



Detección y corrección de fallos

Introducción a la gestión de fallos

¿Qué es un fallo de red?

2

- ❑ Cualquier problema detectado en dispositivos de red, servidores, servicios....,
- ❑ Fallo hace que haya comportamientos no adecuados:
 - ❑ Reinicio inesperado de servidores.
 - ❑ No respuesta de un servidor.
 - ❑ Servicios con tiempos de respuesta largos.
 - ❑ Reenvío incorrecto de paquetes por routers.
 - ❑

□ Consiste en:

- ▣ Identificar el fallo en la red de datos.
- ▣ Aislar la causa del fallo.
- ▣ Solucionarlo.

□ Beneficios:

- ▣ Mejora la fiabilidad y efectividad de la red
- ▣ Repercuten en:
 - Mejora del rendimiento de los empleados/clientes
 - Mejora de la percepción de calidad

- **Informes** de problemas:
 - ▣ Enviados por usuarios: email, completar formulario en página web, teléfono...
 - ▣ Informan sobre la observación de un funcionamiento incorrecto: el usuario indica **síntomas**.
- Los **síntomas** sólo son pistas, el gestor debe **investigar** sobre las **causas** del problema.



Resolución de problemas y diagnosis

5

- **Objetivo:** Encontrar la causa de un problema

- **Informe:**

- Muy general, no da información concreta
- Realizado por usuarios sin conocimientos de la red
- Es el punto de partida



- **Diagnosis:**

- El administrador, con conocimientos técnicos, puede:
 - Analizar los componentes de la red que dan problemas
 - Hacer observaciones propias con información más precisa sobre la posible causa del problema



Resolución de problemas y diagnosis

6

□ Pasos:

- Recibir informe (síntoma).
- Establece una hipótesis sobre las posibles causas.
- Investigar para verificar la fuente del problema.
 - Ayudarse de herramientas de diagnosis en la observación más precisa del problema y la búsqueda de la causa.
- Aislar el problema: realiza las acciones necesarias para resolverlo.

Dificultades en el análisis de un problema

7

- Información insuficiente o ambigua.
- Múltiples causas potenciales.
- Propagación del fallo con múltiples observaciones.
- Destrucción de pistas por procedimientos de recuperación.
 - ▣ Ejemplos:
 - TCP recupera paquetes perdidos en IP.
 - Proceso de recuperación automática recupera ficheros dañados.

Prevención de fallos

8

- Una **política adecuada** en la gestión de fallos es la **prevención**.
- Para aplicar prevención de fallos es necesario **monitorizar** parámetros que nos **alerten de la evolución de un indicador** que pueda llegar a ser un **potencial problema**.
- La **gestión de rendimiento y planificación** puede ayudar a detectar posibles **fallos**.
- Ejemplo:
 - ▣ Monitorizar la evolución de utilización de recursos: disco duro, memoria, CPU, ancho de banda.



Detección y corrección de fallos

Monitorización

- Permite **observar parámetros críticos** para detectar posibles problemas.
- Ejemplo: monitorización de tráfico
 - ▣ Monitorizar la evolución del tráfico de salida a Internet de un ISP con el tiempo.
 - ▣ Si hay una caída de tráfico repentina en algún instante de tiempo puede indicar un problema.



□ Problemas de la monitorización:

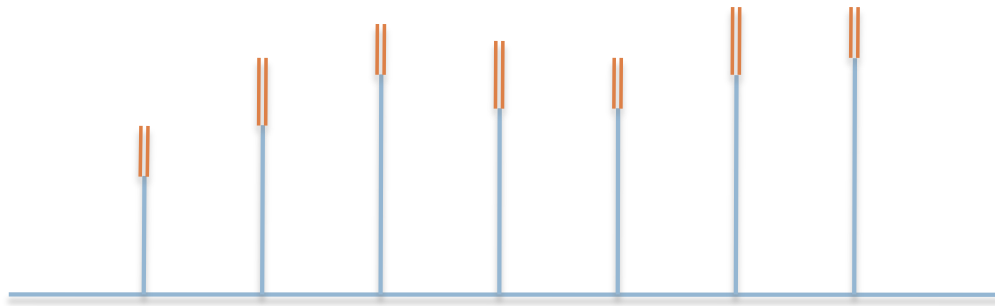
1. **Redes grandes**: imposible monitorizar y observar miles de dispositivos
2. **Comportamiento del tráfico** con fuertes variaciones: hay horas en las que cae fuertemente (ejemplo noche)

□ Solución:

- ▣ Monitorización automática con detección de anomalías
- ▣ Detección de anomalías basada en la observación y comparación estadística, Machine Learning....

□ Ejemplo:

1. Medir el tráfico durante la semana en periodos de 30 minutos
2. Obtener estadísticos (media, desviación estándar) en cada punto de la semana (de media hora)
3. Observar desviaciones de una semana sobre el valor observado en ese punto en semanas anteriores.



Ejemplos de parámetros a monitorizar

13

- Interfaces: permite **localizar problemas** en los interfaces.
 - ▣ ifOperStatus: estado operacional (up1/down2/testing3).
 - ▣ ifAdminStatus: estado administrativo (up1/down2/testing3).
 - ▣ ifLastChange: tiempo desde cambio a estado operacional.

□ ip: **seguimiento de problemas**

□ ipRouteTable: tabla de rutas IP.

- ipRouteType e IpRouteProto permiten conocer cómo fue aprendida la información de las rutas.
- IpRouteNextHop permite conocer el próximo salto en una entrada de ruta.
- IfRouteIfIndex es el interfaz (ifIndex) de salida de una ruta.
- Los 5 objetos ipRouteMetric que permiten conocer la configuración de las métricas.

□ ipNetToMediaTable: tabla de traducción de direcciones

Herramientas de monitorización

15

- Ofrecidas por los **fabricantes** de los productos:
 - ▣ Conmutadores, Routers (enlaces...)
 - ▣ Conexiones WAN
 - ▣ Servidores (email, Web, DNS, Base de datos...)
 - ▣ Aplicaciones software
 - ▣ Impresoras
 - ▣ Bases de datos
 - ▣ Servicios y mecanismos de seguridad
- Desarrolladas por **terceros**:
 - ▣ Network Monitoring tools:
 - <http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html>
 - <https://www.comparitech.com/net-admin/network-monitoring-tools/>



Detección y corrección de fallos

Eventos

Correlación de eventos

17

- Hemos visto cómo se pueden aplicar técnicas de detección de anomalías (modelado estadístico de la observación).
- Una **detección de anomalía** provoca un **evento**.
- La **correlación de varios eventos** puede **ayudar** a la **localización de la causa** de un problema. Ejemplos:
 - ▣ Eventos de múltiples interfaces de un mismo conmutador indica problema en el conmutador.
 - ▣ Eventos de varios routers de una misma zona.
 - ▣ Eventos en servidor de bases de datos y web pueden estar relacionados.

Etapas de la correlación de eventos

18

1. Filtrado de eventos:

- ▣ Descartar eventos irrelevantes

2. Agregación de eventos:

- ▣ Agrupar eventos similares o duplicados

3. Enmascarado:

- ▣ Ignorar eventos relacionados con el fallo estudiado
- ▣ ejem: “**no alcanzar el servidor**” se enmascara con “**fallo en el router**” que da acceso al servidor

4. Raíz de la causa:

- ▣ Analizar dependencias entre eventos (grafos de dependencias)
- ▣ ¿Unos eventos pueden ser explicados por otros?

Respuesta a eventos

- Se puede implementar acciones de **respuesta automática**.
- Nos podemos ayudar de **herramientas de toma de decisiones**:
 - ▣ Ejemplo de herramienta: ILOG JRules de IBM
 - ▣ http://en.wikipedia.org/wiki/IBM_Operational_Decision_Management
 - ▣ Permite definir conjuntos de condiciones y acciones a tomar en caso de cumplirse
 - ▣ Ejemplo de aplicación: PROPUESTA DE DISEÑO DE CORRELACION DE ALARMAS PARA ASOCIAR EVENTOS SIMILARES OCURRIDOS EN LA RED IP MPLS BASADO EN CENTRALES CDMA . Marina de Jesús Viña.