Introducción a la Gestión de Redes

Hervey Allen/NSRC

Carlos Armas/Roundtrip Networks Corp.

Con materiales de:

Carlos Vicente/José Domínguez

Universidad de Oregón

Introducción a la Gestión de Redes

Preparado con materiales de:

Carlos Vicente/
University of Oregon

Hervey Allen
hervey@nsrc.org

Carlos Armas
carmas@roundtripnetworks.com

¿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 monitorear, 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).

Estándares para la Gestión de Redes

- Una red tiene poco valor a largo plazo si esta no es administrada correctamente
- Uno de los problemas principales a resolver es la provisión de soluciones de gestión propietarias (no estándar) de vendedores
- La estandarización permite que equipos de diferentes vendedores puedan ser administrados por un solo agente de gestión.

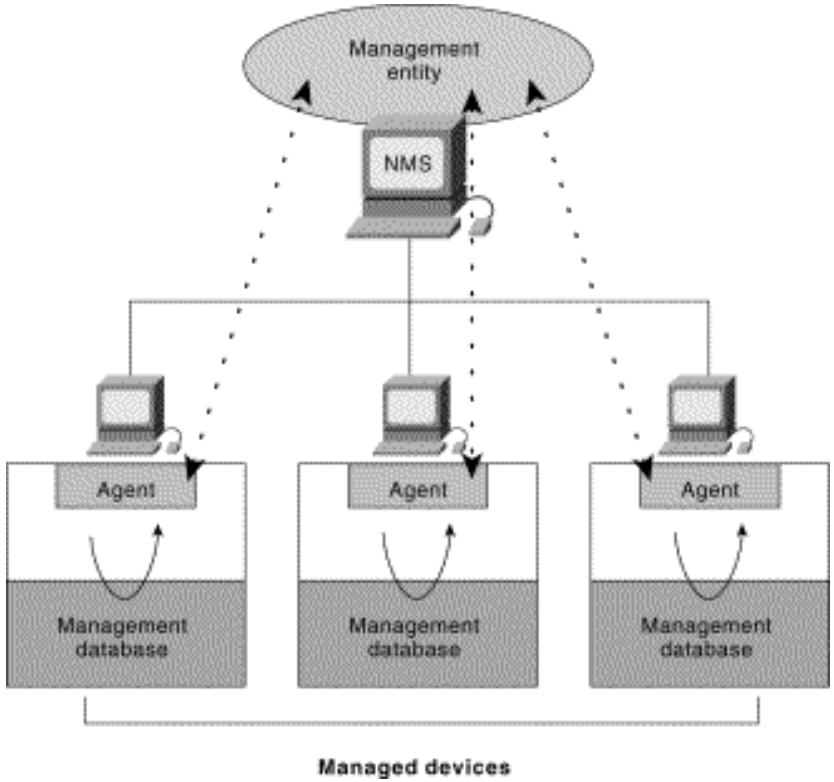
Elementos de la Gestión de Redes

- Agente
  - Reporta el estado de los elementos de redes que están siendo administrados
  - Recibe comandos del Sistema de Gestión de Redes (NMS)
- Sistema de Gestión de Redes (NMS)
  - Dirige las operaciones de los agentes
- Base de Datos de Información de Gestión (MIB)
  - Base de datos compartida entre los agentes y el NMS que provee información sobre los elementos de redes

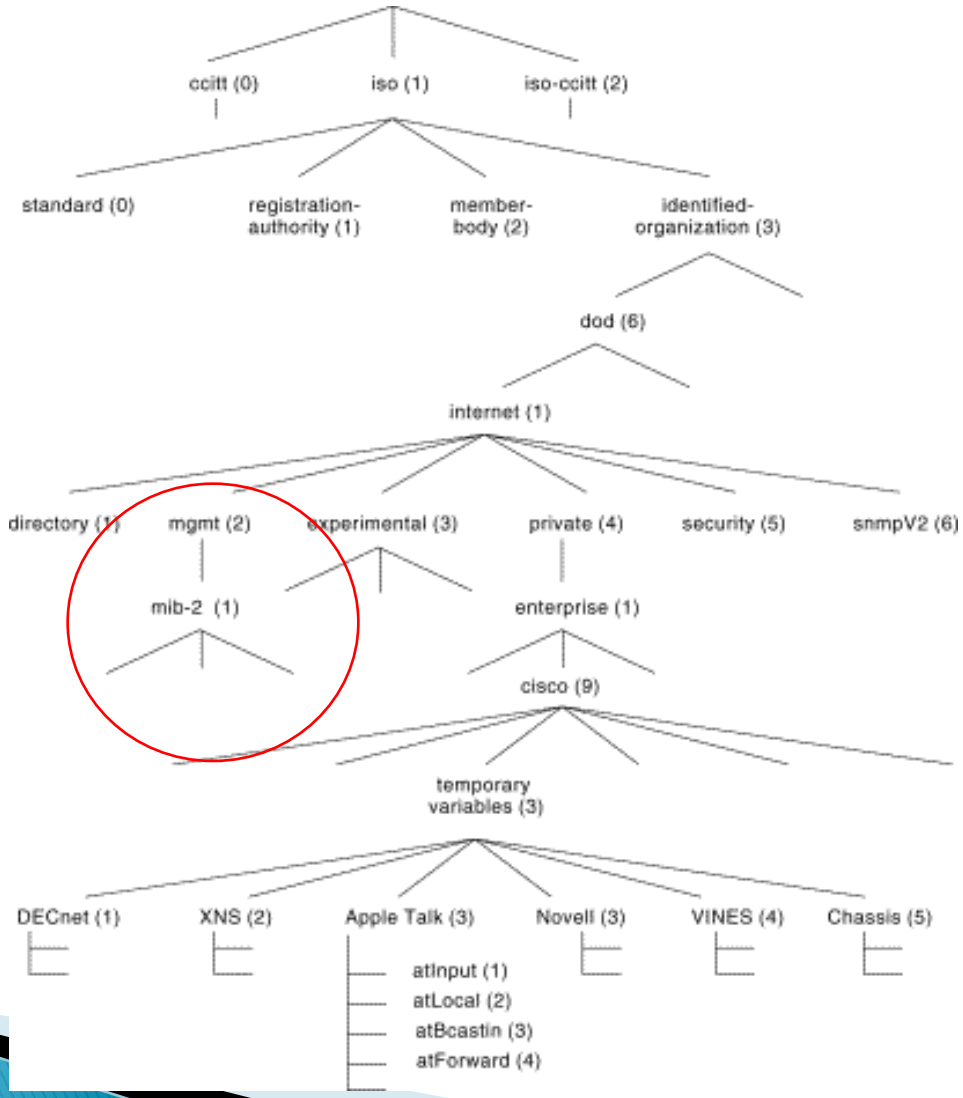
¿Qué es SNMP?

- Simple Network Management Protocol
  - (Protocolo Simple de Gestión de Red)
- Sistema tipo consulta/respuesta
  - Se puede obtener el estado de un dispositivo
    - Con variables estándares
    - Con variables específicas del fabricante
- Utiliza bases de datos definidas en MIBs

Componentes de SNMP



El árbol MIB


ccitt (0)
iso (1)
iso-ccitt (2)
standard (0)
registration-authority (1)
member-body (2)
identified-organization (3)
dod (6)
internet (1)
directory (1)
mgmt (2)
experimental (3)
private (4)
security (5)
snmpV2 (6)
mib-2 (1)
enterprise (1)
cisco (9)
temporary variables (3)
DECnet (1)
XNS (2)
Apple Talk (3)
Novell (3)
VINES (4)
Chassis (5)
atInput (1)
atLocal (2)
atBcastin (3)
atForward (4)

¿Para qué usamos SNMP?

Consultar enrutadores y switches para obtener, entre otras muchas variables:

- Tráfico por unidad de tiempo
- Carga de trabajo del CPU
- Memoria utilizada y disponible
- Por cuanto tiempo el equipo ha estado en operación
- Estado de las sesiones BGP
- Tablas de resolución de direcciones (ARP)
- Tablas de reenvío

¿Para qué usamos SNMP?

- Cambiar los valores de ciertos atributos
  - Habilitar/deshabilitar puertos en switches
  - Reiniciar dispositivos remotamente
  - Cambiar el valor de una variable de configuración

- En esencia: permite automatizar en masa el monitoreo y administración de equipos de red

¿Qué es un NOC?

Network Operations Center
(Centro de Operaciones de Red)

- Centro desde donde se monitorea y administra la red
  - Información sobre la disponibilidad actual, histórica y planeada de los sistemas.
  - Estado de la red y estadísticas de operación
  - Monitoreo y gestión de fallas

Gestión de Redes: Diferentes Tipos

Según la ISO:

- Gestión de configuraciones/cambios
- Gestión de rendimiento
- Gestión de fallas
- Gestión de contabilidad
- Gestión de seguridad

Gestión de Configuraciones

Controlar el estado de las configuraciones lógicas y físicas de dispositivos de la red, ademas de detectar cambios

Gestión de Configuraciones

- Estado actual de la red
  - **Registro de la topología**
    - **Estático**
      - **Qué está instalado**
      - **Dónde está instalado**
      - **Cómo está conectado**
      - **Quién es responsable por cada dispositivo**
      - **Cómo contactar a los responsables**
    - **Dinámico**
      - **Estado operacional de los elementos de la red**

Gestión de configuraciones

- Gestión de inventario
  - Base de datos de elementos de la red
  - Historia de cambios e incidentes (problemas)
- Mantenimiento de Directorios
  - 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

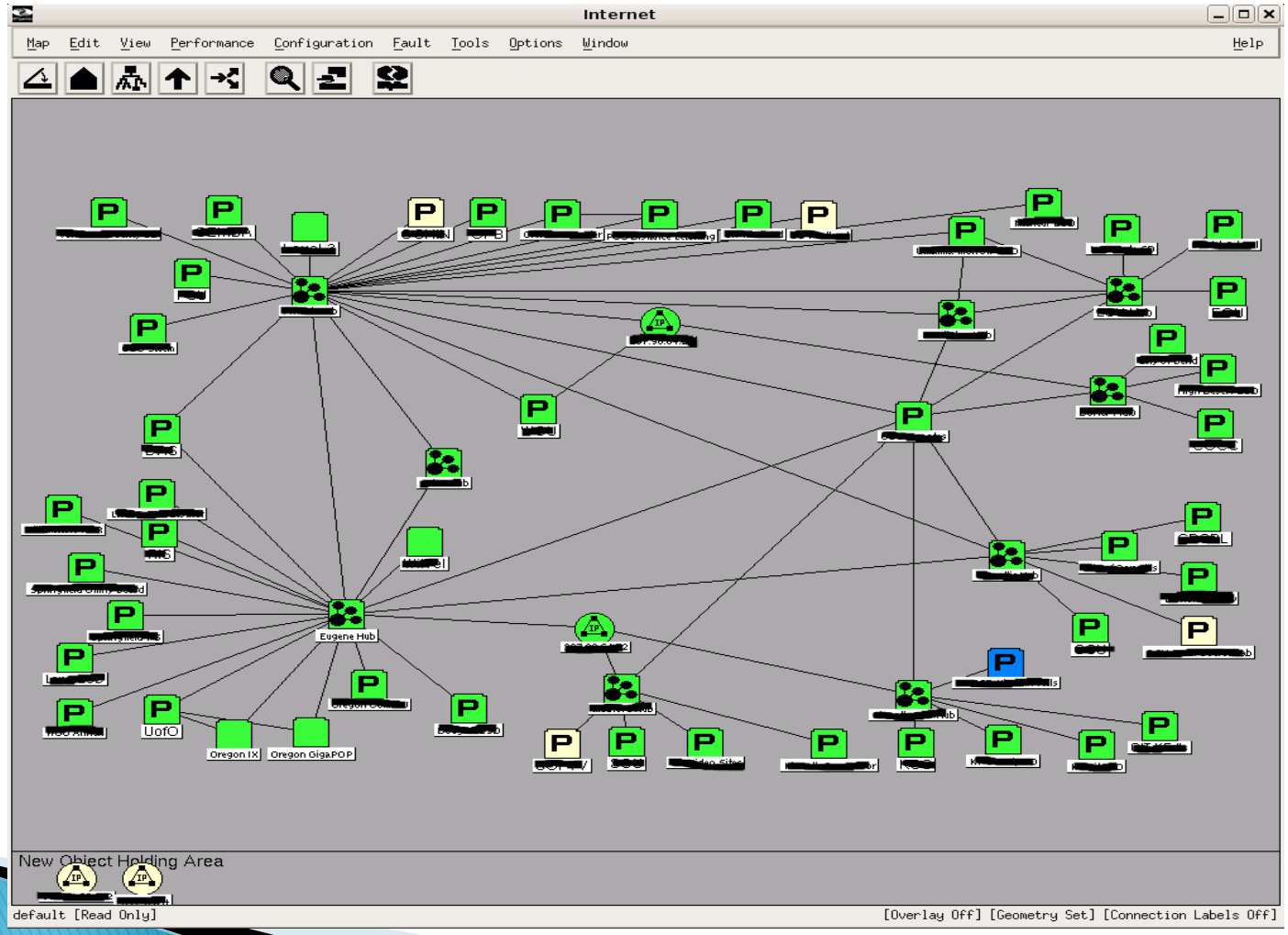
Control operacional de la red

- Iniciar/Detener componentes
- 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)

Gestión de Configuraciones

Visualización generada via SNMP



Gestión de Configuraciones

Herramientas para controlar y administrar configuraciones de equipos

- *CiscoWorks*
  - Paquete comercial costoso
  - Solamente soporta equipamiento de marca Cisco

- *RANCID* (http://www.shrubbery.net/rancid)
  - Utiliza Subversion o CVS para mantener un repositorio con registros 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

Objetivo: Garantizar un nivel de rendimiento consistente

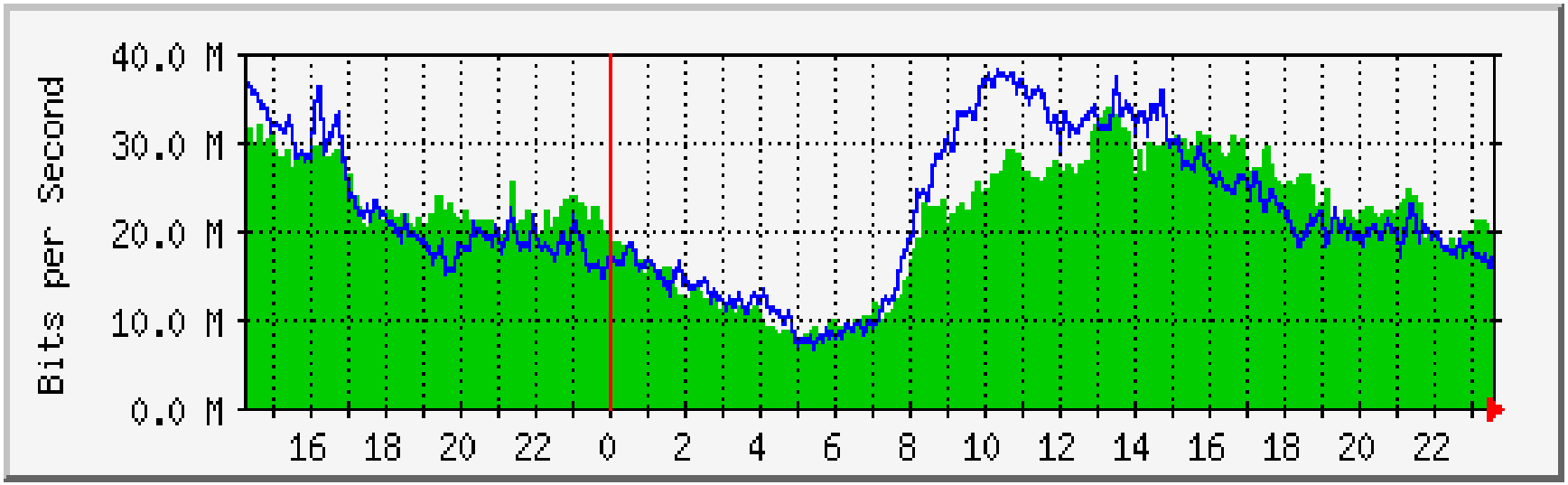
- Colección de datos
  - Estadísticas de interfaces
  - Tráfico
  - Tasas de error
  - Utilización del canal y/o dispositivo
  - Disponibilidad
- Análisis de datos para mediciones y pronósticos
- Establecimiento de niveles límite de rendimiento
- Planificación de la capacidad e instalaciones

Importancia de las estadísticas de red

- Para qué colectar estadísticas?
  - Contabilidad
  - Resolución de problemas
  - Pronósticos a largo plazo, y planificación de capacidad
- Tipos de mediciones:
  - Activas
  - Pasivas
- Las herramientas de gestión suelen tener funciones de análisis estadístico

MRTG

Herramienta de colección y visualización de tráfico

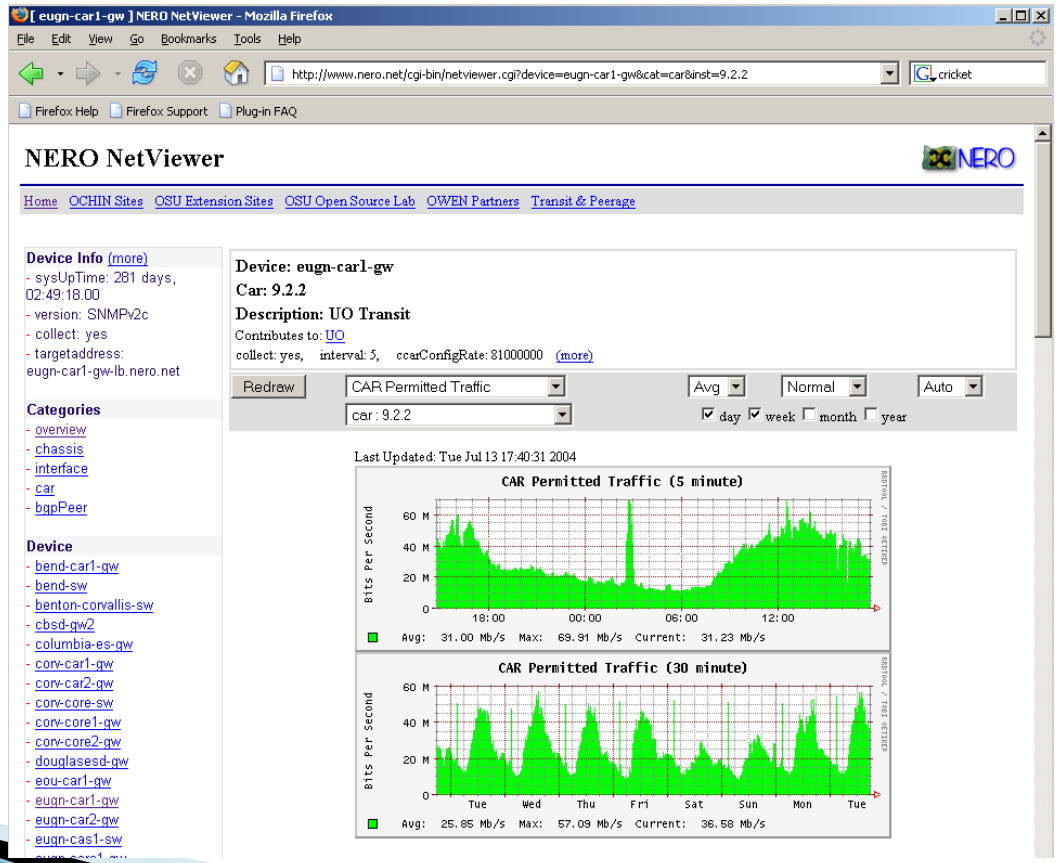


RRD

- Round Robin Database
  - Creado por el mismo autor de MRTG
  - Optimizado para más flexibilidad, granularidad y control del espacio de almacenamiento requerido
  - Contiene:
    - 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)

  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

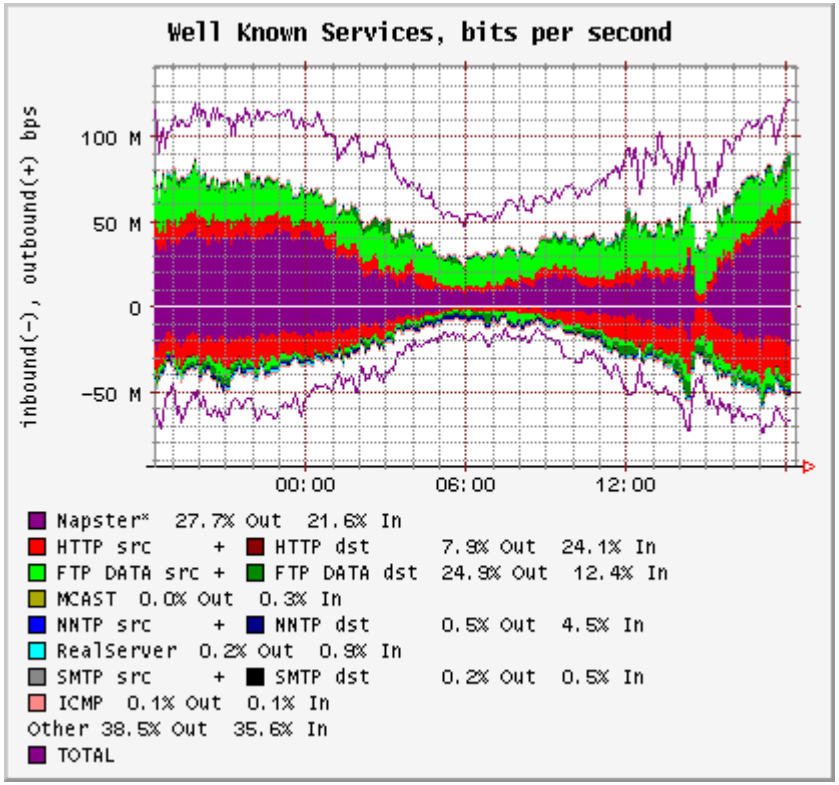
- Listas tipo *Top-Ten* (o *top-five*)

```
##### 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 #######
             input                    output
 port      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


Well Known Services, bits per second
inbound(-), outbound(+) bps
100 M
50 M
0
-50 M
00:00
06:00
12:00
Napster* 27.7% Out 21.6% In
HTTP src + HTTP dst 7.9% Out 24.1% In
FTP DATA src + FTP DATA dst 24.9% Out 12.4% In
MCAST 0.0% Out 0.3% In
NNTP src + NNTP dst 0.5% Out 4.5% In
RealServer 0.2% Out 0.9% In
SMTP src + SMTP dst 0.2% Out 0.5% In
ICMP 0.1% Out 0.1% In
Other 38.5% Out 35.6% In
TOTAL

Gestión de fallas

- Identificación
  - Sondeo regular de los elementos de la red
- Aislamiento y Diagnosis
  - Establecer el “dominio de fallo”
  - Diagnosis de los componentes de la red
  - Documentación es esencial!
- Reacción
  - Asignación de recursos para resolver fallas
  - Determinación de prioridades
  - Proceso pre-establecido de escalada técnica y de gestión
- Resolución
  - Resolver, o escalar
  - Notificación al cliente y demás partes interesadas

Requisitos para tener un buen sistema de gestión de fallas (lista de chequeo)

- Establecer procedimientos de notificación:
  - Enlace al NOC
  - Notificación al personal técnico de guardia
  - Notificación a clientes , gerentes u otro personal de acuerdo a protocolo pre-establecido
- Tener un buen sistema de monitoreo y alarma
  - Sistema Automático (Nagios, Cacti, otros)
- Establecer procedimientos de reparación/recuperación
  - Documentar procedimientos estándares (SOP)
  - Entrenar al personal técnico,
  - Especialmente a personal recién contratado
  - Mantener la documentación actualizada
- Mantener un sistema de manejo de incidencias (ticketing system)
  - Para conocer cantidad, prioridad, y estado de resolución de cada problema
  - Excelente base de conocimiento, datos históricos
  - Regla de 80-20: 80% del tiempo se emplea en diagnóstico
  - Administrar carga de trabajo del NOC e ingenieros
  - Ejemplo: RT (Request Tracker)

Detección y Gestión de Fallas

¿Quién detecta un problema en la red?

- Idealmente, sistema de monitoreo
- Personal de guardia 24x7 (NOC)
- Otros operadores de la red
- Empleados no técnicos
- Llamada de cliente (¡mejor que no! :)

Que' pasos se deben tomar?

- Crear un un caso en el sistema de gestión para dar seguimiento al problema
- Diagnosticar el problema (usualmente 80%)
- Establecer posibles soluciones (básicas, preliminares)
- Punto de decisión:
  - Asignar un ingeniero al caso o escalar la incidencia
  - Notificar a partes interesadas de acuerdo con el protocolo de notificación

Detección y Gestión de Fallas

¿Cómo saber si hay un problema en la red?

- Herramientas de monitoreo
  - Utilitarios (linea de comando o GUI)
    - ping
    - traceroute
    - Ethereal (wireshark)
    - Net-SNMP
  - Sistemas de Monitoreo
    - Nagios
    - Big Brother

- Reportes de estado
  - Mantener el sistema actualizado, separando:
    - Nodos no-operativos (down)
    - Nodos no alcanzables (unreachable)
    - Nodos fuera de servicio por causas administrativas

Gestión de Fallas: Sistema de Control 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 tomadas

Gestión de Fallas: Sistema de Control de Incidencias

- El sistema provee:
  - Programación y asignación de tareas
  - Registro de la notificación
  - Registro de tiempo de notificación y otros pasos
  - Comentarios, escalamiento, notas técnicas
  - Análisis estadístico
  - Supervisión y delimitación de responsabilidades (quién hizo qué)

Gestión de fallas: guía de acción

- Crear un caso por cada notificación
- Crear un caso por cada incidente
- Crear un caso por cada evento programado (mantenimiento)
- Enviar una copia del caso a quién reporta, y a una lista de distribución
- A cada caso se asigna una identificación única.
- Todas las acciones en la vida de un caso están inter-relacionadas vía el numero de caso.
- El caso transita a través de una “máquina de estado”
  - ejemplo: abierto => asignado => en_progreso => resuelto (o escalado) => cerrado
- Quién creó el caso determina cuándo debe ser cerrada la incidencia

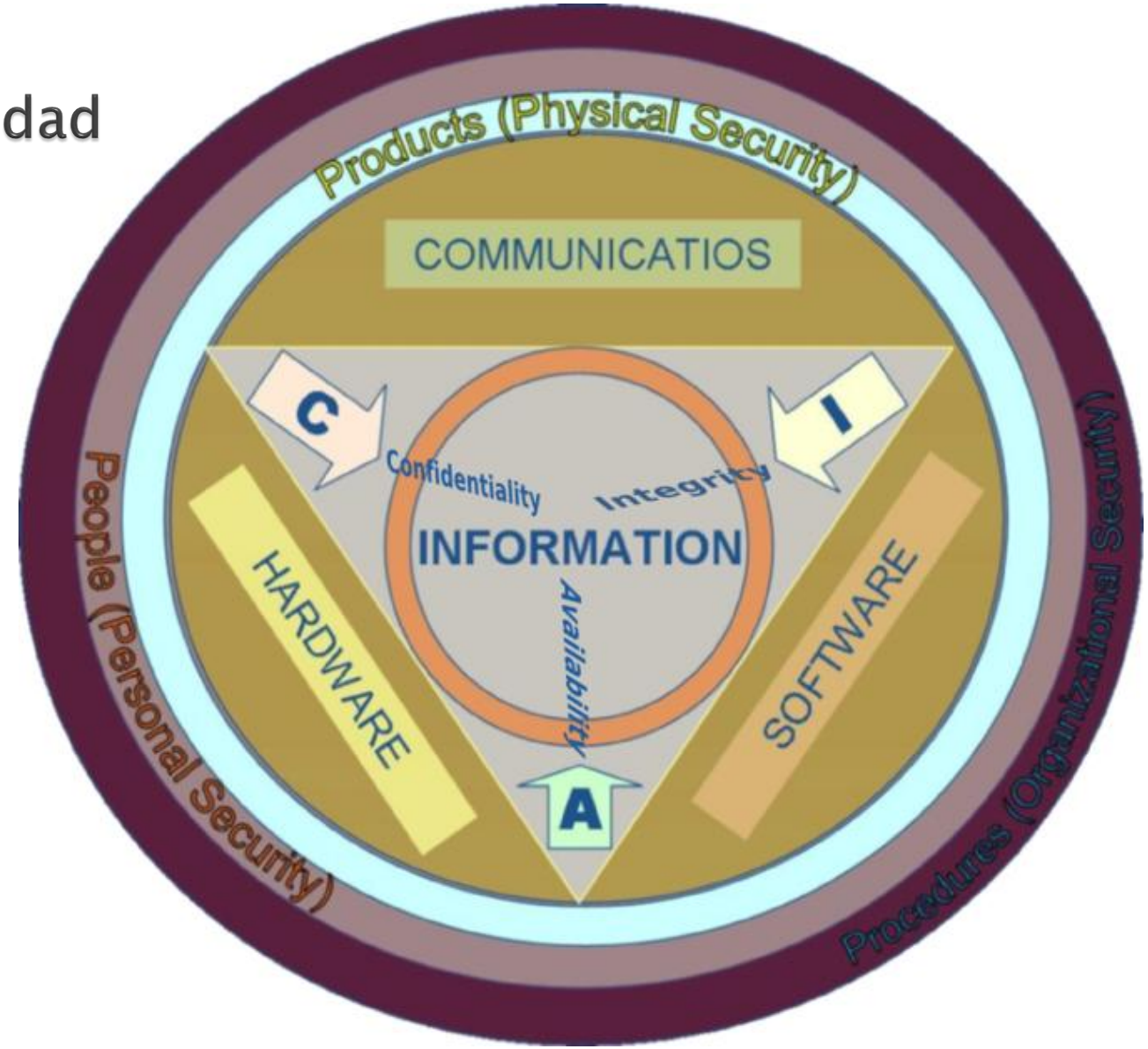
Gestión de contabilidad

- ¿Qué se 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 Seguridad

- Controlar acceso a los recursos de la red de acuerdo a regulaciones bien definidas
  - Medidas organizativas y técnicas que combinadas garantizan disponibilidad, confidencialidad, e integridad de la red
  - Determinar quién autoriza acceso, y que proceso se sigue
  - Establecer egulaciones respecto al tipo de control de acceso (palabras claves, generadores de claves aleatorias, certificados de SSL)
  - Uso periódico de herramientas para analizar y controlar el uso legítimo de la red

Gestión de Seguridad



Gestión de Seguridad: Herramientas

- Herramientas
  - Sondeo de vulnerabilidades
    - Nessus (www.nessus.org)
  - Análisis de bitácoras (logs)
    - swatch – reportes via e-mail
  - Filtros de Servicios
    - iptables, tcpwrappers, firewalls
  - Cifrado
    - SSH – cifrado de sesiones interactivas
    - SSL
  - Revisión de Integridad
    - Tripwire – monitorea cambios en sistema de ficheros
- Mantenerse actualizado es muy importante
  - Reportes de “bugs”
    - CERT
    - BugTraq
  - Mantener software en versiones confiables y recientes

Gestión de Seguridad

Este es un caso tomado de la vida real….

…..

```
tcp4       0      0 147.28.0.34.80       193.169.4.191.10558    SYN_RCVD
tcp4       0      0 147.28.0.62.80       193.169.4.154.10589    SYN_RCVD
tcp4       0      0 147.28.0.34.80       193.169.4.154.10589    SYN_RCVD
tcp4       0      0 147.28.0.62.80       193.169.4.164.11353    SYN_RCVD
tcp4       0      0 147.28.0.34.80       193.169.4.164.11353    SYN_RCVD
tcp4       0      0 147.28.0.62.25       201.88.17.237.2104     SYN_RCVD
tcp4       0      0 147.28.0.62.80       193.169.4.224.5167     SYN_RCVD
tcp4       0      0 147.28.0.34.80       193.169.4.224.5167     SYN_RCVD
tcp4       0      0 147.28.0.34.80       193.169.4.178.5323     SYN_RCVD
tcp4       0      0 147.28.0.62.80       193.169.4.178.5323     SYN_RCVD
tcp4       0      0 147.28.0.34.80       193.169.4.207.7156     SYN_RCVD
tcp4       0      0 147.28.0.62.80       193.169.4.207.7156     SYN_RCVD
tcp4       0      0 147.28.0.34.80       193.169.4.203.6892     SYN_RCVD
tcp4       0      0 147.28.0.62.80       193.169.4.203.6892     SYN_RCVD
tcp4       0      0 147.28.0.62.80       193.169.4.213.7608     SYN_RCVD
tcp4       0      0 147.28.0.34.80       193.169.4.213.7608     SYN_RCVD
tcp4       0      0 147.28.0.62.80       193.169.4.227.72       SYN_RCVD
tcp4       0      0 147.28.0.34.80       193.169.4.227.72       SYN_RCVD
tcp4       0      0 147.28.0.34.80       193.169.4.131.760      SYN_RCVD
$ netstat -na | grep SYN_RCVD | grep 193.169 | wc -l
    248
```

Gestión de Seguridad: Prácticas recomendadas

- Proveer puntos de fácil contacto
  - Dirección de “abuso” para quejas de clientes
    - (abuse@su-dominio.net)
  - Teléfonos bien conocidos y accesibles
    - Asignar tiempos “de guardia” por turnos
  - 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 gestionar la red?

- ¿Qué herramientas usar?
  - Mientras más simple de mantener, mejor
  - No gastar demasiado tiempo desarrollando las herramientas
  - Hacer uso de herramientas gratuitas
    - SourceForge.net
    - FreshMeat.net
  - Automatizar, automatizar, automatizar!

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
```

Referencias

- 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