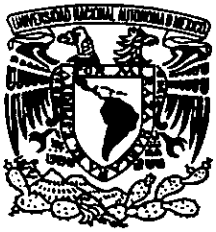
2
2ej.



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN

ADMINISTRACION CENTRALIZADA DE REDES

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A :

LUCILA AGUILAR SALVADOR

ASESOR: ING. JUAN GASTALDI PEREZ

MEXICO 1998

A Dios por guiar mi camino en todo momento

A mis padres por el profundo amor y apoyo que me han brindado toda la vida, ya que gracias a sus esfuerzos logre terminar mi carrera profesional.

Lucila Aguilar Salvador.

CONTENIDO

IV. CONTROL DE FALLAS

V. CONTABILIDAD DE LOS RECURSOS.

VI. SEGURIDAD.

VII. EVALUACIÓN OPERATIVA.

VIII. SOFTWARE DE APLICACIÓN.

INTRODUCCIÓN

En la actualidad las redes de computadoras son una área muy dinámica en la que los avances y nuevos descubrimientos se producen a una velocidad asombrosa. Es difícil estar al día y más aún prever los cambios que habrá en ésta área. Por lo cual empresas grandes, medianas y pequeñas deben de estar a la vanguardia en cuanto al proceso de su información, esto permitirá que alcancen un nivel alto de desempeño.

El objetivo de este trabajo consiste en ofrecer un conocimiento de como se debe realizar la administración centralizada de una red de computadoras, debido a que en la actualidad se administra conforme se van presentando los eventos y en el lugar donde ocurren éstos, sin tener un control total de todo el sistema, para esto necesitamos establecer una relación completa entre hardware y software que nos permita visualizar y accesar a todos y cada uno de los dispositivos y/o recursos que forman una red.

La tesis primeramente pretende dar un bosquejo de todos los conceptos necesarios para entender el funcionamiento de los componentes más importantes que forman una red de computadoras.

Un punto importante en el que se hace hincapié, es en el control de dispositivos ya que se explican los conceptos y bases necesarias para que trabaje un software administrador de red.

Asímismo se expone cómo mediante dicho software se facilita el manejo de cada una de las áreas que forman la administración de una red.

Finalmente se analiza un software de aplicación y sus diversas características que permiten una administración centralizada de redes, además de hacer mención de otros productos que tienen la misma función.

I. ANTECEDENTES

En los años 60´s y 70´s la información se procesaba en sistemas grandes como son minis y macrocomputadoras que son sistemas de proceso centralizado, es decir manejan una gran cantidad de información la cual es solicitada por terminales tontas, dichas terminales no realizan ningún proceso, conforme iba evolucionando la tecnología de las computadoras estas se hicieron cada vez mas potentes en cuanto a procesamiento, almacenamiento y en general en su arquitectura; hasta que en la actualidad se cuenta con computadoras tan evolucionadas que cuentan con inteligencia artificial y reconocimiento de voz entre otras características. Es tan grande el desarrollo tecnológico que ha tenido el mundo de la computación, que es muy importante estar al tanto de cada descubrimiento tecnológico sobre esta área y hacer de esto un hábito para estar enterado y no quedar fuera del gran auge de evolución informática que estamos viviendo.

En la actualidad las redes son una parte primordial dentro del desarrollo informático ya que las grandes empresas, industrias, Instituciones educativas y corporaciones de todo tipo procesan su información mediante redes de computadoras ya sean de cobertura pequeña (LAN) o de gran cobertura (WAN).

1.1 DEFINICIÓN.

Para entender la importancia de las redes es necesario entender que es una red. Una red es la comunicación que existe entre computadoras, dicha comunicación se establece mediante medios físicos (cable) y medios de software como son los protocolos de comunicación los cuales indican bajo que estándares se va a establecer la comunicación, logrando con esto compartir información (archivos), compartir recursos como impresoras, plotters, dispositivos de almacenamiento, o poder accesar a otros sistemas como pueden ser minis o macrocomputadoras.

Componentes:

- Uno o más servidores.
- Estaciones de trabajo.
- Dispositivos periféricos.
- Tarjetas de red.
- Medio de comunicación.

Cada estación de trabajo y servidor deben de tener una tarjeta de red, la cual conecta a los servidores con las estaciones de trabajo a través de un medio de comunicación que puede ser un cable, es necesario mencionar que existen redes inalámbricas las cuales realizan su comunicación mediante rayos infrarrojos o por radio. Los dispositivos periféricos pueden ser atados a los servidores, estaciones de trabajo o al cable.

- **SERVIDOR**

Un servidor es por lo general una computadora con una capacidad muy alta de proceso, de memoria y de almacenamiento en la cual se instala un sistema operativo de red para proveer a dicha red de recursos y servicios para las estaciones de trabajo y otros clientes.

- **ESTACIÓN DE TRABAJO**

Una estación de trabajo es una computadora sola que puede estar atada a un servidor o funcionar independiente de la red, es dueña del proceso y puede administrar su software y sus archivos de datos, se le considera el cliente mas común dentro de una red ya que un cliente es aquel que pide recursos o servicios al servidor.

- **DISPOSITIVOS PERIFERICOS**

Los dispositivos periféricos son las impresoras, discos duros, módems etc. los cuales complementan a la red para que ésta pueda ofrecer todos sus servicios y recursos.

- **TARJETA DE RED**

Una tarjeta de red es un conjunto de circuitos que permite al servidor y la estación de trabajo comunicarse entre si.

- **MEDIOS DE COMUNICACIÓN**

El medio de comunicación es el enlace entre dos dispositivos en la red que permite comunicarse entre si. El medio de comunicación puede ser cable coaxial, par trenzado, fibra óptica etc. el cual va conectado a la tarjeta de red en cada estación de trabajo hacia un concentrador o hacia el servidor directamente dependiendo de la topología de la red.

1.2 ARQUITECTURA DE UNA RED.

La arquitectura de una red esta definida principalmente por:

- La topología.
- El método de acceso al cable.
- Protocolos de comunicación.

- **TOPOLOGÍA**

La topología de un red es la forma física en la que queda instalado el cable que conecta a las estaciones de trabajo con el servidor, esto es muy importante cuando se va a instalar una red ya que se debe hacer una evaluación rendimiento contra costo pues depende del tipo de topología que elijamos para tener cierto rendimiento en nuestra comunicación.

Existen básicamente 3 tipos de topologías las cuales son: bus, anillo y estrella .

- **BUS**

Consiste en que todas las computadoras estan conectadas al servidor mediante un cable lineal, es como una avenida a la cual se accesa por todas las calles perpendiculares a esta, tiene un método de acceso al cable llamado CSMA/CD (Carrier Sense Multiple Access with Collision Detection) Acceso múltiple por detección de portadora con detección de colisiones.

- **ANILLO**

Consiste en comunicar a las computadoras mediante un cable que termina cerrándose así mismo formando un anillo o circulo, tiene un método de acceso al cable de pase de testigo.

- **ESTRELLA**

Consiste en comunicar a las computadoras mediante un cable para cada una, que va hacia un concentrador y este concentrador a su vez al servidor o a otro concentrador estableciéndose una conexión de tipo jerárquica hacia el servidor, puede usarse ambos métodos de acceso al cable como es CSMA/DC o PASE DE TESTIGO.

En la realidad es muy difícil ver una topología solo en anillo , en bus, o en estrella; normalmente es más común encontrarse con combinaciones de éstas, por ejemplo una red Ethernet idealmente usaría una topología en bus lineal y en la práctica se encuentran redes Ethernet cableada con par trenzado desde las estaciones de trabajo hacia un concentrador lo cual implica una topología en estrella y no la de un bus, pero usa el método de acceso al cable CSMA/DC.

- **METODO DE ACCESO AL CABLE**

Algo muy importante es el método de acceso al cable que utiliza una red, es decir como envía señales una estación de trabajo a otra a través del cable. Existen dos métodos de acceso al cable los cuales son: CSMA/DC y PASE DE TESTIGO.

- **CSMA/CD**

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) Acceso múltiple por detección de portadora con detección de colisiones, que consiste en que una estación de trabajo checa si el cable esta siendo accesado, si no, esta envía su señal la cual se transmite por todo el cable lineal y las estaciones, cada estación revisa si la señal es para ella, si lo es la recibe, si no la rechaza, cuando dos estaciones o nodos emiten a la vez su señal se produce lo que se llama colisión y la sesión de transmisión se bloquea y dichas estaciones de trabajo volveran a intentar enviar su señal esperando un tiempo aleatorio. Las colisiones es un factor que disminuye el rendimiento de una red, pero se ha comprobado que dicho rendimiento disminuye en forma mínima debido a las colisiones.

- **PASE DE TESTIGO**

Un testigo es una estación de trabajo que puede acceder al cable, este tipo de acceso al cable se utiliza normalmente en una topología de anillo, y consiste en que un testigo revisa que el cable no este siendo accesado y verifica que exista otro testigo y emite su señal hacia el testigo que esta disponible esto evita en su totalidad que dos testigos quieran accesar al cable al mismo tiempo ya que al transmitir la señal la receptora revisa si la información es para ella, si no lo es checa que exista un testigo libre y se la pasa a éste y así sucesivamente de una en una hasta que la señal llegue a la estación de trabajo adecuada. Parece ser muy lento pero realmente se transmiten miles de paquetes de información en un segundo.

- **PROTOCOLOS DE COMUNICACIÓN**

Un protocolo de comunicación es un conjunto de reglas o normas que se deben de cumplir para que se realice la comunicación entre equipos o sistemas. Existen protocolos que actúan en los diferentes niveles de una red, como lo son los protocolos de bajo nivel que se aplican para que diferentes equipos se puedan interconectar y funcionar correctamente, es decir funcionan en el nivel físico, en el de enlace de datos o en el de red, logrando que las señales se puedan transmitir entre los diversos equipos, también existen protocolos que trabajan en los niveles mas altos que consiste en la interoperatividad de los sistemas, es decir lograr que una aplicación funcione correctamente o que se pueda trabajar con diferentes sistemas operativos.

Se puede decir que la complejidad de un protocolo se basa en el nivel en el que esta funcionando es decir un protocolo que trabaja en el nivel físico es menos complejo al que trabaja en el nivel de aplicación aunque esto no implica que se pueda prescindir del protocolo de bajo nivel, ya que este es indispensable para establecer la comunicación. Un protocolo de área central hace que el hardware y el software trabajen en conjunto. En síntesis un protocolo que funciona en un nivel bajo se encarga de que funcione el hardware y un protocolo de nivel alto se encarga de que funcione el software.

1.3 CLASIFICACION DE LAS REDES

Existen diferentes formas de clasificar las redes tomando en cuenta diferentes características de estas, un tipo de clasificación se basa en su extensión, es decir si son redes pequeñas llamadas (LAN) o si son extensas que abarcan continentes o países (WAN).

- **RED DE ÁREA LOCAL (LAN)**

Es una red pequeña que normalmente se encuentra en un solo edificio o que tiene de 3 a 200 usuarios y la comunicación entre estaciones y servidor es realizada mediante cables, o líneas telefónicas (utilizando módems).

- **RED METROPOLITANA**

Consiste en la comunicación de varias redes LAN las cuales pueden abarcar cierta área grande especifica, ya sea una ciudad o varias ciudades, para lo cual necesitan un sistema de cableado

especial, es decir ya requieren de comunicaciones mediante líneas telefónicas de alta velocidad, y de antenas de microondas.

- **RED WAN**

Consiste en la comunicación de redes en varios países o en todo el mundo, para lo cual se valen de sistemas de comunicación tan complejos como lo son las antenas de microondas y satélites; además de los medios de comunicación que emplean las redes pequeñas para comunicarse entre sí.

1.4 ORGANISMOS Y NORMAS.

Algunas de las principales organizaciones que se ocupan de actividades de normalización en el campo de los sistemas distribuidos y en el de transmisión a través de redes públicas de datos son las siguientes:

ORGANISMO	ÁREA DE TRABAJO
ISO -Organización Internacional de Normalización	-Interconexión de Sistemas Abiertos (Open Systems Interconection)
CCITT -Comité Consultivo de Telegrafía y Telefonía	-Recomendaciones serie V: Transmisión de datos a través de la red telefónica y Telex. -Recomendaciones serie X: Transmisión de datos a través de la red Pública.
ECMA -Asociación Europea de Fabricantes de Ordenadores	- Transmisión de datos
IFP -Federación Internacional para el tratamiento de la Información	-Comunicación de Datos.
EIA -Asociación de Industrias de Electrónica	-Responsabilización del desarrollo y publicación de estándares para la comunicación de terminales.
IEEE - Instituto de Ingenieros Eléctricos y Electrónicos	-Organización de Normalización y desarrollo en el área de Ingeniería y especialmente en redes locales (LAN).

En base a características como lo es el tipo de cable, el método de acceso al cable, por su topología, o en general por su arquitectura tenemos un conjunto de normas que definen la forma en que las tarjetas de red transmiten información a través de los medios físicos que utilizan como lo es el tipo de cable, el método de acceso al cable, entre otras cosas dichos estándares trabajan bajo ciertos protocolos para su funcionamiento y fueron desarrollados por el Instituto de Ingenieros Eléctricos y Electrónicos.(IEEE) y también han sido adoptados por la Organización Internacional de Estándares (ISO) como parte del estándar OSI.

Los estándares son:

802.1	Interconexión de Redes.
802.2	Control de Enlace Lógico.
802.3	CSMA/CD (Ethernet).
802.4	Redes Token Bus.
802.5	Redes Token Ring.
802.6	Redes de Área Metropolitana.
802.7	Redes de Banda Ancha.
802.8	Redes de Fibra Óptica
802.9	Integración de voz, datos y vídeo a Ethernet e ISDN
802.10	Modelo de Seguridad en Redes
802.11	Redes inalámbricas
802.12	Redes Ethernet a 100 Megabits

802.1 Es un estándar que establece las relaciones entre las normativas de IEEE con el modelo ISO de interconexión de sistemas abiertos.

Los estándares de **802.2** al **802.5** permiten conectar redes con dispositivos de diferentes vendedores y utilizando diferentes tipos de cables y topologías.

La normativa **802.6** permite establecer redes con fibra óptica de alta velocidad de hasta 155 megabits por segundo en redes de área metropolitana.

El estándar **802.7** suministra consultoria sobre técnicas de banda ancha.

802.8 Es un estándar que suministra consultoria sobre técnicas de tecnología de fibra óptica.

802.9 Grupo de redes integradas de voz y datos que trabaja actualmente en la Integración de datos, voz y vídeo a redes 802 e ISDN.

802.10 Grupo técnico asesor en seguridad de redes que desarrolla una definición estándar de un modelo de seguridad en redes.

802.11 Desarrolla estándares para redes inalámbricas.

802.12 Trabaja en estándares para Ethernet de 100 megabits por segundo.

1.5 LOS TRES GRANDES ESTÁNDARES DE LAN

- **ETHERNET**

Es un estándar de IEEE, desarrollado originalmente por Xerox utiliza una topología de bus lineal principalmente con un método de acceso al cable CSMA/DC, y los nodos de la red están conectados por un cable, éste puede ser coaxial, par trenzado o fibra óptica. Ethernet tiene una velocidad de transmisión de 10 MegaBits /segundo.

Cuando se habla de una red Ethernet se debe de saber que existen diferentes adaptaciones de ésta, es decir adaptaciones del estándar 802.3 dichas adaptaciones varían entre el tipo de cable que utilizan, en la velocidad a la que transmiten y en el largo del cable que soportan, algunas de estas se explica su nomenclatura de la siguiente forma, el primer número implica la velocidad a la que transmite en Mb/seg., el numero final indica los metros por segmento multiplicándose por 100 y la palabra BASE viene de Banda Base y BROAD de Banda Ancha.

Por ejemplo:

10BASE-T . Cable de par trenzado con una longitud máxima de segmento de 100 metros y una velocidad de transmisión de 10 Mb/seg.

10BASE-5. Cable coaxial con una longitud máxima de tramo de hasta 500 metros, usando transmisión en banda base

10BASE-2 . Cable coaxial (RG-58 A/U) con una longitud máxima de segmento de hasta 185 metros usando transmisión en Banda Base.

1BASE-5. Cable de par trenzado con una longitud máxima de segmento de 500 metros y una velocidad de transmisión de 1 Mb/seg.

10BROAD-36. Cable coaxial (tipo RG-59/U CATV) con una longitud máxima de segmento de 3600 metros usando método de transmisión en Banda Ancha.

10BASE-F. Segmentos de cable de fibra óptica con transmisión de 10 Mb/seg.

- **TOKEN RING**

Una red Token Ring esta basada en el estándar 802.5 del IEEE y fue diseñada por IBM. Es una red que usa una topología en anillo pero a su vez puede configurarse en estrella, es decir se establecen jerarquías con los anillos, usa un método de acceso al cable de pase de testigo, para formar su anillo lógico utiliza un hub central o mejor conocido como una unidad de acceso multiestación (MAU), al cual se pueden conectar hasta ocho estaciones.

Los MAU se conectan entre si mediante enchufes que tienen de entrada y salida formándose así un anillo lógico , además cuenta con un sistema de tolerancia a fallas por si el cable que conecta a dos MAU se rompe, simplemente las señales se conducen en dirección opuesta para crear un anillo en sentido contrario. Las placas Token Ring de IBM transmiten de 4 a 16 Mb/seg.

- **ARCNET**

ArcNet es un sistema de red que utiliza un método de acceso al cable de pase de testigo y se puede configurar en estrella y bus, transmite a una velocidad de 2.5 MB/seg., no es un estándar de IEEE, como lo es Token Ring y Ethernet.

En configuración de estrella soporta longitudes grandes en el cable de hasta 600 mts. y en bus de 300 mts., esto hace de ArcNet una opción muy buena cuando el costo es un factor determinante en el diseño e instalación de una red, aunque se transmita a una velocidad baja. En la actualidad ya se puede transmitir a 20 Mb/seg. en configuraciones ArcNet.

1.6 INTECONEXIÓN DE REDES LOCALES

Cuando una red empieza aumentar sus estaciones de trabajo se necesita de dispositivos que permitan expandirla y mejorarla en su rendimiento tal como son los repetidores, puentes o ruteadores. Estos dispositivos logran establecer la comunicación hacia segmentos remotos o enlazar servidores dentro de un edificio o Campus como lo es un backbone entre otros.

- **REPETIDORES**

Un repetidor es un dispositivo que amplifica una señal a través del cable. Cuando una señal se transmite por un cable esta tiende a degenerarse en proporción a la longitud del cable que recorre, a este fenómeno se le llama atenuación de una señal, lo que hace el repetidor es amplificar la señal que le llega para retransmitirla a lo largo del resto del cable, no la modifica o altera solo la amplifica y la retransmite.

Las características mas representativas de un repetidor son:

- Un repetidor amplifica las señales para que lleguen mas lejos
- Se utilizan en sistemas lineales como Ethernet.
- Los repetidores funcionan en el nivel más bajo del modelo OSI que es el nivel Físico.
- Los segmentos que se conectan mediante un repetidor deben de tener el mismo medio de transmisión ,es decir el medio de acceso al cable.

Los repetidores se utilizan por lo general dentro de cierta área como lo es un edificio. Los segmentos de red que se conectan a través de un repetidor tendrán la misma dirección de red ,es decir tendrán la misma dirección del servidor pero no tendrán los nodos la misma dirección ya que al ser parte de la misma red esto implica que los nodos serán diferentes, los repetidores funcionan a la misma velocidad de las redes a las que se conectan, por último es necesario aclarar que **no** se debe de tener la idea de que un repetidor sirve para incrementar el número de estaciones de trabajo, o para hacer más grande la red ya que para esto existen otros dispositivos, si no de que un repetidor sirve para conectar estaciones distantes y que les llegue bien la señal.

- **PUENTES**

En su definición básica un puente consiste en instalar dos o más tarjetas de red en un servidor y así participar una red en dos o más segmentos para que dichos segmentos trabajen sin tanto tráfico

de información que implica estar en una sola red, una característica importante es que dichos segmentos son más pequeños que la red original o pueden ser diferentes en cuanto a tipo de red, como lo es Ethernet, Token Ring, ArcNet, fibra óptica etc., es decir un servidor puede tener dos tipos de red como lo es Token Ring y Ethernet mediante dos tarjetas de red.

Un puente tiene un cierto nivel de inteligencia para conectar redes, por ejemplo al tener dos redes va a distribuir de mejor forma los paquetes de información ya que va a saber a que segmento de red corresponde dicho paquete y este no va estar viajando por toda la red hasta encontrar su destino, el puente coloca los paquetes en el segmento de red adecuado disminuyendo con esto el tráfico de la red y aumentando el rendimiento de dicha red.

Un puente lo que hace es filtrar los paquetes de información y rechaza los que no corresponden a cierto segmento de red, sin filtrado todos los paquetes serían enviados a todos los puntos de la red, este filtrado de paquetes aumenta en un alto porcentaje en los ruteadores y es más completo en ellos.

Los puentes trabajan en el nivel de enlace de datos y se pueden conectar a dispositivos que utilicen diferentes protocolos, cuando se instala un puente se sobreentiende que cada segmento de red tendrá una dirección de red diferente y por lo tanto los nodos también.

Las razones más importantes por las que se instala un puente son:

- Para ampliar una red existente cuando ésta ha alcanzado su máxima extensión.
- Para eliminar los cuellos de botella que se generan cuando hay demasiadas estaciones de trabajo conectadas a un mismo segmento de red. De esta forma la red trabaja con menos usuarios disminuyendo el tráfico y aumentando el rendimiento de la red.
- Par conectar entre sí distintos tipos de redes como Token Ring y Ethernet.

- **RUTEADORES.**

La función mas importante de un ruteador es encontrar el mejor camino entre el origen y el destino de los paquetes de información dentro de una red. Pueden inspeccionar la información en el nivel de red para determinar la mejor ruta del paquete, los ruteadores son muy importantes para las redes de gran alcance que utilizan enlaces de comunicaciones remotas.

Las razones más importantes para instalar un ruteador son:

- Los ruteadores ofrecen un filtrado de paquetes inteligente y avanzado.
- Los ruteadores son necesarios cuando hay diversos protocolos en una interconexión de redes y los paquetes de ciertos protocolos se tienen que enviar a una área específica
- Los ruteadores ofrece un encaminamiento inteligente lo cual mejora el rendimiento. Un ruteador inteligente conoce la estructura de la red y puede encontrar con facilidad y eficiencia el mejor camino para un paquete de información.
- Como los ruteadores realizan un filtrado avanzado son importantes cuando se utilizan líneas de comunicación remotas lentas y caras.

Un ruteador funciona creando tablas de redes locales, dichas tablas contienen direcciones de red y de nodos, cuando un ruteador recibe un paquete consulta estas tablas para ver si puede enviar directamente el paquete a su destino, si no es así determina la posición de un ruteador que pueda enviar el paquete a su destino ya que además, en la tablas cuenta con la información para llegar a los ruteadores adyacentes y de toda la red.

Un ruteador funciona en el nivel de red y puede ser específico para un protocolo o manejar varios, al trabajar en el nivel de red tienen acceso a la información que contienen los paquetes acerca de que dirección de nodo y a que aplicación van dirigidos.

En base al objetivo principal de los routers que es el de encontrar el mejor camino entre el origen y el destino, cuenta con un método de tolerancia a fallas, esto implica tener varios caminos de respaldo en caso de que el primero y segundo falle, existen dos formas para determinar el mejor camino o el más óptimo, uno es en base al número de saltos que tiene que dar un paquete en la red de ruteadores para llegar a su destino, otro es el evitar segmentos de red congestionados, el elegir uno u otro método depende de los recursos con los que se cuenta de comunicación y de la velocidad a la que se quiere o se necesita transmitir y esto lo decide el administrador o puede dejar que los ruteadores lo decidan.

Cuando se conectan redes mediante ruteadores es necesario establecer que, todos los ruteadores deben de tener los mismos métodos de encaminamiento y debemos saber distinguir entre *ruteadores locales* y *ruteadores remotos*, para saber cuales vamos a utilizar y donde, un *ruteador local* tiene entradas para que se le conecte dispositivos locales como segmentos de red Token Ring Ethernet FDDI, un *ruteador remoto* tiene entradas para conexiones MAN y WAN como son puertos FDDI , puertos X.25, para T1, satélite, microondas, o conexiones para larga distancia, las conexiones a

larga distancia se realizan mediante módems o líneas digitales T1, enlaces vía satélite o microondas entre otras.

La velocidad a la que transmiten los routers es muy importante conocerla ya que por ejemplo en una red Ethernet que transmite 10 Megabits por segundo los routers envían generalmente de 8000 a 15000 paquetes por segundo, si los paquetes son de 64 Bytes, estas tasas de envío son menores en transmisiones WAN ya que existe una gran diferencia en transmisiones LAN y WAN pues mientras en una red LAN se transmite a 10 Mb/s en una WAN se transmite 1 MB /s.

- **BACKBONE**

Es una porción de la red que administra el tráfico pesado, puede ser el punto de conexión de varios edificios o localidades y también tener enlazadas pequeñas redes, se forma por cable de fibra óptica que sirve para conectar a 2 o más servidores, y por lo general, dicho cable transmite información a 100 Mb/seg; y debido a que no transmite señales eléctricas sino haz de luz no tiene distorsión e interferencias eléctricas en la señales, tampoco ruidos o bucles de tierra, por lo cual se logra una transmisión muy eficiente, también se puede configurar en forma de anillo, es decir crear un anillo que una los segmentos de una red con un cable de fibra óptica en doble anillo ofreciendo redundancia por si falla la línea , Una de las aplicaciones más comunes en las que se usa un Backbone son los enlaces de Campus o a nivel metropolitano, como por ejemplo universidades, industrias o edificios.

- **CONCENTRADORES.**

Un concentrador es en esencia un dispositivo que recibe y envía señales de todos y cada uno de sus puertos independientemente de que dispositivo este conectado a dicho puerto. Entre los dispositivos que se le pueden conectar estan los propios concentradores que se conectan en cascada, también estaciones de trabajo, servidores tanto de red como de comunicaciones.

Existen concentradores de 4,8,12 y 24 puertos, cuando se utilizan estos dispositivos se genera una configuración tipo estrella estableciendo ciertas jerarquías en la red, no importando si es una red Ethernet, Token Ring o ArcNet. En la actualidad se pueden monitorear y administrar fácilmente gracias a unos agentes que contienen llamados MIBs.

- **FDDI**

(Fiber Distributed Data Interface). Es un estándar de cable de fibra óptica desarrollado por ANSI. Trabaja a 100 Mb/seg. utiliza una topología en anillo doble, los anillos dobles ofrecen redundancia, si falla un enlace del anillo el anillo se reconfigura de modo que se puede seguir transmitiendo información hasta que se repare el daño .

FDDI es un medio excelente para configurar Backbones, es un medio compartido, lo que implica que su ancho de banda disminuye a medida que más estaciones establecen conexión entre redes.

Ventajas para usar cable de fibra óptica:

- El cable de fibra óptica es inmune a las interferencias electromagnéticas
- El cable de fibra óptica es seguro. No emite señales fuera del cable que podrían monitorearse por extraños.

FDDI usa el método de acceso de pase de testigo, en la red pueden circular varios paquetes si una estación libera el testigo mientras sus paquetes todavía están en tránsito, dos estaciones pueden estar transmitiéndose información mientras que otras dos pueden transmitir el testigo en forma normal, como FDDI tiene dos anillos el segundo lo puede usar para transmitir en forma inversa al primero.

Existe un mecanismo de administración y monitoreo de FDDI que es SMT (Station Management) que permite aislar nodos defectuosos y encaminar el tráfico.

FDDI esta orientado a sistemas que requieren transferencia de grandes cantidades de información, tales como imágenes médicas, procesamiento sísmico tridimensional y simulaciones de reservas de petróleo. La versión II del estándar FDDI esta diseñada para redes que transmiten vídeo de movimiento en tiempo real o cualquier otra información que no tolere ningún retraso.

El número máximo de estaciones en este tipo de red es de 500 abarcando áreas de 200 KM., existen dos tipos de cable de fibra óptica, el monomodal y el multimodal, el monomodal deja pasar una frecuencia luminosa y la distancia máxima que puede haber entre estaciones es de 2 KM., o dependiendo del láser que se use, el multimodal deja pasar varias frecuencias y la distancia máxima entre estaciones es de 60 KM.

FDDI resulta caro, tanto en la instalación como en el mantenimiento, pero puede sustituir enlaces como el de microondas o enlaces de telecomunicaciones.

En la actualidad existe CDDI (Copper Distributed Data Interface) que utiliza cable de cobre y ofrece las mismas velocidades que FDDI, es más barato en su instalación y mantenimiento.

- **ATM**

ATM (Asynchonous Transfer Mode) Modo de Transferecia Asíncrono . Es una tecnología de comunicación de datos, para establecer su definición es necesario explicar algunos conceptos en los que se basa ATM.

RED DE BANDA ANCHA. Es aquella en la que las señales viajan por diversos canales por separado, como en la radiofrecuencia, se soporta la transmisión simultánea de datos, voz y vídeo por varios canales.

CONMUTACION DE PAQUETES. Consiste en enviar pequeñas unidades de información por canales ATM, estas unidades de información se les llama paquetes.

La información es dividida en paquetes de 48 bytes y se le agrega una cabecera de 5 bytes que es la dirección a donde van a ser enviados formando un tamaño de celda de 53 bytes. Los paquetes son situados en un canal ATM.

MULTIPLEXACION POR DIVISION DE TIEMPO. Consiste en combinar señales separadas en una única transmisión de alta velocidad, con ATM se transmiten celdas provenientes de muchas fuentes, pueden mezclarse pero cada una tienen su dirección y destino especifico, en la multiplexación por división de tiempo todas las celdas tienen el mismo tamaño y el mismo tiempo entre sí para su envío.

RETARDO VARIABLE. Es más común en las redes locales e implica que cada red puede utilizar un tamaño de paquete distinto. ATM adapta estos paquetes al tamaño de sus celdas de 53 bytes para transmitirlos.

Por lo anterior podemos decir que ATM es un método para enviar simultáneamente información en paquetes pequeños procedentes de varias fuentes sobre una única línea de alta velocidad donde es reensamblada y enviada a su destino.

ATM combina la conmutación y la multiplexación de paquetes en un método universal de transferencia de datos, las celdas o paquetes de ATM son procesadas rápidamente debido a su tamaño pequeño, hay muy poco retardo en la conmutación de paquetes, esto es importante para la transferencia de voz y vídeo que son sensibles al tiempo.

ATM es un protocolo de transporte que funciona básicamente en el subnivel MAC de la jerarquía de protocolos, no se basa en ningún protocolo determinado, puede convertir cualquier tipo de paquete en celdas de 53 bytes y transportarlos sobre un Backbone o WAN.

ATM esta definiendo el futuro de las comunicaciones en redes de gran alcance. Suprimirá la barrera entre LAN y WAN, esta barrera es el retardo que introducen los puentes o routers al convertir los datos LAN en WAN.

1.7 INTERCONECTIVIDAD EN WAN.

Una red LAN puede expandirse a una red MAN o a una red WAN utilizando conexiones remotas o cables troncales de fibra óptica, el método de enlace depende de los requerimientos o recursos con los que se cuenta, entre estos están:

a) Requerimientos de velocidad de transmisión.
b) Distancia a cubrir por el enlace.
c) Volumen de tráfico entre redes.
d) Patrones de tráfico en la red .
e) Presupuesto.

En las redes locales esta optimizada la transmisión de datos, en la actualidad una red local puede transmitir a 100Mb/seg, pero las WAN no, el rendimiento en velocidad al utilizar una WAN cae al tener que transformar los datos de la red local al formato en que se pueden transportar en las líneas de la WAN.

Para que se puedan comunicar redes LAN y convertirse en MAN o WAN se necesita tanto de dispositivos físicos como son puentes, ruteadores y módems, así como también de sistemas de comunicación que permitan enviar las señales de información a distancia, en puntos remotos; entre los sistemas que se usan están:

- Líneas telefónicas conmutadas
- Líneas alquiladas
- Redes de Datos Públicas
- Conexiones a través de microondas
- Conexiones vía satélite
- Conexiones vía infrarrojo y radio
- Enlaces principales de Campus(Backbone)

Estos sistemas de comunicación de voz, datos y vídeo se pueden clasificar como servicios orientados a la conexión y servicios sin conexión.

SERVICIO ORIENTADO A LA CONEXIÓN. Consiste en una línea dedicada entre dos sistemas que se quieren comunicar, las líneas alquiladas son servicios orientados a la conexión o punto a punto.

SERVICIOS SIN CONEXIÓN. Consiste en enviar la información en paquetes con su dirección a una red de conexiones, los paquetes pueden pasar por muchos nodos o puntos de conexión hasta llegar a su destino y el transmisor y receptor no lo notarán. Las redes de datos públicos son servicios sin conexión.

MULTIPEXACIÓN. Es una técnica para transmitir varias señales simultáneamente a través de una única línea o canal de multiplexación, consiste en mezclar varias señales sobre el cable, formando una línea dedicada lógica, cada señal se encuentra separada en el tiempo, espacio o frecuencia, el dispositivo que realiza la mezcla de señales se llama multiplexor.

- **LÍNEAS TELEFONICAS CONMUTADAS**

Son las mismas líneas que se utilizan para la voz (teléfono). Se necesita un módem en cada extremo de la conexión para convertir las señales digitales en analógicas y viceversa, cuando los módems se encuentran en ambos extremos de la línea y utilizan las mismas técnicas de codificación y compresión de datos, se puede alcanzar velocidades de transmisión de hasta 38.4 Kb/seg.

- **LÍNEAS ALQUILADAS**

Son líneas dedicadas, es decir, permanentemente abiertas que ofrecen una conexión a tiempo completo entre segmentos de red local, las líneas pueden ser digitales.

Cuando es necesaria la interconexión entre varias ciudades y el rendimiento en velocidad de las líneas conmutadas no pueden atender el tráfico, es necesario contratar líneas alquiladas o dedicadas, para lograr esto se puede contratar con la compañía telefónica local, en México Telmex o con una que ofrezca la conexión con las áreas que se desea comunicar. Las líneas alquiladas se clasifican en dos tipos:

- *DS-0* Es una línea de 64 Kb / seg., que ofrece un canal de voz, la voz analógica es muestreada 8,000 veces por segundo para convertirla en un señal digital, esta línea es el bloque principal de la línea T1 por lo cual se llama T1 Fractional.
- *DS-1* Es una línea digital que mantiene líneas dedicadas entre dos puntos, su ancho de banda es de 1544 Mb/seg. y se puede dividir en 24 canales de 64 Kb/seg., ofreciendo cada uno una transmisión de datos o de voz.

- **REDES DE DATOS PÚBLICAS.**

CONMUTACION DE PAQUETES. Es una técnica de entrega de mensajes que sitúa los datos en pequeños paquetes y los transfiere de una fuente a un destino a través de uno o más nodos intermedios.

Las redes de conmutación de paquetes son ofrecidas por las empresas que poseen las redes públicas de datos (PDN; Public Data Network), como son AT&T Company, Telnet, CompuServe, en México Telecom, Telmex, Telnor, Optel, Iusanet, Intervan y UniNet. Las conexiones que se establecen con estas empresas son servicios sin conexión, es decir, la red posee a menudo muchos nodos que ofrecen caminos alternativos o de reserva, nunca se sabe con seguridad el camino que siguen los paquetes para llegar a su destino, lo cual carece de importancia siempre y cuando estos lleguen correctamente y a la dirección adecuada.

Las tecnologías que más se han empleado en México para interconectar redes de datos son: X.25 (46.7%) y de ruteadores multiprotocolo (21.7%). En casos donde se tienen redes de voz y de datos se ha empleado redes basadas en multiplexores TDM (Time División Multiplexin; multiplexaje por división de tiempo).

En México el mercado de servicios de transmisión de datos esta siendo atendido principalmente a través de redes públicas o redes privadas, que utilizan como medio de transmisión líneas digitales rentadas a Telmex o frecuencias satelitales arrendadas a Telecom.

Ejemplo de este tipo de redes.

- ***X.25***

Es un estándar internacional para envío de paquetes a través de las redes públicas de datos, fue definido en 1976 por CCITT (Comite Consultatif International Telegraphie et Telephonie) en el protocolo X.25 .

Para conectar una Red local LAN a una Red X.25 se utiliza un puente o un ruteador X.25. El acceso a la red se realiza a través de líneas dedicas o conmutadas, las líneas dedicadas son normalmente sincronas, de forma que se mejora el rendimiento ofreciendo velocidades de transmisión de 19.2 hasta 64 Kb/seg., las líneas conmutadas utilizan métodos de comunicación asincrona por lo que son necesarios módems que posean su propia circuiteria de corrección de errores.

La transmisión asincrona consiste en agregar a la información un Bit de inicio y final, la transmisión sincrona consiste en enviar la información en bloques separados por tiempo, siendo este igual en todos los bloques.

- ***FRAME RELAY***

Este método mejora y aumenta el rendimiento de conmutación de paquetes eliminando el procesamiento a nivel de red asociado a X.25. En este método la multiplexación y conmutación de datos se realiza en el nivel de enlace de datos, se elimina la necesidad de que los nodos intermedios reconozcan la recepción de paquetes como es necesario en X.25. Las tablas de estado que se utilizan en X.25 en cada nodo intermedio para poder llevar la administración, control de flujo y comparación de errores no son necesarias en Frame Relay, estas solo se necesitan en el punto de partida y en el punto de destino y se les llama interfaces inteligentes las cuales se comunican entre sí por lo cual el proceso se hace significativamente más rápido alcanzando velocidades de 64Kb a 2MB.

- **CONEXIÓN A TRAVÉS DE MICROONDAS**

Las conexiones a través de microondas sirven para enlazar redes LAN en áreas metropolitanas, es decir, se pueden conectar dos redes que estén en edificios juntos o en extremos opuestos de una ciudad. Las redes metropolitanas han sido definidas por el Comité 802.6 del IEEE. El requisito primordial para instalar una comunicación con microondas es que todos los puntos remotos se encuentren visibles a unas 5 millas o 8.5 Km. de distancia. Se instala una antena

parabólica para microondas en cada edificio, las antenas deben apuntar las unas a las otras, se necesita ajustarlas para que la intensidad de la señal sea la óptima para cada antena, se transmite a una velocidad de 1544MB/seg.

- **ENLACE VÍA SATÉLITE**

Este tipo de enlace ofrece velocidades de transmisión como el de T1 a 1544Mb/seg. Para su contratación se paga una tarifa fija y además el tiempo que realmente se usa la conexión, en México Telmex ofrece este servicio. Se necesita de antenas para satélite; se obtiene una gran velocidad de transferencia si la antena es grande; para velocidades de T1 es necesaria una antena de 4 metros de diámetro, existe un retardo en la transmisión vía satélite por lo cual es más recomendable usarla para transmisión de datos y correo electrónico que no son sensibles al tiempo.

- **CONEXIONES VÍA INFRARROJO Y RADIO.**

Las LAN inalámbricas no siempre son completamente inalámbricas, se pueden usar para reemplazar el cableado en ciertos segmentos de la red o para conectar grupos de redes que usan cableado convencional, entre los métodos mas generales están los de señal infrarroja y radio frecuencia.

- *LÍNEA DE SEÑAL INFRARROJA.* Se usan las ondas de luz de alta frecuencia para transmitir datos entre nodos con distancias de hasta 24.4 metros, mediante una ruta sin obstrucciones; los rayos infrarrojos no pueden pasar a través de paredes de mampostería. La proporción de datos es relativamente alta en rangos de décimas de megabits por segundo.

- *RADIO DE ALTA FRECUENCIA.* Señales de radio de alta frecuencia transmiten datos a nodos con distancias de 12.2 a 39.6 metros, dependiendo de la naturaleza de la obstrucción que los separe; la señal puede penetrar paredes delgadas, pero no admite mampostería. La proporción de datos generalmente es menor a 1 megabit por segundo.

1.8 MODELO OSI

Lo desarrollo la Organización Internacional de Normas (ISO), como un primer paso hacia la normalización internacional de varios protocolos. A éste modelo se le conoce como modelo de referencia OSI (Interconexion de Sistemas Abiertos), porque precisamente se refiere a la conexión de sistemas heterogéneos, es decir, a sistemas dispuestos a establecer comunicación con otros distintos.

El objetivo principal al crear el modelo OSI es lograr una apertura o compatibilidad en todos los sistemas tanto en hardware como en software, esto ha sido un poco difícil debido a que cuando apareció el modelo OSI muchas empresas como Xerox, IBM, Macintosh, o el Departamento de Defensa de los EU que creo TCP/IP , ya habían creado sus propios protocolos de comunicación para hacer funcionar los diferentes equipos que tenían de diferentes proveedores o vendedores y los habían hecho funcionar en red, por lo tanto el modelo OSI quedo en un segundo plano. En la actualidad protocolos como TCP/IP IP, SPX se están expandiendo en el mercado en un alto porcentaje y hacen que los fabricantes se adapten a sus protocolos de comunicación y que se vuelvan de cierta forma estándares aunque no en un cien por ciento.

Sin embargo el modelo OSI sigue siendo un estándar ideal que sirve para comparar los niveles de interconectividad e interoperatividad en las redes que pueden tener los diferentes fabricantes de hardware y de software y establecer un nivel de compatibilidad en los equipos y aplicaciones.

El modelo OSI tiene siete capas:

- **CAPA FÍSICA**

La capa física se ocupa de la transmisión de bits a lo largo de un canal de comunicación. Su diseño debe asegurar que cuando un extremo envía un bit con valor 1, éste reciba exactamente lo mismo en el otro extremo y no como un bit de valor 0. Preguntas comunes aquí son: cuántos voltios deberán utilizarse para representar un bit de valor 1 o 0; cuántos microsegundos deberá durar un bit; la posibilidad de realizar transmisiones bidireccionales en forma simultánea, la forma de establecer la conexión inicial , y cómo interrumpirla cuando ambos extremos terminan su comunicación; o bien cuántas puntas terminales tiene el conector de la red y cuál es el uso de cada una de ellas.

- **CAPA DE ENLACE**

La tarea primordial de la capa de enlace consiste en partir de un medio de transmisión común, transformarlo en una línea sin errores de transmisión para la capa de red. Esta tarea la realiza al hacer

que el emisor divida la entrada de datos en tramas de datos (típicamente construida por octetos), y las transmita en forma secuencial y procese las devueltas por el receptor, la capa de enlace es la encargada de crear o reconocer los límites de la trama, esto lo hace mediante la inclusión de un bit especial de inicio y otro al termino de la trama.

La trama puede destruirse por completo debido a una ráfaga de ruido en la línea, en cuyo caso se deberá retransmitir la trama, corresponde a esta capa resolver problemas causados por daño, pérdida o duplicidad de tramas.

Otro problema que aparece en la capa de enlace es el referente a como evitar que un transmisor muy rápido sature con datos a un receptor lento, para esto emplea un mecanismo de regulación de tráfico que permita que el transmisor conozca el espacio de memoria que en ese momento tiene el receptor.

- **CAPA DE RED**

Se ocupa del control de la operación de la subred. Un punto de suma importancia en su diseño, es la determinación sobre cómo encaminar los paquetes del origen al destino. Si en un momento dado hay demasiados paquetes presentes en la subred, ellos mismos se obstruirían mutuamente y darían lugar a un cuello de botella. El control de tal congestión dependerá también de la capa de red, también la capa de red deberá saber, por lo menos, cuantos paquetes, caracteres, o bits se enviaron a cada cliente con objeto de producir información para facturación.

También surge en esta capa otro problema, cuando un paquete tenga que desplazarse de un red a otra para llegar a su destino. El direccionamiento en la otra red puede ser distinto al empleado en la primera, los protocolos podrían ser diferentes, etc. La responsabilidad, para resolver problemas de interconexión de redes heterogéneas es la capa de red.

- **CAPA DE TRANSPORTE.**

La función principal de la capa de transporte consiste en aceptar los datos de la capa de sesión, dividirlos, siempre que sea necesario, en unidades mas pequeñas pasarlos a la capa de red y asegurar que todos ellos lleguen correctamente al otro extremo. Bajo condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte solicitada por la capa de sesión. La capa de transporte es una capa del tipo origen-destino o extremo a extremo.

- **CAPA DE SESIÓN**

La capa de sesión permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo un transporte de datos ordinario. Una sesión podría permitir al usuario accesar a un sistema de tiempo compartido a distancia o transferir un archivo entre dos máquinas.

Uno de los servicios de la capa de sesión consiste en gestionar el control del dialogo. Las sesiones permiten que el tráfico vaya en ambas direcciones al mismo tiempo, o bien, en una sola dirección en un instante dado.

La administración del testigo es otro de los servicios relacionados con la capa de sesión. Para el caso de algunos protocolos resulta esencial que ambos lados no traten de realizar la misma operación en el mismo instante, para solucionar esto, la capa de sesión proporciona testigos que pueden ser intercambiados. Solamente el extremo con el testigo puede realizar la operación critica.

Otro de los servicios de la capa de sesión es la sincronización, lo cual consiste en proporcionar una forma para insertar puntos de verificación en el flujo de datos con objeto de que si se llegara a interrumpir la transmisión de datos por una caída de sistema, solamente se tengan que repetir los datos que se encuentran después del último punto de verificación.

- **CAPA DE PRESENTACIÓN**

En particular y, a diferencia de las capas inferiores, que únicamente están interesadas en el movimiento fiable de bits de un lugar a otro, la capa de presentación se ocupa de los aspectos de sintaxis y semántica de la información que se transmite.

La mayor parte de los programas de usuario intercambian información como lo es nombres de personas, datos, cantidades de dinero y facturas. Estos artículos están representados por caracteres, números enteros, números de punto flotante, así como por estructuras de datos constituidas por varios elementos más sencillos. Los ordenadores pueden tener diferentes códigos para representar dichos caracteres (por ejemplo ASCII y EBCDIC), enteros, por ejemplo complemento a uno o complemento a dos, etc. para que exista comunicación entre diferentes ordenadores con diferentes representaciones, la estructura de los datos que se va a intercambiar puede definirse en forma abstracta, junto con una norma de codificación que se utilice "en el cable". El trabajo de manejar estas

estructuras de datos abstractas y la conversión de la representación utilizada en el interior del ordenador a la representación normal de la red, se lleva a cabo a través de la capa de presentación.

La capa de presentación esta relacionada con otros aspectos como son, la presentación de datos y la criptografía, la cual se utiliza por razones de privacidad y autentificación .

- **CAPA DE APLICACIÓN.**

La capa de aplicación contiene una variedad de protocolos que se necesitan frecuentemente. Por ejemplo hay centenares de tipos de terminales incompatibles en el mundo, estos se resuelven definiendo una terminal virtual de red abstracta con el que los editores y otros programas pueden trabajar, esto funciona de la siguiente forma, cuando un editor mueve el cursor de la terminal virtual al extremo superior izquierdo de la pantalla, dicho software (terminal virtual de la red) deberá emitir la secuencia de comandos apropiados para que la terminal real ubique también su cursor en el sitio indicado. El software completo de la terminal virtual se encuentra en la placa de aplicación.

Otras funciones son la transferencia de archivos, el correo electrónico, la entrada de trabajo remota, el servicio de directorio y otros servicios de propósito general específico.

1.9 CARACTERISTICAS DE LOS SISTEMAS OPERATIVOS DE REDES.

Una de las partes más importantes de una red es su sistema operativo, para tener un enfoque global de este es necesario analizar algunas características o puntos importantes que nos describirán en forma general su funcionamiento. Entre las más importantes están:

PUNTO A PUNTO. Un sistema operativo que es punto a punto implica que los usuarios pueden compartir información de su disco duro o impresoras con otros usuarios y dichos usuarios también pueden compartir de igual forma su información o recursos de la red, ,esto quiere decir que un usuario puede pedir y dar servicios a otros usuarios, ejemplo de este tipo de sistema operativo es Windows para Trabajo en Grupo.

CLIENTE/SERVIDOR. Esta forma de operar de los sistemas operativos consiste en que en un servidor esta almacenada toda la información como lo es software de aplicaciones, bases de datos entre otros, y todos los usuarios accesan a dicho servidor para pedir servicios ya sea de una aplicación o de

impresión, es decir el que pide el servicio se le llama cliente y el que da el servicio se le llama servidor, ejemplo de este tipo de sistema operativo es Netware 4.10

PROCESO CENTRALIZADO. Para entender lo que es el proceso centralizado mencionaremos como trabajan las minicomputadoras y los grandes sistemas como Mainframes, dichos sistemas se basan en una computadora muy potente a la cual están conectadas terminales tontas llamadas así por que no son ellas las que realizan el proceso de la información sino que piden el servicio y la minicomputadora o mainframe realiza el proceso, las peticiones o resultados de dicho proceso de información es lo único que se muestra en la terminal tonta.

PROCESO DISTRIBUIDO. En una red donde la información se procesa en forma distribuida , un cliente pide un servicio al servidor, éste le envía a su terminal los archivos necesarios o la información que se requiere para que el cliente procese la información en su terminal y la guarde ya sea en la red o en donde él desee a ésta terminal se le llama inteligente debido a que es ella la que realiza el proceso .

Lo anterior no implica que los sistemas grandes de proceso centralizado sean mas lentos o tiendan a volverse obsoletos, por el contrario se pueden conectar a la red que maneja el proceso distribuido como si fuera otro recurso de la misma red y así ampliarse los recursos que pueda tener una empresa ya que la red soporta la conexión con otros sistemas operativos diferentes obteniendo así lo que se llama interoperatividad con otros sistemas.

TOLERANCIA A FALLAS. En el mundo de los sistemas operativos es muy importante que éstos tengan soporte a fallas, es decir si llega a fallar el hardware, el sistema operativo debe ser capaz de permitir el cambio de dicho hardware sin que el sistema se vea afectado o interrumpido en su operatividad, esto antes se hacia espejeando los discos en la actualidad es más común usar arreglo de discos en los cuales existen varios niveles de seguridad, los sistemas operativos deben de ser capaces de manejar dichos sistemas de seguridad desde el mas simple que es duplicar un disco en otro, hasta poder hacer el cambio de disco dañado por otro en buen estado sin perder información y estando en operación la red, lo que se llama Hot Swap.

UTILERIAS DE DIAGNOSTICO. Algunos de los sistemas operativos de red más importantes ofrecen utilerias para que el supervisor pueda encontrar problemas y repararlos así como también para configurar la red; y ésta este en su óptima operación. Estas utilerias pueden ser reportes de paquetes

II. CONTROL DE DISPOSITIVOS.

2.1 INTRODUCCIÓN.

Para entender como funciona la administración de redes, es necesario explicar como cada dispositivo dentro de la red (que esta formado por hardware y software como una sola entidad), logra la comunicación con otros dispositivos y así, estos se puedan manipular a la conveniencia del administrador de la red. Esto se va hacer explicando cada uno de los elementos que hacen posible lo anterior, empezaremos por los protocolos de comunicación que se utilizan, los agentes y el software administrador, se explicara como funcionan, todo esto con el propósito de entender como y con que elementos se logra una comunicación entre dispositivos para así lograr administrarlos en forma centralizada en las estaciones de control .

Iniciaremos con los protocolos de administración y la necesidad de que estos fueran desarrollados.

En los Años 70´s tuvieron un gran crecimiento las computadoras, se conectaban entre si formando redes y éstas conectándose con otras redes que se fueron interconectando. Estas grandes redes fueron llamadas Internet y su tamaño creció en forma exponencial, llegaron a ser muy difíciles de administrar, monitorearlas y darles mantenimiento, y fue evidente que se necesitaba a la brevedad posible desarrollar un protocolo el cual permitiera la administración de estas redes.

2.2 PROTOCOLO DE ADMINISTRACIÓN DE RED.

Una red de redes necesita software que permita a los administradores depurar problemas, controlar rutas y localizar computadoras que violen los estándares de los protocolos. Nos referimos a estas actividades como administración de red de redes. La red de redes consiste en varias redes físicas interconectadas por ruteadores IP. Como resultado,la administración de red de redes debe de considerar lo siguiente: en primer lugar controlar ruteadores heterogéneos, en segundo lugar, el control completo no puede compartirse en un protocolo de nivel de enlace común, en tercer lugar, el conjunto de máquinas que controla un administrador puede localizarse en puntos arbitrarios en una red de redes. Como consecuencia, el protocolo de administración de red de redes utilizado con el TCP/IP opera sobre el nivel de transporte.

En una red de redes TCP/IP, los ruteadores IP forman los conmutadores activos que los administradores necesitan para las funciones de revision y control. Dado que los ruteadores conectan redes heterogéneas, los protocolos para administración de red de redes operan en el nivel de aplicación y se comunican mediante los protocolos de nivel de transporte del TCP/IP.

Diseñar el software de administración de red de redes para que opere en el nivel de aplicación tiene varias ventajas. Dado que los protocolos pueden diseñarse sin observar el hardware de red subyacente, un conjunto de protocolos puede utlizarse para todas las redes. Como los protocolos se pueden diseñar sin considerar el hardware en la maquina de administración, los mismos protocolos pueden utilizarse para todos los dispositivos de administración. Desde el punto de vista de un administrador, tener un solo conjunto de protocolos de administración significa contar con cierta uniformidad, todos los ruteadores responden exactamente al mismo conjunto de comandos. Además, dado que el software de administración utiliza el IP para comunicarse, un administrador puede controlar los ruteadores a lo largo de una red de redes TCP/IP completa, sin tener conexiones directas con todas las redes físicas o ruteadores.

Por supuesto, el construir el software de administración en el nivel de aplicación también tiene desventajas. A menos que el sistema operativo, el software IP y el software de protocolo de transporte trabajen de manera correcta, el administrador será capaz de contactar a un ruteador. Por ejemplo, si las tablas de ruteo de un ruteador se dañan, puede ser imposible corregir la tabla o arrancar la maquina desde una localidad remota. Si el sistema operativo en un ruteador queda fuera de funcionamiento, será imposible accesar el programa de aplicación que implante los protocolos de administración de red de redes, aún cuando el ruteador pueda devolver interrupciones de hardware y paquetes de ruteo.

2.2.1 MODELO ARQUITECTONICO.

Aún con las desventajas potenciales, tener el software de administración de red operando en el nivel de aplicación ha funcionado bien en la practica. La ventaja más significativa de colocar los protocolos de administración de red en un nivel elevado se pone de manifiesto cuando se considera una red de redes extensa, en la cual la computadora del administrador no necesita conectarse directamente hacia todas las redes físicas que contienen entidades administradas.

El software de administración de red de redes utiliza un mecanismo de autenticación para asegurarse de que solo los administradores autorizados puedan accesar o controlar un ruteador en

particular. Algunos protocolos de administración soportan varios niveles de autorizacion, lo que permite privilegios específicos de administración en cada ruteador. Por ejemplo, un ruteador específico podra configurarse para permitir que varios administradores obtengan información de èl, mientras que solo se permitirá que un subconjunto seleccionado de estos mismos cambie la información o pueda controlarlo.

2.2.2 ARQUITECTURA DE PROTOCOLO

Los protocolos de administración de red[1] TCP/IP dividen el problema de la administración en dos partes y especifican estándares separados para cada parte. La primera parte se relaciona con la comunicacion de información, un protocolo especifica como se comunica el software administrador con los agentes, este protocolo define el formato y el significado de los mensajes que intercambian los agentes administradores así como la forma de nombres y direcciones. La segunda parte se relaciona con los datos que se estan administrando, un protocolo especifica que aspectos de los datos debe conservar un ruteador así como el nombre de cada aspecto de tales datos y la sintaxis utilizada para expresar el nombre.

2.3 TIPOS DE PROTOCOLOS DISPONIBLES.

Existen muchos protocolos disponibles, sin embargo los dos protocolos mas importantes son SNMP (The Simple Network Management Protocol) y CMIP (The Common Management Information Protocol). Generalmente SNMP trabaja bajo TCP/IP (Transport Control Protocol / Internet Protocol) y CMIP trabaja bajo OSI (Open System Interconection).

El primer protocolo usado fue Simple Network Management, este fué considerado rápidamente como la solución "Band-aid" para resolver los problemas entre las redes en lo que otros protocolos mas completos y mejores eran desarrollados.

SNMP es un protocolo de Internet. Los protocolos de Internet son creados por la comunidad de Internet, la cual esta formada por un grupo de individuos y organizaciones que desarrollaron y regularon el uso de diversas redes internacionales que fueron llamadas Internet. Internet derivo de

[1] Técnicamente hay una distinción entre los protocolos de administración de red de redes y los protocolos de administración de red. Históricamente, sin embargo, los protocolos de administración de red de redes TCP/IP se conocen como protocolos de *administración de red*; aquí seguiremos el manejo de esta terminología.

ARPANET (Avanced Research Proyects Agency Network) el cual fué creado por el intercambio de paquetes entre investigadores a principios de los 70´s.

En los 80s surgieron 2 diferentes protocolos de Administración de red, el primero fué SNMPv2 el cual incorporó muchas características del original SNMP (el cual todavía se usa) y también adiciono características de direccionamiento de los protocolos originales. El segundo fué Common Management Information Protocol el cual fue mejor diseñado y su contenido tenía mas características que ambos SNMP v y SNMPv2.

El criterio que se usa para elegir entre estos protocolos coincide en su mayoría en que los usuarios necesitan un excelente sistema de seguridad en la red, un fácil uso de la interface y una relativa implementación barata, además de la reducción de las caídas del sistema.

2.3.1 SNMP.

SNMP fue desarrollado a mitad de los 80s como respuesta a los problemas de comunicación que existían en los diferentes tipos de red, inicialmente fue tomado como una solución "Band-aid" hasta que un mejor administrador de redes estuviera disponible. Sin embargo, el mejor no llego a estar disponible y SNMP llego a ser el protocolo de administración de la red elegido.

Su forma de trabajo es muy simple, consiste en intercambiar información a través de mensajes técnicamente conocidos como PDUs (Protocol Data Units). Desde una perspectiva de alto nivel el mensaje PDU puede mirarse como un objeto que contiene variables y estas a su vez contiene titulos y valores.

Existen varios tipos de PDU´s que SNMP emplea para monitorear la red , algunos leen los datos de la terminal , otros ponen los datos en la terminal y uno, el trap que es usado para monitorear eventos de la red tales como que una terminal este apagada o encendida. Sin embargo si un usuario quiere ver si una terminal esta atachada a la red, el podría usar SNMP para enviar un PDU de lectura a la terminal, si la terminal estaba atachada a la red el usuario recibirla el PDU de regreso y el valor seria igual a "yes the terminal is attached". Si la terminal fue dada de baja el usuario debió recibir un paquete enviado por la terminal informándole que se iba a apagar, en este caso un PDU trap debió haber llegado.

En forma global este es el funcionamiento de SNMP, pero es necesario adentrarnos un poco para comprender mejor su modo de operar .

SNMP es un protocolo estándar, el cual tiene la capacidad de administrad cualquier dispositivo de una red. Esto lo hace poniendo ciertos valores en cada dispositivo con lo cual, los puede monitorear y controlar en diferentes eventos y lugares.

SNMP es un protocolo designado para fácilitar el intercambio de información entre dispositivos de la red. Se usa SNMP para transportar datos (tales como paquetes enviados por segundo y errores en la red, entre otros.), para que los administradores de la red puedan mas fácilmente manejar el *desempeño* de la red.

2.3.1.1 VENTAJAS DE SNMP.

- La ventaja grande de implementar SNMP es que es de uso simple, desde su fácil implementación en la red, su corto tiempo de instalación y sobre todo que se pueden programar sus variables para cubrir ciertas necesidades especificas de la red para ser monitoreadas.

En forma general, cada variable consiste en la siguiente información:

- Titulo de la Variable
- Tipo de la Variable (Integer, String ...)
- Si la variable es de solo lectura ó lectura y escritura
- El valor de la variable.

El resultado de ésto se simplifica en una administración de red que es fácil de implementar y no complicada para una red existente.

Existen dos versiones de SNMP. version 1 y la version 2, muchos de los cambios introducidos en la version 2 incrementaron las capacidades de seguridad en SNMP, otros la interoperatividad.

- Otra ventaja de SNMP es que en la actualidad es el protocolo de administración más usado en el mercado. Esta popularidad llego debido a que no hubo otro administrador de red que remplazara la implementación de SNMP "Band-aid".

Hoy en día SNMP es el protocolo más popular para manejar diversas redes comerciales, redes de Universidades y de organizaciones de investigación. SNMP se estandariza en sus nuevas versiones con los vendedores más importantes del mercado, es un protocolo con la característica de ser lo sufucientemente poderoso para manejar los problemas que presenta el tratar de administrar redes heterogéneas

El resultado de esto es que todos los vendedores más importantes de hardware como son: puentes, ruteadores, concentradores entre otros, soportan SNMP contribuyendo asi a su fácil implementación.

- Expandibilidad es otro beneficio de SNMP; esto implica que es fácil actualizar el protocolo y en base a esto se puede expandir para cubrir las necesidades de los usuarios en un futuro.

2.3.1.2 DESVENTAJAS DE SNMP.

- SNMP no es el protocolo perfecto ya que tiene algunas fallas y deficiencias. La primera deficiencia esta en la seguridad, lo cual permite el acceso a intrusos en la red, un intruso puede hasta dar un shutdown a una PC.

La solución a este problema es simple, por la expandibilidad de SNMP, la ultima versión llamada SNMPv2C ha adicionado algunos mecanismos de seguridad como son los siguientes: Privacidad de datos para prevenir que los intrusos puedan accesar a la información de la red, la autentificación para prevenir que los intrusos puedan enviar falsos datos a través de la red, y el control de acceso el cual restringe el acceso a ciertas variables y a ciertos usuarios, eliminando así la posibilidad de que cierto usuario accidentalmente tire la red.

- Uno de los más grandes problemas de SNMP fué que era considerado tan simple que no había la suficiente información acerca de él; o no estaba muy bien organizada o detallada con respecto a la información generada alrededor de las redes en los 90s. Esto se debio principalmente a su rápida creación.

Este problema ha sido resuelto desde la versión de SNMPv2. Esta nueva versión contiene mas información específica de las variables incluyendo el uso de la estructura de la tabla de datos para una fácil recuperación de los mismos, incluye dos nuevos PDU´s que son usados para variables más especificas, también incluye otros dos PDU´s que manipulan la tabla de objetos, en si, muchas

características que han sido adicionadas a SNMP que ha ampliado la información de 36 páginas que antes tenia a 416 páginas con SNMPv2.

2.3.2 CMIP.

El protocolo CMIP fué creado para reemplazar a SNMP en los 80s. Fundado por el Gobierno de los Estados Unidos y grandes corporaciones, mucha gente penso que realmente iba a reemplazar a SNMP ya que era uno de los proyectos con presupuesto ilimitado. Desafortunadamente, los problemas con su implementación fueron retrasando su disponibilidad y ahora solo esta disponible en formas limitadas por sus propios desarrolladores.

CMIP fué creado sobre SNMP eliminando los defectos que éste tuviera y llegando a ser el más grande, detallado, documentado y completo protocolo administrador de red. Básicamente fué creado en forma similar SNMP con PDU´s que son empleados como variables para monitorear a la red. CMIP sin embargo contiene 11 tipos de PDU´s comparado con SNMP que contiene 5.

En CMIP son más complejas y sofisticadas la estructuras de datos, con muchos atributos, estos incluyen:

- *Atributo de la Variable.* El cual representa las características de la variables, como por ejemplo el tipo de dato, si es de lectura o de escritura.
- *Comportamiento de la variable.* Indica que acciones puede activar la variable.
- *Notificaciones.* La variable genera un reporte de eventos, cuando cierto evento específico ocurre como por ejemplo, el shutdown de una terminal podría causar que la variable notifique el evento.

En comparación, SNMP solo emplea él atributo de la variable y las notificaciones.

2.3.2.1 VENTAJAS DE CMIP.

- La característica más grande de CMIP es que sus variables no solo define la información de una terminal y hacia una terminal (como lo hace SNMP), sino que realiza trabajos que serian imposibles realizar bajo SNMP; ejemplo, si una terminal de la red no puede entrar a su servidor predeterminado en un x número de veces, CMIP puede notificar de esto a la persona adecuada, con SNMP el administrador tendría que monitorear la red para ver que terminal ha intentado cierto

número de veces entrar en cierto servidor y ha fallado, CMIP así resulta el sistema más eficiente en la administración de redes con menos trabajo por parte del administrador para actualizar el estatus de su red.

- Otra ventaja de CMIP es que éste contiene las direcciones de las fallas de SNMP. Por ejemplo ha construido un sistema de seguridad de dispositivos, los cuales soportan autorización, control de acceso y un registro de su seguridad (security logs), el resultado es un sistema seguro desde su instalación, no se necesita actualizar el sistema de seguridad.

- La última ventaja fue sostenida no solo por el Gobierno de los Estados Unidos, sino también por grandes corporaciones, las cuales dicen que aunque CMIP se ha desarrollado con gran presupuesto, en cuanto este disponible en el mercado, va a tener usuarios inmediatos como lo es el Gobierno de los Estados Unidos e Instituciones que dependan del Gobierno o se funden en él.

2.3.2.2 DESVENTAJAS DE CMIP.

- Por la información que hemos dado sabemos que CMIP es grandioso, el mejor, pero ¿porqué CMIP no ha sido ya implementado?; después de todo se ha estado desarrollando desde hace 10 años. La respuesta a ésto es que CMIP tiene una gran desventaja. El protocolo CMIP toma más recursos de la red que SNMP por un factor de 10, en otras palabras muy pocas redes en el mundo podrían manejar una instalación completa de CMIP sin masivas modificaciones a su red, tales como instalación de miles de dólares en memoria y compra de nuevos agentes. Esta gran desventaja es muy cara, por esta razón mucha gente cree que CMIP esta destinado a fallar.

- Otro problema con CMIP es que es muy difícil de programar, porque sus variables estan compuestas de muchas y diferentes variables que solo pocos programadores hábiles pueden ser capaces de manejar y usar en su capacidad total.

- CMIP es más completo y mas grande que SNMP, una de las razones por las que CMIP no ha sido comercializado debido al hecho de que corre bajo el protocolo de comunicación de red OSI (Open System Interconection) OSI es similar a TCP/IP en objetivos, ambos son designados como protocolos para comunicación de redes y en estructura ambos usan las 7 capas del modelo ISO. Sin embargo OSI es diferente a TCP/IP en muchos aspectos, para empezar OSI ejecuta casi todas las funciones de comunicación que TCP/IP hace , pero en mayor proporción. Es por esto que se piensa que es mucho mejor y el más completo protocolo de comunicación de redes. Sin embargo

para implementar OSI se necesitan mayores recursos, se había hablado de un factor de 10 para soportar OSI, por lo cual no es el dueño del mercado, ya que no ha llegado a ser popular en la industria de la computación. Se sabe que son contadas las redes en Canadá y EUA que corren con las 7 capas del sistema OSI.

2.4 COMPARACION DE LOS PROTOCOLOS QUE SIRVEN PARA ADMINISTRAR UNA RED.

Es recomendado que se instale SNMP ya que CMIP es un protocolo que requiere demasiados recursos para su implantación.

CMIP es un protocolo bueno para la administración de redes que tiene una respuesta a demasiadas fallas que puede presentar SNMP, el principal problema con CMIP es que es un protocolo de administración tan completo que solo las mejores redes equipadas pueden correr.

En si la información que SNMP y CMIP pueden tener de la red esta definida como un MIB (Management Information Base). MIB es una estructura de árbol, en la parte de arriba del árbol esta la información mas general acerca de la red. Cada rama del árbol contiene información más detallada de una área específica de la red. Se obtiene la información del árbol tan especifica como el MIB lo consiga.

Con base en lo anterior se estudiará un poco más a fondo como se realiza el control de los dispositivos, para lo cual utilizaremos el protocolo estándar de internet que es SNMP.

SNMP utiliza tres elementos para lograr la comunicacion:

- Manager ó Administrador
- Agente.
- MIB.

2.5 MANAGER ó ADMINISTRADOR.

El Manager ó Administrador es instalado en una estación desde la cual se va a monitorear la red, en donde se pueden ver las gráficas, apagar una estación de trabajo etc.

Su principal función implica mostrar eventos que sucedan en la red en base a la información que ha registrado de los agentes, existen diferentes administradores de red, como por ejemplo HP OpenView, NetView 6000.

A estas estaciones NMS (Network Managemente Station) donde se instala el software administrador, algunas veces son llamadas consolas o estaciones de control, estos dispositivos ejecutan aplicaciónes de administración que monitorean y controlan los elementos de la red. Físicamente, NMS´s son usualmente unas supercomputadoras, con un CPU muy rápido, con pantallas de gran resolución , mucha memoria RAM y generalmente un disco duro muy grande. Al menos un NMS´s debe de estar presente en cada ambiente administrado.

El software manager o administrador envia mensajes de petición a los agentes y recibe respuesta de ellos; y espontáneamente recibe mensajes *trap* de los *agentes.*

2.6 AGENTE.

Los agentes son modulos de software que residen en cada dispositivo de la red. Ellos obtienen y almacenan información que sirve para administrar dichos dispositivos como por ejemplo paquetes recibidos por un elemento de la red etc., un agente recibe mensajes de un *Manager o administrador.* Estos mensajes le piden leer o escribir datos a los dispositivos, el agente recibe las peticiones y envia las respuestas de regreso. Un agente no siempre tiene que esperar para enviar información, cuando un problema serio ocurre, o un evento significativo pasa, el agente envia un mensaje de notificación llamado *trap* a uno o más managers o administradores.

2.7 MIB

Un MIB (Management Information Base) es una colección de objetos y sus atributos controlados, es el componente más importante en la administración de una red, tanto en el modelo OSI como en la implementación de Internet. El MIB contiene objetos los cuales tienen un nombre, sus posibles comportamientos y las operaciones que pueden ejecutar. La información que compone al MIB puede ser considerada como una base de datos que es compartida entre el proceso de administración y agentes que proveen información para el control sobre la administración de los elementos de la red. Típicamente una porción importante del MIB es localizado en la estación de control de la red, donde se administran los procesos. Otras partes del MIB residen en los elementos de la red con los agentes.

Un MIB puede verse como una base de datos la cual esta estructurada y contiene elementos estandarizados. El proceso por el cual el MIB es estandarizado fué originalmente definido en RFC 1065, el cual fue publicado en Agosto de 1988 y ha sido actualizado por nuevas versiones de RFC´s (Request for Comments).

SMI es el estándar que se encarga de definir las variables de un MIB, define que información y que variables de un MIB pueden relacionarse con otras, como son definidas las variables y otra información silimar necesaria para obtener la estandarizacion de un MIB. Para lograr esto RFC utiliza de ISO un lenguaje llamado ASN.1 (Abtracted Syntax Notation One).

2.7.1 MIBs Y OBJETOS IDENTIFICADORES

Un MIB puede ser representado como un árbol abstracto con una raíz sin nombre, los datos individuales hacen los niveles del árbol. Objetos identificadores (ID´s) tienen un nombre único o llamado objeto MIB en el árbol. Los objetos ID´s son organizados jerárquicamente con dígitos y nombres específicos asignados por diferentes organizaciones.

La estructura de un MIB SNMP tiene como base tres ramas principales de objetos ID, los cuales son ISO (International Organization for Standarization), CCITT (Consultative Committe for Internacional Telegraph and Telephone), y la unión de ISO/CCITT.

Mucha de la actividad del MIB ocurre en la rama de ISO definida por el objeto identificador 1.3.6.1 y que esta dedicada a la comunidad de Internet. El actual estándar de Internet MIB, MIB-II es definido en RFC 1213 y contiene 171 objetos. Estos objetos son agrupados por protocolo (incluyendo

TCP, IP, UDP, SNMP y otros); y otras categorías como sistemas e interfaces . El árbol de MIB se hace extenso gracias a ramas de experimentación y ramas privadas. Los vendedores pueden definir su propia rama privada para incluir muestras de sus productos.

2.7.2 EL ÁRBOL DE MIB.

Existe solo un árbol de MIB definido por ISO. Sin embargo parte de este árbol ha sido seccionado para vendedores específicos los cuales tienen sus propias extensiones, usualmente cada vendedor específico es dueño de su MIB el cual contiene sus variables (por ejemplo IBM tiene su propio MIB como también lo tiene SUN, HP y otros.) Los nombres de la variables pueden ser diferentes pero la información que contiene cada MIB de los diferentes vendedores es generalmente la misma.

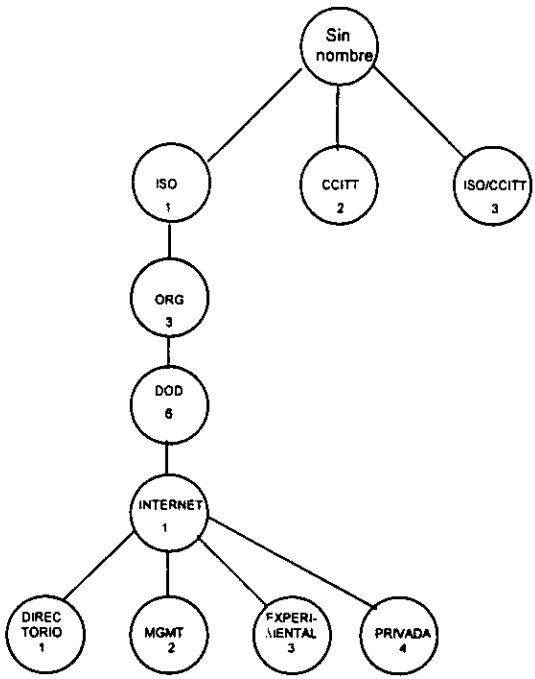


Figura 2.1 Estructura de un MIB.

El nombre de un objeto en la jerarquía es la secuencia de etiquetas numéricas de los nodos a lo largo de la trayectoria desde la raíz hacia el objeto. La secuencia esta escrita con puntos que separan a los componentes individuales. Por ejemplo, el nombre 1.3.6.1.1 denota al nodo con el nombre *directorio*. El MIB ha sido asignado a un nodo bajo el subgrupo INTERNET MGMT con el nombre MIB y el valor numérico 1. Debido a que todas las variables MIB quedan bajo el nodo, todas tienen nombres que comienzan con el prefijo 1.3.6.1.2.1.

Todos los grupos MIB varian dentro de ocho categorías. El significado exacto de las categorías puede explicarse ahora; estos son los ocho subárboles del nodo MIB del espacio de nombres identificador de objetos. La figura 2.1 muestra parte de los subárboles bajo el nodo MIB.

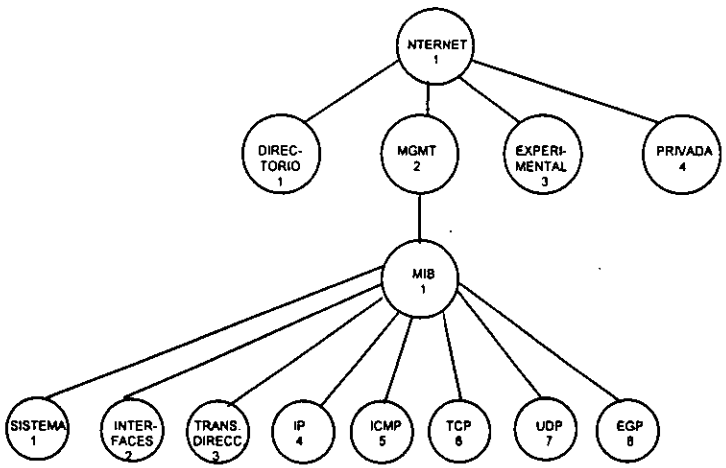


Figura 2 .2 Categorías del MIB.

El MIB para TCP/IP divide la información de la administración en 8 categorías, como se muestra en la tabla 2.1. La selección de categorías es importante, pues los identificadores utilizados para especificar características incluyen un código para cada categoría.

CATEGORIA MIB	INCLUYE INFORMACIÓN SOBRE
SYSTEM	SISTEMA OPERATIVO DEL ANFITRION O DEL RUTEADOR
INTERFACES	INTERFAZ DE RED INDIVIDUAL
ADDR.TRANS.	DIRECCION DE TRADUCCION
IP	SOFTWARE DE PROTOCOLO DE INTERNET
ICMP	SOFTWARE DE PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET.
TCP	SOFTWARE DE PROTOCOLO DE TRANSMISION DE INTERNET
UDP	SOFTWARE DE PROTOCOLO DE DATAGRAMA DE USUARIO
EGP	SOFTWARE DE PROTOCOLO DE COMPUERTA EXTERIOR.

Tabla 2.1

Además del estándar MIB del TCP/IP, que se conoce como MIB-II, muchos RFC documentan variables MIB para dispositivos específicos. Si se examina algunas de las características de datos que incluye el estándar MIB se podrá aclarar su contenido. La tabla 2.3 lista ejemplos de variables MIB con sus categorías

VARIABLE MIB	CATEGORÍA	SIGNIFICADO
SYSUP TIME	SISTEMA	TIEMPO DESDE EL ULTIMO ARRANQUE
IFNUMBER	INTERFAZ	NÚMERO DE INTERFACES DE RED
IFMTU	INTERFAZ	MTU PARA UNA INTERFAZ EN PARTICULAR
IPDEFAULTTTL	IP	VALOR IP UTILIZADO EN EL CAMPO DE TIEMPO LIMITE
IPINRECEIVES	IP	NÚMERO DE DATAGRAMAS RECIBIDOS
IPFORWDATAGRAMS	IP	NÚMERO DE DATAGRAMAS ENVIADOS
IPOUTNOROUTES	IP	NÚMERO DE FALLAS DE RUTEO
IPREASMOKS	IP	NÚMERO DE DATAGRAMAS REENSAMBLADOS
IPFRAGOKS	IP	NÚMERO DE DATAGRAMAS FRAGMENTADOS
IPROUTINGTABLE	IP	TABLA DE RUTEO IP
ICMPINECHOS	ICMP	NÚMERO DE SOLICITUDES DE ECO ICMP RECIBIDAS
TCPRTOMIN	TCP	TIEMPO DE RETRANSMISION MÍNIMO TCP PERMITIDO
TCPMAXCONN	TCP	CONEXIÓN TCP MÁXIMA PERMITIDA
TCPINSEGS	TCP	NÚMERO DE SEGMENTOS QUE TCP HA RECIBIDO
UDPINDATAGRAMS	UDP	NÚMERO DE DATAGRAMAS UDP RECIBIDOS
EGPINMSGS	EGP	NÚMERO DE MENSAJES EGP RECIBIDOS

Tabla 2.2

Finalmente, dos ejemplos aclararan la sintaxis de los nombres. La figura 2.2 muestra que la categoría con la etiqueta IP ha sido asignada al valor numérico 4; así el nombre de todas las variables MIB correspondientes al IP tienen un identificador que comienza con el prefijo 1.3.6.1.2.1.4. Si se quisiera escribir etiquetas textuales en lugar de la representación numérica, el nombre sería:

iso. Org.dod.internet.mgmt.mib.ip

Una variable MIB llamada IPINRECEIVES ha sido asignada al identificador numérico 3 bajo el nodo IP en el espacio de nombres; así su nombre será:

iso. org.dod.internet.mgmt.mib.ip.ipnreceives

y la correspondiente representación numérica es:

1.3.6.1.2.1.4.3.

Cuando los protocolos de administración de red utilizan nombres de variables MIB en los mensajes, cada nombre tiene un sufijo añadido. Para variables simples, el sufijo cero hace referencia a la instancia de las variables con este nombre. Así cuando aparece en un mensaje enviado a un ruteador, la representación numérica de IPINRECEIVES es:

1.3.6.1.2.1.4.3.0

La cual hace referencia a la instancia de IPINRECEIVES en este ruteador. Obsérvese que no hay manera de adivinar el valor numérico o el sufijo asignado a una variable. Se deben consultar los estándares publicados para encontrar que valor numérico ha sido asignado a cada tipo de objeto. Así los programas que proporcionan transformaciones entre las formas textuales y los valores numéricos subyacentes hacen esto consultando tablas de equivalencias, no hay una forma computacional estricta que realice la transformación.

Así la habilidad para entender el proceso de SNMP MIB requiere entender la estructura de un MIB que es realizada por SMI que a su vez requiere un poco de conocimiento del lenguaje de ISO que es ASN.1.

2.7.3 SMI.

Además de estándar MIB, el cual especifica variables de administración de red y sus significados, un estándar separado especifica un conjunto de reglas utilizadas para definir e identificar variables MIB. Las reglas se conocen como especificaciones SMI (Structure of Management Information).

SMI especifica que todos los objetos controlados deben tener un nombre, una sintaxis y un código. El nombre es el ID (Objeto Identificador). La sintaxis define el tipo de datos de los objetos (como por ejemplo "Integer" o "String"), la cual es definida a su vez por ASN.1. El código describe como la información asociada con los objetos administrados es formateada en una serie de datos los cuales puedan ser transmitidos por la red. Existe BERs (Basic Encoding Rules) la cual es una especificación de ISO.

Para mantener los protocolos de administración de red simples, SMI establece restricciones a los tipos de variables permitidas en MIB, especifica las reglas para nombrar tales variables y crea reglas para definir tipos de variables. Por ejemplo, el estándar SMI incluye definiciones de términos como IPADDRESS (Definiéndolo como una cadena de cuatro octetos.) y counter (definida como un entero en el rango de 0 a 2^{32}-1); y especifica que son los términos utilizados para definir variables MIB.

2.7.4 ASN.1

ASN (Abtractect Syntax Notation One). Representa un método específico de objetos abstractos, provee un mecanismo que puede ser usado para definir una variedad de estructuras de datos incluyendo la sintaxis de diferentes protocolos. A través de ASN.1 se definen los tipos de datos, y solo estos tipos de datos definidos se pueden usar bajo SMI.

ASN.1 es un lenguaje formal que tiene dos características principales: Una notación utilizada en documentos que los usuarios pueden leer y una representación codificada compacta de la misma información empleada en los protocolos de comunicación. En ambos casos, la notación formal precisa suprime cualquier posible ambigüedad, tanto de la representación como del significado. Por ejemplo en lugar de decir que una variable contiene un valor entero, un diseñador de protocolos que utilice ASN.1 debe establecer la forma exacta y el rango de los valores numéricos. Esta apreciación es en especial importante cuando las implantaciones incluyen computadoras heterogéneas de las que no todas utilizan la misma representación para los datos.

Además de hacer que los documentos estándar estén libres de ambigüedades, ASN también ayuda a simplificar la implantación de protocolos de administración de red y garantiza su interoperatividad. Define con precisión como codificar los nombres y los datos en un mensaje. Así, una vez que la documentación de un MIB ha sido expresada por medio de ASN.1, la forma que puede ser leída por los usuarios puede traducirse de manera directa y en forma mecánica hacia una forma codificada utilizada en los mensajes. En resumen, los protocolos de administración de red TCP/IP utilizan una notación formal llamada ASN.1 para definir nombres y tipos de variables en el manejo básico de la información. La notación precisa hace que la forma y el contenido de las variables se mantenga libre de ambigüedades.

2.8 OPERACIONES SNMP.

Después de definir las partes de las cuales requiere SNMP para funcionar se presenta las operaciones que hace SNMP para establecer comunicación entre los dispositivos de la red. El protocolo de administración de red SNMP en el cual nos hemos enfocado, especifica la comunicación entre el software manager o administrador y los agentes , define la forma y el significado de los mensajes intercambiados, así como la representación de nombres y valores en estos mensajes, SNMP también define las relaciones administrativas entre los ruteadores que son administrados. Estos proveen la autentificación de administradores.

Se podría esperar que los protocolos de administración de red como lo es SNMP tuvieran un gran número de comandos. Algunos protocolos originales, soportaban comandos que permitían al administrador arrancar el sistema, añadir o borrar rutas, habilitar o inhabilitar una interfaz de red entre otros; pero realmente son pocas las operaciones que realizan y sin embargo con estas logran un control centralizado y total.

SNMP es en si un protocolo por el cual se hacen peticiones o se dan respuestas a NMSs, las cuales pueden enviar múltiples peticiones recibiendo múltiples respuestas, las operaciones de SNMP son seis en la versión SNMPv2:

- ***GET.-*** Permite que NMS recupere un objeto de un agente.

- ***GET NEXT.-*** Permite que un NMS recupere u obtenga el siguiente objeto de una tabla o lista dentro de un agente. En SNMPv1 cuando un NMS quería recuperar todos los elementos de una

tabla de un agente , este inicialmente hacia una operación GET seguida por una serie de operaciones GETNEXT.

- ***GET BULK.-*** Esta operación es introducida en SNMPv2 , la operación GET BULK fué adicionada para hacer mas fácil la adquisición de grandes cantidades de información relacionada, sin inicialmente tener que repetir operaciones GETNEXT. GETBULK fué asignada para eliminar virtualmente la necesidad de operaciones getnext.

- ***SET.-*** Permite a NMS poner valores a los objetos dentro de un agente.

- ***TRAP.*** Usado por el agente para que en forma asíncrona informe al NMS de algún evento.

- ***INFORM.-*** Esta operación es nueva en SNMPv2, la operación inform fue adicionada para permitir que un NMS pueda enviar un trap a otros NMS.

MENSAJE DE SNMPv1

Esta formado de dos partes, la primera contiene la versión y el community name, la segunda parte contiene el actual Protocol Data Unit (PDU) de SNMP, el cual especifica la operación que va a ser ejecutada ("Get" , "Set", etc.), y el objeto involucrado en la operación.

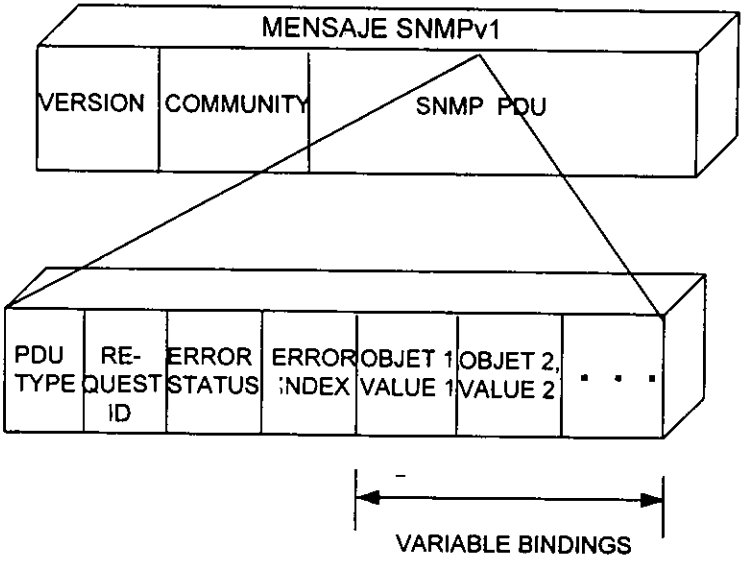


Figura 2.3 Mensaje de SNMPv1

El campo de la versión es usado para asegurarse que todos los elementos de la red están corriendo la misma versión de SNMP. Community name permite el acceso al ambiente para que NMS puedan poner valores. En SNMPv1, los dispositivos no conocen su community name, ya que esta operación no se contemplo.

LOS CAMPOS DE SNMP PDU

- *PDU TYPE.-* Especifica el tipo de PDU que empiezan a ser transmitidos (Protocol Data Unit)
- *REQUEST ID.-* Asocia las peticiones con las respuestas.
- *STATUS ERROR.-* Indica un error y el tipo de error.
- *INDEX ERROR.-* Asocia el error con un objeto en particular.
- *VARIABLE BINDINGS.-* Comprende los datos de SNMP PDU, asocia un objeto en particular con sus actuales valores.

Hemos visto un mensaje de SNMPv1, SNMPv2 también contiene dos partes, la segunda parte de un mensaje de SNMPv2 es virtualmente idéntica a la segunda parte de SNMPv1.
La primera parte de SNMPv2 es la que contiene la gran mayoría de las diferencias entre versiones SNMPv1 y SNMPv2.

MENSAJE SNMPv2

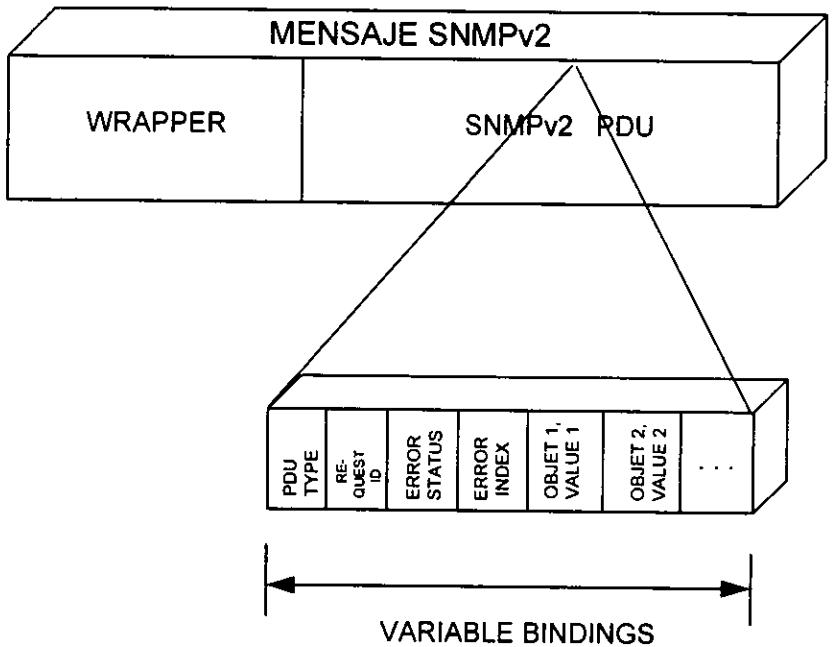


Figura 2.4 Mensaje SNMPv2.

La primera parte de un mensaje es frecuentemente llamada Wrapper. El Wrapper incluye protocolos de autentificación y privacidad en cada *party* destino y fuente. Un party es una entidad lógica de un mensaje SNMPv2 que comprende una identidad, una localización lógica y única dentro de la red, dos protocolos, uno para lograr la autentificación y otro para la privacia. Resaltando que, un party incluye protocolos de autentificación y privacidad , en consecuencia para un party destino y fuente el wrapper incluye un contexto, este contexto especifica los objetos manejados visibles a una operación.

El protocolo de autentificación es el encargado de identificar y checar la integridad del party de un mensaje SNMPv2 . El protocolo de privacidad es el encargado de proteger la información dentro del mensaje SNMPv2, para evitar su divulgación o el acceso a intrusos. Solamente los mensajes autentificados pueden ser protegidos de la divulgación o en otras palabras la autentificación es requerida para la seguridad.

SNMPv2 especifica dos protocolos de seguridad, uno para la autentificación y otro para la privacidad, estos son: Digest Authentication Protocol y Symetric Privacy Protocol.

Digest Authentication Protocol.- Verifica que el mensaje recibido sea el mismo que el enviado. La integridad de los datos es protegida usando un *message digest* en 128-Bit, calculado de acuerdo con el algoritmo Message Digest 5 (MD5).

El *digest* es calculado y enviado dentro del mensaje SNMPv2. El receptor verifica el *digest*. Una clave conocida solo por el emisor y el receptor es puesta de prefijo en el mensaje. Después el *digest* es usado para verificar la integridad del mensaje, la clave es usada para verificar el origen del mensaje.

Para asegurarse de la privacidad del mensaje, el protocolo *Symetric Privacy* usa una llave secreta de encripción conocida solo por el emisor y receptor. Antes de que el mensaje sea autentificado, este protocolo usa el algoritmo Data Encription Standard (DES) para hacer efectiva la privacia. DES es un estándar documentado en NIST (National Institute of Standards and Technology) y ANSI (American National Standards Institute).

Originalmente SNMPv1 especifico que SNMP debería de operar por arriba de Use Data Protocol (UDP) e IP, pero, SNMPv2 define la implantación de SNMP por encima de otros protocolos de transporte, como son OSI, CLNS (Connection Less Network Service), Apple Talk, DDP (Datagram Delivery Protocol), e IPX de Novell (Internet Packet Exchange).

Para finalizar nuestro estudio de SNMP se responde a una pregunta que muchos administradores se hacen hoy en día, ¿Qué necesito para implementar SNMP en mi red?. El primer paso es implementar TCP/IP, esto implica que cada nodo tenga un IP address único. El siguiente paso es tener un administrador SNMP y un Agente. Los agentes deben de ser instalados en cada nodo de la red mientras que los administradores deben ser instalados en las máquinas desde las cuales se va a realizar el monitoreo. Una vez que se han instalado estos elementos lo cual es fácil siguiendo las instrucciones de los manuales, se debe configurar SNMP acorde al tipo de red que se tenga. Existen administradores tales como Netview6000 de IBM y OpenView de HP entre otros.

2.9 MODELO DE ADMINISTRACIÓN DE INTERNET

El modelo de administración de Internet es el mas representativo ejemplo que incluye todos los elementos que hasta ahora se han estudiado y que es una clara aplicación de la teoría antes mencionada para la administración de dispositivos de una red de redes como lo es Internet.

Elementos de la red.- También llamados dispositivos administrados, son por ejemplo computadoras, ruteadores, terminales, servidores, los cuales forman la red.

Agentes.- Los agentes son módulos de software que residen en cada dispositivo de la red.

Manager o administrador. Estos mensajes le piden leer o escribir datos a los dispositivos, el agente recibe
las peticiones y envía las respuestas de regreso.

Objetos Controlados.- Un objeto controlado es una característica de algo que puede ser administrado.

MIB .- Un MIB es una colección de objetos controlados.

Sintax Notation.- Syntax Notation es un lenguaje usado para describir los objetos controlados de los MIBs. Consiste en usar una notación especial la cual permita a diferentes tipo de computadoras compartir información. El sistema de administración de Internet usa ASN.1 el cual define dos cosas, los paquetes de intercambio para el protocolo de administración y los objetos que van a ser administrados.

SMI (Structure of Management Information).- SMI define las reglas para describir la información que va a ser administrada y lo hace usando ASN.1

NMS´s (Network Management Station).- Algunas veces son llamadas consolas, estos dispositivos ejecutan aplicaciónes de administración que monitorean y controlan los elementos de la red.

Protocolo de Administración .- Un protocolo de administración es usado para transmitir información entre agentes y NMS´s, SNMP es el protocolo estándar de administración de Internet.

Party.- Es una entidad lógica de SNMPv2, cada party contiene una identidad, una localización lógica y única en la red y dos protocolos, uno para lograr la autentificación y otro para la privacia.

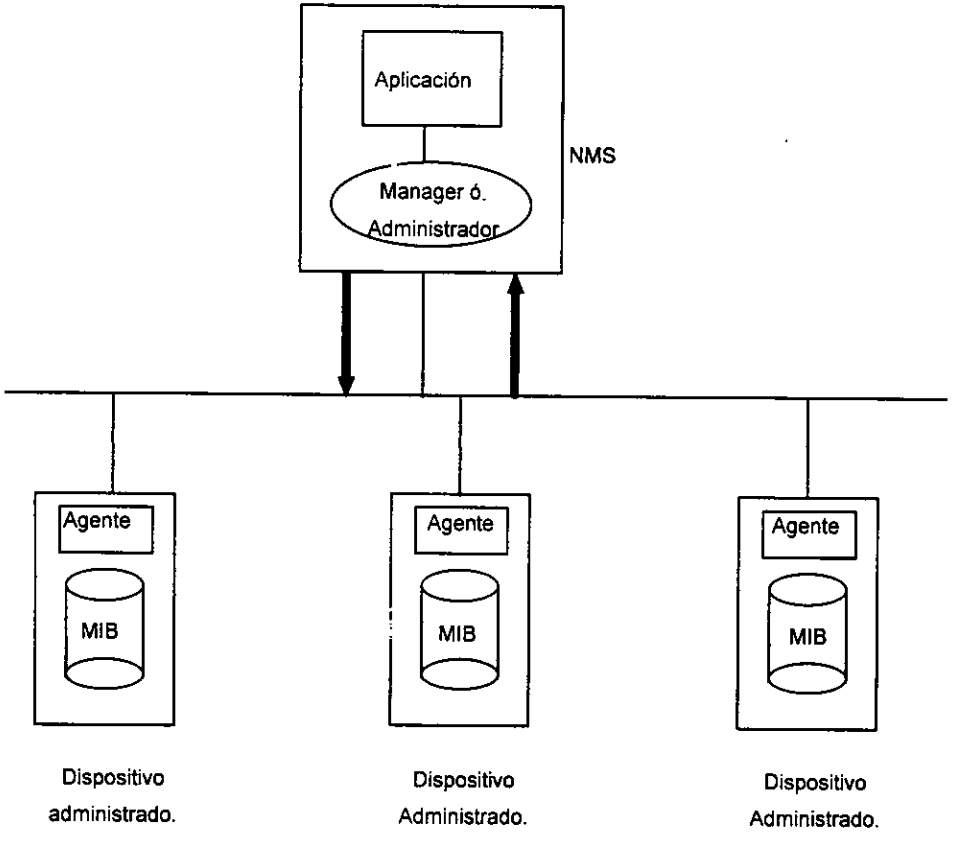


Figura 2.5 Modelo de Administración de Internet.

III. CONFIGURACIÓN.

3.1 INTRODUCCIÓN.

La administración de una red se define como el proceso que controla los datos en la red para maximizar su eficiencia y productividad. El objetivo principal de este trabajo es explicar al lector acerca de la administración centralizada de una red de computadoras, en la practica se administra en una forma desorganizada, sin planeación, conforme se van presentando los problemas se van resolviendo y cuando estos problemas suceden en sitios remotos, por lo general, se tiene que transportar gente de sistemas al lugar donde se presentó la falla teniendo lo anterior como consecuencia más interrupciones en el servicio, o más duración en dichas interrupciones.

Una forma de realizar una administración que nos permita mejorar el desempeño y reducir las fallas en la red es haciendo uso de un sistema administrador de red, el cual nos va a permitir tener el control de todos los dispositivos y aplicaciones en la red en forma centralizada.

Es conveniente aclarar a que nos referimos con centralizada, tener una administración centralizada consiste en tener varias consolas o terminales de control , desde las cuales se va a poder monitorear, cambiar la configuración, en una palabra controlar el dispositivo como si este estuviera enfrente del administrador sin tener que ir al sitio donde esta ubicado. Dependiendo del tamaño de la red se instalaran consolas de control, el que existan varias no indica que se ha descentralizado la administración sino que tienen cada una de ellas el control sobre uno o varios segmentos de la red y tienen centralizada en ellas la administración de dicho segmento o segmentos.

Como se ha mencionado centralizada no implica que exista una sola consola de control, ya que esto seria imposible si estamos hablando de una red grande, significa que en dicha consola se ha centralizado la capacidad de visualizar y cambiar el comportamiento de los dispositivos de la red; es decir administrarlos.

3.2 VENTAJAS QUE PROPORCIONA UN SOFTWARE ADMINISTRADOR DE RED.

En el capitulo anterior vimos como se logra el control de los dispositivos, bajo esas bases trabaja un software administrador de red, el cual es la aplicación necesaria para lograr una administración centralizada.

Existen muchas ventajas que nos proporciona el tener un software administrador de red instalado, mencionaremos algunas de las más importantes para justificar la compra de dicho producto.

- Proceso de alarmas.
- Tamaño de la red y su complejidad.
- Productividad del personal y control de costos.
- Proceso de planeación

3.2.1 PROCESO DE ALARMA.

Cuando se usa un apropiado sistema de administración de red, tomando en cuenta que usamos la palabra "sistema" para representar la combinación de hardware y software trabajando como una sola entidad o unidad, se pueden poner alarmas, las cuales pueden ser de tipo visual o audible, alarmas a las cuales se puede predefinir las condiciones que las generarán. Por ejemplo, el que no exista actividad por un periodo de tiempo predefinido puede indicar que ha ocurrido una ruptura en un cable, y esto permitiría que el administrador revise este problema antes de recibir llamadas de los usuarios finales.

Otra situación de alarma que es muy común, es cuando falla un puente , ruteador, u otro componente de la red; o cuando se pierde la configuración para interconectarse geográficamente con otras redes. Estas alarmas son extremadamente valiosas para los administradores de redes, ya que avisan de situaciones anormales que directa o indirectamente resultan una interrupción del servicio a los usuarios. Otro ejemplo es cuando un disco duro le queda poco espacio libre, se puede predefinir una alarma para que cuando llegue a cierto porcentaje de utilización envíe un mensaje de alarma.

El efecto de las interrupciones puede variar en base al uso de la red, este puede ser desde un pequeño inconveniente y pasar desapercibido hasta ser uno de mayor importancia y tener consecuencias económicas muy significativas, ya que se debe de tener en las grandes redes un desempeño muy alto. Este sistema de alarmas se debe de aplicar a grandes empresas de operación critica como por ejemplo en los bancos, donde perder el acceso a la base de datos o no poder transmitir sus operaciones significa una cuantiosa pérdida de dinero, también en las agencias de viajes donde los proveedores del servicio no pueden dar información de los vuelos debido a una falla en el gateway. Si tales situaciones ocurren frecuentemente o se extienden por periodos largos de tiempo, esto implica pérdidas económicas muy grandes.

3.2.2 EL TAMAÑO DE LA RED Y SU COMPLEJIDAD.

Debido a que surge la necesidad de que se comuniquen las redes a grandes distancias y que dichas redes estén formadas por cientos de dispositivos de diferentes proveedores, se complica la administración, pero es ahí donde un sistema de administración de red cumple uno de sus papeles más importantes que es el control de dispositivos a distancia, sin importar que se trate de una red heterogénea , y que además pueda brindar los servicios y técnicas para implementar cambios en la configuración y en el desempeño en general desde una consola central cuando sea necesario.

Otro aspecto importante es su capacidad para manejar dispositivos que son muy sofisticados dentro de la red, pues dichos dispositivos en la actualidad y así como van evolucionando se incorporan a un estándar para ofrecer un nivel de control y poder competir en el mercado.

3.2.3 PRODUCTIVIDAD DEL PERSONAL Y CONTROL DE COSTOS.

Para hacer más manejable una red, el uso de un sistema de administración de red es el que hace esto posible, ya que administra más dispositivos, medios de transmisión y comunicación con poco personal y de una forma más centralizada, así de esta forma el sistema administrador de red puede ser visto como un dispositivo que tiene la capacidad de monitorear a la red en su desempeño en general. Una función relacionada es la administración de los costos de la red, la cual se debe de evaluar desde un alto desempeño de la red y su alta utilización hasta un nivel bajo de utilización, esto último implicara un gran desembolso de fondos por equipo y servicios que solo son usados parcialmente. La otra forma implica un balance entre el desempeño y la utilización, lo cual minimiza los costos, es decir un alto desempeño y un alto nivel de utilización por parte de los usuarios. Otro de los costos más altos es el generado por los medios de transmisión de una WAN, los cuales ligan geográficamente a varias redes, los diferentes tipos de cableado y estructuras representan costos de instalación, los medios de transmisión de una WAN frecuentemente generan costos que sobrepasan el costo generado por terminales o servidores, así los costos de utilización se deben de examinar en todo lo ancho y largo de la red, en todos sus medios de comunicación, en el equipo y los medios de transmisión, y un sistema de administración de red proporciona estos valores o parámetros para obtener los costos en base al uso de los recursos.

3.2.4 PROCESO DE PLANEACIÓN.

La información que se obtiene del sistema administrador es vital para el proceso de planeación de la red. Si se monitorea la red por un período de tiempo largo, se puede determinar, si la segmentación de la red, o el uso de equipo nuevo va a ser requerido para solucionar los problemas de desempeño, o si los ajustes a la red son autorizados debido al bajo nivel de actividad que se ha presentado. Así de esta manera el sistema de administración de red puede brindar una variedad de herramientas que permite a los administradores desempeñar las funciones de su trabajo en forma más eficiente.

Aunque un sistema de administración de red facilita la configuración muchas organizaciones no tienen uno, en su lugar tienen muchos sistemas, algunos de los cuales controlan módems que obtienen de un vendedor, otros controlar multiplexores o unidades digitales obtenidas de otros vendedores; mientras que otros pueden simplemente ser controlados desde su panel de control. Los vendedores continúan incorporando en sus productos la capacidad de ser administrados en la red en forma estándar, por eso la necesidad de mantener múltiples sistemas de administración va a disminuir paulatinamente, sin embargo muchas organizaciones con una ubicación separada geográficamente y de una gran mezcla de productos obtenidos de diferentes vendedores no tienen una sola plataforma de administración todavía; o están muy lejos de tenerla.

La tabla 3.1 contiene algunas de las principales razones porque se debe de usar un sistema de administración de red.

Determinar el estado de las operaciones de los equipos y los medios de transmisión.
Obtener una notificación ya sea visual o audible de las fallas que ocurren en la red.
Mejorar la administración de redes grandes y complejas.
Se enfrenta a la sofisticación de los dispositivos
Facilita los cambios de configuración.
Hace mas eficiente el uso del personal
Crea un balance en el desempeño y capacidad de la red
Proporciona los parámetros necesarios para obtener los costos de operación.

Tabla 3.1

Una vez que se ha explicado a grandes rasgos los beneficios que implica tener un software administrador de red, se explicará como funciona dentro de las cinco áreas en las que se ha dividido la administración, y como optimiza el funcionamiento de dichas áreas para lograr una administración centralizada

En el desarrollo de los estándares ISO definió cinco áreas funcionales o disciplinas para administrar una red las cuales son indicadas en la tabla 3.2

Administración de la configuración
Administración de fallas
Administración de performance
Administración de la seguridad
Administración de la contabilidad de los recursos

Tabla 3.2

Para lograr una administración centralizada en la red es necesario explicar en que consiste y como se deben manejar cada una de las cinco áreas en las que se dividió la administración de una red.

En este trabajo se les llamará a estas áreas de la administración en una forma equivalente a la designada por ISO y es la siguiente:

1. Configuración
2. Control de fallas
3. Contabilidad de los recursos
4. Seguridad
5. Evaluación operativa.

3.3 CONFIGURACIÓN.

Este proceso consiste en guardar la estructura en la que se encuentran los dispositivos y sus parámetros, además de los medios necesarios para levantar una red.

Para redes complejas que tienen cientos o miles de dispositivos debe existir un sistema de administración de red especializado el cual va a facilitar el control de la red desde algunos puntos. Estos sistemas van a desplegar la representación geográfica de la red, en consecuencia el administrador va a tener la capacidad o habilidad de leer o cambiar los parámetros de un dispositivo, también como desplegar una variedad de líneas que indican ciertos parámetros o comportamiento de la red.

En esta situación se tiene la habilidad para rápidamente desplegar una línea de parámetros y obtener un conocimiento acerca del estado de todos los medios de comunicación con cada dispositivo, también se puede habilitar un procedimiento alternativo de ruteo para ser implementado cuando una interrupción o falla en los medios sea reportada.

Para administrar la configuración de una red se debe de tener una base de datos la cual contenga los parámetros puestos, esta base de datos puede ser usada para determinar alternativas e implementar cambios en la operación de los componentes de la red así como la estructura de la red.

En este capitulo se vera como un software administrador de red ayuda a un desempeño más eficiente en las tares de la configuración.

La configuración consiste en adaptar el hardware con el software para funcionar como un componente mas de la red, algunos ejemplos de configuración son:

- Instalación de un nuevo software.
- Instalación de un software ya manejado.
- Conexión de un dispositivo.
- Cambios en la topología de la red.
- Cambios para disminuir el tráfico de la red.

Para lograr esto se listan algunos de los datos que se necesitan conocer acerca del software y hardware a configurar:

- Parámetros del protocolo.
- Parámetros para la conexión
- Conocer las tablas de ruteo, nombres de servidores, directorios etc.
- Parámetros de filtrado para puente (dirección, protocolos, manufacturas)
- Parámetros para el ruteo (Interfaces, direcciones, velocidad etc.)
- Datos sobre el software (espacio en disco duro necesario, memoria necesaria, número de usuarios, tipo de instalación)

La configuración es la parte fundamental en la administración de una red, de una buena configuración depende el desempeño que tenga una red, esto no implica que una vez configurado el equipo ésta configuración sea permanente sino que el propio funcionamiento dinámico de la red requiere de cierta flexibilidad y rapidez para volver a configurar los dispositivos o redirigirlos hacia otra ruta .

Para lograr una configuración que sea permanente o flexible, cuando así se requiera, es necesaria la planeación, dicha planeación nos va a ayudar a elegir el equipo, los medios de transmisión, la estructura que va a tener la red, la instalación de las aplicaciones y en general de todos y cada uno de los elementos que forman una red, por lo tanto es necesario analizar primero las tareas que abarca una planeación ; para después cubrir las que abarca la configuración aunque debido a la estrecha relación de ambas a veces se mezclan o se intercalan unas con otras para lograr el funcionamiento eficiente de la red.

3.3.1 TAREAS DE LA PLANEACIÓN.

- Colección de datos.
- Análisis de los requerimientos.
- Análisis de las tendencias.
- Modelado de la red.
- Designación del equipo
- Designación del software.
- Optimización.
- Implementación.

- **COLECCION DE DATOS**

Como su nombre lo indica , esta tarea consiste en obtener los datos necesarios, tipo y cantidad de información que se va a manejar , saber de dónde y quiénes son los indicados para dar este tipo de información, saber que tipo de datos se necesitan para la implantación de una red o para su expansión.

- **ANALISIS DE LOS REQUERIMIENTOS**

Cuando por primera vez se va a instalar una red es necesario hacer un estudio a fondo de las necesidades que se deben cubrir por ejemplo:

- Saber la cantidad de información que se va a manejar.
- Ubicación geográfica de los lugares donde se va a manejar la información
- Elección del equipo adecuado.
- Elección del software adecuado
- Tipo de red a instalar (topología, medio de transmisión, estructura).
- Presupuesto disponible.

Una parte que ya se debe de empezar a tomar en cuenta desde la planeación es la posibilidad de instalar un software administrador de red, para lo cual es necesaria una evaluación de lo compleja que va a ser la red, si se van a tener diferentes plataformas, diferente equipo; y revisar cual es el software administrador de red más indicado o en que parte de la red se instalaría, evaluar las ventajas y desventajas de varios productos como pueden ser OpenView de HP, NetView 6000 de IBM .

- **ANALISIS DE LAS TENDENCIAS**

Esta parte de la planeación consiste en analizar cuales son las tendencias en el crecimiento de la información, cuales son las tendencias en la evolución del hardware y software que se desea manejar, cuánto tiempo pasará sin que se necesite actualizar, cuáles son sus tendencias de renovación, etc. Se debe de planear la actualización a corto y largo plazo así como también la capacitación del personal para realizar dicha actualización.

Aquí, algo que debemos remarcar es analizar las tendencias de crecimiento de nuestra red, de la empresa o corporación, si en un principio se tiene planeado la instalación de una red pequeña que se pueda administrar sin un software dedicado a esto; pero no se debe por ningún motivo eliminar la

posibilidad de comprar el equipo que permita ser administrado por un software de administración para que cuando la red necesite crecer y expandirse se pueda instalar dicho software.

- **MODELADO DE LA RED**

Esta parte consiste en crear un modelo de la red que se desea instalar , es como una simulación ya que con la información que se ha obtenido y analizado, se puede crear un modelo que represente lo que se va a implementar, cuando se elabora esta parte se van viendo detalles que no aparecieron en los procedimientos anteriores y sirve para tener una visión más real acerca de lo que se desea implantar.

En este proceso ya se debe de tener definido que tipo de red, estructura y aplicaciones se van a usar.

Se debe de apreciar en qué lugar se va a necesitar de mejor equipo, qué tipo de seguridad en cuanto a respaldo de la información se va a tener, cuál es el procedimiento a seguir en caso de desastre, (es decir de pérdida de información) y cómo se va a restablecer.

A grandes rasgos se debe de tener un esquema del funcionamiento en general que se ha planeado para la implantación de la red.

- **DESIGNACION DEL EQUIPO**

Esta es una parte que se necesita analizar realmente a fondo, existen básicamente dos opciones cuando se trata de una empresa que no cuenta con mucho presupuesto para la instalación de su red de computadoras y cuando se trata de una corporación grande la cual si tiene el presupuesto necesario para la instalación de su red de computadoras.

En el primer caso no hay mucho que hacer ya que debido a que se trata de una organización pequeña se comprara el equipo con el cual se soporte la información que en el presente y a corto plazo se pueda manejar, sin embargo en la actualidad todo el equipo y todos los vendedores están poniendo a la venta equipo que soporta un estándar como SNMP para poder ser administrado, es decir que aunque no se quisiera comprar el equipo con estas características, el mundo del hardware ha evolucionado tanto que todo lo que se vende ya cuenta con estas características, aquí lo que hacen las pequeñas empresas es comprar equipo pequeño y nos referimos a pequeño en cuanto a capacidad de procesamiento y almacenamiento; que quizá se ha sobrepasado por el crecimiento de su

información y tenga que cambiarlo a corto plazo, si esto no pasa y el equipo pequeño no es reemplazado entonces la red pequeña no necesitara de un software sofisticado para ser administrada y el equipo con el que cuenta estará perfecto para sus necesidades.

La segunda opción, en la cual se trata de una corporación muy grande y que tiene el presupuesto necesario para comprar el equipo avanzado, se tiene que tener en cuenta las perspectivas de crecimiento, el equipo debe de sobrar para manejar la información con la que se cuenta en un principio, pero debe de ser capaz de manejar la información que se tenga a largo plazo y se debe de hacer una aproximación real de que tiempo implica el largo plazo.

Si se tiene el presupuesto necesario es recomendable instalar un software administrador de red ya que éste nos va a permitir un control de la red en toda su complejidad y nos va a ayudar a incrementar su productividad y eficiencia.

En las dos opciones explicadas existen casos que son contradictorios pero que suceden, uno es cuando se trata de una red pequeña y que cuenta con un equipo de gran capacidad el cual se le esta dando un uso muy por debajo de su nivel, lo cual implica pérdida ya que se invirtió una gran cantidad en ese equipo y no se le esta utilizando al 100% de su capacidad, el otro caso y el más grave se presenta en las grandes empresas que contando con el presupuesto necesario tienen un equipo que no alcanza a cubrir sus necesidades o que si las cubre no esta automatizado como podría estarlo, es decir existen muchas empresas grandes como lo son bancos, que realizan su actualización de antivirus con personal que se traslada de estación en estación, o que realiza su configuración de equipo desplazándose al sitio remoto o de PC en PC, esto es realmente increíble pudiendo hacerse con un software con la capacidad de hacer dichos cambios desde una estación de control sin interrumpir el trabajo de los usuarios.

Es aquí donde es primordial la capacidad del administrador para poder demostrar la necesidad de la compra de un producto que pueda automatizar hasta donde sea posible el funcionamiento de la red. Esto lo debe de demostrar con una evaluación de los costos que genera tener a personal que se traslade de estación en estación y el costo que implica el comprar un software administrador de la red con el cual se pueda centralizar la administración , y que si en un principio se dispara el costo del software administrador de red, a largo plazo se encontrara que se obtienen mayores rendimientos con el software.

Para concluir esta parte se presenta la lista del equipo en el cual se debe de tener mayor cuidado en su elección:

- Servidores.
- Ruteadores.
- Puentes
- Concentradores
- Tarjetas de red
- Estaciones de trabajo.

Se debe de revisar que dicho equipo soporte los agentes de SNMP para poder controlarlos mediante un software de administración.

Otro aspecto importante en la elección del equipo, es la elección de suministro de energía para la red, este debe de tener gran capacidad y ser ininterrumpida su alimentación, así como contar también con las instalaciones adecuadas en cuanto a espacio y temperatura para que el equipo este en perfecto estado.

- **ANALISIS DEL SOFTWARE**

De igual forma que la elección de equipo se debe de hacer la elección de software, se debe de analizar que tipo de software, versión y capacidad de usuarios soporta, entre los más importantes esta el elegir el sistema operativo de la red sobre el cual van a funcionar todas las aplicaciones. En forma general se debe de evaluar el siguiente software:

- Sistema Operativo de la red.
- Aplicaciones para manejar la información (bases de datos como Oracle, Informix, Sysbase etc.).
- Software para crear respaldos de información (por ejemplo Arcserve de Cheyenne).
- Correo electrónico (CC Mail de Lotus, Microsoft, el del Sistema operativo de la red)
- Tipo de antivirus que se va a usar tanto para la red como para las estaciones de trabajo (McAfee, Norton Antivirus, Dr Solomons).
- Software Administrador de la red (Open View de HP, Net View 6000 de IBM, Cysco y otros).
- Software que se usa ocasionalmente.

Sobre lo anterior se debe de considerar que tipo de configuración se va a establecer, tener cuidado en aspectos como por ejemplo versiones, para cuántos usuarios se va a comprar, que requerimientos de hardware necesita y si son óptimos para su funcionamiento, cada cuándo se tiene que actualizar, qué capacidad de información pueden manejar, entre otros.

- **OPTIMIZACION**

La optimización consiste en ver de que forma la implementación del hardware y el software se puede optimizar, como se puede optimizar el funcionamiento de la red.

Uno de los aspectos más importantes se realiza en la elección del equipo y software, ya que si se realiza una buena elección de ambos, se va a optimizar el funcionamiento, es decir que las versiones del software sean las más actuales junto con el equipo y saber explotar sus características de principio a fin.

Otro aspecto de optimizar la red es planear, reducir al mínimo los tiempos muertos, es decir planear que las actualizaciones de antivirus o nuevas configuraciones se hagan en forma automática y de preferencia en la noche cuando no haya actividad en la red así como también el mantenimiento del equipo, la programación de respaldos para horas en las cuales no haya o sea mínima la actividad de la red.

Un punto importante en la optimización de la red es la capacitación del personal , que el personal conozca perfectamente el equipo y aplicaciones que existen en la red, para que pueda administrar y obtener mayores rendimientos de las características de ambos, tanto de software como de hardware.

- **IMPLANTACION**

La implantación es la realización de todo lo planeado, esto se debe de hacer con una rigurosa programación de tiempos en los cuales se debe cubrir cierto objetivo.

La implantación consiste en llevar a cabo el funcionamiento de todos los dispositivos de una red, es decir instalar el sistema operativo de la red, conectar todas las estaciones de trabajo y configurarlas conforme a lo planeado, establecer configuración en los ruteadores, en los gateways, cascadear correctamente los concentradores y revisar que realmente exista una buena comunicación con las otras redes o segmentos de la misma.

Instalar todo el software predeterminado y configurarlo, revisar el funcionamiento y ver si realmente cumple con lo programado.

Implementar todas las medidas de seguridad tanto para el equipo como para la información como lo es el software para la creación de respaldos, así como también la seguridad para el acceso a los usuarios hacia los recursos.

Y bueno por fin el punto final, empezar a manejar información, que los usuarios tengan acceso a todos los recursos, que exista la comunicación.

Después de la implementación, el proceso de configuración tiene que cumplir con nuevas tareas, para mantener en continuo funcionamiento a la red, pues el proceso de la administración continua ya que solo se ha cumplido una parte de la administración de una red que es la planeación e implantación de la misma.

3.3.2 TAREAS DE CONFIGURACION.

- Monitorear el estado de la red.
- Controlar el ruteo de la red.
- Tener una base de datos de los parámetros del sistema.
- Control y facilidad en la configuración.

- **MONITOREAR EL ESTADO DE LA RED**

Este proceso se utiliza en varias de las áreas de la administración de la red, ya que es indispensable para cada área, en especial en esta área de configuración se debe de monitorear la red para saber de su estado, para en caso de que así se requiera cambiar la configuración de cierto dispositivo, esto en base a lo que se ha observado en el monitoreo.

Cuando se cuenta con un software para administrar una red ésta parte del monitoreo se lleva a cabo en forma automática de todos los dispositivos de la red, éste monitoreo es en forma gráfica, es decir se muestran líneas que representan la comunicación entre dispositivos.

Se puede resumir los aspectos más importantes del monitoreo de la siguiente forma:

- Información instantánea acerca de todos los recursos de la red.
- Muestra los errores que suceden en la red.
- Muestra el tráfico en la red.
- Permite la visualización del desempeño de la red en forma gráfica para su análisis.

- **CONTROL DEL RUTEO EN LA RED.**

Se deben de configurar todos los ruteadores y guardar dicha configuración, saber los parámetros que se necesitan y tenerlos disponibles para que en caso de que se requiera cambiar la configuración o redirigirla a otro lado esto se haga con facilidad.

Con software como Open View de HP o Net View 6000 de IBM este trabajo se realiza con gran facilidad y algo que es muy importante es cuando se tiene que cambiar la configuración de un router que se encuentra en otra ciudad, no va a ser necesario desplazarse al sitio remoto, sino que desde la estación administradora de la red (NMS) y con los parámetros necesarios se puede reconfigurar el router sin problema alguno.

- **TENER UNA BASE DE DATOS DE LOS COMPONENTTES DE L SISTEMA.**

El tener una base de datos con la información de la configuración del sistema y en general de todos los datos más relevantes que en cierto momento servirían para reinstalar la red es algo muy importante y que lamentablemente pocos administradores de redes lo hacen, ya que debido al continuo cambio en la configuración, optan por no hacerla o no actualizarla si es que tienen una base de datos con este tipo de información.

Todas las bases de datos deben incluir :

- **Documentación de los dispositivos de la red.**

- Localización (Ubicación, edificio, salón o cuarto, dirección, organización o empresa, teléfono)
- Propiedades (tipo de manufactura, sistema operativo, características del hardware)
- Personas responsables (nombre, teléfono, área de responsabilidad)
- Interfaces de red (controlador, tarjeta de red, protocolo con nombre y direcciones)

- **Documentación de las líneas de comunicación**

- Posición (dónde empieza, dónde termina, su trayectoria)
- Propiedades (tipo de cable, velocidad a la que se transmite)
- Responsables (nombre, teléfono, área de responsabilidad)

- **Documentación de los cambios.**

- Versiones del software o modelos de hardware, controladores específicos.
- Información adicional u observaciones, tales como fecha y razón por la cual se hizó el cambio o responsable del cambio.

- **Documentación de la topología.**

- Trayectoria de la topología y tipo de cable (coaxial, par trenzado, fibra óptica)
- Planes de cambio de topología o instalación

- **Documentación de errores.**

- Tipo de error
- Fecha que se presento el error y duración.
- Cómo se corrigió
- Estadísticas y tendencias de los errores

- **CONTROL Y FACILIDAD EN LA CONFIGURACION**

Tener el control de la configuración ayudará a elevar el performance en la red, con la ayuda de la base de datos la cual contienen los parámetros del sistema, del ruteador o dispositivo a configurar, se puede establecer el control desde una estación de trabajo (NMS), esto implicará cierta facilidad en el cambio de configuración ya que con todos los parámetros necesarios y teniendo una aplicación como OpenView de HP se hará el cambio rápidamente sin mayor complicación.

Lo anterior se resume en la implantación de ciertas subtareas como son:

- Actualización automática de la configuración
- Reconfiguración de los recursos (por ejemplo en caso de errores)
- Configuración remota
- Soporte a nuevas versiones en hardware y software
- Iniciación y ejecución de trabajos

Cuando se cuenta con una red instalada, el software como OpenView y algunos de sus productos proporcionan herramientas que nos ayudan en la planeación, que en esta ocasión sería de un nuevo segmento de la red o para planear su expansión a otros lugares.

Las herramientas que nos proporcionan nos ayudan a obtener los datos automáticamente de cierta información que se esta manejando, nos permitirá crear un modelo lo más cercano a la realidad y por supuesto nos brindaría datos reales de la utilización del equipo y del software, así como también permitiría evaluar el tráfico que existe en la red y determinar si el tipo de estructura, cableado o medio de transmisión está funcionando correctamente o se debe de cambiar; lo cual nos permitiría elegir nuevo equipo, software o estructura, si no, seguir trabajando en la misma línea ya establecida.

Es muy clara la ventaja de tener un software con el cual nos proporcione datos reales que nos servirán para la planeación de una nueva red, y es igualmente eficiente en tareas de configuración como lo es el monitoreo, la configuración del ruteo, la creación de una base de datos con los parámetros del sistema y la facilidad de control en todo aspecto de configuración, ya que todo lo anterior lo hace mediante herramientas que permite el acceso a dispositivos remotos, permite visualizarlos y configurarlos desde una estación de control, convirtiéndose esto en facilidad de control y menos tiempo en configuración.

La siguiente tabla ilustra esta facilidad de configuración y ejemplifica claramente como diversos dispositivos pueden o no, administrarse desde una estación de control (manager o administrador), los dispositivos que si tienen esta capacidad son los que permiten llevar a cabo una administración centralizada .

	EtherTwist Hub /8	EtherTwist Hub /12	EtherTwist Hub Plus/12	EtherTwist Hub Plus/24 S	EtherTwist Hub Plus/48	ThinLAN Hub Plus	Fiber-Optic Hub Plus	AvancedStack Hub 12	AvancedStack Hub-24	AvancedStack Hub-48	Ether Twist LAN Switch	Bidge LB	Bridge MB	Router LR	Router BR
Device configuration			●	●	●	●	●	♦	♦	♦			●	●	●
Port on/off			●	●	●	●	●	♠	♠	♠				●	●
Intelligent segmentation				●				♠	♠	♠					
Device status			●	●	●	●	●	♦	♦	♦	●		●	●	●
Port status			●	●	●	●	●	♦	♦	♦			●	●	●
LAN activity %			●	●	●	●	●	♦	♦	♦			●	●	●
Remote management			●	●	●	●	●	♦	♦	♦			●	●	●
Password protection			●	●	●	●	●	♠	♠	♠			●	●	●
IP configuration								♠	♠	♠			●	●	●
Link/Ping/IPX test			●	●	●	●	●	♠	♠	♠	●		●	●	●
Backup links								♠	♠	♠					
Firmware download								♠	♠	♠	●		●	●	●
Intruder prevention				●				♠	♠	♠					
Eavesdrop prevention				●				♠	♠	♠					
Authorized manger				●				♠	♠	♠					
Security policy			●	●	●	●	●	♠	♠	♠					
Soft reset			●	●	●	●	●	♦	♦	♦			●	●	●
Factory default reset			●	●	●	●	●	♠	♠	♠			●	●	●
Identify			●	●	●	●	●	♠	♠	♠					
Show end nodes			●	●	●	●	●	●	●	●					
Autodiscovery			●	●	●	●	●	♦	♦	♦	●		●	●	●
Automatic layout			●	●	●	●	●	♠	♠	♠	●		●	●	●
Basic counters			●	●	●	●	●	♠	♠	♠	●		●	●	●
Full counters			●	●	●	●	●	♠	♠	♠			●		
Basic graphs/logging			●	●	●	●	●	♦	♦	♦	●		●	●	●
Full graphs/logging			●	●	●	●	●	♠	♠	♠			●		
Action on events			●	●	●	●	●	♠	♠	♠	●		●	●	●
Traffic management			●	●	●	●	●	♠	♠	♠			●	●	●

♠ Requiere el modulo SNMP en el hub para ser administrado .

♦ Requiere el modulo SNMP para ser administrado o estar encadenado a otro hub que contenga el modulo SNMP.

● Se realiza desde la estación de control (NMS) a cualquier hub en cadena.

IV. CONTROL DE FALLAS

4.1 DEFINICIÓN.

El proceso de control de fallas consiste en la detección del problema, ubicarlo, darle una clasificación y orden para atenderlo, aislarlo y darle seguimiento a su solución, a la condición anormal que lo generó.

Desde que el administrador sabe de la existencia del problema, el primer paso y uno de los más importantes en la administración de una red es detectar cual es la situación anormal que lo generó. Esto se realiza por una variedad de caminos, uno de los cuales puede ser las condiciones que generan diferentes tipos de alarmas al excederse , otro cuando los usuarios llaman a sistemas para reportar un problema. Una vez que el problema ha sido detectado, muchos sistemas operativos tienen procedimientos predefinidos para hacer una comparación entre la situación anormal y su lista de errores (log) y si coincide la situación anormal, le asigna un número de error y da una descripción general de lo que se puede tratar.

Es importante entender que muchos problemas relacionados con las llamadas de los usuarios, son inmediatamente resueltos ya que estos por lo general se resuelven diciéndole al usuario como conectar su equipo o como hacer uso correcto de su aplicación, tales llamadas requieren personal capacitado para que en pocos minutos u horas pueda revisar el hardware o software y también para realizar otras funciones que resuelvan el problema sin acciones futuras y no se resuelva en un tiempo largo.

Otras llamadas o alarmas pueden deberse a un problema que requiera asistencia directa de los proveedores, ya sea por mantenimiento o falla física del dispositivo.

El aislamiento del problema puede hacerse desde un simple cuestionamiento al usuario final, una prueba al equipo o medio de comunicación, hasta una extensa investigación.

Una vez que se ha aislado el problema, este puede deberse a un bajo desempeño en el equipo o dispositivo, así como también a una falla en un circuito del mismo, lo cual como ya habíamos mencionado el mas indicado de solucionar es el proveedor o personal externo, en consecuencia otra parte importante en el control de fallas, es revisar el esfuerzo tanto de gente interna como externa para corregir las fallas.

Para controlar las fallas se requiere de una base de datos en la cual se tenga clasificadas las fallas que se han tenido tiempos atrás, pues esto daría una solución apropiada en un tiempo mas corto. Es muy importante revisar como resuelve la gente externa o proveedores el problema y si realmente le están dando una solución terminal, ya que en ocasiones se cierran los reportes por x causa sin realmente dar una solución, también es importante revisar en que consistió la solución.

Mientras la solución de fallas parece ser el último trabajo en el control de fallas, en la actualidad este proceso requiere de una configuración bien realizada o de un cambio en el desempeño general de la red. Por ejemplo si una situación anormal es resultado de la implementación de un ruteador, la solución del problema depende del cambio de la configuración, esto indica a grandes rasgos la interrelación que existe entre cada una de las áreas de la administración.

4.2 TAREAS DE LA ADMINISTRACIÓN DE FALLAS

Esta área funcional de la administración se puede describir como de una "particular importancia" y de una "particular complejidad". Las tareas de la administración de fallas tienen como objetivo tener disponibles todos los recursos de la red para su uso y lograr con esto un alto desempeño de la misma.

Algunas de las más importantes son:

- Monitoreo del estado de la red
- Recibir y procesar las alarmas generadas
- Diagnosticar las causas de las fallas
- Aislar la falla.
- Solucionar la falla.
- Proveer al usuario final de ayuda técnica (soporte técnico a usuarios).

Una de las preguntas más usuales de usuarios finales es porqué surgen las fallas, problemas, errores o interrupciones en el sistema si ya estaba funcionando correctamente. La respuesta a esto son dos factores muy importantes, uno de ellos es la natural complejidad en la tecnología de las comunicaciones, lo cual complica el manejo de las mismas. El otro factor es el resultado de constantes reconfiguraciones, extensiones de sistemas, pequeñas desconexiones en los componentes de la red (a veces son momentáneas), y la comunicación en la red la cual esta sujeta a muchos cambios dinámicos los cuales en su mayoría no se manejan adecuadamente.

Por lo anterior podemos definir que un error es una desviación de los objetivos o funciones de operación en la red.

Existen muchas formas de llamarle a una interrupción del servicio de red, estas son por lo general falla, error, problema, caída entre otros. En este trabajo se le llamara falla.

4.2.1 MONITOREO DEL ESTADO DE LA RED.

En esta área de la administración como en todas las demás, el monitoreo desempeña un papel muy importante, ya que debido a éste el administrador puede observar o enterarse de que se esta presentando una falla en la red, sin esta herramienta de monitoreo se complica el detectar fallas en la red y se atenderían cuando ya se hubiesen propagado.

Del monitoreo depende mucho el controlar las fallas, pues si se logra detectar la falla antes de que se presente esto ayudaría a su pronta solución, y a evitar que se propague si es que es una falla que tiende a eso.

4.2.2 RECIBIR Y PROCESAR LAS ALARMAS GENERADAS.

Una de las ventajas más claras cuando se obtiene un software como OpenView o Net View 6000 es la facilidad para crear diferentes tipos de alarmas y la flexibilidad para su recepción.

Se puede predefinir cualquier situación que el administrador de red determine para que se genere una alarma, para esto se debe establecer prioridades de funcionamiento en el equipo, es decir que es más importante tener funcionando, un servidor, un ruteador o una estación de trabajo.

Por ejemplo se pondría una alarma si se presentaran las siguiente situaciones:

- No existe conexión con un ruteador, concentrador, puente o servidor (dispositivos de alta prioridad).
- Se esta acabando el espacio en el disco de un servidor.
- No se crearon los respaldos de información.
- No existe comunicación con x estación de trabajo de cierta prioridad (nómina, gerencia, respaldos)

Se pueden establecer tantas alarmas como el administrador lo desee y de acuerdo a las prioridades.

Existen dos formas de recibir las alarmas, una es la gráfica, que consiste en que en una estación de trabajo (NMS) se observe dicha alarma, de que algún dispositivo se desconecto, se desconfiguró o está lleno como es el caso de los discos duros. Este tipo de alarma también envía un mensaje a través de la red a cierta estación de trabajo o a cierta persona encargada según se le programe. La otra forma es la audible, que consiste en que sistemas como OpenView manden un mensaje también a través de la red o a través de un radio localizador (Biper) al administrador o a la persona indicada, este mensaje tiene como objetivo primordial localizar al administrador no importando el lugar donde este se encuentre, ya que en muchas ocasiones no se encuentra en la empresa o la falla puede presentarse en días no laborables o en la noche.

Este tipo de alarma es muy importante ya que no importando el momento en que se presente la falla, la persona encargada recibirá la alarma y dependiendo de la forma en que se haya definido se podrá atender la falla, o en su mejor caso evitarla.

4.2.3 DIAGNOSTICAR LAS CAUSAS DE LAS FALLAS.

Para poder controlar las fallas es muy importante diagnosticar las causas o situaciones que las generaron, para esto es necesario establecer cuales son las fuentes que generan esta fallas y en donde se presentan con más frecuencia.

Entre las causas más generales están :

- Tener un gran número de componentes
- La distribución geográfica de los componentes
- Tener software y hardware heterogéneo
- Responsabilizar a varias personas de los mismos componentes o a ninguna de cierto componente.
- Errores de los operadores (usuarios).

Estas fallas se presentan en los diferentes componentes de una red como son:

- Cableado (coaxial, par trenzado, fibra óptica)

- Componentes de la red (transceivers , repetidores, puentes, ruteadores, servidores y terminales entre otros.)
- Software de la red (aplicaciones y sistemas operativos).

Para realizar el análisis y diagnosticar la causa de la falla se deben analizar todos los aspectos que rodeen la falla, es decir primero que tipo de componente fallo, la alarma puede dar información muy importante y precisar que genero la falla, si el administrador no se entero por una alarma sino que el usuario le llamo, es necesario analizar todo el medio que rodea al dispositivo, es claro que un alto porcentaje de las fallas por lo general se deben al cableado.

La forma de ir despejando el problema se puede hacer de lo general a lo particular o viceversa dependiendo de la falla, pero casi siempre se revisan los siguientes aspectos:

- Área donde se presento la falla
- Componente de la red que presento la falla, hardware, software (aparentemente)
- Revisar el cableado que llega a tal componente
- Revisar el suministro de energía
- Revisar configuración (hardware y software)
- Revisar que el usuario lo este usando adecuadamente
- Revisar si es el único dispositivo el que esta fallando
- Revisar si existe una alarma que se haya generado (la cual daría una causa directa)
- Determinar si son fechas de una alta utilización de la red como son cierres, fin de año, nómina entre otros.
- Hacer diversas pruebas al equipo (hardware),o a la aplicación (software).

Para lograr este análisis se necesitan de herramientas con las cuales se facilita esta tarea de diagnostico, las cuales pueden ser un software administrador de red (para el monitoreo, administración remota, generación de alarmas entre otras), analizador de cableado, un analizador de protocolos, manuales del hardware y software instalado, una base de datos de todos los componentes del sistema, un analizador de voltaje (por ejemplo power watch) entre las más importantes .

4.2.4 AISLAR LA FALLA.

La tarea de aislar la falla es tenerla muy bien definida, saber que la causó y cuál es la solución que se le debe dar, para esto se toma en cuenta el diagnostico que se hizo anteriormente.

Una vez que se identifica la causa y se define la falla se debe aislar dicha falla para que afecte lo menos posible el rendimiento de la red.

El aislamiento de la falla depende mucho de que tipo de falla se presenta , por ejemplo es muy difícil aislar la falla cuando se trata de un ruteador, o de un servidor, ya que de estos depende que muchos otros recursos de la red estén disponibles.

Existen diversas formas de aislar una falla, cuando se puede hacer, va a depender si la falla se presenta en hardware o software.

Cuando se trata de hardware por ejemplo, si un ruteador falla por lo general se debe de contar con una ruta de soporte (a través de otro ruteador) la cual entraría en funcionamiento enseguida que el primero haya fallado, de igual forma si hablamos del disco duro de un servidor, entraría otro de soporte sin interrumpir la operación en la red (si es que se cuenta con un arreglo de discos o algún otro sistema de respaldo) de esta forma se aísla una falla para no interrumpir la operatividad de la red o que sea mínima esta interrupción, mientras que se resuelve la falla, para este ejemplo sería reparar o reconfigurar el ruteador, y en el caso del disco duro reemplazarlo si es necesario.

En caso de que la falla sea en el software también se aplican las situaciones anteriores, ya que si el que falla es el sistema operativo de la red esto será muy difícil de aislarlo para su solución ya que involucra a toda la red, pero si se trata de alguna aplicación que afecta sólo a algún o algunos usuarios esto se puede aislar ya sea asignando al usuario a otro grupo para que pueda trabajar o haciendo uso de otra aplicación equivalente mientras el administrador soluciona la falla de la aplicación o la reconfigura y le da los parámetros adecuados.

4.2.5 SOLUCIONAR LA FALLA

Una vez que se ha aislado la falla el siguiente paso es solucionarla, ya que se ha identificado muy bien la falla toca revisar en que consiste la solución, quién la va a realizar y de que forma.

Cuando la falla se presenta en el hardware, el administrador puede volver a configurarlo cambiarle algún componente o definitivamente enviarlos con el distribuidor y que éste se encargue de su reparación, cuando esto sucede es necesario revisar que realmente se haya reparado y saber en que consistió la reparación ya que dispositivos como un ruteador o un concentrador en la actualidad tienen garantía de por vida, cuando llegan a fallar es común que el distribuidor entregue uno nuevo pero si se trata de un servidor verificar si se reparó correctamente el disco o se reemplazó por otro nuevo, o si la fuente de energía se reparó, o se cambio por una nueva.

Cuando la solución depende de la gente interna de la empresa, es necesario cambiar e instalar correctamente el cableado, cuando se trate de cableado, configurar y conocer todas las características del hardware cuando se trate de reconfiguración o hacer funcionar el hardware conforme a sus características e implementarlo con el software adecuadamente, cuando se trate de hardware.

Cuando se trata de software, el administrador debe de saber cual es el camino a seguir para solucionar la falla, lo cual consiste en su mayoría en reconfiguración de los parámetros de la aplicación, en cambiar la forma de administrar (derechos, restricciones, prioridades entre otros) y la otra opción un poco mas drástica que es la reinstalación del software.

Es importante contar con soporte técnico por parte del proveedor del software, ya que esto idealmente reduce el tiempo de solución.

4.2.6 PROVEER AL USUARIO FINAL DE SOPORTE TÉCNICO.

Una herramienta muy importante en el control de fallas es el soporte técnico a los usuarios finales, ya que un alto porcentaje de las fallas (dependiendo del tipo de empresa) es generado por las llamadas telefónicas de los usuarios que reportan las fallas en su equipo.

En algunas empresas consideradas como grandes contratan a otras empresas para que desarrollen este trabajo, el cual es muy importante ya que de la eficiencia del soporte a usuarios

depende el calificativo que se le da al trabajo desempeñado por toda el área de sistemas (nivel de servicio del departamento de sistemas ante todos los usuarios).

Para tener un soporte técnico a usuarios eficiente es necesario contar con gente capacitada, que conozca perfectamente las aplicaciones y sistema operativo con el que cuenta la red, y que tenga también un alto conocimiento del equipo y en general de toda la estructura de la red.

Algunas de las características a tomar en cuenta para elegir a una empresa que proporcione el soporte técnico a usuarios finales son:

- Empresa con alta experiencia en el área de consultoria.
- Que maneje las aplicaciones y sistemas operativos de red con los que se cuenta.
- Nivel de servicio alto.

Como hemos mencionado este servicio puede ser proporcionado por gente interna de la empresa o por gente externa como lo es una empresa dedicada a dar soporte.

En ambos casos la gente que proporcione este servicio debe de contar con los siguientes requisitos:

- Estar capacitada y experimentada en los sistemas operativos de red y aplicaciones que existan en la empresa.
- Tener un programa de cursos de actualización y capacitación.
- Conocer el equipo y estructura general de la red.
- Conocer el organigrama de la empresa para ser capaz de tomar decisiones donde se involucren ciertas jerarquías y prioridades.
- Tener un alto nivel de servicio.

Pero, ¿cuándo se debe de contratar a alguien externo y para qué?. Se debe de contratar a una empresa externa cuando se cuenta con una red muy grande y esta empresa externa se puede encargar del soporte a usuarios finales que por lo general reportan fallas "sencillas" en tanto que la gente interna de sistemas se dedica a desarrollar nuevas vías de comunicación o nuevas mejoras que incrementaran el desempeño de la red.

También por ejemplo se puede contratar cuando existe un desastre en la red y se ha perdido la información, ya que este tipo de empresas hace este trabajo con mayor frecuencia que la gente interna de la empresa, o cuando se instala una nueva aplicación o actualización de versiones, ya que ellos cuentan con mayor experiencia en realizar estos trabajos que en una empresa solo se harían una vez al año.

En enero de 1998 la empresa dedicada a la consultoria de nombre Rone SCL cobraba 60 dólares la hora por sus servicios a Banco Santander Mexicano, teniendo en promedio un tiempo de 50 minutos en dar solución a fallas "sencillas "; es necesario aclarar que existen diferentes tarifas y que éstas varían dependiendo del tipo de falla y su severidad.

V. CONTABILIDAD DE LOS RECURSOS

5.1 INTRODUCCION.

El proceso de obtener información correcta en un tiempo correcto, es la base para establecer un desarrollo empresarial eficiente, esto debe de tener un costo y este se obtiene estableciendo cargos por uso de los recursos de la red. Tareas asociadas con la contabilidad o costos de administración se establecen, facturando, haciendo la depreciación y los cargos de amortización. Para asignar costos a los usuarios por hacer uso de la red, existen algoritmos y además la revisión periódica de la facturación para asegurarse de la justa y equitativa asignación de los costos basados en el uso de la red.

El proceso de administrar la contabilidad de los recursos requiere del esfuerzo de un equipo especial en las grandes organizaciones, para pequeñas y medianas organizaciones, este proceso es substancialmente menor especialmente cuando existen otras funciones de administración con mayor prioridad que realizar.

Esta área de la administración consiste en contabilizar el uso de los recursos de la red y asignarles un costo, ya que el que exista comunicación en la red, servicios de servidor o cualquier otro recurso implica un gasto, en pequeñas empresas este trabajo no alcanza mayor relevancia, ya que todos los gastos son asumidos por el área de sistemas y la empresa absorve el gasto como un gasto general sin importar si el departamento de ventas o el de ingenieria uso más dichos recursos.

En cambio en las grandes empresas, corporaciones, instituciones educativas o servicios a tiempo compartido a menudo necesitan hacer un seguimiento del uso de los recursos de la red y facturarlo según el tiempo a los usuarios o áreas.

El administrador puede monitoriear los registros de uso, de forma que se puede determinar con exactitud los recursos que están siendo utilizados y por que usuarios o áreas.

Esta información es de utilidad cuando se necesita determinar si son necesarios equipos y sistemas de almacenamiento adicionales y justificar su compra.

La administración de la contabilidad de los recursos implica una serie de puntos los cuales si se tiene un software como OpenView de HP, se logran mas fácilmente y son:

- Registro del uso de datos.
- Mantenimiento de la contabilidad de las cuentas.
- Asignación de costos a las cuentas.
- Monitoreo de las cuotas.
- Estadísticas del uso de la red.

5.2 REGISTRO DEL USO DE LOS DATOS

Para poder asignar un costo a los servicios que proporciona una red, se debe conocer los siguientes parámetros:

- Número de paquetes transmitidos.
- Duración de la conexión.
- Ancho de banda de la conexión.
- Comunicación realizada por medio de otros sectores (por ejemplo cuando se usan redes públicas).
- Conversión de costos por servicios de gateway u otros.
- Uso de los recursos del servidor.
- Uso del diverso software.

Esta asignación de costos que se realiza usando los parámetros antes mencionados se puede hacer también para diferentes áreas o sectores entre los mas usuales están:

- Contabilizacion de recursos a cada departamento.
- Contabilizacion de recursos a cada estación de trabajo.
- Contabilizar los recursos por proyecto.
- Contabilizacion de recursos a usuarios en ciertos puntos fijos y tiempos determinados (mensualmente).
- Contabilizacion dinámica a usuarios (por ejemplo cuando han sobrepasado el limite de uso y por lo tanto de costos permitidos).

Algunos de los ejemplos mas claros de este tipo de tarea son el uso de Internet, ya que este servicio se le asigna un costo por su uso, otro ejemplo podría ser el uso del espacio en disco en cierto servidor. Todos los recursos se pueden contabilizar para distribuir su costo de instalación y mantenimiento en forma proporcional al uso que se haga de estos.

5.3 MANTENIMIENTO DE CONTABILIDAD DE CUENTAS.

Una cuenta es el derecho que se le otorga a un usuario, grupo o departamento, para poder hacer uso de los recursos de la red.

Las cuentas son creadas por los administradores y estas pueden tener derechos sobre ciertos recursos, restricciones , o pueden ser eliminadas o creadas nuevamente. Una cuenta de un grupo o departamento puede ser usada por varios usuarios, así mismo un usuario puede tener varias cuentas.

Este trabajo de mantenimiento a las cuentas es muy importante para lograr una administración de la contabilidad de los recursos ya que una vez establecidos los parámetros de como medir la cantidad de información o recursos usados es necesario establecer la correspondencia con las cuentas, las cuales de forma automática, con aplicaciones como Netview 6000 de IBM arrojan datos que indican cuanta información o recursos ha usado cierta cuenta para así asignarle un costo.

En esta parte es indispensable el mantenimiento a las cuentas y establecer como se desea asignar el costo, ya sea por departamento, grupo, usuario o proyecto y determinar el tiempo que va a servir como parámetro para establecer el costo.

También se debe de tener claro que servicio se va a cobrar o si se va a obtener el costo en base a todos los recursos ofrecidos por la red.

En síntesis el mantenimiento de las cuentas consiste en tener claramente definido el tipo de cuentas que se han creado (usuario, grupo, área, departamento o proyecto), el tipo de recurso del que hacen uso (impresión a color, espacio en disco duro, transmisión remota entre otros) y mantener actualizada esta relación, o dependiendo del tipo de empresa, esta relación se puede llevar a cabo solo para cierto recurso como por ejemplo para la transmisión remota.

5.4 ASIGNACIÓN DE COSTOS A LAS CUENTAS.

Es necesario determinar los tipos de cargo y las tarifas con que se desea facturar a los usuarios por los servicios que les ofrece la red.

Pueden existir muchas tarifas; se puede tener una tarifa distinta en momentos distintos del día, por ejemplo, se podría establecer una tarifa de conexión superior durante el día que durante la noche.

Una vez que se tienen ya definidos los parámetros para medir el uso de los recursos de la red y además se tienen bien definidas las cuentas, es decir quien usa esos recursos, el siguiente paso es asignar los costos a las cuentas.

Con base en los parámetros que se necesitan para establecer el uso de los recursos de la red se explicaran algunos de los tipos de tarifas más comunes que son usadas por el sistema operativo de red Netware 4.10 para dejar claramente como se establece la correspondencia entre uso de los recursos de la red y cargos que se generan por el uso de dichos recursos.

- Tarifas por lectura de bloques.
- Tarifas por escrituras de bloques.
- Tarifas por tiempo de conexión.
- Tarifas por espacio para almacenamiento en disco.
- Tarifas por utilización de servidor.

- **TARIFAS POR LECTURAS DE BLOQUE.**

Consiste en fijar las tarifas de facturación sobre la cantidad de información leída en el servidor. No incluye el control de los bloques escritos en disco. Se asigna una tarifa por cada bloque leído, siendo el tamaño de bloque 4096 bytes o 4 Kb, la tasa puede ser distinta para cada intervalo de media hora.

La cantidad de bloques leídos puede llevar a confusión ya que cada vez que se abre una base de datos y se lee, se añaden los cargos, incluso en el caso de que no se realice ningún trabajo.

Cada vez que el usuario lee un bloque se realiza un cargo a su cuenta.

- **TARIFAS POR ESCRITURA DE BLOQUES**

Es similar a la anterior, excepto en que realiza el seguimiento de la información que los usuarios escriben en el disco, en lugar de la que leen. Se asigna una tarifa por cada bloque de 4096 bytes (escrito 4 Kb), pudiendo darse un valor distinto por cada intervalo de media hora.

Cada vez que se escribe un bloque en el disco se hace un cargo en la cuenta del usuario o grupo. Se debe de tener cuidado al utilizar esta opción de control, ya que algunos programas escriben continuamente en el disco.

- **TARIFAS POR TIEMPO DE CONEXIÓN.**

Se factura o se hace el cargo por periodos de media hora, que los usuarios están conectados al servidor, para aplicar este método es importante analizar el tipo de usuario o grupo y los recursos disponibles en la red.

- **TARIFAS POR ESPACIO PARA ALMACENAMIENTO EN DISCO.**

Se hace un cargo por cada bloque de disco ocupado, los bloques son de 4096 bytes (4K). Se establece una tarifa para los incrementos del número de bloques en intervalos de media hora; este incremento se asigna en base a un número de bloques/día que corresponde al número de bloques almacenados en un día.

- **TARIFAS POR UTILIZACION DEL SERVIDOR.**

Establece cargos por el uso en general del servidor. Cada vez que un usuario envía una petición al servidor para cualquier operación, se hace un cargo en su cuenta. Las tarifas se pueden definir por cada intervalo de media hora, facturándosele al usuario por petición recibida. Se hacen cargos desde el momento de conexión hasta el de desconexión.

Se pueden establecer tarifas distintas en cada servidor de la red, pero el administrador de ésta debe de asegurarse de que todos los sistemas utilicen el mismo método para fijar las tarifas.

Para aclarar este proceso de asignación de cargos se ejemplifica con el método usado por Netware 4.10

En este sistema operativo de red las tarifas (en forma de fracción) se calculan según la formula:

Numerador de la tarifa / Denominador de la tarifa

El numerador es la cantidad de dinero que se desea facturar por un tipo de servicio, como puede ser la lectura de bloques. El denominador es normalmente lo que indica una unidad de servicio.

Esta fracción se asigna, seguidamente a periodos específicos del día, pudiendo utilizarse hasta veinte fracciones. De esta forma por ejemplo, los cargos pueden ser mayores durante el día que durante la noche, las tarifas se muestran para cada media hora en un período semanal, utilizando los siguientes métodos de facturación:

Tarifa por bloques leídos	Cargo por bloque
Tarifa por bloques escritos	Cargo por bloque
Tarifa por tiempo de conexión	Cargo por minuto
Tarifa por almacenamiento en disco	Cargo por bloque-dia
Tarifa por petición de servicios	Cargo por petición recibida.

5.5 MONITOREO DE LAS CUOTAS.

Consiste en revisar periódicamente el comportamiento de las cuotas asignadas por servicio prestado; para poder modificarlas, crear nuevas, en base a las ya creadas o eliminarlas si así se requiere.

Esta parte de monitoreo de cuotas sirve para cuando un grupo o usuario se ha pasado del limite y se le tiene que asignar más recursos o cuando también cierto usuario no sabe como usar ciertas aplicaciones y esta usando los recursos y absorviendo cuotas sin ser realmente productivo.

5.6 ESTADÍSTICAS DEL USO DE LA RED.

Las estadisticas son muy importantes para la asignación de tarifas a los recursos, ya que en base a estas se podrá establecer los parámetros necesarios para asignar cuotas.

Un software como OpenView de HP brinda automáticamente las estadísticas del uso de la red, con lo cual veríamos como se ha comportado la red, estos datos son reales y automáticos en base a la ejecución que ha tenido la red y por lo tanto son la base para asignar costos a los servicios.

Además de esto, nos permiten tener un enfoque a futuro, ya que estas estadísticas brindan la información necesaria para la planeación de compra de nuevo equipo así como también la proyección

de crecimiento en cuanto a la red y nos proporcionan información precisa de cuanta inversión será necesaria.

Estas estadísticas son una herramienta poderosa para los administradores ya que con ella pueden determinar que recurso o recursos de la red están siendo mas utilizados y que usuario o grupo de usuarios usan más la red, ésto servirá para que el administrador se preocupe por mejorar el servicio que es más usado o por asignarle eficientemente los recursos a los usuarios que mas usan la red.

VI. SEGURIDAD.

6.1 INTRODUCCIÓN.

La seguridad consiste en tareas para asegurarse que solo el personal autorizado puede hacer uso de la red, tareas y funciones asociadas con la administración de la seguridad son la autenticación de los usuarios, la encripción de datos, el manejo y distribución de llaves o claves, entre otros.

Otra tarea que concierne a la seguridad es la prevención contra virus y establecer métodos para cuando sea necesario recuperarse de un desastre y restaurar toda la información, es decir la creación de respaldos confiables. Así en una red, el administrador debe evitar que los usuarios manejen información no autorizada, como podrían ser juegos y debe de establecer métodos para revisar el software desconocido que se pudiera instalar, así como también establecer procedimientos de seguridad que se deben de seguir para trabajar con Internet.

El tema de la seguridad es un tema muy amplio e importante, existen empresas donde la seguridad es de alta prioridad como lo son bancos, en estas empresas como en otras grandes corporaciones que necesitan que su red este segura, el administrador es el encargado de analizar y cubrir en todos los aspectos la seguridad de la red, ya sea de ataques por parte de gente externa así como de las fallas que pueda tener el equipo debido a causas impredecibles (como lo es una descarga, un rayo, etc.) o por mal uso de usuarios (borrar archivos del sistema).

Cuando se quiere mantener algo seguro, es necesario analizar de quién o contra qué se debe de asegurar, en el mundo de la informática, se ha incrementado el delito como la piratería, saboteo de información, daño intencionado entre otros, en una red básicamente se puede clasificar a la gente que realiza estos delitos o causas que generan la pérdida de información:

- Gente externa (robo de información, destrucción de información, introducción de virus).
- Gente interna (instalación de software no autorizado, introducción de virus, borrado de información por error o intencionalmente, robo de la misma entre otros)
- Causas naturales (fallas aleatorias del equipo, caída de un rayo, un terremoto, un incendio)

Este tipo de causas o ataques contra la información en una red es atendido por las siguientes áreas:

- Seguridad física del equipo.
- Seguridad proporcionada por el equipo
- Seguridad contra desastres de información.
- Seguridad de la información interna.
- Monitoreo de la seguridad de la red.
- Implementación de medidas de seguridad.
- Mantenimiento de la seguridad.

6.2 SEGURIDAD FÍSICA DEL EQUIPO.

Esta parte de la seguridad de la red consiste principalmente en tener o adecuar las instalaciones a los requerimientos ambientales que requiere el equipo, éstos son factores externos como: la electricidad estática, el calor, el frío, el polvo, la humedad, los ruidos eléctricos, los altibajos de tensión, los cortes de corriente, la suciedad, los incendios y el agua, y protección contra robo y destrucción.

- PROTECCIÓN CONTRA ELECTRICIDAD ESTÁTICA.

Entre las precauciones que se han de tomar, esta la de tratar regularmente las alfombras, con productos antiestáticos, y tener la instalación de corriente a tierra, entre otras.

- ADECUAR LA TEMPERATURA DE LAS INSTALACIONES

Se debe de tener una buena instalación de aire acondicionado que mantenga la temperatura de la sala entre 18° C y 26° C y evitar la acumulación de polvo.

- MANTENER CONTINUO EL SUMINISTRO DE ENERGÍA.

Contar con el equipo UPS (Uninterrumptible Power Supply) lo suficientemente potente para suministrar energía a la red o componentes más importantes de la red (como servidores) para cuando el servicio normal de energía es interrumpido o cae por debajo de los niveles aceptables.

Además, cada dispositivo de la red podría tener un filtro de energía eléctrica como protección de las sobretensiones.

- **LA SUCIEDAD**

Se debe de tener la sala en un estado de perfecta limpieza, evitar cualquier derrame de líquidos o restos de alimentos, así como también ceniza de los cigarros porque pueden producir daños importantes.

- **PROTECCION CONTRA INCENDIOS Y AGUA.**

Se debe tener protección contra incendios, detectores de humo de alta sensibilidad y un sistema contra incendios, éste sistema debe de producir un aviso previo a su utilización.

También deberá existir protección contra inundaciones y goteras, que podrían provocar cortocircuitos eléctricos.

- **PROTECCIÓN CONTRA ROBO Y DESTRUCCION.**

Se debe de poner una protección efectiva que imposibilite tanto el robo del equipo o de alguno de sus componentes como. la posibilidad de algún atentado que provoque la destrucción de todo (tanto de hardware como de software).

La sala deberá estar protegida con sistemas antirobo y las puertas que conducen a la sala deberán permanecer cerradas y se deberán identificarse o tener una clave de acceso las personas autorizadas para accesar a dicha sala.

6.3 SEGURIDAD PROPORCIONADA POR EL EQUIPO.

En el aspecto de seguridad es necesario recordar que algunos dispositivos de mayor importancia incluyen dentro de sí sistemas de seguridad, que permiten el funcionamiento de los mismos sin interrupción alguna, por ejemplo un servidor puede contar con un arreglo de discos el cual si falla algún disco, otro entrará en funcionamiento sin que se note (a los usuarios) que un disco ha fallado.

Para lograr mantener segura una red en forma centralizada es necesario contar con el hardware y software adecuado, para que se logre un control rápido y eficiente en ciertos dispositivos de mayor prioridad dentro de la red .

Como se mencionó en el capítulo de configuración, un software administrador de red como lo es HP OpenView nos permite tener mayor control sobre los dispositivos de red. Se explicarán como funcionan algunos métodos de seguridad en cierto equipo como son:

- Arreglos de discos en servidores.
- Seguridad en concentradores.
- Seguridad en puentes.
- Seguridad en ruteadores.

Estos métodos de seguridad en el equipo tienen como fin principal el funcionamiento continuo de la red y el cuidado de la información.

- **ARREGLO DE DISCOS EN SERVIDORES.**

RAID (Redundant Array of Inexpensive Disks) es un arreglo de discos que proporciona tolerancia a fallas debido a la redundancia que brinda al guardar la información.

Por lo general se utiliza en redes o aplicaciones de misión critica utilizando varias unidades de discos duros, que en su mayoría son de tipo SCSI debido al alto rendimiento en lectura y escritura. RAID ofrece redundancia, el nivel de redundancia depende del nivel de RAID usado. Muchos sistemas RAID permiten la sustitución de los discos estando en funcionamiento el servidor, al sustituir un disco se utiliza la información de paridad para reconstruir los datos del disco dañado. La reconstrucción se produce mientras el sistema operativo continua realizando otras operaciones por lo que hay algunas pérdidas de rendimiento durante la operación de reconstrucción, estas pérdidas son mínimas.

Existen distintos niveles de RAID, se debe de elegir el más adecuado a las necesidades de la red, el más seguro es el nivel 5 es decir RAID 5.

- **SEGURIDAD EN CONCENTRADORES.**

Para evitar los ataques de un intruso en la red mediante el cableado, existen dos caminos, un camino es si se tiene cableado de par trenzado o coaxial, cambiar el cableado a fibra óptica la cual es muy difícil para la intromisión de intrusos (para introducirse en la señal de un cable de fibra óptica se requiere romper o desconectar el cable). Se puede poner HP OpenView interconectado a un manager o estación de control para notificar si la continuidad de un cable de fibra óptica ha sido rota. El otro camino es configurar los dispositivos de la red para proveer seguridad adicional.

Varios concentradores de HP como por ejemplo HP EtherTwist Hub Plus/24s y 100VG AnyLAN Hubs pueden ser configurados con la prevención de intrusos, esta prevención puede ser configurada en varios niveles . En el nivel más alto de prevención de intrusos, un simple dispositivo es autorizado para usar un puerto en particular en el concentrador, si otro dispositivo intenta transmitir a través de ese puerto, el concentrador deshabilita el puerto y notifica al administrador de la red (vía HP OpenView interconectado a un manager).

Si el intruso trata de transmitir paquetes dentro de la red, el concentrador ve que la dirección de la estación no es una de las autorizadas para el puerto y desconecta el puerto de la red. Esto significa que un intruso puede oír el tráfico que llegue al nodo al que esta atachado, pero no puede explorar la red. Un nivel de prevención contra intrusos es eavesdrop "prevención contra intrusos indiscretos", si esta se habilita en el concentrador, se limita al intruso solo a oír el tráfico direccionado al nodo A (nodo donde esta atachado el intruso).

Cuando es habilitada la prevención eavesdrop el concentrador examina la dirección del destino en cada paquete y envía el paquete en su forma original al puerto donde esta atachado el nodo destino, y envía una señal de colisión a los otros puertos. Así si el nodo B envía un paquete al nodo D , los nodos C y A (si el intruso esta atachado al cable del nodo A) no van a ver el contenido del paquete.

- **SEGURIDAD EN PUENTES.**

La seguridad en un puente opera por filtrado, examina la llegada de paquetes con ciertas características y descarta cualquier paquete que no coincida con el criterio establecido de filtrado. La seguridad de muchos puentes esta basada en el filtrado de las direcciones y hace uso de una tabla de direcciones que el puente mantiene dentro de él.

En el modo normal de operación del puente, el administrador de la red puede crear una tabla de direcciones que puede dejar dentro del éste permanentemente, la cual va a causar que el puente descarte cualquier paquete de una dirección no especificada dentro de la tabla. Por ejemplo si la dirección de la estación 104 no esta en la tabla de direcciones, el nodo 104 no podrá enviar paquetes a través del puente hacia el otro segmento de la red o departamento de contabilidad .

Para más seguridad el puente puede operar en el modo de seguridad. En el modo de seguridad el puente envía paquetes sólo si la dirección de ambos nodos, fuente y destino están en la tabla de direcciones. Así un paquete enviado por el nodo 102 hacia el nodo 202 se puede enviar por el puente sólo si la tabla de direcciones contiene las direcciones de ambos nodos.

- **SEGURIDAD EN RUTEADORES.**

La seguridad de un ruteador es parecida a la seguridad de un puente, ésta opera por filtrado de paquetes. Los ruteadores son dispositivos más complejos que los puentes y ofrecen más opciones de filtrado. El filtrado disponible depende de que protocolo de ruteo se este usando (los ruteadores de HP tienen cinco diferentes protocolos de ruteo construidos dentro de ellos).

6.4 SEGURIDAD CONTRA DESASTRES DE INFORMACIÓN.

Es esta parte la encargada de asegurar la información total o de mayor prioridad de una red, así como también de atacar a los virus que se puedan introducir en la red ya sea en forma de juego o totalmente intencionada para dañar la información.

La primera parte consiste en la creación de respaldos, para esto es necesario hacer el análisis de ciertos aspectos como son:

- Tener el hardware adecuado (por ejemplo Sure store 6000).
- Tener el software adecuado (por ejemplo Arcserve de Cheyenne)
- Definir qué información se va a respaldar (bases de datos, directorios de trabajo de los usuarios, o alguna aplicación completa)
- Definir cuando se van a hacer los respaldos (en la noche, fines de semana, fines de mes)

Es importante planear y programar la creación de respaldos y tomar en cuenta ciertos puntos que se presentan por ejemplo, cuando se hace el respaldo de una base de datos no debe existir ningún usuario trabajando en ella ya que esto impediría un respaldo completo de dicha base, otro punto es saber exactamente cuanta información se va a respaldar ya que se pueden necesitar varias unidades de cintas y determinar si se cuenta con un sistema automático de cambio o va a depender de una persona el cambio de cintas, también es necesario cuidar el tiempo que se tardan en la realización los respaldos, ya que en ocasiones hay que esperar a que todos los usuarios dejen libre la base de datos y la noche no alcanza para crear el respaldo de toda la información.

Otro punto a cuidar es la programación de los respaldos y donde se deben de guardar estos, la programación puede ser diaria, semanal y por lo general se hace una anual.

¿Pero cuándo se utilizan estos respaldos?. Se utilizan cuando existe un desastre y se pierde toda o parte de la información, es cuando entran en acción los respaldos, en el caso más critico se reinstala todo el sistema operativo y sobre él se hace una restauración de los respaldos, volviéndose a tener toda la información hasta la fecha del último respaldo, cuando es parcial la pérdida sólo se restaura la información pérdida.

Cuando se cuenta con HP OpenView conectado a un manager éste puede notificar que un respaldo no se llevo a cabo y mandar el mensaje al administrador.

La segunda parte de la seguridad contra desastres de información involucra la prevención y ataque a los virus informáticos. Esta es una de las ventajas que presenta software como HP OpenView ya que mediante este producto se puede hacer la instalación y actualización de antivirus de todas las estaciones tanto remotas como locales en forma automática y sin interrumpir el trabajo de los usuarios, pero no sólo consiste en instalar y actualizar los antivirus para resolver el problema, se deben de revisar aspectos como son:

- Elegir el tipo de vacuna (marca)
- Elegir el nivel de seguridad que se va a instalar en estaciones y servidores.
- Capacitar a los usuarios acerca de como evitar y vacunar a los virus
- Usar otras medidas de seguridad.

- **ELEGIR EL TIPO DE VACUNA**

Este depende del criterio y experiencia del administrador ya que por lo general todos los productos antivirus ofrecen casi el mismo nivel de eficacia para terminar con los virus. Por ejemplo McAfee, Dr´Solomons, Norton Antivirus por mencionar algunos.

- **ELEGIR EL NIVEL DE SEGURIDAD**

Esto consiste en conocer los diferentes tipos de configuración de la vacuna y adecuarla a las necesidades de la red, es decir en ocasiones ocupan demasiada memoria convencional que alentan notoriamente el desempeño de la red, así como también determinar si se va hacer una revisión en el servidor residente o sólo en ciertos días específicos como podrían ser los fines de semana.

Existen por lo general tres niveles de seguridad que son: el mínimo, estándar, y el máximo, los cuales su nombre corresponde a la memoria de la que hacen uso, además se diferencian en que algunos revisan todos los archivos que se leen o que se escriben, o solo al análisis de los posibles archivos portadores de virus, en eso principalmente se diferencian los niveles de seguridad que ofrece una vacuna ya sea a nivel servidor o estación de trabajo.

- **CAPACITAR A LOS USUARIOS.**

La capacitación consiste en que un usuario entienda perfectamente que es un virus, como puede contaminar a la red, como se reproduce y que hacer para eliminarlo, cuando el usuario sea consciente de todo lo anterior y se dé cuenta de que su información se puede perder total o parcialmente debido a un virus, será capaz de prevenirlo o vacunarlo y gran trabajo del administrador será resuelto.

Se dará una explicación breve de lo antes mencionado:

- **VIRUS.**

Es un programa que tiene la capacidad de reproducirse y tiene algún objetivo en especifico como por ejemplo dañar la tabla del FAT, borrar archivos o mandar mensajes inofensivos entre otros.

Existe una inmensa variedad de virus, algunos son inofensivos y son creados solo para molestar, algunos otros son totalmente dañinos ya que pueden terminar con toda la información de una empresa o usuario sin el consentimiento de ésta o éste respectivamente, los más conocidos pueden ser natas, monkey.B, esto te pasa, y los más actuales que son los macrovirus.

- **CÓMO CONTAMINAN O SE TRANSMITEN.**

La forma más básica es copiando un archivo contaminado a otro disco o PC, estos por lo general están hechos en un código especial el cual no permite que se vea el programa del virus y la gente se pasa archivos en disquetes o a través de la red sin cuidado alguno contaminándose en ocasiones con sólo la lectura de los archivos contaminados, ya que al leerlos queda el virus en memoria y después este se copia al disco duro.

- **CÓMO SE REPRODUCEN.**

Estos virus están hechos como ya habíamos mencionado en un código especial con el cual se puede programar su forma de reproducción, es decir como se van a ir copiando. Esto lo realiza el que hizo el virus y determina como se va a reproducir.

- **CÓMO SE VACUNAN.**

La forma ideal es tener una vacuna residente en memoria y cuando se vaya a introducir un disquete vacunarlo antes de leerlo, con esto se elimina el virus, cuando aparece el mensaje de virus encontrado se debe de cerrar las aplicaciones como normalmente se hace y vacunar el disquete.

Para vacunar una estación de trabajo se debe de bootear con un sistema operativo limpio de virus y vacunar al disco duro con la vacuna elegida.

Para vacunar la red el primer paso es tener todas las estaciones de trabajo limpias, luego vacunar desde una estación la red sin estar como supervisor, después, ya como supervisor vacunar nuevamente a la red en su totalidad.

- **USAR OTRAS MEDIDAS DE SEGURIDAD.**

Las otras medidas de seguridad contra virus corresponden en su totalidad al administrador y esto consiste en revisar todo el software que existe en la red, y el que se instala temporalmente, revisar su autenticidad, mediante la administración de cuentas cuidar los directorios de mayor prioridad para que los usuarios no puedan escribir en ellos, revisar que los usuarios tengan activas sus vacunas y configurar las vacunas para que le avisen al administrador cuando se tenga un virus; y no permitir que un usuario pueda renombrar la vacuna y sobre todo actualizar continuamente la vacuna ya que día con día aparecen nuevos virus, y en el caso más drástico quitarle los flopys a las estaciones de trabajo.

6.5 SEGURIDAD DE LA INFORMACIÓN INTERNA.

Una parte importante en el tema de la seguridad es sin duda alguna la protección de la información que fluye dentro de la red y sobre todo controlar la que entra del mundo exterior así como también se debe de asegurar la información que se transmite entre redes o segmentos de la misma, para esto existen diferentes opciones que nos permiten cumplir con este propósito.

La seguridad que se requiere para resguardar la información de una red es en parte implantada por el sistema operativo de red que este operando, uno de los sistema más seguros es UNIX, así todos los sistemas operativos de red proporcionan su propio sistema de seguridad otros ejemplos son Windows NT y Netware 4.10 .

Por lo general los procesos de seguridad tienden a ser molestos para el usuario, ya que estos tienen la característica de hacer más difícil el uso de la red.

Estas son algunas de las acciones más comunes que se deben realizar para lograr la seguridad de la información en una red :

- Control de acceso a terminales
- Distribución de claves.
- Contraseñas de archivos
- Restricción del acceso a archivos.
- Autenticación de usuarios.
- Encripción de la información.

- **CONTROL DE ACCESO A TERMINALES.**

Consiste en poner contraseñas para que solo el usuario asignado sea el que use el equipo, esta contraseña idealmente solo la debe de saber el usuario y el administrador en ciertos casos, para que este último pueda hacer cambios cuando así se requiera.

Esta contraseña la cual se puede deshabilitar vía hardware (mediante swichts) o vía software (en el setup de la máquina) según se desee , tiene como objetivo que solo el dueño de la máquina sea el que haga uso de ella y otros usuarios no tengan el acceso a la información que esta contenga.

- **DISTRIBUCION DE CLAVES.**

Este proceso consiste en la asignación de claves a todas las cuentas y establecer un formato de cómo se van a crear dichas claves, de cuántos caracteres van a estar formadas, que se cambien forzosamente en cierto período de tiempo, de no usar el login como clave, que no se repitan, que se establezcan claves para accesar a todos los lugares de mayor importancia y que el usuario sea el único que conozca su clave.

- **CONTRASEÑAS DE ARCHIVOS.**

Esto consiste en asignarle constraseñas a los archivos de gran importancia para que se pueda accesar a ellos así, sólo los usuarios autorizados y que cuentan con la contraseña podrán accesar al archivo protegido.

- **RESTRICCION DEL ACCESO A ARCHIVOS.**

Esto consiste en restringir el acceso a usuarios hacia los archivos, además de las contraseñas que se les puede poner, se puede cambiar las propiedades de un archivo protegiéndolo contra escritura o cualquier modificación y dejarlo de sólo lectura, también se puede filtrar el acceso a ciertos usuarios solamente.

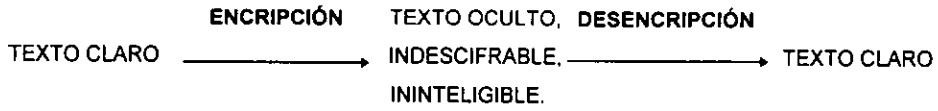
- **AUTENTICACIÓN DE USUARIOS.**

La autenticación consiste en verificar la identidad de alguien, este proceso un tanto complejo tiene como objetivo verificar que un usuario sea realmente un usuario de la red , la autenticación

involucra la comparación del nombre y las contraseñas con una lista de usuarios; si hay coincidencia, el usuario puede ingresar al sistema de acuerdo con los derechos o permisos que se le han asignado a su cuenta, y si no lo es y es un intruso, se puede notificar al administrador del o de los intentos que éste intruso lleva tratando de entrar a la red.

- **ENCRIPCIÓN DE LA INFORMACIÓN.**

El proceso de encriptar la información consiste en ocultar la información que se ha escrito y se esta transmitiendo, esto se logra utilizando diferentes algoritmos los cuales ponen de una forma ininteligible la información y no se puede descifrar sino hasta que se desencripta con el receptor indicado.



Existen otros servicios que ayudan a la encripción y desencripción, estos son: la revisión de la integridad de la información (integrity checking) que consiste en checar que el mensaje no haya sido alterado desde que este fue generado por la legítima fuente y la autenticación que consiste en verificar la identidad de alguien.

Existen diferentes algoritmos para la encripción , un ejemplo es DES (Data Encryption Standard) método estándar de encripción (cifrado) y desencripción (descifrado) de datos creado por la oficina nacional de estándares de los Estados Unidos. Trabaja como una combinación de transposición y sustitución, lo utiliza el Gobierno Federal, la mayoría de los bancos y los sistemas de transferencia de fondos para proteger la información. Durante los años que se ha venido utilizando, nunca ha sido descifrado . Este método convierte la información en datos aleatorios, de tal manera que es imposible determinar la clave para descifrarlos, incluso si se conoce parte del texto original.

Otro ejemplo es el MD5 (Message digest 5) que es el que usa SNMP v.2 para su seguridad en la transmisión de datos.

6.6 MONITOREO DE LA SEGURIDAD DE LA RED.

Otra parte para lograr la seguridad en una red es el monitoreo que va a detectar la entrada de intrusos o los intentos que estos han hecho para entrar en la red, el rastreo de estas cuentas ayuda a ver porque sector se intenta violar las reglas de seguridad.

El monitoreo de la seguridad ayudara al administrador a tener un control central desde la estación manager o administrador para prevenir fallas en el equipo como puede ser un ruteador, para verificar que los respaldos se estén realizando conforme a lo planeado y para controlar a los usuarios vía administración de cuentas.

Existen diferentes productos de HP OpenView que nos proporcionan herramientas para controlar la seguridad de la red y los veremos en el capitulo 8.

6.7 IMPLEMENTACION DE MEDIDAS DE SEGURIDAD.

El administrador debe evaluar los requerimientos de seguridad de la red, establecerlos y sobre todo hacer que se lleven a cabo, como puede ser que se tenga activa la vacuna, que cambien su password, entre otros. Además de las medidas de seguridad que se han mencionado es fundamental establecer la seguridad en cuanto al uso de Internet y bloquear la entrada de información del mundo exterior o extraña a la empresa según se determine. Para esto el administrador debe de poner uno o varios firewall o la combinación de otras medidas de seguridad como las proporcionadas por ruteadores y puentes para impedir que los intrusos dañen la información.

6.8 MANTENIMIENTO DE LA SEGURIDAD.

El mantenimiento de la seguridad en una red consiste fundamentalmente en obligar al seguimiento de los procedimientos implantados de seguridad, por ejemplo revisar que se vacunen disquetes, que se realicen los respaldos correctamente, que los usuarios solo usen el equipo que les corresponde entre muchos otros que ya se han mencionado y hacer que funcionen eficientemente.

Como el funcionamiento de una red es dinámico, también se debe de manejar en forma dinámica la seguridad ya que quizá se deban implantar nuevas reglas de seguridad o conforme a las estadísticas cambiar o quitar ciertas partes en la seguridad ya establecida.

VII. EVALUACIÓN OPERATIVA.

7.1 DEFINICIÓN.

La evaluación operativa consiste en tareas para evaluar la utilización de la red, del equipo y los medios de comunicación, además de hacer ajustes a éstos como se requiera. Las tareas de evaluación pueden variar desde una observación visual de los indicadores del equipo, hasta el agrupamiento y selección de información en una base de datos para proyectar las tendencias de utilización, sin importar el método usado, el objetivo de la evaluación operativa de la red consiste en asegurarse que exista la suficiente capacidad para soportar al usuario final.

Si la red no tiene la suficiente capacidad de desempeño, el usuario final se quejará en cualquier momento y el tiempo de respuesta hacia él se incrementará; de forma inversa el administrador de la red recibirá pocas quejas de los usuarios, los cuales siempre recibirían respuestas en un tiempo corto, esto significa una suficiente capacidad que se refleja en el reconocimiento por parte del personal que integra la empresa o corporación.

Una variedad de herramientas son usadas para evaluar el desempeño de la red, éstas consisten en: un sistema administrador de red, analizadores de protocolos, pruebas de equipo y por su puesto de las facturas que se generan por gastos de comunicación.

Las facturas pueden indicar la utilización de las líneas de comunicación, en otras palabras seria la actividad de paquetes enviados a través de la red, el sistema administrador de red provee información concerniente a la utilización individual o segmentada de una red, así como el uso de la líneas para módem, la operación de los puentes, ruteadores y otros dispositivos de la red. El uso de un analizador de protocolos puede generar información estadística del desempeño, así como el nivel de utilización de la red y los dispositivos conectados a diferentes componentes de la red.

En forma concreta la evaluación operativa de la red tiene como principio evaluar el desempeño en general de la red, su operatividad, su eficiencia, y realizar tareas que optimicen esta operatividad.

La evaluación operativa permite revisar que nivel de funcionalidad se tiene, si éste es alto o bajo; y se determina en que sectores o dispositivos se tiene un nivel bajo de desempeño, se determinan las causas, una vez determinadas éstas causas se toman acciones que eleven este nivel de desempeño; y si existe un nivel alto, también tomar medidas para mantenerlo.

Las tareas que ayudan a evaluar la operatividad o desempeño de la red son:

- Monitoreo del desempeño de la red.
- Análisis de las estadísticas.
- Análisis de la base de datos del sistema.
- Medir el nivel de servicio.
- Capacidad para planear.
- Optimizar el desempeño de la red.

7.2 MONITOREO DEL DESEMPEÑO DE LA RED.

El monitoreo en este capítulo cumple una función primordial para la evaluación del desempeño de una red, como se ha mencionado en capítulos anteriores, es una herramienta tan potente que va a permitir observar gráficamente como se esta comportando la red.

El monitoreo del tráfico de la red es uno de los más importantes para la evaluación, ya que éste indica que sector de la red o que estación de trabajo esta generando mas tráfico; y se pondría especial atención para corregirlos.

HP OpenView cuenta con diversos productos que son aplicaciones para administrar una red, las cuales revisan el desempeño de una red, éstas se explicaran más a fondo en el capitulo 8. La estación de trabajo (NMS) o de control donde esta instalado este software, permite capturar el tiempo real en la transmisión de información y mostrar gráficamente en que lugar de la red existe más tráfico.

Se puede monitorear el tráfico que esta enviando una estación de trabajo a un servidor, o el tráfico generado por un cliente remoto y su tiempo de transmisión, así como también el tráfico entre diferentes dispositivos como son servidores, impresoras y otros; en general puede brindar gráficas de todo el tráfico de la red.

La evaluación operativa es un poco la continuación del control de las fallas, por lo tanto otra parte importante es el monitoreo de las fallas, ya que esto ayudara a la solución o a la prevención.

Es importante que se monitoree todo el funcionamiento en general de la red, desde la continuidad del cableado; la seguridad, el uso de recursos por cierta cuenta, la realización de respaldos, y la transmisión remota entre otros.

Diversos productos que funcionan en forma similar a OpenView de HP proporcionan éstas facilidades para todas y cada una de las partes de la red que se deseen monitorear.

La figura 7.1 muestra una imagen de un producto de OpenView que indica gráficamente el comportamiento de diversos dispositivos de la red.

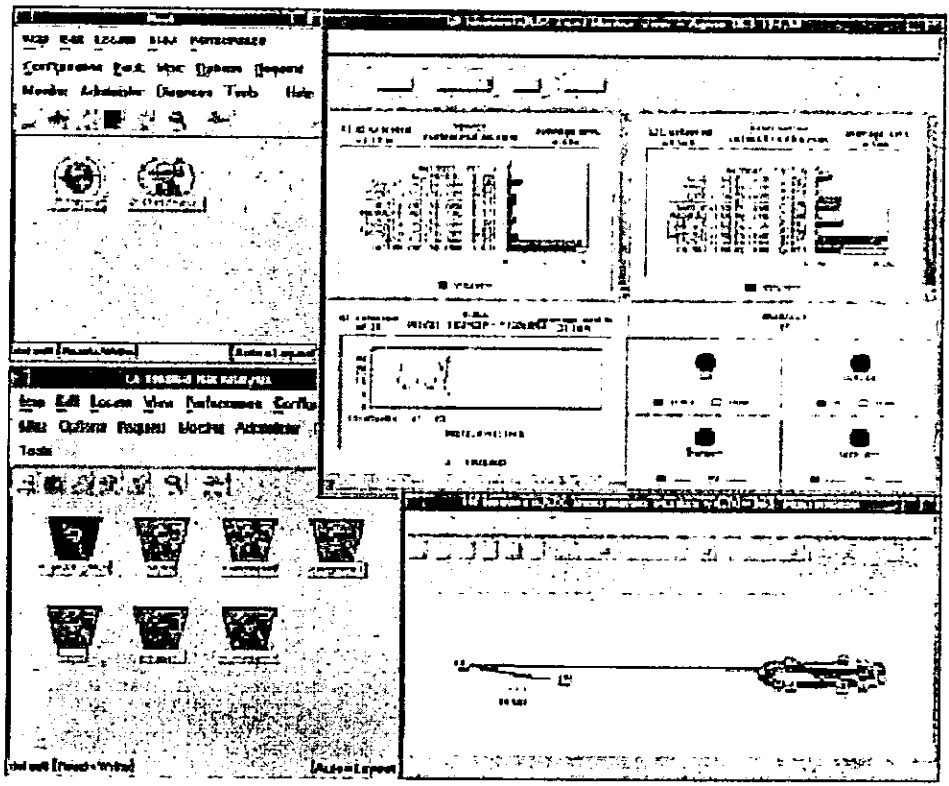


Figura 7.1 Comportamiento de diversos dispositivos de una red.

7.3 ANÁLISIS DE ESTADÍSTICAS.

Si se tiene un desempeño por debajo del nivel planeado, se debe hacer uso de recursos como lo son las estadísticas; existen diversos tipos estadísticas como son: estadísticas de errores, de cambios , del tráfico en la red, de fallas en determinada aplicación o hardware, de uso de los recursos de la red, de usuarios problemáticos, de la información transmitida y su velocidad de transmisión; todas éstas estadísticas ayudan a mejorar el nivel de operatividad de la red con su análisis, y dependiendo que área se quiera mejorar se requerirán las estadísticas correspondientes para implementar nuevas medidas de funcionalidad.

El que existan estadísticas que indican de que forma se esta desarrollando y creciendo la red, es vital, para poder con bases fundadas ser proactivo en la solución de fallas y lograr tener un enfoque a futuro de como se va a comportar la red, además de que dichas estadísticas nos proporcionan información para realizar una planeación más estable.

Un software como lo es HP OpenView proporciona éstas estadísticas de forma automática y las muestra para que el administrador las analice; y en base a el comportamiento de éstas, tomar decisiones que tengan como fin elevar el nivel de operatividad, éstas medidas pueden ser: compra de equipo nuevo, ampliar el ancho de banda en la transmisión, cambio en la configuración, cambio en asignación de recursos o tomar nuevas medidas de seguridad.

7.4 ANÁLISIS DE LA BASE DE DATOS.

En el capítulo 3 se menciona la necesidad de crear una base de datos que incluya toda la información de hardware y software de la red, esta base de datos se debe de analizar y mantenerla actualizada, para que mediante este análisis y con la información del monitoreo de desempeño de la red se haga un balance de operatividad del equipo y aplicaciones para compararlo con lo planeado y tomar decisiones de como actualizar software o hardware según el balance desarrollado.

El software administrador de red permite hacer el balance mas fácilmente ya que proporciona la información necesaria que indica el comportamiento de los dispositivos de la red.

7.5 MEDIR EL NIVEL DE SERVICIO.

Es muy difícil en el mundo de las redes que los usuarios digan que esta funcionando muy bien la red, por lo general se quejan del funcionamiento, que esta lenta etc., aunque se este logrando un desempeño aceptable; siempre habrá algo por mejorar tanto de software como de hardware.

Un recurso que es importante que opere a su máxima capacidad son los medios de comunicación, es decir la transmisión de información en la red y la transmisión remota.

Pero ¿cómo medir el nivel de servicio?, existen muchas formas, como son: las estadísticas que generan los dispositivos de su funcionamiento, las estadísticas que indican cuanta información se transmite en determinado tiempo, éstas brindan la información que indica el nivel de servicio que se esta proporcionando a los usuarios de la red, se observa si es el esperado en base a lo planeado o si fue menor y se determina a que se debe la deficiencia.

Todo el equipo debe ser evaluado y verificar si esta alcanzando su nivel óptimo de operatividad o si se esta desaprovechando su capacidad, y si esto último pasa, reconfigurarlo para explotar al máximo sus capacidades esto puede ser tanto en hardware como en software.

Las estadísticas son las que indican con datos reales si la red tiene un desempeño óptimo o esta por debajo de lo planeado o de su capacidad.

Los gastos generados por los servicios prestados por una red es otra forma de medir el nivel de servicio, ya que estos datos nos indican si los gastos por transmisión, equipo, personal etc., están dentro de lo programado o se sobrepasan, esto es un poco complicado ya que se hace un balance de costos contra beneficios, es la forma más real que indica lo rentable que es la red.

Otra forma de evaluar el nivel de servicio es creando un base de datos la cual contenga todos los reportes hechos por los usuarios de fallas en la red, y cuando el personal de sistemas lo atienda y resuelva, que el usuario evalúe el servicio ya sea de gente interna o de una empresa contratada para dar soporte técnico a usuarios. Esta evaluación debe ser sencilla, directa y objetiva, donde se indique el nivel de servicio que se tuvo al resolver el problema, además de proporcionar información para ser proactivos en solución de fallas.

7.6 CAPACIDAD PARA PLANEAR.

Con toda la información que proporciona el monitoreo de la red, las estadísticas de funcionamiento y las estadísticas en general que indican el comportamiento de la red, se debe tener la capacidad para la planeación ya sea de la instalación de nuevos segmentos de red o la actualización, reconfiguración del equipo; así como también aspectos de administración de recursos y seguridad.

Con datos reales se debe planear las actividades para lograr elevar el nivel de operatividad en la red.

Esta parte sirve para comparar y evaluar con datos reales, si se esta desarrollando la red conforme a lo planeado en un principio, si no fué así definir en que parte se fallo, a que se debió la falla y sobre todo como se va a solucionar.

Con toda la información que nos proporciona el monitoreo y las estadísticas, se tiene una visión mas amplia para poder planear a futuro el nuevo desarrollo de la red y poder establecer las nuevas tendencias que optimicen el funcionamiento de la red.

7.7 OPTIMIZAR EL DESEMPEÑO DE LA RED.

¿Cómo se puede optimizar el desempeño de la red?, el primer paso es realizar una evaluación rígida de que puntos se alcanzaron en su totalidad conforme a lo planeado, establecer en donde se fallo o se esta fallando y dar soluciones que resuelvan las fallas.

Una vez evaluado el desempeño de la red se deben de seguir los pasos que mantengan el nivel de servicio si este fué bueno, o que lo mejoren si este fué malo.

Para mejorar el desempeño de la red se debe de contar con la información necesaria que nos indique que parte o sector la red esta lenta o esta fallando, una vez localizado el problema se deben de tomar medidas que mejoren el funcionamiento, éstas pueden ser en cada una de las áreas en las que se dividió la administración de la red, es decir tomar medidas que optimicen la configuración, que controlen las fallas, que administren mejor los recursos de la red o incrementen la seguridad en la misma.

Algunos ejemplos podrían ser: instalar firewall en la red, instalar niveles de filtrado más complejos en los ruteadores, comprar un nuevo antivirus más eficiente, actualizar a la última versión el software que crea los respaldos, actualizar equipo como tarjetas de red que transmitan a mayor velocidad, actualizar software para enlace remoto y que transmita más rápidamente entre otros.

Esta parte de la administración de la red consiste en esencia en evaluar como está funcionando la red y aplicar otras nuevas opciones que mejoren el desempeño de ésta. Además de cuidar que se sigan todos los procedimientos que se han planeado e implementado en todas las áreas anteriores y mantener la continuidad en su funcionamiento.

VIII. SOFTWARE DE APLICACIÓN

En el capítulo dos se explicó bajo que plataforma y que requerimientos necesita un software administrador de red para que funcione, en este capítulo se profundizara en una en especial que es OpenView de HP, sin olvidar por supuesto la existencia de otros como son NetView 6000 de IBM y Cisco.

8.1 DEFINICIÓN.

Un software administrador de red, es una aplicación que facilita mediante diversas herramientas, la administración de todos los dispositivos de una red, incrementando así su desempeño.

Para que esta aplicación funcione se necesita de software y hardware, así como de un protocolo de comunicación mediante el cual se va a controlar a todos los dispositivos.

HP OpenView es un conjunto integrado por aplicaciones que vienen en mas de 30 productos HP, y además existen mas de 300 aplicaciones compatibles para integrarse con OpenView; y administrar una red y sus sistemas. Estas aplicaciones se implementan en la red y se controlan desde un sistema administrador NSM (Network System Management) que en los capítulos anteriores se le dio el nombre de NMS (Network Management Station), o estación de control.

Las aplicaciones por lo general trabajan mediante ventanas que permiten ver a los administradores y operadores IT (Information Technology) problemas dentro de la red; y usar aplicaciones HP OpenView para darles una solución.

Las soluciones HP OpenView son designadas para los administradores IT (Information Technology) y los operadores IT quienes son responsables de administrar en su totalidad una red. Un ***IT administrador*** es la persona o grupo de personas responsables de la red, los sistemas y aplicaciones. Un ***IT operador*** es el responsable o responsables para monitorear, configurar y actualizar la red, los sistemas y aplicaciones.

La familia integrada por productos de HP OpenView ayuda al personal IT en la configuración, monitoreo, mantenimiento, disponibilidad y en optimizar el desempeño en los siguientes componentes:

- Servidores.
- Estaciones de trabajo.
- Aplicaciones.
- Bases de datos.

8.2 SERVICIO DE ADMINISTRACIÓN.

El servicio de administración es el proceso que habilita aplicaciones IT en conjunto con el departamento de costos para implementar soluciones que mantengan un ventaja competitiva, y lograr establecer niveles equilibrados de calidad y costo. Por ejemplo un departamento IT puede realizar una prueba que mejore el servicio con una tecnología moderna, pero si el departamento encargado de asignar presupuesto lo considera demasiado alto, este avance no se va a realizar ya que comúnmente el departamento de presupuestos quiere invertir en equipo lo menos posible, aunque el nivel de servicio y soporte barato que se esta ofreciendo no sea lo que realmente necesite la compañía. Para cubrir esta deficiencia existe SLAs (Service Level Agreements).

SLASs son acuerdos mutuos entre el departamento de presupuesto y el departamento IT para establecer, ¿qué tipo de servicio se va a brindar?, ¿cuánto se desea gastar o invertir para ofrecer un servicio eficiente?.

El programa de servicio de administración de HP OpenView ayuda a los administradores IT a monitorear, mantener y corregir fallas mediante SLAs que proporcionan estas herramientas.

Las aplicaciones en conjunto de HP OpenView incrementan la productividad de los administradores y operadores IT, ya que se disminuye considerablemente el monitoreo manual y las fallas dentro de la red. Incrementando la eficiencia del departamento IT también disminuyen los costos, mejora la calidad y velocidad de servicio antes de que los problemas afecten al usuario final; y ayuda a la compañía o corporación a ser más competitiva.

8.3 INTEGRACIÓN.

En una red, el sistema de administración comprende el monitoreo y manejo de una variedad de componentes como estaciones de trabajo, servidores, segmentos de red, aplicaciones y bases de datos entre otros.

Una sola aplicación no puede manejar todos los componentes de la red, la integración de ciertas aplicaciones mejora en mucho la funcionalidad.

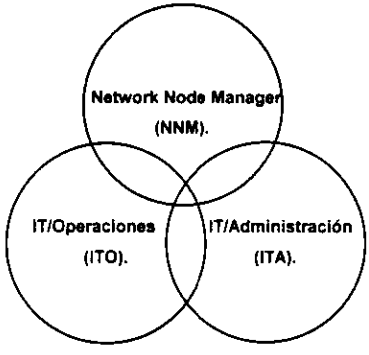


Figura 8.1 Integración de HP OpenView.

La figura 8.1 representa las tres principales aplicaciones de HP OpenView, éstas aplicaciones se pueden integrar para brindar una mejor administración centralizada, se les puede adicionar aplicaciones como HP NetMetrix, HP PerfView, HP OmniStorage o HP Omni Back II; y complementarse para que incrementen la funcionalidad.

8.4 MÉTODOS DE COMUNICACIÓN.

- **SNMP (v1 y v2C):** Éste protocolo maneja alrededor del 95% de todos los objetos, permite que solo los administradores puedan preguntar por cierta información y recibir esta información vía los agentes.
- **RPC :** Este servicio actúa como un transporte para procesos UNIX, se usa solamente para la comunicación entre administradores y agentes.
- **NFS :** Éste servicio habilita a los nodos de la red para poder compartir su sistema de archivos

PRODUCTO	MÉTODO DE ACCESO	AGENTE
NNM	SNMP	AGENTE SNMP
ITO	RPC	AGENTE INTELIGENTE ITO
ITA	RPC	AGENTE INTELIGENTE ITA
PERFVIEW	RPC	AGENTE MEASURE WARE
OMNIBACK II	PRC (CONTROL) SOCKETS (DATA)	AGENTE OMNIBACK II
OMNISTORAGE	NATIVE NETWORK MIGRATION (DEFAULT) O NFS	AGENTE OMNISTORAGE

Tabla 8.1

8.5 COMPAÑÍAS ALIADAS.

Las primeras compañías que se aliaron a HP, para desarrollar hardware y aplicaciones de software las cuales pudiesen usarse con los productos ya establecidos por HP OpenView fueron:

3Com	Cascade Communications Corp.	PLATINUM Technology, Inc.
Accugraph Corp.	Compuware Corp.	PROLIN Software, Inc.
ael-Advanced Graphics System, Inc.	General DataComm, Inc	Racal-Datacom, Inc.
American Power Conversion.	HiPerformance Systems	Remedy Corp.
Autotrol Technology Corp.	Madge Networks	software Artistry, Inc.
Bay Networks	NetTech, Inc.	Sterling Software
BMC Software	Onion Peel Software	UB Network, Inc.
Boole & Babbage	Optical Data Systems	Unison Software
Cambio Networks	Peregrine Systems, inc.	

Tabla 8.2

8.6 PRODUCTOS DE LA FAMILIA HP OPENVIEW Y CARACTERÍSTICAS DE ADMINISTRACIÓN.

HP OpenView ofrece aplicaciones para la administración de redes de grandes empresas cubriendo cinco áreas básicas, cada aplicación de HP cubre cierta categoría o área como son:

- Administración de la red.
- Operaciones y administración de problemas.
- Inventario, software y administración de usuarios.
- Recursos y administración del desempeño.
- Datos y administración del almacenamiento.

8.6.1 ADMINISTRACIÓN DE LA RED.

NNM (NETWORK NODE MANAGER).

Esta aplicación automáticamente dibuja mapas de la red y monitorea el estado de cada dispositivo. NNM también proporciona varias herramientas en un solo lugar o punto, para configurar, diagnosticar y reparar problemas en la red. En una red que contiene aplicaciones multi-vendedor, se puede ver en una sola ventana cada aplicación o dispositivo, lo cual facilita el monitoreo como se ve en la figura 8.2.

También dentro de esta ventana se puede ir de lo general a lo particular, es decir se puede obtener un submapa que muestre cierta área o problema en específico, y verlo a una escala mayor dentro de la misma ventana o mapa principal.

Los mapas generados por NNM usan símbolos para representar sistemas y dispositivos dentro de la red, los símbolos son un código de colores para indicar el estado de cada dispositivo o sistema en particular, si el sistema o dispositivo es verde esto indica que esta funcionando correctamente, cuando esta en rojo indica que existe algún problema.

NNM puede automáticamente dibujar mapas de redes TCP/IP, también puede mapear redes IPX.

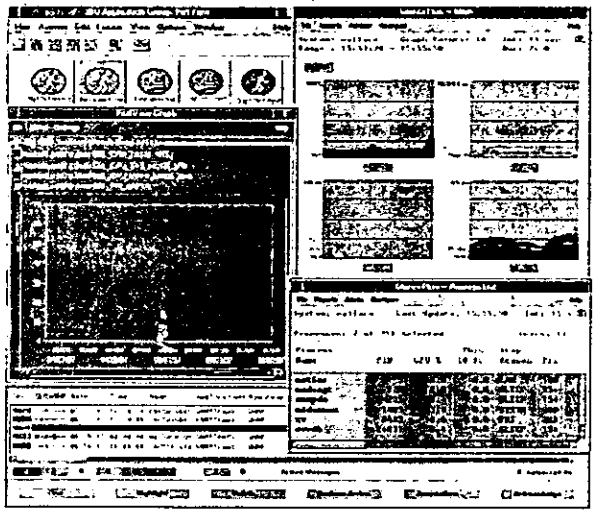


Figura 8.2. Monitoreo a través de HP OpenView.

SUBSISTEMA DE EVENTOS.

Una herramienta de NNM es el subsistema de eventos, que consiste en registrar todos los eventos que han sido problemas potenciales en la red. Los administradores IT pueden usar un browser de eventos para monitorear y ver los eventos del sistema.

Otro componente de un subsistema de eventos es el configurador de eventos, el cual permite a los administradores asociar una acción con cierto evento, cuando estos eventos ocurren, la acción es automáticamente ejecutada. Por ejemplo si un ruteador o concentrador no esta funcionando correctamente, este evento activa una acción tal como entrar otro dispositivo de respaldo o cambiar de ruta.

REGISTRO DE DATOS.

NNM tiene una herramienta que mejora el monitoreo en la red, y es el registro de datos. NNM usa pings y comandos TCP/IP para verificar la conexión de hosts remotos , para determinar el estado de los componentes.

El registro de datos ayuda al monitoreo en la red ya que guarda los valores de los datos SNMP de un sistema remoto, tal como el tráfico generado por una interface, el espacio en disco duro, o la utilización de un CPU. Estos valores son comparados con los predefinidos, un evento es generado si un valor sobrepasa los valores ya establecidos; y una acción de corrección es realizada o un aviso es enviado.

Esta información o registro de datos también puede ser almacenada en una base de datos para realizar un análisis histórico y crear estadísticas.

MIB BROWSER Y LOADER.

NNM ofrece un soporte de MIB universal el cual permite leer información MIB de cualquier agente SNMP en la red. El MIB loader carga información MIB de cualquier vendedor dentro de NNM, y el MIB browser inspecciona los valores MIB de toda la red no importando que sean de diferentes proveedores.

HP NETMETRIX.

Esta aplicación ayuda a monitorear el tráfico en la red, habilita que el administrador pueda ver el contenido de los datos que se están transmitiendo nodos problemáticos o sospechosos dentro de cierta localización geográfica. NetMetrix también habilita la herramienta para simular los efectos que causarían ciertos cambios en la red antes de que el administrador los implemente.

NetMetrix sirve para monitorear la comunicación en la red, las ligas WAN y el intercambio de rutas en la red. Esta integrado por las siguientes aplicaciones:

- **Internetwork Monitor:** Proporciona en forma visual la información del tráfico que existe en la red, la que se genera de cliente a servidor, permite a los administradores IT anticiparse a las necesidades de la red mediante la simulación de posibles modificaciones en la red.
- **Web Reporter:** Ofrece a los administradores IT la información del desempeño de la red.
- **Internetwork Response Manager:** Integrado con PerfView y MeasureWAre Agent proporcionan información del desempeño de la red.
- **Internetwork Response Agents:** Habilita a los operadores IT aislar problemas potenciales.

CISCO WORKS

Cisco Works es una aplicación para administrar ruteadores y gateways Cisco, permite la configuración de dispositivos, el monitoreo y la capacidad para resolver problemas.

CASCADE VIEW /UX

Es una aplicación para manejar Frame Relay, SNDS, y Switch ATM en la red, provee una configuración centralizada, administración y monitoreo desde un solo punto a cualquier switch en la red.

ael-AGS

ael Adcvanced Graphics system's Visionael Net es una aplicación que permite ver como esta ubicada la red de computadoras físicamente, es decir se crea un mapa que indica en que área se encuentra, y también se ubica esta área de acuerdo a la ubicación actual y real dentro de la empresa (ver figura 8.3).

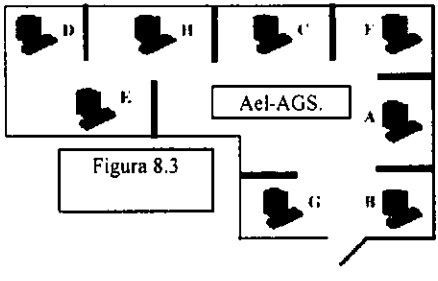


Figura 8.3 ael-AGS.

HP PROFESIONAL SUITE.

HP OpenView profesional suite es un grupo integrado por aplicaciones de HP, Symantec, Ex Machina, McAfee y Microsoft para manejar PCs heterogéneas de redes LAN, y pequeños ambientes de grupo de trabajo. La siguiente lista esta integrada por aplicaciones que son incluidas en HP Profesional Suite

- **HP OpenView Windows Workgroup Node Manager:** Maneja grupos de trabajo heterogéneos.
- **HP AdvancedStack Assistant:** Monitorea el tráfico en la red.
- **HP Jet Admin:** Maneja instalación, configuración y administración remota de impresoras y plotters en la red.
- **HP PowerWise Assintat:** Monitorea la fuente de poder (UPS).
- **HP TopTOOLS:** Monitorea en tiempo real y administra componentes de PCs en multi-plataformas.
- **HP NetServer Assintat:** Monitorea, identifica y maneja problemas en los componentes del servidor.
- **HP NetMetrix/Win:** Proporciona información acerca del estado de la red y ofrece tips para la solución de problemas; y para optimizar el desempeño de la red.
- **Exposé from HP:** Manejo proactivo de los servidores en la red.
- **Norton pcAnywhere from Symantec:** Proporciona el acceso remoto a clientes y la administración de estos desde una consola.
- **Norton Administrator for Networks (NAN) from HP:** Proporciona una serie de herramientas para realizar una administración centralizada de las computadoras en toda la red.
- **Notify! Connect from Ex Machina, Inc:** Monitorea el estado de dispositivos remotos en la red.

  Saber LAN Wokstations from McAfee : Permite tomar el inventario de software y hardware, además de la distribución e instalación de software en forma automática en las estaciones de trabajo de la red.

8.6.2 OPERACIONES Y ADMINISTRACIÓN DE PROBLEMAS.

IT/OPERACIONES (ITO).

Esta aplicación tiene la capacidad de reunir en un punto central todos los problemas, junto con la aplicación NNM permite manejar con la misma consistencia y simplicidad el monitoreo (ver figura 8.4). ITO puede notificar a personal IT de un problema o resolverlo automáticamente basado en las soluciones preestablecidas.

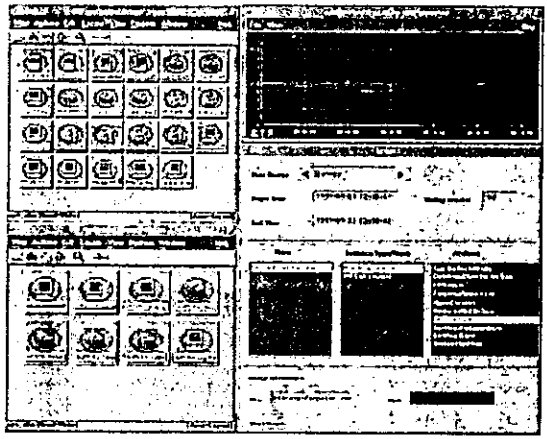


Figura 8.4 Monitoreo de diversos dispositivos.

Los agentes inteligentes de ITO registran todos los datos de aplicaciones y sistemas, los resultados de aplicaciones de diagnostico, los mensajes de la consola y los datos de los trap de SNMP. ITO revisa que los datos correspondan con los establecidos , y los filtra basándose en el tipo, severidad y otros requerimientos de administración.

Los agentes inteligentes ITO automáticamente ejecutan acciones correctivas para resolver problemas remotos . Por ejemplo si el espacio en disco rebasa el valor establecido ITO puede borrar automáticamente todos los archivos core más viejos o con el tiempo establecido para poder borrarse, si el agente inteligente no es capaz de manejar el problema, el evento es enviado a la consola ITO Manager donde es almacenado y registrado en un sistema de eventos como mensajes, éstos mensajes son enviados a cierto IT operador especifico que es el responsable de reparar ese tipo de problema.

Por ejemplo si un operador IT recibe un mensaje que el disco ha sobrepasado la capacidad establecida, el IT operador puede dar permiso o asignar los derechos para que un agente inteligente mediante Omni Back II, respalde todos los archivos viejos del último mes dentro de una cinta y luego borrar estos.

Oracle 7 para OpenView es una base de datos que fue desarrollada para usarse con OpenView. ITO requiere la base de datos Oracle para almacenar sus eventos o logs para su posterior análisis. Oracle es solamente una base de datos que es usada actualmente por ITO.

ADMINISTRACIÓN AVANZADA

ITO puede redireccionar responsabilidades sobre los errores a diferentes sitios, redireccionando los mensajes de eventos a cierto sistema de administración ITO en cualquier parte de la red a cualquier hora. Por ejemplo al final de un día de trabajo en Sydney Australia, los operadores pueden cambiar el destino de los mensajes a sus colegas en Frankfurt Alemania, donde el día esta justamente empezando. Este método de "follow the sun" alivia la necesidad de tener operadores IT especializados las 24 horas del día.

CENTROS IT

Un agente IT es capaz de enviar un problema a un IT operador basado en su experiencia. Los errores pueden ser direccionados a un experto en cualquier lugar de la red. Por ejemplo todos los eventos ocurridos con bases de datos pueden ser automáticamente direccionados al experto en administración de bases de datos, esto alivia la necesidad de tener especialistas IT localizados en todos los lugares.

8.6.3 INVENTARIO, SOFTWARE Y ADMINISTRACIÓN DE USUARIOS.

IT/ADMINISTRACIÓN (ITA).

Esta aplicación automáticamente toma el inventario de todo el hardware, software e información de los usuarios de todos los sistemas de la red y los almacena en una base de datos, también habilita al personal IT para adicionar usuarios dentro de todos los sistemas, este software detecta en cada sistema qué versiones de software están corriendo, luego instala la última versión en el sistema apropiado.

Proporciona un sistema administrador de software sólido para ambientes UNIX y PC desde una estación de control, puede detectar automáticamente los cambios de configuración en cualquier sistema de la red, o la eliminación de cualquier dispositivo.

ITA es una herramienta para la distribución de software que trabaja en conjunto con la base de datos Oracle. ITA puede integrarse con ITO, ITA reporta problemas detectados a una consola de administración ITO; en consecuencia las herramientas ITA pueden ser accesadas por ITO.

DISTRIBUIDOR DE SOFTWARE.

SD (Software Distributor), es una herramienta para la instalación y distribución de software que se puede implementar en Unix, Windows NT, y PCs con sistema operativo, incluye un programador para la distribución e instalación del software en sitios remotos para realizarse cuando se tenga menos carga de trabajo en la red.

8.6.4 RECURSOS Y ADMINISTRACIÓN DEL DESEMPEÑO.

PERFVIEW / MEASUREWARE AGENT / GLANCE PLUS.

PerfView y MeasureWare trabajan juntos para monitorear, analizar y reportar acerca del desempeño de todo el hardware y software en la red.

GLANCE PLUS

Realiza diagnósticos de problemas en tiempo real del desempeño del hardware y software, también permite ver en diferentes niveles de detalle el problema para poder dar una solución eficiente, antes de que se afecte a los usuarios finales.

PerfView, MeasureWare y Glance Plus proporcionan información mas detallada acerca de los sistemas y aplicaciones que NNM, y permiten aislar los problemas dentro de la red.

MeasureWare registra datos de todas las aplicaciones, bases de datos y sistemas de red, luego de tener los logs, PerfView usa estos datos para monitorear el sistema y el desempeño de las aplicaciones, las alarmas son desplegadas y enviadas a NNM o a un browser de eventos ITO. PerfView puede realizar análisis históricos del sistema y aplicaciones que se desempeñan en la red.

Un operador IT puede usar Glance Plus para diagnosticar y corregir sistemas y aplicaciones en tiempo real una vez que Perf View ha enviado la alerta.

8.6.5 DATOS Y ADMINISTRACIÓN DEL ALMACENAMIENTO.

OMNI BACK II.

Esta aplicación respalda grandes cantidades de datos de la red, realiza el respaldo y restauración de datos en línea, el respaldo se realiza de base de datos, archivos y aplicaciones de misión crítica, también permite delegar estas tareas de administración en los diferentes sitios donde se encuentran y a diferentes personas que no sean expertas, es decir es de uso fácil.

Omni Back se puede ejecutar en ambiente UNIX, NT o NOVELL. Omni Back divide a la red en celdas para facilitar la administración de los respaldos, el administrador determina que sistema quiere incluir en cada celda basado en las necesidades de respaldo.

OMNI STORAGE.

Esta aplicación de administración de almacenamiento de datos proporciona alta accesibilidad, migra automáticamente los datos a discos ópticos, cintas de almacenamiento etc.

8.7 COMPAÑÍAS QUE SE ADMINISTRAN MEDIANTE SOLUCIONES HP OPENVIEW.

Algunas de las grandes compañías donde actualmente se esta administrando con soluciones HP OpenView son:

ALCATEL
ASSOCIATED GROCERS (AG).
FIRST CHICAGO BANK.
HEWLETT-PACKARD, MUNDIAL FRANCIA 98
LSL
PEPSI
PIRELLI
TELSTRA

El equipo que se administra en estas compañías es generalmente grande, por ejemplo:

PEPSI. Usando soluciones HP OpenView en :

Mas de 17,000 Nodos en 1996.
Mas de 300 Sites en U.S. y Canadá.

PIRELLI. Usando soluciones HP OpenView en :

14	Sites en Europa
50	Ruteadores Cisco
30	Servidores HP 9000
70	Servidores NT
1	Help desk en Milán.
1000	PCs

Todas estas compañías tienen instaladas las tres aplicaciones básicas de HP OpenView que son NNM, IT/Operaciones, IT/Administración además de un conjunto de aplicaciones que ayudan a mejorar el desempeño de la red como lo es Omni Back II, NetMetrix, y varias aplicaciones de HP Profesional Suite que antes se han mencionado.

CONCLUSIONES

Un software administrador de red, sirve para hacer más eficiente el desempeño de una red mediante una administración centralizada, desde una estación de control, de donde se configura, instala o repara cualquier dispositivo de red que tenga el agente SNMP, no importando su ubicación.

OpenView es una software administrador de red formado por productos HP diseñados para automatizar la instalación, configuración y monitoreo de una red, logrando que se disminuyan costos como los que implican el traslado de personal a sitios remotos, instalaciones manuales en horarios de servicio y sobre todo, en la rapidez de solución.

Básicamente los requisitos que se necesitan cubrir para instalar OpenView son: tener instalado TCP/IP (cada nodo tiene un IP address único), contar con un protocolo de administración como lo es SNMP; tener un administrador y un agente. Los agentes se instalan en cada nodo de la red que se desee controlar, y los administradores en las estaciones de control desde las cuales se va a realizar la administración centralizada.

Las empresas que en la actualidad tienen instalada esta plataforma de administración son generalmente grandes, es decir con suficientes recursos económicos para comprar equipo sofisticado y software para administrar una red; además tienen que controlar gran número de nodos a distancias considerables, lo cual seria muy difícil sin esta aplicación.

Las tendencias de esta plataforma tienen gran futuro, ya que con el gran avance tecnológico que se esta presentando y debido a la gran competencia entre fabricantes de software y hardware; el equipo y aplicaciones paulatinamente se han ido abaratando, lo cual indica que a corto plazo, empresas medianas y pequeñas tendrán la posibilidad de implementar un software administrador de red.

B I B L I O G R A F I A

REDES DE COMPUTADORAS, INTERNET E INTERREDES
DOUGLAS E. COMER
PRENTICE HALL, PRIMERA EDICION

REDES DE ORDENADORES
ANDREW S TANENBAUM
PRENTICE HALL HISPANOAMERICANA, S. A.

INTEGRATED NETWORK AND SYSTEM MANAGEMENT
HEINZ-GERD HEGERING SEBASTIAN ABECK

NOVELL NETWARE 4.10
MANUAL DE REFERENCIA
TOM SHELDON
MC GRAW HILL