1 Introducción

La gestión de red trata sobre la planificación, la organización, la supervisión y el control de elementos de comunicaciones para garantizar un adecuado nivel de servicio, y de acuerdo con un determinado coste. Los objetivos principales de la gestión de red consisten en mejorar la disponibilidad y el rendimiento de los elementos del sistema, así como incrementar su efectividad.
Se definen cinco áreas funcionales para la gestión de red, las de supervisión y fallos, configuración, tarificación, prestaciones y seguridad.

1.1 Monitorización, control, gestión

monitorización: acciones consistentes en obtener información de la red con el fin de detectar anomalías. Se utiliza para proporcionar información en la gestión de las funciones de prestaciones, fallos, contabilidad y en determinados aspectos de configuración.
control: se establece una señalización en toda red que se ocupa de regular activamente las comunicaciones y, en general, el tráfico de la red. Se aplica a las funciones de configuración y seguridad
gestión: la integran las redes más avanzadas RDSI, GSM,etc, por ejemplo TMN.

2 Gestión de servicios

2.1 Introducción al sistema de señalización nº 7 (SS7)

El protocolo SS7 se ocupa de la señalización y es el modelo en capas que cubre la comunicación entre nodos inteligentes en la red Channel Common Signalling (CCS). Esta red se define de forma separada de la red de transporte de información. En su forma básica consta de nodos llamados puntos de señalización (SPs) interconectados por enlaces de transmisión.

2.2.2 Introducción a las redes inteligentes

La introducción de ordenadores y, por tanto, de software en los nodos de la red permite configurar mediante programación el comportamiento, los servicios y, por tanto, la inteligencia del sistema.

El motivo básico del desarrollo de esta red es el de obtener mayores beneficios para el operador al aumentar el tráfico telefónico y también los ingresos debido a las suscripciones de los usuarios a los nuevos servicios, y gestionar mejor los recursos del sistema con el fin de optimizar el rendimiento y reducir costes en el servicio.

La ITU-T ha especificado una serie de servicios inteligentes CS1 (Capability Services 1). Dentro de los tipos de servicios CS1, en los que se basan la gran mayoría de infraestructuras de operadores de servicio actuales, pueden citarse los siguientes: servicios de tarificación en llamadas (números 900,...), servicios de encaminamiento, numeración, etc. Entre los servicios especificados en CS2 destacan los servicios de interconexión con otras redes, multiconferencia, movilidad personal, movilidad de terminal y servicios multimedia, etc.

2.2.4 Componentes de la red inteligente avanzada *(Advanced Intelligent Network, AIN)*

Service Switching Point (SSP): Su misión consiste en 'interceptar" las solicitudes de los servicios mediante condiciones de disparo ("triggers") debidas a tomas de línea, prefijos marcados o condiciones de la línea destino, reconociendo así las llamadas que precisan un tratamiento especial por parte de la RI.
Signal Transfer Point (STP): enrutan mensajes SS7 entre los nodos de la red. Existe una tabla en cada STP que indica para cada número el SCP y el enlace que se debe utilizar para enviar el mensaje. Cada número concreto accede a un servicio diferente.
Los STP utilizan enlaces para sus interconexiones que suelen calcularse para un 40 % de su capacidad, si uno de ellos (enlace o STP) falla, el otro soportaria hasta un 80 % de tráfico, sin saturarse.

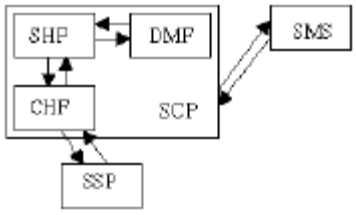


Fig. 2.7 Esquema de funcionalidades del nodo SCP

Service Control Point (SCP): Los SCP son bases de datos que almacenan datos de clientes y programas lógicos de servicios (SLPs) para responder a peticiones procedentes de SSPs.
Por ejemplo, convertir números 800 (900) en encaminamientos para números de la red básica, validar números, etc.
Sea la DMF la función de procesado de la llamada, la CHF la función que realiza de interfaz decomunicaciones con el módulo SSP y la SHF el programa del servicio lógico que ejecuta el SLP.

Service Data Point (SDPs): bases de datos asociadas a los SCPs.
Signaling Links (SLs): interconexiones entre los nodos,
Service Management System (SMS): realiza funciones de mantenimiento, administrativas y de provisión para los SCPs. También realiza la función de creación de servicios.
Intelligent Peripherals (IP): añaden funciones de comprensión a la red tales como reconocimiento de voz, síntesis y anuncios de voz específicos.
Adjunct (AD) / Services Node (SN): nodos AIN que se conectan a los SSPs y que realizan las mismas funciones que SCPs.

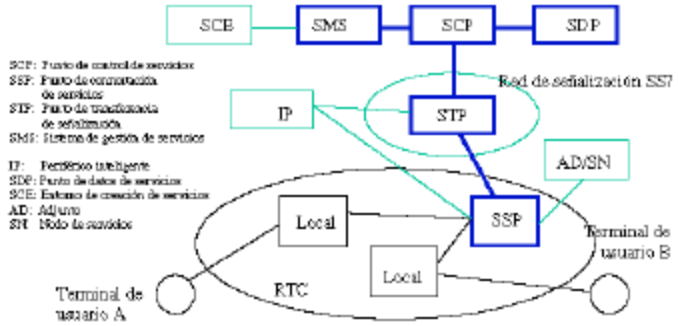


Fig. 4.4 Esquema de arquitectura de la red inteligente

2.2.7 Modelo de llamada básico de la red inteligente

Para proporcionar los servicios de red inteligente, algunas funciones de procesado de la llamada se desplazan desde el SSP y se convierten en programas lógicos de servicio residentes en el SCP.
En puntos de detección de disparo (TDPs) es donde la información almacenada se transfiere al SCP, esta información es lo que define un tipo de servicio AIN.

2.3 TINA (Telecommunications Information Networking Architecture).

TINA define los servicios de telecomunicaciones y los sistemas de gestión como aplicaciones basadas en *software* que operan en una plataforma de computación distribuida, orientada a objetos CORBA.
La arquitectura TINA se estructura en cuatro grandes áreas: arquitectura de computación, arquitectura de servicio, arquitectura de red y arquitectura de gestión.

2.3.1 Arquitectura de computación TINA

La arquitectura de computación define los conceptos de modelado que deberían de usarse para especificar el *software* orientado a objetos en sistemas TINA. Además define un entorno de proceso distribuido (DPE) que proporciona un sistema de soporte que permite a los objetos localizar e interactuar entre ellos. Estos conceptos se basan en el *Reference Model for Open Distributed Processing (RM-ODP).*
El modelado computacional utiliza los objetos computacionales como las unidades de programación y encapsulación. Los objetos interactúan entre ellos mediante el envío y la recepción de información a/desde interfaces.

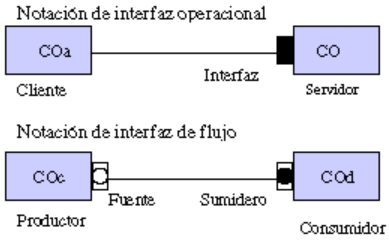


Fig. 2.9 Tipos de interfaz de objeto computacional

2.3.2 Arquitectura de servicio TINA

Describe cómo debería estar estructurado un servicio distribuido para proporcionar sus funciones al usuario.
Con TINA se reemplaza el concepto de llamada por el de sesión, entendiendo como el propósito de un servicio de realizar un conjunto de actividades durante un periodo específico de tiempo.

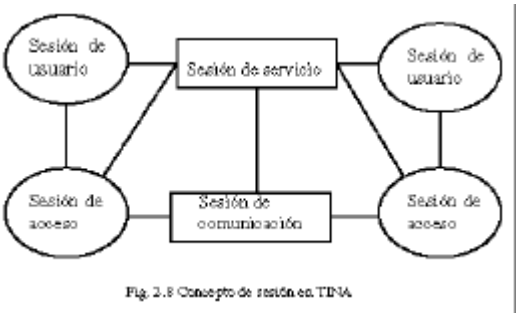


Fig. 2.8 Concepto de sesión en TINA

2.3.3 Arquitectura de red TINA

La arquitectura de red intenta proporcionar un conjunto de abstracciones que describen redes de transporte de una forma independiente a la tecnología *(Network Resource Information Model, NRIM).*

Se pueden considerar los siguientes niveles de gestión:
Nivel de elementos de red:
Nivel de gestión de recursos:
Nivel de gestión de servicios:

2.3.4 Arquitectura de gestión TINA

Las áreas funcionales de gestión son las ya clásicas cinco definidas por la TMN en la ITU: fallos, rendimiento, seguridad, configuración y tarificación. En TINA además, se subdivide la gestión de configuración en gestión de conexiones y en gestión de configuración de recursos.
A menudo se utiliza otro tipo de clasificación:
Gestión de computación: relacionada con la gestión de los ordenadores, las plataformas, y el *software* que se ejecuta en esa plataforma. Su principal interés es el empleo, la instalación, y la carga de *software*.
Gestión de las telecomunicaciones: se refiere a los servicios de telecomunicaciones, el *software* de control y la gestión de redes de transmisión y conmutación. La gestión de telecomunicaciones se divide, en gestión de servicio, red y elemento.

3 Soluciones para la gestión de redes

3.3 Mecanismos para la detección de configuraciones de red

En el proceso de detección se envían de modo secuencial mensajes ICMP a cada uno de los nodos, en el caso de que no contesten al cabo de un determinado tiempo, los nodos se dan por inactivos.
Existen una serie de problemas en el caso de que se produzca una inundación de mensajes ICMP. Para evitarlo el algoritmo COP-N restringe el número de mensajes que pueden estar no reconocidos (N) en un determinado instante. Una política de gestión usual es utilizar un sistema con N=3 y un tiempo de *timeout* de 10 segundos, que se suele duplicar en los tres subsiguientes intentos.
El algoritmo RPE *(Regulated Poll Emission)* los mensajes de prueba se emiten a una tasa que no supera un determinado nivel mediante un mecanismo de *leaky bucket.*

3.3.2 Modelado de la duración de un ciclo de consultas de estatus

Sea un ciclo de *polling* con K intentos.

Probabilidad de que el k-ésimo intento no sea reconocido es:

$P_k=1-(1-\gamma_?)(1-\gamma_2)(1-\gamma_3)P(A_k \leq T_k)$:

La duración media del tiempo restante del ciclo de polling al comienzo del k-ésimo intento es:

$E[S_k]=E[C]+(1-P_k)E[A_k]+ P_k(E[T_k]+E[S_{k+1}])$

γ_1: El mensaje de *polling* ICMP se pierde en su viaje
γ_2: El nodo no es alcanzable porque el camino está cortado
γ_3: Pérdida del mensaje de reconocimiento, por ejemplo debido a congestión en la red
$P(A_k \leq T_k)$: El ack. no se devuelve antes que expire el *timeout*
S_k : tiempo restante de resolver la interrogación al comienzo del k-ésimo intento
C: tiempo en emitir un mensaje de *polling* ICMP
T_k: intervalo de timeout.
A_k: tiempo en recibir un reconocimiento (ack)

Número esperado de intentos de *polling* en un ciclo: $E[N_p]=\sum_{k=1}^{K-1} K(1-p_k)\prod_{j=1}^{K-1} p_j + K\prod_{k=1}^{K-1} p_k$

N_p: número de intentos de polling requeridos dentro de un ciclo

La máxima demanda de ancho de banda de *polling* viene acotada por: $S_p X E[N_p]$

S_p: denota el tamaño de un mensaje de polling,
X: flujo máximo

3.3.5 Flujos del ciclo de *polling*

Método COP-N

La tasa máxima resulta ser: $X_H = \frac{N}{E[S_1]}$

El período de congelamiento resulta ser: $\sum_{i=1}^{K} T_i$

Si la red funciona perfectamente $X_H^* = \frac{N}{a+C}$

a: tiempo de reconocimiento medio en ausencia de fallos

Método RPE

Tasa máxima $\frac{1}{\tau}$

τ: el tiempo mínimo entre emisiones de consultas ICMP.

Número medio de peticiones de *polling* residentes en memoria: $X E[S_1]$

Para que el sistema funcione correctamente $X < min\left[\frac{1}{\tau}, \frac{M}{E[S_1]}\right]$

M: máximo número de nodos permitido para que peticiones de *polling* no sean reconocidas

Si la red funciona correctamente, el método COP-N puede atascar la red de forma intermitente, mientras que con el método RPE, se puede escoger un τ apropiado para evitar bloqueos.

3.3.6 Análisis del retardo

Método COP-N $t+(n-N-1)E[S_1]+\sum_{k=1}^{K} T_k$

Método RPE $t+(n-1)\tau$

5 Gestión según OSI

El fundamento del sistema de gestión OSI es la BBDD que contiene información relativa a los recursos y elementos que deben ser gestionados (MIB).
Cada recurso que se monitoriza y controla por el sistema de gestión OSI se representa por un objeto gestionado.

modelos de gestión de sistemas:
- Modelo de comunicaciones: se detalla el protocolo de gestión y el servicio que proporciona.
- Modelo de información: se definen los recursos de red usando una sintaxis abstracta.
- Modelo funcional: se definen las funciones de gestión que proporcionan una interfaz a la aplicación de gestión. Describe las cinco áreas: gestión de fallos, gestión de configuración, gestión de prestaciones, gestión de contabilidad y gestión de seguridad.
- Modelo de organización: se exponen las posibles subdivisiones de la red en dominios de gestión.

5.3 Modelo de comunicaciones: CMIP

El *Common Management Information Protocol* (CMIP) ofrece un mecanismo de transporte en la forma de servicio pregunta-respuesta para capas OSI.

Versión de CMIP sobre protocolos TCP/IP (CMOT), versión de CMIP sobre protocolos IEEE de LANs (CMOL).

5.3.1 Características principales del protocolo CMIP

- Las especificaciones son dificiles de realizar y tediosas de implementar en aplicaciones.
- La comunicación con los agentes está orientada a conexión.
- La estructura de funcionamiento es distribuida.
- El protocolo asegura que los mensajes llegan a su destino.

El hecho de que se trate de una gestión conducida por eventos se traduce en que:
- El agente notifica al gestor de sucesos la información concerniente a los recursos gestionados.
- El agente es responsable de monitorizar los recursos.
- Presenta la ventaja de que existe menor gestión de tráfico.
- Presenta la desventaja de tener agentes más complejos.

5.3.3 Servicios ofrecidos por CMIP

A través de CMISE *(Common Management Information Service Element)*, CMIP proporciona tres tipos de servicio:
- Manejo de datos: usado por el gestor para solicitar y alterar información de los recursos del agente.
- Informe de sucesos: usado por el agente para informar al gestor sobre diversos sucesos de interés.
- Control directo: usado por el gestor para solicitar la ejecución de diversas acciones en el agente.

También hace uso del servicio de operaciones remotas proporcionado por ROSE.

5.4.1 MIB (Management Information Base)

Una MIB es un conjunto de definiciones de uno o varios recursos formado por clases de objetos gestionados, acciones, notificaciones, atributos, sintaxis, etc, y los *name bindings*.
La sintaxis de MIBs se basa en la notación GDMO *(Guidelines for Definition of Managed Objects).*
Permite el uso de herencias y referencias a otras MIBs.

5.4.2 GDMO (Guidelines for Definition of Managed Objects)

Se hace uso de unas macros que se definen mediante ASN.1.
Proporciona normas útiles para diseñar MIBs, como son el agrupamiento de datos, el uso de herencia y la definición de relaciones.

6 Red de gestión de las telecomunicaciones (TMN)

La TMN *(Telecommunications Management Network)* proporciona funciones de gestión y comunicaciones para la operación, la administración y el mantenimiento de una red de telecomunicaciones y sus servicios en un entorno de multiples fabricantes La TMN define la relación entre los bloques funcionales básicos constituyentes de la red a través de interfaces estándares.

Las recomendaciones que regulan la TMN son las de la serie M.3XXX de la ITU-T. En estas recomendaciones se definen los siguientes modelos y arquitecturas:
- Arquitectura física: estructura y entidades de la red.
- Modelo organizativo: niveles de gestión.
- Modelo funcional: servicios, componentes y funciones de gestión.
- Modelo de información: definición de recursos gestionados.

6.1 Arquitectura física

Interfaz Qx: es una interfaz apropiada para pequeños elementos de red
Interfaz Q3: soporta un complejo conjunto de funciones. Está compuesta por:
Modelo de comunicaciones: protocolo CMIP
Modelo de información: semántica de datos (MIB's GDMO).
Interfaz X: soporta el conjunto de funciones para la interconexión de diferentes OSs, ya sea entre entornos de TMNs o no.

6.2 Modelo organizativo

El modelo organizativo (de capas de TMN) definido por la ITU-T
- gestión comercial
- gestión de servicios
- gestión de red
- gestión de elementos de red
- elementos de red.

Capa de gestión de red: con las siguientes funciones asociadas:
- provisión, cese o modificación de las capacidades de la red para el soporte de servicios a clientes.
- control y coordinación de todos los elementos de la red con su ámbito y dominio.

Capa de gestión de elementos de red:
- mantenimiento estadístico, control y coordinación de elementos de la red.

6.3 Modelo funcional

El modelo funcional se compone de Bloques de Servicios, Componentes y Funciones de gestión. La idea consiste en descomponer las funcionalidades de mayor a menor nivel en bloques reaprovechables

Servicios de gestión TMN

Los servicios de gestión que se definen son del siguiente tipo:
- Administración de abonados. Administración de encaminamiento y análisis de digitos. Administración de medidas y análisis de tráfico. Administración de la tarificación.
- Gestión de la seguridad de la TMN. Gestión de tráfico. Gestión del acceso de abonado. Gestión de circuitos entre centrales y equipo asociado. Gestión de la red de conmutación. Gestión de equipos en la instalación del usuario. Gestión del servicio controlado por el abonado. Gestión del sistema de señalización por canal común. Gestión de redes inteligentes. Gestión de la TMN.
- Administración de instalación del sistema. Administración de calidad de servicio y funcionamiento de la red
- Restablecimiento y recuperación.
- Gestión de materiales.
- Programa de trabajo del personal.

Componentes del servicio de gestión

TMN define muchos componentes, un ejemplo
- vigilancia de alarmas.

Funciones de gestión

Para el caso del componente de vigilancia de alarmas del citado ejemplo se podrían utilizar las siguientes funciones:
- funciones de informes de alarmas
- funciones de informes resumidos de alarmas
- funciones de criterios de sucesos de alarmas
- funciones de gestión de indicación de alarmas
- funciones de control de registro de alarmas.

6.4 Modelo de información

El modelo de información utilizado en TMN es el definido por el interfaz Q3 en la semántica de datos (MIBs GDMO).
El nivel de aplicación suele cubrirse mediante el protocolo CMIP.

7 Áreas funcionales de gestión

Se puede definir la gestión de red como la planificación, la organización, la supervisión y el control de elementos de comunicaciones para garantizar un adecuado nivel de servicio, y de acuerdo con un determinado coste.

Las recomendaciones de la OSI, posteriormente recogidas por la ITU, definen las siguientes áreas funcionales para la gestión de red:
Supervisión y fallos: conjunto de facilidades que permiten la detección, aislamiento y corrección de una operación anormal.
Configuración: facilidades que permiten controlar, identificar, recoger y proporcionar datos a objetos gestionados, con el propósito de asistir a operar servicios de interconexión.
Contabilidad: facilidades que permiten establecer cargos por el uso de determinados objetos e identificar costes por el uso de éstos.
Prestaciones: facilidades dedicadas a evaluar el comportamiento de objetos gestionados y la efectividad de determinadas actividades.
Seguridad: aspectos que son esenciales en la gestión de red y que permiten proteger los objetos gestionados.

El esquema de funcionamiento que sigue un sistema de gestión parte de las mediciones que se realizan de los recursos de la red a partir de los agentes que los mismos nodos contienen. Estos nodos, a través de sus agentes, proporcionan la información a los gestores de la red. Los gestores, a partir de los parámetros definidos en sus políticas de gestión, actúan sobre la red mediante mensajes de control sobre los agentes de los nodos, optimizando el funcionamiento a través de cambios de configuración, etc. Este control realizado sobre la red modifica las condiciones del tráfico y el ciclo se repite realizando nuevas mediciones sobre los recursos.

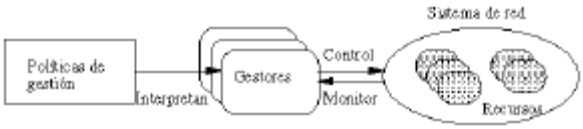


Fig. 7.1 Flujo de información de gestión

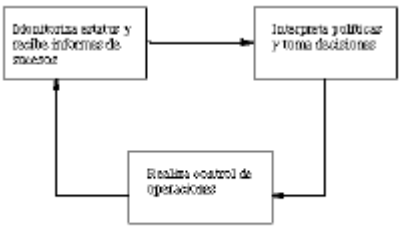


Fig. 7.2 Bucle de actividades de gestión

7.1 Gestión de fallos

El determinar el máximo de información sobre los fallos es el elemento fundamental para su buena gestión.

7.3 Gestión de prestaciones

Entre los indicadores de prestaciones se pueden definir los que están orientados al servicio, como la disponibilidad, el tiempo de respuesta, y la fiabilidad, otros indicadores están orientados a la eficiencia, como el throughput o la utilización.

7.5 Gestión de seguridad

La gestión de seguridad está relacionada con la generación, distribución y almacenamiento de claves de cifrado, información de passwords o bien información de control de acceso y autorización que debe mantenerse y distribuirse.

12 Gestión en Internet

La familia de protocolos SNMP es actualmente la configuración de gestión más extendida y propia de las redes con pilas de protocolos TCP/IP.

12.3 Estructura de la información de gestión

Se utiliza un método común para nombrar a los objetos (Object Identifiers, OID). son una secuencia de enteros separados por un punto que forman un árbol. El árbol está formado por ramas y nodos.
Estos OIDs son los que permiten alcanzar (nombrar) objetos mediante SNMP.

12.4 Sintaxis ASN.1

La sintaxis abstracta ASN.1, define el tipo de datos que modela el objeto. La sintaxis abstracta se utiliza para describir tanto las estructuras de datos como la información de gestión que contienen estas estructuras de datos
La sintaxis de transferencia proporciona, a partir de la definición de las estructuras de datos, una forma determinada de transmitir los datos a través de la red (Basic Encoding Rules, BER).

Una colección de descripciones ASN.1 relacionadas con un mismo tema se conoce como módulo.
Se definen tres tipos de objetos con ASN.1:
- Tipos (types), que definen nuevas estructuras de datos, pueden ser simples, estructurados, subtipos.
- Valores (values), que son realizaciones (variables) de un tipo.
- Macros, que se utilizan para cambiar la gramática ASN.1.

12.5 Bases de información de gestión (MIB)

Las bases de información de gestión (MIB) son un conjunto de objetos gestionados de un recurso que se publican para ofrecer interoperabilidad de gestión. Estos objetos se organizan en grupos, existen los siguientes tipos de MIBs: las estándares, las experimentales y las privadas, que incorporan la información de los diversos fabricantes de equipos.

12.5.1 MIB-I

La MIB-I constituye la primera MIB normalizada. Está formada con objetos de la torre de protocolos de TCP/IP.

12.5.2 MIB-II

Se define un nuevo grupo para cada tipo específico de interfaz, así como un nuevo grupo con objetos de SNMP.

12.6 Simple Network Management Protocol (SNMP)

(SNMP) es un protocolo de aplicación que ofrece servicios de gestión de red al conjunto de protocolos Internet.
El programa cliente (llamado el gestor de red) realiza conexiones virtuales a un programa servidor (llamado el agente SNMP) ejecutando en un dispositivo de red remoto. La base de datos controlada por el agente SNMP se denomina Management Information Base (MIB), y es un conjunto estándar de valores estadísticos y de control de status.

Los mensajes enviados por el cliente (gestor de red) a los agentes SNMP están formados de identificadores de objetos MIB, junto con instrucciones a fin de cambiar u obtener un valor.

La torre de comunicaciones SNMP se apoya en la estructura de protocolos TCP/IP de Internet

Entre las características principales del protocolo SNMP se puede destacar el hecho de que es un protocolo de gran flexibilidad y que permite una gran extensibilidad a todo tipo de redes.

La eficiencia del protocolo para la transmisión de información es baja, ya que se trata de una arquitectura basada en polling de acuerdo con una estructura de funcionamiento centralizada. El gestor pregunta periódicamente a la información del agente sobre los recursos gestionados, es el gestor el responsable de monitorizar los recursos.

Al ser un protocolo basado en UDP/IP no garantiza la llegada de los mensajes

12.6.1 Operaciones de SNMP

Destacan las Traps como mensajes especiales que especifican alarmas o sucesos inusuales.
El uso de MIBs privadas junto con mensajes tipo Trap permite la respuesta del sistema a alarmas específicas de los equipos de cada fabricante.

12.6.2 Codificación para la transferencia de la información de gestión: BER

para la codificación se utilizarán las BER (Basic Encoding Rules) permiten traducir una estructura de datos cualquiera en una secuencia de bytes y viceversa.

12.8 Marco administrativo

Para una gestión con SNMP adecuada se define un nombre de comunidad (community) que es una relación entre un agente y gestores

12.9.3 Valoración crítica de las MIB en SNMP

aspectos negativos MIB:
- Comunicaciones datagrama son ineficientes para la obtención de grandes cantidades de información.
- No existen mecanismos para la obtención agregada de datos de las MIB.
- No existen mecanismos de compresión de la información en la fuente.
- No existen mecanismos de correlación de la información en la fuente (p.e. la unión de tablas SNMP).
- No existe control de acceso a MIB.
- La estructura estática de la información en las MIB limita la manipulación y la reconfiguración dinámica,

12.10 Conclusiones sobre SNMP

ventajas del protocolo SNMP:
- Es un estándar de mercado.
- Es simple, fácil de usar.
- Modelo útil para el acceso a datos de gestión de la red.
- Acceso y organización eficientes de los datos gestionados.
- Independencia del entorno de comunicaciones.

Inconvenientes del protocolo SNMP:
- Limitaciones en el mecanismo de obtención de información
- Limitaciones de las capacidades de modelado de datos:
    MIB estática
    Correlación de datos difícil
    Modelados de sistemas complejos.

12.11 Comparación entre los protocolos CMIP y SNMP

SNMP hace uso de un árbol de directorios estático y CMIP hace uso de un árbol de directorios dinámico.
SNMP utiliza un número mínimo de tipos de datos ASN.1, mientras que CMIP hace usa un rango extendido de tipos ASN.1.
SNMP utiliza datagrama, mientras que CMIP utiliza conexiones con fuerte dependencia del estándar OSI.
CMIP obtiene un mayor rendimiento de los mensajes enviados ya que se reduce la señalización respecto al protocolo SNMP.
CMIP también es más seguro que el SNMP.
CMIP se basa en una arquitectura jerárquicamente distribuida, lo que permite que el número de objetos supervisados sea mayor que en el protocolo SNMP.
CMIP es más escalable, permite la herencia de atributos y es más flexible que el protocolo SNMP.
SNMP que es más simple y que el personal requerido para su mantenimiento se reduce.
SNMP es el utilizado por la gran mayoría de fabricantes y clientes, y existe una multitud de productos comerciales.

12.12 SNMPv2

- Admite mecanismos de seguridad como la autentificación y el cifrado
- Permite la comunicación entre estaciones de gestión.

Sin embargo, el hecho de su incompatibilidad con la versión SNMP y la mayor complejidad añadida a las plataformas están desestimando su futura implementación.

12.13 SNMPv3

Las áreas a las que SNMPv3 va enfocado son primordialmente mejorar la seguridad y la administración respecto a SNMPv2.

12.14 Remote Network-Monitoring (RMON)

Define una MIB para permitir la monitorización remota, y proporciona al gestor de red información vital acerca de la interconexión con otras redes.

RMON permite el uso de agentes “inteligentes” que responden de acuerdo con acontecimientos excepcionales. Esto reduce el tráfico asociado con la red de gestión, mientras que permite al equipo remoto alertar a la plataforma de gestión SNMP cuando ocurre algún problema.

Entre las características principales cabe destacar:
- Monitorización preventiva: se puede enviar periódicamente información de estatus de la red
- Multiples gestores: RMON permite la estructura de plataformas gestoras dispuestas de forma distribuida y jerárquica.

El estándar RMON es un sistema de monitorización remota que está creciendo muy deprisa como solución a problemas de gestión de red centralizada. Proporciona una arquitectura distribuida, frente al carácter centralizado del protocolo SNMP.

- Red con sonda RMON (agente RMON): reduce el tráfico de gestión ya que analiza el tráfico, las alarmas, etc. y procesa toda la información de la red, mandando únicamente los datos significativos a la estación de gestión
- Red sin sonda RMON: un polling continuo de la estación de gestión al monitor. provoca un mayor tráfico de gestión.

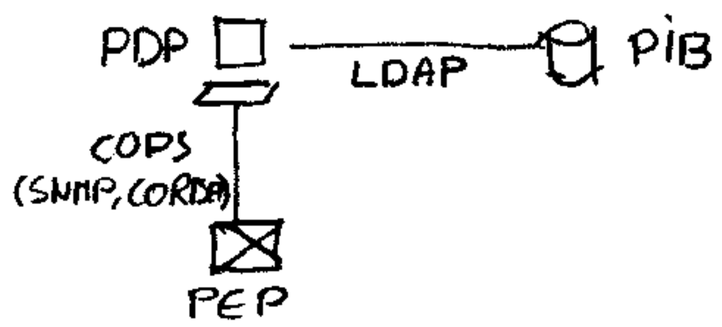
12.15 RMON 2

Una sonda RMON2 puede monitorizar tráfico de acuerdo con protocolos de nivel de red y direcciones, incluido el Internet Protocol (IP). puede decodificar y monitorizar tráfico a nivel de aplicación.

* GESTIÓN BASADA EN POLÍTICAS

- Potente, ágil, complicada
- POLÍTICA: conjunto de reglas if (cond1 or cond2 ...) then (acción)
  Se almacenan en contenedores de políticas
- PCIM: modelo marco de referencia de las políticas. Estructura en árbol

- Arquitectura



PIB (Policy Info Base): params básicos definidos con ASN.1

PDP (Policy Decision Poin): gestor

PEP: sistema gestionado

- SLA: Contrato entre proveedor y cliente, se especifican niveles de QoS.
  - dinámicos: basados en PBNM, pedir servicios no contratados de forma puntual

- COPS:
  - Protocolo orientado a conexión
  - Más complicado que un protocolo que solo monitorice
  - Admite más nodos que SNMP, se basa en traps.
  - No es jerarquicamente distribuido (+ de un gestor) → es más flexible.

- PBNM:
  - Al reservar un servicio, un gestor comprueba que haya recursos libres en cada red por las que se va a pasar
  - Se suele reservar hasta un punto y dar prioridad en el resto.

* GESTIÓN BASADA EN WEBS

- WBEM (Web Based Enterprise Management)
  - Orientado a objetos
  - Funcionalidades (Fallos, Rendimiento, Tarificación, Config, Seguridad)
  - Las notificaciones no están especificadas en http.
  - Estos sistemas se integran en otros (JAVA, SNMP)
    - ✗ Menor rendimiento
    - ✓ Más flexibilidad
    - ✓ Menos costes

- CIM: modelo para los objetos gestionados.
- MOF: formato de la sintaxis

* GESTION BASADA EN JAVA

- JDMK (Java Development Management kit)
  Define API·s para la interconexión con CORBA, SNMP, CMIP, WBEM, ..

  - Nivel de instrumentación : recoge info de los niveles inferiores (monitoriza)
  - Nivel de agente : gestiona los recursos
  - Nivel de servicios distribuidos : plataforma gestión, interfaz con otros modelos

* GESTIÓN DISTRIBUIDA

- Fundamentada en OMG
- Arquitectura distribuida → optima y de alto rendimiento.
  → difícil aplicación, elevado coste
  - Se aplica a grandes redes (redes ópticas, com. moviles 3G)

CORBA

- Busca interconectar objetos con independencia de su ubicación.
- Estructura cliente-servidor, simétrica (serán uno u otro depende del modelo)

FUNCIONES BÁSICAS:

- Invocación de métodos estáticos y dinámicos
- Incluir seguridad en las com.
- Conexión con sistemas existentes (CMIP, SNMP, WBEM, ...)

COMPONENTES

- ORB → Agentes distribuidos por la red → se comunican con IDL
  → pueden dar seguridad y QoS a las com.
- IDL → Lenguaje, usa plantillas, define métodos y objetos.
- DII (Dynamic Invocation Interface)
- IR → Almacen de interfaces
- OA → Compatibiliza objetos

- Se puede integrar sobre la torre de protocolos de inet, SS7, Red Básica, ...

- PASARELAS CMIP/CORBA : permite configuración dinámica de la info del diccionario
- PROGRAMACIÓN CON JAVA :
  - Mayor portabilidad
  - Agente movil → se ejecuta de forma autónoma
    Objeto movil → se mueve por la red
  - RMI → Protocolo de invocación remota
- GESTIÓN POR DELEGACIÓN
  - Se da inteligencia a los nodos, → es mejor que sistema centralizado si #nodos↑
  - Comunicación entre agentes → intercambio info, conocimiento, cooperación.
  - Red inteligente → Aprende de las acciones
    → Resumen de la info.

* GESTIÓN DE SERVICIOS MULTIMÉDIA

Evolución:

CS1: tarificación, # universal, prefijos, ...
CS2: inet
CS3: com. moviles
CS4: QoS sobre inet (VoIP)

- H323: primer sistema de telefonía IP normalizado

Arquit < Pasarelas
Gatekeeper → Gestor controlador de red
- Funciones de seguridad: cifrado, ctrl de acceso
- Reserva de BW
- Conversión dominio IP a # telefónico.

Como dar QoS en inet:
- Servicios diferenciados → mediante prioridades
- " integrados → RSVP (reserva de recursos a nivel bucle abonado)
  MPLS (asigna prioridades, ayuda a dar QoS)
- Gestión de tráfico

Problemas VoIP → Fiabilidad, Seguridad, Soluciones propietarias incompatibles

* GESTIÓN DE REDES DE BDA ANCHA

- ATM
  - Funciona sobre red SDH
  - Tipos de tráfico → CBR (cte)
    VBR (variable)
    ABR (a ráfagas)
  - SLA especifica (QoS, tasa celdas pico, retardo tolerado, tolerancia ráfagas)

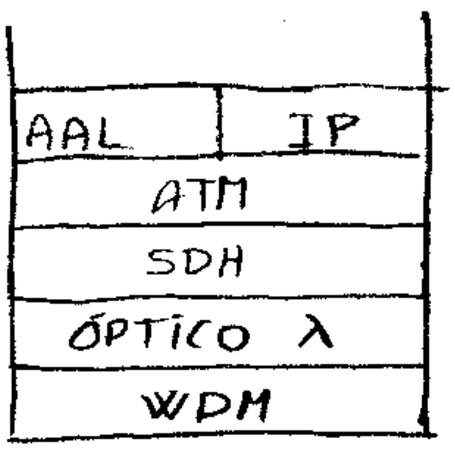
Gestión en ATM
- Ctrl de flujo → Alisado de tráfico, Leacky-Bucket, Prioridades
- Ctrl de congestión → bits EFCI/BFCI → descarte celdas
- Definición de puntos de referencia
- ILMI: interfaz de gestión entre terminales — nodos conmutación, usa SNMP

- GSMP → gestor de nodos ATM
  - Mensajes: de sincronismo, peticion-respuesta
  - Config: IP, interfaces, estadísticas, ...

* REDES ÓPTICAS

- OSMP → extensión GSMP, incluye config λ, fibras
- WDM: varios planos, uno por λ
- Las redes suelen tener extructura de anillo, con redondancia
- Redes reconfigurables → típico en redes jerarquicamente distribuidas
  - son muy rápidas
  - orientadas a circuito
- Gestión complicada, equipos caros y tecnología insuficiente
  En el nivel eléctrico se usa como en ATM → SNMP
- OSPF: protocolo encaminamiento para redes orientadas circuitos.

-Torre de protocolos

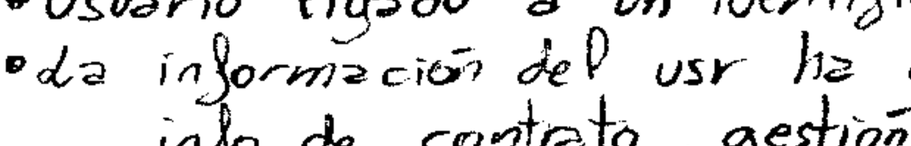


* GESTIÓN DE COM. INALÁMBRICAS

	Redes Fijas	Redes Moviles
Red de acceso	- QoS estable - Fijo, Bucle dedicado	-Qos inestable -Topologia variable
Distribución equipos	-Centralizado	-Distriburdo
Proveedor de servicios	- Fijo	-Dinámico
Seguridad	-Pocas amenazas	-Para cada llamada
Tarificación	-Simple	-Complicada, compartida

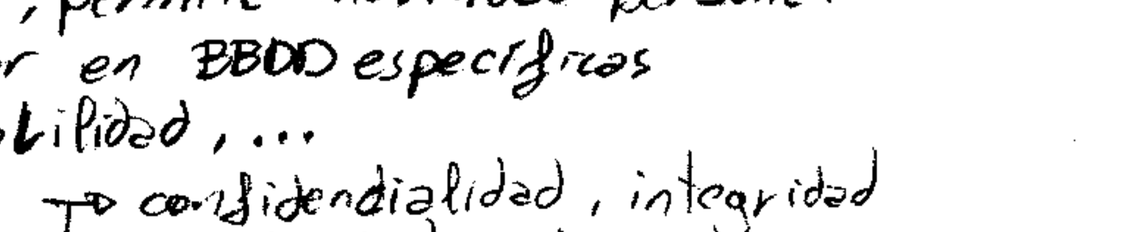
- Sistema de com. personales
  - Usuario ligado a un identificador, permite movilidad personal
  - La información del usr ha de estar en BBDD específicas
    info de contrato, gestión, movilidad, ...
  - Seguridad orientada a info en tránsito → confidencialidad, integridad
    → autenticidad, ctrl acceso
  - Arquitectura de servicios
    TR46: Orientado a terminal (estilo GSM)
    T1/P1: Orientado al usuario
  - Gestión de redes moviles → PCS: Servicios de Com. Personales
    → PCN: Red " "

GSM
- Red centralizada



BSC: Parámetros radioeléctricos
MSC: Servicios de RI
VLR, HLR: BBDD (info usr, gestión, movilidad)

UMTS
- Red jerarquicamente distribuida



- Permite cnx inet
- Gestión TMN (CMIP, CORBA)

- Mensajeria instantanea
  - Protocolos → WAP, I-MODE
  - Redes → SMS / MSS

* GESTIÓN DE REDES WIFI (802.11)

- Seguridad → RADIUS, cortafuegos IDS
- Comunicaciones de voz → requieren prioridades → SIP
  - ↳ problemas con los HO
- Gestión de tráfico: mediante HO forzados

* GESTIÓN DE REDES ACTIVAS

- Se adaptan a las necesidades del usr

ANEF (Active Network)
- Mensajes (de info, de config, de vuelta atras)
- Agentes inteligentes → recopila info, toma decisiones, aprende de sus errores.
- Gestion de tráfico proactivo → predicciones