

Administración y Monitoreo de Redes

▶ Diseño y Operaciones de Redes

▶ *Hervey Allen*

▶ hervey@nsrc.org



▶ *Carlos Armas*

▶ carmas@roundtripnetworks.com



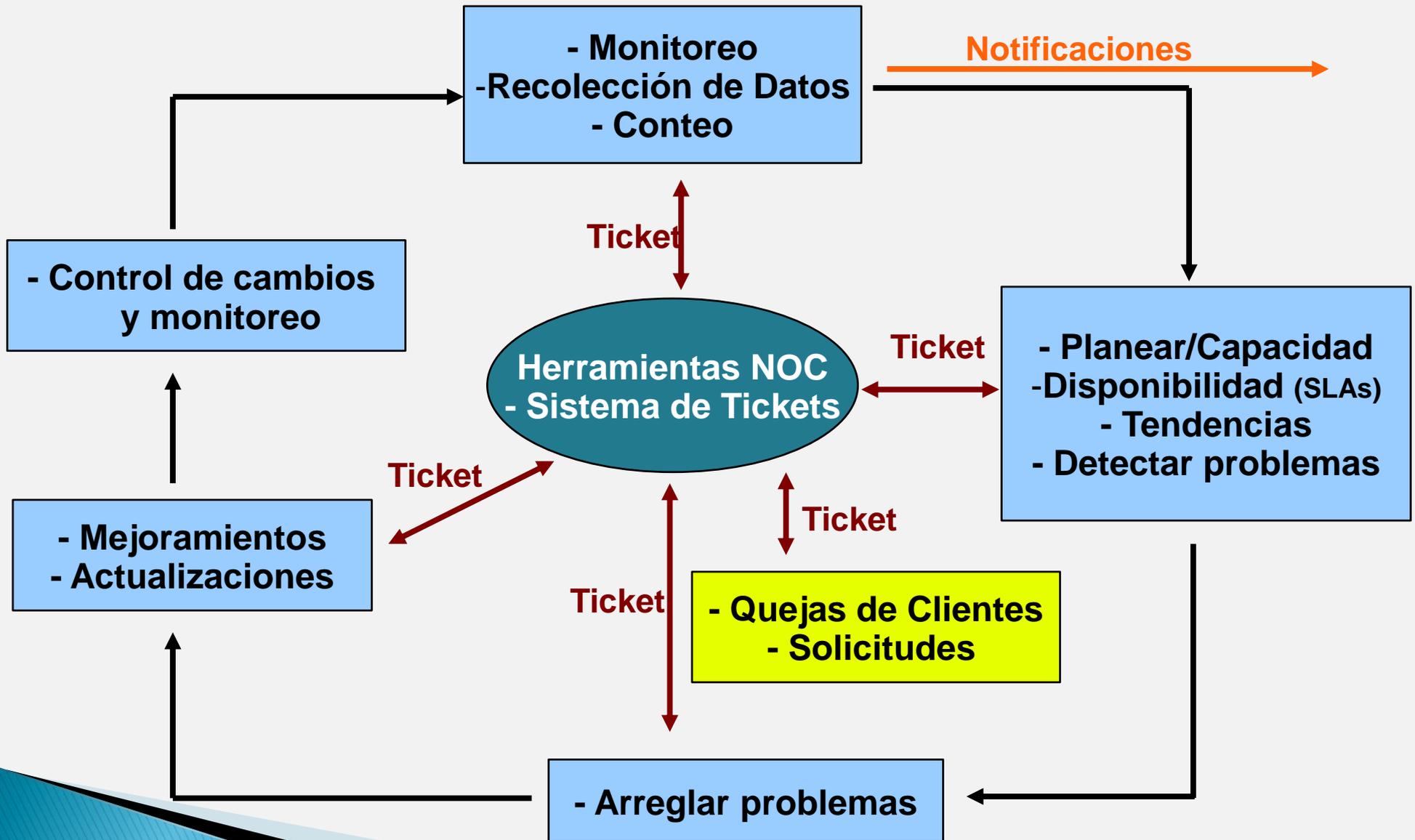
Introducción

- Este es un tópico extenso...
- Muchas herramientas para escoger:
 - Open Source
 - Comerciales
 - Para Linux/Unix, para Windows
 - Herramientas de proveedores de equipos de red (Cisco, Juniper, others)
- No hay una combinación perfecta
- La decisión debe basarse de acuerdo a lo que se necesita saber de la red

Qué es administración de redes?

- **Monitoreo de Sistemas y Servicios**
 - Accesible? Disponible?
 - **Medición de recursos**
 - Planificación de capacidad futura, disponibilidad
 - **Monitoreo de Rendimiento**
 - RTT, volumen de tráfico
 - **Medición de Estadísticas, y Facturación**
 - **Gestión de Fallas, Detección de Intrusos**
 - Detección de fallas, diagnóstico, seguimiento
 - NOC, Sistemas de Gestión de Incidencias
 - **Gestión de Cambios, y Monitoreo de Configuraciones**
- 

Visión General



Por qué administración de redes?

- Asegurarse que la red está funcionando. Se necesita monitorearla!
 - Proveer el nivel de servicios acordado (SLA)
 - Depende de factores administrativos
 - A qué aspira la gerencia?
 - A qué aspiran los usuarios, y clientes?
 - Monitoreo 24x7?
 - No es posible proveer servicios a 100% disponibilidad

Para qué administrar la red? – 2

- Dado que los conmutadores y enrutadores de la red soportan SNMP...
- Use herramientas de dominio público (y gratis!) para monitorear esos equipos:
 - Nagios – <http://nagios.org/>
 - Sysmon – <http://www.sysmon.org/>
 - Open NMS – <http://www.opennms.org/>
 - Cacti – <http://www.cacti.net>
- La meta es saber que la red tiene problems antes que los clientes empiezen a telefonear

Para qué administrar la red? – 3

- Qué se necesita para proveer 99.9 % de disponibilidad?
 - $30,5 \times 24 = 762$ horas al mes
 - $(762 - (762 \times .999)) \times 60 = 45$ minutos – máximo límite de tiempo de red no disponible al mes!
- Necesita detener la red 1 hora / semana?
 - $(762 - 4) / 762 \times 100 = 99.4\% \leq \text{☹}$

– Recuerda!

- Tener en cuenta mantenimientos planificados para el cálculo del nivel de servicio (SLA).
 - Notificar a los clientes al respecto, vía acuerdo o contrato
-
- Cómo se mide la disponibilidad?
 - En el núcleo de la red?
 - De extremo a extremo?
 - Desde Internet?

Para qué administrar la red? – 4

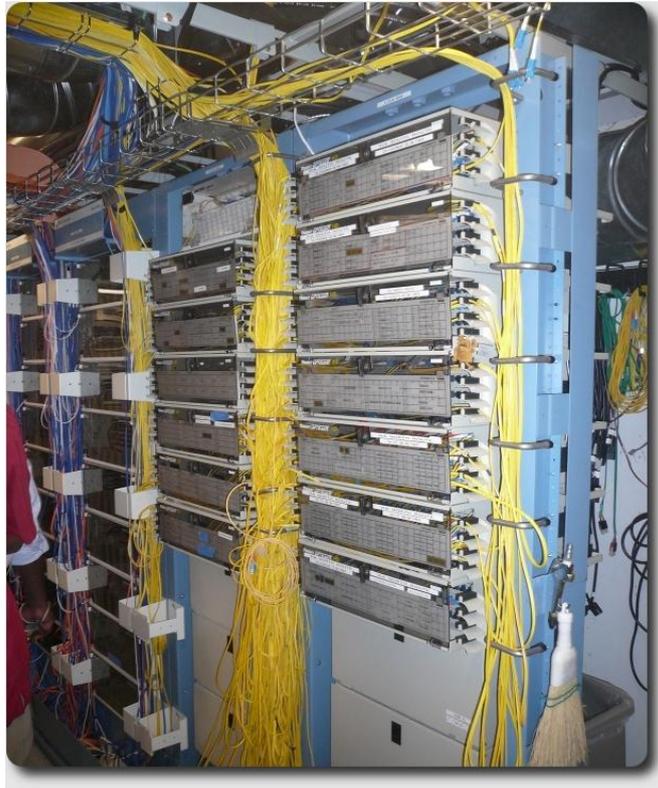
- Para saber cuando aumentar recursos
 - Es el uso de ancho de banda muy alto?
 - Hacia donde va el tráfico?
 - Se necesita una conexión más rápida, o más líneas? Otros proveedores para redundancia?
 - Es el equipamiento muy viejo u obsoleto?
- Para mantener un registro de cambios
 - Registrar todos los cambios
 - Facilitar el establecimiento de las causas de fallas, cuando estas fueron motivadas por cambios o actualizaciones
 - Donde consolidar estas actividades?
 - El Centro de Operacion de Red (NOC)

El Centro de Operación de Red (NOC)

- El lugar donde todo sucede!
 - Coordinación de tareas
 - Estado actual de la red y servicios
 - Notificación de incidentes y quejas referentes a la red
 - El hogar de las herramientas de red ("servidor NOC")
 - El hogar de la documentación, incluyendo:
 - diagramas de red
 - Base de datos de cada puerto en cada conmutador
 - descripción de la red
 - Y mucho más!

Documentación

▶ Cómo controlar toda esa información?



...En la Universidad de Oregon, crearon un programa para ello...

{net.}
NETwork DOcumentation Tool

Netdot!

Documentación

- Datos básicos, por ejemplo, conmutadores...

- A qué se conecta cada puerto?
- Puede ser un simple fichero texto:

health-switch1, port 1, Room 29 - Director's office

health-switch1, port 2, Room 43 - Receptionist

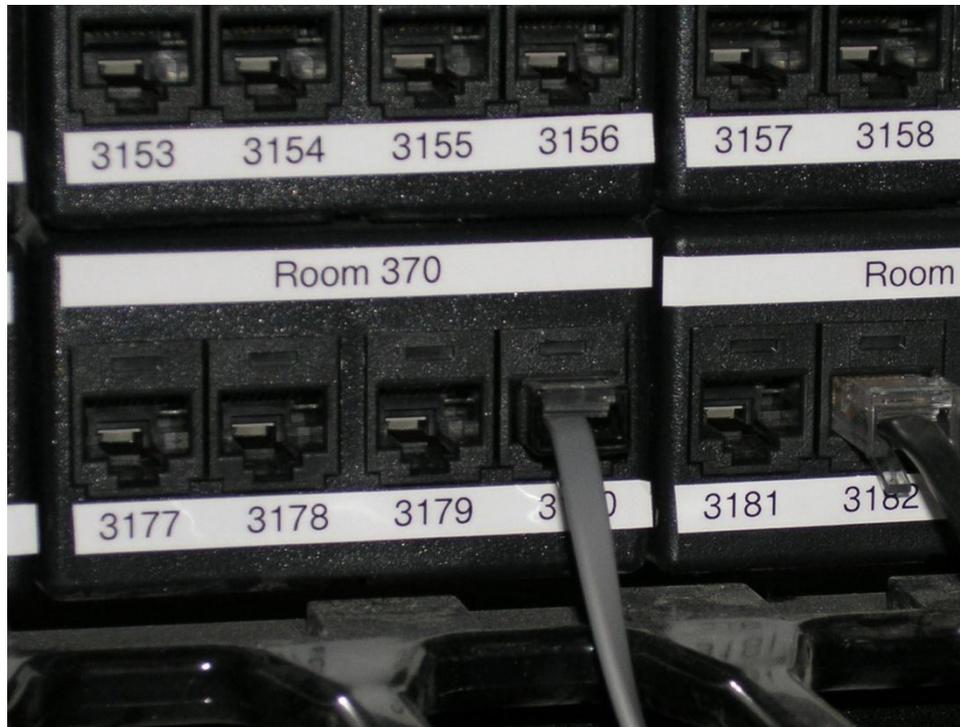
health-switch1, port 3, Room 100 - Classroom

health-switch1, port 4, Room 105 - Hervey's computer closet

- Esta información puede ser accedida por el grupo de redes, NOC, o demás empleados
- Recuerda: pon etiquetas de identificación en los puertos!

Documentación: Etiquetas

- ▶ Como diría Hervey: "Nice!" 😊



Documentación:

Programas y Descubrimiento

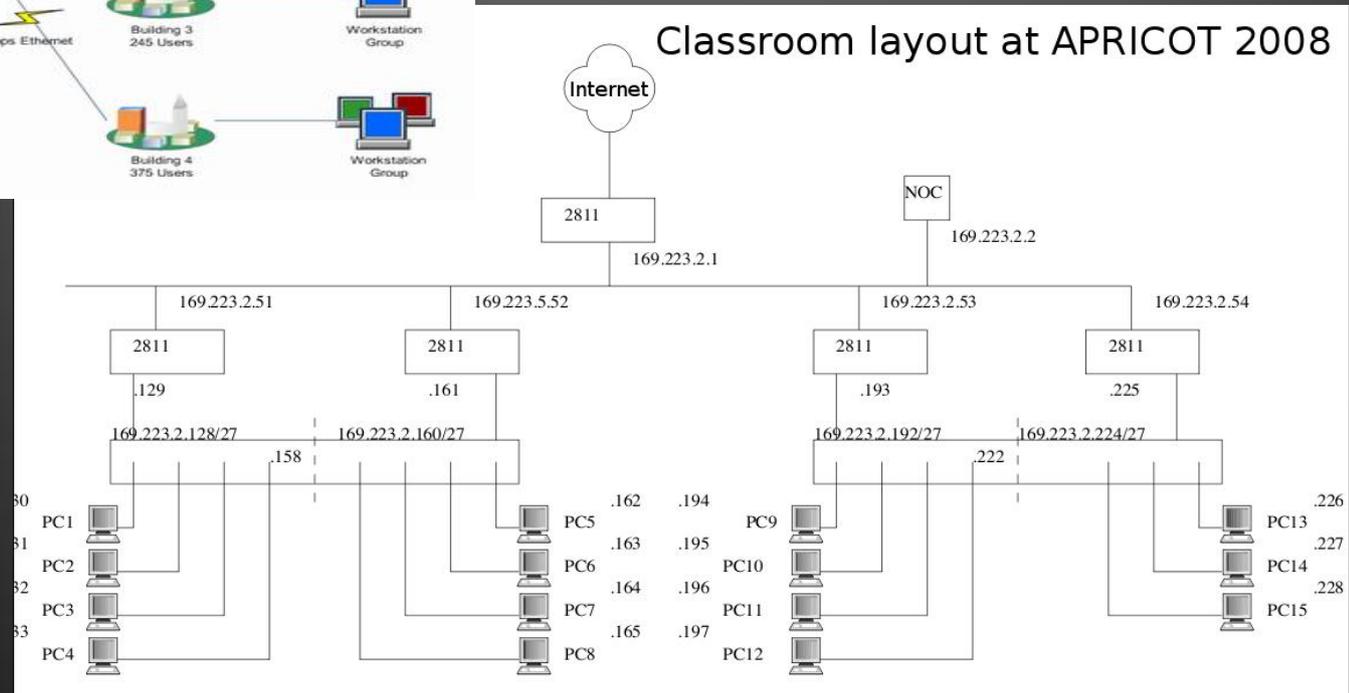
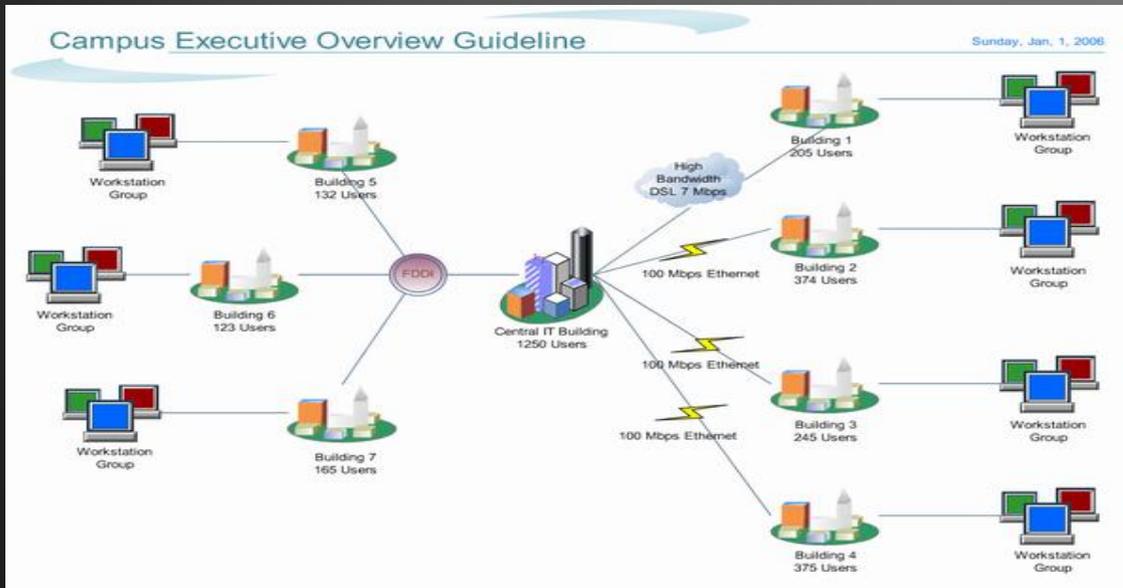
▶ Otros proyectos de Código Abierto:

-  **Maintain** DHCP y DNS
powerful network management
– See <http://maintainproject.osuosl.org>

-  **Netdisco:**
 - Localiza una estación en la red via dirección MAC o IP, y muestra en cuál conmutador y puerto está conectada. Contiene herramientas de inventario y registro de bitácora.
 - Inventario de la red: modelo, fabricante, firmware, otros
 - Reporta uso de direcciones IP y puertos, tanto actual como histórico.

- **[[IPplan]]** Software web, multilingue, para administración de direcciones IP, y una herramienta de auditoria

Documentación: Diagramas



Documentación:

Programas de Diagramas

▶ Windows

- Visio:

<http://office.microsoft.com/en-us/visio/FX100487861033.aspx>

- Ezdraw:

<http://www.edrawsoft.com/>

Código Abierto

- Dia:

<http://live.gnome.org/Dia>

- Cisco reference icons

<http://www.cisco.com/web/about/ac50/ac47/2.html>

- Nagios Exchange:

<http://www.nagiosexchange.org/>

Sistemas y herramientas de monitoreo de redes

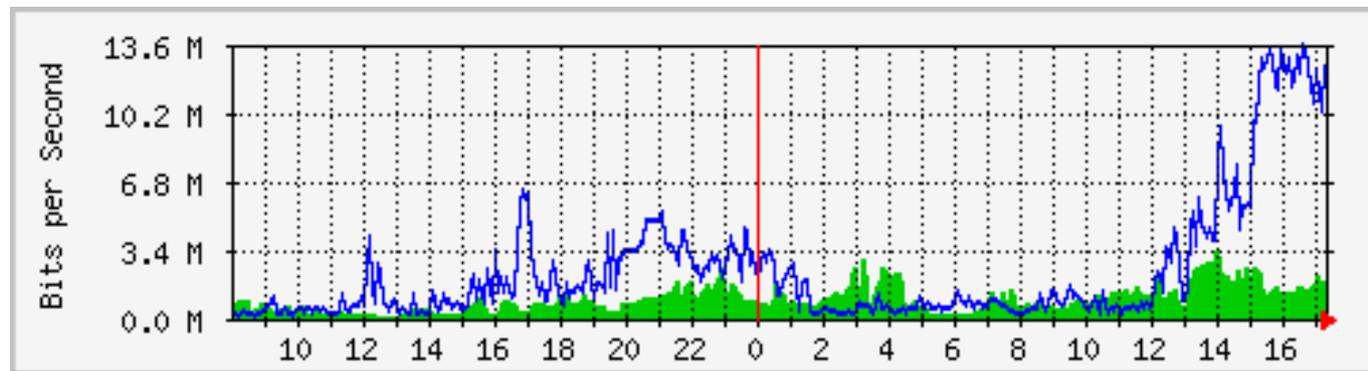
- Tres Tipos
 - **Diagnóstico** – para probar conectividad, y acceso, o si el dispositivo está disponible. Herramientas generalmente activas
 - **Monitoreo** – corren “tras bambalinas” (background) como servicios “daemon”. Coleccionan incidentes, pero tambien pueden iniciar pruebas, a una determinada frecuencia, y registrar los datos.
 - **Rendimiento** – cómo la red está funcionando y manejando el flujo de datos, “cuellos de botella”, y otros.

Sistemas y herramientas de monitoreo de redes - 2

▶ Rendimiento

● Herramientas comunes:

- <http://cricket.sourceforge.net/>
- <http://www.mrtg.com/>
- <http://www.cacti.net/>



Sistemas y herramientas de monitoreo de redes – 3

- Herramientas Activas
 - Ping – prueba conectividad a un dispositivo
 - Traceroute – muestra la via a un dispositivo
 - MTR – combinación de ping + traceroute
 - Collectores de SNMP (en mode encuesta)
- Herramientas Pasivas
 - Monitoreo de logs, Colectores de “trampas” SNMP , NetFlow
- Herramientas iterativas
 - SmokePing – muestrea, registra y grafica demora a un grupo de dispositivos, usando ICMP (Ping) u otros protocolos
 - MRTG/RRD – registra y grafica ancho de banda a intervalos regulares

Sistemas y herramientas de monitoreo de redes – 4

Herramientas de Monitoreo de Servicios y Redes

- Nagios – monitor de servidores y servicios
 - Puede monitorear casi todo
 - HTTP, SMTP, DNS, espacio en disco, uso de CPU, ...
 - Es fácil crear extensiones (plugins)
 - Con habilidades básicas de programación (scripting) :
 - Perl, Shellsript, python, ruby
 - Muchas herramientas de código abierto
 - Zabbix, ZenOSS, Hyperic, Cacti, OpenNMS, Groundworks

Sistemas y herramientas de monitoreo de redes – 5

- Monitorea los servicios esenciales de la red
 - DNS
 - Radius/LDAP/SQL
 - SSH a enrutadores
- De que forma recibirá notificaciones?
- No olvidar la recolección de trazas!
 - Cada dispositivo de red (al igual que servidores UNIX y Windows) son capaces de reportar incidencias vía *syslog*
 - **DEBE** recolectar y monitorear trazas!
 - La omisión de esta tarea esencial es uno de los errores más comunes en la administración de redes

Protocolos de Administracion de Red

- **SNMP** – Protocolo Simple de Administración de Red
 - no tan simple, en realidad ☺
 - Estándar, cientos de herramientas lo utilizan como núcleo operacional
 - Presente en cualquier dispositivo de red decente
 - Volúmen de datos, errores, carga de CPU... muchas variables a monitorear ...
 - UNIX y Windows lo implementan
 - Espacio en disco, procesos en ejecución, ...
- **SSH y telnet**
 - Es también posible programar procesos batch para automatizar el monitoreo de servidores y servicios

Herramientas SNMP

- Conjunto de herramientas SNMP
 - <http://net-snmp.sourceforge.net/>
- Es muy fácil construir herramientas simples
 - Ejemplo 1: qué IP es asignada a una dirección MAC?
 - Ejemplo 2: Que dirección MAC existen en la tabla ARP de un conmutador? Y asignado a cual puerto?

Estadísticas y tabulación

- Tabulación y análisis de tráfico
 - Para qué se está usando la red, y cuanto tráfico?
 - Util para establecer Calidad de Servicio (QOS), detectar abusos de recursos, así como facturación
 - NetFlow
 - Identificar “flujos” de tráfico: protocolo, fuente, destino, cantidad de bytes
 - Existen diferentes herramientas para procesar este tipo de información
 - Flowtools, flowc
 - NFSen
 - ...

Fallas y gestión de problemas

- Es el problema temporal?
 - Sobrecarga, carencia temporal de recursos
- Es el problema permanente?
 - Fallo de equipmento, enlace caído
- Cómo detectar un error?
 - Monitoreo!
 - Quejas de clientes
- Un sistema de gestión de incidencias (tickets) es esencial
 - Abrir un caso para seguir una incidencia detectada o reportada (planificada, o de emergencia)
 - Definir asignación de caso, y escalamiento si es necesario
 - Quién se encarga de arreglar el problema?
 - Quién recibe el caso (escalamiento) si no hay nadie disponible?

Sistema de Gestión de Incidencias

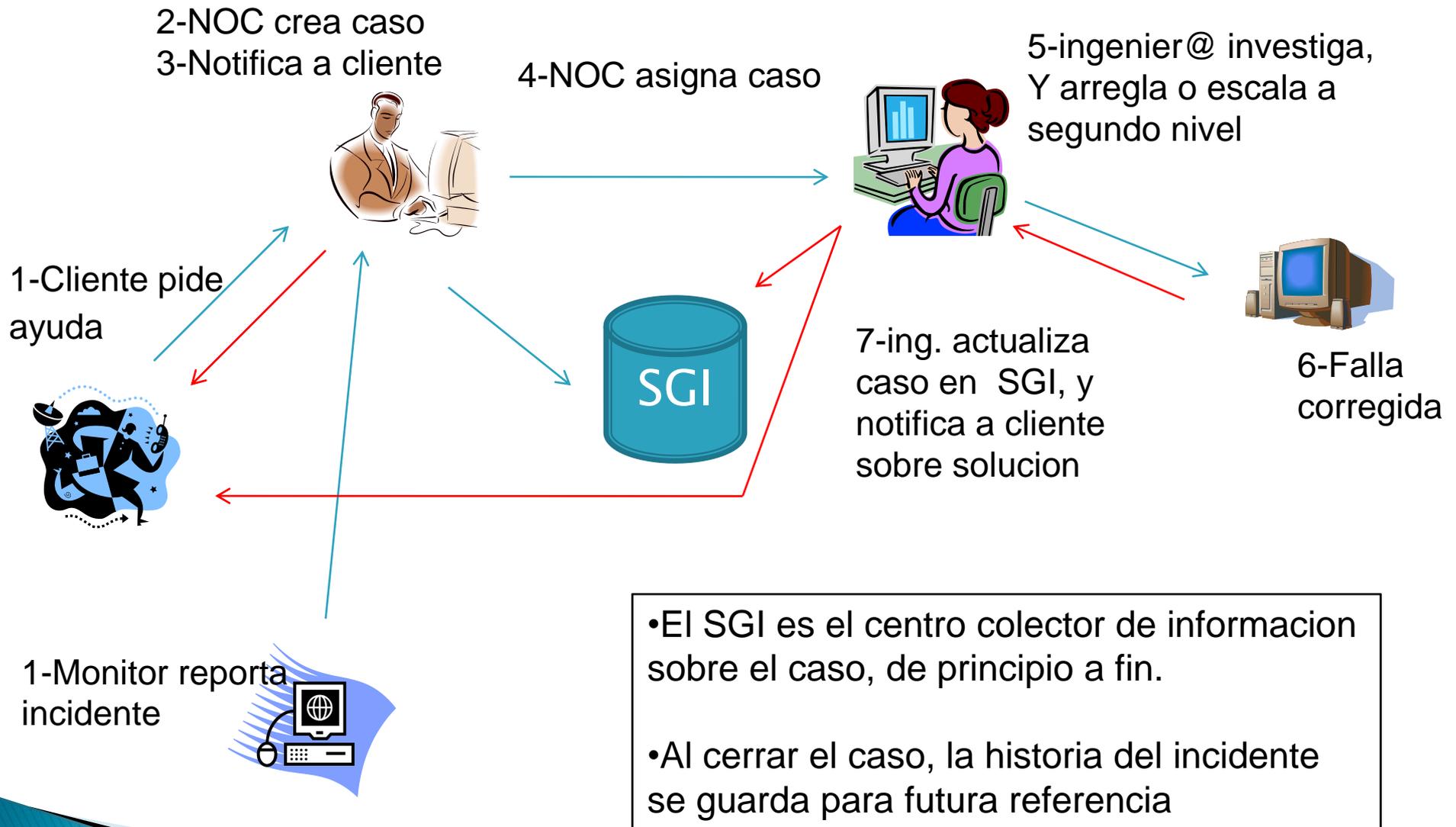
- Importancia ?
 - Registro y control de incidencias, fallas y problemas
- Punto focal de comunicaciones con el buró de ayuda
 - Registrar y seguir todas las comunicaciones
 - Tanto internas como externas
- Incidentes externos:
 - Quejas y solicitudes de clientes
- Incidentes internos:
 - Fallas de servicios y sistemas
 - Notificados por sistema de monitoreo
 - Mantenimiento planificado – actualización, nuevos equipos
 - No olvide notificar a los clientes!

Sistema de Gestión de Incidencias – 2

- Use el sistema para seguir cada caso
 - Incluyendo comunicaciones internas entre técnicos
 - A cada caso se asigna un número único
- Cada caso sigue el mismo ciclo
- (también conocido como “maquina de estado”)
 - caso Nuevo
 - caso Abierto
 - caso En-Progreso
 - Caso Resuelto
 - Caso Cerrado

Sistema de Gestión de Incidencias – 3

Ciclo de vida de un caso



Sistema de Gestión de Incidencias – 4

▶ Algunos sistemas de gestión de incidencias:

▶ **rt**

- Extensivamente usado
- sistema clásico, puede ser adaptado a necesidad local
- relativamente complejo de instalar
- capaz de manipular grandes volúmenes de transacciones

trac

- Sistema híbrido que incluye un wiki, así como un gestor de proyectos
- El sistema de gestión no es tan robusto como **rt**. Pero funciona bastante bien
- Frecuentemente usado para gestionar proyectos de grupo.

– **redmine**

- Parecido a **trac**, aunque más robusto. Instalación compleja.

Sistema de Detección de Intrusiones – NIDS

- ▶ Monitorean de tráfico en busca de patrones de ataque conocidos, o condiciones sospechosas
 - Ejemplos:
 - Servidores actuando como ‘spamming’
 - Gran cantidad de conexiones TCP “medio-abiertas” procedentes de una misma dirección IP
 - **SNORT** is the most common open source tool
<http://www.snort.org/>

Control de cambios

Tres principios básicos:

- Mantener un registro e historia de cambios
- Dar acceso público a la información
- Mantener diferentes versiones de un mismo conjunto de datos

Qué tipo de datos ?

Código fuente,

- Documentación
- Ficheros de configuración
- En general, cualquier dato

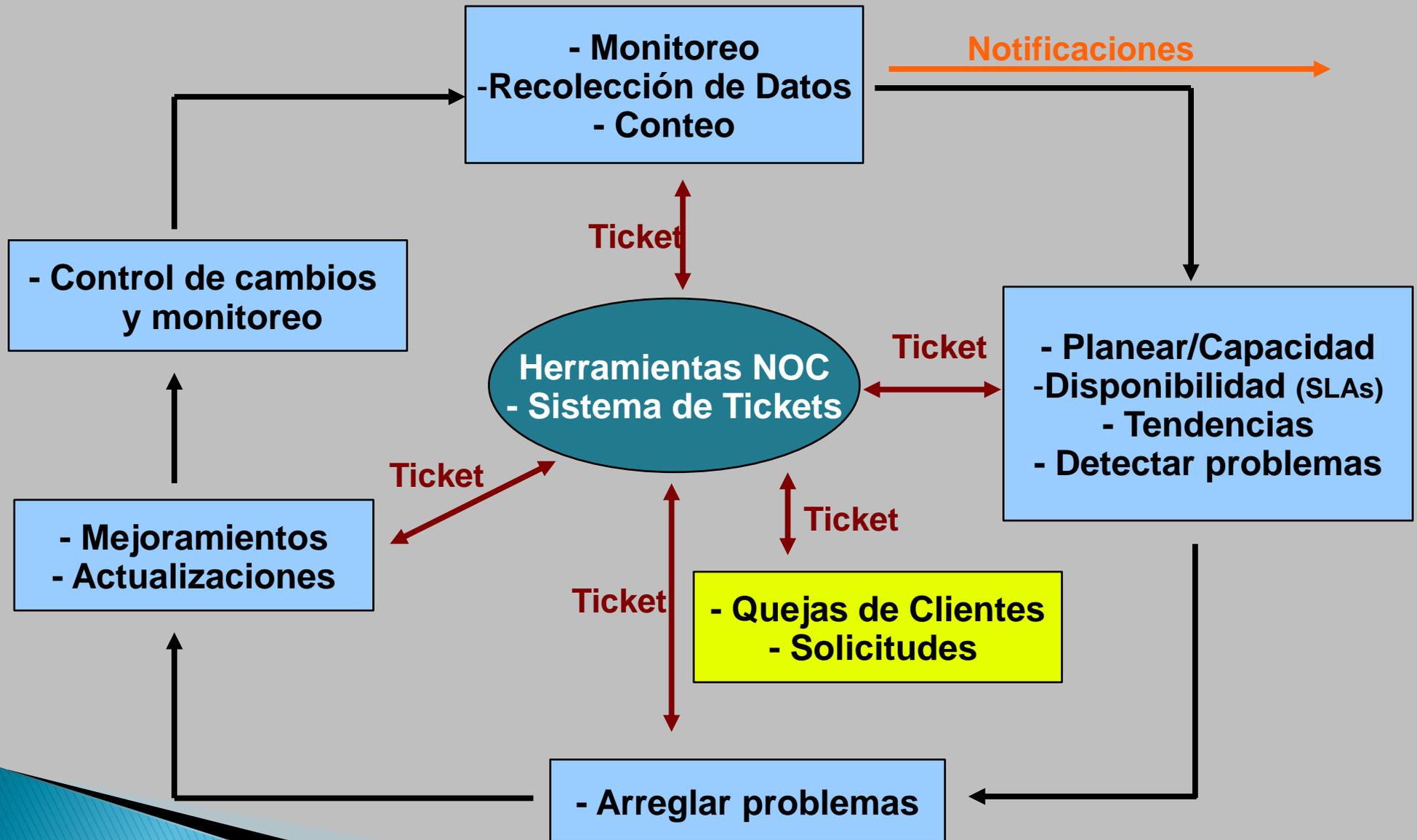
Control de Cambios – 2

Buenas Prácticas :

- Disciplina de cambios:
 - Registrar todos los cambios
 - Consultar todos los cambios
 - El personal más experimentados analiza los cambios propuestos antes de implementar
- Prueba de cambios
 - Tener un “banco de prueba” para verificar cambios
 - Asignar responsabilidad de control de calidad
- Controlar el proceso de cambios
 - Mantener historia de cambios en un registro
 - Crear casos en el SGI para cada cambio aprobado e implementado

En un team disciplinado, nunca se cambia nada sin consultar!!!

Visión General, otra vez



Resumen de Herramientas de Código Abierto

▶ Rendimiento

- Cricket
 - IFPFM
 - flowc
 - mrtg
 - netflow
 - NfSen
 - ntop
 - pmacct
 - rrdtool
 - SmokePing
- SNMP/Perl/ping

▶ Administración

- Big Brother
- Big Sister
- Cacti
- Hyperic
- Munin
- Nagios*
- Netdisco
- Netdot
- OpenNMS
- Sysmon
- Zabbix

Manejo de Cambios

- Mercurial
- Rancid (routers)
- RCS
- Subversion

Security/NIDS

- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Ticketing

- RT, Trac, Redmine

Resumen – las “reglas de oro”

- ▶ *Mantener una organización (NOC) responsabilizada con la administración de la red*
 - ▶ *Monitorear la red para garantizar niveles de servicio en el presente y el futuro*
 - ▶ *Mantener y velar por la seguridad de la red. Una red segura garantiza integridad, confidencialidad, y disponibilidad de sus datos y servicios*
 - ▶ *Controlar , analizar, probar y registrar cambios en la red*
 - ▶ *Mantener un registro de incidentes y solicitudes*
- 