CAPÍTULO 2: Introducción a la gestión de redes.

En este apartado, se pretende analizar un modelo genérico para la gestión de redes, como es el propuesto por la ISO (*International Organization for Standardization*). Se trata del modelo FCAPS (*Fault, Configuration, Accounting, Performance, Security*). Este modelo define los objetivos que debe cumplir un sistema de gestión de redes, para administrar a esta de forma integral. Deberá adaptarse a las necesidades del entorno real según las necesidades del mismo. Tras el análisis de este modelo, se pasará a realizar una breve descripción del protocolo más utilizado en la gestión de redes, el SNMP (*Simple Network Management Protocol*).

2.1 - MODELO FCAPS

La gestión de redes de telecomunicación se define como cualquier acción para planificar, instalar, mantener, explotar y administrar redes y servicios de telecomunicación, con el objetivo de preservar la calidad del servicio y maximizar su rendimiento.

La gestión de una red de comunicaciones según el modelo OSI, puede descomponerse en cinco áreas funcionales [1]:

- Gestión de Fallos (Fault).
- Gestión de la Configuración (Configuration).
- Gestión de la Contabilidad (Accounting).
- Gestión de las Prestaciones (Performance).
- Gestión de la Seguridad (Security).

A continuación, se pasan a explicar cada una de ellas.

2.1.1 - GESTIÓN DE FALLOS

La gestión de fallos es un conjunto de funciones que permiten detectar, aislar y corregir un funcionamiento anormal de la red de telecomunicaciones y de su entorno, con el objetivo de conseguir que siempre esté disponible. En esta definición, el fallo se refiere a toda desviación del conjunto de objetivos operacionales, servicios o funciones del sistema.

La finalidad de las funciones de esta gestión será conseguir los siguientes objetivos:

• Garantía de la calidad de RAS (*reliability, availability and survivability*). El RAS reúne a tres componentes importantes, cuya evaluación es indispensable para la protección de la calidad del servicio. Se trata de la fiabilidad, la disponibilidad y la supervivencia. Se definen de la forma siguiente:

- La fiabilidad puede definirse como la probabilidad de que un sistema se mantenga operativo durante un determinado periodo de tiempo, bajo condiciones ambientales normales. Esta función difiere de la disponibilidad en que la primera sólo implica el fallo del sistema, mientras que la disponibilidad afecta al fallo y a la capacidad de recuperación.

- La disponibilidad es el porcentaje de tiempo que un sistema se encuentra disponible para realizar sus funciones correctamente. Puede medirse con respecto a la plataforma o con respecto a la disponibilidad de un servicio en relación con un cliente.

- La supervivencia mide la facilidad y la eficacia en el mantenimiento y reparación del producto. No existe una sola métrica exacta y bien definida, ya que esta función puede incluir tanto el tiempo medio de reparación como la capacidad de diagnóstico.

Estas medidas permitirán llevar a cabo una política de mantenimiento y sustitución de los distintos componentes, antes de que alguno pueda fallar. Es lo que se conoce como política proactiva, que conseguirá adelantarse a los posibles fallos y evitarlos.

• Vigilancia de alarmas. El sistema de gestión de red debe ofrecer la posibilidad de supervisar los fallos, casi en tiempo real. Para conseguirlo, realizará la monitorización de la red y el estado de la misma. Deberá ser capaz de crear, configurar y recoger las distintas alarmas de cada dispositivo. Antes de todo, se deberán elegir las características de la red que puedan inducir posibles fallos. Este paso es complicado y sin duda, se irán añadiendo alarmas a medida que se vayan dando nuevos errores.

• Localización de averías. Cuando ocurra una avería, deberá localizarse la zona a la que afecta y aislarla para que la red continúe funcionando. Una vez aislada, se diagnosticarán las posibles causas y se crearán las alarmas correspondientes para detectarla cuando se vuelvan a producir factores similares.

• Reparación de averías. Tras el diagnóstico, se irán realizando las reparaciones necesarias. En algunos casos, la avería puede ser muy leve y el propio sistema de gestión podrá solucionarlo con la ejecución de órdenes remotamente en la máquina fallida.

• Administración de anomalías. La anomalías se detectarán de los datos recogidos y de los informes creados por los propios clientes. Es preferible, por imagen de la empresa, que se intente evitar este segundo tipo. Se deben clasificar, resolver y dejar almacenadas las soluciones por si se vuelven a producir las mismas circunstancias.

Un ejemplo de modelo que recoge estas funcionalidades sería el de *trouble ticket system* (Sistema de partes de avería) representado en la figura 2.1.

La mayor dificultad de la gestión de fallos es sin duda el diagnóstico de errores.

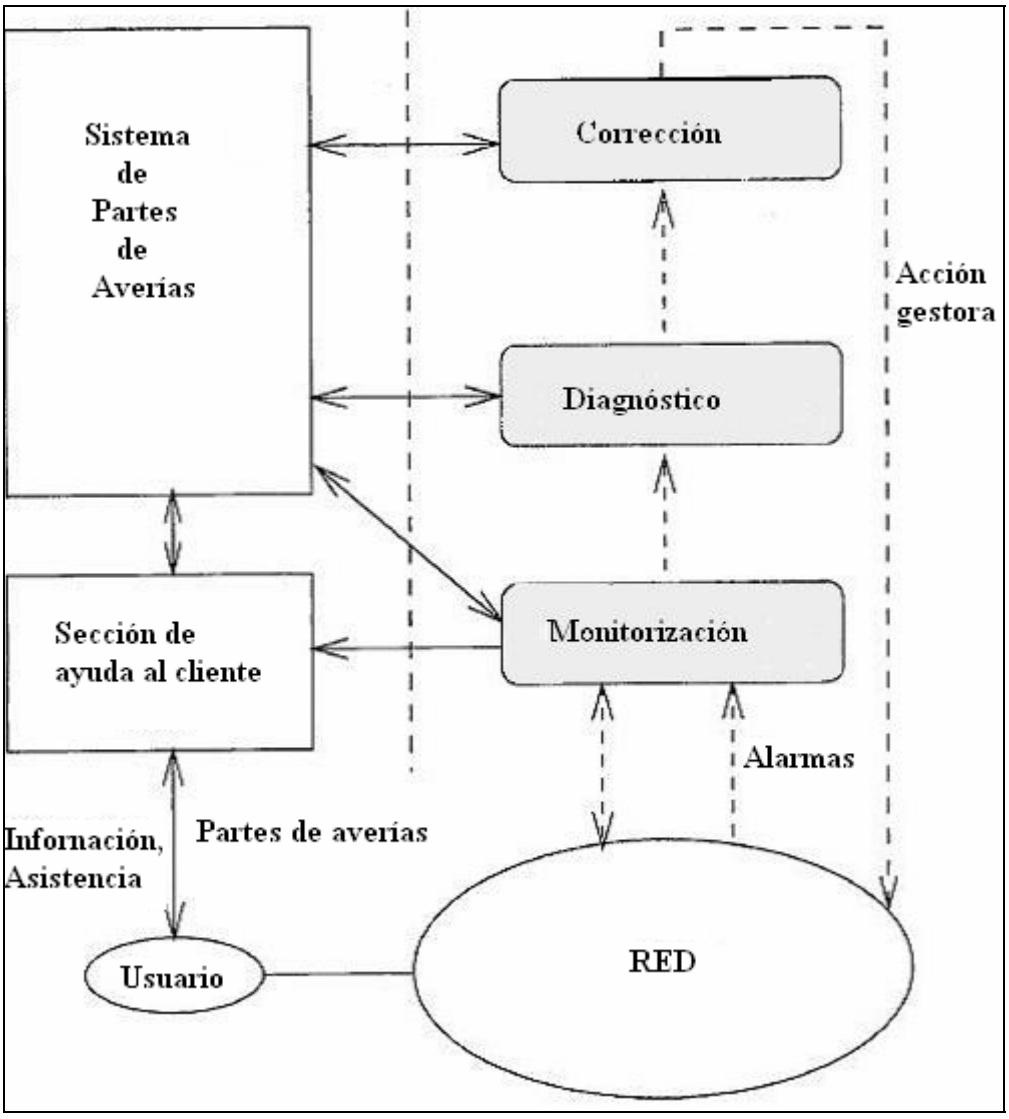

Figura 2.1 - Sistema *trouble ticket system.*

Existen numerosos recursos técnicos que hacen posible este tipo de gestión. Algunos de estos son:

- Auto-identificación de los componentes del sistema.
- Prueba aislada de componentes.

- Traza de mensajes.
- Log de errores.
- Mapas de red.
- Mensajes de prueba de vida para todos los niveles: ping y echo.
- Recuperación de "*cores*".
- Generación de errores de prueba.
- Rutinas de autotest y pruebas de transmisión BER, traceroute, ping.
- Disparos de reset planificados y reinicialización de puertos, grupos de puertos y componentes.
- Equipos de medida y prueba.
- Soporte para mecanismos de filtrado de fallos.
- Gestión de fallo desde la asistencia al usuario.

2.1.2 - GESTIÓN DE LA CONFIGURACIÓN

La gestión de la configuración proporciona las funciones con las que ejercer el control sobre los elementos de la red, identificarlos, recoger datos de los mismos y suministrar información a estos.

La gestión de la configuración comprende a los grupos de funciones que deben encargarse de las siguientes tareas:

- Planificación de la red. Se encargará de determinar si existe la necesidad de aumentar la capacidad de la red y de introducir nuevas tecnologías.
- Instalación. El sistema de gestión de red puede soportar la instalación de los equipos de la red de telecomunicación. Esa capacidad de soporte incluye la de ampliación o reducción de un sistema. Otra tarea que podría realizar, sería la instalación de programas dentro de elementos de red desde los sistemas de base de datos. Además, se pueden intercambiar datos administrativos entre los elementos de red y el sistema.
- Planificación y negociación de servicios. Esta función se refiere a la planificación de la introducción de servicios y los contactos con los clientes para establecer nuevos, cambiar características de servicios y desconectar servicios.
- Provisión. La provisión consiste en el conjunto de procedimientos necesarios para poner en servicio un equipo, sin contar la instalación. El estado de la unidad, por

ejemplo, en servicio, fuera de servicio, en reserva activa o reservado, y determinados parámetros pueden controlarse también mediante funciones de provisión.

- Situación y control. El sistema debe proporcionar la capacidad de supervisar y controlar determinados aspectos de los elementos de la red: comprobación o cambio de estado de servicio, iniciación de pruebas de diagnóstico, etc.

Las funciones de situación y control pueden también formar parte del mantenimiento de rutina, cuando se ejecutan de manera automática o con una planificación periódica. Un ejemplo al respecto es la puesta fuera de servicio de un canal para efectuar pruebas de diagnóstico rutinarias.

El sistema de gestión de red hará que se retire de funcionamiento un equipo averiado y, en consecuencia, podrá reconfigurar los equipos o reencaminar el tráfico. Además puede permitir la introducción de una configuración propuesta para analizar automáticamente su viabilidad antes de implementarla.

Podemos incluir como recursos técnicos a los siguientes:

- Auto-topología y auto-descubrimiento.
- Documentación de la descripción de la configuración.
- Mapas de la red con datos de configuración.
- Herramientas para activar backup en caso de fallo.
- Herramientas para poner y recuperar parámetros y estado sistema.
- Herramientas de distribución de software y control de licencias.
- Herramientas de supervisión y control de autorización.

2.1.3 - GESTIÓN DE LA CONTABILIDAD

La gestión de la contabilidad permite la medición del uso de los servicios de red, la determinación del coste que representa para el proveedor de servicios y la cantidad que se ha de cobrar al cliente por el mencionado uso. Permite también la determinación de los precios de los servicios.

El grupo gestión de la contabilidad comprende las siguientes funciones:

- Medición de la utilización. Un sistema de operaciones interno puede recoger datos de los dispositivos, que sirven para determinar los importes que deben cargarse a las cuentas de los clientes.

- Tarificación o fijación de precios. Una tarifa es un conjunto de datos de un elemento de red, utilizados para determinar el importe del pago por los servicios utilizados. La clase de tarifa será definida en función del servicio, del origen y destino, del periodo de tarificación y de la categoría del día. Estos atributos pueden cambiar durante la comunicación.

- **C**obros y finanzas. Se encarga de la transferencia de datos financieros para la gestión de red, a efectos tales como los de administración de cuentas de clientes e información a los clientes sobre saldos, fechas de pago y recepción de pagos.

- **C**ontrol de la empresa. Estas funciones de gestión soportan el flujo de datos necesarios para actuar con diligencia sobre el flujo de fondos apropiado dentro de la empresa y entre la empresa y sus propietarios y acreedores. Este grupo soporta las responsabilidades fiduciarias de los directivos de la empresa.

Con el fin de conseguir dichos propósitos, se pueden realizar en esta gestión las siguientes tareas:

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

2.1.4 - GESTIÓN DE LAS PRESTACIONES

La principal diferencia entre este tipo de gestión con la de fallos, es que esta última pretende que la red funcione bien en el presente, mientras que el objetivo de la primera es garantizar la calidad de la misma en el futuro.

La gestión de prestaciones proporciona funciones destinadas a evaluar e informar sobre el comportamiento de los equipos de telecomunicación y de los elementos de red y la efectividad de la misma. Su cometido consiste en reunir y analizar datos estadísticos, para supervisar y corregir el comportamiento y la efectividad de la red, del elemento o equipo de red y facilitar la planificación, la provisión, el mantenimiento y la medición de la calidad.

El sistema de gestión recoge datos sobre la calidad de servicio (QOS, *quality of service*) de los elementos de red y contribuye a las mejoras de la misma. Para ello, se pedirán informes de datos de QOS a los distintos elementos, o bien se enviarán informes automáticamente con arreglo a un plan en casos de excepción. En cualquier momento, se puede modificar el plan y/o los umbrales vigentes. Los informes de los elementos de red sobre los datos referidos a la QOS, pueden consistir en datos en bruto (datos recogidos durante la prestación de los servicios de telecomunicación) que luego se analizan, o bien en datos analizados por el propio dispositivo.

La calidad del servicio incluye la supervisión y el registro de parámetros relacionados con:

- El establecimiento de la conexión. Por ejemplo, demoras en el establecimiento de la comunicación o peticiones de llamada logradas y fallidas.
- La retención de la conexión.
- La calidad de la conexión.
- La integridad de la facturación.
- El mantenimiento y el examen de ficheros cronológicos del estado de los sistemas.
- La cooperación con la gestión de fallos, a fin de establecer posibles averías de un recurso, o con la gestión de la configuración, para cambiar los parámetros/límites de encaminamiento y de control de carga de enlaces, etc.
- La iniciación de llamadas de prueba para supervisar los parámetros de QOS.

La gestión de prestaciones debe encargarse de las siguientes funciones:

- Garantizar la calidad de funcionamiento. Soporta procesos de decisión que establecen, conforme progresa la ciencia y varían las necesidades del usuario, las medidas de calidad apropiadas para este área de gestión.
- Supervisar la calidad de funcionamiento. Su función básica consiste en seguir la pista a las actividades del sistema, la red o el servicio para reunir los datos apropiados, que determinen la calidad de funcionamiento. Esto implica la continua recogida de datos, referentes a este aspecto, de los elementos de red. Se utilizarán métodos de vigilancia de alarmas para detectar las averías graves y se medirá la calidad global para determinar la del funcionamiento total. Estas funciones permitirán detectar cuellos de botella o desbordamientos de umbrales.

- Controlar la gestión de calidad de funcionamiento. Soporta la transferencia de información para controlar el funcionamiento de la red. En lo que respecta a la gestión del tráfico de la red, esto incluye la aplicación de controles de tráfico que repercuten en el encaminamiento del mismo y el procesamiento de las llamadas. En lo que concierne a la supervisión de la calidad de funcionamiento del transporte, este grupo se encarga de la recogida de datos referentes a la calidad de funcionamiento, de la definición de algoritmos para el análisis de estos y de la fijación de umbrales, pero no tiene ningún efecto directo en la red gestionada.

- Análisis de la calidad de funcionamiento. Estos datos podrían requerir un tratamiento adicional para evaluar el nivel de calidad de funcionamiento de la entidad. Se analizarán las tendencias de la red para la prevención de fallos.

En este tipo de gestión se utilizarán herramientas como los *log* históricos, modelos estadísticos de la predicción de prestaciones o distintas simulaciones.

2.1.5 - GESTIÓN DE LA SEGURIDAD

Todas las áreas funcionales de gestión y todas las transacciones de la red necesitan este tipo de gestión. La funcionalidad esta gestión [2] comprende los servicios de seguridad de las comunicaciones y la detección y notificación de eventos de este tipo:

Los servicios de seguridad de las comunicaciones son los referidos a la autenticación, el control de acceso, la confidencialidad e integridad de los datos, que pueden prestarse en el curso de cualquier comunicación entre sistemas, clientes y sistemas o usuarios internos y sistemas. Se define además, un conjunto de mecanismos penetrantes de seguridad que son aplicables a cualquier comunicación, como por ejemplo, la detección de eventos, la gestión de pistas de verificación de seguridad o la recuperación de la seguridad.

Mediante la detección y notificación de eventos se comunica a las capas superiores de seguridad, cualquier actividad que pudiera ser interpretada como una violación de la misma. Entrarían en este grupo, por ejemplo, la actuación de un usuario no autorizado o la manipulación indebida de un equipo.

La gestión de la seguridad comprende los siguientes grupos de conjuntos de funciones:

- De prevención. Se necesitan para evitar una intrusión.

- De detección. Son los que detectan intrusiones.

- De contenencia y recuperación. Son las funciones que se utilizan para denegar el acceso a un intruso, reparar los daños causados por un intruso y recuperar las pérdidas.

- De administración de la seguridad. Son aquellos que se necesitan para planificar y administrar la política de seguridad y gestionar la información relacionada con la seguridad.

Podemos citar algunas herramientas de sotfware libre que se utilizan para este tipo de gestión, como son:

- GPGP y PGP.
- SATAN (System Administrator's Tool for Analyzing Networks),
- SAINT (Security Administrator's Integrated Network Tool).
- SARA (Security Auditor's Research Assistant)
- Tripwire (integridad de ficheros)

El problema es encontrar la manera de adecuar estos procedimientos en la arquitectura de gestión y controlarlos de manera uniforme en un marco de la política de seguridad.

2.2 - PROTOCOLO SNMP

El Comité Asesor de Internet, IAB (*Internet Advisory Board*), ha adoptado varias normas para la administración de la red. En su mayoría, estas se han diseñado para ajustarse a los requisitos de TCP/IP, aunque cuando es posible cumplen con la arquitectura OSI. Para cubrir dichas necesidades se han creado varios protocolos con funcionalidades parecidas, pero sin duda el más utilizado hoy en día gracias a su simplicidad, es SNMP [3] y por eso se va a realizar un breve estudio sobre este.

SNMP es un protocolo de nivel de aplicación que permite realizar la gestión remota de dispositivos. Su predecesor, SGMP (*Simple Gateway Management Protocol*) fue diseñado para administrar sólo *routers*, pero SNMP puede gestionar prácticamente cualquier dispositivo, utilizando para ello comandos para obtener y modificar la información.

Este protocolo fue definido por la IETF que publicó una serie de RFC según el progreso de este [4]:

- SNMPv1: RFC1157.
- SNMPv2p: RFC1441 y RFC1452.
- SNMPv2c: RFC3416, RFC3417 y RFC3418.
- SNMPv3: RFC3410, RFC3411, RFC3412, RFC3413, RFC3414, RFC3415, RFC3416, RFC3417, RFC3418 y RFC2576.

2.2.1 - VERSIONES DEL PROTOCOLO SNMP

La primera versión de SNMP es la más antigua y básica. Su principal limitación es que la seguridad se basa en comunidades, que son simplemente contraseñas sin ningún tipo de encriptación. Esto se trató de resolver proporcionando una seguridad más fuerte en la versión 2p de este protocolo, SNMPv2p, pero este esquema bastante más complicado de implementar, no fue adoptado por muchos fabricantes. Esta versión además, añadía funciones para aumentar la eficiencia cuando se trabajaba con grandes cantidades de datos. Rescatando esta ventaja y volviendo a la autenticación basada en comunidades, se introdujo la versión 2c. Existen además otras dos versiones de SNMP, la SNMPv2* y la SNMPv2u, pero no han sido muy difundidas. En general, cuando se habla de SNMPv2 se hace referencia a la SNMPv2c.

Actualmente, la versión 3 (SNMPv3) es reconocida como el estándar de la IETF desde el 2004. Su principal característica es la seguridad, por lo cual este protocolo está diseñado para proveer autenticación, privacidad, autorización y control de acceso.

Existen dos aspectos a resaltar en lo concerniente a estas versiones. El primero es que todas pueden ser soportadas de manera simultánea y el segundo, es que si bien la RFC1157 que describe el SNMPv1 está ya archivada como histórica, es la más utilizada actualmente a pesar de las carencias de seguridad mencionadas.

2.2.2 - ARQUITECTURA SNMP.

Por la forma en la que el protocolo está implementado, se distinguen dos entidades:

2.2.2.1 - Agentes

Son componentes lógicos o físicos que manejan la información que puede ser gestionada de los elementos de red e interactúan con los sistemas gestores. Esta información puede reflejar el estado de los elementos, su configuración y, en general, las características de funcionamiento del dispositivo de red en concreto. El grado de gestión permitido dependerá de la mayor o menor funcionalidad que haya añadido el fabricante en su diseño. El propósito principal de estas funciones en los agentes es responder a las operaciones invocadas por los gestores, en relación con la información que manejan. En definitiva, los agentes no son más que procesos que se ejecutan en los dispositivos a gestionar y que van actualizando y manteniendo los valores de una variable que describe una determinada característica del equipo.

2.2.2.2 - Gestores -

Son estaciones administradoras que interactúan con los operadores humanos y permiten a estos realizar las operaciones de gestión sobre los elementos de red, a través de los agentes. Los gestores pueden realizar un seguimiento del elemento de red y un control de su comportamiento mediante la consulta y modificación de la información de gestión, que viene definida de fábrica en el dispositivo.

Las comunicaciones entre gestor y agente son de naturaleza cliente-servidor, donde el servidor es el agente y el cliente el gestor. Este modo de funcionamiento es pasivo, pero también puede ser activo. Este segundo se produce cuando el agente, por iniciativa propia, notifica al gestor de ciertas situaciones o eventos críticos. Estas notificaciones son conocidas como *traps*.

Cabe resaltar que los elementos a gestionar pueden encontrarse en la misma LAN, en la WAN o en otras LAN a las que el gestor tenga acceso. Incluso dentro de la máquina que contiene al gestor, puede instalarse un agente para monitorizar sus características.

Por último, resaltar que la topología puede ser centralizada o distribuida según las necesidades de la red a gestionar.

2.2.3 - TIPOS DE MENSAJES

Entre el gestor y los agentes se intercambian varios tipos de mensajes agrupados en tres conjuntos principales:

- Los mensajes de petición de información que se utilizan en el *pooling* o sondeo realizado entre gestor y agente de manera periódica. Estas solicitudes se realizan mediante las primitivas de petición que se explican a continuación:
  - GET REQUEST: Solicita el valor de una variable del agente.
  - GET NEXT REQUEST: Solicita el valor de la siguiente variable.
  - GET BULK REQUEST: Presente en SNMPv2, solicita un amplio conjunto de valores en una sola petición.
- Los mensajes de modificación de información:
  - SET REQUEST: Escribe un dato en una variable del agente.
  - SET NEXT REQUEST: Escribe un valor en la siguiente variable.

El agente contesta a todos estos mensajes, tanto de petición como de modificación con la primitiva "GET RESPONSE".

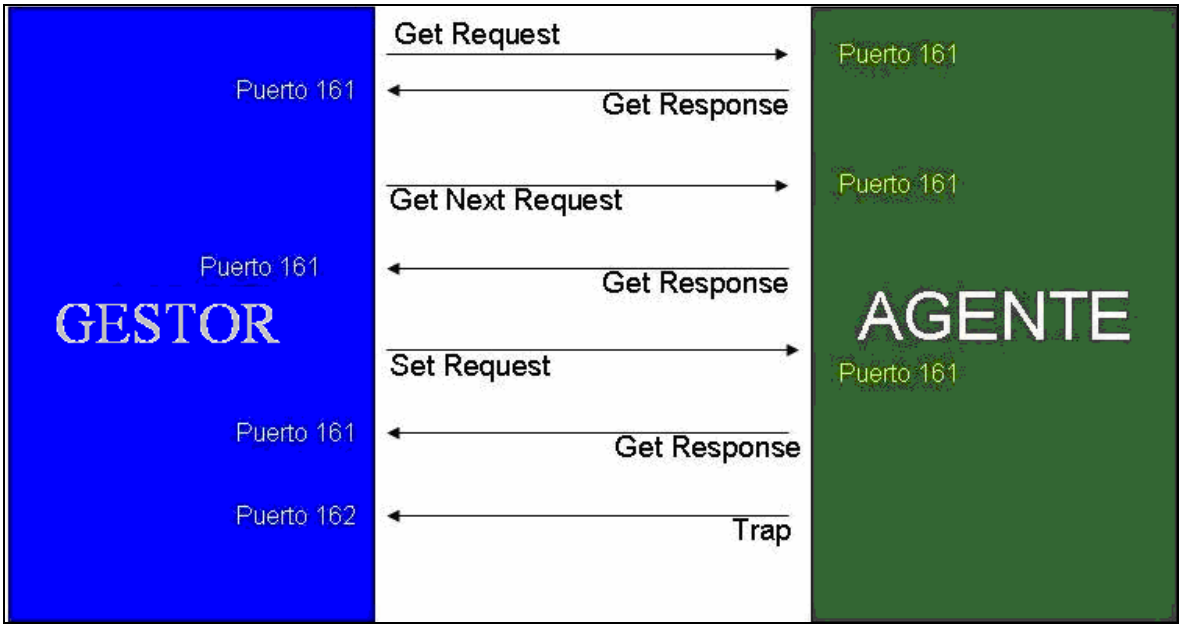

Figura 2.2 - Intercambio de PDU entre gestor y agente.

– Notificación de eventos. En este grupo se distinguen en primer lugar los *traps*, que como se comentó anteriormente, se corresponden con mensajes no confirmados que puede mandar el agente en el caso de que ocurra una situación crítica, como podría ser, la desconexión de una interfaz en un *router*. Y por otro lado, existe un servicio de notificación confirmado entre gestores, que utiliza la primitiva "INFORM". Este sólo permite informar sobre situaciones muy concretas y preprogramadas.

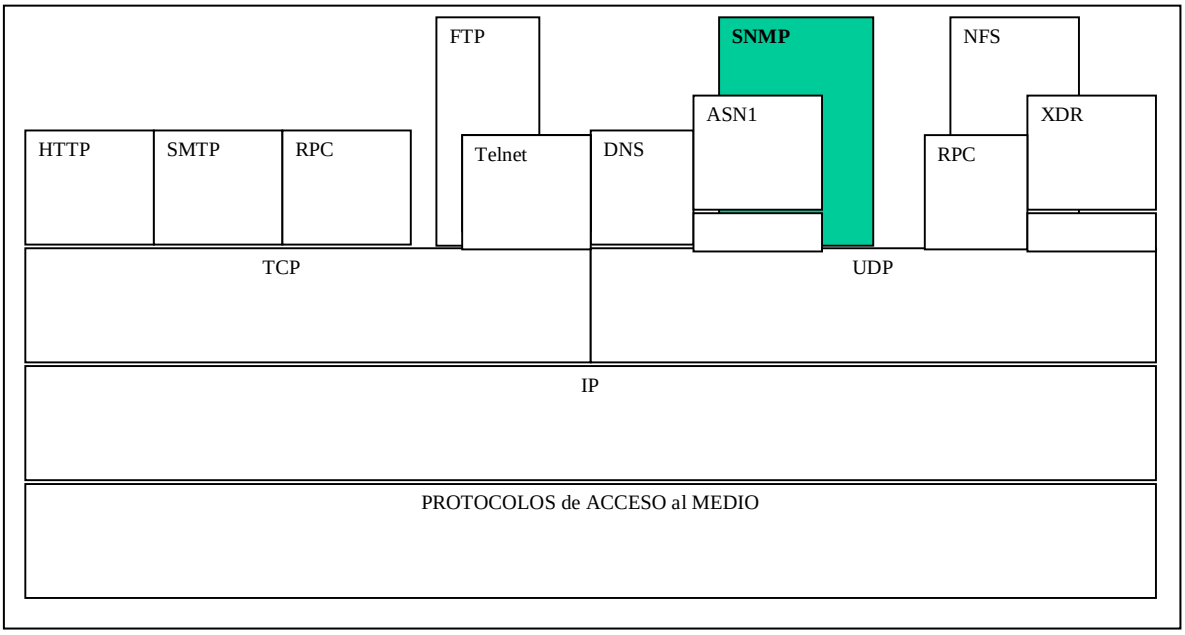

Figura 2.3 - Pila de protocolos.

Un aspecto a considerar es que si bien el *pooling* es usualmente periódico, al igual que el *trap* es de naturaleza asíncrona, ya que no tiene un tiempo determinado de inicio. Por tanto, el agente debe estar preparado para responder peticiones o generar *traps* en cualquier momento.

Se puede observar un ejemplo de intercambio de PDU en la figura 2.2.

El protocolo SNMP corresponde a la capa de aplicación del modelo de referencia OSI. La pila de protocolos de TCP/IP puede visualizarse en la figura 2.3. Los datagramas correspondientes a este protocolo viajan sobre UDP, utilizando normalmente el puerto 161 para mensajes y el 162 para *traps*. El utilizar UDP implica que no se establece una sesión entre el gestor y los agentes, lo cual hace que las transmisiones sean más rápidas y que la red no se sobrecargue, pero también implica que el que envía los mensajes debe, por algún medio, asegurar que este ha sido recibido. En el caso del sondeo el gestor puede esperar un tiempo por la respuesta y, en caso de que no se reciba, se puede reenviar el paquete. El problema se da en el caso de los *traps*, ya que el agente no espera ninguna respuesta del gestor y por ello, el trap puede perderse sin que ninguno de los equipos lo perciba.

2.2.4 - ASN.1

ASN.1 (*Abstract Syntax Notation One*) es un estándar de la ISO y la ITU-T para describir los mensajes intercambiados entre las aplicaciones. Provee un conjunto de reglas para describir la estructura de los objetos. SNMP utiliza un subconjunto de las reglas definidas por este estándar, para la representación y transmisión de los datos.

2.2.5 - SMI

La SMI (*Structure of Management Information*) define los nombres y tipos de datos de las variables que se pueden gestionar. Se distinguen por tres características:

- El OID (Object Identifier) que las define de manera unívoca.
- Tipo y sintaxis: Para esto se utiliza ASN.1, que se convierte en la sintaxis universal para conseguir la comunicación entre sistemas diferentes.
- Codificación: Existen una serie de reglas para codificar y decodificar la información transferida en una cadena de octetos.

2.2.6 - MIB

La MIB (*Management Information Base*) es la colección de variables administrables definidas utilizando la SMI. Para estas se sigue una estructura jerárquica en forma de árbol.

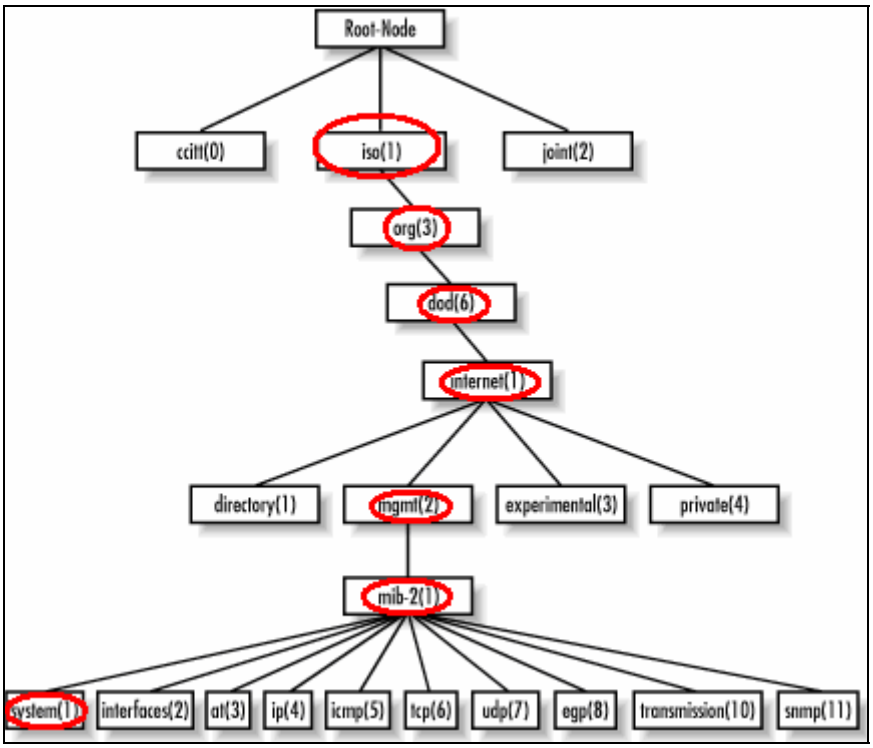

Figura 2.4 - Estructura jerárquica de la MIB-II.

En la Figura 2.4, se muestra la estructura de la MIB-2, su posición dentro del árbol y las variables administrables dentro de esta. La jerarquía se inicia en la raíz que se divide en tres ramas, la administrada por la ITU-T, la de la ISO y la tercera para las variables que se administran de forma conjunta.

Dentro de la rama de la ISO, la tercera subdivisión corresponde a organizaciones. Por ejemplo, Internet nace por un proyecto del departamento de defensa de los Estados Unidos y por ello, su OID se encuentra dentro de DOD (*Department of Defense*). Debajo del subárbol Internet, existen ramas relacionadas con la administración de redes y SNMP. Estos subárboles son administrados por la IANA.

Son de especial interés los nodos "mgmt.mib-2" y "private.enterprises". En el primero se define la MIB estándar de Internet y el segundo es utilizado por las empresas para que puedan registrar OID particulares, utilizados en soluciones propias de hardware o software.

2.2.7 - OID (OBJECT IDENTIFIER)

Un OID es la dirección de una variable o nodo dentro de la estructura de la MIB. Está constituida por números enteros positivos separados por puntos que indican la ruta jerárquica que ocupa la variable. Para entenderlo mejor, puede observarse la figura 2.4. Para conseguir el OID de *system*, deben recorrerse las ramas de la MIB desde el principio hasta el lugar donde se encuentra este nodo, de arriba a abajo y de izquierda a derecha. Por cada nivel se irá añadiendo el número del nodo que se recorra para llegar al destino y se separará de los demás por un punto. El nodo raíz no está enumerado y para expresarlo, sólo se pondrá un punto al iniciar el OID. Para llegar al nodo *system*, se recorre "nodo raíz->iso -> identified organization->dod->internet->mgmt->mib-2->system". Por tanto, el OID de *system* será ".1.3.6.1.2.1.1".

Para finalizar el capítulo, se añade a continuación un ejemplo de funcionamiento de este protocolo que es el mostrado en la figura 2.5. Cabe resaltar que tanto agente como gestor disponen de MIB comunes para conocer a través del OID, las variables expresadas en las peticiones y respuestas. Comentar también, que el gestor a veces dispone de una base de datos externa donde almacena todos los valores recogidos con el propósito de realizar estudios de la red actual y mejorarla.

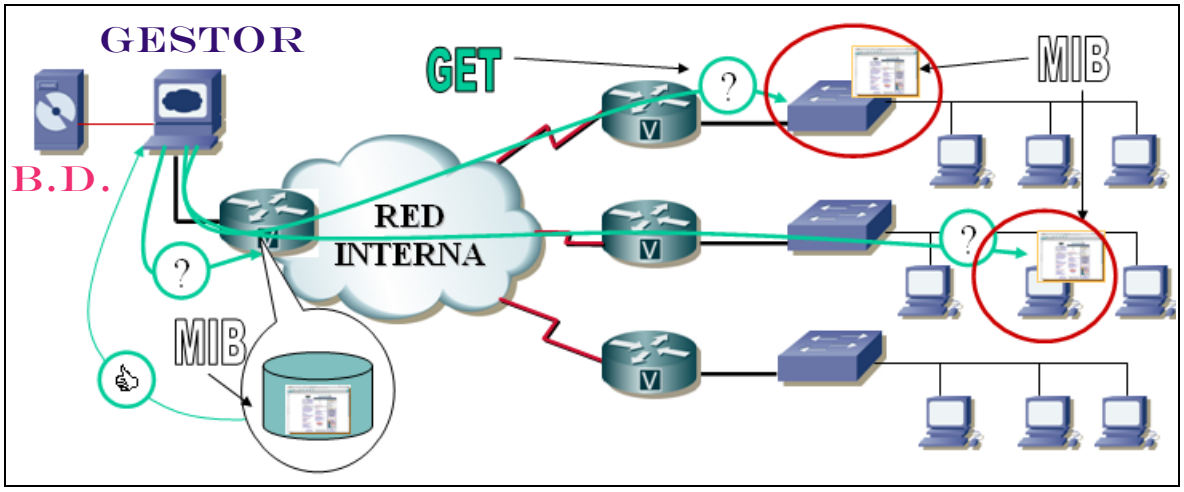

Figura 2.5 - Funcionamiento de SNMP.