



Gestión de Redes

Introducción a la Gestión de Redes



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

Sección I: Panorama

Conceptos claves:

- Qué es la monitorización de redes
- Qué es la gestión de redes
- Lo básico
- Por qué gestión de redes
- Los tres grandes elementos
- Detección de ataques
- Documentación
- Consolidación de la información
- La visión completa

Detalles de la Gestión de Redes

Monitorizamos

- **Sistemas y servicios**
 - Disponible, alcanzable
- **Recursos**
 - Planificación de expansión, mantener disponibilidad
- **Rendimiento**
 - Tiempo de ida y vuelta, tasa máxima de transmisión
- **Cambios y configuraciones**
 - Documentación, control de versiones, logs

Detalles de la Gestión de Redes

Seguimos la pista de

- **Estadísticas**
 - Para fines de contabilidad
- **Fallos**
 - Detección,
 - Historial de fallos y sus soluciones
- Los sistemas de gestión de incidencias son buenos para esto

Expectativas

Una red en operación debe ser monitorizada para:

- Asegurar los SLA proyectados (Acuerdos de Nivel de Servicio)
- Los SLAs dependen de políticas
 - Qué espera la dirección?
 - Qué esperan los usuarios?
 - Qué esperan los clientes?
 - Qué espera el resto de la Internet?
- Qué se considera bueno? 99.999% de disponibilidad?
 - No hay tal cosa como disponibilidad 100% →

Expectativas de Disponibilidad

Qué hace falta para 99.9 %?

30.5 días x 24 horas = 732 horas por mes

$(732 - (732 \times .999)) \times 60 = 44$ minutos

Sólo 44 minutos de baja por mes!

Tiene que apagar 1 hora por semana?

$(732 - 4) / 732 \times 100 = 99.4 \%$

Recuerde tomar en cuenta el tiempo de baja planeado, e informe a sus usuarios si está o no incluido en el SLA

Cómo se mide la disponibilidad?

En el núcleo (core) ? Extremo a extremo? Desde la Internet?

Puntos de Referencia

Qué se considera normal en su red?

Si nunca ha monitorizado su red, tendrá que saber cosas como:

- Carga típica de los enlaces (→ Cacti)
- Nivel de variabilidad (jitter) entre dos puntos (→ Smokeping)
- Utilización típica de recursos
- Niveles de “ruido” típicos:
 - Escaneos de red
 - Datos descartados
 - Errores reportados y fallos

Por qué hacer todo esto?

Saber cuándo se necesita una mejora

- Su ancho de banda está saturado?
- A dónde vá su tráfico?
- Necesita un enlace de más capacidad, u otro proveedor?
- Es demasiado viejo el equipo?

Mantener una auditoría de cambios

- Anotar todos los cambios
- Facilita conocer el origen de los problemas después de cambios y actualizaciones

Mantenga un histórico de las operaciones

- Use un sistema de gestión de incidencias
- Le permite protegerse y saber lo que ha ocurrido

Por qué la gestión de redes?

Contabilidad

- Medir el uso de los recursos
- Cobrar a clientes basado en utilización

Saber cuándo hay problemas

- Entérese antes que los usuarios, sino quedará mal!
- El sistema de gestión puede crear incidencias y notificar al equipo técnico

Tendencias

- Toda esta información sirve para ver las tendencias en la red
- Esto es parte del establecimiento de un punto de referencia, planificación de la capacidad, etc.

Los tres “grandes” elementos

Disponibilidad

- [Nagios](#) Servicios, servidores, enrutadores, etc.

Fiabilidad

- [Smokeping](#) Retardo, pérdidas, variabilidad

Rendimiento

- [Cacti](#) Utilización de enlaces, CPU, memoria, disco, etc.

Existe cierta coincidencia de funcionalidades entre los tres

Detección de ataques

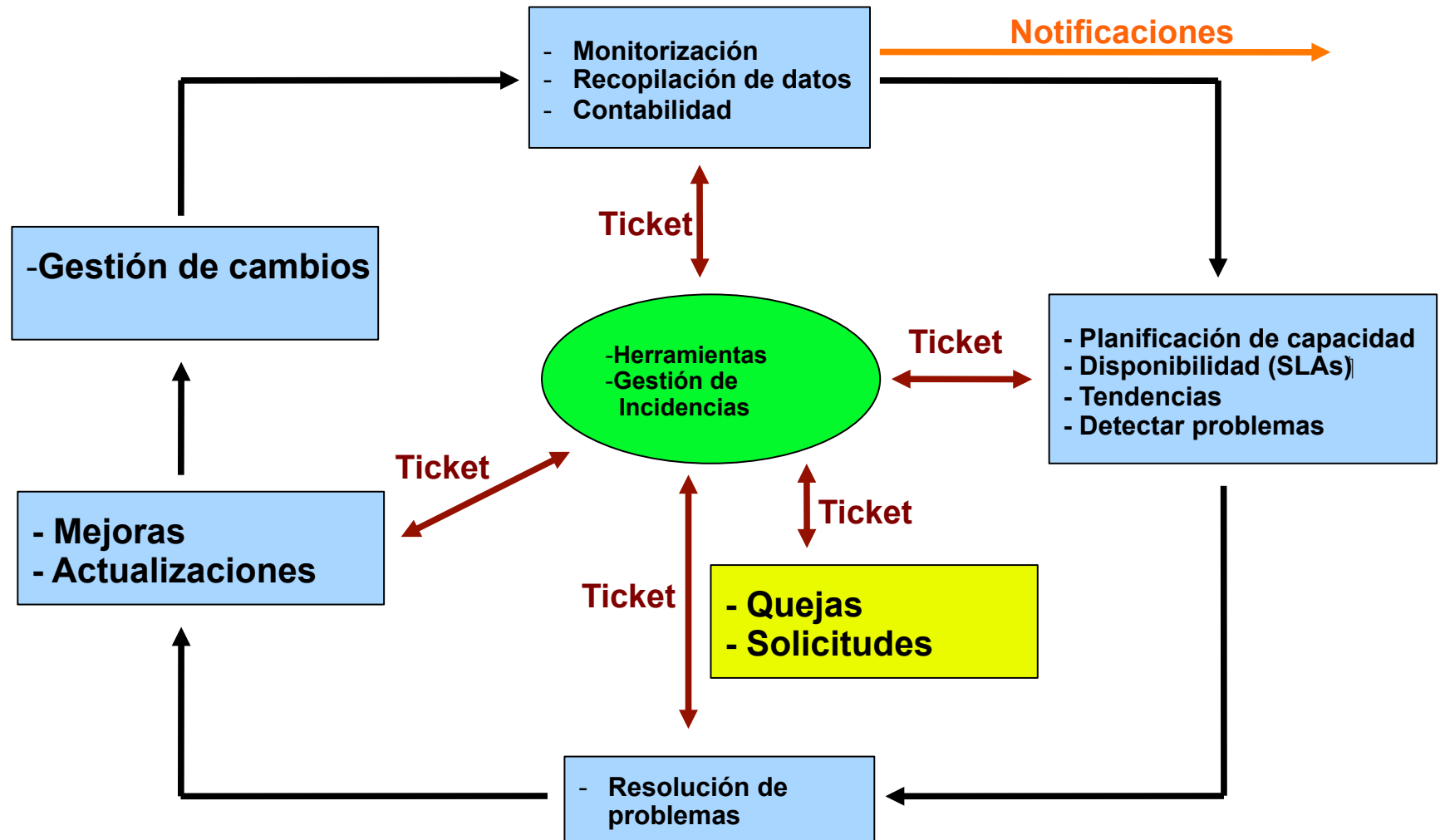
- La utilización de las tendencias y la automatización, permiten determinar cuándo es víctima de un ataque
- Las herramientas le pueden ayudar a mitigar estos ataques:
 - Flujos (netflow) a través de interfaces
 - Saturación de servicios o servidores específicos
 - Fallos en múltiples servicios

Consolidación de Datos

El Centro de Operaciones de la Red (COR, o NOC) es “Donde ocurre todo”

- Coordinación de tareas
- Estado de la red y los servicios
- Atención de incidencias y quejas
- Donde residen las herramientas (“servidor NOC”)
- Documentación que incluye:
 - Diagramas de red
 - Asignación de puertos en conmutadores y enrutadores
 - Descripción de la red
 - Y como veremos mas adelante, mucho más

Visión General



Unas *pocas* soluciones Open Source...

Rendimiento

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

Manejo de Incidencias

- RT*
- Trac*
- Redmine

Gestión de Cambios

- Mercurial
- Rancid* (routers)
- CVS*
- Subversion*
- git*

Seguridad/(SDI)

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

Registro de Eventos

- swatch*
- syslog-ng/rsyslog*
- tenshi*

Gestión de Redes

- Big Brother
- Cacti*
- Hyperic
- Munin
- Nagios*
- OpenNMS*
- Observium*
- Sysmon
- Zabbix

Documentación

- IPplan
- Netdisco
- Netdot*
- Rack Table

Protocolos/Utilidades

- SNMP*, Perl, ping

Preguntas hasta ahora?

?

Sección II: Detalles

Algunos detalles sobre los conceptos :

- Continuación de la Documentación de Redes
- Herramientas de Diagnóstico
- Herramientas de Monitorizado
- Herramientas de Rendimiento
- Herramientas Activas y Pasivas
- SNMP
- Sistemas de Gestión de Incidentes
- Gestión de configuración y cambios

Sección III: Detalles

Algunos detalles acerca de los conceptos claves:

- Herramientas de Diagnóstico
- Herramientas de Monitorizado
- Herramientas de Rendimiento
- Herramientas Activas y Pasivas
- SNMP
- Sistemas de Gestión de Incidentes
- Gestión de configuración y cambios

Sistemas de monitorización

Tres tipos de herramientas

1. **Diagnóstico** – probar conectividad, comprobar que una ubicación es alcanzable, o que un dispositivo está disponible. Generalmente herramientas activas.
2. **Monitorización** – ejecución en segundo plano ("demonios" o servicios, que recopilan eventos, pero que también pueden iniciar sus propias verificaciones de estado (usando herramientas de diagnóstico), y anotan el resultado, de manera programada.
3. **Rendimiento** – Nos dicen cómo la red está manejando los flujos de datos

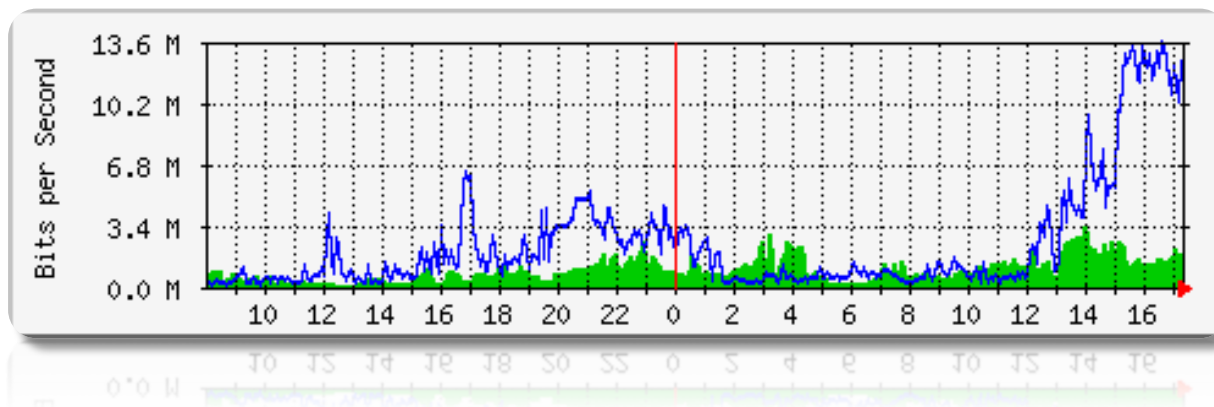
Sistemas y herramientas de monitorización

3. Herramientas de rendimiento

Mirar cada interfaz del enrutador y conmutadores

Dos herramientas populares:

- Netflow/NfSen: <http://nfsen.sourceforge.net/>
- MRTG: <http://oss.oetiker.ch/mrtg/>



MRTG = “Multi
Router Traffic
Grapher”

Sistemas y herramientas de monitorización

Herramientas activas

- Ping – Probar conectividad hacia un nodo
- Traceroute – Mostrar la ruta de los paquetes
- MTR – Combinación de ping + traceroute
- Colectores de SNMP (polling)

Herramientas Pasivas

- Monitorización de eventos, SNMP traps, NetFlow

Herramientas Automáticas

- SmokePing – Recopilar y graficar el retardo en alcanzar nodos y servicios, usando ICMP (Ping) y otros métodos
- MRTG/RRD – Recopilar y graficar la utilización del canal en cada interfaz de un dispositivo

Sistemas y herramientas de monitorización

Monitorizado de la red y servicios

- Nagios – Monitor de servidores y servicios
 - Puede monitorizar prácticamente de todo
 - HTTP, SMTP, DNS, Disco, CPU, ...
 - Fácil de escribir nuevas extensiones (plug-ins)
- Solo requiere conocimiento básico de *programación* para desarrollar nuevas pruebas – Perl, Shell scripts, php, etc...
- Muchas buenas opciones de Fuente Abierta
 - Zabbix, ZenOSS, Hyperic, OpenNMS ...
- Los mecanismos de dependencias son muy útiles

Sistemas y herramientas de monitorización

Monitorice sus servicios críticos

- DNS/Web/Email
- Radius/LDAP/SQL
- SSH

Cómo va a recibir alarmas?

No olvide la gestión de eventos!

- Cada dispositivo de red (así como servidores Linux y Windows) pueden reportar eventos usando Syslog
- Debe recopilar y monitorizar sus archivos de eventos!
 - No hacerlo es uno de los principales errores en la gestión de red

Protocolos de Gestión de Red

SNMP – Simple Network Management Protocol

- Estándar de la industria, cientos de herramientas
- Presente en cualquier elemento de red decente
 - Utilización de canal, errores, CPU, temperatura, ...
- Disco, procesos, ...
- UNIX y Windows también lo implementan

SSH y telnet

- También es posible usar scripts (programas sencillos) para monitorizar remotamente

Herramientas SNMP

Conjunto de herramientas Net SNMP

- <http://net-snmp.sourceforge.net/>

Muy sencillo desarrollar herramientas basadas en estas utilidades

- Recopilar las tablas ARP de enrutadores
- Recopilar las tablas de conmutación de los switches
- Solicitar el estado de un arreglo de discos en RAID.
- Solicitar las temperaturas de servidores, enrutadores, etc.

Herramientas de estadísticas

Contabilidad y Análisis de Tráfico

- Cómo está siendo utilizada la red, y qué tanto
- Util para calidad de servicio (QoS), detectar abusos, y facturación
- Protocolo dedicado: NetFlow
- Identificar flujos de tráfico: protocolo, fuente, destino, bytes
- Diferentes herramientas
 - Flowtools, flowc
 - NFSen
 - Muchas más: <http://www.networkuptime.com/tools/netflow/>

Gestión de Fallos

Es transitorio el problema?

- Sobrecarga, falta temporal de recursos

Es permanente el problema?

- Fallo del equipo, línea caída

Cómo detectar un problema?

- Monitorización!
- Quejas

Un sistema de incidencias es esencial

- Abrir ticket para seguir un evento (ya sea planificado o por fallo)
- Definir reglas de escalado
 - Quién es responsable de resolver el problema?
 - A quién se le asigna si éste no está disponible?

Sistemas de Incidencias

Por qué son importantes?

- Seguir todos los eventos, fallos y problemas

Punto central de comunicación del Help Desk

Utilízelo para registrar toda comunicación

- Tanto interna como externa

Eventos originados desde fuera:

- Quejas de clientes

Eventos originados desde dentro:

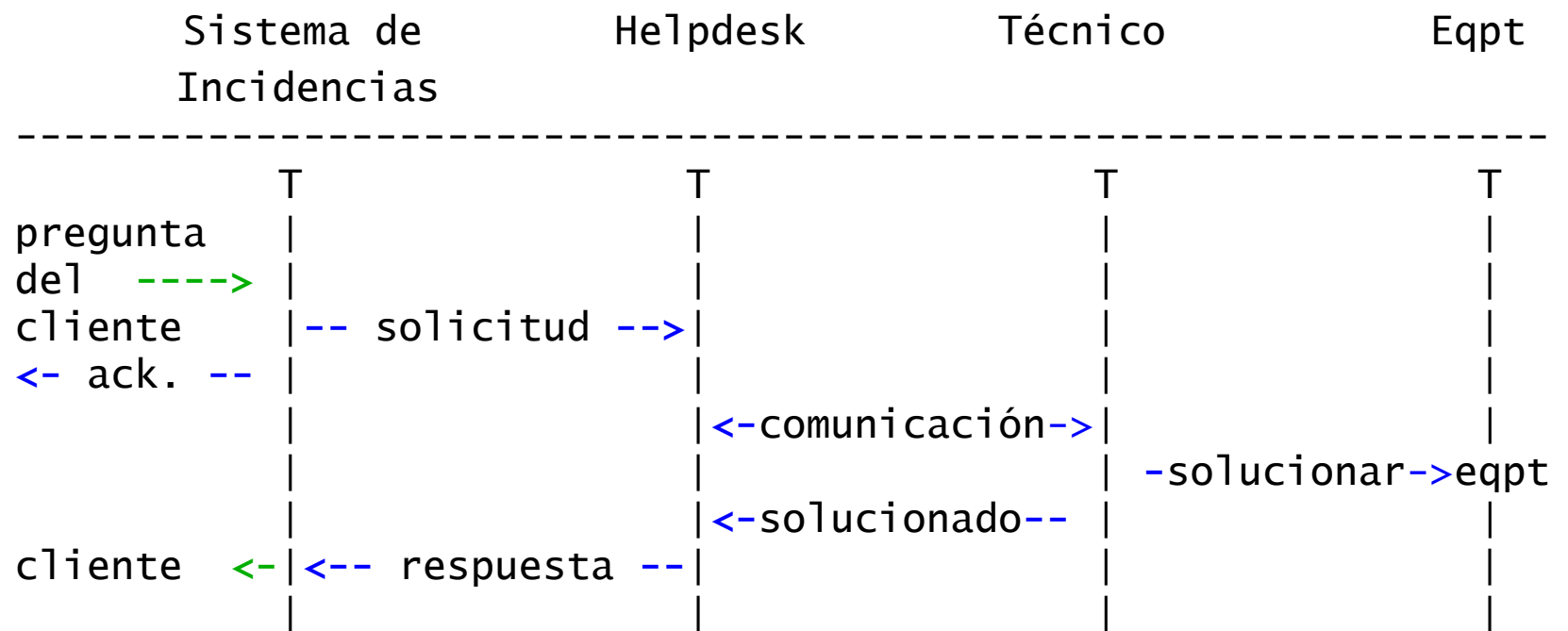
- Salidas de servicio de sistemas
- Actualizaciones o mantenimiento planificados – Recuerde notificar a los clientes!

Sistemas de Incidencias

- A cada caso se le asigna un número
- Cada caso atraviesa un ciclo similar:
 - Nuevo
 - Abierto
 - ...
 - Resuelto
 - Cerrado

Sistemas de Incidencias

Flujo de tareas:



Sistemas de incidencias: Ejemplos

RT (Request Tracker)

- Muy usado mundialmente.
- Un sistema clásico de incidencias que se puede ajustar a cada entidad.
- Un poco difícil de instalar y configurar.
- Puede manejar grandes volúmenes de transacciones

Trac

- Sistema híbrido que incluye wiki y manejo de proyectos
- Sistema de incidencias inferior a RT, pero funciona bien
- Usado para seguir proyectos de grupo

Redmine

- Como trac, pero más robusto. Mucho más difícil de instalar.

Sistemas de Detección de Intrusiones de Red (SDI)

Programas que observan los flujos de tráfico y envían alarmas cuando detectan cosas como:

- Nodos infectados o que actúan como fuentes de Spam.

Algunas herramientas:

- **SNORT** – Un sistema IDS muy popular:
<http://www.snort.org/>
- **Prelude** – Sistema de Gestión de Información de Seguridad
<https://dev.prelude-technologies.com/>
- **Samhain** – SDI Centralizado
<http://la-samhna.de/samhain/>
- **Nessus** – Escáner de vulnerabilidades:
<http://www.nessus.org/download/>

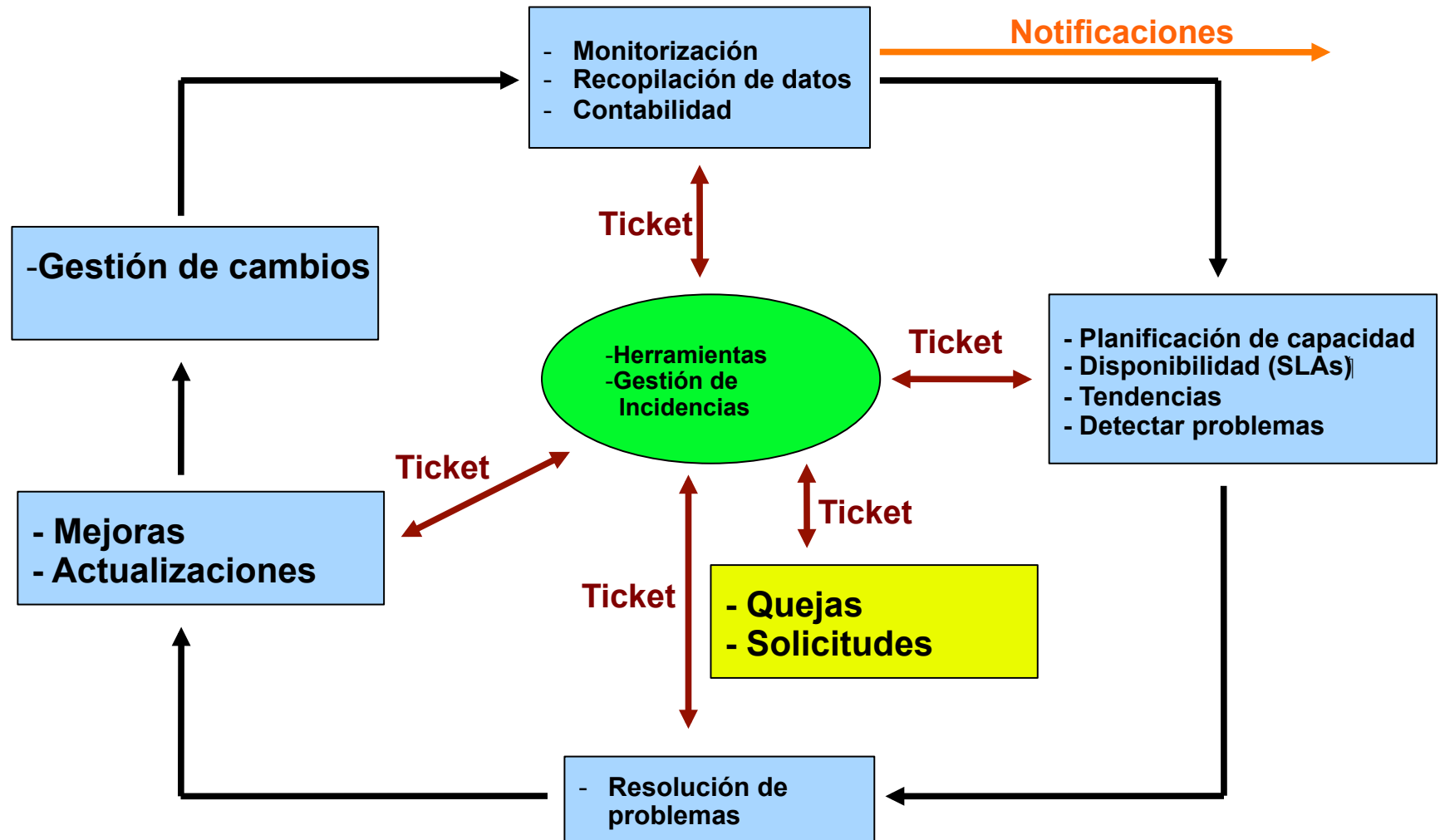
Gestión y monitorización de configuraciones

- Registrar cambios en configuraciones de equipos de red usando *control de versiones*
- Gestión de Inventario (Equipos, IPs, interfaces)
- Usar control de versiones
 - Tan simple como:
`"cp named.conf named.conf.20070827-01"`
- Para archivos de configuración:
 - **CVS, Subversion (SVN)**
 - **Mercurial**
- Para enrutadores:
 - **RANCID**

Gestión y monitorización de configuraciones

- Se solía usar para código fuente (programas)
- Funciona bien para cualquier configuración en formato texto
 - También para archivos binarios, pero no es posible ver diferencias
- Para equipos de red:
 - **RANCID** (Recopilación y registro automático de configuraciones para Cisco y otros fabricantes)
- Incluido en software de gestión de proyectos como:
 - **Trac**
 - **Redmine**
 - Y muchos otros productos de Wikis. Excelente para documentar la red.

Revisión de la visión general



Preguntas

?