/respuesta en un RPC es tratado como una unidad de trabajo independiente, así, cada petición deberá contener suficiente información para que el servidor la pueda procesar.

- **Remote Data Access RDA (Acceso de datos remoto).** Este paradigma permite al cliente y/o a las herramientas del usuario final generar peticiones remotas, que son regularmente *queries* de SQL, hacia bases de datos localizadas en sitios remotos. La diferencia fundamental entre el RDA y los RPC se basa en que el tamaño del resultado en RDA es desconocido porque el resultado de un *query* SQL puede ser un renglón o miles de renglones. RDA actualmente es ampliamente soportado por los desarrolladores de bases de datos.

- **Queued Message Processing QMP (Proceso de mensajes encolados).** En este paradigma, el mensaje del cliente es almacenado en una cola y el servidor lo procesa de manera local cuando se



encuentra desocupado. El servidor almacena la respuesta en otra cola y el cliente activamente recibe las respuestas desde esta cola. Este modelo, usado en muchos sistemas de procesamiento de transacciones, permite a los clientes enviar de manera asíncrona las peticiones al servidor. Una vez que la petición es encolada, la petición es procesada aunque el que la envió esté desconectado (intencionalmente o debido a alguna falla). QMP actualmente está comenzando a ser soportado ampliamente.

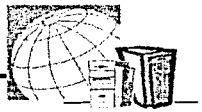
2.1.5 Ventajas de la arquitectura cliente-servidor

La arquitectura cliente-servidor es un sistema abierto. Ofrece a las organizaciones la habilidad de distribuir el procesamiento y los datos a lo largo de la infraestructura de red usando poderosas estaciones de trabajo gráficas, servidores, y mainframes. El modelo cliente-servidor permite escoger de manera correcta el tamaño de las máquinas a utilizar, la selección y localización de los recursos de cómputo de acuerdo a las necesidades de los individuos o grupos de trabajo. Uno de los beneficios primarios de los sistemas cliente-servidor son los bajos costos. Otra más es el incremento de la productividad del individuo hacia la corporación que resulta del mejor acceso a la información y la distribución de los recursos a través de la corporación. Beneficios adicionales de la arquitectura son las siguientes:

- Interoperabilidad. La red, el cliente y el servidor trabajan de manera conjunta.
- Escalabilidad. Cualquiera de los elementos fundamentales puede ser reemplazado cuando las necesidades así lo requieran, sin impactar en mayor medida a los demás elementos.
- Adaptabilidad. Las nuevas tecnologías pueden irse incorporando al sistema.
- Integridad de los datos. Debido a que toda la información se almacena en la misma base de datos.
- Accesibilidad. Los datos pueden ser accesados desde cualquier lado y desde múltiples aplicaciones clientes.
- Desempeño. El performance puede ser optimizado en *hardware* y procesamiento de la información.
- Seguridad. La seguridad de la información se centraliza en el servidor.

2.1.6 Desventajas de la arquitectura cliente-servidor

Aunque la arquitectura cliente-servidor provee soluciones innovadoras para cierto tipo de negocios, puede no ser el indicado para todo. La flexibilidad de los sistemas cliente-servidor y la complejidad de los requerimientos de red



necesita de una planeación muy cuidadosa. Otras desventajas del sistema son:

- Si el *hardware*, *software* y las comunicaciones no ofrecen un ambiente estable y maduro, las aplicaciones cliente-servidor pueden acarrear demasiados problemas a la operación de las tareas diarias en el procesamiento de la información.
- Los costos de mantenimiento pueden elevarse hasta en tres veces comparados con el esquema tradicional.
- El rediseño y la re-programación no son ejercicios triviales.
- El respaldo y recuperación en un esquema cliente-servidor pueden ser muy costosos.
- Entre más distribuida sea la red, más vulnerable se volverá.
- La tecnología cliente-servidor es envolvente y no existe una estandarización

En teoría, la arquitectura cliente-servidor puede ser muy atractiva, porque permite a las organizaciones crear de manera rápida aplicaciones gráficas que se amolden a las necesidades de cambios en las organizaciones. Sin embargo debajo de estas características, se pueden esconder costos que pueden hacer a éste sistema más costoso en su operación que los sistemas centralizados cuya base está fundamentada en una máquina centralizada de gran tamaño, que puede ser un mainframe.

2.2 ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

En general, las tareas de administración son las mismas para todos los sistemas operativos, en lo que difieren es en las utilerías que se tienen disponibles para esta tarea y en los archivos de configuración. Dado esto, y considerando que en el Instituto se tienen únicamente servidores Unix (Solaris, Linux y AIX) nos enfocaremos a este sistema operativo.

2.2.1 Componentes del Sistema Operativo Unix

Antes de comenzar a estudiar las tareas de administración, veamos brevemente como está compuesto este sistema operativo.

Unix en un sistema multicapas. En un sentido estrictamente físico, el *kernel*, *shell* y utilerías se encuentran trabajando sobre el *hardware*. Lógicamente el sistema se encuentra dispuesto como se muestra en el diagrama de la figura 2.2.1.1.

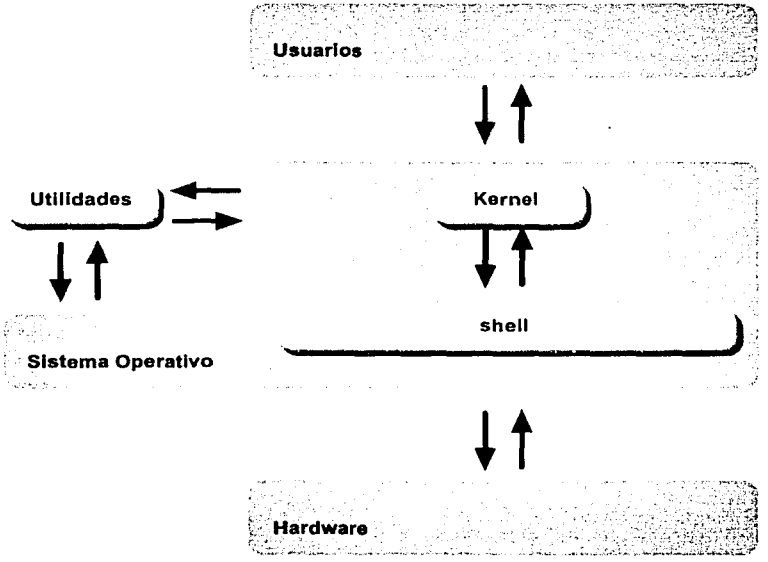
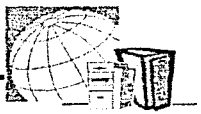


Figura 2.2.1.1 Componentes de Unix



Las utilerías se comunican con el *shell* y utilizan funciones conocidas como llamadas al sistema, para solicitar servicios del *kernel*, ya que no interactúan directamente con él.

Kernel

Como su nombre lo indica, el *kernel* es el núcleo del sistema operativo, está compuesto por una pequeña colección de *software* que hace posible que provea servicios.

Las funciones del *kernel* tales como manejo de memoria y CPU son realizadas sin la petición explícita de los procesos de usuario, algunas otras como manejo de recursos, creación y administración de procesos son iniciadas a petición de los procesos.

Un proceso es la ejecución de un programa, todos los procesos tienen dueño, un usuario es dueño del proceso que se haya iniciado a petición de éste. Un proceso a su vez puede crear subprocesos, donde al proceso original se le conoce como proceso padre y a los subprocesos como procesos hijos, los cuales adquieren los privilegios de lectura, escritura y ejecución del proceso padre.

Shell

Un *user* (usuario) accesa a los servicios del *kernel* a través de una interfaz llamada *shell*, que es un intérprete de comandos que permite al usuario iniciar procesos para realizar una infinidad de tareas.

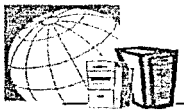
Existen varios *shells* estándar, que incluyen C *shell*, Bourne *shell* y Korn *shell*, entre otros; además, existen las herramientas gráficas (GUIs) que simplifican o automatizan las funciones del *shell*.

En general, las tareas que realiza el *shell* son:

- Manipulación de archivos y directorios (copiar, renombrar, mover)
- Ejecución de comandos
- Redirección entradas / salidas
- Control de trabajos

Utilities

Las utilerías son programas que realizan tareas del sistema. A diferencia de las utilerías en muchos otros sistemas operativos, la mayoría de las utilerías Unix están separadas del sistema, esto es que no son cargadas con el *kernel*.



Unix provee diversas categorías de utilerías, que incluyen:

- Administración de **filesystems** (sistemas de archivos)
- Comunicación local y de red
- Editores
- Filtros y procesadores de texto
- Lenguajes de programación

2.2.2 Instalación del sistema operativo

Conceptualmente este proceso es el mismo para cualquier sistema operativo, los pasos que se deben seguir son:

- Tener a la mano el medio de donde se instalará el sistema (generalmente un CD-ROM) para posteriormente insertarlo en el **drive** (manejador)
- Reiniciar el sistema del dispositivo de CD-ROM
- Los proveedores ofrecen un modo automático de instalación que permite:
  - Configurar el particionamiento del disco duro y crear los filesystems
  - Elegir los paquetes que se desean instalar, adicionales al sistema operativo
  - Configurar el nombre del *host* y su dirección IP
  - Especificar el **default-gateway** (ruteador de salida)
  - Configurar fecha y hora
- Reiniciar el sistema desde el disco duro
- Editar archivos de configuración del sistema para optimizar la operación del equipo.

2.2.3 Proceso de *boot* (iniciación del sistema operativo)

El proceso de *boot* es aquel que permite iniciar o levantar el sistema operativo cuando éste se encuentra en su nivel más bajo, consta de cuatro fases, como se muestra en la figura 2.2.3.1.

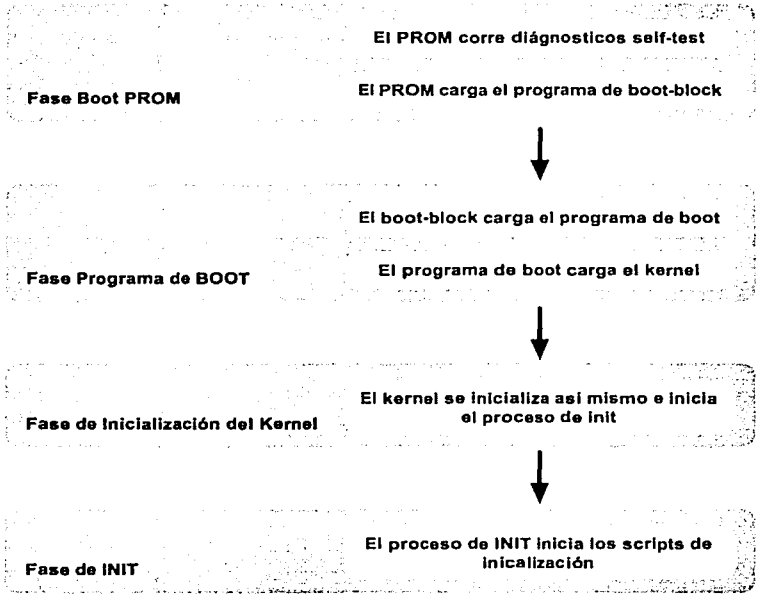


Figura 2.2.3.1 Fases del Proceso de Inicialización del Sistema Operativo

Se carga el código de memoria residente para posteriormente correr la rutina **self-test** (prueba que permite verificar el *hardware* y memoria del sistema) y cargar el *boot-block* que a su vez carga el programa de *boot*.

El programa de *boot* carga el *kernel* y le pasa el control, para que este último identifique y configure los dispositivos de la máquina. También inicializa el sistema y sus procesos, levanta el sistema en modo **single-*user*** (modo de administración desde consola) si es necesario e inicia el proceso de INIT, el cual corre los **scripts** (programas) de inicialización necesarios, para finalmente levantar el sistema en modo de operación multiusuario.

2.2.4 Estados del sistema

Completamente abajo y listo para apagar la máquina. Generalmente para realizar algún tipo de mantenimiento al *hardware* o externo al equipo.

Modo de reinicio. Generalmente utilizado cuando hay cambios en el sistema que requieran la reiniciación de la máquina para tomar efecto.

Modo Single-*user*. Corre como el usuario *root*, permite, desde consola y sin usuarios conectados, realizar algunas tareas de administración, como verificar la consistencia de un filesystem y reconfigurar la lista de terminales, entre otras.

2.2.5 Estados de los procesos

En Unix existen cinco estados, aunque en otros sistemas pueden existir más, estos son:

- *Runnable*. El proceso puede estar ejecutándose o listo para ello
- *Sleeping*. El proceso se encuentra bloqueado esperando algún evento
- *Zombie*. El proceso está tratando de finalizar su tarea
- *Stopped*. Proceso suspendido
- *Swapped*. El proceso no se encuentra en memoria, sino en disco, en la partición de *swap*

2.2.6 Scripts de Inicialización

Escritos en *shell*, generalmente los scripts de inicialización se encuentran en el directorio /etc, y sus nombres inician con rc.

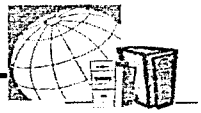
Algunos sistemas definen varios niveles de inicialización donde un conjunto específico de procesos se corre en cada uno de ellos, este conjunto de procesos es definido en el archivo /etc/inittab.

En general, las siguientes tareas son realizadas por los scripts de inicialización:

- Configurar el nombre del *host* (nodo de red)
- Configurar fecha y hora
- Verificar la consistencia de los filesystems
- Montar particiones del sistema
- Iniciar demonios y servicios de red
- Configurar la o las interfases de red
- Encender quotas (cantidad de espacio en disco asignado a cada usuario)

2.2.7 Archivos de configuración

Los archivos de configuración son de texto plano y contienen información acerca de la estructura o manejo de partes específicas del sistema, éstos se localizan en el directorio /etc.



A continuación se mencionan las características de los más utilizados:

/etc/dfstab: Archivo de configuración del sistema de archivos, el cual contiene la lista de las particiones que fueron creadas y la función de cada una de ellas. Éste es utilizado por algunos comandos, entre ellos mount; gracias a éste, las particiones se montan automáticamente al momento de iniciar el sistema.

/etc/passwd: Éste se modifica cada vez que se ingresa un nuevo usuario, contiene siete campos separados por dos puntos (:)

- ***Login*** (clave de acceso)
- *Password* encriptado
- ***User* ID** (UID Identificador de Usuario)
- **Group ID** (GID Identificador de Grupo) principal
- Campo de información del usuario
- Directorio **home** (el raíz del usuario)
- *Shell*

/etc/shadow: Si en el archivo /etc/passwd se tiene una letra «x» en el campo de *password*, el sistema sabe que el *password* se encuentra en un archivo llamado /etc/shadow, donde se tiene un mapeo de *logins* con su *password* respectivo encriptado.

/etc/group: Contiene los nombres de los grupos y los usuarios de cada uno.

/etc/inetd.conf: Es el archivo de demonios de Internet.

/etc/hosts: Archivo de mapeo de nombres de *hosts* con sus respectivas direcciones IP, aquí es donde se mantiene la dirección IP del equipo.

/etc/inittab: Ayuda a regular la operación de las interfases seriales.

/etc/export: Contiene la lista de filesystems que se tienen disponibles para que otras máquinas los vean vía **Network *File System*** (NFS, Sistema de Archivos en Red).

/etc/mnttab: Mantiene información de los filesystems montados

2.2.8 Tipos de Filesystems

• **Filesystems Físicos o Particiones.** El espacio de almacenamiento en disco en una computadora generalmente reside en diferentes tipos de dispositivos, es decir, diferentes tipos de medios, incluyendo disco duro, CD-ROM y **floppy** (unidad de disco flexible). Cada uno de éstos está asociado con un filesystem físico diferente; existen numerosos tipos en Unix, como:

- UFS. Unix *File System*. Filesystem estándar en Unix.
- NFS. Network *File System*. Es el que se utiliza para accesar a dispositivos a través de la red.
- BFFS. Berkeley Fat Fast *File System*. Es un ufs mejorado.
- MSDOSFS. Filesystem utilizado por ms-dos, en ocasiones disponible en Unix.
- CD9660. El filesystem de ISO-9660 para dispositivos de cd-rom.

• **Filesystems Lógicos.** Son una estructura de datos o colección de archivos, formados por un árbol de directorios como se muestra en la figura 2.2.8.1. Donde un filesystem se encuentra sobre una partición de disco y donde todos sus archivos son contenidos lógicamente en el directorio *root*.

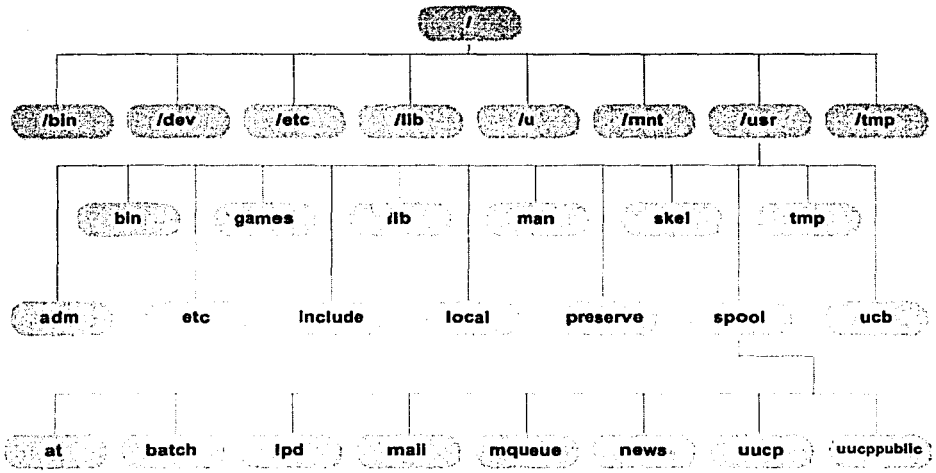
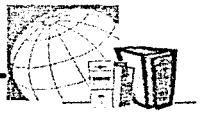


Figura 2.2.8.1 Estructura de directorios de BSD



Existen diversas operaciones en los filesystems, como son:

- Creación de nuevos filesystems. Para lo que se utilizan los comandos *mkfs* o *newfs*.
- Montaje y desmontaje de los filesystems. Utilizando los comandos *mount* y *umount* respectivamente
- Diagnósticos y reparaciones del filesystem. Se utiliza el comando *fsck* teniendo el filesystem desmontado.

2.2.9 Estructura Interna del Filesystem de Unix

Boot Block (Bloque de Inicialización). Normalmente es parte de la etiqueta del disco, consta de un conjunto especial de bloques que contienen información acerca del particionamiento del disco, y contiene el cargador para inicializar el sistema operativo.

Super Block. Cada partición de Unix contiene normalmente un bloque especial llamado superbloque, que contiene información básica de todo el *filesystem*. Esto incluye tamaño, la lista de bloques libres y utilizados, el nombre de la partición y la hora en que se modificó el *filesystem*.

Inodos. Contienen información de cada archivo en el *filesystem* y son almacenados en una estructura especial del *kernel*. Un inodo contiene un puntero a los bloques de disco que contienen los datos del archivo, contiene además el tipo de archivo, permisos, dueño, grupo, tamaño del archivo y hora de última modificación, entre otros.

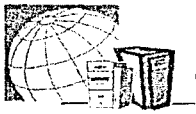
2.2.10 Creación de cuentas de usuarios

Para tener acceso a una máquina se requiere de una clave de usuario (*login*) y un *password*, para lo que es necesario crear una cuenta.

Es muy importante al crearla tomar algunas consideraciones, cada usuario en el sistema debe tener un *login* único y un UID (Identificador) único, entre 100 y 32767, del 0 al 100 están reservados para el sistema. Normalmente éstos se encuentran en minúsculas y son de máximo ocho caracteres.

Cada usuario debe pertenecer por lo menos a un grupo, y como máximo a 16.

Para crearlas hay varios métodos, utilizar un comando, alguna herramienta gráfica de administración o modificar los archivos necesarios manualmente, aunque el /etc/passwd no es muy recomendable modificarlo a mano, ya que si hay algún error, se podría corromper, lo que representaría un riesgo de seguridad.



2.2.11 Introducción a la Seguridad

Esta es responsabilidad del administrador del *host*, de la organización que lo adquirió, de los usuarios del sistema y de todo aquel que tenga acceso físico a este.

Para tener una máquina segura se deben considerar los siguientes puntos:

- **Seguridad Física.** Dependiendo de qué tan crítica sea la información que se tenga en el *host*, son los cuidados que se deben tener; ésta va desde el cableado, de tal forma que no se pueda desconectar el *host* fácilmente, hasta tenerlo aislado, con acceso restringido, temperatura y humedad adecuadas.

- ***Passwords.*** Es muy importante que todos los usuarios tengan uno, que lo cambien periódicamente y que no se lo proporcionen a nadie, para evitar que algún extraño accese al equipo sin autorización del administrador.

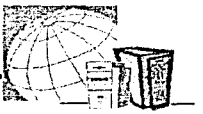
- **SUID y GUID.** Son permisos especiales sobre archivos que permiten a los usuarios ejecutar comandos que normalmente ejecuta *root*, convirtiéndose en él únicamente en el momento de la ejecución de estos sin que conozcan el *password* de *root*, los distinguimos por la letra «s» dentro de los permisos.

- **Backdoors (Puertas traseras).** Es una entrada en modo privilegiado al sistema, los programadores los utilizan para pruebas y monitoreo, los administradores los utilizan para no perder el acceso en caso de olvidar el *password* de *root*. Hay que tener mucho cuidado con éstas, ya que alguien no autorizado podría accesar al sistema con privilegios.

- **Sistema de monitoreo.** Unix tiene ciertos archivos que guardan toda la información respecto a los procesos ejecutados dentro de la máquina, accesos y salidas de los usuarios, comandos ejecutados por cada uno, etc., éstos se encuentran en el directorio /usr/adm.

- **Auditorias de seguridad.** Para cumplir con este punto se debe verificar:

  - Que todas las cuentas de usuario tengan *password*
  - Cuentas expiradas
  - Cuentas extrañas
  - Archivos que no tengan dueño
  - UIDs o GIDs duplicados



- Cambio de permisos en archivos
- Programas con permisos SUID y GUID en particular los que pertenecen a *root*
- Cambio en archivos del *kernel*
- Comandos recientemente agregados
- Cambios no autorizados a algún *filesystem*
- Actividad inusual del sistema

• Respaldos. Es muy importante tener respaldada la información del sistema en algún otro medio, como cinta, discos ópticos, etc., sobre todo los archivos críticos y la información de los usuarios, para si se llega a requerir en algún momento dado.

2.2.12 Instalación de nuevo *hardware*

La mayoría de los equipos traen consigo interfases estándar, puerto(s) serial(es), puerto paralelo, etc., lo cual permite a algunos periféricos ser instalados sin agregar *hardware* o *software* adicionales; por ello se recomienda revisar las especificaciones del nuevo *hardware* antes de instalarlo.

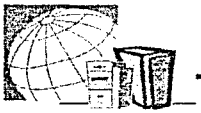
2.2.13 Volúmenes lógicos

Un disco se puede particionar hasta en 7 secciones, si se desea tener una partición mas grande que el tamaño de un disco o tener redundancia en los datos es necesario utilizar volúmenes.

Para esto es necesario conocer el concepto de **Redundant Array of Independent (Inexpensive) Disks** (RAID, Arreglo Redundante de Discos Independientes o No Caros), que utiliza porciones de discos y los transforma en un dispositivo grande y puede proveer recuperación de datos. Existen varios niveles de RAID que proporcionan diferentes niveles de seguridad en la información.

2.2.14 Introducción a la automatización de tareas

Una parte importante de la administración es el mantenimiento de la máquina. Debido a que la información almacenada es cambiante, es necesario realizar una verificación básica y periódica.



Este mantenimiento incluye:

- Diariamente
  - Remover archivos core (son generados cuando se produce un error en una aplicación).
  - Eliminar archivos innecesarios del directorio /tmp
  - Monitorear el espacio en disco en los directorios de los usuarios

- Semanalmente
  - Realizar un chequeo de *filesystems*
  - Monitoreo de procesos
  - Limpiar archivos de log (bitácoras de accesos, servicios, etc.)

- Mensualmente
  - Correr reportes mensuales
  - Localizar archivos grandes que ya no se utilizan

Creación de crones

Un cron es un comando o programa que se ejecuta periódicamente. Existe un demonio cron que despierta cada minuto y verifica los archivos de crones que se almacenan en un directorio especial, si encuentra alguno que esté programado para ese minuto en particular, lo ejecuta.

2.2.15 Monitoreo del performance (desempeño) de la red

Para determinar si se está experimentando un cuello de botella en el performance de la red se tienen varias herramientas de medición, entre ellas el comando *netstat*, que es utilizado para reportar una variedad de información de red incluyendo la cantidad de utilización de memoria del *kernel*.

2.2.16 Monitoreo del performance de la memoria

Para determinar cuellos de botella de entradas y salidas existe en el sistema el comando *iostat* que puede desplegar la cantidad de datos en movimiento entre el sistema y el disco o un dispositivo terminal.

2.3 ADMINISTRACIÓN DE BASES DE DATOS

La tecnología de las bases de datos se ha descrito como una de las áreas de la ciencia de la computación y la información de más rápido desarrollo. Como campo comercial, aún es relativamente nueva; los fabricantes y vendedores no empezaron a ofrecer sistemas de administración de bases de datos hasta mediados de la década de 1960 (aunque es verdad que ciertos paquetes de *software* antiguos incluían algunas de las funciones que ahora se asocian con tales sistemas. Pese a su calidad de innovación, sin embargo, el campo rápidamente ha cobrado importancia práctica y teórica. La cantidad total de datos encomendados a las bases de datos se mide, sin exagerar, en varios miles de millones de bytes; la inversión financiera al respecto alcanza una cifra igualmente enorme; y no es exagerado afirmar que muchas miles de organizaciones dependen de la operación continua y eficaz de un sistema de bases de datos, **DBS** (Data Base System).

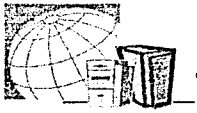
Un sistema de bases de datos, en esencia, no es más que un sistema de mantenimiento de registros basado en computadoras, es decir, un sistema cuyo propósito general es registrar y mantener información. Tal información puede estar relacionada con cualquier cosa que sea significativa para la organización donde opera el sistema, en otras palabras, cualquier dato necesario para los procesos de toma de decisiones inherentes a la administración de la organización.

Se puede decir que un sistema de bases de datos incluye cuatro componentes principales: datos, *hardware*, *software* y usuarios.

- **Datos.** Los datos almacenados en el sistema se dividen en una o más bases de datos. Una base de datos es un repositorio de datos almacenados, y en general, es tanto *integrada* como *compartida*.

  Por *integrada* se entiende que la base de datos puede considerarse como una unificación de archivos de datos independientes, donde se elimina parcial o totalmente cualquier redundancia entre los mismos.

  Por *compartida* se entiende que partes individuales de la base de datos pueden compartirse entre varios usuarios distintos, en el sentido de que cada uno de ellos puede tener acceso a la misma parte de la base de datos (y utilizarla con propósitos diferentes). Tal comportamiento es consecuencia del hecho de que la base de datos es integrada. Otra consecuencia del mismo hecho se advierte en que cualquier usuario específico, por lo general, tendrá acceso tan sólo a algún subconjunto de la base de datos completa; además, subconjuntos de diferentes usuarios se trasladarán de muy diversas maneras. Diferentes usuarios



percibirán de modos muy distintos una base de datos específica: aunque dos usuarios compartan el mismo subconjunto de la base de datos, sus percepciones o vistas de ese subconjunto pueden diferir mucho a nivel de detalle.

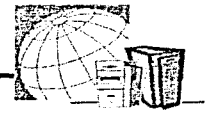
La palabra *compartida* a menudo se amplía para abarcar no sólo al comportamiento antes descrito, sino también al comportamiento *concurrente*, es decir, la oportunidad de que diversos usuarios tengan acceso a la base de datos al mismo tiempo. En la actualidad, la mayoría de los DBSs permiten el acceso multiusuario a las bases de datos.

• ***Hardware.*** Se compone de los equipos en los cuales residen los sistemas de bases de datos y las unidades de almacenamiento secundario que albergan las bases de datos. El *hardware* necesario para cada sistema de bases de datos se define de acuerdo a las especificaciones del fabricante o desarrollador del sistema atendiendo a las necesidades de uso de las bases de datos por parte de la organización.

• ***Software.*** Entre la base de datos física (almacenamiento real de los datos) y los usuarios del sistema existe un conjunto de programas y aplicaciones que comúnmente se conocen con el nombre de Sistema de Administración de Bases de Datos o **DBMS** (Data Base Management System).

• **Usuarios.** Se consideran tres clases generales de usuarios. La primera la representa el *programador de aplicaciones*, encargado de escribir programas de aplicación que utilicen las bases de datos. Estos programas de aplicación operan con los datos de todas las maneras usuales: recuperación de información, creación de información nueva, borrado o modificación de información existente, etc. Todas estas funciones se realizan formulando las solicitudes adecuadas al DBMS. Los programas en sí pueden ser aplicaciones convencionales de procesamiento por lotes o programas en línea diseñados para apoyar a un usuario final que interactúa directamente con el sistema.

La segunda clase de usuario es el *usuario final*, que es el que se encarga de realizar los movimientos sobre las bases de datos. Un usuario final puede emplear un lenguaje de consulta proporcionado como parte integral del sistema o recurrir a un programa de aplicación escrito por un programador. De cualquier manera, el usuario final puede realizar todas las funciones de consulta, creación, borrado y



modificación sobre las bases de datos, siendo las dos primeras las actividades más comunes del usuario final.

La tercera clase de usuario la representa el *administrador de bases de datos* o **DBA** (Data Base Administrator), que es el encargado de brindar y habilitar los servicios necesarios tanto para el programador como para el usuario final con el objetivo de que puedan hacer uso de las bases de datos. El DBA comúnmente lleva a cabo las actividades de administración del sistema operativo del equipo donde reside el DBMS.

2.3.1 Necesidad del uso de bases de datos

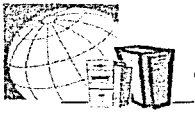
Un sistema de bases de datos proporciona a la empresa un control centralizado de sus datos de operación, que constituyen uno de sus activos más valiosos.

Lo anterior implica que en una empresa que utilice un sistema de bases de datos debe existir una persona específica o área cuya responsabilidad central sea controlar los datos de operación. Esta persona es el administrador de bases de datos, el DBA; su trabajo requiere un elevado nivel de destreza técnica y capacidad de entender e interpretar los requerimientos administrativos a nivel gerencial. El DBA ocupa un puesto de gran importancia dentro de la empresa.

Las ventajas de tener un control centralizado de los datos se mencionan a continuación.

- Se reduce la redundancia. En sistemas que no usan bases de datos, cada aplicación tiene sus propios archivos. Esto a menudo origina una enorme redundancia en los datos almacenados, así como desperdicio resultante del espacio de almacenamiento; por ejemplo, una aplicación de personal y otra de registros educativos pueden poseer cada una un archivo que contenga información del departamento de empleados. Estos dos archivos pueden integrarse (para eliminar la redundancia) si el DBA está consciente de los requerimientos de información para ambas aplicaciones, es decir, si el DBA tiene el control global necesario.

  No toda la redundancia debe eliminarse por fuerza. A veces hay sólidas razones comerciales o técnicas para mantener múltiples copias de los mismos datos. En un sistema de bases de datos la redundancia debe controlarse, es decir, el sistema debe estar al tanto de la redundancia y asumir la responsabilidad de propagar las actualizaciones correspondientes.



• Se evita la inconsistencia. Esto es corolario del punto anterior. Supóngase un sistema en el cual un dato se representa por dos entradas distintas y el sistema no cuenta con los mecanismos para estar al tanto de esta duplicidad. Habrá ocasiones en que las dos entradas no concuerden, es decir, cuando una y sólo una de ellas se haya actualizado. En tales circunstancias se dice que la base de datos es inconsistente. Una base de datos que se halle en estado de inconsistencia puede suministrar información incorrecta o contradictoria.

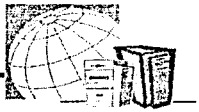
No hay duda de que si el dato en específico se representa por una sola entrada (es decir, si la redundancia se elimina), tal inconsistencia no puede ocurrir. Por otra parte, si la redundancia no se suprime, pero se controla, entonces se puede garantizar que la base de datos nunca sea inconsistente para el usuario al asegurar que cualquier cambio hecho a una de las dos entradas se efectúe de manera automática en la otra. Este proceso se denomina *propagación de actualizaciones*, donde el término actualización se usa para abarcar todas las operaciones de creación, borrado y modificación de datos. Cabe señalar que no todos los sistemas son capaces de propagar las actualizaciones de modo automático, pero la mayoría admiten mecanismos para contar con una redundancia controlada.

• Los datos se pueden compartir. No sólo significa que las aplicaciones existentes pueden compartir los datos de la base de datos, sino también que es factible desarrollar nuevas aplicaciones que operen con los mismos datos almacenados.

• Se hacen cumplir las normas establecidas. Con un control central de la base de datos, el DBA puede garantizar que se cumplan todas las formas aplicables a la representación de los datos. Las normas aplicables pueden comprender la totalidad o parte de lo siguiente: normas de la compañía, de instalación, departamentales, industriales, nacionales o internacionales. Es muy deseable unificar los formatos de los datos almacenados como ayuda para el intercambio o migración de datos entre sistemas.

• Se pueden aplicar restricciones de seguridad. Al tener jurisdicción completa sobre los datos de operación, el DBA puede:

- Asegurar que el único medio de tener acceso a la base de datos sea a través de los canales establecidos.



- Definir controles de autorización para que se apliquen cada vez que se intente el acceso a datos sensibles. Diferentes controles pueden establecerse para cada tipo de acceso a cada parte de la información de la base de datos.

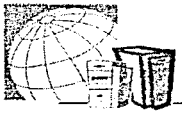
• Se conserva la integridad. El problema de la integridad es garantizar que los datos de la base de datos sean exactos. La inconsistencia entre dos entradas que representan el mismo dato es un ejemplo de la falta de integridad. Aún cuando la redundancia se elimine, la base de datos puede contener aún datos incorrectos. El control centralizado de la base de datos ayuda a evitar estas situaciones en la medida de lo posible, pues permite al DBA definir procedimientos de validación que habrán de ejecutarse cada vez que se intente una operación de actualización. Es conveniente señalar que la integridad de los datos es más importante en un sistema de bases de datos que en un sistema de archivos propietarios, precisamente porque el primero comparte y porque sin procedimientos de validación adecuados es posible que un programa con errores genere datos incorrectos que afecten a otros programas que utilicen esa información.

• Se pueden equilibrar los requerimientos contradictorios. Cuando se conocen los requerimientos globales de la empresa, en contraste con los requerimientos de cualquier usuario individual, el DBA puede estructurar el sistema de bases de datos para brindar un servicio que sea el mejor para la empresa en términos globales. Por ejemplo, puede elegirse una representación de los datos almacenados que ofrezca rápido acceso a las aplicaciones más importantes, a costa de un desempeño menor en algunas otras aplicaciones.

2.3.2 El Administrador de las Bases de Datos, DBA

Los administradores de bases de datos deben tener las habilidades y capacidades necesarias para el desarrollo y administración de sistemas de carácter institucional vinculadas con los servicios de la Intranet corporativa y los servicios de Internet que se ofrecen al público en general. Los DBAs deben orientar su trabajo dentro de cinco rubros fundamentales de la administración de las bases de datos:

- Seguridad de los sistemas de bases de datos.
- Disponibilidad de las bases de datos para los usuarios.
- Monitoreo del desempeño y planeación para la escalabilidad.
- Integración con aplicaciones de terceros.
- Administración del DBMS, de acuerdo a las especificaciones de cada fabricante.



Responsabilidades del administrador

El trabajo de un DBA es un conjunto de actividades transparentes para el usuario que hace uso de las bases de datos. Actualmente los administradores de bases de datos deben tener un perfil proactivo para llevar a cabo su trabajo. En el pasado, la mayor parte del trabajo de los DBAs era reactivo, actuando únicamente cuando se presentaban los problemas (reaccionaban ante la causa). Afortunadamente muchas cosas han contribuido para ayudar al DBA a tomar acciones antes de que se presenten los problemas y anticiparse a los hechos, entre ellas, las nuevas plataformas y tecnologías introducidas por los grandes desarrolladores de sistemas de bases de datos. Aún así, los problemas persisten, pero el DBA tiene más herramientas y un mejor conocimiento de los DBMS gracias a la automatización y mejora de los productos.

Muchas de las herramientas del arsenal del DBA se encuentran en el mercado a través de terceros, como son Platinum, BMC, Embarcadero e IBM. La existencia de este mercado de terceros, se debe a que los grandes vendedores de los sistemas de bases de datos, como son Oracle, Sybase e Informix, entre otros, no cuentan con aplicaciones adicionales que ayuden a automatizar los procesos de administración y detección de problemas, dejando el camino libre a terceros y haciendo alianzas estratégicas. Sin embargo, esta tendencia se ha empezado a revertir; por ejemplo, Oracle ha desarrollado una gran gama de aplicaciones cuyo objetivo es brindar herramientas que permitan a la empresa y al DBA minimizar los problemas y optimizar el desempeño de los sistemas de bases de datos. Las demás empresas han seguido esta misma línea, generando una competencia más agresiva entre los fabricantes de productos de terceros, lo cual ha ayudado a mejorarlos.

Independientemente de las herramientas con que cuente el DBA, sus responsabilidades principales deben ser:

- Decidir el contenido de la información de la Base de Datos. Es trabajo del DBA decidir con exactitud qué información se mantendrá en la base de datos, es decir, identificar las entidades de interés para la empresa y la información que debe registrarse acerca de esas entidades. Después de hacerlo, el DBA debe definir el contenido de la base de datos escribiendo su correspondiente esquema conceptual.

- Decidir la estructura de almacenamiento y la estrategia de acceso. El DBA también debe decidir de qué manera habrán de representarse los datos y especificar la representación escribiendo la definición de la estructura de almacenamiento (mediante lenguajes de definición de datos internos, **DDLs**, Data Definition Languages). Además, debe

especificar la correspondencia asociada entre la definición de la estructura de almacenamiento y el esquema conceptual; es decir, la forma en que físicamente serán almacenados los datos y la forma en que se verán representados a nivel lógico.

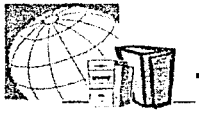
• Vincularse con los usuarios. Es responsabilidad del DBA tener un estrecho y continuo vínculo con los usuarios, garantizar que los datos que requieran estén disponible y apoyar en el diseño del esquema mediante el cual harán uso de las bases de datos.

• Definir los controles de autorización y los procedimientos de validación. Los controles de autorización y los procedimientos de validación pueden considerarse extensiones lógicas del esquema conceptual.

• Definir una estrategia de respaldo y recuperación de datos. Una vez que una empresa adopta un sistema de bases de datos, empieza a depender en forma decisiva en la operación exitosa del mismo. En el caso de que se dañe alguna parte de la base de datos por cualquier causa (un error humano, o una falla en el *hardware* o en el sistema operativo), es esencial poder reparar los datos pertinentes con la mayor brevedad reduciendo al mínimo posible las repercusiones en el resto del sistema. El DBA debe definir y poner en marcha una estrategia de recuperación adecuada, que incluya el vaciado periódico de las bases de datos en cintas de respaldo u otros dispositivos de almacenamiento masivo, y procedimientos para reponer las partes pertinentes de la bases de datos cuando se requiera.

• Controlar el desempeño y responder a los cambios de requerimientos. El DBA se encarga de organizar el sistema de tal manera que se logre un desempeño que sea el mejor para la empresa, así como de hacer los ajustes adecuados a medida que los requerimientos cambian. Cualquier cambio en los detalles de almacenamiento y de acceso debe ser acompañado por un cambio respectivo en la definición de la correspondencia con el almacenamiento, de modo que el esquema conceptual se mantenga inmutable.

El DBA necesitará de varios programas o aplicaciones de utilería para facilitar estas tareas. Tales programas formarán parte esencial de un sistema práctico de bases de datos; como se mencionó anteriormente, estas aplicaciones pueden ser proporcionadas por terceros o por el mismo fabricante del sistema de bases de datos.



Como actividades adicionales el DBA tiene a su cargo:

- Instalación, configuración y actualización del manejador o manejadores de las bases de datos.
- Evaluación de las características y funcionalidades de los manejadores de bases de datos y las aplicaciones relacionadas.
- Apoyar en el diseño e implementación de las bases de datos.
- Implementar y mantener la seguridad correspondiente en las bases de datos (creación y mantenimiento de usuarios, roles y asignación de privilegios).
- Implementar el monitoreo continuo del desempeño de las bases de datos y las aplicaciones relacionadas.
- Hacer los ajustes necesarios a las bases de datos y a las aplicaciones relacionadas con la finalidad de obtener un desempeño óptimo en cada una de ellas.
- Llevar a cabo la planeación del crecimiento y los cambios necesarios (planeación de la capacidad), tanto de los manejadores como de las bases de datos.
- Trabajar como parte de un equipo y brindar un soporte acorde a las necesidades de los usuarios.
- Atender y resolver problemas de carácter técnico.
- Brindar la consultoría necesaria a los grupos de desarrollo de sistemas.
- Mantener un estrecho vínculo con los equipos de soporte de los fabricantes de los manejadores de bases de datos.

Entre las habilidades con que debe contar el DBA, algunas de las principales son:

- Tener un buen nivel de conocimiento de los manejadores de bases de datos, aplicaciones relacionadas y herramientas que utilice la empresa para la implementación de los sistemas.
- Tener un buen nivel de conocimiento de los sistemas operativos en los que residan los manejadores de bases de datos.
- Tener un conocimiento detallado del diseño físico de las bases de datos.
- Tener habilidad para llevar a cabo los ajustes necesarios en los sistemas operativos y manejadores de bases de datos para optimizar el desempeño.
- Tener responsabilidad y liderazgo para manejar múltiples proyectos.
- Un buen conocimiento de la forma en que se administra y funciona la empresa.

2.3.3 Bases de Datos Distribuidas

La tecnología de bases de datos distribuidas constituye un avance relativamente reciente dentro del campo general de las bases de datos. Una base de datos distribuida es, por lo común, una base de datos no almacenada en su totalidad en un solo lugar físico, sino que se distribuye a lo largo de una red de computadoras y servidores geográficamente separados que se conectan mediante una red.

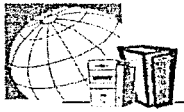
En una base de datos distribuida los datos se almacenan en el sitio donde se usan con mayor frecuencia, pero también están disponibles a través de la red, para los usuarios de otros lugares. Las ventajas de tal distribución son elocuentes: combina la eficiencia del procesamiento local (sin excesivos costos de comunicación) de la mayoría de las operaciones y todas las ventajas que ofrece un sistema centralizado, ya que a la vista del usuario, parecería que solo existe una sola base de datos. Las desventajas de las bases de datos distribuidas son pocas: los costos de comunicación pueden ser elevados y al momento existen dificultades técnicas significativas para instrumentar un sistema así.

2.3.4 PostgreSQL

Varios desarrollos de proyectos nunca han abandonado el ambiente académico. Ocasionalmente, sólo algunos de ellos sobreviven la transición de su uso en las universidades, a su uso en el mundo real de las empresas e instituciones; y más difícil es aún que se vuelvan un fenómeno. PostgreSQL es uno de esos proyectos. Su popularidad y éxito son un testamento de la dedicación y el trabajo duro del equipo de desarrollo de PostgreSQL. Desarrollar un sistema de bases de datos avanzados no es algo sencillo, sobretodo el mantener y mejorar el código base. El equipo de desarrollo de PostgreSQL a impulsado la expansión del uso de este sistema de bases de datos dentro de la comunidad de Internet, además de que mejora continuamente la calidad y facilidad de uso del producto.

Postgres95, después llamado PostgreSQL, empezó como un pequeño proyecto creado por estudiantes y personal de la Universidad de California en Berkeley y desde su nacimiento ha sido uno de los sistemas de bases de datos que incorporan estándares definidos en los Fórums mundiales. Se puede decir que PostgreSQL es el DBMS más avanzado del tipo Open Source (de código fuente disponible).

El antecesor de PostgreSQL fue *Ingres*, también desarrollado por la Universidad de California en Berkeley. El código fuente de Ingres fue mejorado posteriormente por Relational Technologies/Ingres Corporation, que fue la



primera en comercializar exitosamente servidores de bases de datos relacionales. Posteriormente Michael Stonebraker dirigió el equipo encargado de desarrollar una base de datos relacional con objetos al cual se llamó Postgres. En 1996 se tuvo la visión de seguir con el desarrollo de este sistema incluyendo el lenguaje **SQL** (Simple *Query* Language).

A la fecha, el desarrollo de PostgreSQL ha sido continuo y se han incrementando las funcionalidades, haciendo de él un sistema de bases de datos robusto que soporta:

- Acceso de tipo complejo a las bases de datos
- Transacciones
- SQL con un grado de funcionalidades de tipo comercial
- Tipos de datos complejos

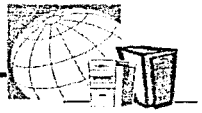
Actualmente, la distribución más utilizada del sistema operativo Linux, RedHat, incluye la última distribución de PostgreSQL. Esto ha beneficiado a muchas pequeñas empresas que soportan sus bases de datos mediante este producto. Al ser del tipo Open Source, permite que los mismos usuarios (si tienen un buen nivel de conocimientos en programación) hagan modificaciones al código fuente y adapten el sistema de acuerdo a sus necesidades, o mejor aún, solucionen problemas de la distribución original. Esto hace posible que las distribuciones posteriores implementen todas las mejoras necesarias en un menor tiempo, lo cual no sucede con los productos comerciales.

Dentro de las funcionalidades básicas de administración que soporta se encuentran:

- Manejo de archivos
- Creación de usuarios
- Creación de bases de datos
- Configuración del acceso
- Opciones para respaldos y restauraciones de datos
- Administración del servidor
- Monitoreo de su operación
- Monitoreo y optimización del desempeño
- Tablas de sistema
- Internacionalización
- Actualizaciones

2.3.5 Oracle

El sistema de bases de datos Oracle es el más popular en el ámbito comercial y ha llegado a eclipsar a sus competidores más cercanos. Oracle Corporation ha llegado a una posición envidiable al desarrollar y comercializar un producto



que tiene como características principales ser: compatible, escalable, portable y robusto. En cuanto a desempeño, la velocidad de respuesta y acceso a las bases de datos puede ser muy rápido. Oracle es un producto que se vuelve cada vez más complejo con cada nueva versión. Como resultado de ello, la administración se vuelve cada vez más crítica haciendo del DBA la llave fundamental en el óptimo aprovechamiento del producto.

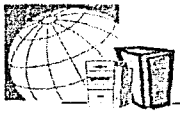
La última versión de Oracle es *Oracle9i*, desde la versión *Oracle8i* ya cuenta con una gran cantidad de herramientas orientadas a satisfacer la demanda de los servicios de Internet y su relación con las bases de datos, sobretodo en el ámbito del comercio electrónico y servicios de información.

Al ser una herramienta tan robusta y completa las actividades del DBA tienen que estar muy bien establecidas de acuerdo al tipo de empresa o institución. Para ello Oracle cuenta con una gran gama de aplicaciones que ayudan a automatizar y simplificar el trabajo del administrador de Oracle.

Para satisfacer el rubro de la *seguridad*, Oracle proporciona aplicaciones y mecanismos flexibles y escalables para la autenticación de usuarios, auditoría, encripción de datos, control de acceso altamente especializado y esquemas de seguridad integral del sistema de bases de datos.

En el aspecto de la *disponibilidad*, Oracle cuenta con mecanismos para la recuperación en caso de desastres, para los respaldos y las recuperaciones de datos de forma especializada, para el óptimo almacenamiento de la información y para la administración confiable de recursos. Oracle permite la *integración* de productos de terceros, clasificados en: aplicaciones para el manejo de mensajes y correo electrónico, aplicaciones para el control y la organización dentro de la empresa, aplicaciones de comunicación asíncrona (transaccionales), aplicaciones para transformación de datos, aplicaciones para el manejo de recursos financieros (el sistema SAP R/3 puede integrar su base de datos mediante Oracle) y aplicaciones de servicios de directorio, como es el caso de LDAP.

Oracle Enterprise Management es una herramienta que permite la optimización del *desempeño* y la automatización de la *administración* del sistema mediante una arquitectura unificada para la administración de todos los módulos del sistema, una consola centralizada que sirve como punto único de control y módulos adicionales para requerimientos puntuales. A través de esta aplicación, los productos Oracle instalados pueden ser monitoreados mediante protocolos de administración de red estándares, lo cual permite obtener reportes de operación y desempeño de todo el sistema, necesarios para la toma de decisiones y la planeación del crecimiento y atención inmediata de requerimientos.



2.4 TECNOLOGÍAS DE TRANSPORTE

Las redes de datos pueden ser clasificadas de acuerdo a su extensión geográfica en las siguientes categorías:

Las **LANs** (Redes de Área Local) son típicamente usadas para conectar computadoras dentro de un área relativamente pequeña, como lo es una oficina, un edificio o un campus. Una LAN maneja velocidades que van de los 10 **Mbps** (Mega bits por segundo) a los 100 Mbps o incluso ahora, hasta 1 **Gbps** (Giga bits por segundo) con la introducción de las nuevas tecnologías que más adelante vamos a abordar. Generalmente las LANs conectan algunos cientos de dispositivos sobre áreas de entre 5 y 10 Km2. Las LANs se hicieron populares porque permiten a muchos usuarios compartir recursos como son: procesamiento, archivos, impresoras, etc.

La siguiente clasificación se refiere a las **MANs** (Redes de Área Metropolitana) que abarcan un área geográfica que cubre una ciudad. Las MANs conectan varias LANs localizadas en diferentes edificios distribuidos a lo largo de una ciudad; típicamente las MANs abarcan áreas que van de los 10 Km2. a unos cuantos cientos de Km2. Las velocidades en una MAN van de los 1.5 Mbps hasta los 150Mbps.

La última clasificación se refiere a las **WANs** (Redes de Área Amplia) que están diseñadas para interconectar sistemas de una ciudad a otra, por ejemplo. Las velocidades en las líneas WAN van desde los 64 Kbps hasta incluso 2.4Gbps. En la WAN los costos de transmisión son muy altos y la red como tal es operada por los dueños de las redes públicas comúnmente llamados Carriers (Compañías como TELMEX que ofrecen servicios públicos para la transmisión de datos). Las compañías rentan esos servicios para interconectar sus oficinas regionales dispersas por todo un país o incluso dispersas alrededor del mundo.Para el caso particular de nuestro estudio, vamos a enfocarnos en saber a grandes rasgos como funcionan las tecnologías utilizadas por el IFE tanto en sus redes LANs como en su red WAN.

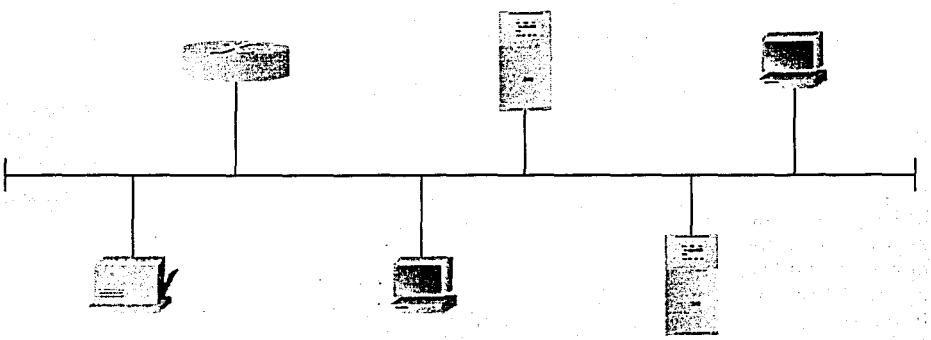
2.4.1 Tecnologías LAN

Ethernet es una tecnología que fue inventada por Xerox, que opera a 10Mbps y utiliza **CSMA/CD** (Censado de Portadora de Múltiple Acceso y Detección de Colisión) como método de acceso al medio. En su versión original el cableado sobre el cual la tecnología fue utilizada era coaxial; sin embargo, en la actualidad sabemos que existen más medios sobre los cuales puede utilizarse. *Ethernet* fue diseñado para dar servicio a redes con tráfico esporádico y que ocasionalmente pueda ser alto. La segunda versión de ésta tecnología fue desarrollada por Digital Equipment Corporation, Intel Corporation, y Xerox

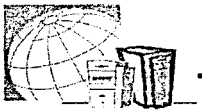
Corporation. Es compatible con su antecesor también conocido como *Ethernet* 802.3 desarrollado en los 80s y que también estuvo basado en la versión original de Xerox. La forma en que opera esta tecnología se describe a continuación. Como todos sabemos, *ethernet* trabaja bajo un ambiente de broadcast, en donde todas las estaciones ven los frames que son enviados a la red. Seguido de cualquier transmisión, cada estación debe examinar cada frame para poder determinar si dicho frame está o no dirigido hacia ella. Los frames que se identifican dirigidos a cierta estación son pasados hacia los protocolos de capas superiores para su posterior procesamiento.

En CSMA/CD cualquier estación puede accesar la red en cualquier momento. Pero antes de enviar cualquier dato, cada estación debe verificar si existe en ese momento tráfico en la red o no. Cuando una estación detecta que no hay tráfico en la red, en ese momento puede comenzar a transmitir sus frames. Sin embargo pueden ocurrir colisiones que se generan cuando dos estaciones censan que no hay tráfico en la red y transmiten sus frames al mismo tiempo. En esta situación ambas transmisiones son descartadas y cada una de ellas tiene que esperar nuevamente a que la red este libre de tráfico para poder transmitir sus frames. Existen algoritmos que determinan cuando pueden comenzar a censar el medio nuevamente las estaciones involucradas en una colisión. En la siguiente figura se muestra la forma en que fue ideado de manera original *ethernet* y que de hecho así fueron las primeras implementaciones de esta tecnología, utilizando cable coaxial y añadiendo nuevas estaciones al segmento por medio de dispositivos que se unían al coaxial, formando así un bus de datos.

SEGMENTO ETHERNET



Fast *ethernet* es otra tecnología LAN utilizada en grandes proporciones en



las redes de hoy. 100BaseT es la especificación para la versión de 100Mbps de *ethernet* implementada sobre **UTP** (Cable de Par Trenzado Sin Blindaje) o bien sobre **STP** (Cable de Par Trenzado Con Blindaje). El control de acceso al medio es compatible con 802.3 y la estandarización de esta tecnología está dictada por la especificación 802.3u de la **IEEE** (Instituto de Ingenieros Eléctricos y Electrónicos).

100BaseT utiliza la especificación 802.3 de CSMA/CD. Como resultado el formato del frame es el mismo, también su tamaño y el mecanismo de detección de errores. Adicionalmente, 100BaseT soporta todas las aplicaciones y el *software* de red que actualmente se pueda estar utilizando en las redes *ethernet* tradicionales. 100BaseT soporta velocidades de 10 y 100 Mbps utilizando los **FLP** (Pulsos de Enlace Veloz). Los **switches** (dispositivos a los cuales se conectan las estaciones finales en una red, conmutadores de datos) de fast *ethernet* deben ser capaces de detectar dichos pulsos para poder negociar la velocidad a la cual la tarjeta de red del usuario final se va a incorporar a la red. Las tarjetas de red por su parte pueden soportar velocidades de 10Mbps, 100Mbps o ambas.

La diferencia principal entre 10BaseT (*Ethernet*) y 100BaseT (Fast *Ethernet*) es la limitación de distancia entre sus nodos. En fast *ethernet* la distancia mayor entre cualquier par de nodos es de 205 metros mas o menos 10 veces menor que en 10BaseT.

La reducción de la distancia es necesaria debido a que 100BaseT utiliza el mismo mecanismo de detección de colisiones que 10BaseT. Con 10BaseT, las limitaciones de distancia son definidas de la premisa de que si una estación transmite un frame de 64 bytes (el frame más pequeño permitido) esta estación pueda saber si se generó o no una colisión con cualquier otro nodo, incluso con el que, en distancia, esté más alejado de la estación que transmitió el frame de 64 bytes. A este rango de detección de colisión se le llama comúnmente dominio de colisión.

Para poder hacer que la velocidad se incremente utilizando el mismo método de contención que en 10BaseT se debe reducir, obviamente, las distancias entre los nodos más lejanos, es decir, el dominio de colisión. Esto se debe a que la velocidad de propagación de las señales en el medio no es alterado, así que si una estación puede transmitir 10 veces más rápido, entonces las señal en el cable tiene que recorrer 10 veces menos distancia para poder cumplir con la premisa de detección de colisiones. Como resultado, cualquier estación sabe si se produce o no una colisión en la red cuando transmite sus frames.

100BaseT soporta tres tipos de cable a nivel de la capa física del modelo OSI: 100BaseTX, 100BaseFX, y 100BaseT4. Los tres tipos de medios, que hacen interfaz con la capa IEEE 802.3 MAC, se muestran en la figura 2.4.1.2

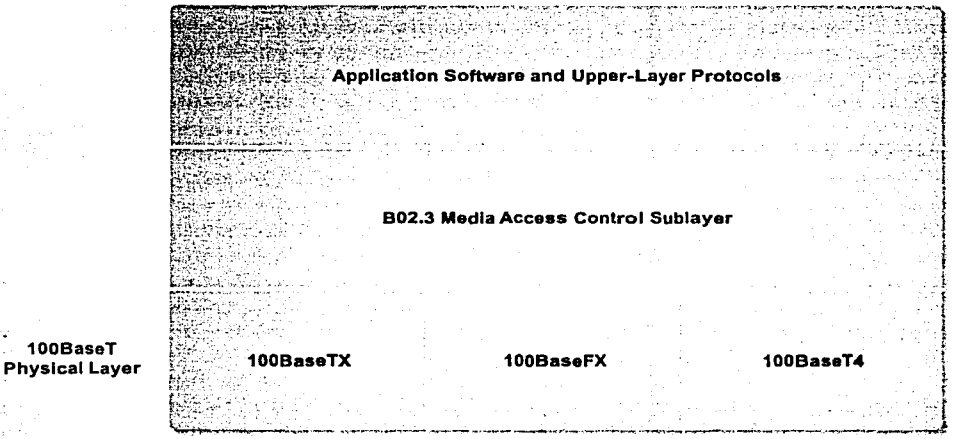


Figura 2.4.1.2 Tres tipos de medio existen para la implementación de 100BaseT.

También en la siguiente figura se muestran las características para cada tipo de medio.

Características	100BaseFX	100BaseFX	100BaseT4
Tipo de Cable	Categoría 5UTP, o tipo 1 y 2 STP	Fibra Óptica 62.5/125 micron multi-modo	Categoría 3,4, 5 UTP
Número de pares o hilos	2 pares	2 hilos	4 pares
Conector	ISO 8877 (RJ-45)	Duplex SCmedia-interfase connector (MIC) ST	ISO 8877 (RJ-45) connector
Máxima Longitud de segmento	100 metros	400 metros	100 metros
Diámetro Máximo de la red	200 metros	400 metros	200 metros

Figura 2.4.1.3 Características de los tipos de medio en 100BaseT

Gigabit *ethernet* es una extensión del estándar IEEE 802.3. Gigabit *ethernet* incrementa la velocidad de Fast *ethernet* para llevarla a 1000 Mbps o bien 1 Gbps.

Para acelerar la velocidad de 100 Mbps a 1 Gbps, es necesario hacer varios cambios a la interfaz física. Se decidió que gigabit *ethernet* sería idéntico a *ethernet* de la capa de enlace de datos hacia arriba. Sin embargo hay varios problemas que fueron resueltos al fusionar dos tecnologías: El *ethernet* IEEE 802.3 y el ANSI X3T11 **Fibre Channel** (Canal de fibra). En la figura 2.4.1.4 se muestran los componentes principales de cada tecnología para formar el gigabit *ethernet*.

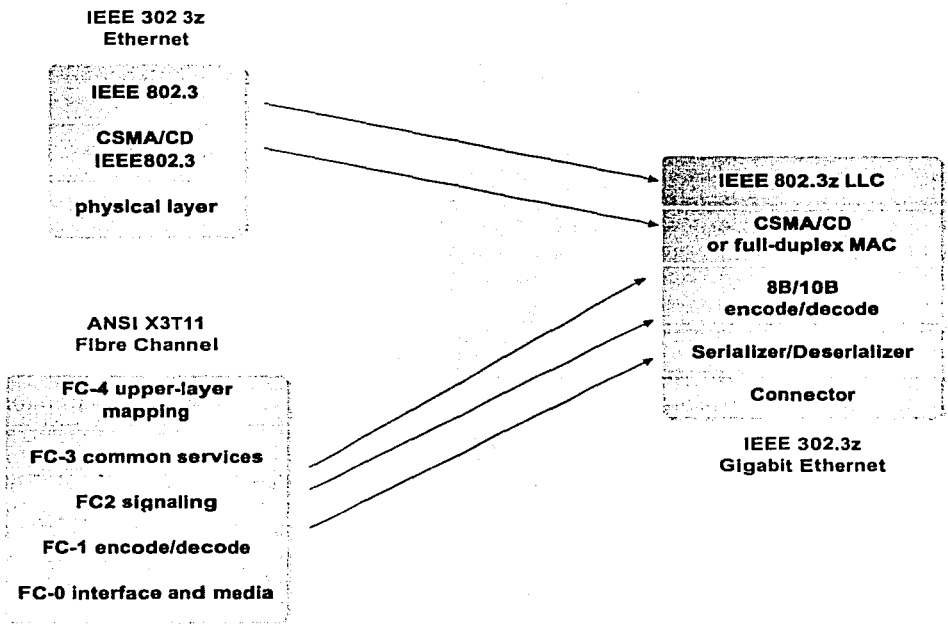
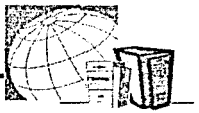


Figura 2.4.1.4 Gigabit *ethernet* esta formado en parte por el estándar *ethernet* IEEE 802.3 y el estándar ANSI X3T11

2.4.2 Tecnologías WAN

Frame Relay es una tecnología WAN que opera en las capas física y de enlace de datos del modelo de referencia **OSI** (Modelo de Referencia de Interconexión de Sistemas Abiertos). Frame Relay fue originalmente diseñado para ser usado a través de la interfaces de **ISDN** (Red integrada de servicios digitales). Actualmente es utilizada también para muchas más variedades de interfaces.



Frame Relay es un ejemplo de una tecnología basada en el **switcheo** (conmutación) de paquetes. Las redes de switcheo de paquetes les permiten a las estaciones compartir dinámicamente el medio de transmisión y el ancho de banda disponible en el mismo. Los paquetes de tamaño variable son usados de manera más eficiente generándose así transferencias de información más flexibles. Estos paquetes son switchados mediante diferentes técnicas de control de acceso en los diferentes segmentos de la red hasta que es alcanzado el destino final. Técnicas estadísticas de multiplexado controlan el acceso al medio en una red de conmutación de paquetes. La ventaja de esta técnica es que maneja de manera más flexible y eficiente el uso del ancho de banda disponible. La mayoría de las LANs actuales que utilizan tecnologías como *ethernet* o *token ring* utilizan alguna técnica de switcheo de paquetes.

Frame Relay comúnmente es descrita en estos días como una versión especial de X.25 que no contiene varias características como el **windowing** (uso de ventanas) y la retransmisión de datos que eran utilizadas por la tecnología de X.25. La pérdida de este tipo de funcionalidades en Frame Relay tiene como fundamento el hecho de que actualmente las conexiones de los puntos remotos se realizan a través de circuitos más confiables a los que se podían contratar en la época de los 70s y principios de los 80s en donde la mayoría de los servicios de transporte de datos corrían a cargo de X.25 en la WAN. Como mencionamos anteriormente Frame Relay trabaja estrictamente en la capa dos del modelo OSI. Esto le permite ofrecer un mejor desempeño y una transmisión mayor y más eficiente que X.25 y la hace ideal para la transmisión de datos de las aplicaciones que actualmente se utilizan.

Las propuestas iniciales para estandarizar Frame Relay fueron presentadas por el **CCITT** (Comité Consultivo en Telefonía y Telegrafía Internacional) en 1984. Debido a la ausencia de interoperabilidad y de una completa estandarización, sin embargo, Frame Relay no experimentó desarrollo significativo durante finales de los 80s. El mayor desarrollo en la historia ocurrió en 1990 cuando Cisco Systems, Digital Equipment, Northern Telecom y Stratacom formaron un consorcio enfocado en el desarrollo de esta tecnología. Este consorcio desarrolló una especificación que extendió las capacidades para poder soportar ambientes de redes mucho más complicados comparados con las capacidades de soporte del Frame Relay propuesto en un principio por la CCITT. Estas extensiones de Frame Relay son conocidas como **LMI** (Interfaz de Administración Local). Aunque la especificación de la CCITT fue publicada formalmente, muchos de las compañías desarrollaron soporte en sus equipos para las extensiones propuestas por el consorcio citado. **ANSI** (Instituto Americano Nacional para la Estandarización) y la CCITT subsecuentemente estandarizaron sus propias variantes de la especificación original del LMI y estas estandarizaciones son las que hoy en día soportan la mayoría de los fabricantes de equipo para Frame Relay.

Internacionalmente, Frame Relay fue estandarizado por la **ITU-T** (Unión Internacional de Telecomunicaciones, Sector Telecomunicaciones).

Una implementación de red privada de Frame Relay está equipada de un multiplexor que cuenta con interfaces Frame Relay e interfaces No-Frame Relay.

El tráfico que no es de Frame Relay es dirigido hacia la interfaz especifica de la aplicación o servicio tal como un **PBX** (conmutador telefónico) o bien hacia una aplicación de video conferencia.

Una red típica de Frame Relay consiste de cierto número de dispositivos tipo **DTE** (Equipo Terminal de Datos), tal como ruteadores, conectados hacia puertos remotos en un multiplexor vía servicios tradicionales punto a punto como puede ser un **E1** (circuito privado de comunicaciones digitales cuyo ancho de banda es 2.048Mbps) o circuitos fraccionales de 64Kbps. Un ejemplo de una red Frame Relay que muestra sus componentes se especifica en la figura 2.4.2.1.

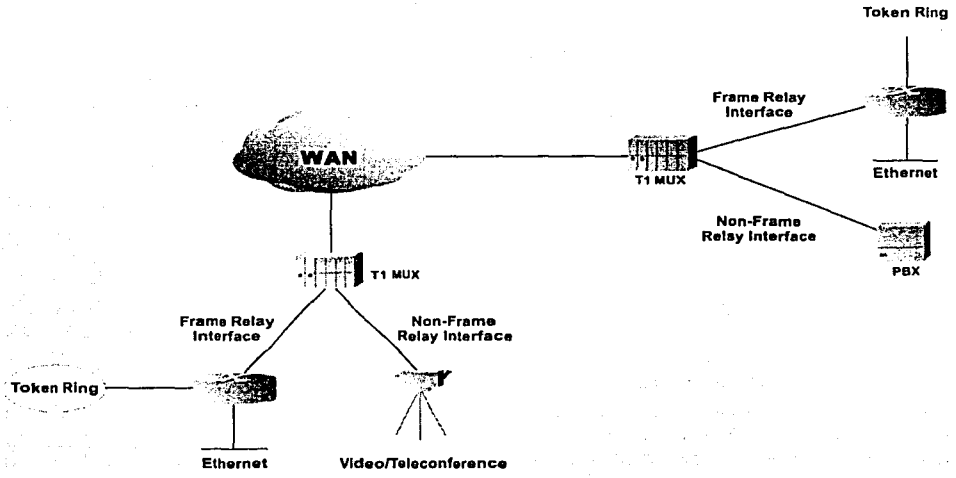
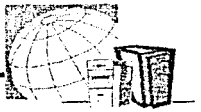


Figura 2.4.2.1 Ejemplo simple de una red Frame Relay que conecta varios servicios en una WAN.

La mayoría de las redes Frame Relay instaladas tienen proveedores de servicio quienes intentan ofrecer servicios de transmisión a sus clientes. Esto es generalmente referenciado como un servicio público de Frame Relay, el cual



puede ser implementado en ambientes públicos o privados. Los siguientes párrafos examinan ambas opciones.

En redes Frame Relay públicas, los dispositivos que forman la nube de Frame Relay se encuentran localizadon en las oficinas de los proveedores de servicio y estas empresas son las dueñas de los mismos. Los clientes son facturados según la utilización de sus circuitos pero no son responsables del mantenimientos de los equipos de Frame Relay ni del buen funcionamiento de la red pública. Generalmente el **DCE** (Equipo de Comunicaciones de Datos) puede ser propiedad del cliente o incluso también del prestador de servicios que renta el dispositivo como parte de su servicio. La mayoría de las redes Frame Relay instaladas hoy en día son de este tipo.

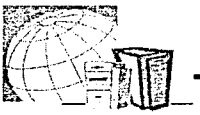
Sin embargo, existen organizaciones que pueden determinar la implementación de sus propias redes Frame Relay. Este tipo de redes son privadas y tanto la administración como el mantenimiento de los equipos y la responsabilidad de mantener funcionando los circuitos corren por parte de la empresa misma. Todo el equipo es propiedad de la empresa privada y solo los servicios de red (no-Frame Relay) son rentados con los grandes carriers.

La forma en que Frame Relay reduce el **overhead** (tráfico de control) es implementando métodos simples de notificaciones de congestión en lugar de los mecanismos explícitos de control de flujo por circuito virtual. Frame Relay implementa dos mecanismos de notificación de congestión:

- **FECN** (Notificación de Congestión Explícita Hacia Adelante)
- **BECN** (Notificación de Congestión Explícita Hacia Atrás)

Los FECN y BECN son controlados por un solo bit contenido en el encabezado del frame de Frame Relay. El encabezado también contiene un bit conocido como DE (Elegible para Descartar) que es utilizado para identificar tráfico menos significativo que puede ser descartado durante periodos de congestión.

El bit de FECN es parte del campo de dirección en el frame de Frame Relay. El mecanismo de FECN es inicializado cuando un dispositivo DTE comienza a enviar frames a la red. Si la red se encuentra congestionada, los dispositivos DCE (switches) cambian el valor del bit FECN para que tenga un 1. Cuando los frames alcanzan su destino en el DTE, el campo de dirección (con el bit FECN encendido) indica que el frame experimentó congestión en la ruta desde el origen hasta el destino. El dispositivo DTE puede relevar esta información hacia las capas superiores para ser procesado. Dependiendo de la implementación, el control de flujo puede ser inicializado, o la indicación de congestión ignorada.



El bit de BECN también es parte del campo de dirección en el encabezado del frame. Los dispositivos DCE inicializan el bit a 1 en los frames que viajan en sentido opuesto a los frames con el FECN encendido. Esto informa al DTE receptor que una ruta en particular en la red se encuentra congestionada. El DTE entonces puede relevar esta información hacia las capas superiores para su procesamiento. Nuevamente, dependiendo de la implementación de la tecnología, un mecanismo de control de flujo puede ser inicializado o la indicación de congestión puede ser simplemente ignorada.

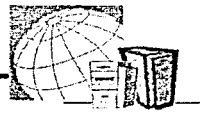
El bit de DE es utilizado para indicar que un frame tiene poca importancia con respecto a otros frames. El bit DE también es parte del campo de dirección en el encabezado de Frame Relay. Los dispositivos DTE pueden cambiar el valor del bit DE en un frame para indicar que el frame tiene poca importancia. Cuando la red se congestiona, los dispositivos DCE descartarán los frames cuyo bit DE se encuentre encendido antes de descartar aquellos que contengan dicho bit apagado. Esto reduce la posibilidad de que frames de importancia sean descartados por los dispositivos DCE en una red Frame Relay durante periodos de congestión.**PPP** (Protocolo Punto a Punto) originalmente surgió como un protocolo de encapsulación para transporte de tráfico **IP** (Internet Protocol) sobre circuitos punto a punto. PPP también estableció un estándar para la asignación y manejo de direcciones IP, encapsulación asíncrona (start/stop) y encapsulación síncrona orientada a bit; multiplexaje de protocolos de red, configuración del circuito, chequeo de calidad del circuito, detección de errores y opciones de negociación de direcciones de la capa de red y negociación de compresión de datos. PPP soporta estas funciones provisionando un extenso **LCP** (Protocolo de Control de Circuito) y una familia de **NCP** (Protocolos de Control de Red) que negocian parámetros opcionales de configuración y algunas otras facilidades. Adicionalmente a IP, PPP soporta otros protocolos incluyendo IPX de Novell y DECnet. En los siguientes párrafos describiremos los elementos básicos del protocolo y su funcionamiento.

Componentes de PPP

PPP provee un método de transporte de datagramas sobre circuitos seriales (enlaces WAN) punto a punto. PPP tiene tres principales componentes:

- Un método para encapsular datagramas sobre circuitos seriales – PPP utiliza **HDLC** (Control de Alto Nivel de Enlace de Datos) como base para encapsular datagramas sobre circuitos seriales punto a punto.

- LCP para establecer, configurar y probar la conexión a nivel de enlace de datos.



• Una familia de NCPs para establecer y configurar diferentes protocolos de la capa de red –PPP está diseñado para permitir el uso de múltiples protocolos de la capa de red de manera simultánea-.

El formato de frame de PPP aparece en la siguiente figura.

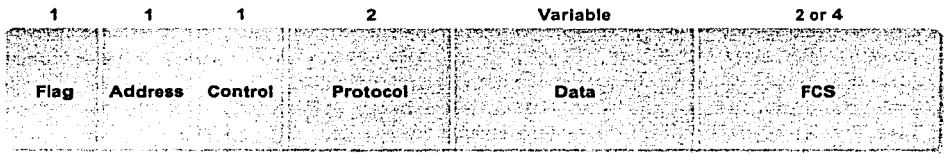


Figura 2.4.2.2 Formato del frame de PPP

Las siguientes descripciones resumen la utilidad de los campos del frame de PPP mostrado en la figura anterior:

Flag. Un byte que indica el principio o final de un frame. El campo flag consiste de una secuencia binaria como 01111110.

Address. Un byte que contiene la secuencia binaria 11111111, La dirección estándar del broadcast. PPP no asigna direcciones a estaciones individuales.

Control. Un byte que contiene la secuencia binaria 00000011, indica transmisión de datos en un frame sin secuencia. Una conexión no orientada a conexión (conectionless) similar a LLC.

Protocol. Dos bytes que identifican el protocolo encapsulado en el campo de información.

Data. Cero o más bytes que contienen al datagrama del protocolo especificado en el campo de protocolo. El máximo tamaño de frame es 1 500 bytes.

Frame Check Sequence (FCS). Normalmente 16 bits (2 bytes). Se pueden utilizar también 32 bits pero la finalidad es el chequeo de errores.

LCP puede negociar las modificaciones a la estructura estándar del frame de PPP.

Funcionamiento General de PPP

Para establecer la comunicación sobre un circuito punto a punto, el que origina de la llamada envía en primer lugar frames LCP para configurar y opcionalmente probar el enlace de datos en el circuito. Después de que el circuito se ha establecido y las facilidades opcionales han sido negociadas de acuerdo a los requerimientos de LCP, el que origina de la llamada envía frames NCP para escoger y configurar uno o más protocolos de la capa de red. Cuando cada uno de los protocolos escogidos han sido configurados, los paquetes de cada uno de ellos pueden ser enviados a través de la conexión que se ha establecido. El circuito permanecerá configurado para envío de información hasta que frames explícitos de LCP o NCP decidan cerrar la conexión, o hasta que algún evento externo (como la expiración de algún timer (contador) de inactividad o bien la intervención misma del usuario) ocurra.

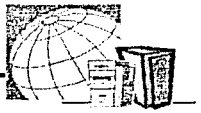
Funcionamiento de LCP

LCP como habíamos dicho es el encargado de proveer el método para establecer, configurar, mantener y cerrar la conexión PPP. Para poder hacer lo que se menciona, LCP tiene que pasar por las siguientes fases:

- Primero, el establecimiento y la configuración del circuito toman lugar. Antes de que cualquier tipo de datagrama de protocolos superiores puedan ser intercambiados, LCP debe abrir una conexión y negociar los parámetros de configuración del circuito. Esta fase se completa cuando un frame de **acknowledge** (reconocimiento) ha sido enviado y también recibido.

- Enseguida se determina la calidad del circuito. LCP permite una determinación optima de la calidad del circuito inmediatamente después de haber establecido el circuito. En esta fase, el circuito es probado para determinar si la calidad del mismo es suficiente para poder entonces utilizar los protocolos de la capa de red. Ciertamente esta fase es opcional. Sin embargo, LCP puede retrasar la transferencia de información de protocolos de red hasta que se complete la determinación de la calidad del circuito.

- En este punto, se efectúa la negociación de los protocolos de la capa de red. Después de que LCP ha determinado la calidad del circuito, los protocolos superiores pueden ser configurados de manera independiente por el NCP correspondiente y pueden también ser



utilizados y dejados de utilizar en cualquier momento. Si LCP cierra la conexión, éste informa a los protocolos de red para que tomen las medidas necesarias en los niveles superiores.

• Finalmente, el cierre del circuito toma lugar. LCP puede cerrar la conexión del circuito en cualquier momento. Esto será llevado a cabo usualmente a partir de una petición del usuario pero puede ocurrir también debido a un evento físico, como la pérdida de una señal o la expiración de un cierto timer.

Existen tres tipos de frames LCP. Frames de establecimiento de conexión, frames de terminación de conexión y frames de mantenimiento del circuito que son utilizados para saber en cualquier momento las características actuales del circuito y también para poder llevar a cabo las labores de administración del mismo.

Estos tres tipos de frames son utilizados para llevar a cabo cada una de las fases descritas para el LCP.

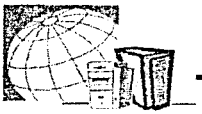
SDLC (Control de Enlace de Datos Síncrono) y sus derivaciones.

IBM desarrolló SDLC a mediados de los 70s para ser usado en sus ambientes **SNA** (Arquitectura de Sistemas de Red). SDLC fue el primer protocolo basado en una operación síncrona orientada a bit. Después de que IBM publicará en varios comités de estandarización su protocolo, la **ISO** (Organización Internacional para la Estandarización) lo modificó para crear el HDLC. La ITUT subsecuentemente modificó el HDLC para crear el **LAP** (Procedimiento para acceso al circuito) y el **LAPB** (Procedimiento para Acceso al Circuito, Balanceado). La IEEE modificó el HDLC para crear la especificación del 802.2. Todos estos protocolos han sido importantes dentro de su campo de acción, pero SDLC se mantiene como el protocolo principal para el transporte de SNA en la WAN.

Tipos de SDLC y sus topologías

SDLC soporta una variedad de tipos de circuitos y topologías. Puede ser utilizado con circuitos punto a punto o con multipuntos, utilizar transmisiones half-duplex y *full-duplex*, y también puede usarse en redes de conmutación de circuitos o redes de conmutación de paquetes.

SDLC identifica dos tipos de nodos de red: primarios y secundarios. Los nodos primarios controlan la operación de las demás estaciones, llamadas nodos secundarios. El primario se comunica con los secundarios utilizando un orden específico y los secundarios pueden transmitir si tienen datos de salida. El



primario también se encarga de levantar y cerrar los circuitos y administrarlos mientras se encuentren operacionales. Los nodos secundarios son controlados por el primario, lo cual significa que estos pueden enviar información si y solo si el primario les ha otorgado el permiso para hacerlo. Los nodos primarios y secundarios de SDLC pueden conectarse en cuatro configuraciones básicas.

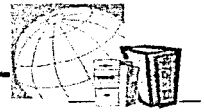
- **Punto a punto**. Comprende solo dos nodos, un primario y un secundario.

- **Multipunto**. Comprende un nodo primario y múltiples secundarios.

- ***Loop***. Consta de una topología de *loop*, con el primario conectado al primer y último nodo secundario. Los nodos secundarios intermedios pasan los mensajes a través de los demás secundarios tal como van siendo respondidos por el primario.

- **Hub go-ahead** (Concentrador Adelante). Consta de un canal de entrada y uno de salida. El primario utiliza el canal de salida para comunicarse con los secundarios. Los secundarios utilizan el de entrada para comunicarse con el primario. El canal de salida está encadenado hacia el primario a través de cada secundario.

Una red típica basada en SDLC se muestra en la figura 2.4.2.3. Tal y como se observa, un controlador de IBM en un site remoto se conecta a terminales tontas y a un anillo de *token ring*. En el site local, un *host* IBM se conecta a un Front-end processor (FEP) que también tiene conexiones locales al *token ring* local y a la red SNA. Los dos sites se conectan a través de una línea serial basada en SDLC de 56 Kbps.



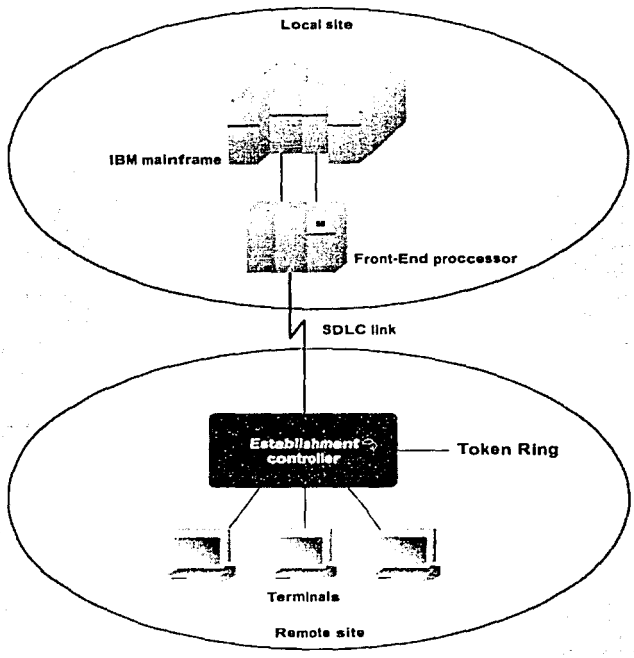


Figura 2.4.2.3 Una línea SDLC conecta un site local con el remoto sobre una línea serial.

Específicamente hablando del caso del IFE, se utiliza el protocolo HDLC en la WAN (conexiones punto a punto) ya que es el protocolo por omisión de las interfases seriales de los ruteadores que redIFE tiene instalados. A continuación se describirá de manera breve cuáles son las diferencias fundamentales entre el SDLC y el HDLC.

HDLC comparte el mismo formato de frame que SDLC y los campos de HDLC proporcionan las mismas funcionalidades que SDLC. También, como SDLC, HDLC soporta la operación de circuitos síncronos *full-duplex*.

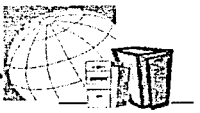
HDLC es diferente en cosas muy específicas como que cuenta con una opción para manejar un checksum de 32 bits. HDLC no soporta configuraciones tipo **loop** (lazo) tal y como lo hace SDLC.

Sin embargo, la mayor diferencia entre estos dos protocolos de transporte es que SDLC soporta un solo modo de transferencia, mientras que HDLC soporta tres:

- **NRM (Modo de Respuesta Normal).** Este modo de transferencia también es utilizado por SDLC. En este modo, los dispositivos secundarios no pueden comunicarse con los primarios sino hasta que estos les conceden el permiso para hacerlo.

- **ARM (Modo de Transferencia Asíncrona).** Este modo de transferencia permite a los dispositivos secundarios iniciar la comunicación con el primario sin necesidad de esperar a que éste se los permita.

- **ABM (Modo Asíncrono Balanceado)** ABM introduce el concepto de nodo combinado, en donde un nodo puede actuar como primario o secundario según la situación. Toda la comunicación ABM ocurre entre múltiples nodos combinados. En ambientes ABM, cualquier estación combinada puede inicializar la transferencia de datos sin tener que esperar el permiso de ninguna otra estación.



2.5 PROTOCOLOS RUTEABLES

Las redes se han convertido en una parte fundamental, se puede decir, la más importante de los sistemas de información de hoy. Forman la espina dorsal (backbone) para compartir información dentro de empresas, grupos empresariales y científicos.

La mayoría de estas redes fueron instaladas en la década de los 60s y 70s, cuando el diseño de red era el asunto de investigación más importante relacionado a la computación. Dio lugar a múltiples modelos de redes tales como tecnología de conmutación de paquetes, detección de colisiones en redes de área local, redes jerárquicas de la empresa, y muchas otras tecnologías.

Desde el inicio de 70s, otro aspecto de redes tendió a ser importante: protocolo en capas, que permite que las aplicaciones se comuniquen una con otra. Un rango completo de arquitecturas de modelos fue propuesto e implementado por varios equipos de investigadores y fabricantes de computadoras.

Dentro del conjunto de protocolos que sirven para establecer la comunicación entre *hosts* a través de una red de datos, es a lo que llamamos arquitectura de red. Cada arquitectura de red define capas que permiten dividir el proceso de comunicación en subprocesos. Entre las principales arquitecturas de red tenemos: AppleTalk, Novell IPX y TCP/IP.

Estas arquitecturas de red o conjunto de protocolos dada su implementación tienen la capacidad de ser ruteables. A continuación mencionaremos las características de estos:

2.5.1 AppleTalk

AppleTalk es un conjunto de protocolos desarrollado por Apple Computer a inicios de los años 80s, en conjunto con Macintosh computer. El propósito de AppleTalk fue el permitir a múltiples usuarios el compartir recursos, tales como, archivos e impresoras. Asimismo, fue una de las primeras implementaciones de un sistema de red cliente-servidor distribuido.

AppleTalk fue diseñado como una interfase de red transparente, es decir, la interacción entre la computadora cliente y el servidor de red requerían una mínima interacción del usuario. Actualmente la operación de los protocolos de AppleTalk es invisible para los usuarios finales, quien es solo ven los resultados de esta operación. Existen dos versiones de AppleTalk: AppleTalk Fase 1, AppleTalk Fase 2

AppleTalk Fase 1

Es la primera especificación que se realizó a inicios de los 80s, estrictamente para uso en grupos de trabajo locales.

AppleTalk Fase 2

Es la mejora a la implementación original, fue diseñada para uso en redes más complejas, soportando el interconectar redes *AppleTalk*.

En la figura 2.5.1 se muestran los protocolos de *AppleTalk* en conjunto con el modelo de referencia OSI.

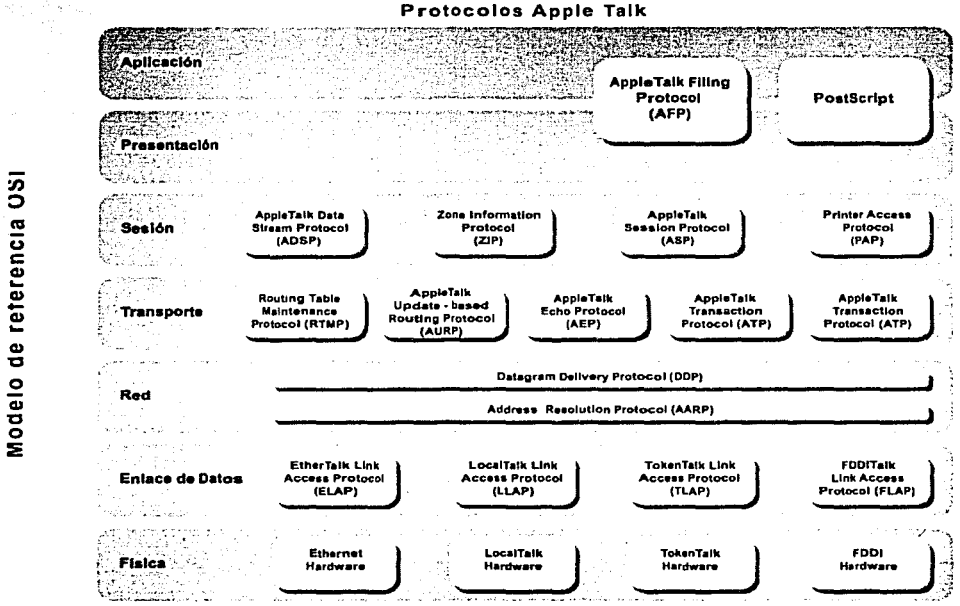
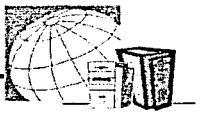


Figura 2.5.1 Protocolos *AppleTalk*

AppleTalk es uno de los protocolos que tiene mayores similitudes respecto al modelo OSI, ya que sus capas, protocolos y funciones están más delimitados.

Capa física y capa de enlace

AppleTalk fue diseñado para ser independiente a la capa de enlace, es decir, teóricamente puede correr sobre cualquier implementación de ésta. Apple



soporta una variedad de implementaciones, incluyendo *Ethernet*, *Token Ring*, *Fiber Distributed Data Interfase* (FDDI), y *LocalTalk* (interfaz de red implementada por Apple).

Capa de Red.
Direccionamiento.
AppleTalk utiliza direcciones para identificar y localizar los dispositivos de red y se lleva una administración similar a la que se lleva a cabo en protocolos como, TCP-IP o IPX. Estas direcciones las cuales son asignadas dinámicamente, se componen de tres elementos:

Número de red:
Un valor de 16 bits que identifica la red *AppleTalk*

Número de nodo:
Un valor de 8 bits que identifica un nodo *AppleTalk* que se encuentra en una red específica.

Número de socket:
Un valor de 8 bits que identifican un socket específico corriendo en un nodo de red.

Una de las características de *AppleTalk* es el direccionamiento dinámico de los dispositivos. Los nodos de *AppleTalk* son asignados dinámicamente cuando ellos son agregados a una red.

AppleTalk **Address-Resolution Protocol** (AARP) es un protocolo de capa de red, el cual asocia la dirección de red *AppleTalk*, con la dirección del *hardware*. Los servicios de AARP son utilizado por otros protocolos *AppleTalk*.

El **Datagram Delivery Protocol** (DDP) es el protocolo principal de la capa de red, este tiene dos funciones principales: transmisión y recepción de paquetes, es decir, provee el servicio no orientado a conexión de datagramas entre los sockets de *AppleTalk*.

Capa de Transporte
La capa de transporte implementa servicios confiables de transporte de datos que son transparentes para capas superiores. Las funciones de esta capa comúnmente son el control de flujo, multiplexaje, administración de circuitos virtuales, y verificación y recuperación de errores.

Las implementaciones que existen en la capa de transporte son:

- *Routing Table Maintenance Protocol (RTMP)*
- *Name-Binding Protocol (NBP)*
- *AppleTalk Update-Based Routing Protocol (AURP)*
- *AppleTalk Transaction Protocol (ATP)*
- *AppleTalk Echo Protocol (AEP)*

Capas Superiores

Las implementaciones de la capa de sesión, establecen, administran y determinan la comunicación entre las sesiones y las entidades de la capa de presentación. La comunicación entre sesiones consiste en la petición y respuesta de servicio que ocurre entre las aplicaciones localizadas en los diferentes dispositivos de red. La petición y respuesta son coordinados por los protocolos implementados en la capa de sesión. *AppleTalk* soporta diversos protocolos en esta capa:

- *AppleTalk* Data Stream Protocol (ADSP), Zone-Infomation Protocol (ZIP),
- *AppleTalk* Session Protocol (ASP), y Printer-Access Protocol (PAP).

El *AppleTalk* Filing Protocol (AFP) es una implementación de las capas de presentación y aplicación.

Los datagramas *AppleTalk* difieren según la versión que se utilice: *AppleTalk* Fase 1 o *AppleTalk* Fase 2, como se muestran en las Figuras 2.5.2 y 2.5.3

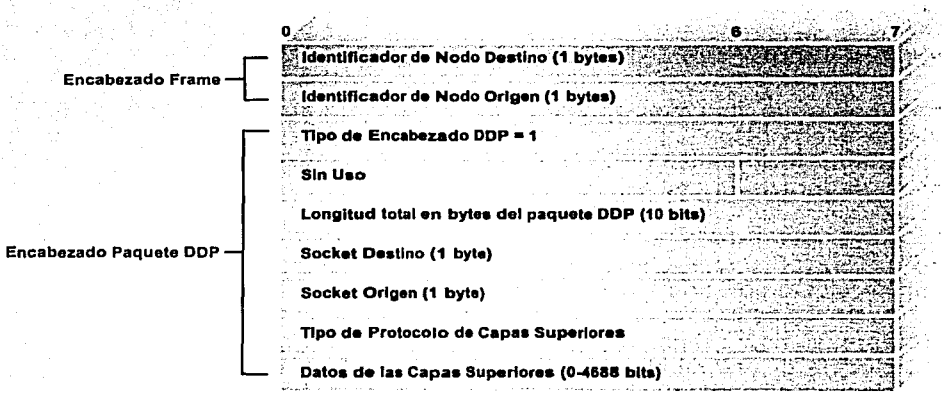


Figura 2.5.2 Datagrama *AppleTalk* Fase 1

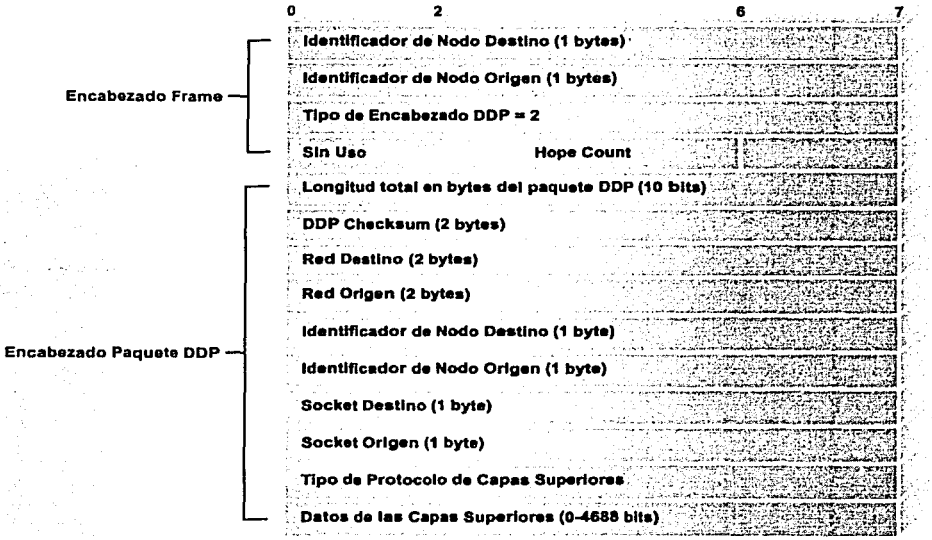


Figura 2.5.3 Datagrama *AppleTalk* Fase 2

HOPE COUNT = Número de dispositivos por los cuales el paquete ha pasado (4bits)

2.5.2 Novell IPX (Netware Protocols)

Netware es un sistema operativo de red (network operating system - NOS), fue creado por Novell Inc., y se introdujo al mercado a inicios de los 80s. Es utilizado principalmente para aplicaciones de redes de área local (LAN) en computadoras personales (PCs).

La mayor parte de la tecnología implementada por Netware fue derivada de Xerox Network System (Sistema de Red Xerox XNS), un sistema de red creado por Xerox Corporation a finales de los años 70s.

Netware, como un sistema operativo de red, especifica las 5 capas superiores del modelo de referencia OSI. En la figura 2.5.4 se muestran los protocolos de Netware y su relación con el modelo OSI.

Capa física y Capa de enlace.

El conjunto de protocolos de Netware soportan diversos protocolo de acceso al medio como son: *Ethernet* / IEEE 802.3, *Token Ring* / IEEE 802.5, Fiber Distributed Data Interface FDDI), y ARCnet.

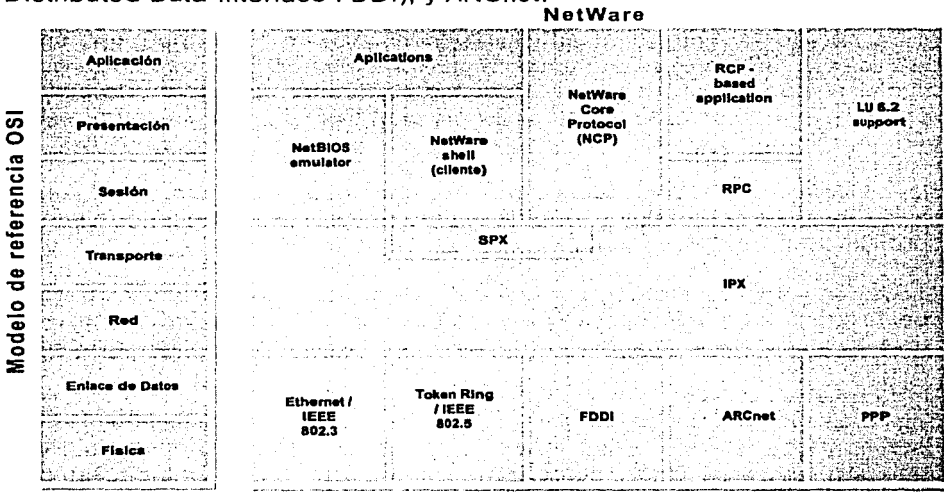


Figura 2.5.4 Protocolos Netware

Capa de Red

Internet Packet Exchange (IPX) es el protocolo original de Novell, utilizado para rutear paquetes a través de la red. IPX es un protocolo de red no orientado a conexión. En la figura 2.5.5 se muestra el paquete de IPX

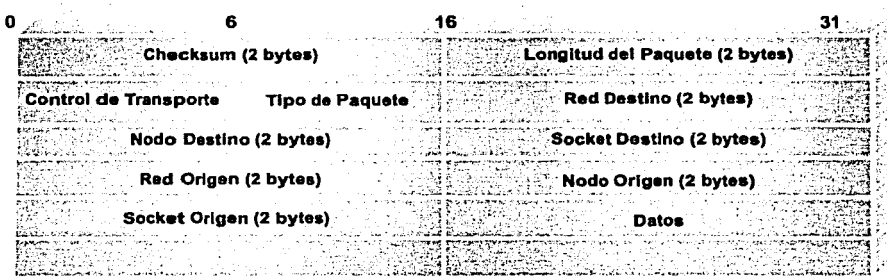
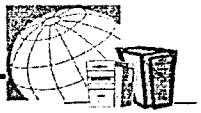


Figura 2.5.5 Datagrama IPX



IPX utiliza los servicios del protocolo distance-vector (Routing Information Protocol -RIP), o el protocolo de ruteo link-state (NetWare Link State Protocol– NLSP).

El direccionamiento IPX debe de ser único. Estas direcciones son representados en forma hexadecimal y consisten en dos partes: un número de red y un número de nodo. El número de red IPX, es asignado por el administrador de red y tiene una longitud de 32 bits. El número de nodo, el cual generalmente es la dirección de *hardware* (Media Access Control - MAC) tiene una longitud de 48 bits.

Novell NetWare IPX soporta diversos esquemas de encapsulamiento en una misma interfaz del ruteador. Los esquemas de encapsulamiento que soporta son: Novell Propietary, 802.3, *Ethernet* Version 2, SNAP.

El Service Advertisement Protocol (SAP), es el protocolo de IPX a través del cual los dispositivos de red, como servidores de archivos, de impresión, entre otras, publican o anuncian sus direcciones y el servicio que están ofreciendo.

Capa de Transporte.
Sequenced Packet Exchange (SPX) es el protocolo mas utilizado en esta capa. Este protocolo es confiable debido a que es orientado a conexión. Novell también ofrece soporte de Internet Protocol (IP), en la forma de *User* Datagram Protocol (UDP). Los datagramas IPX son encapsulados dentro de los encabezados de UDP/IP para ser enviados a través de una red basada en IP.

Protocolo de Capas Superiores.
NetWare soporta una variedad amplia de protocolos en las capas superiores, incluyendo, NetWare *Shell*, NetWare Remote Procedure Call, NetWare Core Protocol, y Network Basic Input/Output System.

2.5.3 TCP/IP

El conjunto de protocolos de Internet son el sistema abierto mas popular, porque puede utilizarse para comunicar a través de cualquier conjunto de redes interconectadas y son igualmente utilizados para las comunicaciones LAN y WAN. Esta arquitectura tiene su origen en el Gobierno de los Estados Unidos de Norte América, concretamente en su Departamento de Defensa (DoD). La DARPA (Defense Advanced Research Projects) comenzó a trabajar con una internet (red de redes) a mediados de los años 70s.

Las dos razones principales por las que el departamento de defensa creó el estándar de los protocolos de comunicación para una arquitectura fueron las siguientes:

- Una rápida proliferación de las computadoras y otros elementos de procesamiento de señales dentro de la milicia y la necesidad de conectar equipos de diferentes fabricantes.

- El creciente uso de redes de comunicaciones en la milicia y la necesidad de una variedad de tecnologías de interconexión.

TCP/IP es una colección de protocolos. Debe su nombre a sus dos protocolos más conocidos; TCP o Transmission Control Protocol, corresponde a la capa 4 del modelo OSI (la capa de transporte) y ofrece transmisión confiable de datos. IP o Internet Protocol trabaja en la capa 3 del modelo OSI (capa de enlace de red) y ofrece el servicio de datagramas sin conexión.

TCP/IP esta estructurado en cuatro capas, cada una define funciones específicas que se llevan a cabo en el proceso de comunicación. En la figura 2.5.6 podemos observar el modelo de referencia OSI vs. la familia de protocolos TCP/IP.

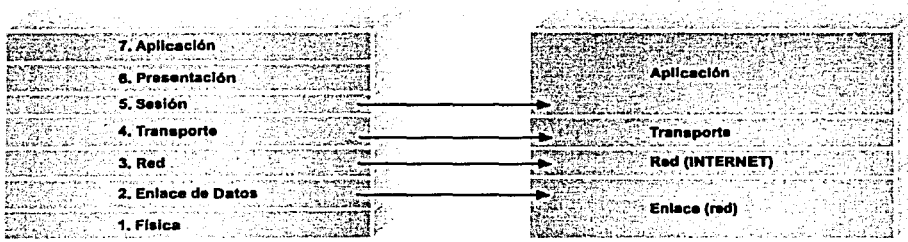
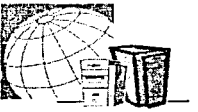


Figura –2.5.6 Modelo de referencia OSI y stack de protocolos TCP/IP.



TCP/IP es un protocolo definido principalmente por las siguientes capas: Capa de Enlace(red), Capa de Red(Internet), Capa de Transporte y Capa de Aplicación

TCP/IP se refiere a una gran familia de servicios y protocolos. Estos protocolos aparecen en la siguiente figura 2.5.7, la cual muestra que IP y los protocolos de los niveles superiores se pueden implantar en diversos tipos de redes. *Ethernet*, FDDI, etc.

A continuación se muestra una lista con los nombres de los protocolos cuyos acrónimos aparecen en la figura 2.5.7 y el servicio que ofrecen.

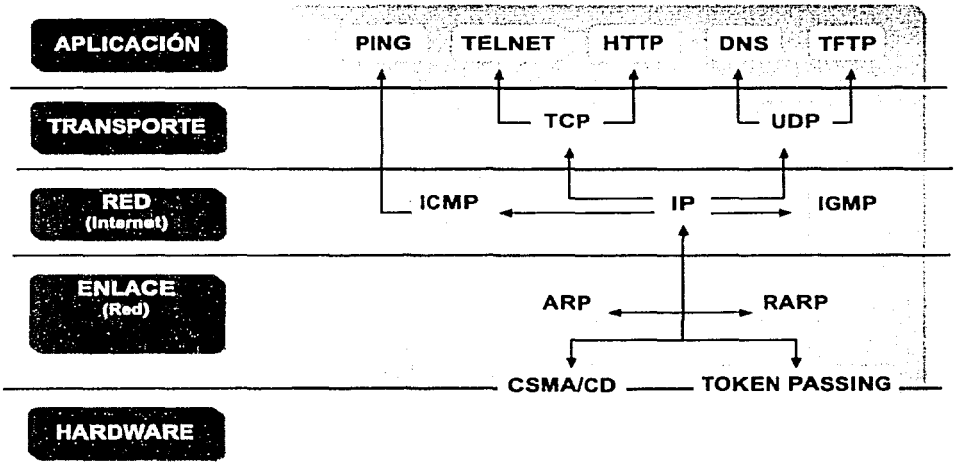
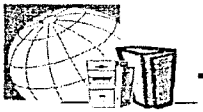


Figura 2.5.7 Familia de servicios y protocolos.

Capa de enlace

- *ARP (Address Resolution Protocol)*
  Mapea una dirección IP a su dirección *Ethernet* asociada.
- *RARP (Reverse ARP)*
  Mapea una dirección *Ethernet* a su dirección IP asociada.



Capa de red

- *IP (Internet Protocol)*
  Define la unidad básica de encapsulamiento de TCP/IP: Datagrama
  Es No orientado a conexión
  Es no confiable
  Su función es el ruteo de datagramas y la fragmentación de estos.

- *ICMP (Internet Control Message Protocol)*
  Usado por lo gateways y *hosts* para evaluar las condiciones de funcionamiento de los servicios IP.
  Es un protocolo dependiente de IP. Los mensajes ICMP van en el campo de datos del Datagrama. Su función es el envió de mensajes de control de errores entre ruteadores y/o *hosts*.

- *IGMP (Internet Group Multicasting Protocol)*
  Es un protocolo dependiente de IP. Los mensajes IGMP van en el campo de datos del Datagrama, siendo su función, la administración de grupos de multicast: creación de grupos transitorios, ingreso o retiro de un grupo, confirmación de estancia en un grupo.

Capa de transporte

- *TCP (Transmission Control Protocol)*
  Protocolo orientado a la Conexión con acuse de recibo.
  Es un protocolo orientado a conexión, por lo tanto es confiable, usado por aplicaciones que requieren seguridad sobre rapidez en la entrega de datagramas. Siendo su función el transporte de segmentos entre *hosts* a nivel aplicación.

- *UDP (User Datagram Protocol)*
  Es un protocolo no orientado a conexión, por lo tanto no confiable, usado por aplicaciones que requieren rapidez sobre seguridad en la entrega de datagramas. Siendo su función el transporte de mensajes entre *hosts* a nivel aplicación.

Capa de aplicación

- *SMTP (Simple Mail Transfer Protocol)*
  Envío y recepción de correo.

- *FTP (File Transfer Protocol)*
  Intercambio de archivos completos.

- *TELNET (Telecommunications Network)*
  Terminal virtual para acceso interactivo a servidores remotos.

- *NFS (Network File System)*
  Sistemas de Archivos Distribuidos.

- *SNMP (Simple Network Management Protocol)*
  Servicios de Administración Centralizada de Sistemas Remotos.

El Internet Protocol (IP) es un protocolo de capa 3 que contiene la información de direccionamiento y alguna información de control que permite el ruteo de paquetes. El Internet Protocol, esta definido por el RFC 791, y es el corazón de la capa de Red (Internet). IP provee un esquema de direccionamiento conocido como IP Address o dirección lógica. Tiene el propósito de conocer la dirección a la cual se desea enviar u obtener información.

La analogía entre una red física y una Internet TCP/IP es muy fuerte. En una red física, la unidad de transferencia es un Frame que contiene un encabezado y datos, donde el encabezado proporciona información tal como las direcciones fuente y destino (físicas). La Internet le llama datagrama de Internet a su unidad básica de transferencia, a la que frecuentemente se le llama datagrama IP o simplemente datagrama. Al igual que un Frame típico de una red física, un datagrama se divide en áreas del encabezado y de datos. El encabezado del datagrama contiene las direcciones fuente y destino y un campo de tipo que identifica el contenido del datagrama. La diferencia, por supuesto, es que el encabezado del datagrama contiene direcciones IP mientras que el encabezado de un Frame contiene direcciones físicas. La figura 2.5.8 muestra la forma general de un datagrama.

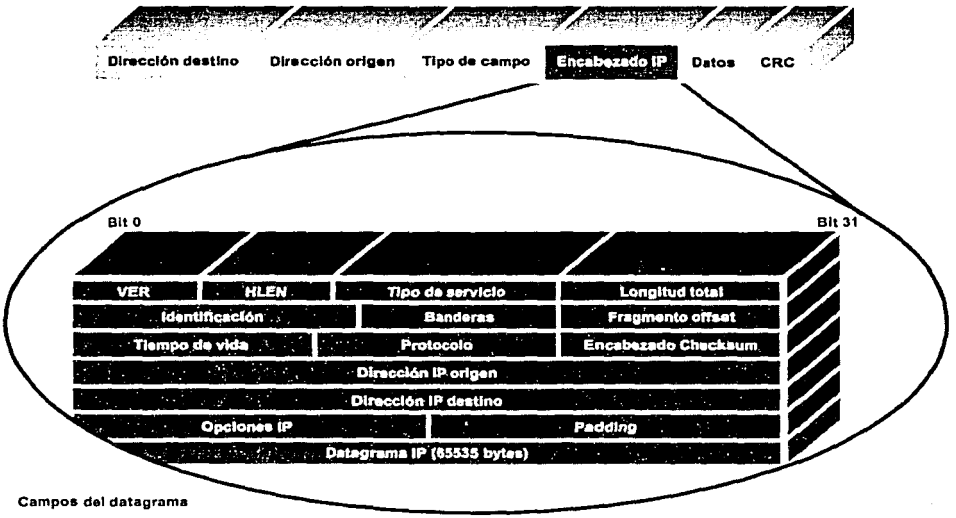


Figura 2.5.7.1 Campos del datagrama.

Los campos relevantes de la porción de la cabecera de IP son:

Versión, se está utilizando la versión 4 lo que indica que el direccionamiento de IP es de 32 bits.

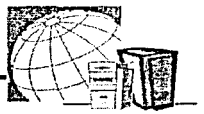
Identificación, en caso de ser fragmentado algún paquete entre los puntos intermedios el mismo debe ser reensamblado y se usa este campo para identificar información del mismo.

Protocolo, tipo de protocolo que usarán las capas superiores.

Checksum, método de verificar la integridad de la cabecera.

Dirección IP fuente y destino, dirección IP de 4 bytes o su equivalente en bits (32).

Tamaño del Datagrama, MTU de la Red y Fragmentación.



Como en cualquier otro protocolo de red, el esquema de direccionamiento IP es integral al proceso de enrutamiento a través de la red.

Una dirección IP esta compuesta de 4 bytes (32 bits) y esta dividida en dos partes, los bits más significativos (MSBs) identifican una RED en particular y los demás bits especifican un NODO perteneciente a esa red.

Estos 32 bits de dirección IP se escriben normalmente como cuatro números decimales, en el rango de 0 a 255, separados por un punto, uno para cada byte de dirección.

Se expresa en formato X.X.X.X
El máximo valor para cada octeto es de 255
Por ejemplo 192.100.180.15

Para aprovechar de manera más eficiente el espacio de direccionamiento IP y ajustar el tamaño de las redes a las necesidades individuales de cada entidad, el InterNIC (Organismo que administraba el direccionamiento en Internet) identificó las redes de Internet en cinco clases de direccionamiento, Clase A, Clase B, Clase C, Clase D, Clase E.

Cada red Clase A agrupa alrededor de 16,000,000 direcciones únicas, la clase B agrupa aproximadamente 65,000, y la clase C solo agrupa 254 direcciones diferentes.

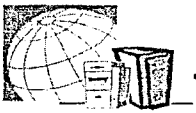
La Clase a la que pertenece una dirección IP define cuantos de los 32 bits deberán ser interpretados como dirección de Red y cuantos como dirección de Nodo.

Clase A	R.N.N.N	8 bits red - 24 bits nodo
Clase B	R.R.N.N	16 bits red - 16 bits nodo
Clase C	R.R.R.N	24 bits red - 8 bits nodo
Clase D	Multicast Group ID	32 bits
Clase E	Reservada	

R= Red
N= Nodo

Algunas restricciones en cuanto al uso de las direcciones IP son:

- Los nodos deben tener dirección de nodo diferente a la CERO (puros bits en cero).
- La dirección de nodo con puros unos se reserva para 'broadcasts'.



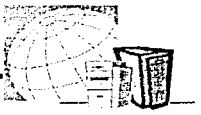
En ocasiones tenemos que dividir una red grande en varias pequeñas para:

- Reducción de tráfico.
- Optimizar performance.
- Simplificar la administración.

Para esto se hace uso de subredes, que no son otra cosa más que una extensión a la dirección de Red. Para hacer la extensión se utilizan la máscara de red (Netmask).

En general, los protocolos ruteables también son referenciados como protocolos de red o arquitectura de red. Estos protocolos de red llevan a cabo una variedad de funciones para la comunicación de aplicaciones entre un dispositivo origen y otro destino. Los protocolos de red se llevan a cabo dentro de las capas superiores del modelo de referencia OSI; capa de transporte, capa de sesión, capa de presentación, capa de aplicación.

Es muy común la confusión entre protocolos de ruteo y protocolos ruteables. Protocolos ruteables son aquellos protocolos que son ruteados sobre una red. Ejemplos de estos protocolos como lo vimos son Novell Netware, *AppleTalk* y TCP/IP. Por otro lado, los protocolos de Ruteo, son aquellos que implementan algoritmos de ruteo. Ejemplos de estos protocolos son: Interior Gateway Routing Protocol (IGRP), Border Gateway Protocol (BGP), Routing Information Protocol (RIP).



2.6 MODELO ISO DE ADMINISTRACIÓN DE REDES

Una red de cómputo es un conjunto de dispositivos y enlaces que conforman una infraestructura necesaria para la transferencia de datos entre las computadoras conectadas; permite que los usuarios que se encuentran en diferentes lugares puedan compartir y tener acceso a recursos de computadoras ubicadas en lugares remotos, desde la oficina contigua o desde la sucursal que se encuentra en otro estado de la república.

Todos los días las personas hacen uso de las redes de cómputo y nunca dan importancia a los aspectos que hacen posible su funcionamiento. Un ejemplo son los cajeros automáticos; permiten a los usuarios hacer consultas de sus saldos, retirar efectivo u otras operaciones sin importar el lugar geográfico donde se encuentren.

Al interconectar un conjunto de computadoras en una red de datos para compartir información, las empresas e instituciones obtienen un mejor control, manejo y acceso a la información; se vuelven más productivas y eficientes.

Papel del Ingeniero en Redes

El correcto funcionamiento de una red de cómputo es crítico al convertirse en una herramienta indispensable para la empresa, generalmente un grupo de ingenieros de redes tienen la responsabilidad de instalar, mantener y atender los problemas relacionados con la red de cómputo a su cargo. Para este conjunto de expertos, la solución a un problema de red puede ser tan simple como aclarar las dudas de algún usuario que apenas comienza a hacer uso de los servicios de red, o tan complicada como identificar y reemplazar un equipo de comunicaciones que presenta fallas.

Es lógico que al presentar una expansión la red de cómputo, se incrementan proporcionalmente el número y la cantidad de los problemas potenciales, haciendo el trabajo del ingeniero de redes más complejo en virtud de que debe contar con una mayor cantidad de información técnica acerca de la red. El manejo de este volumen de información puede volverse muy complicado en poco tiempo, de acuerdo a los cambios o crecimientos que se tengan que hacer en la red. Sobretodo, si no se cuenta con una administración de la red correctamente organizada y sistematizada. El objetivo de la administración de redes es ayudar al ingeniero de redes a realizar su trabajo correctamente, no importando la complejidad de la red y asegurar que la transmisión de los datos a través de la red, sea con la mayor eficiencia y transparente para el usuario (este es el mayor reto al implementar una red de cómputo).

Implementación de una red de datos

Instalar una red de datos no implica que automáticamente todos los usuarios van a poder compartir recursos e información. El primer objetivo de una red de datos es satisfacer las necesidades de comunicación y transferencia de información de una organización. Esto requiere de una adecuada planificación, se debe realizar un análisis de los diferentes tipos de usuarios y sus necesidades específicas de comunicación, así como la interacción entre las diferentes áreas que componen la organización. El diseño puede contemplar la adición de nuevo equipo para dar acceso a la red a nuevos usuarios u oficinas, proporcionar redundancia de acceso a nodos de carácter crítico, o incrementar el ancho de banda de los enlaces de comunicación, dependiendo de las aplicaciones que utilizan los usuarios y los protocolos de comunicaciones.

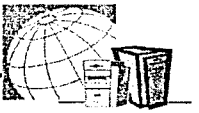
El ingeniero de redes encargado de la implementación de una red de datos debe cubrir cada una de las siguientes actividades:

1 Diseño y construcción de la red.
2 Mantenimiento.
3 Expansión.
4 Optimización.
5 Monitoreo y Administración
6 Atención y solución de problemas.

Una de las primeras responsabilidades del ingeniero es determinar el equipo y esquemas de interconexión requeridos para la implementación de la red, basándose específicamente en dos tipos de tecnologías utilizadas para proporcionar la conectividad necesaria: tecnologías para redes de área local (LAN) y tecnologías para redes de área amplia (WAN).

Una vez instalada la red de cómputo, es necesario llevar a cabo el mantenimiento continuo a toda la infraestructura, independientemente de lo bien que se haya diseñado. Las versiones de sistema operativo de los equipos se deben actualizar regularmente para cubrir las nuevas necesidades en los servicios de red, de acuerdo al cambios en las aplicaciones de los usuarios. Además, ningún equipo es infalible y en cualquier momento puede suceder algún tipo de acontecimiento que afecté el servicio de red de los usuarios.

La expansión de cualquier red es algo inevitable, las aplicaciones día con día se van mejorando, demandando más recursos en procesamiento y velocidad de transmisión. Conforme se van automatizando los procesos de la organización, nuevas áreas van surgiendo y nuevos usuarios deben ingresar a la red. Si un diseño, desde un inicio, no contempla la expansión de la red,



puede ser necesario el rediseño completo de la red para dar servicio a los nuevos usuarios; esto es costoso y difícilmente se puede llevar a cabo en un corto o mediano plazo.

El ingeniero de redes también debe tener dentro de sus actividades cotidianas la optimización de la red. Generalmente, las redes de cómputo de las organizaciones cuentan con cientos de equipos interconectados, cada uno con sus propias particularidades, obviamente todos tienen que trabajar en armonía; es responsabilidad del ingeniero de red asegurar que cada uno de los equipos contribuya a un óptimo desempeño de la red de comunicaciones en su conjunto, independientemente de la diversidad de marcas y modelos de los equipos.

En la medida que se implemente un buen diseño y que se lleve a cabo la correcta ejecución de los pasos anteriores, se disminuirán el número de problemas que se puedan presentar en la red; pero de cualquier manera se deberá contar con los mecanismos necesarios para la atención oportuna de fallas y su solución inmediata: una red de datos debe estar en operación el mayor tiempo posible, en caso de presentarse una falla, esta debe durar el menor tiempo posible.

Arquitectura de administración de redes

La mayoría de las arquitecturas de administración de redes hacen uso de la misma estructura básica y del conjunto de relaciones entre los elementos que la conforman. La figura 2.6.1 muestra las entidades que conforman la arquitectura típica de administración de redes.

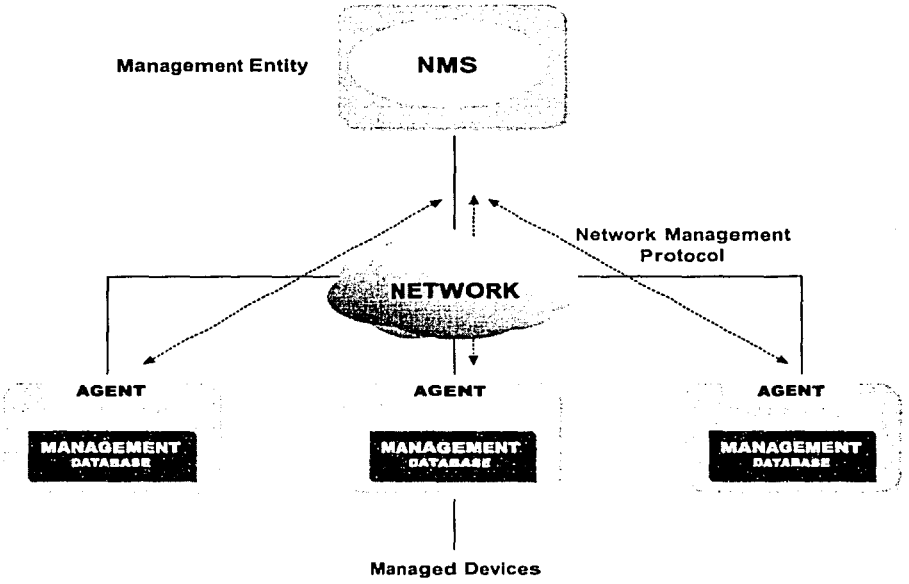
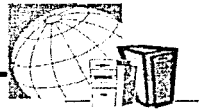


Figura 2.6.1 Componentes de la arquitectura de administración de redes.

• Dispositivos. Los dispositivos (Managed Devices) en una arquitectura de administración de redes pueden ser de diversos tipos: computadoras personales, impresoras, concentradores, switches, ruteadores, etc. Todo aquel equipo que sea crítico para el funcionamiento de la red y sus servicios debe ser administrado. Todo equipo susceptible de ser administrado debe contar con un agente (agent) y una base de datos de administración (management database). El agente es un conjunto de programas que reside en el dispositivo encargados de administrar y controlar la información contenida en la base de datos de administración, que es entregada al sistema de administración de red de forma regular o cuando se presenta algún evento o alarma. La base de datos de administración contiene información de carácter operacional e histórica del dispositivo, cada uno de los datos se conocen con el nombre de MIBs (Management Information Bases, Unidad básica de información de administración).



- Sistema de administración de red o **NMS** (Network Management System). También conocidos como **Management Entities** (Entidades de Administración) son los encargados de hacer las consultas a los agentes acerca de las variables y parámetros operacionales de los equipos contenidos en las bases de datos de administración. Los sistemas de administración, en general, son las aplicaciones con las cuales interactúa el operador o ingeniero de redes mediante las cuales puede llevar a cabo el monitoreo y la administración de la red.

- Protocolo de administración de red o **NMP** (Network Management Protocol). Estos protocolos son un conjunto de reglas y algoritmos perfectamente definidos mediante los cuales interactúan el sistema de administración y los agentes para el intercambio de información. Uno de los protocolos más utilizados es SNMP, aunque existen otros como CMIP y RMON.

- Los proxies son entidades que tienen como función controlar el acceso a ciertos agentes que no pueden ser consultados directamente por el sistema de administración de red. Se utilizan generalmente cuando la organización cuenta con políticas de seguridad para la restricción de acceso a la información de ciertos equipos, o cuando se desea distribuir la carga del sistema de administración de red y minimizar el tráfico originado por la comunicación entre NMS y agentes.

Desde el punto de vista de la arquitectura Cliente-Servidor, el agente de los dispositivos cumple con la parte del servidor al controlar y administrar las MIBs; su contraparte, el sistema de administración, es el cliente dentro de la arquitectura, ya que se encarga de hacer las peticiones a los agentes de acuerdo a las necesidades de los usuarios.

Actividades de la administración de redes

Las organizaciones invierten importantes cantidades de tiempo y dinero para implementar redes grandes y complejas. Es preferible que en vez de dedicar varios ingenieros de redes únicamente al mantenimiento de la infraestructura, el sistema de administración de red cubra la mayor parte de las actividades que en determinado momento pueden ser automatizadas. De esta manera, los ingenieros de redes pueden dedicar mayor parte del tiempo al desarrollo y expansión de la red.

Se vuelve necesario que los sistemas de administración puedan servir como un gran apoyo en la realización de las actividades necesarias para el buen funcionamiento de las redes. La Organización Internacional de Estándares o **ISO** (International Organization of Standars) ha contribuido a estandarizar

las actividades de la administración de redes mediante el Modelo ISO de Administración de Redes, el cual se compone de cinco áreas funcionales en las cuales se engloban cada una de las funciones que deben cumplir los ingenieros de redes al igual que los sistemas de administración. Las áreas funcionales son:

- Administración del Desempeño (Performance Management)
- Administración de las Configuraciones (Configuration Management)
- Administración del uso de los Recursos (Accounting Management)
- Administración de las Fallas (Fault Management)
- Administración de la Seguridad (Security Management)

2.6.1. Administración del Desempeño

El objetivo de la administración del desempeño es medir los diferentes parámetros de desempeño (valga la redundancia) de una red y tenerlos a la disposición en el momento en que se requieran con el fin de mantener del desempeño global y particular de la red en los niveles aceptables.

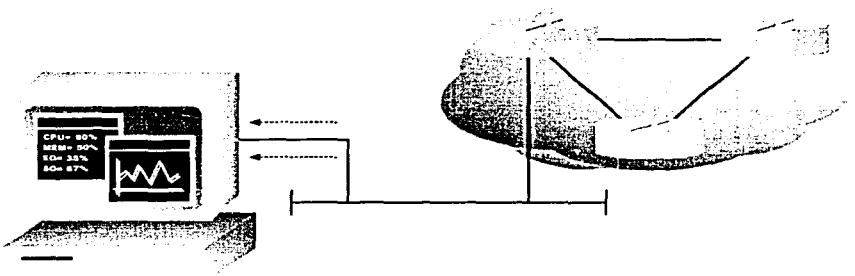
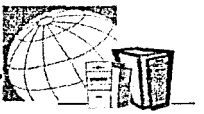


Figura 2.6.1.1 Administración del Desempeño.

Una red de datos es como una autopista en la cual la información viaja a través de medios de comunicación en la organización. Y así como una autopista se puede congestionar, una red de cómputo se puede saturar a causa de la demanda de uso por parte de los usuarios. Tanto los equipos de comunicaciones pueden llegar al nivel máximo de carga en procesamiento y recursos, como los enlaces pueden llegar a presentar una saturación que evidentemente afectará el desempeño de la red. Si esto llega a suceder, el concepto de transparencia de la red hacia los usuarios se pierde completamente.



La administración del desempeño debe estar orientada a mantener la disponibilidad de los servicios de red a todos los usuarios con un óptimo desempeño. Esto se debe hacer mediante:

- El monitoreo de las tasas de utilización y errores generados en toda la infraestructura de comunicaciones y servicios de red.

- Asegurar que la capacidad de los equipos y enlaces no rebase los niveles permitidos para mantener el nivel de servicio.

Para llevar a cabo esto, es necesario seguir cuatro pasos:

1. Obtener y almacenar los valores de los parámetros de utilización de los equipos y enlaces.
2. Llevar a cabo un análisis sobre los datos recolectados para identificar los valores máximos de utilización y operación.
3. Definir umbrales de operación aceptables.
4. Hacer simulaciones para determinar la forma en que la red puede ser configurada y modificada para maximizar el desempeño.

Determinar la utilización de un dispositivo no es una tarea sencilla. Cada equipo o elemento de la red puede tener diferentes características para representar los niveles de utilización y sus diferentes valores operacionales. Corresponde al ingeniero de redes, aplicar las fórmulas correspondientes para obtener los datos necesarios y aplicar sus conocimientos sobre comunicaciones de datos y sus diferentes elementos.

Los datos recolectados acerca de las variables operacionales de los equipos se deben almacenar en una base de datos que permita utilizarlos posteriormente para llevar a cabo un análisis sobre ellos. Es necesario contar con datos históricos acerca del desempeño de una red para representarlos en gráficas y poder identificar las tendencias del comportamiento de la red. De igual manera es conveniente contar con herramientas que permitan una graficación en tiempo real de los parámetros de utilización de equipos y enlaces con el fin de identificar problemas que únicamente se presenten en ciertos momentos y no puedan observarse mediante los datos históricos.

Una vez que ya se han revisado los niveles de utilización de la infraestructura, es necesario establecer umbrales de desempeño apropiados; es decir, establecer máximos (principalmente) y mínimos (si es necesario), con el objetivo de poder identificar síntomas de una posible falla antes de que se presente. Esto puede ser implementado mediante el sistema de administración y la generación automática de alarmas.

Es necesario simular los diferentes escenarios que se pueden tener en una red de cómputo al variar de forma controlada, la utilización de todos los componentes de la infraestructura, para ello se pueden desarrollar o adquirir herramientas como los generadores de tráfico y analizadores de protocolos.

2.6.2 Administración de las Configuraciones

El objetivo de la administración de las configuraciones se basa en el monitoreo regular de la composición de la red, así como de las configuraciones, sistemas operativos y aplicaciones adicionales de los dispositivos y equipos de cómputo de carácter crítico, tanto a nivel *hardware* como *software*.

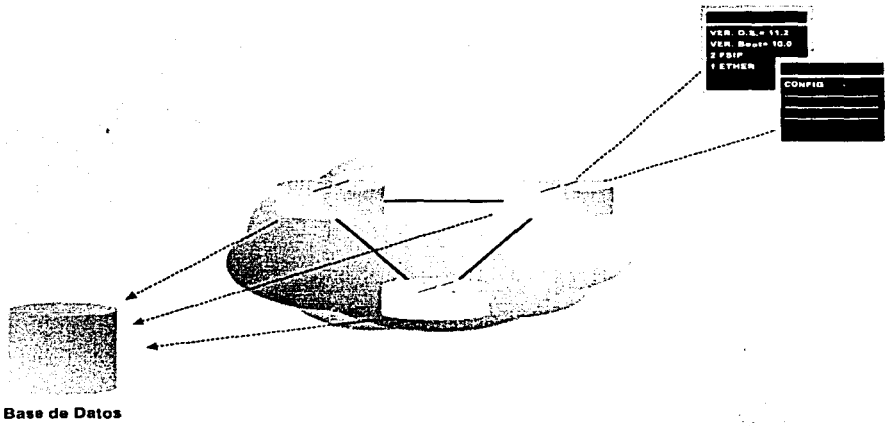
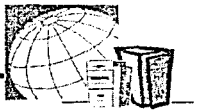


Figura 2.6.2.1 Administración de Configuraciones.

Mediante la recolección de la información acerca de las configuraciones de la infraestructura de la red, se puede configurar los equipos, almacenar la información, mantener el inventario de los equipos y generar reportes con los datos almacenados.

Esta actividad ayuda al ingeniero de redes a tener un mayor control sobre los dispositivos de la red y un acceso rápido a las configuraciones, haciendo más sencillo el proceso de actualización de versiones y una rápida toma de decisiones en aspectos económicos.

La administración de configuraciones se recomienda llevar a cabo mediante las siguiente actividades:



1 Obtener información de los equipos que conforman la infraestructura de la red. Si esta actividad no se lleva a cabo o no se atiende de forma correcta, el ingeniero de redes desperdiciará tiempo valioso en solución de un problema que pudo haberse ocasionado por un error en la configuración del equipo involucrado. La información puede ser recolectada de forma manual o automática mediante el sistema de administración de red.
2 Usar la información para modificar la configuración de los equipos. En muchas ocasiones, las configuraciones de los equipos se deben modificar continuamente, por ello es conveniente llevar un seguimiento de los cambios efectuados y utilizar los datos para modificar las configuraciones, ya sea de forma manual o automática. En muchas ocasiones se puede contar con herramientas que permitan la actualización de las configuraciones de varios equipos al mismo tiempo, o corregir listas de acceso mediante la información recolectada.
3 Almacenar la información, mantener y actualizar el inventario de los equipos y aplicaciones para producir reportes. Esta es una de las actividades más complejas y necesarias en virtud de que de esto depende la inversión hecha por la empresa en la infraestructura. Los reportes pueden ayudar a dimensionar de forma precisa el aprovechamiento de los equipos de cómputo y comunicaciones a largo plazo.

2.6.3 Administración del uso de los Recursos

El objetivo de la administración del uso de los recursos es medir y contabilizar los parámetros de utilización de la red para poder regular uso a los usuarios o grupos de usuarios, de los diversos servicios disponibles.

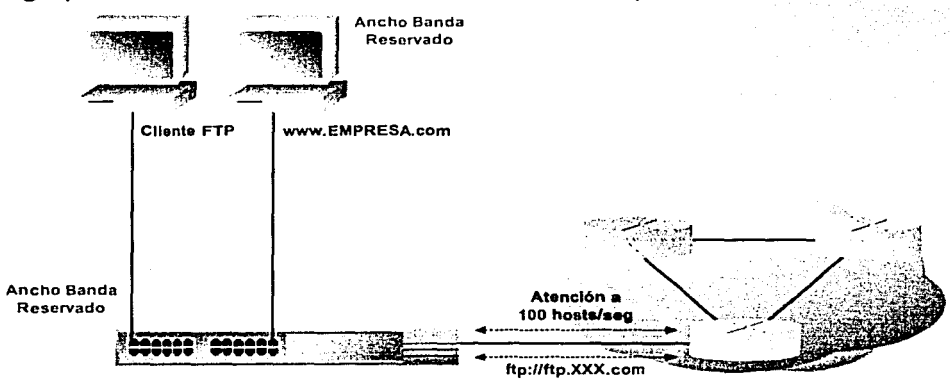
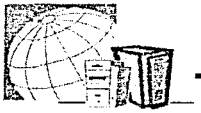


Figura 2.6.3.1 Administración del uso de los Recursos.



Es necesario medir el uso de los recursos de la red por parte de los usuarios con el fin de establecer métricas, cuotas, determinar costos de uso y en un casos específicos, facturar el servicio brindado. Para llevar a cabo el proceso de administración del uso de los recursos, es conveniente:

1. Obtener los datos acerca del uso de los recursos.
2. Ajustar los parámetros para especificar los diferentes niveles de servicio: por usuario y por grupo.
3. Generar reportes periódicos en base a los datos obtenidos.

Los datos del uso de la red se pueden obtener mediante los sistemas de administración o las propias herramientas con que cuentan las aplicaciones o dispositivos para llevar la contabilidad del uso de los recursos de la red. Cuando hablamos de recursos, el término se refiere a todo aquel componente de la infraestructura del cual hacen uso los usuarios y las aplicaciones. En algunas ocasiones es necesario utilizar la ingeniería de tráfico para obtener información acerca del uso del ancho de banda, ya sea por las aplicaciones o por un conjunto de usuarios.

Una vez que se hayan obtenido los datos para determinar el uso de los recursos, es necesario hacer un análisis de necesidades que permitan identificar prioridades entre usuarios o grupos de estos, con el fin de establecer métricas de uso de cada uno de los servicios. En base a la ingeniería de tráfico se pueden llevar acabo implementaciones de Calidad de Servicio (Quality of Service) con el fin de reservar recursos, principalmente ancho de banda, a los diferentes usuarios o aplicaciones en base a la criticidad de cada una de ellas.

La generación de reportes y/o facturas para justificar las restricciones o cobros que se deberán imponer a los usuarios de la red, existen varios productos que permiten obtener los reportes de una manera sencilla y que se pueden complementar al sistema de administración de red con el fin de automatizar este proceso en la medida de lo posible.

2.6.4 Administración de las Fallas

El objetivo de la administración de fallas es detectar cualquier problema que se presente, registrarlo en bitácoras, notificar a los usuarios afectados y (si es posible) darle solución de forma automática para mantener la red en operación y con un óptimo desempeño.

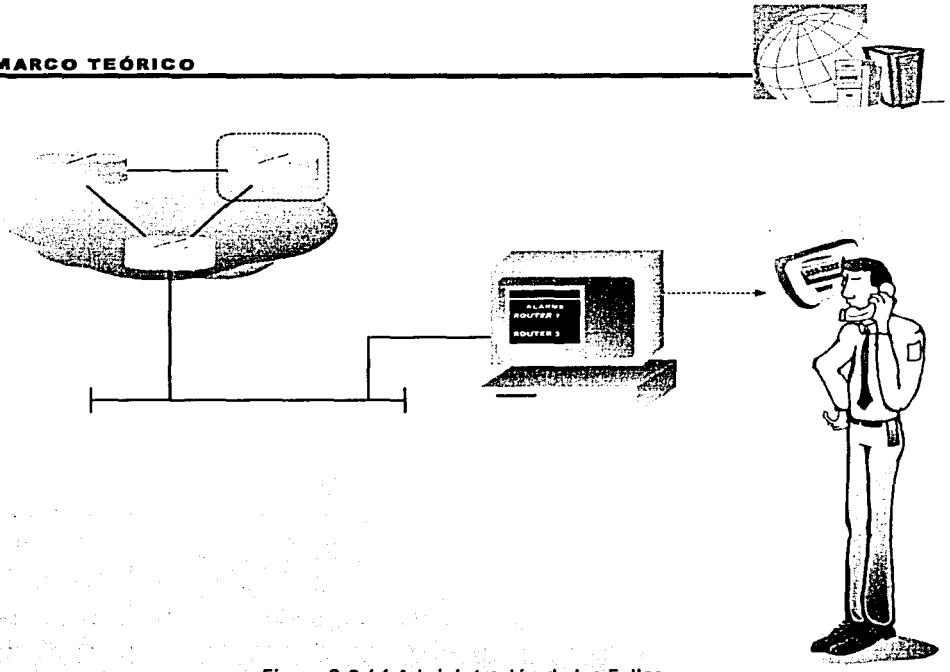
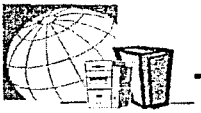


Figura 2.6.4.1 Administración de las Fallas.

La administración de fallas es una de las áreas funcionales del modelo ISO de administración de redes más complicadas para el ingeniero de redes. Es una pieza fundamental para el buen mantenimiento de una red de cómputo; su correcta aplicación y ejecución incrementa su confiabilidad y el desempeño. Se compone de cinco pasos básicos que se llevan a cabo de forma cotidiana una vez que la red se encuentra en operación:

1. Identificación del problema
2. Delimitación de la causa del problema
3. Corrección del problema
4. Revisión de la solución
5. Registro del seguimiento al problema

Cuando llega a presentarse alguna falla en la red, es necesario revisar los síntomas o características de la misma. Es común que los usuarios se comuniquen con el personal encargado de la operación de la infraestructura de comunicaciones para informar que «no tienen red». La verdad es que está frase puede traducirse en una gran variedad de causas por las cuales el usuario no puede hacer uso de la red, que pueden ir desde el hecho de que el usuario no tenga conocimiento sobre el manejo de la computadora, hasta tener



un problema crítico con los enlaces digitales o los equipos de comunicaciones.Es importante que el ingeniero de redes identifique claramente el problema mediante preguntas y pruebas que se tienen que ir haciendo con el usuario.

Si el usuario que reporta el problema al personal encargado de la operación como un «no tengo acceso a la red», y el operador que lo atiende encausa el problema directamente al área de comunicaciones o conectividad, siendo que realmente el problema es que el usuario no cuenta con su clave para tener acceso al correo electrónico, la solución se va a llevar más del tiempo justificado. Por ello es indispensable que los operadores hagan las preguntas precisas al usuario, así como las pruebas pertinentes, para identificar rápidamente el problema.

Una vez identificado un problema, es necesario delimitar la causa. Por ejemplo, si los usuario de una sucursal u oficina reportan un problema de red a las oficinas centrales, la causa del problema puede deberse a una falla en el equipo que les da servicio directamente, a una falla en el enlace de comunicaciones o una falla en el equipo de las oficinas centrales, entre otros. El ingeniero debe identificar cuál es la causa real de la falla mediante pruebas manuales o mediante la correcta interpretación de las alarmas generadas por el sistema de administración de red.

Ya que la causa del problema se ha verificado, se corrige el problema mediante los procedimientos establecidos. Puede haber una o más soluciones para un problema en particular, es responsabilidad del ingeniero encargado corregir el problema y verificar si la solución que se dio no tiene efectos secundarios para otros usuarios de la red.

Es necesario contar con un sistema que permita registrar el problema, desde su recepción hasta su solución, con el objetivo de generar una base de conocimiento que ayude a corregir problemas posteriores con características similares o permita tomar acciones derivadas de estadísticas de fallas reiterativas en equipos de cómputo o comunicaciones y enlaces.

2.6.5 Administración de la Seguridad

El objetivo de la administración de la seguridad se basa en el control del acceso a los recursos de la red de acuerdo a las políticas de la organización para evitar un posible sabotaje (de tipo intencional o accidental) y que la información de carácter restringido y privada no pueda ser consultada o utilizada sin una autorización previa.

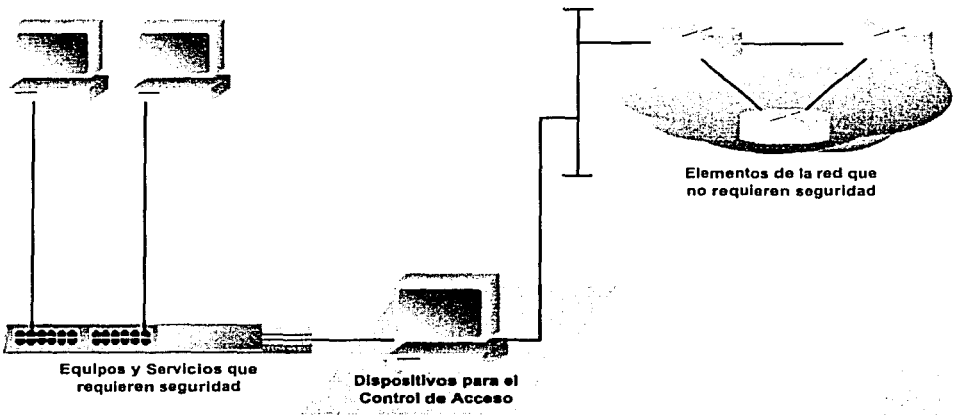


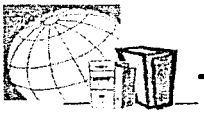
Figura 2.6.5.1 Administración de la Seguridad.

La información de carácter crítico es cualquier dato que la organización considere que debe estar seguro, como son las cuentas de los clientes, la nómina, los sistemas de inventarios de bienes y servicios, etc.

La administración de seguridad permite a los ingenieros de redes proteger la información de carácter crítico limitando el acceso a los servicios y dispositivos de red por usuario, tanto del exterior como del interior de la organización. También permite notificar la ingeniero de cualquier intento de intrusión a los sistemas y acerca de los posibles huecos de seguridad que existan en los servicios de la red. Para ello es necesario llevar las siguientes actividades a cabo.

1. Identificar la información de carácter crítico que necesita ser protegida.
2. Identificar los diferentes puntos de acceso a los sistemas o información definidos.
3. Implementar mecanismos para asegurar los puntos de acceso identificados.
4. Mantener la seguridad en los puntos de acceso a la información.

Muchas organizaciones tienen políticas bien definidas que catalogan los diferentes tipos de información; dentro de estas políticas comúnmente se incluyen los aspectos relacionados con la información de contabilidad, financiera, clientes, mercado, ingeniería y de los empleados. Podría parecer

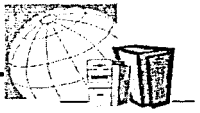


sencillo identificar la información crítica, más sin embargo tiene sus complicaciones en virtud de que el punto de vista de las áreas de la organización puede ser muy diferente.

Una vez que se ha identificado la información de carácter crítico y donde está ubicada, es necesario revisar los métodos utilizados por los usuarios para tener acceso a ella. Hay que tomar en cuenta que el primer punto de acceso de los usuarios a la información son los cables, y conforme se van identificando los puntos se llegan a las aplicaciones y la forma en que funcionan.

Existen varias técnicas y herramientas para asegurar los puntos de acceso a la información y esto se puede hacer en las múltiples capas de los protocolos de comunicaciones: se pueden encriptar los paquetes al nivel de la capa de enlace del modelo OSI; se pueden implementar listas de acceso de acuerdo a las direcciones origen y destino de los paquetes; o se pueden filtrar los usuarios a nivel de las aplicaciones que se utilizan comúnmente para proporcionar los servicios de red.

Dentro del mantenimiento de los esquemas de seguridad se debe considerar la implementación de bitácoras en las cuales se registren los accesos a los servicios protegidos, tanto de usuarios válidos como de intentos de ataque. Esto permitirá tomar las acciones necesarias, ya sea en tiempo real o a corto plazo para fortalecer el esquema de seguridad implementado.



2.7 SISTEMAS DE ADMINISTRACIÓN DE RED

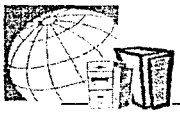
El Sistema de Administración de Red es un conjunto de programas de *software* que sirven como herramientas para la operación de la red. Como cualquier sistema, se basa en un conjunto de componentes; en este caso, son dos: la Plataforma y las Aplicaciones.

2.7.1 Plataforma de Administración de Red

El centro donde se administra una red puede tener sistemas independientes para la administración de cada unos de los dispositivos que la conformen, como es el caso de los módems, los multiplexores, los concentradores, los puentes, los ruteadores y otros tipos de dispositivos. Este tipo de esquemas de administración basados en sistemas independientes para grupos de dispositivos que conforman la red puede llevarnos a problemas de costos, espacio físico y experiencia técnica para poder llevar la administración de cada uno de ellos; por ello es conveniente que la administración de los dispositivos de red recaiga sobre un solo sistema de administración, y que además permita la visualización de las interconexiones entre todos los equipos. Debido a esta necesidad surge el concepto de: plataforma de administración de red.Una plataforma de administración de red la entendemos como un *software* que dadas sus funcionalidades, permite llevar a cabo las tareas de administración de los diversos dispositivos de una red. De aquí que el objetivo principal de una plataforma de este tipo es que permita una administración genérica de todos los equipos de una red, independientemente de la diversidad de marcas y modelos que pueda haber. Las funcionalidades básicas con que debe contar un *software* de esta naturaleza son:

- Una Interfaz Gráfica (**GUI**).
- Un Mapa de interconexión de dispositivos.
- Un Sistema de Administración de Base de Datos (**DBMS**).
- Un Método estándar para el poleo de los dispositivos.
- Un sistema que permita la personalización de los menús y el ambiente de usuario.
- Procesos para almacenar la información relacionada con los eventos que puedan presentarse en los dispositivos de red.

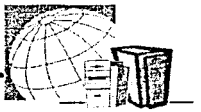
La interface gráfica es recomendable ya que proporciona al usuario una forma simple para accesar las herramientas y recursos con que cuenta la plataforma de administración de red. La interface gráfica debe estar basada en un estándar de ambiente gráfico, como MicroSoft Windows, OSF Motif u Open Look (Sun MicroSystems). Existen una gran variedad de desarrolladores de



software y fabricantes que implementan interfaces gráficas, si todos ellos lo hacen en base a un estándar facilitan al usuario el manejo y uso de los sistemas.Los mapas de red son útiles ya que dan un acercamiento sencillo de cada parte de la infraestructura de red que se necesita administrar. Las herramientas gráficas para la atención y control de fallas ayudan a aislar los problemas o causas que implican fallas en la red; estas herramientas hacen uso de colores que ayudan a identificar claramente los tipos de falla en una red. Las herramientas para el manejo de las configuraciones pueden mostrar la configuración física y lógica de toda la red y de cada uno de los dispositivos. Aunado a estas herramientas también se puede contar con aplicaciones que permitan visualizar gráficamente el desempeño de los dispositivos, permitiendo la evaluación de problemas y la acción proactiva en la solución de fallas. Si la plataforma de administración de red tiene utilerías para que de manera automática se puedan localizar y visualizar los dispositivos en los mapas de red se tiene entonces una herramienta capaz de eficientar las actividades que lleva a cabo el personal encargado de la operación y mantenimiento de la red y de los sistemas.En redes heterogéneas es común encontrar diferentes marcas y modelos de equipos, por ello es conveniente que la plataforma de administración de red sea capaz de obtener la información operativa y de configuración de cada uno de ellos. Es necesario entonces que el método para poder obtener todos estos datos sea un estándar que permita el poleo de todos los dispositivos.

Un sistema de administración de base de datos (DBMS) es indispensable para poder llevar a cabo las tareas de administración de una manera correcta. Las aplicaciones pueden hacer uso de la Base de Datos para almacenar los datos de tipo estadístico. De esta manera se pueden relacionar todo tipo de datos que permitan un diagnóstico anticipado de posibles eventos en la red y una mejor administración de ella. La mayor parte de los sistemas de bases de datos permiten que los usuarios puedan generar reportes y estadísticas de acuerdo a las necesidades particulares y con la alternativa de automatizar los procesos.

La última característica con la que debe contar una plataforma es la generación de una bitácora de eventos o sucesos. En esta bitácora se deben registrar cada uno de los eventos que se presentan en la red de una manera cronológica y en un formato estándar de lectura para su posterior procesamiento. Por un lado, de acuerdo a la capacidad de poleo, la plataforma debe registrar todos los eventos en esta bitácora; pero aunado a ello, es aconsejable que los dispositivos tengan la capacidad de enviar mensajes de estado a la plataforma de manera asíncrona con el fin de que sean almacenados en la bitácora. De esta manera el operador de red tiene la documentación y la herramientas de análisis para poder determinar el estado general de la red y de los dispositivos críticos.



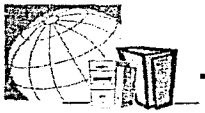
Adicionalmente, entre las funcionalidades básicas con las que debe contar la plataforma de administración para brindar una solución estratégica en la administración están:

- Herramientas de graficación
- APIs
- Sistema de Seguridad

La plataforma de administración debe permitir a los ingenieros la facilidad de generar gráficas de diversos tipos. Es benéfico que este tipo de gráficas se puedan adjuntar a los reportes, ya que dan una mejor visión de los diversos parámetros de la red que los reportes tabulares o de texto. Las gráficas de tiempo real del tráfico, de la carga y de los errores ayudan a la resolución de problemas y el mejoramiento del desempeño de los dispositivos y enlaces; las gráficas obtenidas en base a datos almacenados por ciertos intervalos de tiempo ayuda a predecir los eventos que pueden llagarse a presentar en la red.

Un API es una librería de procedimientos y funciones de programación que permiten acceder a la información que maneja y almacena la plataforma de administración. El API permite que programas externos puedan hacer uso del mapa de red de la plataforma; que se puedan integrar a los menús del sistema; que puedan almacenar y accesar información de la base de datos; que puedan registrar eventos en la bitácora y más. Además el API basa su importancia en dos aspectos: permite la integración de aplicaciones de otros desarrolladores o fabricantes y posibilita a los ingenieros el desarrollo de programas y aplicaciones de acuerdo a sus necesidades particulares. Sin el API, la plataforma de administración puede ser vista como una «Caja Negra», lo cual restringe el desarrollo de la misma en ambientes abiertos (Open Systems). El API debe tener la posibilidad de ser estandarizado hacia diversos tipos de plataformas; si un API no es estándar para diversas plataformas, entonces una aplicación que tiene comunicación con una plataforma específica tendrá que ser modificado si la organización decide cambiar de plataforma.

Otra característica importante en una plataforma es que debe contar con un mecanismo de seguridad. Esto deriva del hecho de que la plataforma de administración y las aplicaciones asociadas a ella tienen y manejan una gran cantidad de información relacionada con la red: la configuración de los dispositivos, su desempeño, la contabilidad, los esquemas de seguridad de la red y las aplicaciones, etc. Esta información puede ser sumamente importante para aquella persona que desee comprometer la seguridad de la red. El sistema de seguridad de la plataforma debe ser adicional al sistema de seguridad que provee el sistema operativo del equipo de cómputo en el cual está instalada.



Estas funciones básicas de una plataforma de administración de red deben permitir al operador de red cumplir con todas las actividades de administración que se llevan a cabo en una red. Con ello el operador debe tener la posibilidad de monitorear todos los dispositivos y enlaces de la red, obteniendo información clave que pueda utilizar de diversas maneras. Por ejemplo, un operador de red que requiere obtener una gráfica de la utilización de los enlaces seriales de una red tendrá que seguir los siguientes pasos:

1. Decidir que tipo de información requiere de cada uno de los dispositivos.
2. Obtener la información apropiada de los dispositivos mediante la plataforma de administración.
3. Proporcionar los datos adquiridos de cada uno de los dispositivos a las herramientas de graficación.

El primer paso es el más difícil. Aunque la plataforma debe tener la habilidad de obtener toda la información de todos los dispositivos, cada uno de ellos la puede entregar de diferente manera. Actualmente todos los parámetros de operación de los equipos pueden ser obtenidos en un formato estándar denominado MIB (Management Information Base). Esto quiere decir que se puede obtener ciertos parámetros o ciertos datos que son comunes a todos los dispositivos.

En el mercado actual, existen un gran número de plataformas para la administración de redes: Sun Net Manager (Sun MicroSystems), HP (Hewlett Packard) Open View, IBM Net View, AT&T StarSentry, Spectrum (Cabletron), Transcend Enterprise Manager (3Com). Todas estas proporcionan las funcionalidades básicas de las que hemos hablado, pero también proporcionan características particulares que las hacen a unas más eficientes para ciertos escenarios que otras.

Aplicaciones para Administración de Redes

Como hemos visto, una plataforma debe proporcionar la funcionalidad necesaria para la administración de todos los dispositivos de una red. En contraste, las aplicaciones para la administración de redes se diseñan como herramientas que ayuden al operador en la administración de un conjunto específico de dispositivos y/o servicios. Generalmente, la mayoría de las aplicaciones son diseñadas y desarrolladas por los fabricantes de equipos con el fin de ayudar a sus clientes en la administración de sus dispositivos.

Por ejemplo, un fabricante de un cierto dispositivo de red, como pude ser un módem, un concentrador, un ruteador, un bridge, etc. podría desarrollar un

conjunto de aplicaciones que trabajarán en conjunto con la plataforma de administración con el fin de integrar en un solo producto un conjunto de herramientas para facilitar las tareas del ingeniero o encargado de la red.

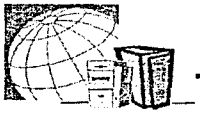
Mediante esta estrategia, el ingeniero solo se vería en la necesidad de invertir en el conjunto de herramientas (aplicaciones) para el manejo y administración de un conjunto de dispositivos en particular. Si se requiere de la administración de ciertos concentradores o servidores, por ejemplo, se puede solicitar al proveedor de dichos equipos las aplicaciones necesarias que interactúen y se integren a la plataforma de administración. Esto permite contar con un sistema de administración de red que proporcione la funcionalidad necesaria a través de la plataforma y las aplicaciones para el control de parámetros específicos de los dispositivos mediante el uso del mismo mapa topológico, la misma interface gráfica, los mismos menús y la misma base de datos.

Los objetivos principales de las aplicaciones para la administración de redes son:

- La administración efectiva de un conjunto específico de dispositivos.
- Evitar que su funcionalidad se traslape con la de la plataforma.
- Integrarse a la plataforma a través de APIs y el conjunto de menús.
- La posibilidad de trabajar con diversas plataformas.

Una aplicación para la administración de red busca la administración efectiva de un conjunto de dispositivos de red. Por ejemplo, un fabricante de un determinado Hub (concentrador) puede desarrollar una aplicación que permita desplegar los conectores físicos del concentrador en el momento en que el ingeniero lo seleccione en el mapa de red que brinda la plataforma. De esta manera la aplicación permitirá al ingeniero configurar ciertos parámetros característicos del concentrador, activar y desactivar los puertos remotamente, o monitorear el ancho de banda utilizado o la tasa de errores que esta presentando cierta conexión o enlace. Con ello la aplicación ayudara en las tareas de configuración y administración de una manera más sencilla para este dispositivo en particular.

Las aplicaciones para la administración de redes deben cumplir con cierta funcionalidad siempre y cuando esa funcionalidad no se traslape con la de la plataforma. Si esto llega a suceder se puede incurrir en el hecho de que la interface sea confusa para el usuario; ya que no esta claramente definido si la aplicación o la plataforma es la que cumplirá con cierta función. Por otro lado, seria un gran desperdicio de tiempo y esfuerzo para los desarrolladores de las aplicaciones el implementar características en las aplicaciones que ya estén incluidas en las plataformas y viceversa.



Se puede hacer la excepción en el caso de que la plataforma no cuente con ciertas características que son convenientes para las aplicaciones. Por ejemplo, si la plataforma cuenta con las herramientas para la elaboración de gráficas lineales y la aplicación necesita de gráficas en forma de **Pie** (pastel), es válido que la aplicación cuente con esa opción. Pero, si los desarrolladores de aplicaciones necesitan incluir en ellas la característica de poder desplegar **pie charts** (Gráficas de pastel) para determinada plataforma, entonces es obvio y válido que hagan notar a los desarrolladores de la plataforma que se requiere de esa característica en ella. De esta manera se reducen costos y aumentan los beneficios para el usuario; uno de ellos: menos confusión y más sencillez.

Una aplicación de administración de red debe tener como una de sus metas importantes el poder tener una interface hacia la plataforma a través de un API y los menús del sistema en general. Esto permite que el usuario visualice tanto las aplicaciones como la plataforma como un solo sistema de administración de red. El API tiene como función básica crear la interface de la aplicación hacia la plataforma; el sistema de menús permite que los programas asociados a la aplicación sean invocados desde el mismo sistema de menús de la plataforma de los cuales hace uso directamente el usuario. En muchas de las plataformas, el incluir opciones al sistema de menús para accesar ciertas aplicaciones es tan sencillo como el editar un archivo de texto. Si la aplicación es ejecutada como un proceso aparte de la plataforma, el integrarlo al menú de opciones de la plataforma es una tarea algo trivial. Si todas las aplicaciones de las que hace uso el ingeniero de redes por medio de la plataforma coexisten de la manera que hemos señalado con ella, es posible tener un conjunto vasto de características y herramientas que ayuden de manera considerable a la administración de una o varias redes.

Una aplicación que solo está disponible para una plataforma única forza al ingeniero de redes a hacer uso de esa plataforma específica para llevar a cabo las tareas de administración. Por lo que hemos descrito, esta no es una situación ideal para las personas que llevan a cabo estas actividades, ya que una plataforma específica puede no tener las características o la funcionalidad necesaria que requieren otras aplicaciones. Por ello las aplicaciones de administración tienen como meta poder integrarse a las plataformas más comunes y comerciales que existen para la administración de redes. De cualquier manera, la integración de las aplicaciones con la plataforma requiere de una cuidadosa planificación que permita mantener un esquema de administración sin importar las variaciones que pueda sufrir la plataforma debido a el desarrollo de nuevas versiones o componentes.

El tener un sistema de administración de red de este tipo incrementa la eficiencia de las tareas que se deben realizar, esto gracias a las aplicaciones

y las plataformas de red que trabajan en conjunto; pero siempre existe el hecho de que no hay un sistema perfecto: Las aplicaciones no comparten información. Por ejemplo, supongamos que una estación de trabajo de la marca «A» se integra a una red conectándola por medio de par trenzado a un concentrador. El concentrador, a su vez, está conectado a través de par trenzado a un bridge, el cual tiene una conexión al resto de la red de datos. Un determinado día, el puerto del concentrador que lo conecta al bridge falla por una excesiva cantidad de errores en la transmisión. La aplicación que se encarga de monitorear la estación de trabajo reporta que el equipo se encuentra fuera de servicio o no disponible. Otra aplicación que se encarga de monitorear el concentrador reporta problemas para accesar al equipo. Una tercera aplicación que se encarga del monitoreo del bridge indica que uno de los puertos del dispositivo ha presentado una falla. En este caso, la plataforma recibe tres notificaciones que ingresan en ese momento a la bitácora de reportes y fallas. De acuerdo a esto, dependiendo el sistema de seguimiento de fallas que se implemente y que personas estén disponibles, teóricamente tres ingenieros serán asignados para trabajar en la resolución de cada uno de los «problemas» que se presentaron en la red. Con el fin de evitar que se presente este problema en cuanto a duplicidad de funciones, la plataforma requiere de un sistema inteligente que se encargue de monitorear la bitácora de errores. Si una aplicación encargada de la atención y control de fallas toma los registros (eventos) de la bitácora y computa la topología de la red de acuerdo a la información almacenada en la base de datos relacional de la plataforma, el sistema podrá deducir que un conjunto de problemas tienen una causa en común, lo cual ayuda a minimizar el tiempo de respuesta para la resolución de los mismos. Este tipo de aplicación deberá tener la capacidad de entender el esquema jerárquico de dependencia de los diferentes dispositivos que conforman la red, de tal manera que permita la visualización del problema desde un punto de vista objetivo: no hay acceso a la estación de trabajo debido a que el puerto de su concentrador que lo conecta al bridge se encuentra fuera de servicio.

2.7.2 Arquitecturas de Administración de Redes

Una plataforma de administración puede hacer uso de varios tipos de arquitectura con el fin de proporcionar la funcionalidad deseada. Las tres arquitecturas de administración más comunes son:

- Centralizada
- Jerárquica
- Distribuida

De estas tres no hay una que sea la «mejor»; cada una de ellas tiene ciertas características que la hacen idónea para ciertos escenarios. Por experiencia,

es una buena regla escoger una arquitectura que se acerque más a la estructura de la organización. Generalmente, la red tiene una estructura similar a la de la organización.

Arquitectura Centralizada

En una arquitectura centralizada, la plataforma de administración de red se encuentra instalada en un solo equipo de cómputo, en un lugar en donde se llevan a cabo las tareas de administración de red y donde recae las responsabilidades asociadas a la misma, ver figura 2.7.2.1

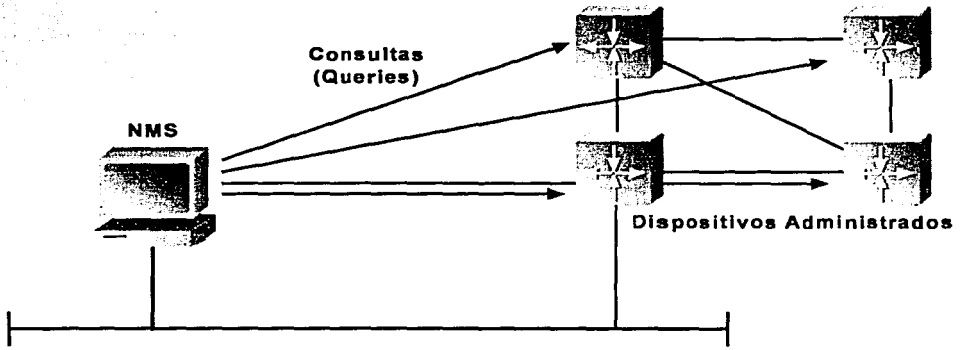


Figura 2.7.2.1 Arquitectura centralizada

Este sistema hace uso de una sola base de datos de tipo centralizado. Para una completa redundancia, este sistema debe tener un sistema espejo al cual se hagan respaldos en intervalos regulares de tiempo. De cualquier manera, el sistema central es el punto en el que recae la administración de la red; este sistema puede permitir el acceso y enviar información a otras terminales por medio de la red. Bajo arquitectura centralizada, el nodo central tiene como fin:

- Recibir todas las alarmas y eventos que se presenten en la red.
- Difundir y recibir todo tipo de información relacionada.
- Tener acceso a todas las aplicaciones de administración.

Al hacer uso de una arquitectura centralizada, el ingeniero de redes tiene un solo lugar en donde estar al tanto de alarmas y eventos, lo cual es muy útil cuando se requiere de atención de fallas y correlación de problemas. Tener

un sistema central desde el cual se puedan accesar todas las aplicaciones de administración y la información brinda al ingeniero de redes conveniencia, accesibilidad y seguridad en el manejo y operación de la red. En este mismo sentido, un esquema de administración central facilita el mantenimiento de la seguridad. Físicamente, el equipo en el cual se encuentra la plataforma de administración puede ubicarse en un área cerrada y de acceso restringido; de igual manera, el sistema puede ser configurado para restringir el acceso a un determinado conjunto de usuarios.

Sin embargo, el hecho de que todas las tareas y funciones para la administración de la red dependan de un solo sistema no implica que exista una completa redundancia y que sea a prueba de fallas. Los respaldos del mismo deberán hacerse en un equipo situado en otro lugar físico (idealmente). Un sistema de administración centralizada puede ser difícil y costoso de escalar para cubrir con las necesidades de administración en proporción al crecimiento y cambios en la infraestructura de red. Una desventaja significativa de este tipo de arquitectura es el que solo un sistema es el encargado de polear todos los dispositivos de la red. Esto ocasiona que el tráfico en las conexiones de red del sistema de administración se incremente de forma notoria, al igual que a lo largo de toda la red. Si la conexión de red de la estación de administración se ve considerablemente afectado, la funcionalidad del sistema de administración se verá mermada. Una recomendación para evitar este tipo de situaciones cuando se utiliza una arquitectura de este tipo, es que el sistema de administración se ubique en un punto estratégico a nivel topológico de la red con el objetivo de que el acceso a todos los dispositivos de la red sea de manera balanceada y rápida.

Solo que el llevar a cabo esta recomendación no es del todo sencillo, puesto que generalmente el lugar ideal para el sistema de administración, no es siempre el lugar ideal en el cual puedan trabajar o residir los ingenieros de redes.

Un ejemplo de una arquitectura de red centralizada que se utiliza en la actualidad es NetView de IBM, el cual se instala en un solo equipo de cómputo y se encarga de llevar a cabo todas las funciones de administración en una red que hace uso del protocolo SNA.

Arquitectura Jerárquica

Una arquitectura de administración de red jerárquica hace uso de un conjunto de sistemas -no solo uno-, de los cuales, uno de ellos hace la función de servidor y los demás hacen la función de clientes, ver figura 2.7.2.2.

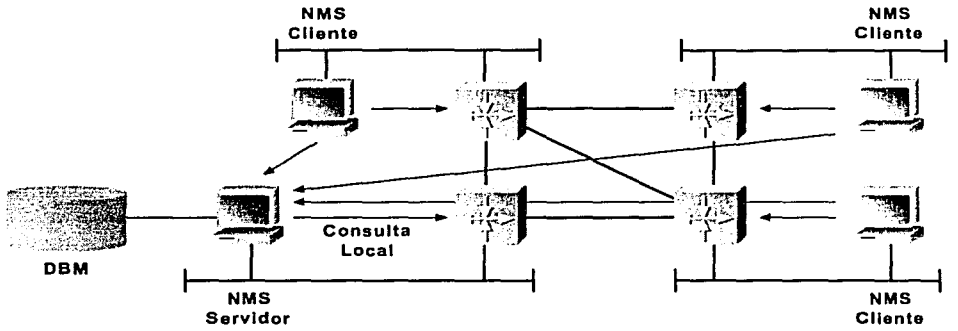


Figura 2.7.2.2 Arquitectura jerárquica

Dentro de este esquema, el servidor ejecuta o lleva a cabo una parte de las funciones del sistema de administración, mientras que los clientes ejecutan las restantes. Por ejemplo, los ingenieros de redes pueden configurar varios clientes con el fin de que cada uno de ellos se encargue del monitoreo de cierta parte de la red.

Para esta arquitectura, la plataforma puede hacer uso de una base de datos basada en la arquitectura Cliente/Servidor. Esto no significa que cada cliente tendrá su propia base de datos, en algunos casos esto puede ser ineficiente; lo que significa es que cada cliente podrá accesar los recursos del servidor central a través de la red con el fin de que obtener cierta información particular. Debido a la importancia que tiene el servidor central en esta jerarquización, será necesario que exista un servidor de respaldo o un sistema de respaldos adecuado.Una arquitectura jerárquica para la plataforma de administración, tiene las siguientes características:

- No es dependiente de un solo sistema
- Distribución de las actividades relacionadas con la administración
- El monitoreo de la red se hace de forma distribuida
- Un almacenamiento de información de tipo centralizado

Este tipo de arquitectura ayuda a eliminar los problemas relacionados con la administración centralizada de redes al hacer una distribución de las actividades de administración entre el sistema central y los clientes. Los ingenieros de red pueden distribuir el monitoreo de la red entre los diversos clientes, lo cual ayuda a aprovechar mejor el ancho de banda de los enlaces y las redes locales que conforman toda la red. De la misma manera, los clientes

no necesitan tener toda la funcionalidad que deberá tener el sistema central, ya que esto ocasionaría que el esquema se volviera ineficiente. RMON (Remote Network Monitoring) es un protocolo que se utiliza para implementar este tipo de arquitectura. Muchas de las tareas de administración de red requieren de contar con la información acerca de muchos de los aspectos de la red; por ello es recomendable tener un lugar central donde se almacenen los datos.

Esta arquitectura - como ya mencionamos - hace uso de uno o varios sistemas de administración de red para controlar y operar de mejor manera toda la red; por lo cual ya no se tiene un lugar central donde se llevan a cabo las tareas de administración y se almacena toda la información relacionada a las actividades. Esto vuelve un poco más difícil la tarea de la administrador de la red, además de que hace que se empleé más tiempo del necesario en la conjunción de la información derivada de las actividades de administración. Por otro lado, la lista de dispositivos y equipos que se encarga de administrar cada cliente, tiene que ser predeterminada lógicamente y configurada manualmente. Si esto no se hace de manera cuidadosa puede incurrirse en que tanto el sistema central como el cliente, estén monitoreando o poleando el mismo dispositivo. Esto tiene como resultado un desperdicio de funcionalidad tanto en el sistema central como en el cliente y un consumo innecesario de ancho de banda.

La mayor parte de las plataforma de administración mencionadas anteriormente pueden implementar un sistema de administración jerárquica mediante la adecuada configuración de las mismas por parte del ingeniero de red.

Arquitectura Distribuida

La arquitectura distribuida es el producto de las principales características de las arquitecturas jerárquica y centralizada, como se muestra en la figura 2.7.2.3

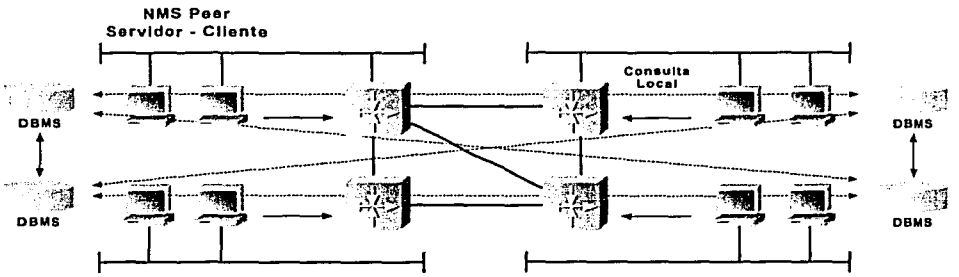


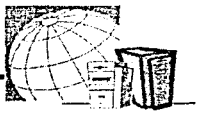
Figura 2.7.2.3 Arquitectura distribuida

En lugar de tener una plataforma de tipo centralizado o una jerarquía de plataformas Cliente/Servidor-Central, el acercamiento a una arquitectura distribuida hace uso de un esquema de «múltiples conjuntos de plataformas». La forma en que trabaja este esquema es la siguiente: se tiene una plataforma principal que encabeza a un conjunto de sistemas de administración; cada conjunto puede contar con una base de datos que contenga todos los dispositivos y equipos de toda la red; esto permite llevar a cada conjunto varias actividades, reportando los resultados de las mismas a un sistema central.

Debido a que la plataforma distribuida engloba las características de la arquitectura centralizada y la arquitectura jerárquica, ésta tiene las ventajas de las dos:

- Un solo lugar en donde se almacena toda la información de la red: información de dispositivos, alarmas y eventos o sucesos.
- Un solo lugar desde el cual se pueden accesar todas las aplicaciones relacionadas con la administración de la red.
- No es dependiente de un solo sistema.
- Distribución de las tareas de administración.
- Distribución del monitoreo entre varios clientes en diferentes puntos de la red.

La tecnología de «replicación de la base de datos» del servidor es la parte más importante de esta arquitectura. Un sistema de replicación mantiene varias bases de datos en diferentes sistemas o servidores de manera sincronizada, lo cual no es una tarea sencilla, pero si bastante compleja. De hecho, la sincronización de las bases de datos necesaria para esta implementación puede llegar a consumir ancho de banda innecesario si no se implementa de la forma correcta y óptima.



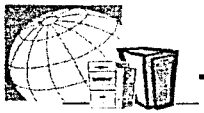
¿ Cómo seleccionar un sistema de administración de red ?

Como hemos vistos, los sistemas de administración de red se basan prácticamente en la plataforma y las aplicaciones. Si cada uno de estos componentes se seleccionara cuidadosamente, se puede consolidar un sistema que ayude a los ingenieros de red a llevar a cabo las tareas de administración de red de una manera eficiente y sencilla. Los pasos que hay que seguir para seleccionar un sistema de administración de red pueden ser los siguientes básicamente:

1. Hacer un inventario de los dispositivos y equipos de red.
2. Dar prioridad a cada una de las funciones a llevar a cabo en la administración de la red.
3. Hacer una revisión de las aplicaciones necesarias.
4. Seleccionar la plataforma de administración.

El primer paso en la selección de un sistema de administración es el identificar los dispositivos que componen la red. Generalmente dentro de este conjunto están incluidas las estaciones de trabajo, las computadoras personales, controladores, gateways, ruteadores, switches, bridges, hubs, impresoras y módems. Junto con ello es indispensable verificar de todos ellos, cuáles pueden ser administrados por cualquier de los protocolos de administración de redes existente, sea estándar o propietario. Si un dispositivo no puede ser administrado por un protocolo estándar de administración no se debe eliminar del inventario; posiblemente exista un *software* (gateway) que permita la traducción entre el protocolo del dispositivo y el protocolo estándar. Una vez que se tenga la lista de dispositivos, se necesita prioritizar aquellos que cumplan con una función delicada y crítica hacia la red en general; comúnmente estos dispositivos son switches o ruteadores que conforman el backbone. Por ejemplo, aunque puede ser conveniente el estar monitoreando los concentradores que dan servicio a una red local en particular, el monitorear el ruteador que da acceso a todos esos concentradores tiene más alta prioridad, ya que si este llega a tener un fallo, los concentradores se verán afectados al proporcionar el servicio de red a las computadoras que requieren de salida hacia el resto de la red de datos.

El siguiente paso consiste en dar prioridades a las tareas y funciones de administración de la red de la organización. En la mayoría de los casos, una de las principales tareas de la administración de redes es la de atención y control de fallas (Fault Management). De cualquier manera, la organización posiblemente requerirá que el control y administración de la seguridad o las tareas de configuración de los equipos tengan la más alta prioridad. Este paso es esencial ya que en eso se basa la selección de las aplicaciones de administración.

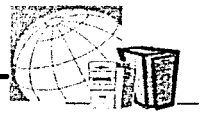


El tercer paso, como ya lo mencionamos, es el encontrar y seleccionar las aplicaciones que ayuden a realizar las actividades de administración de los dispositivos de la red. Sin estas aplicaciones, solo se podrá contar con la funcionalidad básica que proporcione la plataforma de administración de red. Hacer uso de aplicaciones diseñadas para la administración de los dispositivos prioritizados permite distribuir mejor los recursos para llevar a cabo las tareas relacionadas y no existe la necesidad de desarrollar aplicaciones para llevar a cabo tales tareas.

El último paso que hay que seguir en la selección es el escoger la plataforma a usarse para la administración de la red. Idealmente, las aplicaciones seleccionadas deben trabajar en, al menos, una plataforma de administración.Si todas ellas pueden trabajar juntas en una sola plataforma, la selección de ésta es sencilla. Si se ha hecho una selección de varias plataformas, se debe escoger aquella que tenga una arquitectura que se acerque lo más posible a la forma en que se quiere llevar a cabo la administración de la red por parte de la organización. Por ejemplo, si la organización tiene como planes la administración de la red de manera centralizada teniendo a los ingenieros encargados en un solo sitio, una plataforma con esquemas centralizados o jerárquicos puede ser la mejor opción. Si la organización pretende tener varios sitios donde se lleve a cabo la administración de diversas partes de la red, entonces es conveniente una plataforma de tipo distribuido.

Otro criterio para la selección de una plataforma de administración, son los requerimientos de *hardware* necesarios para que el *software* pueda trabajar correctamente y con holgura de memoria y almacenamiento. Una plataforma de administración requiere de un *hardware* donde pueda correr o ser ejecutada, si este *hardware* presenta problemas continuamente por saturación o mal funcionamiento las tareas de administración de la red se verán mermadas y se dificultará el trabajo del ingeniero de red. Actualmente las plataformas de administración de red pueden ser instaladas en una gran variedad de equipos y pueden ser soportadas por una gran variedad de sistemas operativos.

Las organizaciones comúnmente tienden a hacer las selección de los sistemas de administración de red de una manera poco formal y sin seguir los pasos o el orden descrito. Muchas veces la selección de la plataforma de administración es lo que se hace primero; debido a esto, las organizaciones se encuentran posteriormente con el hecho de que no existen aplicaciones que puedan integrarse a esa plataforma en particular para la administración de los diversos dispositivos de la red. Por ello es necesario que los pasos mencionados se sigan de acuerdo al orden presentado, esto beneficiará al esquema de administración de la red y a la organización.



2.8 MIB MANAGEMENT INFORMATION BASE

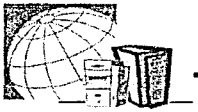
Hasta hace poco tiempo, los ingenieros necesitaban aprender una variedad de métodos para poder obtener información de los dispositivos de red. Así como los nuevos productos eran introducidos, eran desarrollados métodos propietarios para habilitar la obtención de datos, el resultado era que dos dispositivos que tenían la misma funcionalidad al venir de dos fabricantes diferentes podían tener muy diferentes métodos de obtención de datos.

En un ambiente de red heterogéneo podía resultar lento e incomodo la utilización de diversos métodos para la obtención de datos. Dada la necesidad de un método consistente para la obtención de información acerca de todos los componentes en una red de datos, los ingenieros de red optaron por herramientas genéricas estándar. Sin embargo, aunque estas herramientas fueron mas simples de utilizar que muchos métodos desarrollados por los fabricantes de los productos, estas no eran diseñados específicamente para la administración de la red y por lo tanto contaban con desventajas.

En redes que utilizaban arquitectura de red TCP/IP, los ingenieros de red podían utilizar mensajes ICMP Echo y Echo Reply para obtener información limitada pero útil para la administración de la red. Dadas estas desventajas, era indispensable la creación de un sistema estándar. Consecuentemente la comunidad en redes ha creado dos tecnologías divergentes para la administración de redes específicamente. Primeramente, Simple Network Management Protocol (SNMP) la cual tuvo poco éxito. Una segunda versión de este protocolo SNMPv2 tiene mucho mayor impacto en la comunidad de redes.

Los protocolos de red que han emergido recientemente proveen una forma de acceder a un conjunto de valores estándar de cualquier dispositivo de red elaborado por cualquier fabricante. Los *queries* para los dispositivos de red deben incluir lo siguiente:

- Nombre del dispositivo
- versión de *software* en el dispositivo
- Numero de interfaces
- Numero de paquetes por segundo en una interface



Los parámetros de los dispositivos de red que podían obtenerse, debían incluir:

- Nombre del dispositivo
- Dirección de red de la interfaz
- Estatus operacional de la interface de red
- Estatus operacional del dispositivo

La estandarización de los protocolos de administración de red trajo beneficios adiciónales al proveer una apariencia uniforme de los datos enviados y obtenidos de un dispositivo.

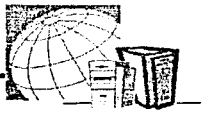
La *Management Information Base* (Base de Información de Administración MIB) es una definición precisa de la información accesible a través de un protocolo de administración. En el Request for Comment (Documentos en los cuales hay recomendaciones para estándares de uso en Internet - RFC) 1052, el Internet Arquitecture Board (Comité técnico de Internet encargado de la planeación e ingeniería de la red - IAB) recomienda la alta prioridad que tiene el definir una MIB para uso de SNMP y CMIS/CMIP, aunque ese esfuerzo de tener una MIB para estos dos protocolos de administración es poco realista, debido a la semántica diferente entre estos dos protocolos.

Usando una jerarquía, un formato estructurado, la MIB define la información de administración de red disponible de un dispositivo. Cada dispositivo, para ajustarse con el protocolo estándar de administración de red, debe utilizar el formato para presentar la información que esta definida por la MIB.

El RFC 1065 describe la sintaxis y tipo de información disponible en la MIB para la administración de redes TCP/IP. Titulada « Structure and Identification of Management Information for TCP/IP-based Internets (SMI) «, este RFC define reglas simples para nombrar y crear tipos de información.

Utilizando las reglas de SMI, RFC 1066 presenta la primera versión de la MIB para uso con el conjunto de protocolos TCP/IP. Este estándar, ahora se conoce como MIB-I explica y define la base de información exacta necesaria para monitorear y controlar internets basadas en TCP/IP. RFC 1066 fue aceptado por la IAB como un estándar completo en RFC1156.

RFC 1158 proporciona una segunda MIB, MIB-II, para uso con el conjunto de protocolos TCP/IP. Su propósito era el formalizar como un estándar y proveer por IAB en RFC1213, aumentar la base de información definida en MIB-I al expandir el conjunto de objetos definidos en la MIB.



Para facilitar la migración de los protocolos específicos de los fabricantes a un protocolo de administración estándar, RFC 1156 permite aumentar la expansión de la MIB para las especificaciones del fabricante.

Un subconjunto de la ISO Abstract Syntax Notation One (ISO Notación de sintaxis abstracta ISO ASNN.1) define la sintaxis para la MIB. Cada MIB utiliza una arquitectura de árbol definida en ASN.1 para organizar toda la información disponible. Cada pedazo de información en el árbol es un nodo etiquetado.

Cada nodo contiene un identificador de objeto y una descripción corta. El identificador de objeto (OID) es una serie de enteros, separados por puntos, para nombrar el nodo y denota el árbol ASN.1 transversal.

Un objeto es una de varias características especificas de un dispositivo administrable. Los objetos administrables son conjuntados en una o mas grupos y cuentan con identificadores de objeto.

Dos tipos de objetos existen, escalar y tabular. Los objetos escalares definen una instancia. Los objetos tabulares definen múltiples objetos relacionados que son agrupados en una tabla MIB.

Un nodo puede tener subárboles que contengan otros nodos. Cada nodo es un subárbol que es numerado en orden ascendente. Este orden lexicografito provee un esquema para numerar todos los objetos en el árbol de MIB.

Si el nodo no tiene subárboles, o es un nodo hoja, este contiene una valor y es conocido como un objeto. Los nodo hoja son también numerados en orden ascendente.

La figura 2.8.1 muestra un ejemplo de un árbol de MIB con sus correspondientes números ASN.1; La representación léxica del árbol de MIB de la figura es 1, 1.1, 1.1.1, 1.2, 1.2.1,1.2.1.1, 1.2.2, 2.

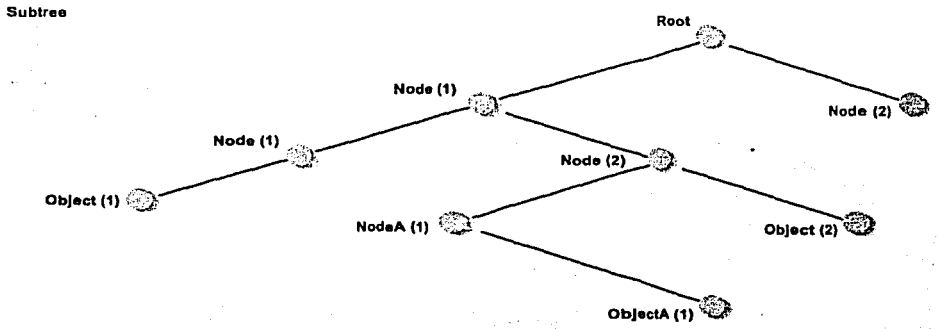


Figura 2.8.1 Ejemplo de árbol ASN.1

El nodo raíz del árbol de MIB no tiene un nombre, ni numero, pero tiene subárboles, como sigue:

Ccitt(0), administrada por la CCITT
Iso(1), administrada por la IOS
Joint-iso-ccitt (2), administración conjunta por ISO y CCITT.

La sintaxis, tal como ccitt(0), denota que el nodo llamado ccitt tiene el identificador de objeto 0 en este nivel del árbol de MIB.

Asimismo, existen muchos mas subárboles bajo el nodo iso(1), incluyendo el subárbol para las organizaciones, org(3). Bajo este subárbol, un nodo en particular de interés es el utilizado por el Departamento de Defensa de los U.S. (DOD): dod(6). Toda la información acumulada de los dispositivos de comunicaciones que manejan los protocolos de DOD, tales como TCP/IP, residen bajo este subárbol que tiene el identificador de objeto 1.3.6.1. Este identificador de objeto es conocido como internet. La descripción de este identificador es iso org(3) dod(6),1. En la figura 2.8.2 se muestra la estructura de arriba de este árbol de MIB.

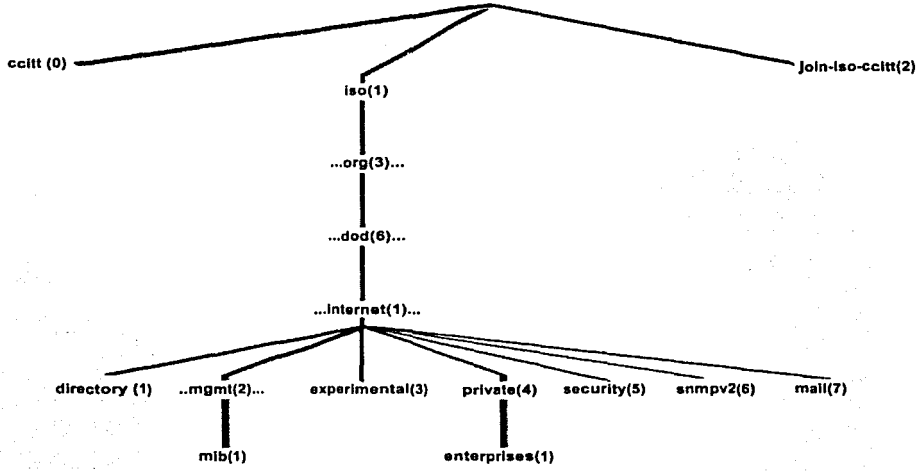


Figura 2.8.2 Estructura del árbol de MIB

Siete de los subárboles bajo el identificador de objeto internet son: directory(1), mgmt(2), experimental(3), private(4), security(5), snmpv2(6), y mail (7).

El subárbol directory(1) se encuentra reservado para uso futuro. Este subárbol podría contener información acerca del servicio de directorio OSI (X.500).

En la figura 2.8.3 se muestra la estructura del subárbol mgmt(2) e incluye algunos de los objetos de cada categoría. El subárbol mgmt(2) designado para administrar la información de los protocolos para la DOD. Los objetos en este subárbol son los que se encuentran mas ampliamente implementados. MIB-I (RFC1156), originalmente tenia asignado el identificador de objeto 1.3.6.1.2.1, o {mib 1}, ha sido suplantada por MIB-II (RFC 1213). MIB-II ha obtenido el mismo identificador de objeto.

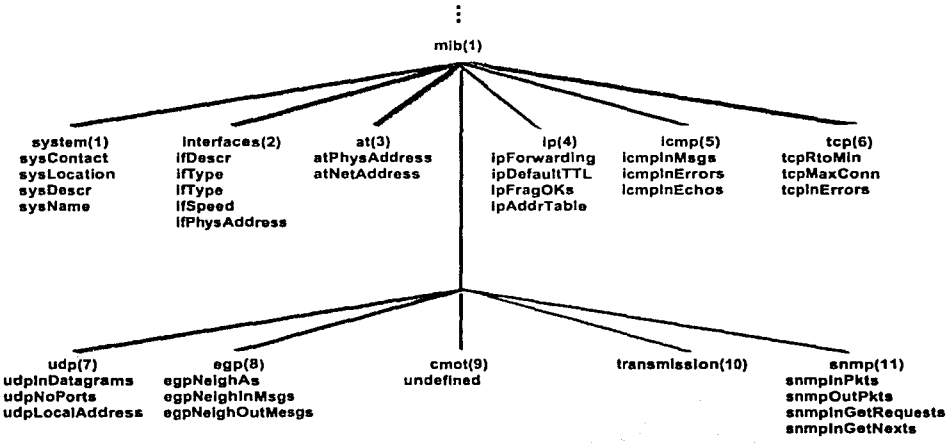
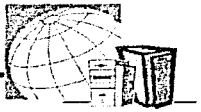


Figura 2.8.3 Estructura del subárbol Mgmt(2) y algunos objetos MIB-II

En la figura 2.8.3 se muestran los objetos utilizados para obtener la información especifica de los dispositivos de red. Estos objetos son desglosados en once categorías que se muestra en la Tabla 2.8.1

Categoría	Información
System(1)	Sistema Operativo del dispositivo de red
Interfaces(2)	Características de la interface de red
Address translation(3)	Mapeo de direcciones
Ip(4)	Características Protocolo Internet
Icmp(5)	Características ICMP
Tcp(6)	Características Protocolo Transmission
Udp(7)	Características UDP
Egp(8)	Características Exterior Gateway Protocol
Cmot(9)	Características de Common Management Information Services en TCP
Transmission(10)	Características medio de transmisión
Snmp(11)	Características SNMP

Tabla 2.8.1 Categorías del subárbol Mgmt(2)



Grupos en MIB-I y MIB-II

Los objetos administrables son organizados en grupos por dos razones. Primeramente, el agrupar lógicamente facilita la utilización de los identificadores de objeto y la estructura jerárquica. Por otra parte, el agente del protocolo de administración de red debe de tener un diseño simple porque la implementación de un grupo implica la implementación de todos los objetos de ese grupo.

MIB-I contiene 114 objetos. MIB-II la cual es compatible con MIB-I, contiene los 114 objetos, mas 57, para tener un total de 171 objetos.

Grupo System

El grupo system proporciona una descripción textual de la entidad, en caracteres ASCII. Este texto incluye una descripción, OID, el tiempo que lleva desde que se reinicializó esa entidad de red administrable, así como otros detalles administrativos. La implementación del grupo system es obligatoria.

Grupo Interfaz

El grupo de interfaz {1.3.6.1.2.1.2} provee información acerca de la interface de un dispositivo administrable. Esta información es presentada en una tabla. El primer objeto (ifNumber) indica el numero de interface en el dispositivo. Por cada interfaz, un renglón es introducido en la tabla, con 22 columnas por renglón. Las columnas proporcionan información acerca de la interfaz, tal como, velocidad de la interfaz, dirección física (*hardware*), estado operacional actual, y estadísticas de paquetes.

Grupo Address Translation

MIB-I incluye el address translation Group, pero este fue obsoleta en MIB-II. Esto significa que MIB-II incluye este grupo por compatibilidad con MIB-I, pero probablemente se excluya para futuras actualizaciones de MIB. Este grupo proporcionaba una tabla que relacionaba direcciones IP y direcciones físicas. En MIB-II cada grupo de protocolo contiene su propia tabla.

Grupo IP

El Grupo IP, es obligatorio para todos los nodos administrables y proporciona información sobre el uso de IP en *hosts* y ruteadores. Este grupo provee un número de objetos escalares que provee estadísticas de datagramas y las siguientes tres tablas: Tabla de direcciones (ipAddrTable); Tabla de translación de direcciones IP a direcciones físicas (ipNetToMediaTable); Tabla de Ruteo (ipForwardTable).

Grupo ICMP

El Grupo Internet Control Message Protocol, es un componente obligatorio de IP y esta definido en el RFC 792. El Grupo ICMP proporciona mensajes de control y contiene 26 objetos escales que mantienen estadísticas de los diversos mensajes de ICMP, tales como número de mensajes ICMP de echo request recibidos o mensajes de ICMP redirect enviados. Este grupo es designado con el OID {1.3.6.1.2.1.5}.

Grupo TCP

Este grupo es obligatorio y provee información referente a la operación y conexiones TCP. Este grupo contiene 14 objetos escalares y una tabla. Los objetos escalares almacenan varios parámetros y estadísticas de TCP, tales como el numero de conexiones TCP que el dispositivo soporta, o el número total de segmentos transmitidos. La tabla, tcpConnTable, contiene información concerniente a una conexión TCP en particular. El OID de este grupo es {1.3.6.1.2.1.6}.

Grupo UDP

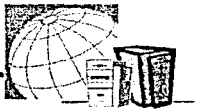
El grupo es obligatorio y proporciona información acerca de la operación de UDP. Debido a que UDP no es orientado a conexión, este grupo es menor que el grupo orientado a conexión TCP. Este no tiene que compilar información acerca de las conexiones, establecimiento, reset, etc. El grupo UDP contiene cuatro objetos escalares y una tabla. Los objetos mantienen estadísticas de datagramas, tales como número de datagramas enviados desde una entidad. La tabla, udpTable, contiene información acerca de puertos y direcciones. El OID de este grupo es {1.3.6.1.2.1.7}.

Grupo EGP

El grupo Exterior Gateway Protocol (EGP), es obligatorio para todos los sistemas que implementan EGP. EGP se comunica entre sistemas autónomos, el RFC 904 lo describe a detalle. Este grupo incluye cinco objetos escalares y una tabla. Los objetos mantienen estadísticas de mensajes. La tabla egpNeighTable, contiene información sobre vecinos EGP. El OID de este grupo es {1.3.6.1.2.1.8}

Grupo CMOT(OIM)

Durante el desarrollo de Internet Network Management Framework, estaba la labor de utilizar SNMP como un paso intermedio para un estándar de administración de red, y hacer Common Management Information Protocol (CMIP) sobre TCP/IP (CMOT) un termino a utilizar. Como resultado CMOT grupo fue colocado en MIB-II. La experiencia mostró, sin embargo que SNMP no es un paso intermedio, y que el protocolo de administración de red OSI solo requería de MIBs.



Grupo Transmisión

Este grupo contiene objetos relacionados con la transmisión de datos. RFC 1213 no define ninguno de estos objetos explícitamente. Sin embargo, el documento menciona que estos objetos de transmisión residirán en el subárbol experimental {1.3.6.1.3} hasta que hayan sido aprobados.

El documento «Assigned Numbers» lista los siguientes objetos bajo el grupo de transmisión.

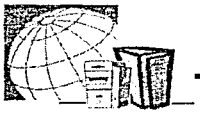
- X25 Objetos paquete X.25
- IEEE802.3 Objetos CSMA/CD
- IEEE802.4 Objetos Token Bus
- Dot5 Objetos *Token Ring*
- FDDI Objetos FDDI
- LAPB Objetos X.25 LAPB
- DS1 Objetos T1
- E1 Objetos E1
- PPP Objetos Point to Point Protocol
- DS3/E3 Objetos Interface DS3/E3
- SIP Objetos Interface SMDS
- FRAME-RELAY Objetos *Frame Relay*
- RS-232 Objetos RS-232
- Parallel Objetos Impresora paralelo
- ARCNET Objetos red ARC
- ATM Objetos ATM
- MIOX25 Objeto Multiprotocol interconnect sobre X.25
- SONET Objeto SONET

RFC 1700 también lista las referencias de RFC que proporcionan detalles de estos tipos de transmisión.

Grupo SNMP

Proporciona información acerca de los objetos SNMP. Hay un total de 30 objetos escalares, incluyendo estadísticas de mensajes SNMP, el número de traps SNMP enviados. Este grupo le es asignado el OID {1.3.6.1.2.1.11} Los protocolos experimentales y el desarrollo de MIB que se pretende convertir en estándar utilizan el subárbol experimental(3). Todos los objetos bajo el subárbol DOD tienen identificador de objeto que inicia con 1.3.6.1.3.

El subárbol private(4) es utilizado para especificar objetos definidos unilateralmente., es decir, permite a los fabricantes registrar MIB para sus equipos. Para muchos sistemas de administración de red la parte que tiene mayor acceso de este subárbol es el nodo enterprises(1) o {private 1} . Una enterprise es una organización que ha registrado su propia extensión en la MIB. Cada enterprise puede crear atributos bajo este subárbol para sus productos.



2.9 PROTOCOLOS DE ADMINSITRACIÓN DE REDES

Existen numerosos dispositivos de red, tanto de *hardware* como de *software*, donde cada uno juega un rol diferente e importante en la área de las telecomunicaciones.

Cuando se comenzaron a utilizar estos dispositivos, los administradores de red demandaron una forma de configurar, monitorear y probar su equipo, por lo que cada proveedor comenzó a crear un producto que hablara con dicho equipo utilizando un lenguaje especial. Fue por ello que se implementaron los protocolos de administración de redes.

2.9.1 SNMP

El **Simple Network Management Protocol** (SNMP, Protocolo de Administración Simple de Red) está basado en el modelo cliente-servidor; donde al cliente lo llamaremos administrador o sistema de administración, y al servidor agente o sistema administrado. Se dice que es un protocolo simple debido a que el agente requiere de muy poco *software*, ya que la mayoría del poder de procesamiento y almacenamiento de datos reside en el sistema de administración, y solamente un subconjunto complementario de esas funciones reside en el agente.

SNMP incluye un conjunto limitado de comandos de administración y respuestas como se muestra en la figura 2.9.1.1. El sistema de administración contiene mensajes **Get** (Obtener), **GetNext** (Obtener Siguiente) y **Set** (Configurar) para obtener la información deseada o establecer el valor de una variable. El sistema administrado envía un mensaje **Response** (Respuesta) para completar el Get, GetNext o Set; además de enviar la notificación de un evento, trap, al sistema de administración para informarle alguna condición anormal en el sistema.

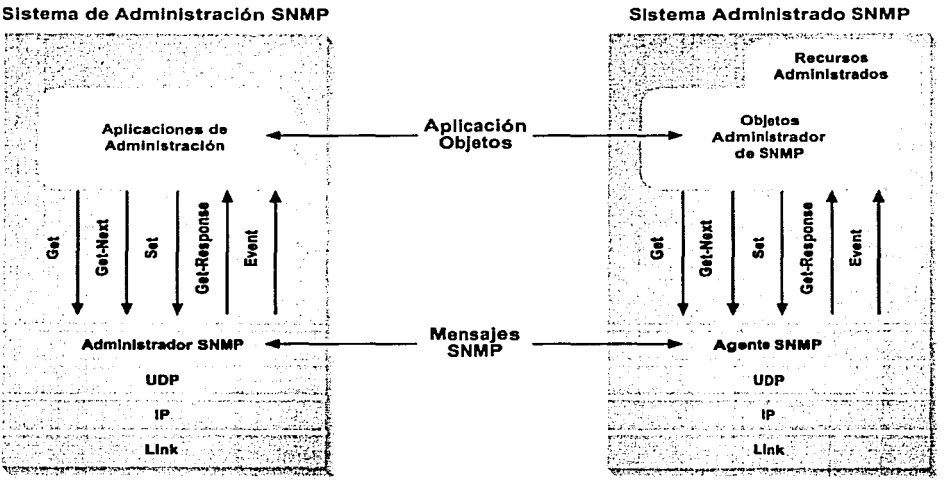


Figura 2.9.1.1 Arquitectura SNMP

El mensaje de SNMP es dividido en dos secciones: un identificador de versión (Version) y un nombre de Comunidad (Community), algunas veces llamados encabezado de autenticación de SNMP, y un Protocol Data Unit (PDU, Unidad de Protocolo de Datos) (Ver figura 2.9.1.2). Existen cinco diferentes tipos de PDUs: GetRequest, GetNextRequest, GetResponse, SetRequest y Trap.

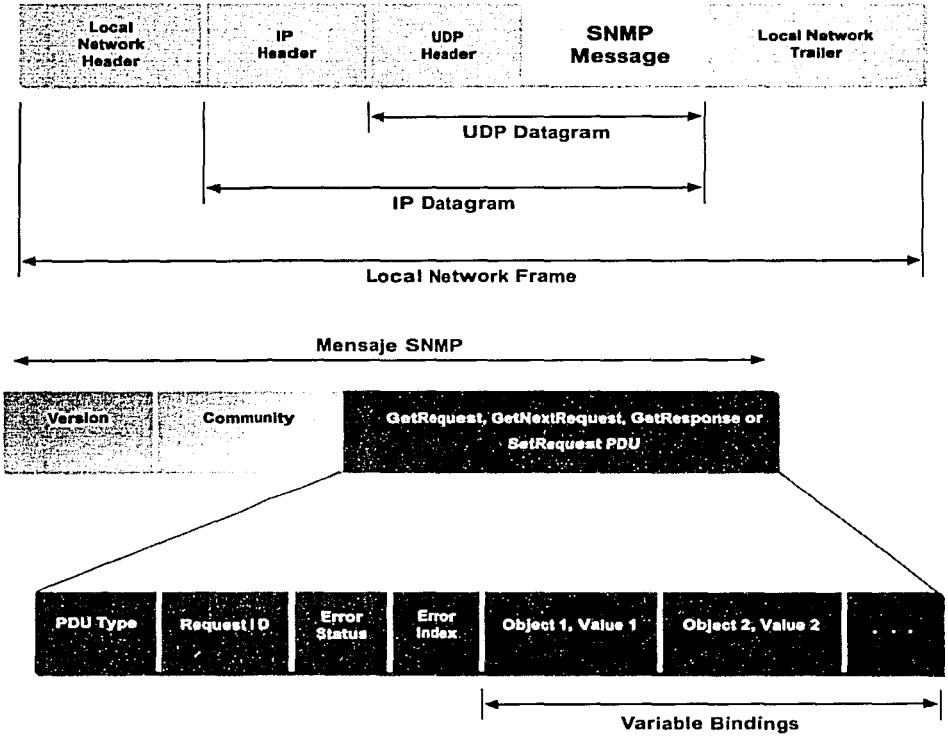
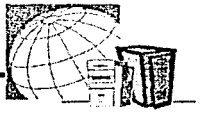


Figura 2.9.1.2 Mensaje SNMP

El campo Version asegura que tanto administrador como agente estén utilizando la misma versión de SNMP, si contienen diferentes versiones el mensaje es descartado. El campo Community autentica al administrador antes de permitirle el acceso al agente, el nombre de la comunidad junto con la dirección IP del administrador son almacenados en el agente.

Las PDUs Get Request, SetNextRequest, GetRequest y GetResponse comparten un mismo formato. El campo PDU **Type** (Tipo) contiene un valor entero:



PDU	Valor del campo Type
GetRequest	0
GetNextRequest	1
GetResponse	2
SetRequest	3
Trap	4

El campo Request ID correlaciona la petición del administrador con la respuesta del agente. El campo **Error Status** (Estado de Error) indica una operación normal (noError) o una de cinco condiciones de error: **TooBig** (Muy Grande), **noSuchName** (No existe el nombre), **badValue** (Valor Incorrecto), **readOnly** (Solo Lectura), **genErr** (Error No Definido).

Cuando ocurre un error, el campo Error Index (Índice) identifica la entrada dentro de la lista de **Variable Bindings** (Ataduras Variables) que causan el error. Por ejemplo, si ocurre en error readOnly, regresaría un Error Index = 4.

El campo Variable Binding contiene parejas de datos, el nombre de una variable y su valor.

GetRequest PDU

El administrador utiliza esta PDU para obtener el valor de uno o más objetos de un agente. En la figura 2.9.1.3 se muestran las PDUs que viajan en la red y los valores de cada uno de sus campos.

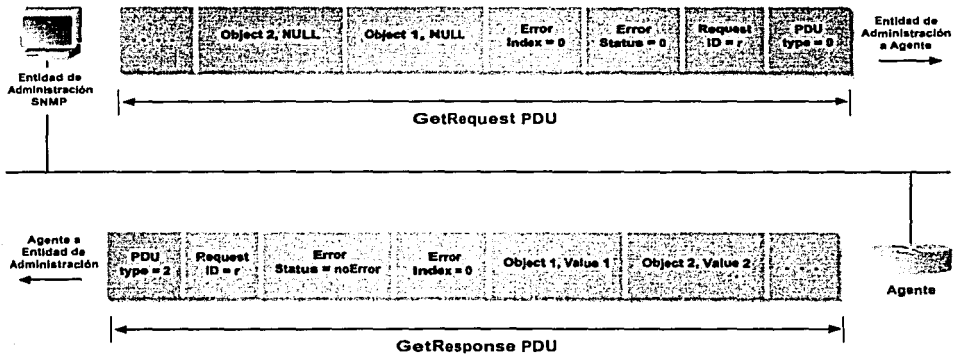


Figura 2.9.1.3 Transmisión de las PDUs GetRequest y GetResponse

GetNextRequest

El administrador la utiliza para obtener uno o más objetos de un agente. En muchos casos, estos objetos múltiples residen en una tabla. En la figura 2.9.1.4 se muestran los campos de este PDU y de la de respuesta con sus respectivos valores. La diferencia entre GetRequest y GetNextRequest es que GetNextRequest obtiene el valor del siguiente objeto dentro de las MIBs de los agentes.

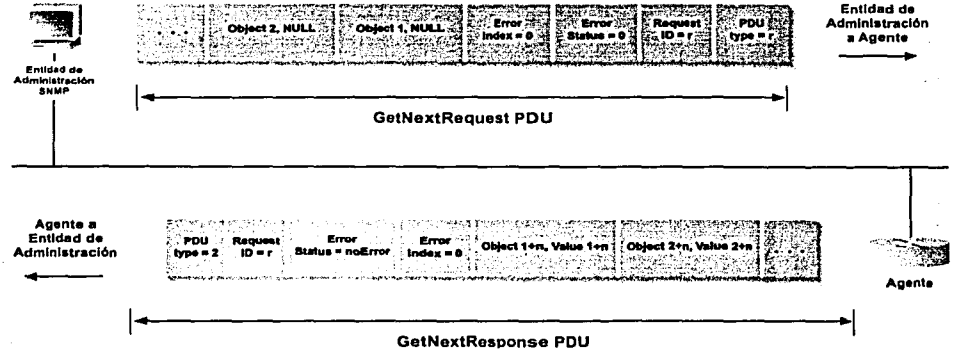


Figura 2.9.1.4 Transmisión de las PDUs GetNExtRequest y GetNextResponse

SetRequest

El administrador la utiliza para asignar un valor a un objeto que reside en el agente. En la figura 2.9.1.5 se muestran las PDUs con los valores de sus campos.

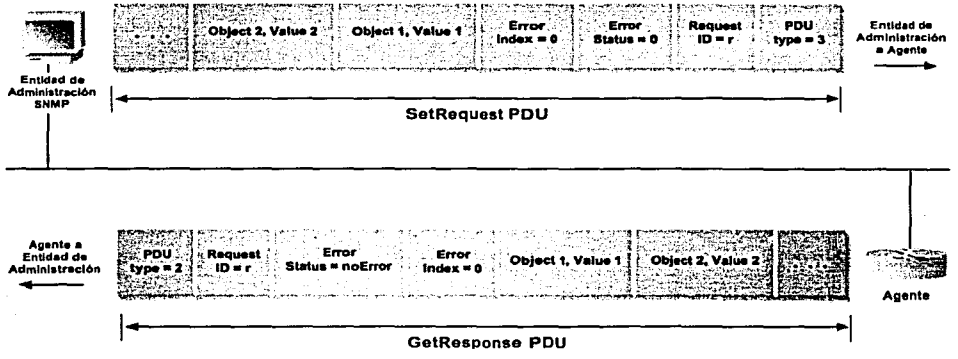
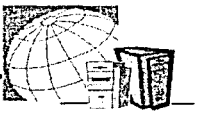


Figura 2.9.1.5 Transmisión de las PDUs SetRequest y GetResponse

Trap



Su formato es distinto a los cuatro anteriores, como se puede observar en la figura 2.9.1.6. El primer campo indica el tipo de PDU = 4. El campo Enterprise identifica al nombre del proveedor bajo el cual se definió el Trap. El campo Agent Address contiene la dirección IP del agente; si no se está utilizando el protocolo IP, regresa un valor de 0.0.0.0. El campo Generic Trap Type provee mayor información sobre el evento que se está reportando.

El campo Timestamp contiene el valor del objeto sysUpTime, que representa el tiempo entre la última reinicialización del agente y la generación de esa Trap (Mensaje de alarma). El último campo contiene los Variable Bindings.

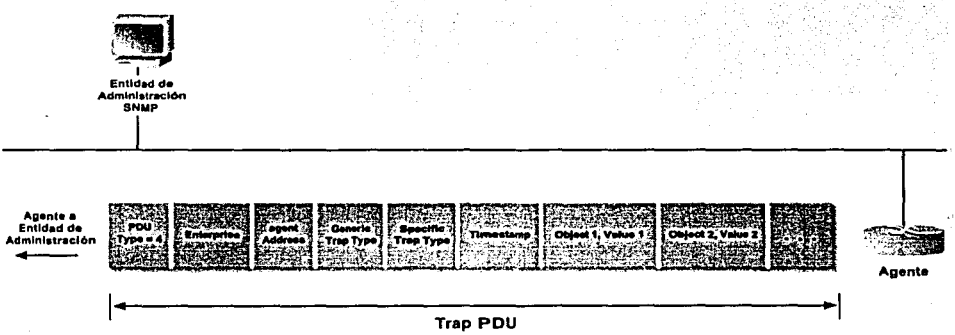


Figura 2.9.1.6 Transmisión de la PDU de Trap

El agente utiliza esta PDU para alertar al administrador de que un evento predefinido ha ocurrido. Las Traps son específicas para cada aplicación.

2.9.2 SNMPv2

SNMPv2 provee tres tipos de acceso a la información de administración de la red. El primer tipo es un request-response, donde un administrador envía una petición e un agente, y este último responde. El segundo tipo es un request-response donde ambas entidades son administradores. El tercer tipo es una interacción no confirmada, donde un agente envía mensajes no solicitados al administrador, trap, sin recibir respuesta.

SNMPv2 define ocho tipos de PDU, de las cuales tres son nuevas:

GetBulkRequest, InformRequest y Report. Además, el formato del trap de SNMPv2 ha sido modificado para que tenga el formato y estructura de las otras PDUs.

La siguiente tabla muestra la lista de PDUs de SNMPv2:

PDU	Descripción
GetRequest	Obtiene valores de los objetos listados dentro del campo Variable Bindings.
GetNextRequest	Obtiene valores de objetos múltiples.
Response	Generado en respuesta a GetRequest, GetNextRequest, GetBulkRequest, SetRequest o InformRequest.
SetRequest	Establece el valor de una variable
GetBulkRequest	Obtiene una gran cantidad de datos, como por ejemplo el contenido de una gran tabla.
InformRequest	Permite a un administrador proporcionar información en su vista de MIBs a otro administrador.
SNMPv2-Trap Report	Señal de alarma. Incluida en SNMPv2 pero no definida en un RFC. Su uso y semántica no están bien definidos.

El mensaje de SNMPv2 consiste en la capa que encapsula una PDU de SNMPv2. La capa es determinada por una estructura administrativa y puede contener información aislada y de autenticación.

La PDU contiene cuatro campos: Type, Request ID, Error Status y Error Index; además de las Variable Bindings, como se muestra en la figura 2.9.2.1.

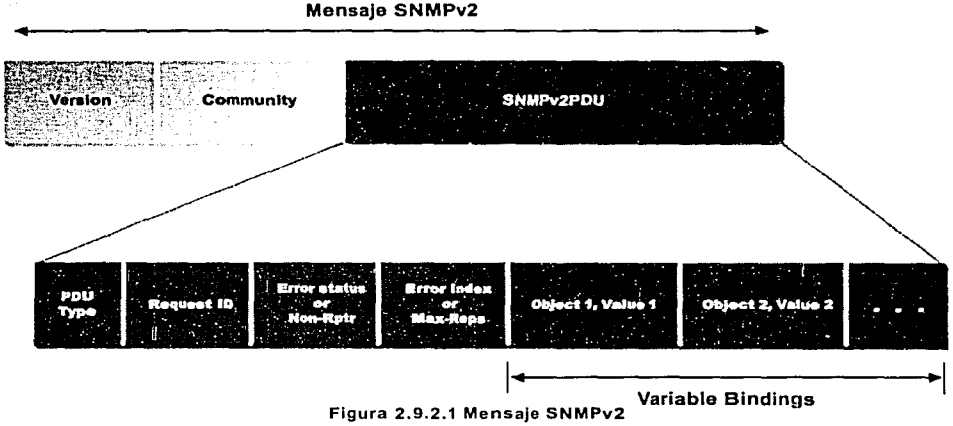
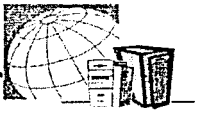


Figura 2.9.2.1 Mensaje SNMPv2



El campo PDU Type especifica cual de las ocho PDUs está siendo transmitida. El Request ID correlaciona las PDUs de Request y Response.

El campo Error Status incluye condiciones nuevas. Cuando un error ocurre en el procesamiento del GetRequest, GetNextRequest, GetBulkRequest, SetRequest o InformRequest, la entidad de SNMPv2 prepara un Response con el campo Error Status establecido para ayudar al sistema de administración a identificar y corregir el problema. Las primeras cuatro PDUs tienen exactamente la misma función que en SNMPv1, y la última prácticamente no se utiliza, por lo que solamente describiremos las siguientes tres.

PDU GetBulkRequest
Esencialmente ejecuta múltiples peticiones GetNext, su estructura es similar a la de las otras PDUs, solo cambia la sintaxis de dos campos. Remplaza Error Status con Non-Repeaters y Error Index con Max-Repetitions, donde el campo Non-Repeaters define el número de variables solicitadas que no serán procesadas repetidamente. El campo Max-Repetitions define el número máximo de ejecuciones.

PDU InformRequest
Este lleva a cabo la comunicación administrador-administrador y no agente-administrador.

PDU SNMPv2-Trap
Actualmente el trap de SNMPv1 es obsoleto, y ha sido reemplazado por la SNMPv2-Trap, que mantiene una estructura consistente con la de las otras PDUs. El agente transmite una SNMPv2-Trap cuando ocurre un evento excepcional.

SNMPv1 originalmente fue definido para transmitir sobre UDP e IP. SNMPv2 formalmente define implementaciones sobre la capa de transporte del modelo OSI, el Protocolo de Entrega de Datagramas (DDP) de *Apple Talk* y el Intercambio de Paquetes entre Redes (IPX) de Novell.

SNMPv1 y SNMPv2 pueden trabajar en conjunto de dos maneras. Una, teniendo un agente proxy que traduzca los mensajes de una a la otra, como se muestra en la figura 2.9.2.2. Cuando se traduce de SNMPv2 a SNMPv1, las PDUs GetRequest, GetNextRequest o SetRequest de la entidad de administración se pasan directamente al agente de SNMPv1. GetBulkRequest se traduce en PDUs GetNext. Para traducir de SNMPv1 a SNMPv2, el GetResponse pasa sin ser alterado a la entidad de administración. Un Trap de SNMPv1 es mapeado a uno de SNMPv2 con las dos nuevas Variable Bindings, sysUpTime.0 y snmpTrapOID.0.

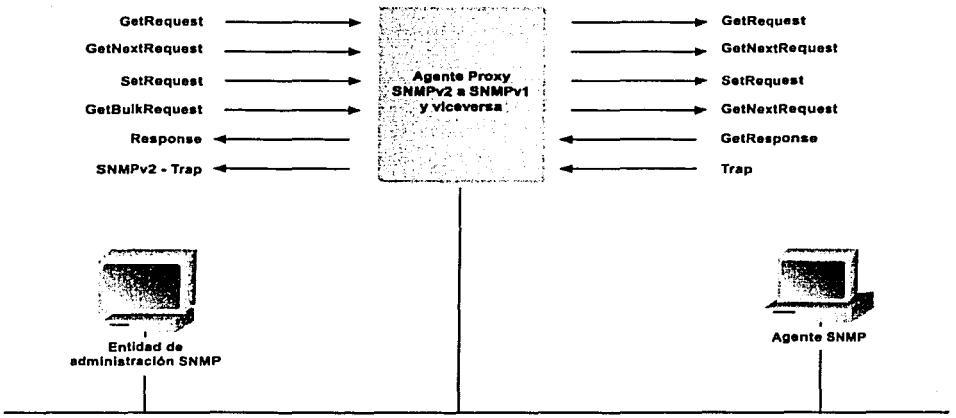


Figura 2.9.2.2 Interacción entre SNMPv1 y SNMPv2

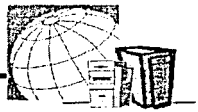
La segunda alternativa es una entidad de administración bilingüe, el cual incorpora ambos protocolos. Cuando la entidad de administración requiere comunicarse con el agente, selecciona el protocolo apropiado para la aplicación.

Cuando se publicó SNMPv1, el nombre de la comunidad y el número de la versión en el encabezado eran la única forma de seguridad que se manejaba. Para SNMPv2 se diseñó un direccionamiento de autenticación y privacidad en la comunicación de administración de la red, donde la autenticación asegura el origen correcto del mensaje y la privacidad protege al mensaje de ser descubierto.

Desgraciadamente la implementación de éstos probó ser más compleja de lo que se creía, y como consecuencia se desarrollaron muy pocos productos con estas características.

2.9.3 RMON

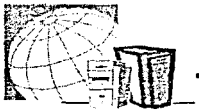
Remote MONitoring (RMON, Monitoreo Remoto) es un estándar para el monitoreo de tráfico en redes de área local (LAN). Es muy parecido a SNMP pero RMON permite un monitoreo remoto. Ambos estándares están basados en el hecho de que un agente remoto envía información a un sistema centralizado. A diferencia de SNMP, RMON permite al administrador de red tener acceso a información detallada del tráfico que circula en una red local sin necesidad de estar continuamente enviando Requests al servidor. En



RMON, el agente remoto va almacenando estadísticas y solo en caso de que el NMS lo pida, las estadísticas serán transferidas por la red.

El estándar de RMON está definido como una MIB dentro de la especificación de SNMP, es por esto que puede ser accesado utilizando el protocolo SNMP. Dentro de la especificación de RMON1 existen tablas conocidas como grupos. El agente remoto (conocido como RMON Probe) utiliza estas tablas estadísticas para recolectar datos del segmento de red en donde está conectado. La MIB deRMON es dependiente del estándar de red; es decir, existe un diferente tipo de MIB para cada tipo de estándar de red, siendo el de *Ethernet* el más común. El estándar RMON para *Ethernet* define los siguientes 9 grupos:

Grupo RMON	Función	Elementos
Statistics Group	Contiene estadísticas medidas por el RMON Probe para cada interfaz monitoreada del dispositivo.	Paquetes desechados, paquetes enviados, bytes enviados, paquetes de broadcast, paquetes de multicast, errores de CRC, fragmentos, colisiones, etc.
History Group	Graba muestras estadísticas de manera periódica de la red y las almacena para ser enviadas al NMS posteriormente.	Periodo de muestreo, número de muestras, elementos muestreados.
Alarm Group	Periódicamente toma muestras estadísticas de variables y las compara con umbrales previamente determinados en el RMON Probe. Si la variable monitoreada excede el valor del umbral se genera un evento. Un mecanismo de histéresis es implementado para limitar la generación de alarmas. Este grupo incluye la tabla de alarmas y requiere de la implementación del grupo de eventos.	Tipo de alarma, intervalo, umbral de inicio, umbral de fin.
Host Group	Contiene estadísticas asociadas con cada *host* descubierto en la red.	Dirección del *host*, paquetes y bytes recibidos y enviados, broadcast, multicast y paquetes erróneos.
Host TopN Group	Prepara una tabla ordenada a partir de los N *hosts* más activos con respecto a cierta variable. Las estadísticas disponibles son muestras de alguna variable base sobre un intervalo definido en la estación de administración. Lo cual significa que los valores de la tabla en realidad se refieren a la tasa del valor de una variable (p.e. Tasa de paquetes, tasa de errores, etc.)	Estadísticas, cuales *hosts*, periodos de muestreo de inicio y fin, tasa base, duración.

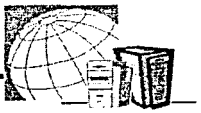


Matrix Group	Almacena estadísticas de conversacionesentre grupos de dos direcciones. En cuanto el dispositivo detecta una nueva conversación, crea una nueva entrada en la tabla.	Direcciones origen y destino, paquetes, bytes y errores de cada estación.
Filter Group	Permite que los paquetes sean filtrados mediante una ecuación. Dichos paquetes serán capturados o generarán un evento.	Filtro basado en el valor del bit, expresiones basados en el valor de los bits y condiciones de expresión (and, or, not, etc.) para con otros filtros.
Packet Capture Group	Permite que los paquetes sean capturados antes de ser enviados por el canal.	Tamaño del buffer para la captura de paquetes, estado de buffer lleno (alarma), número de paquetes capturados.
Event Group	Controla la generación y notificación de eventos desde éste dispositivo.	Tipo de evento, descripción, tiempo del último evento enviado.

La MIB de RMON2 añade los siguientes grupos:

- **Protocol Distribution:** Este grupo se encarga de analizar el porcentaje de tráfico por suite de protocolos (por ejemplo: IP, IPX, etc.) o por aplicación (por ejemplo: FTP, WWW, DNS, etc.)
- **Address Mapping:** Provee información adicional con respecto a los *hosts* (por ejemplo: Mapeo de dirección IP a nombre en el DNS)
- **Network Layer *Host* Table:** Se encarga de construir una tabla sobre variables como paquetes y errores por protocolo de red.
- **Application Layer *Host* Table:** Hace lo mismo que el grupo anterior pero solo que construye la tabla en base a la aplicación; y no en base al protocolo de red.
- **Application Layer Matrix Table:** Mantiene una matriz de conversaciones entre *hosts* por protocolo de aplicación.
- **Probe Configuration:** Provee una manera estándar de configurar agentes remotos con parámetros, como dirección, hacia donde los traps serán enviados, etc.
- **History:** Almacena estadísticas de acuerdo a filtros durante un periodo preestablecido de tiempo.

RMON se convirtió en un estándar en 1992. La especificación de RMON permite a los administradores de red hacer un diagnóstico específico del comportamiento de la red para poder estudiar y planear mejor los cambios; es decir, provee al administrador de información precisa con la que podrá realizar un mejor **perfomance tunning** (desempeño). Los nueve grupos de RMON mencionados anteriormente son opcionales, lo cual quiere decir que los proveedores no necesariamente deben soportar los nueve grupos en sus equipos.



Un equipo básico que soporta RMON puede brindar los siguientes tipos de información:

- Información que permita a los administradores realizar un análisis de la utilización de la red, incluyendo estadísticas de errores y datos por separado.
- Información histórica de la tendencia de la red y análisis estadístico.
- Matrices de información que describan las comunicaciones entre sistemas y la cantidad de datos que intercambiaron entre ellos.

La mayoría de los proveedores implementan solo la especificación suficiente de RMON en sus equipos (usualmente los 7 primeros grupos) para soportar las funciones de análisis del enlace de datos y el flujo de tráfico.

Un RMON Probe que implementa todos los grupos ofrece más capacidades para la captura de paquetes, permitiéndole ser usado como mecanismo de recolección de datos necesario para un análisis más exhaustivo y para ser utilizado en las aplicaciones de **accounting** (contabilidad).

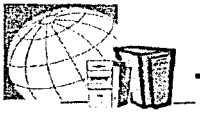
Los grupos 8 y 9 de RMON, brindan la información necesaria para soportar un análisis sofisticado de protocolos de red y funciones de accounting de la red como pueden ser:

- Envío de traps a los monitores de red para la generación de alarmas.
- Captura de paquetes para la descodificación de tráfico en la red.
- Fuentes de datos para soportar de accounting / billing sobre la utilización de la red.

2.9.4 CMIS / CMIP

SNMPv1 ha tenido un gran seguimiento y desarrollo por parte de la industria, y SNMPv2 contiene muchas características deseables para cualquier ingeniero en telecomunicaciones. Sin embargo, la suite (conjunto) de protocolos que mejor satisface las necesidades de administración de red es el protocolo de administración de redes OSI, **Common Management Information Services / Common Management Information Protocol** (CMIS / CMIP, Servicios de Información de Administración Común / Protocolo de Información de Administración Común).

CMIS define los servicios generales provistos por cada componente de la red para la administración de ésta; CMIP es el protocolo que implementa los servicios de CMIS.



CMIS / CMIP intentan proveer una suite de protocolos de administración completa de red para utilizarse con cualquier dispositivo.

Una diferencia básica entre CMIS / CMIP y cualquier versión de SNMP es que los protocolos CMIS / CMIP solicitan a un agente realizar muchas mas tareas. SNMP fue diseñado para tener la carga de administración en el dispositivo de administración, lo que permite al agente la simplicidad. CMIS / CMIP distribuye mas equitativamente esta carga, solicitando requerimientos de capacidad y recursos significativos en cada dispositivo administrado.

Llamaremos sistema abierto a cualquier componente de red que utilice el modelo OSI. A dos dispositivos que se comunican utilizando los protocolos OSI en la misma capa de este modelo los conoceremos como par de sistemas abiertos.

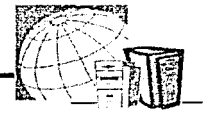
Los procesos de aplicación de administración de red utilizan la capa de aplicación del modelo OSI. Además en esta capa, el Common Management Information Service Element (CMISE) provee el medio para que las aplicaciones utilicen CMIP. CMISE, a su vez, utiliza otros dos protocolos de aplicación: Association Control Service Element (ACSE), el cual establece y cierra asociaciones entre aplicaciones, y Remote Operation Service Element (ROSE), que maneja las interacciones request / reply entre aplicaciones.

CMIS

Cada servicio CMIS es una operación simple que una aplicación de administración de red puede efectuar. Cualquier aplicación que lleva a cabo tareas de administración es un usuario de servicio CMISE. CMIS tiene definidas tres clases de servicio para usuarios de servicio CMIS, que son: Management Association Services (Servicios de Asociación Administrativa)

Esta primer clase controla la asociación entre el par de sistemas abiertos. Estos servicios son utilizados principalmente para establecer y liberar conexiones entre sistemas, controlar la inicialización, terminación anormal de una conexión de una asociación de administración con los siguientes servicios:

- M-INITIALIZE: instituye una asociación con un par de servicios de usuario CMISE para sistemas de administración.
- M-TERMINATE: finaliza una conexión entre un par de servicios de usuario CMISE.
- M-ABORT: utilizado cuando una conexión entre servicios de usuario CMISE finaliza anormalmente.



Estos servicios asumen el uso de servicios ACSE para la operación, desde que ACSE es utilizado para establecer y cerrar conexiones entre aplicaciones. Otros servicios CMIS, que utilizan una conexión existente para la administración de información, utilizan ROSE.

Management Notification Services (Servicios de Administración de Notificación)

Así como los mensajes trap de SNMP proveen información de eventos en la red, estos servicios proveen una funcionalidad similar para CMIS. El servicio M-EVENT-REPORT le dice al par de usuarios de servicio CMISE acerca de un evento que ha ocurrido en otro usuario de servicios CMISE.

Management Operation Services (Servicios de Administración de Operación)

Estos servicios son:

- M-GET
- M-CANCEL-GET
- M-SET
- M-ACTION
- M-CREATE
- M-DELETE

El servicio M-GET, utilizado por un usuario de servicio CMISE para recuperar información de administración de un par de usuarios de servicio CMISE, es análogo al mensaje Get-Request de SNMP. M-CANCEL-GET es usado para cancelar un M-GET después de enviarlo y antes de recibir respuesta.

El servicio M-SET permite a un usuario de servicio CMISE modificar la información de administración de un par de usuarios de servicio CMISE. Este es similar al mensaje Set-Request de SNMP.

El servicio M-ACTION es invocado por un usuario de servicio CMISE para pedirle a un par de usuarios de servicio CMISE que ejecute una acción deseada. Estas acciones son específicas para cada dispositivo. Este concepto es similar al mensaje Set-Request de SNMP. La figura 2.9.4.1 muestra un ejemplo del uso de M-ACTION.

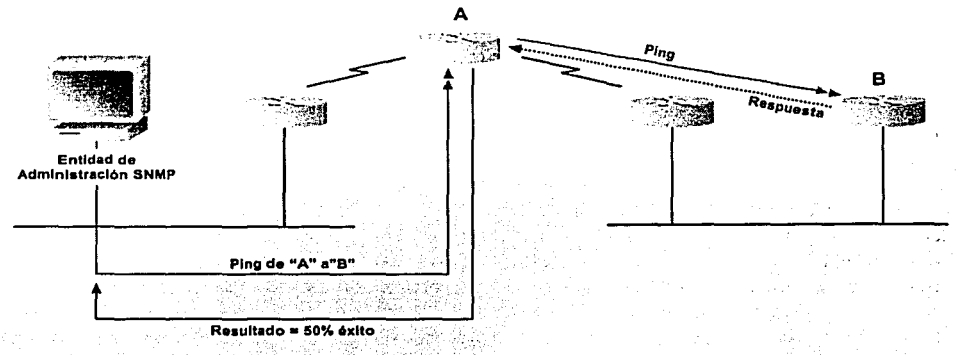


Figura 2.9.4.1 Ejemplo de M-ACTION

El servicio M-CREATE es utilizado por un usuario de servicio CMISE para solicitarle a un par de usuarios de servicio CMISE que cree otra instancia del objeto administrado. El objeto administrado representa al usuario de servicio CMISE en un agente. En CMIS cada objeto administrado tiene una instancia asociada. CMIS permite muchas instancias del mismo objeto, pero solo una definición de este.

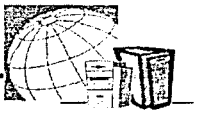
El servicio M-DELETE es utilizado por un usuario de servicio CMISE para solicitar que un par borre una instancia de algún objeto administrado.

Asociaciones de Administración

Una asociación de administración es una conexión entre dos pares de sistemas abiertos para la administración de sistemas. Cuatro tipos de asociaciones pueden existir entre pares de sistemas abiertos:

- Eventos. Permite a dos sistemas abiertos enviar mensajes M-EVENT-REPORT.
- Evento / Monitoreo. Esta asociación es igual que la de evento, excepto que cada sistema también puede recibir y generar mensajes M-GET.
- Monitoreo / Publicación. Esta es permitida para la comunicación de peticiones M-GET, M-CANCEL-GET, M-SET, M-CREATE, M-DELETE y M-ACTION, aunque no se permiten reportes de eventos.
- Administrador / Agente Completo. Esta asociación soporta lo servicios CMIS.

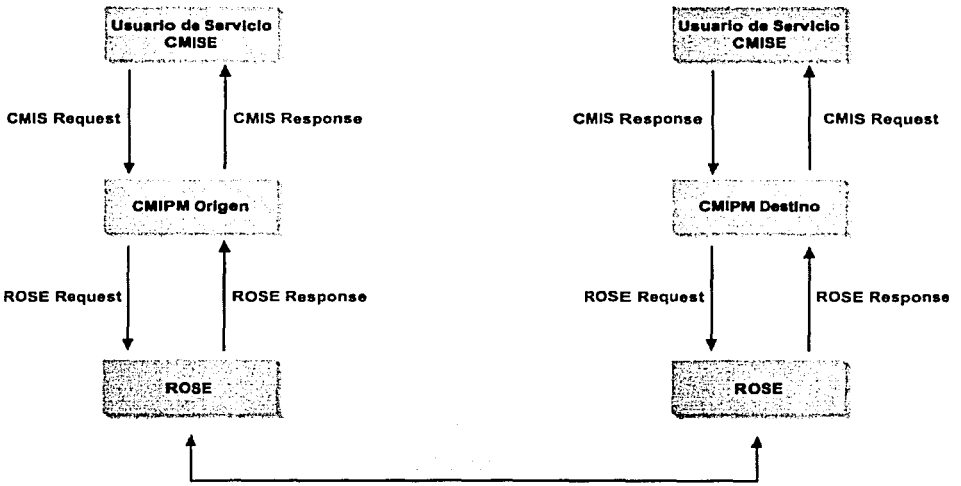
Listas de Acceso



Al igual que la cadena community de SNMPv1 y los contextos y grupos de SNMPv2 para verificar que un sistema pueda accesar a la información de administración, CMIS utiliza listas de acceso.

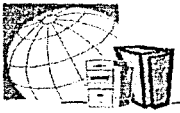
CMIP

El protocolo que implementa CMIS es el Common Management Information Protocol (CMIP), el cual requiere una máquina CMIP (CMIPM) para funcionar de acuerdo a una especificación definida. El CMIPM es un *software* que realiza dos tareas: Primero, acepta operaciones enviadas a él por un usuario de servicio CMISE e inicia el procedimiento apropiado para cumplir con la operación asociada. Segundo, el CMIPM utiliza ROSE para enviar mensajes a través de la red. La figura 2.9.4.2 muestra el flujo de una petición de servicio CMIS entre dos usuarios de servicio CMISE.



CMIP únicamente define como descifrar la información en un paquete; este no state lo que un usuario de servicio CMISE debería hacer con la información solicitada por un objeto administrado.

Existen dos principales problemas con CMIS / CMIP, primero, requiere una gran cantidad de recursos de cómputo. Segundo, es difícil de implementar.



El Common Managemet Information Services and Protocol sobre TCP / IP (CMOT) tiene el propósito de implantar el servicio CMIS en la parte superior de la suite de protocolos TCP / IP.

CMOT requiere el uso de otro protocolo en la misma capa del modelo OSI, el Lightweight Presentation Protocol (LPP, Protocolo de Presentación Ligero), el cual provee la interfaz a cualquiera de los protocolos de la capa de transporte UDP y TCP.

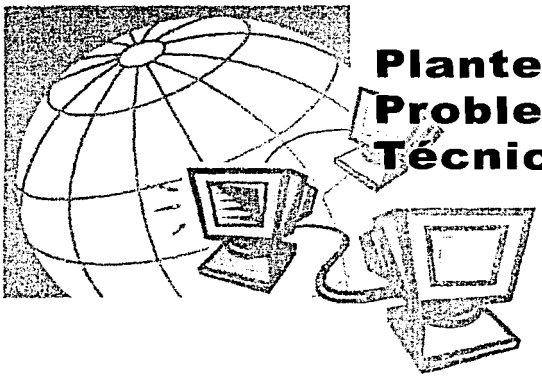
El problema con este es que las empresas no han querido gastar tiempo implementando herramientas que lo utilicen, en su lugar usan SNMP.

Esperamos que la explicación que se dio en los capítulos anteriores sirva de base para fundamentar el complemento de nuestro trabajo de tesis, que consiste en delimitar el problema y proponer la solución más adecuada.

A continuación, en el capítulo 3, entramos de lleno al proceso de solución, en donde utilizamos toda la información expuesta en los dos capítulos anteriores. Por un lado recordando la operación actual de la red, hasta antes de la implementación de la solución, exponiendo las necesidades tanto actuales como futuras de los usuarios de la red.

Posteriormente en el último capítulo estableceremos de manera puntal la forma en que integraremos los sistemas y presentaremos el prototipo de la solución que consideramos más viable para el Instituto.

CAPITULO III



Planteamiento del Problema y Propuesta Técnica

3.1 OPERACIÓN ACTUAL DE LA RED NACIONAL DE INFORMÁTICA DEL IFE

Como se trato en el primer capítulo, la infraestructura de la red de cómputo y comunicaciones del Instituto Federal Electoral ha ido creciendo y volviéndose más compleja con el fin de cubrir la necesidad de que las diferentes áreas cuenten con sistemas de comunicación para el intercambio de información y cumplir con sus diversas tareas y actividades.

Pero no solo es necesario la correcta planeación en el proceso de instalación de la infraestructura de red y comunicaciones, de igual forma es indispensable contar con sistemas que permitan la constante operación de ésta y se tenga la capacidad de tener información histórica de eventos y fallas para poder realizar un análisis del desempeño de la red y sus componentes.

La mayor parte de los sistemas de los que hace uso y esta desarrollando el Instituto, operan bajo un esquema descentralizado y consolidaciones de Bases de Datos de forma constante y periódica, para la captura y consulta de información, haciendo de esta manera un uso intensivo de la infraestructura de la red nacional de informática. Por lo que, se requiere solucionar los problemas que se presenten de forma proactiva, es decir, ser capaces de detectar las posibles fallas antes de que el usuario las reporte, así como realizar análisis y pronostico del desempeño de la infraestructura y uso de los servicios .

Antes de instalarse la infraestructura de cómputo y comunicaciones para la red nacional de informática, la comunicación entre las áreas del Instituto se

realizaba solamente utilizando teléfono, fax y paquetería. Por ello, la mayor parte del personal no cuenta con los conocimientos necesarios para trabajar con una computadora personal; este trabajo generalmente es delegado al área secretarial.

En virtud del atraso tecnológico y de los rezagos en cultura informática del Instituto, la infraestructura de red instalada se tiene que administrar de forma centralizada, ya que no se cuenta con personal capacitado en cada una de las redes locales remotas para operar los equipos de cómputo (servidores) y comunicaciones.

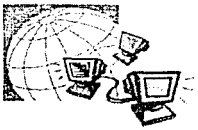
La Unidad Técnica de Servicios de Informática, encargada de la operación y administración de la red, cuenta con pocos recursos humanos para realizar todas las actividades que tiene encomendadas. Inclusive, no cuenta con herramientas que le permitan automatizar procesos y actividades, por lo que el personal debe desarrollar sus propias herramientas para poder mantener cierto nivel de servicio.

Esto no permite aprovechar al máximo la capacidad de los recursos humanos de la Unidad y causa tiempos de respuesta inadecuados en la atención de fallas.

En la figura 3.1.1 se muestra de forma esquemática la situación actual de la operación y administración de la red nacional de informática del IFE, es decir, se puede apreciar el flujo de información de las áreas que interactúan con los usuarios de la red para poder llegar a resolver algún problema que se presente ya sea en los servicios, o sistemas de red, así como en los equipos de cómputo y comunicaciones.

El usuario de RedIFE, al enfrentarse a algún problema en el uso de la infraestructura de cómputo, principalmente en la utilización de algún sistema o aplicación, reporta a cualquiera de las áreas de la Unidad Técnica de Servicios de Informática , ya sea mediante oficio, llamada telefónica o correo electrónico.

Al no contar con aplicaciones para el monitoreo de la red, la solución de problemas se lleva a cabo de forma reactiva: el usuario reporta una falla en el servicio de red antes de que el personal encargado de la operación lo detecte, en la mayoría de los casos. Adicionalmente, el registro de eventos y fallas en los equipos se tiene que hacer de forma manual, por lo que los datos recopilados no pueden ser manipulados de forma eficiente para una atención proactiva.



Los problemas asociados a los reportes de los usuarios, los podemos agrupar en las siguientes categorías:

- Servicios de red
- Sistemas en red
- Equipos de computo
- Equipos de Comunicaciones
- Enlaces de Comunicaciones

No existe una base de datos para el registro de los problemas reportados por el usuario o presentados en la infraestructura de red y servicios ofrecidos. Asimismo tampoco se cuenta con la información relacionada al funcionamiento de los equipos o enlaces, provocando que no se puedan generar reportes acerca del desempeño y funcionamiento de la infraestructura de la red. Como consecuencia de lo anterior, no se puede realizar un análisis para dimensionar el crecimiento futuro.

Al recibir un reporte, cualquiera de las áreas que conforman la UNICOM, (Soporte Técnico, Comunicaciones, Administración de Servidores, Personal administrativo, etc), trata de realizar un primer diagnostico del problema, analizando los síntomas de éste, y deciden si les corresponde atender el problema.

En caso de que no les corresponda la atención de dicho problema, éste es reasignado al área correspondiente de acuerdo al diagnóstico que se haya realizado. El área a la cual se le haya reasignado el problema, realiza nuevamente el análisis de la situación para determinar si realmente le corresponde la atención.

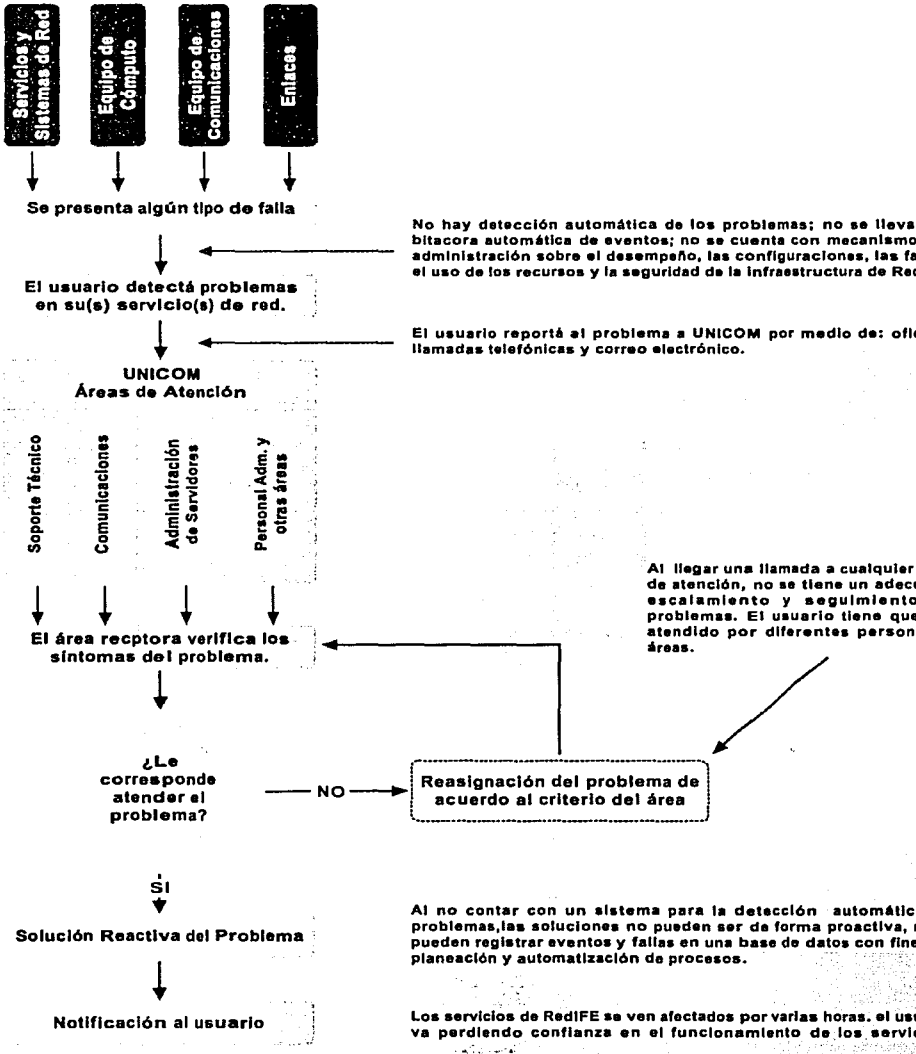


Figura 3.1.1 Operación y Administración actual de la Red Nacional de Informática del IFE

El registro de las llamadas se hace de forma manual, lo cual no permite obtener resultados estadísticos acerca del servicio: llamadas recibidas, llamadas perdidas, tiempo de solución del problema, etc, así mismo no se lleva un control del registro y seguimiento eficiente a los reportes, así como control de la reasignación de problemas a las demás áreas.

Debido a esto el servicio se puede ver afectado por varias horas, ya que si no se notifica de manera adecuada y no se le da el correcto seguimiento, un problema puede quedar sin atender por un período considerable de tiempo, provocando conesto la falta de satisfacción del usuario y con ello, se va perdiendo la confianza en el funcionamiento de los servicios.

Al ver la necesidad de contar con una herramienta de administración y monitoreo de la infraestructura de computo y comunicaciones del Instituto, se han desarrollado por el personal operativo herramientas que se compone de una gran cantidad de programas desarrollados de forma aislada y sin interacción o mínima interacción entre ellos.

Algunas de las herramientas que se han desarrollado son:

3.1.1 Seguimiento de reportes

Para poder llevar un mejor seguimiento de los reportes que se generan en cada una de las áreas dentro de la UNICOM, cada área cuenta con un pequeño sistema para abrir reportes, en el cual se concentra información del problema y usuario que esta siendo afectado, así como la información que pueda ser útil para la solución del mismo. Los sistemas de cada área de acuerdo a sus necesidades, obtiene diferente tipo de información y en diferentes formatos, que pueden ir desde tener la información en una base de datos, hasta en un archivo de texto, es decir, no es un solo sistema. Esto es, se han desarrollados sin considerar la integración con la información que cuentan las demás áreas. Otro punto importante es que no se pueden visualizar los reportes de otra área de una manera automática, provocando que se pueda estar tratando de dar solución a un mismo problema desde dos áreas diferentes.

Cuando se realizan reasignación de problemas generalmente se realiza de manera verbal, o mediante un correo electrónico. El correo electrónico no siempre es enviado a toda el área o encargado de ésta, sino a solo parte de la misma, provocando que si un problema se reasigna y solo es enviado a una persona en particular, y dicha persona no se encuentra, el problema quedaría en espera de ser atendido, causando insatisfacción en el usuario.

Debido a la falta de integridad de las herramientas para llevar el seguimiento de los reportes y fallas, no es posible llevar una base de conocimiento para la

solución de problemas tipo, y esto provoca que el tiempo de solución no pueda disminuir, así como la capacitación de personal de nuevo ingreso sea paulatina.

3.1.2 Monitoreo de enlaces

Se cuenta con diferentes tipos de enlace para comunicarnos a los órganos desconcentrados del Instituto, estos son :

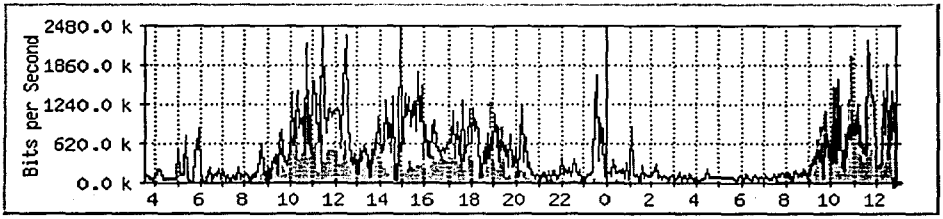
- Enlaces DS0 (Frame-Relay) a Juntas Ejecutivas Distritales y Locales
- Enlaces telefónicos (Respaldo) a Juntas Ejecutivas Distritales y Locales
- Enlaces DS0 y E1 a Oficinas Centrales en el área metropolitana.
- Enlaces E1 - conexión con nuestros servidores de servicio de Internet.

Para poder llevar un control de su correcto funcionamiento se desarrollo una herramienta, la cual haciendo uso del programa PING, -el cual mediante mensajes de ICMP proporciona información si un dispositivo esta activo-, ha determinadas horas del día se ejecuta desplegando información acerca si tenemos acceso al dispositivo que esta recibiendo el enlace.

El que en la salida del programa indique que el dispositivo no esta activo, esto no significaría que el enlace esta fuera de servicio, se tendría que verificar si la falta de comunicación se debe a el medio físico o al equipo que recibe el enlace, entre otras causas, así es como se esta realizando el monitoreando, aunque no en tiempo real, a ciertas horas del día.

Otra herramienta que se instalo para la obtención de estadística de utilización de los enlaces es **Multi Router Traffic Grapher** MRTG, la cual permite obtener vía mensajes de SNMP cierta información de los enlaces de comunicación como utilización, procesamiento de un ruteador. En la figura 3.1.2.2 se muestran un ejemplo de las gráficas que se pueden obtener con MRTG.

Daily' Graph (5 Minute Average)



Max In	2027.0 kb/s (51.1%)	Average In 211.6 kb/s (5.3%) Current
In	470.0 kb/s (11.8%)	
Max Out	2477.2 kb/s (62.4%)	Average Out 437.3 kb/s (11.0%) Current
Out	511.5 kb/s (12.9%)	

Figura 3.1.2.2 Gráfica de Utilización de un enlace de comunicaciones mediante MRTG.

Un inconveniente de MRTG es que los datos no son en tiempo real, y como son peticiones de información a cada uno de los enlaces, dichas peticiones no pueden ser muy constantes, porque consumen muchos recursos del equipo donde se encuentra trabajando MRTG.

En la mayor parte de los casos los enlaces que se encuentran fuera de servicio, se detectan, debido a que el usuario, reporta que no puede navegar en Internet, o que no puede acceder a información que se encuentra en un servidor fuera de su red local.

3.1.3 Monitoreo de equipos de comunicaciones y servidores

Para realizar el monitoreo de los equipos de comunicaciones y servidores, se utiliza la misma herramienta que se describió para verificar el funcionamiento de los enlaces de comunicaciones, es decir, se realizan ping a los equipos que se desean monitorear, en este caso son:

Juntas Ejecutivas Distritales y Locales:

- Ruteador
- Concentrador(es)
- Servidor

Oficinas Centrales dentro y fuera del complejo Tlalpan.

- Ruteador(es)
- Concentrador(es)
- Switch(es)
- Servidores Centrales

En la tabla 3.1.3.1 se muestra la salida del programa (IPScan) que permite el monitoreo de enlaces, y equipos de computo y comunicaciones.

[01] Aguascalientes						
Junta	SP	SB	A0	E0	HB	SV
000	Ok	Ok	**	Ok	Ok	Ok
001	Ok	Ok	**	Ok	OK	OK
002	Ok	Ok	OK	Ok	**	Ok
003	Ok	Ok	OK	Ok	Ok	**

[SP]: OK=04 | **= 00
[SB]: OK=04 | **= 00
[A0]: OK=02 | **= 02
[E0]: OK=04 | **= 00
[HB]: OK=03 | **= 01
[SV]: OK=03 | **= 01

Tabla 3.1.3.1 Información que presenta el programa IPScan

En la salida del programa se puede apreciar si se encuentra funcionando el enlace principal *Frame Relay* (SP), el enlace de respaldo *Frame Relay* (SB), el enlace telefónico de respaldo (A0), la interfaz *Ethernet* del ruteador (E0), el concentrador (HB) y el servidor (SV).

En el caso de que alguno de ellos aparezca «**» significa que no se recibió respuesta de la interface del ruteador relacionada. Por otra parte, los respaldos de información (configuraciones, bases de datos y sistemas) se hacen de forma manual. El registro de eventos y fallas en los equipos al realizarse de forma manual; los datos recopilados no pueden ser manipulados de forma eficiente para una atención proactiva, sobre todo en el caso de fallas.

Al no contar con herramientas adecuadas que permitan generar reportes acerca del desempeño y funcionamiento de la infraestructura de cómputo y comunicaciones, el análisis para dimensionar el crecimiento de la infraestructura que soporta las aplicaciones y servicios de RedIFE se vuelve complejo.

3.2 NECESIDADES DE LOS USUARIOS DEL INSTITUTO

La red nacional de cómputo del Instituto Federal Electoral es una de las innovaciones tecnológicas que ha tenido a bien adoptar el IFE con el fin de aprovechar las ventajas de una herramienta tan poderosa y versátil como una red de cómputo institucional.

Antes de 1991, el Instituto no contaba con redes de cómputo y por consecuencia, todas las actividades se llevaban a cabo de forma manual, utilizando los medios de comunicación básicos para la operación normal: teléfono, fax, mensajería y paquetería. Las computadoras, en aquel entonces, eran escasas y solo se utilizaban para actividades muy específicas, relacionadas con la áreas administrativas.

Red del Registro Federal Electoral: Primeros Usuarios

Como se mencionó anteriormente, el IFE se constituyó a raíz de las reformas electorales de 1990, teniendo a su cargo entre otras importantes actividades, la conformación de un padrón electoral completamente nuevo, por lo cual era necesario la implantación de un sistema de cómputo para el mantenimiento de la base de datos que tendría que generar. Después de un análisis y revisión exhaustiva de las tecnologías y productos en el mercado, se diseño una red de cómputo exclusiva para el funcionamiento del Sistema de Actualización Permanente de padrón electoral, conocido como SAP. La implementación de este desarrollo se llevo a cabo en 1991, teniendo a su cargo la Dirección Ejecutiva del Registro Federal Electoral el mantenimiento y operación de la infraestructura instalada, compuesta por 17 Centros de Cómputo Regionales, de los cuales uno funge como el Centro de Cómputo Nacional donde se consolidan las bases de datos para la verificación y eliminación de posibles duplicados.

Para operar el Sistema de Actualización Permanente fue necesario capacitar y contratar en su momento a personal con un perfil técnico en diferentes ramas del cómputo:

- Capturistas
- Programadores
- Administradores de Bases de Datos
- Administradores de Servicios de Red
- Administradores de Servidores
- Ingenieros de redes
- Técnicos en Comunicaciones y Soporte

Generalmente la gestión del cambio es uno de los pasos más complicados al implementar nuevas tecnologías en las organizaciones, ya que en la mayoría de las ocasiones, la operación normal y procedimientos de la organización deben sufrir un cambio radical. Esto siempre es una inversión a mediano o largo plazo, por lo cual su planeación y definición deben realizarse tomando en cuenta todos los elementos involucrados.

En una red de datos, existen usuarios a diferente nivel y con diferentes necesidades. Para los ingenieros de redes y técnicos en comunicaciones, los usuarios son todas las personas de la organización que tienen una computadora en su escritorio conectada a la red de datos institucional; para el administrador de servidores, el universo de usuarios puede reducirse a simplemente los administradores de bases de datos y administradores de servicios de red, pero esto es muy relativo, dependiendo la delimitación de las actividades del administrador de acuerdo a la organización; para el administrador de bases de datos, los usuarios directos pueden ser única y exclusivamente los administradores de los servicios y sistemas, y en algunas ocasiones los capturistas. En realidad, no existe un método o un estándar que pueda definir de manera objetiva una estructura en la cual se establezca de forma sistematizada la relación entre usuarios y administradores, ya que esta es una función que en principio debe establecer la organización de acuerdo a su estructura y procedimientos particulares.

En el caso del Instituto, el usuario final del sistema de actualización permanente del padrón electoral ha sido fundamentalmente todo aquel mexicano y mexicana mayor a 18 años. Por ser una institución pública, el personal debe estar comprometido a llevar a cabo sus actividades de tal manera que cualquier posible elector pueda contar con una credencial que le permita ejercer su derecho constitucional al voto, así como contar con una credencial de carácter oficial para llevar a cabo los trámites normales ante otras instituciones públicas o de la iniciativa privada.

El sistema de actualización permanente del padrón electoral obligó al Instituto a entrar a la revolución de la información, ya que en la actualidad, si una organización cuenta con mecanismos de cómputo que le permitan manejar mayores volúmenes de información en menor tiempo y a un mayor nivel de detalle, podrá ofrecer mejores servicios y productos al cliente o el público. Sin embargo, la infraestructura instalada ayudó única y exclusivamente a tener un padrón electoral más confiable para los procesos electorales, pero no contribuyó a mejorar la operación interna del instituto; los beneficios de la red instalada no se trasladaron a las demás actividades que tenía encomendadas por ley el instituto.

PREP 1997: Nuevos usuarios en la red e Internet

Es un hecho que invertir en tecnología es algo costoso para las instituciones públicas en México en virtud de que los proyectos presupuéstales son anuales y dependen de la autorización del Congreso de la Unión; sin embargo, este no es un factor que decida la adquisición de infraestructura en cómputo y comunicaciones en la mayoría de los casos. El principal obstáculo que se tiene para llevar un proyecto de redes y cómputo a su realización, es la visión limitada que puedan tener los directivos o autoridades de la Institución debido a la falta de conocimiento en tecnología. En muchas ocasiones, es complicado cambiar la forma de trabajar de las personas que durante mucho tiempo han trabajado de cierta manera con procedimientos que ya tienen dominados y muy bien controlados.

Esta es una de las razones de por qué el IFE no extendió los sistemas de cómputo y las redes de datos de forma sustancial a las demás áreas del Instituto hasta el proceso electoral de 1997. En ese año, el IFE tuvo a su cargo la elección del Jefe de Gobierno de la Cd. de México por primera y única vez. Era de vital importancia la transparencia de los resultados de la elección, por ende el Programa de Resultados Electorales Preliminares debería funcionar sin inconvenientes, como en años anteriores ya había sucedido, para asegurar la confiabilidad del Instituto y asegurar que las reformas de 1996 fincaron la pauta para constituir al IFE como una institución sólida y confiable.

Una de las innovaciones del PREP de 1997 fue el uso de Internet y sistemas basados en TCP/IP para hacer la difusión de los resultados preliminares conforme iban llegando las actas a cada una de las 300 Juntas Distritales Ejecutivas. Por ello fue necesario instalar cableado estructurado en el Conjunto Tlalpan de las oficinas centrales del Instituto en la Cd. de México, para interconectar los pocos equipos de cómputo de diversas áreas en cada uno de los edificios. Una vez finalizada la instalación de la infraestructura física y los enlaces de comunicaciones, incluyendo el acceso a Internet, muchas de las autoridades y directivos tuvieron acceso por primera vez a los servicios de Internet y al uso de servicios por medio de la red interna, como compartir archivos e impresoras. Esto amplio de forma considerable la visión de las autoridades electorales respecto al uso de las redes de datos en la operación cotidiana del IFE.

A pesar de que el PREP sería un proyecto exclusivo para el proceso electoral de 1997, la infraestructura instalada se quedó funcionando en virtud del aprovechamiento y el beneficio que proporcionaba a los nuevos usuarios. Parte del personal que participó activamente en el PREP permaneció laborando en el Instituto brindando soporte y colaboración en cuestiones de informática a las demás áreas.

Consolidación de RedIFE: Usuarios de Intranet e Internet

Después del éxito del proceso electoral de 1997 y de la red instalada en oficinas centrales, las autoridades del Instituto decidieron crear la Unidad Técnica de Servicios de Informática (1998), encargada de extender la red de informática a todas las oficinas del Instituto, no importando su ubicación física, así como de brindar el apoyo necesario para la implementación de tecnología informática en el Instituto para apoyar y hacer eficientes las actividades de todas las áreas.

A finales de 1998 e inicios de 1999 se consolidaron la mayor parte de los servicios de Intranet dentro del Instituto en las oficinas centrales, además de los servicios de Internet ya en operación:

Página WWW del IFE (http://www.ife.org.mx)
Correo electrónico

Una de la necesidades que inició los servicios de Intranet dentro del Instituto fue por parte de los usuarios de la Coordinación Nacional de Comunicación Social. Una de las actividades importantes de esa área ha sido el monitorear los medios de comunicación (impresos y electrónicos) 24 hrs. al día y publicar de forma diaria síntesis informativas y el resumen del monitoreo de los medios en diversos horarios. Esta publicación se hacia de forma impresa con las suficientes copias para distribuir a consejeros, asesores, coordinadores, directivos y demás autoridades que requerían de dicha información.

Este procedimiento requería de un presupuesto considerable para el papel en el cual se imprimían y fotocopiaban los documentos, además de tiempo desperdiciado en dichas actividades por parte del personal del área. Por razones presupuéstales, fue necesario hacer un recorte en el uso de papel, por lo cual fue necesario buscar alternativas para hacer llegar la información de los productos informativos a las autoridades. La única alternativa era el uso de la red instalada, por lo cual se hizo un análisis y se encontró como opción crear la página de la Intranet institucional. A través de la misma se pusieron a disposición de los usuarios toda la información de las síntesis y monitoreos, lo cual no requirió de ningún gasto ya que se contaban con las herramientas, el personal y la infraestructura necesarios.

Se vio la necesidad de incrementar el número de nodos de red para aquellos usuarios que no contaban con el acceso a la red y dar cursos de capacitación a aquellos que no tuvieran conocimiento del manejo de computadoras. Esta inversión en tiempo y desarrollo trajo consigo un ahorro considerable para el Instituto en papel y tiempo, así como un mejor servicio por parte del área, ya

que por medio de la red y de los servicios de Intranet todo el personal del instituto (que contará con una computadora conectada a la red) tiene acceso a sus productos.

El éxito del servicio de la síntesis informativa a través de la red aumentó las expectativas de el alcance de RedIFE, por lo cual se promovió el apoyar el proyecto y que el proceso electoral del 2000 se llevara a cabo con la ayuda de sistemas informáticos que hicieran uso de la red.

Durante 1999 se llevó a cabo la instalación de cableado estructurado en las oficinas distritales y locales de cada uno de los estados de la república con enlaces vía módem a las oficinas centrales. Se vio la necesidad de capacitar en cómputo al personal de las oficinas con el fin de aprovechar las nuevas herramientas y poder estar preparados para los sistemas para el proceso electoral del 2000. Para inicios del año electoral, se contó con toda la infraestructura de red instalada en los órganos desconcentrados y la mayor parte de las oficinas centrales en el área metropolitana, con lo cual se extendieron los servicios de red a todo el personal del IFE en la república.

Usuarios actuales y sus necesidades.

La instalación de la infraestructura de cómputo y comunicaciones en el Instituto, ha originado nuevas necesidades para el personal de las diferentes áreas:

Equipo de cómputo y herramientas de *software*.

Con la adopción de la tecnología de la información por parte del Instituto, se ha visto la necesidad de proporcionar a los usuarios equipos de cómputo y aplicaciones para llevar a cabo las actividades definidas por el Consejo General. Con el advenimiento de la red y los sistemas informáticos institucionales, se ha visto como una necesidad de que el instituto adquiera equipo de cómputo suficiente y las aplicaciones necesarias para que el personal pueda hacer uso de los servicios de red. En muchas áreas se han adoptado políticas para la transferencia de información, se ha dejado a un lado los faxes y se ha establecido como lineamiento el uso de correo electrónico para el envío de comunicados y documentos importantes.

Si el personal no cuenta con los suficientes elementos para realizar su trabajo mediante la red de datos, no se podrá atender con la rapidez necesaria las solicitudes de servicio por parte de cada una de las áreas. Esto involucra no únicamente la adquisición de bienes informáticos, sino también la actualización y un mejor control de los mismos. Una de las actividades importantes de la Unidad Técnica de Servicios de Informática, es llevar el control del inventario

de los bienes informáticos del Instituto, por ello se vuelve indispensable implementar los mecanismos que permitan llevar un buen control del *hardware* con amplio detalle, así como también, el adecuado licenciamiento de los productos de *software* que requiere cada una de las áreas.

Existen sistemas en el mercado que permiten llevar un buen seguimiento al inventario de bienes informáticos y un control de garantías estricto con los proveedores. Es recomendable que los mecanismos implementados tengan un adecuado nivel de automatización que permita a los responsables, dedicar tiempo al dimensionamiento de recursos a corto, mediano y largo plazo de acuerdo a las necesidades de herramientas de cómputo por parte de los usuarios y las áreas a las que pertenecen.

Capacitación

Es una realidad que la mayor parte del personal del Instituto no ha tenido un contacto constante con el cómputo, ni mucho menos al detalle que muchos de los sistemas y servicios demandan por parte de los usuarios. La mayoría de las áreas cuentan con plazas del Servicio Profesional Electoral; es decir, las personas tienen que tener una continua capacitación sobre aspectos de carácter legislativo, jurídico, económico y, por supuesto, electoral. A la fecha no se contempla dentro de las políticas de capacitación del Instituto una instrucción formal en cómputo al personal que principalmente tiene a su cargo el manejo de sistemas informáticos institucionales.

La Unidad Técnica de Servicios de Informática, ha tenido a bien implementar métodos de capacitación masivo en virtud de que no se cuenta con el suficiente número de instructores para capacitar a todo el Instituto. Dentro de los métodos a los que ha recurrido se tienen:

- Producción de videos educativos acerca de los servicios y sistemas de la red.Elaboración de manuales del uso de los servicios de RedIFE.

- Contratación de instructores encargados de hacer recorridos por la república para capacitar al personal del IFE.

Hay que mencionar que el personal al cual se ha capacitado, en muchas ocasiones es de carácter operativo contratado por honorarios y no tiene una plaza definitiva, por lo cual se vuelve necesario que el personal que cuenta con plaza definitiva, en su mayoría mandos medios, cuente con la capacitación necesaria para no depender de personal no fijo y poder dar continuidad al uso y manejo de sistemas y servicios.

De igual manera se vuelve imprescindible contar con proceso de administración de la red que implementen altos niveles de automatización en virtud de que es difícil que los usuarios puedan apoyar en actividades técnicas cuando se presenta una falla o problema en la red.

Soporte y asesoría

A la par de la capacitación, una necesidad esencial por parte de los usuarios, es contar con un soporte técnico bien estructurado y sistematizado, que le permita llevar a cabo sus actividades cotidianas con la confianza de que si se presenta alguna duda en el manejo de una aplicación o alguna falla en el equipo o en la red, tendrá a su disposición un equipo de soporte técnico.

El IFE ha implementado una variedad de servicios que van desde el correo electrónico, pasando por el servicio WWW, hasta llegar a aplicaciones especializadas como el Sistema de Actualización Permanente del padrón electoral. Sobre cada uno de esto servicios existen los manuales correspondientes; sin embargo, no son perfectos y es comprensible que los usuarios que por obligación tienen que capturar información no sepan, en algunas ocasiones, ni siquiera el manejo de Windows. Es necesario contar con una mesa de ayuda encargada de atender en primera instancia cualquier duda o necesidad por parte del usuario al nivel que sea; esta área debe ser la encargada de encausar o escalar el problema al área correspondiente, así como dar el seguimiento adecuado. El usuario debe ver siempre una sola cara encargada de atenderlo para cualquier asunto relacionado con la red o las aplicaciones de cómputo.

La Mesa de Ayuda debe contar con las herramientas necesarias para automatizar sus procedimientos y hacer óptimo su desempeño y la atención al usuario, para ello debe estar correctamente integrada con las demás áreas de atención de acuerdo a los problemas o dudas que se deban atender.

Reestructuración de procedimientos de operación

Esta es una de los aspectos más críticos de la implantación de una red de cómputo y sistemas informáticos. Como ya se mencionó, la mayor parte de las actividades del Instituto se llevaron a cabo durante un largo tiempo de forma manual, por lo cual se requirió de un gran número de personas para realizar una función específica.

Como ejemplo de ello se tienen el Sistema de Información de la Jornada Electoral (SIJE). Este sistema tiene por objetivo informar al Consejo Electoral del avance de instalación de casillas durante la jornada electoral. En el proceso electoral de 1997 este sistema se llevo a cabo mediante el envío de reportes

de instalación de casillas vía fax desde cada una de las 300 oficinas distritales del país; fue indispensable instalar un gran número de equipos de fax y disponer del personal para el manejo de los documentos y la captura correspondiente en las oficinas centrales. En el proceso electoral del 2000 el SIJE paso por una reingeniería de procesos y se diseño para que hiciera uso de la red de datos instalada a nivel nacional. El sistema funcionó satisfactoriamente y proporcionó un nivel de detalle acerca de la instalación de las casillas que en la elección anterior jamás se hubiera visualizado, haciendo transparente y confiable la jornada electoral.

Ejemplos como este son característicos del Instituto; la adopción de sistemas informáticos basados en red ha originado un cambio en los procedimientos de operación del Instituto y las actividades particulares de cada una de las áreas y las personas que las integran.

Reglamentación y normatividad del uso de los servicios de red y sistemas

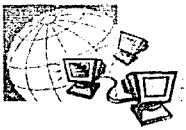
Al usuario no se le puede dejar a la deriva en uso de los servicios de la red de datos, es indispensable que cuente con la reglamentación y normatividad de los servicios que definan clara y puntualmente, las restricciones acerca de su uso, así como los requisitos para la solicitud de los mismos.

El Reglamento Interno del IFE ya cuenta con una serie de lineamientos a seguir de carácter general; sin embargo, es necesario detallar a gran profundidad acerca de cada una de las facilidades con que cuenta RedIFE. Cualquier organización quepretenda dar un buen servicio a sus usuarios debe contemplar la definición del alcance de los servicios que se deben ofrecer a través de la red, así como el uso correcto de las herramientas de cómputo, todo con el objetivo de beneficiar al cliente o usuario final, de forma directa o indirecta.

Difusión de los servicios y políticas

Es común que en las instituciones de carácter público, se implementan servicios que en principio deben estar disponibles para todos los usuarios, pero solamente se informa al área que lo solicitante de la puesta en operación del mismo.

Actualmente existen métodos sencillos, como el correo electrónico, que pueden ser utilizados para informar a los usuarios acerca de las disposiciones de carácter institucional, adicionalmente al fax y teléfono. Estos mismos medios pueden servir para hacer del conocimiento de todos los usuarios información relevante como son: comunicados, boletines, cortes de servicio de red, mantenimientos, políticas, etc. Esto es necesario llevarlo a cabo con



el fin de tener siempre presente que el usuario debe estar enterado atendiendo a dos objetivos fundamentales: que identifiqué las áreas con las cuales tiene que tener interacción para un correcto desempeño de sus actividades y que pueda retroalimentar para la mejora y realización de nuevos proyectos.

Las necesidades anteriores están basadas en dos tipos de usuarios que podemos definir a continuación:

Usuarios en Oficinas Centrales

Se consideran oficinas centrales a las áreas de las direcciones ejecutivas, unidades técnicas, secretaria ejecutiva, presidencia y consejeros electorales. Los usuarios de estas áreas comúnmente tienen un mayor conocimiento de cómputo y cuentan con personal encargado para dar soporte directo cuando se presenta algún problema. De igual forma, una buen porcentaje ya ha utilizado los servicios de Internet y ha asistido a cursos de capacitación.

Las necesidades de estos usuarios están basadas comúnmente en la implementación de nuevos sistemas informáticos mediante el uso de bases de datos y publicaciones WWW, dada la experiencia que tienen en el manejo de las computadoras.

Usuarios en Órganos Desconcentrados

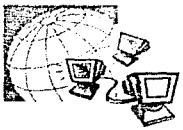
Se consideran órganos desconcentrados a las juntas ejecutivas en todo el país, locales y distritales. A diferencia de los usuarios de oficinas centrales, estos usuarios no cuentan con los conocimientos básicos de cómputo. De igual manera no tienen un personal encargado que les ayude a solucionar un problema de red o que brinde la asesoría para el manejo de las aplicaciones o sistemas.

Las necesidades básicas de estos usuarios son la capacitación, el soporte técnico y la asesoría. Requieren de un buen servicio por parte de una mesa de ayuda, ya que son quienes más se comunican a oficinas centrales para resolver problemas muy sencillos.

Anteriormente mencionamos que el público en general ve al IFE como el encargado de proporcionarle una credencial oficial con fotografía que es requerida por la mayoría de las instituciones públicas y privadas por su grado de confiabilidad. La necesidad esencial de este tipo de usuario es que este servicio sea más eficiente.

Actualmente la entrega de una credencial para votar con fotografía tarda 39 días en el proceso de entrega, como se verá en el siguiente tema

(«Requerimientos de los servicios que se ofrecen a través de RedIFE»), este servicio se encuentra en una reingeniería de procesos para disminuir este tiempo. Este proyecto involucra hacer modificaciones al Sistema de Actualización Permanente del padrón electoral de forma sustancial, tanto en infraestructura de comunicaciones como en desarrollo de aplicaciones, por lo cual será necesario que el área encargada de la administración de la red cuente con los mecanismos indispensables para tener un porcentaje alto de disponibilidad de la infraestructura.



3.3 REQUERIMIENTOS DE LOS SERVICIOS QUE SE OFRECEN A TRAVÉS DE LA RED

Como ya se mencionó en el capítulo 1, el Instituto proporciona una serie de servicios que deben estar funcionando correctamente al momento que los usuarios los requieran; para esto es indispensable que enlaces, equipos y *software* tengan un buen mantenimiento, tanto preventivo como correctivo.

Para esto, a continuación se mencionan los servicios que se proporcionan actualmente, los que se encuentran en desarrollo y sus requerimientos.

3.3.1 Servicios en Uso

Correo Electrónico

Actualmente se tiene planeada la migración del correo de las 332 Juntas Ejecutivas a un servidor central en un equipo Sun Ultra 3000, a fines de este año, para facilitar la administración del correo electrónico del Instituto.

WWW

Para que funcionen adecuadamente las páginas web del Instituto, cada vez que se reinicie el equipo se debe levantar el demonio de Apache, que es el *software* que se utiliza en el Instituto, y se debe verificar que todo el tiempo esté activo.

Acceso Vía Módem

Para que los usuarios no tengan problemas de acceso, se debe mantener trabajando el servidor de autenticación, Tacacs.

3.3.2 Servicios en Desarrollo

Mantenimiento del Padrón Electoral

Como se puede observar en la figura 3.3.2.1, el proceso de credencialización actual es muy largo, hay muchas cosas que se hacen manualmente, y la transmisión de información a los centros de acopio es muy tardada.

Se tiene planeado el mejoramiento de este servicio con la instalación de los módulos en las Juntas Distritales, para que tengan acceso a la red del Instituto, también se planea tener módulos semifijos que se encontrarán en remolques y módulos móviles en donde una persona se estará desplazando a zonas de

difícil acceso y se plantará en el sitio que le sea permitido por uno o varios días según sea necesario, con el material indispensable, cámara digital, digitalizadoras de huella y firma, laptop, módem y papelería. La información que se recopilará en estos módulos será, los datos del ciudadano, firma, huella y fotografía digitalizadas; y se enviarán al centro de acopio, habrán únicamente 2, uno principal y otro de respaldo.

Teniendo la información en el centro de acopio y después de verificar duplicidades, se enviará la credencial a impresión y ésta será entregada directamente en los módulos, únicamente para enviar la notificación al ciudadano de que ya está lista su credencial y pueda pasar a recogerla (ver figura 3.3.2.2).

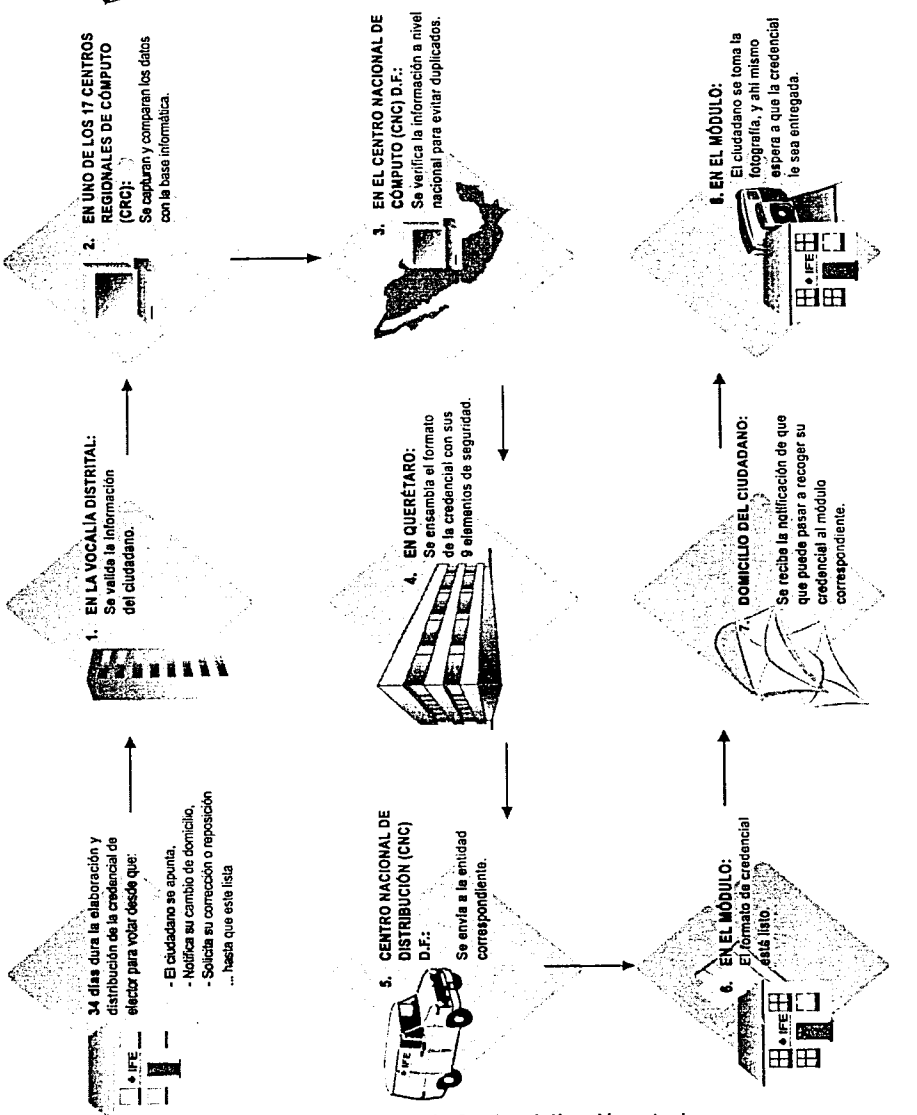


Figura 3.3.2.1 Proceso de Credencialización actual

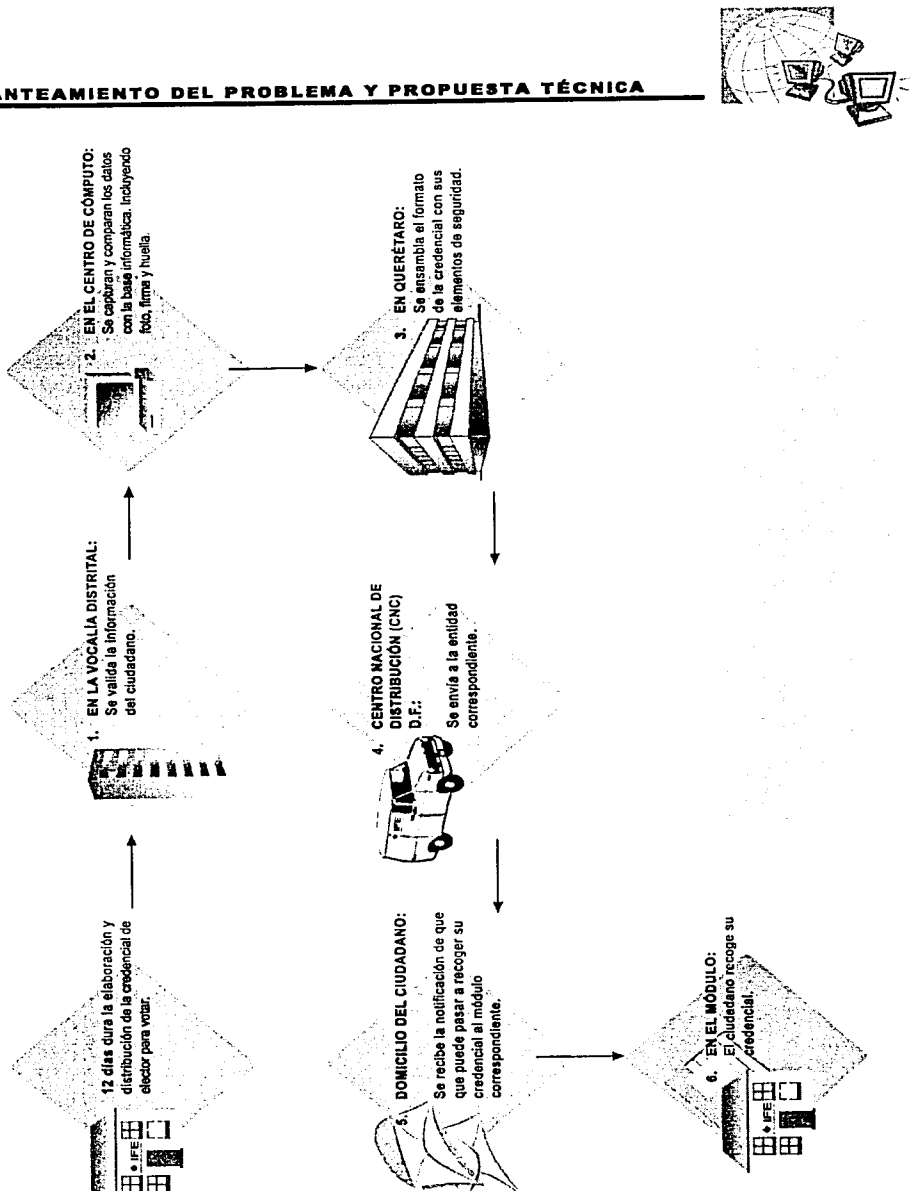


Figura 3.3.2.2 Proceso de credencialización a futuro

Este proceso se planea llevar a cabo en doce días.

Para esto se planea integrar la red del Registro Federal Electoral a la red del Instituto, por lo que serán necesarios nuevos enlaces y equipos que soporten esto.

Sistema de Integración de Administración de Recursos

Como ya habíamos mencionado, actualmente se tiene funcionando un sistema muy básico, ya que no se basa en la arquitectura cliente-servidor.

El SIAR (Sistema de Integración de Administración de Recursos) se encuentra instalado y opera en 50 redes Novell locales distribuidas en el ámbito nacional.

El sistema se puede correr en cualquier equipo de los más de 1000 que se tienen funcionando para este fin. La comunicación de datos se realiza vía módem y correo electrónico, para posteriormente almacenarlos en una base de datos centralizada, utilizando como manejadores de bases de datos Clipper y FoxPro.

Se planea utilizar una aplicación basada en la arquitectura cliente-servidor que sea más robusta y esté más automatizada, una Entreprise Resource Planning (ERP, Planeación de Recursos Empresariales). En el mercado se encuentran una serie de productos de planeación que son sistemas integrales empresariales diseñados para ayudar a las organizaciones a correr sus procesos empresariales.

Utilizan el modelo cliente-servidor y proveen la habilidad de almacenar, recuperar, analizar y procesar los datos almacenados para realizar un análisis financiero, administración de recursos humanos, financieros, materiales y de servicios.

Intranet

Se está desarrollando algo similar a un portal de Internet que contendrá:

- Un Sistema Integral de Control de Cuentas de Correo, para que los usuarios se suscriban y puedan también cancelar sus cuentas de correo.
- Una agenda de actividades por áreas de trabajo, para llevar un mejor control.
- Un control de proyectos, que permitirá verificar el avance de los mismos.
- Un repositorio de archivos compartidos, donde se encontrarán archivos de interés general.

- Anuncios.
- Sitios de interés.
- Noticias.
- Directorio telefónico.
- Foros de discusión.
- Directorio de cuentas de correo mejorado y actualizado.

Voz sobre IP

Actualmente se cuenta con una red telefónica analógica. Para aprovechar más la red del Instituto; la voz viajará a través de la red del Instituto, esto se logrará utilizando una tecnología llamada Voz sobre IP (VoIP), lo que reducirá considerablemente los costos de telefonía, ya que la comunicación es a nivel nacional, lo que implica altos costos tarifas de largas distancias.

Como se muestra en la figura 3.3.2.3, al marcar un número telefónico desde y hacia el Instituto, la voz viajará del Private Branch Exchange (PBX, Intercambio de Líneas Privadas) que tenga el número origen a un VoIP gateway, el cual se encarga de digitalizar la señal y encapsularla en IP, para que esta pueda viajar a través de la red del Instituto, finalmente llega a otro VoIP gateway que se encargará de transformar la señal de digital a analógica para que pase al PBX destino y finalmente al teléfono destino.

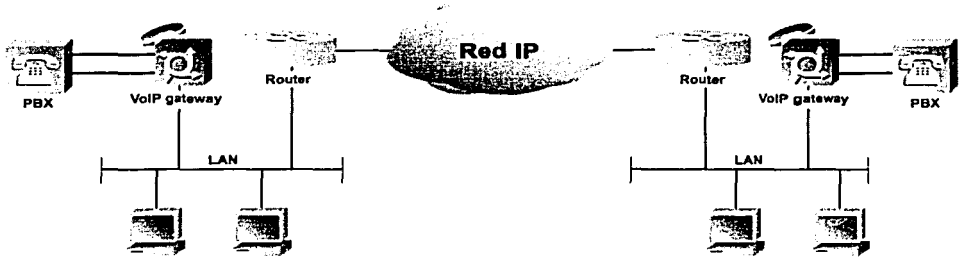
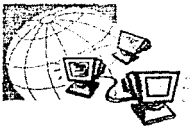


Figura 3.3.2.3 Implementación de VoIP

La implantación del PBX con el VoIP gateway en las Juntas Locales se realizará utilizando el ruteador cisco MC3810, al cual se le agregará un módulo que se encargue de realizar esta tarea, y el cual tendrá conectado un teléfono especial.



Todos los servicios que se mencionaron en el Capítulo I, deben estar funcionando las 24 horas del día, los 365 días del año, y obviamente el servicio debe ser de calidad, por lo que es necesario:

En el caso de los servidores UNIX:

Verificar que las particiones no excedan más allá del 90 % de ocupación, sobre todo /var, donde se guardan las bitácoras del equipo constantemente y /tmp, ya que este reside en memoria *swap*, lo que indica que al saturarse, la memoria se agota y es necesario verificar el motivo.
Verificar también que la memoria sea suficiente.
El procesamiento no se debe elevar demasiado para que los servicios no presenten lentitud.
Verificar que los servicios estén activos, sobre todo correo y web.

En el caso de los equipos de comunicaciones:

- Se debe estar monitoreando que el porcentaje de procesamiento no exceda del 80% para que trabaje en condiciones óptimas.
- Se debe monitorear la utilización de las interfaces y los errores que éstas estén generando. Con esto se verifica la utilización de los enlaces, en caso de exceder del 80% de utilización, la red se vuelve muy lenta.
- Verificar la utilización de la memoria.
- Verificar configuraciones, para evitar que se haga un cambio indebido, y subir nuevas configuraciones.
- Verificar la temperatura de los equipos.
- Verificar que todas las interfaces estén activas.

Todo esto para poder prevenir y corregir posibles problemas y que los servicios se encuentren fuera el menor tiempo posible.

3.4 IDENTIFICACIÓN DEL PROBLEMA

Es evidente que después de haber realizado un análisis de la operación actual de la red nacional de informática del IFE y de los aspectos relacionados con la misma se pueden describirse claramente las deficiencias en los procesos involucrados así como en los flujos de trabajo entre las áreas involucradas.

Esto no es extraño, sobretodo si se considera que el proyecto para la instalación y extensión de la infraestructura de red inició en 1999 de manera formal y empezó a dar los primeros frutos a partir del primer semestre del año 2000. Para el IFE ese fue un año electoral donde el principal objetivo era consolidar el trabajo de la institución de acuerdo a sus atribuciones. Con esta premisa, era evidente que el personal encargado de la administración de la red tenía que cumplir con actividades muy puntuales y tiempos muy restringidos que no permitían llevar a cabo un análisis exhaustivos de necesidades y requerimientos para mejorar la administración de la red.

Pero estas limitaciones sirvieron para poder delimitar claramente los requerimientos para una adecuada administración de la red, partiendo del hecho de que se ha vuelto una herramienta indispensable para el trabajo y operación normal del instituto, además de que ha contribuido a eliminar gastos y un mejor aprovechamiento de los recursos.

Las necesidades y requerimientos para la operación de la red derivan de los problemas que se han identificado en lo que a la operación actual se refiere. El hecho de desarrollar pequeñas herramientas, como las que se mencionaron en el tema 3.1, como apoyo para poder detectar algunas fallas y poder llevar de cierta manera un registro de éstas y de los reportes que se han levantado, absorbe tiempo que podría dedicarse para el desarrollo de nuevos proyectos, que por falta de tiempo se van rezagando.

El que en la mayoría de los casos se estén atacando fallas de manera reactiva, y que los usuarios, pierdan el servicio por un periodo mayor del necesario, es otro gran problema, además de que el usuario no siempre lo reporta en el momento que lo detecta, sino que hace suposiciones con relación a este, pensando que solo se va a corregir, y puede llegar el reporte a UNICOM hasta un día después de haberse presentado.

Lo que también atrasa en gran medida la atención de dicho reporte es que éste llega a cualquier área, y en lo que se verifica si le corresponde atenderlo o no, y si no es así lo pasa a otra área a la que probablemente tampoco le concierne, y en esto se pierde mucho tiempo en que el usuario, con toda razón se desespera y va perdiendo la confianza en el funcionamiento de los servicios.

Como no existe una base de conocimientos en la que se tenga información relacionada con el tipo de problemas que se han tenido y las posibles soluciones a estos, es necesario siempre realizar toda una serie de pruebas antes de poder detectar exactamente en donde radica la falla. Es muy difícil compartir las experiencias de los diferentes reportes entre el personal encargado de resolverlas sin tener esta base de datos de problemas tipo. Además de que no se pueden obtener estadísticas de los problemas presentados para poder prevenirlos en un momento dado.

Al no contar con una base de datos de la utilización de recursos, desempeño y funcionamiento de la infraestructura de cómputo y comunicaciones, el análisis para dimensionar y planear el crecimiento de esta se vuelve complejo.

Si se da el caso de que se detecta algún equipo dañado, el cual requiere hacer uso de su garantía, no hay un área específica que se encargue de éstas, ni un registro adecuado de estos equipos, su atención es muy tardada, y mientras tanto, dependiendo del equipo, el sitio afectado se queda sin algún servicio por más tiempo del necesario.

Como se puede deducir, el problema principal lo podemos resumir en una falta de procedimientos y herramientas que permitan administrar y operar la red de forma adecuada cumpliendo con los aspectos que marca de forma clara y concisa el Modelo ISO de administración de redes. Lo cual, evidentemente, afecta la operación normal del Instituto que depende en gran parte de la red nacional de informática.

3.5 OPCIONES DE SOLUCIÓN ¿ADMINISTRACIÓN CENTRALIZADA O DISTRIBUIDA?

En el presente trabajo haremos referencia al término «administración centralizada» como aquella en donde las decisiones de administración son tomadas desde un número limitado de locaciones, no un solo sitio. La estación de administración que toma estas decisiones será llamada manager (administrador); y representa lo que sería considerado como la parte inteligente de la administración y que a veces es nombrado como la aplicación de administración.

Para manejar la operación de las funciones primarias, los agentes deberán ser añadidos a los sistemas que realizarán las funciones primarias. Estos agentes representan el soporte de administración a través de los cuales el manager inicializa, monitorea y modifica el comportamiento de dichas funciones primarias. Comparados con los managers los agentes son usualmente simples. En la administración centralizada, un numero grande de sistemas pueden ser controlados por un solo manager, ver figura 3.5.1. Para que estos managers se puedan comunicar con los sistemas administrados, es necesario utilizar un protocolo de administración. Ejemplos de estos protocolos pueden ser CMIP y SNMP.

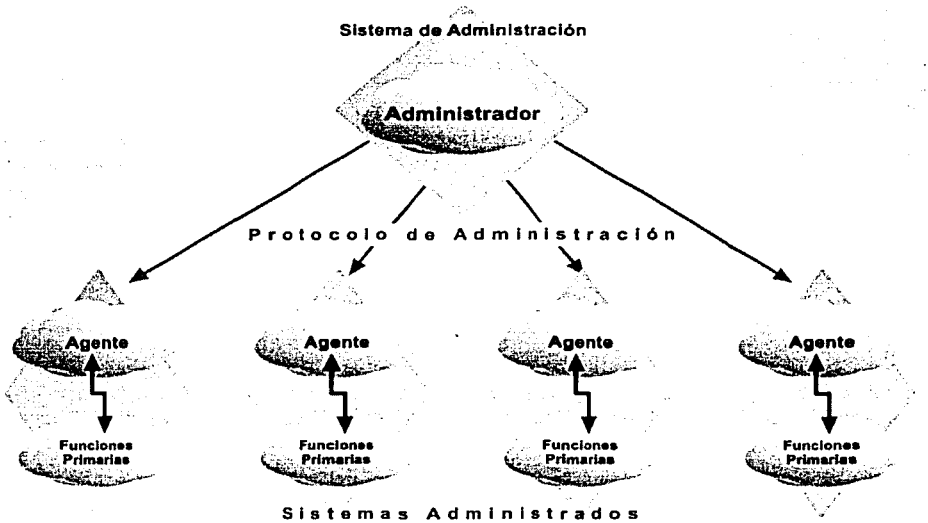
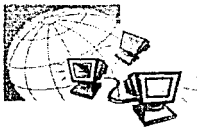


Figura 3.5.1 Administración centralizada



Para hacer más clara esta forma de administrar la red y los sistemas basémonos en el siguiente ejemplo.

El envío de tablas de ruteo son utilizadas por las funciones primarias de los sistemas administrados para determinar la ruta que los paquetes deben seguir para llegar a su destino. El contenido de esas tablas puede ser determinado por un manager central , quien calcula los nuevos valores de manera periódica o después de que haya habido un cambio de topología en la red. En redes grandes dichos cálculos pueden utilizar muchos recursos de tiempo de CPU y memoria. Después de la creación de las tablas, el manager las tiene que enviar a cada una de las estaciones administradas.

El término administración distribuida será utilizado en este trabajo de manera opuesta al de administración centralizada. En la administración distribuida no existe un dispositivo central en donde las decisiones de administración sean tomadas. En lugar de esto, las funciones serán añadidas a los sistemas administrados que son los mismos que realizan las funciones primarias. Este nuevo código será ejecutado de forma proporcional, lo cual significa que todos los sistemas que ejecuten las mismas funciones primarias obtendrán funciones de administración similares.

Por ejemplo, con el arribo de nuevos componentes electrónicos cada vez más poderosos, se ha vuelto normal que sistemas de red puedan calcular sus propias tablas de ruteo. Como consecuencia, ahora no hay necesidad de contar con dispositivos centrales que distribuyan dichas tablas ya que esta tarea se realiza de manera distribuida.

Para llevar a cabo dicha tarea, se debe intercambiar información de administración entre varios sistemas dentro de la red. Para que los protocolos de intercambio de información puedan ser compatibles entre las diferentes marcas de equipo, existen organismos de estandarización que se han dado a la tarea de proponer la implementación de dichos protocolos.

La tabla 3.5.1 muestra algunos de los protocolos utilizados para el propósito de nuestro ejemplo, ruteo de paquetes.

Número	Título
ISO 9542	ES-IS routing exchange protocol para utilizarse en conjunto con el ISO 8473
ISO 10589	IS-IS Intra-domain routing exchange protocol para utilizarse en conjunto con el ISO 8473
ISO 10747	IS-IS Inter-domain routing exchange protocol para utilizarse en conjunto con el ISO8473
ISO 10030	ES-IS routing exchange protocol para utilizarse en conjunto con el ISO 8878
RFC 1058	Routing Information Protocol (RIP)
RFC 1267	Border gateway Protocol (BGP)
RFC 1583	Open Shortest Path First (OSPF)

Tabla 3.5.1 Algunos protocolos de ruteo importantes

La característica principal de la administración distribuida es que cada uno de los sistemas toma sus propias decisiones. Una desventaja de la administración distribuida es que se vuelve difícil hacer cambios una vez que la fase operacional haya sido inicializada. Esto se debe a que dichos cambios requieren de la modificación de un número considerable de estaciones monitoreadas.

Por otro lado, la desventaja de tener una administración centralizada es que la red puede llegar a ser incontrolable cuando sucede algún desperfecto con el sistema de administración central. Comparada con la administración distribuida, la administración centralizada puede ser considerada menos eficiente debido a que mucha más información debe ser intercambiada entre el sistema central y los elementos administrados que están dispuestos a lo largo y ancho de la topología de la red a administrar.

Jerarquía de Administración

Debido a que las redes actuales utilizan en mayor medida protocolos de administración estándares como SNMP, RMON, y en general protocolos del stack de TCP/IP concentraremos nuestra atención en estos ya que RedIFE es una de ellas.

La experiencia práctica con el protocolo original de SNMP mostró que en muchos casos los NMS (Network Management Systems) eran incapaces de manejar más allá de algunos cientos de agentes. La causa de esta restricción se encuentra en la naturaleza del poleo: El manager tiene que estar poleando de manera periódica cada sistema y esto toma tiempo. Para resolver este problema SNMPv2 introduce la idea de tener managers intermedios. Así el poleo se realiza por medio de los managers intermedios que son a su vez controlados por el o los managers del nivel superior. La figura 3.5.2 muestra un ejemplo.

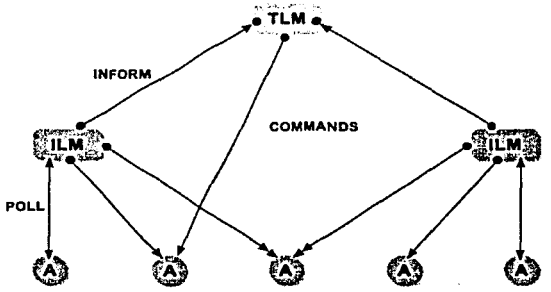


Figura 3.5.2 Disposición jerárquica de los NMS

Antes de que el manager intermedio comience a polear, el manager del nivel superior le dice al manager intermedio cuales variables debe polear en cada uno de los agentes. Además, el manager de nivel superior les indica a los managers inmediatos de los eventos que necesita ser informado. Después de que esta configuración se lleva a cabo, entonces comienza el poleo. En caso de que un manager intermedio detecte un evento en un agente en particular de los que el manager de nivel superior le pidió ser informado, se genera un paquete especial que se le envía al manager de nivel superior. Después de la recepción de dicho paquete, el manager de nivel superior reacciona de acuerdo al evento que recibe sobre el agente individual.

Adicionalmente a los comentarios anteriores, necesitamos tener en cuenta que el sistema no solo comprende el uso de NMS sino también de un sistema de atención de solicitudes y reportes o sistema de mesa de ayuda (**help desk**).

Existen en el mercado sistemas de help desk que se integran a los NMS de diferentes fabricantes y que tienen algunas características que de una u otra forma se tienen que amoldar a cada una de las instalaciones o redes en donde vayan a ser utilizados.

Sin embargo, esta no es la única ventaja que podemos obtener de ellos, también nos sirven para producir información estadística; para que los operadores de las redes realicen su trabajo de manera más eficiente y en general que el tiempo de resolución de problemas se minimice con el paso del tiempo.

Un buen sistema help desk de un centro de operación deberá servir al menos para los siguientes propósitos:

Memoria de corto plazo y comunicación.- El objetivo primario del sistema es actuar como una memoria de corto plazo acerca de los problemas específicos que atiende cada integrante de un NOC. De esta manera, todos los adelantos que se van registrando sobre la solución de un problema contribuyen a la solución del mismo y no importa quien lo esté atendiendo en cierto momento dado que la información es manejada por dicho sistema al cual los operadores tendrán acceso.

Esto es muy importante los NOC en donde se manejan los problemas con personal de diferentes horarios o con diferentes áreas de especialización. El sistema de atención y seguimiento de fallas y solicitudes deberá proveer una historia completa del problema, para que cualquier operador pueda retomarlo en cualquiera de sus fases de manera rápida y sin tener que consultar con las personas que en algún momento han contribuido para el avance de la solución. Es cierto también que en los NOC pequeños en donde todos los operadores se encuentran dentro de un mismo espacio, alguno puede preguntar sobre el seguimiento del problema que va a abordar pero el reporte o solicitud nos provee una comunicación más formal y todas las acciones quedan a su vez documentadas.

Planeación y asignación de actividades.- Los NOCs generalmente trabajan sobre diferentes problemas de manera simultanea con diferentes prioridades. Un sistema **trouble ticket** (TT, Sistema de reporte y seguimiento de fallas y solicitudes) en línea puede proveer en tiempo real (o con información que se actualiza y despliega constantemente) listas de los problemas abiertos, y hasta ordenados por prioridad. Esto permitirá a los operadores repartirse las actividades al inicio de sus turnos de la manera más adecuada. También permitirá a los supervisores y operadores tener una cierta medida de la carga de trabajo del Centro de Operación y en determinado momento asignar más personal a la resolución de los problemas.

Asignación y envío de reportes. – Si el sistema está lo suficientemente integrado a un sistema de correo electrónico, o si es usado por los ingenieros de la red y los operadores de la misma, entonces algunos problemas pueden ser asignados de una manera muy simple, lo único que tenemos que hacer es llenar con el nombre del ingeniero u operador en el campo de «asignado a» del sistema trouble ticket.

Relojes de alarma.- Típicamente, muchos de los tickets se abren con la descripción del problema y se quedan en ese estado hasta que sucede algo. Obviamente debe haber un tiempo relacionado con cada uno de los tiempos de espera entre actualización de los tickets. Si el problema requiere de la intervención de la compañía telefónica (carrier), deberá haber un tiempo de escalación asociado al tiempo de respuesta del carrier. Para tickets asignados

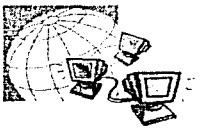
a personal en sitios remotos, deberá haber tiempos de escalación más arbitrarios. También deberán existir tiempos de escalación diferentes para las actividades de los ingenieros del NOC y de los programadores de herramientas. De esta manera un buen sistema trouble ticket deberá poder permitir ajustar los tiempos de escalación dependiendo del problema que se traté y de cada ticket en particular. Estos tiempos de escalación generarán mensajes de alerta para cada ticket cuando se cumpla un tiempo apropiado para su solución.

Preferentemente, el sistema deberá permitir la entrada de pequeños mensajes de texto que serán incluidos cuando se cumpla cada determinado tiempo de escalación; por ejemplo «Verificar estado: TT ##». Estos pequeños mensajes pueden seguir cierto estándar propuesto por el NOC.

Estos tiempos de escalación también podrán aplicarse a los niveles administrativos –no solo los técnicos-. Un tiempo de escalación podrá ser implantado de acuerdo al tipo de red, a la complejidad del problema y el tiempo en que ocurrió la falla.

Resúmenes de estado para ingenieros y clientes o representantes de cada sitio.- Los NOC´s generalmente operan más de una red, o al menos tienen personal que es responsable de ciertas áreas de la red total. Para estos representantes individuales, los resúmenes del reporte o solicitud deben poder ser filtrados por red o nodo y poder ser enviados electrónicamente hacia varios representantes o encargados de área. Estos resúmenes incluyen los reportes del día anterior y el listado de los tickets que aún no han sido cerrados por alguna causa e inclusive un listado de los problemas recurrentes. Estos reportes permiten a los representantes de sitio estar informados del estado actual de su sitio y de los problemas generales de la red. El reporte también permite tener acceso a los detalles particulares de cada reporte así que las personas que reciben los resúmenes de los problemas pueden tener acceso de manera remota las particularidades de los problemas haciendo referencias a ellos por medio del número de reporte o solicitud.

Análisis Estadístico. – Los campos de tamaño fijo en las formas de llenado de los reportes y solicitudes permite su caracterización, lo cual es muy útil para el análisis de los requerimientos y desempeño de los NOC´s. Estas estadísticas incluyen: Tiempo medio de solución de problemas, tiempo medio de solución de fallas sobre equipos muy específicos. Estos campos pueden utilizarse para generar reportes de control de calidad que ayudarán a predecir de manera anticipada los tiempos en que le deberá dar mantenimiento a un equipo evitando que comience a fallar o que sufra un desperfecto grave. Todos estos reportes deberán poder ser generados por el sistema tanto de manera textual como en forma gráfica.



Filtrado de las alarmas actuales.- Deberá ser posible utilizar la información que genera el sistema acerca del estado de la red para filtra las alarmas que serán desplegadas en la pantalla de alerta. Por ejemplo, si se sabe que un nodo XXX está caído dado que existe un TT abierto para su solución, la pantalla de alerta podrá ser actualizada automáticamente para indicar que es un problema conocido. Los TT pueden tener mucho más información útil que puede ser procesada por un sistema lo suficientemente inteligente encargado de estar actualizando constantemente la pantalla de alerta.

Responsabilidad, facilidad de seguimiento e imagen del NOC. – Teniendo un sistema perfectamente amoldado a la forma de trabajo del personal el tipo de seguimiento del problema para los usuarios finales generará clientes gustosos (y buena imagen del NOC) para situaciones normales que regularmente se presentan. Pero también, por su naturaleza, los NOC's tratan con problemas complejos y se encuentran en situaciones de alta presión por los problemas que se generan y tienen que tratar con administradores de red disgustados por las fallas. Los sistemas de TT documentan los esfuerzos de los NOC's para resolver problemas en caso de contratiempos.

De acuerdo a lo anterior, podemos decir que las opciones viables de solución pueden ser las siguientes alternativas. La primera es encontrar alguna herramienta que nos proporcione la funcionalidad de ser tanto un administrador de sistemas (sistemas operativos y aplicaciones), un administrador de redes (que considere no solo a los elementos de red sino a las tecnologías que RedIFE actualmente utiliza) y que además pueda funcionar como un sistema de atención y seguimiento de fallas.

En este sentido son pocas las herramientas que existen en el mercado y su mayor desventaja es el precio. Otras dos importantes desventajas son la dificultad para amoldarlas a la forma de trabajo de las organizaciones y el tiempo que se lleva implementarlas en un ambiente de producción. La figura 3.5.3 muestra a manera de bloques de *software* como son desarrolladas estas herramientas.

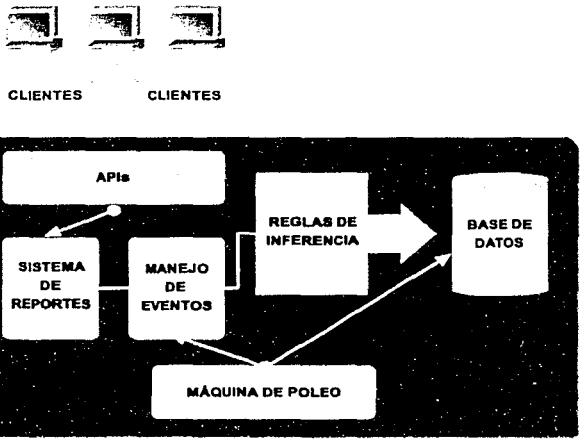


Figura 3.5.3 NMS con su propio sistema de solicitudes y reportes

Sin duda la gran ventaja de este tipo de herramientas es el tener todo integrado en un solo sistema y que los usuarios del mismo manejen solo una herramienta.

La segunda opción es utilizar la misma idea de integración pero separando ciertos bloques funcionales en dos o más herramientas. La ventaja más atractiva es poder amoldar por separado cada una de las herramientas e incluso tener diferentes interfaces de usuario dependiendo del tipo de personal que las vaya a manejar. Por ejemplo, una interfaz de help desk para el personal técnico que recibe las llamadas en un call center (centro de atención de llamadas); una interfaz de alertas para el grupo del NOC; una vista de la topología de los sistemas administrados para despliegue en el NOC o el site principal de comunicaciones; una interfaz de web para los ingenieros de soporte móviles, etc.

También existen otras ventajas como el eliminar la necesidad de tener una sola máquina con muchos recursos para correr una solo aplicación; el instalar las aplicaciones incluso en sistemas operativos diferentes y poder trabajar en paralelo en la implementación del sistema. La desventaja de este tipo de implementaciones radica en el tener que trabajar en la integración de los mismos. En la figura 3.5.4 se muestra el diagrama de bloques de este tipo de implementaciones.

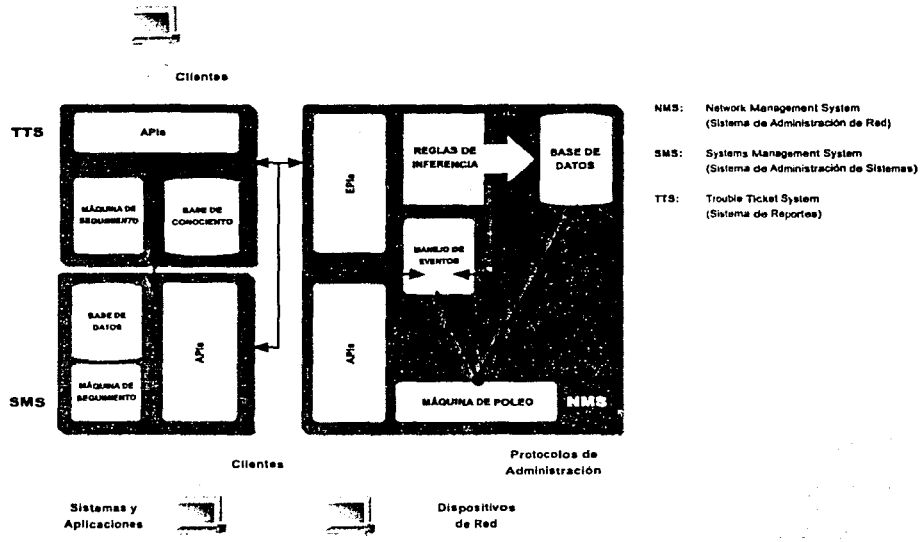


Figura 3.5.4 Sistemas integrados para un NOC

3.6 SOLUCIÓN A IMPLEMENTAR

La solución que más se acerca al sistema que RedIFE está buscando implementar en realidad es una combinación de lo que sería un sistema centralizado, jerárquico y con las herramientas de help desk, systems management y network management.

Las herramientas con los que estaremos construyendo el sistema son las siguientes: Network Management, SPECTRUM; Systems Management, PATROL y Help Desk, Clarify. A continuación se describe de manera breve la arquitectura de cada uno de ellos.

Spectrum es una aplicación basada en la arquitectura cliente servidor. El sistema fue concebido para ser un NMS que pudiera administrar dispositivos de redes de datos y voz de diferentes fabricantes, con lo cual cumple con la premisa de ser un sistema abierto. El servidor puede comunicarse con distintos tipos de clientes cuyas interfaces pueden ser diferentes tales como el propio GUI de Spectrum, una interfaz tipo Java o bien una tipo HTML. Esto lo hace a través diferentes APIs y también cuenta con interfaces tipo EPI para soportar la integración de otros aplicaciones o desarrollos de terceros. Además la arquitectura de Spectrum soporta una configuración de servidores distribuidos, proporcionando una gran flexibilidad para el manejo de redes extendidas sobre grandes extensiones territoriales, tales como la RedIFE.

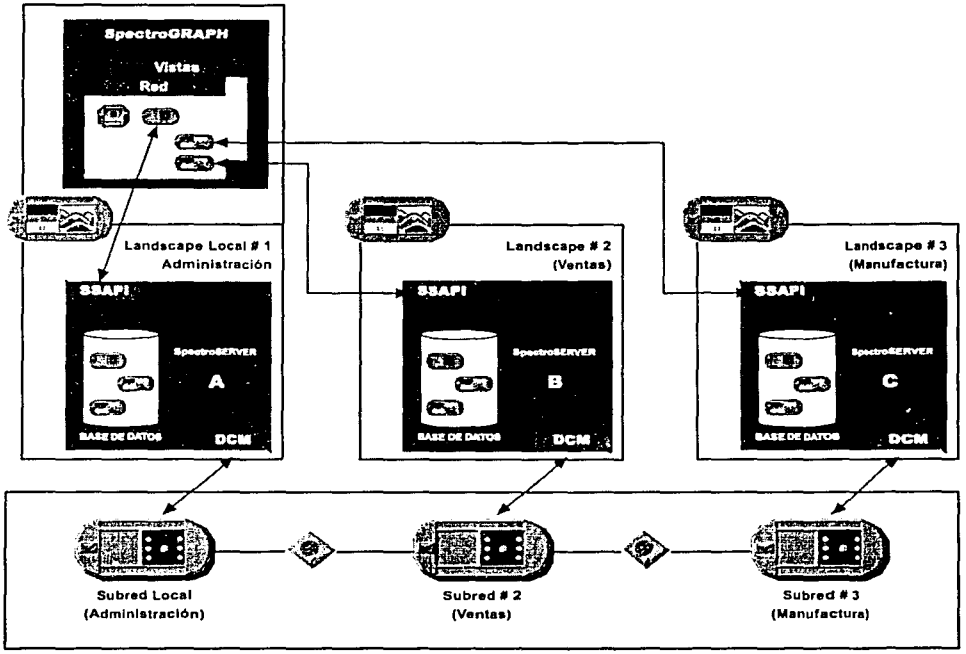


Figura 3.6.1 Arquitectura de Spectrum

En la figura 3.6.1 la parte superior se muestra el cliente propio de la aplicación llamado SpectroGRAPH. Existen otro tipos de interfaces de usuario que se integran a la herramienta y que en determinado momento usaremos dependiendo del tipo de usuario que se trate. La forma en que se conecta a los servidores se realiza a través de un API llamado SSAPI, pero también existen interfaces de CORBA que facilitan la comunicación con el Java y el Web. Posteriormente los servidores a través del **DCM** (Device Communication Manager – Administrador de comunicación hacia los dispositivos) polean a los dispositivos de la red utilizando diversos protocolos de administración y mantienen una comunicación entre ellos para mantenerse sincronizados. Esto hace que un cliente pueda estar conectado a un servidor (p.e. SpectroServer A) y accesar la información de los demás SpectroServers (B y C) sin necesidad de desconectarse del primero. A este tipo de configuración se le conoce como **DSS** (Distributed Spectro Server – Configuración distribuida de SpectroServers).

Tanto los clientes como el servidor pueden correr en cualquiera de los siguientes sistemas operativos: Solaris en máquinas Sparc de SUN o bien sobre Windows NT sobre máquinas con procesador Intel.

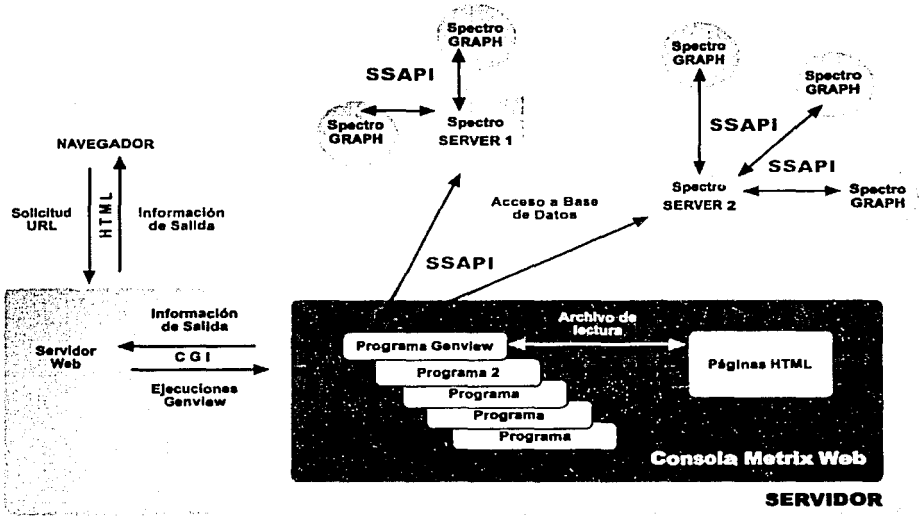


Figura 3.6.2 Integración de aplicaciones de terceros en Spectrum

La figura 3.6.2 muestra como se integran a través del SSAPI aplicaciones de terceros que utilizan tecnologías de Web. Actualmente esta SSAPI puede ser incluso una interfaz de CORBA.

Patrol es una aplicación diseñado por BMC *software* especialmente para administrar sistemas y aplicaciones. Además de poder administrar estos componentes patrol puede optimizar el desempeño de procesos, bases de datos y aplicaciones. La meta de esta aplicación es tener a las aplicaciones altamente disponibles y utilizar la información de administración para optimizarlas.

Existen tres componentes que forman parte del producto patrol, como se muestra en la figura 3.6.3. El agente que es un programa que se instala en cada maquina a monitorear y que es autónomo y autosuficiente. Este es un diferenciador que BMC utiliza para poder manejar grandes cantidades de

agentes en ambientes de redes complejas. El agente de patrol busca eventos y condiciones de excepción e inicializa acciones correctivas así como procedimientos de notificación y escalación basados en las reglas que vienen encapsuladas en los **Knowledge Modules** (Módulos de conocimiento KM). El KM es una encapsulación de experiencia acerca del comportamiento de la aplicación, base de datos, servicio de Internet o bien sistema operativo. Además contiene una serie de reglas para envío de mensajes sobre las excepciones. El KM provee al agente de patrol con la inteligencia necesaria para manejar de manera automática al sistema en donde reside. El tercer componente son las consolas de administración, que pueden ser elegidas por el usuario según sus necesidades.

Así como en Spectrum, existe la consola propietaria, consolas tipo html y consolas que se integran a desarrollos de terceros. Por ejemplo, un operador de red puede elegir algún NMS como Spectrum para monitorear la red, pero también desea tener control sobre la BD de patrol y los eventos de los sistemas y aplicaciones que esté manejando; en este caso tendría que utilizar una aplicación llamada PatrolView que integrase al NMS con la información que los agentes de patrol estén generando.

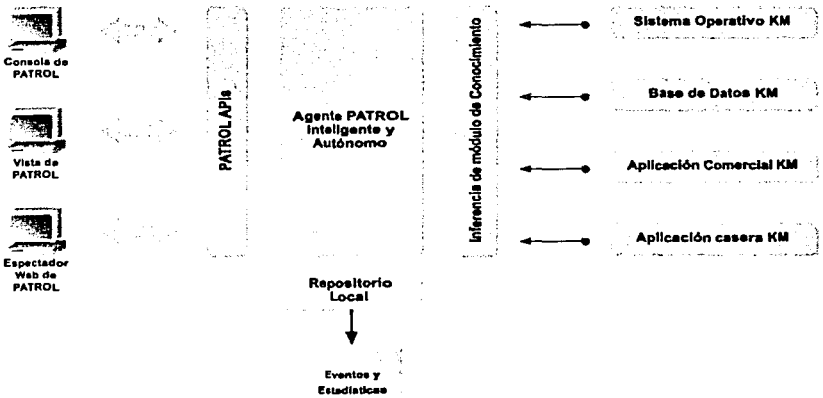


Figura 3.6.3 Arquitectura de Patrol

Clarify. La arquitectura de esta aplicación ha sido diseñada para ofrecer un alto desempeño y escalabilidad. Clarify utiliza una arquitectura three-tier como componente principal para asegurar una máxima flexibilidad y escalabilidad sin sacrificar el desempeño.

En el Clarify eFrontOffice, el servidor de la aplicación que está basado en BEA Tuxedo) le permite a Clarify tratar a la lógica de la aplicación como una capa separada del servidor y del cliente. El servidor de Clarify representa una plataforma escalable y de procesamiento distribuido. Provee acceso a las funcionalidades de Clarify mientras maximiza el número de posibles conexiones a la base de datos, que resulta en un aumento de desempeño cuando se utiliza con manejadores de bases de datos como Microsoft SQL Server, Oracle, y Sybase.

La arquitectura three-tier de Clarify permite tener un control preciso sobre la lógica de la aplicación, optimizando el desempeño y el uso de recursos mientras que se provee una máxima flexibilidad a los usuarios u operadores del sistema. Provee la habilidad de instalar una aplicación solo una vez en un sitio central y tener acceso vía la red LAN o WAN con un cliente propietario o un navegador de Internet sin sacrificar la administración y/o la seguridad.

Clarify también cuenta dentro de su arquitectura algunas características relacionadas con el desempeño entre las cuales podemos mencionar:

- Particionamiento inteligente de la lógica de la aplicación
- Particionamiento dinámico de las tareas de procesamiento
- Administración del tráfico de la aplicación en la red
- En la figura 3.6.4 se puede observar la arquitectura de ésta aplicación.

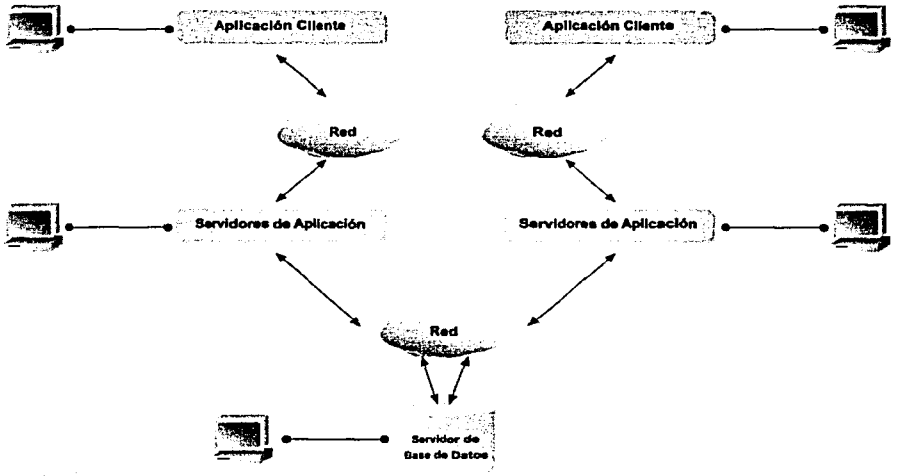
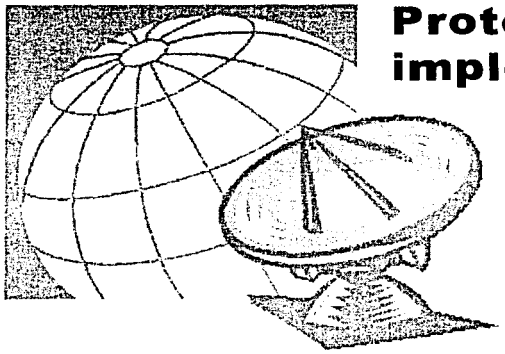


Figura 3.6.4 Implementación n-tier de Clarify

CAPITULO IV



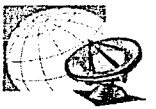
Prototipo de implementación

4.1 DEFINICIÓN DE LOS REQUERIMIENTOS DE OPERACIÓN

Una vez hecho el análisis de necesidades del Instituto para que la red nacional de cómputo del mismo funcione adecuadamente, es necesario hacer una definición de aspectos relativos a la integración del sistema general; en este caso, del prototipo de implementación.

De acuerdo a la solución propuesta, se integrará el sistema de administración de redes y atención a usuarios mediante las aplicaciones: *Spectrum/Patrol* y *Clarify* principalmente. Cómo ya se mencionó en el capítulo anterior, *Spectrum* y *Patrol* son herramientas que trabajan en conjunto formando un sistema integral de administración de redes. *Spectrum* es una plataforma de administración; es decir, cuenta con las funcionalidades básicas definidas en el tema 2.7:

- Una Interfaz Gráfica de Usuario, la cuál se denomin *SPECTROGRAPH*.
- Permite modelar y visualizar un mapa topológico de la red o redes y los dispositivos que las componen mediante un sistema orientado a objetos y en capas, permitiendo delimitar y diferenciar los aspectos operativos de los equipos críticos para el funcionamiento de la red.
- Cuenta con una Base de Datos propietaria y permite la exportación e importación de los datos a otros manejadores comerciales: *Oracle, Sybase*, etc.
- Implementa protocolos comunes de administración de redes como son: SNMP en sus diferentes versiones y RMON.



- El ambiente de la interfaz gráfica tiene flexibilidad para añadir opciones de menús de acuerdo a las aplicaciones y permite personalizar las pantallas para visualizar la información que proporciona la herramienta.
- Cuenta con un sistema de bitácora de eventos donde se almacenan los datos relativos a los cambios en las variables de operación de los equipos y maneja un sistema de alarmas utilizando inteligencia artificial.

Por otra parte, *Patrol* es una aplicación que puede trabajar independientemente a *Spectrum* o se puede integrar a él. Esta herramienta está enfocada principalmente a la administración puntual y detallada de diversas aplicaciones:

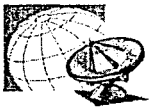
- Sistemas Operativos
- Manejadores de Bases de Datos
- Administración de usuarios de sistemas
- Servidores de Correo Electrónico
- Servidores *World Wide Web*

Por la cantidad de aplicaciones instaladas de este tipo en el Instituto fue necesaria la selección de herramientas para poder detectar de forma automática problemas en los servicios que afectan a los usuarios de forma directa y poder actuar inmediatamente para solucionarlos.

Clarify se integra con las dos aplicaciones anteriores con el objetivo de proporcionar una herramienta para la administración de fallas mediante la cual se pueda llevar un control y registro de todos los problemas que se presenten en la red. La configuración de *SPECTRUM/PATROL* como se explicará posteriormente, se basará en la definición de mecanismos que permitan filtrar las alarmas y enviarlas a *Clarify* para la generación y escalación automática de los reportes.

Dentro del modelo ISO de administración de redes están consideradas las actividades que se deben llevar a cabo para tal efecto. Sin embargo, es responsabilidad de la organización que implementa el modelo, considerar los recursos humanos y materiales para llevar a cabo tales actividades, así como también diseñar la organización que tendrán los grupos de trabajo y la forma en que interaccionarán entre sí; es decir, se deben definir los requerimientos de operación para la implementación adecuada de un sistema integral de administración y atención a usuarios.

En el caso del IFE, se consideró que los requerimientos de operación están divididos en dos rubros:



- Centro de Operaciones
- Flujos de trabajo entre las áreas de atención

4.1.1 Centro de Operaciones

El Centro de Operaciones será una entidad dentro de la organización del Instituto encargada de la administración y operación de toda la infraestructura de cómputo y comunicaciones del IFE.

Como todo Centro de Operaciones, requiere contar con diferentes tipos de recursos que le permitan desarrollar sus actividades; dichos recursos se mencionan a continuación.

Recursos Humanos

El personal debe estar capacitado en el ámbito de administración de redes de cómputo y manejo de los diferentes estándares de red que existen en el IFE. En este sentido, se deberán establecer programas de formación de recursos humanos que permitan la capacitación formal del personal del grupo administrativo y operativo de la red. Un aspecto importante que no se debe dejar de tomar en cuenta, es que esta capacitación debe ser de manera constante, procurando siempre que el personal acuda a cursos o líneas de especialización que le permitan estar en permanente actualización sobre tecnologías y equipos de red.

En esta formación de recursos humanos se debe contemplar también el nivel de aptitud y actitud del personal, ya que es fundamental que las personas que brinden este servicio tengan la habilidad y facilidad para la toma de decisiones que se requiere en este tipo de actividad. De igual manera el perfil de la persona que desarrolle sus actividades en el centro de operaciones deberá contar con una actitud emprendedora y de servicio; hay que tomar en cuenta que el usuario es la parte que hace posible la existencia de la infraestructura de comunicaciones y a la que se le debe brindar el servicio con un trato de cordialidad y de disponibilidad.

De acuerdo a la experiencia del personal del Instituto, se pueden llegar a atender hasta ocho reportes de fallas de red al mismo tiempo, originadas por diferentes causas, por lo cual se establece que la cantidad de personal operativo será de 6 personas, con un horario de atención de 5x10 (cinco días, diez horas) de acuerdo a los cambios de horario a nivel nacional y el horario de actividades del Instituto. Las personas tendrán rotaciones semanales con el fin de asegurar la disponibilidad del personal durante las 10 horas diarias.

Recursos de Cómputo

El centro de operaciones para el IFE, requiere de equipo de cómputo para albergar las aplicaciones del sistema de administración de red; *Spectrum/ Patrol* y *Clarify*. Estas herramientas están diseñadas bajo la arquitectura cliente-servidor; generalmente el servidor tiene que residir en un equipo de cómputo robusto y los clientes en equipos con menos recursos que los del servidor. Para el caso del IFE, los sistemas *Spectrum/Patrol* y *Clarify* se deberán instalar en equipos *Ultra Enterprise 3000* de la marca Sun, mientras que los clientes se instalarán en estaciones de trabajo personales, *Ultra10* de Sun y computadoras personales con los recursos de *hardware* necesarios para ejecutar las aplicaciones sin problemas.

Se necesitarán recursos de impresión, ya sea local o remota; impresoras de alta resolución tanto en blanco y negro como en color. Este tipo de recursos es necesario ya que de muchos de los análisis estadísticos que se realicen se tendrá que conservar una copia impresa y así poder contar con el registro histórico del desempeño de la red.

En otras ocasiones se necesitará presentar informes formales que serán utilizados para presentaciones a los directivos del Instituto o bien para ser incluidos en publicaciones que requieren gráficos de alta resolución y manejo de colores.

Infraestructura de red

En virtud de que desde el centro de operaciones se estará vigilando el estado de los dispositivos de RedIFE, es imperante que su red local tenga acceso al resto de las redes por lo menos por dos rutas diferentes, para que en caso de que se presentara alguna falla en alguno de los equipos que conectan la red local del centro de operaciones al resto de la red, se tuviera al menos una ruta alterna de respaldo por la cual se continuaran realizando las tareas de monitoreo y operación de la red.

Dicha redundancia deberá ser diseñada de tal manera que la red no dependa de un solo equipo para el desarrollo de las actividades de administración.

El diseño de la red local deberá contemplar un ancho de banda suficientemente grande para que los equipos conectados puedan comunicarse sin retrasos en la transmisión, tanto de manera local como con el resto de los equipos operados desde este centro.

Adicionalmente, se podría implementar el acceso a los sistemas de administración vía telefónica (módem). Si surgiera algún problema grave fuera

de los horarios y días hábiles, el personal contará con la facilidad de resolverla desde algún punto remoto, siempre y cuando tenga acceso a una computadora con módem y una línea telefónica.

Área o lugar físico

Es indispensable contar con un local en donde instalar los sistemas de cómputo que estarán manejando los operadores de la red. Dicho local deberá contar con el suministro de potencia eléctrica necesario para poder mantener a los sistemas funcionando, de manera ininterrumpida, durante las 24 horas del día, los 365 días del año. Deberá contar con la iluminación y mobiliario necesarios para albergar a los integrantes y la infraestructura de cómputo. Se propone un diseño del Centro de Operaciones similar al de la figura 4.1.1.1.

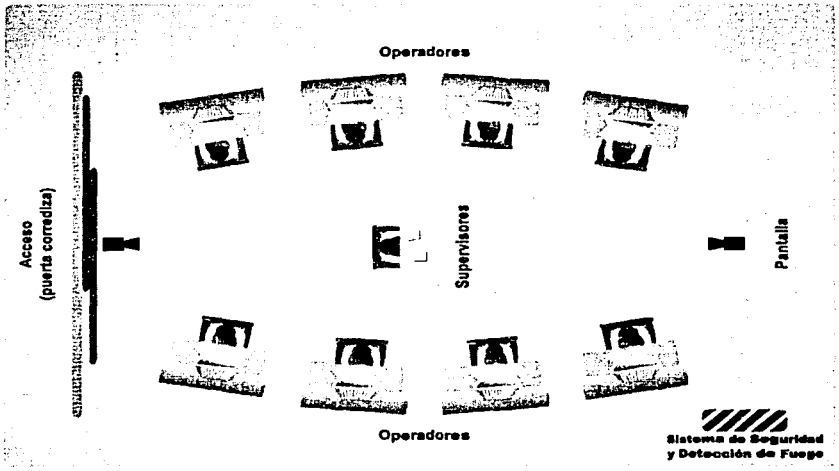
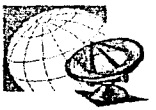


Figura 4.1.1.1 Diagrama esquemático del área necesaria y distribución del Centro de Operaciones.

Comunicaciones

Se deberá tener por lo menos una línea telefónica por cada operador de red, esto con el fin de poder atender a más de un usuario a la vez. Dichas líneas - o extensiones en su defecto -, deberán contar con la facilidad de poder hacer conferencias entre más de tres personas dado que en muchas ocasiones las tareas de coordinación de alguna tarea de operación o mantenimiento,



son realizadas por más de dos personas y las conferencias telefónicas son indispensables para mantener un buen nivel de comunicación entre las personas involucradas.

Algunos de los dispositivos que forman parte de la infraestructura de la red nacional de cómputo cuentan con un puerto serial en donde se puede instalar un módem con el fin de poder tener acceso a un *«shell»* de comandos vía telefónica. Por tanto se requiere tener una línea telefónica dedicada para que en un caso extremo de perdida de comunicación vía red a ese dispositivo, el personal del centro de operaciones pueda conectarse a él, utilizando una computadora y un módem y que no sea necesario desplazarse hasta el local físico en donde se encuentra albergado el equipo en cuestión.

Esquemas de Seguridad

Debido a que desde el Centro de Operaciones se estarán realizando tareas de configuración sobre los equipos de carácter crítico para RedIFE, es indispensable contar con diferentes esquemas de seguridad que mantengan a salvo la integridad de la información y el manejo de los equipos de la red. Para ello se tendrá que restringir el acceso a esta área a toda persona ajena a la operación de RedIFE.

Los equipos en donde corren las aplicaciones de administración y monitoreo deberán protegerse de la mejor manera para evitar ataques de intrusos que intenten obtener acceso a los mismos. Generalmente este tipo de seguridad se implementa vía *software* en el sistema operativo de las máquinas y por lo tanto deberá ser responsabilidad de los operadores de la red implementar dichos esquemas dentro de sus máquinas.

Complementariamente se debe contar con sistemas de monitoreo de los locales donde se encuentran los equipos de red más importantes para la red nacional, permitiendo estar prevenidos contra cualquier siniestro que se pudiese presentar y asegurándose de cumplir con las normas de seguridad necesarias.

Procedimientos de Operación

Finalmente, cada uno de los operadores deberá conocer los procedimientos de operación ante ciertas situaciones comunes en el manejo de las redes. Estos procedimientos serán diseñados por los operadores de la misma y tendrán que acoplarse de la mejor manera a los procedimientos que estén implementados de manera previa en las otras áreas con las que el personal tendrá trato directo.

Dentro del marco de estos esquemas, se tendrán que diseñar ciertas políticas que expresen la forma en que serán recibidos los reportes y peticiones de las redes locales de los usuarios del IFE.

4.1.2 Definición de flujos de trabajo entre áreas de atención

Para entender la relación existente entre las áreas de atención de RedIFE, es necesario observar el diagrama de la figura 4.1.2.1 en el cual se muestra el organigrama de la Dirección de Operaciones de la Unidad Técnica de Servicios de Informática.

La Dirección de Operaciones cuenta con tres subdirecciones entre las cuales se delegan las actividades de operación y atención a usuarios.

- Subdirección de Soporte Técnico. A través de los departamentos de Mesa de Ayuda e Infraestructura está subdirección tiene a su cargo la asesoría y soporte directo al usuario. Se encarga del control de garantías de equipo de cómputo de usuario y de brindar el apoyo en el manejo de *software* y sistemas especiales, así como de la instalación de periféricos y diagnóstico de problemas.

- Subdirección de Administración de Sistemas. Tiene a su cargo el mantenimiento y administración de todos los servidores y servicios informáticos del Instituto: correo electrónico, WWW, FTP, etc.

- Subdirección de Comunicaciones. Es la encargada de la administración de toda la infraestructura de telecomunicaciones del IFE, desde la supervisión e instalación de cableado estructurado de datos hasta la interconexión de redes y mantenimiento de los equipos de comunicaciones del Instituto (ruteadores, switches, concentradores, etc.).

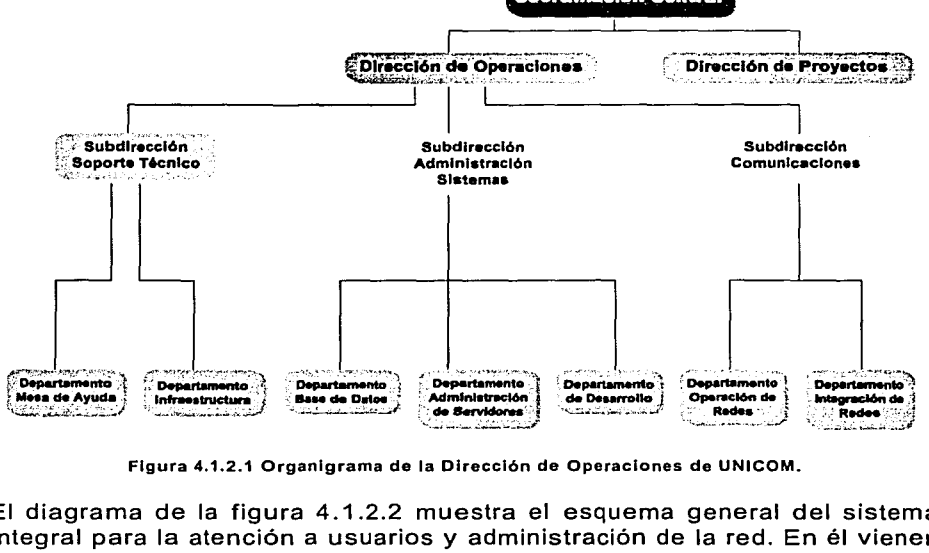


Figura 4.1.2.1 Organigrama de la Dirección de Operaciones de UNICOM.

El diagrama de la figura 4.1.2.2 muestra el esquema general del sistema integral para la atención a usuarios y administración de la red. En él vienen indicados los flujos de trabajo entre las diversas áreas de atención de la Unidad Técnica de Servicios de Informática del Instituto.

En el diagrama se puede observar que las dos principales áreas de atención son la Mesa de Ayuda y el Centro de Operaciones, siendo este último objeto de nuestro tema. De acuerdo a las actividades que se llevan a cabo el Departamento de Operación de Redes de la Subdirección de Comunicaciones y el Departamento de Administración de Servidores de la Subdirección de Administración de Sistemas, se define que el Centro de Operaciones estará conformado por personal de las dos áreas ya que el objetivo de dichos departamentos coincide en el sentido de que su actividad fundamental es el velar que los equipos de cómputo y comunicaciones, así como los enlaces, se encuentren trabajando adecuadamente.

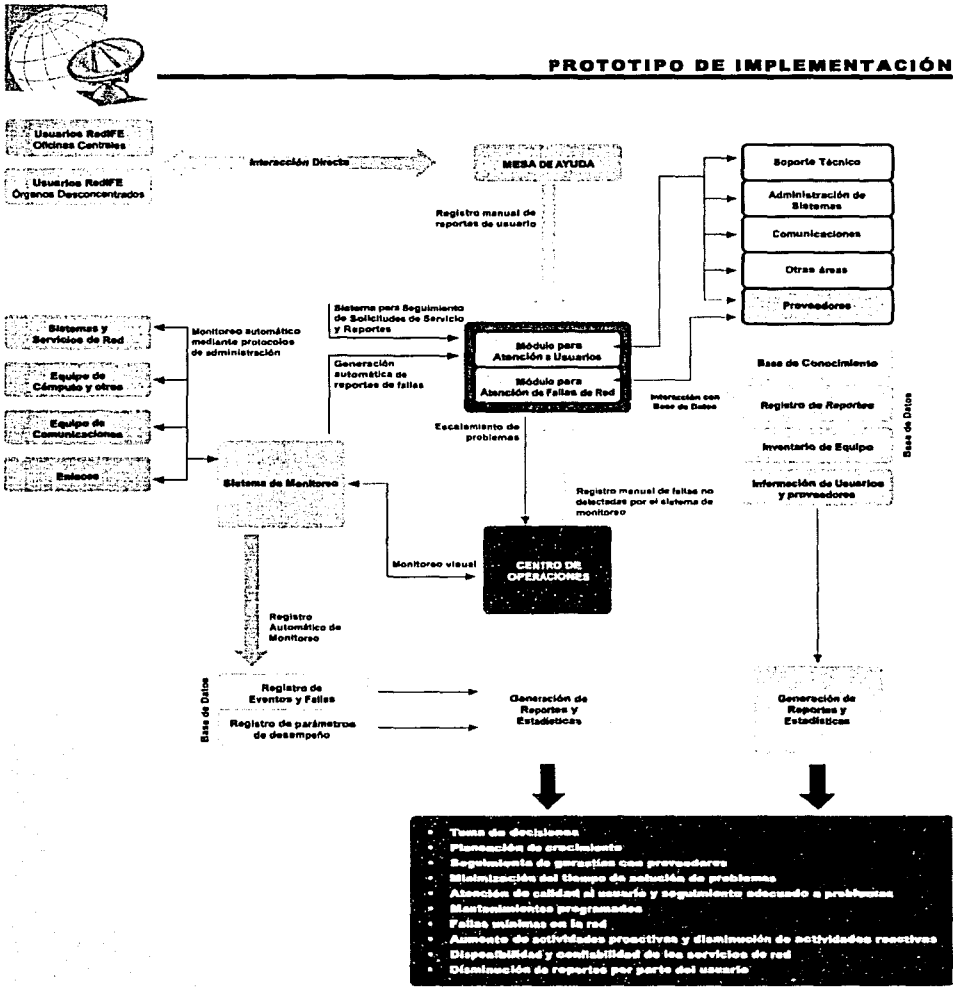
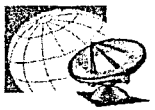


Figura 4.1.2.2 muestra el esquema general del sistema integral para la atención a usuarios y administración de la red

La Mesa de Ayuda es la encargada de recibir los reportes por parte de los usuarios; estos reportes pueden ser recibidos por teléfono, por correo electrónico o fax, entre otros. Es responsabilidad de dicha área otorgar el primer nivel de atención al usuario y tratar de no escalar el problema a un área de segundo nivel. Cuando sea necesario, los problemas que no puedan resolverse en la Mesa de Ayuda en un tiempo establecido o por ser asuntos

que no deben ser resueltos en ese primer nivel, deberán escalarse a las áreas de segundo nivel o proveedores de los equipos dañados. Esto deberá reflejarse en la implementación de Clarify básicamente.

En el mismo diagrama, el sistema de monitoreo (*Spectrum/Patrol*) deberá monitorear y detectar cualquier problema que se presente en los equipos críticos de la infraestructura de la red. Una vez detectados, deberá integrarse con *Clarify* para generar reportes automatizados y escalar automáticamente los problemas al Centro de Operaciones con el objetivo de dar un puntual seguimiento a todas las fallas en la red. Esto incrementará los procesos proactivos y disminuirá los procesos reactivos en la operación de la red, beneficiando al usuario al contar con una mayor disponibilidad de los servicios de red y una confiabilidad en el uso de la misma. En los temas subsecuentes se verá de forma un poco más detallada la forma en que el modelo ISO de administración de redes se aplica al esquema de flujos entre las áreas de atención.



4.2 IMPLEMENTACIÓN DEL MODELO ISO DE ADMINISTRACIÓN DE REDES

Como se mencionó en capítulos anteriores en el Modelo ISO de Administración de Redes, se han estandarizado las actividades que deben de llevarse a cabo para una correcta administración de la red. Estas funciones deben ser cubiertas por los ingenieros de redes al igual que los sistemas de administración.

Las áreas funcionales en las cuales han sido englobadas las actividades a desempeñar en la administración de redes y que tendrán que ser cubiertas por la integración de los sistemas de administración de la Red del Instituto Federal Electoral son:

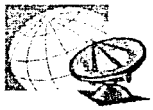
- *Administración del Desempeño (Performance Management)*
- *Administración de las Configuraciones (Configuration Management)*
- *Administración del uso de los Recursos (Accounting Management)*
- *Administración de las Fallas (Fault Management)*
- *Administración de la Seguridad (Security Management)*

4.2.1 Administración del Desempeño

La administración del desempeño debe estar orientada a mantener la disponibilidad de los servicios de red a todos los usuarios con un óptimo desempeño.

El monitoreo de las tasas de utilización y errores generados en toda la infraestructura de comunicaciones y servicios de red, así como, el asegurar que la capacidad de los equipos y enlaces no rebasen los niveles permitidos para mantener el nivel de servicio son las principales actividades que tenemos que llevar a cabo para poder tener una correcta administración del desempeño dentro de nuestro sistema de administración de RedIFE.

Para poder llevar a cabo estas tareas es necesario seguir una serie de pasos, primeramente se deben obtener y almacenar los valores de los parámetros de utilización de los equipos y enlaces que se estarán monitoreando, estos datos deben ser almacenados en una base de datos que permita utilizarlos posteriormente. Estas facilidades nos las proporciona la herramienta de administración *Spectrum*, permitiéndonos contar con una base de conocimiento de la información de la red, esta es obtenida dado que constantemente se recolectan datos que se obtienen a través de ***queries*** (preguntas) y procesamiento de traps, de los equipos que se encuentran modelados en la herramienta.



El modelado de la red dentro de la herramienta de administración nos mostrará la manera en la cual se encuentran interconectados todos los equipos dentro de la red, permitiéndonos visualizarlos de una manera sencilla y rápida. Esto es debido a que se manejan diferentes vistas del modelado, es decir, en una primera vista podremos ver los equipos que conforman el backbone de la red y su interconexión. En otras vistas se podrá visualizar los enlaces y equipos que se desprendan de un equipo en especifico, así como el estado de sus interfaces.

Como una segunda etapa es necesario llevar a cabo un análisis sobre los datos recolectados para identificar los valores máximos de utilización y operación, esto no es una tarea sencilla debido a que cada equipo cuenta con diferentes características para representar los niveles de utilización y sus diferentes valores operacionales, por lo que será necesario aplicar las fórmulas correspondientes para obtener los datos necesarios.

Algunos de los parámetros que tenemos que considerar son:

- Enlaces
  - Estado
  - Utilización
  - Errores
- Interfaz
  - Estado
  - Errores
- Equipos de comunicaciones
  - Estado
  - Utilización del procesador
  - Utilización de la memoria
  - Temperatura
- Servidores
  - Estado
  - Utilización del procesador
  - Utilización de la memoria
  - Utilización de disco
  - Estado de periféricos
  - Estado de Aplicaciones
  - Temperatura
- Aplicaciones
  - Estado
  - Propiedades especificas de cada aplicación

Una vez que ya se han revisado los niveles de utilización de la infraestructura, es necesario establecer umbrales de desempeño apropiados; es decir,

establecer máximos (principalmente) y mínimos (si es necesario), con el objetivo de poder identificar síntomas de una posible falla antes de que se presente. *Spectrum*, nos permite configurar la generación automática de alarmas al configurar los umbrales de desempeño.

Por ejemplo, si la utilización de un enlace sobrepasa un determinado porcentaje, se genere una alarma, para que el ingeniero de red, pueda tomar las medidas necesarias y evitar la saturación del enlace y con esto no afectar la calidad de los servicios ofrecidos al usuario, otro ejemplo sería que si se llegara a una determinada temperatura en cierto equipo, se generará una alarma, para de igual manera tomar las acciones correspondientes y así evitar el posible daño de éste, y como consecuencia una falla en la red.

Spectrum como nuestra herramienta de administración, nos permite el manejo de niveles de alarma, teniendo la posibilidad de generar una alarma de un nivel crítico bajo, hasta un nivel crítico alto. Esto es, podríamos configurar una alarma de nivel bajo cuando el enlace se encuentre en un 50% de utilización y una alarma de nivel critico cuando se encuentre en un 80% de utilización, estos umbrales deben de ser delimitados por el ingeniero de red utilizando sus conocimientos sobre comunicaciones de datos, equipos de comunicaciones, equipos de cómputo, y nivel de afectación al servicio que se esté ofreciendo debido a la falla del elemento.

De igual forma, la herramienta de administración, nos permite tener los datos recolectados acerca de las variables operacionales de los equipos, almacenados en una base de datos, para poderlos utilizar posteriormente y llevar a cabo un análisis de estos. Al contar con datos históricos acerca del desempeño de la red se podrán obtener gráficas y así identificar las tendencias del comportamiento de la red.

Por otra parte algunos de los problemas que se presentan, no pueden observarse mediante los datos históricos, debido a que se presentan solo en ciertos momentos, *Spectrum* nos proporciona una herramienta de graficación en tiempo real de los parámetros de utilización de equipos y enlaces, permitiéndonos llevar a cabo un análisis en el momento en que se está presentando el problema.

En la figura 4.2.1.1 se muestra una pantalla de Spectrum mostrándonos valores en tiempo real.

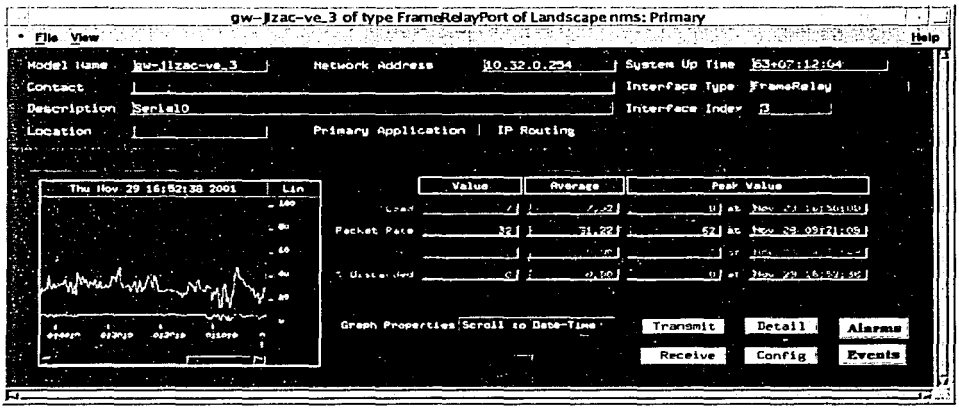


Figura 4.2.1.1 Estadísticas en tiempo real de Spectrum

4.2.2 Administración de las Configuraciones

El objetivo de la administración de las configuraciones se basa en el monitoreo regular de la composición de la red, así como de las configuraciones, sistemas operativos y aplicaciones adicionales de los dispositivos y equipos de cómputo de carácter crítico, tanto a nivel *hardware* como *software*.

Esta actividad nos ayudará a tener un mayor control sobre los dispositivos de la red y un acceso rápido a las configuraciones, haciendo más sencillo el proceso de actualización de versiones.

Con el Administrador de Configuración de *Spectrum*, que se muestra en la figura 4.2.2.1, se dará mantenimiento a la configuración de los equipos de red.

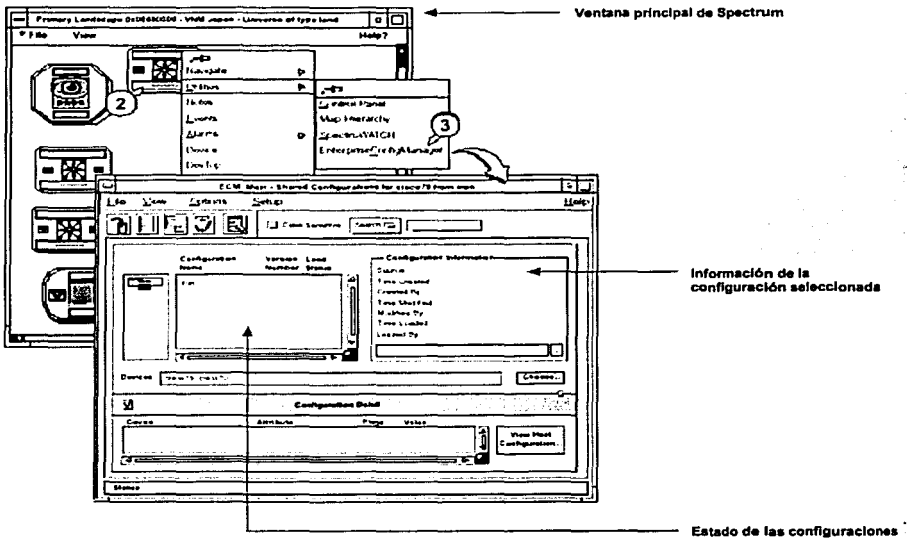


Figura 4.2.2.1 Administrador de configuraciones de Spectrum

Permitiendo:

- **Guardar configuraciones**

Debido a que los equipos que se manejan en el Instituto se encuentran distribuidos en la República Mexicana (donde en ocasiones el clima es extremo) y en la mayoría de las Juntas Ejecutivas no se cuenta con la temperatura adecuada para ellos, estos tienden a dañarse más frecuentemente de lo que lo harían si se encontraran en condiciones óptimas. Además de que los algunos equipos que se manejan en Oficinas Centrales tienen configuraciones largas y diferentes a los demás, se planea guardar respaldos de la configuración de los mismos, y con esto evitar que algún segmento de la red se encuentre fuera de servicio por mucho tiempo a causa de la configuración del mismo.

Spectrum permite guardar versiones de configuraciones, es decir, cada vez que se modifique la configuración de un equipo y se guarde, lo hará con una versión diferente, lo que permitirá poder reconfigurar el equipo con cualquier versión anterior en determinado momento.

- **Actualización de configuraciones**

En las 332 Juntas Ejecutivas se maneja prácticamente la misma configuración, por lo que cada vez que se requiera modificar, se creará una configuración base que se enviará a todos, ya que Spectrum permite enviar configuración a 1000 dispositivos máximo al mismo tiempo.

En los equipos que se encuentran en Oficinas Centrales, no importando que la configuración sea única y probablemente sea más sencillo realizar la modificación directamente en el ruteador, también se hará a través de *Spectrum* para llevar un mejor control de éstas.

- **Calendarizar la actualización de las configuraciones**

Cuando se requiera cambiar la configuración de los ruteadores que se encuentran en las Juntas, se creará un cron de Spectrum para que se haga en el momento que se crea pertinente, esto para evitar exceso de tráfico en la red o que se cargue demasiado el NMS.

- **Crear nuevas configuraciones**

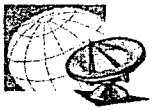
Para crear nuevas configuraciones se podrán manejar plantillas, las cuales contienen una configuración básica que facilita y agiliza la creación de la configuración; o bien, escribirla toda manualmente para posteriormente subirla a los equipos.

- **Verificar configuraciones**

Como medida de seguridad es conveniente tener almacenado en la base de datos, que usuarios han realizado modificaciones en las configuraciones y cuando se han realizado. Además de poder revisar la configuración periódicamente para verificar si se han hecho modificaciones no autorizadas. Spectrum maneja niveles de permisos para sus usuarios, de tal modo que se tendrán dos grupos de usuarios, uno llamado managers en donde se encontrarán los usuarios que tengan permisos para realizar modificaciones en la herramienta, y un segundo grupo llamado staff donde se encontrarán los usuarios que tendrán permisos únicamente de monitorear los equipos y verificar configuraciones sin poder realizar ninguna modificación.

4.2.3 Administración del Uso de los Recursos

El objetivo de la administración del uso de los recursos es medir y contabilizar los parámetros de utilización de la red para poder regular el uso a los usuarios o grupos de usuarios, de los diversos servicios disponibles.



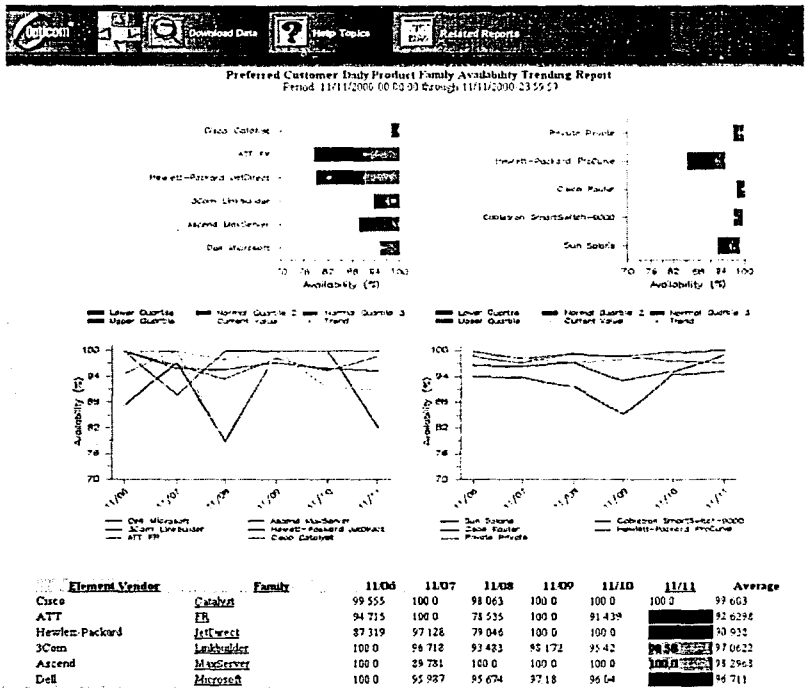
Es necesario medir el uso de los recursos de la red por parte de los usuarios con el fin de establecer métricas, cuotas, determinar costos de uso y en algunos casos específicos, facturar el servicio brindado. Para llevar a cabo el proceso de administración del uso de los recursos, es conveniente:

1. Obtener los datos acerca del uso de los recursos.
2. Ajustar los parámetros para especificar los diferentes niveles de servicio: por usuario y por grupo.
3. Generar reportes periódicos en base a los datos obtenidos.

De acuerdo a las características con que fue concebido el proyecto, nuestro objetivo no fue solo fincar las bases para la obtención de los datos y como aprovecharlos, sino tratar de hacer que todas estas actividades pudiesen realizarse de manera automatizada. Para esto, obviamente tenemos que hacer uso de los recursos con que cuenta el IFE y los que se contemplaron adquirir para llevar a cabo el proyecto. El sistema que utilizamos específicamente para llevar a cabo el análisis del uso de los recursos se llama *Iview* y se integra de manera natural al sistema diseñado desde un principio.

Lo que hace *Iview* es simplemente aprovechar toda la información almacenada en las bases de datos históricas de *Spectrum* y generar reportes en formatos gráficos y tabulares que se presentan de manera automática diariamente en una interfaz de WEB. De esta manera, lo único que se tiene que hacer de forma «manual» es apuntar nuestro browser a las paginas de *Iview*, observar los reportes, analizarlos y concluir en cuanto a la forma en que podemos mejorar el desempeño de la red haciendo un mejor uso de la misma.

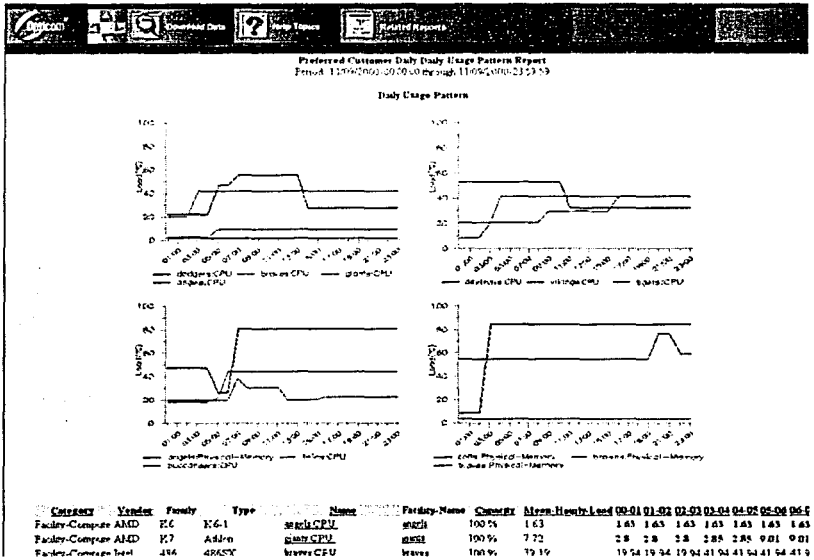
En la figura 4.2.3.1 se muestra lo que acabamos de mencionar. El reporte se refiere a la disponibilidad de diferentes equipos de la red comparativamente día a día. Esto quiere decir que podemos observar en la misma página el comportamiento del equipo en los pasados días y además nos muestra un porcentaje de disponibilidad sobre ese periodo de tiempo. Sobre la misma gráfica se pueden ver algunos números marcados en color rojo o verde. Dichos colores representan «alarmas» de desempeño, dado que previamente se tuvieron que establecer umbrales de desempeño sobre cada uno de ellos. El color verde representa, entonces, un buen desempeño y el rojo un desempeño que no cumple con los umbrales establecidos para su operación. Con estos datos, nosotros solo tendremos que decidir si afinamos los umbrales propuestos o bien hacemos algún cambio a la infraestructura para que el uso de los recursos sea óptimo.



Element Vendor	Family	11/06	11/07	11/08	11/09	11/10	11/11	Average
Cisco	Catalyst	99 555	100 0	98 063	100 0	100 0	100 0	99 603
ATT	FR	94 715	100 0	78 535	100 0	91 439	[redacted]	92 6298
Hewlett-Packard	JetDirect	87 319	97 128	79 046	100 0	100 0	[redacted]	90 932
3Com	LinkBuilder	100 0	96 718	93 483	95 172	95 42	[redacted]	97 0622
Ascend	MaxServer	100 0	89 781	100 0	100 0	100 0	[redacted]	98 2963
Dell	Microsoft	100 0	95 987	95 674	97 18	96 64	[redacted]	96 711

Figura 4.2.3.1 Reporte de análisis de disponibilidad

Además de poder observar el desempeño de los equipos de la red, con la misma herramienta podemos observar los niveles de uso que los diferentes sistemas han experimentado sobre un cierto periodo de tiempo.



Category	Vendor	Family	Type	Name	Factory Name	Capacity	Mean Hourly Load	00-01	01-02	02-03	03-04	04-05	05-06	06-0
Factory-Compute	AMD	K6	K6-1	angels CPU	angels	100 %	1.63	1.63	1.63	1.63	1.63	1.63	1.63	1.63
Factory-Compute	AMD	K7	Athlon	guest CPU	guest	100 %	7.72	2.8	2.8	2.8	2.85	2.85	9.01	9.01
Factory-Compute	Intel	x86	486SX	leaves CPU	leaves	100 %	79.19	19.54	19.54	19.54	19.54	19.54	19.54	19.54

Figura 4.2.3.2 Reporte de análisis de la utilización

Es importante señalar que con este tipo de reportes también podemos llevar a cabo un análisis comparativo no solo tomando en cuenta el tiempo como variable sino también el uso de los recursos sobre sistemas similares, tal y como se muestra en la figura anterior.

4.2.4 Administración de las Fallas

Como se ha mencionado ya en los capítulos anteriores, la parte más delicada de la administración de la red del IFE es el manejo de las fallas de una manera eficiente y dado que hay una gran variedad de posibles desperfectos, solo haremos referencia a algunos ejemplos que se puedan exponer de una manera sencilla y clara.

- **Identificación del problema**

El primer problema que hay que enfrentar es identificar de manera efectiva cual es la causa de la falla en RedIFE. En este sentido la manera más complicada y tardada va a ser cuando un usuario llame directamente al *help*

desk para anunciar la existencia de un problema. En este sentido el operador va a tener que llenar el formato de *trouble ticket* con la información necesaria y describir brevemente de que se trata el problema. Debido a que las personas del *help desk* no contarán con los conocimientos técnicos de un ingeniero de un centro de operación, en esta etapa aún no se podrá haber identificado la falla. La tarea del *help desk* será únicamente tratar de canalizar el ticket al área de especialización que corresponda.

Por otro lado, si el ticket se deriva de una alarma del NMS, el proceso de identificación será mucho más sencillo. Debido a la naturaleza de los sistemas que el NMS estará monitoreando, desde el inicio el esquema que será llenado en el *help desk*, además que se hará de manera automática, contendrá información que ha pasado por una etapa muy importante dentro de su ciclo de vida; tal etapa se conoce como correlación de eventos. A continuación se presenta una imagen de la pantalla de captura de un nuevo ticket en *Clarify*.

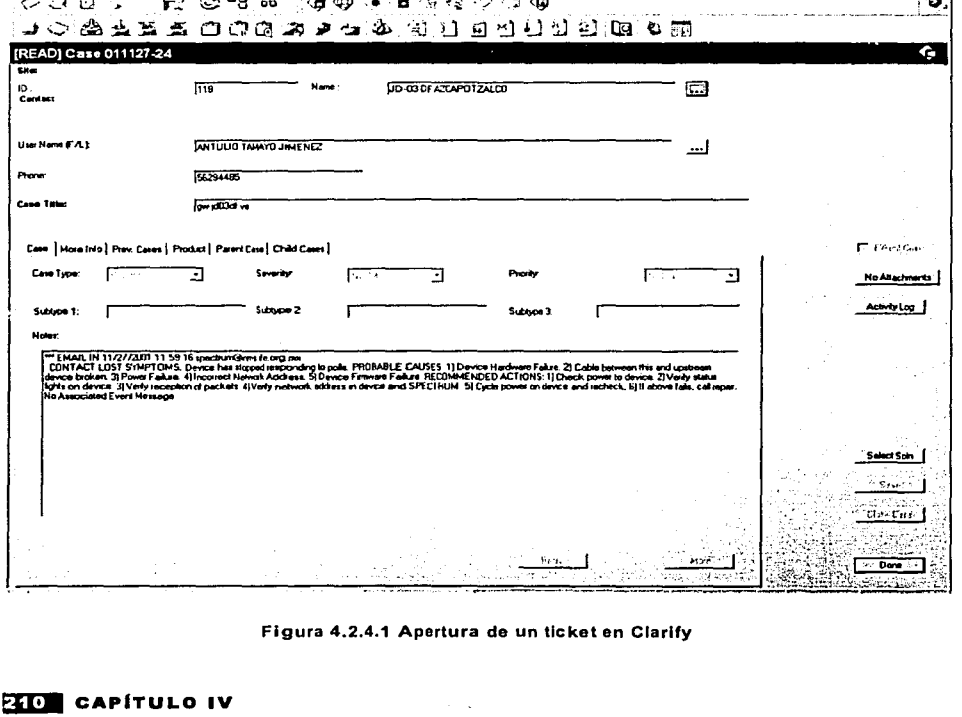


Figura 4.2.4.1 Apertura de un ticket en Clarify

La correlación de eventos se lleva a cabo dentro del sistema de monitoreo ya que cuenta con la suficiente inteligencia como para poder decidir si una alarma en una aplicación se genera por poco espacio en disco duro, por la utilización del CPU del servidor o a veces incluso por un *query* mal programado. Por la parte de la infraestructura, el NMS nos dirá cual es el puerto especifico en que se presentó la falla.Con esta información, el ticket estará más que nutrido de información para llevar a cabo la identificación plena del problema.

En la figura 4.2.4.2 se muestra uno de los problemas que típicamente no pueden ser detectados por los sistemas de NMS, pero que sin embargo los usuarios finales notan de manera inmediata. En este caso el *help desk* necesitará llenar el formato de *Clarify* para notificar al NOC de una falla que ha generado un *trouble ticket*.

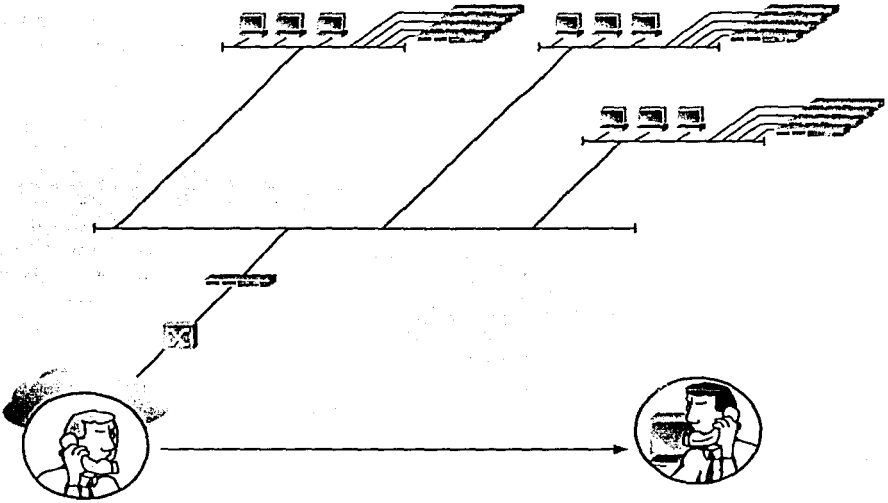
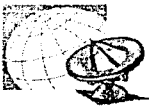


Figura 4.2.4.2 El usuario reporta al help desk una falla

- **Delimitación de la causa del problema**

Una vez que ya se sabe cual es la causa del problema, se dará seguimiento a través de las pantallas de *Clarify* y se irá nutriendo de información cada uno de los *tickets* que se encuentren abiertos.

Sin embargo, ahora hay que comenzar a dar seguimiento a la falla para resolverla de la mejor manera y en el menor tiempo posible.



Cuando *Clarify* haya detectado que la falla actual es un problema recurrente, la delimitación del mismo va a ser inmediata ya que le podremos pedir un reporte de los casos similares que hayan sido registrados y la información que obtendremos será el fruto de la base de conocimiento que se irá formando en nuestros sistemas conforme vaya transcurriendo el tiempo.

Ahora bien, si no existe un caso similar, el responsable del ticket tendrá que consultar las pantallas del NMS con el fin de obtener más información y poder así delimitar la falla.

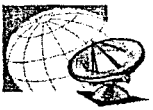
El delimitar la falla se refiere a conocer con certeza, que partes de la red están siendo afectadas; si existe o no un sistema de respaldo para subsanar la falla; si podremos tratar de solucionarla de manera remota o habrá que enviar a otra persona al site de la falla, etc.

Es importante señalar que hasta este momento no hemos comenzado a resolver nada, solo se trata de una recolección de información que nos permitirá decidir cual es la mejor manera de atacar el problema y decidir si solo personal del IFE intervendrá en su resolución o tendremos que involucrar a terceras personas, digamos el *Carrier*, el ISP, o un *outsourcer*.

Como un dato adicional debemos comentar que en esta etapa se debe identificar cuales son los equipos, enlaces o sistemas involucrados, pero también cuales tendrán un comportamiento diferente al que normalmente tienen.

Por ejemplo, supongamos que tuviéramos caído un enlace a una junta y que tenemos la posibilidad de cambiar la configuración de algunos equipos para no dejar sin comunicación a la junta mientras el *Carrier* soluciona la pérdida de enlace. Lo que tendríamos que documentar en *Clarify* aparte de la configuración que se llevará a cabo en los equipos, cuales serían las consecuencias esperadas en el comportamiento de otros equipos o enlaces de comunicación, tales como incremento de tráfico en enlaces secundarios y/ o de respaldo; aumento de procesamiento en servidores, *routers*, etc.

Esto nos servirá después porque dado que todo quedará documentado, al momento en que se lleve a cabo el análisis de los reportes podremos tener un panorama más global del comportamiento de la red en condiciones adversas y lo más importante, podremos medir su desempeño comparado con las condiciones normales. Sin un sistema como el que se plantea en el presente trabajo, este tipo de información simplemente no podría ser obtenida.



- **Corrección del problema**

Todas las tareas necesarias para corregir el problema irán siendo registradas en el sistema de *help desk* para que en cualquier momento cualquier otro usuario pueda tener acceso a la información relacionada con el problema y en su momento incluso retomar un problema que se haya complicado o escalado a un nivel superior de soporte.

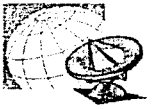
De esta manera se cuidará de forma especial el profesionalismo de los servicios ofrecidos por el NOC a los usuarios de RedIFE.

Por otro lado, cuando el problema no pueda ser subsanado más que por terceras personas (ajenas al IFE, por ejemplo el *Carrier*) entonces la persona del IFE que tenga asignado el problema será el indicado para hacer las anotaciones correspondientes dentro del expediente de *Clarify* y tendrá que comunicarse de manera regular con los encargados del problema del lado del *Carrier*.

El encargado del ticket también podrá escalar el problema después de haber transcurrido cierto tiempo preestablecido por las reglas de tiempos de escalación concertadas con el *Carrier* (en este caso). Este proceso estará disponible para que se lleve a cabo de manera automática, pero para algunos casos puede ser también manual.

Si el problema se resuelve de manera local por personal del IFE, toda la documentación del problema deberá hacer referencia a los equipos propios de RedIFE de una manera estándar y previamente definida ya que esto es de especial importancia cuando se lleva a cabo una integración como la que estamos proponiendo en este trabajo. En nuestro caso particular, debido a que los sistemas estarán compartiendo información de manera bidireccional, el manejo de los nombres de los campos en cada sistema deberá ser necesariamente el mismo.

Debido a que la integración entre *Clarify* y *Spectrum/Patrol* se hará a través de mensajes de correo electrónico, es necesario resaltar el hecho de una convención en el uso de los nombres en ambos sistemas. El servidor de e-mail de *Clarify* estará constantemente revisando su propio buzón para ver si no hay mensajes nuevos y tratará de asociar los mensajes de correo con un usuario local (un usuario de *Clarify*). Lo mismo sucederá de manera inversa; *Spectrum* también estará revisando los mensajes de e-mail en su propio sistema y tratará de asociarlos con un usuario local. Debido a que esto se llevará a cabo de manera automatizada, no solo los nombres de los equipos, sino también los nombres de usuarios con privilegios de administración deberán coincidir.



Si el usuario existe en la base de datos de *Clarify* y tiene privilegios de crear un ticket, el ticket se creará y *Clarify* enviará de regreso un mensaje a *Spectrum* para notificarlo de que se ha creado un ticket en *Clarify*. *Spectrum* únicamente la registrará como un evento y será registrado en su base de datos histórica; nuevamente se hará una verificación de permisos y de usuarios en ambos sistemas. Este mismo procedimiento se llevará a cabo cada vez que ambos sistemas intercambien información.

Una vez llevado a cabo el proceso de solución del problema, el responsable del ticket no lo podrá cerrar sino hasta la siguiente etapa.

- **Revisión de la solución**

Como una medida especial de seguimiento de problemas, el usuario asignado a la solución de la falla trabajará en conjunto con el Centro de Operación para verificar que la solución implementada haya sido la mejor y que no se haya afectado a nadie más.

Cuando esto suceda, el NOC dará su visto bueno para que el ticket pueda ser cerrado por el responsable.

En este momento, el *help desk* será notificado de manera automática que un problema ha sido resuelto y será su obligación contactar a los usuarios que habían sido afectados que verifiquen por ellos mismos que el problema a sido resuelto y dará en caso de ser necesario una explicación de que fue lo que sucedió y cuales fueron las medidas que se tomaron para resolver su falla. Toda esta información esta contenida dentro del sistema de *help desk* y por tanto documentada de principio a fin.

Todo este proceso de documentación es automático y va formando una base de conocimiento que irá creciendo con el tiempo, con lo cual estaríamos cumpliendo con la última premisa de la implementación de una administración de fallas según la ISO.

4.2.5 Administración de la Seguridad

Como se ha mencionado con anterioridad, como parte integral del modelo ISO de administración de redes, tenemos que considerar la parte de seguridad de los recursos de la red.

En este sentido, el tema será abordado durante el presente trabajo de manera en que se pueda mostrar cuales son las formas utilizadas por las tres herramientas que utilizaremos para proveer seguridad a nivel de la propia

aplicación y cual es su utilidad para poder salvaguardar la integridad de los datos contenidos en los diferentes sistemas que conforman a RedIFE.

Comenzaremos hablando de *Clarify* y *Spectrum* y posteriormente hablaremos de *Patrol*, que en este caso es el sistema que más inferencia tiene con respecto a la seguridad.

Clarify

Como parte primordial de cualquier sistema de cómputo multiusuario se debe considerar la autenticación. En el caso específico de Clarify se provee una forma un tanto flexible para configurar la autenticación.

En primera instancia, podemos configurar la longitud mínima del ***password*** (contraseña). Recordemos que los passwords se guardan dentro de las bases de datos de *Clarify* y para poder accesar a ellos, primero se debe tener acceso al sistema y tener los permisos necesarios para poder cambiar/consultar esos campos.

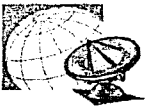
Existe en Clarify un objeto de configuración llamado *password* en donde podemos manipular la forma (en este caso longitud) del campo. Es necesario resaltar que la longitud de este campo tiene que ver con el acceso del cliente de la aplicación al servidor.

La sintaxis del objeto de configuración es la siguiente:

```
OBJECT TYPE=»config_itm», NAME=»password»
UNIQUE_FIELD=name
FIELDS
name=»password specification»;
value_type=minimum_password_length;
i_value=integer;
END_FIELDS
RELATIONS
END_RELATIONS
END_OBJECT NAME=»password»
```

Para cambiar la longitud del *password* solo hay que cambiar el «*value_type*» al número que nosotros deseáramos que sea la cantidad mínima de caracteres. Es de común práctica tener *passwords* que al menos sean de 8 caracteres.

Adicionalmente el campo llamado «*I_value*» se utiliza para especificar si se permitirá la facilidad de auto *login*.



Auto-login values	I_value description
0	Enable auto-login
1	Disable auto-login

Tabla 4.2.5.1 Valores del campo auto-login en Clarify

El auto-login se refiere a que si se va a permitir tener un acceso directo a la aplicación sin necesidad de teclear un *password*. En el caso del IFE el valor del campo será 1 para obligar a los usuarios a teclear un *password* cada vez que utilicen la herramienta.

Además del manejo de los *passwords*, también se estarán manejando los perfiles de usuarios.

A continuación se presentan dos tablas que resumen los niveles de acceso (aplicaciones que pueden utilizar) para los usuarios finales y los administradores:

Application	Description
ClearSupport	Create, track, and resolve external customer support cases.
ClearHelpdesk	Create, track, and resolve internal customer support cases.
ClearQuality	Help your quality assurance group to track change requests, enhancements, and resolutions
ClearLogistics	Create and route part requests to track inventory transfers (orders, returns, repairs, and shipments) through your organization.
ClearSales	Create, track, and manage sales opportunities, quotes, literature requests, and action items within your organization.
ClearCallCenter	Create and track interactions, sales opportunities, quotes, literaturerequests, action items, and customer support cases.
ClearContracts	Create, track, and manage quotes and contracts within your organization.

Tabla 4.2.5.2 Aplicaciones disponibles para usuario final

De acuerdo a la tabla anterior y de acuerdo al tipo de operaciones de la RedIFE algunas aplicaciones no se utilizarán y algunas otras irán destinadas a usuarios específicos, es decir no todo usuario final tendrá acceso a todas ellas.Las aplicaciones de configuración, también disponibles a través del cliente de *Clarify*, les permite a los administradores configurar ciertas características que determinan como podrán interactuar con la aplicación los usuarios finales. Estas características incluyen a las reglas del negocio, grupos de trabajo y colas.

Las aplicaciones administrativas, listadas en la tabla 4.2.5.3 están disponibles solo para los usuarios con privilegios administrativos. Los privilegios de los

usuarios en conjunto con las opciones de licenciamiento controlan el nivel de acceso a las distintas funcionalidades de la aplicación.

Application	Description
Policies and Customers	Add and configure sites, contacts, and employees; set up business rules, workgroups, and queues; add or change some of the dropdown list items that appear in other parts of the Clarify application.
Product Manager	Add products and part numbers, configure product hierarchies, and create bills of materials

Tabla 4.2.5.3 Aplicaciones de configuración en Clarify

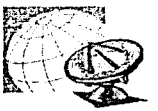
Spectrum

La seguridad que ofrece *Spectrum* está enfocada a prevenir un acceso no autorizado y la modificación de las vistas propias de la aplicación y sus modelos. Estos niveles de seguridad también pueden prevenir cambios no autorizados a los dispositivos de la red, sin embargo la seguridad de Spectrum no reemplazará al sistema de seguridad propio de la red (existen sistemas dedicados a cuidar específicamente la seguridad de la red). *Spectrum* contribuirá como sistema de administración a cuidar la seguridad de la red y así extender la misma a los sistemas o estaciones que el mismo Spectrum estará monitoreando. Al respecto podemos mencionar que las áreas de seguridad que *Spectrum* ayudará a cubrir son las siguientes:

- Áreas de la red que los usuarios pueden examinar o ver
- Los valores de los atributos que los usuarios pueden cambiar
- Los modelos existentes y las vistas de Spectrum que los usuarios pueden modificar.

Los siguientes términos describen los conceptos que son el fundamento de la seguridad en *Spectrum*.

Security Community. Las comunidades de seguridad en *Spectrum* definen las áreas de acceso a la aplicación. ADMIN es una comunidad global que contiene a todos los modelos. Todas las demás comunidades son subconjuntos de ADMIN y se crean a través de la asignación de ***security strings*** (contraseña de seguridad) que se les configuran a los modelos de *Spectrum*. El administrador de la aplicación determina la estructura de las comunidades como parte de la planeación de la seguridad de la red. Las comunidades pueden establecerse como peers o subconjuntos de otras comunidades. La estructura de comunidades en *Spectrum* puede ser construida como una jerarquía anidada, establecer todas las comunidades a un mismo nivel o establecer una combinación de ambas estructuras son anidadas (grupos de comunidades en diferentes niveles jerárquicos). La figura 4.2.5.4 muestra un ejemplo de una estructura de comunidades.



Las estructuras jerárquicas forman relaciones padre-hijo. Las comunidades contenidas dentro de otra son consideradas como hijas de esta última. Una comunidad que contiene a otras se considera padre de las demás.

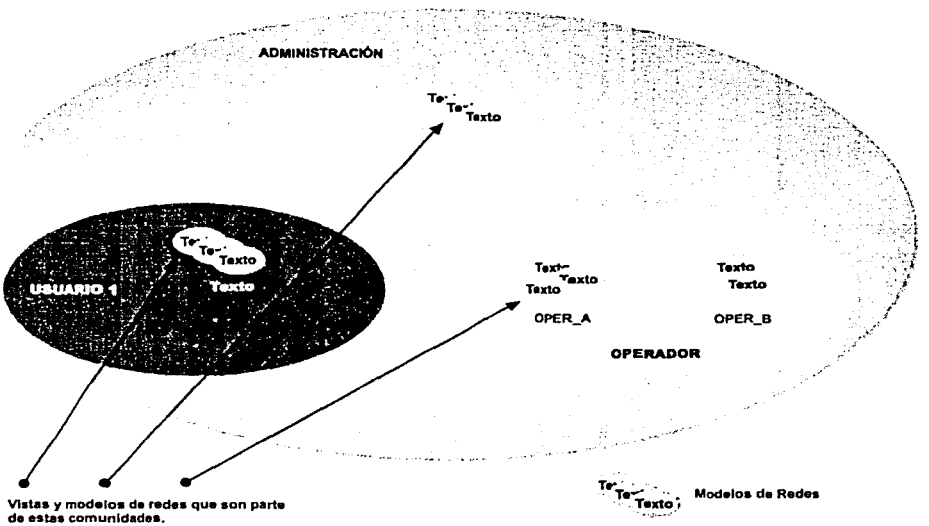
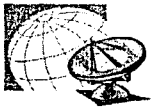


Figura 4.2.5.4 Ejemplo de las Security Communities de SPECTRUM

Security Strings. *Spectrum* utiliza security strings para colocar candados a los modelos. Un *security string* se establece cuando un modelo es creado. El *security string* también puede ser asignado o modificado después por algún usuario que tenga privilegios de escritura.

El *security string* de un modelo específico consiste de valores (*security strings*) heredados del security string del modelo padre y el propio del modelo. Si al ser creado, a un modelo no se le especifica un security string dicho valor es tomado del valor del *security string* del padre, si existe, dependiendo de en qué vista se vaya a colocar dicho objeto. Cuando no se asigna ningún *security string*, el acceso al modelo no esta restringido.

El *security string*, candado, de una comunidad o de un modelo es comparado con el ***community string*** (Llave) que cada usuario tiene asignado. Cuando el *community string* de un usuario contiene un texto idéntico del *security string* del modelo, entonces el usuario tiene acceso al modelo, en caso contrario aparecerá una ventana de dialogo que diga que no se tiene acceso al mismo.



Community Strings. Los *community strings* son las «llaves» que se les dan a los usuarios de *Spectrum* para obtener acceso a una comunidad. El *community string* de un nuevo usuario se hereda del *community string* del grupo de usuarios al que pertenece. Cuando no se da ningún *community string* a un usuario o grupo, *Spectrum* asigna un default que es «ADMIN,0» dándole al usuario o grupo de usuarios acceso ilimitado a todas las comunidades. El *community string* puede ser modificado en cualquier momento por el administrador de la aplicación. Esta comunidad se lee cuando un usuario levanta un cliente de *Spectrum* (*SpectroGRAPH*). Los cambios a los *community strings* se reflejan de inmediato.

El *community string* consiste de dos componentes. El primer componente define a cual de las comunidades (haciendo match) el usuario va a tener acceso y el segundo componente establece el nivel de acceso permitido para cada comunidad, por ejemplo *view only* (solo lectura), *view and update* (lectura y actualización) o *view and edit* (lectura escritura). Por ejemplo *PhoneSupport,5:LocalAdmin,5.*

En la siguiente tabla se muestran los niveles de acceso que un usuario puede tener de acuerdo al segundo componente del *community string*.

Nivel de acceso	Privilegios
0-4	View, update and Edit. Normalmente el único numero que se utiliza es el 0 pero bien se podrían utilizar del 1 al 4, que tienen exactamente los mismos privilegios. Los números del 1 al 4 están reservados para futuros accesos intermedios que se podrían utilizar en *Spectrum*.
5-9	View only. Los niveles del 5 al 9 son exactamente los mismos, pero igual al caso anterior, los números del 6 al 9 están reservados para futuros usos dentro de *Spectrum*.

La implementación de estos niveles de seguridad en *Spectrum* se lleva a cabo en dos partes del sistema; en las vistas jerárquicas y en el *UserEditor*. A continuación se muestran ejemplos de estas ventas de administración.

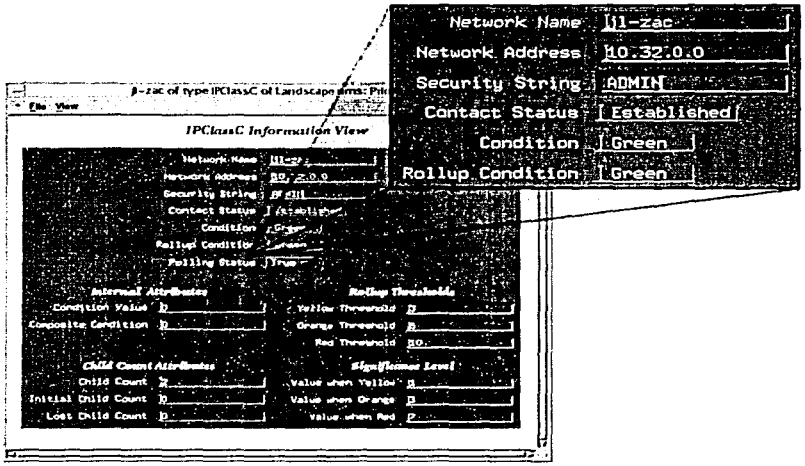


Figura 4.2.5.5 Vista en donde se configura el Security String

Recordemos que los *security strings* se aplican a las vistas jerárquicas de *Spectrum* y que estos se heredan a las vistas jerárquicamente más bajas (o bien más específicas).

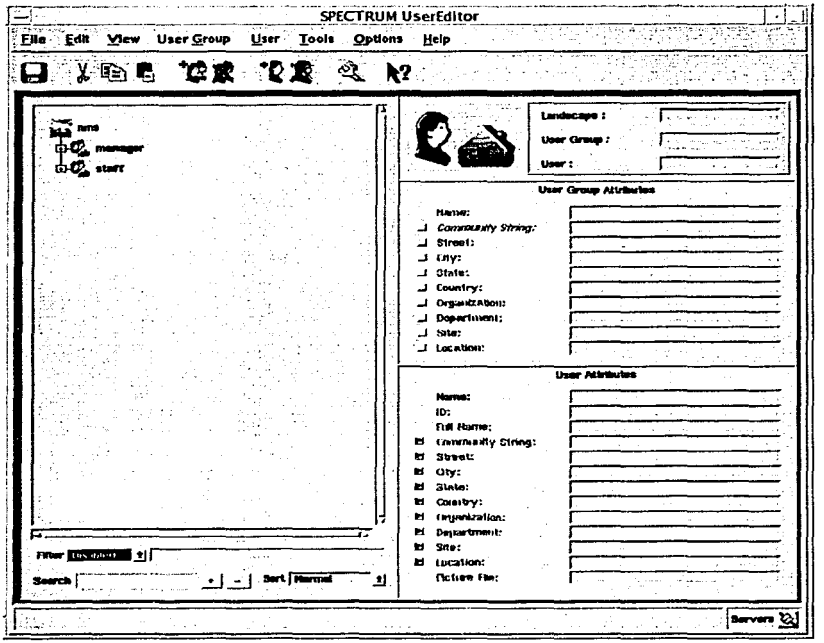


Figura 4.2.5.6 Spectrum User Editor

Como se puede observar en la figura anterior, existe tanto un community string para los grupos de usuarios como para cada usuario individual. Como el grupo de usuarios es el modelo padre del usuario individual, el grupo heredará el community string a cada usuario perteneciente al mismo.

Patrol

En patrol también existen mecanismos similares para garantizar la seguridad propia de la aplicación como las descritas para *Clarify* y *Spectrum*, pero lo más importante es que *Patrol* a través de sus agentes instalados en las máquinas a monitorear, puede darnos información relevante en cuanto al manejo individual de la seguridad de cada estación.

En este trabajo haremos mención de las variables de *Patrol* relacionadas con las estaciones *UNIX*, que ocupan el mayor porcentaje de los sistemas que se estarán monitoreando en RedIFE.

La aplicación de seguridad dentro de Patrol para UNIX contiene los siguientes componentes:

- *Administration.* Provee una lista de los archivos de grupo y *passwords* y muestra los intentos fallidos de login.
- *List SUID and SGID Files.* Despliega todos los archivos que tienen el SUID o el SGID (GUID) bit encendido.
- *List Failed su/msu Logins.* Despliega información respecto a cada usuario que trata de ejecutar los comandos «su» o «msu» y que fallan en la autenticación.
- *List Users Without Password.* Despliega todos los usuarios que no tienen *password.*
- *List Duplicate User Id Entry.* Despliega todos los usuarios que tienen múltiples sesiones activas.
- *List Files With Global Write.* Despliega todos los archivos que pueden ser modificados/borrados por cualquier usuario del sistema.

La aplicación de seguridad de *Patrol* puede ser accesada a través de la pantalla en donde aparece el icono de seguridad que se muestra al centro la siguiente figura 4.2.5.7.

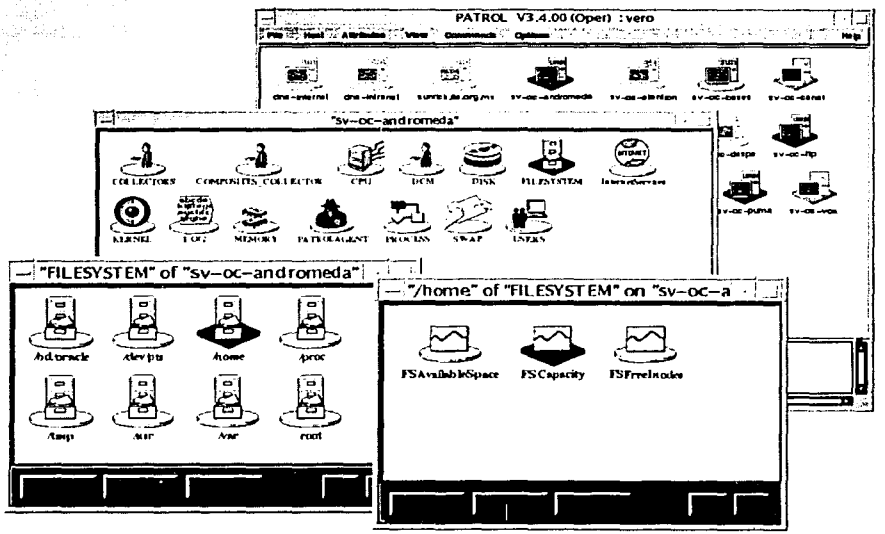
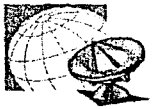


Figura 4.2.5.7 Vista de los elementos de un sistema UNIX



Además de poder monitorear la seguridad de los sistemas, *Patrol* puede establecer seguridad a nivel de ejecución de comandos hacia las máquinas administradas. Se puede establecer también la seguridad para que se herede a todos los comandos de una misma máquina, a un grupo de ellas o bien a todas.

4.3 CREACIÓN DE REPORTES Y ESTADÍSTICAS DE DESEMPEÑO

Se generarán diversos tipos de reportes, tanto en formato tabular como en formato gráfico.

Se tendrán dos tipos principales de reportes, aquellos que informan del comportamiento de los dispositivos de red, los cuales veremos a continuación, y los que se refieren a la atención de reportes o casos.

Reporte de Alarmas

Este reporte muestra información de problemas actuales en la red, es decir, problemas que se estén presentando al momento de generar el reporte, como se muestra en las Figura 4.3.1a y 4.3.1b. Estos presentan las siguientes columnas:

- Fecha y hora en que se obtiene el reporte
- Tipo de equipo
- Nombre
- Identificador de la alarma
- Condición de la alarma
- Causa
- Total de alarmas

Donde las condiciones de alarmas se muestran por colores:

- Rojo significa que Spectrum ha perdido contacto con ese dispositivo.
- Naranja indica que el equipo tiene una alarma de segundo nivel, como puede ser, que se detecto falla en algún puerto o tarjeta dejándolo parcialmente funcional.
- Amarillo es una alarma menor.
- Gris indica un status desconocido, esto debido a que el equipo es inalcanzable ya que hay una falla en un equipo anterior.
- Azul es una condición inicial, en la que se encuentra el equipo al modelarlo antes de que se tenga contacto con él.

En este reporte se puede especificar que se muestren datos de los equipos que presenten algún o algunos tipos de alarmas en particular.

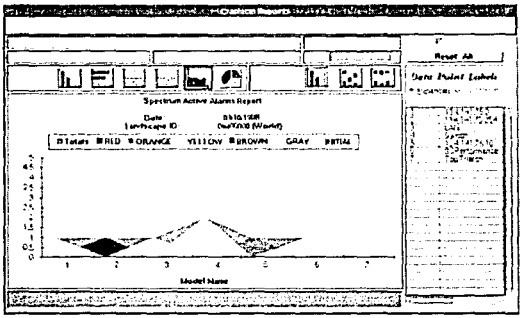


Figura 4.3.1a Reporte de alarmas gráfico

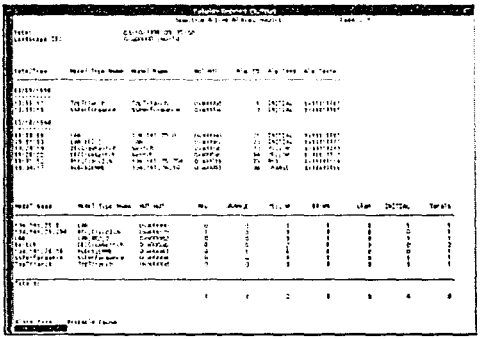
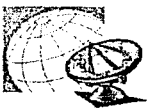


Figura 4.3.1b Reporte de alarmas tabular

Reporte de Eventos

Este permite obtener datos históricos de los dispositivos de red, donde un evento es cualquier suceso que se presente en un equipo, como puede ser una alarma, una modificación en la configuración, etc.

El reporte de eventos muestra, como en la Figura 4.3.2, la siguiente información:



- Rango de tiempo del que se obtuvo la información
- Fecha y hora del reporte
- Equipo o equipos que se están reportando
- Tipo de evento

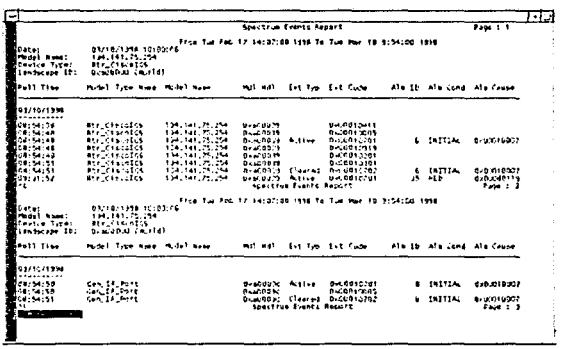


Figura 4.3.2 Reporte de eventos

Reporte Estadístico

Este provee información del performance de la red, analizando sus dispositivos y las interfaces de estos (ver Figuras 4.3.3a y 4.3.3b), mostrando los siguientes datos:

- Equipo
- Índice de errores
- Índice de paquetes
- Índice de paquetes descartados
- Utilización

Con estos datos se pueden obtener cálculos estadísticos como promedios, máximos y mínimos, desviación estándar, y totales, además de la utilización de expresiones aritméticas para realizar cálculos adicionales.

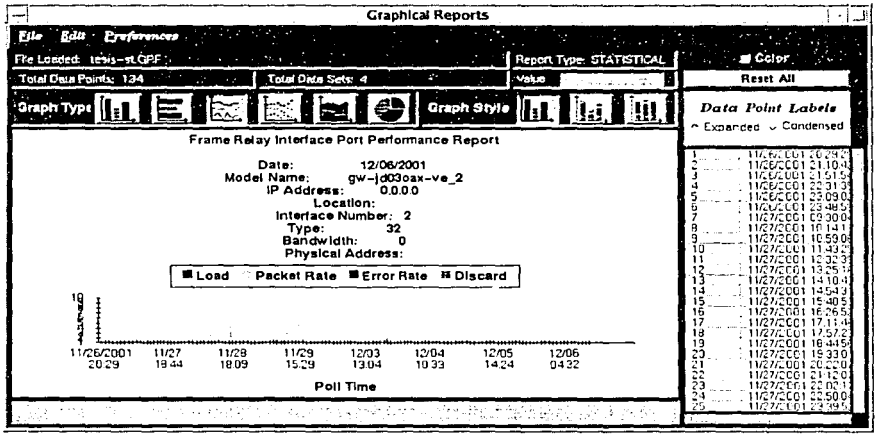


Figura 4.3.3a Reporte estadístico gráfico

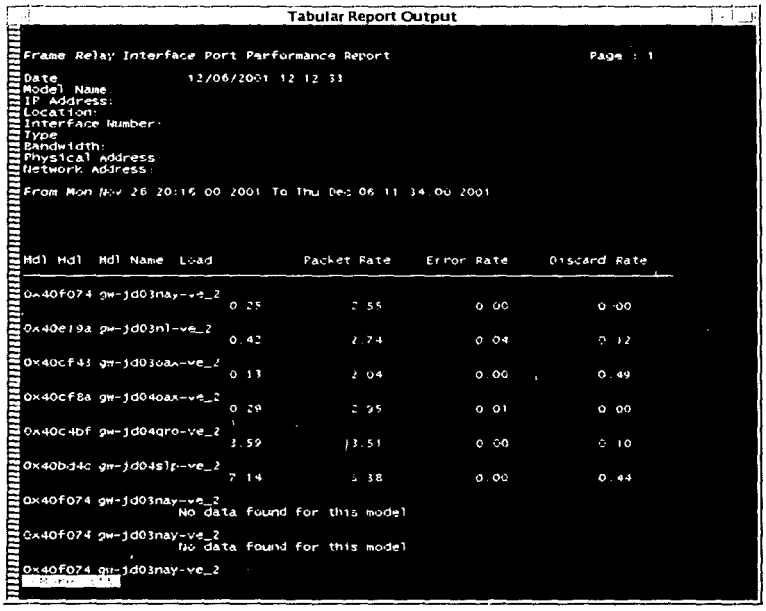
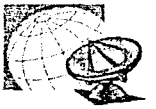


Figura 4.3.3b Reporte estadístico tabular

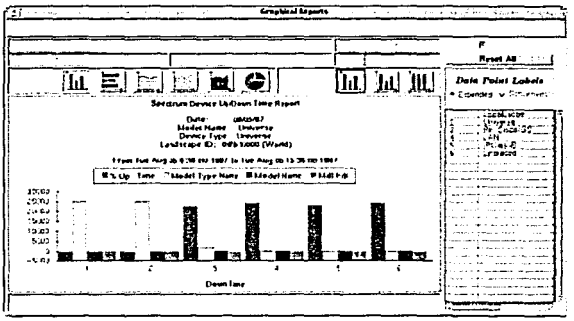


Reporte Up/Down

Permite verificar cuando se ha perdido contacto con los dispositivos y cuando se ha reestablecido, y puede calcular el tiempo en el que un dispositivo estuvo *up* y/o *down*. Tomando en cuenta que cuando se pierde contacto, se considera al dispositivo down, cuando se tiene contacto se dice que el dispositivo se encuentra up. Mostrando los siguientes datos:

- El dispositivo
- Hora en que se perdió la conexión
- Hora en que se reestableció la conexión
- Tiempo total que no se tuvo contacto
- Tiempo total en que se tuvo contacto
- Porcentaje de tiempo que no se tuvo contacto
- Porcentaje de tiempo que se tuvo contacto

En las Figuras 4.3.4a y 4.3.4b se muestran ejemplos de un reportes up/down.



4.3.4a Reporte Up/Down gráfico

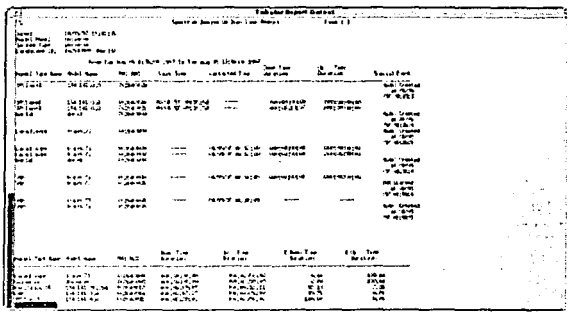


Figura 4.3.4b Reporte Up/Down tabular

A continuación veremos los reportes referentes a los casos y a los Ingenieros que los llevan.

En forma tabular, se obtendrán los siguientes reportes:

Reporte de casos

Este contendrá un listado detallado de los casos de uno o varios Ingenieros. El cual contendrá la siguiente información:

Encabezado:
- Periodo de tiempo que incluye el reporte
- Los Ingenieros que están incluidos en el reporte, por default son todos

Columnas:
- El sitio donde radica el problema, que puede ser alguna Junta Ejecutiva o algún site en Oficinas Centrales
- El número de caso
- Fecha y hora de creación
- Status del caso
- Tiempo que lleva el caso abierto, si no se ha cerrado, o en su defecto el tiempo que tardó en resolverse
- El equipo o enlace que halla presentado la falla
- Descripción del problema
- Tiempo total que se utilizó hablando con el sitio problema
- Tiempo total utilizado para resolver el problema
- Tiempo total de trabajo, que es la suma de los dos anteriores

Reporte por tipo de falla

Muestra un resumen informativo de las fallas que se asignaron a cierto Ingeniero, ordenados por problema, incluyendo:

Encabezado:
- Periodo de tiempo que incluye el reporte
- Los Ingenieros que están incluidos en el reporte, por default son todos

Columnas:
- Tipo de falla
- Número de casos abiertos durante el lapso de tiempo especificado
- Número de casos cerrados en el periodo indicado
- Número de casos abiertos y cerrados en ese periodo

- Promedio de tiempo utilizado para resolver los casos
- Promedio de tiempo que pasa entre que se creó el caso y se le comenzó a dar seguimiento
- Promedio de tiempo utilizado en el teléfono
- Promedio de tiempo utilizado en la investigación de la falla
- Tiempo total utilizado en el teléfono con los casos
- Tiempo total utilizado en la solución del caso
- Tiempo total de trabajo en los casos

Reporte por Ingeniero

Muestra información del trabajo desarrollado en los casos por Ingeniero:

Encabezado:
- Periodo de tiempo que incluye el reporte
- Los Ingenieros que están incluidos en el reporte, por default son todos

Columnas:
- Apellido del Ingeniero analizado
- Número de casos abiertos durante el lapso de tiempo especificado
- Número de casos cerrados en el periodo indicado
- Número de casos abiertos y cerrados en ese periodo
- Promedio de tiempo utilizado para resolver los casos
- Promedio de tiempo que pasa entre que se creó el caso y se le comenzó a dar seguimiento
- Promedio de tiempo utilizado en el teléfono
- Promedio de tiempo utilizado en la investigación de la falla
- Tiempo total utilizado en el teléfono con los casos
- Tiempo total utilizado en la solución del caso
- Tiempo total de trabajo en los casos

Reporte por sitio

Muestra una lista detallada de los casos creados por sitio:

Encabezado:
- Periodo de tiempo que incluye el reporte

Columnas:
- Sitio analizado
- Número de caso
- Fecha de creación
- Status

- Tipo de caso
- Tiempo que se llevó o se está llevando en solucionar la falla
- Ingeniero que está llevando o llevó el caso
- Equipo o enlace que falló
- Descripción del problema
- Tiempo total utilizado en el teléfono con el caso
- Tiempo total utilizado en la solución del problema
- Tiempo total de trabajo en el caso

En forma gráfica mostramos a continuación algunos ejemplos:

Reporte por tipo de caso (figura 4.3.5)

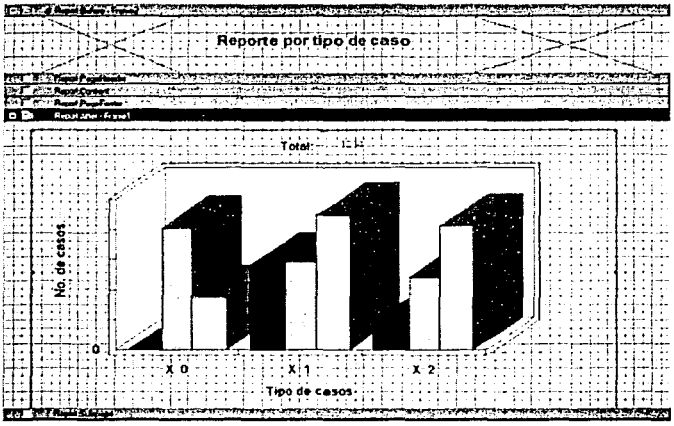


Figura 4.3.5 Reporte por tipo de caso

Reporte de productividad (casos abiertos)

Este nos muestra el número de casos que se encuentran en alguna cola de atención y que aún no han sido solucionados (figura 4.3.6)

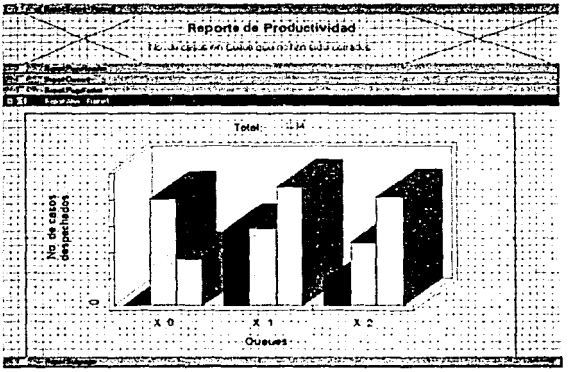


Figura 4.3.6 Reporte de Productividad (Casos abiertos)

Reporte de casos creados por Consultor

Este indica el número de casos que ha creado cada consultor (figura 4.3.7)

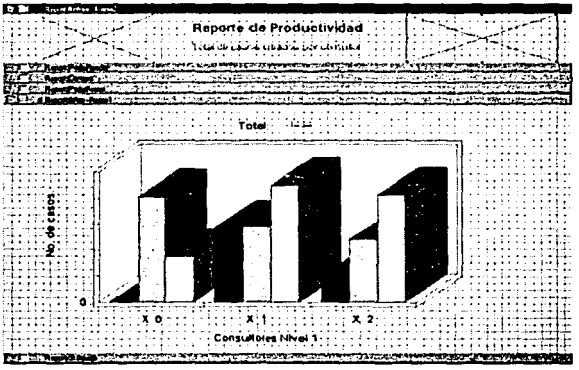


Figura 4.3.7 Reporte de casos creados por Consultor o Ingeniero

Reporte de casos atendidos por Consultor o Ingeniero

Este indica el número de casos que ha atendido cada Consultor o Ingeniero (figura 4.3.8)

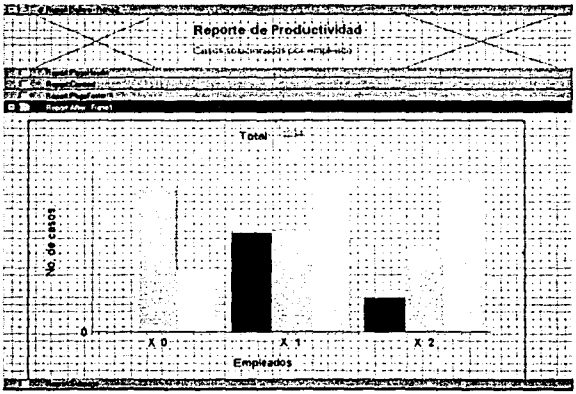
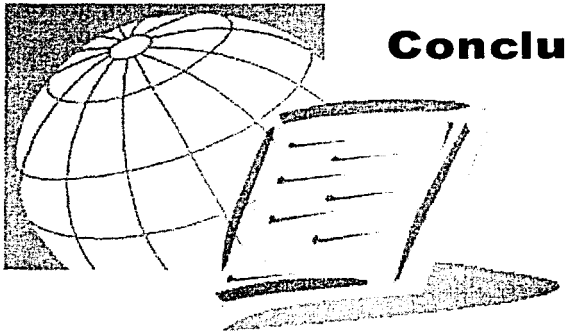


Figura 4.3.8 Reporte de casos solucionados por Consultor o Ingeniero



Conclusiones

En el presente trabajo de tesis se desarrolló un proyecto enfocado a la administración de redes. Este tipo de proyectos requieren de un trabajo multidisciplinario dentro de la rama de la computación y las telecomunicaciones, sin dejar a un lado el aspecto de la administración de proyectos y análisis de procesos.

Es un hecho que el tipo de implementación propuesta depende de un amplio conocimiento y experiencia por parte del ingeniero de redes encargado de proponer y llevar a cabo la coordinación de las actividades y la integración de sistemas para el fin que persigue el proyecto. Sobre todo si los requerimientos establecidos se satisfacen con recursos propios del organismo responsable, en este caso el Instituto Federal Electoral.

Actualmente, existen empresas que se encargan de brindar servicios de administración de redes mediante lo que conocemos como «outsourcing»; es decir, se contrata una empresa encargada de brindar cierto tipo de servicios que no pueden ser proporcionados por el organismo en virtud de la falta de recursos humanos (principalmente) y materiales. Sin embargo, a la vista del público o el usuario, el procedimiento es transparente.

Para el caso del Instituto, el contratar servicios de administración de redes no fue una alternativa debido a las características de organización del mismo. Además de que por motivos de transparencia y confiabilidad de los sistemas y la disponibilidad de la red es necesario mantener la operación de la misma con recursos propios del Instituto.

Se encontró que la solución propuesta y el prototipo de implementación satisfacen las necesidades del Instituto relacionadas con los objetivos del presente proyecto de Tesis.

Las herramientas seleccionadas para integrar el sistema cumplieron con los requerimientos mínimos solicitados por el IFE para la administración de la red.

Spectrum es una plataforma de administración de red suficientemente robusta que integra los elementos y funcionalidades necesarias planteadas por el Modelo ISO de administración de redes, sobre todo las que son prioritarias para el Instituto: administración del desempeño, administración de fallas y administración de configuraciones.

Por su lado Patrol, de BMC, es una aplicación de administración de redes que se integra transparentemente a Spectrum conformando un sistema de administración de redes capaz de brindar mecanismos para la automatización de las actividades de administración de equipos, enlaces y aplicaciones de manera centralizada y con la opción de migrarse a una arquitectura distribuida en caso de ser necesario.

Por su lado, Clarify, es un sistema que proporciona funcionalidades complementarias al sistema de administración de red (Spectrum/Patrol) para atender las fallas de forma proactiva y eficiente cumpliendo completamente con este aspecto del Modelo ISO. La herramienta es lo suficientemente personalizable y adaptable a las necesidades del organismo y se acopla perfectamente a los flujos de trabajo que normalmente se llevan en las empresas e instituciones.

Este tipo de implementaciones, a pesar de que en cada institución o empresa se tienen que amoldar a las necesidades propias del organismo, se pueden llevar a cabo de manera sistematizada y atendiendo a estándares y modelos definidos. Por ende, este documento puede servir como una buena referencia para personas que tienen a su cargo la administración de redes complejas y heterogéneas utilizadas para el uso de sistemas de carácter crítico y que requieren de una alta disponibilidad de la infraestructura.

Este trabajo representó un reto importante para nuestro desarrollo personal. Para el desarrollo del mismo fue necesario aplicar en gran medida la experiencia y conocimientos adquiridos a lo largo de algunos años al estar trabajando con redes de datos y atendiendo a las personas que las usan. Es claro que la administración de redes no es una labor sencilla, en muchos casos se considera como una actividad más de los servicios de valor agregado, sin embargo esto hace la diferencia al evaluar la productividad que proporciona

una red de datos para el manejo de sistemas informáticos, transferencia de archivos y comunicación interna de la organización.

Como hemos visto, en los últimos años, el auge que han tenido las comunicaciones y el desarrollo de la tecnología nos ha permitido crecer como país, esto lleva a que una institución como lo es el IFE, de quien dependen las Elecciones Federales, debe tener una buena comunicación interna y servicios eficientes que ayuden a su labor, y con esto a la credibilidad y transparencia en su trabajo.

Es precisamente por esto la creación del Centro de Operación, de quien depende el buen funcionamiento de la red y de los servicios que se proporcionan.

La parte más importante de un Centro de Operación reside en la forma en que se hagan convivir las herramientas a utilizar y que tan flexible sea para futuras adecuaciones, sin embargo un buen diseño de las políticas de notificación y escalación junto con un robusto sistema de reportes nos darán una idea muy aproximada de como nuestra empresa esta funcionando y cuales son las áreas en donde se pudieran hacer mejoras.

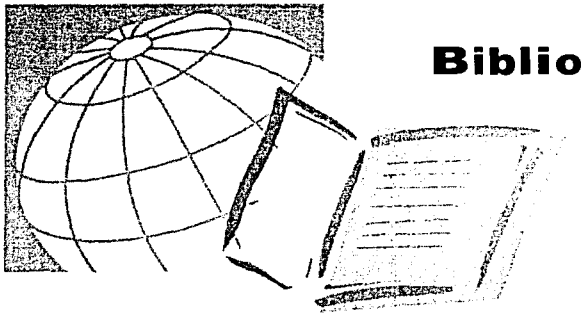
La idea detrás de los sistemas de operación de la red, es capturar la mayor cantidad de conocimiento de sus empleados para llegar a automatizar al máximo las tareas sin necesidad de utilizar demasiado tiempo de sus empleados. Sin embargo el fin de todo NOC es invertir en sistemas y gente que nos hagan ser más eficientes ahorrando así a mediano y largo plazo dinero invertido en la operación del negocio o servicio que se ofrezca a nuestros usuarios, sean internos (gente perteneciente a la organización) o externos.

Al automatizar los procesos operativos vimos reflejados las necesidades e importancia de interacción entre las diversas áreas de operación y atención a usuarios dentro del Instituto, obteniendo así un mayor conocimiento sobre los flujos de trabajo que existen en él, así como el compromiso de servicio ante las diversas áreas que lo componen.

Es importante mencionar el impacto que se obtuvo con el usuario al tener un mayor control en la operación de la red, es decir, cuando el usuario ve a la red como una herramienta con la cual agiliza su trabajo y no se preocupa de su funcionamiento. Esto significa que la operación de la red es transparente para él, esto gracias a la proactividad ante posibles fallas y buen monitoreo de ésta.

Sobre la formación que adquirimos en la Facultad de Ingeniería, tenemos que reconocer que el esfuerzo que hay detrás de las clases impartidas en las

aulas y fuera de ellas, se ve recompensado con ese sentido analítico al que a cada Ingeniero distingue de entre los demás. A nuestra forma de ver, esa es una de las grandes enseñanzas que la Facultad de Ingeniería nos legó y que más hemos aprovechado al desarrollar nuestras actividades profesionales.



Bibliografía

- Haight, T. «The Steady Increase of Client/Server.»
  Client/Server Computing:The Strategic Edge For A Changing Landscape.
  A Supplement To InformationWeek, (1993): Pag. 80

- Hachtel, George. «A Best of Breed Approach to Client/Server.»
  Data Management Review, vol 4. no. 1
  Enero, 1994, Pags: 17-19.

- Huff, Richard A. «Client/Server Technology: Is It A Bill of Goods?»
  Information Strategy: The Executive's Journal, v12 n1
  Otoño 1995, Pags: 21-28.

- Diamond, Sidney «Client/server: Myths & realities.»
  Journal of Systems Management, v46 n4
  Jul/Ago 1995, Pags: 44-48.

- Rifkin, Glenn. «Information technology: The Client/server challenge»,
  Harvard Business Review, v72 n4
  Jul/Aug 1994, Pags: 9-10.

- Ramarapu, Narender K. «Client/server computing : Is it the right choice»,
  Information Strategy: The Executive's Journal, v12n2
  Invierno 1996, Pags: 39-41.

- Parr, Harvey. «Can Client server live up to its promise?.»,
  Insurance System Bulletin, v11 n4
  Oct 1995, Pags:6-8.

- Renaud, Paul E. (1993). Introduction to Client/Server Systems. New York: John Wiley & Sons, Inc.

- Pras, A.
  Network Management Architectures
  [CTIT Ph. D.-thesis series No. 95-02], ISSN 1381-3617 / ISBN 90-365-0728-6, 17 February 1995, 195 pp.

- Understanding Client-Server Computing
  Bill Fastie, PC Magazine.
  Enero 18, 1999.

- Broadband Communications
  Balaji Kumar
  McGraw Hill, Nueva York 1998

- Total SNMP
  Sean Harnedy
  Prentice Hall, 1998

- Esencial System Administration
  Aeleen Frisch
  O'Reilly, 1995

- Solaris 2.x System Administration I y II
  Student Guide
  Sun, 1998

- Solaris 2.x Server Administration
  Student Guide
  Sun, 1998

- Funciones del Instituto Federal Electoral
  http://www.ife.org.mx
  Responsable de la página: Instituto Federal Electoral

- Infraestructura de cómputo y comunicaciones, y servicios proporcionados a través de la red nacional de cómputo del IFE
  http://intranet.ife.org.mx
  Responsable de la página: Instituto Federal Electoral

- Fundamentos cliente-servidor
  http://www.networkcomputing.com/shared/netdesign/1005part1a.html
  Responsable de la página: United Business Media

- Arquitectura cliente-servidor
  http://www.zdnet.com/devhead/stories/articles/0,4413,382414,00.html
  Responsable de la página: ZDnet

- Arquitectura cliente-servidor
  http://www.sei.cmu.edu/str/descriptions/clientserver_body.html
  Responsable de la página: Carnegie Mellon Software Engineering Institute

- Tecnologías de transporte.
  http://grouper.ieee.org/groups/802/3/
  Responsable de la página: IEEE

- Tecnologías de transporte
  http://standards.ieee.org/catalog/it_toc.html
  Responsable de la página: IEEE

- Tecnologías LAN (ethernet)
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm
  Responsable de la página: Cisco Systems

- Tecnologías WAN (frame relay)
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm
  Responsable de la página: Cisco Systems

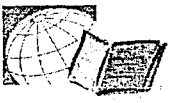
- Tecnologías WAN (PPP)
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ppp.htm
  Responsable de la página: Cisco Systems

- Tecnologías WAN (Control de enlace de datos síncrono)
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/sdlcetc.htm
  Responsable de la página: Cisco Systems

- Características de Spectrum
  http://www.enterasys.com/products/whitepapers/
  Responsable de la página: Enterasys Networks

- Características de Clarify
  http://www.clarify.com
  Responsable de la página: Nortel Networks

- Documentación de Spectrum
  http://www.enterasys.com/support/manuals
  Responsable de la página: Enterasys Networks



- Características de Patrol
  http://www.bmc.com/
  Responsable de la página: BMC Software