Gestión y Monitoreo de Redes

Introducción a la Gestión de Redes

Parte I: Resumen

Conceptos Principales:

- Que es el monitoreo de redes
- Que es la gestion de redes
- Empezando
- Porque la gestion de redes
- Los “Tres Grandes”
- Deteccion de los ataques
- Documentacion
- Consolidando los datos
- El panorama en grande

Monitoreo de Redes

Una definicion…

“Monitoreo de una red activa de comunicaciones para diagnosticar problemas y recopilar estadísticas por la administración y ajustamiento de la red.”

PC Magazine

Gestión de Redes

…las actividades, metodos, procedimientos y herramientas que pertanescan a la operacion, administracion, mantenimiento y aprovisionamiento de sistemas conectadas por la red.

FCAPS

Falla, **C**onfiguracion, Contabiliad, Rendimiento y **S**eguridad
(El modelo deTelecommunicaciones de Gestion de Redes por ISO)

Fuente: wikipedia

Detalles: Gestión de Redes

Monitoreamos

- **Servicios y sistemas**
  - Disponible, alcanzable
- **Recursos**
  - Planificación de expansión, mantener disponibilidad
- **Rendimiento**
  - Tiempo de ida y vuelta (rtt), banda de ancha
- **Cambios y configuraciones**
  - Documentación, control de revisión, logging (registro de datos)

Detalles: Gestión de Redes

Mantenemos Informados de

- **Estadísticas**
  - Para los propósitos de contabilidad y medición
- **Fallas (detección de intrusos)**
  - La detección de problemas
  - Solución de problemas y el seguimiento de su historia

Con tiempo los sistemas de ticketing tienen muchos datos utiles

Las Expectativas

Una red en operacion tiene que estar bajo vigilancia para:

- Cumplir con los Acuerdos de Nivel de Servicio (SLAs en ingles)
- SLAs depende en política local
  - Que espere su administración?
  - Que espere sus usuarios?
  - Que espere sus clientes?
  - Que espere el resto del Internet?
- Que es acceptable? 99.999% disponibilidad?
  - Disponibilidad de 100% es “muy dificil” →

Expectativas de Disponibilidad

Que es necesario para entregar disponibilidad de 99.9%?

30.5 x 24 = 762 horas al mes

(762 – (762 x .999)) x 60 = 45 minutos

Solo 45 minutos de mantenimiento al mes!

Tienes que bajar los equipos 1 hora/semana?

(762 - 4) / 762 x 100 = 99.4 %

Recuerda tomar en cuenta mantencion planificada en sus calculos, y informa sus usuarios/clientes si o no el periodo de mantencion esta incluido en el SLA.

Como se mide disponibilidad?

En el nucleo? Extremo a extremo? Desde el Internet?

Recompilando Los Datos

Que es “normal” por su red?

Si nunca ha medido su red va a necesitar saber algunas cosas como:

- La carga tipica de los enlaces (➔ Cacti)
- El nivel tipico de “jitter” entre los puntos de extremo (➔ Smokeping)
- Porcentaje tipico de uso de los recursos
- El nivel tipico de “ruido”:
  - Escaneos de la red
  - Paquetes perdidos
  - Informes de errores o fallos

Porque hacer todo esto?

Saber cuando actualizar

- Es el uso de su banda de ancha demasiado alto?
- Donde va su trafico?
- Necesita una coneccion mas rapida, mas proveedores?
- Ya estan demasiadas viejas sus equipos?

Mantener un estado de cambios

- Grabar todo los cambios en su red
- Lo hace mas facil encontrar el causa de problemas hechas por cambios de configuracion y actualizaciones

Mantener una historia de sus operaciones

- Usando un sistema de tickets mantiene una historia de eventos
- Le permite defenderse y verificar realmente que paso

Porque Gestion de Reds?

Contabilidad

- Seguir el uso de recursos
- Facturar a los clientes

Saber cuando tengas problemas

- Mantenerse mas informado que sus usuarios!
- Software de monitorero puede generar tickets y notificar en forma automatica a su personal de problemas.

Tendencias

- Se puede usar estes datos para ver tendencias por todo su red.
- Esto es un parte de recompilar datos, planificacion de capacidad y deteccion de ataques.

Los “Tres Grandes”?

Disponibilidad

- Nagios — Servicios, servidores, enrutadores, switches

Confiabilidad

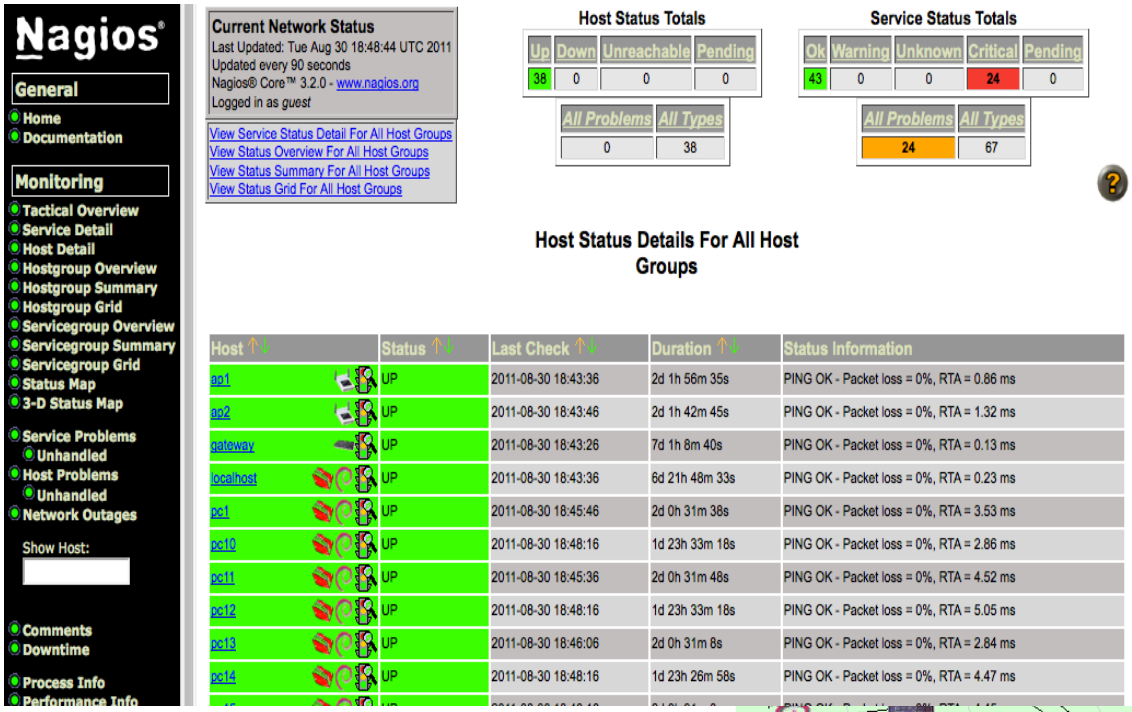
- Smokeping — Salud de conectividad, rtt, tiempo de respuesta de servicios, latencia

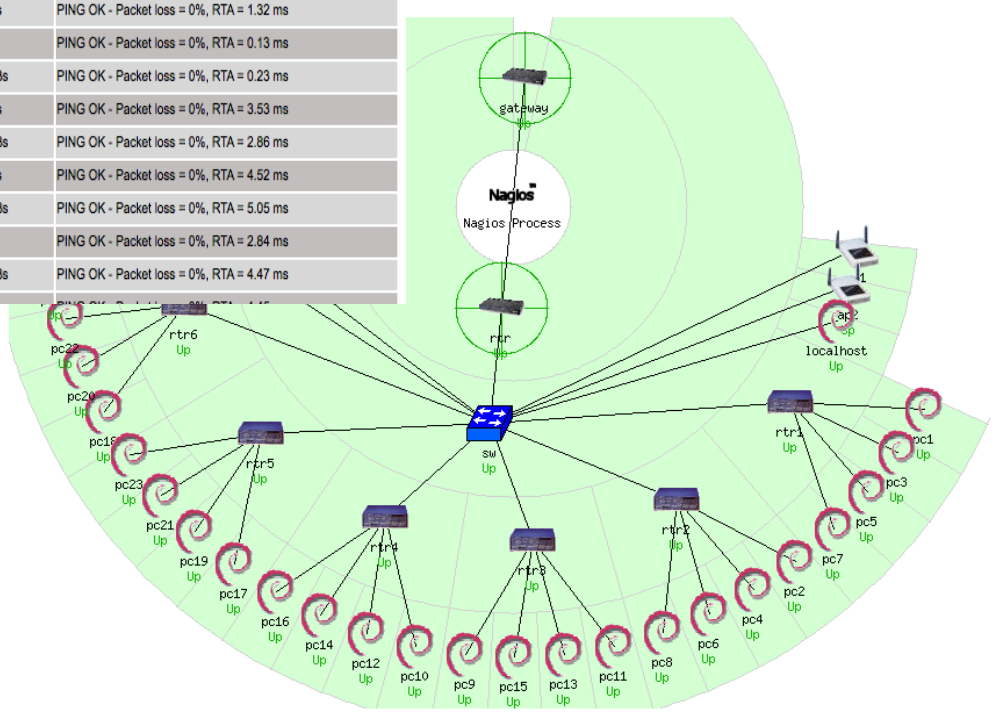
Rendimiento

- Cacti — Trafico en total, uso de puertos, CPU, Memoria Disco, procesos

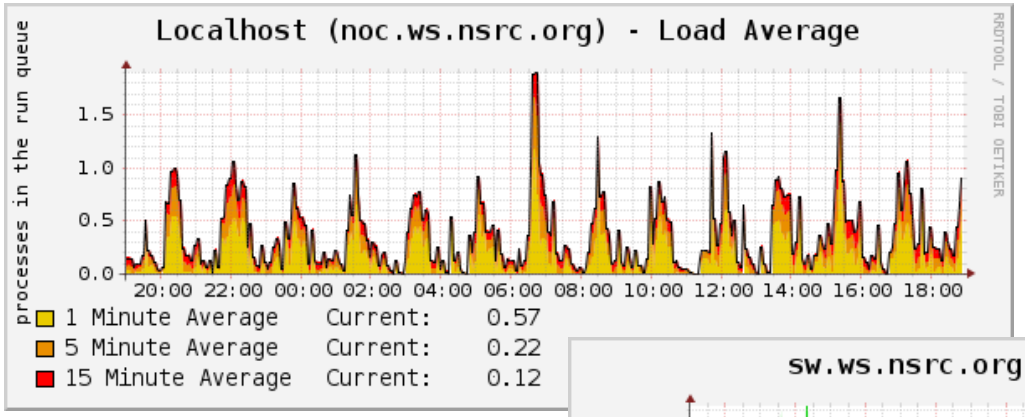
Existe superposición de funcionalidad entre estes programas!

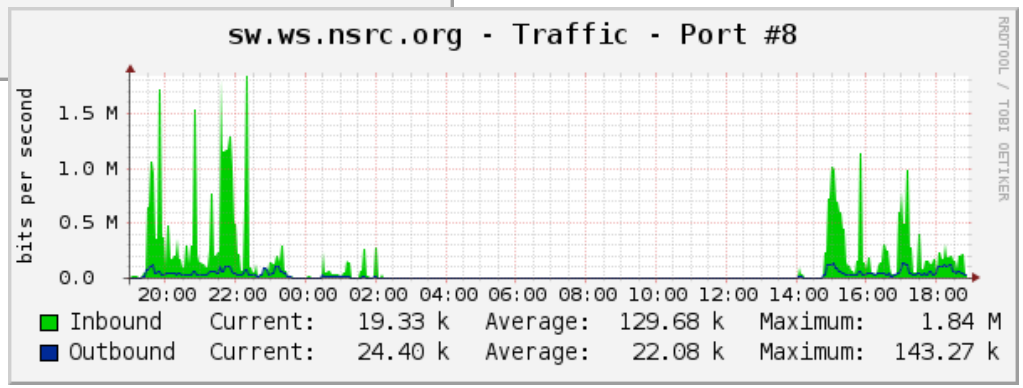
Nagios: Disponibilidad

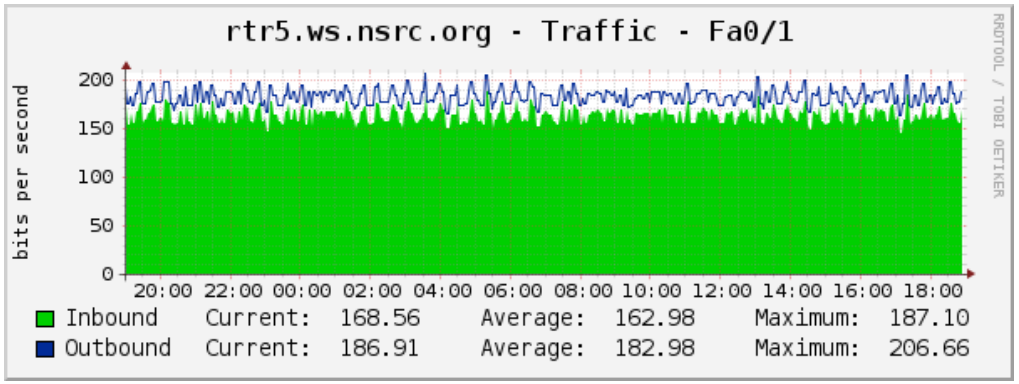




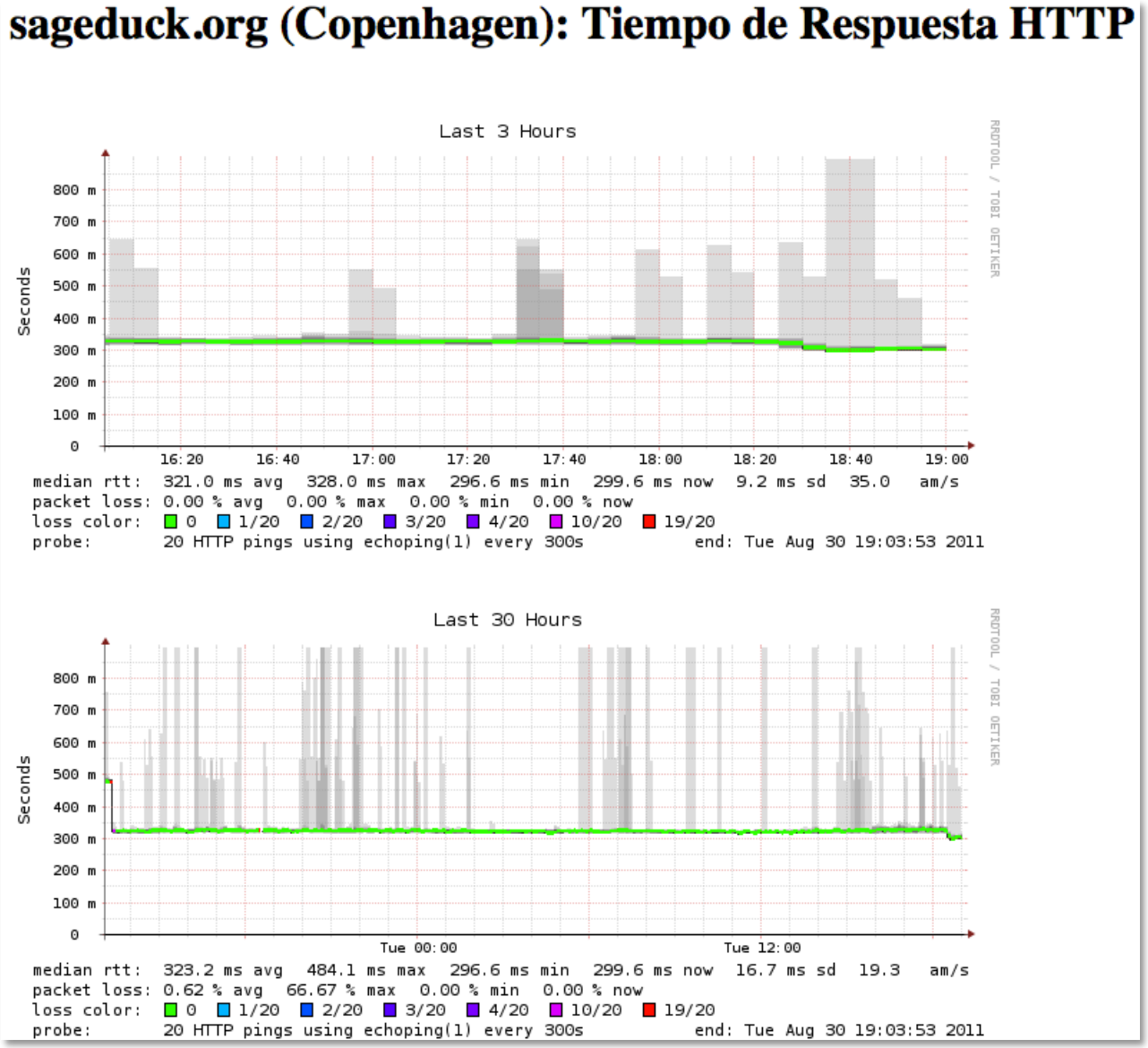
Cacti: Rendimiento







Smokeping: Confiabilidad



Detección de Ataques

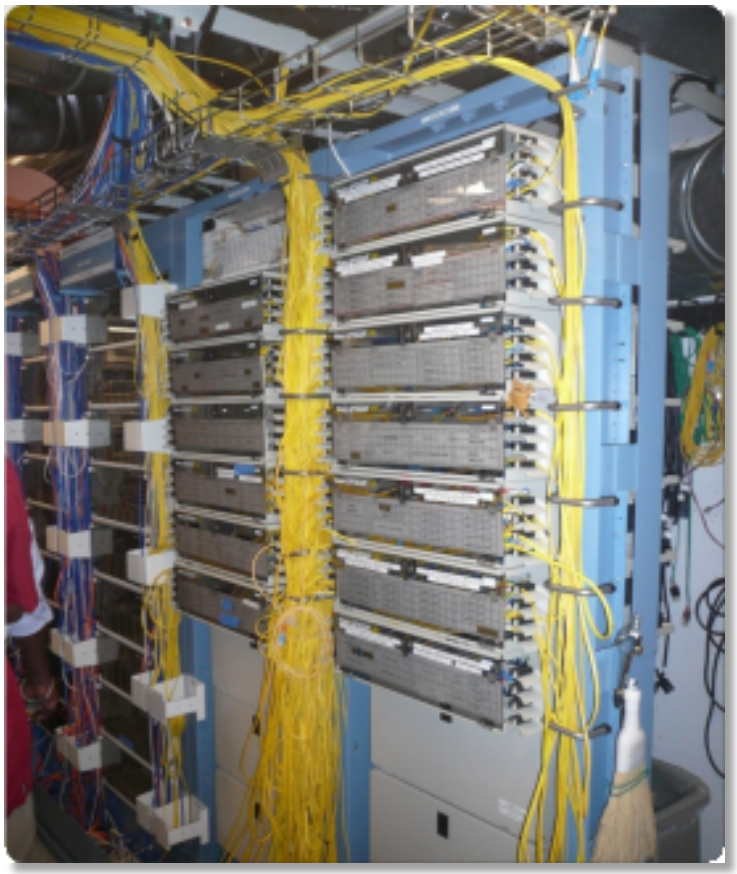
- Tendencias y automatizacion le permite saber cuandos esta bajo ataque.
- Las herramientas en uso le puede ayudar mitigar los ataques:
  - Los flujos a través los interfaces red
  - La carga en servidores o por servicios
  - Fallas multiples servicios
  - Y, escaneos preventitivos (Nessus, Saint)

Documentación

Conocer configuración de dispositivos de la red, y detectar cambios

Documentación

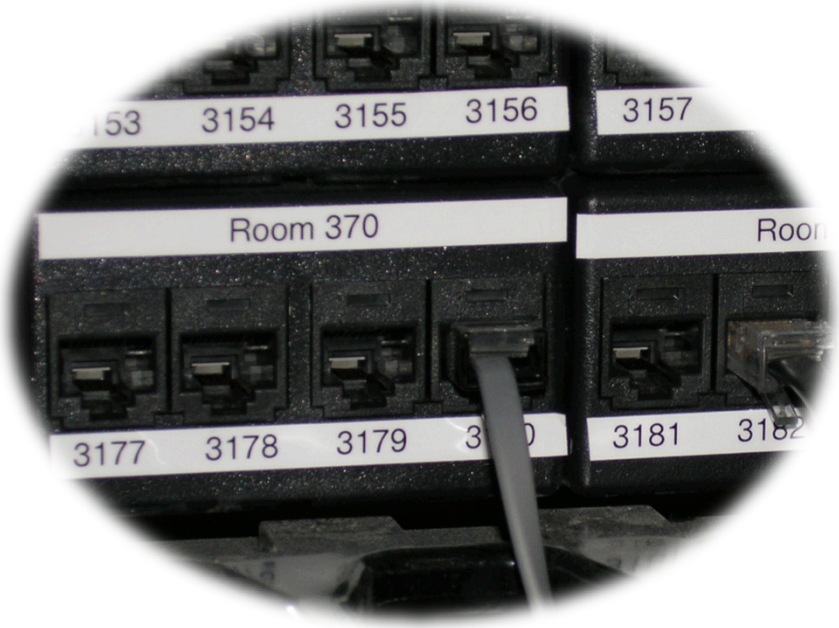
Tal vez ha preguntado, "*Como uno se puede un seguimiento de todo esto?*"



**Documentar,
documentar,
documentar…**

Documentación: Etiquetar

Bueno…



Documentación

Los basicos, como documentar sus switches…

- A que esta conectado cada puerto?
- Puede ser un archivo simple de texto con una linea por cada puerto en un switch:
  - health-switch1, puerto 1, Sala 29 – Oficina Rector
  - health-switch1, puerto 2, Sala 43 – Recepcionista
  - health-switch1, puerto 3, Sala 100 – Sala del curso
  - health-switch1, puerto 4, Sala 105 – Oficina de profesor
  - …..
  - health-switch1, puerto 25, enlace a dorsal-de-salud
- Esta informacion puede estar disponible a su personal de la red, de los help desks, a través un wiki, por software, etc.
- Recuerda a etiquetar a sus puertos!

Documentación de la Red

Tal vez mas automatizacion es necesario. Un sistema automatizado de documentacion de redes es algo para considerar.

- Puede escribir sus propias escripts.
- Puede considerar algunos sistemas de documentacion automaticas.
- Probablemente va a terminar haciendo los dos.

Sistemas Automatizados

Hay varios. Cada uno hace algo diferente:

- IPplan:
  http://iptrack.sourceforge.net/
- Netdisco:
  http://netdisco.org/
- Netdot:
  https://netdot.uoregon.edu/
- Rack Tables:
  http://www.racktables.org/

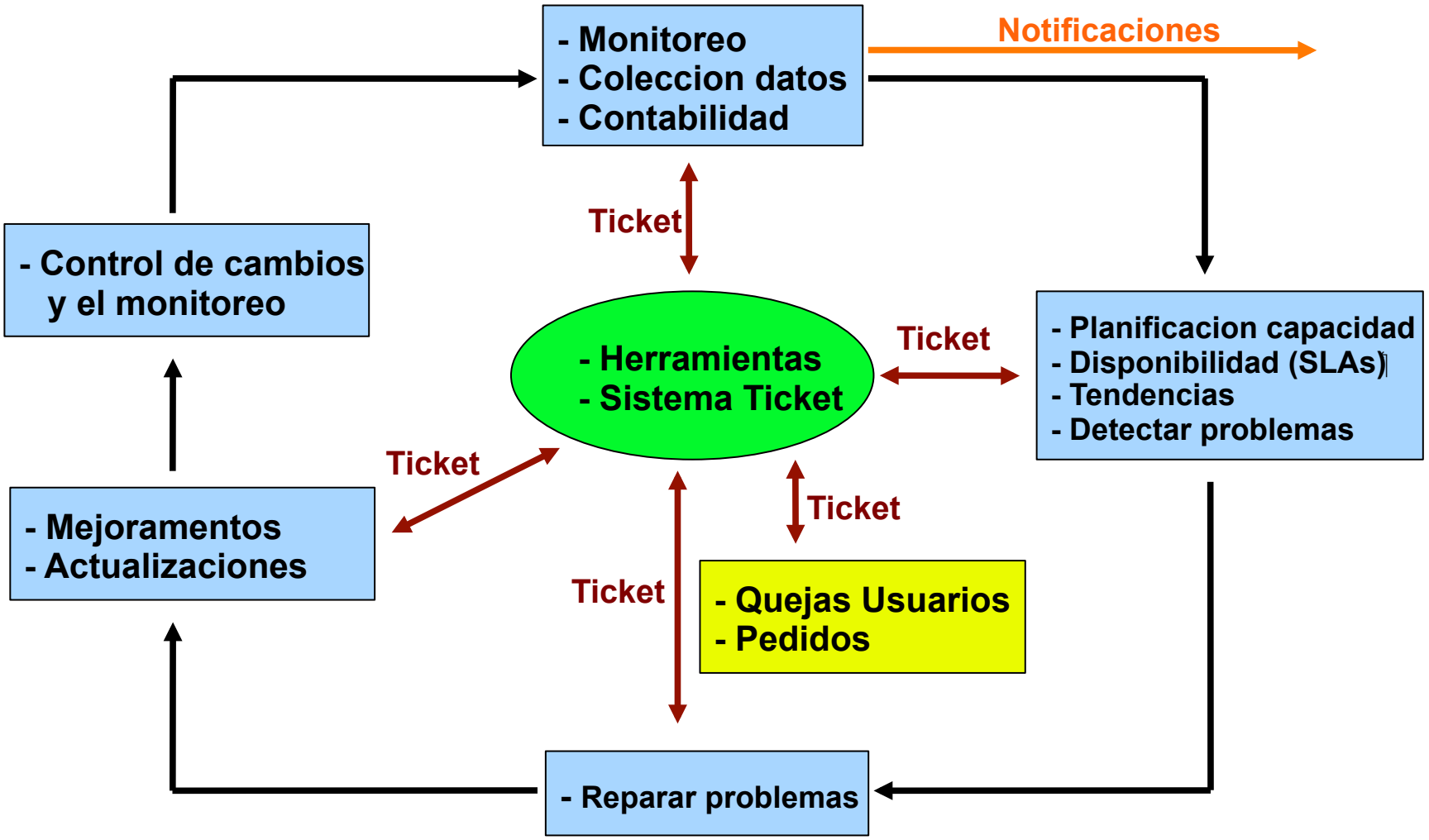
Consolidando los Datos

El Centro de Operaciones de la Red (NOC)

“Donde todo pasa”

- Coordinacion de tareas
- Estatus de los servicios y de la red
- Recibiendo incidentes y quejas relacionados con la red.
- Donde viven las herramientas (“servidor NOC”)
- Documentacion incluyendo:
  - Diagramas de las redes
  - Base de datos y/o archivo de texto de cada puerto en cada switch
  - Descripcion de la Red
  - Mucho mas…

La cuadra en grande



Algunas soluciones fuente abierto…

Rendimiento
- Cricket
- IFPFM
- flowc
- mrtg*
- NetFlow*
- NfSen*
- ntop
- perfSONAR
- pmacct
- rrdtool*
- SmokePing*

Ticketing
- RT*
- Trac*
- Redmine

Manejo de Cambios
- Mercurial
- Rancid* (routers)
- CVS*
- Subversion*
- git*

Seguridad/SDIR
- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Logging (Registro)
- swatch*
- syslog/rsyslog*
- tenshi*

Gestion Red
- Big Brother
- Big Sister
- Cacti*
- Hyperic
- Munin
- Nagios*
- OpenNMS*
- Sysmon
- Zabbix

Documentacion
- IPplan
- Netdisco
- Netdot*
- Rack Table

Protocolos/Utilidades
- SNMP*, Perl, ping

Preguntas?

?