GESTIÓN DE REDES

PARTE I

Introducción a la Gestión de Red y Estándares

INTRODUCCIÓN

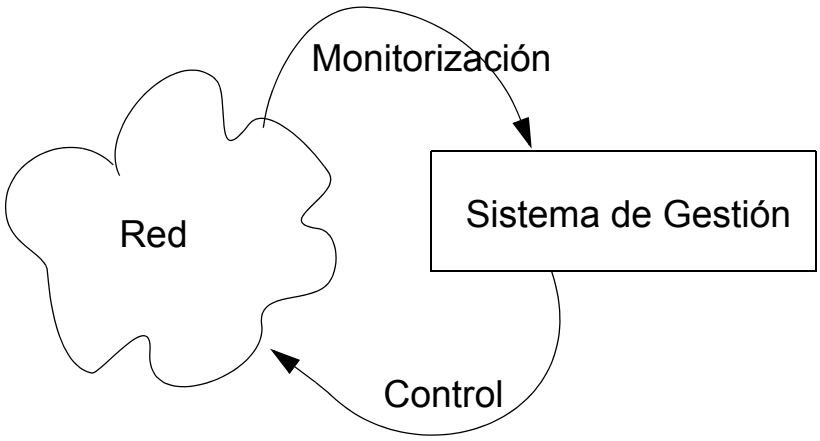
1. Introducción
2. Conceptos y Áreas Funcionales
3. Monitorización de Red vs Control de Red
4. El Por Qué de una Gestión de Red Integrada
5. Conceptos Básicos de los Estándares de Gestión
6. Gestión centralizada, jerarquizada y distribuida.
7. Estándares y Organismos de Estandarización

INTRODUCCIÓN

1. Introducción

1.1 ¿Qué es gestionar una red?

Actividades de **inicialización, monitorización y control** de una red de comunicaciones con el objetivo de que ésta cumpla los **requisitos de usuario** para los que fue construida.



INTRODUCCIÓN

1.2 Areas Funcionales de Gestión de Red

La gestión de una red de comunicaciones puede descomponerse en cinco áreas funcionales (OSI) o tambien llamadas FCAPS:

Gestión de Fallos (Fault)

Gestión de la Configuración (Configuration)

Gestión de la Contabilidad (Accounting)

Gestión de las Prestaciones (Performance)

Gestión de la Seguridad (Security)

INTRODUCCIÓN

GESTIÓN DE FALLOS

Se ocupa de mantener un funcionamiento correcto de la red, tratando de protegerla de los fallos que puedan aparecer en el sistema en su conjunto o en los elementos que lo componen.

Fallo conviene diferenciarlo de **error**: el fallo (situación que requiere de algún tipo de acción correctora) es descubierto debido a la imposibilidad de operar correctamente o por una gran cantidad de errores.

Sin embargo, los **errores** ocurren ocasionalmente y no tienen por qué ser fallos (Ej. todo enlace tiene una tasa de error de bit).

Ante un fallo:

- **Diagnosticar** y determinar rápidamente donde se localiza dicho fallo.
- **Aislar** a la red del fallo, reconfigurándola de forma que el impacto de éste sea lo menor posible.
- **Resolver** el problema de forma que la red vuelva a su estado inicial. Esto puede suponer la sustitución de los componentes fallidos.

Los usuarios desearían ser notificados del error, así como una solución rápida del problema.

El impacto y duración de los fallos depende de la **redundancia** (tanto en nodos como en rutas) que exista

en la red. Incluso en la redundancia del propio sistema de gestión de fallos.

Una vez solucionado, el usuario desearía que la red se encuentre realmente operativa y que no se han introducido otros problemas.

INTRODUCCIÓN

GESTIÓN DE LA CONTABILIDAD

En todas las redes resulta interesante mantener un **registro del uso que los usuarios hacen de la red:**

En **redes públicas**, para la **facturación**

En **redes corporativas**, para distribuir **el gasto entre departamentos**, vigilar el **uso excesivo** que hacen de ella ciertos usuarios (y que puede perjudicar a los demás), **planificar el futuro crecimiento** o **redistribución de los recursos** de la red.

El gestor de red debe ser capaz de establecer los parámetros de contabilidad que van a ser medidos en cada nodo, así como el intervalo de tiempo entre sucesivas envíos de información al gestor, el algoritmo de cálculo de la factura.

El acceso a esta información debe ser restringido.

INTRODUCCIÓN

GESTIÓN DE LA CONFIGURACIÓN

Las redes están formadas por componentes y sistemas que pueden ser configurados para muy diferentes funciones.

Ej. un nodo puede actuar como router o como host, se pueden variar los temporizadores de retransmisión en el nivel de transporte...

Se ocupa de inicializar la red, mantener, añadir y actualizar el estado de los componentes y las relaciones entre dichos componentes.

INTRODUCCIÓN

GESTIÓN DE LAS PRESTACIONES

Se ocupa de monitorizar las prestaciones de la red para comprobar que están dentro de los límites permisibles y eventualmente realizar operaciones de control para mejorarlas.

Ejemplo de parámetros a monitorizar: **porcentaje de utilización, tráfico cursado, tiempos de respuesta.**

El gestor de la red debe ser capaz de establecer los indicadores a medir aplicados en qué puntos de la red que una vez analizados permiten monitorizar la degradación de las prestaciones.

Utiliza la información de prestaciones para descubrir cuellos de botella y poder planificar ampliaciones de la red.

El usuario desearía conocer la **calidad del servicio** que le está siendo ofrecido. Desea, lógicamente un servicio con las mejores prestaciones posibles.

INTRODUCCIÓN

GESTIÓN DE LA SEGURIDAD

Se ocupa fundamentalmente de:

Gestionar la generación, distribución y mantenimiento de **claves** para encriptación

Gestionar los mecanismos de **control de acceso** (Ej. Passwords)

Monitorización del **acceso** a las máquinas de la red y a la propia información de gestión.

Herramienta importante: **log.**

INTRODUCCIÓN

Podemos analizar los fundamentos de la gestión de red centrándonos **no en las funciones**, sino en las dos principales **operaciones** involucradas: **monitorización** y **control.**

1.3 Gestión = Monitorización + Control

a) Monitorización

La **información de monitorización** puede clasificarse en:

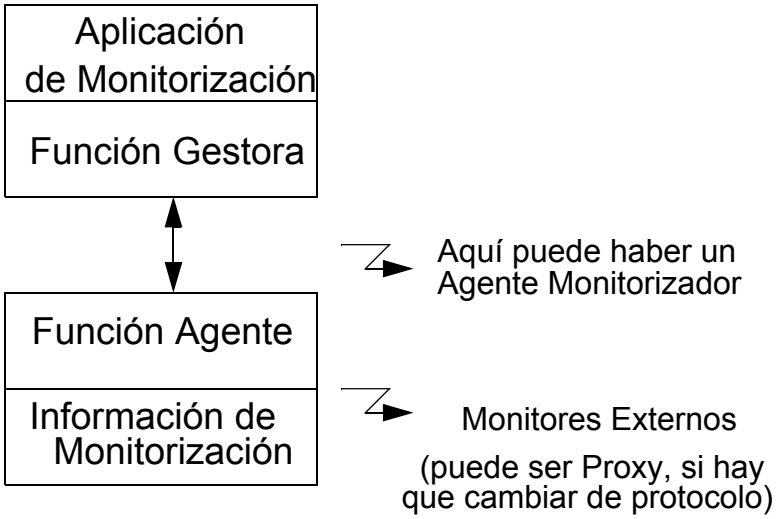
Estática: Información que no cambia frecuentemente, como la que caracteriza la **configuración de la red y los dispositivos que la componen.** Ej. el número de interfaces de un router. Suele ser mantenida por el elemento de red involucrado.

Dinámica: Información relacionada con **eventos** de la red. Cambia frecuentemente. Suele ser mantenida por el elemento de red que genera los eventos, pero también puede hacerse externamente..

Estadística: Información **derivada de la dinámica**. Ej. Tasa media de paquetes generados por un nodo. Generada por cualquier sistema que tenga acceso a la información dinámica.

INTRODUCCIÓN

Modelo Gestor/Agente



Distinguimos los siguientes **elementos de un sistema de monitorización:**

*__Aplicación de Monitorización__, necesita de los datos monitorizados. Puede ser de cualquier área funcional.

***Función Gestora,** realiza la función básica de obtener los datos de monitorización para la aplicación.

***Función Agente,** recolecta y almacena la información de monitorización para facilitársela al gestor.

***Información de Monitorización.**

***Agente Monitorizador,** genera agregaciones y análisis estadísticos de la información. Si no está junto al gestor, toma el papel de agente para comunicarse con él.

INTRODUCCIÓN

a1) Polling / Event Reporting

Polling: Interacción basada en mensajes de **Petición/ Respuesta entre Gestor y Agentes.**

El **Gestor** solicita parte o toda la información de algún elemento de red. Pueden ser peticiones más inteligentes, solicitando información que cumple determinados criterios.

El **Agente** espera peticiones y devuelve respuestas.

El polling puede hacerse **periódico**, para detectar cambios de estado, o puede ser disparado como consecuencia de algún evento que precisa de obtener más información.

Con **event-reporting**, la iniciativa (y la complejidad) es del Agente, que periódicamente o cuando se haya cumplido alguna condición envía información al gestor.

Aquí el Gestor sólo tiene que configurar la actividad del Agente (periodo de recepción de informes o condición para el envío de informes) y pasar a la espera.

a2) Monitorización de Prestaciones

Dificultad: seleccionar los medidores apropiados (hay medidores no comparables, no todos los fabricantes de equipos soportan los mismos medidores...). Algunos indicadores genéricos:

Indicadores orientados a Servicio

Indicador	Descripción
Disponibilidad	Porcentaje de tiempo que un elemento de red, componente, aplicación está disponible para el usuario.
Tiempo de Respuesta	Tiempo que el usuario debe esperar la respuesta a una acción iniciada por él.
Fiabilidad	Porcentaje de tiempo sin errores en la transmisión y entrega de la inforamción.

Indicadores orientados a Eficiencia

Indicador	Descripción
Throughput	Tasa de ocurrencia de eventos de usuario: generación de transacciones, mensajes.
Utilización	Porcentaje actualmente utilizado de la teórica capacidad total de un recurso.

Los primeros son más importantes (reflejan la calidad del servicio ofrecido), pero los segundos nos indican a qué coste estamos ofreciendo esa calidad. El objetivo, lógicamente, es minimizarlo.

INTRODUCCIÓN

Disponibilidad:

Se puede medir en base a la fiabilidad de los componentes, que normalmente se calcula con los parámetros MTBF (*Mean Time Between Failures*) y MTTR (*Mean Time to Repair*).

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

Pero la disponibilidad de un sistema completo o un servicio depende de la de los componentes y como estén relacionados.

Además, influye la carga de la red.

Tiempo de Respuesta:

Lógicamente, un menor tiempo de respuesta exige más coste: más recursos, tanto de máquina como de red.

En la mayoría de ocasiones, conviene realizar mediciones separadas para los distintos elementos que intervienen, para así detectar los posibles cuellos de botella del sistema.

INTRODUCCIÓN

Corrección (Accuracy):

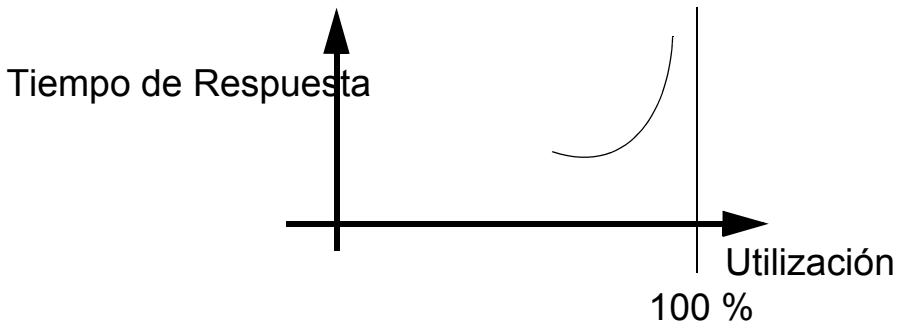
A pesar de que los protocolos disponen de mecanismos para detectarlos e incluso corregirlos, conviene monitorizarlos para descubrir posibles enlaces con problemas que conviene corregir.

Throughput:

Es útil monitorizar las llamadas atendidas, las transacciones realizadas, como forma de prever posibles problemas de prestaciones como consecuencia de incrementos de la demanda.

Utilización:

Se trata de detectar cuellos de botella y áreas de importante congestión. Por teoria de colas sabemos que con un alto grado de utilización, el tiempo de respuesta se comporta exponencialmente.



INTRODUCCIÓN

Podemos detectar recursos infrautilizados y sobreutilizados. Los primeros suponen un coste inútil a evitar y los segundos degradan las prestaciones del sistema.

Las medidas de prestaciones puede realizarlas un agente específico para cada nodo, pero en algunos casos, puede hacerlo un monitor externo.

Estas medidas pueden ser interesantes para realizar un análisis o procesamiento para extraer conclusiones o, simplemente, presentarle los datos al gestor de la red o al usuario final.

INTRODUCCIÓN

a3) Monitorización de fallos

Problemas propios de la gestión de fallos:

Fallos inobservables: Hay fallos inherentemente inobservables, como un deadlock entre procesos distribuídos. O porque el equipo en cuestión no dispone de mecanismos para detectar ese error.

Fallos Parcialmente Observables: Puede ser que lo observable no sea suficiente para diagnosticar la causa real.

Incertidumbre en la observación: Aunque tengamos observaciones muy detalladas, puede que haya incertidumbre acerca de la causa. Ej. Un nodo que no responde puede haber fallado, haberse caido la red o haberse retardado la respuesta por congestión.

INTRODUCCIÓN

Debemos identificar la **causa** original del problema.

Causas potencialmente múltiples: Si la red está formada por múltiples tecnologías, tendremos una gran variedad de problemas y puntos de fallo.

Múltiples observaciones relacionadas: Un simple fallo puede ser detectado en numerosos sitios de la red. Debemos considerar que una capa en una red puede soportar servicios de comunicación de capas superiores.

Procedimientos locales de recuperación pueden destruir evidencias importantes de cara a diagnosticar el problema.

No suele ser fácil desarrollar procedimientos de prueba que aislen las verdaderas causas (la red esta dando servicio).

a4) Monitorización de la Contabilidad

Los requisitos de este área funcional varían mucho dependiendo de la naturaleza de la red: corporativa o pública.

¿Qué debe monitorizarse?

Recursos de Comunicaciones: LANs, WANs, líneas dedicadas...

Recursos Hardware

Software y aplicaciones en servidores

Servicios de información ofrecidos de forma comercial por la red.

b) Control

b1) Control de la Configuración

***Definición de la información de configuración**:* la información de configuración describe la naturaleza y estado de los recursos de la red, tanto lógicos como físicos.

Existen muy diferentes enfoques para estructurar esa información de gestión.

Esta información es necesaria en la estación gestora y está disponible para ser accedida en los agentes.

Aunque la definición de esta información de gestión se suele hacer actualmente off-line, sería interesante que pudiera ser controlado desde la estación gestora.

Cambio de valores de atributos: Puede necesitarse autentificación para cambiar ciertos parámetros.

Algunos atributos no son alterables, porque reflejan la realidad de la red. Ej. El número de interfaces de un router.

El cambio del valor de un atributo puede significar:

- Alteración en la base de datos del agente.
- Cambio en la base de datos y modificación del recurso gestionado.
- Cambio en la base de datos y acción a tomar sobre el recurso.

Definición y modificación de relaciones*:* de tipo topológico, jerárquicas, conexiones físicas y lógicas, de dominios de gestión.

Inicialización y terminación de la operación de la red.

Distribución de software: funcionalidad para atender peticiones de carga de software (nuevas versiones), transmitir nuevas versiones a los nodos de una red...

Incluimos aqui todo tipo de datos que influyen en el comportamiento de la red (tablas de enrutamiento...).

b2) Control de la Seguridad

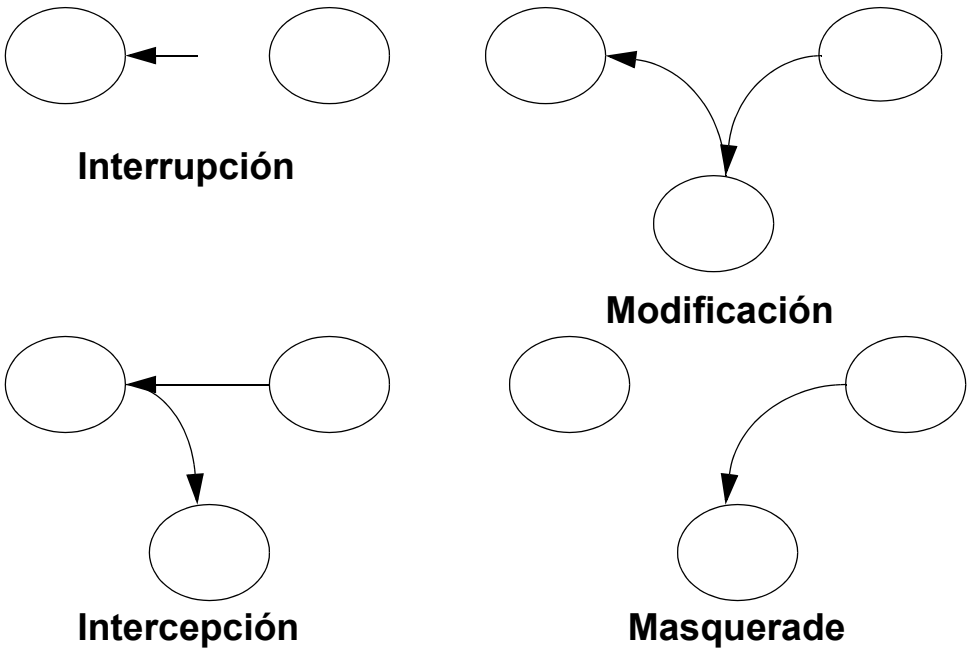
Se encarga de ofrecer seguridad en los ordenadores y en la red para los recursos gestionados, incluído el propio sistema de gestión.

Amenazas:

Contra la Privacidad: Sólo deben acceder a la información las personas autorizadas. Intercepción.

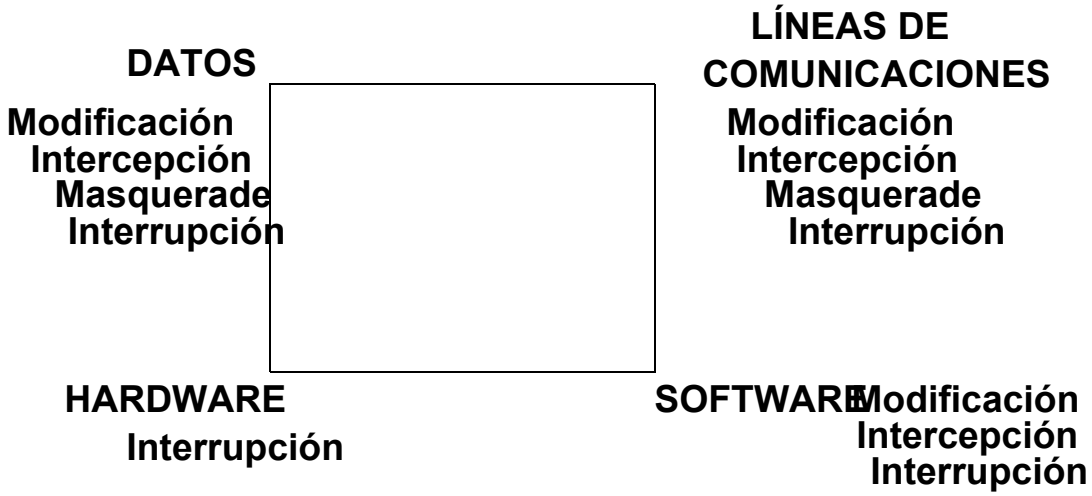
Contra la Integridad: Sólo debe ser modificada por personas autorizadas. Modificación y Masquerade.

Contra la Disponibilidad: para los autorizados. Interrupción.



INTRODUCCIÓN

También los podemos clasificar dependiendo del tipo de activos de la red al que ataquen: contra el hardware, el software, las líneas de comunicaciones o los datos.



Si nos centramos en las líneas de comunicaciones podemos distinguir distintos ataques:

Captura de Mensajes

Análisis de Tráfico: aunque el contenido de un mensaje no pueda ser descubierto (criptografía), el simple análisis del flujo de información (nodos que se comunican y su localización, frecuencia y longitud de los mensajes) puede aportar algo de información.

Estos ataques no alteran la información y son difíciles de detectar.

Debemos tratar de **prevenirlos**.

INTRODUCCIÓN

Modificación de mensajes.

Negación de Servicio: ataque que trata de evitar el normal uso de los recursos de comunicaciones. Ej. Saturación de la red para conseguir una degradación de las prestaciones.

Masquerade: Suplantación de la identidad de un nodo o usuario. Lleva asociado normalmente la captura y manipulación de los mensajes de autentificación.

Deben **detectarse** y **evitar efectos desastrosos.**

No olvidemos que **el sistema de gestión** se compone de diferentes aplicaciones y bases de datos que están soportadas por distintas plataformas hardware, también puede ser el **blanco** de violaciones de seguridad.

Se aplican los mismos ataques, pero **la información de gestión es especialmente sensible** dado que de ella depende el normal funcionamiento de la red.

Funciones de la gestión de la seguridad:

Mantenimiento de la información que necesitan los sistemas de seguridad de la red: claves, información de autentificación, información de derechos de acceso...

La gestión de la seguridad debe **registrar la actividad** sobre esta información como ayuda para la recuperación

ante ataques exitosos.

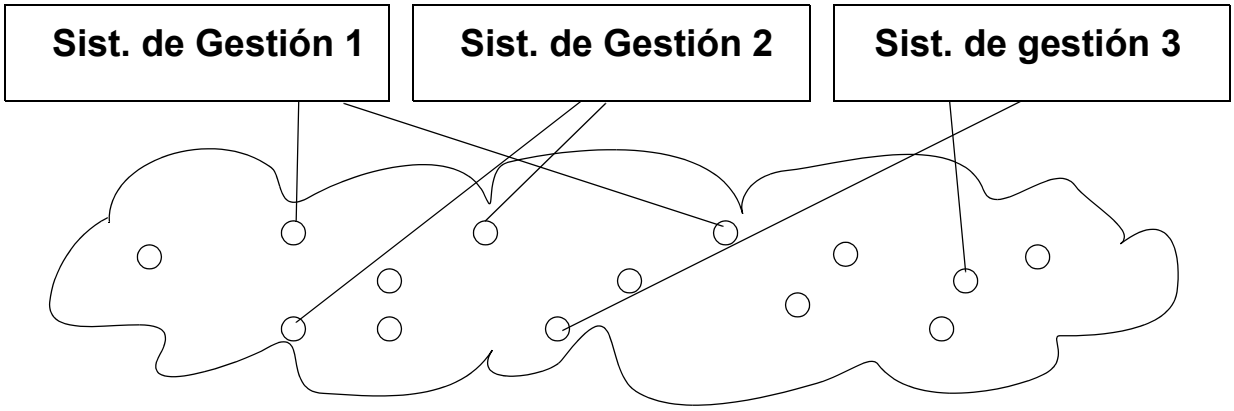
Control del acceso a los recursos: Debe autentificarse al usuario para concederle el acceso a determinados recursos.

Control del proceso de encriptación: entre agentes y gestores. Debe gestionarlo también para otras entidades: elección de algoritmo de encriptación, distribución de claves.

INTRODUCCIÓN

1.4 El Por Qué de una Gestión de Red Integrada

Enfoque Tradicional



- Acoplamiento entre servicios específicos a ciertos recursos de la red.
- Múltiples Sistemas de Gestión para cada una de las redes. Incluso para diferentes equipos de la misma red.
- Múltiples equipos de personas realizando funciones similares.

Conclusión: Conjunto no interoperable de soluciones parciales ineficientes, complejas, poco flexibles y caras de administrar.

INTRODUCCIÓN

Qué está cambiando?

Evolución de los servicios: Desde los clásicos servicios de poca capacidad hasta los nuevos servicios ofrecidos por las redes de banda ancha (Video bajo demanda, Videoconferencia...)

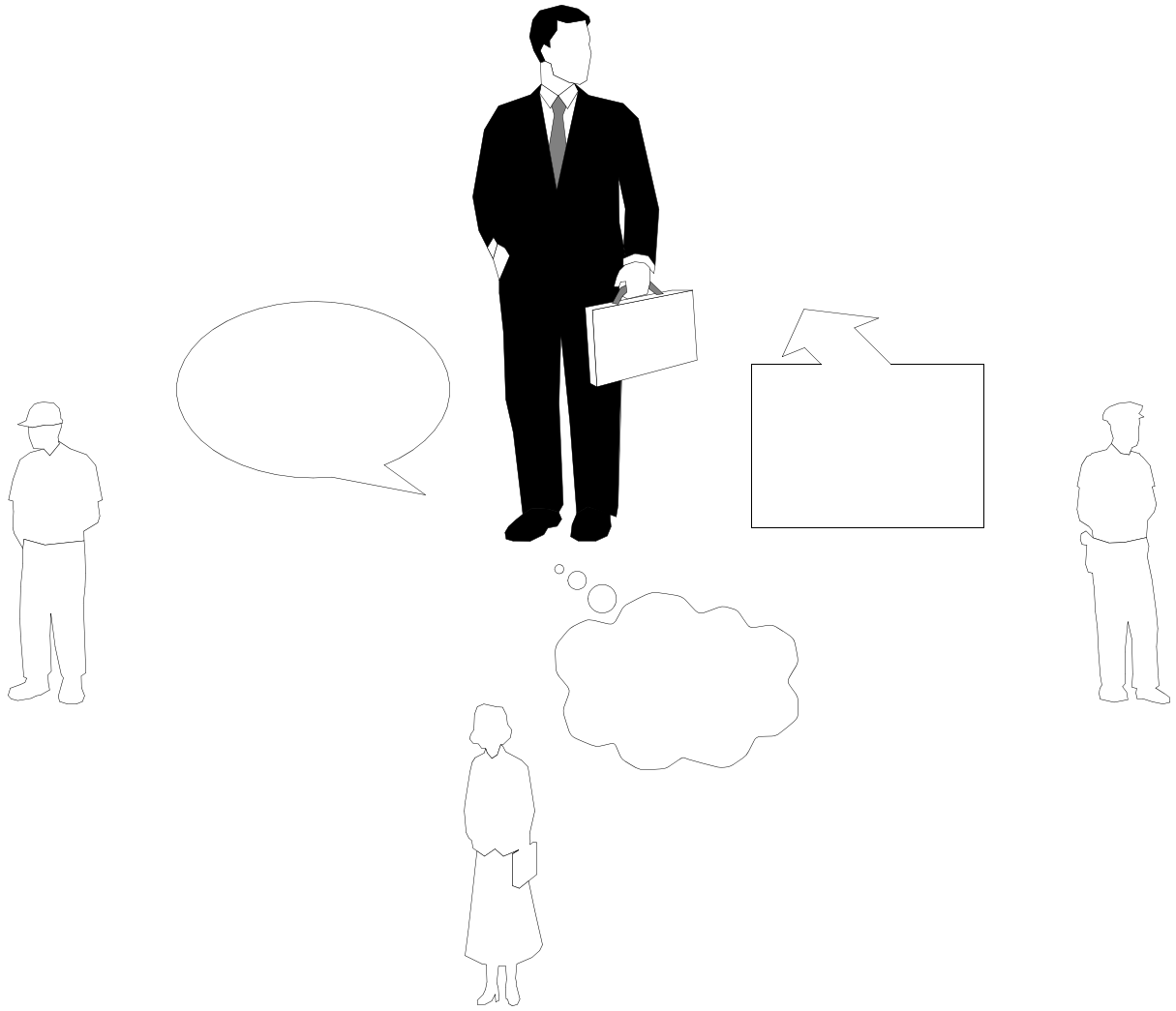
Evolución de la tecnología: Introducción de tecnologías síncronas en las redes de transmisión (SDH/ SONET). Introducción de Asynchronous Transfer Mode (ATM), tanto en redes locales como en redes más extensas.

Evolución en las demandas de los clientes: Los clientes demandan servicios fiable con capacidades para remotamente solicitar cambios, informar de problemas, acceso a información de facturación, con tiempos de provisión de servicio cada vez menores

Competitividad: El panorama del sector de las telecomunicaciones está cambiando radicalmente debido a la liberalización del mercado: existe la necesidad imperiosa de disminuir los costes de operación de la red, un uso más eficiente de los recursos, acelerar la implementación de nuevos servicios...

Solución: Los Estándares de Gestión de Red

INTRODUCCIÓN

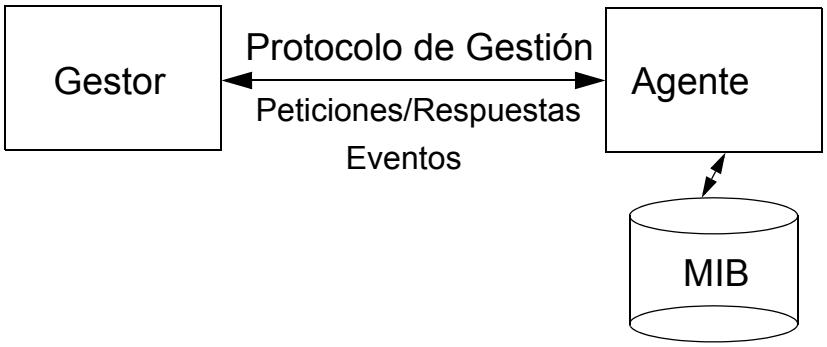


Importante estandarizar:

Una manera de preguntar a los subordinados: **Protocolo de Gestión.**

Una manera de expresar las informaciones: **El Modelo de Información.**

1.5 Conceptos Básicos de los Estándares de Gestión



Gestor: típicamente, una estación de trabajo donde se ejecutan las aplicaciones de gestión de red, que disponen de interfaces gráficas para presentar información al usuario y para facilitarle la invocación de operaciones de gestión.

Agente: Suele ejecutarse en el dispositivo a gestionar (host, router, hub...) o en una estación con acceso a los recursos gestionados. Responde a peticiones del gestor y puede asíncronamente enviarle información acerca de algún evento importante.

Base de Datos de Gestión (MIB): Información mantenida en el Agente y sobre la que realiza las peticiones el Gestor.

Protocolo de Gestión: El utilizado para la comunicación Gestor/Agente.

1.6 Gestión de red Centralizada, Jerarquizada y Distribuida

1.7 Organismos de Estandarización

Internet Architecture Board (IAB)

Creada en 1983, con el nombre Internet Activities Board. Su objetivo era observar la evolución de la red de ARPANET (y después la NSFNET) y las posibles mejoras a realizar. También se ocupaba de detectar dónde era necesario o conveniente especificar un nuevo protocolo.

La información circulaba en documentos en forma de documentos técnicos denominados RFC (Request For Comments). Los RFCs siguen siendo hoy en día el mecanismos de publicación de los estándares de Internet.

En 1989 el IAB se reorganiza para acomodarse a la evolución de la red. Se crearon dos subcomités:

- Internet Engeneering Task Force (IETF). Resuelve cuestiones de ingeniería más inmediatas.
- Internet Research Task Force (IRTF). Se concentra en los problemas a a largo plazo.

Actualmente una propuesta de un nuevo estándar debe

explicarse con todo detalle en un RFC y tener el interés suficiente en la comunidad Internet para que sea tomada en cuenta; en ese momento se convierte en un Estándar Propuesto (Proposed Standard). Para avanzar a la etapa de Borrador de Estándar (Draft Standard) debe haber una implementación operativa que haya sido probada de forma exhaustiva por dos instalaciones independientes al menos durante cuatro meses. Si supera esta fase, el software funciona y el IAB considera que la idea es buena se declarará el RFC como un Estándar Internet (Internet Standard). Además se prevé también un mecanismo de 'envejecimiento', es decir que un protocolo pueda quedar anticuado debido a la aparición de otros nuevos y más avanzados que le sustituyan, por lo que un Estándar Internet puede pasar al estado de Obsoleto o Histórico.

Un RFC puede describir un RFC que nunca llega a aceptarse como estándar y pasar después al estado histórico.

Existen RFCs de carácter informativo.

Internet Society (ISOC)

En 1991 se creó la Internet Society (ISCO), una asociación internacional para la promoción de la tecnología y servicios Internet en todos los ámbitos de la

sociedad.

Cualquier persona física o organización puede ser miembro de la ISOC.

Absorbió en su seno el IAB con sus dos subcomités, el IRTF y el IETF.

International Telecomunications Union (ITU)

Organización creada en 1934 y con la creación de las Naciones Unidas se vinculó a ésta en 1947. La ITU tiene tres sectores de los cuales solo nos interesa el conocido como ITU-T que es un Comité de Estandarización en temas de telecomunicaciones. El objetivo de este comité es la estandarización de técnicas y operaciones de telecomunicaciones para conseguir la compatibilidad terminal-terminal en las conexiones internacionales de telecomunicaciones, sin importar países de origen y destino.

Desde 1956 a 1993 la ITU-T se conoció como CCITT (Comité Consultivo Internacional en Telefonía y Telegrafía).

En 1993 el CCITT fue reorganizada y se le cambió el nombre a ITU-T.

Los miembros de la ITU-T son de cinco clases:

- Representantes de los países.
- Operadores privados reconocidos (por Ej. British Telecom, Global One, AT&T).
- Organizaciones regionales de telecomunicaciones (p. Ej. el ETSI).
- Empresas que comercializan productos relativos a telecomunicaciones y organizaciones científicas
- Otras organizaciones interesadas (bancos, líneas aéreas, etc.)

Sólo los representantes de los países tienen derecho a voto.

Para desarrollar su trabajo se organiza en Grupos de Estudio (hasta 400 personas). Los Grupos de Estudio se dividen en Equipos de Trabajo (Working Parties), que a su vez se dividen en Equipos de Expertos (Expert Teams).

Cuenta con **Grupos de Estudio:**

- - Grupo 1: Servicios.
- - Grupo 2: Organización de red.
- - Grupo 3: Tarificación y principios de contabilidad.
- - Grupo 4: Mantenimiento.
- - Grupo 5: Protección contra efectos electromagnéticos.
- - Grupo 6: Planta exterior.
- - Grupo 7: Redes de Comunicaciones de datos.

- Grupo 8: Terminales para servicios telemáticos.
- Grupo 9: Redes y equipos terminales de telégrafos.
- Grupo 10: Lenguajes para aplicaciones de telecomunicación.
- Grupo 11: Conmutación y señalización.
- Grupo 12: Performancia de transmisión de redes y equipos terminales de telefonía.
- Grupo 15: Equipos y Sistemas de Transmisión.
- Grupo 17: Transmisión de datso en redes de telefonía.
- Grupo 18: ISDN.

La ITU-T denomina a sus estándares 'recomendaciones'.

Todos los estándares de la ITU-T se nombran mediante una letra seguida de un punto seguido a su vez de números.

En ciclos de 4 años la asamblea plenaria decide y planifica en función del trabajo de un grupo de estudio. Aprobación de las recomendaciones (*Draft Recomendations*) para su posterior publicación en libros.

También decide sobre la creación o eliminación de grupos de estudio.

INTRODUCCIÓN

International Organization for Standarization (ISO)

Organización voluntaria creada en 1946 con sede en Ginebra.

Agencia Internacional para el Desarrollo de Estándares en un amplio rango de temas. Sus miembros son las organizaciones de estandarización de naciones participantes y otras organizaciones observadoras sin derecho a voto. Conocida su labor de estandarización en arquitecturas de comunicación para la interconexión de sistemas abiertos.

Se organiza en cerca de 200 comités técnicos denominados TC (Technical Committee) que se numeran en orden ascendente según su fecha de creación. El que nos interesa a nosotros es el TC97 que trata de ordenadores y proceso de la información. Cada comité tiene subcomités (SCs) que a su vez se dividen en grupos de trabajo o WGs (Working Groups).

Un grupo de trabajo de un comité técnico publica un "*committee draft*" compuesto de unas especificaciones técnicas para el estándar propuesto. Una vez aceptado por los miembros interesados se adapta a las prácticas ISO y se edita un "*draft international standard*". Al cabo de 6 meses si es aprobado por un 75% del comité técnico se convierte en "*International Standard*".

INTRODUCCIÓN

Enfoques.

Tradicionalmente la ISO ha abordado aspectos de **comunicaciones por ordenador y procesamiento distribuido (niveles 4 a 7 de la capa OSI)**, mientras que la ITU ha trabajado más los temas de r**edes de comunicaciones y transmisión de datos (niveles 1 a 3).**

La evolución de la tecnología de redes ha hecho que ambas converjan y tengan que colaborar en la definición de nuevos estándares.

Foros industriales

La elaboración de estándares en ITU-T y la ISO se ha caracterizado por una gran lentitud, debido a la necesidad de llegar a un consenso entre muchos participantes y a procedimientos excesivamente complejos y burocratizados.

Los fabricantes de equipos, que perdían gran cantidad de mercado por culpa de estos retrasos.

A principios de los 90 surgió un nuevo mecanismo para acelerar la creación de estándares, que fue la creación de foros industriales.

La idea era simple: un conjunto de fabricantes, usuarios

y expertos interesados en desarrollar una tecnología concreta forman un consorcio que se ocupa de fijar los estándares necesarios para garantizar la interoperabilidad entre diversos fabricantes; los estándares se hacen públicos de forma que cualquier fabricante que lo desee puede desarrollar productos conformes con dicho estándar.

No pretenden competir con las organizaciones internacionales de estándares, sino cooperar con ellas y ayudarlas a acelerar su proceso.

Características:

- Intentan aclarar ambigüedades
- Definir subconjuntos de funciones que permitan hacer una implementación sencilla
- Comprobar la viabilidad y la interoperabilidad entre diversos fabricantes.
- Establecen fechas límite para la producción de estándares

Ejemplos: Forum Frame Relay, el Forum ATM y el Forum ADSL.