UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

GENERADOR DE MONITOR DE RED

EDGAR FRANCISCO RODAS ROBLEDO

Asesorado por Ing. Giovanni Galindo

Guatemala, octubre de 2003.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

GENERADOR DE MONITOR DE RED

TRABAJO DE GRADUACÍON

PRESENTADO A JUNTA DIRECTIVA DE
LA FACULTAD DE INGENIERÍA
POR

EDGAR FRANCISCO RODAS ROBLEDO

AL CONFERÍRSELE EL TIULO DE

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERIA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yasminda Vides Leiva

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Herbert René Miranda Barrios
EXAMINADOR	Ing. Luis Alberto Vettorazi España
EXAMINADOR	Ing. Ricardo Alfredo Girón Solórzano
EXAMINADOR	Ing. Rolando Alonzo Ordoñez

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

GENERADOR DE MONITOR DE RED

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas con fecha enero 2002.

EDGAR FRANCISCO RODAS ROBLEDO

DEDICATORIA :

A:

DIOS	Porque Jehová es bueno; para siempre es su misericordia, y su verdad por todas las generaciones.
Mis padres	José Rodas y Silvia de Rodas, como un agradecimiento por todos los sacrificios que han hecho por mí. Dios los bendiga.
Mi hermana	Mayrita, por su apoyo y formar parte especial de mi vida.
Mis sobrinitos	Gaby y Héctor con cariño.
Mis abuelitas	En especial a Francisca de Rodas (Q.E.P.D)

Mis amigos Avimael, Alan, Anibal, Cristian, Cresencio, Deily, Elmer, Eliseo, Harry, Héctor Hugo, José Carlos, Julio, Luis, Mercy, Rudy, Raquel, Samy, Sara, Nivia, vinicio.

Mi asesor Giovanni Galindo, gracias por su amistad.

Especialmente A usted, que es testigo de mi logro.

ÍNDECE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

ASN.1 — *Abstract Syntax Notation*. Notación de sintaxis abtracta. Norma de representación de datos. El protocolo SNMP usa el ASN.1 para representar nombres de objetos.

Base de datos — Conjunto de datos organizados de modo tal que resulta fácil acceder a ellos, gestionarlos y actualizarlos.

Bit — *Binary digit*. Dígito binario, *el bit* es la unidad más pequeña de almacenamiento en un sistema binario dentro de una computadora.

Bridge — Dispositivo usado para conectar dos redes y hacer que las mismas funcionen como si fueran una. Típicamente se utilizan para dividir una red en redes más pequeñas, para incrementar el rendimiento.

Byte Conjunto significativo de ocho bits que representan una carácter.

CGI *Common Gateway Interface*. Interface común de enlace. Metodología propia del software que trabaja con servidores web.

Cifrado Mecanismo de seguridad, que permite modificar un mensaje de modo que su contenido sea ilegible, salvo para su destinatario.

CMIP *Common Management Information Protocol*. Es un sistema de manejo de redes muy bien diseñado, que mejora mucho los defectos y debilidades de SNMP.

CMOT *Common Management Over TCP/IP*. Es un protocolo propuesto como estándar de Internet para la arquitectura de gestión de red con vistas de mantener una relación más estrecha con el CMIP.

Correo electrónico Es un sistema que permite enviar y recibir mensajes escritos a través de la red Internet a cualquier parte del mundo.

Criptografía Arte de escribir con clave secreta. Cualquier procedimiento que permita a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, tras haberlo descifrado.

Cursor Es la marca que indica en que punto del documento tendrá lugar la siguiente introducción de datos. En la mayoría de casos se representa con una pequeña línea vertical negra que parpadea.

Dispositivo Punto de conexión de una red.

Ethernet Uno de los protocolos de comunicación mas extendidos en el campo de las redes locales.

FDI *Fiber Distributed Data Interface*. Interfaz de datos distribuidos por fibra óptica.

Http *Hiper Text Transfer Protocol*. Protocolo de transferencia de hipertexto. Es el protocolo encargado de trasladar el hipertexto desde el servidor de web hasta el cliente.

IAB *Intenet Activities Board* . La IAB ha sido muchas cosas a lo largo de los años. Desde 1992 pasó a ser una sección de la *Internet Society*. Es responsable de supervisar las actividades de otras secciones de la Internet como la IETF.

Interface Elemento de transición o conexión que facilita el intercambio de datos. El teclado por ejemplo, es una interface entre el usuario y la computadora.

ISO *International Organization for Standarization*. Fundada en 1946, es una federación internacional que unifica normas en unos cien países.

LAN *Local Area Network*. Una red de comunicación que une varias computadoras, impresoras, etc, entre sí, permitiendo compartir recursos y archivos entre ellos. La red abarca un área geográfica máxima de unos pocos kilómetros cuadrados.

MB *Megabyte*. Unidad de medida de la capacidad de memoria y de dispositivos de almacenamiento informático. Un MB corresponde a 1024 bytes.

MIB *Management Information Base*. Información base de la administración. Es un documento que describe y define cada uno de los objetos que pueden ser manipulados por protocolos de administración como el SNMP.

Módem Modulador-demulador. Dispositivo periférico que conecta la computadora a la línea telefónica.

NMS *Network Management Station*. Estación de administración de red, es una máquina que ejecuta el protocolo de administración de red y una o más aplicaciones de administración de red.

OSI — *Open Systems Interconnection*. Es una arquitectura de gestión definida por ISO cuya función es permitir supervisar, controlar y mantener una red de datos.

Paquete — *Packet*. Es la parte de un mensaje que se transmite por una red. Antes de ser enviada a través de Internet, la información se divide en paquetes.

Password — Contraseña. Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

PERL — Lenguaje para manipular textos, ficheros y procesos, PERL proporciona una forma fácil y legible para realizar trabajos. Se utiliza mucho en aplicaciones dinámicas para Internet.

PING — *Packet Internet Groper*. Programa que se utilize para comprobar si un destino esta disponible

Protocolo — Grupo de normas que permiten estandarizar un procedimiento repetitivo. Reglas que se siguen dos computadoras para intercambiar mensajes y la descripción formal de los formatos de dichos mensajes.

Puerto — Número entero pequeño usado para identificar un programa de aplicación en una computadora remota. Los protocolos de transporte como el TCP, asignan un número de puerto único a cada servicio por ejemplo, el correo electrónico usa el puerto 25.

RAM	*Random Access Memory*. Memoria de acceso aleatorio.
RMON	Monitoreo remoto de redes. Es útil para la administración de red ya que recolecta y analizan los paquetes que pasan por ellos.
Router	Ruteador. Dispositivo que dirige el tráfico entre redes y que es capaz de determinar los caminos mas eficientes, asegurando un alto rendimiento.
SGMP	Protocolo de monitoreo de gateway simple. Protocolo de administración de red que se tuvo en cuenta para la normalización de Internet y es el origen de SNMP.
Sistema operativo	Software o programas que se encargan de administrar los recursos de un equipo de computación. También realiza las funciones de comnicador entre el usuario y el equipo de cómputo.
SMFA	*Specific Managment Functional Areas*. Nombre que reciben las cinco categorías de servicios de gestión en las que se divide OSI.
SMI	*Structure Management Information*. Estructura de la administración de la información. Define las reglas para definir la información de administración

	independientemente de los detalles de implementación.
SNMP	*Simple Network Management Proto*col. Protocolo simple de administración de red. Es el protocolo definido por los comités técnicos de Internet para ser utilizado como una herramienta de gestión de los distintos dispositivos en cualquier red.
TCP IP	*Transmission Control Protocol Internet Proto*col. Es el juego de normas que regula las comunicaciones entre los dispositivos de la red. Establece el camino que debe seguir cada mensaje hasta alcanzar su destino y se encarga de corregir posibles errores de transmisión.
Token Ring	Red de anillo. Una red de anillo es un tipo de LAN con dispositivos cableados en anillo. Cada dispositivo pasa constantemente un mensaje de control al siguiente, de tal forma que cualquier dispositivo que tiene el mensaje de control puede enviar un mensaje.
Topología	La forma de la red. Predominan tres tipos de tecnologías: Bus, estrella y anillo.
Wireless	Comunicación inalámbrica.

X.25 Interface estándar para conexión de terminales de datos a redes públicas. Es un protocolo de empaquetamiento conmutado.

OBJETIVOS

General

Explicar la necesidad y las etapas de la gestión de redes y desarrollar una herramienta que permita gestionar en tiempo real y a través de la red de INTERNET servicio bajo el protocolo TCP/IP activos en un dispositivo, notificando al administrador cuando uno de esos servicios falle.

Específicos

1. Desarrollar una aplicación en ambiente Web que permita gestionar servicios TCP/IP en un dispositivo, notificando cuando uno de estos servicios falle.

2. Explicar la definición de la gestión de redes y las ideas fundamentales necesarias para una comprensión global de su significado.

3. La aplicación debe ser gráfico amigable para el usuario.

4. La aplicación debe ayudar al operador a restablecer el servicio que falle en un dispositivo.

5. Demostrar el potencial y facilidad de PERL para interactuar con equipos de red, elementos de interface (CGI's) y HTML.

RESUMEN

El tamaño y la complejidad de las redes han ido creciendo sin cesar debido en gran parte a la aparición de las redes públicas de datos y a la creciente oferta de servicios de comunicación de valor añadido.

Este crecimiento de servicios, también implica un crecimiento en los dispositivos de la red. El crecimiento de dispositivos hace más compleja la administración de la red y el detectar un fallo en uno de sus servicios se hace complejo y, por lo tanto, el tiempo de respuesta ante una eventualidad se complica dejando muchas veces por largo tiempo sin servicio a los usuarios.

Debido al crecimiento de las redes, surge la necesidad de gestionarlas, es decir, controlar los recursos que las componen en términos de rendimiento, capacidad, utilización, reconfiguración, diagnóstico, planificación, disponibilidad, etc. El gestionar los servicios en un dispositivo nos garantiza recuperarnos de cualquier eventualidad en el menor tiempo posible.

Utilizando PERL, CGI's y HTML se desarrollo una herramienta que gestiona en tiempo real servicios TCP/IP en un dispositivo, notificando al administrador por correo electrónico cuando uno de estos servicios falla y así restablecer el servicio que fallo en el menor tiempo posible.

La herramienta es amigable al usuario y trabaja en ambiente Web y nos permite definir un dispositivo para gestionarlo, notificación de fallas a través de
alarmas, procedimientos para restablecer un servicio, herramientas de diagnostico para detectar fallas y corregirlas.

INTRODUCCIÓN

La gestión de red es un conjunto de elementos de control y supervisión de los recursos que permite que la comunicación tenga lugar en la red.

Actualmente, los sistemas de comunicación prestan servicios a los usuarios utilizando redes privadas y redes públicas.

La interconexión entre las redes privadas y públicas proporciona mejores posibilidades en la provisión de servicios pero complica el control de las redes.

Habiendo conseguido la transferencia de información a través de esta complejidad de redes, surge la necesidad de gestionarlas, es decir, de controlar los recursos que las componen en términos de rendimiento, capacidad, utilización, disponibilidad, etc.

Este trabajo se realiza con el propósito de poner a disposición de los administradores de red una herramienta que permite gestionar en tiempo real servicios TCP/IP activos en un dispositivo de red, notificando cuando uno de esos servicios falle para restablecerlo en el menor tiempo posible.

La herramienta de desarrollo en PERL, CGI's y HTML y permite una gestión a nivel de servicio para garantizar la disponibilidad y minimizar el impacto asociado a una falla.

PERL, CGI's y HTML son herramientas de distribución gratuita y presentan un potencial y facilidad para el desarrollo de herramientas de software en ambiente Web.

1. GESTIÓN DE RED

La ISO (Organización Internacional de Estandarización) define la gestión de red como: El conjunto de elementos de control y supervisión de los recursos que permite que la comunicación tenga lugar sobre la red.

El tamaño y la complejidad de las redes han ido creciendo sin cesar debido en gran parte a la aparición de la redes públicas de datos y a la creciente oferta de servicios de comunicación de valor añadido.

Actualmente los sistemas de comunicación prestan servicios a los usuarios utilizando redes privadas y redes públicas.

La interconexión entre las redes privadas y públicas proporciona mejores posibilidades en la provisión de servicios pero complica el control de las redes.

Habiendo conseguido la transferencia de información a través de esta complejidad de redes, surge la necesidad de gestionarlas , es decir, de controlar los recursos que las componen en términos de rendimiento, capacidad, utilización, reconfiguración, diagnóstico, planificación, etc.

Las organizaciones dependen cada vez más del buen funcionamiento de los sistemas de comunicación, dado que un gran número de los empleados, utilizan recursos informáticos para la realización de su actividad diaria.

Cada vez, es menos justificable la expresión “la red no funciona bien” de cara al interior de la empresa, o la expresión “la línea es caída” de cara al cliente.

Hoy, debido a la competencia de servicios, las organizaciones y empresas que no dispones de una buena gestión de sus redes y servicios de

comunicaciones son cautivas de la tecnología y, en vez de emplear los recursos informáticos para hacer negocios, sus recursos informáticos pueden estar impidiendo el progreso de su negocio.

1.1 Funciones de la gestión de red

La gestión de redes comprende las herramientas necesarias para realizar las siguientes funciones:

1.1.1 Supervisión de la red

Se suele realizar de dos formas: mediante una estación de gestión con una computadora personal o estación de trabajo que reciba mensajes de los dispositivos de red (puentes o bridges, encaminadores o routers, servidores de terminales, etc.) o mediante una estación que pregunte regularmente el estado de los dispositivos.

1.1.2 Control de los dispositivos de red

Se realiza enviando comandos por la red desde la estación de gestión hasta los dispositivos de la red para cambiar su configuración.

Los sistemas de gestión de redes permiten satisfacer requisitos de tipo técnico y funcionales.

Requisitos técnicos:

- Administración de entornos heterogéneos desde una misma plataforma.

- Administración de elementos de interconexión.

- Interfaces con grandes sistemas.

- Interfaz gráfico amigable.

- Evolución según las necesidades del cliente.

Requisitos funcionales:

- Gestión del nivel de servicios para garantizar la disponibilidad, la atención a los usuarios, el tiempo de repuesta, etc.

- Gestión de problemas para facilitar la segmentación de los mismos resolviéndolos en etapas o niveles.

- Gestión de cambios para minimizar el impacto asociado habitualmente con los procesos de modificaciones de las configuraciones existentes.

- Apoyo a la toma de decisiones y facilitar que la gestión de red actúe de puente, o interfaz entre el personal técnico y la dirección, gracias a la facilidad de generar informes.

- Apoyo en la resolución de incidencias para preservar la experiencia del grupo de gestión, reduciendo el tiempo de resolución de situaciones que deberían ser familiares.

- Apoyo en la formación para reducir el esfuerzo de aprendizaje y optimizar el grado de uso requiriendo perfiles de personal poco exigentes.

Los sistemas de gestión deben poder crecer a medida que crecen las necesidades de los usuarios, de forma que se puedan proteger las inversiones realizadas.

Un entorno integrado de gestión es una combinación de recursos humanos, organizativos y tecnológicos. La gestión de redes es una estrategia a largo plazo que puede afectar a todo el personal de una organización:

- A los usuarios de la red que necesitan acceder a la información de estado de la misma.

- A los directivos que han de preocuparse de cómo afectarán las prestaciones de la red al desarrollo de sus áreas dentro de la organización.

- A los administradores de red que se encargan de la operativa diaria.

1.1.3 Administración de la red

Además de la gestión operativa (atender usuarios, resolver fallos en el menor tiempo posible, monitorizar, etc.) existen otros aspectos involucrados que permiten definir el análisis y la optimización de la red:

- Descripción funcional de tareas que serán objeto de la gestión.

- Adecuación organizativa en las entidades, organismos, centros o empresas.

- Especificación de procedimientos que faciliten la tramitación de sucesos de interés.

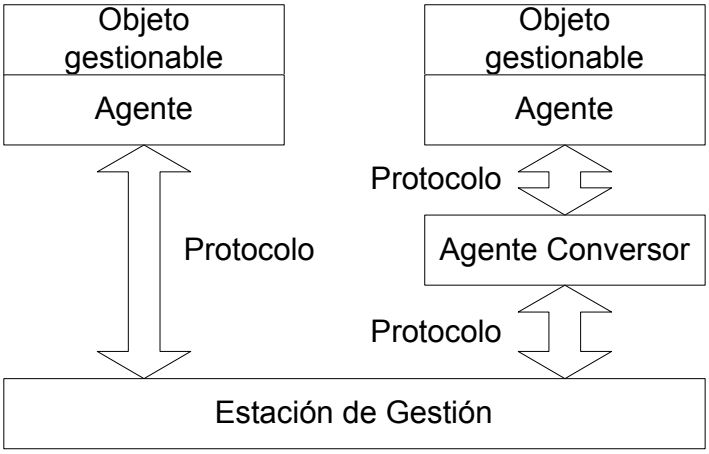
- Adquisición de medios técnicos.

- Adaptación de los medios humanos disponibles.

1.1 Componentes de un sistema de gestión

Los componentes de un sistema de gestión de red y las relaciones entre ellos se representa en el siguiente diagrama:

Figura 1 Componentes de un sistema de gestión



Cada uno de los elementos tiene el siguiente significado:

- Objeto gestionable: representa cualquier dispositivo físico o lógico de la red y el equipamiento lógico relacionado con el que permita su gestión.

- Agente: es el equipamiento lógico de gestión que reside en el objeto gestionable.

- Protocolo: Utilizado por el agente para pasar información ente el objeto gestionable y la estación de gestión.

- Objeto ajeno: Se define como un objeto gestionable que utiliza un protocolo ajeno, es decir un protocolo distinto al de la estación de gestión.

- Agente conversor: Actúa de conversor entre el protocolo ajeno y el protocolo utilizado por la estación de gestión.

- Estación de gestión: Está formada por varios módulos o programas corriendo en una estación de trabajo o computadora personal.

A continuación se hace una descripción de los componentes de la estación de gestión:

- Interfaz de usuario: es la interfaz entre el usuario y el sistema y puede ser en modo carácter o gráfico.

- Base de datos: Mantiene cualquier información de la red (descripciones de diferentes parámetros, configuración de contadores, etc.) almacenando el histórico de eventos y permitiendo la realización de seguimientos.

- Programa monitor: Supervisa las condiciones actuales y permite la inspección futura, visualiza las alarmas activadas por los agentes y realiza actualizaciones mediante sondeos regulares.

- Arranque y configuración: Comprueba que cada estación pueda ser 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.

La estación de gestión puede acceder a los objetos gestionables de cuatro maneras diferentes:

- En banda (*in-band*): la gestión del objeto se realiza utilizando la red.

- Fuera de banda (*out-of-band*): el sistema de gestión accede a los objetos gestionables a través de otros canales. Esto se puede realizar mediante un

terminal conectado directamente a un puerto del objeto gestionable o que el objeto gestionable tenga algún tipo de visualizador o panel de control.

- Remotamente: la gestión se realiza desde otra estación que no es la estación principal de gestión. Existen varias posibilidades:

- Mediante una estación adicional operadora que permite a varios operadores gestionar todo el sistema o partes de el.

- Utilizando una estación remota conectada a otro segmento de la red que da servicio a estaciones locales.

- Empleando un terminal remoto conectado mediante un módem.

- Un dispositivo de gestión dedicado que puede llamar al operador a través de un servicio de buscapersonas o correo electrónico.

- El sistema de gestión puede ser un elemento dentro de un gran sistema supervisado por un gestor de sistemas.

2. ARQUITECTURAS DE GESTIÓN DE RED

En este capitulo se describen las dos principales arquitecturas de gestión de red:

- Modelo OSI
- Modelo Internet (SNM)

2.1 Modelo OSI

ISO ha definido una arquitectura de gestión OSI (*Open System Interconnection*) cuya función es permitir supervisar, controlar y mantener una red de datos. Está dividida en cinco categorías de servicios e gestión denominadas áreas funcionales específicas de gestión (*Specific Management Functional Areas, SMFA*). Estas categorías son las siguientes:

2.1.1 Gestión de configuración

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

- Construcción de la topología de la red de acuerdo con la visión del usuario.

- Incluir y dar de baja dispositivos.

- Establecimiento de un inventario de los dispositivos instalados y de la 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.

A continuación se exponen en más detalle el conjunto de funciones incluidas en esta área funcional:

- Definición de nuevos recursos a gestionar.
- Asignación y gestión de nombres a los recursos gestionados.
- Creación, modificación y destrucción de relaciones entre los recursos.
- Establecimiento y modificación de las características de operación.
- Borrado de recursos gestionados.
- Obtención de informes a voluntad de la identidad, condiciones de funcionamiento de los objetos gestionados.
- Reflejo en tiempo real de los cambios significativos en los modos de operación de los recursos gestionados.

Para el sistema de gestión los recursos gestionados pueden presentar los siguientes estados de operación:

- No preparado: El recurso a gestionar no es operativo debido, por ejemplo a que no está instalado, está defectuoso, etc., o a causa de que otros recursos de los que depende para su funcionamiento no están operativos.
- Preparado: El recurso de comunicaciones está operativo por en el momento actual no se está utilizando.

- Activo: El recurso de comunicación está operativo y en uso pero no tiene capacidad residual para poder realizar funciones adicionales de gestión en ese momento.

Para el sistema de gestión los recursos gestionados pueden presentar los siguientes estados administrativos:

- Bloqueado: El recurso a gestionar no se puede utilizar.

- Cerrado: El recurso a gestionar solamente lo puede utilizar el usuario actual.

- Abierto: El recurso a gestionar lo puede utilizar cualquier usuario.

Empezamos explicando los diferentes estados operativos:

- NP-B: No preparado-bloqueado : El recurso a gestionar está administrativamente prohibido de utilizar y además no está operativo. Para hacerlo disponible para la gestión es necesario obtener permiso administrativo y realizar sobre él alguna acción correctora.

- P-B: Preparado-bloqueado: El recurso a gestionar está administrativamente prohibido de utilizar pero está operativo. Para hacerlo disponible para la gestión es necesario obtener permiso administrativo.

- T : Se realiza una transición automática a preparado-bloqueado.

- C-B: Activo-cerrado: El recurso a gestionar está operativo y en uso pero la utilización del mismo solamente está permitida al usuario actual. Para que otros usuarios puedan utilizarlo es necesario obtener permiso. Cuando el usuario actual haya finalizado su utilización, pasara a estado preparado bloqueado.

- C-O: Cerrado-ocupado: El recurso a gestionar está operativo y en uso pero la utilización del mismo solamente está permitida al usuario actual. Además no tiene capacidad para atender otras operaciones de gestión de otros usuarios.

Para poder atender a los requerimientos de gestión de otros usuarios es necesario esperar a que finalice sus operaciones el usuario actual y además obtener el correspondiente permiso administrativo.

De otra forma cuando el usuario haya terminado la utilización del recurso gestionado, este realizará la transición automática al estado Preparado-Bloqueado.

- A-NP: Abierto-no preparado: Está permitido el uso administrativo del recurso a gestionar, pero el recurso no está operativo. Se necesita realizar alguna operación correctora para hacerlo disponible para la gestión.

- A-P: Abierto-preparado: El recurso está operativo y disponible para la gestión pero en este momento no se está utilizando.

- A-P: Abierto-activo: El recurso está operativo y se está utilizando pero tiene capacidad residual para su utilización adicional.

- A-P: Abierto-ocupado: El recurso está operativo y se está utilizando y no tiene capacidad residual para su utilización adicional. Por lo que para que otros usuarios puedan utilizarlo es necesario esperar a que finalice el usuario actual.

Tabla I. Estados de operación de los recursos gestionados

Estados Administrativos	Estados Operativos			
	No Preparado	Preparado	Activo	Ocupado
Bloqueado	NP-B	P-B	NO	NO
Cerrado	T	T	A-C	O-C
Abierto	NP-A	P-A	A-B	A-B

La gestión de cambios de la configuración:

Proporciona un entorno para poder revisar cambios y la interacción entre los mismos.

Proporciona un mecanismo para detectar los conflictos reales y potenciales cuando se realizan cambios de configuración.

Proporciona ayuda en la localización de fallos al disponer de un registro de los cambios recientes en la red.

Proporciona ayuda para optimizar las prestaciones de la red.

Es un soporte para la distribución de versiones de software.

La gestión de nombres y direcciones:

Permite realizar la topología de la red adaptada al usuario.

Permite dirigirse a los dispositivos por nombres amigables y significativos para el usuario.

2.1.2 Gestión de fallos y recuperación

La gestión de fallos y recuperación comprende el conjunto de facilidades que permite la detención, el aislamiento y la corrección de las operaciones anormales de las redes o sistemas de comunicación.

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 o 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 el número de errores con la misma causa supera un cierto umbral da lugar a un fallo.

Por orden de importancia los dispositivos causantes de fallos de los sistemas de comunicación son los siguientes:

- Líneas de comunicación
- Terminales
- Computadoras centrales
- Módem
- Procesadores de comunicaciones
- Otros componentes

La disponibilidad de un componente aislado se puede calcular de la siguiente manera:

D = TMEF / (TMEF + TMR)

Donde:

TMEF = Tiempo medio entre fallos

TMR = Tiempo medio de reparación

En el tiempo medio de reparación hay que incluir el período de tiempo necesario para informar del fallo, el tiempo dedicado al diagnóstico del mismo,

el propio tiempo de reparación y el tiempo necesario para restaurar el servicio de comunicaciones interrumpido.

La disponibilidad de un sistema de comunicaciones podría calcularse como un porcentaje de terminales-hora disponibles sobre el porcentaje total.

Los actuales servicios de redes privadas virtuales ofrecen por contrato una determinada disponibilidad de servicio expresada en tanto por ciento, y calculada de la forma anteriormente mencionada.

La disponibilidad de un componente aislado puede mejorarse de dos maneras factibles:

- Aumentando el tiempo medio entre fallos, incrementando la fiabilidad del componente o sistema.

- Disminuyendo el tiempo de reparación.

La disponibilidad de los servicios de comunicaciones que proporcionan las las redes puede ser mejorada por las siguientes acciones:

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

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

- Añadido de componentes redundantes.

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 diagnóstico 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 diagnóstico.

- Control y seguimiento de la resolución de los fallos. Para ello se suele disponer de facilidades para gestión de los boletines de averías.

  Un boletín de avería es un documento informativo que tiene existencia mientras dura un fallo.

Una buena gestión de los boletines de averías es indispensable para tener una buena calidad de servicios.

La base de datos histórica de boletines de avería ayuda a identificar las partes más débiles de las redes y por tanto proporciona información muy valiosa para que en futuras adquisiciones de equipos se seleccionen aquellos más fiables a los procedentes de vendedores con mejor servicio.

Detección, diagnóstico, corrección de los fallos de la red y de las condiciones de error, incluye:

- Notificación de fallos
- Sondeo periódico en busca de mensajes de error
- Establecimiento de alarmas

2.1.3 Gestión de prestaciones

Se define como la evaluación del comportamiento de los elementos de la red, para poder efectuar este análisis es preciso mantener un histórico con datos estadísticos y de configuración.

Esta área funcional comprende el conjunto de funciones destinadas a la obtención de información para conocer en todo momento:

- El grado de utilización de los recursos 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. Son posibles por tanto cuatro situaciones distintas y algunas adicionales intermedias.

La recogida de estadísticas acerca del tráfico de los elementos de la red, es el método más empleado para el cálculo y conocimientos del grado de utilización de los recursos de la red.

Estas estadísticas deben guardarse en bases de datos históricas para poder disponer de la historia de la red.

Del análisis comparativo de estas bases de datos históricas pueden obtenerse datos sobre el ritmo de crecimiento del tráfico con objeto de realizar ampliaciones, etc.

Para la obtención del nivel de servicio al usuario es necesaria la realización de medidas orientadas a las características de servicio.

La mayoría de estas medidas van orientadas a la obtención de:

- Tiempo de respuesta
- Ritmo de errores
- Caudal de *bits/s*
- Porcentaje de éxito en la obtención del servicio

En la tabla siguiente se consideran los valores extremos del grado de utilización y nivel de servicio, teniendo en cuenta:

- A-A : En este caso y suponiendo valores medios, es necesario prever la ampliación de los recursos de la red.

- A-B : Si la situación está estabilizada desde hace mucho tiempo significa que la red está sobredimensionada.

- B-A : Aquí es necesario realizar una ampliación de los recursos de la red.

- B-B : Esta situación es indeseable y necesita un rediseño de la red, porque la solución de que se dispone no se adapta al servicio que proporciona.

Tabla II. Valores extremos del grado de utilización y nivel de servicio de los recursos de la red

Nivel de Servicio	Grados de Utilización	
	Alto	Bajo
Alto	A-A	A-B
Bajo	B-A	B-B

Anteriormente hemos considerado valores medios, pero es necesario disponer de medidas de nivel de servicio en condiciones de carga para prever el comportamiento de la red en condiciones extremas.

Los resultados obtenidos pueden proporcionar información para la incorporación de recursos en las redes, orientadas a evitar las consecuencias de las situaciones extraordinarias.

2.1.4 Gestión de contabilidad

Esta área funcional permite identificar los costes de la utilización de los recursos para que en función de los mismos poder establecer los cargos por consumo de los mismos.

Dependiendo del sistema gestionado, los cargos pueden convertirse en facturas. Por ejemplo, en los sistemas de comunicaciones que dan servicios comerciales.

Esta área funcional proporciona las herramientas necesarias para mantener informados a los usuarios de la red de la utilización realizada de los recursos.

Los procedimientos que permiten conseguir esta funcionalidad son:

- La identificación del uso de recursos y el intercambio de información entre diferentes sistemas de comunicaciones.

- La información sobre tarifas y límites para ciertos recursos, y la posibilidad e establecer estos límites.

- La posibilidad de compartir costes cuando dos o más sistemas de comunicaciones cooperan en la prestación de un servicio.

En el caso de redes de una corporación, los usuarios de los recursos son internos y no se cobra ni se paga por utilización de los servicios.

Aún en este caso llegan a calcularse los cargos aunque no se pasan facturas.

Los procedimientos destinados a la medida de los recursos consumidos en el caso de redes que prestan servicios comerciales son de la máxima importancia ya que:

- La facturación a los usuarios finales es el fin último 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 comprensión y administración.

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

- Las estrategias para establecer los cargos pueden basarse en:

  - Localización geográfica

  - Nivel de utilización:
    - Número de paquetes / caracteres.
    - Transacciones.
    - Tiempo de conexión

- Tamaño del departamento o división

2.1.5 Gestión de seguridad

El propósito de esta área es el de servir de soporte a la aplicación de políticas de seguridad. Los mecanismos que proporciona son.

- La creación, eliminación y mantenimiento de servicios y mecanismos de seguridad de acuerdo con la política de seguridad establecida.

- La distribución de información de seguridad.

- La información acerca de las violaciones de la seguridad. También de los intentos fallidos.

El punto de partida del diseño de la seguridad de un sistema es la identificación de las vulnerabilidades del mismo. Las actuales comunicaciones son vulnerables porque corren el riesgo de ser escuchadas y modificadas de forma impune.

En general una comunicación es vulnerable si existe la posibilidad de que se produzca un efecto desautorizado en la misma.

Las comunicaciones están amenazadas por todos aquellos que puedan obtener algún beneficio de su conocimiento. Por ataque entendemos la acción encaminada a modificar o alterar el sistema para llevar a cabo dicha amenaza.

Por tanto el diseño de las medidas de seguridad va orientado a evitar el efecto de los ataques.

La política de seguridad establece en rasgos generales lo que está o no permitido, luego cualquier posibilidad de comportamiento no autorizado en una red es un riesgo para el sistema.

La finalidad de las medidas de protección para hacer a los sistemas seguros, no es contrarrestar todos los ataques posibles, sino hacer el costo de los mismos suficientemente alto como para reducir el riesgo a límites aceptados.

La introducción de medidas de seguridad excesivas en los sistemas de comunicaciones incrementa el costo de los mismos y puede afectar negativamente a sus prestaciones.

En función de la valoración de los riesgos se adopta una determinada política de seguridad que contempla principalmente, además de procedimientos, métodos, normas, etc., las medidas de protección específicas que denominamos servicios de seguridad para contrarrestar los efectos de las amenazas.

No todos los usuarios del sistema necesitan el mismo nivel de seguridad. La seguridad depende de sus aplicaciones en concreto. La solución adecuada es que los usuarios definan sus políticas de seguridad y para su realización se apoyen en facilidades de seguridad sobre todo de gestión.

La política de seguridad de un sistema de comunicación debe establecer y definir lo que está o no autorizado. Indica la protección deseada incluyendo servicios de seguridad en la definición del sistema de comunicaciones con el fin de contemplar a nivel de especificación general del mismo las medidas de protección adecuadas para reducir a un nivel aceptable el riesgo.

Los riesgos que hay que tener en cuenta cuando se maneja información que se transmite por redes de telecomunicación se pueden clasificar en dos categorías:

- Referidos a la información: Lo más importante son la ausencia de disponibilidad, la alteración y destrucción e la misma y la revelación de las comunicaciones. Los sistemas de comunicaciones están sometidos a gran número de amenazas que no se habían previsto en el diseño de los mismos, como, falsificación de datos y programas, bombas lógicas, virus informáticos, caballos de troya y gusanos.

- Referidos a los interlocutores: El riesgo más importante es la falsificación de identidad. Las actuales técnicas de verificación de identidad basadas en contraseñas (*password*) pueden ser vulnerables.

En cuanto al análisis de riesgos, va estrechamente unido al servicio de comunicaciones especifico que preste el sistema de comunicaciones consideradas.

En general se deben seguir los siguientes pasos:

- Valorar el costo que supone para el intruso (posible atacante) la acción de llevar a cabo cada posible amenaza.

- Valorar los beneficios que puede obtener el intruso en caso de llevar a cabo con éxito el ataque.

- Valorar las pérdidas que para el usuario ocasionaría la realización el ataque.

- Valorar el coste de las medidas de protección que contrarrestan la amenaza. Desde ningún punto de vista será razonable la incorporación de medidas de seguridad que resulten más caras que los propios ataques a que se oponen.

Proporcionar seguridad completa en las redes abiertas de comunicaciones contra estos riesgos es un problema más complejo que proteger entornos informáticos centralizados, por ejemplo centros de cálculo.

En general, al especificar las medidas de seguridad necesarias para protección de la información en entornos de redes de comunicaciones, se deben considerar los siguientes aspectos: seguridad física, seguridad personal, seguridad administrativa, seguridad de los servidores y de seguridad de las comunicaciones.

Dado que, por razones económicas, es inviable pensar en medidas de protección físicas extensibles a todo el ámbito de las redes, la técnica adecuada es el empleo de la criptografía, complementada con algunas medidas adicionales de protección física en puntos localizados.

Las técnicas criptográficas ofrecen las mejores soluciones para hacer frente a los riesgos comentados anteriormente. Pueden resolver los problemas de seguridad externa de las redes de comunicaciones y mejorar los aspectos de seguridad interna de las mismas.

Desde hace una década se han empezado a utilizar en redes privadas pero, hasta ahora, su empleo no se ha extendido al entorno de las redes públicas debido, fundamentalmente, al problema de la distribución de las claves.

La gestión de claves comprende los procedimientos necesarios para la generación, distribución, administración y mantenimiento de las claves.

Los sistemas de cifrado simétricos y asimétricos plantean problemas de gestión de claves diferentes, pues mientras en los simétricos hay que distribuir una clave secreta que comparten los interlocutores de la comunicación, en los asimétricos desaparece el problema de mantener en secreto las claves al poder hacer pública una de ellas pero, sin embargo, sigue siendo necesaria la verificación de origen de la clave pública.

En cuanto a la generación de las claves, se trata esencialmente de procesos de obtención de números aleatorios.

En general, se pueden considerar los siguientes procedimientos:

- Generación manual

- Generación basada en medidas de fenómenos impredecibles.

- Generación de números seudoaleatorios.
- Generación basada en utilización de un sistema criptográfico.

En cuanto a la distribución de las claves criptográficas, se han venido utilizando diversos procedimientos en función del entorno concreto de comunicaciones en que se introduce el sistema criptográfico. A continuación se hace una clasificación de los mismos:

- Instalación en el equipo criptográfico. No requiere ninguna actividad de gestión de claves y tiene una aplicación limitada.

- Distribución manual. La clave a utilizar en la comunicación es generada por duplicado y se distribuye de forma manual a los interlocutores por un canal físicamente seguro.

- Distribución jerárquica. Se utilizan varios niveles de claves. Una clave de nivel superior se utiliza para cifrar una clave de nivel inferior que posteriormente se envía al otro interlocutor por la red de comunicaciones.

- Distribución centralizada. Toda la gestión de las claves se realiza en un centro que comparte una clave distinta con cada uno de los terminales. Este puede realizar funciones de: centro de distribución de claves, centro de traducción de claves o centro de gestión de claves.

- Comunicación de la clave en claro. El método más conocido es: el método de intercambio exponencial de claves.

- Utilización de una guía de claves públicas. Es necesario garantizar que las claves públicas sean verídicas.

- Utilizando las claves públicas para comunicar la clave simétrica a utilizar en cada comunicación.

2.2 Componentes de la arquitectura de gestión OSI

La arquitectura de gestión OSI define un objeto gestionable como la interfaz conceptual que han de presentar los dispositivos que ofrecen funciones de gestión. El proceso de supervisión y control de un objeto gestionable se realiza mediante una serie de interacciones. Estas interacciones son de dos tipos:

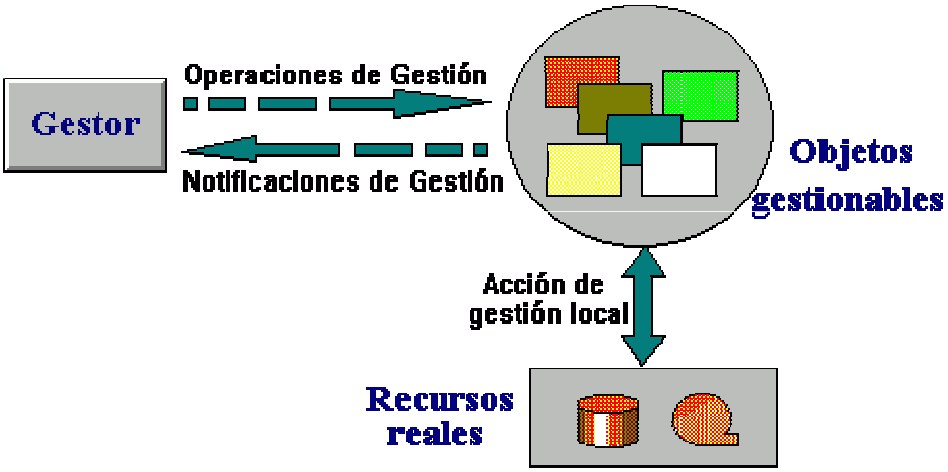
- De operación: el gestor solicita algún dato al objeto gestionable o desea realizar alguna acción sobre él.

- De notificación: cuando el objeto gestionable intenta enviar algún dato al gestor como consecuencia de algún evento ocurrido en el dispositivo.

  Un objeto gestionable se caracteriza además por un conjunto de atributos que son las propiedades o características del objeto, y un comportamiento en respuesta a las operaciones solicitadas.

En la siguiente figura se presenta un ejemplo de estas interacciones.

Figura 2. Interacciones de un objeto gestionable



La comunicación entre el gestor y el objeto gestionable no es directa, se realiza mediante un intermediario: el agente de gestión, esto se corresponde con modelo centralizado gestor-agente. La función del agente es controlar el flujo de información de gestión entre el gestor y el objeto. Este control lo realiza comprobando una serie de reglas de gestión por ejemplo que el gestor tenga la capacidad para solicitar una determinada operación. Estas reglas se incluyen en los datos como parte de la solicitud de una operación.

El flujo de la información de gestión y control entre el gestor y el agente se realiza mediante el protocolo CMIP, perteneciente al nivel de aplicación OSI.

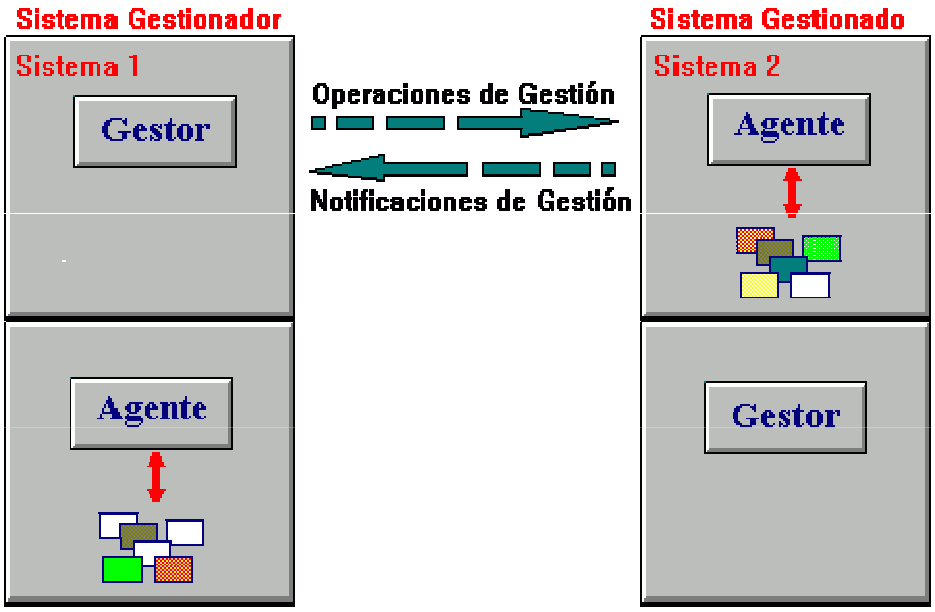
El protocolo permite que un sistema se pueda configurar para que opere como gestor o como agente. La mayoría de las realizaciones prácticas de sistemas gestionadas se configuran con unos pocos sistemas operando en modo gestor, controlando las actividades de un gran número de sistemas operando en modo agente.

Cuando dos procesos se asocian para realizar una gestión de sistemas, deben establecer en qué modo va a operar cada uno de ellos (en modo agente o en modo gestor). Lo procesos indican, mediante las denominadas unidades

funcionales, qué funcionalidades de gestión y estándares utilizarán durante la asociación.

La asociación de dos procesos de gestión la ejemplificamos en la siguiente gráfica:

Figura 3. Asociación de dos procesos para realizar una gestión de sistemas.



Otros componentes de la arquitectura de gestión OSI son:

- Estructura de la Información de Gestión (*Structure of Managment Information, SMI*). Define la estructura lógica de la información de gestión OSI. Establece las reglas para nombrar a los objetos gestionables y a sus atributo. Define un conjunto de subclases y tipos de atributos que son en principio aplicables a todos los tipos de clases de objetos gestionables.

- Base de información de Gestión (*Managment Information Base, MIB*). Representa la información que se está utilizando, modificando o transfiriendo en la arquitectura de los protocolos de gestión OSI. La MIB conoce todos los objetos gestionables y sus atributos. No es necesario que este centralizada físicamente en un lugar concreto, puede estar distribuida a través del sistema y en cada uno de sus niveles.

- CMIS (*Common Managment Information 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 servicio CMIS que son utilizadas por las SMFAs.

2.3 Modelo de INTERNET (SNMP)

En 1998, el IAB (*Intenet Activities Board*, Comité de Actividades de Inter.-red) determinó la estrategia de gestión para TCP/IP (*Transfer Control Protocol* /*Internet Protocol*, Protocolo de Control de Transimisión/Protocolo de Inter-red). Esto significó el nacimiento de dos esfuerzos paralelos, la solución a corto plazo, SNMP, y la solución eventual a largo plazo, CMOT (*CMIP over TCP/IP*, CMIP sobre TCP/IP).

CMOT pretendía implantar los estándares del modelo de gestión OSI en el entorno de Internet (TCP/IP). CMOT tuvo que afrontar los problemas derivados de la demora en la aparición de especificaciones y la ausencia de implementaciones prácticas. Como consecuencia de ello, la iniciativa CMOT fue paralizada en 1992.

SNMP es una extensión del protocolo de gestión de red para gateways SGMP (*Simple Gateway Monitoring Protocol*, Protocolo sencillo de supervisión de pasarelas), que se convirtió en 1989 en el estándar recomendado por Internet.

Está dirigido a proporcionar una gestión de red centralizada que permita la observación, el control y la gestión de las instalaciones. Utilizando SNMP, un administrador de red puede direccionar preguntas y comandos a los dispositivos de la red.

SNMP se ha convertido, debido al enorme éxito que ha tenido desde su publicación, en el estándar de facto de gestión de redes. Prácticamente todo el equipamiento de redes puede ser gestionado vía SNMP.

Algunas de las funciones que proporciona SNMP son:

- Supervisión del rendimiento de la red y su estado.

- Control de los parámetros de operación.

- Obtención de informes de fallos.

- Análisis de fallos.

El protocolo SNMP incorpora varios elementos presentes en otras estándares como el modelo gestor-agente, la existencia de una base de datos de información de gestión (MIB) o el uso de primitivas de tipo PUT y GET para manipular dicha información. A continuación se describen dichos elementos:

- Agente : equipamiento lógico alojado en un dispositivo gestionable de la red. Almacena datos de gestión y responde a las peticiones sobre dichos datos.

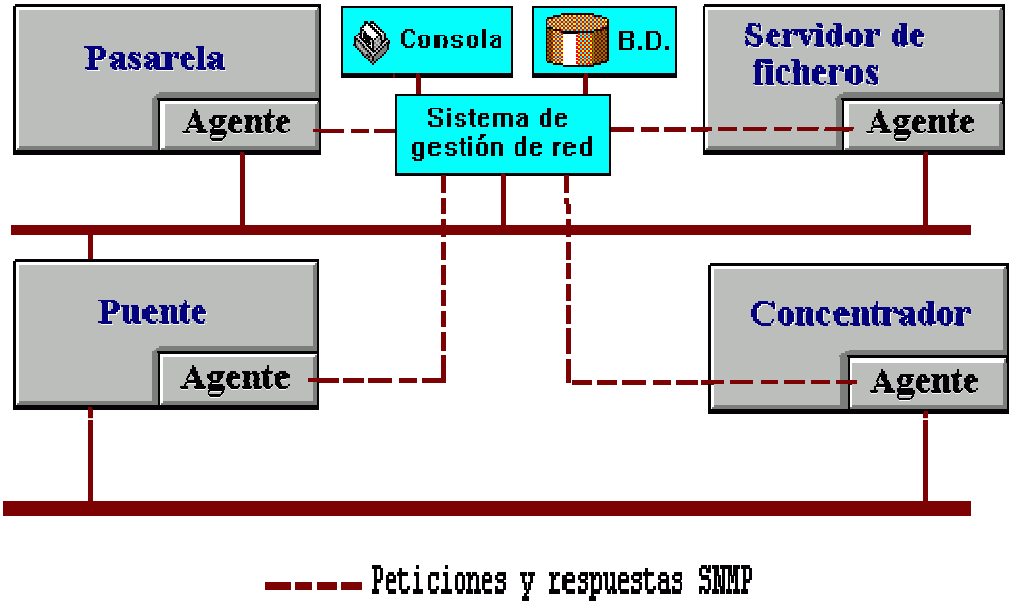
- Gestor : equipamiento lógico alojado en la estación de gestión de red. Tiene la capacidad de preguntar a los agentes utilizando diferentes comandos SNMP.

- MIB (Base de Información de Gestión) : base de datos virtual de los objetos gestionables, accesible por un agente, que puede ser manipulada vía SNMP para realizar la gestión de red.

El protocolo SNMP realiza las funciones descritas anteriormente llevando información de gestión entre los gestores y los agentes.

En la figura siguiente se presenta un ejemplo de sistema de gestión SNMP.

Figura 4. Sistema de gestión SNMP



El protocolo SNMP es sólo un aspecto dentro de toda la estructura de gestión, la cual está compuesta de los siguientes elementos:

- Estación de Gestión de Red (*Network Managment 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 computadora personal.

- Estructura de Información de Gestión (SMI) : Es un conjunto de reglas que definen 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 (MIB) : Es una colección de objetos, que representan de forma abstracta los dispositivos de la red y sus componentes internos. La MIB es conforme a la SMI para TCP/IP. Cada agente SNMP contiene instrumentación que, como mínimo, debe ser capaz de reunir objetos MIB estándar. Estos objetos incluyen direcciones de red, tipos de interfaz, contadores y datos similares.

El estándar MIB de Internet define 126 objetos relacionados con los protocolos TCP/IP. Los fabricantes que deseen pueden desarrollar extensiones del estándar MIB. Estas MIBs privadas incorporan un amplio rango de objetos gestionables, y algunas veces contienen objetos que son funcionalmente similares a los MIBs ya definidos, en otros casos el cambio de una variable en un objeto inicia una batería de funciones en el dispositivo gestionado, como por ejemplo un autodiagnóstico.

La carga de la gestión de todas las MIBs y de las extensiones privadas recae en el sistema de gestión. Las MIBs están escritas en una variante simple de lenguaje de definición OSI ASN.1 .

En 1990 se introdujo una nueva versión de MIB, MIB II, done la mayor aportación es la utilización de 185 nuevos objetos de extensiones privadas.

Aparte de la MIB, existe la base de datos de estadísticas de red (NSD) que está en la estación de trabajo de gestión. En esta base de datos se recoge

información de los agentes para realizar funciones de correlación y planificación.

Las limitaciones de SNMP se deben a no haber sido diseñado para realizar funciones de gestión de alto nivel. Sus capacidades lo restringen a la supervisión de redes y a la detección de errores. Como todos los elementos TCP/IP, ha sido creado pensando más en su funcionalidad y dejando a un lado la seguridad.

2.3.1 SNMPv2 y V3

En 1996 se publicó un nuevo estándar, el protocolo SNMPv2, resultado de una serie de propuestas para mejorar las características de SNMP. Los cambios se traducen fundamentalmente en una mejora de las prestaciones, un aumento de la seguridad y en la introducción de una jerarquía de gestión.

Prestaciones

SNMPv2 mejora el mecanismo de transferencia de información hacia los gestores, de forma que se necesitan realizar menos peticiones para obtener paquetes de información grandes.

2.3.1.1 Seguridad

A diferencia de SNMP, que no incorpora ningún mecanismo de seguridad, SNMPv2 define métodos para controlar las operaciones que están permitidas.

Desafortunadamente surgieron dos planteamientos diferentes en cuanto al modelo de seguridad, que han dado lugar a dos especificaciones conocidas como SNMPv2 y SNMPv2u.

Se están realizando esfuerzos para unificar ambos enfoques en un único estándar el SNMPv3.

2.3.1.2 Gestión jerárquica

Cuando el número de agentes a gestionar es elevado, la gestión mediante el protocolo SNMP se vuelve ineficaz debido a que el gestor debe sondear periódicamente todos los agentes que gestiona.

SNMPv2 soluciona este inconveniente introduciendo los gestores de nivel intermedio. Son estos últimos los que se encargan de sondear a los agentes bajo su control. Los gestores intermedios son configurados desde un gestor principal de forma que solo se realiza un sondeo de aquellas variables demandadas por este último, y solo son notificados los eventos programados.

SNMPv2 también introduce un vocabulario más extenso, permite comandos de agente a agente y técnicas de recuperación de mensajes.

2.3.2 RMON

La especificación RMON (monitorización remota) es una base de información de gestión (MIB) desarrollada por el organismo IETF (Internet Engineering Task Force) para proporcionar capacidades de monitorización y análisis de protocolos en redes de área local. Esta información proporciona a los gestores una mayor capacidad para poder planificar y ejecutar una política preventiva de mantenimiento de la red.

Las implementaciones de RMON consisten en soluciones cliente servidor. El cliente es la aplicación que se ejecuta en la estación de trabajo de gestión, presentando la información de gestión al usuario. El servidor es el agente que se encarga de analizar el tráfico de red y generar la información estadística. La comunicación entre aplicación y agente se realiza mediante el protocolo SNMP.

RMON es una herramienta muy útil para el gestor de red pues le permite conocer el estado de un segmento de red sin necesidad de desplazarse físicamente hasta el mismo y realizar medidas con analizadores de redes y protocolos.

Las iniciativas se dirigen en estos momentos hacia la obtención de una mayor y más precisa información. En concreto, se trabaja en la línea de analizar los protocolos de nivel superior, monitorizando aplicaciones concretas y comunicaciones extremo a extremo. Estas facilidades se incorporarán en versiones sucesivas de las espedificación RMON II.

2.3.3 Comparación SNMP – CMIP

A continuación se hace una comparación entre los protocolos SNMP y CMIP:

- SNMP está basado en técnicas de sondeo, mientras que CMIP utiliza una técnica basada en eventos. Esto permite a CMIP ser más eficiente que SNMP en el control de grandes redes.

- CMIP es un protocolo orientado a conexión mientras que SNMP es un protocolo sin conexión. Esto significa que la carga de proceso de SNMP es reducida, pero cuando se envía un mensaje nunca se puede asegurar que el mensaje llega a su destino. La seguridad de los datos no es prioritaria para SNMP.

- CMIP permite la implementación de comandos adicionales sofisticados, mientras que SNMP necesita el nombre de cada objeto.

- CMIP permite, mediante una única petición, la recogida de gran cantidad de datos de los objetos gestionables, enviando información de retorno en múltiples respuestas, esto no está permitido en SNMP.

- CMIP está especialmente preparado para gestionar grandes redes distribuidas, mientras que SNMP está recomendado para la gestión Inter-red.

- CMIP realiza una distinción clara entre los objetos y sus atributos. SNMP no permite esto, lo cual hace imposible la reutilización de atributos y definiciones.

2.4 Funcionalidades básicas de un sistema de gestión

A continuación se describen las funciones básicas que contempla un sistema de gestión, dependiendo del tipo de red en dónde se utilice.

2.4.1 Gestión de redes pequeñas

En redes con pocos usuarios, con un número de dispositivos de red bajo, es suficiente con un sistema de gestión que ofrezca las funciones básicas de supervisión:

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

- Presentación de la información de la configuración.

- Representación gráfica de los nodos instalados en la red.

- Indicación del estado de los componentes individuales, es decir, cuáles están activos y cuáles inactivos.

- En caso de avería, indicación del tipo de está.

- 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.

Es importante que los sistemas de gestión sean fáciles de instalar y operar, y con interfaz gráfica (menús, iconos, campos de texto, ayudas, etc.). Es conveniente que se presenten los resultados de forma comprensible y que los procedimientos de consulta sean sencillos.

2.4.2 Gestión de redes medianas y grandes

En redes de mayor complejidad son necesarias 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, pérdidas de rendimiento y problemas de configuración mediante políticas de gestión preventivas.

- Recuperación automática ante fallos.

- Proveer los mecanismos avanzados para la seguridad de la red y de los datos.

- Capacidad para representar gráficamente en tiempo real la totalidad de la red, partes de la misma y los sistemas conectados en cada punto, de forma que la gestión no se convierte en una tarea excesivamente compleja.

- Capacidad para supervisar desde una única estación la totalidad de los tipos de red que pueden existir como por ejemplo: *Ethernet, Token ring, FDI*, etc.

- 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.

3. HERRAMIENTAS DE GESTIÓN

3.1 Introducción

Un sistema de gestión que dispusiera de facilidades para la realización de todas las funciones de gestión, sería un sistema muy caro y muy complejo.

La solución es la especialización de los sistemas de gestión. La utilización de sistemas de gestión normalizados permite la gestión integrada aún utilizando distintos sistemas de gestión para controlar una red.

El estado del arte actualmente en gestión de redes es la existencia de un conjunto de equipos especializados en determinadas funciones de gestión que complementan a los sistemas de gestión de redes.

Actualmente, aunque se pueden diseñar sistemas de gestión que sean completos, e el sentido de incluir toda la funcionalidad necesaria para gestionar una red, no es la práctica habitual porque serían sistemas muy complejos y caros.

Se entiende por herramientas de gestión a las utilidades hardware y software que se emplean para ayudar a la realización de las actividades de gestión de red y que habitualmente no están incluidas en los sistemas de gestión.

Tradicionalmente el término herramientas de gestión se ha aplicado a equipos específicos diseñados para la monitorización y localización de fallos en los sistemas de comunicaciones.

El sistema de gestión informa del funcionamiento de la red y a partir de la información recogida se detectan malfuncionamiento.

A posteriori, con estos equipos específicos se trata de aislar e identificar el problema. Estos equipos se aplican a un trozo de la red en concreto y en un momento determinado.

Luego hay una diferencia fundamental en cuanto a las prestaciones de estos equipos respecto a las mismas funciones incluidas en el sistema de gestión.

El monitor de red consiste en una computadora y unos programas específicos que le permiten la captura de datos para poder realizar estadísticas de funcionamiento. Estos equipos incluyen también la facilidad de monitorización de señales en las interfaces.

Normalmente decodifican los protocolos sencillos carácter a carácter, los protocolos de nivel de enlace y a veces también X.25.

Lo más habitual es que sean equipos portátiles, que se pueden instalar en distintos puntos de la red para extraer de ella información de tipo estadístico, evolución de parámetros de funcionamiento, histogramas, tráfico por cada enlace, etc. Esta información es mostrada en forma de gráficos que hacen más fácil su interpretación.

Las funciones básicas que debe tener un monitor de red son:

- Poder extraer estadísticas globales de tráfico, número de errores, bytes transmitidos y recibidos, etc.

- Poder extraer estadísticas para cada terminal de la red y los errores que provoca.

- Proporcionar estadística en tiempo real y estadística históricas (carga máxima y medida por intervalos de tiempo)

- Determinar que ancho de banda se está utilizando en cada momento.

- Estatus de los servicios activos en un dispositivo.

Los analizadores de red son también computadoras que se pueden conectar a la red y que disponen de programas adecuados para poder decodificar protocolos de hasta nivel 4. Permiten capturar parte de la información que circula por la red, para después decodificar e interpretarla para ayudar en la localización de problemas.

Los analizadores de red permiten simular tráfico con el formato del protocolo correspondiente.

Las funciones básicas que debe tener un analizador de red son:

- Poder capturar y decodificar tramas, llegando hasta el nivel 4 de OSI, interpretando la información de los cuatro niveles para los protocolos más comunes.

- Generar tráfico simulado, de la forma más real posible, para presentar situaciones de mayor cargo en la red y así poder planificar y decidir futuras ampliaciones.

Son los equipos más completos para comprobar el funcionamiento de los sistemas de comunicaciones. Tiene capacidad para decodificar e interpretar protocolos de hasta nivel siete (capa de aplicación). A veces estos equipos son configurables por módulos de tal forma que se elige su configuración en función de los protocolos que implemente la red en particular.

4. ASPECTOS TÉCNICOS EN EL PROCESO DE ADQUISICIÓN DE UN SISTEMA DE GESTIÓN DE REDES

4.1 Tendencias tecnológicas y del mercado

En este capítulo se presenta la orientación suficiente a una organización para la preparación del conjunto de especificaciones que definirán los requisitos que han de cumplir los sistemas de gestión de redes, objeto de la adquisición.

Se realiza en primer lugar un análisis de las necesidades del comprador, a continuación se recogen los factores relevantes a tener en cuenta en el proceso de adquisición y , finalmente, se describe cómo deben ser planteadas las especificaciones técnico funcionales para la elaboración de un pliego de prescripciones técnicas, qué normas, estándares y cláusulas tipo pueden ser de aplicación, y cuál es el cuestionario técnico diseñado para normalizar las ofertas y facilitar su evaluación.

4.2 Análisis de las necesidades del comprador

Las razones para proceder a la adquisición de un sistema de gestión de redes pueden estar determinadas por diferentes factores. Es labor del administrador de la red la realización de un análisis de necesidades existentes dentro de su organización que permita determinar las necesidades actuales y futuras de los usuarios y las limitaciones o restricciones que ha de plantearse respecto al dimensionamiento del sistema. Es necesario tener en cuenta y analizar en profundidad los costes y beneficios asociados para obtener argumentos de peso en la toma de decisiones.

En la fase de análisis de necesidades, fase inicial del proceso de adquisición, hay que tener en cuenta todos aquellos requisitos, limitaciones y restricciones que afecten, entre otros, a los siguientes puntos:

4.2.1 Elementos gestionables

El comprador debe analizar los tipos de elementos que deben ser gestionados:

- Cables físicos
- Dispositivos de red
- Topologías de red
- Sistemas operativos de red

4.2.2 Equipos de comunicación que son gestionados e interoperatividad de protocolos

En el momento de comprar un sistema de gestión de red, el usuario debe analizar cuáles son sus necesidades relativas a qué protocolos deben ser soportados, de modo que el sistema que se adquiera ofrezca los máximos niveles en cuanto a flexibilidad, adaptabilidad y capacidad de expansión. Se deben realizar estimaciones de crecimiento de la red y tenerlas en cuenta durante esta fase.

Si en el entorno de gestión existen protocolos propietarios, el nuevo sistema de gestión debe tener, la capacidad y facilidad para la gestión de estos últimos.

4.2.3 Facilidades de detección y recuperación ante fallos

Ante fallos en la red, el usuario debe analizar cuáles son sus necesidades relativas a:

- Capacidad para aislar los elementos de red

- Facilidades de mantenimiento y recuperación ante errores.

4.2.4 Interfaz gráfico de usuario

Si las redes que van a ser gestionadas se encuentran geográficamente dispersas por un campus, conectan varias plantas de un edificio, interconectan diferentes edificios, etc., resulta muy interesante que el sistema de gestión que se vaya adquirir disponga de una interfaz gráfica de usuario con facilidades para el dibujo de mapas, planos de edificios sobre los que se podrá situar los equipos de comunicaciones, facilidades de zoom con las que se pueden observar diferentes niveles de detalle de red y capacidades para añadir y configurar nuevos iconos especialmente cuando se trate de un sistema de gestión de diseño a medida.

4.2.5 Facilidades de gestión remota

En ocasiones puede ser de gran utilidad disponer de un sistema de gestión que permita configurar la red remotamente y que la información disponible sobre la red sea consistente, independientemente de la ubicación física desde la que accede a la misma.

4.3 Factores relevantes en el proceso de adquisición de sistemas de gestión de redes

- Capacidad para soportar todos los elementos de la red:

El sistema de gestión debe permitir la integración de diferentes componentes y sistemas de interconexión. Cuando se dispone de diferentes redes, protocolos y dispositivos de red de diferentes fabricantes, se hace necesario que el sistema de gestión permita la gestión y supervisión de los diferentes elementos de red.

- Diseño a la medida:

Es muy importante que el sistema de gestión tenga capacidades de incorporación dinámica de nuevos elementos (nodos, enlaces, dispositivos, etc.) a la medida de las necesidades del usuario, de forma que se pueden definir, o programar, las características de cada elemento. El usuario debe poder adaptar la representación gráfica en caso de producirse cambios en la red, permitiéndosele realizar altas, bajas y modificaciones de cada uno de los elementos que forman parte de la red.

4.4 Cuestionario técnico de sistemas de gestión de redes

El siguiente cuestionario es de utilidad para conocer los protocolos de gestión, el tipo de redes gestionadas, el equipamiento físico y lógico, las operaciones y mantenimiento que ofrece una herramienta de gestión. Y se puede utilizar para ayudarnos en el momento de querer adquirir una herramienta de gestión.

Nota: (*) quiere decir que hay que indicar “1” en caso afirmativo.

Tabla III. Cuestionario técnico de sistemas de gestión de redes

Cuestión	Respuesta	Referencia a oferta (Página)
Protocolo de gestión		
CMIP(*)		
SNMP(*)		
SNMPv2(*)		
RMON(*)		
Otros (detallar)		
Equipamiento Físico y Lógico		
Características Físicas		
Tipo de Procesador		
Memoria Principal (RAM,MB)		
Capacidad de disco duro (MB)		
Resolución gráfica		

Continuación

Disponibilidad:		
UCP redundante (*)		
Fuente alimentación redundante (*)		
Sistema de impresión (*)		
Características Lógicas:		
Sistema Operativo:		
Unix (*)		
Windows 95/98/2000/XP (*)		
Windows NT/2003 (*)		
Otros (detallar)		
Interfaz de usuario:		
Carácter (*)		
Gráfico (*)		
Windows (*)		
PM (OS/2) (*)		
X-windows (*)		
Gestión vía web (*)		
Otros (detallar)		
Administración de red		
Tipos de redes gestionadas:		
LAN/MAN:		
8802.3 (*)		
8802.4 (*)		

Continuación

8802.6 (*)		
9384 (*)		
Wireles		
WAN (detallar)		
Otro detallar		
Configuración de red (topología)		
Indicación del estado de los componentes individuales (*)		
Herramientas de ingeniería y planificación (*)		
Operación de red		
Gestión, supervisión y actualización de los nodos en tiempo real (*)		
Seguridad:		
Establecimiento de derechos de acceso:		
Identificación (*)		
Palabra de paso (*)		
Detección de violación de seguridad (*)		
Flujo de datos y alarmas (*)		
Filtrado y gestión avanzada de eventos		

Continuación

Automatización Alarmas		
Mantenimiento:		
Control de dispositivos (*)		
Notificación automática de errores (*)		
Acceso automático desde la consola de gestión de red (*)		
Filtrado de alarmas (*)		
Definición de valores de umbral de alarmas (*)		
Aislamiento de fallos:		
De equipo Físico (*)		
De equipo lógico		
Recuperación automática ante fallos (*)		
Medidas preventivas (*)		

5. CASO PRÁCTICO

La herramienta de software que se implemento son un conjunto de módulos de libre distribución, que permite principalmente gestionar en tiempo real la disponibilidad de uno o más servicios que corren bajo el protocolo TCP/IP en un dispositivo de red.

Cuando un servicio de un dispositivo pasa de estado activo a inactivo la herramienta de gestión nos presenta dos tipos de notificación:

- En la pantalla donde se indica el estado de cada uno de los servicios de un dispositivo, el servicio que fallo cambia de color, indicando que esta en estado inactivo.

- Automáticamente se envía un correo electrónico al administrador del dispositivo indicándole que servicio ha fallado y en que dispositivo se encuentra la falla.

Cuando un servicio falla se nos permite abrir una nueva ventana para seguir las acciones definidas por el administrador para restablecer el servicio.

La herramienta de software incluye otros módulos adicionales que nos ofrecen servicios de red y de administración los cuales son:

- PING
- TRACEROUTE
- SCAN
- LOG
- Definir Nodo
- Eliminar Nodo
- Agregar Servicio

La herramienta de gestión se desarrollo en PERL, HTML y CGI.

5.1 PERL

Perl (*Practical Extraction and Report Lenguaje*) es un lenguaje de programación surgido a inicios de los noventas, que busca antes que nada el facilitar la elaboración de tareas comunes en sistemas de tipo UNIX, donde tradicionalmente las tareas de administración y proceso de datos se realiza con herramientas muy rudimentarias.

Las versiones de PERL son gratuitas.

Las plataformas donde más se ha desarrollado Perl son los servidores Unix, por sus necesidades de administración y lo robusto de su manejo de memoria y de procesos, además de la facilidad de Perl para realizar los así llamdos CGIs, interfaces para comunicar recursos del servidor con un servicio de INTERNET particular.

Algunas de las ventajas del uso del lenguaje Perl son las siguientes:

- Construcción de pequeños programas que pueden ser usados como filtros para obtener información de archivos.

- Se puede utilizar en varios sistemas operativos, siendo necesario únicamente el interprete de Perl correspondiente para cada sistema operativo.

- Es uno de los lenguajes mas utilizados en la programación de CGI scripts que utilizan la interface CGI (*Common Gateway Interface*), para intercambio de información entre aplicaciones externas y servicios de información.

5.2 *Cgi (Common gateway Interface)*

El CGI es una posibilidad de poner a disposición programas en Internet que pueden ser llamados con ayuda de páginas HTML y que pueden generar código HTML y enviarlos a un navegador.

Cuando uno busca en la WWW en un dato de bancos, firma un libro de visitas o mira un contador con la cantidad de visitantes, hay que tener en cuenta que por lo general siempre existe un CGI o un interfaz como CGI detrás de todo esto.

CGI son programas que se encuentran en un servidor en Internet y que al ser ejecutados procesan determinados datos. El procesamiento de datos ocurre en el servidor. Programas de CGI pueden memorizar en el servidor, por ejemplo, ha cuantas páginas se ha tenido acceso, o que ha escrito un visitante en un libro de visitas. Un programa CGI puede también por ejemplo generar código HTML llamando y leyendo datos ya memorizados. Esas páginas generadas dinámicamente son enviadas al navegador del usuario y pueden ser representadas en la pantalla, por ejemplo en la cantidad de visitantes en un contador o los mensajes que se encuentran en un libro de visitas.

La llamada interfaz o interface CGI debe ser apoyada por el software del servidor WWW. A vista de una persona que alquile un espacio en un servidor WWW, la interfaz CGI se encuentra a su disposición en forma de un determinado directorio. La mayoría de las veces este directorio tiene el nombre de cgi-bin. En este directorio se pueden almacenar programas que toman funciones de CGI.

5.3 HTML

El HTML es el lenguaje en que se escriben los hipertextos del *Word Wide Web*. Cumple la norma SGML (*Standardized Generalized Markup Languaje*) y, como si de un procesador de textos usual se tratara, permite añadir a un documento de texto diferente títulos y estilos y además puede incluir objetos multimedia (por ejemplo imágenes y sonido) y conexiones hipertextuales.

Todas estas características se representan en este lenguaje en forma de etiquetas (tags) que se insertan en el propio texto. Estas etiquetas se delimitan por medio de los signos “<” y “>”.

Un documento HTML comienza con la etiqueta “<html>”, y termina con “</html>”. En un documento existen dos zonas (entre las etiquetas de principio y fin de html) bien diferenciadas: el encabezamiento, delimitado por “<head>” y “</head>”, que sirve para definir diversos valores válidos en todo el documento; y el cuerpo, delimitado por “<body>” y “</body>”, donde reside la información del documento.

La utilidad más importante en el documento es “<title>” (que finaliza con el correspondiente “</title>”). Con esta instrucción declaramos cuál es el título de la página que estamos construyendo, y es muy importante para hacerse una idea de lo que contiene el documento.

Por otro lado, tenemos el cuerpo del documento. Bien, aquí es donde definimos todos los “enlaces”, insertamos las imágenes, e incluimos los diferentes formatos dentro del texto que vamos a introducir en nuestra página.

5.4 Explicación de los módulos de la aplicación de gestión

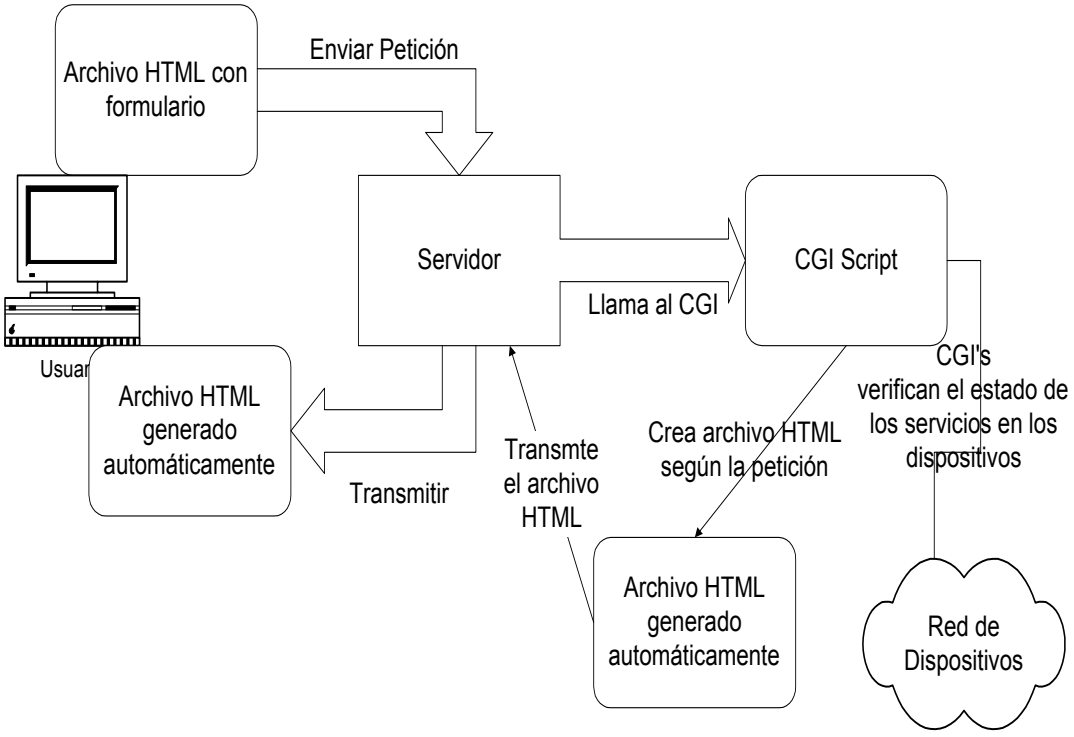
En PERL están los programas que a bajo nivel se encargan de traer el estado de cada unos de los dispositivos que se están gestionando, la información se almacena en archivos de texto en formato HTML.

En HTML están los archivos de la capa de presentación. Estos archivos son los que se presentan al usuario de una forma amigable indicando el estado de los servicios de un dispositivo o el resultado de cualquier otro modulo.

CGI es el intermediario entre los archivos generador en PERL y los archivos que se presentan al usuario.

La siguiente gráfica nos ilustra la comunicación que se lleva a cabo entre PERL, HTML y CGI.

Figura 5. Comunicación entre cgi*'s* en perl y páginas html



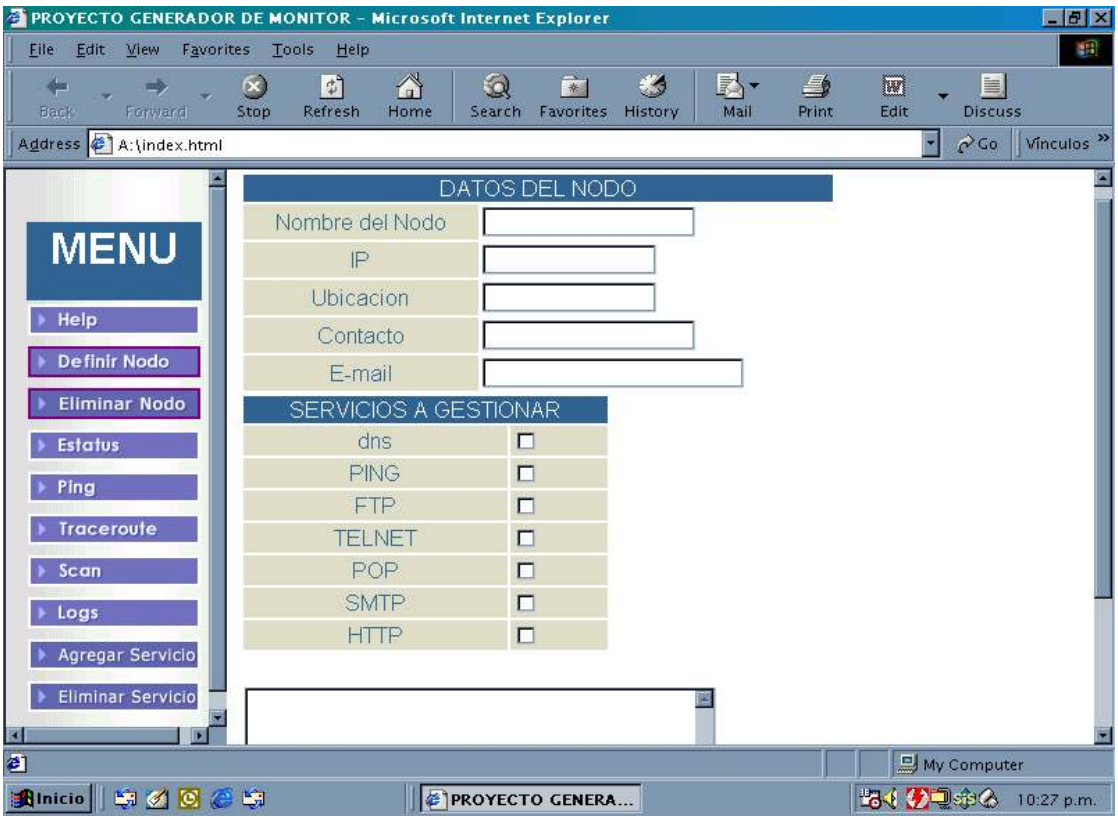
5.4.1 Módulo definir nodo

En este módulo se define el dispositivo y los servicios que se quieren gestionar, los datos más importantes que se indican aquí son los siguientes:

- IP : es la dirección IP del dispositivo
- *E-mail*: Es la dirección de correo electrónico del administrador del dispositivo, a dicha dirección se envía la notificación si un servicio llega a fallar.

También se seleccionan los servicios que se quieren gestionar en ese dispositivo. Si el servicio no existe se debe ir al módulo de agregar servicio e indicar el nombre del servicio y el puerto.

Figura 6. Módulo de definir nodo



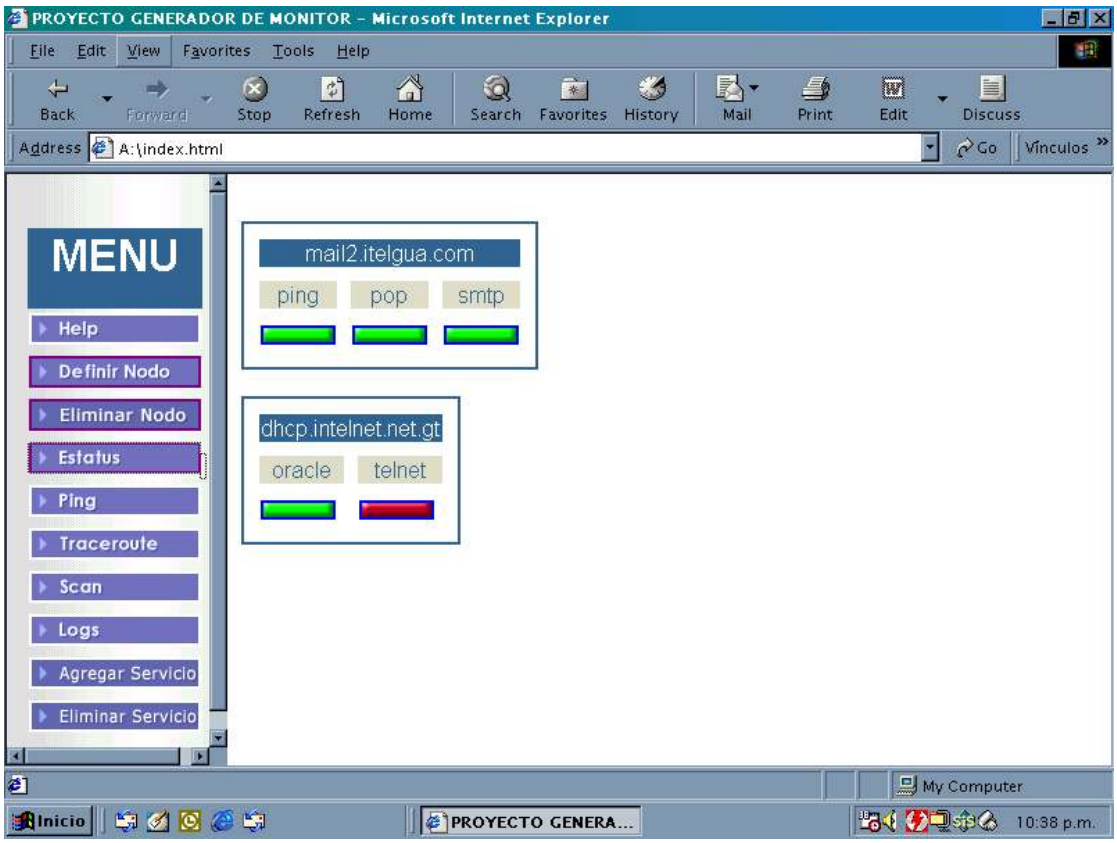
5.4.2 Módulo estatus

El módulo estatus es el más importante, en este módulo se visualiza el estado de los servicios de cada uno de los dispositivos.

Si el servicio está en color verde significa que su estado es activo, si está en color rojo significa que el servicio está en estado inactivo.

Cuando un servicio pasa de estado activo a estado inactivo se envía automáticamente un correo electrónico al administrador indicando el dispositivo y el servicio donde ocurrió la falla.

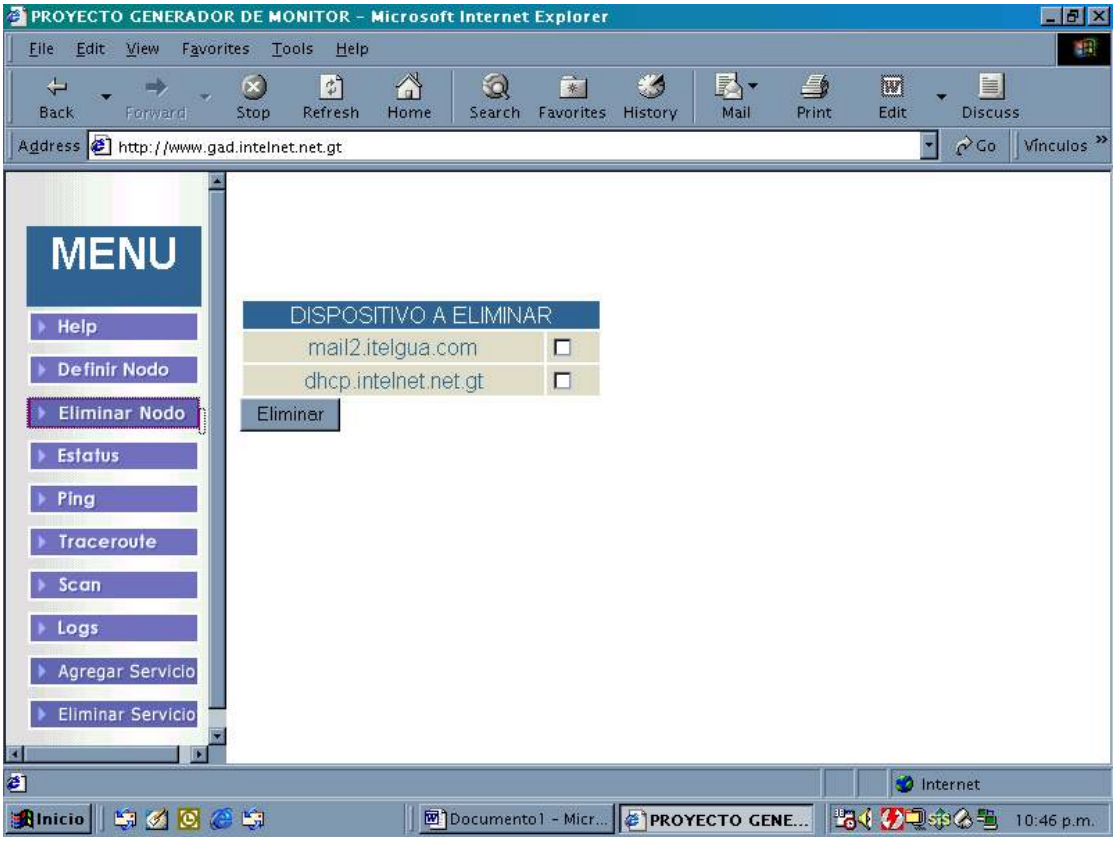
Figura 7. Módulo estatus.



5.4.3 Módulo eliminar nodo

El módulo eliminar nodo nos permite seleccionar el dispositivo que queremos eliminar. El dispositivo que se elimina desaparece automáticamente de la página del modulo estatus.

Figura 8. Módulo eliminar nodo

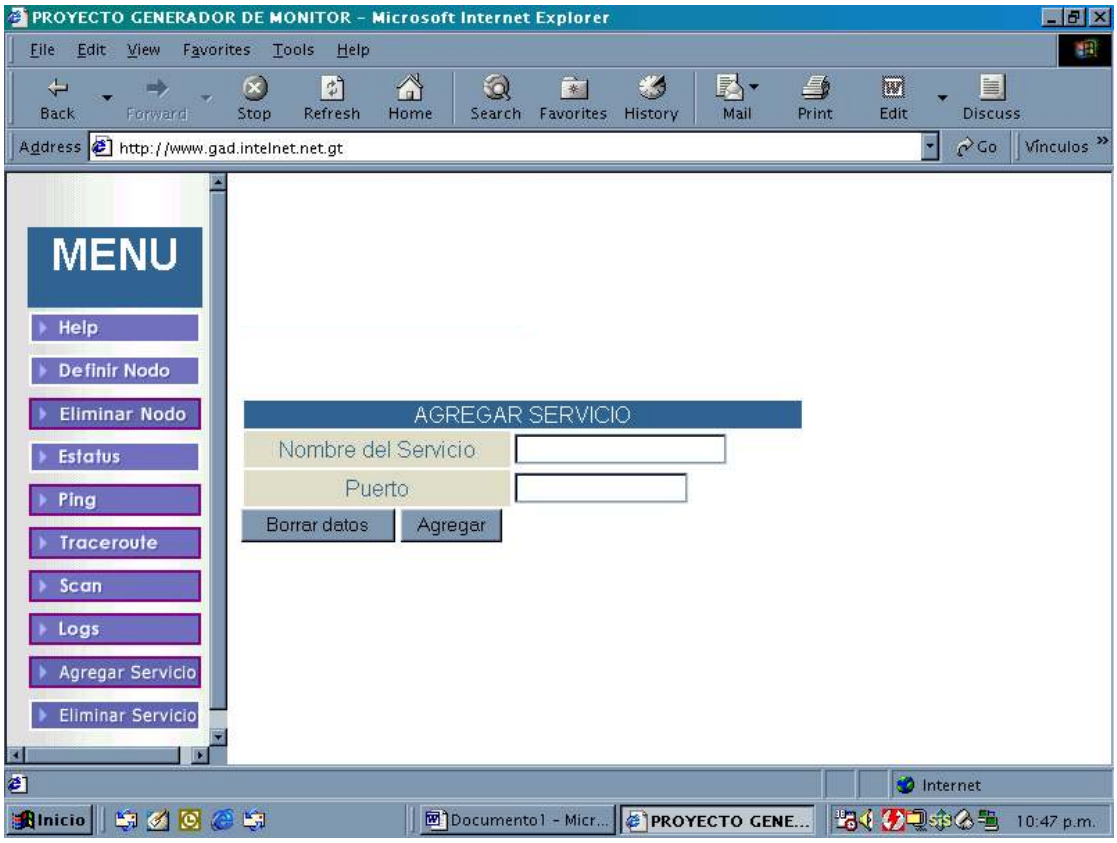


5.4.4 Módulo agregar servicio

Este módulo nos permite agregar un servicio indicando el nombre del servicio y el puerto del mismo. El servicio definido aparece automáticamente en el módulo de definir nodo.

Por ejemplo si queremos gestionar en un dispositivo el servicio de HTTP tenemos que indicar el nombre del servicio y el puerto donde corre dicho servicio, en el caso de HTTP es el puerto 80.

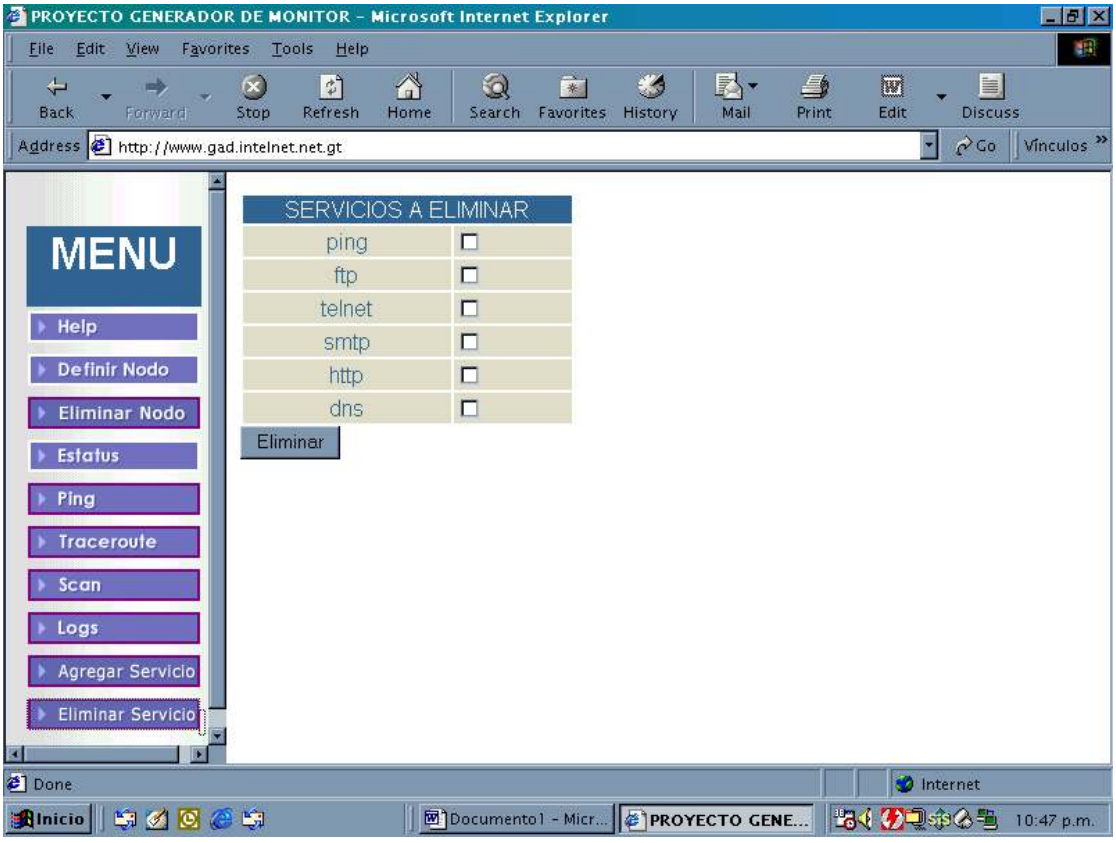
Figura 9. Módulo agregar servicio



5.4.5 Módulo eliminar servicio

El módulo eliminar servicio nos permite seleccionar un servicio para darle de baja. El servicio eliminado desaparece automáticamente de la página del módulo definir nodo.

Figura 10. Módulo eliminar servicio



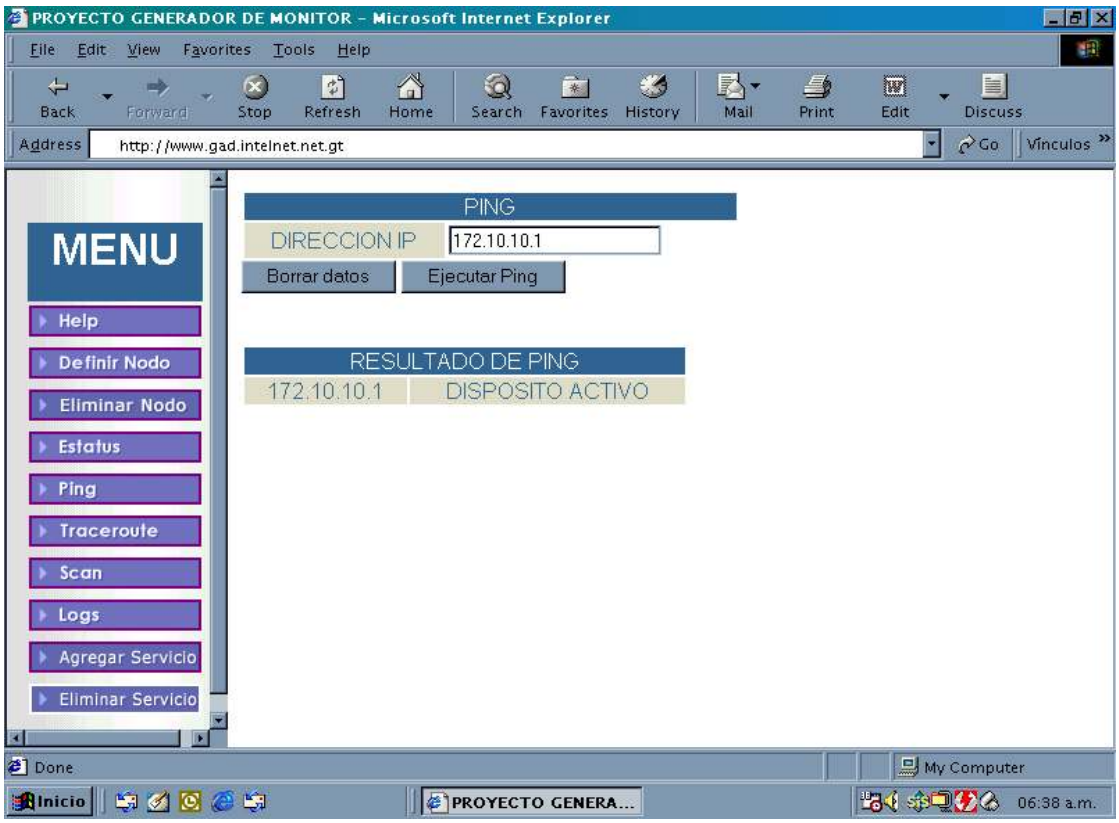
5.4.6 Módulo *ping*

Ping (Packet Internet Groper) es una herramienta de diagnostico para verificar la conectividad entre dos dispositivos de la red.

Este herramienta funciona de forma muy sencilla el comando seria ping y la dirección IP del dispositivo.

Cuando se ejecuta este comando, el dispositivo envía una serie de pequeños paquetes al dispositivo destino, cuando el dispositivo destino los recibe entonces manda una respuesta, y podemos estar seguros que ese dispositivo esta “vivo” o esta en la red.

Figura 11. Módulo de *ping*



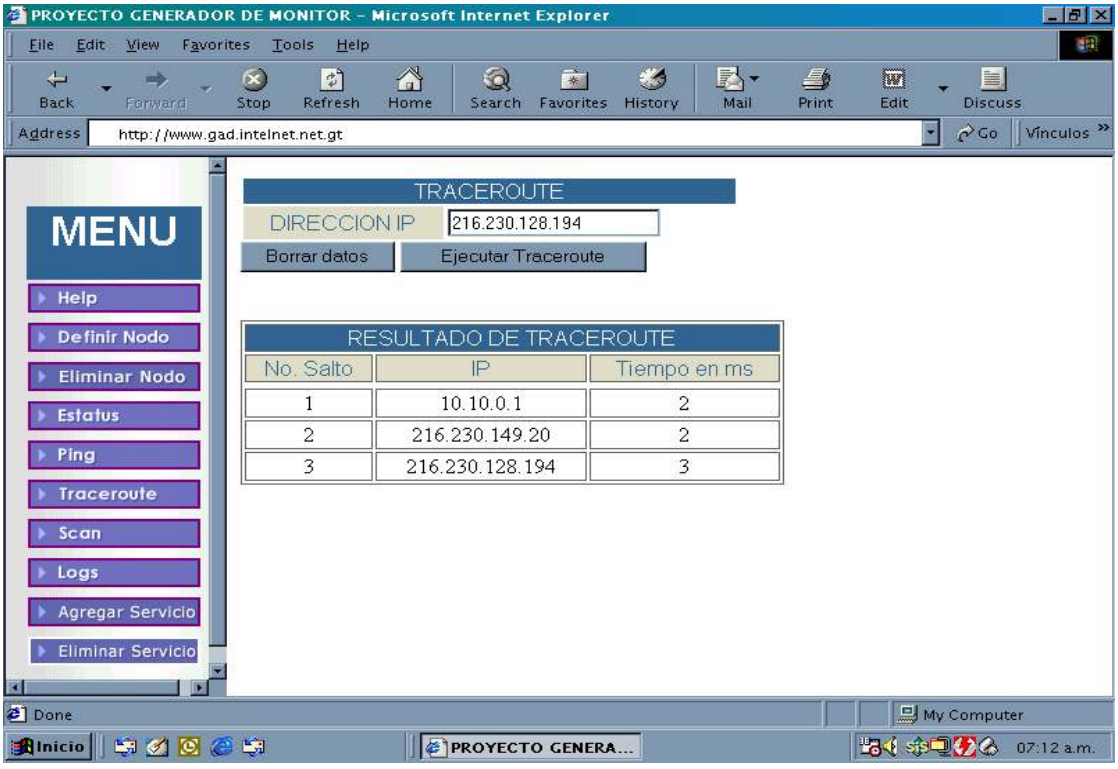
5.4.7 Módulo *traceroute*

El módulo *traceroute* se utiliza para mostrar la ruta que siguen los paquetes desde un dispositivo origen a un dispositivo destino. Es una herramienta estándar para solucionar problemas en las redes. Si se encuentra una situación en la que no podemos conectarnos con un dispositivo *traceroute* ayuda a localizar el problema.

Traceroute al igual que Ping se basa en el protocolo ICMP.

En el siguiente ejemplo se hace un *traceroute* a la dirección IP 216.230.128.194, y los saltos para llegar a ese dispositivo son tres.

Figura 12. Módulo *traceroute*



5.4.8 Módulo scan

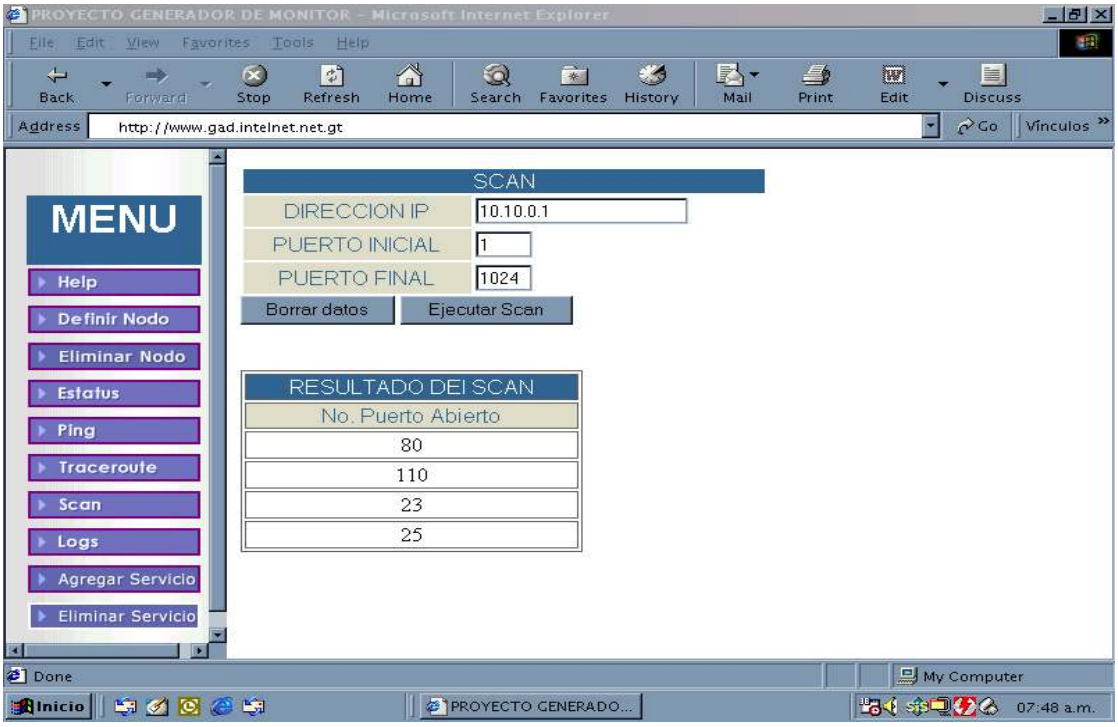
El módulo scan nos permite saber que puertos están abiertos en un dispositivo. Es importante saber para que nos sirve cada puerto y el servicio que proporciona mi equipo.

Lo recomendable es tener abierto únicamente los puertos de los servicios que esta dando el dispositivo y desactivar los demás para evitar cualquier ingreso no autorizado al dispositivo.

El módulo scan nos permite hacer un barrido (Scaneo) de puertos en un dispositivo y para eso hay que indicar el puerto inicial y final y sobre ese rango se realiza el barrido.

En el siguiente ejemplo se hace un barrido al dispositivo identificado con la dirección IP 10.10.0.1 el rango es del puerto 1 al puerto 1024. El resultado del barrido fue que solo tengo abierto cuatro puertos.

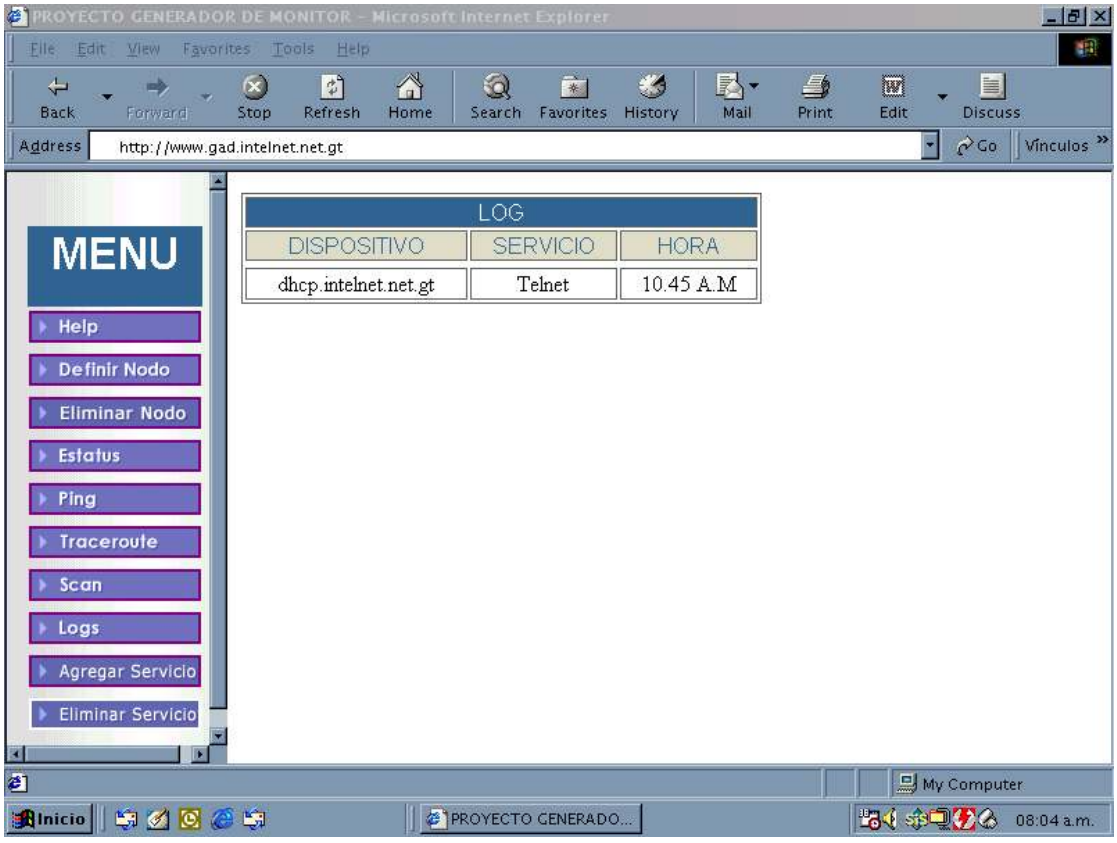
Figura 13. Módulo scan



5.4.9 Módulo *logs*

El módulo *logs* nos permite llevar un registro de las últimas 24 horas de los servicios que han fallado en un dispositivo. Aquí se nos indica la hora en que ocurrió la falla.

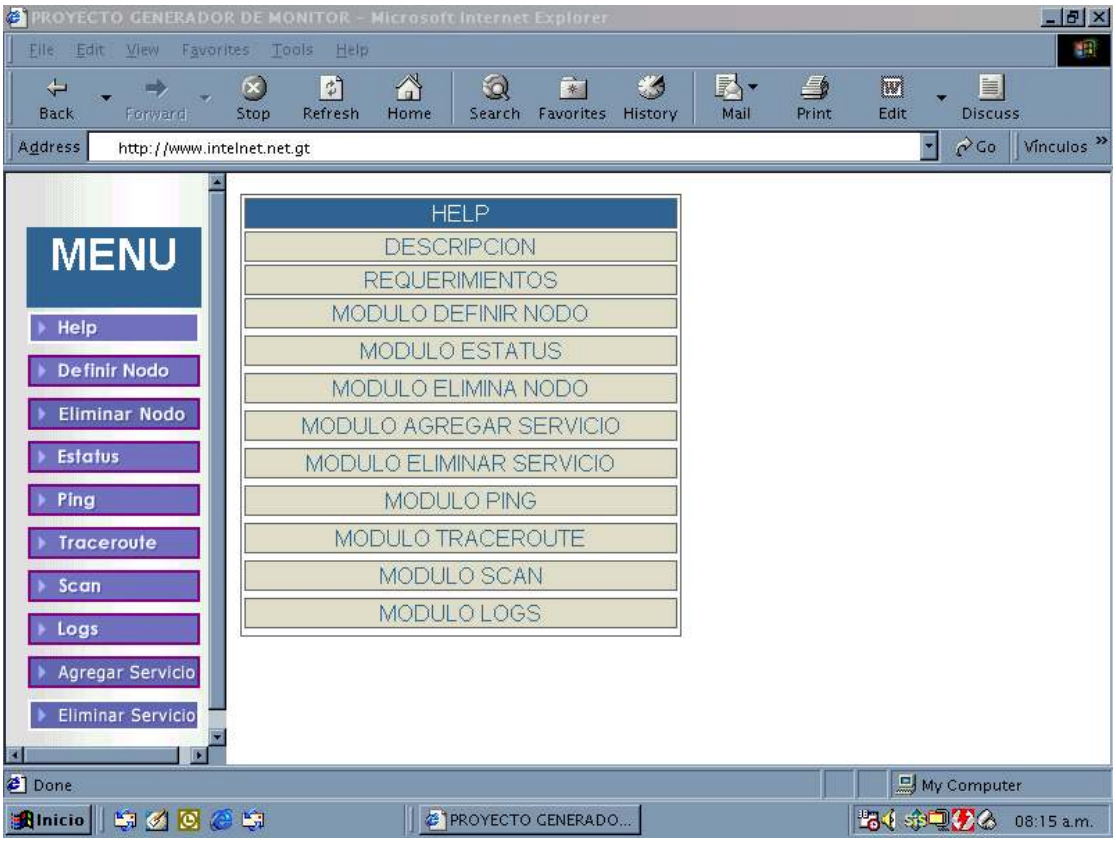
Figura 14. Módulo *logs*



5.4.10 Módulo *help*

El módulo *Help* contiene la información necesaria para la instalación y operación de la herramienta de gestión.

Figura15. Módulo *help*



CONCLUSIONES

1. El tamaño y la complejidad de las redes han ido creciendo sin cesar, debido en gran parte a la creciente oferta de servicios de comunicación de valor añadido. Este crecimiento hace más compleja la administración de la red y por lo tanto el tiempo de respuesta ante una eventualidad se complica dejando muchas veces por largo tiempo sin servicio a los usuarios. Debido al crecimiento de las redes es necesario gestionarlas, es decir, controlar los recursos que las componen en términos de rendimiento, capacidad, utilización, reconfiguración, diagnóstico, planificación, disponibilidad, etc.

2. El gestionar un servicio, en un dispositivo nos garantiza recuperarnos de cualquier eventualidad en el menor tiempo posible.

3. PERL es un lenguaje de fácil uso y potente para comunicarse con dispositivos de red y combinado con la metodología CGI y HTML podemos presentar en tiempo real el resultado de un programa en PERL en páginas web dinámicas e interactivas.

4. Un sistema de gestión que dispusiera de facilidades para la realización de todas las tareas de gestión, sería un sistema muy caro y muy complejo, la solución es la especialización de los sistemas de gestión.

5. La herramienta de gestión que se desarrolló permite gestionar la disponibilidad de uno o más servicios TCP/IP en un dispositivo de red, notificando cuando un servicio falla lo cual permitirá a los administradores de red restablecer un servicio que falle en el menor tiempo posible.

6. La herramienta de gestión que se desarrolló es una aplicación que trabaja en la red Internet. Ya que Internet nos ofrece muchas ventajas que podemos aprovechar muy bien y es, la forma mas económica, actual y práctica de comunicarse con el resto del mundo, por ejemplo:

   a) Puedo tener un servidor de gestión de red en un país centroamericano y estar gestionando un dispositivo de red que está localizado en Europa.

   b) Proporcionar al usuario un ambiente agradable de trabajo y de fácil comprensión.

   c) Proporciona mucha información para la investigación de cualquier tipo.

RECOMENDACIONES

1. La herramienta de gestión que se desarrolló es de libre acceso y código abierto, lo cual permite darle seguimiento con el fin de hacerle mejoras.

2. La herramienta de gestión debe implementarse en la Facultad de ingeniería para la gestión de la red e ir implementándola en el resto de la red de la Universidad de San Carlos de Guatemala con el fin de llegar a tener un centro de gestión centralizado y así restablecer cualquier servicio que falle en el menor tiempo posible.

3. Motivar a los estudiantes de la carrera de Ingeniería en Sistemas a desarrollar este tipo de aplicaciones, debido a que el precio de las aplicaciones comerciales de gestión son muy altos.

BIBLIOGRAFÍA

1. Hahn, Harley. The Internet Complete Reference. 2a. ed. United States of America: Editorial Osborne McGraw-Hill. 1996. 802 pp.

2. http://www.perl.com

3. http://www.cgi.com

4. Hunt, Craig. TCP/IP Network Administration. United States of America: Editor Mike Loukides. 1992. 472 pp.

5. James D. Mccabe. Practical Computer Network Análisis and Design. United States of America: Editor Jennifer Mann. 1998. 304 pp.

6. Kauffels, Franz-Joachim. Network Management. United States of America: Editor Addisos-Wesley. 1992. 427 pp.

7. Liu, Cricket y otros. Managing Internet Information Services. United States of America: Editor Adrian Nye. 1994. 630 pp.

8. Muller, Nathan J., Davidson, Robert P. LANs to WANs: Network Management. United States of America: Editor Mike Loukides. 1995. 536 pp.

9. Olaf Kirch, Terry Dawson. Network Administration Guide. United States of America: Editor Andy Oram. 2000. 438 pp.

10. Scott M. Ballew. Managing IP Networks. United States of America: Editor Mike Loukides. 1997. 315 pp.

ANEXO

ANEXO 1

Programa en *PERL* que verifica el estado de un servicio en un dispositivo.

```
!/usr/bin/perl
use IO::Socket;
use Date::Format;
use Mail::Sendmail;
use Net::Ping;

#HACEMOS UN CICLO INFINITO DEL TESTEO

$bandera=1;

while ($bandera==1)
{

  #ABRIMOS EL ARCHIVO DONDE ESTAN LOS SERVICIOS
    DEFINIDOS POR EL HOST

  open (ARCH,"</usr/local/apache/cgi-bin/resultado");
  #LEEMOS LINEA POR LINEA
  while ($linea=<ARCH>)
  {
     chop $linea;
     print "$linea \n";
     @campos=split(' ',$linea);
     $elementos=@campos;
      print "$elementos campos del vector\n";

     $contador=4;

     for ($cont=0;$contador<=$elementos;$cont++)
     {

        if ($campos[$contador]  eq "icmp1")
         {
```

```
  $p = Net::Ping->new("icmp");
  if ($p->ping($campos[2]))
  {
    $ima=$campos[1] . $campos[$contador-1] . ".gif";
    print " CONECTADO\n";
    $imaestado="cp /usr/local/apache/htdocs/proyecto/green.gif
                  /usr/local/apache/htdocs/proyecto/$ima";
    system($imaestado);
  }#if
  else
  {
    $ima=$campos[1] . $campos[$contador-1] . ".gif";
    $imaestado="cp /usr/local/apache/htdocs/proyecto/red.gif
                  /usr/local/apache/htdocs/proyecto/$ima";
    system($imaestado);
    print "fallo  $ima\n";
  } #else del ping
 }#del if

 else
{
   puerto:$campos[$contador+1]: protocolo :$campos[$contador]:\n";
   $sock = IO::Socket::INET->new(PeerAddr => $campos[2],
                          PeerPort => $campos[$contador+1],
                          Prot => $campos[$contador],
                          Timeout =>"5" );

   if ($sock)
    {
    $ima=$campos[1] . $campos[$contador-1] . ".gif";
    print " CONECTADO $ima\n";
    $imaestado="cp /usr/local/apache/htdocs/proyecto/green.gif
                  /usr/local/apache/htdocs/proyecto/$ima";
    system($imaestado);
   }#if
   else
    {
    $ima=$campos[1] . $campos[$contador-1] . ".gif";
    $imaestado="cp /usr/local/apache/htdocs/proyecto/red.gif
                  /usr/local/apache/htdocs/proyecto/$ima";
    system($imaestado);
    print "fallo  $ima\n";

    #GRABAMOS EN EL LOG QUE EL SERVICIO ESTA ABAJO
    open (FILE, ">> /usr/local/apache/htdocs/proyecto/logfallo") || die "$!\n";
    $fecha=ctime(time,%C);
    chop($fecha);
```

```
        print FILE "FALLO : $fecha :  $campos[2] : $campos[$contador-1] \n";
        close (FILE);

         #MANDAMOS UN EMAIL DICIENDO QUE EXISTE UN FALLO EN EL
ì¥Á□9       □□□ø□¿□□□□□□□□□□□□□□□□□u2□□
```

□bjbjýÏýÏ□□□□□□□□□□□□□□□□□□□□□□

□□5□□□Ÿ¥□□Ÿ¥□□Z.□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ÿÿ□□□□□□□
□□□□ÿÿ□□□□□□□□□□□□ÿÿ□□□□□□□□□□□□□□□□□□□□□□□□l□□□□□¬□□□□□□□□¬□□□
¬□□□□□□□¬□□□□□□□¬□□□□□□□¬□□□□□□□¬□□□□□□□□□□□□□□□□□□□□À□□□□
□□□>¬□□□□□□□>¬□□□□□□□>¬□□8□□□v¬□□d□r-1]"
□□□□u2□□

□bjbjýÏýÏ□□□□□□□□□□□□□□□□□□□□□□

□□5□□□Ÿ¥□□Ÿ¥□□Z.□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ÿÿ□□□□□□
□□□□ÿÿ□□□□□□□□□□□□ÿÿ□□□□□□□□□□□□□□□□□□□□□□l□□□□□¬□□□□□□□¬□□□□
¬□□□□□□□□¬□□□□□□□□¬□□□□□□□□¬□□□□□□□□¬□□□□□□□□¬□□□□□□□□□□□□□□□□□□□À□□□□
□□□>¬□□□□□□□>¬□□□□□□□>¬□□8□□□v¬□□d□r-1]"
□□Ÿ¥□□Ÿ¥□□Z.□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ÿÿ□□□□□□□□□□□□
ÿÿ□□□□□□□□□□□□ÿÿ□□□□□□□□□□□□□□□□□□□□□□l□□□□□¬□□□□□□□¬□□□¬□□□□
□□□□¬□□□□□□□□¬□□□□□□□□¬□□□□□□□□¬□□□□□□□□□□□□□□□□□□□À□□□□□□□□>
¬□□□□□□□>¬□□□□□□□>¬□□8□□□v¬□□d□r-1]"
□□□□□□□□□ÿÿ□□□□□□□□□□□□ÿÿ□□□□□□□□□□□□ÿÿ□□□□□□□□□□□□□□□□□□□□□□l□
□□□□¬□□□□□□□□¬□□□¬□□□□□□□□¬□□□□□□□□¬□□□□□□□□¬□□□□□□□□¬□□□□
□□□□□□□□□□□□□À□□□□□□□□>¬□□□□□□□>¬□□□□□□□>¬□□8□□□v¬□□d□r-1]"
□□□□¬□□□□□□□□¬□□□□□□□□¬□□□□□□□□□□□□□□□□□□□□□À□□□□□□□□>¬□□□□□□□>
¬□□□□□□□>¬□□8□□□v¬□□d□r-1]"

```
            );
            $mail{Smtp}='ns.intelnet.net.gt';
            sendmail(%mail) or die $Mail::Sendmail::error;

            print "OK. Log says:\n", $Mail::Sendmail::log;
          }#else

        } #else

        $contador=$contador+3;

     } #for

    } #while
    close(ARCH);

} #while del ciclo infinito
```