Universidad de Los Andes
HACER
Asesoría, Computación, Entrenamiento y Redes

Programa de Formación en
TELEINFORMATICA

Introducción a la Gerencia Técnica de Redes

Versión 1.0

Jacinto A. Dávila

Julio 1993

Hoja Técnica.

Documento: Introducción a la Gerencia Técnica de Redes (Network Management)
Versión: 1.0
Fecha: Julio de 1993
Autor: Jacinto A. Dávila.
Supervisor: Ermanno Pietrosémoli (Ms Sc).
Coordinador de Publicaciones: Luis Felipe González.
Edición y montaje gráfico: Yaneira Vargas, Marisol Buela, Jacinto Dávila
Coordinador General: Vicente Ramírez.
Coordinación Docente Asesoría, Computación, Entrenamiento y Redes. HACER-ULA Universidad de Los Andes.

Edificio A. Núcleo La Hechicera
Mérida. Edo. Mérida. Venezuela.
Teléfonos: 401128-401379-401288

Contenido

I.- Rastreo y análisis de redes

II.- Administración de Redes (Network Management)

Introducción a la Gerencia Técnica de Redes

Rastreo y análisis de redes

Revisión de conceptos de redes

La administración de redes, al igual que otras ramas ingenieriles, plantea problemas prácticos que exigen capacidad creativa y madurez en el trabajo técnico. La experiencia es muy importante para los administradores de redes, quienes suelen resolver sus problemas recurriendo a su conocimiento de situaciones similares anteriores. Sin embargo, no es posible hablar de destreza práctica cuando no se manipulan adecuadamente los conceptos y las teorías que soportan las nuevas tecnologías. El desarrollo de esa certera *intuición* que acompaña a los mejores administradores, tiene que ver con una *comprensión vivida* del funcionamiento de los sistemas que administran.

El propósito de este material es presentar a los participantes una serie de herramientas de asistencia a los administradores de redes. Esas herramientas no son, como podría pensarse, productos especiales (hardware y software) para administrar, sino antes los conceptos, ideas y estrategias que se emplean para la administración profesional de redes. Para ello, se hace preciso recordar dos conceptos en torno a los cuales gira el contenido de este curso.

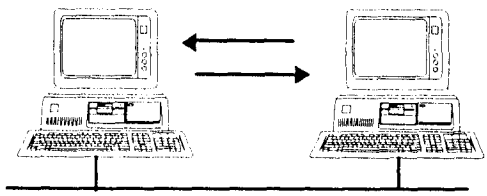
1. **Red de computadores**: Una red es un sistema de intercambio de señales. En particular en las redes de computadores esas señales representan datos, los cuales a su vez, habrán de constituirse en información en las entidades que los *consumen*. Las primeras redes tenían como propósito el intercambio de información entre usuarios. La tendencia hacia el control total y la automatización de los procesos de producción, ha hecho surgir nuevas aplicaciones. Actualmente, las redes permiten la compartición de recursos para el procesamiento de la información. Se mantiene el objetivo de intercambio de información, pero son ahora los computadores los gestores del intercambio, como parte de una estructura sinergética de mayor alcance.

2. **Administración de redes**: Las tareas de diseño, planificación, instalación, configuración, entonamiento, mantenimiento y seguimiento de los sistemas de redes definen el alcance de la administración de redes. La diversidad de tareas plantea la necesidad de una estrategia para la administración. Si se agrega la necesidad de responder con prontitud y mejor aún, de anticiparse a los requerimientos de los usuarios (los componentes fundamentales del *sistema*), entonces esa necesidad de sistematizar los mecanismos de administración es inexcusable.

HACER ULA

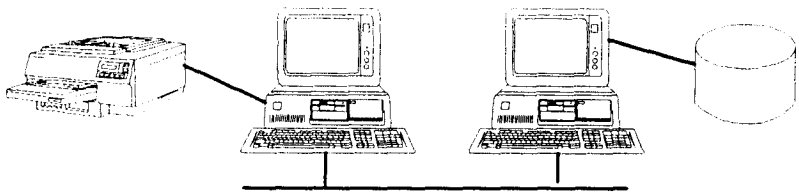
Gerencia Técnica de Redes

Administración de Redes de Computadores



Diseño
Planificación
Instalación
Configuración
Entonamiento
Mantenimiento
Supervisión

Administración



Notas:

¿Qué es la Gerencia Técnica de Redes?.

Un conjunto de prácticas para administración de redes, en las que se emplean dispositivos y sistemas especializados para supervisión, detección de fallas y control remoto de estaciones, servidores, pasarelas (*gateways*) y otras máquinas conectadas a redes.

La gerencia técnica de redes tiene como objetivos:

1. **Prevenir las fallas y reducir el tiempo de restauración del sistema cuando ocurran**. Con el seguimiento sistemático del comportamiento de la red es posible anticipar alteraciones. En caso de fallas, la posibilidad de *observar* el desenvolvimiento del sistema ayuda a aislarlas y corregirlas en muy corto tiempo.

2. **Mejorar el rendimiento de la red**. El perfil de uso de la red puede guiar decisiones acerca de la expansión de la red, permitiendo una asignación ptima de los recursos y una planificación realista del crecimiento.

3. **Facilitar la evaluación de productos de redes**. Con herramientas de rastreo y control remoto es posible precisar, sin lugar a dudas (con ejercicios concretos, cuyos resultados son bien registrados), la capacidad de integración de un producto (hardware y software) a un ambiente de red (antes de comprarlo).

4. **Mejorar la productividad del personal de administración**. Mas soluciones en menor tiempo, prevención de los desastres que desmoralizan al grupo de soporte, incentivo a la creatividad sobre la base de conocimiento adquirido de la red, todas son tendencias favorecidas por la gerencia de redes.

HACER ULA

Gerencia Técnica de Redes

Objetivos de la Gerencia Técnica de Redes

1.- Prevenir fallas y reducir el tiempo de reparación

2.- Mejorar el rendimiento de la red.

3.- Facilitar la evaluación de los productos de redes.

4.- Mejorar la productividad del personal de administración.

5.- Control total de infraestructura.

Notas:

Herramientas para Gerencia Técnica de Redes

Una primera clasificación, en función de su complejidad, de las herramientas para Network Management, se muestra a continuación:

Sistema	Funciones	Objetivos	Ejemplos
Programa para verificación y control de canales.	Envío de mensajes de control	Facilitar la instalación y prueba de redes.	PING.
Protocolos para intercambio de mensajes de control.	Envío de mensajes de control	Verificación y control de las conexiones de comunicación.	I.C.M.P.
Programas de supervisión.	Revisión del estado de las entidades de red	Permitir la revisión de los programas y sistemas de red.	netstat
Monitores o rastreadores de red.	Rastreo de redes.	Supervisión de tráfico a todo nivel.	snoop, etherfind, trace.
Analizadores de red.	Rastreo y análisis de variables y "diálogos".	Interpretación detallada del tráfico y su contenido.	• Sniffer, • LAN Analyzer, • NetVisualyzer, • Sun Net Manager.
Protocolos de administración.	Obtención de información y transmisión de instrucciones.	Permitir la administración remota de los dispositivos y entidades de red.	S.N.M.P. C.M.I.P.
Sistemas de Administración.	Integración de todas las funciones anteriores	Administración centralizada y jerarquizada de redes	• IBM's NETView, • AT&T Accumaster Integrator. • DEC's DECmcc • HP's OpenView. • Sun Net Manager • SG NetVisualyzer.

Revisaremos algunas de esas herramientas inmediatamente.

HACER ULA

Gerencia Técnica de Redes

Herramientas para Gerencia Técnica de Redes

Herramienta	Ejemplo
Verificación y Control	PING/ICMP
Muestreo del tráfico y/u otras variables	Netstat Snoop Etherfind Trace/KA9Q
Analizadores de Red	Sniffer Lan Analyzer
Protocolos de Administración	SNMP CMIP
Sistemas Administrativos	Net Visualyzer Sun Net Manager

Notas:

Monitoring de fallas.

Monitorizar o como le llamaremos en este curso, **rastrear** (hasta ahora es incorrecta la traducción monitorear) es la estrategia por excelencia para anticiparse a los requerimientos crecientes de los usuarios. En las modernas redes el rastreo adopta diversas modalidades: rastreo de los dispositivos (uso de discos, impresores, memoria y procesadores), rastreo o seguimiento de usuarios (crecimiento de la *población*), rastreo de mensajes (de correo) y rastreo de tráfico, son las más comunes.

Realmente, como dice José A. Beltrão [1] "*la definición de las medidas depende de la utilización que se pretende con los datos a recolectar*". Así, para definir la estrategia, en el presente texto se establece que el propósito de las mediciones será la prevención, detección y corrección de fallas. Las fallas son comportamientos irregulares en los sistemas causados por: error en la configuración de los sistemas, daños o defectos en las estructuras y/o saturación.

El rastreo periódico y sistemático del tráfico, por ejemplo, puede ser la herramienta para prevenir saturación de los canales de transmisión o detectar daños y configuraciones erradas en los equipos.

En las redes de área local, caracterizadas por la compartición de un medio único entre todos los nodos, las medidas típicas (llamadas *medidas de prestaciones* [1]) son:

- **Retardo medio de mensajes T**. Una medida de la rapidez de respuesta del sistema, es la media de los retrasos observados (T) en la entrega de los mensajes desde que se colocan en el medio hasta que alcanzan su destino. Este estadístico puede emplearse a diversos niveles, aunque más difícilmente, en los niveles inferiores. En cualquier caso supone *intercambio de paquetes con reconocimiento*, o captura del tiempo de envío y recepción en sistemas que deben poseer un *timing* común.

- **El uso del medio, rendimiento, caudal o *throughput*** (o Vaciamiento[1]): "El número de bits de mensajes (excluyendo el *overhead*) que son transmitidos por unidad de tiempo". Este estadístico permite establecer el *nivel de aprovechamiento del medio*, atributo particularmente importante en redes de acceso contencioso como *Ethernet*.

NETMAN 1. Recordando conceptos.

¿Qué es un protocolo de acceso al medio?.

HACER ULA

Gerencia Técnica de Redes

MONITORING DE FALLAS

"La definición de las medidas depende de para qué van a ser utilizadas"

Medidas de prestaciones en redes de área local

- **Retardo medio entre mensajes**
- **Uso del medio, rendimiento, caudal o throughput**

Notas:

La mayoría de las redes locales comerciales han sido fabricadas a partir de productos de investigación cuidadosamente modelados. La formalización matemática de los esquemas y protocolos de acceso al medio ha permitido en muchos casos, prever el comportamiento del sistema antes de implementarlo. En otros casos, sin embargo, la complejidad teórica obliga a otros métodos.

Esos modelos matemáticos permiten decir como se comportan las redes locales bajo ciertas condiciones. Así, por ejemplo, las redes de acceso contencioso CSMA/CD alcanzan teóricamente, su nivel máximo de eficiencia cuando están sometidas a la mitad de la *carga posible*, como puede observarse en la lámina. Cabe indicar que se entiende por carga posible y qué son las variables S y G [2]

- **Carga posible**: es la magnitud de carga que el canal puede manejar en un *tiempo de trama*, suponiendo que los usuarios pertenecen a una población infinita (que no se agota aunque los usuarios se ocupen en otra cosa). La carga máxima posible es 1.

- **Tiempo de trama**: es una simplificación adoptada por los matemáticos para reducir la complejidad del modelo. Se define como [2] "la cantidad de tiempo necesaria para transmitir una trama normal de longitud de *fija*"

- **Rendimiento por tiempo de trama S**: Es un valor que establece el nivel de la carga. Se supone que los usuarios generan aleatoriamente tramas para cada tiempo de trama, con una media de S tramas/tiempo de trama. Si S>1 el canal está sometido a una carga superior a la que puede manipular.

- **Tráfico absoluto ofrecido a la red G**: Es un valor que combina los efectos del tráfico nuevo y el que se ha retrasado por colisiones previas. Se define como la media de la distribución Poisson que permite establecer la probabilidad de k intentos de transmisión (de k tramas) en un mismo tiempo de trama.

NETMAN 2. Tráfico en redes.

Explique las gráficas mostradas en la lámina. ¿Qué significa esto para los efectos de tráfico en una red Ethernet?.

¿Por qué el rendimiento de la red Ethernet no depende únicamente de su velocidad de transmisión?.

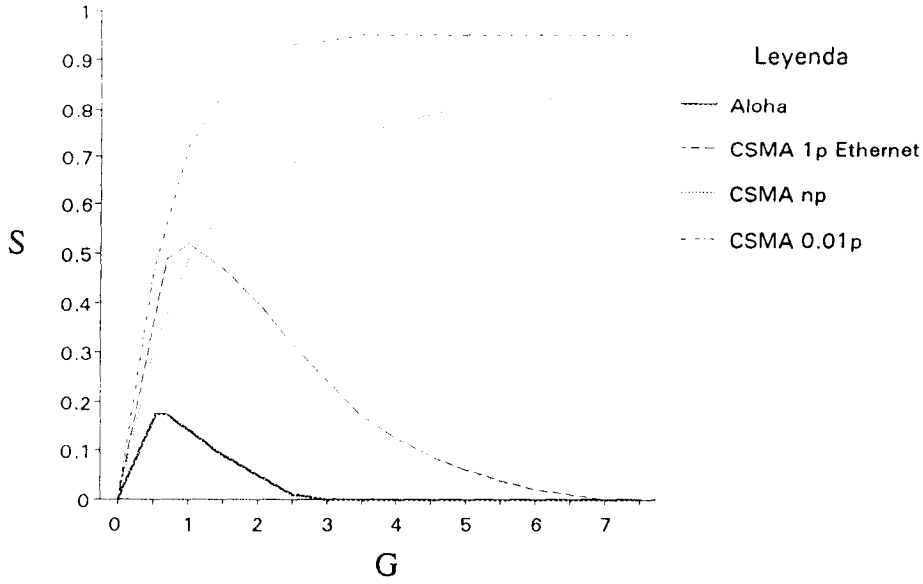
¿Cómo podría Ud. *medir* el nivel de carga de una red Ethernet?. ¿Para qué medir el nivel de carga de una red?.

HACER ULA

Gerencia Técnica de Redes

Prestaciones en redes de acceso aleatorio

Uso del medio vs. carga



Notas:

¿Cómo se rastrea?. Herramientas básicas para *monitoring.*

Existen algunos mecanismos estándares para rastreo de las condiciones en una red. Algunos son protocolos ampliamente difundidos, otros son productos implementados sobre diversas plataformas.

Cada arquitectura de red tiene un conjunto de herramientas que permiten a sus administradores rastreo y algunas acciones de control. Sin embargo, con la tendencia de los últimos años a implementar sistemas de comunicaciones independientes de la arquitectura protocolar, algunas de estas aplicaciones y herramientas son empleadas para rastrear variables muy diversas.

Como parte de este curso introductorio, se revisarán tres de esas herramientas (Ping, Netstat y Snoop), pero antes se describirán algunas plataformas que las implementan y que se emplearán en la realización de los ejercicios.

NETMAN 3.- Revisión de las arquitecturas de red.

Nota: Es importante realizar este ejercicio antes de continuar.

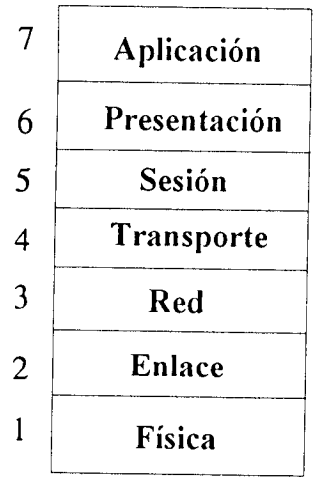
¿Qué es Internet?. ¿A qué se denomina familia TCP/IP?. Ind. Ver lámina.

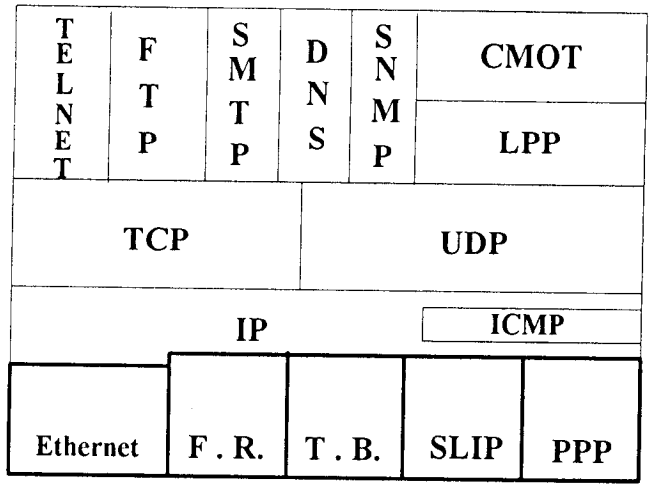
Identifique y ubique los siguientes *productos* en el modelo OSI: Ethernet, Token Ring, SDLC, X.25, IP, CLNP, TCP, TP0, IPX, NetBeui, NetBIOS, RPC, NFS, ARP, Telnet, FTP, SMTP, X500.

HACER ULA

Gerencia Técnica de Redes

Revisión de las arquitecturas de redes.





Notas:

El presente curso pretende realizar una presentación general de los conceptos y herramientas para Network Management. En este sentido, se trata de mantener la discusión al margen de inclinaciones por algún producto comercial específico. Lamentablemente, no existen productos para Network Management que no estén inclinados a una plataforma particular. Por esta razón, nos vemos en la necesidad de presentar algunas de esas soluciones comerciales y sus herramientas. Por otra parte, existen productos capaces de soportar soluciones de red de bajo costo, que son de dominio público o por lo menos muy poco restringido. Aunque no es el propósito del curso adiestrarlos en esos productos (existen otros cursos con ese objetivo en HACER), vamos a presentarlos y a emplear sus herramientas para rastreo, a sabiendas de que para los administradores es fundamental conocer alternativas.

KA9Q

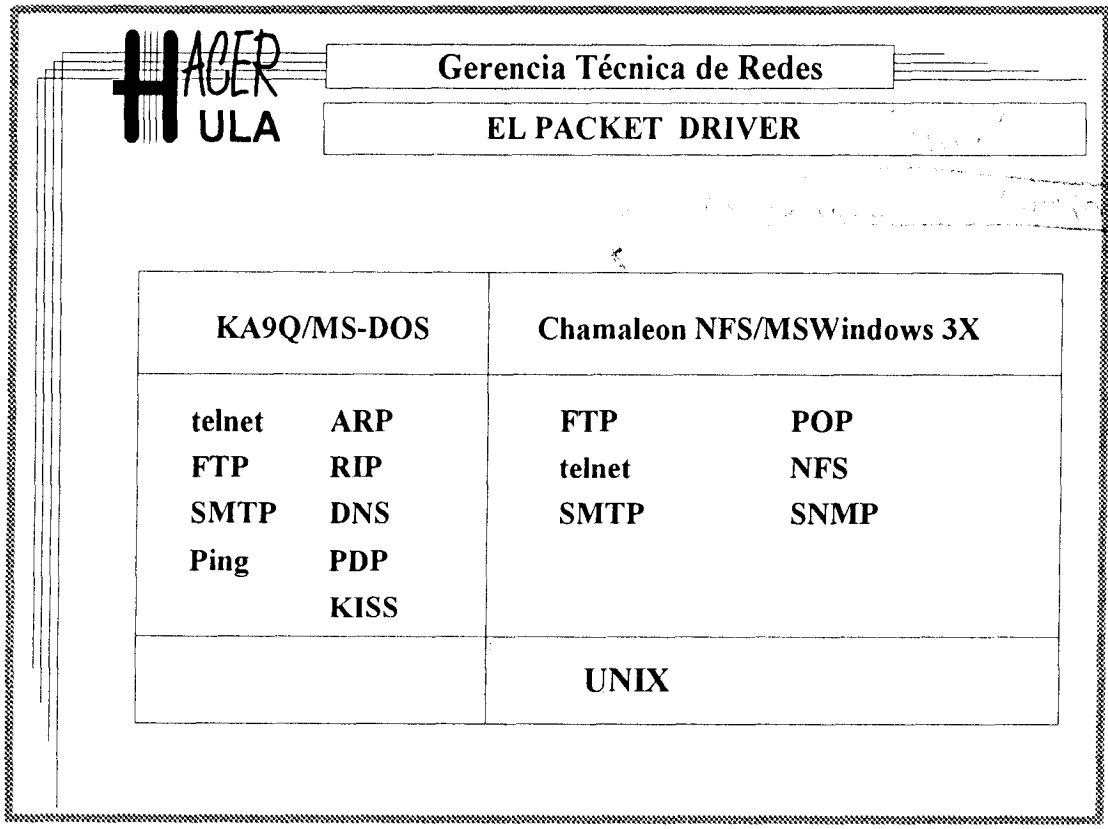
El KA9Q fue desarrollado por Phil Karn [3] de Bellcore, New Jersey. USA. Se trata de un ambiente integrado de red para computadores personales (plataforma Intel) con MSDOS (existen realizaciones UNIX y Macintosh). Karn lo propone como un SOR. El KA9Q combina una nada común variedad de soluciones de conectividad en un ambiente sencillo y económico (cualquier máquina DOS puede soportarlo). El potencial de las redes inalámbricas AX.25, la economía de las conexiones seriales y las ampliamente difundidas redes locales Ethernet pueden reunirse empleando un computador personal cualquiera con el KA9Q. Por otra parte, la gama de servicios posibles en redes TCP/IP está muy bien representada en este producto que dispone de servicios Telnet y FTP (Cliente y Servidor), SMTP, Ping, ARP,. RIP (la máquina puede convertirse en un enrutador), DNS, el nuevo PPP y el KISS, además de un servicio de rastreo del medio físico al cual esté conectado. Esta es la razón de su inclusión en este manual.

Construido gracias a la colaboración de muchos investigadores e ingenieros de redes[3], el KA9Q es un buen representante de una familia de productos de software para redes que se apoyan en una idea novedosa: Los *Packet Drivers* (Manejadores de Paquetes, Ver lámina).

- **Packet Driver** (PD): Un PD es una relativamente pequeña pieza de software (un manejador residente en memoria) que se adueña de la tarjeta de red Ethernet del PC y proporciona una única interfaz a todos los demás paquetes de software.

NETMAN 4. KA9Q.

En las máquinas dispuestas para tal efecto, active el KA9Q. (Ind. arranque la máquina, verifique que el PD esté en memoria y ejecute el comando: `net autoexec.net`). Ejecute después los comandos `?` y `exit`.


HACER
ULA
Gerencia Técnica de Redes
EL PACKET DRIVER
KA9Q/MS-DOS
telnet
FTP
SMTP
Ping
ARP
RIP
DNS
PDP
KISS
Chamaleon NFS/MSWindows 3X
FTP
telnet
SMTP
POP
NFS
SNMP
UNIX

Notas:

ChamaleonNFS

Este producto comercial es una plataforma de red TCP/IP bastante completa para PC con MS Windows 3.x. Además de los servicios básicos (FTP, Telnet y SMTP) incluye el Post Office Protocol (Servicio de correo para las PC), un módulo NFS (Cliente y servidor) y una gama de agentes que trabajan con SNMP, el protocolo de administración que será revisado más adelante. Por esta razón se incluye en este curso.

Sistemas UNIX

UNIX fue el primer sistema operativo que integró la plataforma TCP/IP. Además, la popularidad que ha alcanzado lo ha hecho partícipe de los nuevos avances de computación en red. Dos importantes aplicaciones para *Network Management* (*Sun Net Manager* y *Netvisualizer*) son programas UNIX (que funcionan sobre plataformas *Sun SPARC* y *Silicon Graphics*, respectivamente). Ambas comparten un esquema de rastreo que será estudiado en este curso: **snoop**. Por otra parte, en la plataforma *Intel*, el ODT de *Santa Cruz Operation Inc.* ha incorporado una serie de herramientas para Network Management, incluyendo los agentes y programas SNMP.

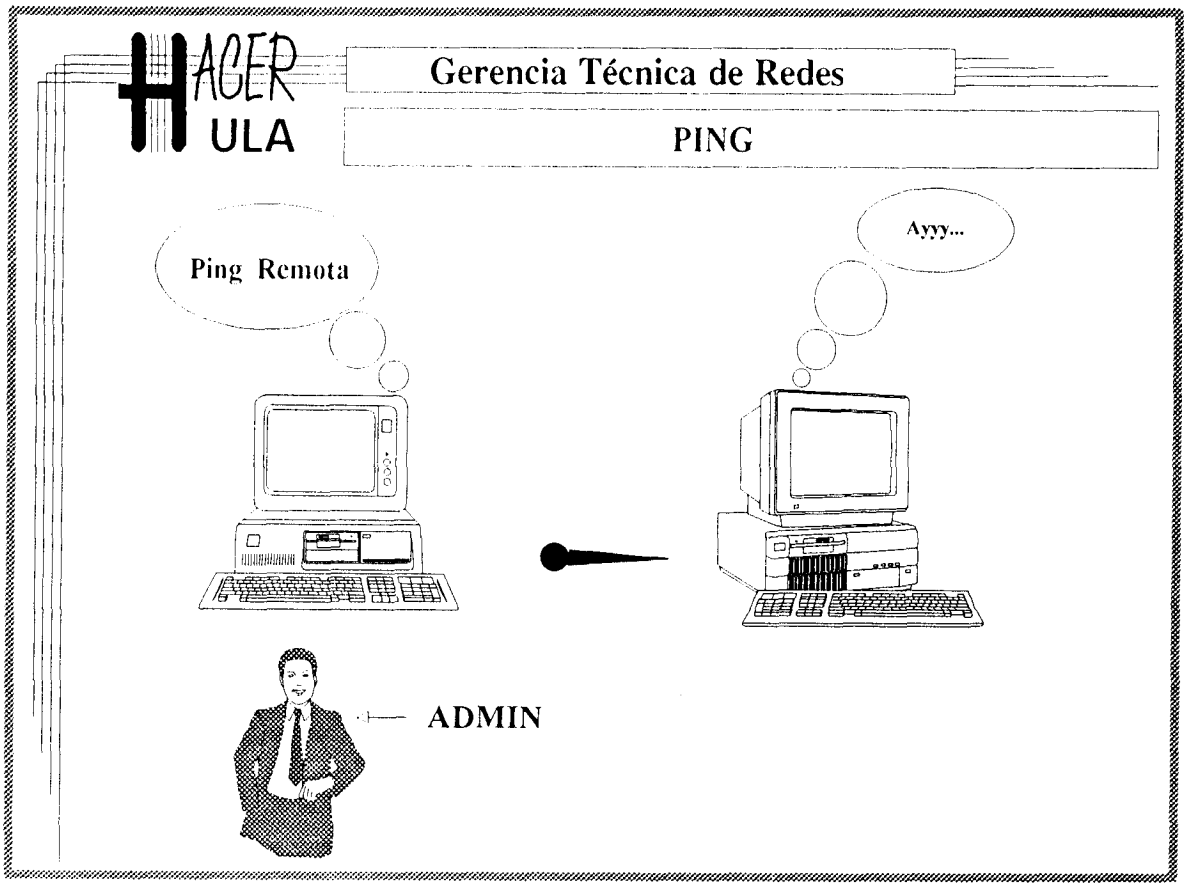
Estos son los productos y sistemas operativos que se manipularán en el curso. La variedad mostrada supone un primer paso en el trabajo de integración que forma parte de la misión del administrador de redes. Veamos ahora algunas herramientas que se encuentran en esas plataformas.

Packet Internet Groper PING.

El PING es un programa que suele acompañar a todas las implementaciones TCP/IP. Es la realización parcial del protocolo ICMP (*Internet Control Message Protocol*), diseñado para permitir el intercambio de mensajes de control entre máquinas IP. Se dice que es la realización parcial porque, generalmente, el programa activa una secuencia ICMP del tipo *request-reply*. De acuerdo al comportamiento de la secuencia es posible conocer (o inducir) el estado de alguna máquina lejana, e inclusive el tiempo y ruta empleada por el mensaje para llegar hasta ella.

NETMAN 5. Ping.

Ejecute el comando PING en todas la plataformas TCP/IP del laboratorio (KA9Q, Unix, etc.). Ind: Ejecute el comando `ping` *`máquina`*. Solicite el nombre o número de la máquina al instructor. Pruebe otras variantes del `ping`.


HACER
ULA
Gerencia Técnica de Redes
PING
Ping Remota
Ayyy...
ADMIN

Notas:

Netstat

En todos los sistemas UNIX conectados en red, existe un comando con este nombre (`netstat`) que permite revisar el estado de las interfaces, estructuras y procesos involucrados en la comunicación. Como ocurre en otros comandos UNIX, puede invocarse acompañado de una serie de parámetros que permiten escoger uno u otro tipo de despliegue. Está diseñado para mostrar el estatus de la red, sin importar el tipo particular. Sin embargo, la mayoría de la implementaciones sólo disponen de rastreo TCP/IP (familia *inet*). La sintaxis, salvo variantes agregadas, es similar a:

```
netstat [-Aaimnrs] [-ffamilia] [-I interfaz] [-p protocolo] [interva]
                        [system] [corefile]
```

- Para verificar el estado de todas las conexiones (sockets): `netstat -a`
- Para revisar las tablas de enrutamiento: netstat -r (-rn)
- Para verificar el estado de la interfaces: netstat -i
- (en algunos sistemas). Si se quiere realizar un seguimiento del tráfico por las interfaces se puede activar el programa con un intérvalo (en seg.) , por ejemplo `netstat 5`

NETMAN 6. Netstat.

Ejecute el comando `netstat` con las variantes mostradas, en todos los sistemas disponibles en el laboratorio. Explique cada salida. ¿Qué utilidad práctica puede tener este programa para el *monitoring* del sistema?.

HACER ULA

Gerencia Técnica de Redes

NETSTAT

Netstat - Aaimis - Ffamilia - Iinterfaz - Pprot int. sys cor

Netstat - rn ⇒ tabla de enrutamiento

Netstat - i ⇒ Interfaces

Notas:

Snoop

Este término no es usado para definir la misma entidad en todas las plataformas. No obstante, los propósitos son similares (snoop = fisgón). El soporte del *NetVisualizer* de *Silicon Graphics* (Sistema de administración de redes) contempla el uso de una familia de protocolos (raw protocols) compuesta por dos *protocolos para rastreo* (*decapsulation protocols*) capaces de capturar paquetes directamente desde la capa de enlace de datos en Ethernet. Esos protocolos son `snoop` y `drain`. El primero empleado en el rastreo de paquetes de protocolos conocidos (sobre los que se puede realizar cierta clase de análisis y filtraje) y el segundo para los que no lo son. Lo interesante de esta propuesta de SG es que la plataforma está a disposición de los programadores en los *sockets* tradicionales del UNIX, de manera que cualquier programador puede construir su unidad de rastreo.

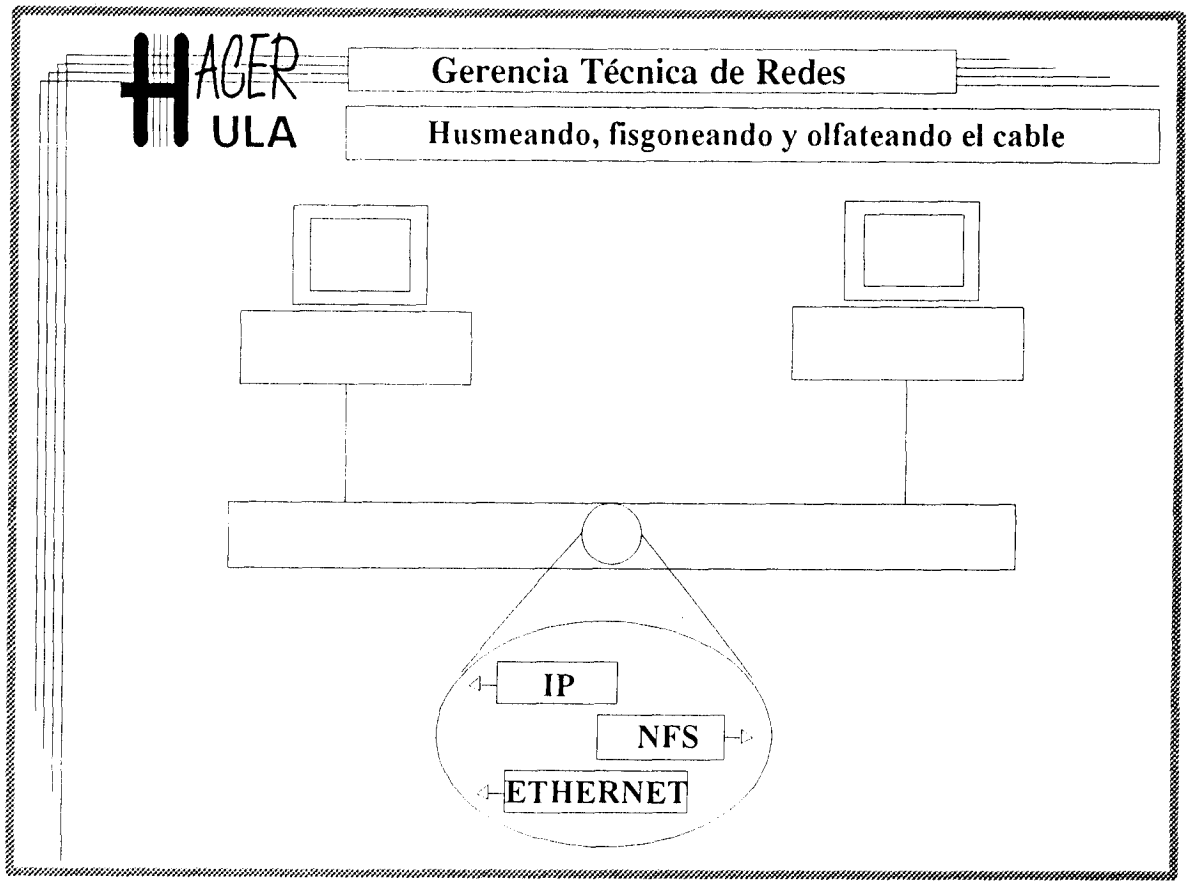
Sin olvidar ese uso del término, se presenta a continuación la descripción de una aplicación denominada `snoop`, disponibles en diversos ambientes UNIX (incluyendo SG (netsnoop) y Sparc), que permite capturar los paquetes de la red e inspeccionarlos. Como el netstat y el ping, se invoca con el comando cuya sintaxis (SunOS) es:

```
snoop [-aPDSvVNC] [-d disp] [-s tampaq] [-c maxcount] [-i arch ] [-o arch
      ] [-n file]       [-t [r | a | d ] ] [-p primero[,último]] [-x
                        offset[,long]  [expresión]
```

Como puede verse, la sintaxis permite muchas variantes. Mostraremos algunos ejemplos procurando reunir elementos para diseñar un experimento de rastreo o como se le conoce también, una *campaña de recolección*.[1]

- `snoop -P`: Captura los paquetes de la primera interfaz, pero en modo no promiscuo, esto es, sólo aquellos paquetes dirigidos a esta máquina o difundidos a todas (*broadcast*). Es de hacer notar que, a menos que se indique esta variante -P, snoop opera en *modo promiscuo*, es decir, capturando todos los paquetes que escuche por la interfaz en cuestión. Los paquetes son mostrados en pantalla hasta que se cancele el programa (Ctrl+C).

- `snoop -d le0 -s 34 -c 1000 -o trafico` : Captura los primeros 1000 paquetes escuchados en la interfaz "le0", separando solamente los primeros 34 bytes de cada paquete (justo el encabezado ip, si se quiere capturar el encabezado udp debe usarse -s 42 y 54, 80 y 120 para tcp, rpc y nfs respectivamente) y los guarda con formato resumido (*summary line*) en un archivo llamado trafico.


HACER
ULA
Gerencia Técnica de Redes
Husmeando, fisgoneando y olfateando el cable
IP
NFS
ETHERNET

Notas:

- `snoop -d le0 -S -t a -V -x 0 -o datag ip`: Captura todos los paquetes ip (nótese la ubicación de indicador, se trata de una expresión), mostrando el tamaño (-S) y el tiempo absoluto del reloj (-t a). El sistema muestra el contenido de cada paquete (-x 0) y además en un formato que permite observar el encabezado agregado por cada capa protocolar (-V). Los paquetes son guardados en el archivo datag, mientras haya espacio en disco o hasta que se cancele el programa.

- `snoop -i datag | grep NFS`: "Lee" el archivo datag (creado con una instrucción como la anterior) y entrega su contenido al comando grep. Nótese que esta es una manipulación UNIX para obtener en pantalla sólo paquetes NFS

Para completar la explicación, referimos algunos detalles respecto al campo *expresión*. Se trata de una construcción booleana que se utiliza como referencia. Sólo serán capturados aquellos paquetes para los cuales la expresión, al dispararse, sea verdadera. La expresión vacía es siempre verdadera. La expresión se puede construir con las siguiente primitivas:

`host` *`nombre`*; ethertype número; greater long; less long; net netid; port puerto; rpc programa[,versión][,procedimiento]; gateway pasarela; > ;< ; >= ;<= ; = ; !=; and ; or (se puede usar ","); and (dos operadores buleanos contiguos presuponen un "and"); not (!) ; ip; arp; rarp; broadcast; multicast; apple; decnet; udp; tcp; icmp; nofrag.

Los nombres y direcciones IP e Ethernet aplican también como primitivas. Si se quiere hacer referencia a alguna porción del paquete, se puede usar la siguiente sintaxis: *base* [*primero* [*:tam*]], donde base se sustituye por ether, ip, udp, tcp o icmp.

También se pueden usar los modificadores from, src, to y dst para afectar a las primitivas host, net, port o rcp, así como a nombres y direcciones.

NETMAN 7. Ejercicios de rastreo con snoop.

Rastree la red empleando en lo posible los comandos mostrados en el texto.
Con snoop, ¿cómo podría detectar que los paquetes viajan a través de determinado gateway?.

HACER ULA

Gerencia Técnica de Redes

SNOOP

Campaña de Recolección

Snoop - p

Snoop - d le0 - s34 - c 1000 - o trafico

Snoop - d le0 - s - ta - v - x0 - o datag ip

Snoop - i datag | grep ip

Notas:

Cabe destacar que en la plataforma SunOS existen otras herramientas nativas para rastreo. Tal es el caso del programa `etherfind` (y el demonio `etherd`) con el cual se puede realizar ejercicios similares a los permitidos por snoop [4].

NETMAN 8. *Monitoring* con KA9Q.

1. Active el KA9Q. (Recuerde que debe invocar el programa net con el archivo autoexec.net como parámetro: `net autoexec.net`). Antes de proceder revise el contenido del archivo y averigüe el nombre y dirección IP de su estación.

2. Una vez en el ambiente KA9Q, ordene el rastreo de los encabezados de todos los paquetes que escuche por la red. Coloque la salida del rastreo en un archivo. `trace ec0 0011` *`archivo1`*.

3. Ejecute un "ping" con alguna otra máquina de las cercanías. Active sesiones telnet y ftp con esa máquina momentáneamente. `ping` *`máquina`* `- telnet` *`máquina`* `- ftp` *`máquina`*.

4. Desconecte el rastreo establecido en 2. `trace eco off`

5. Ordene el rastreo de los paquetes icmp que su estación emita o reciba. `icmp trace on`.

6. Desconecte este rastreo. `icmp trace off`.

7. Ordene la captura de todo el contenido de todos los paquetes y almacénelos en otros archivos. `trace ec0 0111` *`archivo2`*; `trace ec0 0211` *`archivo3`*

8. Establezca sesiones telnet, ftp y ping con otras máquinas que le indique el instructor.

9. Abandone el KA9Q (`exit`) y revise el directorio del programa. Allí deberá encontrar los archivos creados por el rastreo. Revíselos.

NETMAN 9. Un problema real.

Suponga que una máquina del laboratorio tiene dificultades tratando de conectarse a otra como terminal remoto (telnet). Diseñe y realice la campaña de recolección de información para detectar la causa de esa falla.

HACER ULA

Gerencia Técnica de Redes

KA9Q

Trace [iface [off | btio [tracefile]]]

Campaña de recolección

1. net autoexec.net
2. trace ec0 0011 archivo1
3. ping,telnet,ftp
4. trace ec0 off
5. icmp trace on; ping
6. icmp trace off
7. trace ec0 0111 archivo2;
   trace ec0 0211 archivo3;
8. exit

Notas:

Organización y análisis de la información de rastreo

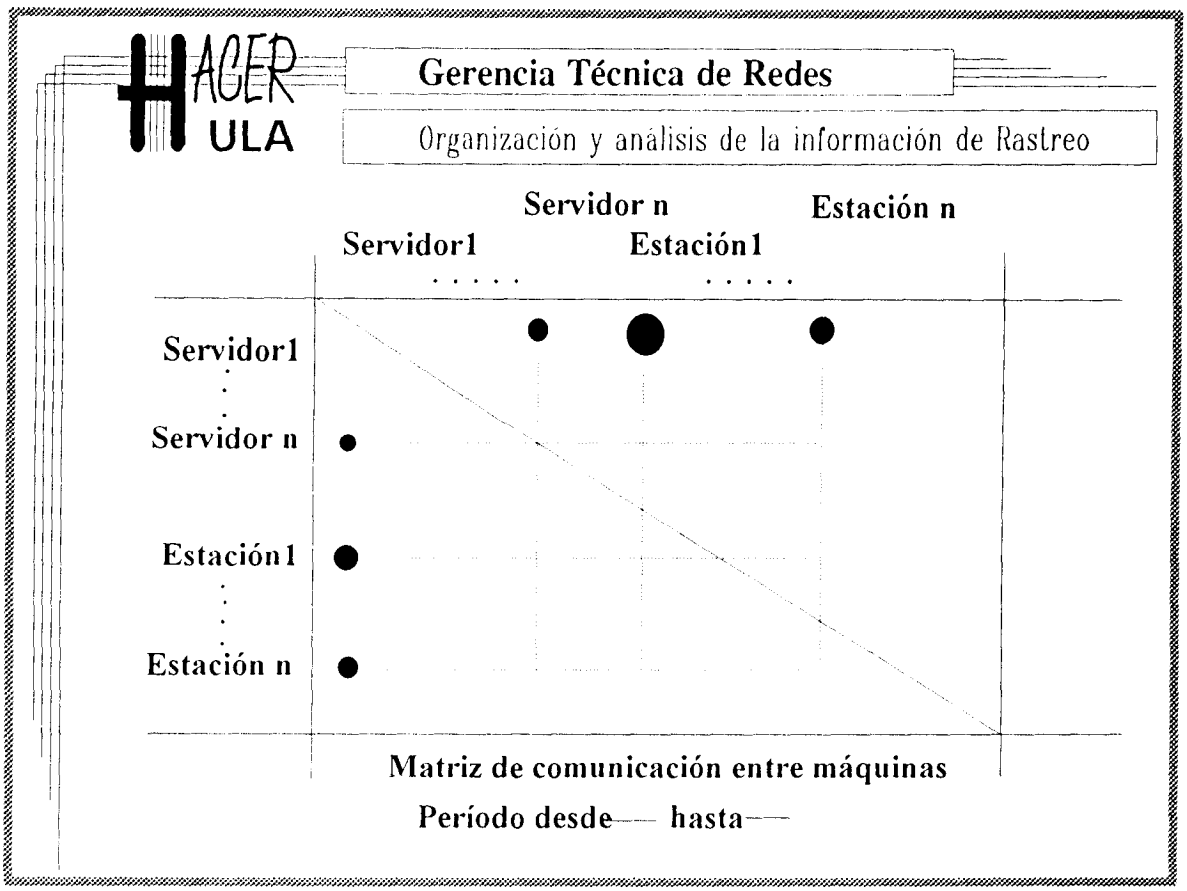
El volumen de datos que puede llegar a transitar por una red local desborda fácilmente al más paciente lector de listados de archivos. Si se admite la importancia de un rastreo periódico de la red que se administra, tiene que aceptarse también que es indispensable automatizar el proceso. Esta automatización tiene también aspecto que vale la pena destacar. En principio, el volumen de datos puede colmar fácilmente la capacidad de almacenamiento en disco de cualquier sistema. En consecuencia, no se puede hacer rastreo exhaustivo y almacenar todo en archivos para su posterior revisión, por muy automatizada que esta sea. El trabajo de revisión debería hacerse sobre muestras del tráfico, de las cuales se deducirían los estadísticos significativos. Es importante recordar que este tipo de tratamiento estadístico acarrea la perdida de confiabilidad y verosimilitud de los estadísticos (promedios de promedios) Pero antes de continuar hablando de los experimentos, se debe fijar el propósito de los mismos.

A continuación y como ejemplo se presentan algunas sugerencias de informes a elaborar con las campañas de rastreo en una red. Estos informes pueden permitirle mostrar, en cualquier momento, un perfil bastante completo de la red. Algunos de esos informes han sido usados por el *National Bureau of Standards* en EE.UU para examinar su red [1].

> **Informe 1**: Matriz de comunicación entre máquinas.
> **Descripción**: Muestra la relación de tráfico que ha circulado entre cada par de estaciones de la red o por lo menos entre las más significativas (servidores).
> **Obtención**: Debe realizarse rastreo exhaustivo de la red (todos los paquetes) y una posterior exploración (con algún programa) de los datos obtenidos. Para cada par de estaciones debe contabilizarse la cantidad de paquetes enviados y recibidos, así como la cantidad de bytes. (Puede escogerse esta última). Dependiendo del propósito el rastreo puede realizarse en las horas de mayor tráfico, tomando muestras por cortos períodos (5 min) que son analizadas inmediatamente.
> **Objetivo**: Precisar los patrones de tráfico entre máquinas e identificar aquellas que están sometidas a mayor exigencia.

NETMAN 10. Automatizando el rastreo.

¿Qué herramientas del sistema UNIX le puede ayudar a automatizar el rastreo?. (Ind.¿ necesita ejecutar programas periódicamente?).

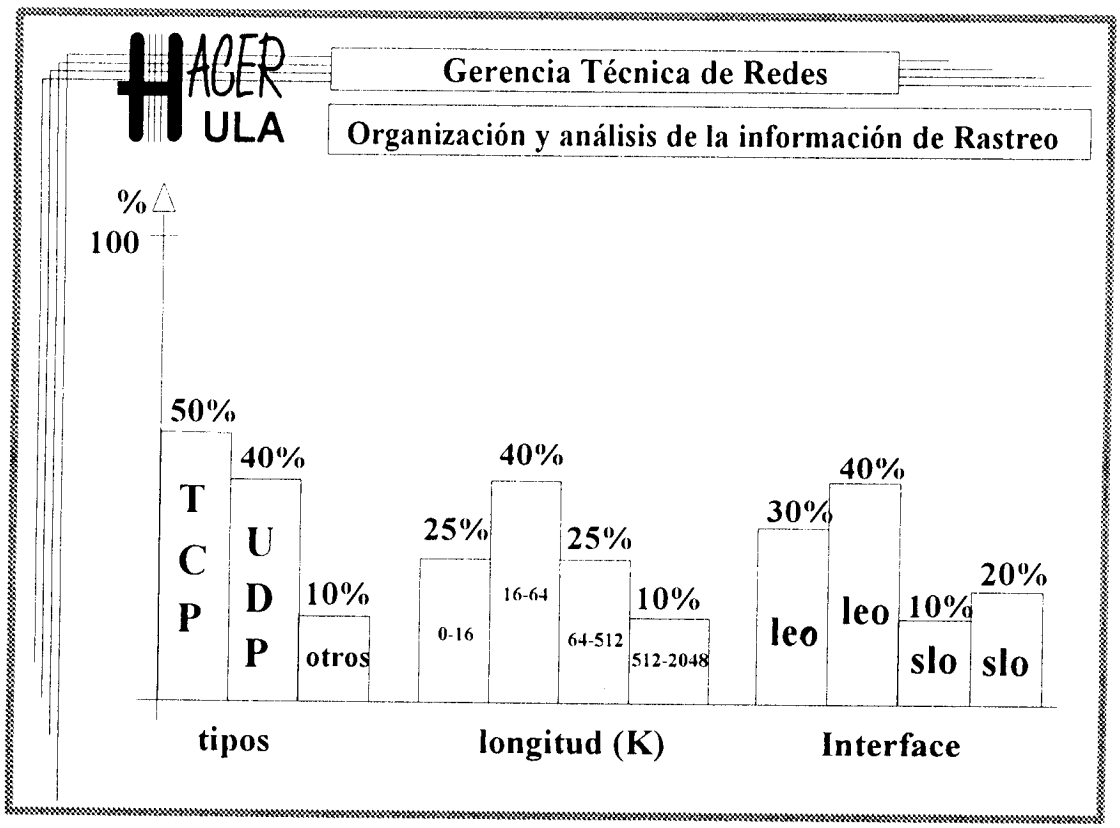

HACER ULA
Gerencia Técnica de Redes
Organización y análisis de la información de Rastreo
Servidor n
Estación n
Servidor1
Estación1
Servidor1
Servidor n
Estación1
Estación n
Matriz de comunicación entre máquinas
Período desde— hasta—

Notas:

Informe 2: Histograma de los tipos de paquetes.
Descripción: Enumera los paquetes de cada tipo (protocolo), capturados en determinado período o campaña.
Obtención: Sobre los mismos datos y archivos precisados en informe 1, se puede contar los paquetes de cada tipo en la muestra.
Objetivo: Precisar la influencia sobre el tráfico de determinados protocolos y aplicaciones.

Informe 3: Histograma de la longitud de paquetes.
Descripción: "Lista el número y proporción de paquetes de datos de longitudes diferentes".
Obtención: Se debe especificar "clases" o rango para el tamaño y, para cada muestra, contabilizar la cantidad de paquetes en cada rango.
Objetivo: La proliferación de paquetes pequeños puede significar un gran desperdicio por overhead en las redes de acceso contencioso. Eso es lo que se quiere precisar.

Informe 4: Distribución de uso del medio.
Descripción: Indica la utilización del medio por cada interfaz (con y sin *overhead*).
Obtención: Estableciendo un período de rastreo, se trata de estimar la porción de ese tiempo que cada interfaz emplea para transmitir su información. Por supuesto, combinando el efecto de todas la interfaces es posible estimar también el uso total del medio. Más aún, con un periodo de rastreo de un día completo (cuidado con el espacio en disco en la estación rastreadora) puede obtener el uso de medio en ese periodo y en periodos incluidos (¿Que ocurrió en el segundo de mayor tráfico?).
Objetivo: Perfilar el nivel de carga de la red


HACER
ULA
Gerencia Técnica de Redes
Organización y análisis de la información de Rastreo
%
100
50%
TCP
40%
UDP
10%
otros
25%
0-16
40%
16-64
25%
64-512
10%
512-2048
30%
leo
40%
leo
10%
slo
20%
slo
tipos
longitud (K)
Interface

Notas:

Informe 5: Histograma de los tiempos entre llegadas de paquetes
Descripción: Para cada estación, suministra el resumen de los tiempos entre llegada de paquetes al medio de transmisión.
Obtención: Esta medida es una primera aproximación en la estimación de la cantidad de información que genera cada estación por unidad de tiempo. Disponer de esta estadística permitiría "calcular" con mayor precisión, la estructura de red necesaria para atender determinada corporación. Una medida más realista se podría obtener si cada estación calculara la velocidad de generación de información de cada proceso (en respuesta al usuario). Sin embargo, esto implicaría colocar un programa rastreador en cada estación, lo cual no siempre es factible (casi nunca). Quizás el aspecto más importante a tomar en cuenta, si se usa el rastreo del medio para estimar la tasa de generación de tráfico, es que lo rastreado es lo que *logra* llegar al medio, no lo que *se requiere* colocar en él. Parte del tráfico generado se puede perder o retardar por insuficiencia de los *buffers* o por influencia de las colisiones al acceder al medio. En la práctica, mientras menos máquinas y tráfico tenga la red, más confiable es esta aproximación.
Objetivo: Perfilar la carga sobre la red.

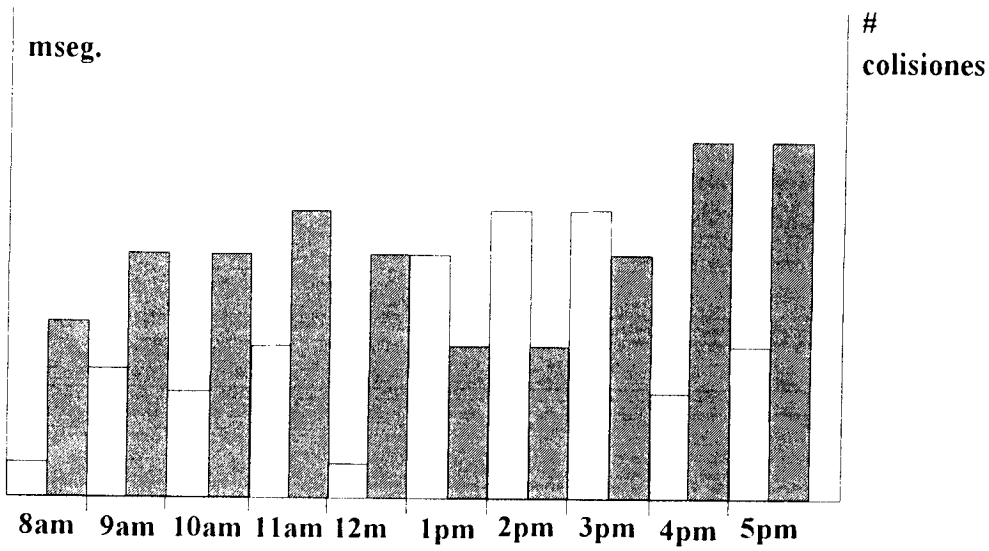
Informe 6: Histograma de colisiones.
Descripción: Tabula el número de colisiones por paquete (de cualquier tipo) transmitido al medio.
Obtención: Los rastreadores generalmente capturan la información en algún nivel por encima de la capa de enlace de datos. Esto indica que se requiere un rastreador especial, capaz de registrar el estado de los indicadores de colisión en la tarjeta. Un número alto de colisiones puede indicar que la red está muy cargada.
Objetivo: Perfilar el nivel de carga de la red

Existen productos comerciales que suministran toda esta información, sin necesidad de que el administrador emplee mucho tiempo diseñando y realizando el experimento. En ***Sniffer Network Analyzer*** de *Network General* y el ***LANAnalyzer*** de *HP* son dos buenos (y costosos) equipos para el rastreo intensivo y exhaustivo de redes. Por otra parte, tanto ***NetVisualizer*** como ***Sun Net Manager*** tienen incorporados programas para convertir a las tarjetas de las estaciones de trabajo en verdaderos rastreadores.

HACER ULA

Gerencia Técnica de Redes

Organización y Análisis de la Información de Rastreo



Notas:

Beneficios del Rastreo de redes.

1. Control anticipativo de la red.

    ¿Cómo está evoluacionando la red?.

2.- Optimización de Recursos.

    ¿Realmente necesitamos un puente?
    ¿Necesitamos una red local más rápida?
    ¿Qué tipo de estaciones (interfaces) será el adecuado para nuestra red?.

3.- Planificación de crecimiento.

    ¿Cuánto de cada recurso, hace falta en la nueva extensión de la red?

HACER ULA

Gerencia Técnica de Redes

BENEFICIOS DEL RASTREO DE REDES

1.- Control anticipado de la red.

2.- Optimización de recursos.

3.- Planificación de crecimiento.

Notas:

Introducción a la Gerencia Técnica de Redes

Network Management

Elementos de administración de redes

Permitir que la propia infraestructura de red favorezca su administración ha sido la aspiración de los administradores desde los comienzos mismos de la computación en red. Se han hecho grandes esfuerzos que incluso han terminado en otras aplicaciones. El UUCP en UNIX, por ejemplo, un sistema para transmisión de archivos y ejecución remota de comandos, fue concebido como un sistema de apoyo a la administración y terminó siendo el soporte de una muy extensa red de intercambio de correo.

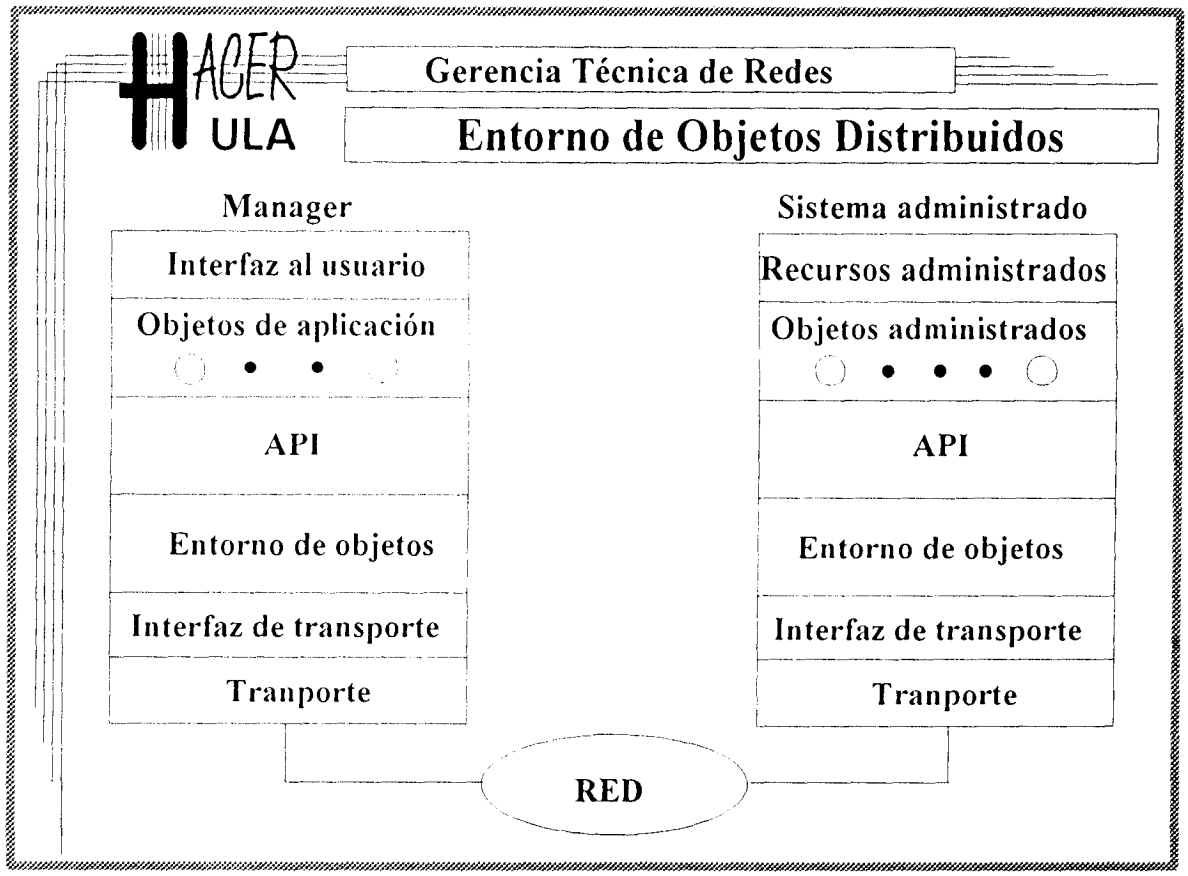
Sin embargo, la tendencia hacia la automatización de la administración continúa. Impulsados por la difusión de los sistemas abiertos, uno de los avances significativos de los últimos tiempos en redes, ha sido la aparición de protocolos de comunicaciones especialmente diseñados para administración remota. Protocolos que se han estandarizado rápidamente (aunque, como es común en este campo, continúa la paradójica existencia de más de un estándar) en respuesta a las necesidades de administración, pero también como parte de un esfuerzo sistemático hacia *la integración.* [6]

En ese sentido, se habla de que los sistemas administrativos están ahora en una tercera etapa de evolución. La primera etapa fue la administración local de máquinas. La segunda fue la administración centralizada con productos de un mismo fabricante, puesto que los sistemas *de propietarios* evolucionaron como respuesta a esta necesidad de *administrar todo desde un sólo punto.* La tercera etapa, propulsada por la aparición de esos *protocolos abiertos,* es la de los ***sistemas administrativos basados en estándares.*** [6]

Existen dos (todavía más de uno, pero menos de cien) conjuntos o familias de protocolos estándares para estos nuevos sistemas gerenciales. Uno es el presentado por la Organización Internacional de Normalización OSI, el ***Common Management Information Protocol***, considerado el estándar del futuro. Entretanto, el estándar del presente parece ser el ofrecido por Internet sobre su ampliamente difundida plataforma TCP/IP: ***Simple Network Management Protocol.*** Aunque difieren en su idea de administración, estas dos plataformas o conjuntos de protocolos comparten lo que algunos han llamado entorno de objetos distribuidos (*Distributed-object framework*)[6] para la administración. Introduciendo los conceptos de la Ingeniería del software orientada a objetos, se han diseñado protocolos, estructuras de datos (más bien clases de objetos) e interfaces de desarrollo, para implementar los nuevos sistemas administrativos. La lámina muestra las ideas subyacentes.

NETMAN 11. Diseño orientado a objetos.

¿Qué es un objeto?.


HACER
ULA
Gerencia Técnica de Redes
Entorno de Objetos Distribuidos
Manager
Interfaz al usuario
Objetos de aplicación
API
Entorno de objetos
Interfaz de transporte
Tranporte
Sistema administrado
Recursos administrados
Objetos administrados
API
Entorno de objetos
Interfaz de transporte
Tranporte
RED

Notas:

La administración de redes en OSI

El SNMP de Internet es el actual estándar de facto de la administración de redes. Será descrito en detalle más adelante. Ha sido implantado en una gran cantidad de productos de red por lo que se presume que tardará mucho en ser desplazado. No obstante, los comités conductores de Internet han admitido que el enfoque de administración de redes de ISO incluye aspectos muy interesantes. ISO ha clasificado las tareas de administración en los siguiente tipos [6]:

- **Administración de la configuración y de los nombres** (*Configuration and name management*): Se refiere a la preparación de los componentes de red, estableciendo sus parámetros de configuración de manera que puedan arrancar y funcionar. En esto se incluye la configuración de interfaces, actualización de parámetros en archivos de configuración y la asignación de nombres y direcciones a cada objeto.

- **Administración de fallas** (*Fault management*): Las operaciones de rastreo y análisis de variables que se discutieron en la primera parte, caen en esta categoría. El propósito es, entonces, prever, detectar y corregir fallas.

- **Administración del rendimiento** (*Performance management*): Nuevamente las operaciones de rastreo son parte de una categoría. En este caso el propósito es la planificación de capacidad y crecimiento (*).

- **Administración de seguridad** (*Security management*): Los procedimientos de control de acceso a cada sistema, permisología, verificación de identidad y encriptamiento. (Administración de passwords, cuentas y conexión externa).

- **Administración contable** (*Accounting management*): Inventario de recursos, tarifas de uso y facturación de recursos y dispositivos. Adquisición de dispositivos y sistemas.

NETMAN. 12.- Administración de Rendimiento.

(*)¿Por qué?.

HACER ULA

Gerencia Técnica de Redes

Administración de Redes en OSI

- Administración de la configuración y nombres.
- Administración de fallas.
- Administración de rendimiento.
- Administración de seguridad.
- Administración contable.

Notas:

Conceptos de administración de redes

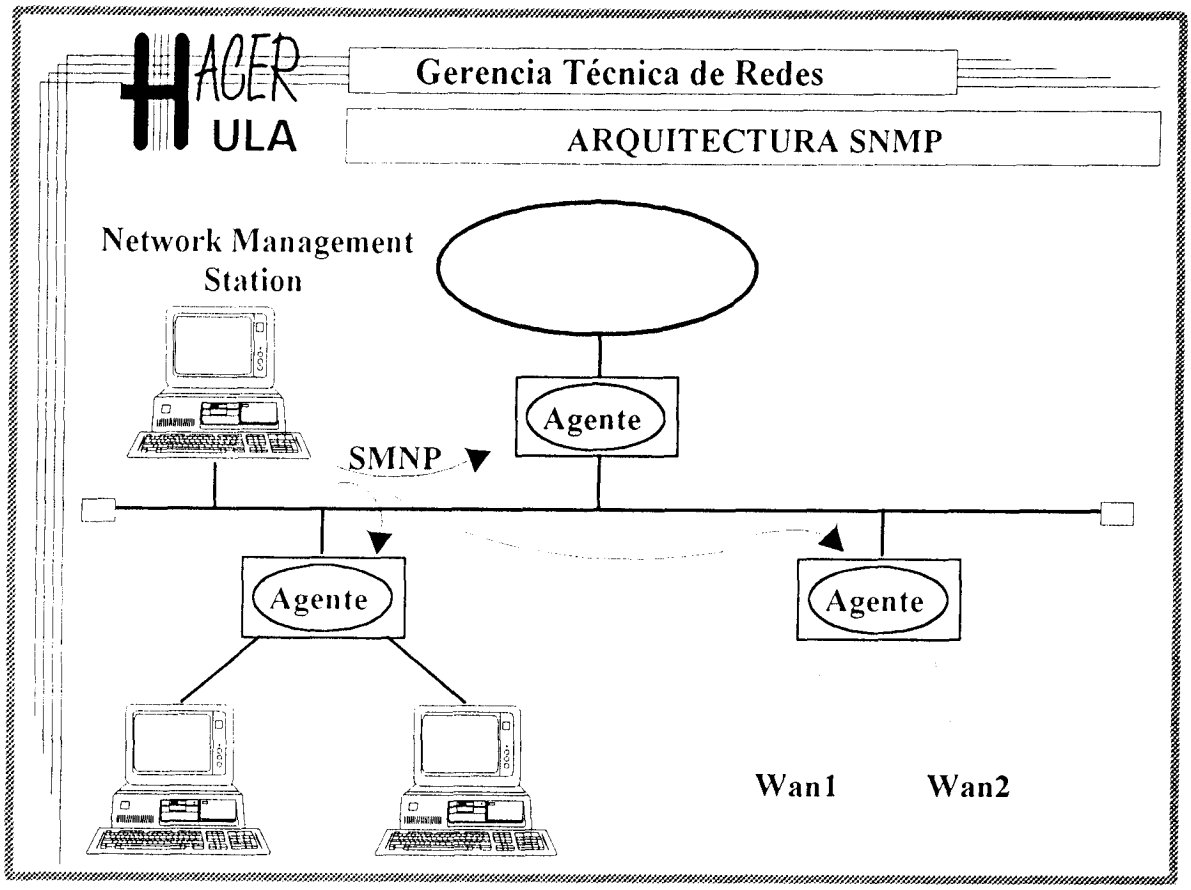
Esa clasificación de ISO muestra su enfoque del problema de administración basado en *áreas funcionales* [7]. El enfoque de Internet, por su parte, simplemente habla de *monitoring*, en los términos que se han venido explicando en el curso y *control*, "el proceso de modificar en tiempo real el comportamiento de la red, ajustando los parámetros mientras la red continúa operando, con el propósito de mejorar su funcionamiento o corregir fallas [7]".

Curiosamente, ambos modelos de organización se traducen en implementaciones similares. En ambos casos el modelo de trabajo implementado ofrece "protocolos de aplicación usados para efectuar transacciones o llamadas a procedimientos entre los sistemas administrados y los administrativos [7]".

En la plataforma TCP/IP (Internet) el modelo de trabajo es a grosso modo el siguiente: El administrador interactúa con una aplicación de administración, instalada en lo que se denomina el sistema administrativo (*Manager Station*). Esa aplicación interactúa a su vez con los llamados *agentes*, instalados en los sistemas administrados. Cada agente mantiene una base de datos de clases de objetos que representan al sistema administrado o sus subsistemas. Por ejemplo, una estación de trabajo puede tener una clase de objetos que representa a los programas de comunicaciones, otra al sistema operativo y otra a alguna aplicación más específica. Administrar el sistema es el proceso de supervisar esos objetos (instancias) obteniendo su estado actual (*getting*) y cambiando sus configuraciones (*setting*). Esos objetos son abstraciones empleadas por el sistema administrativo. En cada dispositivo administrado, el agente tiene que traducir las instrucciones para los objetos, en las acciones específicas (*). Como puede observarse, esta aproximación al problema es compatible con el entorno de objetos distribuidos.

NETMAN 13. Como convertir objetos abstractos en dispositivos reales.

Imagine la acción de rearrancar el sistema administrado. Si sólo es posible revisar y establecer valores de variables ¿ cómo puede implementarse esta acción en un objeto abstracto.?


HAGER
ULA
Gerencia Técnica de Redes
ARQUITECTURA SNMP
Network Management Station
Agente
SMNP
Agente
Agente
Wan1
Wan2

Notas:

Si el modelo de trabajo se dejara tal como está, la supervisión de la red implicaría que las estaciones administradoras deberían consultar (*polling*) periódicamente a los agentes. En una red *estable* esto puede significar ancho de banda perdido en consultas innecesarias (*). Por esta razón el modelo incluye otra herramienta: el evento. Ante la ocurrencia de un suceso que pueda alterar el funcionamiento de un dispositivo, el agente correspondiente genera un mensaje para el sistema administrado informándole la novedad. Ese mensaje se conoce en general como un evento, aunque en la jerga de Internet se le denomina *trap*.

Puede ocurrir, además, que el sistema a administrar no pueda entenderse con el sistema administrativo (o con la MS) (**). En ese caso se requiere de una agente traductor que sirva de intermediario entre el sistema administrativo y el dispositivo a administrar. Tal intermediario es conocido en Internet como el agente sustituto (*proxy agent*). Este agente sustituto debe poseer los objetos necesarios en su base de datos para representar al dispositivo administrado. No obstante, la conversión de las instrucciones en acciones sobre el dispositivo, sigue siendo asunto privado del agente.

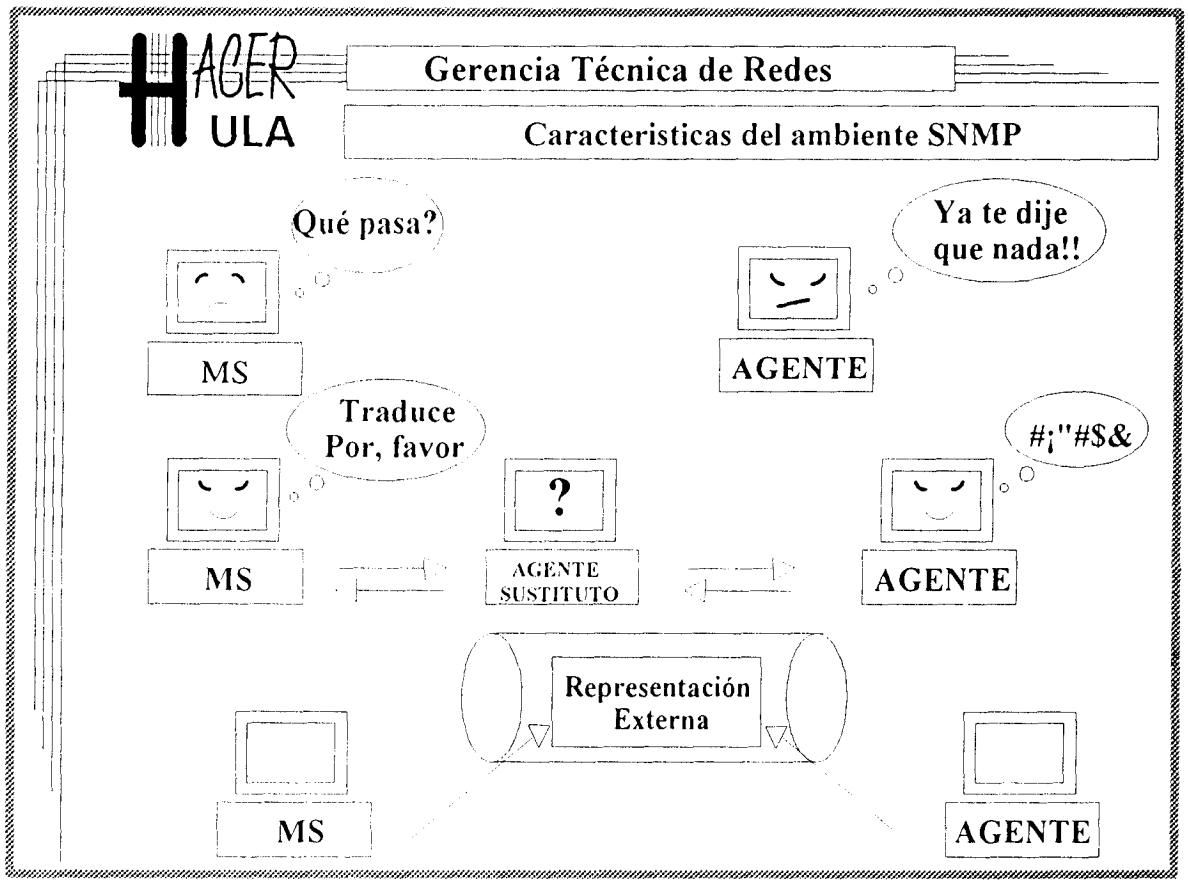
El último concepto indispensable para comprender el proceso de administración que se describe, es el de representación externa de datos (*External Data Formats)*. No podía quedar fuera de discusión este tópico fundamental en sistemas distribuidos. Al intercambiar datos entre máquinas distintas, uno de los primeros problemas a enfrentar es la homogeneización de la representación de los datos. Podría recurrirse a un módulo de programa que convierta los datos al formato que se usa en el sistema destino. Sin embargo, este enfoque implica crear ese programa para cada nueva máquina destino. Una aproximación más adecuada es la de convertir los datos a un formato público preestablecido. Ese es el enfoque empleado tanto por Internet, como por ISO. De hecho, la especificación de ese formato público fue creada por ISO y se denomina *Abstract Syntax Notation One* (ASN.1)

Con estos conceptos generales, continuamos ahora con un recorrido mucho más preciso sobre la implementación TCP/IP.

NETMAN 14. Más conceptos de administración.

(*) ¿Por qué?.

(**) Señale algunos ejemplos de esa situación. (Ind. ¿Cómo administrar desde una red TCP/IP, dispositivos en una red SNA?. ¿Cómo administrar un modem?)


HACER
ULA
Gerencia Técnica de Redes
Caracteristicas del ambiente SNMP
Qué pasa?
MS
Ya te dije
que nada!!
AGENTE
Traduce
Por, favor
MS
?
AGENTE
SUSTITUTO
#¡"#$&
AGENTE
Representación
Externa
MS
AGENTE

Notas:

Network Management en Internet.

La estrategia Internet para especificar la plataforma de administración se puede esbozar como sigue:

- Empleando los conocidos memoranda *Request For Comments* (RFC), y comenzando con la declaración general de la estrategia (cuyo formato y contenido es descrito en RFC 1052), se crea una base documental que describe completamente los componentes de sistemas administrativos. El comité coordinador de Internet, *Internet Activities Board* (IAB) asigna la tarea global de crear esas especificaciones a los *Internet Engineering Task Force* (IETF).

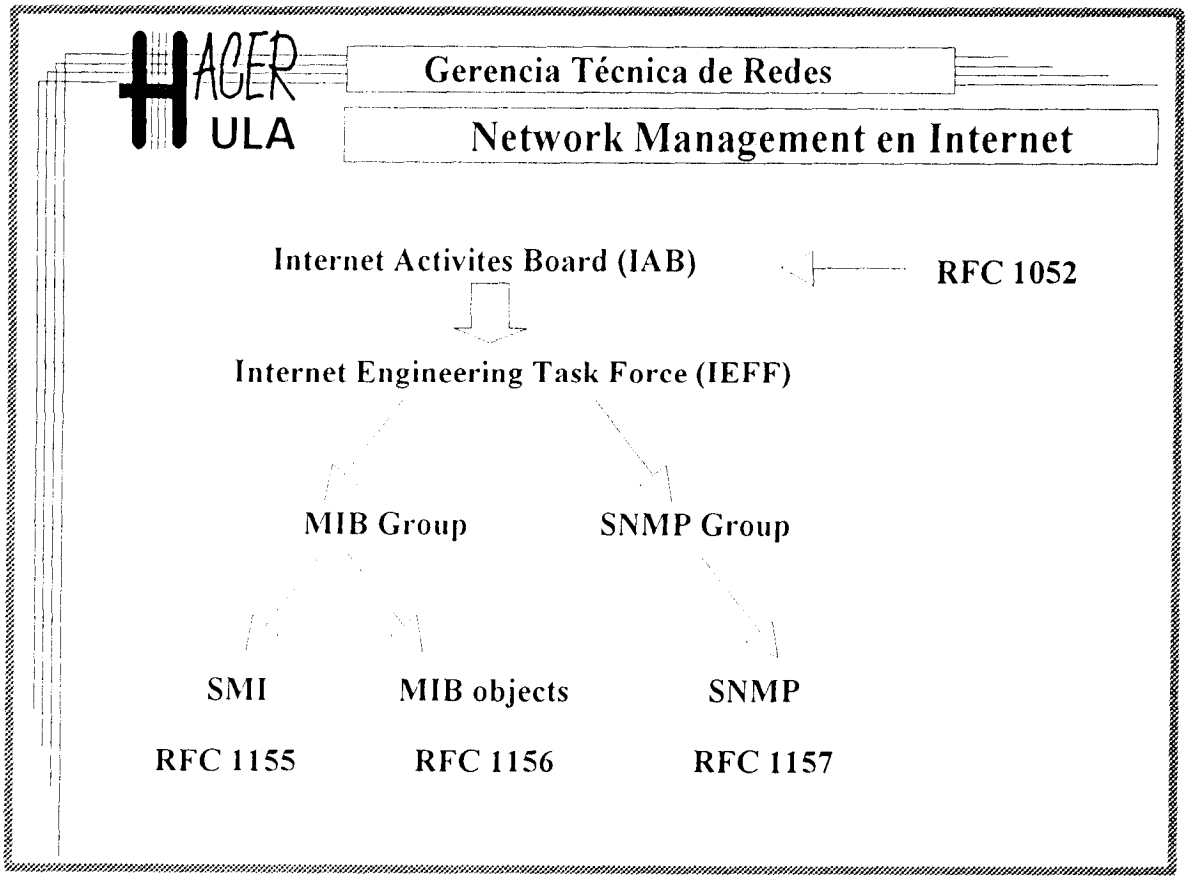
- IETF crea dos grupos de trabajo. El grupo MIB encargado de especificar la estructura y la propia familia de clases de objetos y el grupo SNMP, encargado de especificar el protocolo de aplicación.

- La definición de la base de objetos "administrables" es separada en dos. Por una parte se define la estructura de esa base, dando origen a la estructura de información administrativa (*Structure of Management Information*, SMI), contenida en el RFC 1155. Por la otra, se definen, siguiendo lo establecido en SMI, los objetos administrables (la base propiamente) agrupados en la *Management Information Base* MIB (RFC 1156).

- El grupo SNMP, especifica el *Simple Network Management Protocol* aprovechando experiencias previas (HEMS, SGMP) y atendiendo a la necesidad de disponer de un protocolo sencillo, económico y rápido de implementar (RFC 1157).

NETMAN 15. Consiguiendo las RFC.

Las RFC son documentos públicos que pueden obtenerse a través de Internet con una conexión `ftp anonymous` a `nic.ddn.mil`.


HACER
ULA
Gerencia Técnica de Redes
Network Management en Internet
Internet Activites Board (IAB)
RFC 1052
Internet Engineering Task Force (IEFF)
MIB Group
SNMP Group
SMI
RFC 1155
MIB objects
RFC 1156
SNMP
RFC 1157

Notas:

Management Information Base (MIB)

SMI

Antes de presentar la MIB, es necesario explicar SMI. La SMI declara los tipos de datos que pueden emplearse en una MIB, como se definen e identifican los objetos de la base y como esta pueden extenderse. Definir SMI fue particularmente crítico, puesto que el objetivo principal de diseño era permitir que aquellas MIBs que se crearan según SMI, pudieran ser accedidas y empleadas tanto con el protocolo SMNP como con CMOT, la versión Internet del CMIP de ISO. Todo un galimatías.

SMI emplea los siguientes tipos de datos (tomados de ASN.1). 4 tipos primitivos (no estructurados): INTEGER, OCTET STRING, OBJECT IDENTIFIER y NULL. 1 tipo estructurado: SEQUENCE, con la restricción severa para algunos, de que no se permite el anidamiento (*nesting*) de secuencias.

Un OBJECT IDENTIFIER es un secuencia de números que señala un nodo en el árbol de nombres de objetos definido por ISO. Cada nuevo nodo de ese árbol puede definirse una etiqueta y un número, extendiendo una de sus ramas. La raíz de ese árbol no tiene nombre, pero tiene tres hijos cuyas etiquetas representan a las dos organizaciones internacionales de estandarización, reservando el número 0 para CCITT, el 1 para ISO (**iso(1)**) y el 2 para los trabajos conjuntos. Es importante destacar que los objetos representados en el árbol no están restringidos a un tipo de objeto. De igual forma se hace referencia a ISO, a uno de sus documentos o a un producto. Más aún, el mismo esquema se usa para referirse a clases de objetos y a instancias. La jerarquía de nombres es simplemente un arreglo administrativo.

De esta forma, bajo la rama que origina el nodo ISO, se ha asignado un nodo en siguiente nivel a las organizaciones internacionales **org(3)**. El National Institutes of Standards and Technology, cedió uno de los subnodos de org(3) que le correspondieron al Ministerio de Defensa Norteamericano (DOD) y por ello este tiene asignado ahora el **DOD(6)**. Para oficializar la existencia de Internet como un "objeto" adscrito al DOD, en algún lugar (MIB) debería existir una declaración de OBJECT IDENTIFIER como la que sigue:

Internet OBJECT IDENTIFIER ::= { iso org(3) DOD(6) 1 }

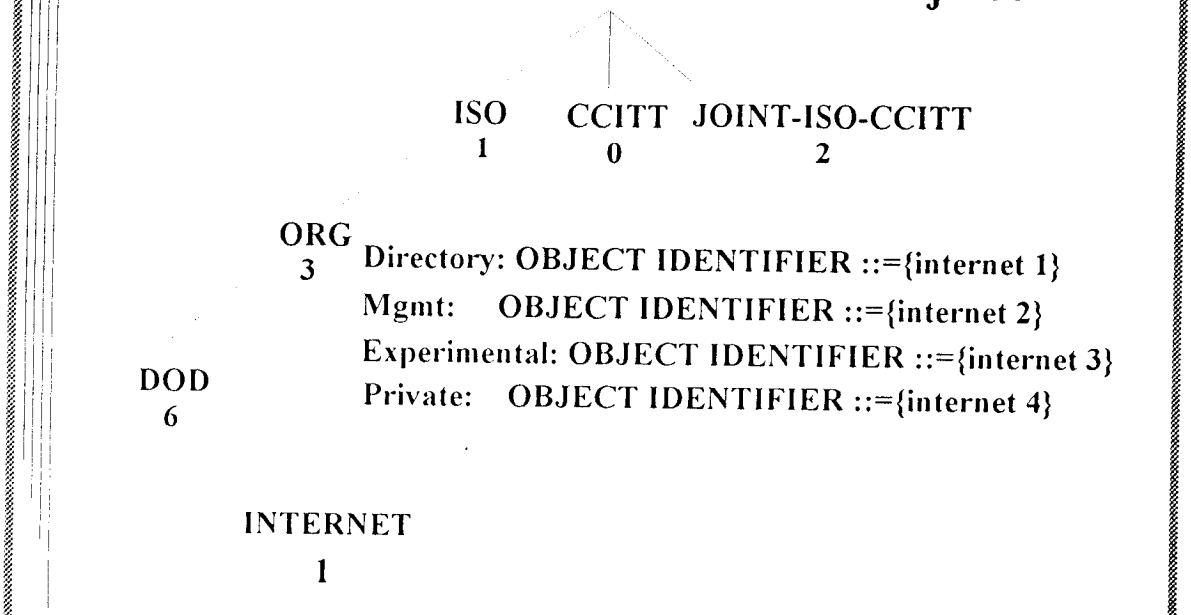
En lo sucesivo cada vez que nombremos los objetos de Internet, veremos aparecer la cadena 1.3.6.1. En algunos casos, cuando la referencia a Internet está sobreentendida, se menciona directamente el objeto siguiente en la jerarquía (Ver lámina):

HACER ULA

Gerencia Técnica de Redes

SMI

Arbol de identificadores de objetos



Notas:

Además de esos 5 tipos tomados directamente del ASN.1 (IMPLÍCITA), en el SMI se definen otros tipos de objetos específicos para la aplicaciones administrativas.

- **NetworkAddress**: Con la expectativa de emplear otro tipo de protocolos de red en el futuro, se crea este tipo estructurado (CHOICE) de objeto para permitir escoger la familia de protocolos. Actualmente solo tiene una opción: Internet.
- **IpAddress**: un OCTET STRING de longitud 4 ordenado por bytes (*).
- **Counter**: un contador con retorno en el rango 0 - 2^{32-1}.
- **Gauge**: un contador sin retorno en el mismo rango.
- **TimeTicks**: contador en milésimas de segundos transcurrido en un época.
- **Opaque**: Sin tipo.

Finalmente, en SMI se define el formato que se usará en las MIBs para especificar los tipos de objetos, el cual tiene la forma siguiente: (Ver ejemplo en la lámina).

1. **OBJECT**: Una especificación del nombre con el formato: descriptor { OBJECT IDENTIFIER }.
2. **Syntax**: El tipo de objeto según ASN.1
3. **Definition**: Descripción del objeto.
4. **Access**: Tipo de acceso permitido (*read-only*, *read-write*, *write-only* o *not-accessible*).
5. **Status**: Condición actual del objeto (*mandatory*, *optional* o *obsolete*).

NETMAN 16. Objetos e identificadores.

(*) ¿Por qué ese objeto tiene ese formato?.

Si tuviera que comparar a la SMI con alguna parte del código fuente de un programa, ¿cual se le parecería más?.

Muchos han lamentado la ausencia de objetos *umbral* en SMI (y por ende en las MIBs). Su instructor le explicará el porqué.

HACER ULA

Gerencia Técnica de Redes

TIPOS DE OBJETOS BASICOS EN SMI

atIndex OBJECT-TIPE
SINTAX INTEGER
ACCESS read -write
STATUS mandatory
:: = {atEntry 1}

atPhysAddress OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read - write
STATUS mandatory
:: = {atEntry 2}

atNetAddress OBJECT-TYPE
SYNTAX NetworkAddress
ACCESS read - write
STATUS mandatory
:: = {atEntry 3}

atEntry OBJECT-TYPE
SYNTAX AtEntry
ACCESS read - write
STATUS mandatory
:: = {atTable 1}

atTable OBJECT-TYPE
SYNTAX SEQUENCE OF AtEntry
ACCESS read - write
STATUS mandatory
:: = {at 1}

AtEntry :: = SEQUENCE{
atIndex
INTEGER
atPhysAddress
OCTET STRING
atNetAddress
NetworkAddress
}

Notas:

MIB:

El documento donde se especifica MIB si contiene la definición de los objetos que serán "manipulados por los protocolos de administración" [7]. Concentrando la atención en lo que significa administrar cualquier sistema (una misma abstracción representando productos distintos), se puede apreciar la dificultad que implicó crear MIB. Se requirió, en principio, que cada objeto a incluir cumpliera con las siguientes condiciones [7]:

1. Debía ser esencial para administrar fallas y manipular configuraciones.
2. Util para alguna plataforma protocolar.
3. De utilidad general. Objetos específicos de alguna aplicación no fueron considerados.

La primera versión de MIB (ya existe una MIB II y muchos MIBs particulares), contenía 126 objetos. Fue dividida en ocho grupos de objetos: *System Group*, *Interfaces Group*,. *Address Translation Table Group*, *IP Group*, *ICMP Group*, *TCP Group*, *UDP Group* y *EGP Group*. Algunos elementos de esos grupos se muestran en las láminas.

Es importante observar el cambio de paradigma en Ingeniería del software que se ha reflejado en los sistemas administrativos en red. En lugar de recurrir a un sistema de base de datos relacionales, se adoptan plataformas orientadas a objetos para el almacenamiento y manipulación de la información administrativa.

NETMAN 17. MIB.

Su instructor le indicará los archivos que contienen especificaciones MIB para los agentes de las estaciones de trabajo. Revíselos e identifique los conceptos hasta aquí planteados. (Ind. Busque los directorios del software de red, ChameleonNFS).

HACER ULA

Gerencia Técnica de Redes

Management Information Base

Condiciones para incluir objetos en MIB

1. Debe ser esencial para detectar y corregir fallas y controlar configuraciones.
2. Util para alguna plataforma.
3. De utilidad general.

Los grupos en MIB

System,Interfaces,Address translation table,IP,ICMP,TCP,UDP,EGP.

Notas:

Simple Network Management Protocol

En las siguiente secciones gracias a que se ha establecido el marco referencial necesario (SMI, MIB), se hará una revisión general del SNMP siguiendo el esquema del documento oficial RFC 1157. Comenzando con una descripción del arquitectura y después un resumen de la especificación del protocolo.

Arquitectura SNMP.

Una red administrada con SNMP es una colección de estaciones de administración (MS) y elementos de red . Las estaciones de administración alojan y ejecutan los programas de administración para rastrear y controlar los agentes, programas estos que se alojan y ejecutan en los dispositivos administrados (elementos de red). Entre estos se cuentan: Las estaciones, puentes, concentradores, enrutadores, pasarelas (gateways), servidores de terminales y todos aquellos dispositivos a los que se pueda controlar y supervisar a distancia. Las estaciones de administración (mas propiamente las aplicaciones de administración) se comunican con los agentes usando el protocolo SNMP.

Los objetivos de diseño de esta arquitectura administrativa son:

1. Reducir el número y complejidad de las funciones administrativas que tiene que realizar el propio agente en el elemento administrado (*).

2. Tomar previsiones para que, en el marco del paradigma Internet de rastreo y control, puedan implementarse soluciones a aspectos no contemplados de la administración.

3. Que la arquitectura se mantenga tan independiente como le sea posible de la arquitectura de hardware y mecanismos particulares de los elementos de red.

NETMAN 18. Ventajas del SNMP.

(*) ¿Qué sentido puede tener reducir la complejidad de los agentes?.
¿Mencione alguna característica que pueda ser común a todos los enrutadores y otra que no?.

HACER ULA

Gerencia Técnica de Redes

PROPOSITOS DE LA ARQUITECTURA INTERNET

- "Minimizar la complejidad y cantidad de funciones administrativas ejecutadas por los agentes."
- "Proveer una plataforma capaz de admitir aspectos administrativos y operación de la red que no hayan sido considerados."
- "Proveer una plataforma independiente en lo posible de la arquitectura y mecanismos de un dispositivo particular."

Notas:

Elementos de la arquitectura SNMP:

A título referencial presentamos los elementos de la arquitectura, algunos de los cuales ya han sido explicados:

- El *ámbito* de la información transmitida con el protocolo. Ya se ha dicho que los datos se refieren a objetos definidos en las *Management Information Bases.*

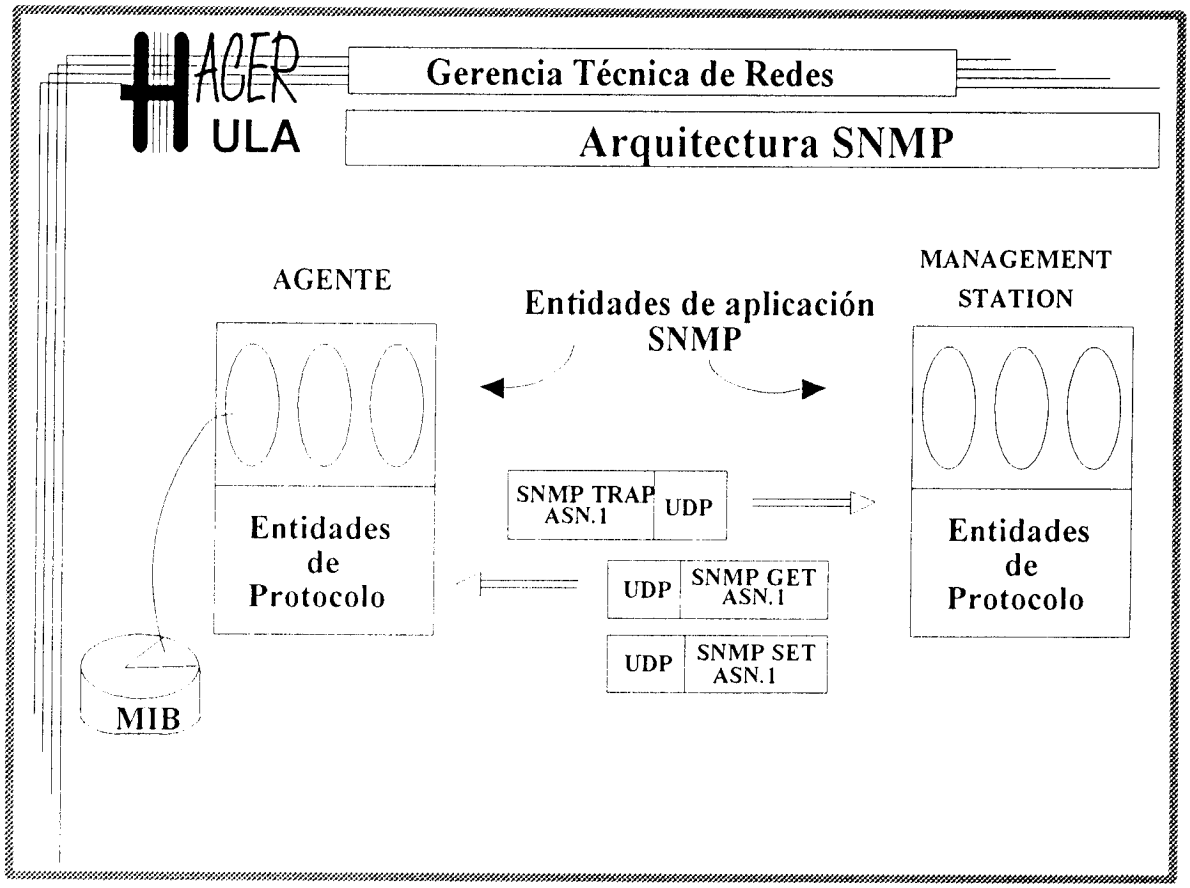
- La representación de la información. También se ha dicho que se emplea el esquema estandar establecido por ISO en la *Abstract Syntax Notation One.* (Realmente un subconjunto de ASN.1).

- Las operaciones sobre la información (y los objetos) que son soportadas por el protocolo. Una función administrativa en SNMP consiste de la inspección (get) y/o alteración (set) de una variable en el agente. En consecuencia, son estas dos las primitivas de interacción entre agentes y aplicaciones, establecidas por el SNMP. No obstante, el protocolo admite una primitiva más para permitir al agente reportar una situación irregular, sin esperar a que sea solicitada la novedad. Se trata de los *traps* o mensajes de eventos.

- La sintaxis y semántica de los diálogos entre entidades. Una y otra serán explicadas al especificar el protocolo. Acerca de los medios empleados para el intercambio de mensajes (así es que como se realizan los diálogos) debe decirse que SNMP requiere solamente un protocolo de transporte no orientado a conexión. Cada mensaje viaja en un *datagrama.* En las primeras realizaciones de SNMP se ha empleado el UDP.

NETMAN 19. Rastreo SNMP.

Empleando alguno de los sistemas estudiados en la primera parte, rastree un diálogo SNMP en la red del laboratorio. (Ind. Siga las indicaciones de instructor cuidadosamente).


HACER
ULA
Gerencia Técnica de Redes
Arquitectura SNMP
AGENTE
Entidades de aplicación SNMP
MANAGEMENT STATION
Entidades de Protocolo
SNMP TRAP ASN.1
UDP
UDP
SNMP GET ASN.1
UDP
SNMP SET ASN.1
Entidades de Protocolo
MIB

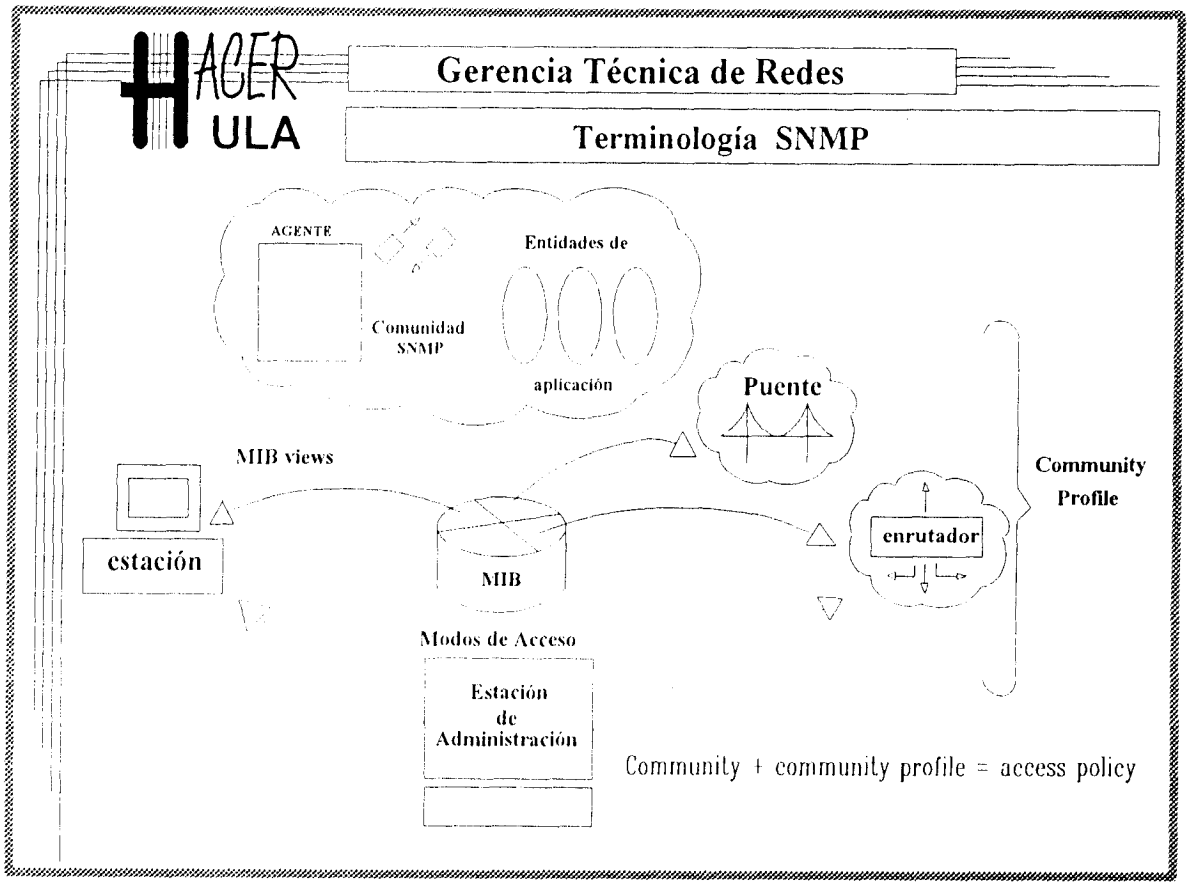
Notas:

- Definición de las relaciones administrativas. Son varias las vinculaciones que pueden establecerse entre los elementos de un sistema SNMP. Veamos la terminología empleada para identificarlas:

  - Las entidades (procesos) que residen en las MS y en los otros elementos de la red, se denominan *entidades de aplicación SNMP*.
  - Los procesos que implementan el protocolo SNMP (entidades pares, según la terminología OSI) se llaman *entidades de protocolos*.
  - La asociación (arbitrariamente establecida por el administrador) entre un agente y un conjunto de arbitrario de entidades de aplicación, se denominan *comunidad SNMP* (*community*). Cada comunidad SNMP es designada por su *nombre de comunidad* (*community name*).
  - Un mensaje enviado por una entidad a otra en su misma comunidad y que se identifique como tal, es un *mensaje auténtico* (*authentic SNMP message*).
  - El conjunto de objetos en las MIBs que se refiere a un particular elemento de red (estación, enrutador u otro) es llamado *SNMP MIB View*.
  - Se define como modo de acceso (access mode) a un elemento del conjunto { READ-ONLY, READ-WRITE, WRITE-ONLY, NOT-ACCESIBLE }.
  - La asociación de un modo de acceso con un SNMP MIB View es llamada *SNMP community profile* y representa diversos privilegios de acceso a variables en la MIB.
  - Finalmente, la asociación de un SNMP comunity profile con una comunidad SNMP es llamada *política de acceso SNMP* (*SNMP access policy*). "Una política de acceso señala el *comunity profile* (MIB view, access mode) que un agente ofrece a su comunidad [8]". Dada una política de acceso, si el elemento de red en el que reside el agente NO es el mismo al que se refiere la *MIB View*, entonces la política de acceso debe denominarse *proxy access policy* y su agente es un *proxy agent*. (*).

NETMAN 20. Utilidad de los agentes sustitutos.

(*)¿Para qué pueden emplearse los agentes sustitutos?.


HACER
ULA
Gerencia Técnica de Redes
Terminología SNMP
AGENTE
Entidades de
Comunidad
SNMP
aplicación
Puente
MIB views
Community
Profile
estación
MIB
enrutador
Modos de Acceso
Estación
de
Administración
Community + community profile = access policy

Notas:

- Forma y significado de las referencias a los objetos administrados. En particular nos interesa el mecanismo que se empleará para referenciar *instancias* particulares de un objeto. La solución adoptada no es más que una extensión de la estrategia empleada para referenciar a los propios tipos de objetos. En la RFC 1157 [8], se encuentra un ejemplo muy esclarecedor: " Suponga que se desea identificar una instancia de la variable *sysDescr*. La clase de objeto para *sysDescr* es 1.3.6.1.1.1.11. En este caso, la instancia correspondiente se identifica agregándose un número con lo que el OBJECT IDENTIFIER se convierte en 1.3.6..1.1.1.1.1.0".

iso	org	DOD	Internet	mgmt	mib	system	sysDescr	instance
1	3	6	1	1	1	1	1	0

Para referirse a una conexión TCP (socket), por otra parte, se puede usar una composición similar: tcpConnState.150.185.128.1.21.150.185.131.1.2059 (*).

Esto completa la descripción de la arquitectura protocolar del SNMP. A continuación la descripción del protocolo propiamente.

Especificación del protocolo SNMP.

"El SNMP es un protocolo de aplicación a través del cual se puede consultar o alterar las variables un una MIB contenida en un agente [8]".

El diálogo SNMP es un intercambio de datagramas de usuario UDP. Cada datagrama contiene un mensaje, el cual a su vez, consta de identificador de versión, un nombre de comunidad y una unidad de datos de protocolo (PDU, definidas más adelante). Los mensajes para consultar y configurar (*get and set*) son recibidos en el puerto 161 del agente. Los traps son recibidos en el puerto 162 (¿de quién?).

NETMAN 21. Instancias de objetos.

(*). Indique los componentes de ese "formato" para referirse a la instancia. Haga lo mismo (con ayuda del instructor) en las siguientes:

ifType.2
atPhysAddress.3.1.150.185.140.1
ipAdEntAddr.150.185.128.10
ipRouteNextHop.150.185.128.1

HACER ULA

Gerencia Técnica de Redes

REFERENCIAS A OBJETOS

iso	org	dod	internet	mgmt	mib	system	sysDescr	instance
1	3	6	1	1	1	1	1	0

Para obtener información acerca de un sistema administrado, se deben solicitar los datos vinculados al objeto.

1.3.6.1.1.1.1.1.0

Para hacer referencia a una instancia u objeto particular generalmente se usa un nombre de variable compuesto con otros valores que caractericen al objeto. ejemplo:

tcpConnstate.150.185.128.1.21.150.185.131.1.2059.

Notas:

Las unidades de datos de protocolos PDU, que se emplean en SNMP son:

GetRequest-PDU, GetNextRequest-PDU, GetResponse-PDU, SetRequest-PDU y Trap-PDU.

Su descripción formal se muestra en los anexos. Es oportuno presentar las nuevas versiones de SNMP.

Nuevas versiones y extensiones.

A partir de 1993 está en el mercado la nueva versión de SNMP llamada SNMP II o *Simple management protocol* (SMP). SMP se inspira en lo que se ha denominado SNMP secure, una serie de especificaciones (RFC 1351 al 1353) que incorporan al SNMP las posibilidad de encriptamiento de datos usando el *Data Encryption Standard* (DES), pero a título opcional, puesto que el gobierno norteamericano no permite la exportación de esta tecnología.

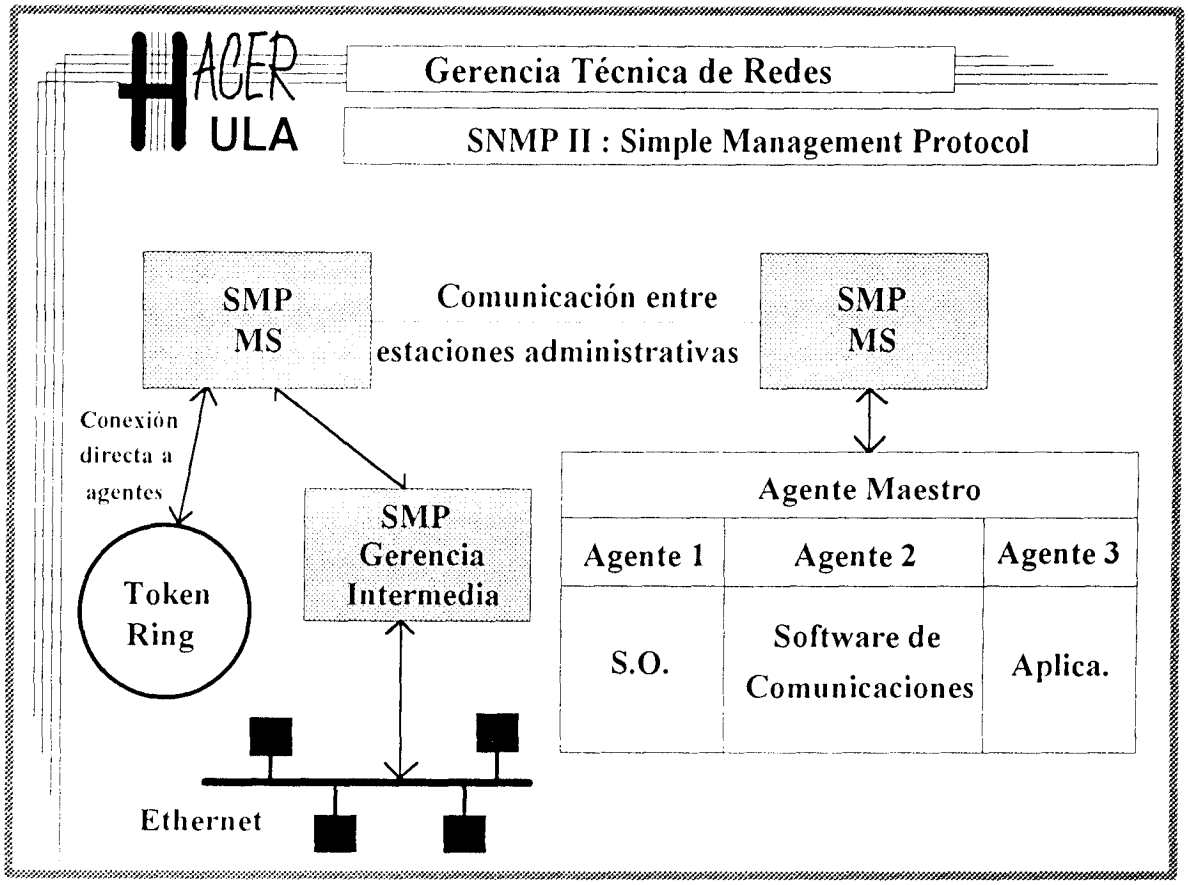
SMP agrega también, las siguiente facilidades a SNMP [9]:

1. Introduce un esquema de *bloqueo*, por medio del cual una estación tiene acceso ininterrumpido y exclusivo a un agente mientras lo configura.
2. Para aumentar el rendimiento en el uso del canal, SMP incorpora un nuevo comando de consulta (GETBULK) que permite a la MS consultar un rango de variables simultáneamente (antes era necesario varios GETNEXTs).
3. SMP incorpora un nuevo tipo de contador de 64 bits.
4. Con el primer SNMP una consulta que no podía ser atendida por un agente, debido a que no conocía el MIB en cuestión, era rechazada completamente. SMP permite responder a consultas parcialmente, indicando como "condiciones de excepción" aquellas que no alcanza a resolver.
5. La interfaz que soporta a SMP permite que este sea implantado sobre otras plataformas distintas a TCP/IP (IPX, Appletalk, CLNP).
6. SMP permite la comunicación entre estaciones administrativas, permitiendo la inserción de jerarquía administrativa. Una estación podría actuar como administradora o como agente (Ver lámina).

NETMAN 22. Integración de un ambiente de administración con SMNP.

Su instructor le guiará en un ejercicio de consulta a varios elementos de red (enrutadores de distintos fabricantes), usando los sistemas alcanzables desde su laboratorio.

¿Qué es orden lexicográfico de objetos SNMP?.


HACER
ULA
Gerencia Técnica de Redes
SNMP II : Simple Management Protocol
SMP
MS
Comunicación entre
estaciones administrativas
SMP
MS
Conexión
directa a
agentes
SMP
Gerencia
Intermedia
Agente Maestro
Agente 1
Agente 2
Agente 3
Token
Ring
S.O.
Software de
Comunicaciones
Aplica.
Ethernet

Notas:

Common Management Information Protocol (CMIP)

El uso de la palabra *common* (común) en el nombre de este protocolo pretende sugerir su condición de protocolo de administración para las 5 áreas funcionales definidas por ISO (que han sido tratadas antes). ISO ha establecido que el trabajo de administración se realice en el marco del *Common Management Information Service*, en el cual estaciones y agentes se comunican usando CMIP.

CMIP fue especificado casi al mismo tiempo que SNMP, pero este tomó la delantera en implementación y soporte. En constraste con este, la filosofía de desarrollo de CMIP hace énfasis en la versatilidad de su plataforma, incluyendo en ella una gran variedad de funciones. Curiosamente, la disputa entre la visión CMIP y la SNMP es similar a aquella entre la filosofía RISC y la CISC para diseño de procesadores.

CMIP está basado en transacciones y es orientado a conexión, en los mismos términos que otros protocolos de aplicación (capa 7) en OSI. Se establece una asociación entre las entidades que requiere un establecimiento y liberación de conexión.

CMIP es, todavía, una propuesta para estandar (aunque está a punto de ser declarado norma internacional). Sin embargo, se han hecho previsiones para migrar los sistemas administrativos hacia esa plataforma, en el largo plazo. Entre esas previsiones se cuenta el establecimiento de un sistema de gestión de objetos común (MIBs con ASN.1) con SNMP. Por su parte, Internet adoptó una estrategia doble. Implementó y difundió ampliamente el SNMP, pero también presentó su versión de CMIP sobre la plataforma TCP/IP, que se denomina *Common Management Information Protocol over TCP/IP* (CMOT).

Common Management Information Protocol over TCP/IP (CMOT)

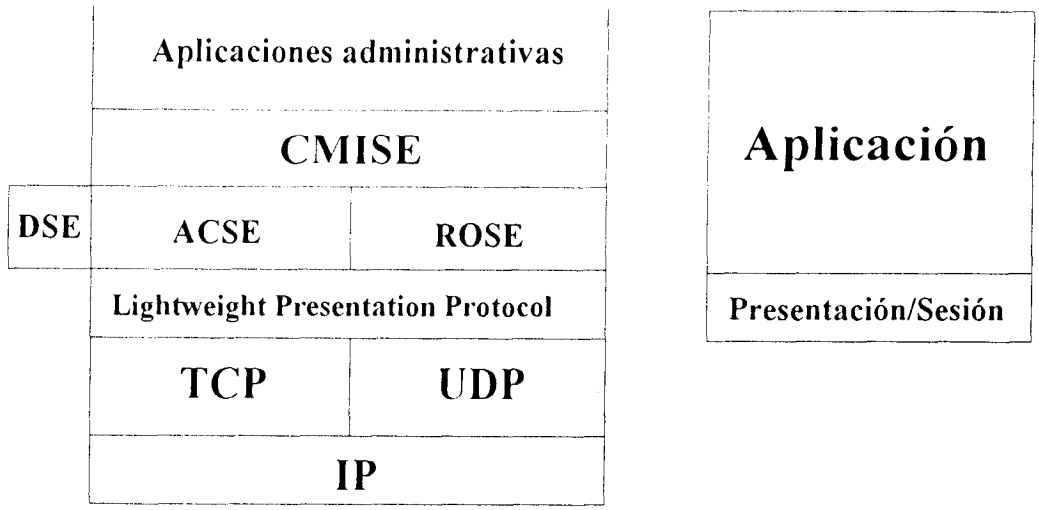
Internet se aprovecha de la estrategia OSI de definir protocolos independientes en cada capa, para implementar CMIP. Para codificar los programas con los protocolos de aplicación empleados en el CMIS, Internet debió resolver la implementación de la capa de presentación (que como sabemos, no se define en el modelo DOD). Para ello, crea el *Lightweight Presentation Protocol* (LPP), protocolo de presentación compatible con OSI, pero apoyado en TCP y UDP, como muestra la lámina [7].

Los restantes elementos son exactamente los empleados por CMIP. Tres elementos de servicios de aplicación conocidos como: *Association Control Service E.* (ACSE), con los mecanismos para establecer y liberar asociaciones; *Remote Operation S. E.* (ROSE), para las transacciones solicitud-respuesta; y el CMISE que implementa el CMIS para las aplicaciones de administración, cuyas primitivas veremos más adelante.

HACER ULA

Gerencia Técnica de Redes

Estructura protocolar de CMOT



Notas:

Es el estilo de los protocolos OSI, mantener abierta la posibilidad de configuración posterior de cada uno. Para completar la configuración de parámetros y variables que se dejan sin especificar al momento de desarrollo, el instalador puede recurrir a un archivo *profile* para crear una adecuada a sus necesidades. CMIP ofrece esta facilidad e Internet la aprovecha para especificar (el documento RFC 1095 es el mismo *profile*), entre otras cosas, los puertos empleados para las conexiones administrativas. El puerto 163 es usado por la estación administrativa y el 164 por el agente, tanto en TCP como en UDP.

La relación de CMOT con SMI.

No todo resultó tan transparente en la estrategia doble de Internet. Sin olvidar el acuerdo de emplear las MIBs tanto para CMIP como para SNMP, el enfoque OSI de las *Management Information Bases* es esencialmente distinto al de Internet. Mientras que el SMI Internet plantea un espacio de objetos plano, el OSI SMI habla de jerarquías de objetos. La que causa mayor trastorno al enfoque Internet es la llamada jerarquía contentiva (*containment hierarchy*), usada por OSI para definir las instancias de objetos que, como vimos antes, es asunto del protocolo según Internet. Fue necesario entonces, establecer un sistema relacionante entre esa jerarquía y el SMI de TCP/IP.

En OSI's SMI las instancias de clases de objetos sobre los que se actúa se denominan *objetos administrados* (*managed objects*), cada uno caracterizado por un conjunto de atributos. Algunos de estos atributos, cuando se les asigna un valor puede identificar unívocamente al objeto, por lo que se les llama *atributos distintivos* (*distinguished atributes*). Los atributos distintivos pueden ser usados, con sus valores, para identificar a instancias de clases, denominándose en tal caso *nombres relativos distintivos* (*relative distinguished names*). Reuniendo todos los nombres relativos a un objeto se puede construir el *nombre distintivo* del mismo (*distinguished name*).

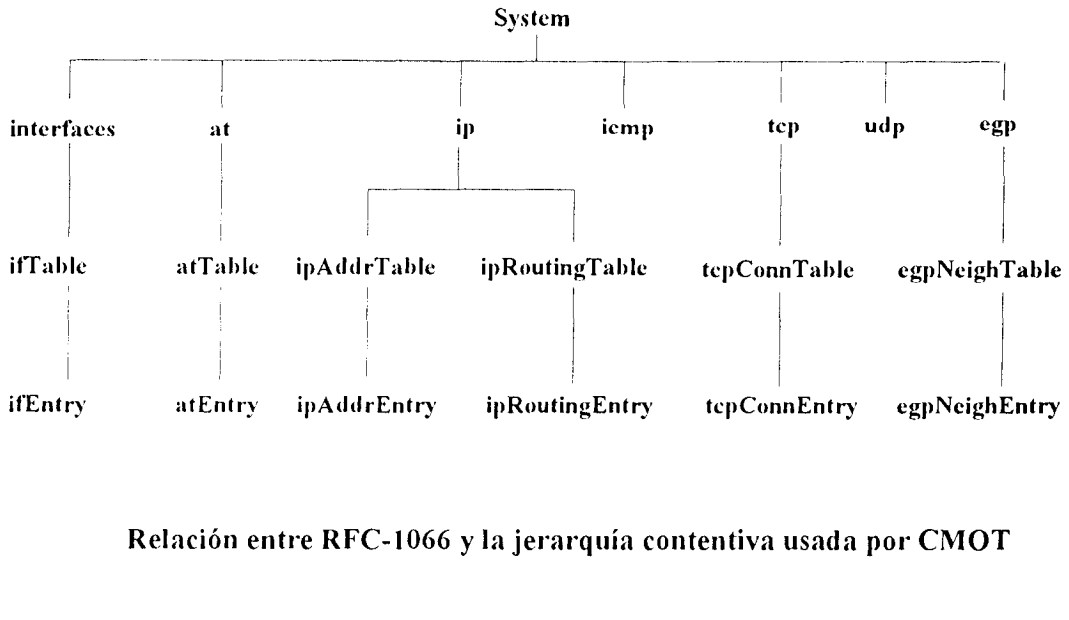
A título ilustrativo, la lámina muestra la relación de correspondencia entre el grupo *system* (usado en SNMP e incluido en RFC 1066) y los atributos de la jerarquía contentiva OSI SMI.

25

HACER ULA

Gerencia Técnica de Redes

Correspondencia entre OSI's SMI y TCP/IP SMI.



Relación entre RFC-1066 y la jerarquía contentiva usada por CMOT

Notas:

Operaciones CMIP.

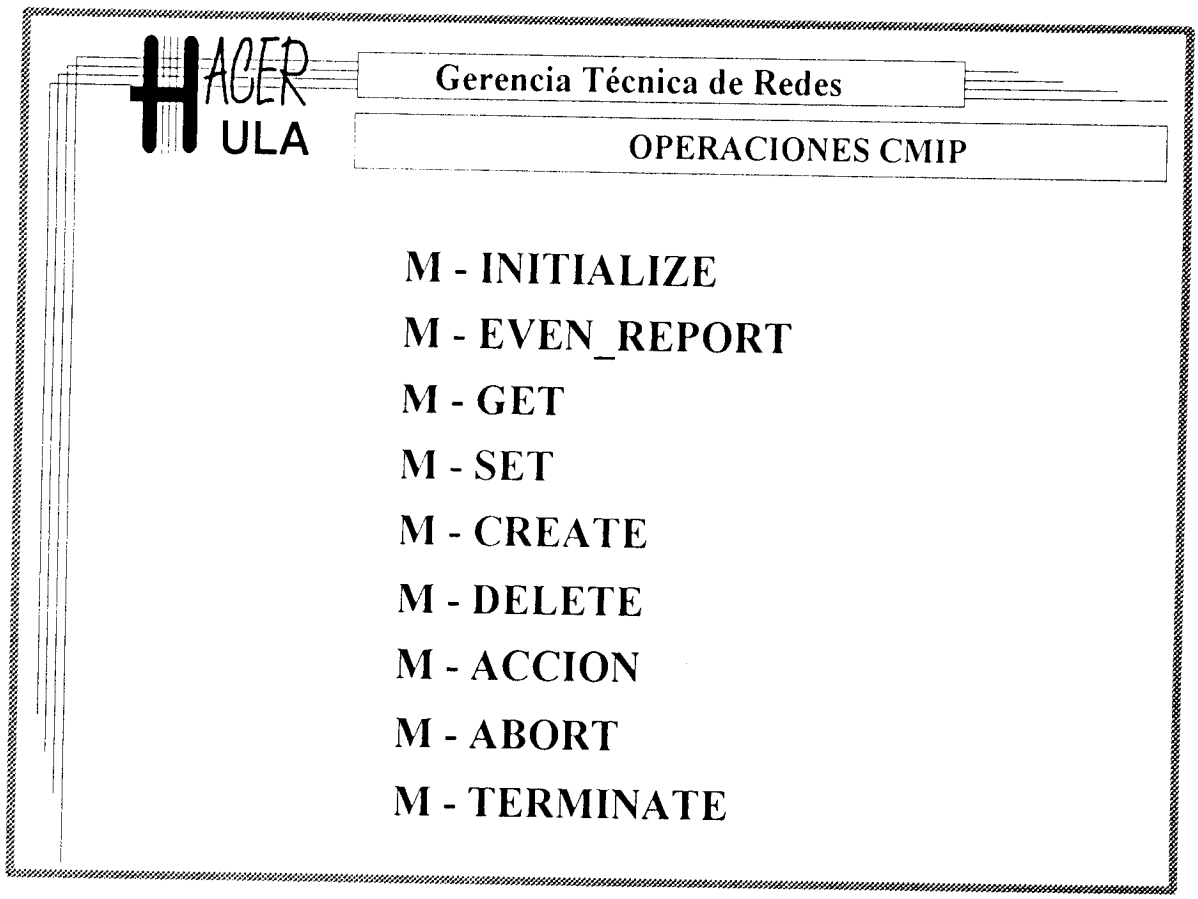
La aplicaciones administrativas se apoyan en la primitivas que ofrece el CMIS, el cual usa CMIP para comunicar la entidades. Las primitivas en cuestión se muestran en la tabla siguiente:

Primitiva	Acción	Requiere confirmar
M-INITIALIZE	Establece una asociación.	N/A
M-EVEN-REPORT	Notifica a la estación adm. la ocurrencia de algún evento, asincrónicamente.	Si/No
M-GET	Obtiene los valores de un conjunto dado de atributos (en uno o varios objetos).	Si
M-SET	Establece los valores de un conjunto dado de atributos (en uno o varios objetos).	Si/No
M-CREATE	Crea una nueva instancia de objeto, indicando los valores de sus atributos.	Si
M-DELETE	Elimina instancias de objetos.	Si/No
M-ACTION	Ejecuta una acción sobre una o más instancias.	Si/No
M-ABORT	Aborta una asociación.	N/A
M-TERMINATE	Cierra una asociación.	N/A

Para referirse a grupos de objetos y/o instancias, CMIP emplea dos operaciones: *scoping* (definición del ámbito), para seleccionar grupos de clases de objetos y *filtering* (filtrado), para seleccionar instancias de clases.

Las operaciones sobre instancias son abordadas de dos formas distintas: Cuando se trata de impedir que una operación se vea interferida por otra, se habla de una operación *atómica*. Si dicha independencia se procura, pero no se garantiza, se habla de operación con el *mejor esfuerzo* (*best effort*).

CMIP admite como SNMP, el uso del agente sustitutos (*proxy agent*). Aún no se ha completado la especificación CMIP en cuanto a los procedimientos de autenticación y seguridad, por lo que CMOT emplea simplemente un campo para una clave sin encriptar. CMIP si incorpora el uso de valores umbral (*Counter threshold, Gauge thresholds*), pero estos no son incluidos en CMOT dada su dependencias de TCP/IP SMI.


HACER
ULA
Gerencia Técnica de Redes
OPERACIONES CMIP
M - INITIALIZE
M - EVEN_REPORT
M - GET
M - SET
M - CREATE
M - DELETE
M - ACCION
M - ABORT
M - TERMINATE

Notas:

Los productos de administración.

Como ya se habrá podido notar, el concepto de administración de redes que se maneja en este contexto excluye elementos como el soporte a aplicaciones, a sistemas de base de datos, los problemas de instalación y la muy significativa atención y entrenamiento a usuarios. Todos esos también son problemas del administrador, quien tendrá que atenderlos al tiempo que enfrenta los otros inconvenientes que se han venido describiendo. La lámina muestra lo que se conoce como la *sombrilla de la administración*[5] con todos los aspectos discutidos.

Para poder asumir esa variedad de tarea es probable que el Administrador solicite o adquiera un producto de administración de redes, varios de los cuales ya han sido mencionados en este manual. Lamentablemente, no es posible garantizar que un sólo producto cubra todas las necesidades. No obstante, esa es la tendencia que se ve favorecida con el uso de estándares como SNMP y CMIP.

Sólo nos resta transmitirles algunos consejos en caso de que deseen adquirir (o construir) una o más estaciones de administración para su red. Una aplicación de administración debería [5].

- Estar basada en estándares.
- Permitir el rastreo del rendimiento de los dispositivos remotamente.
- Permitir que el administrador configure los dispositivos remotamente.
- Permitir el establecimiento de valores umbrales que, de ser sobrepasados, activen alarmas en el sistema.
- Almacenar la *historia* del sistema en un formato transferible a otras aplicaciones. (Esta opción no es más que la **bitácora del sistema** automatizada, ***que todo administrador debe mantener***).
- Permitir la visualización de las condiciones de operación de la red, de manera que el administrador pueda detectar rápidamente condiciones irregulares y tenga una visión global del comportamiento del sistema.
- Ofrecer mecanismos para seguimiento de fallas. Es decir, sistemas de rastreo incorporados.
- Ser capaz de entenderse con productos de otros fabricantes (esta debería ser la primer condición).

NETMAN 23. Evaluando sistemas administrativos.

Si está disponible en su laboratorio un producto de administración, sométalo a una evaluación detallada procurando verificar si cumple con las recomendaciones descritas en esta parte.

HACER ULA

Gerencia Técnica de Redes

PLANILLA DE EVALUACION

Producto a adquirir: Sistema de administración de red.

Descripción	Méritos
● Está basado en estándares ● Permite el rastreo ● Permite configurar remotamente ● Permite el control con alarmas ● Permite registro de eventos (bitácora) en formato exportable. ● Permite visualizar la red ● Incluye mecanismos para detección de fallas. ● Puede entenderse con otros productos	

Notas:

Referencias bibliográficas

[1] Beltrão Moura, José Antão *et al.* Redes Locales de Computadoras. Protocolos de Alto Nivel y Evaluación de Prestaciones. McGraw-Hill/Interamericana de España. 1990.

[2] Tanembaum, Andrew. Redes de Computadores. 2da. Edición. Prentice-Hall Hispanoamericana, S.A. 1991.

[3] Karn, Phil. The KA9Q Internet (TCP/IP) Package: A Progress Report. Proceeding of the 6th ARRL Amateur Radio Computer Networking Conference. ARRL. 1987

[4] López, José; Díaz, Gilberto; Marcano, Nestor. Análisis de prestaciones en Redes de Area Local. Informe de pasantía. Centro de Innovación Tecnológica. HACER-ULA. Venezuela.1992.

[5] Schnaidt, Patricia. Enterprise-Wide Networking. SAMS Publishing. 1992.

[6] Bye, Peter, Implementing integrated systems management. Networking Management Europe. May/June 1993. PennWell Publishing Company, 1421. South Sheridan. Tulsa, OK 74122, USA.

[7] Stallings, William, Handbook of Computer Communications Standards. Vol 3. Howard W. Sams & company. 1989. Segunda Edición.

[8] Case J, Fedor, Schoffstall & Davin. A Simple Network Management Protocol (SNMP). Request For Comments 1157. Network Working Group. Mayo 1990.

[9] Case J, McCloghrie K, Rose T, Waldbusser S. SMP-Straight from the source. Data Communications. November. 1992.

Gerencia Técnica de Redes

Anexo 1. Especificación SNMP

```
RFC1157-SNMP DEFINITIONS ::= BEGIN

 IMPORTS
    ObjectName, ObjectSyntax, NetworkAddress, IpAddress, TimeTicks
      FROM RFC1155-SMI;

    -- top-level message
    Message ::=
          SEQUENCE {
             version        -- version-1 for this RFC
                INTEGER {
                   version-1(0)
                },

             community      -- community name
                OCTET STRING,

             data           -- e.g., PDUs if trivial
                ANY         -- authentication is being used
          }

    -- protocol data units

    PDUs ::=
          CHOICE {
                  get-request
                     GetRequest-PDU,

                  get-next-request
                     GetNextRequest-PDU,

                  get-response
                     GetResponse-PDU,

                  set-request
                     SetRequest-PDU,

                  trap
                     Trap-PDU
                }
```

```
-- PDUs

GetRequest-PDU ::=
   [0]
      IMPLICIT PDU
GetNextRequest-PDU ::=
   [1]
      IMPLICIT PDU
GetResponse-PDU ::=
   [2]
      IMPLICIT PDU

SetRequest-PDU ::=
   [3]
      IMPLICIT PDU

PDU ::=
      SEQUENCE {
        request-id
            INTEGER,
         error-status      -- sometimes ignored
            INTEGER {
               noError(0),
               tooBig(1),
               noSuchName(2),
               badValue(3),
               readOnly(4),
               genErr(5)
            },
         error-index       -- sometimes ignored
           INTEGER,
         variable-bindings -- values are sometimes ignored
            VarBindList
      }

Trap-PDU ::=
   [4]
     IMPLICIT SEQUENCE {
        enterprise        -- type of object generating
                          -- trap, see sysObjectID in [5]
           OBJECT IDENTIFIER,
```

```
        agent-addr      -- address of object generating
          NetworkAddress, -- trap
        generic-trap    -- generic trap type
          INTEGER {
            coldStart(0),
            warmStart(1),
            linkDown(2),
            linkUp(3),
            authenticationFailure(4),
            egpNeighborLoss(5),
            enterpriseSpecific(6)
          },
        specific-trap  -- specific code, present even
          INTEGER,   -- if generic-trap is not
                     -- enterpriseSpecific
        time-stamp     -- time elapsed between the last
          TimeTicks, -- (re)initialization of the
                       network
                     -- entity and the generation of the
                       trap
         variable-bindings -- "interesting" information
          VarBindList
      }

-- variable bindings

VarBind ::=
      SEQUENCE {
        name
          ObjectName,
        value
          ObjectSyntax
      }

VarBindList ::=
      SEQUENCE OF
        VarBind

END
```

Direcciones de los autores de SNMP.

Jeffrey D. Case
SNMP Research
P.O. Box 8593
Knoxville, TN 37996-4800
Phone: (615) 573-1434
Email: case@CS.UTK.EDU

Mark Fedor
Performance Systems International
Rensselaer Technology Park
125 Jordan Road
Troy, NY 12180
Phone: (518) 283-8860
Email: fedor@patton.NYSER.NET

Martin Lee Schoffstall
Performance Systems International
Rensselaer Technology Park
165 Jordan Road
Troy, NY 12180
Phone: (518) 283-8860
Email: schoff@NISC.NYSER.NET

James R. Davin
MIT Laboratory for Computer Science, NE43-507
545 Technology Square
Cambridge, MA 02139
Phone: (617) 253-6020
EMail: jrd@ptt.lcs.mit.edu