

Introducción a la Gestión de Redes

Carlos Vicente

Universidad de Oregon

Presentado por José A. Domínguez

¿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

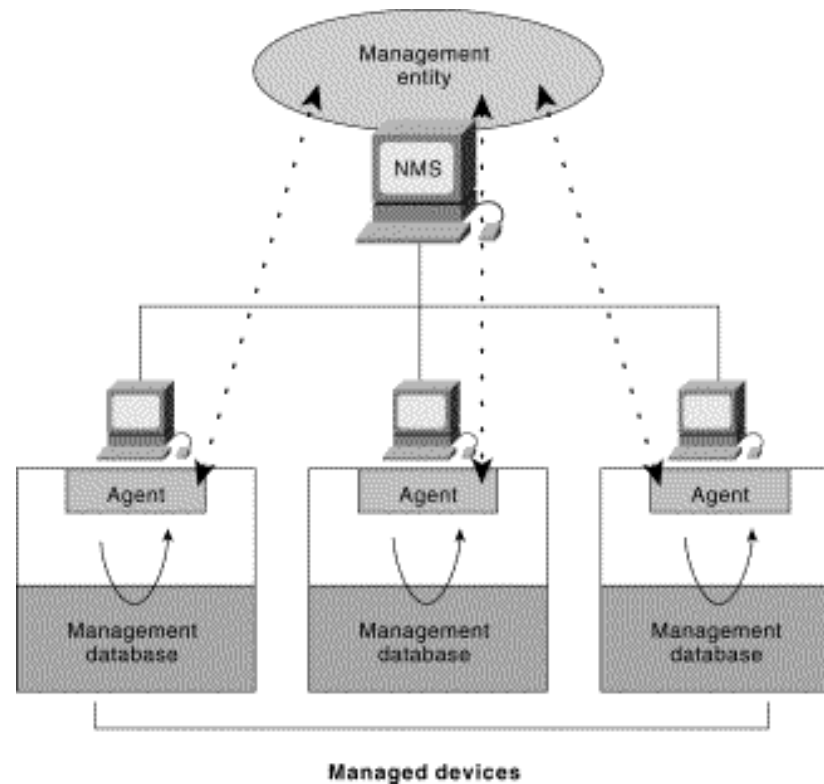
Control operacional de la red

- 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)

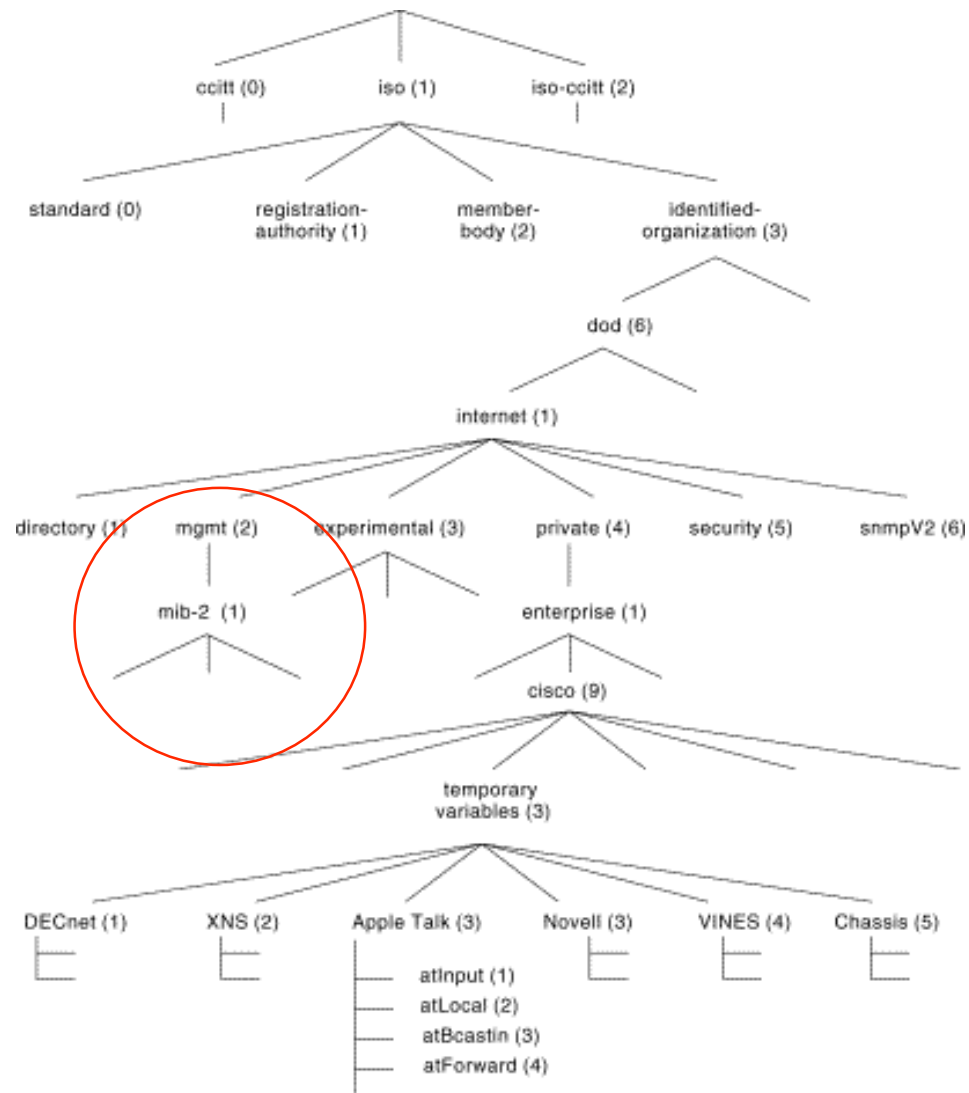
¿Qué es SNMP?

- 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?

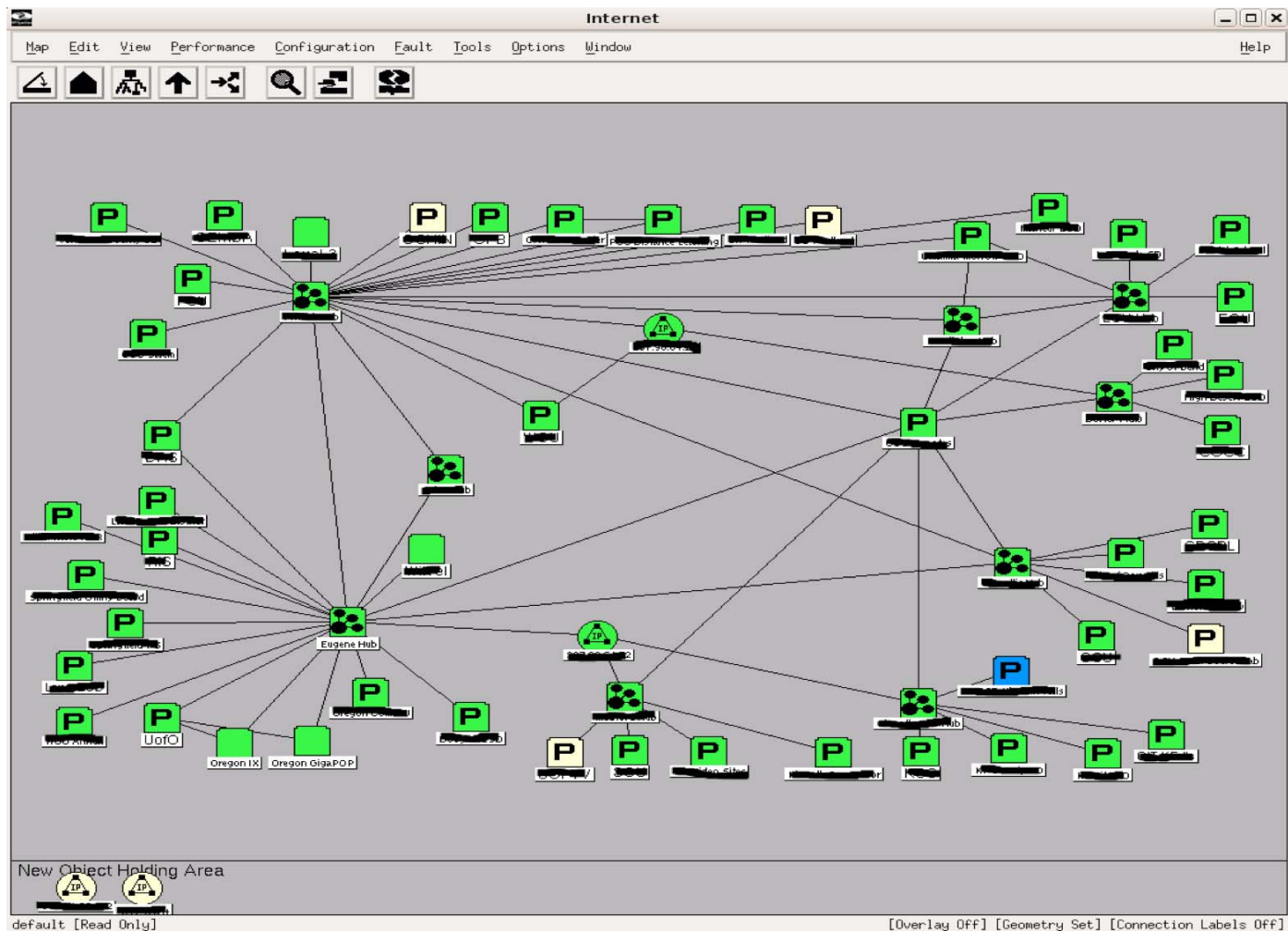
- Consultar enrutadores y switches para obtener:
 - Octetos entrantes y salientes (calcular tráfico por segundo)
 - Carga del CPU
 - Memoria utilizada/disponible
 - Tiempo de operación
 - Estado de las sesiones BGP
 - Tablas de ARP
 - Tablas de reenvío

¿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

Gestión de la configuración

Visualización generada usando SNMP



Gestión de Configuraciones: Herramientas

- Para controlar/gestionar las versiones de las configuraciones
 - CiscoWorks (cuesta \$\$\$)
 - NetMRI (<http://www.netcordia.com>)
 - RANCID (<http://www.shrubbery.net/rancid>)
 - Utiliza CVS (o SubVersion) para mantener un repositorio con registro de cada cambio
 - Funciona con las marcas de equipos más conocidas
 - Puede utilizarse con un *front-end* web
 - <http://www.freebsd.org/projects/cvsweb.html>

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

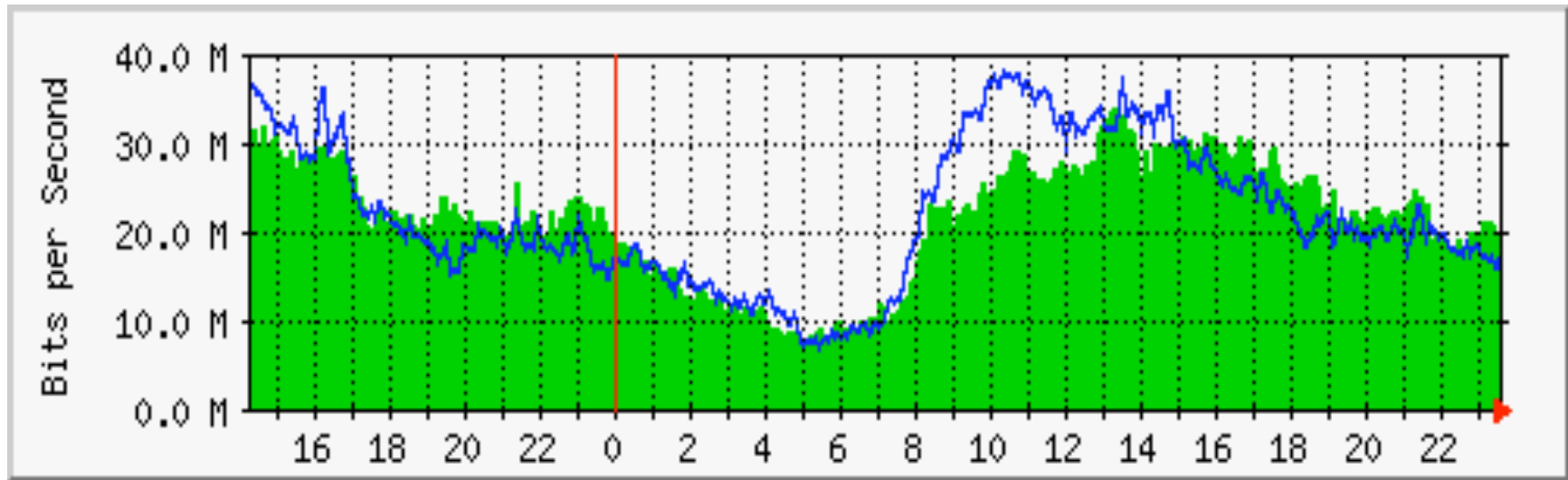
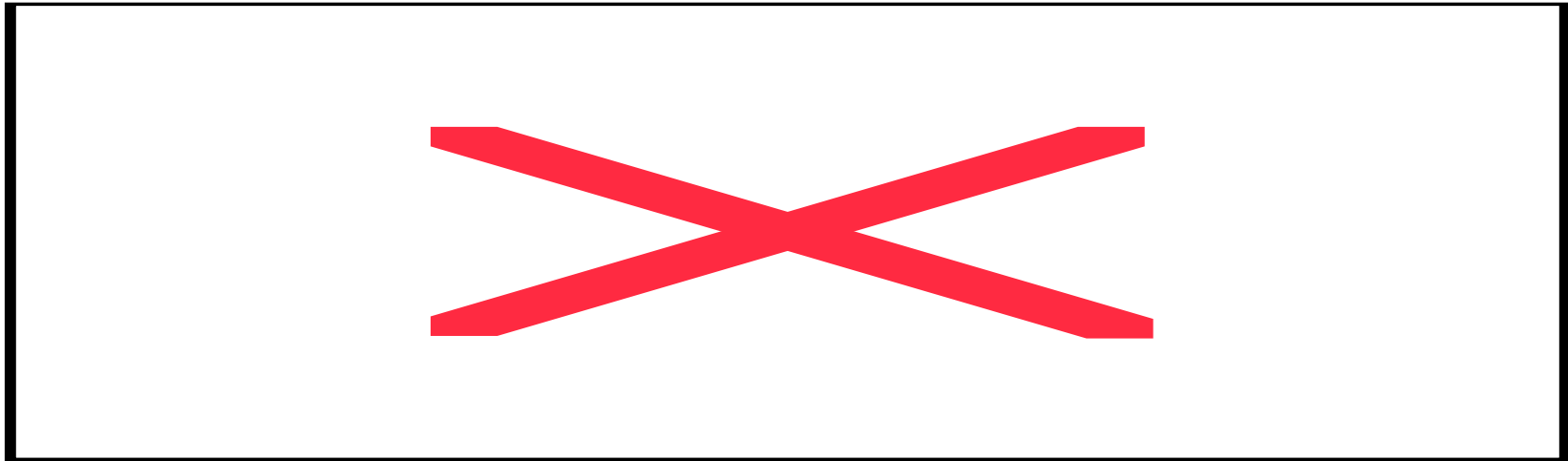
■ Establecimiento de niveles límite de rendimiento

■ 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

MRTG



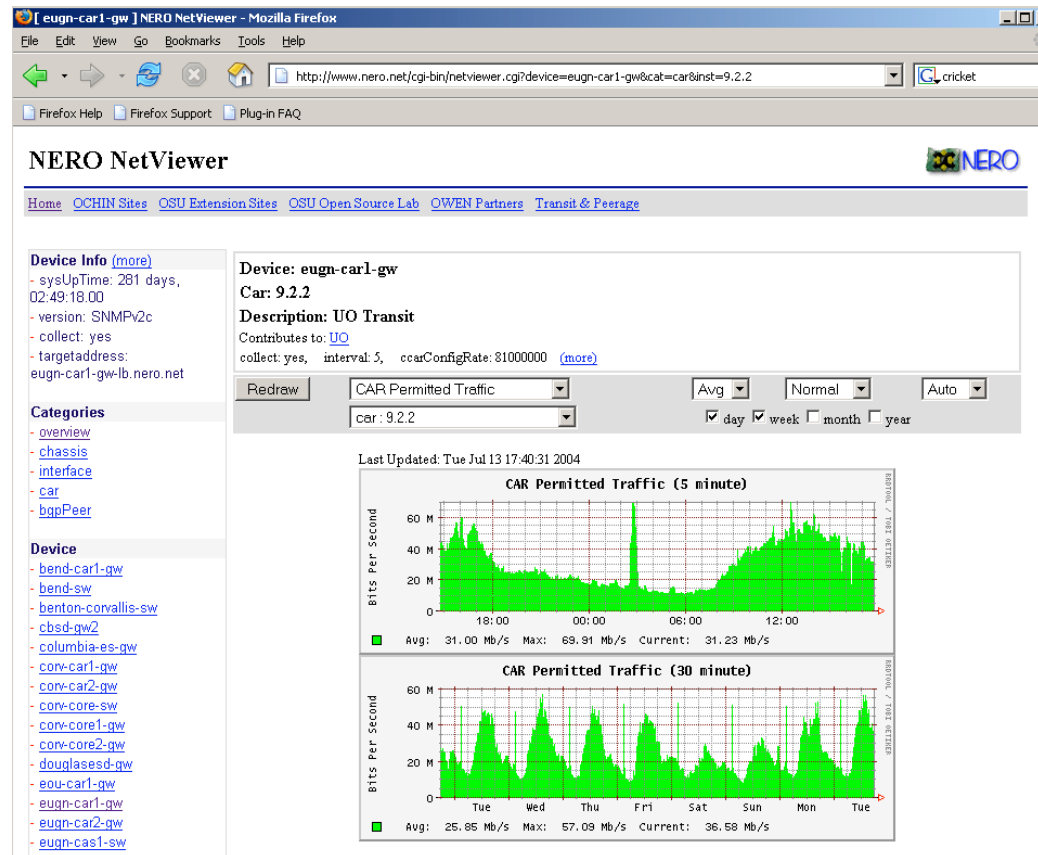
RRD

■ Round Robin Database

- Creado por el mismo autor de MRTG
- Optimizado para más flexibilidad, granularidad y control del espacio de almacenamiento requerido
- Es dos cosas:
 - El formato de la base de datos
 - Herramientas básicas para manipular la BD
- Necesita un *front-end*
 - Colección de datos
 - Presentación de la información

Herramientas de gestión del rendimiento

- Cricket (cricket.sourceforge.net)
- Netviewer (www.nero.net/projects/netviewer)
- Cacti (www.cacti.net)



Herramientas de gestión del rendimiento

■ Netflow

(cflowd, Flow-Tools, Flowscan, FlowViewer)

Reunen y presentan información de flujos de tráfico

- Información de AS a AS
- Información agrupada en dirección y puerto de origen y destino
- Útil para contabilidad y estadísticas
 - ¿Cuánto de mi tráfico es puerto 80?
 - ¿Cuánto de mi tráfico va a AS237?

Ejemplos de Netflow

■ Listas tipo *Top-Ten* (o *top-five*)

```
##### Top 5 AS's based on number of bytes #####
srcAS  dstAS          pkts          bytes
 6461  237             4473872      3808572766
   237  237             22977795     3180337999
 3549  237             6457673      2816009078
 2548  237             5215912      2457515319
```

```
##### Top 5 Nets based on number of bytes #####
```

```
Net Matrix
```

```
-----
```

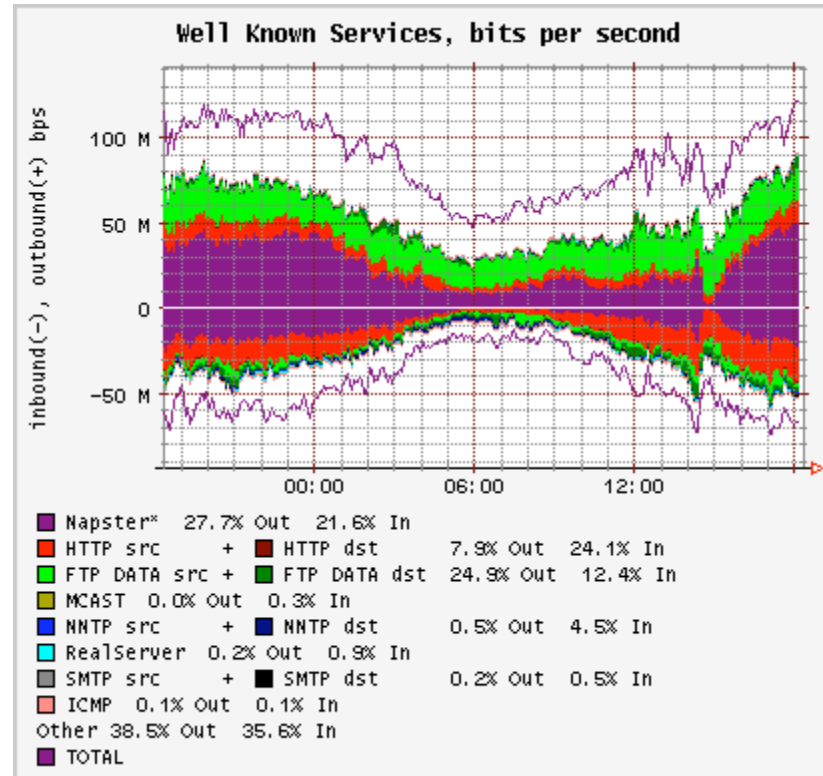
```
number of net entries: 931777
```

SRCNET/MASK	DSTNET/MASK	PKTS	BYTES
165.123.0.0/16	35.8.0.0/13	745858	1036296098
207.126.96.0/19	198.108.98.0/24	708205	907577874
206.183.224.0/19	198.108.16.0/22	740218	861538792
35.8.0.0/13	128.32.0.0/16	671980	467274801

```
##### Top 10 Ports #####
```

port	input		output	
	packets	bytes	packets	bytes
119	10863322	2808194019	5712783	427304556
80	36073210	862839291	17312202	1387817094
20	1079075	1100961902	614910	62754268
7648	1146864	419882753	1147081	414663212
25	1532439	97294492	2158042	722584770

Flowscan



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
 - Diagnósis 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

Gestión de Seguridad: Herramientas

- Herramientas de Seguridad
 - Sondeo de vulnerabilidades
 - Nessus (www.nessus.org)
 - Análisis de bitácoras (logs)
 - swatch – reportes via e-mail
 - Filtros de Servicios
 - iptables, tcpwrappers
 - Cifrado
 - SSH – cifrado de sesiones interactivas
 - Revisión de Integridad
 - Tripwire – monitoriza cambios en los archivos
- Mantenerse al día con la información de seguridad
 - Reportes de “bugs”
 - CERT
 - BugTraq
 - Mantener software en últimas versiones

Gestión de Seguridad: Prácticas recomendadas

- Proveer puntos de contacto fáciles
 - Dirección de “abuso” para quejas de clientes
 - (abuse@su-dominio.net)
 - Teléfonos bien conocidos y accesibles
 - Asignar tiempos “de guardia” por turnos, por ejemplo
 - Definir políticas de acción a priori
- Gestión de *logs*
 - Un nodo centralizado para recibir *logs*
 - Escribir herramientas simples para encontrar información rápidamente
 - Interfaces web
 - Comandos para simplificar filtrado

¿Cómo gestiono mi red?

- ¿Qué herramientas usar? ¿Qué necesito realmente?
 - **¡Mantener lo más simple posible!**
 - No gastar demasiado tiempo desarrollando las herramientas (¡Se supone que son para ayudarle a usted!)
 - Hacer uso de herramientas disponibles en
 - SourceForge.net
 - FreshMeat.net
 - Automatizar las tareas

Herramientas *Looking Glass*

- <http://www.nanog.org/lookingglass.html>

```
route-views.oregon-ix.net>show ip bgp 35.0.0.0
BGP routing table entry for 35.0.0.0/8, version 56135569
Paths: (17 available, best #12)
 11537 237
   198.32.8.252 from 198.32.8.252
     Origin incomplete, localpref 100, valid, external
     Community: 11537:900 11537:950
 2914 5696 237
   129.250.0.3 (inaccessible) from 129.250.0.3
     Origin IGP, metric 0, localpref 100, valid, external
     Community: 2914:420
 2914 5696 237
   129.250.0.1 (inaccessible) from 129.250.0.1
     Origin IGP, metric 0, localpref 100, valid, external
     Community: 2914:420
 3561 237 237 237
   204.70.4.89 from 204.70.4.89
     Origin IGP, localpref 100, valid, external
 267 1225 237
   204.42.253.253 from 204.42.253.253
     Origin IGP, localpref 100, valid, external
     Community: 267:1225 1225:237
```

Enlaces

- <http://www.nanog.org>
- <http://www.caida.org>
- <http://www.nlanr.net>
- <http://www.cisco.com>
- <http://www.amazing.com/internet/>
- <http://www.isp-resource.com/>
- <http://www.ripe.net>