



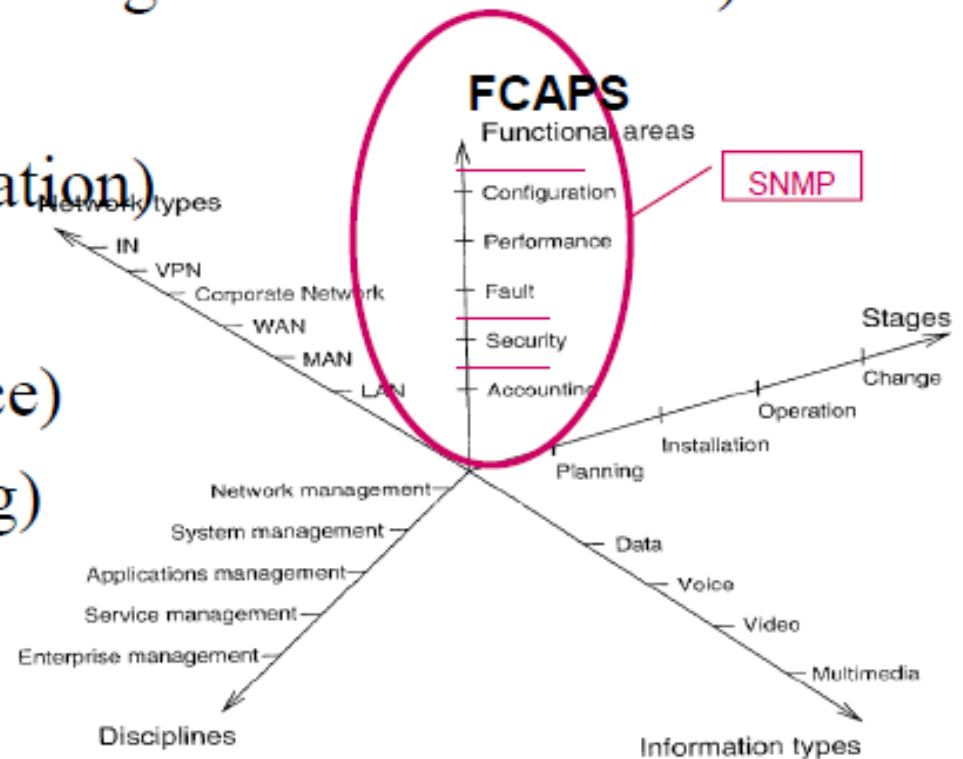
GESTION DE RED



Áreas funcionales (OSI Management Architecture)

FCAPS

- Configuración (Configuration)
- Fallos (Fault)
- Prestaciones (Performance)
- Contabilidad (Accounting)
- Seguridad (Security)



Funciones: Gestión de Configuración

◆ Descripción

- 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

Funciones: Gestión de 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, routers

Funciones: Gestión de 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

Funciones: Gestión de Configuración

- 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.

Funciones: Gestión de Configuración

- ◆ Gestión de configuración de los elementos de red:
 - Herramientas de configuración gráficas y CLI
 - Herramientas de configuración masiva y nodal
- ◆ Gestión de Inventario:
 - Herramientas de autodescubrimiento
 - Combinación con herramientas CAD de gestión de cableado
 - Base de datos utilizable por el resto de funciones
- ◆ Gestión de Topología
 - Herramientas de autotopología
 - Necesidad de distintas vistas topológicas
- ◆ Gestión de Servicios de Directorio

Funciones: Gestión de Configuración

- ◆ Documentación de la descripción de la conf.
- ◆ Bases de datos maestras
 - Mapas de la red con datos de configuración.
- ◆ 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.

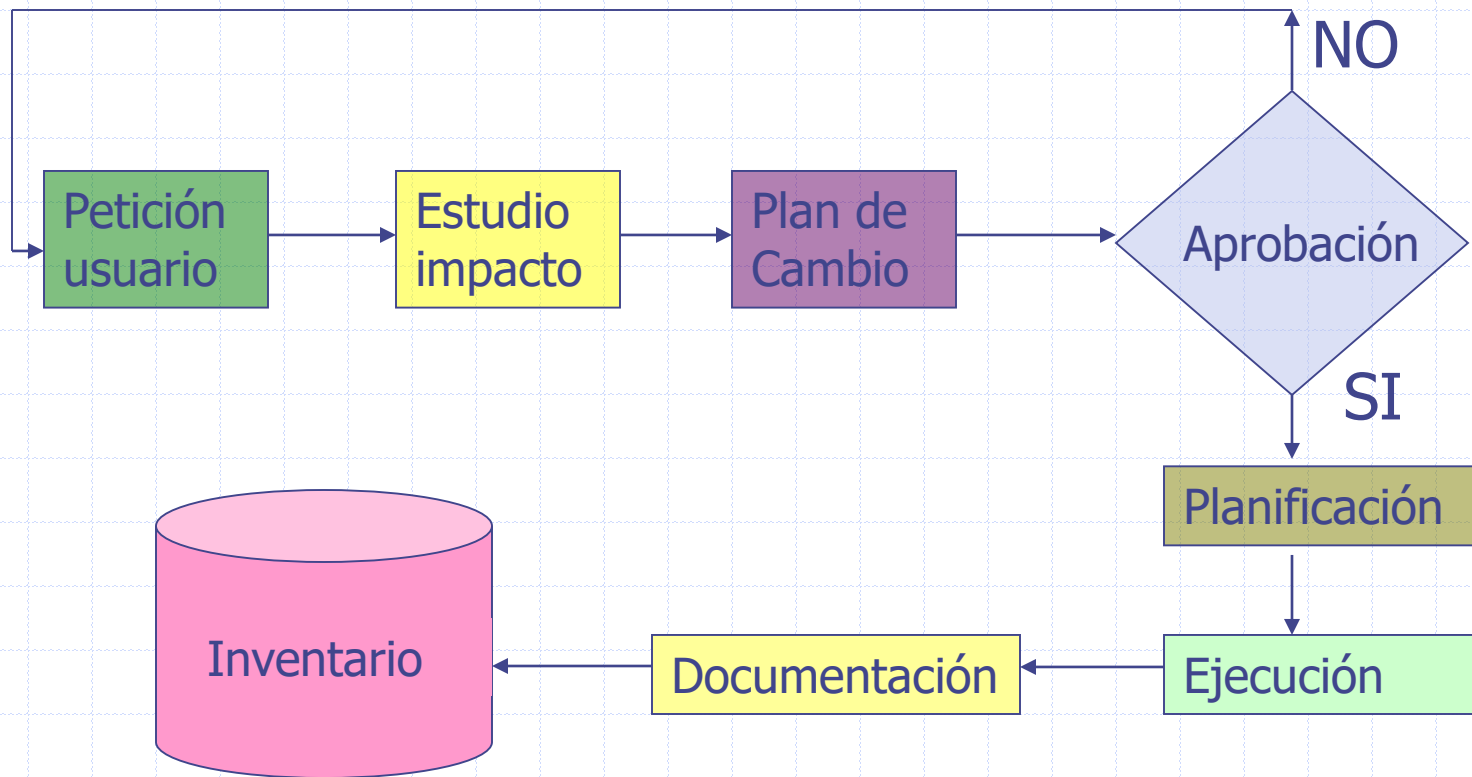
Gestión de Configuración

◆ Gestión de SLAs (Service Level Agreements): Contrato entre cliente/proveedor o entre proveedores sobre servicios a proporcionar y calidades asociadas.

- Identificación de las partes contractuales
- Identificación del trabajo a realizar
- Objetivos de niveles de servicio
- Niveles de servicio proporcionados
- Multas por incumplimiento
- Fecha de caducidad
- Cláusulas de renegociación
- Prestaciones actuales proporcionadas

Gestión de Configuración

- ◆ Gestión de Proveedores Externos (órdenes de procesamiento / aprovisionamiento)
- ◆ Gestión de Cambios (reconfiguraciones)



Funciones: Gestión 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.

Funciones: Gestión de Fallos

- ◆ Objetivo: mantener dinámicamente el nivel de servicio
- ◆ Gestión proactiva: evitar fallos detectando “tendencias” hacia fallos
 - Caracterización de tendencias: determinación de umbrales de ciertos parámetros
 - Objetivo: monitorizar estos umbrales o programar notificaciones automáticas
- ◆ Gestión reactiva: asumir que existen fallos inevitables
 - Detectar lo antes posible el fallo
 - Monitorización periódica (no es posible notificación)

Funciones: Gestión 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.

Gestión de Fallos

- ◆ Gestión del ciclo de vida de incidencias
 - Detección de problema
 - ✓ Alarma de usuarios
 - ✓ Alarma de herramientas
 - Determinación del problema
 - ✓ La información sobre el fallo puede no ser fiable en cuanto a la fuente del fallo
 - Diagnóstico del problema: procedimentado
 - Resolución del problema
 - ✓ Por operadores de help-desk (80-85%)
 - ✓ Por operadores técnicos (5-10%)
 - ✓ Por especialistas en comunicaciones (2-5%)
 - ✓ Por especialistas en aplicaciones (1-3%)
 - ✓ Por fabricantes (1-2%)

Gestión de Fallos

◆ Gestión de incidencias: TTS (Trouble Ticket Systems)

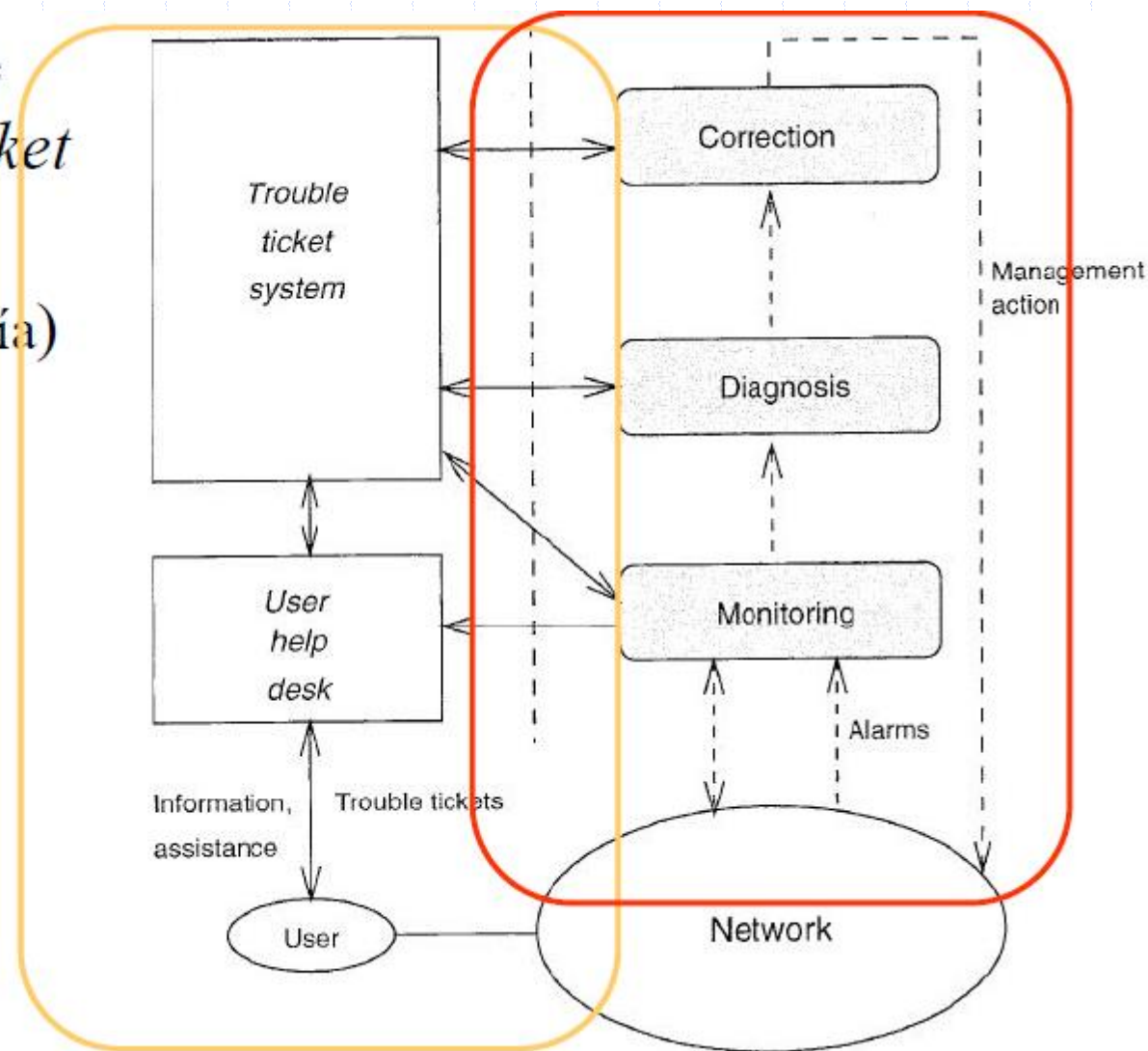
- Fecha / Hora de:
 - ✓ Informe de incidencia
 - ✓ Resolución de incidencia
- Usuario / localización
- Equipo afectado
- Descripción problema
- ESTADO
- Operador (es)
- Grado de severidad
- Historial de incidencia
- Comentarios

Gestión de Fallos

◆ Gestión de Pruebas preventivas

- Pruebas de conectividad
- Pruebas de integridad de datos
- Pruebas de integridad de protocolos
- Pruebas de saturación de datos
- Pruebas de saturación de conexiones
- Pruebas de tiempo de respuesta
- Pruebas de bucle
- Pruebas de diagnóstico

■ Modelo de
trouble ticket
system
(Partes de avería)



Funciones: Gestión 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 del 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.

Funciones: Gestión 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

Funciones: Gestión de Prestaciones

◆ Definición de indicadores de prestaciones:

- Orientados a servicio
 - ✓ Disponibilidad
 - ✓ Tiempo de Respuesta
 - ✓ Fiabilidad
- Orientados a eficiencia
 - ✓ Throughput
 - ✓ Utilización
- Monitorización de indicadores de prestaciones
- Análisis y refinamiento

Indicadores de Prestaciones: Disponibilidad

- ◆ Parámetro necesario: disponibilidad de los servicios
- ◆ Es necesario traducirlo a disponibilidad de componentes individuales
- ◆ Objetivo: maximizar (cumplir) la disponibilidad de los equipos

$$D = \frac{MTBF}{MTBF + MTTR}$$

MTBF: Mean Time Between Failures

MTTR: Mean Time To Repair

MTBF: Indicador de la calidad del equipo

MTTR: Influye:

Tiempo de detección del fallo

Política de mantenimiento utilizada

Indicadores de Prestaciones:

Tiempo de Respuesta

◆ Tiempo de Respuesta: rangos.

- >15 s: inaceptable para servicios interactivos
- >4 s: dificultan servicios interactivos encadenados (con memoria del usuario)
- 2 a 4 s: dificultan servicios interactivos que requieren concentración del usuario
- 2 s: límite aceptable normalmente
- Décimas de segundo: para aplicaciones de tipo gráfico
- <0.1 s: servicios de eco

◆ Componentes:

- Tiempo de transmisión (ida y vuelta)
- Tiempo de proceso de servicio

Indicadores de Prestaciones

◆ Fiabilidad:

- Monitorización de errores: síntomas de fallos.

◆ Throughput:

- Medida de eficiencia de servicio
- Ej: número de transacciones por minuto, número de llamadas cursadas, etc.

◆ Utilización:

- Porcentaje de uso de un recurso durante un periodo de tiempo.
- Ej: Utilización de una línea serie, utilización de una Ethernet, etc.

Funciones: Gestión de Contabilidad

- ◆ La administración de usuarios se basa en:
 - Autenticación
 - Autorización
 - Customización

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

Las g. de prestaciones mide la utilización global.

Funciones: Gestión de Contabilidad

◆ 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

Funciones: Gestión de Contabilidad

- ◆ 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 también 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...

Funciones: Gestión de 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.
- ◆ 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.

Funciones: Gestión de Seguridad

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

Funciones: Gestión de 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 (autenticación)
- Monitorización de ataques.
- Notificación de estado de la seguridad, ataques y violaciones.

Funciones: Gestión de 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)