Los siguientes 10 años de Internet2 en México
CUDI 2009

Administración y Operación de Redes

Por:

Ing. Hans L. Reyes Chávez

Centro de Operación de CUDI,
Dirección de Telecomunicaciones,
DGSCA-UNAM

www.noc.cudi.edu.mx

?

Gestión de Redes

Enrutamiento

RMON

NOC/NIC

TCP/IP

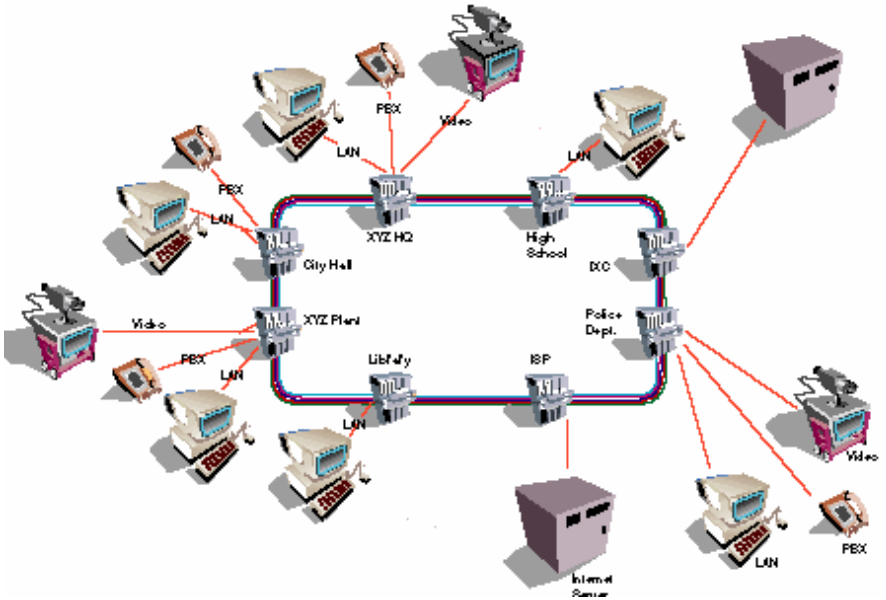
SNMP

Administración y operación de Redes

Depende mucho el tamaño y la complejidad de la red de datos:

- Tan simple como tener a una sola persona verificando los enlaces de la red de área local en una pc
- Tan complicado como puede haber un staff de 50 o más personas con radiolocalizadores y analizadores de protocolos atendiendo las 24 horas del día.

Red de datos

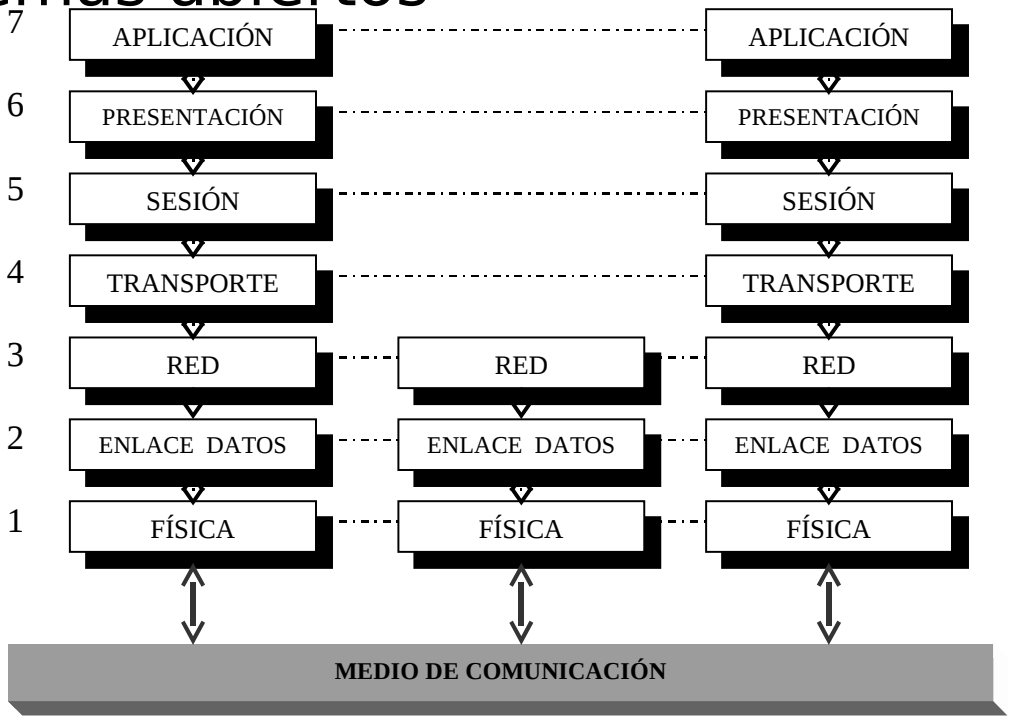


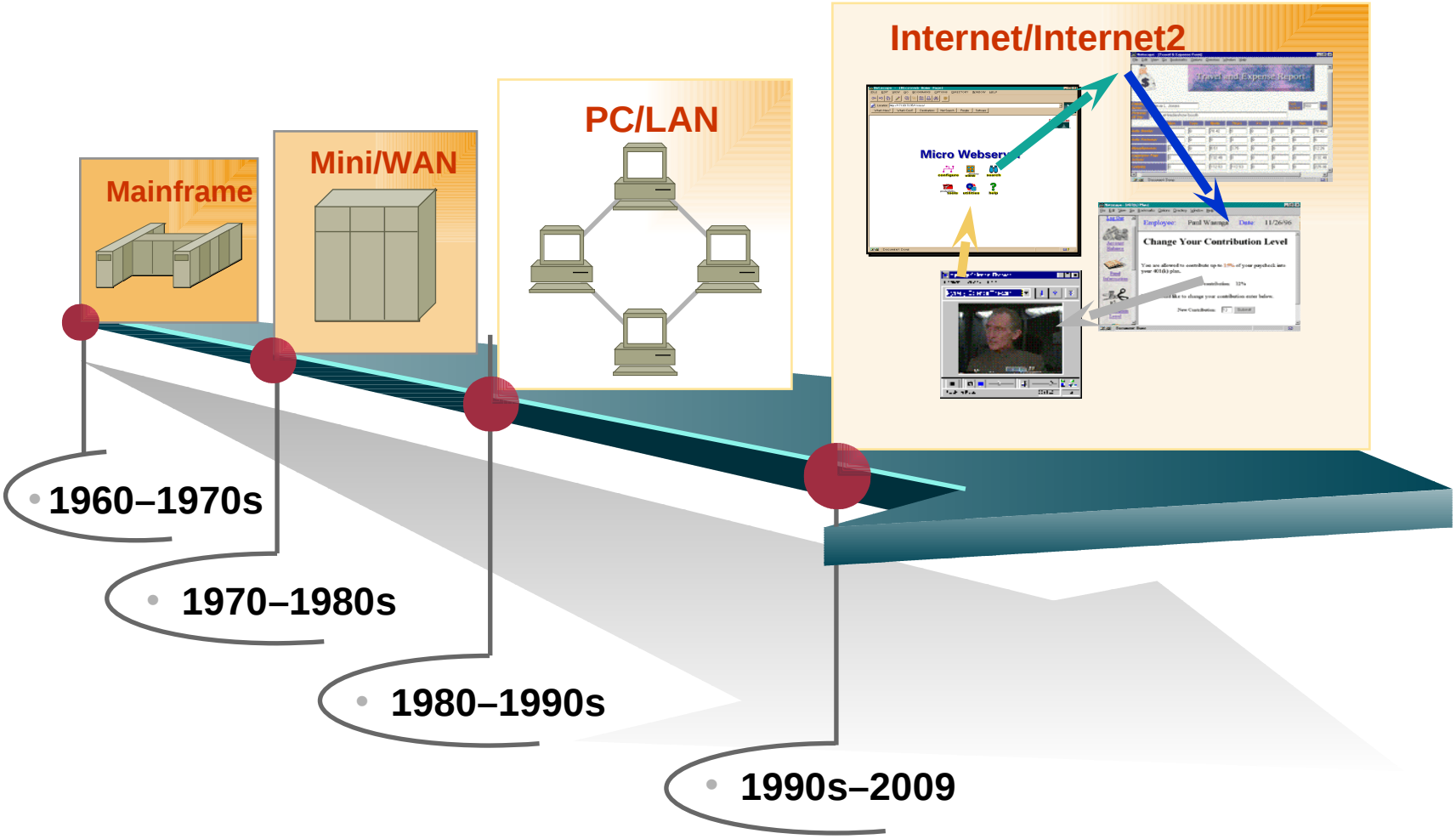
- Conjunto de equipos interconectados entre sí a través de un medio físico (sea cable, fibra óptica, o el aire inclusive) con la finalidad de compartir recursos e información.

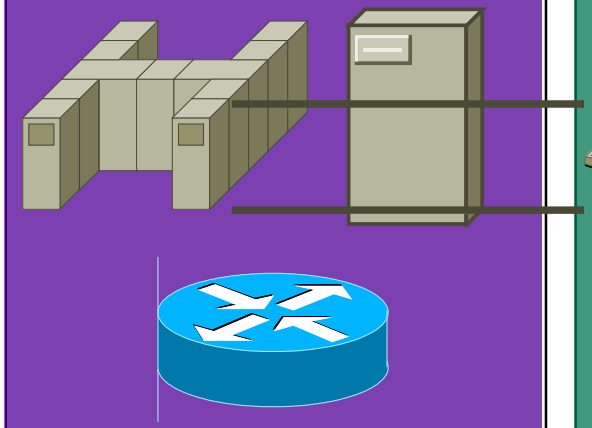
Modelo de referencia OSI

Definido por ISO (International Standards Organization)
Modelo de referencia de 7 capas para asegurar la interconexión de sistemas abiertos

- Aplicación
- Presentación
- Sesión
- Transporte
- Red
- Enlace de Datos
- Física

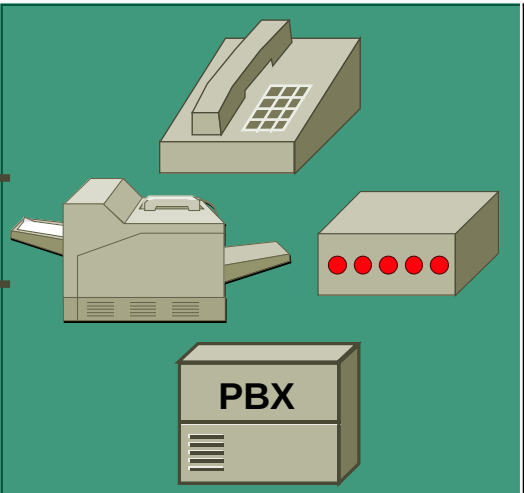



Internet/Internet2
PC/LAN
Mini/WAN
Mainframe
Micro Webserver
Change Your Contribution Level
1960–1970s
1970–1980s
1980–1990s
1990s–2009



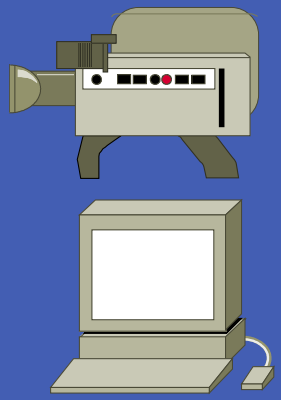
Datos

- Interactivo
- FTP
- Multiprotocolo
- http://www



Voz

- PBX
- Fax
- Modem
- Calidad



Video

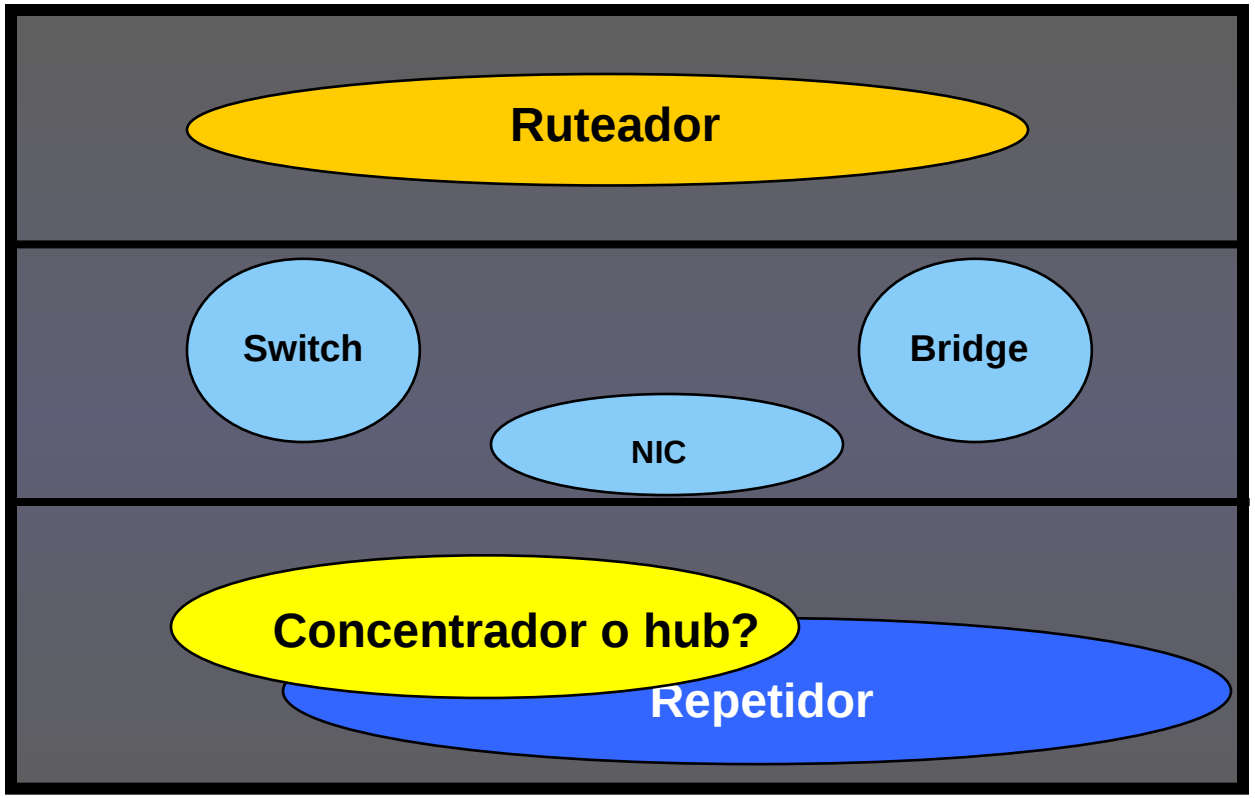
- Educación a Distancia
- Teleconferencia
- Multicast
- Calidad

Localización en el modelo OSI

Red

Enlace de datos

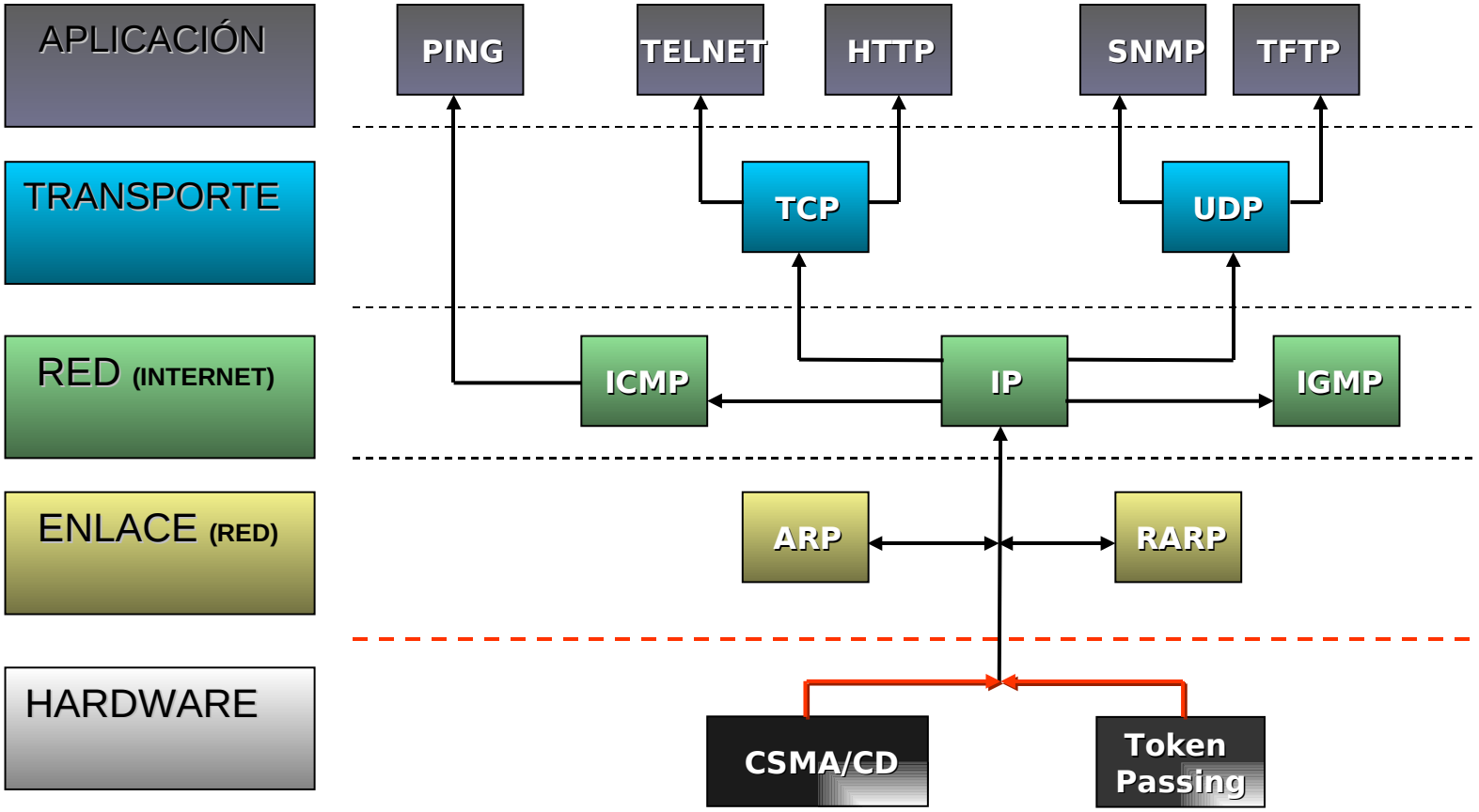
Física



TCP/IP

- TCP/IP es una familia de protocolos de comunicaciones de datos.
- Independencia de la tecnología de red (Ethernet, ATM, FR.POS).
- Arquitectura de sistemas abiertos.
- Direccionamiento universal.
- Protocolos de aplicación estándar (ftp, e-mail, www y SNMP).

TCP/IP


APLICACIÓN
TRANSPORTE
RED (INTERNET)
ENLACE (RED)
HARDWARE
PING
TELNET
HTTP
SNMP
TFTP
TCP
UDP
ICMP
IP
IGMP
ARP
RARP
CSMA/CD
Token Passing

Direccionamiento

IPv4

El protocolo IP v4 define un identificador único llamado dirección IP con una longitud de 32 bits:

10000100 11111000 11001100 00110001

132.248.204.49

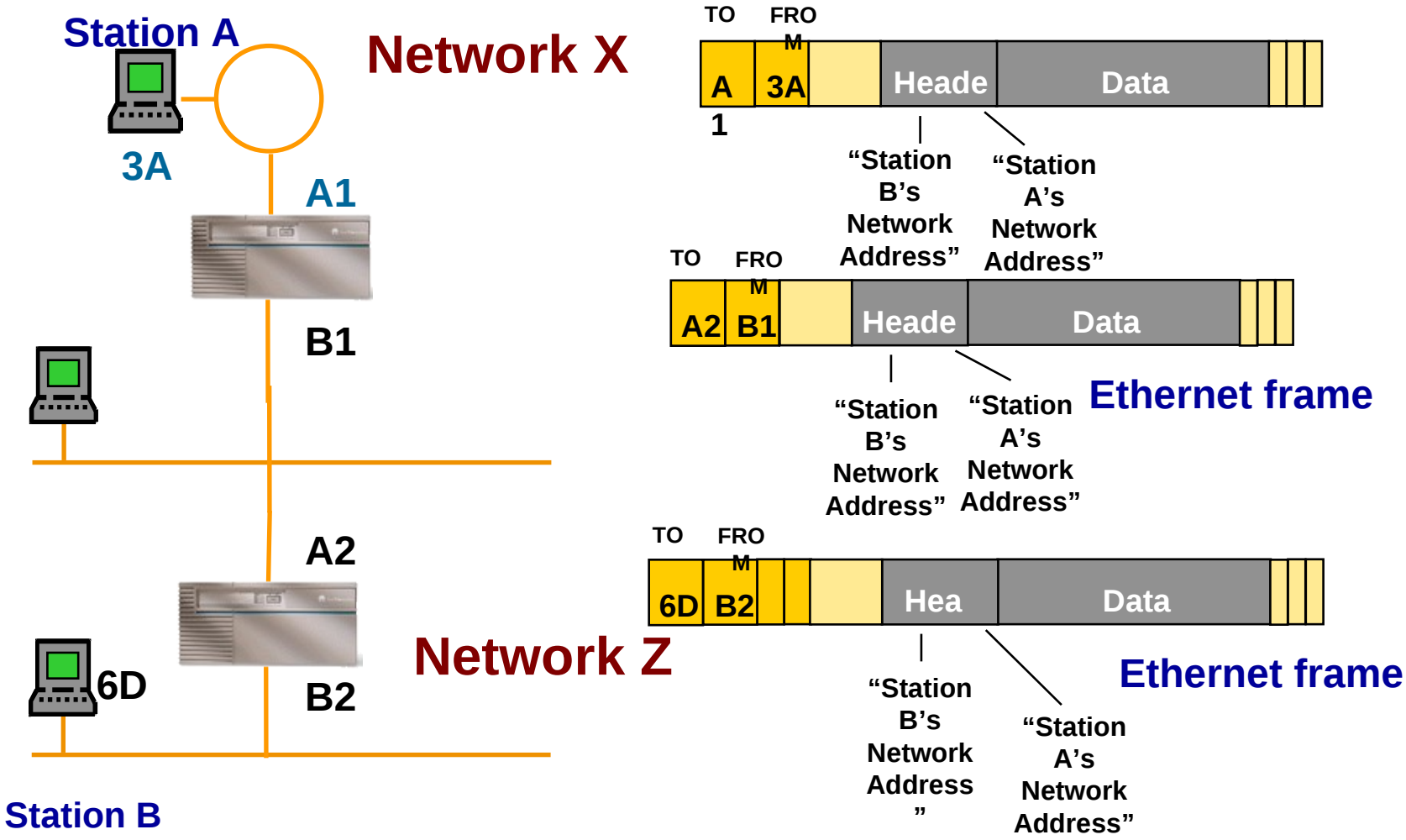
Posee información del host y de la red a la que pertenece.

Por medio del uso de mascara de red.

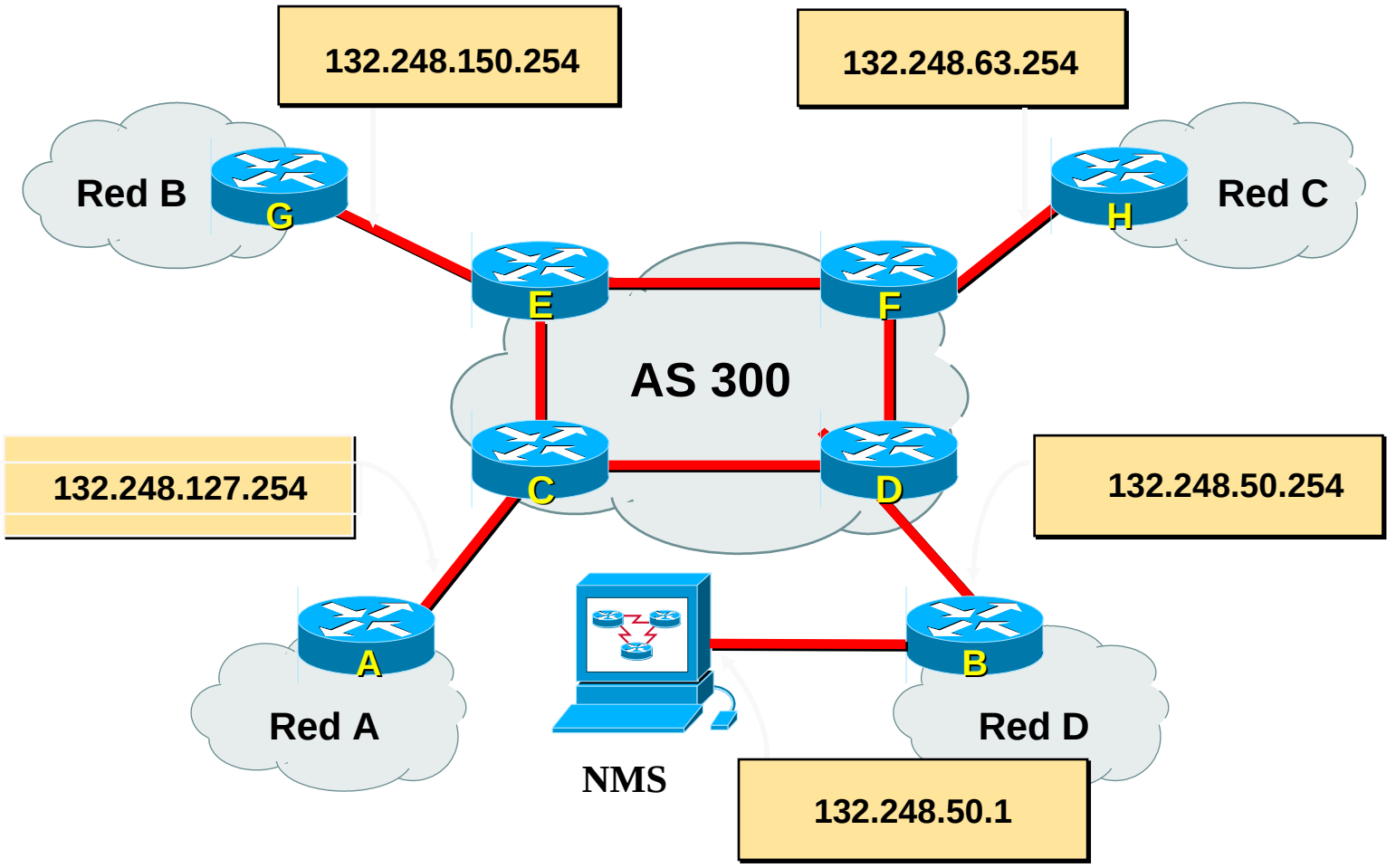
Mascara de red

- Información necesaria para **interpretar** a que **red** (o subred o superred) pertenece un host.
- Debe poseer 32 bits con 1´s contiguos a partir de la izquierda para identificar al netID y los bits restantes deben de ser 0´s para identificar al hostID.

11111111 . 11111111 . 11111111 . 00000000
255. 255. 255. 0

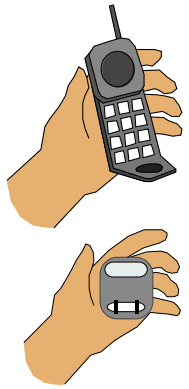

Station A
Network X
3A
A1
B1
A2
6D
Network Z
B2
Station B
TO
FRO M
A
1
3A
Heade
Data
"Station B's Network Address"
"Station A's Network Address"
TO
FRO M
A2
B1
Heade
Data
"Station B's Network Address"
"Station A's Network Address"
Ethernet frame
TO
FRO M
6D
B2
Hea
Data
"Station B's Network Address"
"Station A's Network Address"
Ethernet frame

Administración TCP/IP



Papel del Ingeniero

Debido a la importancia del funcionamiento de una red:



- Uno o más ingenieros de red tiene la responsabilidad de instalar, mantener y solucionar los problemas (troubleshooting).
- Los ingenieros necesitan saber gran cantidad de información a cerca de la red. Esta información rápidamente puede volverse inmanejable.
- Para ayudar al ingeniero: Administración de la red. El objetivo global, ayudar a los ingenieros de red tratar con la complejidad de una red de datos y asegurar que la información esté disponible para el usuario.

Implementación de una Red

- Construcción: ¿Qué se desea conectar y cómo se va a conectar?
- Mantenimiento: La red siempre debe funcionar.
- Expansión: Las necesidades de comunicación van cambiando, AUMENTAN.
- Optimización: Lograr que todos los dispositivos trabajen en completa armonía.

... y como NADA ES INFALIBLE...

- Resolución de los Problemas: Administración y Monitoreo de Redes.

Conceptos básicos de diseño

- Existen 5 puntos básicos de diseño:

Conceptos básicos de diseño

Analizar los requerimientos

- Funcionalidad. *La red debe trabajar*
- Escalabilidad. *La red y su diseño inicial debe crecer junto con la organización*
- Adaptabilidad. *Aceptar nueva tecnología*
- Administrabilidad. *Administración proactiva de la red*
- Costo/Beneficio. *Recursos y presupuestos limitados.*

Conceptos básicos de diseño

Analizar los requerimientos.

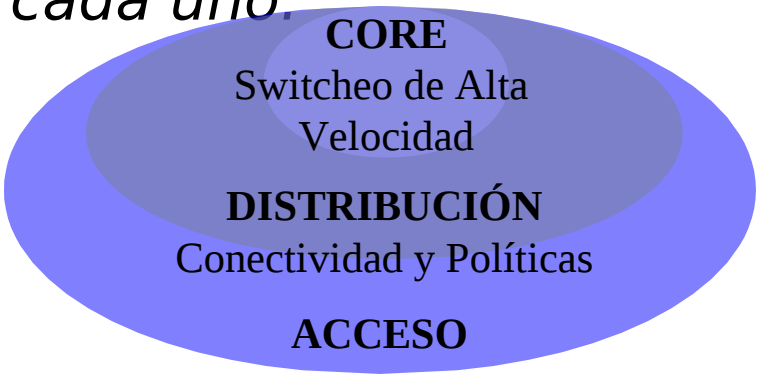
Otros aspectos

- Confiabilidad
- Tiempo de recuperación
- Costo de Recursos en la WAN
- Cantidad de tráfico
- Capacidad de multiprotocolo en la WAN
- Compatibilidad con sistemas legados
- Simplicidad y fácil configuración y admionistración

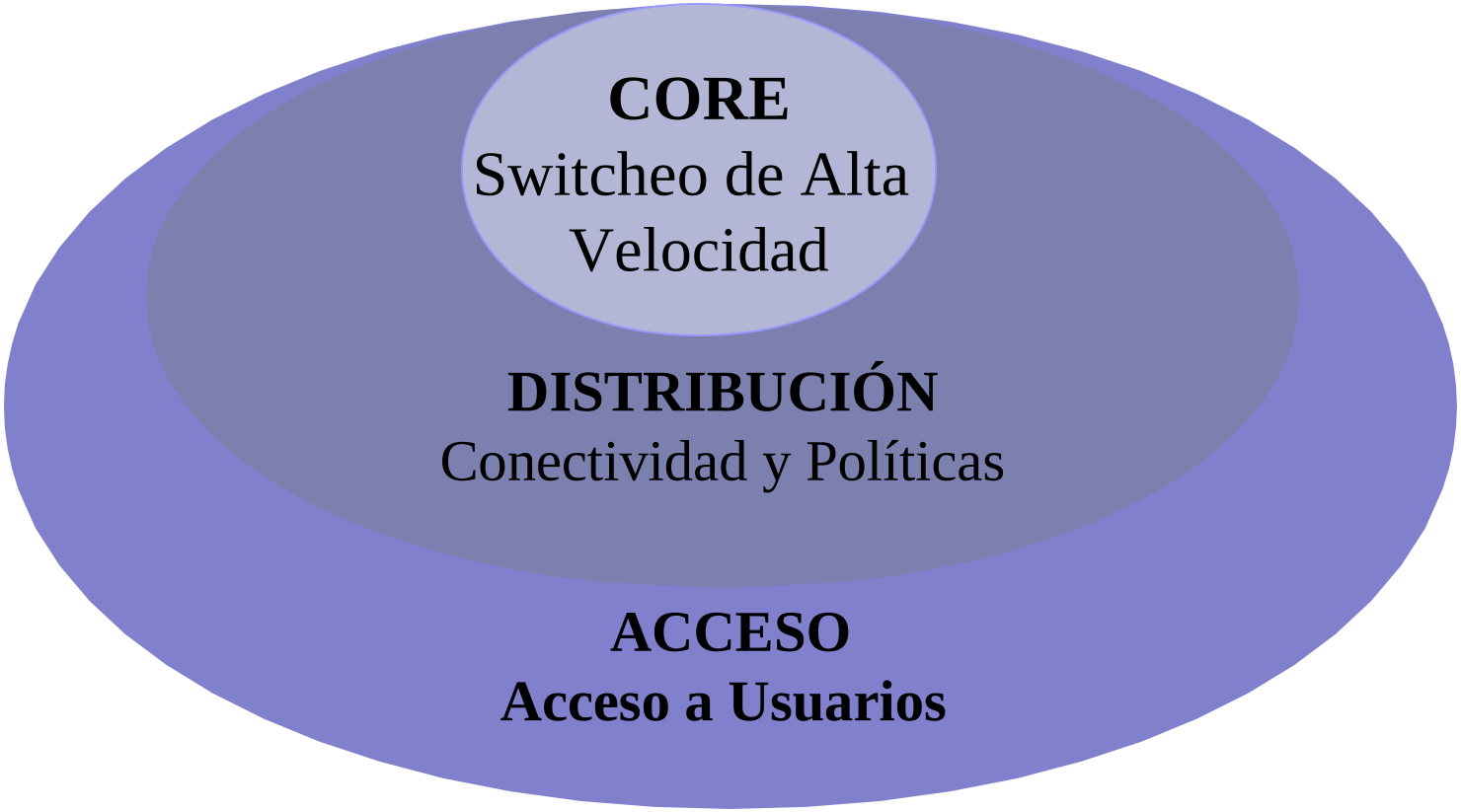
Conceptos básicos de diseño

Desarrollo de la topología de red

- Topología de malla. *Plana y todos los equipos desarrollan la misma función*
- Topología Jerárquica. *Organizada en niveles con funciones específicas para cada uno.*
  - Core.
  - Distribución.
  - Acceso.

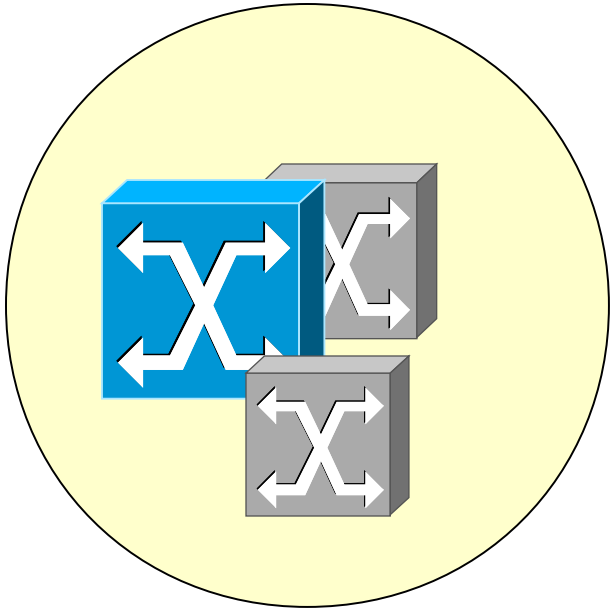


Modelo Jerárquico



Core

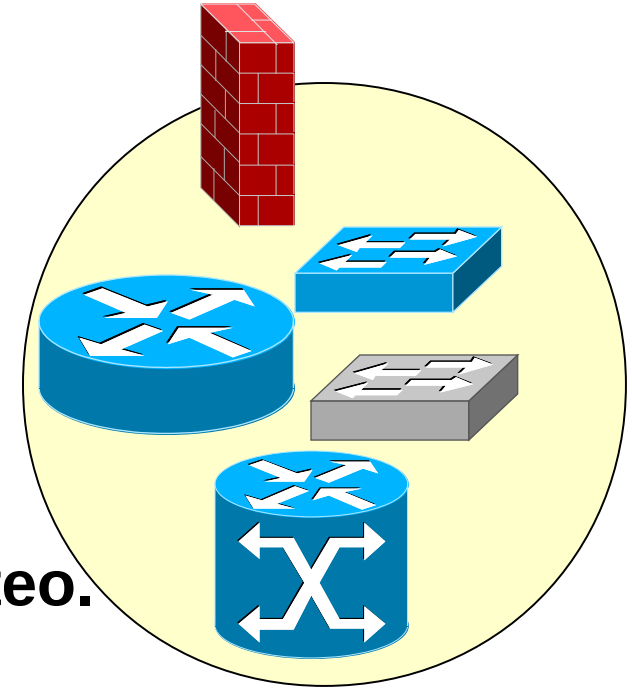
- Alta velocidad
- Capa 2/3
- No procesamiento de paquetes
- Robusto
- Vida Útil Extensa
- Tecnologías: GE, ATM, POS,WDM.



Distribución

Diseño Básico de Redes

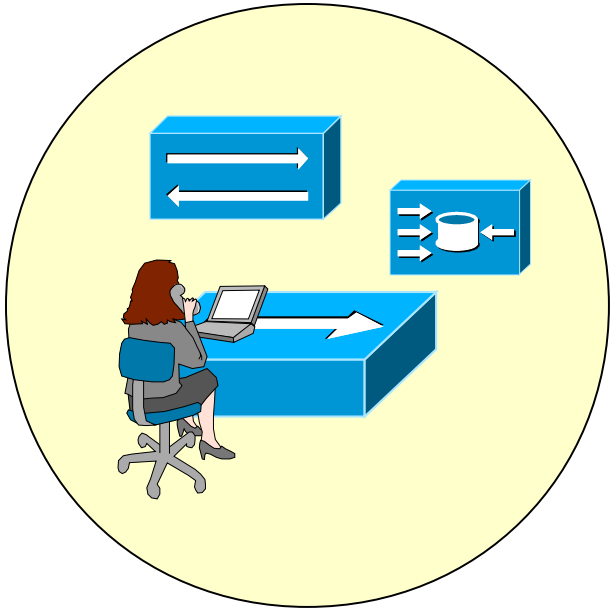
- Frontera entre core y acceso
- Capa 2 y 3
- Manipulación de paquetes
- Funciones
  - Agrupar / Aislar
  - Seguridad
- MPLS, QoS, VLAN, Switches, ruteo.



Acceso

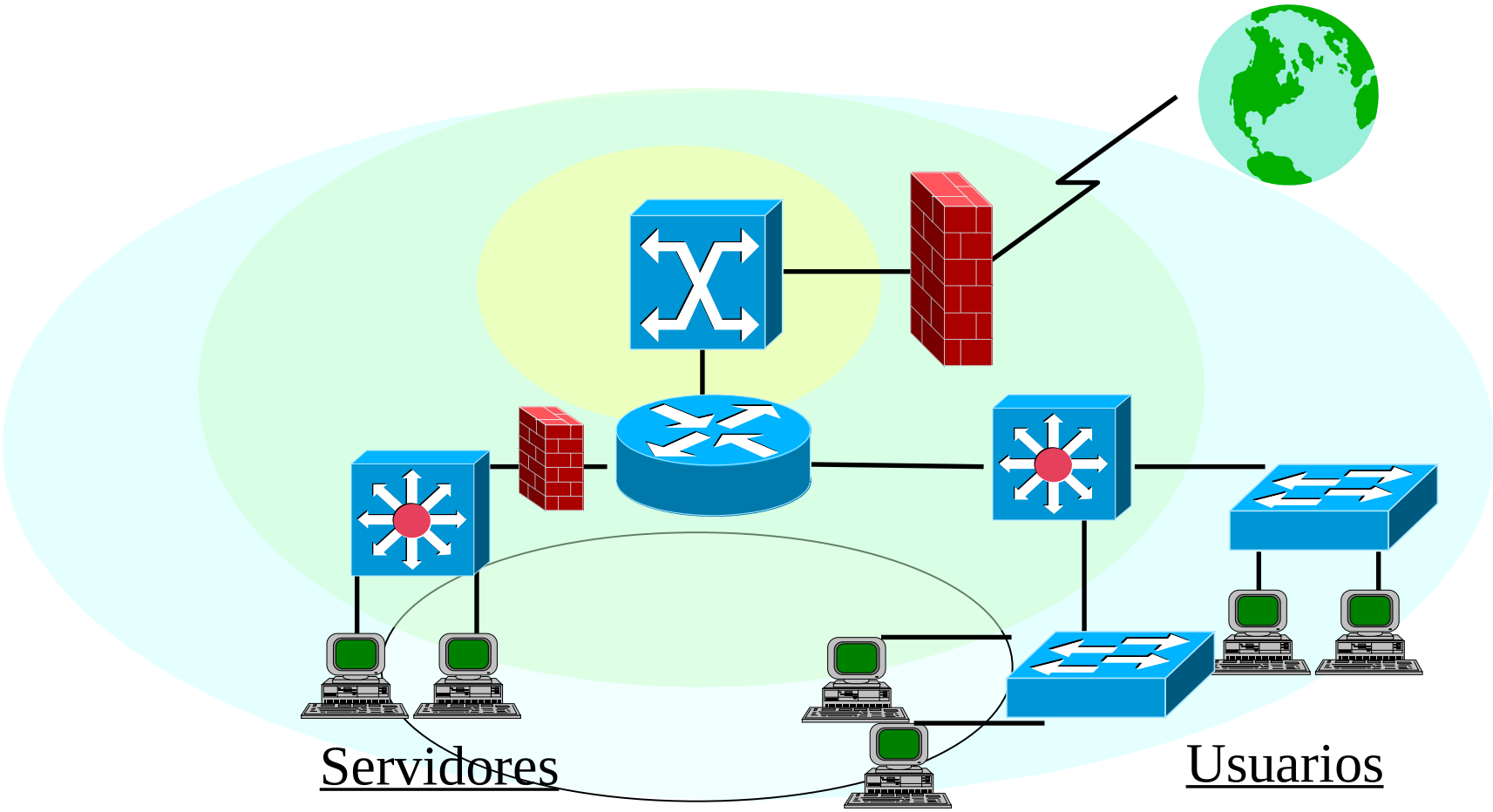
Diseño Básico de Redes

- Interfaz con usuario final
- Capa 2
- Manipulación de paquetes de usuario
- Funciones
  - Servicio de usuario
- E, FE, WIFI,PCs, Servers.



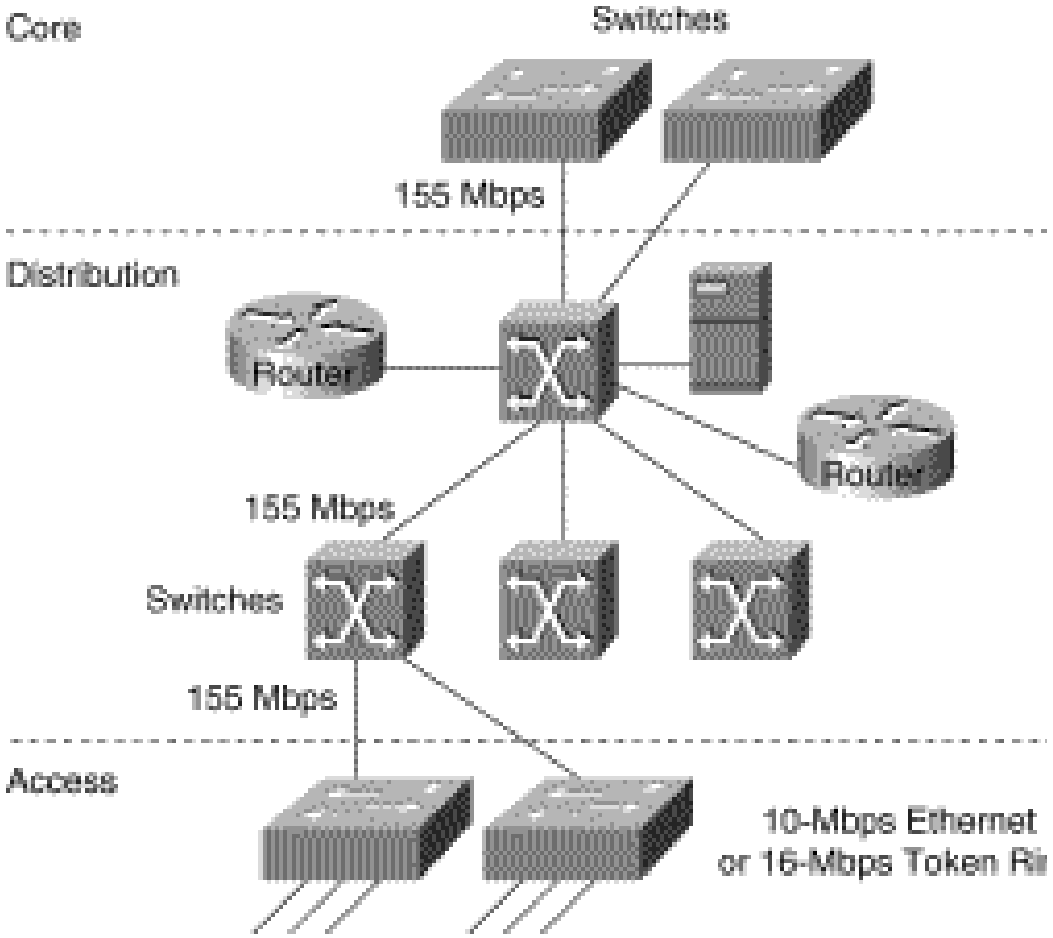
Modelo Jerárquico

Diseño Básico de Redes



Modelo Jerárquico

Diseño Básico de Redes



Conceptos básicos de diseño

Direccionamiento

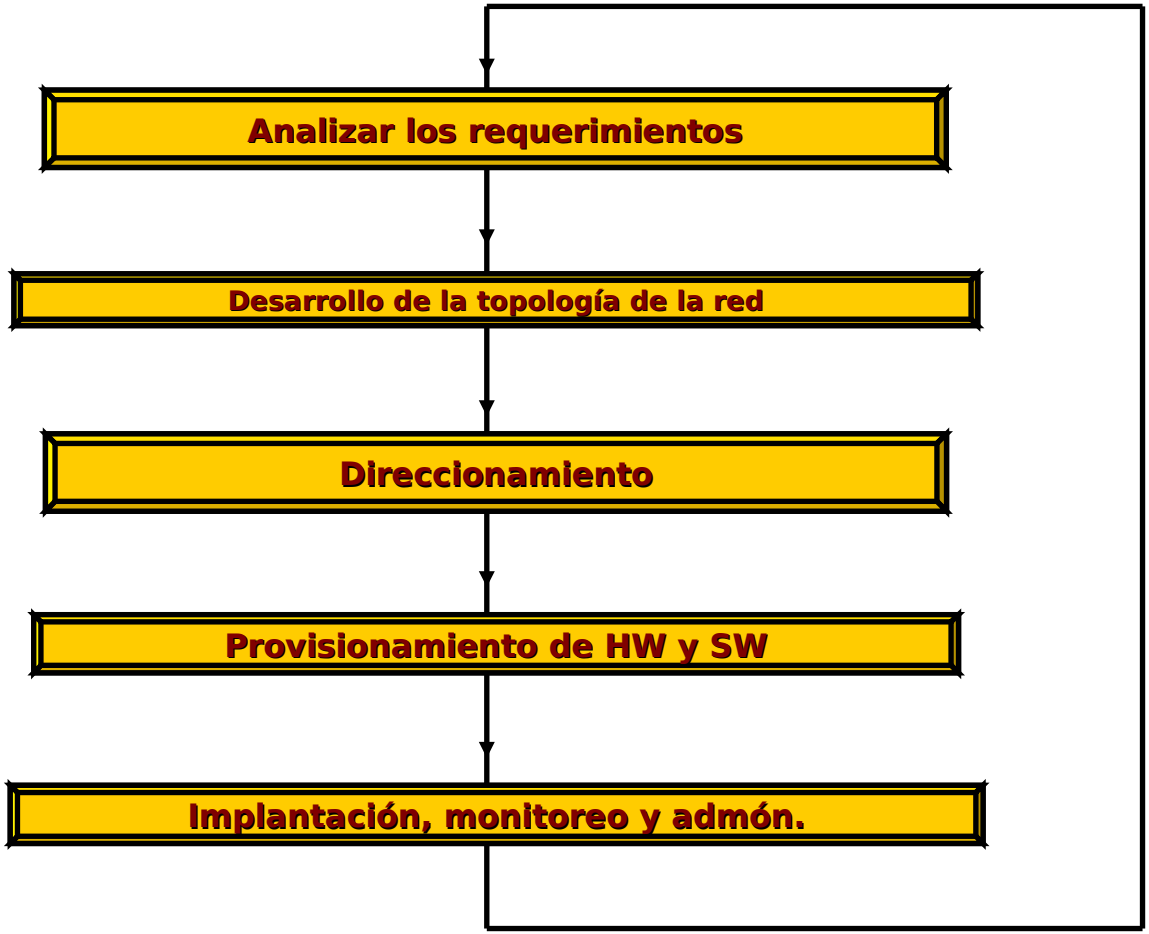
- Asignación esquema de direccionamiento de toda la red.
- La signaión de bloques de direcciones a porciones de la red simplifica la administración, el direccionamiento y el enrutamiento.
- Domain Name Service (DNS).
- Posible direccionamiento privado o público (tener cuidado con crecimiento).
  - HDCP
  - NAT
  - VLSM/CIDR

- Determinar el HW necesario para la red con:
  - Documentación del fabricante
  - Ejecutivos de cuenta
- Determinar el cableado, marcas, modelos, ISPs, integradores, garantias, soporte técnico, etc.

- Determinar el Sf necesario para la red con:
  - Documentación del fabricante
  - Ejecutivos de cuenta
- Determinar versiones de software de equipos, software de gestion de redes, licencias, garantias, soporte técnico, etc.

Conceptos básicos de diseño

Implementación, administración y operación



Administración y operación de Redes

- La administración cubre todas las precauciones y actividades para asegurar el uso efectivo y eficiente de la red.
- Es definido como la suma de todos los procedimientos y productos para el diseño, planeación, configuración, control, monitoreo y administración de la red, así como la solución de problemas.

Beneficios

- Soporte a los objetivos del negocio.
- Brinda el soporte necesario a las redes de misión critica.

Mantener operando la red las 24 horas del día, los 7 días de la semana; es un requisito. Las redes robustas no pueden ser administradas únicamente con el esfuerzo humano, se requiere de mecanismos de administración, control y monitoreo como apoyo.

Beneficios

- Reduce los tiempos de caída de la red.

  Cada minuto que la red esté "caída" equivale a perdidas de dinero que deben ser sufragadas. Aquí es donde el monitoreo cumple su principal función: administración proactiva.

- Se requiere de menos personal para mantener operativa la red.

  Cuando se tiene la red administrada adecuadamente los requerimientos de personal calificado se reducen.

Beneficios

- Se reducen los costos de administración y operación.

  Las labores administrativas se automatizan, permitiendo al personal más tiempo para otras actividades, como diseño y análisis.

- Mejor documentación de la red.

  La automatización del proceso de documentación de la red se automatiza, lo que hace más verídicos y actuales los inventarios, configuraciones, etc.

Beneficios

- Se hace un mejor uso de la infraestructura de red.

  Una buena administración permite un mejor conocimiento de la red que se refleja en una mejor asignación del equipo activo.

- Permite un mejor análisis de los patrones de tráfico así como en la seguridad.

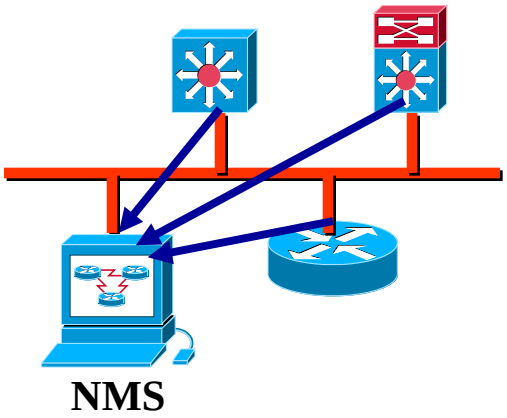
  Esto gracias a las herramientas de monitoreo remoto (SNMP con RMON/ RMON2).

Esquema de Administración

- La forma específica del esquema de administracion va a estar influenciado por:
- Los objetivos de la red
- Las características de la comunicación (tráfico en volumen y tiempos)
- La topología física
- La topología lógica
- La distribución de los servicios
- La organización estructural y operacional de la organización.

Esquema de Administración

Centralizada



- Una plataforma instalada en una sola entidad
  - Una sola entidad recibe todas las alarmas y eventos
  - Única Base de Datos centralizada.
  - En el residen todas las aplicaciones
- Una sola entidad para accesar todas las aplicaciones de administración

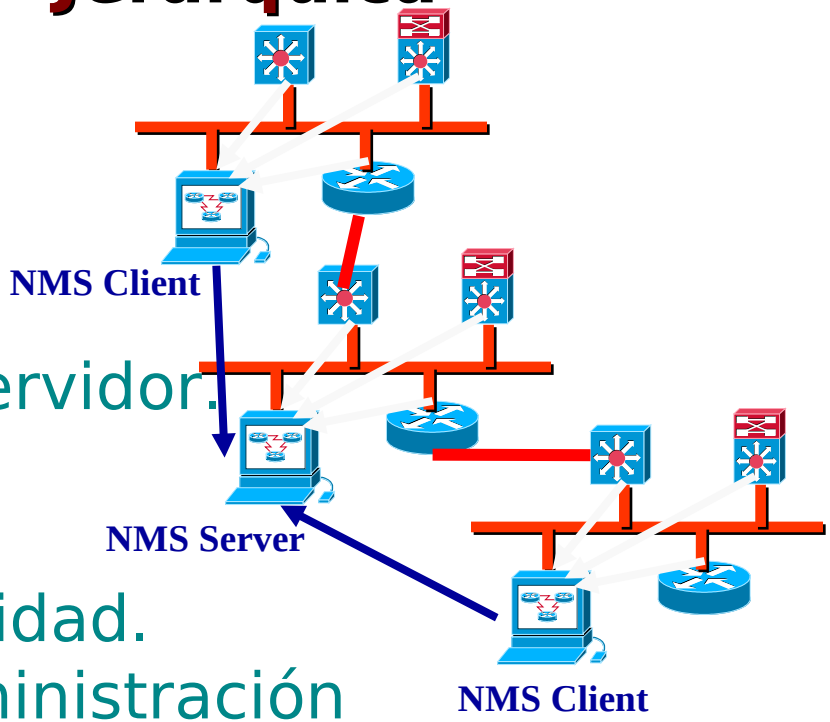
Características:

- Mayor seguridad y control
- Disponible en la mayoría de los proveedores
- Para redes pequeñas

Esquema de Administración

Jerárquica

- Utiliza múltiples sistemas:
  - Servidor.
  - Clientes.
- DB con tecnología Cliente / Servidor.

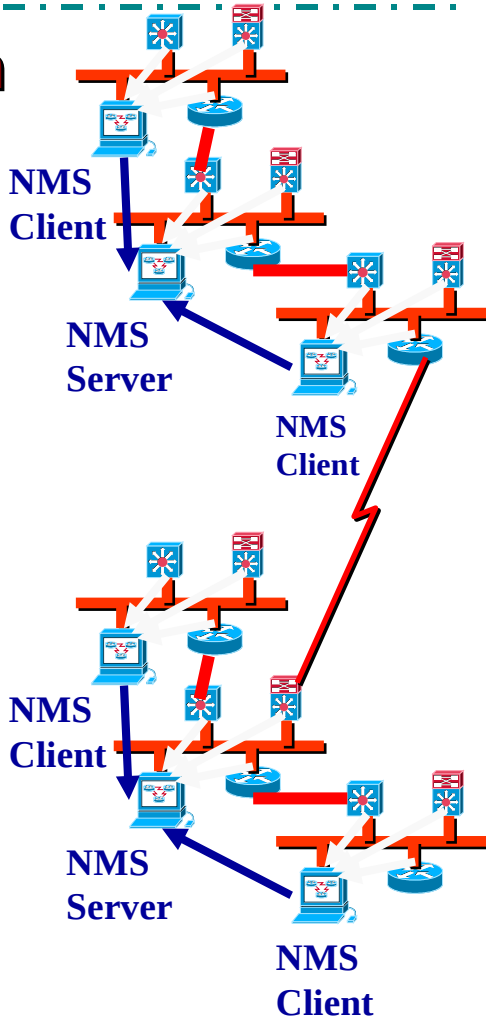


Características:

- No depende de una sola entidad.
- Distribuye las tareas de administración de red.
- Distribuye el monitoreo de la red.
- Almacenamiento centralizado de la información.

Esquema de Administración

Distribuida



- Plataforma instalada en múltiples entidades (WSs).
- Múltiples Bases de Datos instaladas en diferentes entidades.

Características:

- Una sola entidad para toda la información de la red, alarmas y eventos.
- Una sola entidad para accesar todas las aplicaciones de administración.
- No depende de una sola entidad.
- Distribuye las tareas de administración de red.
- Distribuye el monitoreo de la red.

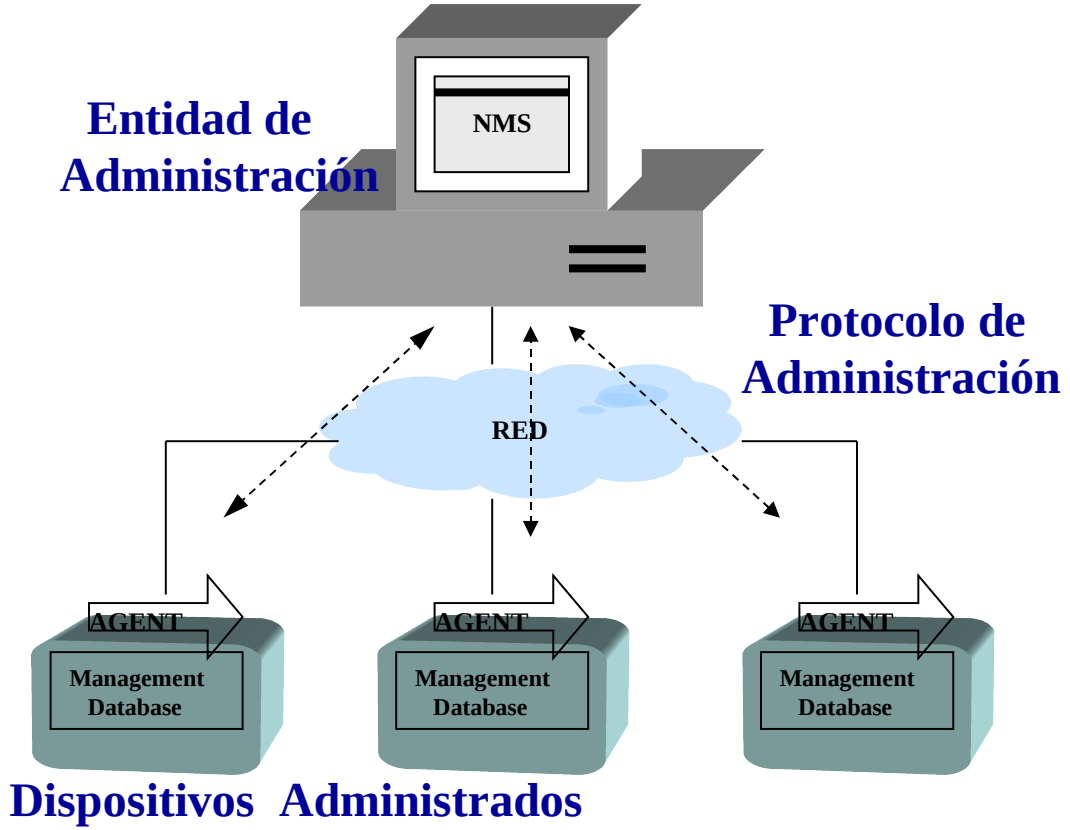
Sistemas de administración de la Red

Cuando se justifican los gastos en la inversión de un sistema de admón.. de red:

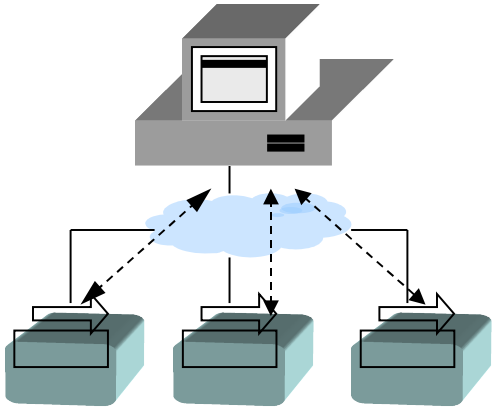
- Se mejora el desempeño, no solo de la red, sino que se refleja en todos los niveles dentro de la compañía.
- Existen diversos tipos de software para tales tareas. Su funcionamiento y arquitectura se describe a continuación:

Arquitectura de administración de Red

Se compone de tres elementos principales que trabajan en arquitectura Cliente/Servidor:



Arquitectura de administración de Red



Network Management System - NMS (Sistema de Administración e Red).

Conjunto de programas cliente encargados de polear (poll) a los agentes con el objetivo de obtener información de los dispositivos de la red.

Agent (agente)

Programa servidor encargado de obtener la información de la base de datos de los dispositivos y entregarla al NMS.

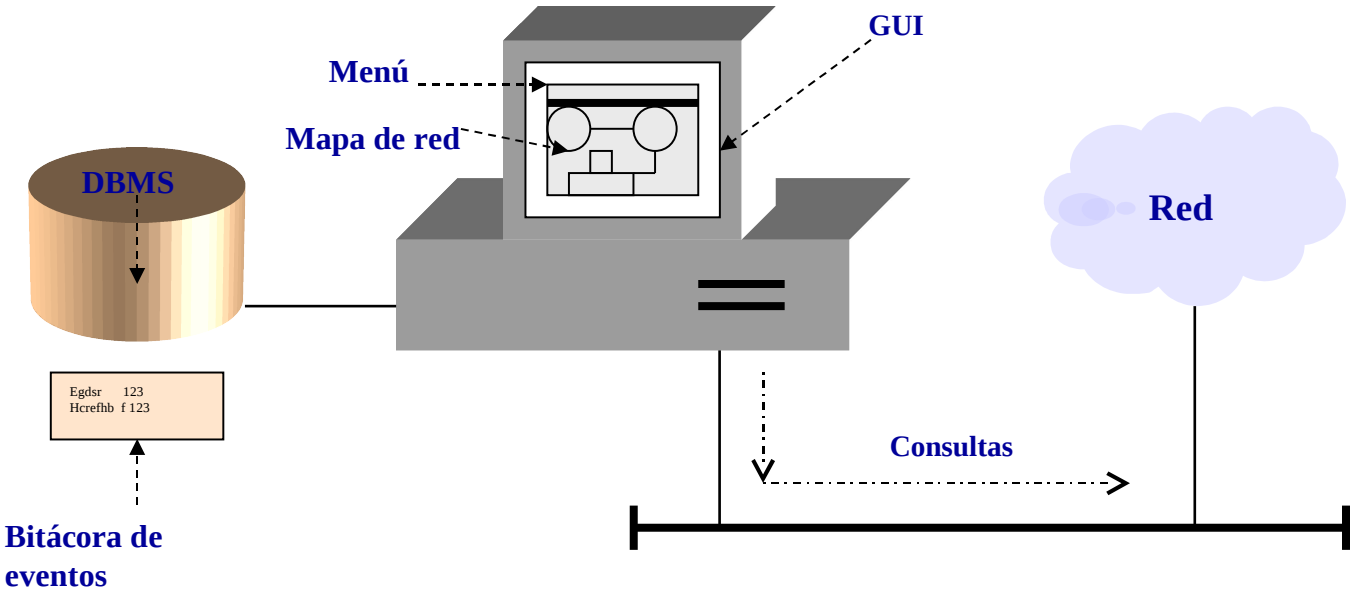
Network Management Protocol (Protocolo de Administración de la Red).

Protocolo de comunicación encargado de comunicar al NMS con el Agent (Cliente/Servidor respectivamente).

Sistemas de administración de la Red

Un Sistema de Administración de Red (NMS) está compuesto por dos partes:

- Una Plataforma de administración de Red
- Una Aplicación de administración de Red



Sistemas de administración de la Red

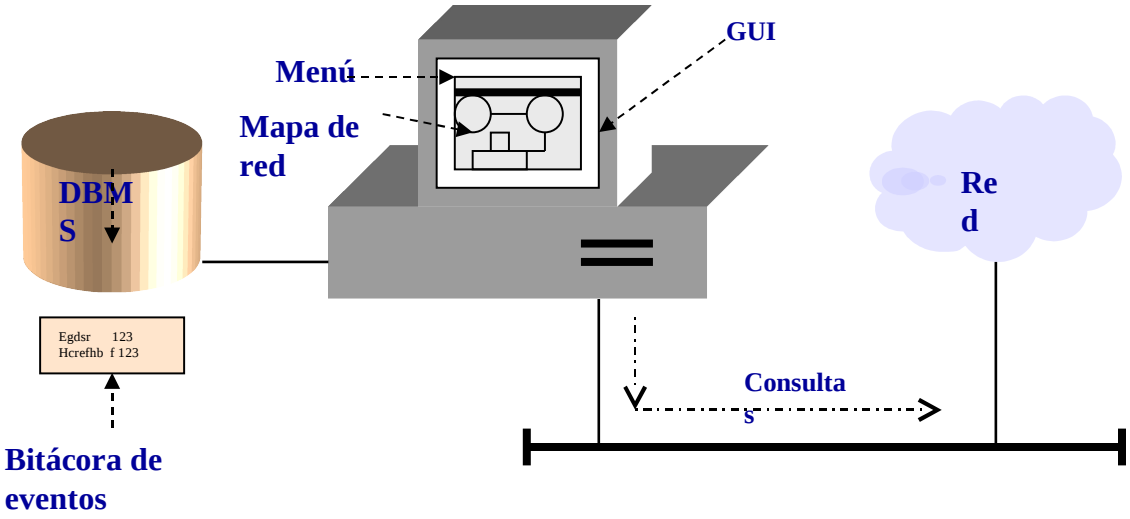
Plataforma de administración

- Colección de herramientas que hacen uso de SNMP, RMON, etc., para monitorearla y controlarla.
- Software que proporciona funcionalidades genéricas de administración para diferentes dispositivos de red.
- Debe contar con:
  - Interfaz gráfica.
  - Mapa de red.
  - Manejador de base de datos.
  - Método estándar de consulta de dispositivos.
  - Sistema de menús flexible.
  - Bitácora de eventos.

Sistemas de administración de la Red

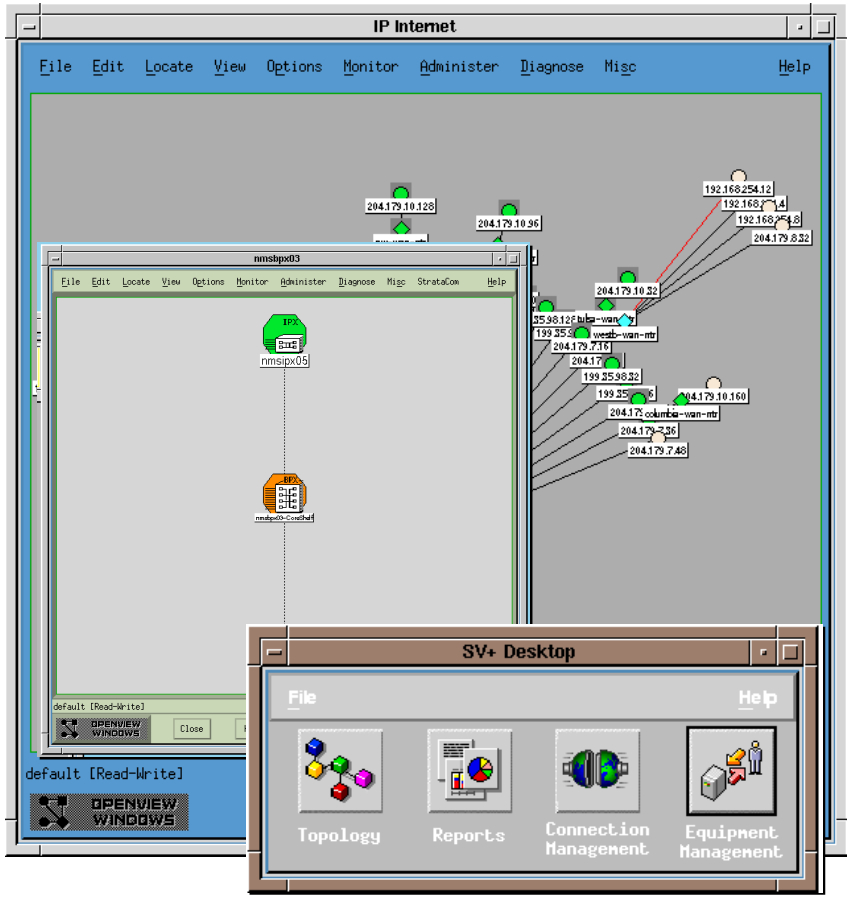
Plataforma de administración

- Las plataformas propietarias comunes son:
  - Cisco Works
  - HP Open View (HP)
  - Tovoli (IBM)
  - Spectrum (CA)



Sistemas de administración de la Red

Plataforma de administración

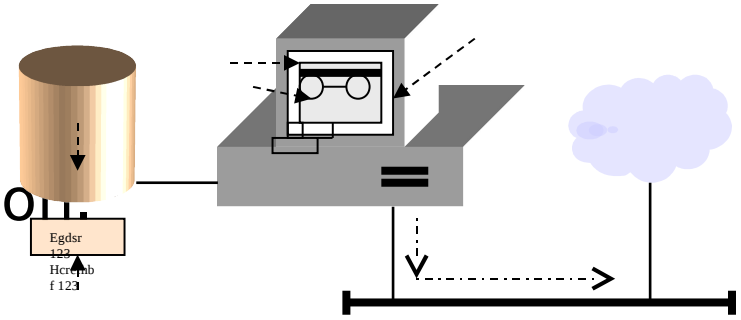


Sistemas de administración de la Red

Aplicaciones de administración

Software propietario que complementa a la Plataforma de Administración de Red y ofrece funcionalidades específicas de acuerdo al equipo activo de red que soporta.

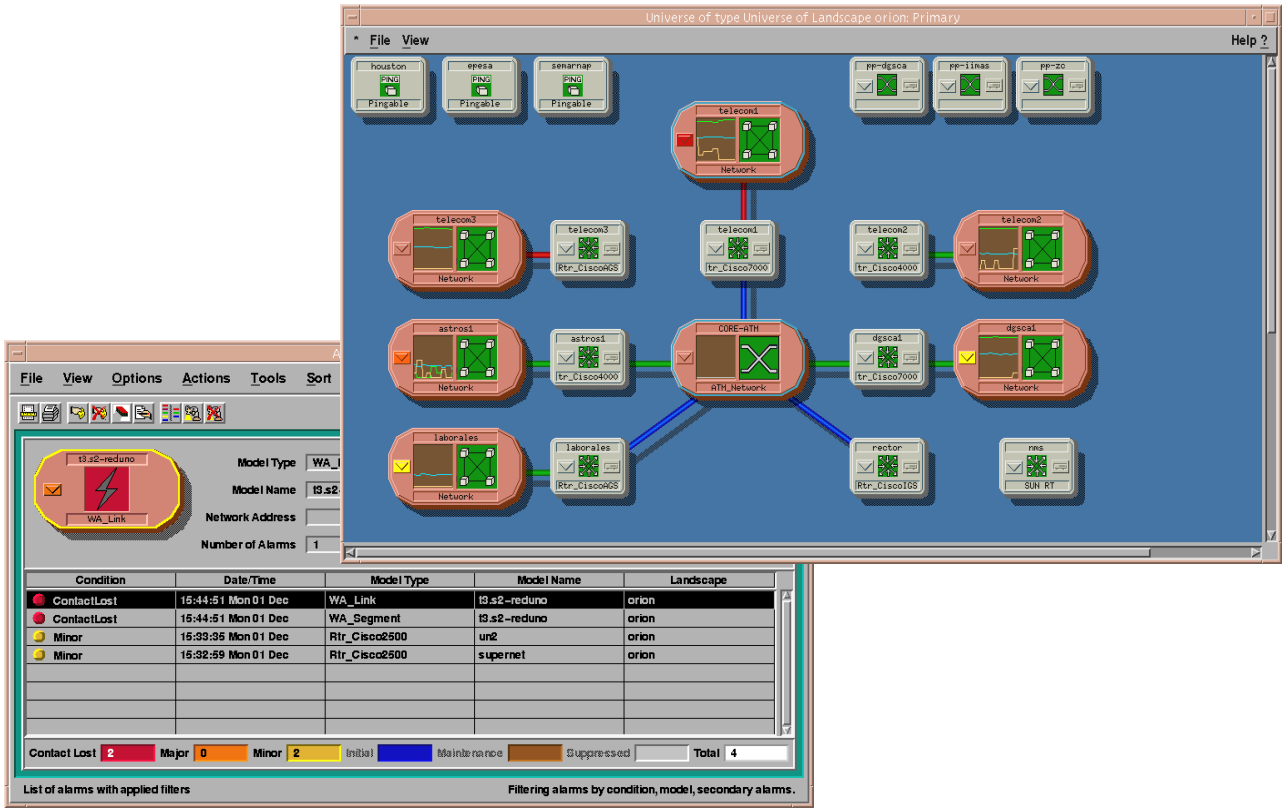
Ejemplo de éste software:



- Transcend de 3Com Corporation.
- Optivity de Nortel Networks
- Spectrum (Cabletron Systems)

Sistemas de administración de la Red

Aplicaciones de administración



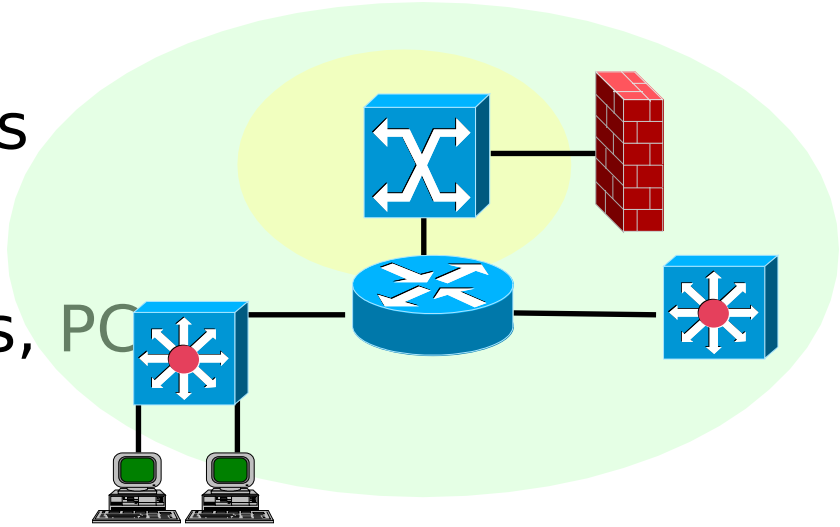
Sistemas de administración de la Red

Agentes

Son en sí los diversos equipos activos que soporten administración bajo este esquema.

Ejemplo de ellos:

- Enrutadores, Switches
- WIFI Controlers
- Workstations, Servers, PC



Sistemas de administración de la Red

Protocolos de administración de redes

Conjunto de reglas y procedimientos en software para la interacción entre una entidad de administración (NMS) y un dispositivo (Agent).

Dentro de los más comunes están:

- SNMP, SNMP v.2 y SNMP v.3
- RMON

Los siguientes 10 años de Internet2 en México
CUDI 2009

Network Information Center

InterNIC
(NetNames)

ISOC

IANA

IETF

Network Operation Center

Administración y Monitoreo de Redes

Definición:

Proceso de controlar una red compleja para maximizar su eficiencia y su productividad.

Se divide en 5 Áreas Funcionales:

- Administración de las Fallas.
- Administración de las Configuraciones.
- Administración de la Seguridad.
- Administración del Rendimiento.
- Administración de la Contabilidad.

Sistema de Administración de Red Plataforma

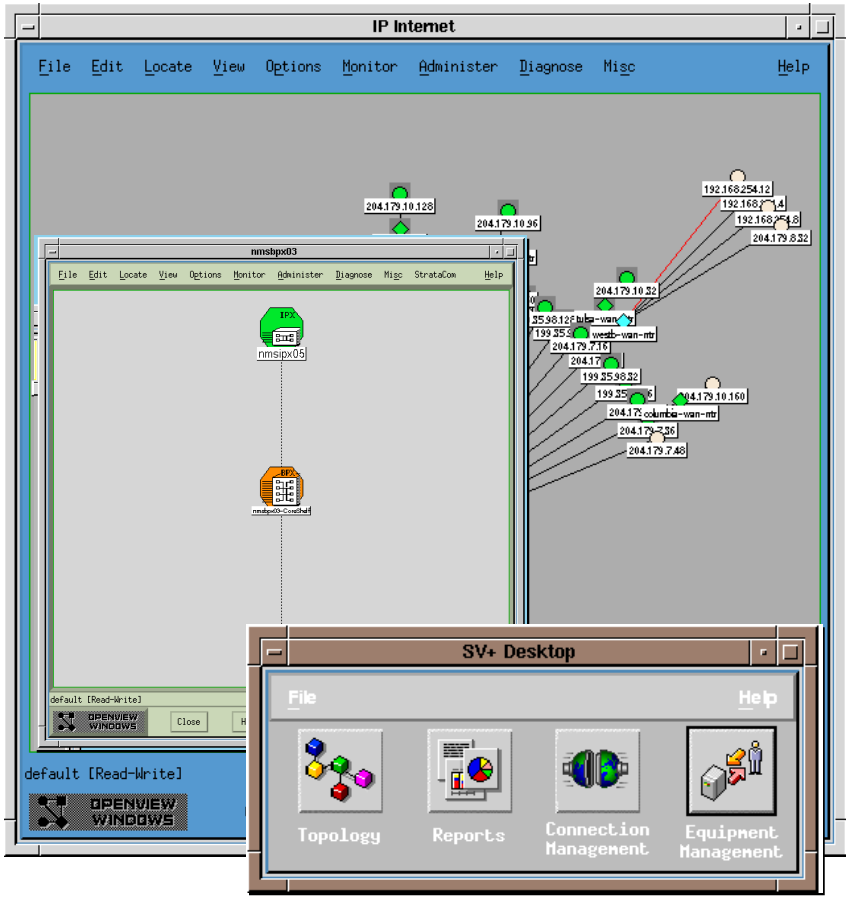
Plataforma de Administración de Red:

Software que provee la funcionalidad para administrar una gran variedad de dispositivos de red.

Funcionalidades Básicas:

- Interfaz Gráfica de Usuario.
- Mapa de la Red.
- Método Estándar para consultar a los diferentes dispositivos (MIBs).
- Sistema de Menú Personalizado.
- Sistema de Administración de Bases de Datos.
- Bitácora de Eventos.

Sistema de Administración de Red Plataforma



Sistema de Administración de Red (Cont.)

Plataforma

Características:

- Herramientas para generar gráficas y reportes.
- Interfaz de Programación para Aplicaciones (API).
- Sistemas de Seguridad.

Sistema de Administración de Red Aplicaciones

Objetivo:

Administrar dispositivos o servicios específicos.

Características:

- Administración de dispositivos específicos.
- Evita sobreponerse a las funcionalidades de la plataforma.
- Se integra a la plataforma a través de sistemas de menú y APIs.
- Reside en múltiples plataformas.

Administración y Monitoreo de Redes
Fallas

¿Qué es Administración de las Fallas?

Proceso de localizar los problemas o fallas en la red mediante diferentes mecanismos (poleo y/o eventos críticos) y corregirlos.

Pasos:

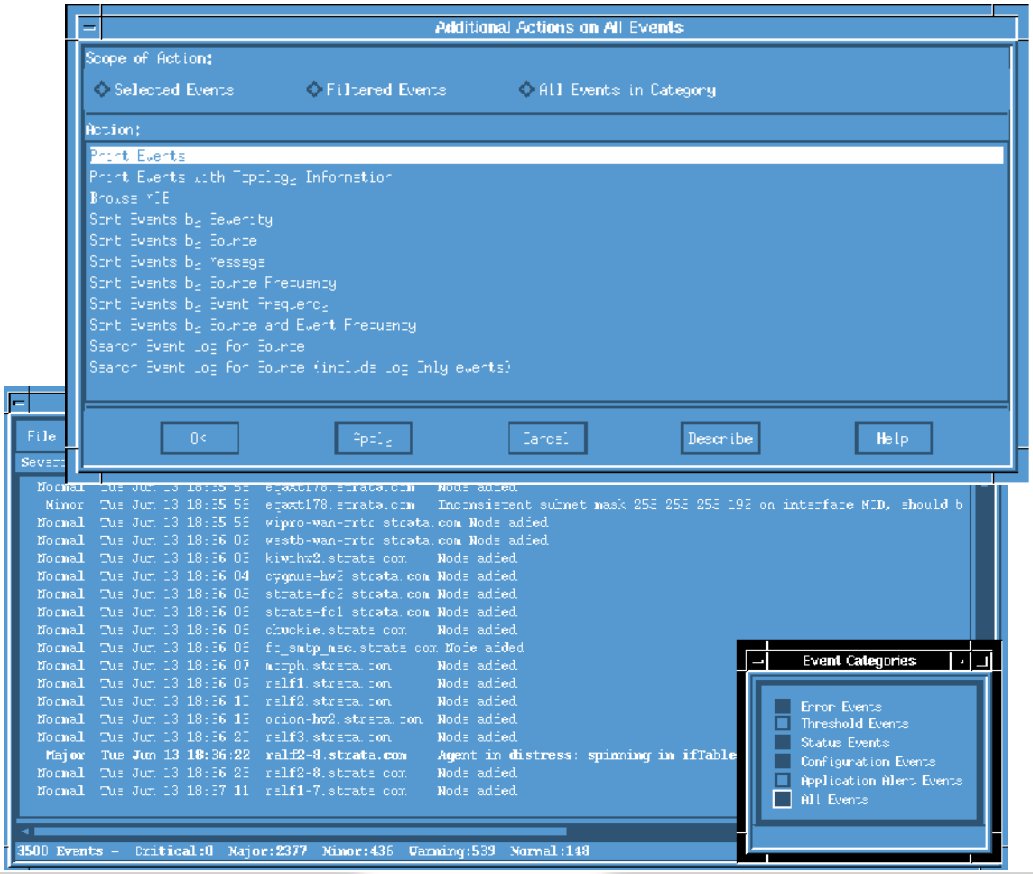
- Identificar el problema.
- Aislar el problema.
- Solucionar el problema.

Beneficios:

Incrementa la confiabilidad de la red dando herramientas para detectar problemas e iniciar procedimientos de recuperación más rápidamente.

Los siguientes 10 años de Internet2 en México
CUDI 2009

Administración y Monitoreo de Redes
Fallas



Administración y Monitoreo de Redes
Configuraciones

¿Qué es Administración de las Configuraciones?

Proceso de obtener datos de la red y usarlos para configurar todos los dispositivos.

Pasos:

- Obtener información del estado actual de la red (errores).
- Usar esos datos para modificar la configuración de los dispositivos de red.
- Almacenar los datos y tener un inventario de todos los dispositivos de la red.

Beneficios:

Permite el acceso rápido a la configuración de todos los dispositivos de red.

Administración y Monitoreo de Redes
Seguridad

¿Qué es Administración de la Seguridad?

Proceso de proteger la información más importante ubicada en los dispositivos conectados a la red controlando los puntos de acceso.

Pasos:

- Identificar la información a proteger.
- Encontrar los puntos de acceso.
- Proteger los puntos de acceso.
- Mantener la seguridad.

Beneficios:

Evita malos manejos de información que pudieran afectar el desempeño de mi red o la integridad de ésta.

Administración y Monitoreo de Redes Rendimiento

¿Qué es Administración del Rendimiento?

Proceso de verificar el desempeño de la red (hardware, software y el medio) para garantizar que no esté congestionada y que esté accesible.

Pasos:

- Obtener información de la utilización actual de los dispositivos de la red y sus enlaces.
- Analizar la información más relevante para discernir las tendencias de utilización.
- Establecer límites de utilización.
- Simular tráfico para predecir su comportamiento y maximizar su rendimiento.

Beneficios:

Proporciona consistencia en el servicio y permite corregir problemas potenciales.

Administración y Monitoreo de Redes
Contabilidad

¿Qué es Administración de la Contabilidad?

Proceso de determinar la utilización por usuario o grupo de usuarios de los recursos de la red para proporcionarlos en forma suficiente.

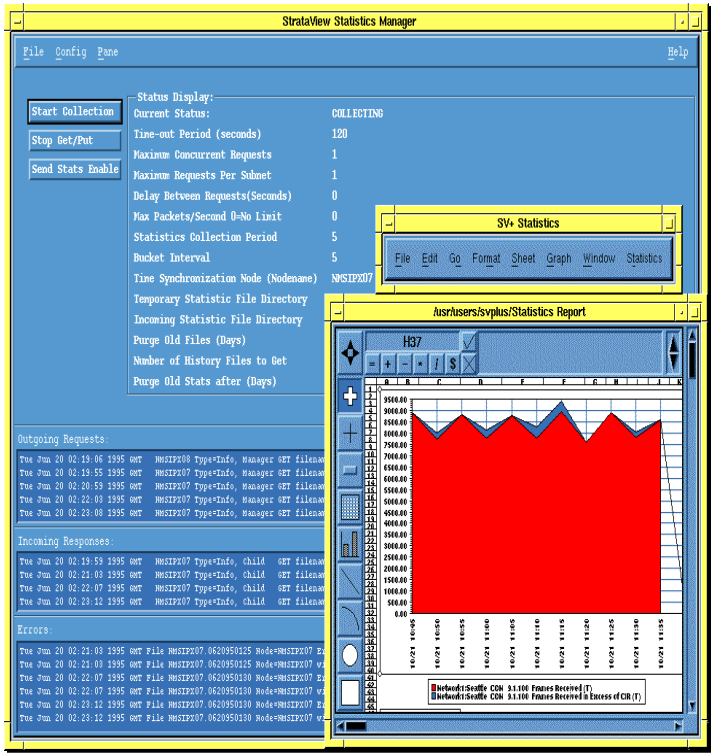
Pasos:

- Obtener información de la utilización de los recursos de la red.
- Establecer cuotas de utilización.
- Realizar el cobro por utilización de la red.

Beneficios:

Da a conocer la utilización de la red para hacerla más productiva, permite medir y reportar la utilización de los recursos por los usuarios y determinar el costo por utilización.

Administración y Monitoreo de Redes
Contabilidad



Implicaciones:

- Diseño y construcción de redes LAN y WAN
- Mantenimiento exhaustivo de hardware y software
- Expansión acelerada
- Optimización
- Mayor número de fallas

Solución:

- Control centralizado de toda la información de la red
- Atención de fallas
- Configuración de equipos de interconexión a nivel LAN y WAN
- Esquemas de seguridad
- Monitoreo del rendimiento de la red
- Contabilidad de utilización por cada usuario

Plataforma de Administración de Red

- **Monitoreo de gran cantidad de equipos con alta prioridad de administración**

Modems	Muxes	WIFI
Ruteadores	Workstations	PC
Impresioras	Switches	Antenas

- **Soporte de aplicaciones de administración**

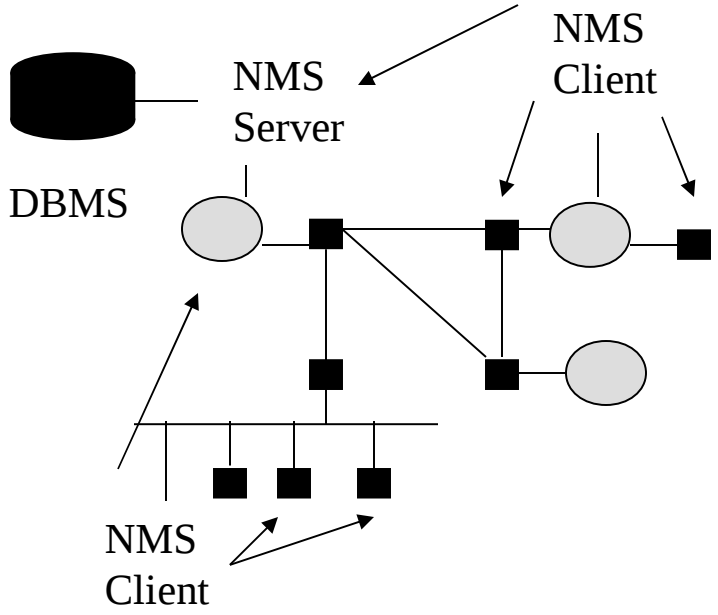
Manejo de un conjunto específico de dispositivos

- Evitar conflicto con la plataforma
- Integración por medio de API y el menu del sistema

Plataforma de Administración de Red

- **Sistema operativo UNIX (GUI = X11 Motif)**
- **Arquitectura jerárquica**

- Bases de datos con arquitectura cliente/servidor
- No dependiente de un solo sistema
- Almacenamiento de información centralizada
- Distribución del monitoreo



Plataforma de Administración de Red

META:

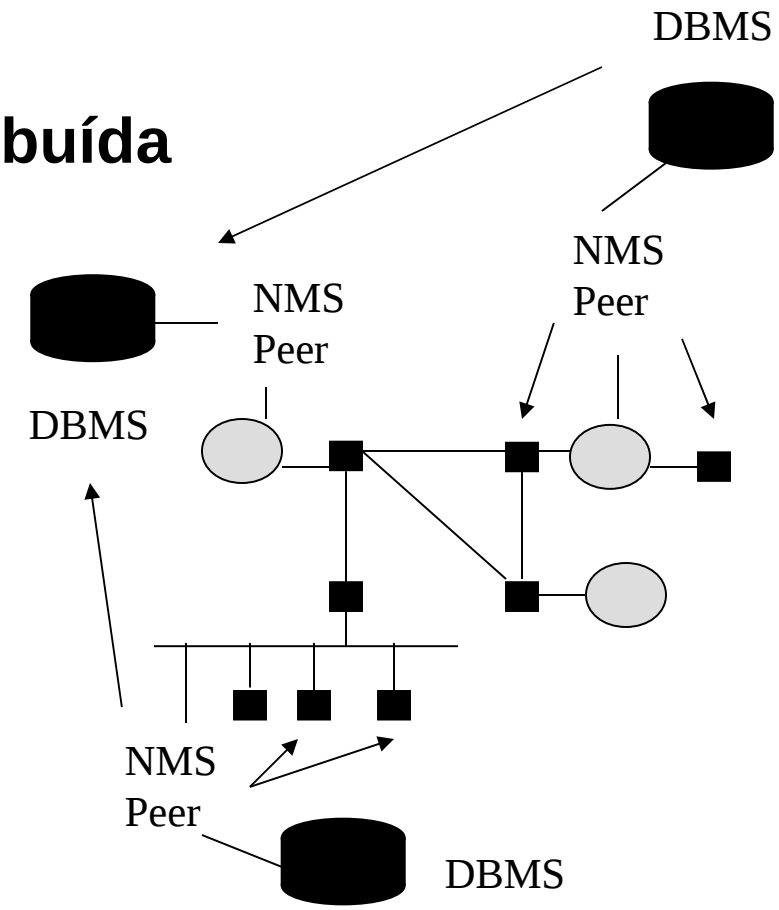
Arquitectura Distribuída

Ventajas

- Tecnología de servidor de réplica de bases de datos completamente sincronizadas
- Información de la red y aplicaciones de administración en un solo lugar

Desventajas

- Mayor consumo de ancho de banda



Administración de Fallas

Nuestro objetivo:

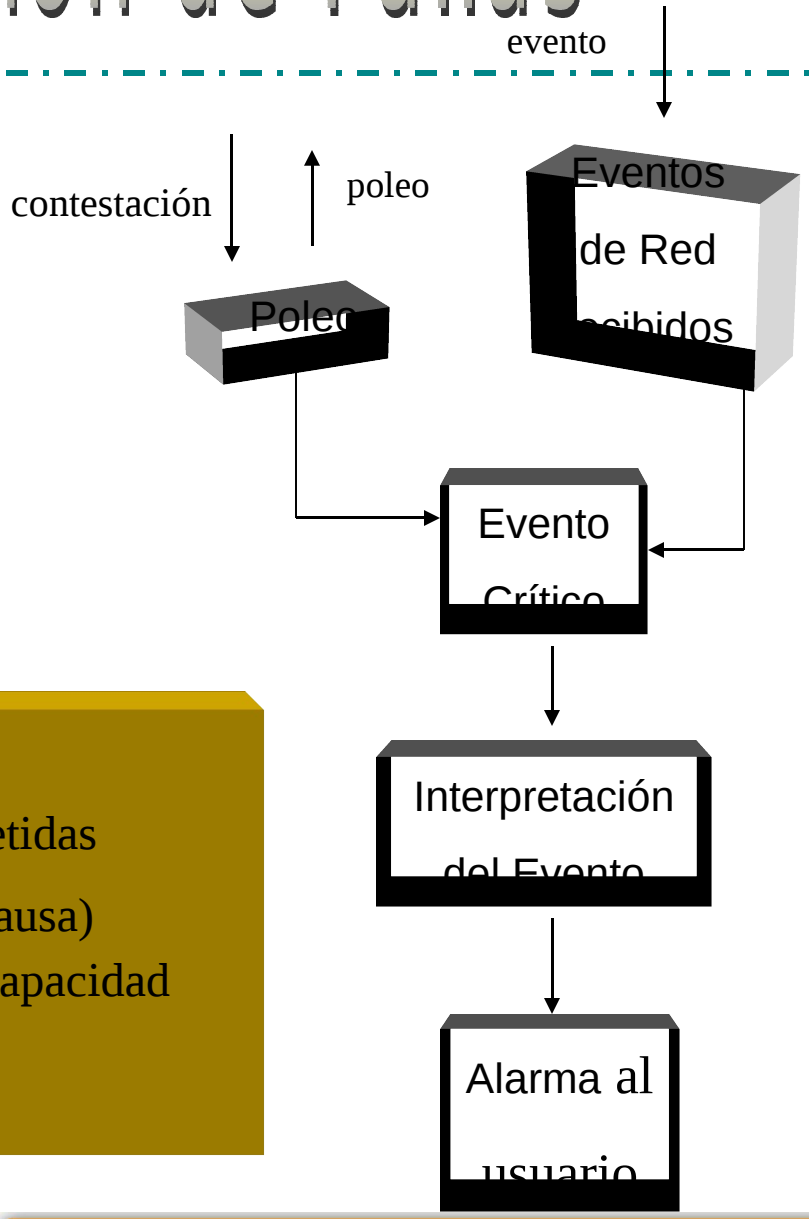
- **Incrementar la confiabilidad y efectividad de la red**
- **Solución rápida**
- **Mantener la “ilusión” de completa y continua conectividad entre usuarios y en toda la red detectando y arreglando la falla antes de que el usuario se dé cuenta de ello.**

Administración de Fallas

Como lo hacemos:

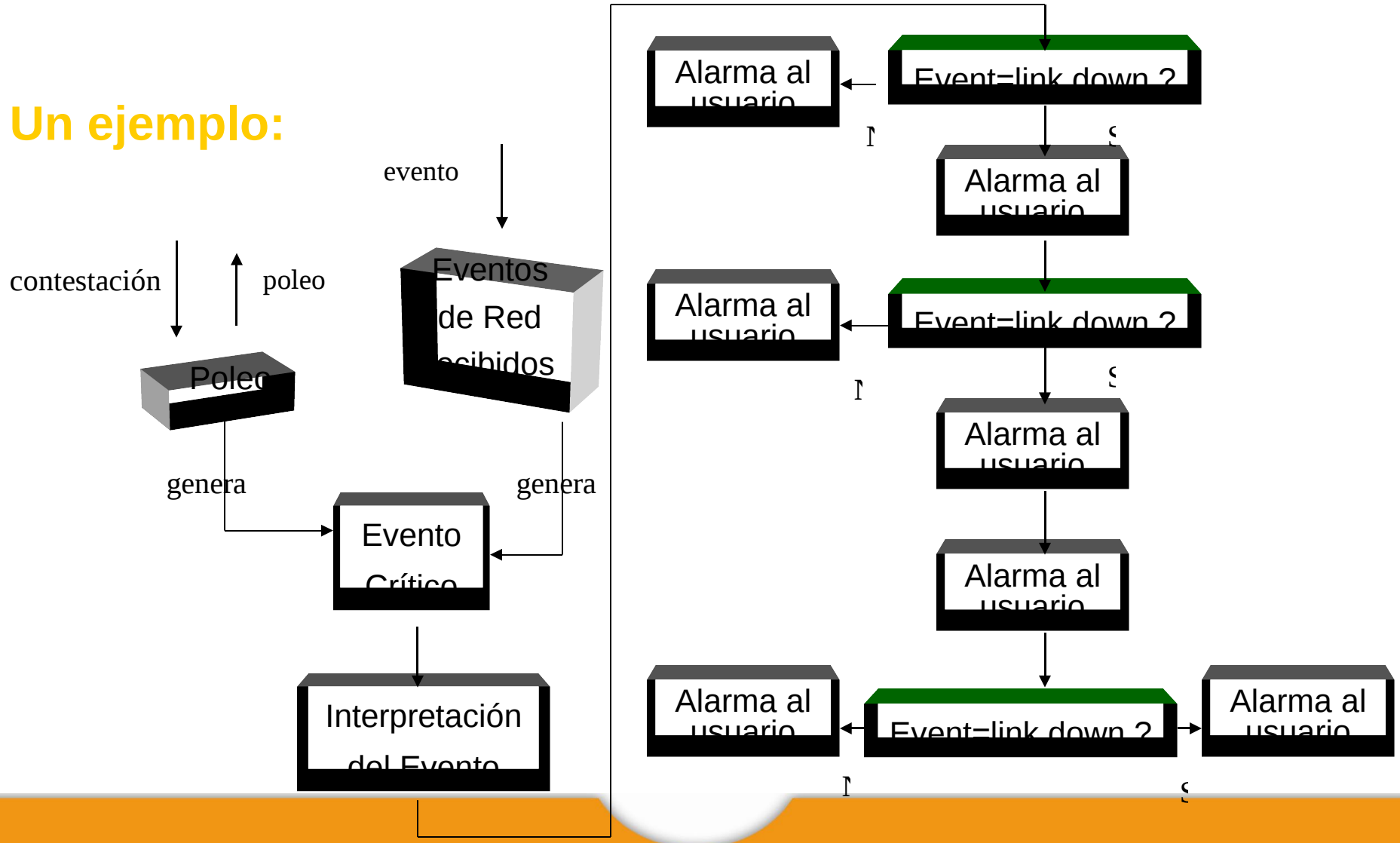
- **Identificación del problema**

- Mensajes de ICMP o conexiones remotas repetidas
  (Existencia de falla; no se identifica la causa)
- Mensajes de poleo o registro de eventos con capacidad de reportar las fallas y sus implicaciones
  (Aislamiento de la causa de la falla)



Administración de Fallas

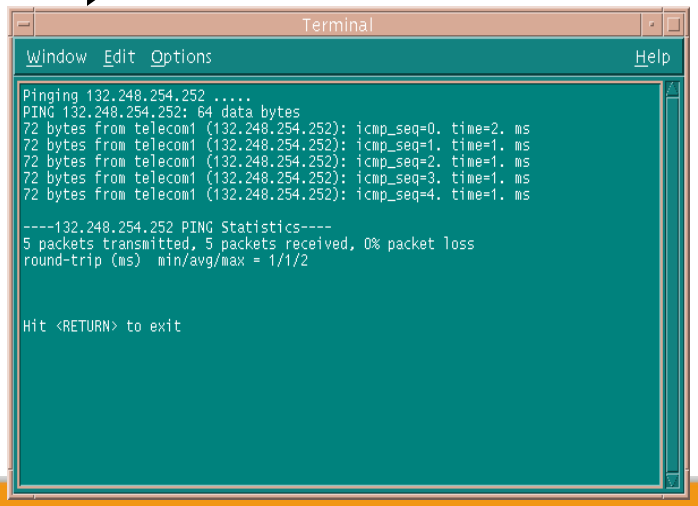
Un ejemplo:

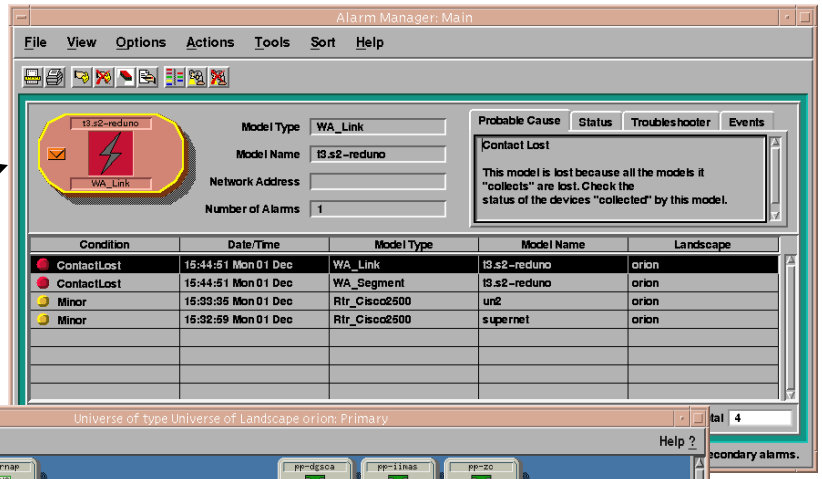


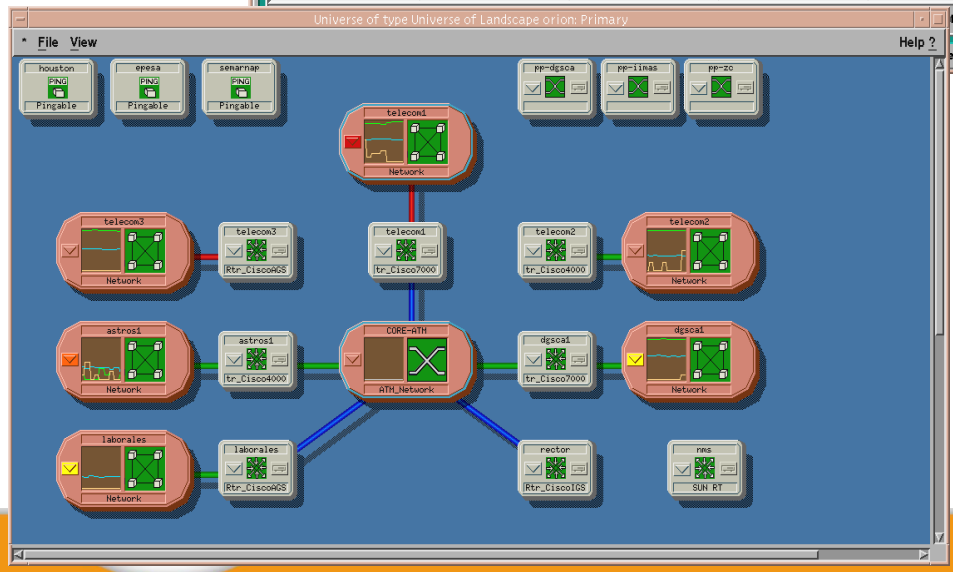
Administración de Fallas

Presentación de fallas por medio de

- Mensajes de texto
- Gráficas en color
- Señales Auditivas

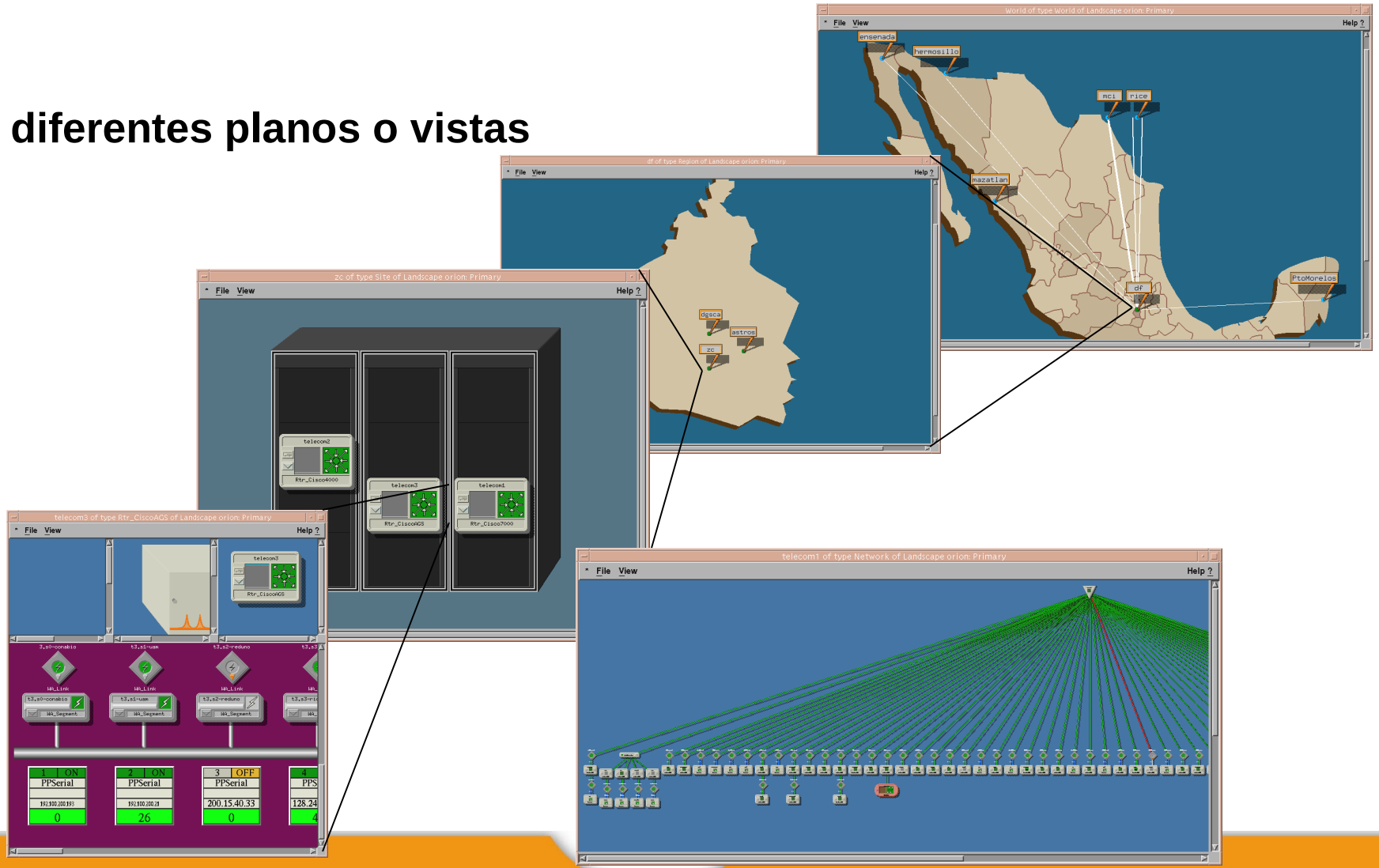






Administración de Fallas

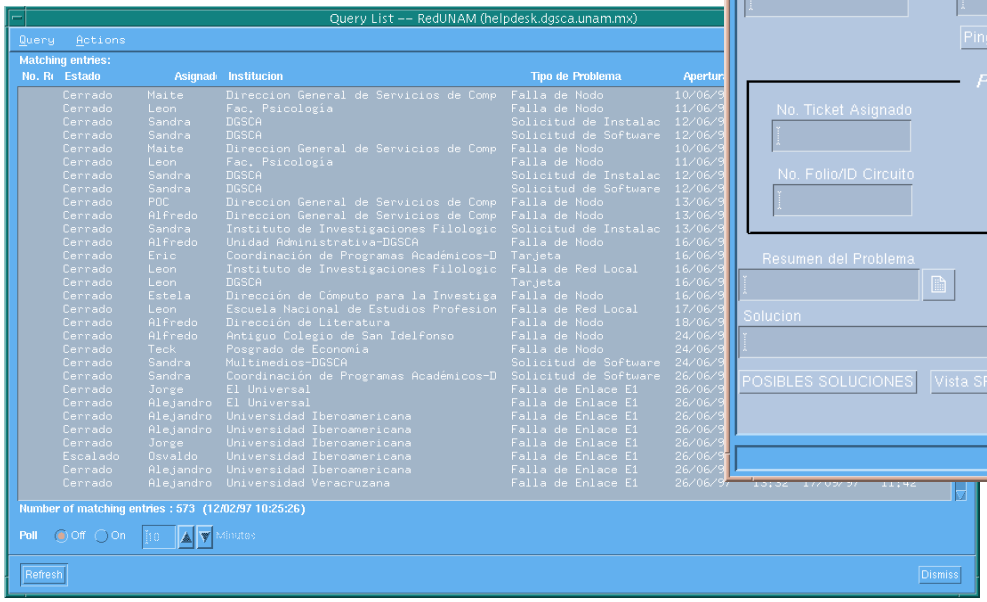
En diferentes planos o vistas

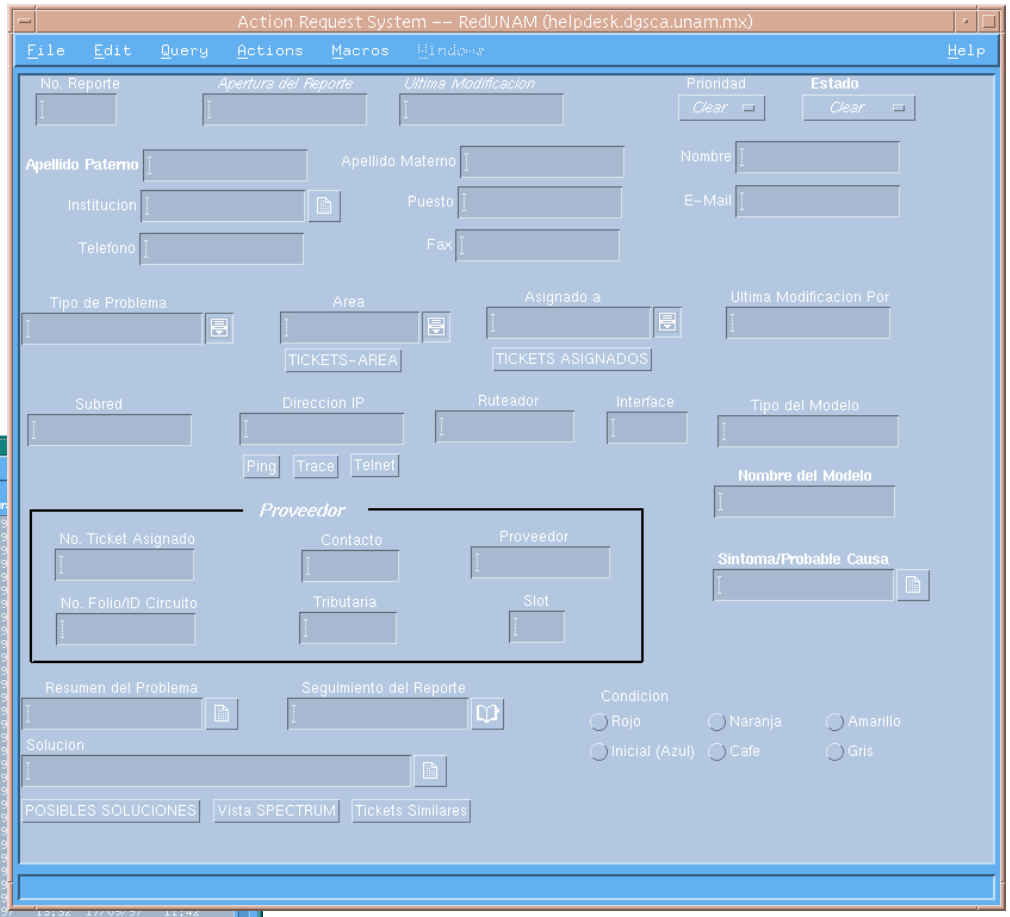


Los siguientes 10 años de Internet2 en México
CUDI 2009

Administración de Fallas

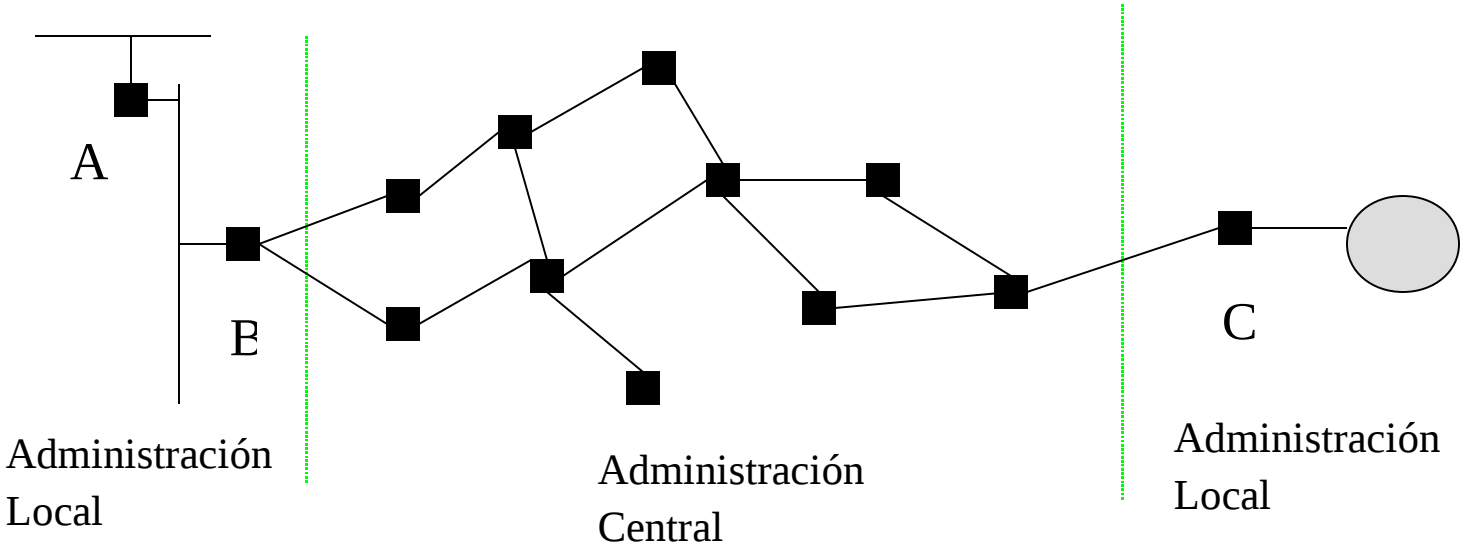
- **Sistema de reportes**





Administración de Fallas

- **Determinar las prioridades de atención de fallas**
  - Alcance del control de la red
  - Tamaño de la red



Administración de Fallas

META:

Elaboración de herramientas que verifiquen las fallas, realicen pruebas y corrijan los errores con ayuda de información perteneciente a bases de datos inteligentes

Administración de Configuración

Nuestro objetivo:

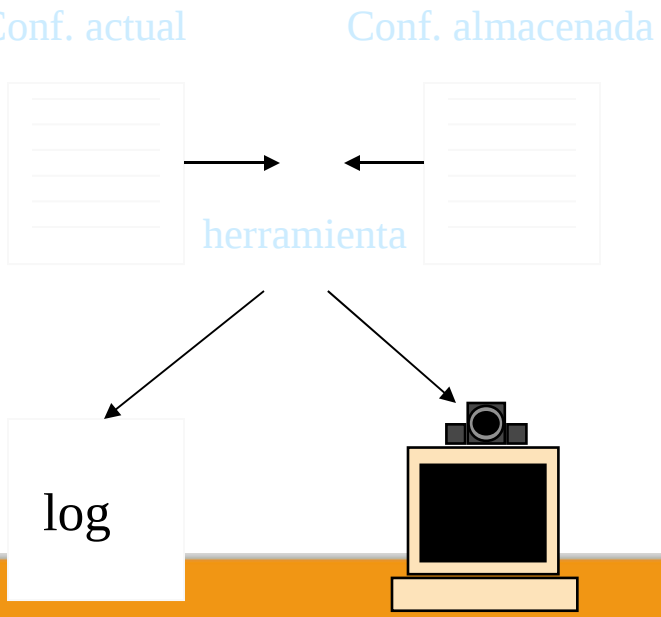
- **Control eficiente de la configuración de los dispositivos importantes de la red**

Administración de Configuración

Como lo hacemos:

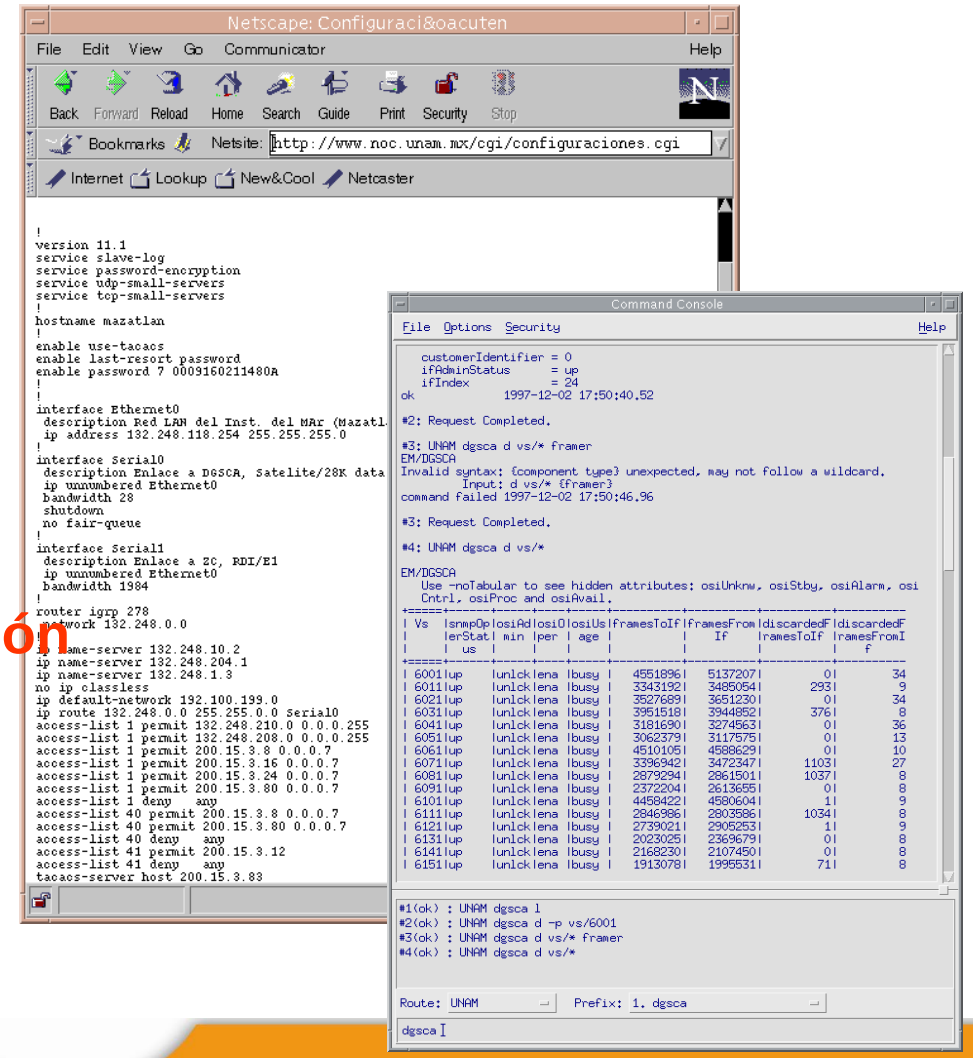
- **Obtención de la configuración de los dispositivos importantes de la red (ruteadores y switches)**

- Utilerías externas: comparan la configuración actual con la almacenada. Los errores se guardan en una bitácora.
- Autodescubrimiento y Automapeo con la plataforma de administración de la red



Administración de Configuración

Como lo hacemos:



- **Acceso rápido a la configuración para realizar modificaciones**
- **Inventario actualizado de los componentes de la red**
- **Generación de reportes**

Administración de Configuración

META:

Elaboración de una base de datos que permita relacionar, consultar e inventariar la información de la red. Asimismo que sirva para evaluar las configuraciones de los dispositivos

Administración de Seguridad

Nuestro objetivo:

- **Proteger la información sensible en dispositivos directamente conectados a la red controlando los puntos de acceso a esa información**

Cómo lo hacemos

- **Identificación de los servidores con información sensible**
  - Servidores : xtacacs, radius, DNS, correo electrónico, www, trouble tickets, ftp, etc.
- **Localización de los puntos de acceso**

Administración de Seguridad

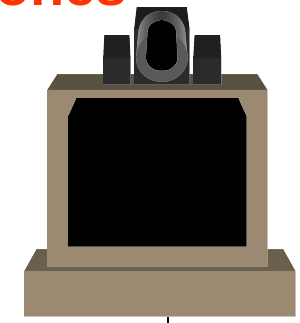
- **Limitaciones de acceso a dispositivos importantes desde cualquier parte de la red a través de:**

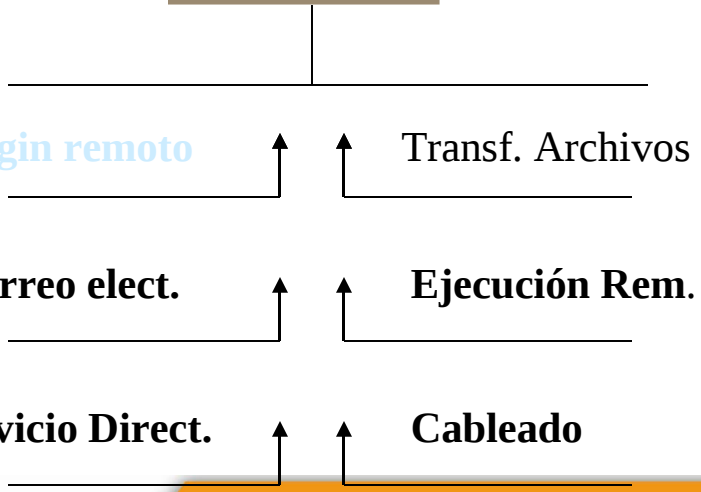
  - Autenticación: Host, Usuario, Key Server
  - Firewall
  - Encripción
  - Filtros de paquetes

Administración de Seguridad

- **Limitaciones en las aplicaciones**

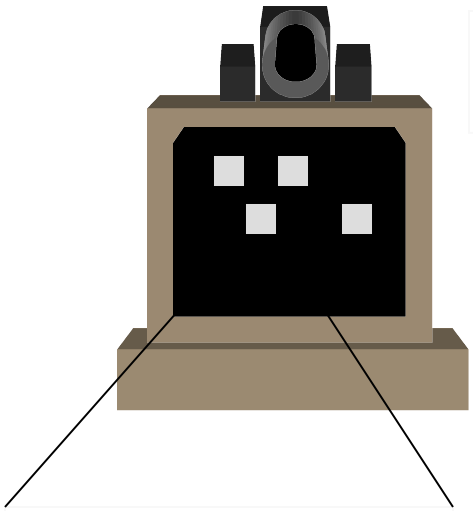
- FTP Anónimo
- Telnet
- NFS





Administración de Seguridad

- **Plataforma de administración de red que notifica los accesos a nodos importantes de la red y genera reportes**



Rlogin excesivos en X

User = YYYY

Hora = 08:03 AM

Intentos de Rlogin

Red

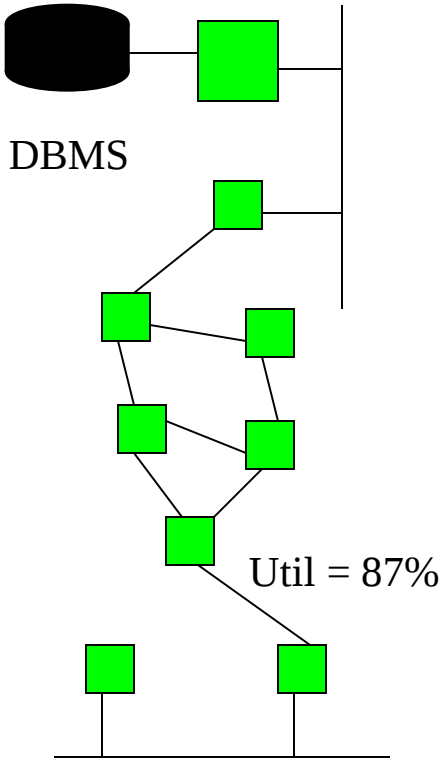
Terminal

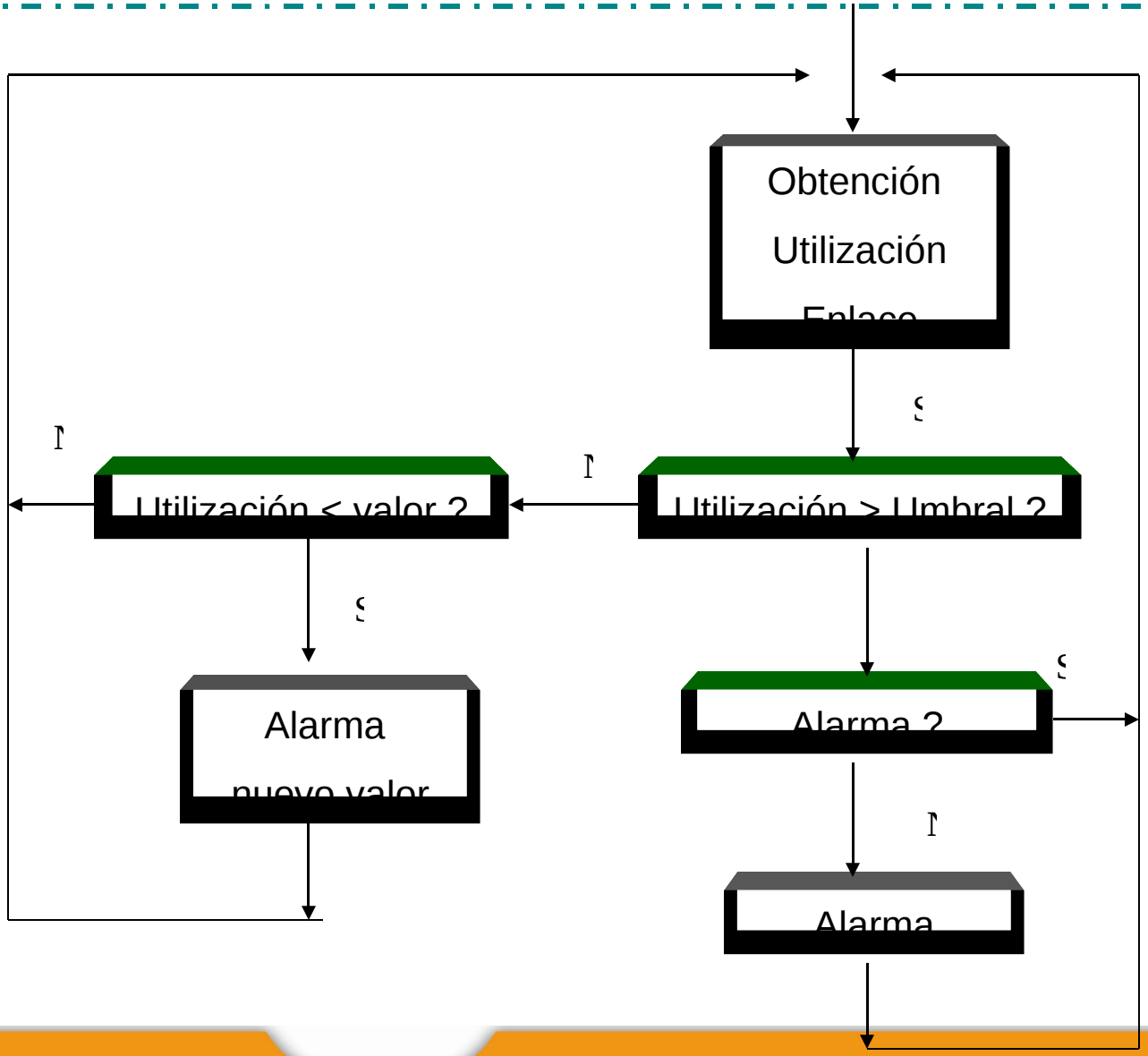
Edit Options Help

```
ate
pielias   tty0     132.248.237.253  Wed Nov 26 09:44 - 09:44  (00:00) 19 inaccur
ate
lombera   tty0     132.248.237.253  Wed Nov 26 09:43 - 09:44  (00:00) 48 inaccur
ate
anava     tty0     132.248.237.253  Wed Nov 26 09:37 - 09:38  (00:01) 70
erick     tty0     132.248.237.253  Wed Nov 26 09:33 - 09:34  (00:01) 82
gypsy     tty0     132.248.237.253  Wed Nov 26 09:32 - 09:33  (00:00) 35 inaccur
ate
hmv       tty0     132.248.237.253  Wed Nov 26 09:32 - 09:32  (00:00) 22
segrera   tty0     132.248.237.253  Wed Nov 26 09:31 - 09:31  (00:00) 5
cyranoar  tty0     132.248.237.253  Wed Nov 26 09:30 - 09:30  (00:00) 12
rdaniel   tty0     132.248.237.253  Wed Nov 26 09:29 - 09:30  (00:00) 22
arbesu    tty0     132.248.237.253  Wed Nov 26 09:27 - 09:28  (00:00) 14
mebs      tty0     132.248.237.253  Wed Nov 26 09:24 - 09:25  (00:01) 77
lopezde   tty0     132.248.237.253  Wed Nov 26 09:23 - 09:24  (00:00) 59
wolfb     tty0     132.248.237.253  Wed Nov 26 09:22 - 09:23  (00:00) 31 inaccur
ate
fermintv  tty0     132.248.237.253  Wed Nov 26 09:21 - 09:22  (00:01) 65 inaccur
ate
anvcorp   tty0     132.248.237.253  Wed Nov 26 09:20 - 09:20  (00:00) 12
xolotl    tty0     132.248.237.253  Wed Nov 26 09:19 - 09:19  (00:00) 3
segrera   tty0     132.248.237.253  Wed Nov 26 09:18 - 09:18  (00:00) 6
anvcorp   tty0     132.248.237.253  Wed Nov 26 09:18 - 09:18  (00:00) 12 inaccur
```

Administración de Seguridad

Un ejemplo:





Administración de Seguridad

META:

Elaboración de herramientas que examinen las implicaciones de la seguridad impuesta

Administración del Rendimiento

Nuestro objetivo:

- **Asegurar que las vías de comunicación permanezcan accesibles y descongestionadas**

Administración del Rendimiento

Cómo lo hacemos

- **Obtención de la información de utilización y tasas de error actuales de los nodos y enlaces importantes de la red**

Host

- Carga del procesador
- Accesos a disco
- Utilización de la interfaz de red

Ruteadores y Switches

- Carga del procesador
- Frames desechados
- Colisiones
- Bytes de entrada y salida

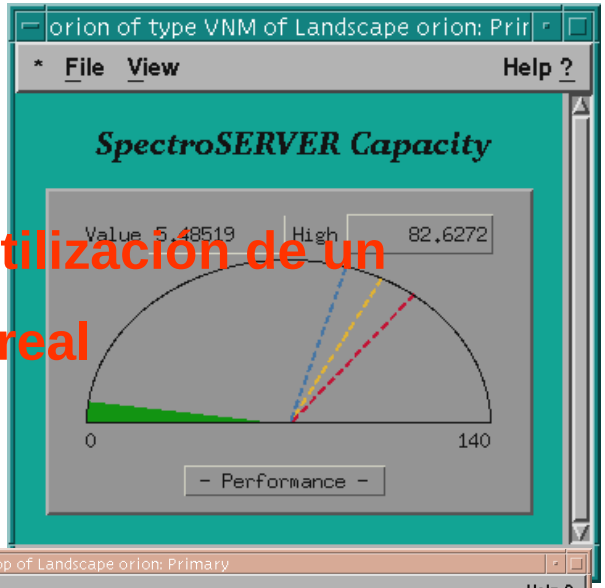
Enlaces

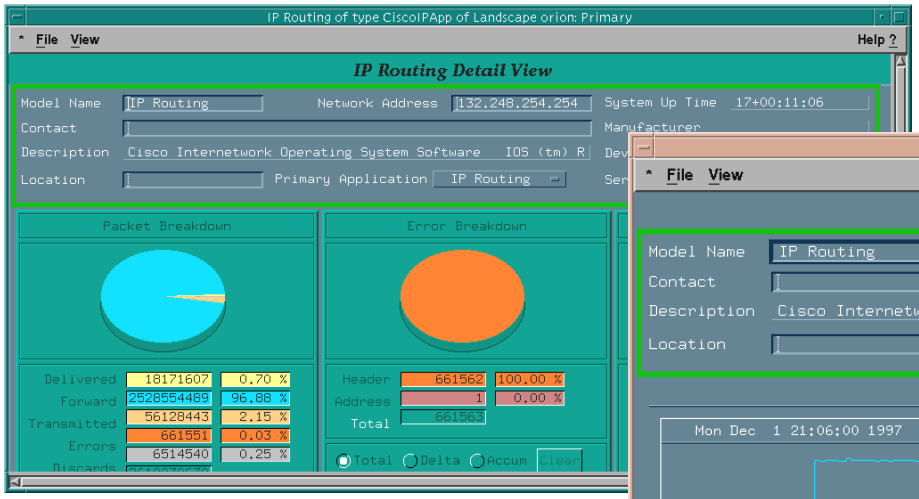
$$util\% = \frac{Max(BytesIn+BytesOut)}{Ancho\ de\ Banda}$$

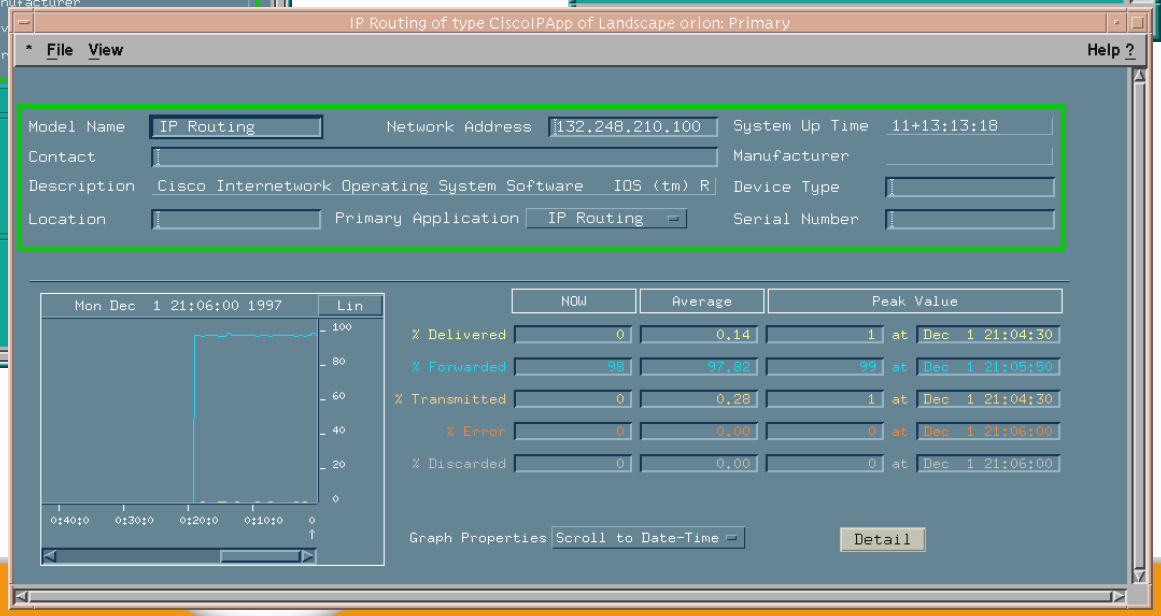
Los siguientes 10 años de Internet2 en México
CUDI 2009

Administración del Rendimiento

- **Representación gráfica y análisis de la utilización de un dispositivo o enlace de la red en tiempo real**





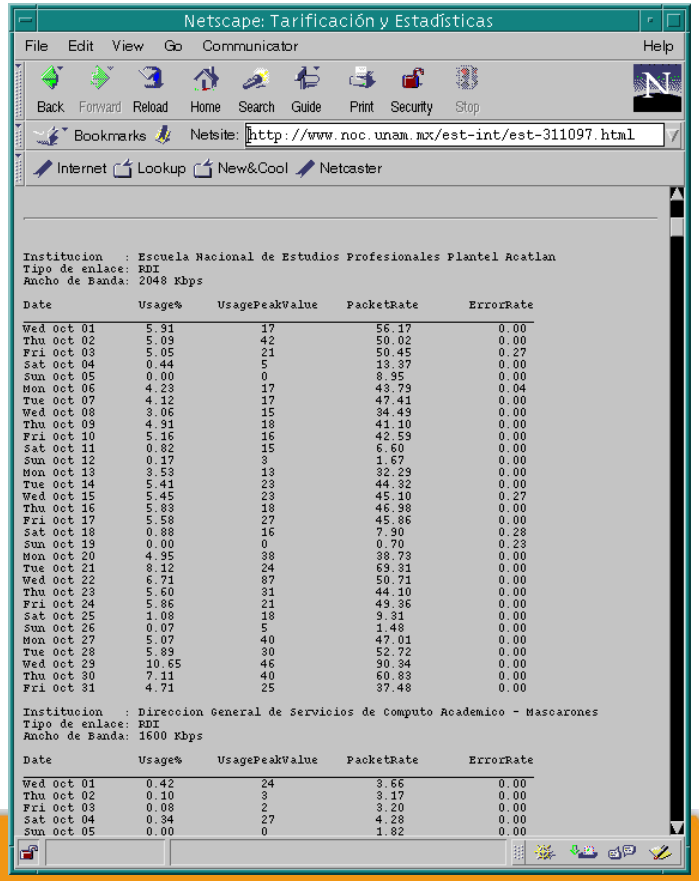


Administración del Rendimiento

- **Determinación de los umbrales**

Utilización

- 45% prioridad baja
- 65% prioridad medio
- 80% prioridad alta



Institucion : Escuela Nacional de Estudios Profesionales Plantel Acatlan
Tipo de enlace: RDI
Ancho de Banda: 2048 Kbps

Date	Usage%	UsagePeakValue	PacketRate	ErrorRate
Wed Oct 01	5.91	17	56.17	0.00
Thu Oct 02	5.09	42	50.02	0.00
Fri Oct 03	5.05	21	50.45	0.27
Sat Oct 04	0.44	5	13.37	0.00
Sun Oct 05	0.00	0	8.95	0.00
Mon Oct 06	4.23	17	43.79	0.04
Tue Oct 07	4.12	17	47.41	0.00
Wed Oct 08	3.06	15	34.49	0.00
Thu Oct 09	4.91	18	41.10	0.00
Fri Oct 10	5.16	16	42.59	0.00
Sat Oct 11	0.82	15	6.60	0.00
Sun Oct 12	0.17	3	1.67	0.00
Mon Oct 13	3.53	13	32.29	0.00
Tue Oct 14	5.41	23	44.32	0.00
Wed Oct 15	5.45	23	45.10	0.27
Thu Oct 16	5.83	18	46.98	0.00
Fri Oct 17	5.58	27	45.86	0.00
Sat Oct 18	0.88	16	7.90	0.28
Sun Oct 19	0.00	0	0.70	0.23
Mon Oct 20	4.95	38	38.73	0.00
Tue Oct 21	8.12	24	69.31	0.00
Wed Oct 22	6.71	87	50.71	0.00
Thu Oct 23	5.60	31	44.10	0.00
Fri Oct 24	5.86	21	49.36	0.00
Sat Oct 25	1.08	18	9.31	0.00
Sun Oct 26	0.07	5	1.48	0.00
Mon Oct 27	5.07	40	47.01	0.00
Tue Oct 28	5.89	30	52.72	0.00
Wed Oct 29	10.65	46	90.34	0.00
Thu Oct 30	7.11	40	60.83	0.00
Fri Oct 31	4.71	25	37.48	0.00

Institucion : Direccion General de Servicios de Computo Academico - Mascarones
Tipo de enlace: RDI
Ancho de Banda: 1600 Kbps

Date	Usage%	UsagePeakValue	PacketRate	ErrorRate
Wed Oct 01	0.42	24	3.66	0.00
Thu Oct 02	0.10	3	3.17	0.00
Fri Oct 03	0.08	2	3.20	0.00
Sat Oct 04	0.34	27	4.28	0.00
Sun Oct 05	0.00	0	1.82	0.00

- **Generación de reportes mensuales de utilización para instituciones internas y externas**

Administración del Rendimiento

META:

Desarrollo de una herramienta que analice el comportamiento de la red a través de la simulación y arroje predicciones a corto y largo plazo sobre el tiempo de respuesta de conexión, tasas de error y disponibilidad

Administración de Contabilidad

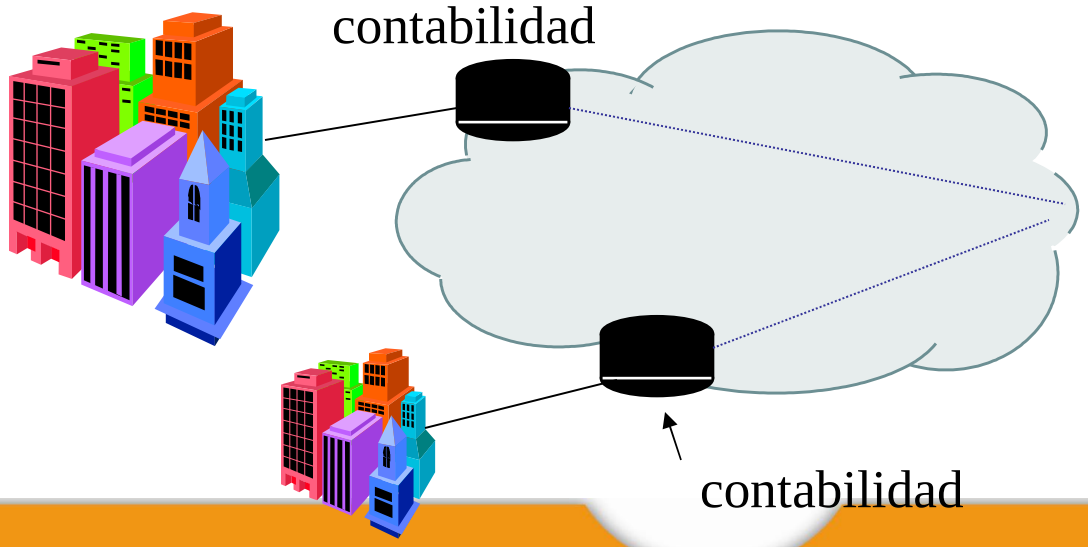
Nuestro objetivo:

- **Realizar la facturación de cada cliente por el servicio de red utilizado (enlaces internacionales)**

Administración de Contabilidad

Cómo lo hacemos

- **Obtención de la información a través de bitácoras de la plataforma de administración de red**
- **Contabilidad diaria de utilización de cada institución**



Administración de Contabilidad

META:

Empleo de otras métricas y correspondientes cuotas

- Número de conexiones realizadas a un host
- Número de transacciones via red con una base de datos
- Tiempo de conexión

Ayuda a usuarios en la predicción de sus costos

Identificación de exceso de cuotas para actualizar el equipo, modificar la cuota, etc.

SNMP
Simple Network Management Protocol.

Existen dos propuesta en cuanto a normas para la implementación de sistemas de gestión integrados:

- RFC 1157
- Gestión SNMP (Simple Network Management Protocol) para redes TCP/IP. Estas normas de gestión surgió en el marco de INTERNET y se explicarán en más detalle más adelante.

Tendencias en normas para la implementación de sistemas de gestión

- Gestión OSI (CMIP-CMISE) que surge como esfuerzo de estandarización de la gestión en el marco del Modelo de Referencia para Interconexión de Sistemas Abiertos.

Antecedentes de SNMP

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

Antecedentes de SNMP

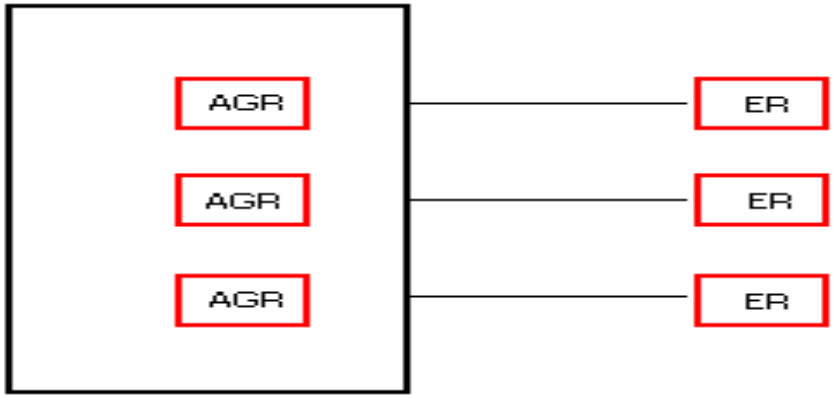
- En 1988 se implementó y comenzó a utilizarse un protocolo de gestión denominado SNMP (Simple Network Management Protocol), un protocolo sencillo para la gestión de red.
- Este protocolo ha sido muy aceptado desde entonces y la mayoría de los fabricantes lo implementan en sus equipos con protocolos TCP/IP.

Antecedentes de SNMP

La Base de Información de Gestión contiene los recursos de comunicaciones según el modelo de estructura de información de gestión. En la figura se muestra el modelo general de la gestión SNMP, sabiendo que:

AGR: Aplicaciones de Gestión de Red

Er: Elementos de Red.



Antecedentes de SNMP

La gestión de red SNMP está formada por un conjunto de estaciones de gestión de red y un conjunto de elementos de red.

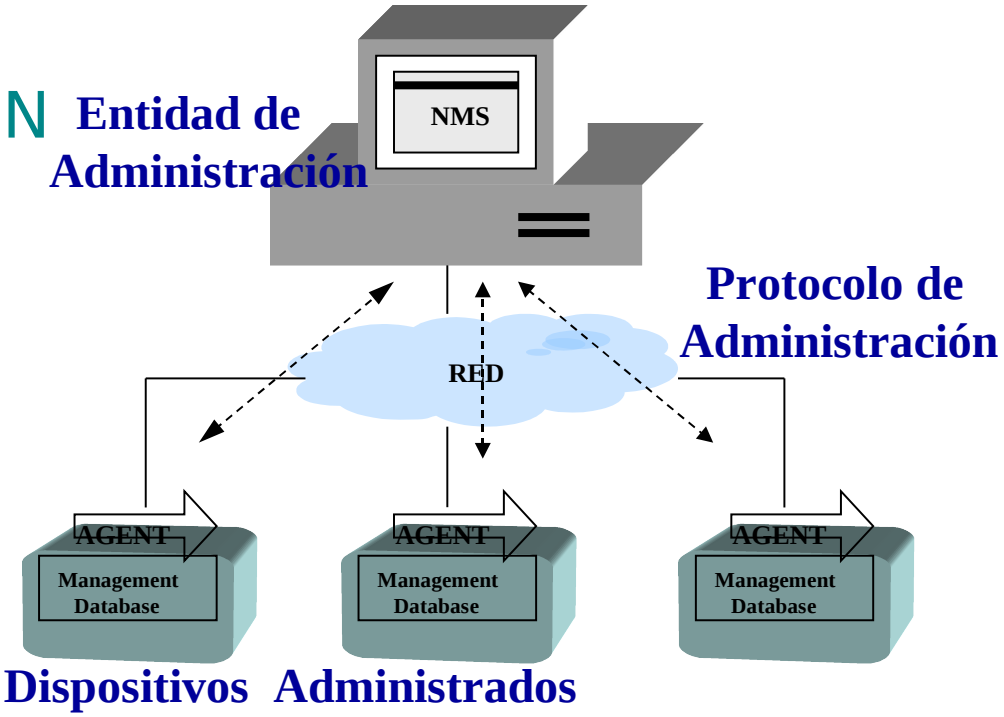
- Las estaciones de gestión de red ejecutan las aplicaciones de gestión que monitorizan y controlan los elementos de red.
- Los elementos de red son dispositivos tales como PCs, Routers,Switches (Sistemas Intermedios o Gateways en terminología de Internet), etc.
- Estos elementos de red disponen de procesos agentes responsables de la realización de las actividades de gestión.

El entorno de Gestión SNMP comprende los siguientes 4 componentes:

- Procesos agentes en los elementos de la red.
- Procesos gestores en las estaciones de gestión.
- Un protocolo común que enlaza los procesos gestores y los procesos agentes.
- Información de gestión de red.

Terminología

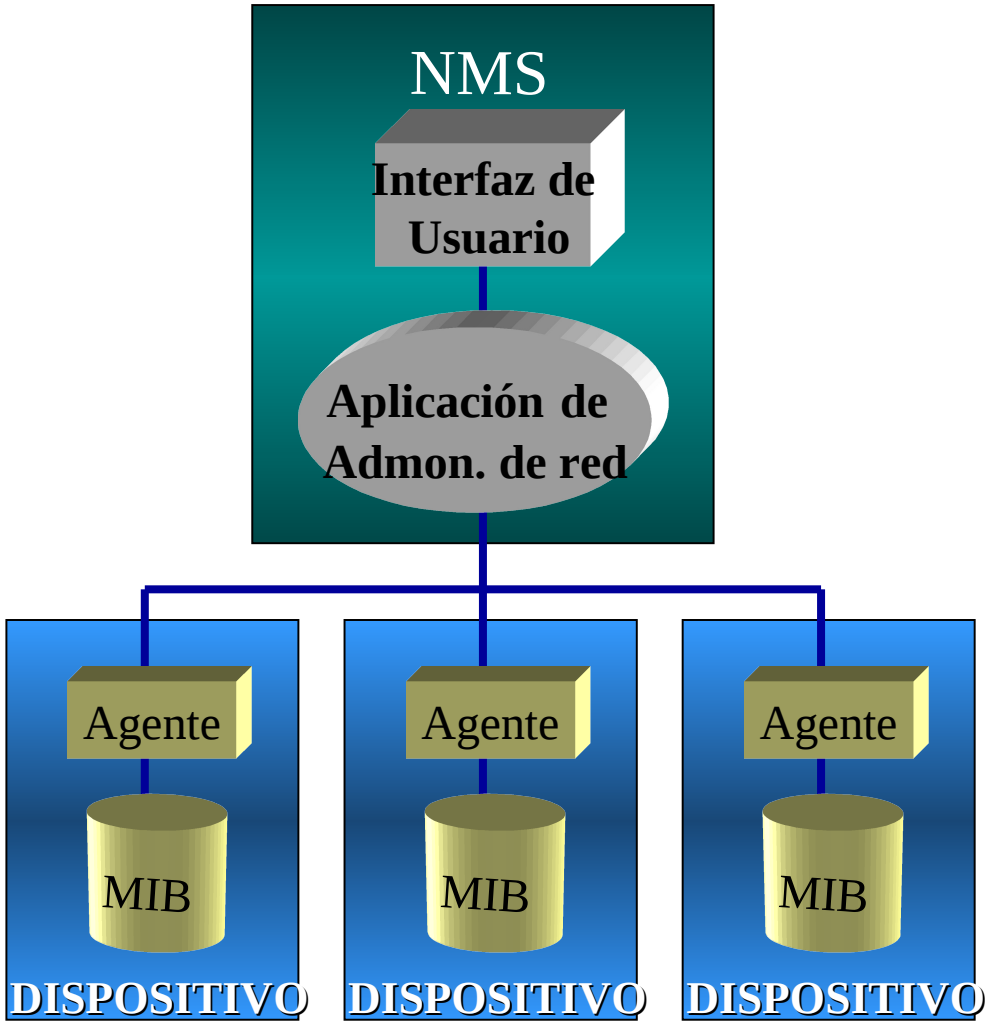
- MANAGMENT STATION
- AGENTE
- MIB



Modo de Operación

- En este punto es necesario que se comunique la estación de administración con el agente.
- La estación de administración hará una petición al agente por medio de un **“object identifier”** para que este pueda entenderla.

Estructura de SNMP



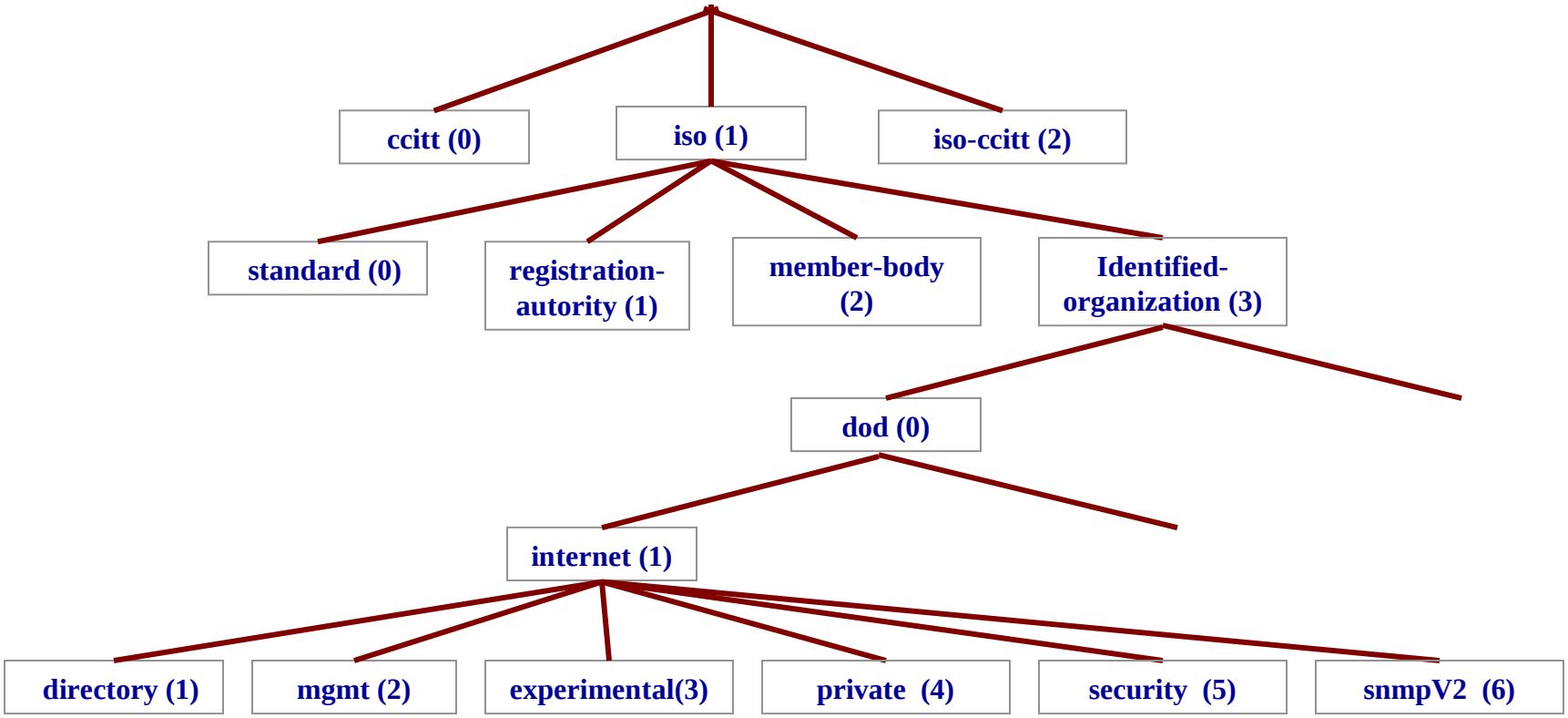
Que es un Object IDentifier?

- SNMP describe un conjunto de grupos para peticiones definidas, estos grupos están alojados dentro de un árbol jerárquico.
- Dentro del cual tenemos que hacer la petición, cada salto que se de dentro del árbol estará definido por un numero de identificación establecido.
- Definido por el Structure of Management Information RFC 1155

Categorías de Información de MIBS

- Systems (1)
- Interface (2)
- Address Translation (3)
- IP (4)
- ICMP (5)
- TCP (6)
- UDP (7)
- S.O del host
- Interface (2)
- Address Translation (3)
- IP (4)
- ICMP (5)
- TCP (6)
- UDP (7)

Arbol de MIBS para SNMP



De tal manera que!!

- El conjunto de dichos números nos han de formar el object identifier para la petición que hagamos.
- Quedando un object identifier de la siguiente manera

- 1.3.6.1.2

Internet Subtree

- Directory
- Mgmt
  - {mgmt 1} or 1.3.6.1.2.1
- Experimental
  - {experimental 23} or 1.3.6.1.3.23
- Private
  - Ejemplo, la compañía X le fue asignado el nodo 43. Esta podría registrar su administración de bridging como: 1.3.6.1.4.43.2

Ejemplo de MIB Objects

- Formato de las Definiciones de MIBs
  - SYNTAX
  - ACCESS
  - STATUS
  - DESCRIPTION
  - REFERENCE
  - INDEX
  - DEFVAL
  - VALUE NOTATION

Ejemplo

- Ejemplo #1

ifMtu		OBJECT-TYPE
	SYNTAX:	INTEGER
	ACCESS:	read-only
	STATUS:	mandatory
	DESCRIPTION:	“The size of the largest IP datagram which can be sent / received on the interface, specified in octects.”
	::=	{ ifEntry 4 }

Ejemplo

- Example #2

```
sysUpTime       OBJECT-TYPE
    SYNTAX:     TimeTicks
    ACCESS:     read-only
    STATUS:     mandatory
    DESCRIPTION: “The time (in hundredths of a second) since the network manamgement portion of the system was last re-initializad”
    ::=         { system 3 }
```

Funciones en SNMP

- GET: Obtiene el valor de objetos .
- GET-NEXT: Obtiene el valor de la variable adyacente.
- SET: Modifica el valor de una variable.

Funciones en SNMP

- GET-RESPONSE: Proporciona el resultado de las operaciones: GET, GET-NEXT y SET.
- TRAP: Informe asíncrono de un evento.

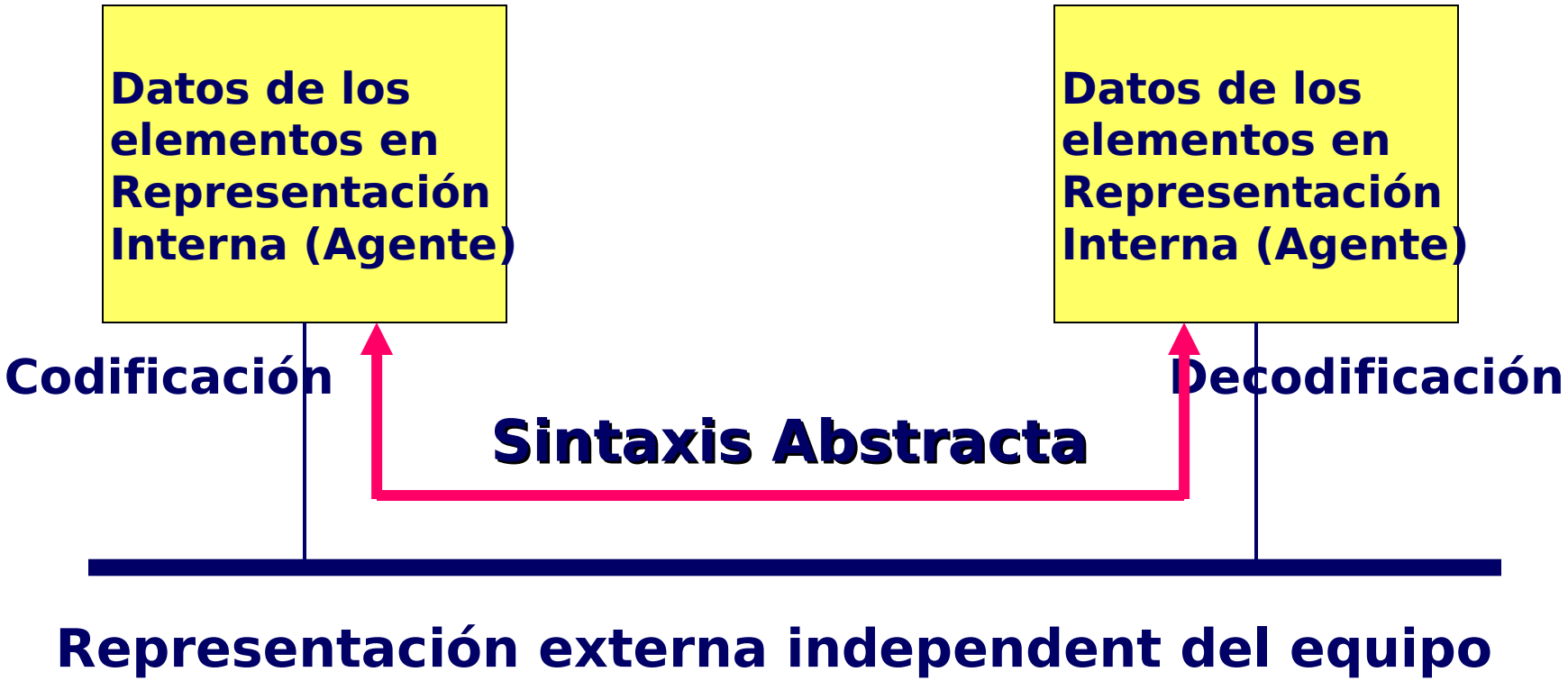
Tipos de PDUs para SNMP

- **PDU Types**
  - GetRequest-PDU
  - GetNextRequest-PDU
  - GetResponse-PDU
  - SetRequest-PDU

Tipos de PDUs para SNMP

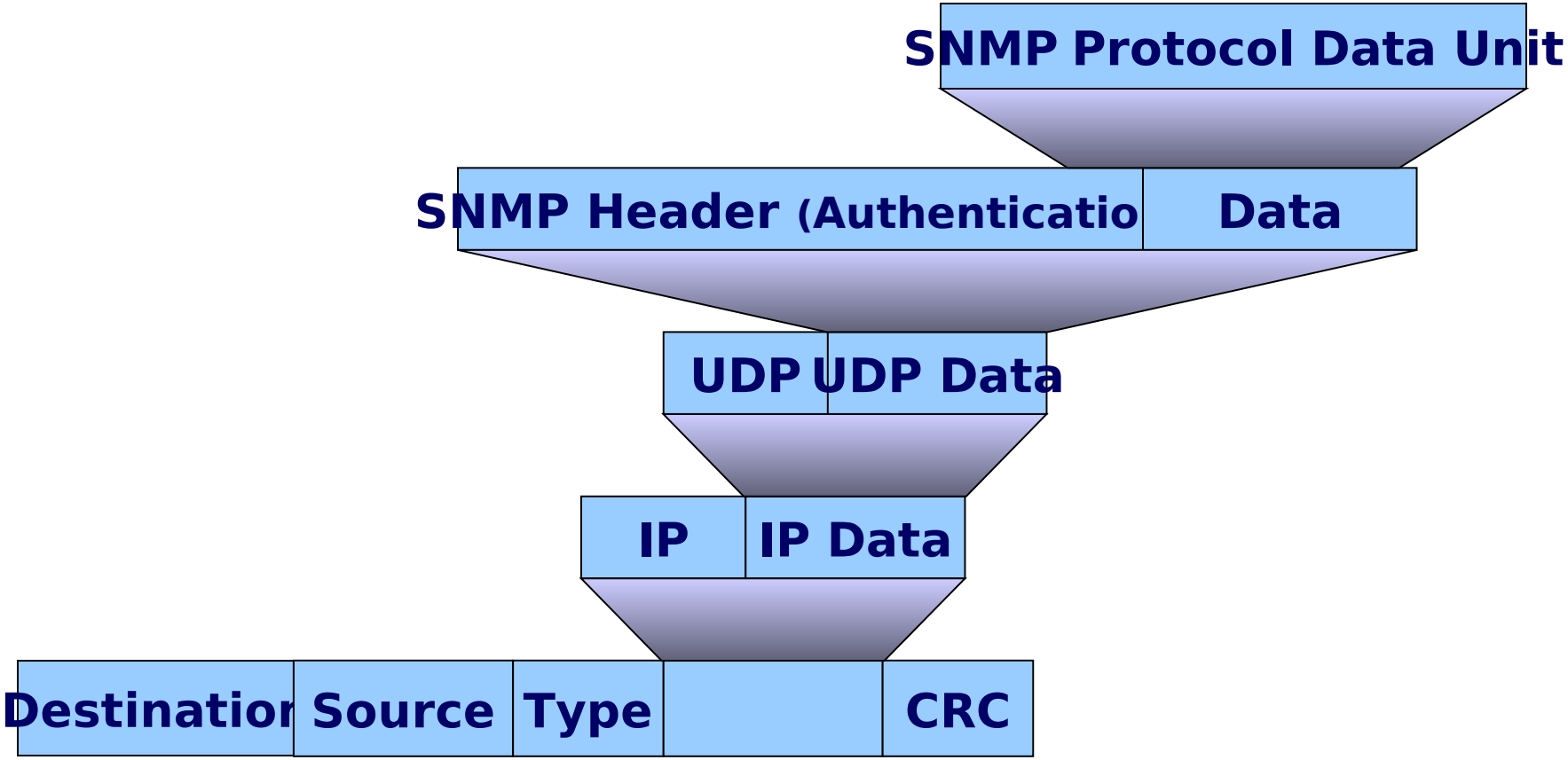
- **Trap-PDU**
  - Cold Start
  - Warm Start
  - Link Down
  - Link Up
  - Authentication Failure
  - EGP Neighbor Loss

Codificación de SNMP



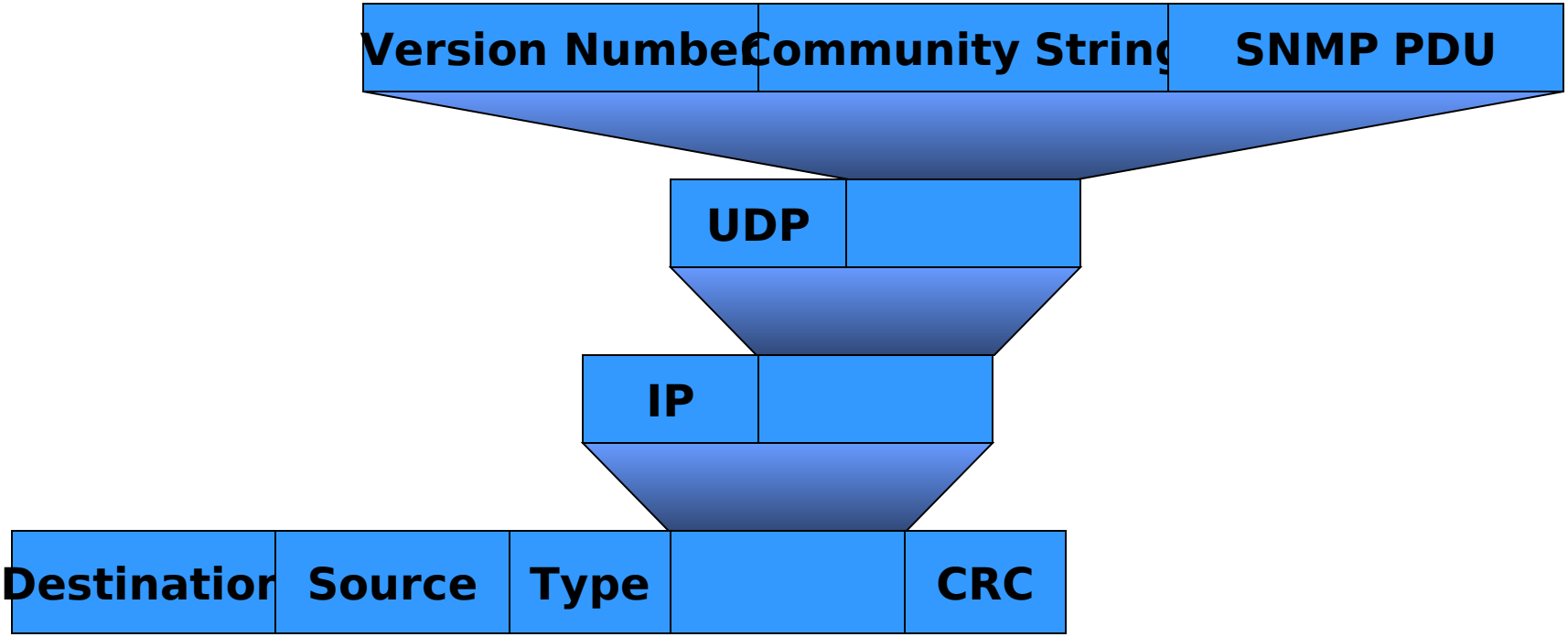
Codificación de SNMP

Encapsulación de paquetes

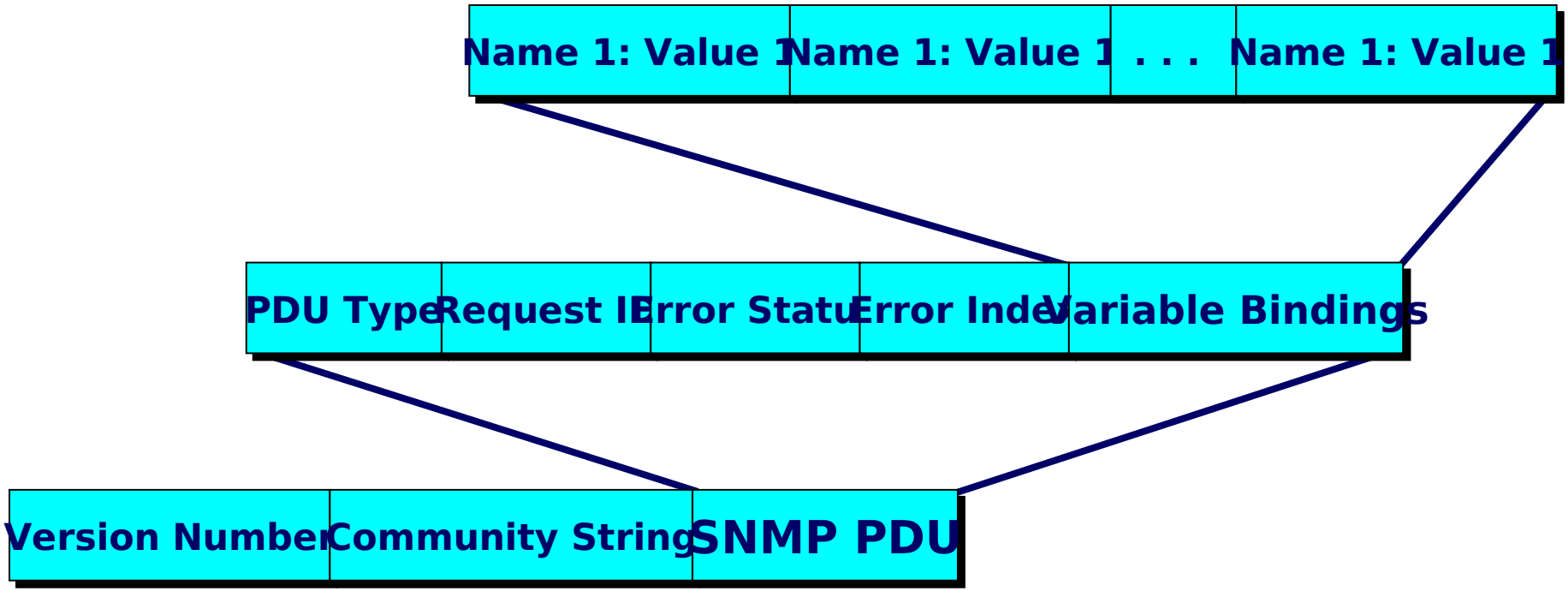


Codificación de SNMP

Formato del Mensaje



Porción del PDU del mensaje de SNMP



SNMP v2
Protocolo Simple de Gestion de Redes.

SNMP v.2

- Mejora a SNMP completamente diferente.
- Once RFC (RFC 1442 a 1452)
- No usado ampliamente
- Más capacidades, incluida seguridad
- Contempla administración para redes OSI (CMIP sobre TCP/IP).

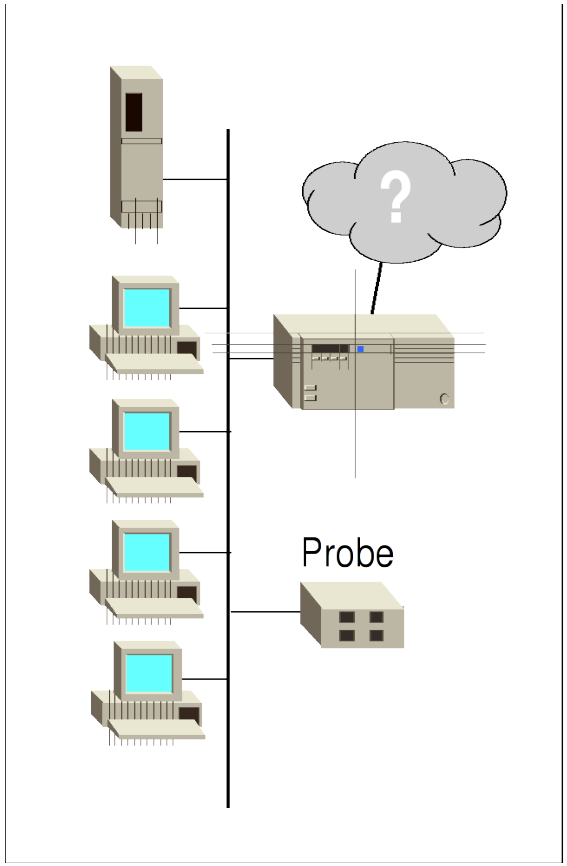
RMON
Remote MONnitoring

Estandar de RMON Probes

- El RFC 1757 define 9 grupos operacionales.
  - C/u define diferentes funciones de monitoreo
  - Contiene funciones específicas para Ethernet
- Futuros RFC contemplarán otros estándares de red

RFC1757	
Statistics	**Host**
History	**Host 'TopN'**
	Matrix
Alarms	**Filter**
Events	**Capture**

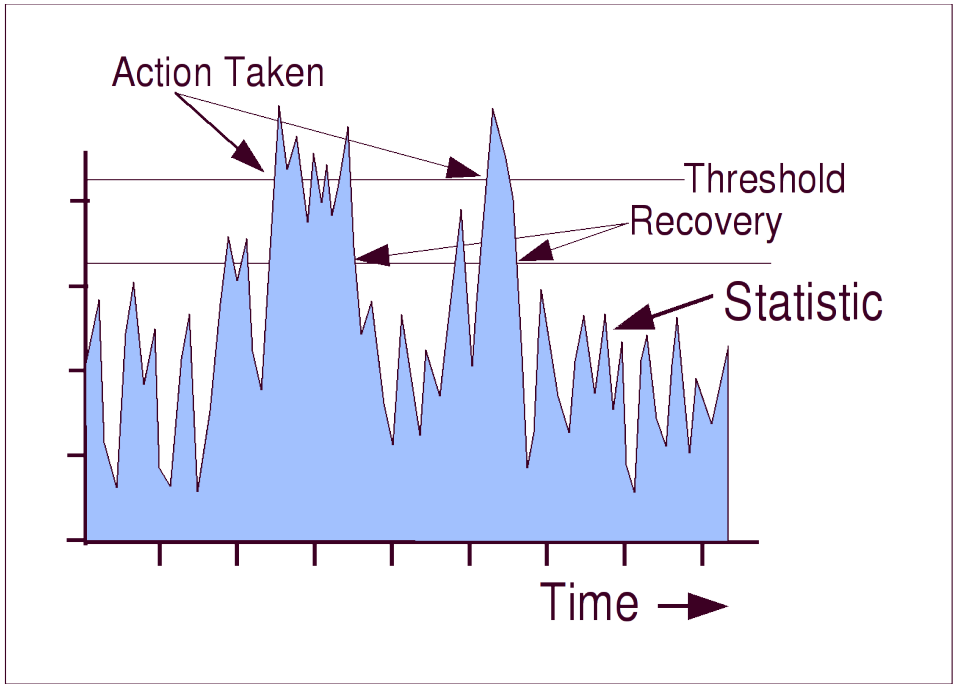
Grupos de RMON



Statistics

- Muestra estadísticas para un segmento LAN
- No contempla host
- Paquetes Totales
- Errores
- Distribución de broadcast y multicast
- Distribución de tamaños de paquete

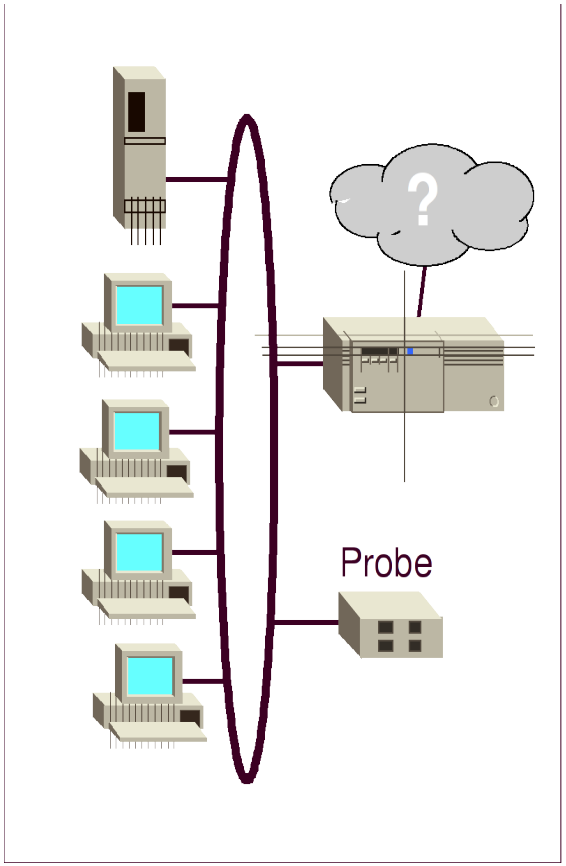
Grupos de RMON



Alarms

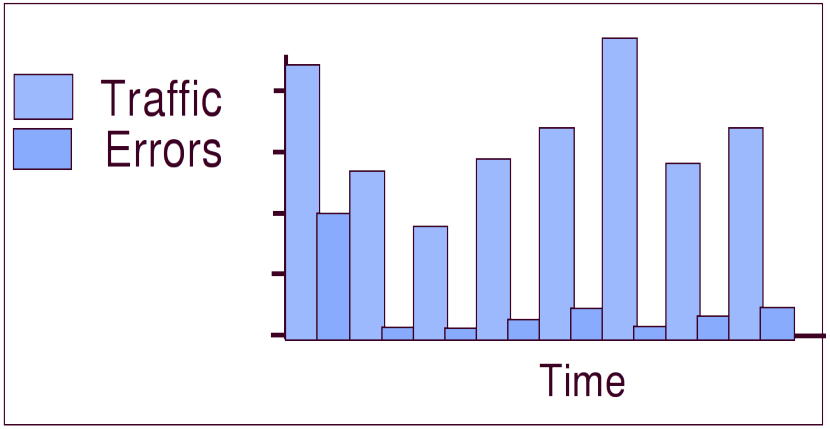
- El Agente de RMON monitorea cualquier estadística de MIBs y envía un evento interno de RMON si el humbral es rebasado.
- No se realiza ninguna acción hasta que el valor decaiga el Valor de Recuperación.

Grupos de RMON

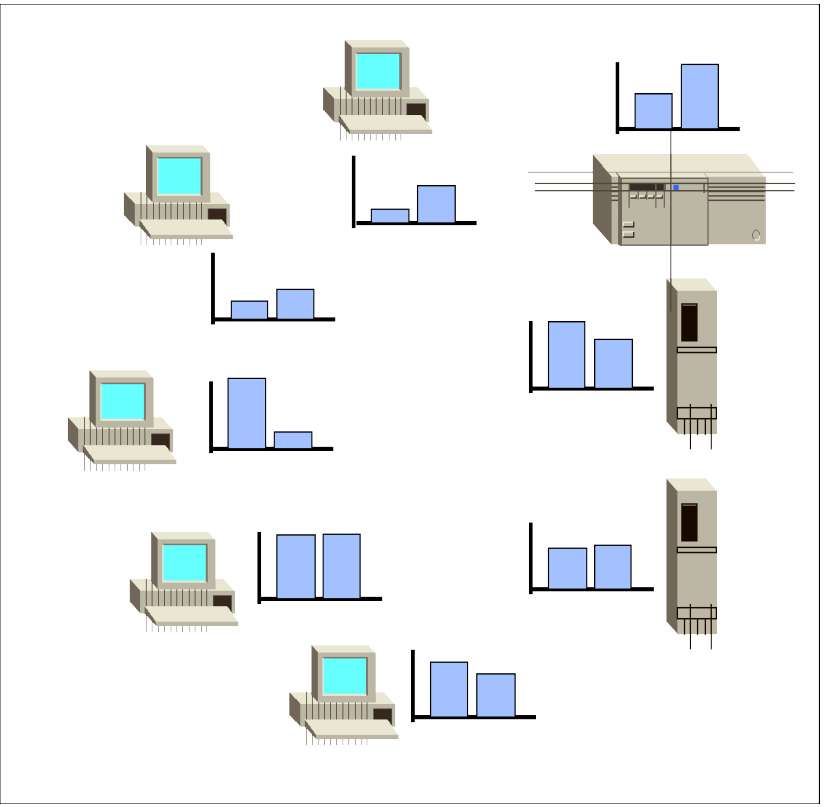


History

- Muestra estadísticas basadas en tiempo en un segmento LAN.
- No se genera tráfico de red.



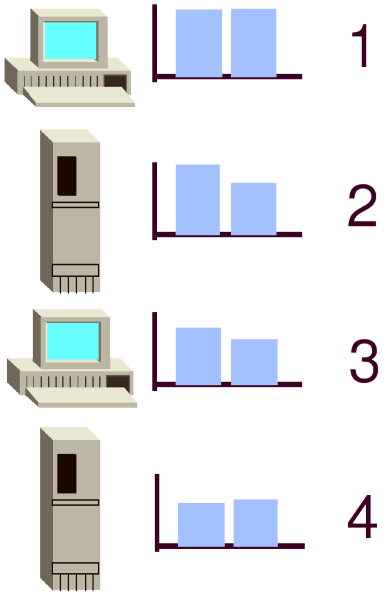
Grupos de RMON



Host

- “Quien habla?”
- Probé estadísticas basadas en direcciones MAC (no por IP).
- Muestra el número de paquetes, bytes, unicats, multicast, broadcast y errores enviados por un host.

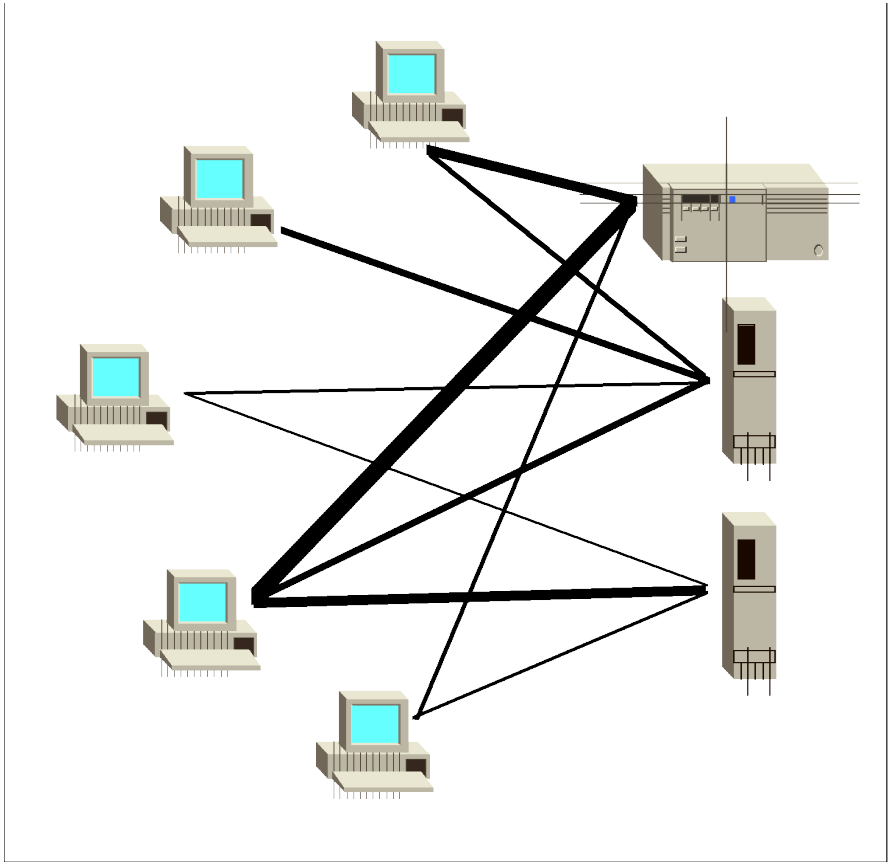
Grupos de RMON



HostTopN

- “Quien habla más?”
- Clasifica a host basado en el tráfico o errores.

Grupos de RMON

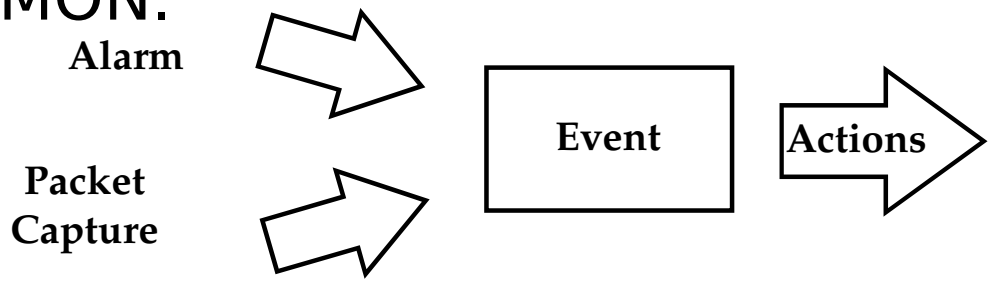


Matrix

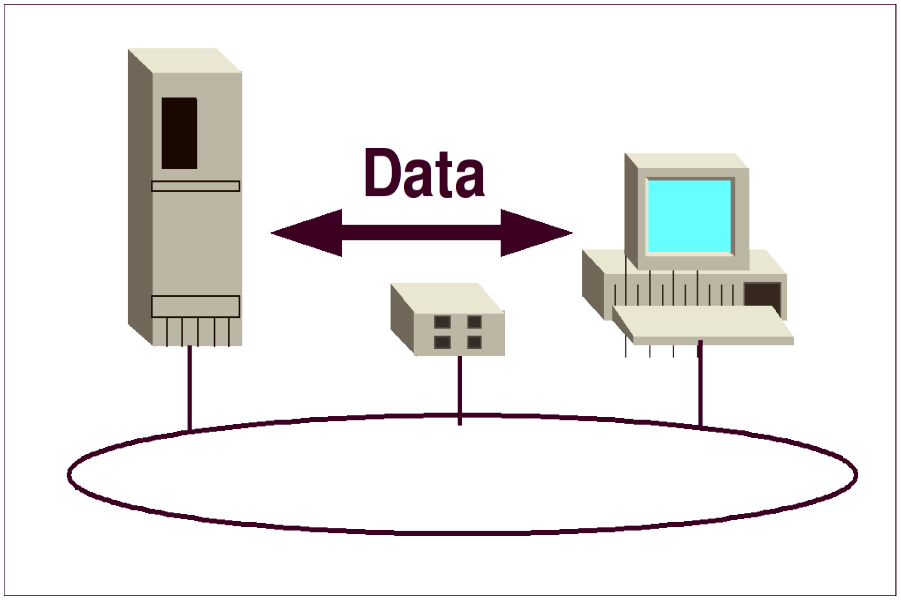
- “Quién habla a quién?”
- Probé estadísticas basadas en la comunicaciones de dos direcciones MAC.
- Ejemplo:
- Paquete enviados de uan estación A a B.

Eventos en RMON

- Algunos eventos pueden ser disparados por otros grupos de RMON. El grupo de Alarms y Packet Filter pueden disparar alarmas.
- Cuando un evento se dispara, se genera una acción dentro del dispositivo.
- Las acciones pueden incluir envia de traps de SNMP, iniciar una captura de sesión, o generar una entrada en el log de RMON.



Grupos de RMON



Filter

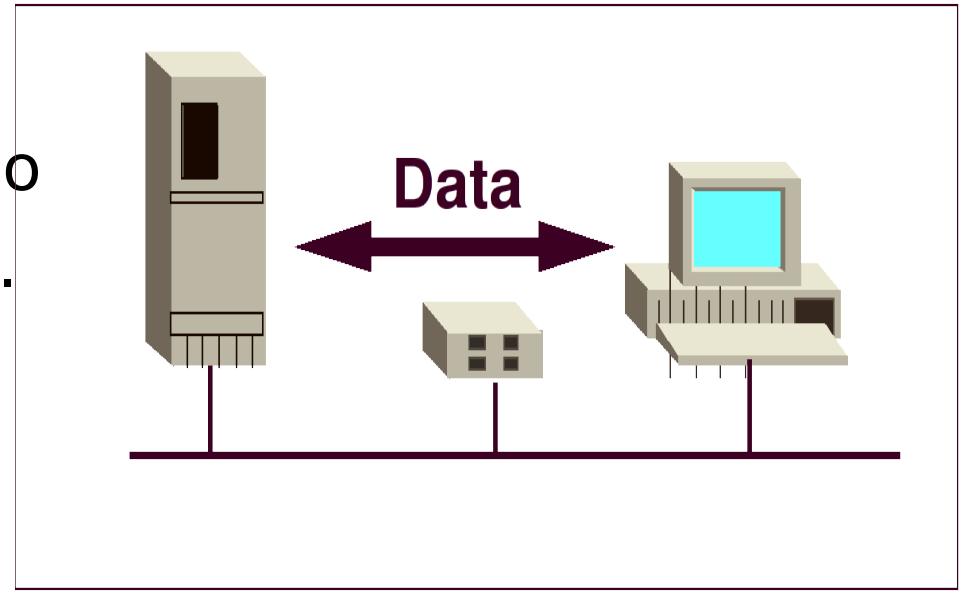
- Permite generar condiciones en contra de parámetro en un paquete (direcciones, protocolos, aplicaciones) ya sea para monitoreo o captura de paquetes.

Grupos de RMON

Packet Capture

- Captura paquetes dentro de un buffer internos de acuerdo a un *filter group.*

- Generalmente utilizado en condiciones de error.



Caso Practico: RedUNAM