CAPITULO II:

MARCO TEORICO

CAPITULO II

MARCO TEORICO

A.- FUNDAMENTACION TEORICA.

1.- MODELO DE DETECCIÓN.

1.1.- MODELO

"Un modelo es la simulación de un sistema que existe en el mundo real, la creación del modelo pretende una mejor comprensión del prototipo -el sistema que sé este modelando- mediante la revisión o modificación de las características del modelo se pueden establecer inferencias acerca del comportamiento del prototipo, los modelos son en su mayoría representaciones graficas de la realidad". (Bryan Pfaffenberger, 1995, p. 330).

1.2.- DETECCIÓN.

Para el autor Bryan Pfaffenberger (1995, p. 182), “es la capacidad que tiene un programa o aplicación para reconocer un error y realizar una acción predeterminada en respuesta a ese error”.

1.3.- MODELO DE DETECCIÓN.

“Se define como la combinación de componentes, elementos y pasos que interactúan entre sí para detectar cualquier variación y localizar defectos de funcionamientos en cualquier proceso y equipo determinado dentro o fuera de una instalación”. (Díaz J., 1995, p.32).

1.4.- MODELO DE DETECCIÓN DE FALLAS.

Un modelo de detección de fallas, según el autores Inciarte y Fernández; 1997, p.60; “Es el conjunto de componentes (eléctricos) que están interactuando continuamente para detectar cualquier variación de los parámetros, previamente establecidos”.

Una falla, como mal funcionamiento de un equipo o sistema, se refleja como una inoperancia o un rendimiento inferior al estándar, el cual

no puede ser corregido por el operador o por los medios de control, normalmente asequible a el durante la operación rutinaria del equipo. (Renal Tocci, 1989, p. 175).

Por otro lado la detección de fallas se puede dividir en las siguientes etapas:

Detección de fallas: consiste en la observación de operación del equipo y comparación con la esperada respuesta, donde en caso de no existir similitud, se produce la detección de fallas.

Aislamiento de fallas: cuando un equipo falla se debe, generalmente a uno o varios componentes, raramente al daño de todos estos a la vez, por lo cual se realizan pruebas y se llevan a cabo mediciones para determinar donde se encuentra(n) la(s) falla(s).

Corrección de las fallas: se refiere al reemplazo de componentes defectuosos, reparación de conexiones, entre otras.

Según Díaz J. (1995), producir una falla, en ciencia significa, poder anticipar sobre las bases de las explicaciones logradas acerca del comportamiento de los fenómenos, la ocurrencia y modo de manifestarse

de los mismos si se dan determinadas condiciones que se conocen previamente.

Para la prevención de fallas se realizan tres fases:

Toma de datos del equipo: son los parámetros vitales de funcionamiento durante la operación normal del equipo.

Análisis de datos: se procesa la información y se presenta mediante diagramas característicos de condiciones operacionales del equipo.

Diagnostico: con la curva característica de comportamiento se efectúan comparaciones con los parámetros preestablecidos y se determinan las derivaciones y las causas que la originan

1.4.1.- VISOR DE SUCESOS.

En Windows NT, un suceso es una incidencia que debe ser notificada al administrador, los sucesos más importantes aparecen como un mensaje en la pantalla. Los sucesos cuya importancia no es critica para el funcionamiento del sistema quedan registrados para una base de

datos de sucesos, que esta organizada en tres registros de sucesos: Sistema, seguridad y aplicación.

Con el visor de sucesos podemos seleccionar un ordenador del dominio y ver sus registros de sucesos con las opciones sistema, seguridad y aplicación del menú registro.

Cada línea del registro esta formada por:

- Un icono (indica la importancia del suceso).
- La fecha y hora en que se produjo el suceso.
- Él modulo del sistema que se ha generado del suceso.
- La categoría en que se haya clasificado el suceso.
- Él numero de identificación del suceso.
- El usuario que ha generado el suceso.
- El ordenador en que se ha generado el suceso.

El registro mas usado, es del **sistema**, ya que recoge las incidencias del funcionamiento del sistema operativo.

El registro de **seguridad**, es el lugar donde se almacenan los sucesos generados por el sistema de auditoria. El sistema de auditoria se activa desde el administrador de usuario.

El registro de **aplicaciones**, es el lugar donde las aplicaciones del usuario, tales como: Servidor de base de datos y de información, registran sus sucesos de manera de manera que no interfiera con los generados pon el sistema.

Se suelen guardar los registros con un formato propio o como fichero de texto simple o delimitado, quizás un filtro diseñado a medida para la solución de algún problema especifico. Con el visor de sucesos podemos seleccionar el tamaño máximo del registro (en incrementos de 64k) y la forma de vaciar el registro, se puede seleccionar:

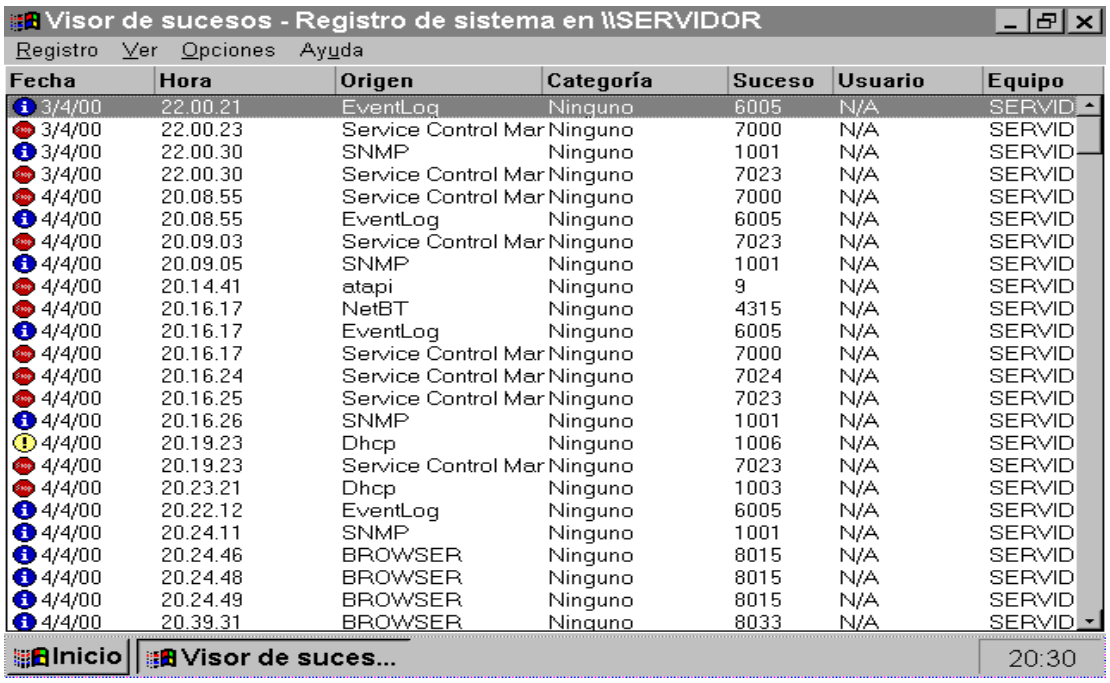
- Que el sistema borre los sucesos según lo necesiten.

- Que borre los sucesos con una cierta antigüedad.

- Obligar al borrador manual. Esta opción se debería seleccionar en sistemas donde la seguridad sea vital para el registro de seguridad.

Figura #1.

Visor de Sucesos



Fuente: Windows NT Server 4.0

1.4.2.- ADMINISTRADOR DE SERVIDORES.

El administrador de servidores, es la herramienta que permite monitorizar el estado de las estaciones de trabajo y servidores de dominio.

El administrador de servidores, muestra una lista de ordenadores de dominio, en ella aparecen:

- El controlador principal del dominio, solo se puede administrar cuando el contador principal de dominio este presente.

- Servidores de dominio, aquellas máquinas que corren Windows NT Server, pero no pueden validar el inicio de sección, suelen dedicarse a tareas difíciles a la gestión de dominio como son: los servidores SQL o de servicios Internet.

- Estaciones de trabajo de dominio, corren Windows NT Workstation y pueden ser administradas desde el administrador de servidores.

- Estaciones de trabajo Windows 95.

- Estaciones de trabajo corriendo otros sistemas operativos.

En la lista de servidores y estaciones de trabajo aparecen dos tipos de máquina, que son:

- Las que pertenecen al dominio.

- Las que no pertenecen al dominio.

En el resumen, aparecen los siguientes datos:

- Archivos abiertos.

- Bloqueo de archivos.

- Canalizaciones abiertas.

- Usuarios (todos los usuarios conectados al servidor).

- Recursos compartidos (permite ver los recursos compartidos de ese servidor, incluso los que se han compartido en modo administrativo).

- En uso (nos lleva al cuadro de diálogo de recursos abiertos, que nos indica para cada recurso, el usuario que ha abierto su estado de bloqueo y la ruta).

- Duplicación (nos lleva al cuadro de duplicación de directorios).

- Alertas (permite seleccionar a los usuarios que recibirán las alertas administrativas provocadas por la estación o el servidor NT.

1.4.3.- ADMINISTRADOR DE DISCO.

El administrador de disco es una herramienta administrativa que permite gestionar los discos y partición de los mismos en NT.

El sistema de archivo de NT soporta tres tipos de particiones:

El sistema de ficheros FAT: Es el sistema de fichero que utilizan MSDOS y Windows, tiene grandes limitaciones, aunque es fácil de reparar con herramientas estándar, toma su nombre de la tabla de asignación de ficheros (File Allocation Table).

El sistema de ficheros HPFS: este sistema se usa en OS/2, a NT permite convertir este tipo de partición en NTFS.

El sistema de ficheros NTFS: ficheros de nueva tecnología (New Technology File System) y soporta un gran numero de características avanzadas sobre los sistemas anteriores:

- Nombres de ficheros largos.
- Atributos extendidos en los ficheros.
- Seguridad y auditoria sobre ficheros y directores.
- Gran capacidad de ficheros y particiones.
- Tolerancia a fallos del sistema de ficheros.
- Optimización general de todos los accesos a los ficheros y directorios.

Este sistema de ficheros no es visible cuando la maquina arranca en modo MSDOS introduce muchos cambios respecto a FAT. La tabla de

asignación de ficheros FAT ha sido sustituida por una nueva estructura llamada Tabla de ficheros maestra (Master File Table).

El sistema de organización de un volumen NTFS esta ligeramente orientado a objetos. Todos los sectores de un volumen pertenecen a un fichero, incluyendo aquellos que contienen la organización del volumen.

1.4.4.- TOLERANCIA A FALLOS EN EL SERVIDOR WINDOWS NT.

La tolerancia a fallos, se refiere a la protección de los sistemas frente a fallos potenciales de hardware, desastre, infecciones por virus, ataques de piratas y otros riesgos. Protege datos creando copias redundantes, usualmente en tiempo real, así como copiando en sistema de cinta magnética o en disco óptico.

Se pueden usar algunos de los métodos para proteger los datos:

- Reflejado de disco.

- Conjunto de bandas para disco con paridad.

- Copias de seguridad en cinta con archivos en localizaciones remotas.

- Alimentación de copias de seguridad.

1.4.4.1.- SERVICIOS DE DIRECTORIOS.

La raíz de esta característica de diseño se llama Servicios de Directorio de Windows NT. Los usuarios de directores se conservan en controladores principales de dominio (PDC; Primary Domain Controller), el cual es la base de datos maestra de usuarios, grupo o información de recursos para el dominio. También permite designar controladores de respaldo de dominio (BDC; Backup Domain Controller), los cuales se localizan comúnmente en servidores adicionales dentro del dominio.

Para copiar la información en los PDC, en los diversos BDC en el dominio, toda o parte puede copiarse a cada BDC y una vez establecida, la actualización de los BDC es automática. El caso de controladores primario y de respaldo significa que la tarea de autentificar a los usuarios en una red muy usada no crea un cuello de botella en un servidor, también si el PDC no esta disponible por alguna razón puede promover uno de los BDC a la categoría de PDC con el clip de un botón.

1.4.4.2.- ESPEJO DE DISCO.

Es una tecnología usada en sistema o con datos críticos, cuando se pone en practica se usan particiones en dos unidades separadas para almacenar información idéntica. La información que se graba en la partición del disco primario también se graba en la partición reflejada otro disco, si un disco falla, el sistema puede usar los datos del otro disco.

El Windows NT Server soporta el espejo de disco como una manera de poner en practica la tolerancia a las fallas. El espejo de disco es transparente para todos los programas y usuarios en un dominio cuando establezca un espejo de disco las dos particiones usadas deben residir en unidades de disco físicamente diferentes. Sin embargo no hay necesidad de usar controladores de disco separados para dos unidades, aunque tiene dos facetas:

- Si tiene dos contadores tiene redundancia adicional. Por lo tanto, si uno de sus controladores de unidad de disco duro falla, todavía puede tener acceso a sus datos.

- Usar dos controladores le permite tener un acceso al disco, más rápido que al usar uno, el espejo de disco significa en realidad que los datos

deben grabarse dos veces, cada vez que se tiene acceso a la unidad. Si usa un controlador, esto significa el doble el doble de tiempo de grabación, debido a que le controlador sólo puede procesar una solicitud a la vez, en cambio si usa dos controladores entonces la grabación puede ocurrir de manera simultánea.

1.4.4.3- FRANJAS DE DISCO.

"Es una tecnología similar al espejo de disco, en cierta forma, pero con una diferencia fundamental, las franjas de disco se basan en la grabación de la información en particiones de diferentes discos, pero la información grabada no se refleja, se divide en franjas. Esto significa que sus datos se dividen en bloques y luego se separan en el número de unidades que se especifique".

1.4.4.4.- SEGURIDAD MEDIANTE LA DUPLICACIÓN DEL DIRECTORIO.

"Es una estrategia tolerante a fallos, para duplicar datos en tiempo real desde un servidor Windows NT y otra computadora, se pueden duplicar datos con propósito de copias de seguridad o para hacer más fácil a las personas situadas en localizaciones remotas, acceder a los datos".

El servidor de Windows NT que almacena los datos maestros se llama Servidor Exportador, sus datos se duplican en los servidores importados.

La duplicación se usa de la siguiente manera:

- Los datos maestros del servidor exportador están en la misma LAN de los administradores o usuarios que actualizan la información. La LAN proporciona un vínculo de alta eficiencia para el transporte de datos.

  - Un servidor importador en la LAN local actúa como dispositivo de copia de seguridad. Importa datos y los almacena en una localización diferente para protegerlos de desastres locales.

  - Los servidores importados pueden también estar en localizaciones remotas y sucursales para suministrar datos a usuarios en esos sitios. Los usuarios pueden acceder a los datos maestros sobre un enlace WAN. En el segundo caso, los usuarios de la LAN local pueden acceder tanto a la computadora exportadora como a la importadora. Esto permite balancear la carga. En el tercer caso, la duplicación de datos en las sucursales periódicamente utilizan

menos ancho de banda de transmisión que si los usuarios tuvieran que acceder sobre un enlace WAN.

La duplicación ocurre automáticamente a medida que los archivos se añaden al directorio maestro o que se actualizan. Es necesario mantener solo la copia maestra de la información, la cual puede ser exportada a múltiple computadoras importadoras.

1.5.- MODELO DE DETECCIÓN DE RENDIMIENTO.

Consiste en medir y hacer disponibles diferentes aspectos del desempeño total de la interred, de tal manera que se pueda mantener en un nivel aceptable.

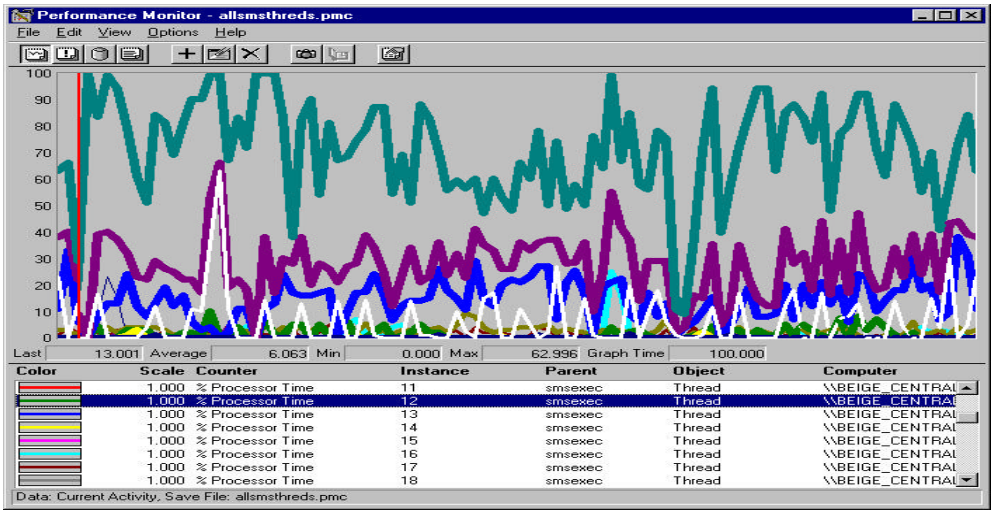
1.5.1.- MONITOR DEL SISTEMA (PERFORMANCE MONITOR).

"El monitor del sistema, es la herramienta que permite ver el estado del sistema, esta herramienta permite generar gráficos a tiempo real del estado de funcionamiento de los diversos componentes del sistema, así como hacer un seguimiento de estos componentes, obteniendo informes e

incluso lanzando aplicaciones en respuestas a determinadas condiciones, hasta incluso encuentra cuellos de botella que enletecen el funcionamiento del sistema; los elementos de monitorización que permiten crear el monitor del sistema son de cuatro tipos: gráficos, alertas, registros e informes. (www.cyberrecursos.net).

Figura #2.

Monitor de Sistema (Performance Monitor)



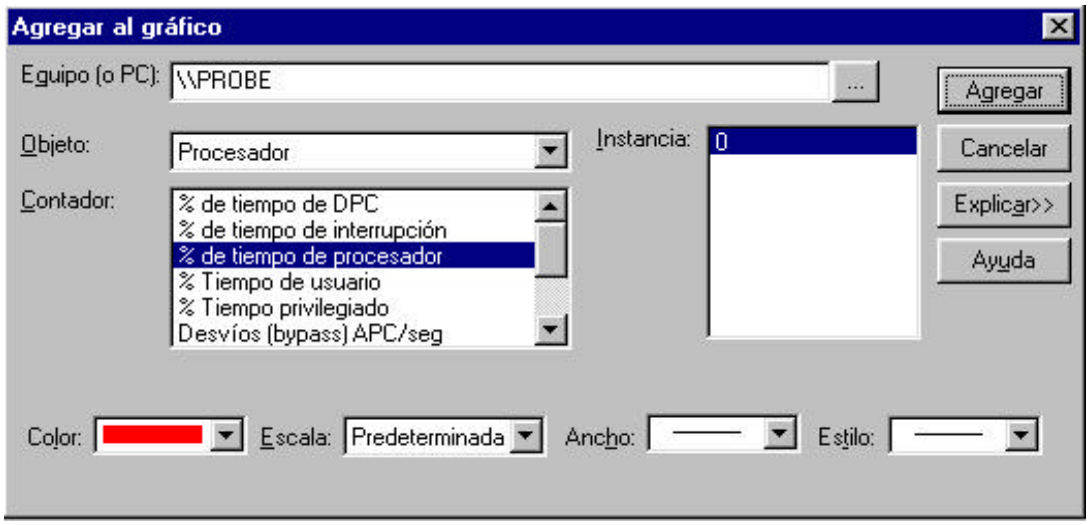
Fuente: Windows NT Server 4.0

1.5.1.1.- FUNCIONAMIENTO DEL MONITOR DEL SISTEMA.

Cada uno de los objetos del sistema operativo contiene una serie de contadores que permiten conocer el estado de actividad del objeto. Para algunos de estos objetos, los contadores deben ser activados antes de ejecutar el monitor del sistema. Un ejemplo seria las unidades de disco físicas, los procesadores, la memoria física y la cache, entre otros; que incluyen los componentes del sistema de red.

Figura #3.

Funcionamiento del monitor de Sistema



Fuente: Windows NT Server 4.0

GRAFICOS:

El primer método para visualizar los contadores de un objeto es el grafico, en este se representa cada uno de los contadores o valores como líneas de colores o barras de histograma.

En primer lugar se debe elegir el ordenador que se va a monitorizar, esto permite visualizar varios contadores procedentes de diferentes ordenadores, luego se elige el tipo de objeto. Los tipos por defectos pueden ser: archivos de paginación, cache, disco físico, disco lógico, examinador, memoria, objetos, procesador, procesos, redirector, servidor, sistema e hilos (Threads).

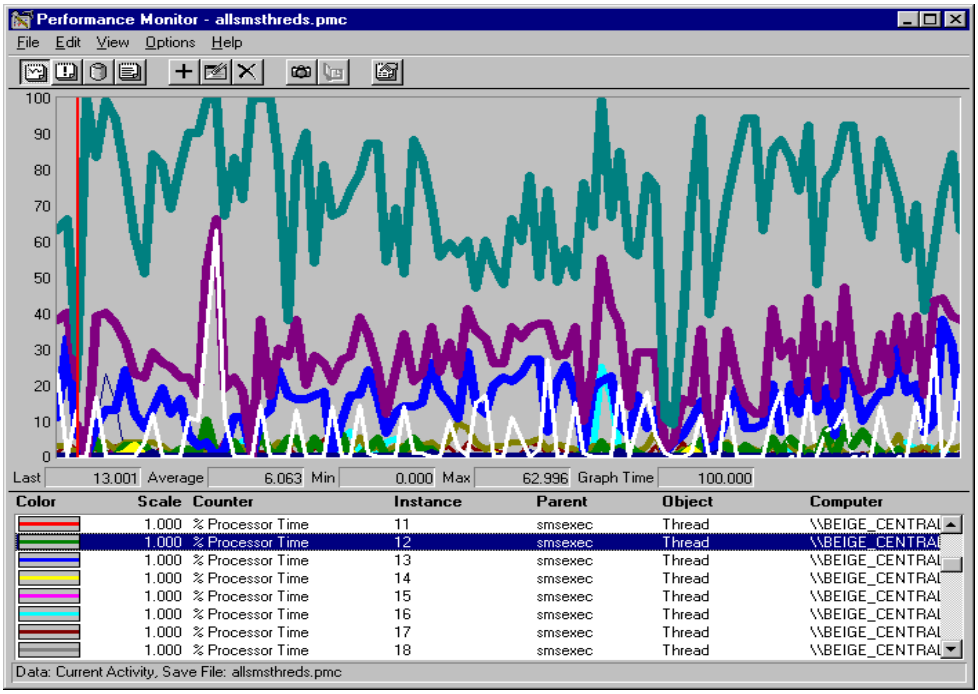
Algunos de estos objetos poseen mas de una instancia, por ejemplo el disco físico y lógico, podemos tener varios discos o particiones para el caso de procesos e hilos; las instancias que aparecen dependen de que aplicaciones sé estén ejecutando en el sistema, para cada uno de los objetos podemos seleccionar cualquiera de los contadores que posee, luego elegir la apariencia del contador en el grafico (color, escala, ancho, estilo), aunque el monitor del sistema elige valores por defecto como

también, se puede elegir si necesita leyendas, barra de valores, tipo de gráfico (líneas, histograma, barras verticales).

El gráfico posee dos nodos de actualización automática con posibilidad de elegir el intervalo de actualización en fracciones de segundo, o manual, cada vez que se elige el menú.

Figura #4.

Gráficos



Fuente: Windows NT Server 4.0

ALERTAS:

Las alertas permiten monitorizar contadores específicos de manera que se produzca una alerta al sobre pararse por exceso o defecto un cierto valor asignado a un contador.

Primero se elige el ordenador, al igual que se hizo para el gráfico; después se elige el contador y la instancia de un modo analógico, se elige el color que sé a de identificar la alerta y el valor que la desencadena. Se introduce el valor de opción " ALERTA SI" y luego se selecciona si es limite superior o inferior.

Además se puede elegir la opción para ejecutar un programa la primera vez que se presente o se produzca la alerta, o en su defecto que se añada la alerta al registro de aplicaciones del sistema, o que se envié un mensaje de red al nombre de red especificado, de otra manera, se puede elegir el tipo de actualización manual o automática.

Figura #5.

Alertas

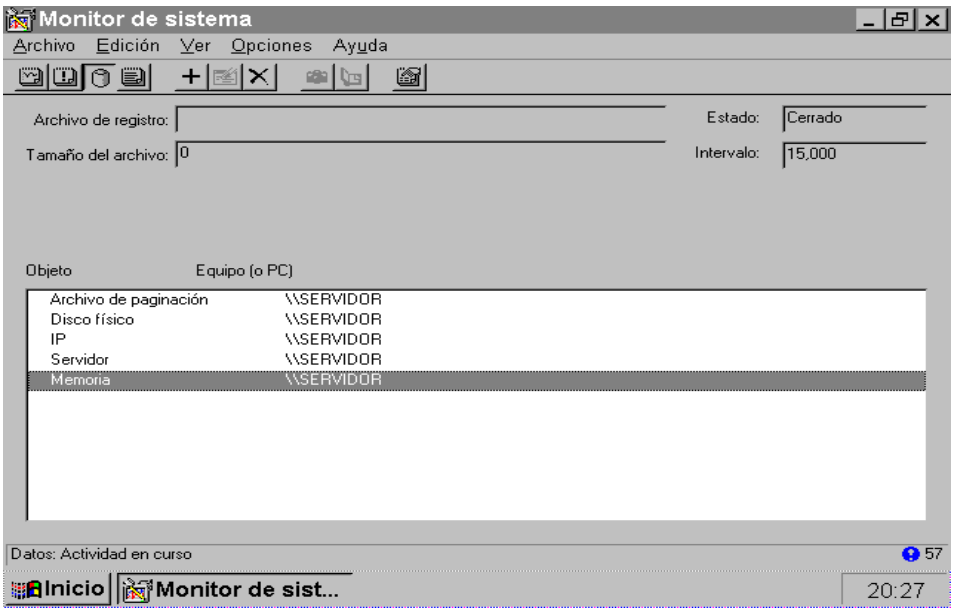
Fuente: Windows NT Server 4.0

REGISTRO:

Permite recoger la información de los diferentes contadores seleccionados llevándolos sobre un archivo de registro (. Log) mediante el menú "EDICIÓN / AGREGAR AL REGISTRO", en esta opción también se puede elegir el ordenador y el objeto a monitorizar.

Figura #6.

Registros



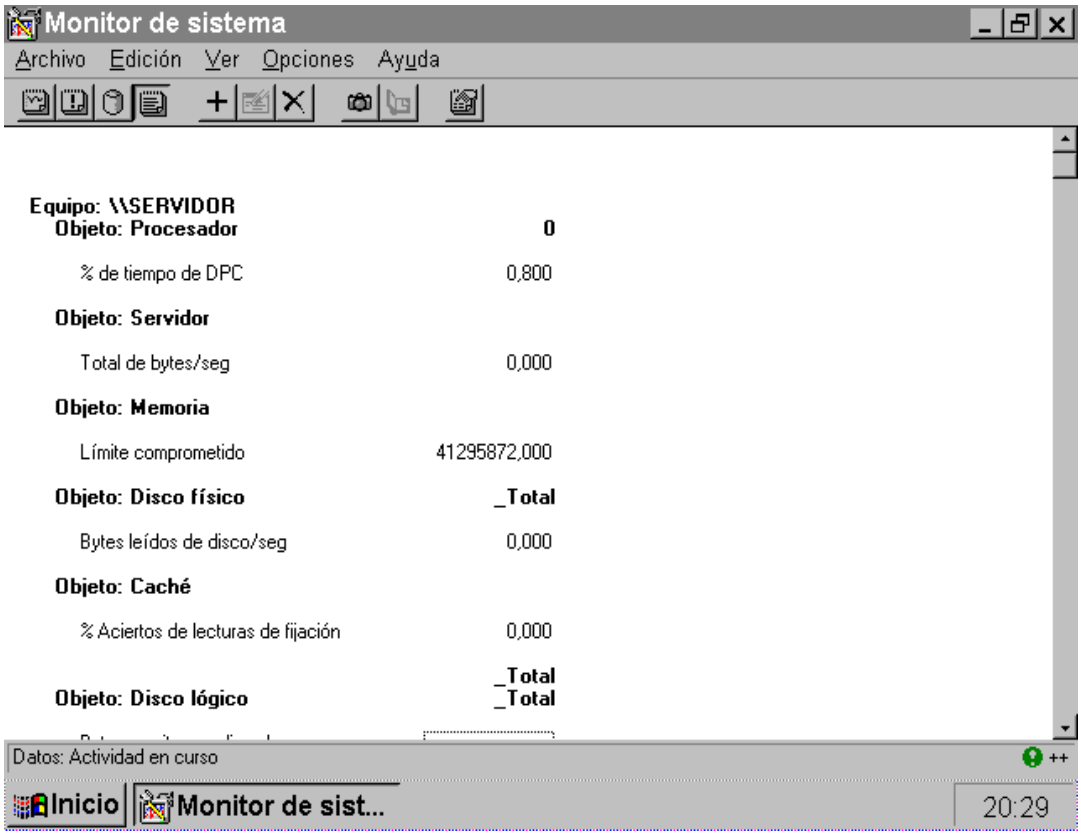
Fuente: Windows NT Server 4.0

INFORMES:

Permiten recoger la información de los contadores de cada tipo de objeto para poder ser representados de una forma textual, trabajando de una forma muy parecida a los gráficos, salvo que la información recogida aparezca en una ventana de texto.

Figura #7.

Informes



1.5.2.- ALERTAS DE SEGURIDAD.

Se utiliza con el monitor del monitor del sistema para alertar algunos sucesos como:

- **Errores de permisos en los accesos:** el numero de veces que e cliente intenta, pero falla, al abrir un archivo y recibe un mensaje de "STATUS-ACCESS DENIED", esta alerta puede indicar si alguien esta intentando aleatoriamente acceder a archivos esperando encontrar a algunos desprotegidos.

- **Errores de accesos concedidos:** el número de veces que los accesos a archivos abiertos con éxito fueron denegados, esto puede indicar los intentos de acceder a archivos sin accesos de autorización adecuado

- **Errores de inicio de sección:** el número de elementos de inicio de sección de fallidos en el servidor adivina los programas que traten de violar la seguridad en el servidor.

1.5.3.- MONITORIZACIÓN DE LA RED.

La utilidad del monitor de red, permite monitorizar el trafico de red de una computadora, solo puede utilizarse par rastrear paquetes de información que son enviados o recibidos por la computadora donde se esta ejecutando el programa.

El monitor de red es una herramienta de diagnóstico para visualizar redes de área local, localizar un servidor apagado o localizar cuellos de botella en la red. Suministra una presentación gráfica de estadísticas de red.

La presentación del monitor a simple vista parece confusa pero ella esta divida en cuatro ventanas distintas, cada una con la siguiente información:

- Información sobre el host que ha enviado una trama por la red.

- Información sobre el host que ha recibido la trama.

- Los protocolos utilizados para enviar la trama.

- Los datos o una porción del mensaje enviado.

La dirección es un numero hexadecimal único (Base 16) que identifica a una computadora en la red; Es la dirección hardware predefinida, asignada a cada tarjeta de interfaz de red.

El monitor de red utiliza un proceso “CAPTURADO” para recoger información sobre la red durante un periodo de tiempo, durante ese periodo, la información sobre todas las tramas transmitidas por la red, es registrada y esta disponible en la ventana del monitor de red. Se puede visualizar de forma grafica o guardarla en archivos para verla luego.

Cuando se captura la información puede configurarse filtros para ver solo la información esencial y así poder detectar intrusos u otros problemas, hasta cuatro parejas de direcciones especificas pueden ser monitorizadas. Una pareja de direcciones incluye las direcciones de las computadoras que se comunican entre sí, también puede configurar disparadores que empiecen una acción prediseñada cuando un suceso ocurre en la red, cuando el espacio de buffer esta casi finalizado o cuando las tramas podrían ser corrompidas.

Puede utilizar servicios del agente del monitor de la red en otras computadoras, Windows NT para así, poder capturar en ellas estadísticas y enviarlas a la computadora de monitor de red.

Para proteger a una red de usos no autorizados del monitor de red, este utiliza protecciones de contraseña y la posibilidad de detectar otras instalaciones de monitor de red en el segmento local de las mismas. La contraseña puede evitar que alguien en el servidor de Windows NT que ejecute el servidor de administración del sistema, se conecte con la computadora y ejecute el monitor de red en ella.

Si otro usuario ejecuta una copia del monitor de red en sus computadoras, podrían hacerlo para vigilar paquetes en la red y capturar información valiosa. El monitor de red detectara otras instalaciones y mostrara la información sobre ellas, con el nombre de la computadora del usuario, la dirección del adaptador, y si la actividad esta ejecutando, capturando o transmitiendo la información.

Desafortunadamente, el monitor de red solo puede detectar la existencia de otra versión del monitor de red, es decir, no puede detectar otro software y/o equipos de monitorización de terceros vendedores.

2.- GESTION DE RED.

2.1.- COMPONENTES DE UN SISTEMA DE GESTION.

Según el autor David J. (1995), “los componentes de un sistema de gestión son los diferentes dispositivos tanto físico como lógicos, que están conectados a la red”, como son los siguientes:

- **Interfaz de usuario:**

Es la interfaz entre el usuario y el sistema y puede ser en modo, carácter o grafico.

- **Base de datos:**

Una base de datos mantiene cualquier información de la red a través de descripciones de diferentes parámetros, configuración de contadores, almacenando el histórico de eventos y permitiendo la realización de seguimiento.

- **Programa monitor:**

Su finalidad es supervisa las condiciones actuales y permite la inspección futura. Visualiza las alarmas activadas por los agentes, y realiza actualizaciones medianotes sondeos regulares.

- **Arranque y configuración:**

Comprueba que cada estación pueda hacer atendida enviándole los parámetros actuales de configuración y el equipamiento lógico de arranque.

- **Protocolo de gestión:**

Controla las operaciones de gestión entre el gestor y el agente.

2.2.- FUNCIONALIDADES BASICAS DEL SISTEMA DE GESTION.

Las funciones básicas que contempla un sistema de gestión, dependen del tipo de red donde se utilice. A continuación se explica:

Gestión de Redes Pequeñas.

Son redes con pocos usuarios, con un numero de dispositivos de red bajo, es suficiente con un sistema de gestión que ofrezca las funciones básicas de supervisión, entre las que se pueden destacar:

- Supervisión y presentación en tiempo real de los componentes individuales de la red.

- Presentación de la información de la configuración.

- Representación grafica de los nodos instalados en la red.

- Indicación del estado de los componentes individuales (cuales están activos y cuales inactivos).

- En caso de avería indicación del tipo de esta.

- Notificación automática de errores.

- Posibilidad de acceso automático a los elementos de la red desde la consola de gestión de red.

- Filtrado de alarmas.

- Supervisión y determinación de los valores de rendimiento para la totalidad de la red, así como en los diversos componentes de la red.

- Modificación de la configuración de la red y establecimiento de los derechos de acceso a los diversos sistemas.

- Aislamiento de errores de equipo físico respecto a los errores de equipo lógico.

Gestión de Redes Medianas y Grandes

Son redes de mayor complejidad, necesarias para las funciones de gestión más avanzadas. Al estar formadas por diferentes tipos de redes, con diferentes protocolos y con elementos de diversos fabricantes. A las funciones descritas anteriormente hay que añadir las siguientes:

- Capacidad de supervisar el rendimiento y generar estadísticas dando una valoración de los resultados.

- Evitar averías, perdidas de rendimiento y problemas de configuración mediante políticas de gestión preventivas.

- Recuperación automática ante fallos.

- Proveer el mecanismo avanzado para la seguridad de la red y de los datos.

- Capacidad para representar gráficamente en tiempo real la totalidad de la red, parte de la misma, o el sistema, conectados en cada punto, de forma que la gestión no se convierta en una tarea excesivamente compleja.

- Capacidad para supervisar desde una única estación la totalidad de los tipos de red que puedan existir (Ethernet, Token King, FDDI, entre otros.

- Posibilidad de intercomunicación local y remota con cualquier elemento de la red.

- Proporcionar interfaces con otros entornos.

- Recogida y análisis de datos de gestión.

- Escalabilidad del sistema de gestión para responder adecuadamente al crecimiento de la red.

- Capacidad para integrar equipos de múltiples fabricantes y que soportan diversos protocolos.

2.3.- ARQUITECTURAS DE GESTION DE RED.

Según la Organización Internacional de Standarizacion (International Organitazation for Standarizacion-ISO), las tres principales arquitecturas de gestión de red son las siguientes:

2.3.1.- Modelo OSI (Open Systems Interconnection, Interconexión de Sistemas Abiertos).

Fue desarrollado en 1.984 por la ISO, el modelo OSI (Open Systems Interconnection), el cual es un modelo conceptual compuesto de siete capas que describe como se transfiere la información desde una aplicación de software de una computadora a través de un medio de transmisión, hasta una aplicación de software en otra computadora. Este modelo es considerado como la principal arquitectura conceptual para la comunicación entre computadoras. Pero así como la ISO, ha contribuido en gran medida a la estandarización de las redes, también se ha pronunciado y con relación a la gestión de redes, planteando un modelo que permite comprender las funciones principales del sistema de gestión de redes.

Están divididas en cinco categorías de servicios de gestión denominadas Áreas funcionales Especificas de Gestión (SMFA), estas categorías son:

1.- GESTION DE CONFIGURACION:

El área funcional de la gestión de configuración incluye al conjunto de facilidades pensadas para la realización de los cincos grupos de actividades siguientes:

- Construcción de la topología de la red de acuerdo a la visión del usuario Establecimiento de los parámetros de funcionamiento, es decir inicialización y modificación de la configuración de todo el recurso de red.

- Mantenimiento de un inventario de los dispositivos instalados y de las líneas que los conecta.

- Administración de la correspondencia entre nombres de dispositivos y sus direcciones de red para que los usuarios manejen los recursos según su visión de la red.

- Gestión racional de los cambios de configuración.

El objetivo de la gestión de la configuración es controlar la información que describe las características físicas y lógicas de los recursos de la red, así como las relaciones entre dichos recurso. Cada componente de la red tiene una amplia gama de información respecto a su marca, modelo, capacidad, versión, velocidad, seriales, entre otros, que son almacenados en una base de datos controlado por él modulo de gestión de la configuración.

2.- GESTION DE FALLOS:

La gestión de fallos y recuperación comprende el conjunto de facilidades que permiten la detección, el aislamiento y la corrección de las operaciones anormales de las redes o sistema de comunicaciones. Esta función en general comprende el conjunto de actividades orientadas a detectar, diagnosticar, anular, reparar e informar sobre los fallos de los equipos que componen las redes y los servicios de telecomunicación utilizados.

Un fallo en la red, trae como consecuencia que el usuario no pueda utilizar algún servicio, por lo que es deseable su pronta detección y

resolución. Es necesario distinguir entre fallos y errores. Un fallo indica que algo no funciona y es necesario repararlo mediante una intervención. Un error en cambio puede ser un suceso aislado, como un error de paridad, que no representa necesariamente un problema. En términos generales cuando él numero de errores con la misma causa supera un cierto umbral da lugar a un fallo.

Según se desprende de diversidad de informes presentados por secciones, departamentos y divisiones referentes a los dispositivos causantes de fallos del sistema de comunicaciones, por lo general, señalan con una frecuencia casi sistemática:

- Líneas de comunicaciones
- Terminales
- Ordenadores centrales
- MODEM Procesadores de comunicaciones
- Otros componentes

De allí que, como consecuencia de lo antes indicado, se afirma que en las redes, la disponibilidad de los servicios de comunicaciones puede ser mejorada por los sistemas acciones:

- Aumento de la disponibilidad de cada sistema o componente aislado.

- Disminución del numero de componentes en serie en todas las partes de la red.

- Añadido de componentes redundantes.

Por lo tanto, la actividad de gestión de fallos requiere la disponibilidad de procedimientos para los fines siguientes:

- Detención y notificación de errores y fallos, se generan alarmas para indicar el mal funcionamiento.

- Registro de errores, normalmente los eventos generados en los recursos gestionados se almacenan en una base de datos.

- Examen y recuperación de errores.

- Ejecución de procesos de diagnósticos y de seguimiento de fallo. En los sistemas de gestión se dispone de recursos para poder llevar a cabo las pruebas necesarias para la realización del diagnostico.

- Control y seguimiento de la resolución de los fallos, para ellos suelen disponer de los boletines de averías.

Dado que, anteriormente se hizo referencia a esta próxima consideración, alerta la presente investigación que un boletín de avería es un documento informativo que tiene existencia mientras dura el fallo. Por lo que, para una buena gestión de los boletines de avería es indispensable tener una buena calidad de servicios. De esta forma, es como la base de datos histórica de boletines de avería que ayuda a identificar las partes más débiles de las redes, y por tanto, proporciona información muy valiosa para las nuevas adquisiciones de equipos para así seleccionar aquellos más fiables con mejor servicio.

En consecuencia, una falla puede ser originada por:

- Degradación del desempeño de algún componente de la red, sobrepasando el umbral establecido.

- Presencia de algún evento controlado o inesperado.

- Intervención planificada o inesperada de algún individuo.

Del mismo modo, se quiere detectar que la gestión de fallas se lleva a cabo en los siguientes pasos:

- Detectar o recibir notificación del problema.

- Registrar el problema y posteriormente solucionarlo.

- Diagnosticar y valorar el problema.

- Resolver o aislar el problema.

3.- GESTION DE RENDIMIENTO:

El objetivo de esta gestión, es medir y hacer disponibles diferentes aspectos del desempeño de la red para que el desempeño total del interés se pueda mantener a un nivel aceptable. Entre las actividades que se incluyen en una gestión de rendimiento se encuentra: el monitoreo del tiempo de respuesta de los sistemas (hardware y software), la medición de

los recursos disponibles, la sintonía, rastreo y control del rendimiento de la red.

Esta área funcional comprende el conjunto de funciones destinadas a la obtención de información para conocer en todo momento el grado de utilización del recurso de la red, el nivel de cumplimiento de servicio a los usuarios; en principio podemos pensar que tanto el grado como el nivel pueden tomar valores altos o bajos.

La recogida de estadísticas acerca del trafico de los elementos de red, es el método más empleado para calcular y conocer acerca del grado de utilización del recurso de la red, estas estadística se deben guardar en base de datos históricos para poder disponer de la historia de la red, como también el crecimiento del trafico con el objeto de realizar ampliaciones.

4.- GESTION DE CONTABILIDAD.

Tiene como propósito medir los parámetros de la utilización de la red, para el uso de la misma, por parte de los individuos o los grupos, para que pueda regularse de manera adecuada, como también proporciona las herramientas necesarias para mantener informados a los usuarios de la red de la utilización realizada de los recursos.

Los procedimientos destinados en caso de empresas que prestan servicios comerciales son importantes ya que:

- La facturación a los usuarios finales es el fin ultimo de los mismos.

- La implementación del cargo o no, en una red depende de la organización de la corporación.

- La nota del cargo o factura en los sistemas comerciales no debería ser tan compleja que haga difícil su compresión y administración.

- Los usuarios necesitan estar bien informados de las políticas o metodologías seguidas para él calculo de los cargos.

- Regula los parámetros de la utilización de la red, con dicha regulación se reducen los problemas de la red, ya que los recursos de la misma pueden dividirse en cantidades iguales dependiendo de las capacidades de los recursos y se hace mas justo el acceso a la red para todos los usuarios.

5.- GESTION DE SEGURIDAD.

En todos los casos, existen varias formas de abordar la seguridad de un sistema, un punto de vista es entenderla como una forma de prevenir futuras perdidas, o una manera de gestionar los riegos relacionados con la tecnología. Otros consideran que es algo necesario para evitar que usuarios maliciosos entren en el sistema parte de las diferencias que puedan existir entre ambas concepciones, podemos encontrar una definición mas o menos rigurosa para este concepto dentro de los sistemas de ordenadores:

Según el autor David J. (1995), “la seguridad en sistemas de ordenadores es la protección de la integridad, disponibilidad y si es necesario la confidencialidad de la información y recursos que se usan, para la entrada de almacenamiento, proceso y comunicación de los mismos”.

Para una organización con gran numero de diversidad de equipos, la gestión de todos ellos se traduce en la necesidad de tener varios sistemas de gestión diferentes, la operación y control de una red con gran numero de sistemas de gestión puede llegar a ser una tarea muy compleja por lo que las organizaciones requieren sistemas de gestión integrados para controlar todos los recursos de comunicaciones.

2.3.2.- Modelo TMN (Telecomunications Management Network, Gestión de Redes de Telecomunicaciones).

A diferencia del modelo OSI, en el cual se definen cinco áreas funcionales, el estándar TMN no entra en consideraciones sobre las aplicaciones de la información gestionada. Por el contrario, se define la siguiente funcionalidad:

- El intercambio de información entre la red gestionada y la red TMN.
- El intercambio de información entre redes TMN.
- La conversión de formatos de información para un intercambio consistente de información.
- La transferencia de información de gestión y la capacidad de actuar en función de ella.

- La manipulación y presentación de la información de gestión en un formato útil para el usuario de la misma.

- El control del acceso a la información de gestión por los usuarios autorizados.

El modelo TMN define tres arquitecturas diferenciadas:

Arquitectura funcional, que describe la distribución de la funcionalidad dentro de la TMN, con el objeto de definir los bloques funcionales a partir de los cuales se construye la TMN. Se definen cinco tipos de bloques funcionales, estos bloques proporcionan la funcionalidad que permite a la TMN realizar sus funciones de gestión. A continuación se describen los distintos tipos de bloques funcionales:

- **Función de operación de sistemas (OSF):** procesan la información relativa a la gestión de la red con el objeto de monitorizar y controlar las funciones de gestión.

- **Función de estación de trabajo (WSF):** este bloque funcional proporciona los mecanismos para que un usuario pueda interactuar con la información gestionada por la TMN.

- **Función de elemento de red (NEF):** Es el bloque que actúa como agente, susceptible a ser monitorizado y controlado. Estos bloques proporcionan las funciones de intercambio de datos entre los usuarios de la red de telecomunicaciones gestionadas.

- **Adaptadores Q (QAF):** este tipo de bloque funcional se utiliza a la TMN aquellas entidades que no soportan los puntos de referencia estandarizados por TMN.

- **Función de medición (MF):** se encarga de garantizar que la información intercambiada entre los bloques de tipo OSF o NEF cumple los requisitos demandados por cada uno de ellos.

Arquitectura física, que describe las interfaces y el modo en que los bloques funcionales se implementan en equipos físicos. Se encarga de definir como se implementan los bloques funcionales mediante equipamiento físico y los puntos de referencia en interfaces. En la arquitectura física se definen los siguientes bloques constructivos:

- Elementos de red (NE)

- Dispositivo de medición (MD)

- Adaptador Q (QA)

- Sistema de operaciones (OS)

- Red de comunicación de datos (DCN)

Arquitectura lógica de niveles, pretenden abordar la gran complejidad de la gestión de redes de telecomunicaciones. Cada uno de estos niveles agrupa un conjunto de funciones de gestión que son:

- **Nivel de elementos de red:** incluye las funciones que proporcionan información en formato TMN del equipamiento de red así como las funciones de adaptación para proporcionar interfaces TMN a elementos de red.

- **Nivel de gestión de elementos:** incluye la gestión remota o individual de cualquier elemento de red que se precise para el establecimiento de conexiones entre dos puntos finales par proporcionar un servicio dado.

- **Nivel de gestión de red:** incluye el control, supervisión, coordinación y configuración de grupos de elementos de red constituyendo redes y subredes para la realización de una conexión.

- **Nivel de gestión de servicios:** incluyen las funciones que proporcionan un manejo eficiente de las conexiones entre los puntos finales de la red, asegurando un optimo aprovisionamiento de los servicios prestados a los usuarios.

- **Nivel de gestión de negocio:** incluye la completa gestión de la explotación de la red, incluyendo contabilidad, gestión y administración, basándose en las entradas procedentes de los niveles de gestión de servicios y de gestión de red.

2.4.- PROTOCOLOS DE COMUNICACIÓN PARA LA GESTION DE RED.

2.4.1.- SNMP (Simple Network Management Protocol, Protocolo Simple de Gestión de Red).

El organismo que administra y regula la red Internet encargó en 1987, a un grupo técnico (que se encarga de encontrar soluciones a los problemas técnicos que plantea el funcionamiento de la red), una solución de gestión integrada para dicha red.

Este grupo técnico propuso una solución en dos tiempos:

- Utilizar un único protocolo capaz de ser entendido por todos los dispositivos de la red, como solución provisional a corto plazo (SNMP)

- Posteriormente cuando estuvieran desarrolladas las normas OSI, utilizar los protocolos de gestión OSI soportados sobre la plataforma de comunicaciones de Internet. Esta solución se conoce como CMOT (CMIT sobre TCP/IP)

En 1988 se implanto y comenzó a utilizarse un protocolo de gestión denominado SNMP (Simple Network Management Protocol), un protocolo sencillo para la gestión de red. Este protocolo ha sido muy aceptado

desde entonces y la mayoría de los fabricantes lo implementan en sus equipos con protocolos TCP/IP.

Sin embargo, la segunda estrategia no ha avanzado lo suficiente, debido quizá a la falta de estabilidad de las normas OSI de gestión por lo que muy pocos fabricantes ofrecen esta solución para Gestión.

Actualmente, la gestión SNMP es un directo competidor de la Gestión OSI y se siguen definiendo normas para la gestión SNMP. La ultima implementación del protocolo SNMP es la norma SNMP3, que actualmente esta en la fase de pruebas y desarrollo.

Los elementos que conforman el SNMP son:

SNMP consta de tres elementos o partes: el manager o administrador, el agente y el MIB (Management Information Base, Base de Información de Gestión)

- **Manager:**

Es un modo que activamente participa en la administración de una red. Solicita e interpreta datos acerca de dispositivos de red y trafico, y

típicamente interactúa con los usuarios para llevar a cabo sus intenciones. Un administrador puede provocar cambios en un agente alterando el valor de una variable en el nodo agente. Los administradores o manager son frecuentemente implementados como aplicaciones de red.

El manager es localizado en el host principal de la red. Su principal función es encuestar a los agentes acerca de cierta información solicitada. Existe mucho software compatible, por ejemplo para PC's Netguard y sobre UNIX el HP Open View.

- **Agent:**

Un agente SNMP es un software que reside en un nodo de red y es responsable de comunicarse con el manager o administradores considerando el nodo. El nodo es representado como un objeto administrado teniendo varios campos o variables que están definidas en el MIB apropiado.

El agente tiene dos propósitos:

- Responder a las solicitudes del manager, suministrando o cambiando los valores de las variables de los objetos según se solicitaron.

- Generar traps para alertar al manager de los eventos notables que ocurren en el nodo, tales como una falla en un componente.

El agente corre en cada nodo de la red. Colecciona información de red y terminal como este especificado en el MIB.

No todos los dispositivos soportan SNMP directamente. Los dispositivos que no lo hacen pueden tener un apoderado que les traduzca entre SNMP y el mismo. Si se tiene cargado SNMP bajo TCP/IP, entonces la computadora será considerada como si tuviera un agente SNMP en ella.

Interacción entre manager y agente:

El manager se comunica con el agente por mensajes de SNMP los cuales están en forma de solicitudes. El manager no necesita saber ningún detalle interno acerca del objeto administrado por el agente.

Además, un agente SNMP puede servir solicitudes de muchos administradores SNMP. El agente no necesita saber el contenido de la solicitud o la estructura del manager que esta haciendo la solicitud. El agente valida la solicitud, los servicios, y entera el estado pasivo, esperando la solicitud. Esta división de responsabilidades simplifica las soluciones de administración de red.

Traps:

Generalmente, el manager solicita información del agente y este responde. Sin embargo, es posible para un agente emitir mensajes sin una correspondiente solicitud. Tal mensaje es conocido como TRAP. Los traps existen bajo condiciones especiales. Por ejemplo, si una interfase en un router principal se daña, el agente del router notificara a la estación de administración de red.

2.4.2.- CMIP (Common Management Information Protocol, Protocolo Comun de Gestión de Información).

Tras la aparición de SNMP como protocolo de administración de red, a finales de los 80, gobiernos y grandes corporaciones plantearon el Protocolo Común de Administración de Información CMIP (Common

Management Information Protocol) que se pensó que podría llegar a ser una realidad debido al alto presupuesto con que contaba. En cambio, problemas de implementación han retrasado su expansión de modo que solo está disponible actualmente de forma limitada.

CMIP fue diseñado teniendo en cuenta a SNMP solucionando los errores y fallos que tenía SNMP y volviéndose un administrador de red mayor y más detallado. Su diseño es similar a SNMP por lo que se usan PDU's (Protocol Data Unit) como variables para monitorear la red.

En CMIP las variables son unas estructuras de datos complejas con muchos atributos, que incluyen:

- **Variables de atributos**: representan las características de las variables.

- **Variables de comportamiento**: qué acciones puede realizar.

- **Notificaciones**: la variable genera una indicación de evento cuando ocurre un determinado hecho.

Tiene cinco puntos que son considerados importantes para una buena administración.

- Detección de fallas.

- Administración de configuración.

- Análisis del rendimiento.

- Control de seguridad.

- Conteo.

Los modelos o grupos de modelos de la inteligencia de administración, son tres:

- Modelo de organización, que describe la forma en que las funciones de administración se pueden distribuir administrativamente. Aparecen los dominios como particiones administrativas de la red.

- Modelo funcional, describe las funciones de administración (de fallos, de configuración, de contabilidad, de seguridad...) y sus relaciones.

- Modelo de información, que provee las líneas a seguir para describir los objetos administrados y sus informaciones de administración asociadas. Reside en el MIB (Management Information Base)

- Estructura para registrar, identificar y definir los objetos administrados.

- Especificación detallada de los objetos administrados.

- Serie de servicios y protocolos para operaciones de administración remotas.

CMIP es un protocolo de administración de red que se implementa sobre el modelo de Interconexión de Redes Abiertas OSI (Open Systems Interconnection) que ha sido normalizado por la ISO (International Organization for Standardization's) en sus grupos de trabajo OIW (OSI Implementors Workshop) y ONMF (OSI Network Management Forum).

Además existe una variante del mismo llamado CMOT que se implementa sobre un modelo de red TCP/IP.

En pocas palabras, CMIP es una arquitectura de administración de red que provee un modo de que la información de control y de mantenimiento pueda ser intercambiada entre un administrador (manager) y un elemento remoto de red. En efecto, los procesos de aplicación llamados administradores (manager) residen en las estaciones de administración mientras que los procesos de aplicación llamados agentes (agent) residen en los elementos de red.

CMIP define una relación igual a igual entre el administrador y el agente incluyendo lo que se refiere al establecimiento y cierre de conexión, y a la dirección de la información de administración. Las operaciones CMIS (Common Management Information Services) se pueden originar tanto en administradores como en agentes, permitiendo relaciones simétricas o asimétricas entre los procesos de administración. Sin embargo, la mayor parte de los dispositivos contienen las aplicaciones que sólo le permiten hacer de agente.

Un sistema CMIP debe implementar una serie de protocolos de los cuales el CMISE (Common Management Information Service Element) es el que trabaja mano a mano con CMIP: todas las operaciones de administración de red que crea CMISE el CMIP las mapea en una operación en el CMIP remoto.

Para comunicarse entre sí dos entidades de aplicación pares del administrador y del agente se utilizan APDU's (Application Protocol Data Units) CMIP está compuesto de los protocolos OSI que siguen:

- ACSE (Association Control Service Element)
- ROSE (Remote Operation Service Element)
- CMISE (Common Management Information Service Element)

2.4.3.- SMI (Structure of Management Information, Estructura de la Información de Gestión).

Define la estructura lógica de la información de administración y como se identifica y se describe. Este SMI esta diseñado para usarse tanto en SNMP como en CMIP, pero cada uno lo implementa de manera especifica.

2.4.4.- CMIS (Common Management Infomation Services).

Es un conjunto de reglas que identifican las funciones de una interfaz OSI, entre aplicaciones, utilizado por cada aplicación para intercambiar información y parámetros. CMIS define la estructura de la información que es necesaria para describir el entorno. Prácticamente todas las actividades de la gestión de red OSI están basadas en diez primitivas de servicios CMIS que son utilizadas por las SMFAS.

2.4.5.- MIB (Management Information Base, Base de Información de Gestión).

Es un método de descripción de objetos administrados especificando los nombres, tipos y orden de los campos que hacen el objeto. Hay un solo árbol, MIB definido por ISO. Sin embargo, parte de este árbol tiene secciones para propietarios específicos, usualmente cada propietario tiene su propio MIB que contiene sus propios nombres de variables (por ejemplo, IBM tiene su propio MIB, así como SUN, HP, entre otros) Los ocho grupos de objetos habitualmente manejados por MIB (MIB-I), que definen un total de 114 objetos (recientemente, con la introducción de MIB-II) se definen hasta un total de 185 objetos), son:

- Sistema (System)
- Interfaces
- ATT (Address Translation Table)
- IP (Internet Protocol):
- ICMP (Internet Comunication Management Protocol)
- TCP (Transmisión Control Protocol)

- UDP (User Datagram Protocol)

- EGP (Exterior Gateway Protocol)

El MIB-II de Internet es uno de los muchos estándares de MIB´s, el propósito de este es definir objetos comunes para administración de redes TCP/IP.

El protocolo SNMP realiza las funciones descritas anteriormente llevando la información de gestión entre el manager y los agentes, este protocolo es solo un aspecto dentro de toda la estructura de gestión, la cual esta compuesta de los siguientes elementos:

- Estación de gestión de red (Network Management Station, NMS)

Es el elemento central que proporciona al administrador una visión del estado de la red y unas funciones de modificación de este estado (puede ser una estación de trabajo o un ordenador personal)

- Estructura de la Información de Gestión (Structure of Management Information, SMI)

Es el conjunto de reglas que define las características de los objetos de la red y cómo obtienen los protocolos de gestión información de ellos. Aunque ha sido diseñado después del SMI de OSI, no es compatible con este.

- Base de información de gestión (Management Information Base, MIB)

2.4.6.- PROTOCOLO TCP/IP.

Es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que estos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión.

Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargara de que la comunicación entre todos sea posible. TCP/IP sirve para la conexión de sistemas diferentes como macro y mini computadoras que ejecutan el sistema operativo UNIX, muchos sistemas soportan este protocolo par conectar LAN de PC a otros tipos de

computadores, no es un único protocolo, sino que es en realidad lo que se conoce con este nombre, es el conjunto de protocolos que cubren los distintos niveles del modelo OSI.

Los dos protocolos más importantes son el TCP (Transmisión control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto.

CARACTERÍSTICAS DE TCP/IP.

Ya que dentro de un sistema TCP/IP los datos transmitidos se dividen en pequeños paquetes, éstos resaltan una serie de características:

- La tarea de IP es llevar los datos a granel (los paquetes) de un sitio a otro. Las computadoras que encuentran las vías para llevar los datos de una red a otra (denominadas enrutadores) utilizan IP para trasladar los datos. En resumen IP mueve los paquetes de datos a granel, mientras TCP se encarga del flujo y asegura que los datos estén correctos.

- Las líneas de comunicación se pueden compartir entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo

tiempo, y se ordenará y combinará cuando llegue a su destino. Compare esto con la manera en que se transmite una conversación telefónica. Una vez que establece una conexión, se reservan algunos circuitos para usted, que no puede emplear en otra llamada, aun si deja esperando a su interlocutor por veinte minutos.

- Los datos no tienen que enviarse directamente entre dos computadoras. Cada paquete pasa de computadora en computadora hasta llegar a su destino. Éste, claro está, es el secreto de cómo se pueden enviar datos y mensajes entre dos computadoras aunque no estén conectadas directamente entre sí. Lo que realmente sorprende, es que sólo se necesitan algunos segundos para enviar un archivo de buen tamaño de una máquina a otra, aunque estén separadas por miles de kilómetros y pese a que los datos tienen que pasar por múltiples computadoras. Una de las razones de la rapidez es que, cuando algo anda mal, sólo es necesario volver a transmitir un paquete, no todo el mensaje.

- Los paquetes no necesitan seguir la misma trayectoria. La red puede llevar cada paquete de un lugar a otro y usar la conexión más idónea que esté disponible en ese instante. No todos los paquetes de los

mensajes tienen que viajar, necesariamente, por la misma ruta, ni necesariamente tienen que llegar todos al mismo tiempo.

- La flexibilidad del sistema lo hace muy confiable. Si un enlace se pierde, el sistema usa otro. Cuando usted envía un mensaje, el TCP divide los datos en paquetes, ordena éstos en secuencia, agrega cierta información para control de errores y después los lanza hacia fuera, y los distribuye. En el otro extremo, el TCP recibe los paquetes, verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De haber error en algún punto, el programa TCP destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

2.4.7. - NET BIOS (Network Basic I/O System).

Es el primer estándar desarrollado por IBM, el cual es usado por los productos Microsoft MS-Net para redes de área local. Es comúnmente visto como un protocolo genérico para PC bajo redes LAN, la mayoría de los sistemas operativos para redes ofrecen compatibilidad a los servidores que él ofrece.

3.- SISTEMA OPERATIVO WINDOWS NT.

3.1.- CARACTERÍSTICAS GENERALES.

Microsoft Windows NT según Alabau (1998, p. 206), se caracteriza por soportar los sistemas Intel (superiores a los 486) y los basados con RISC. Soporta multitareas simétricas, que puede usar hasta cuatro microcomputadores concurrentes para procesar información, lo que da como resultado una capacidad de procesamiento más rápido que la de un solo procesador.

Windows NT Server también soporta administración centralizada y control de cuentas de usuarios individuales además de grupos globales. Los usuarios pueden usar un solo registro a la red para acceder y usar los recursos compartidos disponibles. La administración centralizada permite que las cuentas de usuarios se administren desde una sola computadora. Las funciones de administración pueden delegarse a individuos específicos de características de administración.

Las características de multitareas permiten que se ejecuten simultáneamente varias aplicaciones y que las operaciones de la red adquieran prioridad sobre otros procesos menos críticos lo que da como resultado un mejor rendimiento de la red.

Es necesario destacar que Windows NT Server soporta integración con otras redes basadas en Novell Netware, Vines de Bayan, Lan Manager para OS/2, UNIX, VMS y redes SNA. Así mismo, el Windows NT Server proporciona varias utilerías para la configuración y la administración de la red. El administrador de archivo facilita el manejo de archivos y de directorios. El administrador de impresión permite la configuración y el comportamiento de impresoras de red, además del manejo de trabajos de impresión.

3.2.- ARQUITECTURA WINDOWS NT SERVER.

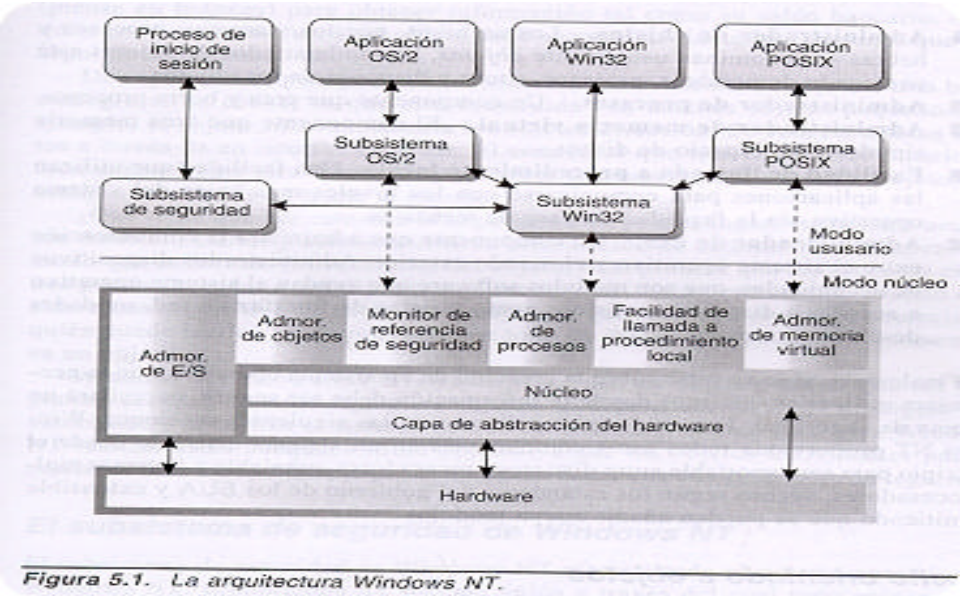


Figura 5.1. La arquitectura Windows NT.

Figura #8. Arquitectura Windows NT Server

3.3.- ADMINISTRADOR DE TAREAS (TASK MANAGER).

Según Guiíta Hallen (1996, p. 421); “Es la parte de Windows NT que le permite controlar con exactitud lo que esta trabajando el sistema en cualquier momento determinado”. El uso principal del administrador de tareas, es cambiar entre programas o terminar programas errantes y evaluar el rendimiento (Performance) de los componentes principales de su sistema.

El rendimiento (Performance) del administrador de tareas, indica en forma general, como están sus recursos en la red, si se requiere de una información mas a fondo, se necesitara usar el monitor del sistema (performance Monitor).

4.- REDES DE COMPUTADORAS.

4.1.- ASPECTOS GENERALES DE LAS REDES.

Para Kevin Stoltz (1994), “Las redes constan de dos o más computadoras conectadas entre sí permitiendo compartir recursos e

información(reportes, diarios, ventas, graficas, entre otros.); los recursos son los dispositivos o las áreas de almacenamiento de datos de una computadora, compartido por otra computadora mediante la red (disco duros, impresoras, plotters, sistema operativo, entre otros." Estas están constituidas tanto del hardware como software.

En este sentido, se permite deducir que al hablar de red sé esta sugiriendo un uso compartido de componentes de hardware y software. En consecuencia, el presente estudio define el termino como un sistema de comunicación de datos basados en la interconexión de dispositivos de procesamiento inteligente, cuya finalidad primera consiste el permitir el uso compartido del hardware y software.

El hardware incluye tarjetas de interfaz y el tipo de cable. Mientras que el software incluye el sistema operativo, protocolos de comunicación, controladores de la tarjeta de interfaz de red del servidor.

4.2.- COMPONENTES DE UNA RED.

Servidor: es un dispositivo que ejecuta el sistema operativo de la red y ofrece los servicios de la red a las estaciones de trabajo. Al no tener que ocuparse en realizar el procesamiento para cada puesto de trabajo. Al

no tener que ocuparse en realizar el procesamiento para cada puesto de trabajo el servidor puede optimizarse para los servicios de archivos y de red, el servidor se utiliza exclusivamente para controlar el almacenamiento y recuperación de información, las tareas de gestión de usuarios, seguridad, las ordenes del responsable de la red, centralización de las colas de impresión.

Estaciones de trabajo: también son llamados nodos, y se conectan al servidor para acceder a los programas, archivos y otros servicios de red como el correo electrónico, estos computadores no suponen una carga para el sistema central, ya que pueden ejecutar por sí misma tantas tareas complejas.

Tarjetas de interfaz de red: es un dispositivo de hardware que debe tener cada estación de trabajo que se desee conectar a la red. Algunas de las tareas de estas tarjetas están definidas por las normas de gestión de protocolos y de acceso al medio usada por cada tarjeta en particular. La tarjeta de interfaz de red debe corresponder al tipo de arquitectura y de cable de red que se utilizara para la conexión una vez que se establece los parámetros de comunicación la tarjeta de red emisora puede comenzar a transmitir y la receptora a capturar los datos.

Sistema de cableado: esta constituido por el cable (medio físico) utilizado para conectar entre si el servidor y las estaciones de trabajo. El cable puede ser coaxial o de par trenzado. El coaxial consiste en un núcleo de cobre rodeado por una capa aislante, que a su vez esta rodeada por una malla metálica que ayuda a bloquear las interferencias, todo el conjunto esta envuelto por una capa protectora. El par trenzado esta compuesto por dos hilos conductores de cobre aislados y trenzados entre si, y en la mayoría de los casos cubiertos por una malla protectora, el trenzado reduce las interferencias eléctricas. Si bien es claro también se puede usar cable de fibra óptica de alta velocidad, el cual se utiliza sobre todo para conectar distintas redes a distancia o en situaciones especiales con mucho trafico de datos mediante luz modulada que pasa por un conductor de vidrio, rodeado por una capa reflectante, el conjunto esta envuelto en una malla protectora.

Recursos compartidos y periféricos: son equipos que forman parte de la red pero que no necesariamente están conectados a los PC, entre ellos se incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de disco óptico, las impresoras, los trazadores, el escáner, entre otros.

4.3.- TIPOS DE REDES.

LAN (Local Area Network): Redes de Área Local, cubren un área geográfica limitada, generalmente marcada por una organización y se han desarrollado como una manera de cubrir los requerimientos de comunicación en distancias cortas entre dispositivos inteligentes.

Su moderada extensión geográfica les permite utilizar medios de comunicación de gran rendimiento que permitan la transferencia de información a grandes velocidades. El área máxima de una LAN se encuentra entre uno y dos kilómetros. De manera igual, una LAN es un medio de comunicación de datos que proporciona conexiones de alta velocidad entre procesadores y periféricos situados en un área limitada.

El Instituto de Ingeniería Eléctrica y Electrónica (IEEE) publica su definición para una red de área local. “Es un sistema de comunicación de datos que permite a un numero de dispositivos independientes comunicarse directamente uno con otros, dentro de un área geográfica de tamaño moderado y sobre un canal físico de comunicación de velocidad de transmisión moderada”. (Martín, Janes; p.342; 1996).

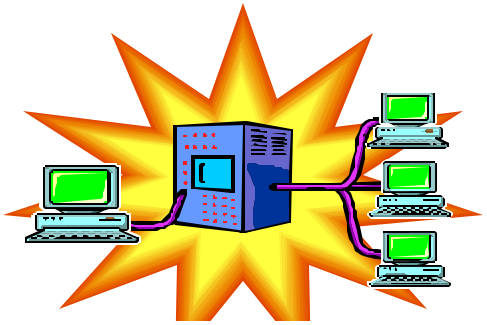


Figura #9. Red de Área Local (LAN)

WAN (Wide Área Network): Redes de Área Amplia, la cual consiste en la interconexión de redes de área local (LAN) o de área metropolitana (MAN) que se encuentran geográficamente lejanas, los enlaces establecen generalmente por medio de líneas telefónicas o líneas dedicadas de alta velocidad por ejemplo fibra óptica, satélite, microondas, entre otros. Una red de gran alcance puede extenderse por todo el mundo ya que puede soportar cientos de miles de kilómetros de diámetro. Las redes WAN son de transmisión menos confiable y poseen menos probabilidad de error y velocidad de transmisión mas baja debido a que comprenden una área geográfica muy amplia.

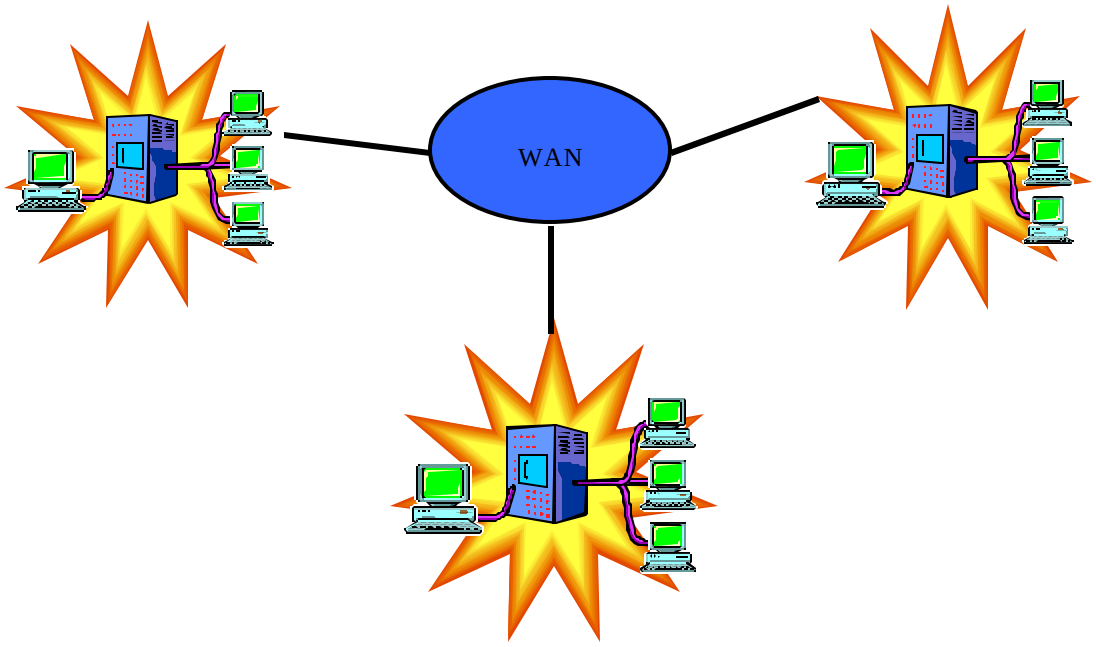


Figura #10. Red de Área Amplia (WAN)

MAN (Metropolitan Área Network): Redes de Área Metropolitana, consisten en un conjunto de redes de área local (LAN) interconectadas dentro de un área especifica, este tipo de red utiliza una base de cableado o sistemas de conexión de alta velocidad, debido a que cubre una área aproximada de 50 kilómetros de diámetro.

INTERNETWORK: Redes Interconectadas, la cual consiste en conectar dos o más redes locales para formar un sistema de red que cubra toda una organización, también pueden dividirse una red extensa en varias redes más pequeñas para optimizar el rendimiento y la gestión.

4.4.- DISPOSITIVOS DE INTERCONEXIÓN DE LAS REDES.

Repetidores: son dispositivos sencillos de bajo nivel que se instalan para amplificar la señal eléctrica del cable, de forma que se pueda extender la longitud del cable. Los repetidores normalmente no modifican la señal, excepto en que la amplifica para poder transmitir por la extensión del cable. Los repetidores se utilizan sobretodo en los sistemas lineales

como Ethernet. Las redes con topología de Token-Passing utilizan cada estación de trabajo para retransmitir la señal que recibe. Algunos repetidores filtran el vidrio.

Los repetidores funcionan sobre el nivel mas bajo de la jerarquía de protocolos, el nivel físico. Los repetidores no han de considerar los protocolos y métodos de acceso, ya que se limitan en amplificar la señal para poder transmitir sobre un tramo de cable adicional. Ambos segmentos deben de utilizar el mismo método de acceso al medio de transmisión.

Bridges (Puentes): son dispositivos que permiten interconectar redes separadas que tenga esquemas de direccionamiento compatibles, haciendo que estas parezcan una sola red. Los bridges pueden ser usados para computadoras personales con estándares para la industria que implica hardware y software apropiados o pueden ser hechos para equipos con propósito especifico. Para un correcto funcionamiento se deben conocer las direcciones de todos los dispositivos a los cuales expedir paquetes. La funcionalidad de un bridge es medida normalmente de dos maneras: por el numero de paquetes que pueda filtrar o examinar y por el numero de paquetes que puede expedir o pasar a otra red.

Los bridges son generalmente necesarios en las WAN donde es necesaria la conexión de muchos equipos, también permiten la ocurrencia de faltas tolerables, que no son mas que la habilidad del sistema para resistir una falla.

Routers (Enrrutadores o Encaminadores): son dispositivos que permiten la conexión de redes que pueden (o no pueden) usar diferentes tecnologías pero, comparten un protocolo común. Los routers se pueden utilizar tanto en las redes locales como en las metropolitanas o de área amplia. Como los bridges, los routers solo reexpiden el trafico dirigido a otro lado. Esto significa que el trafico local en una red no afectara el funcionamiento de la otra haciendo que estas semejen una sola red. El enrutamiento de información (es el proceso de direccionar un mensaje de datos desde su fuente hasta su destino) incluye costos y el numero de hops envueltos en el envió de data por medio de un path hasta el nodo destino.

Gateway (Compuertas): son dispositivos que proveen a los usuarios de las LAN enlaces con otros ambientes computacionales. Los gateways tienen la capacidad de conectar LAN's corriendo en protocolos diferentes, además cuando se conecta un sistema centralizado a una LAN

con gateways, los usuarios de cualquier estación de trabajo pueden acceder al sistema centralizado. Los gateways almacenan y reexpiden paquetes entre redes que no son similares y son utilizados principalmente en redes WAN.

Hub y Concentradores: son un punto central de conexión para nodos de red que estan dispuestos de acuerdo a una topología física de estrella, como en la Ethernet 10BASE-T. Los concentradores son dispositivos que se encuentran físicamente separados de cualquier nodo de la red. El concentrador tiene varios puertos en la parte trasera de la tarjeta, a los que se conecta el cable de otros nodos de la red. Estos pueden conectarse en varios concentradores para permitir la conexión de nodos adicionales.

B. REVISIÓN DE LA LITERATURA.

A continuación se presenta una serie de resúmenes de las investigaciones realizadas las cuales contienen información similar a la expuesta por el modelo de detección.

En 1995, los TSU Bastidas Carlos y Delli Bianca Implantaron un Sistema de Administración de Redes bajo el Protocolo SNMP en la Costa Oeste de Maraven.

Esta investigación se basa en el uso de las plataformas TCP/IP y la herramienta SNMPc que es una herramienta para el monitoreo y administración permanente de la red, mediante la representación grafica de los componentes de las distintas localidades, permitiendo la supervisión centralizada y la planificación del mantenimiento correctivo / preventivo según estadísticas generadas por el sistema, con la finalidad de prever posibles fallas y lograr un alto rendimiento y productividad de la infraestructura de red.

En 1999, los Brs. De Bravo Jakni y Mora Hugo. "Diseño de un Prototipo de un Sistema Integrado para el Acceso, Monitoreo y Administración de Redes de forma Remota" .

Esta investigación consistió en diseñar un prototipo para el acceso, monitoreo y administración de redes en forma remota el cual consiste en una interfaz de conexión a través de Internet entre un usuario y el servidor de su empresa estableciendo la posibilidad de gestión operativa de la red

desde cualquier punto geográfico la importancia de este proyecto esta basada en la capacidad de conectar los usuarios con la red local desde cualquier sitio remoto utilizando enlace de Internet para realizar, tanto operaciones comunes como administrativas, el uso de este sistema reducirá la necesidad de la presencia permanente del administrador de red en el área local.

En 1998, los Brs. Labastidas Neydis y Martinez Roberto. ”Desarrollo y Conexión de una Infraestructura de Cableado para Soportar una Red de Voz, Datos y Comunicaciones Remotas Vía Celular y Telefonía Estándar”.

Esta investigación consiste en desarrollar y conectar una infraestructura de cableado para dar soporte a un sistema de red. El tipo de investigación se estableció como aplicada porque tuvo como finalidad desarrollar un proyecto a corto plazo de un sistema de comunicación de datos y de tecnología de operaciones ya que se trabajo con la información y la integridad de sus procesos operativos administrativos, producción y vente. El desarrollo y conexión de la infraestructura de cableado se trabajo bajo la norma IIEE, funcionando bajo el protocolo TCP/IP y el cable par trenzado Nivel 5, de esta manera permitiendo que se lograse la

comunicación interna de la empresa y externa con los vendedores, solucionándose de esta manera la planificación estricta de los simuladores por parte de los vendedores aumentando los niveles de ventas y productividad.

C. DEFINICIÓN DE TERMINOS BÁSICOS.

ATT (address Translation Table): Contiene la dirección de la red y las equivalencias con las direcciones físicas. Esta información se movió a unas MIB especificas para protocolo en el SNMPv2. (Alam Freedman, 1999, p. 43).

CMIP (Common Management Information Protocol, Protocolo Comun de Informacion): protocolo de manejo de información para monitoreo de redes y control de información en la interconexión de sistemas abiertos (OSI) se denomina ISO 9596 incluye administración de fallas, configuración, ejecución, seguridad y contabilidad. (Bryan Pfaffenberger, 1995, p. 245).

CMIS (Common Management Information Services, Administración Común de Servicios de Información): funciones

estándar para monitoreo de redes y control de información en la interconexión de sistemas abiertos. (S. Collin, 1996, p. 21).

Estándares: son un conjunto de normas ampliamente aceptadas que determinan las características generales de un sistema. (Fredman Alam, 1999, p. 542).

Ethernet: estándares para hardware, cableado, comunicaciones y cableado de redes de área local (LAN), desarrollado originalmente por Xerox Corporation, capaz de enlazar hasta 1024 nodos en una red de bus. (Bryan Pfaffenberger, 1995, p. 182).

Fault Tolerance (Tolerancia a Fallas): método diseñado para asegurar la operación continua del sistema, en caso de fallas individuales, suministrando elementos redundantes; a nivel de componentes, el diseño incluye clips y circuitos redundantes y la posibilidad de esquivar automáticamente las fallas. A nivel del sistema del computador los elementos sensibles a fallas, tales como: los procesadores, las grandes unidades de disco, se duplican las operaciones tolerantes a fallas requieren a menudo sistema de suministro de energía de respaldo o UPS (Uniterruptible Power Suppy, Suministro Interrumpido de Energía) en caso

de fallo de la fuente principal de energía. (Bryan Pfaffenberger, 1996, p. 867).

FDDI, Interfaz de Datos Distribuidas por Fibra: estándar LAN definido por la ANSI X3T9.5 que especifica una red de Token Ring a 100 Mbps, que utiliza cable de fibra óptica con distancia de transmisión de hasta dos kilómetros. El estándar FDI utiliza una arquitectura de anillo doble para proporcionar redundancia. (Ford Merilee, 1998, p. 342).

Gateway: medio a través del cual los usuarios de un servicio de la red de computación puede tener acceso a cierto tipo de información en un servicio de red diferente. (Idem, 1995, p. 210).

Grupo Local (Local Group): en servidores Windows NT 3.5, grupo garantizado de derecho y permisos solamente para los recursos en los servidores de su propio dominio. (Bryan Pfaffenberger, 1996, p. 360).

ICMP (Internet Control Mensaje Protocol, Protocolo de Control de Mensaje en Internet): es la porción de TCP/IP que proporcionan las funciones usadas para mejorar y controlar la capa de la red. (Douglas Comer, 1995, p. 123).

IEEE (Instituto de Ingenieros en Electrónica y Electricidad): organización profesional cuyas actividades incluyen el desarrollo de los estándares de comunicaciones de redes. Los estándares IEEE LAN son los estándares LAN que predominan actualmente. (Ford Merilee, 1998, p. 248).

Interfaz: conexión entre dos dispositivos del hardware, entre dos aplicaciones o entre un usuario y una aplicación que facilita el intercambio de datos. (Idem, 1995, p. 266).

Internet: abreviatura de Internetwork de dos o más redes que utilizan diferentes protocolos de red, conectados por medio de un enrrutador, los usuarios en una Internetwork pueden acceder los recursos de todas las redes conectadas. (Douglas Comer, 1995, p. 79).

ISO (International Standards Organization): organismo internacional emisor de estándares, radicado en Ginebra, que establece estándares globales para comunicaciones e intercambio de información. (Idem, 1995, p. 269).

Manager: aplicación incluida con el sistema operativo de red Bayan Vines, que se utiliza para administrar la red. Se una manager para

establecer los perfiles de usuario, derechos de acceso, grupos, atributos de seguridad y servicios de archivos e impresión. (Bryan Pfaffenberger, 1996, p. 223).

MIB (Management Information Base, Información de Configuración de una Base de Datos de Red): que utilizan SNMP y CMIP para monitorear o cambiar ajustes establecidos de la red. MIB suministra un nombramiento lógico de todos los recursos en la red que estén relacionados con la administración de la red. (Douglas Comer, 1995, p. 590).

MIBF (Mean Time Between Failures, Tiempo Promedio entre Fallas): longitud promedia estadísticamente derivada del tiempo durante el cual los componentes del sistema operan antes de fallar, MIBF se expresa en miles o decenas de miles de horas, también se llama horas de encendido. (S. Collin, 1996, p. 215).

MIS (Management Information System, Sistema de Administracion de Información): sistema de información basado en computadoras, que integra datos de todos los departamentos a los que presta servicios para apoyar la administración de la compañía con la

información necesaria para tomar decisiones oportunas, tener control del progreso y solucionar problemas. (Douglas Comer, 1995, p. 532).

Monitoreo: puede referirse a una medida de rendimiento del sistema que se puede implementar a nivel de hardware y software. (Douglas Comer, 1995, p. 450).

Topología (Topology): Es el arreglo físico de los nodos y el medio de transmisión dentro de una estructura de red corporativa. (Ford Merilee, 1998, p. 359).

D. SISTEMA DE VARIABLE.

A continuación se describe se describen las variables de estudio de la presente investigación:

MODELO DE DETECCION:

Conceptualmente: ”Se define como la combinación de componentes, elementos y pasos que interactúan entre sí para detectar

cualquier variación y localizar efectos de funcionamiento en cualquier proceso y equipo determinado dentro o fuera de la instalación". (Díaz, 1995, p. 182).

Operacionalmente: un modelo de detección se define como una herramienta que permite ubicar el origen de la falla e identificar las causas internas que provocan el problema, avería o disfunción a partir de una serie de datos o síntomas que son consecuencia de las mismas, partiendo del conocimiento de todo el sistema y de las señales de detección e información del diagnostico, obtenida de los diferentes procesos que se dan dentro de una estación de red, minimizando de manera drástica la perdida de tiempo y producción.

DETECCION DE FALLAS Y RENDIMIENTO:

Conceptualmente: Detección de Fallas: "consiste en el conjunto de facilidades que permiten la detección, el aislamiento y la corrección de las operaciones anormales de las redes o sistemas de comunicaciones. (Díaz, 1995, p. 235). **Detección de Rendimiento:** "consiste en medir y hacer disponibles diferentes aspectos del desempeño total de la interred de

manera, que se pueda mantener en un nivel aceptable". (Díaz, 1995, p. 238).

Operacionalmente: la detección de fallas y de rendimiento, le permitirá a la empresa poder supervisar, detectar y controlar el desempeño de los diferentes recursos existentes en la red, al momento de presentarse una falla en los mismos, además de esto, obtener de una manera accesible el rendimiento continuo de dichos recursos, para así poder reducir al máximo actividades anormales o inesperadas que se presenten y solucionarlas en el menor tiempo posible, en su defecto evitar que se presente.

REDES LAN/WAN:

Conceptualmente: Sé definen como el conjunto de redes formadas por varias computadoras conectadas entre sí, de manera que puedan compartir recursos sin tomar en cuenta la localización física del recurso y del usuario. (Kevin Stoltz, 1994, p. 16).

Operacionalmente: son infraestructuras tanto de hardware como de software, que permiten la comunicación interna y externa para así agilizar los procesos directivos, administrativos y de facturación en la

empresa, permitiendo compartir recursos de información entre los diferentes departamentos.