

¿Qué es la Gestión de Redes?

■ Una Definición:

- “La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable”

T.Saydam and T. Magedanz, “From Networks and Network Management into Service and Service Management”, *Journal of Networks and Systems Management*, Vol 4, No. 4 (Dic 1996).

¿Qué es un NOC?

Network Operations Center (Centro de Operaciones de Red)

- Monitoriza y gestiona la red
 - Información sobre la disponibilidad actual, histórica y planeada de los sistemas.
 - Estado de la red y estadísticas de operación
 - Monitorización y gestión de fallas

Gestión de Red: Componentes

Según la ISO:

- Gestión de configuraciones/cambios
- Gestión del desempeño/contabilidad
- Gestión de fallas
- Gestión de seguridad

Gestión de Configuraciones

Mantener información relativa al diseño de la red y su configuración actual

- ¿Cómo está conectado eso?
- Pregúntale a Juan, que él sabe
- Juan se fue de vacaciones
- Había un dibujo en el pizarrón...

Gestión de Configuraciones

■ Estado actual de la red

- **Registro de la topología**
 - **Estático**
 - Qué está instalado
 - Dónde está instalado
 - Cómo está conectado
 - Quién responde por cada cosa
 - Cómo comunicarse con los responsables
 - **Dinámico**
 - Estado operacional de los elementos de la red
 - Estado de conexión de cada dispositivo de infraestructura.

Gestión de configuraciones

■ Gestión de inventario

- Base de datos de elementos de la red
- Historia de cambios y problemas

■ Mantenimiento de Directorios

- Todos los nodos y sus aplicaciones
- Base de datos de nombres de dominio

■ Coordinación del esquema de nombres para nodos y aplicaciones

- "La información no es información si no se puede encontrar"

Gestión de configuraciones

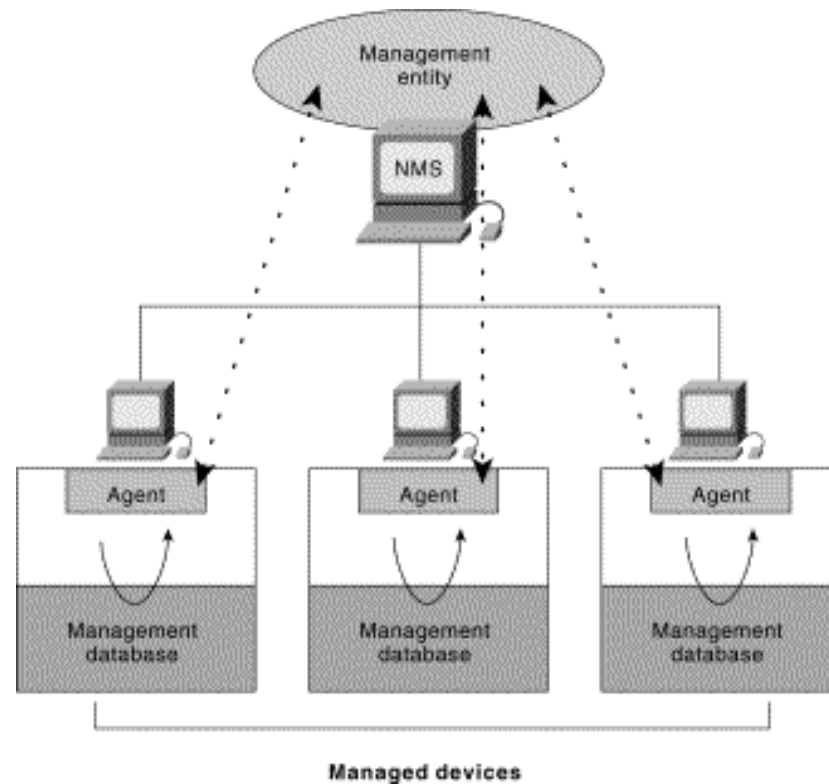
Control operacional de la red

- Iniciar/Detener componentes individuales
- Alterar la configuración de los dispositivos
- Cargar y configurar versiones de configuraciones
- Actualizaciones de Hardware/Software
- Métodos de Acceso
 - SNMP
 - Acceso fuera de banda (OOB)

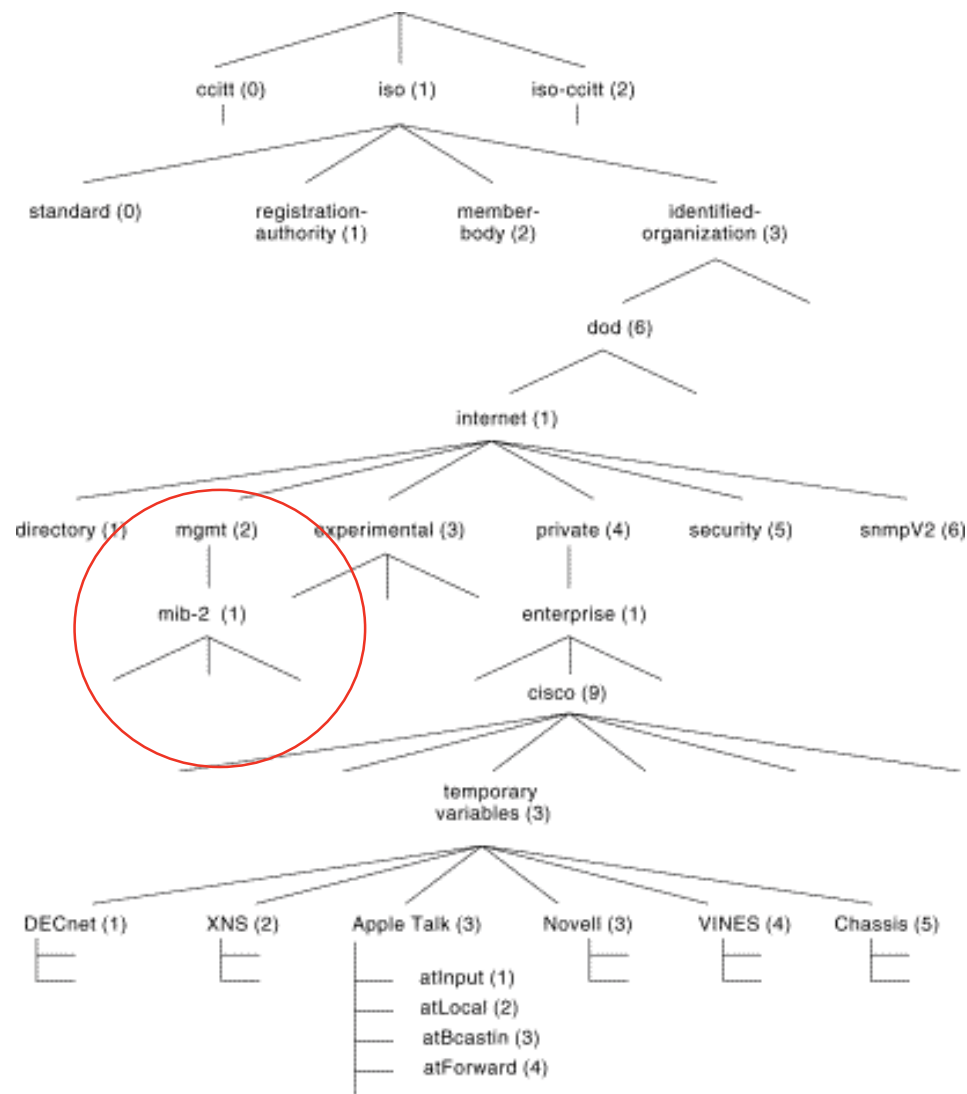
¿Qué es SNMP?

- Simple Network Management Protocol
 - (Protocolo Simple de Gestión de Red)
- Sistema tipo consulta/respuesta
 - Se puede obtener el estado de un dispositivo
 - Variables estándares
 - Variables específicas del fabricante
- Utiliza una base de datos definida en una MIB
 - Management Information Base

Componentes de SNMP



El árbol MIB



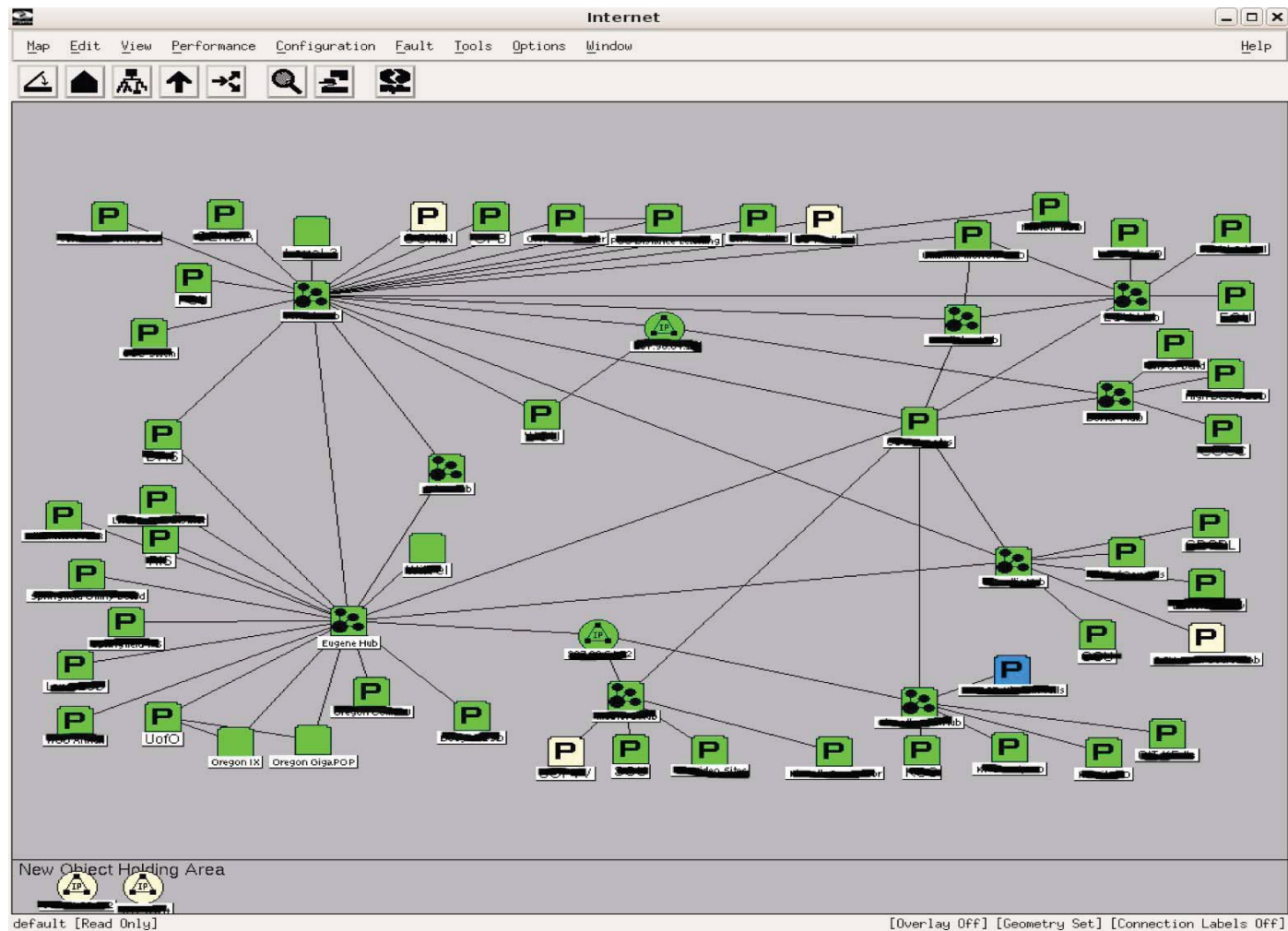
¿Para qué usamos SNMP?

- Consultar enrutadores y switches para obtener:
 - Octetos entrantes y salientes (calcular tráfico por segundo)
 - Carga del CPU
 - Memoria utilizada/disponible
 - Tiempo de operación
 - Estado de las sesiones BGP
 - Tablas de ARP
 - Tablas de reenvío

¿Para qué usamos SNMP?

- Cambiar los valores de ciertos atributos
 - Apagar/encender puertos en switches
 - Reiniciar dispositivos remotamente
- La gran ventaja es que se puede automatizar para grandes cantidades de equipos

Visualización generada usando SNMP



Gestión del Rendimiento

Garantizar unos niveles consistentes de rendimiento

■ Colección de datos

- Estadísticas de interfaces
- Tráfico
- Tasas de error
- Utilización
- Disponibilidad porcentual

■ Análisis de datos para mediciones y pronósticos

■ Establecimiento de niveles límite de rendimiento

■ Planificación de la capacidad e instalaciones

Importancia de las estadísticas de red

- Contabilidad
- Resolución de problemas
- Pronósticos a largo plazo
- Planificación de Capacidad
- Dos tipos diferentes
 - Mediciones activas
 - Mediciones pasivas
- Las herramientas de gestión suelen tener funcionalidad estadísticas

Gestión de contabilidad

■ ¿Qué necesita contabilizar?

- La utilización de la red y los servicios que provee

■ Tipos de datos de contabilidad

- RADIUS/TACACS: Datos de contabilidad de servidores de acceso
- Estadísticas de interfaces
- Estadísticas de protocolos

■ Los datos de contabilidad afectan los modelos de negocio

- ¿Facturar la utilización?
- ¿Facturar tarifa plana?

Gestión de fallas

■ Identificación de la falla

- Sondeo regular de los elementos de la red

■ Aislar la falla

- Diagnóstico de los componentes de la red

■ Reaccionar ante la falla

- Asignación de recursos para resolver fallas
- Determinación de prioridades
- Escalada técnica y de gestión

■ Resolver la falla

- Notificación

Sistemas de gestión de fallas

- Mecanismos de reporte
 - Enlace al NOC
 - Notificación del personal de guardia
- Instalación y control de procedimientos de alarmas
- Procedimientos de reparación/recuperación
- Sistema de manejo de incidencias (ticketing system)

Detección y Gestión de Fallas

¿Quién se da cuenta de un problema en la red?

- NOC con personal 24x7
 - Abrir una incidencia para dar seguimiento al problema
 - Soluciones básicas preliminares
 - Asignar un ingeniero al caso o escalar la incidencia
- Otros operadores de red
- Llamada de Cliente (¡mejor que no!)

Detección y Gestión de Fallas

¿Cómo saber si hay un problema en la red?

- Herramientas de monitorización
 - Utilidades Comunes
 - ping
 - Traceroute
 - Ethereal/Wireshark
 - Snmp
 - Sistemas de Monitorización
 - HP Openview, etc...
 - Nagios
 - Big Brother
- Reportes de estado
 - Separar lo que son:
 - Nodos no-operativos (down)
 - Nodos no alcanzables (unreachable)

Gestión de Fallas: Sistema de Incidencias

- ¡Muy importante!
- Se necesita un mecanismo para dar seguimiento a:
 - Estado actual de la falla
 - Personal asignado
 - Tiempo estimado de solución
 - Tiempo trabajado (si se va a cobrar)
 - Historia de las acciones

Gestión de Fallas: Sistema de Incidencias

■ El sistema provee:

- Programación y asignación de tareas
- Registro de la comunicación
- Remisiones y despachos
- Supervisión
- Análisis estadístico
- Responsabilidades (quién hizo qué)

Gestión de fallas: Utilización de una incidencia

- Crear una incidencia para todas las llamadas
- Crear una incidencia para todos los problemas
- Crear una incidencia para todos los eventos programados (mantenimiento)
- Enviar una copia de la incidencia al que reporta y a una lista de correo
- Todas las acciones en la vida de una incidencia mantienen el mismo número
- La incidencia está “abierta” hasta que se resuelve.
- El que reporta el problema determina cuándo debe ser cerrada la incidencia

Gestión de Seguridad

- Controlar acceso a los recursos de la red de acuerdo a unas políticas bien definidas
 - Uso periódico de herramientas para analizar y controlar el uso legítimo de la red
 - Distribución de certificados