GESTION DE REDES

1.- Introd. a los sist. de gestión de redes

2.- Monitorización de una red

3.- Control de una red

4.- Protocolos de mantenimiento

Dr. Víctor J. Sosa Sosa

Introducción a los Sistemas de Gestión de Redes

Contenidos:

I. Introducción

▪ **Gestión**: conjunto de capacidades que permiten el intercambio y procesamiento de información con el fin de ayudar a cualquier organización que opera o utiliza una red de comunicaciones, a realizar sus actividades de planificación, instalación, operación y administración con Eficacia

• Una **red de comunicaciones** consta de:
  • ***Elementos de red (ER)***: diversos tipos de equipos (sistemas de transmisión, sistemas de conmutación, terminales, concentradores, servidores, encaminadores, puentes, etc.) considerados como 'entes gestionados'
  • ***Elementos de gestión (EG)***: elementos encargados de monitorizar, coordinar y controlar a los ER

• Al ser las redes cada vez más complejas, se hace necesario contar con **herramientas de gestión de red** para controlar posibles fallos o degradaciones en las prestaciones de la red

II. Visión tradicional de la Gestión de Red

• El aumento de tamaño y complejidad en las redes hace que la probabilidad de fallos e ineficiencia crezca

  ❖ El coste de un fallo puede ser muy elevado, tanto en términos económicos como cualitativos (comunicaciones espaciales, transacciones bancarias, redes de centros de investigación)

• La gestión de la red es un elemento clave en toda organización

•Tradicionalmente, cada fabricante implementaba sus propios métodos de gestión
  ❖ Muchos procesos y herramientas
  ❖ Los elementos de red tenían una funcionalidad básica
  ❖ Los elementos de gestión controlaban a los ER
  ❖ No se podían compartir datos ni recursos lógicos entre los EG
• Así, la gestión de red resultaba ineficiente, compleja y cara

II. Visión tradicional de la Gestión de Red

• La solución pasa por unificar criterios en cuanto a:
  - qué se debe monitorizar
  - cómo se debe interpretar
  - cómo se debe controlar el proceso de gestión y análisis

... de manera que sean válidos para entornos heterogéneos y soporten los cambios tecnológicos

• Se requiere por tanto una **estandarización** a varios niveles para conseguir una **gestión de red integrada**:
  - Estándares para la unificación del acceso a los ER
    - ✓ Estructuras de las bases de datos de los ER
    - ✓ Protocolos de gestión para acceder a ellas
  - Estándares para la unificación del significado de la información gestionada o recogida de los ER
  - Estándares para la unificación de los entornos o sistemas de procesamiento de los datos capturados

Objetivo de la gestión de red

reducir los riesgos y costos asociados con las operaciones de una red, manteniéndola en continuo servicio con el requisito de que los costos de gestión sean 'razonables', definiendo un compromiso entre la calidad del servicio ofrecido y su costo de gestión.

III. Sistemas de Gestión de Red

- Un **sistema de gestión de red** es un conjunto de herramientas integradas para la monitorización y control de la red:
  - Interfaz de operador único con capacidad para ejecutar la mayor parte de las tareas de gestión
  - Cantidad mínima de equipo adicional
  - El soporte HW o SW necesario está incorporado en el equipo de usuario existente

- Un **sistema de gestión de red** está diseñado para ver la red completa como una arquitectura única:
  - Direcciones y etiquetas asignadas a cada punto
  - Conociendo los atributos de cada elemento y enlace

III.A. Configuración de un sistema de Gestión de Red

Un sistema de gestión de red (**SGR**) consta de los siguientes elementos:

- ***Entidad de gestión de red*** **(*EGR*)**: está presente en cada nodo o ER, y realiza las siguiente tareas:
  - ✓ Recoger y almacenar localmente estadísticas de actividad de la red
  - ✓ Almacenar estadísticas locales
  - ✓ Responder a comandos del Centro de Control de Red
    - Transmitir estadísticas al CCR, cambiar parámetros, proporcionar información de estado, generar tráfico artificial para pruebas
- ***Aplicación de gestión de red*** **(*AGR*)**: incluye un interfaz de operador para la gestión de la red por parte de un usuario autorizado
  - ✓ Muestra información y/o genera comandos o peticiones a los EGR's a través de la red en respuesta a los comandos del usuario
- La comunicación entre AGR y EGRs emplea un protocolo del nivel de aplicación, como cualquier aplicación distribuida

III.A. Configuración de un sistema de Gestión de Red

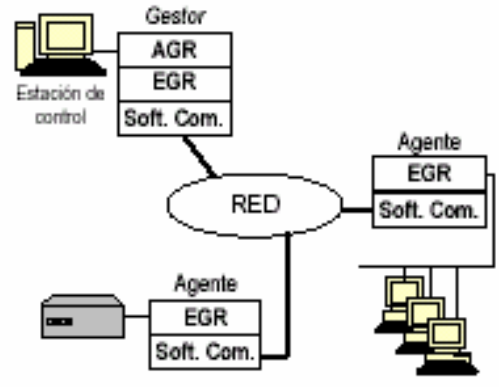
- ***Agentes***: Cada nodo que forma parte del sistema de gestión (un elemento de red) y que incluye un EGR o Incluyen tanto sistemas finales como conmutadores, encaminadores, puentes ...
- ***Centro de Control de Red (CCR) o gestor***: Además de su EGR, contiene el software del AGR
  - Puede haber uno (**arquitectura centralizada**) o varios (**arquitectura distribuida**)

- Tanto los gestores como los agentes utilizan las **MIB** (*Management Information Base*), para almacenar información relacionada con el sistema de gestión
  - La **MIB de un agente** contiene información de ese dispositivo
  - La **MIB de un gestor** contiene información de todos los agentes que controla

III.A. Configuración de un sistema de Gestión de Red

Sistema de gestión centralizado: Solamente existe un gestor en la red

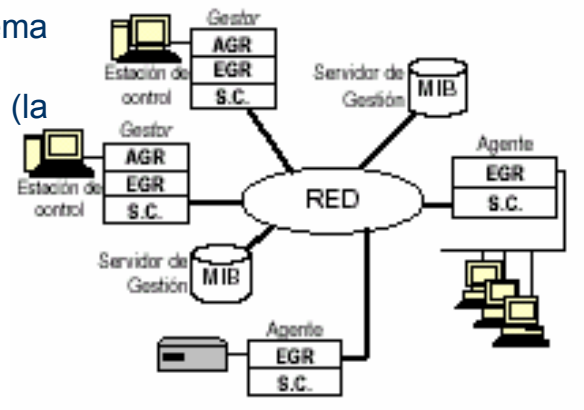
- Normalmente, hay alguno más como sistema de reserva en caso de fallos
- Permite que un único responsable mantenga toda la red



III.A. Configuración de un sistema de Gestión de Red

La tendencia es hacia un **sistema de gestión distribuido**, donde existen varios gestores con acceso limitado, y una estación gestora central con acceso global capaz de controlar todos los recursos de la red

- Mantiene la capacidad del sistema centralizado
- Minimiza el tráfico de gestión (la mayoría no sale de un entorno local)
- Mayor escalabilidad
- Mayor tolerancia a fallos



III.B. Información de un Sistema de Gestión de Red

Información estática: información que caracteriza la configuración actual y los elementos de red; cambia con muy poca frecuencia

Ej.: Identificación de puertos de encaminadores

Información dinámica: información relacionada con eventos en la red

Ej.: Transmisión de un paquete

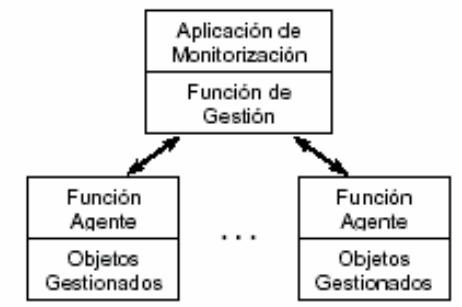
Información estadística: información derivada de la información dinámica

Ej.: Número medio de paquetes transmitidos por unidad de tiempo por un elemento de red

III.C. Componentes de un Sistema de Gestión de Red

Funcionalmente, un **SGR** está compuesto de:

- Aplicación de Monitorización: funciones de la gestión y monitorización visibles por el usuario
- Función de Gestión: módulo que recupera la información desde los elementos de red
- Función Agente: módulo que almacena información de uno o más elementos de red, y comunica la información al gestor
- Objetos gestionados: información que representa los recursos y actividades de los elementos de red



III.D. Obtención de la información

La información útil para la gestión de red se recoge y almacena en el MIB

- Los agentes la depositan, para que los gestores la tengan disponible

Un gestor puede obtener la información mediante dos técnicas:

- ***Polling***: el gestor solicita al agente los valores de ciertos parámetros, y el agente responde con la información contenida en su MIB
  - Se requiere un gestor potente
  - Los agentes son sencillos

- **Informe de eventos**: un agente genera un informe periódico o ante la ocurrencia a algún evento determinado, indicando al gestor su estado
  - Se aprovecha mejor el ancho de banda, sobre todo si la información cambia con poca frecuencia
  - Los agentes son complejos

Normalmente, en un sistema de gestión se pueden utilizar ambos métodos

IV. Áreas funcionales

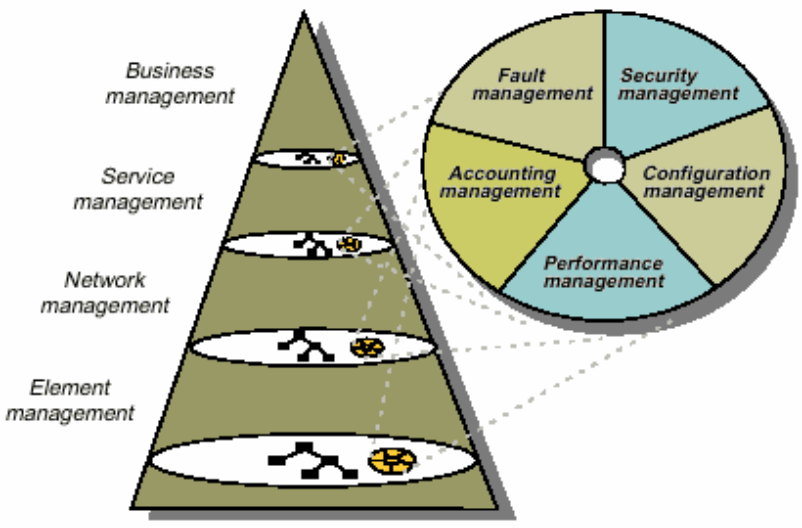
✓ El ITU-T clasifica las funciones de gestión en cinco grandes áreas funcionales*, según el ámbito de utilización

✓ Esta descomposición se desarrolló para el entorno OSI, pero ha sido ampliamente aceptada por los fabricantes de SGR

A. Gestión de fallos
B. Gestión de contabilidad
C. Gestión de configuración
D. Gestión de calidad de funcionamiento
E. Gestión de seguridad

* Este modelo funcional es conocido por sus siglas en inglés como FCAPS. Proviene de la especificación M.3400 de ITU y OSI. Las iniciales refieren a: Fault, Configuration, Accounting, Performance, Security management.

Network Management FCAPS and TMN Model



IV.A. Gestión de fallos

- Localización de problemas o fallos en la red, y su mantenimiento, recuperación, etc.

- Pasos de la gestión de fallos:
  - Determinar dónde está el fallo con exactitud
  - Aislar al resto de la red, para que pueda seguir funcionando sin interferencias
  - Reconfiguración de la red, para minimizar el impacto del fallo en la operación de la red
  - Recuperación o sustitución de componentes

- Otros aspectos a considerar:
  - Medidas preventivas, efecto mínimo sobre el rendimiento...

IV.B. Gestión de contabilidad

- Seguimiento del uso de recursos de la red por parte de un usuario o grupo de usuarios, asegurando que cada uno únicamente utiliza los recursos que necesita

- Motivos:
  - Facturación
  - Vigilancia de abuso de privilegios de acceso, que pueden dar lugar a sobrecargas en la red y prejuicios a otros usuarios
  - Uso ineficiente de la red
  - Planificación del crecimiento de la red

- El gestor de red debe ser capaz de especificar:
  - El tipo de información a almacenar en los distintos nodos
  - El intervalo de tiempo en el que esa información debe enviarse al nodo de mayor nivel jerárquico
  - Los algoritmos a emplear para la facturación:
    - Por tiempo, paquetes transmitidos, bytes transmitidos, ...

IV.C. Gestión de configuración

- La gestión de configuración está relacionada con:
  - Inicialización y desconexión ordenada de la red o de parte de ella
  - Mantenimiento y adición de componentes, y actualización de relaciones entre componentes (reconfiguraciones)

- Es deseable que el arranque y parada de componentes específicos se puedan realizar de forma remota y desatendida

IV.D. Gestión de calidad de funcionamiento

- Funciones destinadas a evaluar el comportamiento de equipos de telecomunicaciones e informar al respecto, midiendo las prestaciones de los diferentes elementos hardware, software y medios de comunicación

- El objetivo es asegurar que la capacidad y prestaciones de la red corresponde con las necesidades de los usuarios

- Parámetros a medir:
  - Productividad, utilización, tasa de error, tiempo de respuesta...
- Hay dos categorías funcionales:
  - Monitorización: seguimiento de actividades en la red
  - Control: realización de los ajustes necesarios para mejorar el rendimiento
- Con las estadísticas sobre el rendimiento, se pueden predecir puntos conflictivos antes de que causen problemas a los usuarios
  - Ejemplo: detección de cuellos de botella, y acciones correctivas (balanceo o redistribución del tráfico)

IV.E. Gestión de seguridad

❖ Proceso para controlar el acceso a la información contenida en los elementos de la red, y protección de la misma ante fallos intencionados o accidentales, accesos no autorizados, etc.

- Control de acceso + encriptación de la información enviada por la red
- Archivos de log, que guardan información de lo que pasa en la red, para su posterior análisis

❖ La gestión de seguridad proporciona los medios para:

- Localizar la información importante
- Establecerlos puntos desde los que se puede acceder
- Registrar los usuarios que consultan dicha información, y durante qué periodos de tiempo, así como los intentos fallidos de acceso

V. Estándares de gestión

❖ Los organismos internacionales de normalización están definiendo **modelos de gestión integrada**, que en teoría permitirán la interconexión abierta entre los recursos de telecomunicación y las aplicaciones de gestión de red

❖ Existen tres modelos principales:

- **Gestión Internet**: definido por la *Internet Society*, para gestionar redes TCP/IP
- **Gestión de red OSI**: definido por ISO, para gestionar los recursos según el modelo de referencia OSI
- **Arquitectura TMN**: definida por la ITU-T, se basa en los modelos anteriores e incluye el acceso a los recursos de telecomunicación

❖ Los dos primeros se refieren a redes de computadores, mientras que el último es de utilidad para los grandes operadores de redes de telecomunicación

MONITOREO

Monitorizacion de una Red

Contenidos:

I. Introducción
II. Arquitectura de monitorización de la red
    A. Información de monitorización
    B. Configuraciones de monitorización
III. Monitorización de prestaciones
    A. Indicadores de prestaciones
        i. Indicadores de prestaciones orientados al servicio
        ii. Indicadores de prestaciones orientados a la eficiencia
    B. Función de monitorización de prestaciones
    C. Medidas estadísticas vs. exhaustivas
IV. Monitorización de fallos
    A. Problemas de la monitorización de fallos
    B. Funciones de la monitorización de fallos
V. Monitorización de contabilidad

I. Introducción

❖ La monitorización de la red está relacionada con la observación y análisis del estado y comportamiento de los sistemas finales e intermedios, y de las subredes que constituyen la configuración a gestionar

❖ La monitorización consiste en tres áreas de diseño:

- Acceso a la información monitorizada: cómo definir la información de monitorización, y cómo pasarla desde un recurso a un gestor
- Diseño de mecanismos de monitorización: cómo obtener información de los recursos de manera óptima
- Aplicación de la información monitorizada: cómo se emplea la información monitorizada en las distintas áreas funcionales de gestión

❖ Las dos primeras áreas las veremos en el punto siguiente, mientras que en el resto del tema veremos aplicaciones de la monitorización, en las áreas de gestión de prestaciones (o de calidad de funcionamiento), de fallos y de contabilidad

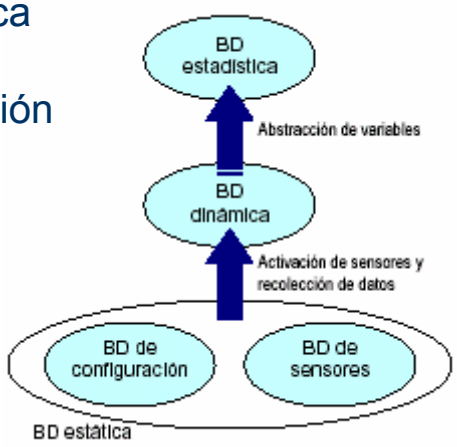
II. Arquitectura de monitorización de la red

A. Información de monitorización

❖ La información de monitorización se puede clasificar como estática, dinámica o estadística

❖ La BD estática contiene información de dos tipos:

- De configuración
- De sensores, para obtener lecturas en tiempo real



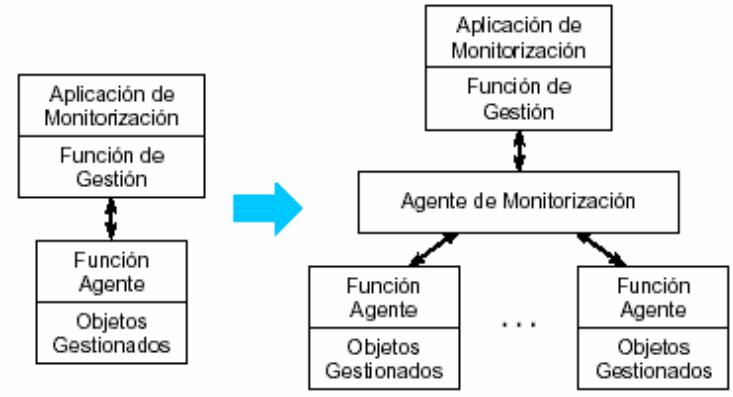
II. Arquitectura de monitorización de la red: A. Información de monitorización

- La **BD dinámica** recoge información acerca del estado de los elementos, y de los eventos detectados por los sensores
- La **BD estadística** incluye medidas agregadas útiles
- La **información estática** es generada por los propios elementos de red, y está disponible para un monitor si el elemento dispone del software de agente apropiado
- La **información dinámica** generalmente es recogida y almacenada por el elemento de red responsable de los eventos subyacentes
  - **Monitor remoto**: en una LAN, gran parte de su actividad se puede medir mediante un dispositivo externo conectado a dicha LAN
- La **información estadística** puede ser generada por cualquier sistema que tenga acceso a los datos dinámicos subyacentes
  - En el monitor, lo que requiere la transmisión de todos los datos
  - En el propio sistema que contiene los datos, si es que el monitor no necesita conocer los datos en su totalidad
    - Esto ahorra tiempo de proceso del monitor, y capacidad de la red

II. Arquitectura de monitorización de la red: B. Configuraciones de monitorización

Al esquema funcional de un sistema de gestión de red, se le suele añadir un módulo funcional adicional, relativo con la generación de información estadística: el **agente de monitorización**

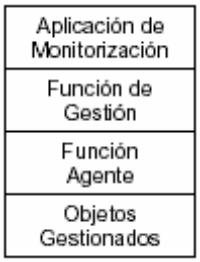
- Genera resúmenes y análisis estadísticos de la información de gestión
- Si es remoto respecto del gestor, actúa como un agente, comunicando la información calculada al gestor



II. Arquitectura de monitorización de la red: B. Configuraciones de monitorización

❖ Los módulos funcionales de la figura anterior se pueden configurar de varias formas distintas:

- ➢ La estación que contiene la aplicación de monitorización debe ser monitorizada también, por lo que contiene un agente y un conjunto de objetos gestionados
  - • De hecho, es fundamental monitorizar el estado y comportamiento del monitor de la red, para asegurar que sigue funcionando, y comprobar la carga tanto de la red como de sí mismo
  - • Es especial, se debe medir la cantidad de tráfico de gestión que entra y sale del monitor de red, instrumentando de forma adecuada el protocolo de gestión de red



II. Arquitectura de monitorización de la red: B. Configuraciones de monitorización

❖ La configuración más usual para monitorizar otros elementos de red requiere que el gestor y los sistemas agentes compartan el mismo protocolo de gestión de red, y la misma sintaxis y semántica de MIB (*Management Information Base*) (Fig. A)

❖ Un sistema de monitorización puede incluir uno o más agentes que monitoricen el tráfico en una LAN: monitores externos o remotos (Fig. B)

❖ En caso de que los elementos de red no compartan el mismo protocolo de gestión de red, es necesario un agente proxy (Fig. C)

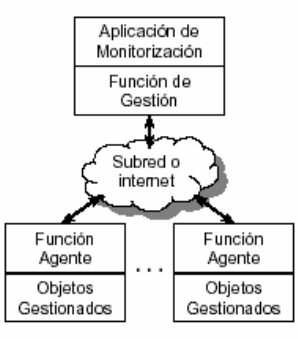


Fig. A

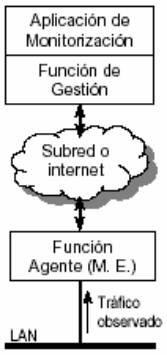


Fig. B

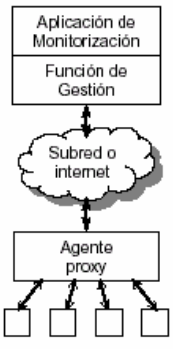


Fig. C

III. Monitorización de prestaciones:
A. Indicadores de prestaciones

❖La monitorización de prestaciones de una red es absolutamente necesaria

❖ El problema, seleccionar y emplear los indicadores apropiados que midan las prestaciones o la calidad de funcionamiento de la red

- Pueden haber demasiados indicadores, o su significado no se entiende bien, o sólo los soportan algunos fabricantes ...
- Lo más usual es que los indicadores se midan correctamente, pero su interpretación sea incorrecta
- Y a veces, el cálculo de los indicadores es tan costoso que los resultados no se pueden emplear para controlar el entorno

❖ Hay dos categorías de indicadores de prestaciones:

- Orientados al servicio: sirven para medir el grado de satisfacción de los usuarios con el servicio que reciben
- Orientados a la eficiencia: los requisitos relativos al servicio de los usuarios se deben de alcanzar con un coste lo menor posible, por tanto es necesario disponer de medidas de la eficiencia

III. Monitorización de prestaciones:
A. Indicadores de prestaciones

i. Indicadores de prestaciones orientados al servicio

❖ **Disponibilidad**: Porcentaje de tiempo que un sistema de red, un componente o una aplicación están disponibles para un usuario

- Se basa en la fiabilidad de los componentes individuales de la red
- Depende de la disponibilidad de los componentes, y de su organización (componentes redundantes, arquitectura robusta....)

❖ **Tiempo de respuesta**: Cuánto tarda en aparecer la respuesta en el terminal después de una petición por parte del usuario

- Tiempo que tarda el sistema en reaccionar ante una entrada dada
- Idealmente, el tiempo de respuesta para cualquier aplicación sería corto, pero un menor tiempo de respuesta siempre implica mayores costes...
  - Mayor potencia de cálculo
  - Penalización a otros procesos... por lo que hay que llegar a un compromiso
- Es necesario examinar con detalle el tiempo de respuesta para identificar posibles cuellos de botella en el sistema

III. Monitorización de prestaciones:
A. Indicadores de prestaciones

i. Indicadores de prestaciones orientados al servicio (cont....)

❖ **Exactitud**: Porcentaje de tiempo durante el cual no hay errores en la transmisión y entrega de información

- Puesto que los protocolos de la arquitectura de red ya se encargan de detectar y recuperarse de errores, el usuario generalmente no debe de preocuparse por ellos
- Sin embargo, es útil medir la tasa de errores que deben ser corregidos, pues pueden ser causados por una línea defectuosa o por interferencias que deben corregirse

III. Monitorización de prestaciones:
A. Indicadores de prestaciones

ii. Indicadores de prestaciones orientados a la eficiencia

❖ **Productividad**: La tasa con la que ocurren eventos orientados a la aplicación (transacciones de mensajes, transferencias de ficheros...)

- Es útil seguir esta medida para intuir las demandas futuras

❖ **Utilización**: Porcentaje de la capacidad teórica de un recurso línea de transmisión, conmutador...) que se está utilizando

- Es una medida con más granularidad que la productividad
- Su principal uso es la detección de cuellos de botella potenciales, la distribución equilibrada de la carga entre los componentes del sistema

III. Monitorización de prestaciones:
B. Función de monitorización de prestaciones

- La monitorización de prestaciones engloba tres componentes:
  - Medida de prestaciones: reunión de estadísticas acerca del tráfico de la red y su temporización
    - La llevan a cabo módulos agentes dentro de los dispositivos de la red, o monitores remotos en caso de LANs
  - Análisis de prestaciones: software para la reducción y presentación de los datos
  - Generación de tráfico sintético: permite observar la red bajo una carga controlada

III. Monitorización de prestaciones:
B. Función de monitorización de prestaciones

Algunas medidas que suelen aparecer en informes de prestaciones de una LAN son:

Nombre	Variables	Descripción
Matriz de comunicaciones entre hosts	Fuente x Destino	Número (o %) de paquetes, bytes ...
Matriz de comunicaciones entre grupos	Fuente x Destino	Número (o %) de paquetes, bytes ..., considerando grupos de direcciones
Histograma de tipos de paquetes	Tipo de paquete	Número (o %) de paquetes por tipo
Histograma de tamaños de paquetes	Tamaños de paquete	Número (o %) de paquetes por tamaño
Distribución de productividad/utilización	Fuente	Bytes (de datos o totales) transmitidos
Histograma de tiempo entre llegadas de paquetes	Tiempo entre llegadas	Tiempo entre señales consecutivas de "red ocupada"
Histograma de retardo de comunicación	Retardo de paquete	Tiempo desde que el paquete original estaba listo en la fuente, hasta su recepción
Histograma de recuento de colisiones	Número de colisiones	Número de paquetes por número de colisiones

III. Monitorización de prestaciones:
B. Función de monitorización de prestaciones

❖ Las cuestiones que se deben plantear se pueden englobar en dos grupos:

- Las relativas a la existencia de posibles errores o ineficiencias
  - ¿El tráfico se distribuye de forma uniforme en la red, o hay caminos con tráfico inusualmente alto?
  - ¿Hay paquetes de algún tipo con una frecuencia demasiado alta? (pueden ser indicativos de error o de un protocolo ineficiente)
  - ¿Los retardos de comunicación son excesivos?
  - ....

- Las relativas al incremento de carga y variación en el tamaño de los paquetes
  - ¿Cuál es el efecto del incremento de carga sobre la utilización, productividad y retardos?
  - ¿Con qué niveles de carga se empiezan a degradar las prestaciones del sistema?
  - ¿Cuál es la capacidad máxima de un canal bajo condiciones normales de uso? ¿Cuántos usuarios activos son necesarios para alcanzar este máximo?
  - ....

III. Monitorización de prestaciones:
C. Medidas estadísticas vs. exhaustivas

❖ Cuando la red está muy cargada, llevar a cabo medidas exhaustivas del tráfico puede no ser posible, debido a que el monitor (sea un agente en un nodo o un agente remoto) no es capaz de procesar tanta información

❖ La alternativa es muestrear el flujo de tráfico y estimar el valor de los indicadores como si fuesen variables aleatorias

❖ Pero las comunicaciones de datos exhiben características peculiares:

- Los errores ocurren a una tasa muy baja (10^{-6} o menos), hay ráfagas y agrupamientos de paquetes...
- Hay que tener en cuenta los principios estadísticos a la hora de diseñar las funciones de muestreo, y de interpretar los resultados

IV. Monitorización de fallos

El objetivo de la monitorización de fallos es identificar fallos tan rápido como sea posible desde el momento en que ocurren, e identificar su causa, para poder remediarlo

IV.A. Problemas de la monitorización de fallos

❖ Cuando el entorno es complejo, pueden darse los siguientes problemas en la observación de fallos:

- Fallos no observables: algunos fallos no se pueden observar de manera local, p. ej., debido a que el equipo no está instrumentado para registrar la ocurrencia de un fallo

- Fallos parcialmente observables: un fallo en un nodo puede ser observable, pero la observación puede ser insuficiente para localizar el problema con exactitud

- Incertidumbre en la observación: cuando hay incertidumbre o inconsistencias asociadas con las observaciones

IV.A. Problemas de la monitorización de fallos

- Una vez que se observa un fallo, es necesario aislarlo a un componente en particular. Los problemas que pueden darse son:
  - Múltiples causas potenciales: cuando están implicadas muchas tecnologías, los puntos potenciales de fallo y su tipo se incrementan, lo que hace difícil encontrar la causa del fallo
  - Demasiadas observaciones relacionadas: Un solo fallo puede afectar muchos caminos de comunicación activos, y un fallo en un nivel de la arquitectura de comunicaciones puede afectar a los niveles superiores, provocando muchos fallos secundarios. Sus datos pueden ocultar el problema subyacente
  - Interferencia entre el diagnóstico y procedimientos locales de recuperación: los procedimientos locales de recuperación pueden destruir evidencias acerca de la naturaleza del fallo, imposibilitando el diagnóstico
  - Ausencia de herramientas de testeo automatizado: el testeo para aislar fallos es difícil y costoso de administrar

IV.B. Funciones de la monitorización de fallos

- Capacidad de detectar e informar acerca de la ocurrencia de fallos
  - Como mínimo, el agente debe ser capaz de mantener un registro (log) de eventos significativos y de errores
  - El agente informará de ciertas condiciones de error a uno o varios gestores
- Capacidad de anticiparse a la ocurrencia de fallos
  - Normalmente, se hace generando un informe cuando una variable monitorizada cruza un umbral prefijado

- Asistencia para aislar y diagnosticar el fallo, mediante diversos tests:
  - De conectividad, de integridad de datos, de integridad del protocolo...
  - De saturación de datos y de conexiones
  - De tiempo de respuesta
  - De loopback ...
- También es necesario un interfaz con el usuario efectivo para la monitorización de fallos

V. Monitorización de contabilidad

❖ La monitorización de contabilidad trata principalmente de seguir la pista del uso que hacen los usuarios de los recursos de la red

❖ Los requerimientos de esta función varían mucho:
- ➢ Desde un recuento detallado del uso por cada usuario individual, con propósitos de facturación
  - • Ej.: en redes que ofrecen un servicio público
- ➢ Hasta un recuento general, para saber por encima el uso de recursos, y cargar los costes de forma proporcional

❖ En el primer caso, la información reunida por el monitor debe ser mucho más detallada y exacta que en un sistema general

V. Monitorización de contabilidad

❖ Algunos ejemplos de recursos que pueden estar sujetos a contabilidad:
- ➢ Facilidades de comunicación: LANs, WANs, centralitas, líneas alquiladas...
- ➢ Computadoras: servidores y estaciones de trabajo
- ➢ Software y sistemas: aplicaciones y utilidades de un servidor o un centro de datos
- ➢ Servicios: todos los servicios comerciales de comunicaciones e información disponibles para los usuarios de red

❖ Algunos datos de contabilidad que pueden ser recogidos para cada usuario son:
- ➢ Identificación de usuario, receptor, número de paquetes transmitidos, nivel de seguridad, marcas de tiempos asociadas con los eventos principales, códigos de estado de la red, recursos utilizados

V. Monitorización de contabilidad

❖ Algunos ejemplos de recursos que pueden estar sujetos a contabilidad:

- Facilidades de comunicación: LANs, WANs, centralitas, líneas alquiladas...
- Computadoras: servidores y estaciones de trabajo
- Software y sistemas: aplicaciones y utilidades de un servidor o un centro de datos
- Servicios: todos los servicios comerciales de comunicaciones e información disponibles para los usuarios de red

❖ Algunos datos de contabilidad que pueden ser recogidos para cada usuario son:

- Identificación de usuario, receptor, número de paquetes transmitidos, nivel de seguridad, marcas de tiempos asociadas con los eventos principales, códigos de estado de la red, recursos utilizados

CONTROL

Control de una red

Contenidos:

I. Introducción

II. Control de configuración
- A. Definición de información de configuración
- B. Establecimiento y modificación de valores de atributos
- C. Definición y modificación de relaciones
- D. Inicialización y terminación de las operaciones de la red
- E. Distribución de software

III. Control de seguridad
- A. Amenazas a la seguridad
  - i. Tipos de amenazas
  - ii. Clasificación de amenazas
  - iii. Amenazas al Sistema de Gestión de Red
- B. Funciones de la gestión de la seguridad
  - i. Mantenimiento de información de seguridad
  - ii. Servicio de control de acceso a recursos
  - iii. Control del proceso de encriptación

I. Introducción

❖ La parte de control de la red de la gestión de red está relacionada con:
- ➢ La modificación de parámetros
- ➢ Provocar acciones por parte de los sistemas que componen la configuración a gestionar

❖ Todas las áreas de la gestión de red implican tanto monitorización como control
- ➢ En las áreas de prestaciones, fallos y contabilidad es más importante la monitorización
- ➢ En las áreas de configuración y seguridad es más importante el control

II. Control de configuración

❖ La **gestión de la configuración** está a cargo de la inicialización, mantenimiento, y cierre de componentes individuales y subsistemas lógicos dentro de la configuración completa de computadores y recursos de comunicaciones de una instalación

- Establecimiento de valores y relaciones por defecto al iniciar el sistema
- Modificación de valores en respuesta a comandos de usuario, o a otras funciones de mantenimiento de red

II. Control de configuración

La gestión de la configuración incluye las siguientes **funciones**:

- Definición de información de configuración
- Establecimiento y modificación de valores de atributos
- Definición y modificación de relaciones
- Inicialización y terminación de las operaciones de la red
- Distribución de software
- Examinar valores y relaciones
- Informar del estado de la configuración

} *Funciones de monitorización de la configuración*

II.A. Definición de información de configuración

❖ La **información de configuración** describe la naturaleza y estado de los recursos que son de interés para la gestión de la red

- ➢ Especificación de recursos y de sus atributos
- ➢ Recursos físicos: sistemas finales, encaminadores, puentes, modems...
- ➢ Recursos lógicos: temporizadores, contadores, circuitos virtuales...
- ➢ Atributos: nombre, dirección, identificador, versión de software...

II.A. Definición de información de configuración

❖ La información de configuración se puede estructurar de varias formas:

- ➢ Lista estructurada de campos de datos, cada campo contiene un solo valor
  - • Enfoque de SNMP
- ➢ Base de datos orientada a objetos, cada elemento se representa por uno o más objetos
  - ▪ Cada objeto contiene atributos, y también 'comportamientos'
  - ▪ Notificaciones que se hacen ante la ocurrencia de ciertos eventos
  - • Relaciones de herencia y composición entre objetos
  - • Enfoque de OSI
- ➢ Base de datos relacional, campos individuales contienen valores que reflejan características de los elementos de red, la estructura de la BD refleja las relaciones entre los elementos de red

❖ La información debe estar accesible para la estación gestora

- ➢ Normalmente se almacena en el recurso en cuestión, o bien en el nodo agente, o en un nodo proxy

❖ La función de control de red debe permitir que el usuario especifique el rango y tipo de valores válidos para cada atributo

❖ También es deseable que se permita la definición de nuevos objetos

II.B. Establecimiento y modificación de valores de atributos

❖ La función de control de la configuración debe permitir que una estación gestora establezca y modifique los valores de los atributos de forma remota, tanto en agentes como en proxies

❖ Hay dos limitaciones a esta capacidad:

- El gestor debe estar autorizado a hacer ciertas modificaciones en determinados momentos; este es un tema de seguridad
- Algunos atributos reflejan la 'realidad' de un recurso, y por tanto no pueden ser modificados remotamente

II.B. Establecimiento y modificación de valores de atributos

❖ Las modificaciones pueden clasificarse en tres categorías

- Actualización de la base de datos: el gestor lanza un comando de modificación a un agente, y éste simplemente actualiza los valores apropiados, y envía un reconocimiento al gestor
- Actualización de la base de datos más modificación de recursos: Además, de actualizar los valores de la BD de configuración, una modificación puede afectar a un recurso subyacente
- Actualización de la base de datos más acción: en algunos sistemas de gestión de red no existe un comando de acción disponible para los gestores; en su lugar hay parámetros que cuando se activan, provocan que el agente ejecute una acción

❖ El usuario debería poder cargar valores predefinidos y por defecto, a nivel de todo el sistema o a nivel de nodos o capas individuales

II.C. Definición y modificación de relaciones

❖ Una relación describe una asociación, conexión o condición que existe entre recursos o componentes de la red

- ➢ Ejemplos: una topología, una jerarquía, una conexión física o lógica, un dominio de gestión
  - • Un **dominio de gestión** es un conjunto de recursos que comparten la misma autoridad de gestión

❖ El usuario debe poder modificar los recursos y sus relaciones sin desconectar la red

- ➢ Ejemplos: establecer y tirar conexiones conmutadas o permanentes, designar direcciones alternativas como destino de una conexión, para emplear en caso de fallo

II.D. Inicialización y terminación de las operaciones de la red

❖ La gestión de la configuración debe incluir mecanismos para que los usuarios inicialicen o cierren la operación de una red o subred

❖ El **proceso de inicialización** incluye:

- ➢ Verificación de que los atributos y relaciones se han establecido adecuadamente
- ➢ Notificación a los usuarios de cualquier recurso, atributo o relación que necesita ser establecida
- ➢ Validar los comandos de inicialización de los usuarios

❖ Para la **terminación** son necesarios mecanismos que permitan que los usuarios soliciten estadísticas, o información de estado antes de que el proceso de terminación se haya completado

II.E. Distribución de software

- La gestión de la configuración debe proporcionar la capacidad de distribución de software tanto a sistemas finales (hosts, servidores, estaciones de trabajo) como a sistemas intermedios (puentes, encaminadores, pasarelas del nivel de aplicación)
- Para ello, se requieren facilidades para:
  - Permitir peticiones de carga de software
  - Transmitir las versiones de software especificadas
  - Actualizar los sistemas de seguimiento de la configuración
- Además, en este apartado se incluye la distribución de las tablas de encaminamiento de puentes y encaminadores
  - Pueden verse modificadas por intereses de seguridad, prestaciones o contabilidad, que requieren una intervención del sistema de gestión
- El usuario necesita mecanismos para examinar, actualizar y gestionar diferentes versiones de software e información de encaminamiento
  - Por ejemplo, se pueden cargar diferentes versiones de las tablas de encaminamiento basándose en condiciones particulares, como las tasas de error

III. Control de seguridad

- **Seguridad del computador**: colección de herramientas destinadas a la protección de datos almacenados en computadores y a la frustración de ataques

- **Seguridad de la red**: medidas encaminadas a la protección de datos durante su trasmisión

- La parte de **gestión de la seguridad** dentro del sistema de gestión de red trata de proporcionar seguridad tanto a nivel de los computadores como al nivel de la red, para los recursos sujetos a gestión, incluyendo el propio sistema de gestión de red

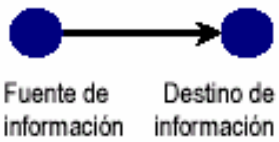
III.A. Amenazas a la seguridad

❖ Requerimientos de seguridad

- **Secreto**: la información dentro de un sistema sólo puede ser leída por entidades autorizadas
- **Integridad**: los elementos de un sistema sólo pueden ser modificados por entidades autorizadas; esto incluye escritura, cambios, cambios de estado, borrado y creación
- **Disponibilidad**: los elementos de un sistema deben estar disponibles para las entidades autorizadas

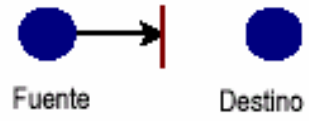
III.A.i. Tipos de amenazas

❖ La función general del sistema de información es proveer información entre una fuente y un destino:



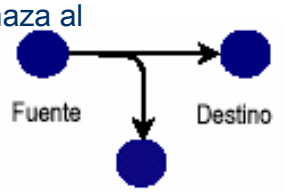
❖ Este funcionamiento normal puede sufrir cuatro categorías generales de amenazas:

- **Interrupción**: un elemento del sistema se destruye o se inutiliza; es una amenaza a la disponibilidad
  - Ejemplos: destrucción de hardware (un disco duro...), corte de una línea de comunicación, deshabilitación del sistema de archivos...

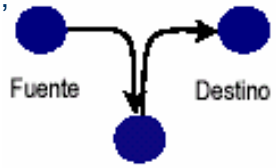


III.A.i. Tipos de amenazas

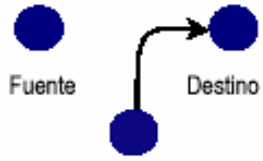
- **Intercepción**: una entidad no autorizada (persona, programa, computador...) gana el acceso a un elemento; es una amenaza al secreto
  - Ejemplos: copias ilícitas de programas, escuchas para capturar datos en una red ...



- **Modificación**: una entidad no autorizada no sólo gana el acceso a un elemento, sino que también lo modifica; es una amenaza a la integridad
  - Ejemplos: modificación de valores en archivos de datos, alteración de programas, modificación del contenido de mensajes...



- **Fabricación**: una entidad no autorizada inserta objetos falsos en el sistema; también se trata de una amenaza a la integridad
  - Ejemplos: inserción de mensajes falsos en la red, adición de registros a un archivo...



III.A.ii. Clasificación de amenazas

- Los elementos de un sistema se pueden catalogar como hardware, software, datos, redes y líneas de comunicación
- Cada uno de ellos debe afrontar distintas amenazas:

- **Hardware**:
  - Interrupción (robo o daño de equipos): se afecta la disponibilidad
    - Medidas administrativas y físicas para tratar estas amenazas

- **Software**:
  - Interrupción (borrados o alteraciones): se afecta la disponibilidad
    - Copias de seguridad de la versión más reciente del software
  - Modificación (virus): el programa funciona, pero se comporta de forma distinta; se afecta la integridad
  - Intercepción (copias ilegales): afecta al secreto

III.A.ii. Clasificación de amenazas

- **Datos**:
  - Interrupción (destrucción de archivos): afecta la disponibilidad
  - Intercepción (lectura de datos por entidades no autorizadas, análisis de datos estadísticos): afecta el secreto
  - Modificación: afecta la integridad de los datos
- **Líneas de comunicación**: se presentan los mismos problemas que con los datos; en este contexto, las amenazas se clasifican en activas o pasivas:
  - *Amenazas pasivas*: tratan de 'fisgar' o monitorizar las transmisiones de una organización. Hay dos tipos de amenazas, relacionadas con la intercepción y que afectan al secreto:
    - Conocer el contenido de los mensajes: solución ? Encriptación
    - Hacer un análisis del tráfico, para conocer patrones de comunicación

  Puesto que estas amenazas son difíciles de detectar, los esfuerzos deben encaminarse hacia su prevención

III.A.ii. Clasificación de amenazas

- *Amenazas activas*: implican alguna modificación del flujo de datos, o la creación de un flujo de datos falso. Podemos subdividirlas en tres categorías:
  - *Modificación del flujo de información*, para producir un efecto no autorizado; afecta a la integridad
  - *Denegación de servicio*, inhibiendo el uso normal de las facilidades de comunicación; afecta a la disponibilidad
  - Supresión de mensajes dirigidos a ciertos destinos
  - Trastorno del servicio, deshabilitando una red o sobrecargándola con mensajes
  - *Enmascaramiento*, cuando una entidad pretende ser otra; afecta a la integridad
  - Normalmente, un ataque de este tipo incluye alguno de los anteriores

Estas amenazas son difíciles de prevenir, por tanto se deben dedicar esfuerzos a su detección y a recuperarse de los trastornos o retardos que puedan acusar. Esto también puede tener un efecto disuasorio, que ayuda a la prevención

III.A.iii. Amenazas al Sistema de Gestión de Red

❖ El SGR es un conjunto de aplicaciones y bases de datos sobre varias plataformas de hardware, distribuidas por toda la configuración; por tanto todas las amenazas expuestas anteriormente pueden considerarse como amenazas al SGR

❖ Algunas amenazas específicas:

- **Enmascaramiento de usuario**
- **Enmascaramiento del gestor de red**
- **Interferencias con el intercambio entre gestores y agentes**

III.B. Funciones de la gestión de la seguridad

❖Las funciones de la gestión de la seguridad se pueden agrupar en las siguientes tres categorías:

- Mantenimiento de información de seguridad
- Servicio de control de acceso a recursos
- Control del proceso de encriptación

III.B.i. Mantenimiento de información de seguridad

❖ La gestión de la seguridad también se basa en el intercambio de información de gestión entre gestores y agentes

❖ Ejemplos de información empleada en el área de seguridad incluyen claves, información de autentificación, información sobre derechos de acceso, y parámetros operativos de mecanismos y servicios de seguridad

❖ La gestión de la seguridad registra la actividad o los intentos de actividad relacionados con estos objetos, para detectar o recuperarse de ataques fructuosos o no

III.B.i. Mantenimiento de información de seguridad

❖ Algunas funciones de gestión de la información de seguridad:

- Registro de eventos
- Monitorización de pistas sobre seguridad
- Monitorización del uso y los usuarios de los recursos relacionados con la seguridad
- Informar acerca de violaciones de la seguridad
- Recibir notificaciones de violaciones de la seguridad
- Mantener y examinar registros de seguridad
- Mantener copias de seguridad de todos o parte de los archivos relacionados con la seguridad
- Mantener perfiles generales de usuarios de la red, y perfiles de uso para recursos específicos, para hacer posibles referencias de conformidad con perfiles de seguridad designados

III.B.ii. Servicio de control de acceso a recursos

❖ Se trata de uno de los servicios principales de cualquier facilidad de seguridad

❖ El control de acceso incluye servicios de autentificación y autorización, y la decisión final de conceder o denegar el acceso a recursos específicos

❖ El servicio de control de acceso está diseñado para proteger un amplio rango de recursos de red. Entre ellos, algunos relacionados con la gestión de la red son:

- Códigos de seguridad
- Información de encaminamiento fuente y registro de rutas
- Directorios
- Tablas de encaminamiento
- Niveles de umbrales para alarmas
- Tablas de contabilidad

❖ El control de acceso se gestiona mediante perfiles generales de usuarios de red para recursos específicos, especificando prioridades en el acceso

❖ La función de gestión de la seguridad permite que el usuario cree y borre objetos relacionados con la seguridad, que modifique sus atributos o su estado, y que afecte las relaciones entre los objetos de seguridad

III.B.iii. Control del proceso de encriptación

❖ La gestión de la seguridad debe poder encriptar la información que intercambian agentes y gestores

❖ Además, debe proporcionarse esta facilidad a otras entidades de red

❖ Esta función también es responsable de designar algoritmos de encriptación, y proporcionar la distribución de las claves

PROTOCOLO DE GESTIÓN

Protocolos de Mantenimiento

Contenidos: