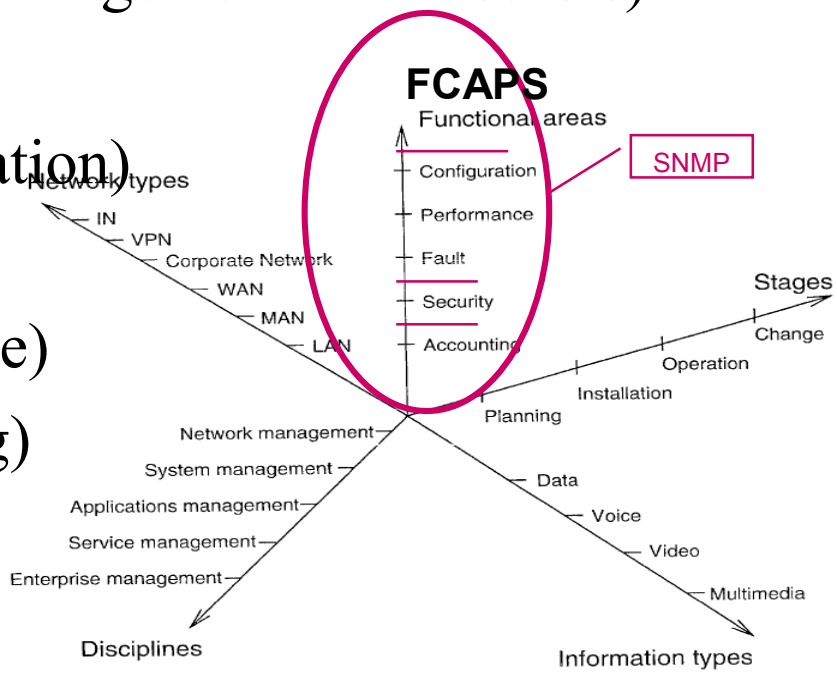
T2. Áreas funcionales de la gestión de red

Gestión de Redes de Comunicaciones

2002/03

- Áreas funcionales de la gestión de red
  - Configuración (Configuration)
  - Fallos (Fault)
  - Prestaciones (Performance)
  - Contabilidad (Accounting)
  - Seguridad (Segurity)

- Funciones de la gestión.
  - La gestión de un sistema distribuido es un sistema distribuido.
  - Abierto "solución multivendedor"
- Áreas funcionales (OSI Management Architecture) FCAPS
  - Configuración (Configuration)
  - Fallos (Fault)
  - Prestaciones (Performance)
  - Contabilidad (Accounting)
  - Seguridad (Segurity)



G. de la Configuración

- ¿ Configuración?
  - Descripción de un S.D.
    - Física: que equipos,...
    - Geográfica: donde y como conectados
  - El proceso de configuración
    - Manipulación de la estructura, poner y cambiar valores que controlan el funcionamiento habitual del sistema
  - El resultado del proceso de configuración
    - “los valores resultantes”
- Adaptación del sistema al entorno operativo

G. de la Configuración

- Incluye:
  - Instalar nuevo sw.
  - Retocar viejo sw.
  - Conectar dispositivos
  - Cambios en topología y tráfico
- Control sw de aspectos que acompañan a la instalación física

  PARAMETROS
  - Ejem. IP, MTU, mascara de red, servicios, BPS, routers

G. de la Configuración

- Herramientas de configuración: Criterios
  - Localización de la conf.
    - Distinto equipo
    - Compatibilidad
    - Seguridad
  - Almacenamiento de la conf.
    - Permite cambios: NVRAM, FD, HD
    - No permite cambios (E)EPROM
    - Distante, se carga en el arranque BOOTP, DHCP
  - Validez de la configuración
    - Conf. Estática: parar y arrancar
    - Conf. dinámica

- Herramientas de configuración: Criterios (II)
  - Interfaz de usuario del “configurador”.
    - Facilidad y rapidez de cambiar parámetros
    - En muchos dispositivos.
  - Perfiles de conf./versiones/macros de configuración
  - seguridad/niveles de seguridad.

G. de la Configuración

- Funcionalidad
  - Auto-topología y auto-descubrimiento
  - Documentación de la descripción de la conf.

    Bases de datos maestras
  - Mapas de la red con datos de configuración.

    GIS
  - Herramientas para activar backup en caso de fallo.
  - H. poner y recuperar parámetros y estado sistema.
  - H. de distribución de sw y control de licencias.
  - H. supervisión y control de autorización.

G. de fallos

- Se encarga de la
  - Detección
  - Aislamiento
  - Eliminación del fallo
- ¿Fallo?
  - Toda desviación del conjunto de objetivos operacionales, servicios o funciones del sistema.

Más difícil en los sistemas basados en red: accesibilidad.

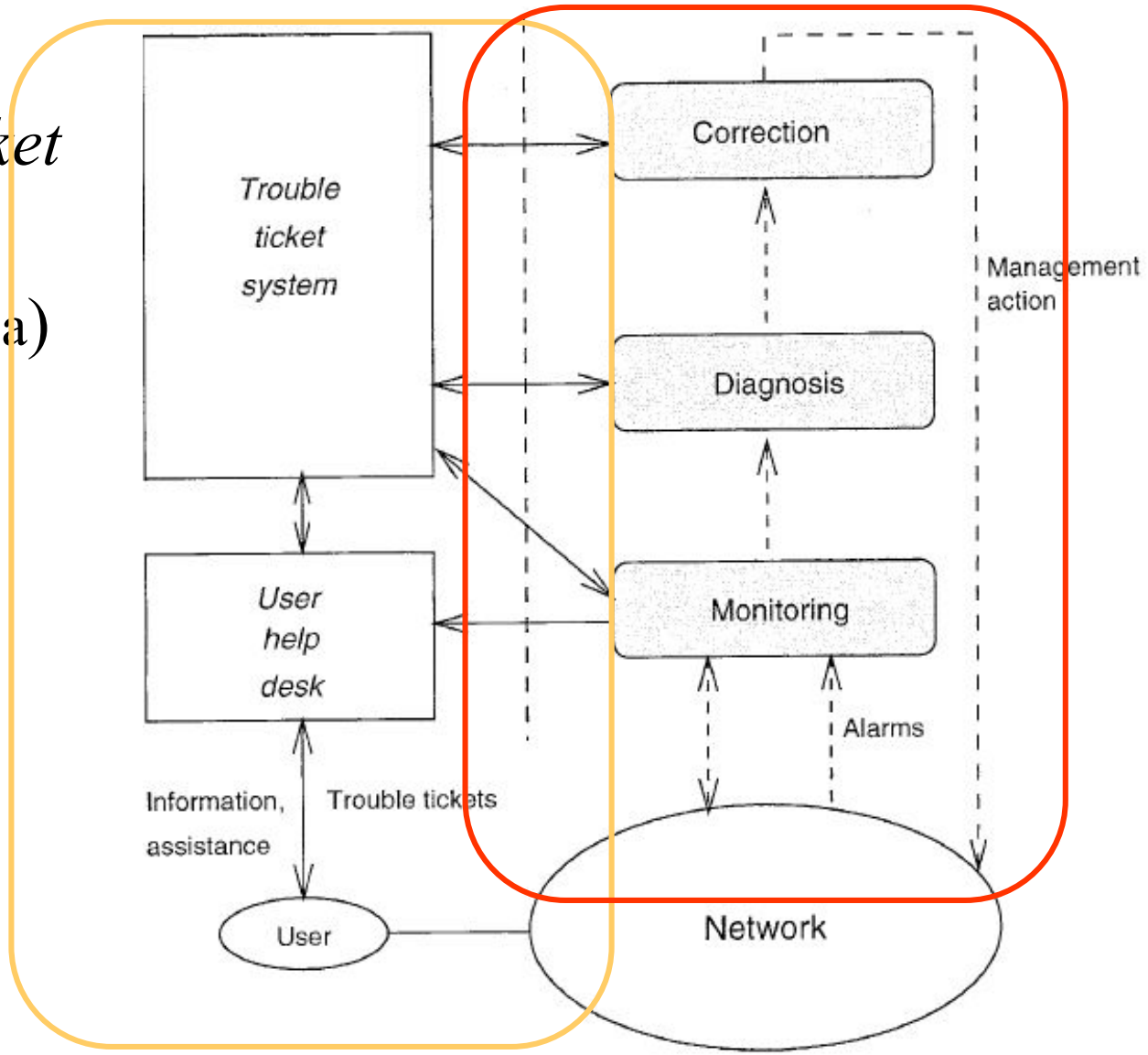
Avisan de fallos los mismos sistemas o los usuarios

La función es detectar y corregir lo antes posible para asegurar los objetivos se mantengan.

G. de fallos

- Modelo de *trouble ticket system*

(Partes de avería)



G. de fallos

- Tareas:
  - Monitorización de red y estado.
  - Responder y reaccionar a las alarmas
  - Diagnóstico de la causa del fallo: aislamiento y causa raíz
  - Propagación de error.
  - Medidas de recuperación y comprobación.
  - Sistemas de aviso de averías de usuario
  - Asistencia a usuarios.

- Ayudas técnicas
  - Auto-identificación de los componentes del sistema.
  - Prueba aislada de componentes
  - Traza de mensajes
  - Log de errores
  - Mensajes de prueba de vida para todos los niveles:

    Ping y echo
  - Recuperación de "*cores*"
  - Generación de errores de prueba.

- Ayudas técnicas (II)
  - Rutinas de autotest y pruebas de transmisión

    BER, traceroute, ping
  - Disparo de reset planificados y rearranques de puertos, grupos de puertos y componentes
  - Equipos de medida y prueba

    Reflectómetro, analizadores de protocolos, comprobadores de interfaces.
  - Soporte para mecanismos de filtrado de fallos.
  - Gestión de fallo desde la asistencia al usuario.

G. de prestaciones

Prestaciones Continuación de la gestión del fallo

- G. de fallo: para que funcione.
- G. de prestaciones: mejora de las prestaciones, garantizar calidad del servicio.

- Interfaz de servicio entre cliente y proveedor
  - Especificación de el servicio y tipo de servicio (estadístico, estático,..)
  - Parámetros de QoS
  - Descripción de operaciones de monitorización: (métodos, puntos y valores)
  - Descripción de reacciones a los cambios en los parámetros de QoS.

G. de prestaciones

- Es difícil
  - Vertical: Distintos niveles con distintos criterios de calidad. Mucho por hacer.
  - Horizontal: Más con distintos proveedores.
  - Métodos de medida ¿indirectos?

    Ejem.

    Ancho de banda / rapidez de descarga

G. de prestaciones

- Tareas
  - Establecimiento de nivel de la calidad de servicio y métricas.
  - Monitorización de recursos para la detección de cuellos de botella y desbordamiento de umbrales.
  - Mediciones y análisis de tendencias para la prevención.
  - Log históricos, proceso de datos, informes de prestaciones.
  - Modelos estadísticos de predicción de prestaciones.
  - Establecimiento de planes, medidas y cambios de planificación
  - Simulación

G. de contabilidad. Administración de usuarios

- La administración de usuarios se basa en:
  - Autentificación
  - Autorización
  - “Customización”

  Y después la contabilidad de la utilización por un usuario o grupo

Las g. de prestaciones mide la utilización global.

G. de contabilidad. Administración de usuarios

- Comprende:
  - Recopilación de datos de uso (medir y monitorizar)
  - Definición de unidades a contabilizar.
  - Mantenimiento de cuentas y logs.
  - Asignación de costes a cuentas
  - Asignación y monitorización de cuotas
  - Estadísticas de uso
  - Políticas de cuentas y tarifas

G. de contabilidad. Administración de usuarios

- Los datos se usan para:
  - Facturación de usuarios.(datos de facturación)
  - Facturación entre proveedores.
  - Política de tarifas.(Gestión de empresa).
- Asignación de costes
  - Fijos y variables
- La contabilidad de costes tb. cuesta, debe estar justificada por los beneficios obtenidos.
- ¿Datos? Bits transmitidos, duración y hora del día/semana de la conexión, velocidad y QoS de la conexión, ubicación de los otros actores, recursos de pasarela y servidor. Tb. coste fijo de la oficina, mantenimiento, amortización...

G. de la seguridad

- Trata de la protección de los recursos de la compañía
- Proteger información, infraestructuras IT, servicios y producción de amenazas de ataques o uso inadecuado.
- El análisis de amenazas y riesgos de seguridad identifican lo que debe ser protegido.

G. de la seguridad

- Amenazas: intencionadas o no.
  - Ataques pasivos: escucha de información, captura de pwd, troyanos,...
  - Ataques activos: manipulación de la información, reconfiguración, reprogramación, sobrecarga, virus,...
  - Mal funcionamiento de recursos.
  - Operación inadecuada o errónea.

G. de la seguridad

- La g de la seguridad se basa en el análisis de las amenazas y valores (recursos y servicios) que se han de proteger.
- La política de seguridad define concretamente los requerimientos de seguridad.
- Política de accesos a datos, cambio de pwd,...

G. de la seguridad

- Comprende :
  - Realización del análisis de amenazas.
  - Definición y exigencia de la política de seguridad.
  - Comprobación de identidad.
  - Establecimiento y exigencia de control de acceso.
  - Confidencialidad (encriptación)
  - Integridad de los datos (autentificación)
  - Monitorización de ataques.
  - Notificación de estado de la seguridad, ataques y violaciones.

G. de la seguridad

- Herramientas:
  - Principalmente software libre.
    http://www.cert.org/tech_tips/security_tools.html
    http://ciac.llnl.gov/ciac/SecurityTools.html
    GPGP y PGP,
    SATAN (System Administrator's Tool for Analyzing Networks),
    SAINT (Security Administrator's Integrated Network Tool).
    SARA (Security Auditor's Research Assistant)
    Tripwire (integridad de ficheros)
  - "El problema es encontrar la manera de adecuar estos procedimientos en la arquitectura de gestión y controlarlos de manera uniforme en un marco de la política de seguridad"

- El tiempo de respuesta