



UNIVERSIDAD
DE MÁLAGA

ESCUELA TÉCNICA SUPERIOR
DE INGENIERÍA INFORMÁTICA

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA
INGENIERO EN INFORMÁTICA

DISEÑO DE UN SISTEMA DE MONITORIZACIÓN DE REDES DE BANDA ANCHA

Realizado por
ADOLFO CARLOS ARIZA RUZ

Dirigido por
FRANCISCO JAVIER GONZÁLEZ CAÑETE
JAVIER LOPEZ MUÑOZ

Departamento
Tecnología Electrónica
Lenguajes y ciencias de la computación

UNIVERSIDAD DE MÁLAGA

MÁLAGA, Octubre 2008



UNIVERSIDAD
DE MÁLAGA

ESCUELA TÉCNICA SUPERIOR
DE INGENIERÍA INFORMÁTICA

UNIVERSIDAD DE MÁLAGA
ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA
INGENIERO EN INFORMÁTICA

Reunido el tribunal examinador en el día de la fecha, constituido por:

Presidente/a Dº/Dª. _____

Secretario/a Dº/Dª. _____

Vocal Dº/Dª. _____

para juzgar el proyecto Fin de Carrera titulado:

DISEÑO DE UN SISTEMA DE MONITORIZACIÓN DE REDES DE BANDA
ANCHA _____

del alumno/a Dº/Dª. ADOLFO CARLOS ARIZA RUZ _____

dirigido por Dº/Dª. FRANCISCO JAVIER GONZÁLEZ CAÑETE _____

ACORDÓ POR _____ OTORGAR LA CALIFICACIÓN
DE _____

Y PARA QUE CONSTE, SE EXTIENDE FIRMADA POR LOS COMPARECIENTES
DEL TRIBUNAL, LA PRESENTE DILIGENCIA.

Málaga, a _____ de _____ del 200_

El/La Presidente/a

El/La Secretario/a

El/La Vocal

Fdo:

Fdo:

Fdo:

ÍNDICE

Capítulo 1 : Introducción.....	1
Capítulo 2 : Escenario	5
2.1 Servicios	5
2.2 Topología.....	6
2.2.1 Elementos de una Red VoIP	8
Capítulo 3 : Tecnología a utilizar	15
3.1 Componentes básicos de SNMP	15
3.2 Comandos básicos de SNMP	16
3.3 Base de información de administración SNMP (MIB)	16
3.4 Notación de sintaxis abstracta 1 o ASN.1	18
3.5 Mensajes SNMP.....	18
3.6 GetRequest.....	20
3.7 GetNextRequest	20
3.8 SetRequest	20
3.9 GetResponse	20
3.10 Trap.....	21
3.11 GetBulkRequest	21
3.12 InformRequest.....	22
Capítulo 4 Gestión de fallos	23
4.1 Capa de recolección.....	24
4.2 Capa de consolidación.....	29
Capítulo 5 Gestión de rendimiento	33
5.1 Indicadores clave de rendimiento o <i>KPIs</i>	36
5.1.1 Indicadores de estado de los equipos.....	36
5.1.2 Disponibilidad	38
5.1.3 Retardo de Tránsito	39
5.1.4 Pérdida de paquetes	40
5.2 Indicadores clave de calidad	41
5.2.1 Disponibilidad del Core	41
5.2.2 Disponibilidad del Backbone	44
5.2.3 Disponibilidad Transporte	47
5.2.4 Disponibilidad Acceso.....	51
5.3 Provisión del sistema de gestión de rendimiento	55
Capítulo 6 Interfaz de usuario unificada	61
6.1 Grupos de usuarios del sistema	62
6.1.1 Administradores	62
6.1.2 Provisionadores	63
6.1.3 Operadores de red.....	64
6.1.4 Usuarios de informes	67
Capítulo 7 Conclusiones	71

ÍNDICE DE FIGURAS

Figura.1 El modelo FCAPS.....	3
Figura 2.1 Topología de los <i>backbones</i>	6
Figura 2.2 Arquitectura lógica del <i>core</i>	9
Figura 2.3 Topología del <i>core</i>	11
Figura 2.4 Arquitectura lógica de los <i>Backbones</i>	12
Figura 2.5 Arquitectura de un <i>Backbone</i>	13
Figura 2.6 Arquitectura completa de la red.....	14
Figura 3.1 Jerarquía MIB	17
Figura 3.2 Tramas SNMP.....	19
Figura 3.3 SNMP PDU	19
Figura 3.4 SNMP PDU para traps	21
Figura 4.1 Arquitectura del sistema de gestión de fallos	23
Figura 4.2 Visión topológica de la red.....	26
Figura 4.3 Visión de servicios dentro del sistema de gestión de fallos	28
Figura 4.4 Visión Flujo de integración entre la gestión de fallos y la gestión incidencias	32
Figura 5.1 Arquitectura del sistema de gestión de rendimiento	35
Figura 5.2 Sistema de gestión de rendimiento con <i>router</i> de sondas	36
Figura 5.3 Monitorización de la disponibilidad del <i>core</i>	42
Figura 5.4 Modelo de objetos de disponibilidad del <i>core</i>	43
Figura 5.5 Modelo de indicadores de disponibilidad del <i>core</i>	43
Figura 5.6 Monitorización de la disponibilidad del <i>Backbone</i>	44
Figura 5.7 Modelo de objetos de disponibilidad del <i>Backbone</i>	45
Figura 5.8 Modelo de indicadores de disponibilidad del <i>Backbone</i>	46
Figura 5.9 Monitorización de la disponibilidad de Transporte	47
Figura 5.10 Elementos a monitorización en la disponibilidad de Transporte.....	48
Figura 5.11 Modelo de instancias de la disponibilidad de transporte de la EB 02.....	49
Figura 5.12 Dependencias entre los indicadores para el cálculo de la disponibilidad de transporte.....	49
Figura 5.13 Ejemplo de red de acceso	52
Figura 5.14 Detalle del método para medir la disponibilidad de acceso	52
Figura 5.15 Elementos a monitorizar para medir la disponibilidad de acceso.....	53
Figura 5.16 Ejemplo de modelo de instancias para la Disponibilidad de Acceso.....	54
Figura 5.17 Dependencias entre los indicadores para el cálculo de la disponibilidad de acceso	54
Figura 5.18 Modelo de instancias de clase sonda (SAA-RTT)	56
Figura 5.19 Modelo de instancias de clase grupo sondas (SAA-GROUP).....	57
Figura 5.20 Modelo de instancias de clase grupo de grupos de sondas (SAA-GLOBAL).....	58
Figura 5.21 Modelo de instancias de clase grupo Sector	58
Figura 6.1 Arquitectura con interfaz unificada.....	61
Figura 6.2 Consola única de fallos.....	64
Figura 6.3 Vistas para operadores de red	65
Figura 6.4 Acceso a la interfaz SNMP de un elemento desde una alarma.....	65
Figura 6.5 Acceso al sistema de rendimiento desde la consola de alarmas	66
Figura 6.6 Vista de nivel del servicio	67
Figura 6.7 Informes para usuarios de planificación.....	68
Figura 6.8 Cuadro de mandos.....	69
Figura 6.9 Informes para clientes	70

ÍNDICE DE TABLAS

Tabla 3.1 Puertos SNMP.....	19
Tabla 5.1 Disponibilidad del core.....	42
Tabla 5.2 Indicador de Disponibilidad SAA.....	43
Tabla 5.3 Indicador de Disponibilidad del GrupoSAA.....	44
Tabla 5.4 Disponibilidad del nodo NODO-01	45
Tabla 5.5 Disponibilidad SAA	46
Tabla 5.6 Disponibilidad Nodal.....	46
Tabla 5.7 Disponibilidad del <i>Backbone</i>	47
Tabla 5.8 Disponibilidad de transporte de la EB.....	48
Tabla 5.9 Propiedad que identifica la profundidad dentro del camino	50
Tabla 5.10 Propiedad que identifica la longitud del camino hasta la EB	50
Tabla 5.11 Disponibilidad del camino hasta la EB.....	50
Tabla 5.12 Disponibilidad de la propia EB	51
Tabla 5.12 Disponibilidad Nodal.....	51
Tabla 5.13 Disponibilidad de Transporte.....	51
Tabla 5.14 Valores de la disponibilidad de acceso.....	54
Tabla 5.15 Detalles de la disponibilidad de un sector	55
Tabla 5.16 Detalles de la disponibilidad de acceso	55
Tabla 5.17 Detalles de la entidad ROUTER	56
Tabla 5.18 Detalles de la entidad Estación Base	56
Tabla 5.19 Detalles de la entidad Sonda	57
Tabla 5.20 Detalles de la entidad Grupo de sondas.....	57
Tabla 5.21 Detalles de la entidad Grupo de Grupos de sondas	58
Tabla 5.22 Detalles de la entidad Sector	58

ACRÓNIMOS

ASN.1: notación de sintaxis abstracta número 1 (*Abstract Syntax Notation One, ASN.1*)

ATM: modo de transferencia asíncrona (*Asynchronous Transfer Mode*)

CPE: equipo local del cliente (*Customer Premises Equipment*)

EB: estación base

FCAPS: fallos, configuración, tarificación, rendimiento y seguridad (*Fault, Configuration, Accounting Performance, Security*)

ICMP: protocolo de mensajes de control de Internet (*Internet Control Message Protocol*)

ISO: Organización Internacional para la Estandarización (*International Organization for Standardization*)

KPI: indicador clave de rendimiento (*Key Performance Indicator*)

KQI: indicador clave de calidad (*Key Quality Indicator*)

LMDS: servicio de distribución local multipunto (*Local Multipoint Distribution Service*)

MIB: información base de gestión (*Management Information Base*)

MPLS: conmutación Multi-Protocolar mediante etiquetas (*Multiprotocol Label Switching*)

MMS: sistema de mensajes multimedia (*Multimedia Messaging System*)

NOC: centro de operaciones de red (*Network Operations Centre*)

OID: identificador de objeto (*Object Identifier Descriptor*)

OSI: modelo de referencia de Interconexión de Sistemas Abiertos (*Open System Interconnection*)

PSTN: red telefónica conmutada (*Public Switched Telephone Network*)

RFC: documento de definición de estándar (*Request for Comments*)

SLA: acuerdo de nivel de servicios (*Service Level Agreement*)

SNMP: protocolo simple de gestión de red (*Simple Network Management Protocol*)

SMS: sistema de mensajes cortos (*Short Messaging System*)

TIC: tecnologías de la información y las comunicaciones

TMN: gestión de redes de telecomunicaciones (*Telecommunications Management Network*)

UIT: Unión Internacional de Telecomunicaciones

VPN: red privada virtual (*Virtual Private Network*)

Capítulo 1 : Introducción

Hoy día todas las grandes compañías y la mayoría de las Pymes soportan sus procesos de negocio en las tecnologías informáticas. Sistemas de información heterogéneos desplegados sobre una red a la que se le exige un alto rendimiento y fiabilidad. Las tecnologías de la información y la comunicación (TIC) se han convertido en parte de la estrategia de las compañías y su gestión ha pasado a ser un proceso crítico. Las compañías más sensibles a las TIC son las operadoras de telecomunicaciones, ya que su negocio se basa directamente en la explotación de una red de comunicaciones.

Las numerosas operadoras de telecomunicaciones del mercado español ofrecen un amplio abanico de servicios a sus clientes como son: servicios de voz mediante telefonía fija y móvil, acceso a internet en diferentes modalidades (MODEM, RDSI, ADSL, *Frame Relay*, GPRS, UMTS) Redes privadas virtuales (*Virtual Private Network*), envío de mensajes cortos (*Short Messaging Service*) y mensajes multimedia (*Multimedia Messaging Service*), televisión y video entre otros. Todos estos servicios son posibles gracias a las redes de banda ancha desplegadas por las operadoras por todo el territorio nacional.

El problema fundamental que se afrontó con estas redes fue el desarrollo de nuevas tecnologías en las comunicaciones que permitiesen altas velocidades en el último tramo de llegada al cliente, a través de medios de transmisión convencionales como el par trenzado telefónico, el cable coaxial de las redes de cable o el espacio radioeléctrico. Cada operadora desplegó su red guiándose por la cartera de servicios que iba a ofrecer y por las estimaciones iniciales de volumen de clientes establecidas por sus equipos de marketing y ventas. Pero las necesidades de crecimiento y la feroz competencia del mercado de las telecomunicaciones obligan a las compañías a establecer políticas de fidelización y captación de clientes, ofreciendo cada vez más servicios y garantizando la calidad de los mismos. Por tanto, una vez desplegada la red de la operadora, su topología no permanecerá estática, crecerá y cambiará constantemente para adaptarse a nuevas exigencias de cobertura y al despliegue de nuevo equipamiento que proporcionará nuevos servicios de valor añadido. Como se puede apreciar, el activo fundamental de una operadora de telecomunicaciones es su red, y esta está la componen un gran número de dispositivos heterogéneos, desplegados en un área geográfica extensa, y que constantemente soporta adaptaciones y extensiones. La tarea crítica para cualquier operadora es sin lugar a dudas, mantener en funcionamiento ininterrumpido esta

red, con un rendimiento óptimo que permita a los usuarios disfrutar de todos sus servicios contratados. Esta tarea crítica es responsabilidad del área de operación de red (*Network Operations Center*) de la operadora, cuyo cometido es mantener el nivel óptimo de servicio de la red en todo momento. Para ello el equipo humano que forma el NOC debe monitorizar todos los dispositivos de la red en tiempo real garantizando su correcto funcionamiento, y debe responder rápida y eficazmente a cualquier eventualidad accediendo a la gestión remota de cualquier equipo para reconfigurarlo si fuese necesario. Para evitar problemas de la red que puedan reducir o bloquear los servicios es necesario anticiparse a los mismos, analizando el estado de la red en cada momento en busca de algún indicador que pueda anunciar un futuro problema. Para poder realizar eficazmente esta tarea los fabricantes de dispositivos de comunicaciones han adoptado como estándar el protocolo SNMP (*Simple Network Management Protocol*) del conjunto de protocolos TCP/IP definido por el *Internet Engineering Task Force* (IETF) en estrecha cooperación con el *World Wide Web Consortium* (W3C) y el ISO/IEC (*International Organization for Standardization/ International Electrotechnical Commission*) De manera que cada fabricante de dispositivos de red (enrutadores, switches, bridges, concentradores, etc.) han desarrollado el software de base necesario para gestionar los dispositivos que forman una red. Usando estos elementos básicos ISO ha definido un modelo de referencia funcional denominado FCAPS que se ha incorporado como modelo de gestión de red al modelo OSI.

FCAPS son las siglas correspondientes a *Fault, Configuration, Accounting, Performance, Security* (Fallos, configuración, medidas, rendimiento, seguridad) que son las categorías en las que el modelo ISO divide las tareas de gestión de red:

- Gestión de Fallos
- Gestión de la Configuración
- Gestión de Administración o contabilidad
- Gestión del Rendimiento
- Gestión de la Seguridad

Éstas son denominadas *Áreas Funcionales de Gestión* (MFAs ó *Management Functional Areas*) Cada MFA se encuentra definida en la serie de recomendaciones M.3000 de la ITU/T (*Internacional Telecommunication Union/ Telecommunication Standardization Sector*)

El propósito del modelo de referencia funcional es encapsular el alcance y diseño de un sistema de soporte a la operación, completamente genérico hacia un nivel de detalle tal que proporcione, de un modo fundamental, la arquitectura lógica. Este detalle incluye una

definición de todas las funciones genéricas dentro del espacio de los sistemas de soporte a la operación, así como los flujos de datos entre ellos.

A continuación, se detallan las áreas que son objeto del Sistema de Gestión de Red, desde un punto de vista funcional, realizando para ello, una descomposición en funciones de sistemas de información, tal como describe en el modelo TMN (*Telecommunications Management Network*)

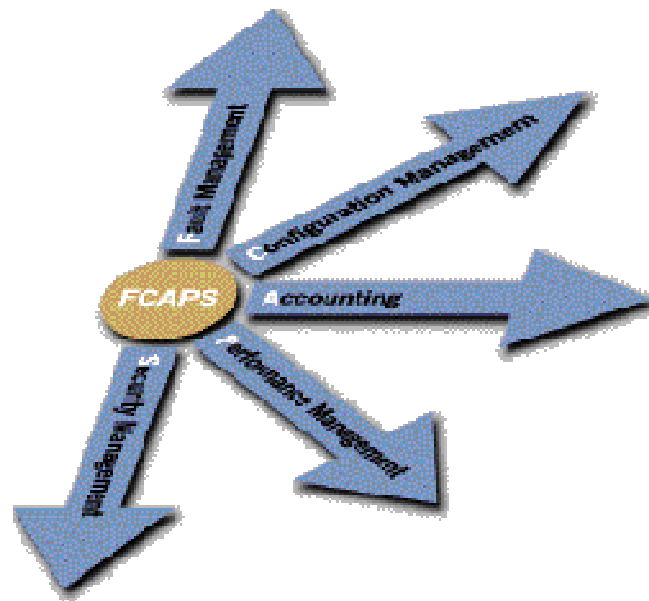


Figura.1 El modelo FCAPS

Por tanto, para cubrir las diferentes necesidades de un NOC es necesario tener indicadores de calidad de servicio. Esta información es utilizada para anticipar situaciones de crisis, organizar el despliegue de la red y optimizar la utilización de los recursos de la red, todo este proceso consiste en las siguientes tareas:

- Recogida de datos en bruto
- Recogida de datos a través de la red de una amplia gama de equipos heterogéneos realizando para ello operaciones de mediación.
- Definición y generación de indicadores elaborados
- Estos indicadores se utilizan para medir la carga global de la red, para dar información sobre el porcentaje de disponibilidad de los recursos disponibles, o para proporcionar indicaciones sobre la calidad del servicio.
- Generación de estadísticas e informes

- Los valores de los indicadores son almacenados en una base de datos, para generar estadísticas o informes sobre un largo periodo de tiempo.
- Anticipación de situaciones de crisis
- La medida de la carga de la red y el uso de umbrales que generan alarmas proactivas previene situaciones de crisis porque se pueden tomar acciones correctivas.
- Planificación de la red

El presente documento tiene como objetivo detallar el diseño de un sistema de gestión de red que cubra algunos apartados del modelo FCAPS, para lo cual se han incluido los siguientes apartados:

- Descripción de un escenario de red, posible en cualquier operadora de telecomunicaciones, para proporcionar un conjunto de servicios.
- Descripción del protocolo SNMP como base de la solución de gestión de red.
- Definición del conjunto de KPIs (Key Performance Indicator) necesario para controlar el rendimiento de la red y la Calidad
- Descripción del módulo de gestión de fallos.
- Descripción del módulo de gestión de medidas.
- Descripción del módulo de gestión de rendimiento.
- Visión del sistema integrado.

Capítulo 2 : Escenario

El primer paso para definir el escenario de red a monitorizar consiste en decidir los servicios que se van a prestar, y por tanto a monitorizar.

2.1 Servicios

DATOS: es el servicio de conectividad a otras redes o a Internet, en definitiva a cualquier red en la cual no estén en un mismo edificio todos sus miembros. Dentro del servicio de datos se proporciona acceso a Internet y VPN.

La red VPN permite al cliente conectar las diferentes sedes de su organización de forma permanente y totalmente privada utilizando la red IP Multiservicio basada en el protocolo MPLS (*Multiprotocol Label Switching*). De esta forma, el Cliente puede crear una VPN para cursar sus comunicaciones corporativas de forma totalmente segura.

VOZ IP: voz sobre protocolo de Internet, también llamado Voz sobre IP, VozIP, VoIP (por sus siglas en inglés), o Telefonía IP, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP. Esto significa que se envía la señal de voz en forma digital, en paquetes en lugar de enviarla (en forma digital o analógica) a través de circuitos utilizables solo para telefonía como una compañía telefónica convencional. La principal ventaja de este tipo de servicios es que evita los cargos altos de telefonía (principalmente de larga distancia) que son típicos al usar la Red Pública Telefónica Conmutada (PSTN). El ahorro en el costo se debe al uso de una misma red para llevar voz y datos. Las llamadas de VoIP a VoIP entre cualquier proveedor son generalmente gratis, en contraste con las llamadas de VoIP a PSTN que generalmente cuestan al usuario de VoIP.

VoIP puede facilitar tareas que serían más difíciles de realizar usando las redes telefónicas comunes:

- Las llamadas telefónicas locales pueden ser automáticamente enrutadas a tu teléfono VoIP, sin importar donde estés conectado a la red. Llevando contigo tu teléfono VoIP en un viaje, y donde quiera que estés conectado a Internet, podrás recibir llamadas.
- Usando teléfonos VoIP los agentes de atención a usuarios pueden trabajar en cualquier lugar con una conexión a Internet lo suficientemente rápida.
- Algunos paquetes de VoIP incluyen los servicios extra por los que PSTN normalmente cobra un cargo extra, o que no se encuentran disponibles en algunos

países, como son las multiconferencias, retorno de llamada, remarcación automática, o identificación de llamadas.

El protocolo estándar para VoIP es el H323, definido en 1996 por la UIT (Unión Internacional de Telecomunicaciones) proporciona a los diversos fabricantes una serie de normas con el fin de que puedan evolucionar en conjunto. Por su estructura el estándar proporciona las siguientes ventajas:

- Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento.
- Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes IP actuales.
- Es independiente del equipamiento hardware utilizado.
- Permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.
- Permite la integración de Video y Videoconferencia.

2.2 Topología

La topología necesaria para prestar estos servicios en un área geográfica amplia, como puede ser España, se compone de las siguientes divisiones:

- Núcleo o *core*: es el centro de la topología en estrella de la red nacional. Está formado por muy pocos equipos de gran capacidad con enlaces de alta capacidad hacia los diferentes *Backbones*.

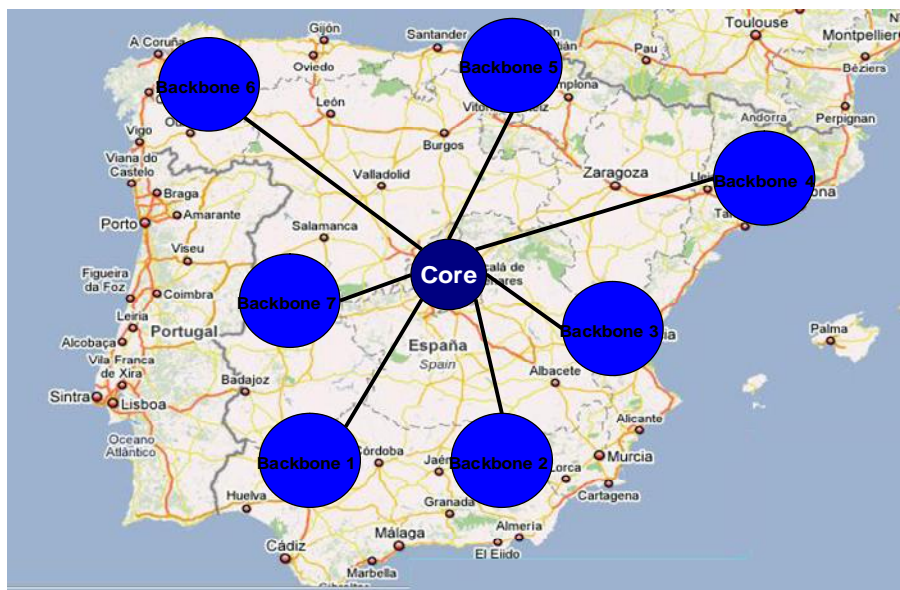


Figura 2.1 Topología de los backbones

- *Backbone*: es el núcleo de cada una de las subdivisiones del territorio al que se va a dar cobertura. Esta formado por equipos de menor capacidad que el *core*, pero capaces de soportar la carga provocada por los usuarios de su demarcación geográfica.
- Acceso o bucle de abonado: abarca los elementos que soportan los enlaces de telecomunicaciones entre los usuarios finales y el *backbone* de su demarcación geográfica. Son las ramificaciones de la red que la operadora despliega para dar cobertura a sus clientes en un área geográfica determinada, por ejemplo una provincia.
- Equipos de cliente o CPE (*Customer Premises Equipment*): es el equipamiento localizado en el lado del cliente y que se encuentra conectado directamente con el bucle de abonado.

La idea de transportar servicios de voz sobre la infraestructura de una red de datos no es nueva y las ventajas asociadas han sido desde hace tiempo el impulso de importantes trabajos en este sentido. Se trata de arquitecturas que proporcionan el transporte de la voz sobre los protocolos de datos más habituales a nivel 2 o 3. Así, podemos hablar de Voz sobre *Frame Relay* (VoFR), Voz sobre ATM (VoATM), Voz sobre IP (VoIP)

Estas tecnologías parten de la transmisión de la voz mediante paquetes cursados sobre la red de datos del operador. Esta paquetización es la que permite acomodar la voz al formato de transmisión de las redes de datos y la unificación de ambos servicios sobre una única red. A priori, todas estas soluciones proporcionan al operador las ventajas de la integración de una red de voz dentro de una infraestructura de transporte basada en la transmisión de paquetes de datos:

- Única infraestructura de transporte de red para las redes del operador.
- Operación unificada.
- Menor número de elementos de red a gestionar.
- Optimización de los recursos de transmisión.

Surgen, no obstante, algunos retos asociados a la utilización de este tipo de tecnologías:

- Complejidad de puesta en marcha y operación.
- Riesgos asociados a la innovación tecnológica.

De todas las tecnologías de Voz sobre Datos (VoD) la que ha centrado los mayores esfuerzos de desarrollo ha sido VoIP, al proporcionar las ventajas asociadas a los protocolos de nivel 3 a costa de una mayor complejidad tecnológica.

Un ejemplo, común en la actualidad, de infraestructura base para servicios de datos y VoIP consta de una red ATM para implementar el nivel 2 o transporte y sobre este nivel de transporte desplegar una red MPLS para implementar el nivel 3 o red. Sobre estos dos niveles se despliegan los elementos específicos del servicio VoIP.

MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel o conmutación IP. La idea básica de separar el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles 2 y 3, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura. Por otro lado, el hecho de que MPLS pueda funcionar sobre cualquier tecnología de transporte, no sólo sobre infraestructuras ATM, va a facilitar de modo significativo la migración para la próxima generación, internet óptica, en la que se acortará la distancia entre el nivel de red IP y la fibra. MPLS permite a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP (normalmente limitadas a encaminar por dirección de destino). Además de poder hacer ingeniería de tráfico IP, MPLS permite mantener clases de servicio y soporta con gran eficacia la creación de VPNs. Por todo ello. MPLS aparece ahora como la gran promesa y esperanza para poder mantener el ritmo actual de crecimiento de la red.

2.2.1 Elementos de una Red VoIP

En una red VoIP de vanguardia se pueden distinguir los siguientes elementos:

- Infraestructura IP: transporte tanto para la señalización de las llamadas como para la voz. Esta red debe seguir unas condiciones de diseño específicas que permitan el transporte de la voz con la calidad adecuada.
- Equipo de cliente o *Gateway* residencial: encargado de originar o recibir las llamadas del cliente. Estos pueden ser equipos que se integran directamente en la red VoIP (teléfonos H.323, etc.) o *gateways* de cliente que proporcionan una interfaz hacia la

red VoIP y una o más interfaces tradicionales de voz hacia el cliente (POTS, RDSI, etc.)

- *Gateway* de red: permite la comunicación entre la red VoIP y las redes tradicionales de conmutación de circuitos (PSTN). A tal fin estos elementos se encargan de convertir las llamadas VoIP, con voz paquetizada, a llamadas de Conmutación de Circuitos. Por lo general la comunicación con la red tradicional se basará en el protocolo SS7.
- *SoftSwitch*: elemento central de la red; realiza la misma función de control de red que el nodo de conmutación de una red de voz tradicional. Sus principales funciones son el enrutamiento de las llamadas (funcionalidades de clase IV) y proporcionar servicios suplementarios (funcionalidades de clase V). El *SoftSwitch* se encarga de recibir la señalización de las llamadas y de enrutarlas hacia su destino.

La arquitectura lógica del *core* teniendo en cuenta la base ATM, la capa MPLS y los elementos para el servicio de VoIP citados, se muestra en la figura 2.2:

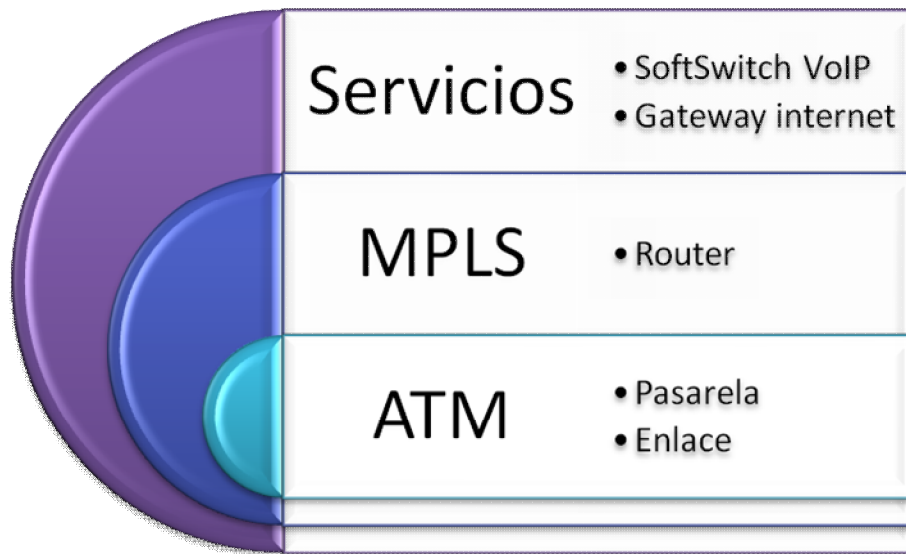


Figura 2.2 Arquitectura lógica del *core*

Para implementar esta arquitectura lógica, el *core* contendrá el siguiente equipamiento:

- ATM
 - El enlace ATM debe ser capaz de soportar 32 Gbps de tráfico ofreciendo garantías de calidad del servicio y alta disponibilidad. El *switch* multiservicio **Passport 15000** de Nortel, con una capacidad de 40 Gbps, puede gestionar el tráfico ATM entre el *core* y los *backbones*, ofreciendo la

posibilidad de integrar diversas configuraciones de red a través de interfaces de diferentes velocidades (DS-0 hasta OC-192/STM-64). Como enlace ATM soporta los protocolos de señalización estándares ATM IISP (*Interim Inter-switch Signaling Protocol*) y PNNI (*Private Network-to-Network Interface*) que proporcionan QoS. El Passport 15000 incorpora la tecnología *hot-swappable* que permite cambiar componentes mientras el dispositivo sigue prestando servicio y una amplia variedad de esquemas redundantes. Finalmente para aumentar las prestaciones en un punto crítico como es la entrada al *core* el Passport 15000 aporta la posibilidad de funcionar en modo multiplexado inverso sobre ATM (IMA) $n \times$ DS-1/E1 para optimizar el reparto del tráfico de la interfaz WAN hacia los mediadores de menor capacidad.

- Pasarelas de mediación entre la red ATM y la red MPLS con capacidad para gestionar más de 20 Gbps o 10 Gbps en *full duplex*. Dos **Juniper M20** que forman la solución de conversión de tráfico ATM a MPLS. Aportará además búsqueda de rutas, filtrado, limitación y balanceo de carga, gestión de *buffers*, *switching*, encapsulación y desencapsulación de servicios IP.
- MPLS
 - *Routers* MPLS capaz de soportar más de 150 líneas T1 o E1, incorporar las mejoras en enrutamiento y gestionar las VPN. Para lo cual se disponen dos *Routers* 7200 de Cisco con capacidad para 180 conexiones T1 o 162 E1 que implementan el enrutamiento MPLS sobre la base ATM en el *core*, aportando mediante el protocolo estándar ATM AAL2 información de redundancia, *Time stamp* y tipo de paquete. Soporta compresión de paquetes de voz y eliminación de silencios y se integra con las capacidades QoS de ATM
- Servicios
 - Para prestar el servicio de datos el *core* incorpora *gateways* a internet, con una capacidad superior a 3 Gbps en alta disponibilidad. Para este apartado se podría contar con dos **Juniper M5** conectados en alta disponibilidad que soportan 6 Gbps cada uno. Los M5 incorporan los protocolos de enrutamiento OSPF y BGP que optimizan el manejo de los paquetes IP. Frente a equipos de Cisco, los M5 de Juniper aportan una mayor capacidad de conmutación de paquetes y es posible configurar enrutamiento MPLS mejorando el encaminamiento IP convencional.

- *Softswitch* para gestión del servicio VoIP con un BHCA (*Busy Hour Call Attempt*) o intentos de llamada en hora punta de 2.000.000. Un **Call Server 2000** (CS2K) de Nortel encargado del direccionamiento del tráfico de VoIP. El Call Server 2000 se compone del propio CS2K, un CICM (*Centrex IP Call Manager*) para tarificar y gestionar la facturación de las llamadas y un UAS (*Universal Audio Server*) para provisionar y gestionar el servicio. Se incorporan en esta configuración dos *router* Cisco 7200 para gestionar el tráfico de VoIP directamente sobre MPLS incorporando etiquetas de servicio.

Todos estos dispositivos se conectarían como se muestra en la figura 2.2:

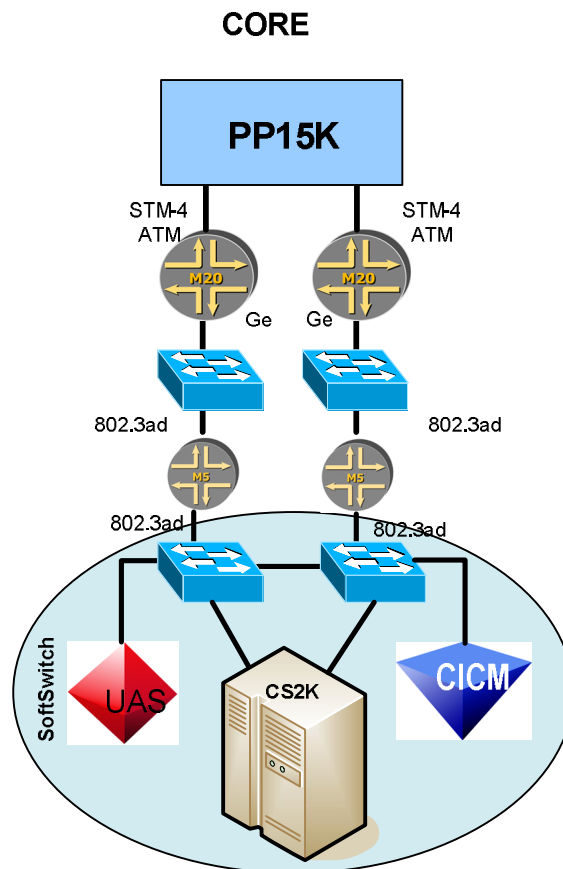
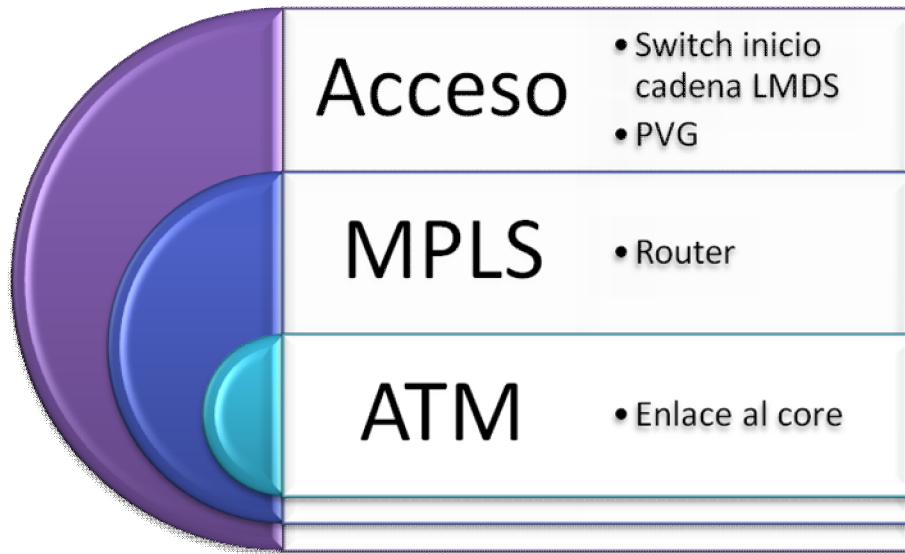


Figura 2.3 Topología del *core*

La arquitectura del *backbone* comparte la filosofía del *core* e incorpora la conexión a la red de acceso. La arquitectura lógica del *backbone* se muestra en la figura 2.5

Figura 2.4 Arquitectura lógica de los *Backbones*

Para implementar esta arquitectura lógica, el *backbone* contendrá los siguientes componentes:

- ATM
 - El enlace ATM debe ser capaz de gestionar 500 Mbps de tráfico o unos 9000 canales DS0, ofreciendo garantías de calidad del servicio y alta disponibilidad. El *switch* multiservicio **Passport 7000** de Nortel, con una capacidad superior a las 384 líneas físicas DS-1/E1, puede gestionar el tráfico ATM entre el *backbone* y el *core*. Como enlace ATM soporta los protocolos de señalización estándares ATM IIS (Interim Inter-switch Signaling Protocol) y PNNI (Private Network-to-Network Interface) que proporcionan QoS. El Passport 7000 incorpora la tecnología *hot-swappable* que permite cambiar componentes mientras el dispositivo sigue prestando servicio y una amplia variedad de esquemas redundantes.
- MPLS
 - De nuevo se necesitan *routers* MPLS capaces de soportar más de 150 líneas T1 o E1, incorporar las mejoras en enrutamiento y gestionar las VPN. Para lo cual se disponen dos *router* 7200 de Cisco con capacidad para 180 conexiones T1 o 162 E1 que implementan el enrutamiento MPLS sobre la base ATM en el *core*, aportando mediante el protocolo estándar ATM AAL2 información de redundancia, *Time stamp* y tipo de paquete. Soporta compresión de paquetes de voz y eliminación de silencios y se integra con las capacidades QoS de ATM.
- Acceso
 - PVG (*Packet Voice Gateway*) para gestionar las llamadas hacia otras operadoras, con una capacidad de más de 40000 canales (DS0). Un *passport* 15000 de Nortel configurado como PVG soporta 48000 canales DS0 e incorpora el estándar de compresión de voz G.729 con eliminación de silencios y control de congestión.
 - Como inicio de la cadena LMDS se necesitan equipos escalables con conexiones *FastEthernet*. Los *switches* Cisco 3750 proporcionan con su

tecnología *StackWise* la posibilidad de apilar hasta 9 *switches* proporcionando 32 Gbps. La configuración recomendada en alta disponibilidad supone apilar dos *switches* con 24 puertos *Ethernet* 10/100/1000 incluyendo fuentes de alimentación redundante.

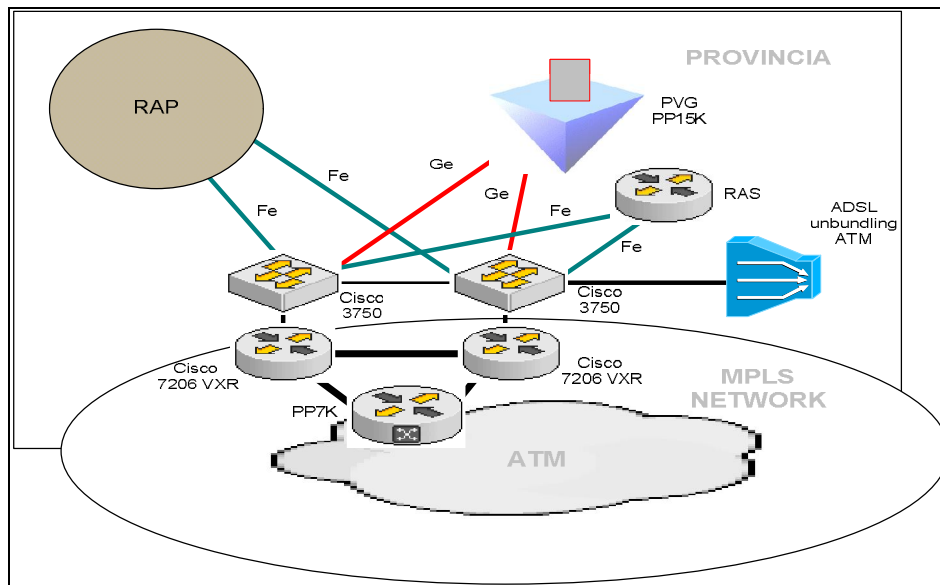


Figura 2.5 Arquitectura de un *Backbone*

Una vez decidida la arquitectura para la infraestructura del *core* y los *backbones* (el núcleo de la red del operador) solo queda decidir la arquitectura para el tramo de acceso. Normalmente este tramo de acceso supone una fuerte inversión en tiempo y dinero para desplegar el cableado sobre el área geográfica a la que se quiere dar servicio. Otra posibilidad es utilizar la tecnología LMDS (*Local Multipoint Distribution Service*) Sistema de Distribución Local, que evita los costosos cableados de fibra óptica o de pares de cobre en el tramo de acceso. Utilizando radio enlaces a 3,5 Ghz se puede ofrecer cobertura a grandes áreas geográficas evitando los problemas de un despliegue de cable. Esta tecnología puede resolver el problema de acceso en puntos geográficamente no rentables, es decir en zonas rurales con un número reducido de clientes o difícil acceso, que impiden rentabilizar un despliegue de cable o fibra óptica.

El tramo desde el *backbone* hasta las sedes de los clientes es lo que llamamos red de acceso. La figura 2.6 muestra la estructura completa de la red necesaria para soportar los servicios citados:

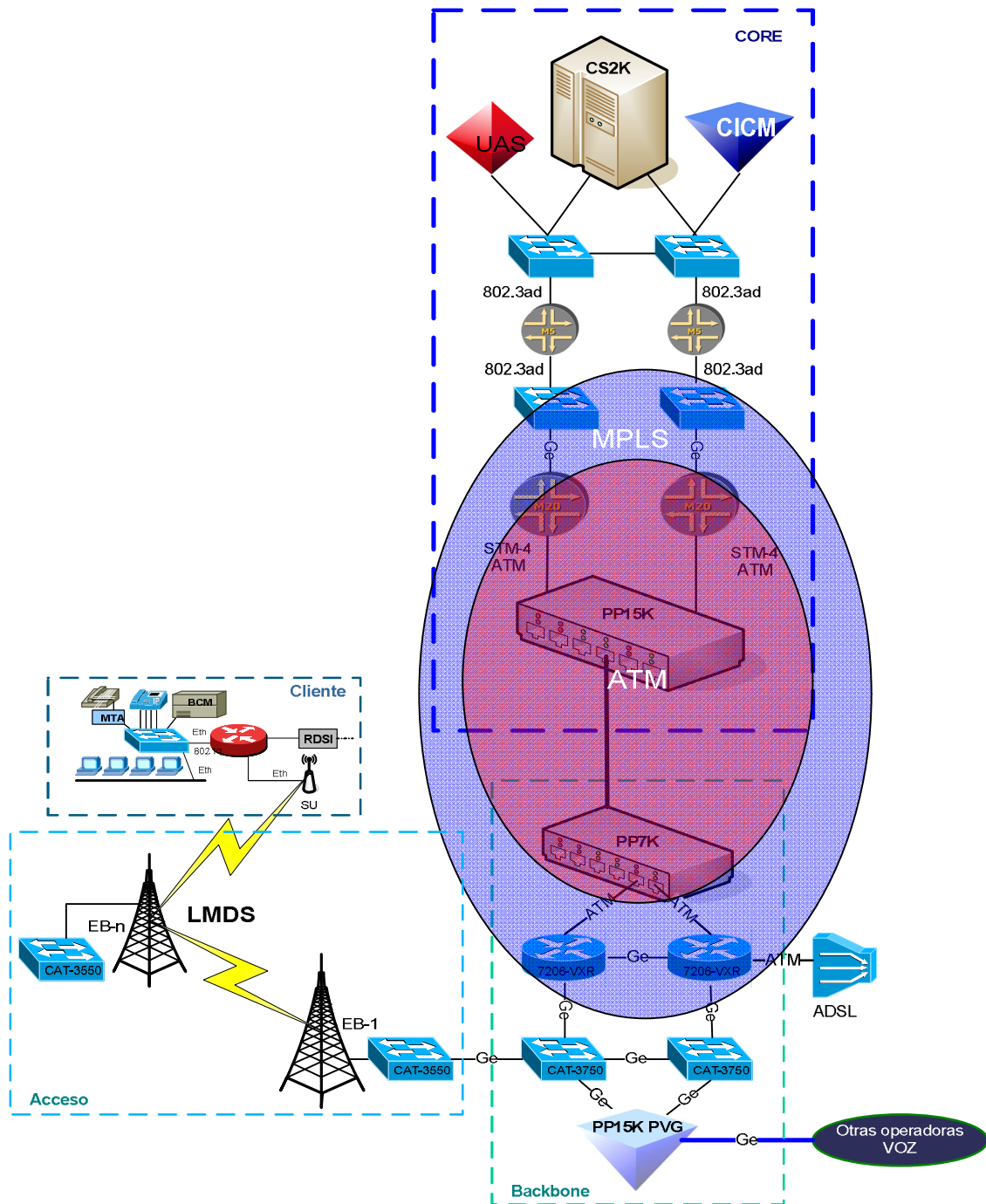


Figura 2.6 Arquitectura completa de la red

Como muestra la figura 2.6 la arquitectura completa de la red consta de una base de transporte ATM sobre la que se despliega una red MPLS que une los *backbones* con el *core* y una red LMDS de acceso hasta los clientes.

Capítulo 3 : Tecnología a utilizar

La base de toda la solución no es otra que el protocolo de la capa de aplicación TCP/IP, SNMP (*Simple Network Management Protocol*) El Protocolo Simple de Administración de Red es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos de Internet utilizando un servicio no orientado a la conexión (UDP). SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

3.1 Componentes básicos de SNMP

Una red administrada a través de SNMP consiste en los siguientes tres componentes claves:

- Dispositivos administrados.
- Agentes.
- Sistemas administradores de red o NMS (*Network Management Systems*)

Un **dispositivo administrado** es un nodo de red que contiene un agente SNMP y reside en una red administrada. Éstos recogen y almacenan información de administración, la cual es puesta a disposición de los NMSs usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser *routers*, servidores de acceso, *switches*, *bridges*, *hubs*, computadores o impresoras.

Un **agente** es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de la información de administración (por ejemplo: memoria libre, número de paquetes IP recibidos, ruta por defecto), la cual es organizada en jerarquías descritas en la base de información de administración o MIB (*Management Information Base*)

Un **NMS** ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMSs proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMSs deben existir en cualquier red administrada.

3.2 Comandos básicos de SNMP

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos:

- **Lectura:** el comando de lectura es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.
- **Escritura:** el comando de escritura es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.
- **Notificación:** el comando de notificación es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.
- **Operaciones transversales:** las operaciones transversales son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger en secuencia información en tablas de variables, como por ejemplo, una tabla de rutas.

3.3 Base de información de administración SNMP (MIB)

Una base de información de administración o MIB es una colección de información que está organizada jerárquicamente. Las MIBs son accedidas usando un protocolo de administración de red, como por ejemplo, SNMP.

Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) corresponde a una de las características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables. Están implementadas usando la notación ASN.1. Existen dos tipos de objetos administrados: escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un ejemplo de un objeto administrado es *atInput*, que es un objeto escalar que contiene una simple instancia de objeto, el valor entero que indica el número total de paquetes *AppleTalk* de entrada sobre una interfaz de un *router*.

Un identificador de objeto (*object ID*) únicamente identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones, como se muestra en la siguiente figura:

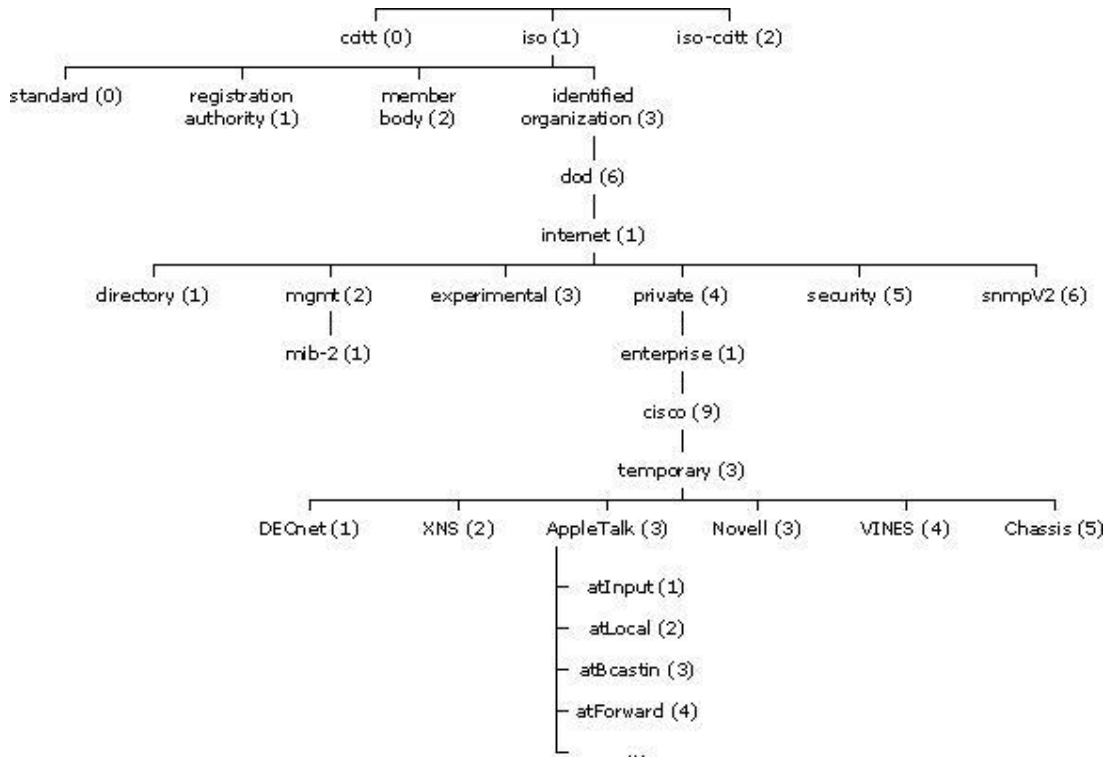


Figura 3.1 Jerarquía MIB

El árbol MIB ilustra las variadas jerarquías asignadas por las diferentes organizaciones. Los identificadores de los objetos ubicados en la parte superior del árbol pertenecen a diferentes organizaciones estándares, mientras los identificadores de los objetos ubicados en la parte inferior del árbol son colocados por las organizaciones asociadas. Los vendedores pueden definir ramas privadas que incluyen los objetos administrados para sus propios productos.

El objeto administrado *atInput* podría ser identificado por el nombre de objeto *iso.identified-organization.dod.internet.private.enterprise.cisco temporary.AppleTalk.atInput* o por el descriptor de objeto equivalente 1.3.6.1.4.1.9.3.3.1.

El núcleo del árbol MIB se encuentra compuesto de varios grupos de objetos, los cuales en su conjunto son llamados mib-2. Los grupos son los siguientes:

- System (1)
- Interfaces (2)
- AT (3)
- IP (4)
- ICMP (5)
- TCP (6)
- UDP (7)
- EGP (8)
- *Transmission* (10)
- SNMP (11)

3.4 Notación de sintaxis abstracta 1 o ASN.1

En las telecomunicaciones y las redes de ordenadores, la notación de sintaxis abstracta número 1 (*Abstract Syntax Notation One, ASN.1*) es una notación estándar y flexible para describir estructuras de datos que pueden ser usadas para representar, codificar, transmitir y decodificar datos. Está compuesta por una serie de reglas formales para describir la estructura de objetos de manera que sean independientes de la máquina en la que se estén interpretando y sean precisos, es decir, que no dé lugar a ambigüedades.

ASN.1 es un estándar conjunto de ISO y la UIT-T, creado originalmente en 1984 como una parte de CCITT X.409:1984. ASN.1 evolucionó y en 1988, dada su gran versatilidad, se convirtió en estándar propio, bajo el nombre de X.208. En 1995 se revisó sustancialmente y el nuevo estándar se definió en la serie X.680.

Una parte de ASN.1, la estructura de información gestionada (*Structure of Management Information, SMI*), se adaptó a SNMP para definir objetos MIB interrelacionados, llamados también módulos MIB.

3.5 Mensajes SNMP

Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP.

Los puertos asignados por la IANA para el protocolo SNMP se describen en la tabla 3.1:

Puerto/protocolo	Descripción
161/tcp	SNMP
161/udp	SNMP
162/tcp	Traps SNMP
162/udp	Traps SNMP

Tabla 3.1 Puertos SNMP

El formato de las tramas SNMP se muestra en la figura 3.2:

Versión	Comunidad	SNMP PDU
---------	-----------	----------

Figura 3.2 Tramas SNMP

Donde **versión** es el número de versión de protocolo que se está aplicando. En SNMPv1, vale 1. La **comunidad** es un nombre que se usa para la autenticación. Generalmente, existe una comunidad de lectura (que puede consultar los valores en el agente, pero no modificarlos) llamada "public" y una comunidad de escritura en algunos casos llamada "private". El contenido de la unidad de datos del protocolo (SNMP PDU) depende de la operación que estemos realizando. Las operaciones *GetRequest*, *GetNextRequest* y *SetRequest* tienen la SNMP PDU que se muestra en la figura 3.3:

Tipo de PDU	Identificador de "request"	Estado de Error	Índice de Error	Enlazado de variables (Variable Bindings)
-------------	----------------------------	-----------------	-----------------	---

Figura 3.3 SNMP PDU

El identificador de *request* es un número. Cuando el agente responda, usará el mismo identificador. De esta manera una estación de gestión puede realizar muchas consultas usando identificadores diferentes. Cuando lleguen las respuestas (*GetResponse*) podrá saber a qué pregunta correspondían fijándose en este valor. El estado de error e índice de error sólo se usan en los *GetResponse*. Las consultas llevan siempre estos valores a cero. El campo índice de error sólo se usa cuando "estado de error" es distinto de cero para proporcionar información adicional sobre qué provocó el error. El estado de error puede tener los siguientes valores:

- 0: No hay error

- 1: Demasiado grande
- 2: No existe esa variable
- 3: Valor incorrecto
- 4: El valor es de solo lectura (si hemos pedido escribir en un valor en el que no podemos).
- 5: Error genérico

3.6 GetRequest

A través de este mensaje el NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre. En respuesta el agente envía una respuesta indicando el éxito o fracaso del requerimiento. Si el requerimiento fue adecuado, el mensaje resultante también contendrá el valor del objeto solicitado. Este mensaje puede ser usado para recoger un valor de un objeto, o varios valores de varios objetos, a través del uso de listas.

3.7 GetNextRequest

Este mensaje es usado para recorrer una tabla de objetos. Una vez que se ha usado un mensaje *GetRequest* para recoger el valor de un objeto, puede ser utilizado el mensaje *GetNextRequest* para repetir la operación con el siguiente objeto de la tabla. Siempre el resultado de la operación anterior será utilizado para la nueva consulta. De esta forma un NMS puede recorrer una tabla de longitud variable hasta que haya extraído toda la información para cada fila existente.

3.8 SetRequest

Este tipo de mensaje es utilizado por el NMS para solicitar a un agente modificar valores de objetos. Para realizar esta operación el NMS envía al agente una lista de nombres de objetos con sus correspondientes valores.

3.9 GetResponse

Este mensaje es usado por el agente para responder un mensaje *GetRequest*, *GetNextRequest*, o *SetRequest*. En el campo "Identificador de *Request*" lleva el mismo identificador que el *request* al que está respondiendo.

3.10 Trap

Un trap es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración. El formato de la PDU se muestra en la figura 3.4

Tipo de PDU	Enterprise	Dirección del agente	Tipo genérico de trap	Tipo específico de trap	Timestamp	Enlazado de variables (Variable Bindings)
-------------	------------	----------------------	-----------------------	-------------------------	-----------	---

Figura 3.4 SNMP PDU para traps

En el campo **enterprise** se identifica el subsistema de gestión que ha emitido el Trap. El campo dirección del agente lleva la dirección IP del agente que emite el Trap. El tipo genérico de Trap puede ser:

- *Cold start(0)*: Indica que el agente ha sido inicializado o reinicializado.
- *Warm start(1)*: Indica que la configuración del agente ha cambiado.
- *Link down(2)*: Indica que una interfaz de comunicación ha dejado de funcionar.
- *Link up(3)*: Indica que una interfaz de comunicación vuelve a estar en servicio.
- *Authentication failure(4)*: Indica que el agente ha recibido un requerimiento de un administrador no autorizado.
- *EGP neighbor loss(5)*: Indica que en sistemas en que los routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio.
- *Enterprise Specific(6)*: En esta categoría se engloban todos los nuevos traps que son incluidos por los vendedores. El tipo de trap se indica en el campo "tipo específico de Trap".

Como se explicó anteriormente, el campo **tipo específico de trap** es el usado para los traps específicos de los fabricantes, así como para precisar la información de un determinado trap genérico. El campo timestamp indica el tiempo que ha transcurrido entre la reinicialización del agente y la generación del Trap.

3.11 GetBulkRequest

Este mensaje es usado normalmente por un NMS que utiliza la versión 2 del protocolo SNMP cuando es requerida una transmisión extensa de datos, tal como la recuperación de

tablas grandes. En este sentido es similar al mensaje *GetNextRequest* usado en la versión 1 del protocolo, sin embargo, *GetBulkRequest* es un mensaje que implica un método mucho más rápido y eficiente, ya que a través de un solo mensaje es posible solicitar la totalidad de la tabla.

3.12 InformRequest

Un NMS que utiliza la versión 2 del protocolo SNMP transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados.

Capítulo 4 Gestión de fallos

Dentro de la gestión de redes, la gestión de fallos es el conjunto de funciones que detectan, aíslan y reparan los problemas de una red de telecomunicaciones, manteniendo y examinando los registros de error, recogiendo las notificaciones y actuando para corregirlos, trazando e identificando los errores, realizando las secuencias de pruebas de diagnóstico e informando de las condiciones de fallo.

En la gestión de fallos mediante SNMP, los problemas son detectados en una entidad, bien interrogando variables de su MIB, esperando las notificaciones enviadas por la entidad o por alguna combinación de ambos mecanismos.

La arquitectura de un sistema de gestión de fallos o alarmas, como se muestra en la figura 4.1, está compuesta por diferentes elementos organizados en capas:

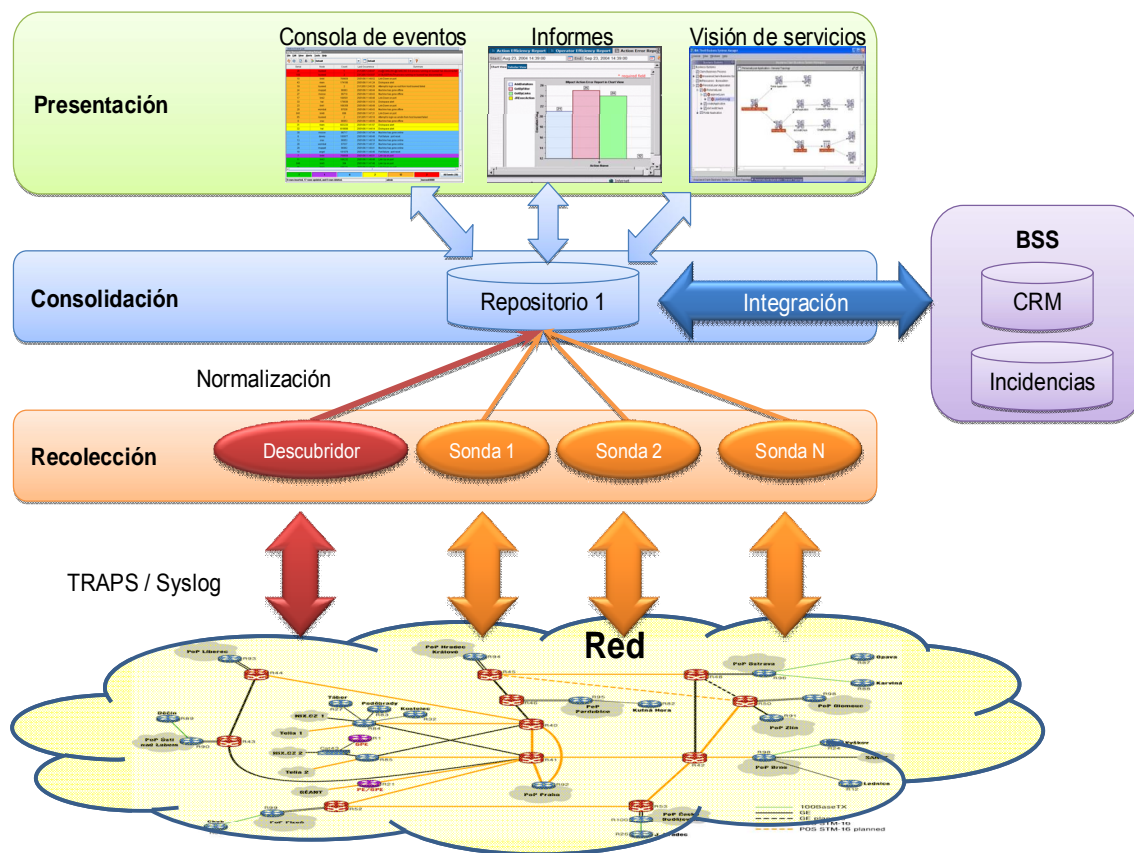


Figura 4.1 Arquitectura del sistema de gestión de fallos

4.1 Capa de recolección

El cometido de esta capa de la arquitectura es recibir los *traps* o alarmas de los equipos e interrogar los valores que no emiten alarma pero indican el correcto funcionamiento de los elementos. Para ello es necesario desplegar una combinación de sondas genéricas para recibir *traps snmp*, y específicas para aquellos elementos a los que hay que interrogar, ya que no emiten traps. Para el escenario definido en el capítulo 2 será necesario desplegar las siguientes sondas:

- Sonda específica Nortel: esta sonda permite mediante una conexión Telnet o rsh, recoger los eventos que afectan a los equipos Nortel.
- Sonda SNMP: esta sonda permite recibir los *traps* de aquellos equipos dotados de un agente capaz de enviar *traps*, además permite interrogar vía SNMP a los dispositivos, obteniendo los valores contenidos en su MIB. De esta forma se amplía la información sobre los eventos y se puede actuar con mayor eficiencia para resolverlos.
- Sonda Syslog: es una sonda especial que aprovecha el mecanismo de UNIX que almacena en ficheros los eventos del sistema. La sonda Syslog se conecta al equipo, lee el fichero de Log y realiza un análisis del mismo buscando eventos que indiquen un mal funcionamiento. Estos eventos son convertidos en alarmas en el sistema de gestión de fallos, apareciendo en la consola de presentación con el nivel de severidad correspondiente.

Es necesario incorporar un sistema cíclico de purgado del fichero de log para eliminar los apuntes que superan un tiempo determinado. De esta manera no se supera la capacidad de almacenamiento del equipo y siempre se tiene en el fichero la información más actual.

Todos los eventos son normalizados de acuerdo al formato homogéneo descrito en el apartado 3.10, que incluye toda la información necesaria para resolver el problema. En esta capa se incorpora el nivel de severidad de cada evento ente las siguientes categorías:

- **Crítica:** Indica que un evento severo ha ocurrido, el cual requiere de atención inmediata. Son fallos que afectan el funcionamiento global de la red. Por ejemplo, cuando un enlace importante está fuera de servicio, su inmediato restablecimiento es requerido.

- **Media:** Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.
- **Leve:** Indica la existencia de una condición que no afecta al servicio, pero que deben ser tomadas las acciones pertinentes para prevenir una situación peor. Por ejemplo, cuando se alcanza cierto límite en la utilización del enlace no indica que el servicio sea afectado, pero lo será si se permite que siga avanzando.
- **Clear:** Indica que el evento ha sido resuelto, dejando de aparecer en la consola de eventos activos.
- **Indefinida:** Cuando el nivel de severidad no ha sido determinado por alguna razón.

Resumiendo, el funcionamiento de esta capa de recolección consiste en recibir los *traps* de aquellos equipos, dotados de agente SNMP, capaces de enviar sus propias alarmas e interrogar, a través de sondas específicas, a aquellos equipos que no envían *traps* o no envían toda la información necesaria para resolver los fallos. Todos los eventos, ya normalizados, son remitidos al repositorio de la capa de consolidación.

Descubrimiento

La tecnología utilizada para monitorizar no es nueva, pero su implantación ha sufrido un gran retraso. Este retraso en adoptar una tecnología tan práctica sobre una tarea tan crítica se ha debido principalmente a la dificultad para mantener actualizado el inventario sobre el que se realiza la monitorización tanto de fallos como de rendimiento. En un principio, el inventario era realizado y mantenido manualmente por el personal responsable de operaciones y despliegue de red. Esto provocaba desfases constantes entre el parque desplegado y el inventario que debían subsanarse revisando ambos. Este esfuerzo enorme y constante condujo a los responsables de dicho inventario a fraccionar el problema para hacerlo más abordable, de manera que el inventario no era único y residía normalmente en sistemas gestores para cada tipo de tecnología y en algunos casos incluso se realizaban divisiones geográficas o administrativas. Todo esto dificulta enormemente la obtención de una visión global e impide la adopción de políticas que alineen la infraestructura con los objetivos de la operadoras de telecomunicaciones.

En la actualidad, gracias a la normalización mayoritariamente extendida entre los fabricantes de equipos de red y a la evolución de las tecnologías de descubrimiento, es posible automatizar el inventario y el proceso de actualización periódica del mismo. Por normalización se entiende la adopción del estándar SNMP para gestión de equipos, incluyendo agentes SNMP en los equipos, y la incorporación de MIBs que incorporan todos los parámetros para gestionar los mismos.

La tecnología para el descubrimiento de equipos y sistemas ha ido sumando tecnologías, desde las más simples a las más complejas, hasta conseguir convencer a los responsables del inventario de su fiabilidad. El primero de los mecanismos utilizados para el descubrimiento fue un simple *Ping*.

Un *Ping* (*Packet Internet Grouper*) se trata de una utilidad que comprueba el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (definidos en el protocolo de red ICMP) para determinar si un sistema IP específico es accesible en una red. Aportando un rango de direcciones IP, es posible lanzar una ráfaga de consultas a la red y determinar los equipos que están accesibles y los que no.

La información que aporta un *Ping* es insuficiente a la hora de gestionar, de manera que se incorporó al proceso de descubrimiento la consulta SNMP. Una vez interrogada la red vía *Ping* se lanza una ráfaga de consultas SNMP a los equipos accesibles para determinar el tipo de equipos que son y la topología. Esta última es una información clave para facilitar el trabajo del centro de operaciones, que mediante una visión topológica como la de la figura 4.2. acceden rápidamente a los equipos en caso de fallo para intervenir y solucionar el problema.

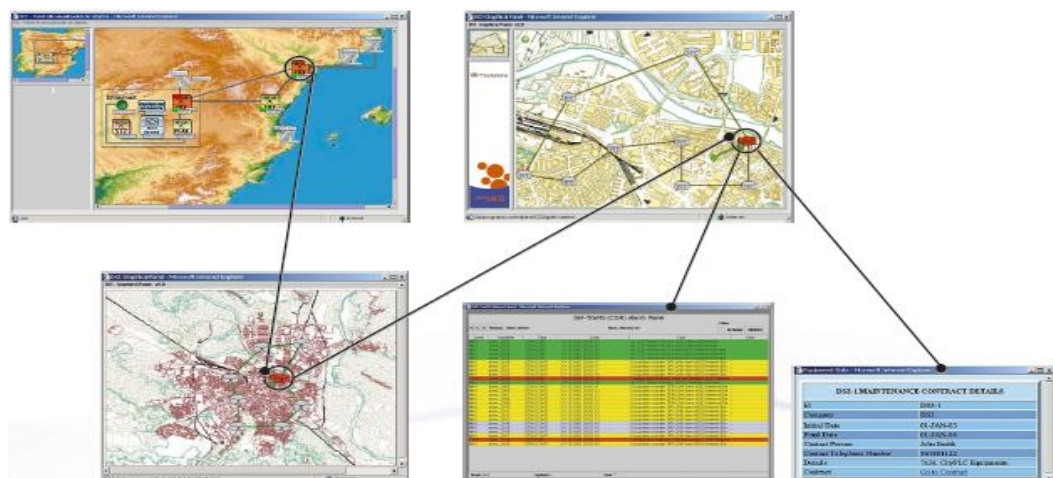


Figura 4.2 Visión topológica de la red

Esta información es suficiente para casi todos los equipos de red, pero existen equipos complejos, como el *softswitch* de VoIP que están compuestos por grupos de servidores que alojan tarjetas de comunicaciones. Por supuesto también es insuficiente para determinar las aplicaciones que corren sobre los servidores, que también son objeto de la gestión de fallos y rendimiento. Para superar esta barrera han aparecido aplicaciones que incorporan agentes específicos para un gran número de aplicaciones comerciales y que permiten desarrollar agentes a medida para casos muy particulares.

Con estos tres mecanismos, *Ping*, *agentes SNMP* y agentes específicos, es posible la completa automatización del inventario y su mantenimiento periódico.

Inventario

Toda la información del descubrimiento se registra en el inventario. Este inventario es un subconjunto del registro de activos de la operadora.

El despliegue de red de una operadora no solo implica elementos de telecomunicaciones, los elementos se alojan en soportes (*racks*, mástiles, etc.) que a su vez se alojan en pequeñas construcciones dotadas de generadores de energía, elementos de acondicionamiento y de seguridad, etc. Todos estos componentes se registran en el inventario de activos de la operadora.

Por otra parte este inventario puede detallarse hasta el nivel que se quiera, por ejemplo es posible incluir el detalle de las interfaces que componen un determinado *router*, y aún más detallar las subinterfaces (que son una división lógica y no física) de cada interfaz, lo cual es muy práctico a la hora de separar tipos de tráfico, o por ejemplo se puede detallar el juego de llaves necesario para acceder a una instalación. Cuanto mayor es el nivel de detalle mayor es el control que se tiene sobre los activos y más fácil resulta gestionarlos. Programar actividades de mantenimiento es mucho más fácil cuando éstas incluyen detalles como el juego de llaves necesario y el armario en el que encontrarlas, pero mantener este nivel de detalle actualizado es una tarea de enorme dificultad y por tanto lo recomendable es encontrar el equilibrio entre lo que es posible y lo que es práctico. Este punto de equilibrio determina el nivel de detalle de dicho inventario.

Modelado de servicios

La última evolución que han sufrido los inventarios es la incorporación de las vistas de servicio. En un nivel de abstracción superior al de la topología de red, podemos relacionar los

elementos que soportan un servicio concreto, como por ejemplo el servicio de datos de la operadora, incorporando al inventario el registro de los servicios y las relaciones con el equipamiento que soporta dichos servicios, se obtiene una visión muy practica para los perfiles ejecutivos de una operadora.

Estas vistas de servicios se apoyan en el CRM (*Customer Relationship Management*) de la operadora, que es la aplicación en la que se registran los datos de los clientes y los servicios que contratan los mismos. Cuando un cliente realiza un pedido a una operadora, contratando por ejemplo una línea ADSL, éste se registra en el CRM y comienza un proceso de activación. Este proceso puede implicar el despliegue de equipamiento hasta la localización del cliente. Una vez desplegado y probado el equipamiento el CRM recibe la información del equipo de red asociado al cliente (la dirección IP asignada) y emite un evento de *Ready for Service* notificando al sistema de facturación la entrada en servicio.

Mediante la integración del inventario con el CRM se incorporan vistas de servicio, de manera que el primero aporta la visión topológica de la infraestructura de red y el segundo aporta la información del servicio concreto que soporta.

Esta información puede a su vez integrarse en el sistema de gestión de fallos de manera que se obtenga una visión en tiempo real del estado de los servicios, tal como muestra la figura 4.3. Esta visión del estado de los servicios permite optimizar la respuesta del equipo de soporte de red, acelerando la respuesta ante fallos y mejorando la priorización de las intervenciones al aumentar la información sobre el impacto de los eventos que se producen en la red

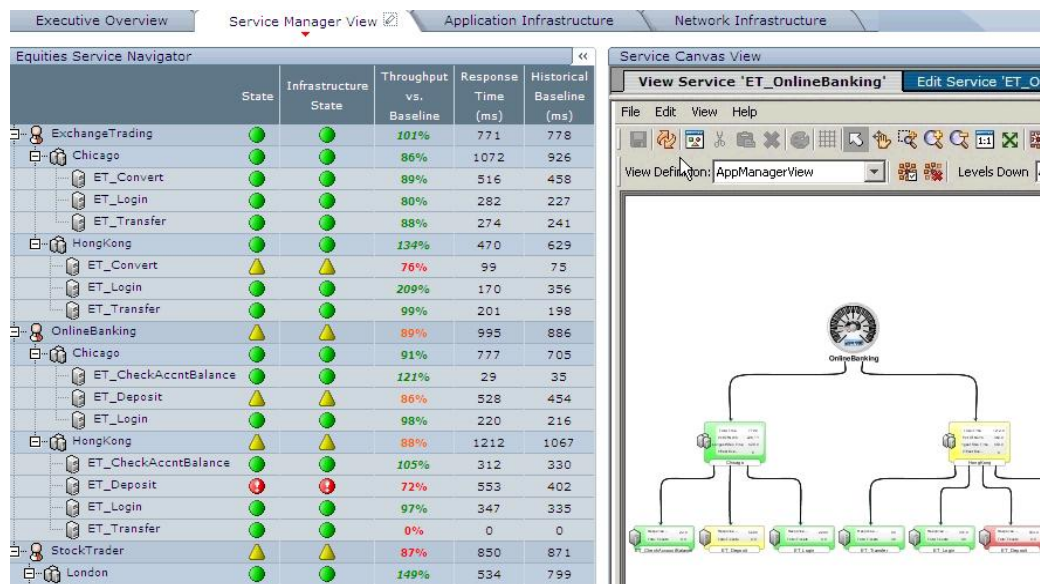


Figura 4.3 Visión de servicios dentro del sistema de gestión de fallos

4.2 Capa de consolidación

Esta capa es el núcleo del sistema de gestión de fallos y se encarga del almacenamiento de los eventos, su correlación y de la integración con otros sistemas. A continuación se describe cada una de estas funcionalidades del sistema:

Correlación de traps

Cuando un elemento monitorizado por el sistema de gestión de fallos tiene un problema, éste es notificado al mismo mediante el envío desde el elemento de un *trap* SNMP o bien es detectado por las ráfagas de interrogación SNMP que éste lanza. En ambos casos la operación se repite periódicamente de manera que la alarma aparece varias veces en el sistema. Para que esto no ocurra se realiza la correlación de alarmas, cuyo cometido es mantener en el sistema solamente una vez cada evento, con la información necesaria para saber el tiempo de duración del mismo. El repositorio será el encargado de realizar la correlación de los eventos que recibe. Los tipos de correlación que se implementarán serán los siguientes:

- Deduplicación de eventos: cada repetición de un evento no dará lugar a la presentación del mismo como un evento nuevo, sino a la actualización de un contador que se irá incrementando para recoger el número de ocurrencias de cada evento. El incremento de este contador puede tratarse en el sistema de manera que llegado un umbral el evento aumente su criticidad.
- Supresión de eventos de transición: Los eventos o alarmas de los elementos a monitorizar se definen en la MIB normalmente por parejas, indicando el evento que inicia la alarma y el que la termina. Por ejemplo, la recepción de un evento del tipo *link-up* posterior al *link-down* correspondiente dará lugar a la modificación de la severidad de ambos al valor *Clear*, que se corresponde con los problemas que han sido resueltos.

Almacenamiento de traps

El tratamiento de *traps* y eventos se realiza en primera instancia por las sondas. Éstas tienen una capacidad de almacenamiento limitada pero suficiente (unos 16 Mb) para acceder a los eventos de los últimos días. Hay que tener en cuenta que la duración temporal depende del número de eventos que se hayan producido, ya que en las sondas se almacenan sin deduplicar.

Esta información puede volcarse a fichero ASCII para su posterior almacenamiento en una unidad externa, permitiendo registrar los eventos tal como se han recibido de los equipos.

Los eventos una vez tratados y deduplicados son enviados a una base de datos relacional. Esta base de datos está destinada a almacenar la información de todos los eventos recibidos para que puedan analizarse los datos históricos y extraer conclusiones que permitan optimizar el rendimiento del sistema.

Almacenamiento y procesamiento de syslogs

Los ficheros de *syslog* permiten la monitorización de elementos mediante el análisis periódico del contenido de dicho fichero, en el que los elementos registran todos los eventos de su funcionamiento. Esto supone un problema cuando el número de elementos a monitorizar es grande y se quiere realizar una monitorización bastante precisa, reduciendo los intervalos de análisis. Por estos motivos el análisis de ficheros de log se usa normalmente para análisis forense, es decir, recopilar la máxima información sobre un evento determinado del que no se pueden determinar las causas analizando el *trap* SNMP que remitió. Pero algunos equipos es necesario monitorizarlos vía *syslog*, es el caso del *softswitch* para gestión del servicio VoIP. Este elemento vital para el servicio de VoIP, por su complejidad, debe ser monitorizado mediante el análisis de su propio fichero *syslog*.

Por lo tanto, para facilitar el análisis forense, se centralizan los mensajes de los enlaces ATM, las pasarelas de mediación, los *routers* MPLS y los *gateways* a Internet en un servidor central de *syslog* situado en la red de gestión. El servidor central de *syslog* realizará un procesamiento de estos mensajes que permitirá consultar de forma simple los eventos procedentes de cada uno de los equipos y su nivel de gravedad.

Para la monitorización del *softswitch* de VoIP se utilizará la sonda de *syslog* del sistema de gestión de fallos que analizará periódicamente dicho fichero en busca de problemas del equipo.

Todos los sistemas gestionados, excepto el *softswitch*, incorporarán agentes SNMP capaces de enviar *traps* al repositorio central de gestión ante eventos graves que deban ser tratados en tiempo real. Una vez analizados estos eventos, los operadores podrán buscar mensajes de *syslog* para determinar con más detalle qué sucesos han ocurrido en las máquinas que puedan estar relacionadas con la avería.

Los mensajes de *syslog* suelen almacenarse durante un periodo largo de tiempo (por ejemplo 7 días) ya que en algunos casos el análisis forense puede ser complejo y necesitar datos históricos para determinar tendencias en el comportamiento de la red. Sobre estos

ficheros *syslog* se realiza un purgado cíclico, y se limita el número de mensajes recibidos a un número máximo diario para no provocar desbordamientos del sistema de ficheros.

Integración con otros sistemas

Desde la capa de consolidación se implementan integraciones con otros sistemas, diferentes al de gestión de fallos, que son necesarias para que la operadora de telecomunicaciones propietaria del sistema pueda gestionar correctamente su nivel de servicio y por tanto su negocio.

El primer sistema con el que se debe integrar la gestión de fallos es el sistema de gestión de incidencias. Los eventos tratados en la capa de consolidación pueden redirigirse hacia el sistema de gestión de incidencias de forma automática, de manera que la aparición de determinados eventos provoque la apertura automática de una incidencia en dicho sistema. Para ello es necesaria la instalación de una interfaz en el sistema de gestión de incidencias asociada al repositorio de la capa de consolidación. Una vez que se soluciona el fallo y el evento es marcado como *Clear* se intercambiarán entre el sistema de gestión de fallos y el sistema de gestión de incidencias las señales necesarias para actualizar el estado de la incidencia.

Para definir la integración entre ambos sistemas es necesario determinar qué eventos van a dar lugar a la apertura de una incidencia en el sistema de gestión de incidencias y qué información debe contener dicha incidencia. Normalmente, si se ha incorporado la visión de servicios al sistema de gestión de fallos, se usará la información del servicio y cliente afectado que es la información que utiliza el sistema de gestión de incidencias. La apertura automática de incidencias desde el sistema de gestión de fallos es lo que se denomina gestión proactiva de incidencias, es decir que la operadora detecta los fallos antes de que el usuario notifique la incidencia.

El flujo puede ser unidireccional o bidireccional, dependiendo de si se quiere integrar la gestión de incidencias con la gestión de fallos de manera que el cierre de incidencias provoque la anulación de eventos. Los flujos de la integración son los siguientes:

- **Unidireccional:** cuando un evento llega al repositorio del sistema de gestión de fallos, éste conecta con el *Gateway* que permite la integración y envía la información del evento hacia el sistema de gestión de incidencias. Concretamente informa del servicio y cliente afectados por dicho evento. El

Gateway conecta con el API de acceso al sistema de gestión de incidencias y transmite la información, manteniéndose a la espera de la asignación por parte del sistema de gestión de incidencias de un identificador para la incidencia. El sistema de gestión de incidencias registra el evento como una nueva incidencia asignándole un identificador único que es remitido al sistema de gestión de fallos.

- **Bidireccional:** la integración inversa permite al sistema de gestión de incidencias notificar al sistema de gestión de fallos cuando el evento ha sido atendido por el equipo de mantenimiento. De esta forma se cierran tanto la incidencia como el evento asociado.

En la figura 4.4 se muestran los flujos descritos.

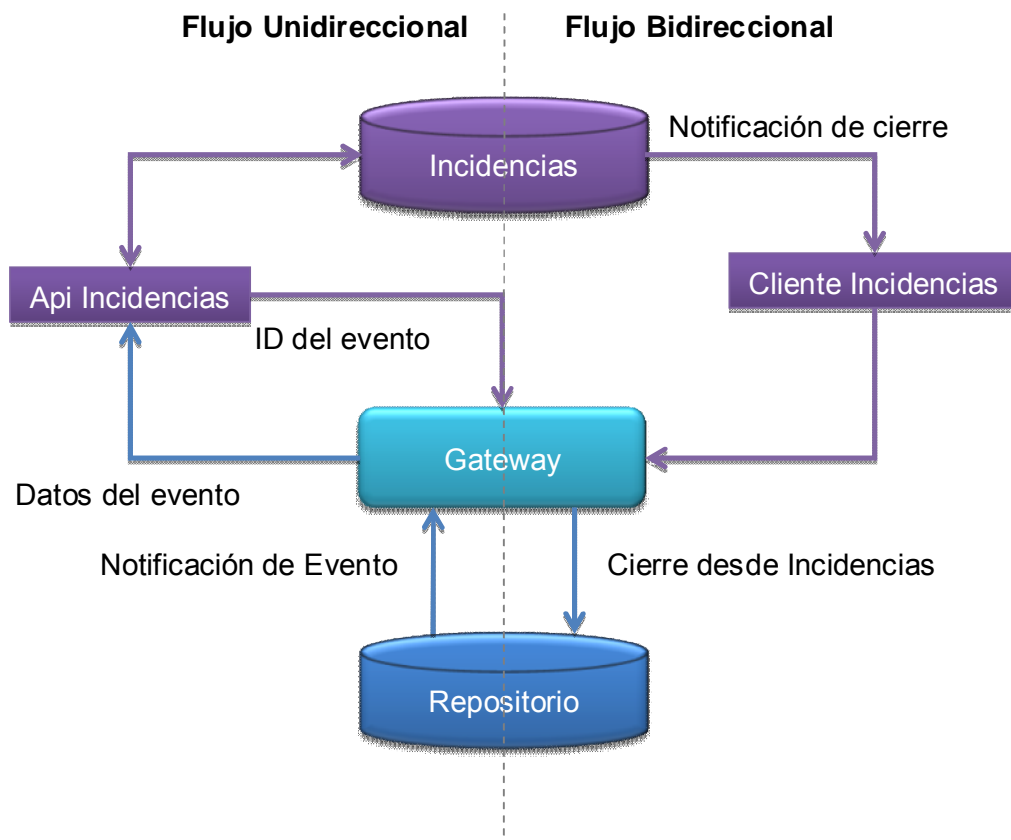


Figura 4.4 Visión Flujo de integración entre la gestión de fallos y la gestión incidencias

Capítulo 5 Gestión de rendimiento

La gestión de rendimiento (algunas veces también referida como gestión de tráfico y rendimiento) proporciona funciones para evaluar e informar sobre el comportamiento del equipamiento de telecomunicaciones y la efectividad de la red y/o elementos de red. Puede involucrar la medición de la intensidad del flujo de datos (tráfico) a lo largo de las diferentes rutas de la red, recolectando, evaluando y mostrando los datos medidos de esta forma, así como también la determinación de índices de eficiencia y el cálculo del análisis de tendencia. La información recogida y evaluada en este proceso puede ser utilizada en conexión con los datos recogidos en el campo de la gestión de fallos.

Sobre la base de estos datos, se puede establecer el nivel de carga de tráfico y se puede determinar si una red dada cumple con los requerimientos de rendimiento necesarios. (Si ocurre alguna congestión, las rutas de red sobrecargadas pueden ser aliviadas por una reconfiguración de sistema o por la alteración de la estrategia de enrutamiento actual. La intervención automática en la operación de la red puede ser ejecutada por el Sistema de Gestión de Red. Si se ha observado una carencia permanente de capacidad de red, se debería tomar la decisión para efectuar nuevas inversiones e incrementar la capacidad de red. La base de la gestión de red son los indicadores clave de rendimiento.

Los indicadores clave de rendimiento o KPIs (*Key Performance Indicator*) aplicados a redes IP son el grupo básico de datos que hay que obtener de la red para evaluar su funcionamiento. Sobre estos indicadores se pueden diseñar medidas compuestas o KQIs (*Key Quality Indicator*) que muestren el estado de los servicios, componiendo cuadros de mando que permitan controlar los acuerdos de nivel de servicio o SLAs (*Service Level Agreement*)

En la actualidad no existen herramientas estándar para la medida del rendimiento de una red IP, por lo que, hasta que se cree algún estándar consolidado, la solución implementada en la mayoría de los ISP es la utilización del protocolo ICMP. Aplicaciones como el *ping* son utilizadas para obtener RTT (*Round Trip Time*) y pérdida de paquetes entre elementos de la red (servidores, routers, etc.) El protocolo ICMP presenta algunos problemas, ya que en la mayoría de los equipos este tipo de paquetes tienen prioridad mínima y en muchos *backbones* el caudal de ICMP es limitado o incluso denegado por motivos de seguridad.

El IETF (*Internet Engineering Task Force*) tiene un grupo especial trabajando en métricas y medidas de rendimiento, que ha generado las RFC 2330, 2678, 2679, 2680, 2681 y

otros muchos borradores. En la RFC 2330 se definen los requisitos que debe cumplir un paquete de medición estándar:

- Su longitud, como en la cabecera IP, corresponderá al tamaño de la cabecera IP más el tamaño de la carga. El tamaño de la carga estará comprendido entre 0 y 65.535 bytes.
- Tendrá una cabecera IP válida: la versión IP será la 4, la longitud de la cabecera será igual o mayor que cinco bytes y el *checksum* será el correcto.
- No será un paquete IP fragmentado.
- Las direcciones origen y destino corresponderán a los equipos en cuestión.
- Dispondrá de un TTL (*Time To Live*) suficiente para ir de la fuente al destino (suponiendo un decremento de TTL de uno en cada salto) o tendrá el TTL máximo de 255.
- No tendrá opciones de IP.
- La cabecera de transporte contendrá un *checksum* válido y el resto de campos válidos.

Para la obtención de métricas se definirá el concepto de un **Paquete tipo Pö** con las siguientes características:

- Será un paquete estándar como se define en la RFC 2330
- La cabecera IP tendrá una longitud de 20 Bytes, no incluirá opciones y el TTL será de 255
- El protocolo a utilizar será el UDP, con una cabecera de 8 Bytes, utilizando el puerto 2000 como destino.
- El tamaño de los datos en el paquete (*payload*) será de 72 Bytes (16 para control del agente SAA y 56 de relleno). De esta manera la longitud del paquete IP será de 100 Bytes: 20 de cabecera IP, 8 de cabecera UDP y 72 de *payload*
- Al no existir técnicas de compresión de paquetes a lo largo de la red, los datos de relleno del paquete no serán bits aleatorios, sino que responderán al siguiente patrón: 0xABCD (1010 1011 1100 1101)

La **arquitectura del sistema de gestión de rendimiento**, tal como se muestra en la figura 5.1, se divide en las tres siguientes capas:

- **Capa de recolección:** encargada de obtener de los dispositivos de red vía SNMP o ICMP la información señalada por los indicadores. Los datos se recogen periódicamente provocando ráfagas de peticiones SNMP. En función del número de dispositivos a monitorizar y del número de datos a recoger de cada elemento será necesario incorporar más servidores para afrontar esta tarea. Dada la cantidad de

información que se puede llegar a recoger, solo almacena un espacio de tiempo reducido (1 día)

- **Capa de consolidación:** cuya función es realizar agrupaciones temporales de la información recogida por la capa de recolección, de manera que se puedan ofrecer datos de amplios espacios de tiempo. La información se promedia por horas, días, semanas, meses y años para mostrar las tendencias de los diferentes indicadores en todos los rangos temporales.
- **Capa de presentación:** encargada de ofrecer la información del sistema a diferentes perfiles de usuarios vía Web. En esta capa se diseña la información de manera que sea útil para los diferentes tipos de usuarios en función de su relación con la red.

Para completar el sistema de gestión de rendimiento es necesario un **sistema de provisión** que introduce la información de los equipos y entidades a monitorizar y un descubridor que completa esta información interrogando a los equipos vía SNMP.

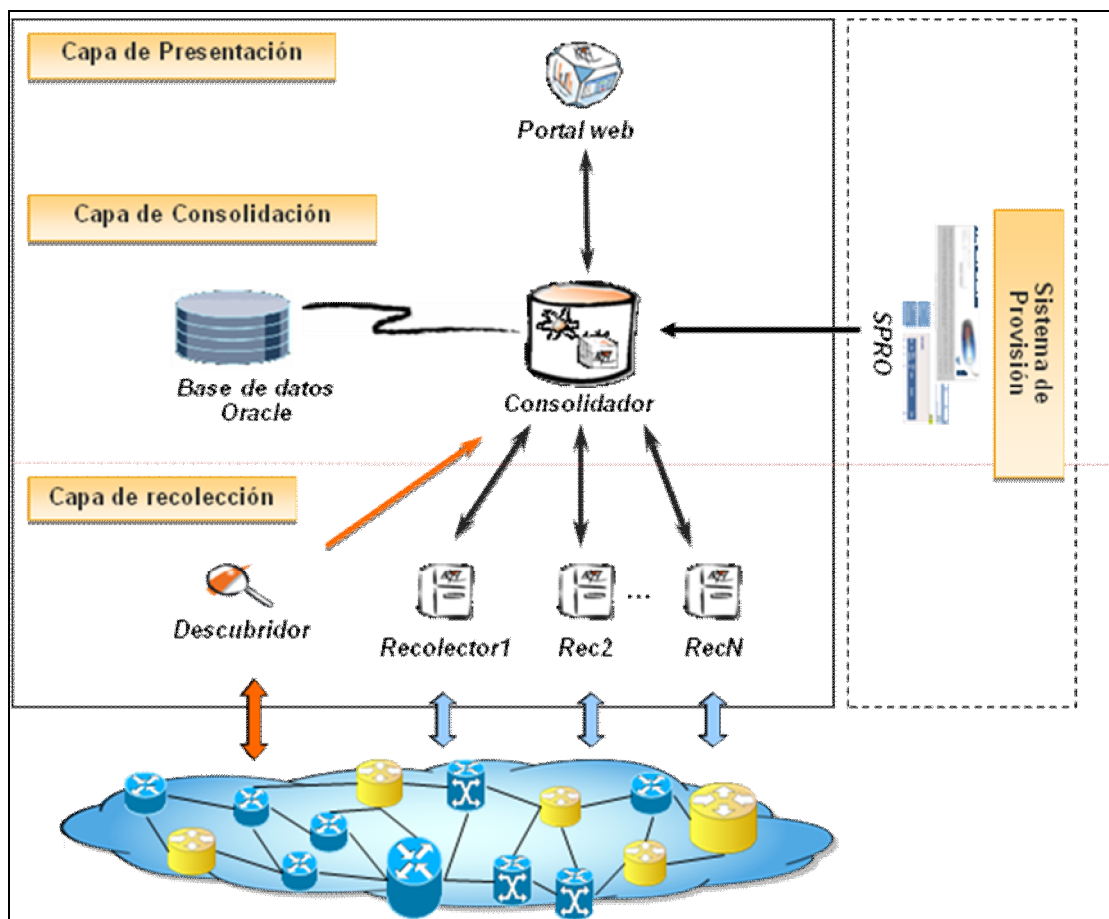


Figura 5.1 Arquitectura del sistema de gestión de rendimiento

Por último hay que tener en cuenta la dificultad que puede suponer recoger información directamente de un gran número de equipos en intervalos cortos de tiempo. Para no sobrecargar el sistema de gestión y concretamente la capa de recolección, se introduce en la red equipamiento específico para recoger parte de los datos, de manera que el sistema de gestión solo tiene que acceder a este equipamiento, y no a todos los dispositivos, para obtener esa información, tal como se muestra en la figura 5.2. Este equipamiento se llama *router de sondas* y en él se configuran procesos, llamados sondas, para interrogar a los dispositivos de red en ráfagas periódicas y almacenar la información un breve rango de tiempo en el que el sistema de gestión, a través de su capa de recolección, obtendrá dichos datos.

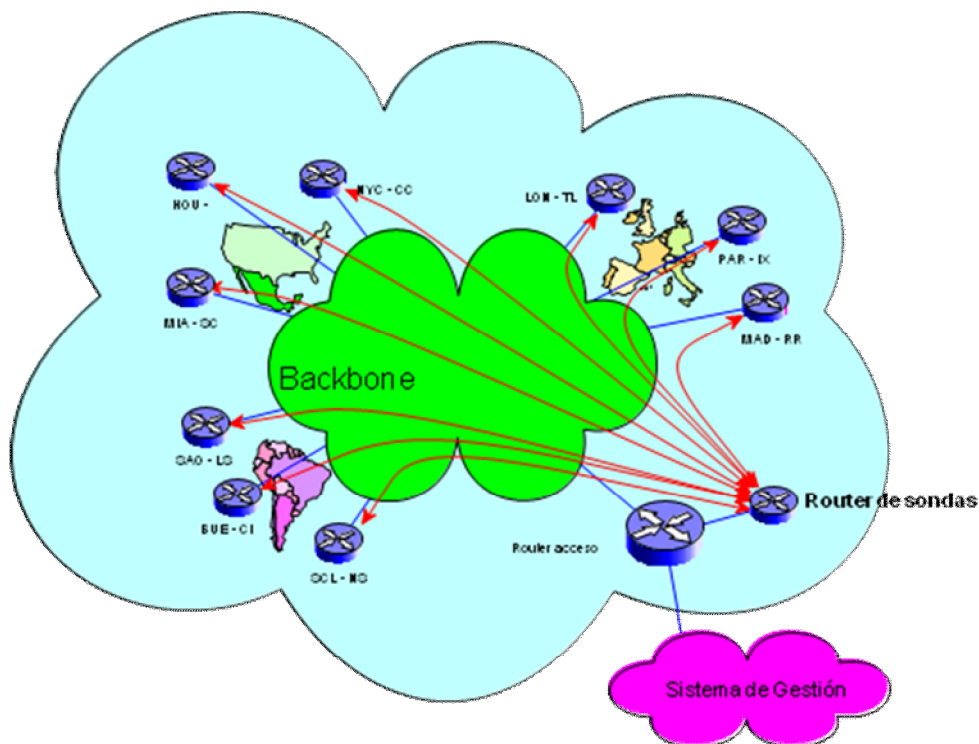


Figura 5.2 Sistema de gestión de rendimiento con *router de sondas*

5.1 Indicadores clave de rendimiento o *KPIs*

Estos conforman la base del sistema de rendimiento siendo el conjunto de medidas básico.

5.1.1 Indicadores de estado de los equipos

Dentro de las variables MIB que podemos consultar en un equipo, se pueden hacer dos grupos: por un lado las variables que necesitan de un seguimiento y representación constante, y por otro lado, las variables que dan información preventiva de eventuales fallos. Para el primer tipo de variables es conveniente hacer un *polling* estándar SNMP desde una estación

de gestión centralizada, pero para el segundo tipo, es más eficiente que sea el propio *router* el que compruebe el valor de estas variables, y que, en caso de que los valores superen cierto umbral, envíe un *trap*.

Las variables a monitorizar se pueden dividir en los tres grupos siguientes:

- Variables relacionadas con el rendimiento, como la ocupación de CPU o memoria.
- Errores de las interfaces, como los paquetes perdidos o el retardo.
- Niveles de servicio diferenciados, como la disponibilidad y el tráfico.

A continuación se describen los KPIs necesarios para gestionar el correcto funcionamiento de una red como la descrita en el Capítulo 2:

- **Porcentaje de ocupación de la CPU:** Es el porcentaje de tiempo que el procesador está ejecutando un hilo no vacío. Este contador se diseñó como indicador primario de la actividad de la CPU. Se calcula midiendo el tiempo que la CPU dedica a ejecutar el hilo vacío en cada intervalo de muestreo y restándolo al 100% (Cada CPU tiene un hilo vacío que consume ciclos cuando no se está ejecutando algún otro hilo). Este indicador muestra el porcentaje medio de tiempo de ocupación durante el intervalo de muestreo.
 - OID (*Object Identifier Descriptor*) 1.3.6.1.4.1.9600.1.1.5.1.5
- **Memoria libre:** MBytes de memoria disponible. Indica la cantidad de memoria disponible para ejecutar procesos en el equipo, en Megabytes (Bytes / 1,048,576). Se calcula sumando el espacio de memoria a cero, libre y en espera. La memoria libre es aquella que está lista para ser usada. La memoria a cero son páginas de memoria rellenas con ceros para prevenir el acceso de procesos posteriores a la información de un proceso anterior. La memoria en espera es la que acaba de liberar un proceso y cuyos datos están siendo transferidos a disco pero aún puede reinvocarse.
 - OID 1.3.6.1.4.1.9600.1.1.2.3
- **Tráfico de entrada:** número total de bytes recibidos por una interfaz.
 - OID 1.3.6.1.2.1.2.2.1.10
 - Rango: 0 a 4294967295
- **Tráfico de salida:** número total de bytes enviados por una interfaz.
 - OID 1.3.6.1.2.1.2.2.1.16
 - Rango: 0 a 4294967295

5.1.2 Disponibilidad

La disponibilidad de la red estará basada en la métrica de conectividad que se describe en este apartado:

- **Nombre de la Métrica:** Conectividad-tipo-P1-P2-en intervalo-Temporal (RFC 2678)
- **Parámetros:**
 - Src, la dirección IP del origen
 - Dst, la dirección IP del destino
 - T, instante inicial
 - dT, duración
- **Unidades:** Valor lógico
- **Definición:** La dirección Src tiene Conectividad-tipo-P1-P2-en intervalo-Temporal con la dirección Dst durante el intervalo (T,T+dT) si existen unos tiempos T1 y T2, y unos intervalos dT1 y dT2 que cumplan:
 - T1, T1+dT1, T2, T2+dT2 están todos comprendidos en [T, T+dT]
 - $T1+dT1 \leq T2$.
 - En el momento T1, Src tiene conectividad instantánea Tipo-P1 con Dst.
 - En el momento T2, Dst tiene conectividad instantánea Tipo-P2 con Src.
 - dT1 es el tiempo que tarda un paquete Tipo-P1, enviado por Src en el momento T1, en llegar a Dst.
 - dT2 es el tiempo que tarda un paquete Tipo-P2, enviado por Dst en el momento T2, en llegar a Src.
- **Metodología:**
 - Entradas:
 - Tipo P1 y P2, direcciones Src y Dst, intervalo [T,T+dT]
 - N, número de paquetes enviados como sondas para determinar la conectividad
 - W, el tiempo de espera que acota la espera para la respuesta de un paquete
 - Requerimientos: $W \leq 255$, $dT > W$
 - Valores:
 - Paquetes P1 y P2 del tipo P
 - $dT = 60$ s
 - $W = 10$ s
 - $N = 20$ paquetes

- **Algoritmo:**
 - Se calcularán N momentos de envío que estarán uniformemente distribuidos en el intervalo $[T, T+dT-W]$
 - En cada momento de envío se transmitirá desde Src un paquete correctamente implementado del tipo P hacia Dst.
 - Se inspeccionará el tráfico de entrada hacia Src para determinar si se recibe una respuesta satisfactoria. Basta con recibir una respuesta satisfactoria de los N paquetes de medida para que el valor de esta métrica sea Verdadero.
 - Si no se han recibido respuestas satisfactorias en el momento $T+dT$, el valor de la métrica será Falso.

5.1.3 Retardo de Tránsito

El retardo de tránsito de la red estará basado en la métrica de retardo que se describe en este apartado:

- **Nombre de la Métrica.-** Retardo-IdaVuelta-Tipo-P (RFC 2681)
 - **Parámetros:**
 - Src, la dirección IP del origen
 - Dst, la dirección IP del destino
 - T, tiempo
 - dT, duración
 - **Unidades:** número real de segundos (generalmente expresado en ms) o un valor indefinido (informalmente, infinito)
 - **Definición:** el Retardo-IdaVuelta-Tipo-P desde Src a Dst en un momento T es dT, cuando Src envía el primer bit de un paquete Tipo-P hacia Dst en un momento T, Dst recibe el paquete, inmediatamente envía un paquete Tipo-P hacia Src y éste recibe el último bit del paquete en un tiempo dT.
- El Retardo-IdaVuelta-Tipo-P desde Src a Dst en un momento T es indefinido (o informalmente infinito), cuando Src envía el primer bit de un paquete Tipo-P hacia Dst en un momento T, y Src no recibe el paquete de respuesta (bien porque Dst no recibe el paquete, bien porque Dst no envía el paquete de vuelta o bien porque se pierde el paquete de vuelta)
- **Metodología:**
 - Entradas:
 - Tipo-P, direcciones Src y Dst, instante T

- W, el tiempo de espera que acota la espera para la respuesta de un paquete
 - Requerimientos: $W \leq 255$
 - Valores:
 - Paquetes Tipo-P
 - $W = 10 \text{ s}$
- **Algoritmo:**
 - En cada momento T de envío, se transmitirá desde Src un paquete correctamente implementado del tipo P hacia Dst
 - Se inspeccionará el tráfico de entrada hacia Src para determinar si se recibe una respuesta satisfactoria. Al recibir la respuesta, se calculará el tiempo de tránsito y éste será el valor de esta métrica.
 - Si no se han recibido respuestas satisfactorias en el momento $T+W$, el valor de la métrica será indefinido.

5.1.4 Pérdida de paquetes

La pérdida de paquetes de la red estará basada en la métrica de descartes que se describe en este apartado:

- **Nombre de la Métrica:** Descarte-tipo-P-en intervalo-Temporal (RFC 2680)
- **Parámetros:**
 - Src, la dirección IP del origen
 - Dst, la dirección IP del destino
 - T, tiempo
- **Unidades:** El valor puede ser un número entero entre 0 y el número de paquetes enviados N.
- **Definición:** El Descarte-tipo-P1-P2-en intervalo-Temporal entre Src y Dst en el intervalo $(T, T+dT)$ es X cuando Src envía el primer bit del primer paquete de N paquetes de Tipo-P hacia Dst en un momento T y con posterioridad, Dst recibe X paquetes de respuesta.
- **Metodología:**
 - Entradas:
 - Tipo-P, direcciones Src y Dst, intervalo $[T, T+dT]$
 - N, número de paquetes enviados como sondas para determinar la conectividad.

- W, el tiempo de espera que acota la espera para la respuesta de un paquete
 - Requerimientos: $W \leq 255$, $dT > W$
 - Valores:
 - Paquetes Tipo-P
 - $dT = 60$ s
 - $W = 10$ s
 - $N = 20$ paquetes
- **Algoritmo:**
 - Se calcularán N momentos de envío que estarán uniformemente distribuidos en el intervalo $[T, T+dT-W]$
 - En cada momento de envío se transmitirá desde Src un paquete correctamente implementado del tipo P hacia Dst
 - Se inspeccionará el tráfico de entrada hacia Src para determinar si se reciben respuestas satisfactorias.
 - El valor de la métrica será el número de respuestas satisfactorias recibidas en el momento $T+dT$.

5.2 Indicadores clave de calidad

Una vez definido el conjunto básico de medidas o *KPIs* se definen sobre estos los indicadores clave de calidad o *KQIs*. Estos indicadores de calidad aportan una visión de aspectos más abstractos de la red. Concretamente aportan información de la disponibilidad en diferentes tramos de la red, de manera que ante una caída el análisis de los informes de las diferentes disponibilidades muestre el tramo que sufrió el problema. Esta acotación optimiza la respuesta que ofrece el centro de operaciones de red.

5.2.1 Disponibilidad del Core

El primer KQI muestra la disponibilidad del núcleo o *core* de la red. Para monitorizar la disponibilidad del *core* de la red, como muestra la figura 5.3, no es necesario interrogar todos los dispositivos que lo componen, basta con asegurar que los *routers* de nivel MPLS permanecen en funcionamiento.

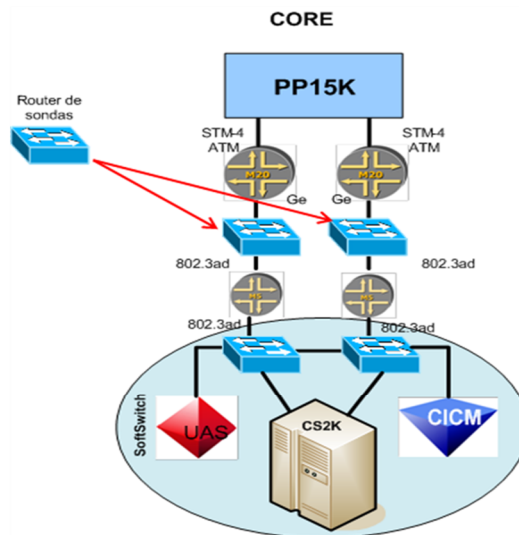


Figura 5.3 Monitorización de la disponibilidad del core.

La disponibilidad de *Core* se calculará por tanto a partir de las medidas obtenidas de las sondas *SA Agent* (*Service Assurance Agent* ó *Cisco*) que tienen como destino los *routers* de tránsito y como origen el *router* de sondas.

Formula:

$$\text{Disponibilidad de Core} = (\text{Disp-SR1}) \text{ OR } (\text{Disp-SR2})$$

Siendo los posibles valores de Disponibilidad de Core los que se muestran en la tabla de decisión 5.1:

Disponibilidad SR1	0	0	100	100
Disponibilidad SR2	0	100	0	100
Disponibilidad de Core	0	100	100	100

Tabla 5.1 Disponibilidad del core

Modelo de objetos:

El modelo de objetos muestra las entidades que utiliza el sistema de gestión de rendimiento para obtener la medida. Estas entidades se introducen en el sistema mediante el sistema de provisión.

Para monitorizar la disponibilidad del *core* el *router* de sondas interrogará a ambos *routers* de transito cada cinco minutos y almacenará dicha información. El sistema de gestión recogerá esta información, también cada cinco minutos, y la almacenará en los indicadores Disponibilidad SAA asociados a las instancias SR1 y SR2 de la vista SAA ó RTT. Finalmente en la vista SAA Group se define una instancia Core que aplica la tabla 5.1 a la

información de Disponibilidad SAA de las instancias SR1 Y SR2, tal como muestra la figura 5.4.

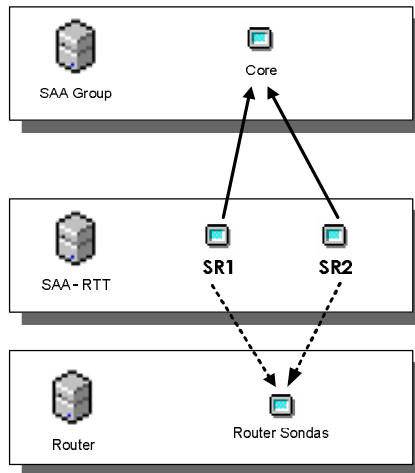


Figura 5.4 Modelo de objetos de disponibilidad del core

Indicadores:

Los indicadores de la vista SAA-RTT son indicadores básicos ya que recogen directamente un valor de la MIB de un dispositivo, en este caso el resultado del *Ping* lanzado por la sonda hacia uno de los *router* de tránsito. Estos indicadores básicos (RTBase) se agrupan en la vista SAA Group para realizar la operación, en este caso calcular el máximo, que indica la disponibilidad del *core*. Estos indicadores que se basan en operaciones sobre otros indicadores son considerados de tipo derivado (*Derived*). La figura 5.5 muestra la relación entre los indicadores.

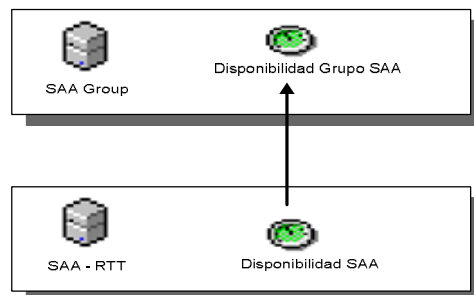


Figura 5.5 Modelo de indicadores de disponibilidad del core

Disponibilidad SAA

El indicador básico para el cálculo de la disponibilidad está definido por las propiedades que se muestran en la Tabla 5.2

Vista	SAA ó RTT
Agregación	Sum
Tipo	RTBase
Expresión	Select(100,0)using(Success > 0)

Tabla 5.2 Indicador de Disponibilidad SAA

Disponibilidad GrupoSAA

El indicador derivado para el cálculo de la disponibilidad del grupo de dispositivos que forman el *core*, está definido por las propiedades que se muestran en la Tabla 5.3

Vista	SAA Group
Agregación	Mean
Expresión	Max(Select(-Disponibilidad SAA[$SAA - RTT$])using(-Disponibilidad SAA[$SAA - RTT$]))

Tabla 5.3 Indicador de Disponibilidad del GrupoSAA

5.2.2 Disponibilidad del Backbone

La *Disponibilidad del Backbone*, como se aprecia en la figura 5.6, muestra el correcto funcionamiento del enlace entre el *core* y los nodos provinciales, es decir del funcionamiento del borde de la red ATM sobre la que trabajan el resto de los protocolos.

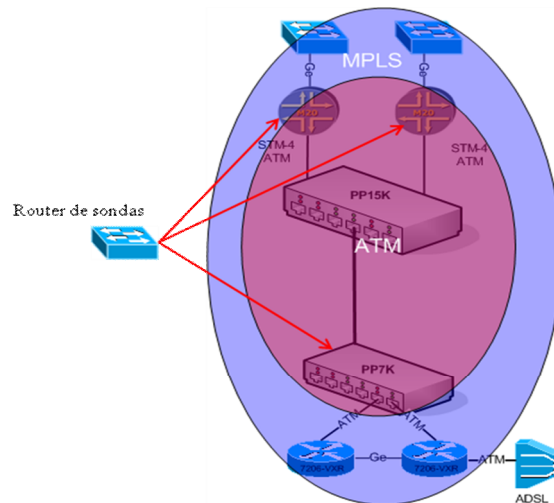


Figura 5.6 Monitorización de la disponibilidad del Backbone

Fórmulas:

Para calcular esta disponibilidad se usa el promedio de la disponibilidad de las pasarelas de mediación del *core* y del enlace ATM de cada nodo provincial. Los enlaces ATM nodales se conectan a las pasarelas de mediación M20 del *core* a través del la pasarela ATM Passport 15000 del *core*. Para obtener la medida final solo se necesitan las medidas obtenidas de las sondas SA Agent que tienen como destino los routers M20 del core y la dirección pública del enlace ATM nodal. En la tabla 5.4 se muestran los posibles valores de la disponibilidad Nodal a partir de los distintos valores de las sondas SAA.

Disponibilidad S-M20-01	0	0	100	100
Disponibilidad S-M20-02	0	100	0	100
Disponibilidad routers M20	0	100	100	100
Disponibilidad routers M20	0	0	100	100
Disponibilidad S-NODO-01	0	100	0	100
Disponibilidad Nodal NODO-01	0	0	0	100

Tabla 5.4 Disponibilidad del nodo NODO-01

Modelo de objetos:

La base para monitorizar la disponibilidad del *backbone* es de nuevo la información del *router* de sondas. En este se define una sonda (SAA RTT) para cada uno de las pasarelas de mediación Juniper M20 (S-M20-1 y S-M20-2) y otra para cada enlace ATM de cada nodo (S-Prov1, S-Prov2, S-Prov3, etc.) De manera que la disponibilidad del nodo de una región se define como se indica en la tabla 5.5, donde NODO-01 sería en este caso Prov1.

En la figura 5.7 se muestra un ejemplo de modelo de instancias, en el que se aprecia como de nuevo usando mecanismos de agrupación se consigue la información sobre el estado del *backbone*.

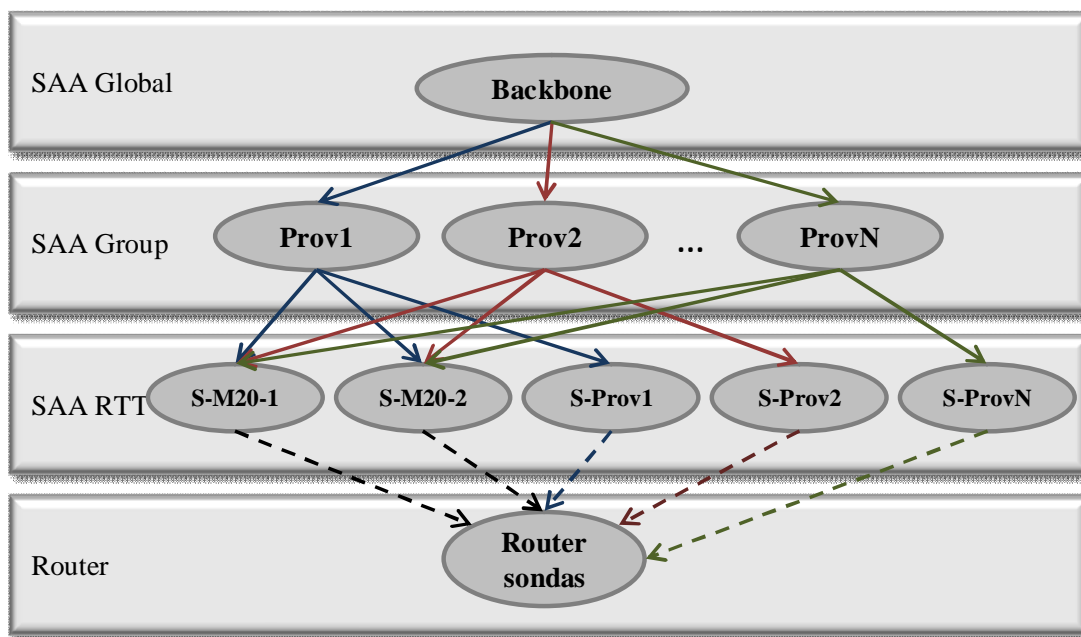
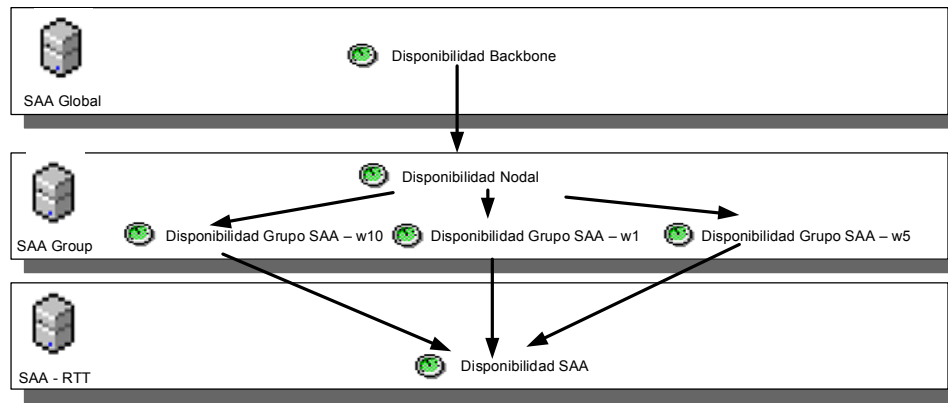


Figura 5.7 Modelo de objetos de disponibilidad del *Backbone*.

Indicadores:

Finalmente la disponibilidad del *backbone* es la media de las disponibilidades nodales de los nodos que componen dicho *backbone*. El diagrama de dependencia entre los indicadores necesarios se muestra en la figura 5.8.

Figura 5.8 Modelo de indicadores de disponibilidad del *Backbone*

Disponibilidad SAA

El indicador básico para el cálculo de la disponibilidad del *backbone* está definido por las propiedades que se muestran en la Tabla 5.5

Vista	SAA ó RTT
Agregación	Sum
Tipo	RTBase
Expresión	Select(100,0)using(Success > 0)

Tabla 5.5 Disponibilidad SAA

Disponibilidad Nodal

Agrupando indicadores básicos y aplicando el cálculo del mínimo, lo que implica que en el momento en que uno de los elementos del grupo tuviera un error el nodo estaría indisponible, se calcula la disponibilidad de cada nodo. El indicador está definido con las propiedades mostradas en la tabla 5.6.

Vista	SAA Group
Agregación	Mean
Tipo	Derived
Expresión	Min(select(¬Disponibilidad SAA∅[¬SAA RTT∅])using¬Disponibilidad SAA∅[¬SAA RTT∅]))

Tabla 5.6 Disponibilidad Nodal

Disponibilidad *Backbone*

Finalmente, agrupando en un segundo nivel los indicadores de disponibilidad nodal y aplicando el cálculo de la media, se calcula la disponibilidad del *backbone*. El indicador está definido con las propiedades mostradas en la tabla 5.7.

Vista	SAA Global
Agregación	Mean
Tipo	Derived
Expresión	Mean(select(:Disponibilidad Nodal[:SAA Group])using(:Disponibilidad Nodal[:SAA Group]))

Tabla 5.7 Disponibilidad del Backbone

5.2.3 Disponibilidad Transporte

El siguiente tramo a monitorizar corresponde a la red de transporte. Este tramo lo componen los *switches* de cada estación base LMDS, permitiendo gestionar la estación sin necesidad de acceder a los elementos de radio. La disponibilidad de transporte será el promedio de las disponibilidades individuales de las EBs (estaciones base) ó dominio de *broadcast* tal como se muestra en la figura 5.9.

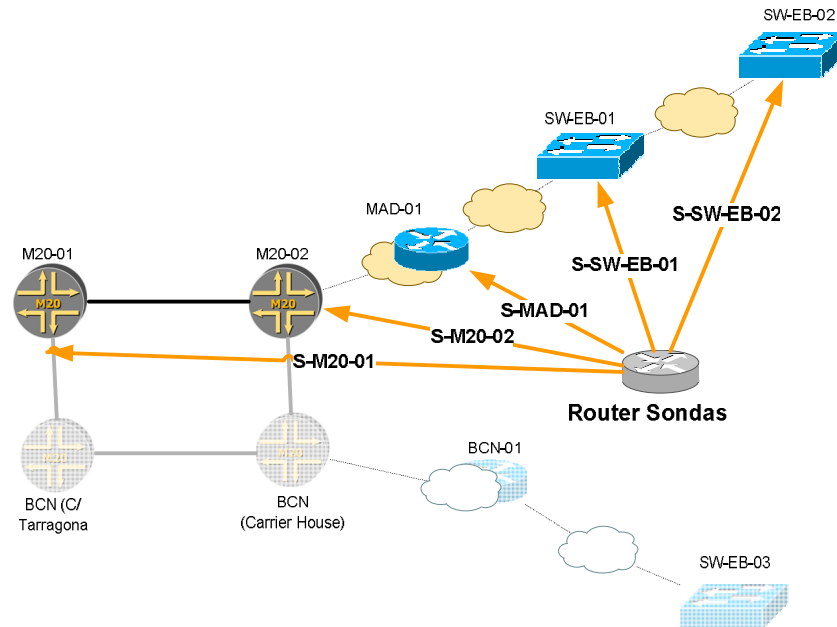


Figura 5.9 Monitorización de la disponibilidad de Transporte

Fórmula:

$$\text{Disponibilidad Transporte} = \frac{1}{N} \sum_{i=1}^N \text{Disponibilidad EB}[i]$$

Si la disponibilidad del tramo de *backbone* (disponibilidad Nodal) o de cualquier EB anterior en el camino, compuesto por los elementos que se muestran en la figura 5.10, hasta la estación a monitorizar, es nula, la disponibilidad del enlace de la EB será nula.

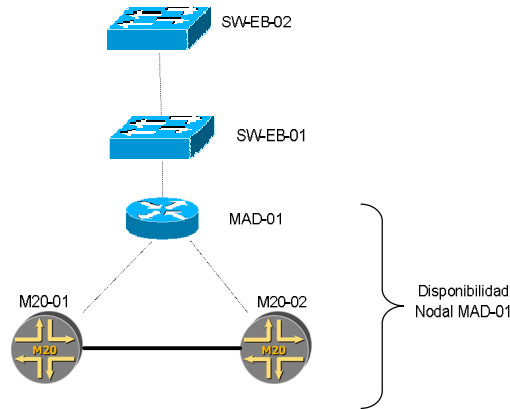


Figura 5.10 Elementos a monitorización en la disponibilidad de Transporte.

La disponibilidad nodal se calculará, tal como se explica en el apartado 5.2.2, monitorizando la disponibilidad de las pasarelas de mediación del *core* y del enlace ATM de cada nodo provincial. El resultado de la disponibilidad nodal se conjugará con la disponibilidad de cada uno de los *switches* de las EB e el camino hasta la EB a monitorizar mediante una operación AND lógica. De manera que la caída de algún elemento mostrará el camino como no disponible. La tabla 5.8 muestra los posibles valores de esta medida:

Disponibilidad S-M20-01	0	0	100	100
Disponibilidad S-M20-02	0	100	0	100
Disponibilidad routers M20	0	100	100	100
Disponibilidad routers M20	0	0	100	100
Disponibilidad S-MAD-01	0	100	0	100
Disponibilidad Nodal MAD-01	0	0	0	100
Disponibilidad Nodal MAD-01	0	0	100	100
Disponibilidad Enalces ASN (n-1)	0	100	0	100
Disponibilidad Enalces ASN (n-1) y Nodal	0	0	0	100
Disponibilidad Enalces ASN (n-1) y Nodal	0	0	100	100
Disponibilidad Enalces ASN (n)	0	100	0	100
Disponibilidad Transporte (SW-EB-02)	0	0	0	100

Tabla 5.8 Disponibilidad de transporte de la EB

Modelo de objetos:

En la figura 5.11 se muestra, mediante un diagrama de instancias, como la disponibilidad de transporte de la EB 02 depende de la disponibilidad nodal del nodo del *core*, compuesto por los elementos S-M20-01, S-M20-02 y S-MAD-01, de la disponibilidad de las EB en el camino desde el *core* hasta la EB 02, en este caso solo la EB 01 y finalmente de la disponibilidad de la propia EB, concretamente de su *switch*.

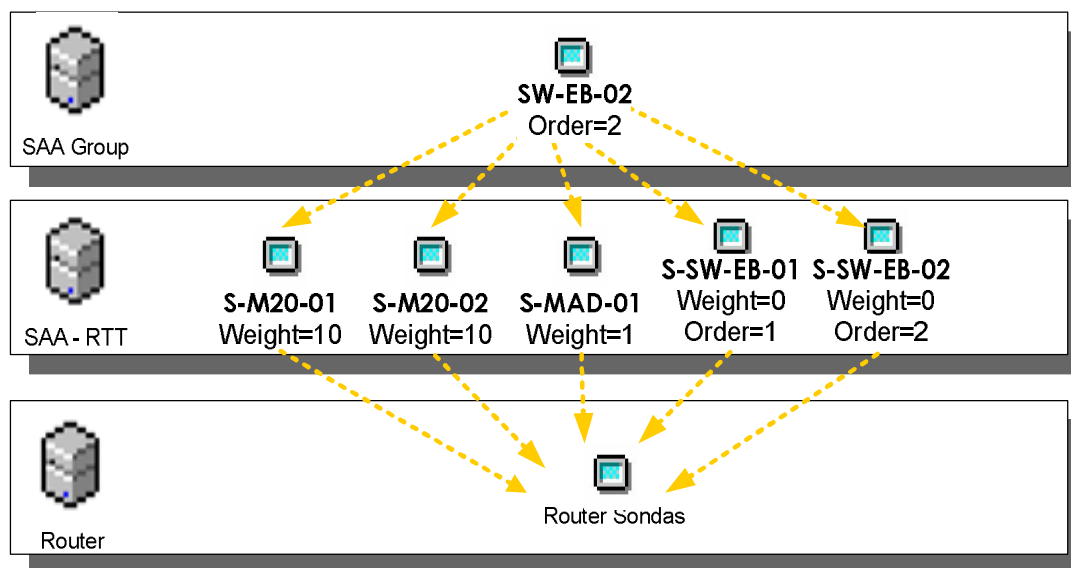


Figura 5.11 Modelo de instancias de la disponibilidad de transporte de la EB 02

Indicadores:

Los indicadores para el cálculo de la disponibilidad de transporte se relacionan en una jerarquía de manera que el proceso es recursivo. Es decir, cuando el camino hasta la EB está compuesto por varias EBs el indicador *Disponibilidad Grupo SAA(n-1)* ó *W0* incluye la disponibilidad de las EB de ese camino.

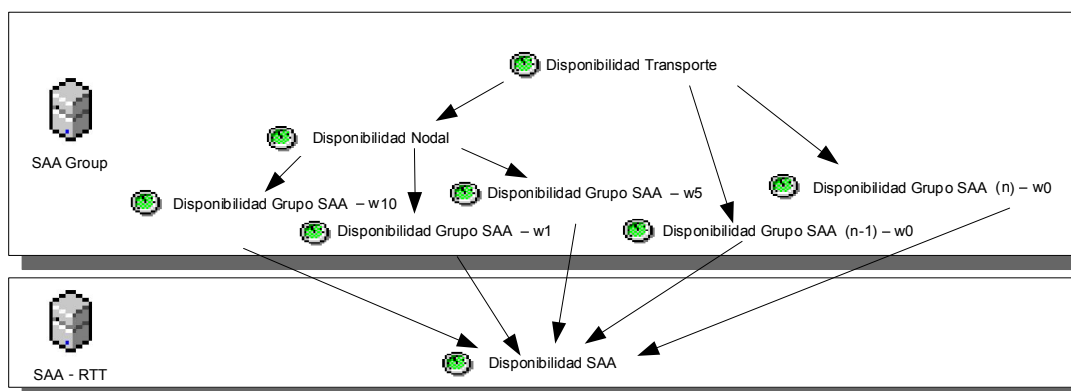


Figura 5.12 Dependencias entre los indicadores para el cálculo de la disponibilidad de transporte

Nivel SAA

Para controlar hasta que nivel del camino se está monitorizando en cada caso es necesario crear indicadores especiales, con las propiedades que se muestran en la tabla 5.9, que permiten a los indicadores jerárquicamente superiores comparar el nivel que se está analizando con el buscado.

Vista	SAA ó RTT
Agregación	Mean
Tipo	RTBase
Expresión	Property(SAA - RTT.order SAA)

Tabla 5.9 Propiedad que identifica la profundidad dentro del camino

Nivel SAA Group

La segunda parte de la comparación comentada en la definición del indicador *Nivel SAA* se aplica sobre el grupo con las propiedades que se muestran en la tabla 5.10

Vista	SAA Group
Agregación	Mean
Tipo	RTBase
Expresión	Property(SAA Group.order Group)

Tabla 5.10 Propiedad que identifica la longitud del camino hasta la EB

Disponibilidad GrupoSAA (n -1) w=0

Realizando un primer nivel de agrupamiento y aplicando la función mínimo, que implica que en el momento que algún elemento del grupo este indisponible el grupo estará indisponible, tal como se define en la tabla 5.11 se obtiene la disponibilidad del camino, sin incluir la EB final (al aplicar el operador \neg menor que \emptyset en la fórmula)

Vista	SAA Group
Agregación	Mean
Tipo	Derived
Expresion	Min(Select(\neg Disponibilidad SAA \emptyset [SAA - RTT])using(\neg Weight SAA \emptyset [SAA - RTT] = 0) and (\emptyset Order of SAA \emptyset [SAA - RTT] < \neg Order of SAA Group \emptyset)

Tabla 5.11 Disponibilidad del camino hasta la EB

Disponibilidad GrupoSAA (n) w=0

Realizando un segundo nivel de agrupamiento y aplicando la función mínimo también, que implica que en el momento que algún elemento del grupo este indisponible el grupo estará indisponible, tal como se define en la tabla 5.12 se obtiene la disponibilidad de la EB final, sin (al aplicar el operador \neg igual que \emptyset en la fórmula)

Vista	SAA Group
Agregación	Mean
Expresión	Min(Select(\neg Disponibilidad SAA \wedge [SAA - RTT])using(\neg Weight SAA \wedge [SAA - RTT] = 0) and (\emptyset Order of SAA \wedge [SAA - RTT] = \neg Order of SAA Group \emptyset))

Tabla 5.12 Disponibilidad de la propia EB

Disponibilidad Nodal

El último elemento necesario es la agrupación de las disponibilidades del *Core* y el router nodal. El indicador se define con las propiedades que se muestran en la tabla 5.12

Vista	SAA Group
Agregación	Mean
Tipo	Derived
Expresión	select(\neg Disponibilidad GrupoSAA w=1 \wedge 100)using((\neg Disponibilidad GrupoSAA w=10 \wedge 0 > 0) and(\neg Disponibilidad GrupoSAA w=5 \wedge 0 > 0))

Tabla 5.12 Disponibilidad Nodal

Disponibilidad de Transporte

Una vez definidos todos los elementos, la disponibilidad de transporte se compone de una agrupación mediante una función lógica \neg And \emptyset , lo que implica que el fallo en cualquiera de los componentes supone el fallo en la disponibilidad del transporte. El indicador para realizar el cálculo tiene las propiedades que se muestran en la tabla 5.13

Vista	SAA Group
Agregación	Mean
Tipo	Derived
Expresión	select(\neg Disponibilidad Grupo SAA (n) \wedge w0 \wedge 100)using((\neg Disponibilidad Grupo SAA (n-1) \wedge w0 \wedge 0 > 0)and(\neg Disponibilidad Nodal \wedge 0 > 0))

Tabla 5.13 Disponibilidad de Transporte

5.2.4 Disponibilidad Acceso

El siguiente tramo a monitorizar corresponde a la red de acceso. Este tramo lo componen la red de transporte y el equipamiento de radio LMDS de las EB, tal como muestra la figura 5.13. El equipamiento de radio de cada EB lo componen sectores que emiten en una dirección y ángulo concreto. En cada EB se pueden encontrar varios sectores con diferente orientación.

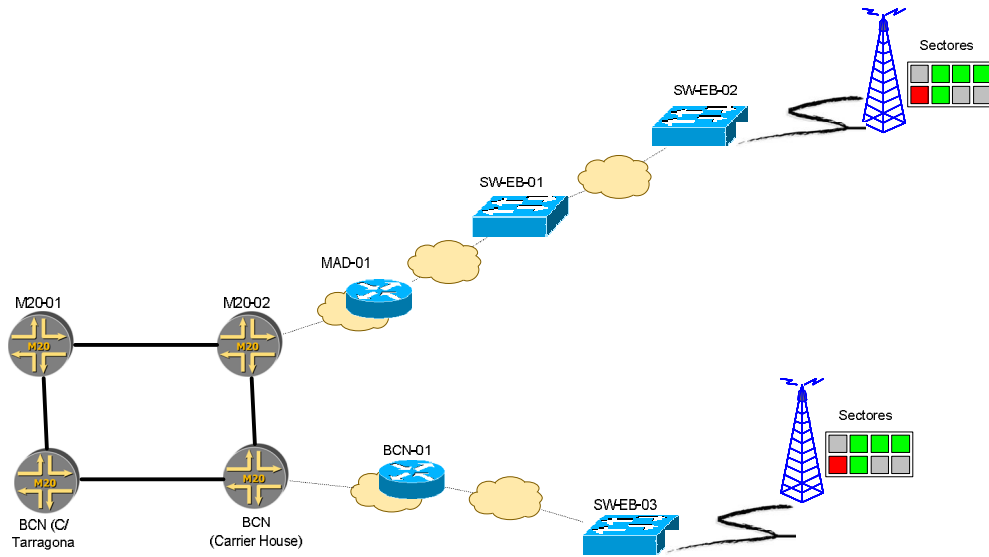


Figura 5.13 Ejemplo de red de acceso

Los sectores no incluyen sondas, de manera que para monitorizar su disponibilidad es necesario interrogar directamente a la antena vía SNMP. La medida de la disponibilidad de acceso estará entonces compuesta por la información de transporte, obtenida del *router* de sondas, y de la información obtenida directamente del sector correspondiente, tal como se muestra en la figura 5.14.

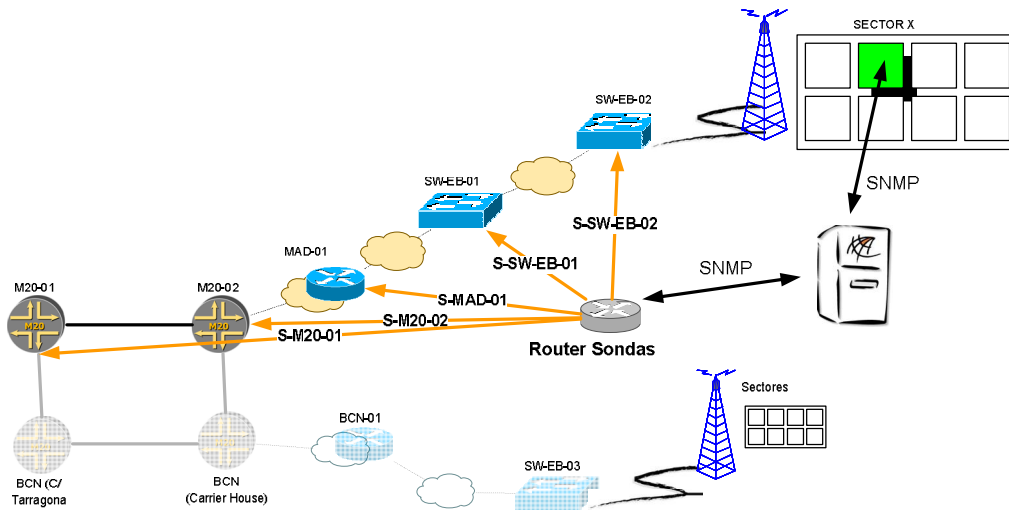


Figura 5.14 Detalle del método para medir la disponibilidad de acceso

Fórmula:

La Disponibilidad Acceso será el promedio de las disponibilidades individuales de los elementos del camino hasta el sector concreto. Esto incluye la disponibilidad nodal del nodo al que se conecta la rama completa, la disponibilidad de transporte incluyendo la del *switch* de la propia EB y el sector concreto que se esté monitorizando:

$$\text{Disponibilidad Acceso} = \frac{1}{N} \sum_{i=1}^N \text{Disponibilidad Acceso EB}[i]$$

Se calcula la **disponibilidad de Acceso EB** como el promedio de las disponibilidades individuales de los elementos de acceso a la EB, incluido el sector objeto de la monitorización:

$$\text{Disponibilidad Acceso EB} = \frac{1}{M} \sum_{j=1}^M \text{Disponibilidad elementos EB}[j]$$

De nuevo el proceso de cálculo es recursivo. Esto no implica que se esté realizando la misma interrogación varias veces. El sistema de gestión de rendimiento realiza las peticiones una sola vez y utiliza esta información para todos los indicadores que la soliciten, evitando sobrecargar tanto el propio sistema de gestión como la red.

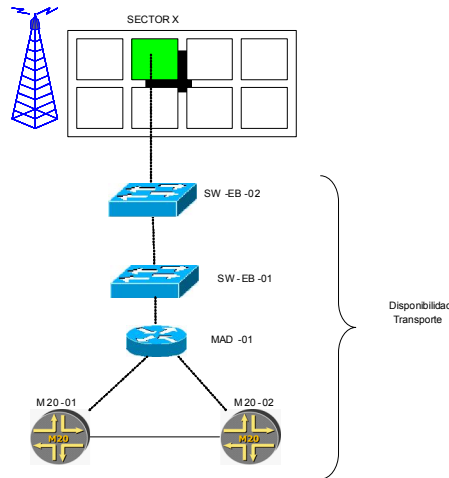


Figura 5.15 Elementos a monitorizar para medir la disponibilidad de acceso

Los valores de la disponibilidad de acceso para un caso como el que representa la figura 5.14, que comprende los electos del *core*, los elemntos del nodo, dos EB en el camino de transporte y finalmente un sector dentro de la EB, se muestran en la y tabla 5.14:

Disponibilidad S-M20-01	0	0	100	100
Disponibilidad S-M20-02	0	100	0	100
Disponibilidad routers M20	0	100	100	100
Disponibilidad routers M20	0	0	100	100
Disponibilidad S-MAD-01	0	100	0	100
Disponibilidad Nodal MAD-01	100	100	0	100
Disponibilidad Nodal MAD-01	0	0	100	100
Disponibilidad Enalces ASN (n-1)	100	0	100	0
Disponibilidad Enalces ASN (n-1) y Nodal	0	0	100	0

Disponibilidad Enlaces ASN (n-1) y Nodal	0	0	100	100
Disponibilidad Enlaces ASN (n)	0	100	0	100
Disponibilidad enlace ASN (SW-EB-02)	100	100	0	100
Disponibilidad enlace ASN (SW-EB-02)	0	0	100	100
Disponibilidad sector x	0	100	0	100
Disponibilidad de acceso Sector X	0	0	0	100

Tabla 5.14 Valores de la disponibilidad de acceso

Modelo de objetos:

En la figura 5.17 se muestra, mediante un diagrama de instancias, cómo la disponibilidad de acceso del sector x de la EB-02 depende de la disponibilidad del core, compuesto por los elementos S-M20-01,S-M20-02 y S-MAD-01, de la disponibilidad de las EB en el camino desde el *core* hasta la EB 02, en este caso solo la EB 01 y finalmente de la disponibilidad de la propia EB del sector x.

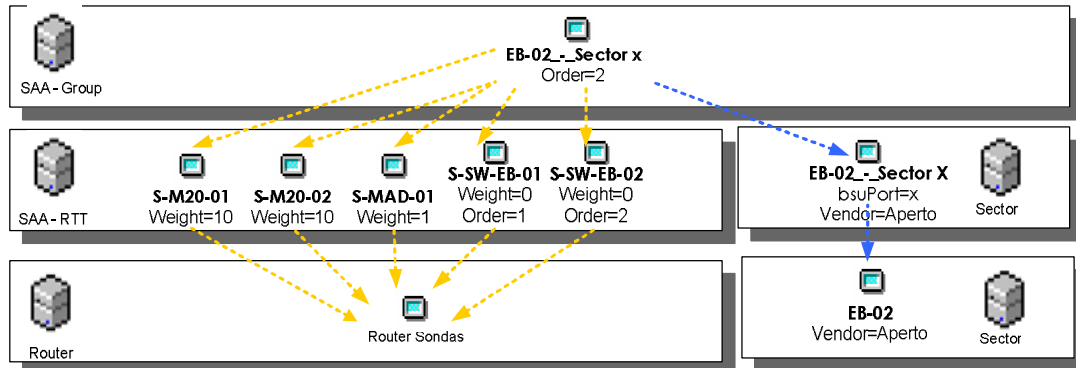


Figura 5.16 Ejemplo de modelo de instancias para la Disponibilidad de Acceso

Indicadores:

Los indicadores para el cálculo de la disponibilidad de acceso se relacionan en una jerarquía, tal como se muestra en la figura 5.18, igual que lo hacían los indicadores para el cálculo de la disponibilidad de transporte. Solo se añade al cálculo la disponibilidad del sector.

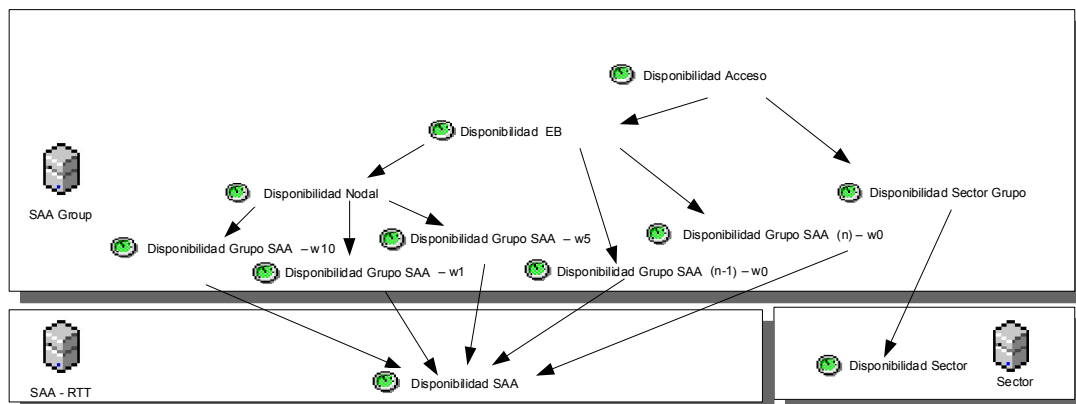


Figura 5.17 Dependencias entre los indicadores para el cálculo de la disponibilidad de acceso

Disponibilidad Sector

La disponibilidad de un sector concreto se calcula realizando una consulta SNMP directamente al sector sobre el valor `rbSlotFaultStatus` indicado en la propiedad `bsuPort` el sector que se quiere interrogar dentro de la EB. Las propiedades del indicador se muestran en la tabla 5.15.

Vista	Sector
Agregación	Mean
Tipo	RTBasic
Para Aperto	Select(100,0)using(aniBsuPortState[aniBSUWirelessPort = property(-SectorØØbsuPortØ)=6)
Para Alvarion	Select(100,0)using(rbSlotFaultStatus[rbSlotNumber = property(-SectorØØbsuPortØ)=1)

Tabla 5.15 Detalles de la disponibilidad de un sector

Disponibilidad de acceso

La disponibilidad de acceso por tanto se calcula combinando la disponibilidad de transporte de la EB y la disponibilidad del sector concreto, tal como se muestra en las propiedades del indicador en la tabla 5.16.

Vista	SAA Group
Agregación	Mean
Tipo	Derived
Expresión	select(-Disponibilidad Sector GrupoØ 100)using(-Disponibilidad Enlace ASN Ø >0)

Tabla 5.16 Detalles de la disponibilidad de acceso

5.3 Provisión del sistema de gestión de rendimiento

Para que el sistema de gestión de rendimiento pueda recoger correctamente la información y calcular los distintos indicadores, es necesario introducir en el sistema la información de los equipos de red correctamente. Esta información se registra normalmente en ficheros de texto, llamados ficheros de topología, que el sistema carga mediante una herramienta de provisión. En cada línea del fichero se reflejan las propiedades de una entidad con el formato que se detalla a continuación:

Registro: ROUTER

Es la entidad que define el router en el que se alojan las sondas base de la monitorización. Las propiedades necesarias para dar de alta este router en el sistema de gestión de rendimiento se muestran en la tabla 5.17

Ejemplo de línea en el fichero de topología: *ROUTER;Router Sondas;x.x.x.x;Public;2c*

Campo	Descripción	Ejemplo
Clave	Tipo de entidad	ROUTER
Instancia	Nombre de la instancia	Router Sondas
IP	Dirección IP del <i>router</i> de sondas	x.x.x.x
snmprd	Contraseña que autoriza al sistema de rendimiento a leer valores de la MIB del agente SNMP del dispositivo	Public
snmpversion	Versión del protocolo SNMP	2c

Tabla 5.17 Detalles de la entidad ROUTER

Registro: ESTACION-BASE

Es la entidad que define las propiedades necesarias para una estación base, tal como se muestra en la tabla 5.18

Ejemplo de línea en el fichero de topología:

ESTACION-BASE;EB-02;y.y.y.y;Public;2c;Aperto

Campo	Descripción	Ejemplo
Clave	Descripción del tipo de vista	ESTACION-BASE
Instancia	Nombre de la instancia	EB-02
IP	Dirección IP del <i>router</i> sondas	x.x.x.x
snmprd	Contraseña que autoriza al IV Server usar el protocolo SNMP	Public
snmpversion	Versión del protocolo SNMP	2c
Fabricante	Fabricante del equipo	Aperto

Tabla 5.18 Detalles de la entidad Estación Base

Registro: SAA-RTT

Es la entidad que aporta al sistema los detalles, mostrados en la tabla 5.19, de cada una de las sondas que se utilizan para monitorizar la red. Estas sondas se alojan en el router de sondas, tal como se muestra en la figura 5.19

Ejemplo de línea en el fichero de topología: *SAA-RTT;S-M20-01;Router Sondas;1;10;0*

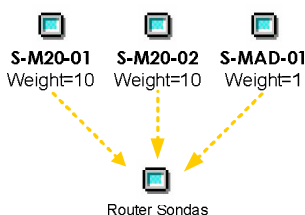


Figura 5.18 Modelo de instancias de clase sonda (SAA-RTT)

Campo	Descripción	Ejemplo
Clave	Descripción del tipo de vista	SAA-RTT
Instancia	Nombre de la instancia	S-M20-01
Referencia	Nombre del instancia (router sondas) donde se ha definido la sonda	Router Sondas
ProbeEntry	Número de sonda definida	1
Weight	Importancia del elemento destino	10
Order	Posición de elemento destino en el ramal	0

Tabla 5.19 Detalles de la entidad Sonda

Registro: SAA-GROUP

Los diferentes tramos monitorizados por el sistema, como la red de transporte, la red de acceso o el *core*, se incorporan al sistema como grupos de sondas, que a su vez han sido incluidas en el sistema como entidades SAA RTT. La figura 5.20 muestra un grupo de sondas de ejemplo, en el que el grupo MAD-01 está formado por las sondas S-M20-01, S-M20-02 y S-MAD-01.

Ejemplo de línea en el fichero de topología:

SAA-GROUP;M20-01;S- M20-01#S- M20-02#S-MAD-01;0

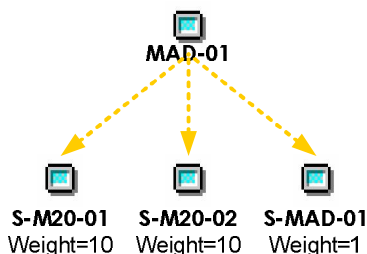


Figura 5.19 Modelo de instancias de clase grupo sondas (SAA-GROUP)

Las propiedades de la entidad se muestran en la tabla 5.20

Campo	Descripción	Ejemplo
Clave	Descripción del tipo de vista	SAA-GROUP
Instancia	Nombre de la instancia	MAD-01
Referencias	Nombre del instancias (SAA ó RTT ó sectores) que contiene el grupo	S- M20-01#S- M20-02#S-MAD-01
Order	Posición de elemento destino en el ramal	0

Tabla 5.20 Detalles de la entidad Grupo de sondas

Registro: SAA-GLOBAL

En un nivel de agrupación superior al de las entidades SAA-GROUP tenemos esta entidad SAA-GLOBAL que se utiliza en el sistema para monitorizar la disponibilidad del *Backbone*, para lo cual utiliza un grupo de grupos de sondas. Tal como muestra la figura 5.20 el *Backbone* depende de todos los nodos de la red, que están definidos como grupos de sondas.

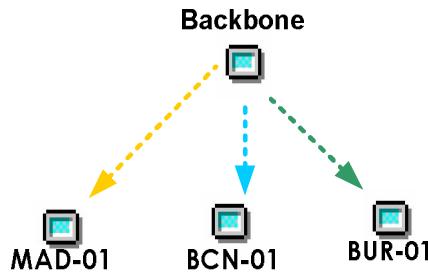


Figura 5.20 Modelo de instancias de clase grupo de grupos de sondas (SAA-GLOBAL)

Las propiedades de la entidad se muestran en la tabla 5.21, y se puede apreciar como se incluye únicamente la referencia a las instancias de grupos de sondas que componen el *backbone*.

Campo	Descripción	Ejemplo
Clave	Descripción del tipo de vista	SAA-GLOBAL
Instancia	Nombre de la instancia	Backbone
Referencias	Nombre del instancias (SAA ó Group) que contiene el grupo	BCN-01#BUR-01#MAD-01

Tabla 5.21 Detalles de la entidad Grupo de Grupos de sondas

Registro: SECTOR

Por último la disponibilidad de acceso contaba con un elemento más a tener en cuenta, el sector. En la definición de esta entidad, tal como se muestra en la figura 5.23, se tendrá en cuenta el fabricante (Campo *vendor*), ya que la manera de interrogar al dispositivo será diferente en cada caso. La propiedad que identifica el sector a interrogar es el puerto. LA definición de la entidad se muestra en la tabla 5.22



Figura 5.21 Modelo de instancias de clase grupo Sector

Campo	Descripción	Ejemplo
Clave	Descripción del tipo de vista	SECTOR
Instancia	Nombre de la instancia	BE-02_-_Sector x
Referencia	Nombre del instancia (estación base) donde está definido el sector	EB-02
bsuPort	Puerto del sector	X
vendor	Nombre del vendedor de la estación base	Aperto

Tabla 5.22 Detalles de la entidad Sector

Ejemplo de archivo de provisión:

```

ROUTER;Router Sondas;10.0.0.1;public;2c
ESTACION-BASE;EB-02;10.0.0.3;public;2c;Aperto
ESTACION-BASE;EB-01;10.0.0.4;public;2c;Aperto
SAA-RTT;S-TRAN-01;Router Sondas;1;10;0
SAA-RTT;S-TRAN-02;Router Sondas;2;10;0
SAA-RTT;S-M20-01;Router Sondas;3;10;0
SAA-RTT;S-M20-02;Router Sondas;4;10;0
SAA-RTT;S-M20-03;Router Sondas;5;5;0
SAA-RTT;S-M20-04;Router Sondas;6;5;0
SAA-RTT;S-MAD-01;Router Sondas;9;1;0
SAA-RTT;S-BCN-01;Router Sondas;10;1;0
SAA-RTT;S-BUR-01;Router Sondas;11;1;0
SAA-RTT;S-SW-EB-01;Router Sondas;12;0;1
SAA-RTT;S-SW-EB-02;Router Sondas;13;0;2
SAA-GROUP;CORE;S-TRAN-01#S-TRAN-02;0
SAA-GROUP;SW-EB-02;S-M20-01#S-M20-02#S-MAD-01#S-SW-EB-01#S-SW-EB-02;2
SAA-GROUP;MAD-01;S-M20-01#S-M20-02#S-MAD-01;0
SAA-GROUP;BCN-01;S-M20-01#S-M20-02#S-M20-03#S-BCN-01;0
SAA-GROUP;BUR-01;S-Aggr-01#S-Aggr-02#S-BUR-01;0
SAA-GLOBAL;Backbone;MAD-01#BCN-01#BUR-01
SECTORES;EB-02_-_Sector x;EB-02;x;Aperto

```


Capítulo 6 Interfaz de usuario unificada

Tras definir los elementos que componen el sistema de monitorización de la red de banda ancha descrita como escenario en el capítulo 2, solo queda por definir el interfaz con los diferentes usuarios.

Tras el despliegue de los sistemas de gestión de fallos y de gestión de rendimiento es posible acceder a los mismos por sus respectivas interfaces con el usuario. Esto implicaría que los usuarios, para acceder a ambos sistemas, tuviesen que abrir dos interfaces diferentes y buscar manualmente la información relativa a cierto evento, ya que la información permanecería desligada. Esto resta eficiencia a la operativa de ambos sistemas y ralentiza la gestión de los servicios y la red de la operadora. Para eliminar esta ineficiencia se unifican las interfaces de ambos sistemas bajo una única interfaz, tal como se muestra en la figura 6.1, de manera que todos los usuarios acceden por un mismo punto inicial.

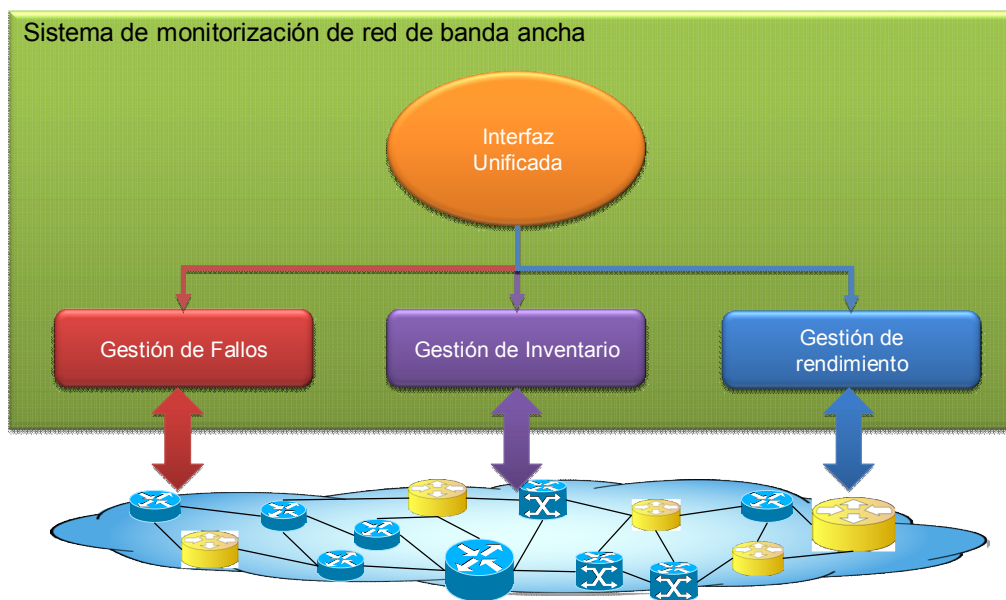


Figura 6.1 Arquitectura con interfaz unificada

Este mecanismo de unificación se llama *single sign on* y es utilizado en general en sistemas de información para minimizar las tareas de gestión de perfiles, grupos y usuarios, concentrándolas en un único sistema. Este mecanismo puede potenciarse incluyendo relaciones entre la información de los sistemas, de manera que, ante la aparición de un evento o a la hora de analizar una tendencia del sistema monitorizado, se acceda al máximo de información lo más rápido posible y desde un único punto de acceso.

La arquitectura del sistema de interfaz unificada, que se muestra en la figura 6.1, es responsable de proporcionar acceso a la siguiente funcionalidad:

- Administración de la interfaz unificada: en la que se definen los usuarios, grupos de usuarios, perfiles y permisos sobre el acceso a cada elemento de la propia interfaz y por tanto de los sistemas integrados
- Gestión del inventario: que permite consultar y corregir manualmente el inventario de equipos resultado del descubrimiento, así como definir manualmente relaciones entre entidades lógicas, como servicios y elementos físicos.
- Consola de eventos: correspondiente a la interfaz de usuario del sistema de gestión de fallos y en la que se ofrece la visión de los eventos ordenada por criticidad y la visión del estado de los servicios en tiempo real.
- Informes: soportados por el sistema de gestión de rendimiento que muestran tanto la información en rangos temporales de los indicadores claves de rendimiento, como la información histórica de los servicios y cuadros de mandos que sintetizan la información para la toma de decisiones ejecutivas.

Para responder a estas funcionalidades se utiliza tecnología web, mediante un servidor de aplicaciones en el que se implementa un grupo de páginas dinámicas sobre una base de datos en la que se almacena la información sobre usuarios y grupos de usuarios. El conjunto de páginas web solo necesita implementar enlaces a las funcionalidades implementadas en cada uno de los sistemas.

6.1 Grupos de usuarios del sistema

La función principal de la interfaz unificada es ofrecer un único punto de entrada a toda la información del sistema de monitorización de red de banda ancha para todos los usuarios del sistema. Para ello se definen los diferentes grupos de usuarios con la funcionalidad a la que necesitan tener acceso y, una vez desplegado el sistema, solo hay que crear los usuarios necesarios y asociarlos a los grupos que corresponda en cada caso.

Los grupos de usuarios recomendados son los siguientes:

6.1.1 Administradores

Los usuarios administradores son aquellos con permisos sobre el sistema para realizar las siguientes tareas:

- Crear usuarios nuevos en el sistema

- Asignar y retirar permisos a los usuarios existentes
- Eliminar usuarios
- Crear nuevos grupos de usuarios
- Asignar y retirar usuarios a los grupos
- Revisar los logs del sistema para comprobar el estado del mismo o analizar posibles fallos

A este grupo de usuarios pertenecerá el equipo de mantenimiento de sistemas y aplicaciones de la operadora.

6.1.2 Provisionadores

El grupo de usuarios provisionadores es el responsable de gestionar el inventario, asegurando en todo momento que la información contenida en el mismo refleja exactamente la red tal como está desplegada.

Cualquier error en el inventario provoca la aparición de datos erróneos en todo el sistema, tales como alarmas o fallos en equipos desconocidos, desviaciones en los datos de los informes de rendimiento a todos los niveles, etc. El inventario, al contener la información sobre la que funciona el resto del sistema, es crítico y marca la diferencia entre una gestión efectiva o la imposibilidad de responder ante cualquier problema.

Las funciones que realizan los usuarios de este grupo son las siguientes:

- Consultar la información de los elementos del inventario.
- Introducir nuevos elementos en el inventario. Esta función solo debería usarse en caso de fallo del sistema de descubrimiento incorporado en el sistema de gestión de fallos, que es el responsable de introducir automáticamente en el inventario la información necesaria.
- Eliminar elementos del inventario. Aunque el inventario debe reflejar únicamente la información que indique el sistema de descubrimiento, hay conjuntos de elementos de los que no se necesitan todos los elementos. Por ejemplo, el descubrimiento introducirá en el inventario la información sobre todas las interfaces de cada elemento, pero no en todas se conectarán otros equipos, es decir, normalmente no están en uso todas las interfaces de todos los elementos de la red, por lo que no es necesario sobrecargar el inventario con información que no se usará en el sistema.
- Modificar la información del inventario. Esta función, al igual que la introducción manual de nuevos elementos, solo tendrá carácter temporal, ya que toda modificación manual realizada será sobrescrita por el siguiente

descubrimiento. Por lo tanto esta función solo se utiliza para corregir temporalmente el inventario hasta intervenir sobre el equipo que contiene el error en su configuración y se subsana el mismo.

A este grupo de usuarios pertenecerán miembros del equipo de provisión de la operadora. Dicho equipo es el responsable de la correcta configuración de los equipos desplegados en la red, siguiendo la definición realizada por el equipo de ingeniería de red.

6.1.3 Operadores de red

La funcionalidad principal del sistema de monitorización de red de banda ancha es la monitorización de fallos, esta funcionalidad está dirigida a los operadores de red. El centro de operación de red es el responsable de la disponibilidad de los servicios que soporta la red y para ello necesita tener visibilidad en tiempo real del estado de todos los elementos de la red a través de una interfaz sencilla y que además permita la intervención sobre dichos elementos para corregir los fallos que provocan errores.

La interfaz que cumple con esos requisitos de sencillez, claridad y potencia a la hora de intervenir es la consola de fallos. Esta consola muestra, como se puede apreciar en la figura 6.2, los fallos activos de la red. Mediante un código de colores se facilita al operador la identificación de la severidad de cada error.

Node	Count	Last Occurrence	First Occurrence	
NYCMLIT1630-T3T	2	12/10/97 07:40:22	12/10/97 07:40:22	Incoming YEL Carrier Group Alarm
NYCMLIT1630-T3T	2	12/10/97 07:40:23	12/10/97 07:40:23	Incoming YEL Carrier Group Alarm
NYCMLIT1630-T3T	2	12/10/97 07:40:23	12/10/97 07:40:23	Incoming YEL Carrier Group Alarm
NYCMLIT1630-T3T	2	12/10/97 07:40:23	12/10/97 07:40:23	REPT INFORMATION
NYCMLIT1630-T3T	3	12/10/97 07:41:44	12/10/97 07:40:32	REPT INFORMATION
NYCMLIT1630-T3T	4	12/10/97 07:40:35	12/10/97 07:40:34	Incoming YEL Carrier Group Alarm
NYCMLIT1630-T3T	2	12/10/97 07:40:46	12/10/97 07:40:34	Controlled Slip Seconds
NYCMLIT1630-T3T	2	12/10/97 07:40:34	12/10/97 07:40:34	Incoming RED Carrier Group Alarm
SomePDSDev	1	12/10/97 07:40:34	12/10/97 07:40:34	ALM MJ BER NPC 0290
SomePDSDev	1	12/10/97 07:40:35	12/10/97 07:40:35	AR01 MISC ALM MJ CGA 0844 A
SomePDSDev	1	12/10/97 07:40:35	12/10/97 07:40:35	ALM MN BER NPC 0853
SomePDSDev	1	12/10/97 07:40:35	12/10/97 07:40:35	ALM MN BER NPC 0916
SomePDSDev	1	12/10/97 07:40:35	12/10/97 07:40:35	ALM MN BER NPC 0908
ATLNLIT5500-PM1	1	12/10/97 07:40:35	12/10/97 07:40:35	Internal Hardware Failure
SomePDSDev	1	12/10/97 07:40:36	12/10/97 07:40:36	ALM MJ BER NPC 0948
SomePDSDev	2	12/10/97 07:40:38	12/10/97 07:40:37	ALM MJ BER NPC 0584
ATLNLIT5500-0554	2	12/10/97 07:40:38	12/10/97 07:40:37	Yellow Signal
SomePDSDev	2	12/10/97 07:40:38	12/10/97 07:40:37	AR01 MISC ALM MJ CGA 0584 R
SomePDSDev	1	12/10/97 07:40:38	12/10/97 07:40:38	ALM MN SLIP NPC 0584
ATLNLIT5500-0723	2	12/10/97 07:40:38	12/10/97 07:40:38	Yellow Signal
SomePDSDev	1	12/10/97 07:40:38	12/10/97 07:40:38	ALM MN SLIP NPC 0280
NYCMLIT1630-T3T	2	12/10/97 07:40:46	12/10/97 07:40:39	Controlled Slip Seconds
SomePDSDev	1	12/10/97 07:40:39	12/10/97 07:40:39	ALM MJ BER NPC 0781
NYCMLIT1630-T3T	1	12/10/97 07:40:39	12/10/97 07:40:39	REPT INFORMATION
ATLNLIT5500-0999	4	12/10/97 07:40:50	12/10/97 07:40:41	Alarm Indication Signal
ATLNLIT5500-0378	4	12/10/97 07:40:52	12/10/97 07:40:42	Yellow Signal
ATLNLIT5500-0250	2	12/10/97 07:40:42	12/10/97 07:40:42	RED

Figura 6.2 Consola única de fallos

La interfaz para cualquier operador de red facilita al máximo su trabajo, que es crítico para el negocio, incorporando en la pantalla de inicio del sistema filtros, como muestra la figura 6.3, aplicados sobre los fallos activos del sistema de manera que solo le sean mostrados aquellos en los que debe intervenir. De esta manera se organiza el equipo de un centro de operaciones de red, dividiendo los fallos entre los operadores para que cada cual atienda aquellos para los que está más cualificado por su formación.

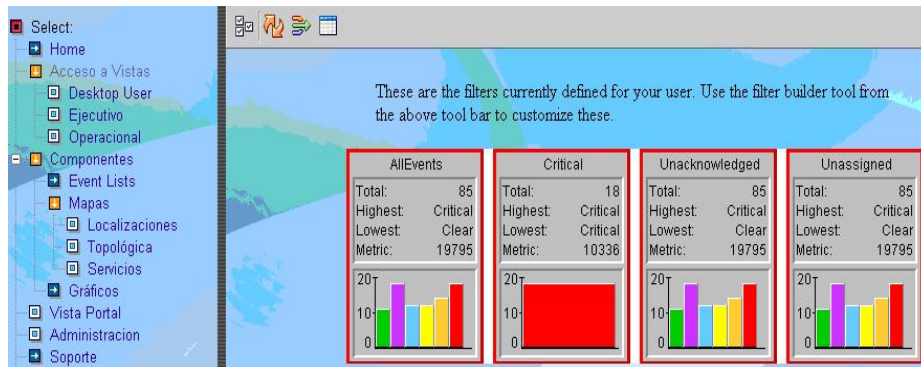


Figura 6.3 Vistas para operadores de red

Al acceder al sistema el operador decide sobre que grupo de fallos va a trabajar y al seleccionar la vista correspondiente accede a la consola que le muestra los fallos de esa vista. Cuando identifica un fallo y quiere intervenir, directamente desde la consola accede a una interfaz de la configuración SNMP del elemento, tal como muestra la figura 6.4, y modifica las propiedades que provocan el error.

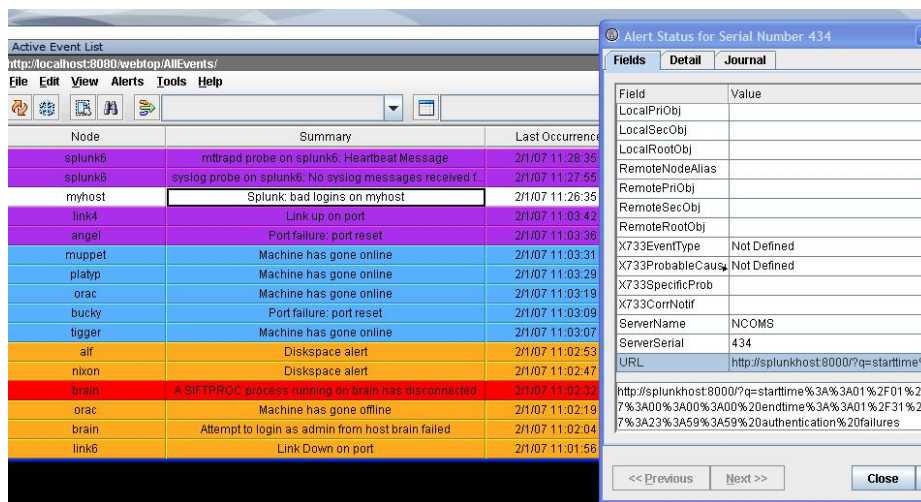


Figura 6.4 Acceso a la interfaz SNMP de un elemento desde una alarma.

Si el operador necesita más información sobre una alarma en concreto, puede acceder al sistema de gestión de rendimiento, tal como muestra la figura 6.5, ya que en la interfaz única se integra el acceso entre los sistemas donde sea necesario. El sistema de rendimiento aportará los datos históricos sobre el comportamiento del elemento. Con el estudio de las tendencias de estos datos, en un plazo anterior a la aparición del fallo, el operador podrá concluir qué lo ha provocado y solucionarlo.



Figura 6.5 Acceso al sistema de rendimiento desde la consola de alarmas

Finalmente, la interfaz del sistema de gestión de fallos incluye una vista global de alto nivel, dirigida al responsable del centro de operaciones de red, que permite de un rápido vistazo, obtener una idea del estado de la red y de los servicios que está prestando, permitiéndole priorizar las intervenciones de su equipo en función de la criticidad de los fallos y de las necesidades del negocio. Para obtener esta vista se incorporó al inventario un sistema de relaciones entre los equipos o elementos de red, resultado del proceso de descubrimiento, y entidades lógicas que representan los servicios. Evidentemente estas entidades lógicas no pueden ser descubiertas por el sistema y son introducidas manualmente, el máximo nivel de automatización al que se puede llegar consiste en la integración entre el sistema de CRM (*Customer Relationship Management*) en el que se introducen los servicios contratados por cada cliente, y el inventario. En esta integración es necesaria la intervención de un operador que relacione cada servicio con los equipos del inventario que lo soportan.

Esta vista marca la evolución de los sistemas de gestión, que han pasado de ser simplemente gestores de equipamiento a convertirse en gestores de servicios, permitiendo a

los directivos de la compañía alinear el nivel de servicios prestados con los objetivos estratégicos del negocio, a través de cuadros de mandos como el que muestra la figura 6.6.

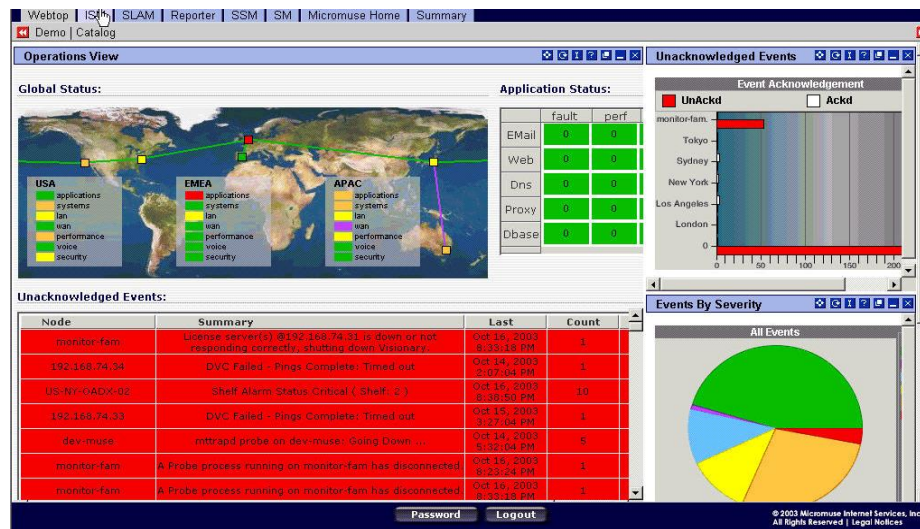


Figura 6.6 Vista de nivel del servicio

El cuadro de mandos que aporta el sistema de gestión de fallos muestra el estado actual de los servicios, pero no incorpora una visión histórica que es necesaria para mantener acuerdos de nivel de servicio. La visión histórica es aportada por el sistema de gestión de rendimiento, tal como se explica en el apartado 6.1.4.

6.1.4 Usuarios de informes

El último grupo de usuarios a definir abarca varios perfiles que realizan tareas diferentes dentro de la operadora, utilizando distinta funcionalidad del sistema de gestión de rendimiento.

El primer perfil corresponde a los usuarios operadores. Como se ha visto en el apartado 6.1.3, los operadores de red necesitan acceder a la información relacionada con las alarmas activas desde la consola de fallos y el responsable del área necesita acceder al cuadro de mandos del estado de las incidencias o fallos para controlar el acuerdo de nivel de servicio que ha adquirido con las áreas de negocio de la compañía. Este perfil implementa un puente entre la gestión de fallos y la gestión de rendimiento permitiendo el análisis forense de los fallos y su rápida resolución.

El siguiente perfil usuario de los informes de la plataforma de gestión de rendimiento corresponde al personal de planificación de red. La responsabilidad de esta área de la operadora es determinar el crecimiento de la red para soportar la creciente demanda de servicios y calidad de los usuarios. Para ello necesitan analizar los informes de disponibilidad de los diferentes tramos de la red para identificar los puntos que están soportando una carga superior a la planificada y programar ampliaciones que mejoren el servicio disminuyendo el tiempo de indisponibilidad. Una vez alcanzado un nivel adecuado de rendimiento de la red el análisis del área de planificación pasa a ser predictivo, mediante el estudio de la evolución del tráfico de entrada y salida de las interfaces de la red. Tal como muestra la figura 6.7, pueden adelantarse a los fallos por sobrecarga programando actualizaciones del equipamiento o reconfiguraciones del enrutamiento. En este análisis predictivo es básico la acumulación de información histórica de los distintos sectores de la red, de manera que aumentos temporales en algunos sectores, como la mayor demanda estival en zonas turísticas, estén contempladas.

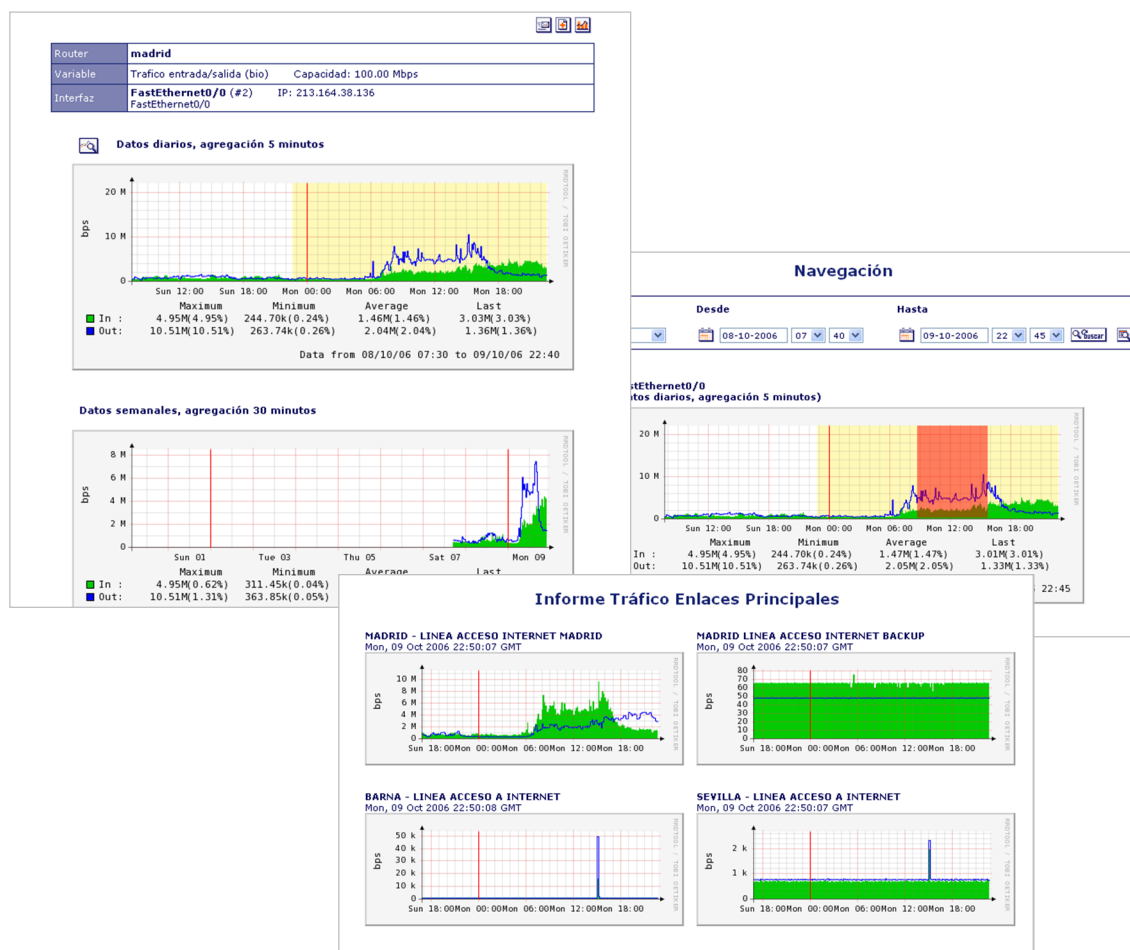


Figura 6.7 Informes para usuarios de planificación

Dentro de la propia operadora es muy importante que la ejecutiva de la compañía reciba información sobre el rendimiento de la red en un formato adecuado para facilitar la toma de decisiones. Para ello el sistema de gestión de rendimiento ofrece cuadros de mandos con resúmenes de la información de rendimiento que permiten a la dirección de la compañía valorar la correcta adjudicación de presupuestos a áreas concretas. La información de estos cuadros de mandos muestra el nivel de los diferentes servicios, tal como muestra la figura 6.8, acumulando la información histórica de los distintos tramos de la red para cada cliente.



2007 - Web based Integrated Management

Figura 6.8 Cuadro de mandos

Una vez que la plataforma de gestión esta funcionando a pleno rendimiento, se ofrece como servicio de valor añadido para los clientes importantes, grandes compañías con un alto grado de contratación que supone un porcentaje importante de la facturación de la operadora, acceso a informes sobre la calidad del servicio que se les presta. Esto incluye acceso a la información de disponibilidad y tráfico, tal como muestra la figura 6.9. De esta manera los clientes pueden controlar fácilmente que están recibiendo la calidad de servicio que han contratado.

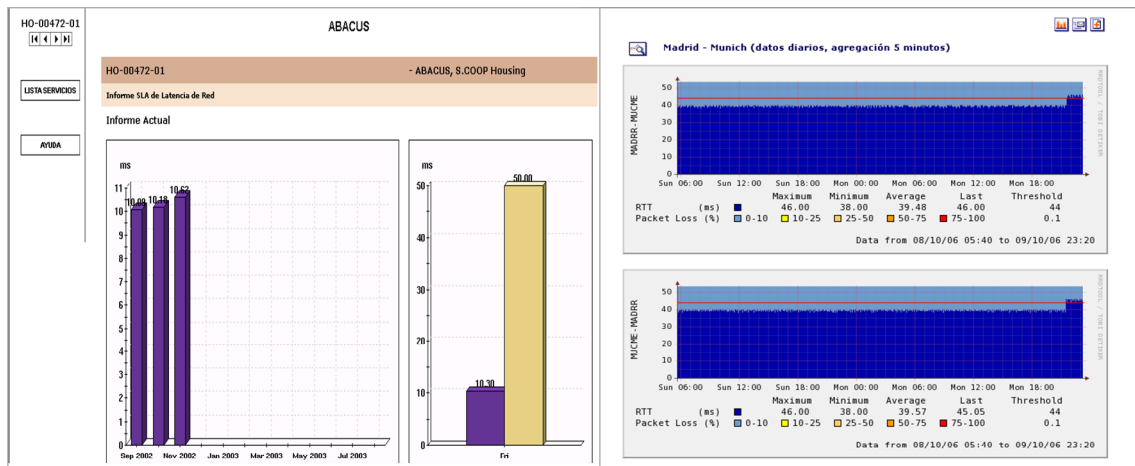


Figura 6.9 Informes para clientes

Capítulo 7 Conclusiones

Como se ha explicado desde la introducción de esta memoria, las comunicaciones soportan hoy día la mayoría de negocios, habiéndose convertido en un activo importante y estratégico para cualquier compañía, especialmente para aquellas dedicadas a ofrecer servicios de telecomunicación que siempre han tenido en cuenta que su principal activo es su red, pero igualmente se han visto obligadas a aumentar la variedad y calidad de los servicios prestados ante una feroz competencia del sector y una fuerte demanda por parte de los usuarios.

El desarrollo de las redes como soporte para acelerar los procesos de negocio ha impulsado iniciativas para mejorar el control de las mismas y asegurar un nivel de servicio adecuado a las necesidades de las compañías. Las áreas responsables del mantenimiento y operación de la red, los centros de operación de red, han contado con el apoyo de los fabricantes de equipos de red y las instituciones que han respondido a la necesidad de facilitar el control y gestión de la red, adoptando como estándar el protocolo SNMP del conjunto de protocolos TCP/IP. El ISO aportó además un modelo de referencia funcional en la serie de recomendaciones M.3000 del ITU/T en las que se definen las áreas necesarias de la arquitectura lógica, incluyendo todas las funciones genéricas, dentro del espacio de los sistemas de soporte a la operación. Estas funciones son las siguientes:

- Gestión de Fallos
- Gestión de la Configuración
- Gestión de Administración o contabilidad
- Gestión del Rendimiento
- Gestión de la Seguridad

De estas funciones, la base para la monitorización del estado de la red lo componen las funciones de gestión de fallos y gestión de rendimiento. Los otros tres grupos de funciones cubren el resto de aspectos fundamentales para la operación de red.

Para explicar cómo se aplica en un caso real la arquitectura lógica definida en las recomendaciones citadas, se ha definido un escenario correspondiente a una operadora de telecomunicaciones que ofrece a sus usuarios los siguientes servicios:

- **DATOS:** acceso a Internet y VPN

- **VOZ IP:** voz sobre protocolo de Internet, también llamado Voz sobre IP, VozIP, VoIP (por sus siglas en inglés), o Telefonía IP

Para ofrecer estos servicios en un área geográfica extensa, como por ejemplo toda España, se necesita una topología compuesta por las siguientes capas:

- **Núcleo o *core*:** es el centro de la topología en estrella de la red nacional.
- ***Backbone*:** es el núcleo de cada una de las subdivisiones del territorio al que se va a dar cobertura.
- **Acceso o bucle de abonado:** abarca los elementos que soportan los enlaces de telecomunicaciones entre los usuarios finales y el *backbone* de su demarcación geográfica.
- **Equipos de cliente o CPE (*Customer Premises Equipment*):** es el equipamiento localizado en el lado del cliente y que se encuentra conectado directamente con el bucle de abonado.

La arquitectura completa de la red consta de una base de transporte ATM sobre la que se despliega una red MPLS que une los *backbones* con el *core* y una red LMDS, con tecnología de radio, de acceso hasta los clientes.

Una vez definido el escenario podemos explicar los componentes necesarios para monitorizar dicha red, comenzando por la tecnología en la que se basa la solución, es decir el protocolo SNMP. Este protocolo de la familia TCP/IP se basa en los siguientes componentes:

- Dispositivos administrados
- Agentes
- Sistemas administradores de red o NMS (*Network Management Systems*)

Estos componentes se despliegan en una arquitectura cliente servidor, donde los agentes instalados en los elementos de red funcionan como clientes y los sistemas administradores como servidores. El agente tiene acceso a toda la información del elemento en el que está instalado y los sistemas administradores pueden recopilar esta información para ponerla a disposición de los operadores de red.

El protocolo SNMP consta tan solo de las siguientes cuatro operaciones:

- Lectura
- Escritura
- Notificación

- Operaciones transversales

Las cuatro operaciones actúan sobre la MIB de cada elemento, que es una colección de información que está organizada jerárquicamente, aplicando la notación de sintaxis abstracta número 1 (*Abstract Syntax Notation One, ASN.1*)

Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar e intercambiar los siguientes mensajes:

- *GetRequest*: solicita al agente el valor de un objeto mediante su nombre.
- *GetNextRequest*: una vez que usado el mensaje *GetRequest* para recoger el valor de un objeto, puede ser utilizado el mensaje *GetNextRequest* para repetir la operación con el siguiente objeto de la tabla.
- *SetRequest*: utilizado por el NMS para solicitar a un agente modificar valores de objetos.
- *GetResponse*: usado por el agente para responder un mensaje *GetRequest*, *GetNextRequest*, o *SetRequest*
- *Trap*: es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración
- *GetBulkRequest*: a través de un solo mensaje permite solicitar la totalidad de una tabla.
- *InformRequest*: usado por un NMS para notificar a otro NMS información sobre objetos administrados.

Con esta base tecnológica es posible definir un sistema de gestión de fallos que abarca el conjunto de funciones que detectan, aíslan y reparan los problemas de una red de telecomunicaciones, manteniendo y examinando los registros de error, recogiendo las notificaciones y actuando para corregirlos, trazando e identificando los errores, realizando las secuencias de pruebas de diagnóstico e informando de las condiciones de fallo.

La arquitectura de un sistema de gestión de fallos consta de las siguientes tres capas:

- Capa de recolección: el funcionamiento de esta capa consiste en recibir los *traps* de aquellos equipos dotados de agente SNMP, capaces de enviar sus propias alarmas e interrogar, a través de sondas específicas, a aquellos equipos que no envían *traps* o no envían toda la información necesaria para resolver los

fallos. Todos los eventos, ya normalizados, son remitidos al repositorio de la capa de consolidación.

- Capa de consolidación: se encarga de la correlación de *traps*, lo que incluye la deduplicación y la supresión de eventos, el almacenamiento de los *traps*, el almacenamiento y procesado de los ficheros *syslog* y la integración con otros sistemas, como el de gestión de incidencias.
- Capa de presentación: encargada de mostrar en una consola única los eventos sobre los que deben actuar los distintos perfiles de usuarios del sistema.

Las cúpulas gestoras de las compañías demandan actualmente que todas las actividades estén alineadas con las líneas estratégicas de la compañía y pueda medirse como afecta cada una de estas actividades a los objetivos que la propia compañía se haya fijado. Para ello es necesario dotar a los sistemas como el de gestión de fallos de un inventario que registre las dependencias entre el equipamiento y los servicios que soportan.

El complemento perfecto para el sistema de gestión de fallos es el sistema de gestión de rendimiento que proporciona funciones para evaluar e informar sobre el comportamiento del equipamiento de telecomunicaciones y la efectividad de la red. La arquitectura de este sistema también está formada por tres capas: una capa de recolección de los datos interrogando vía SNMP directamente al equipamiento, una capa de consolidación en la que los valores recogidos se componen para formar indicadores clave del rendimiento o KPIs y una capa de presentación para los usuarios. Los indicadores usados habitualmente para analizar la calidad del servicio de red son la disponibilidad, el retardo de tránsito y la pérdida de paquetes. Indicadores como el tráfico de entrada y salida son muy útiles para estudiar tendencias y otros indicadores como la disponibilidad sectorial de la red facilitan a los operadores la rápida localización de problemas.

Todos estos indicadores permiten definir cuadros de mando con la información del rendimiento de los diferentes servicios en periodos largos. Finalmente esta información se compone en informes y se ofrece a los usuarios a través de la capa de presentación.

Para facilitar el trabajo del centro de operación de red es necesario unificar las interfaces de los sistemas que se han definido de manera que diferentes perfiles accedan a la información que necesitan para realizar su trabajo sin necesidad de acceder a varias aplicaciones. Los perfiles definidos para cubrir las principales actividades son los siguientes:

- Administradores: que gestionan los usuarios y grupos de usuarios del sistema
- Provisionadores: responsables de gestionar el inventario

- Operadores de red: responsables de atender los fallos a través de una consola en la que se les muestran con un código de colores para identificar la prioridad de los mismos.
- Usuarios de informes: que utilizan los productos generados por el sistema de rendimiento para analizar las tendencias de los servicios y anticiparse a los posibles problemas. En esta categoría se encuadran también los ejecutivos que acceden a los cuadros de mandos para tomar decisiones en base a los niveles de servicios que se quieran ofrecer a los usuarios y clientes.

Esta memoria esta centrada en el problema de la monitorización de redes de banda ancha, en un enfoque más amplio que abarcase toda la operación y mantenimiento de red sería necesario incorporar los apartados de gestión de configuración, que ampliaría el concepto de inventario hasta una base de datos de gestión de la configuración o CMDB (*Configuration Management DataBase*) y gestión de seguridad que definiría los mecanismos de acceso a los diferentes sistemas de gestión. Finalmente otro apartado contemplado en el modelo funcional OSI trata el problema de la contabilidad, propio de las operadoras de telecomunicaciones, que afronta el problema de recoger la información de las comunicaciones realizadas para tarificarlas y poder cobrar por el servicio prestado.

Otras líneas de ampliación del presente trabajo podrían abordar el futuro de los sistemas de gestión, a los que los usuarios empiezan a demandarles sistemas de aprendizaje capaces de aprender la resolución de problemas habituales de manera que los operadores puedan dedicar más tiempo a problemas complejos.

BIBLIOGRAFÍA

- **RFC 1052**, Abril 1988 Recomendaciones del IAB para el desarrollo de estándares de gestión de red para Internet
- **RFC 1066**, Agosto 1988 Base de información de gestión para redes basadas en TCP/IP
- **RFC 1155**, Mayo 1990. Estructura e identificación de la información de gestión para redes basadas en TCP/IP
- **RFC 1157**, Mayo 1990 Protocolo SNMP
- **RFC 1212**, Marzo 1991 Definición concisa de MIB
- **RFC 1213**, Marzo 1991 Base de información de gestión para redes basadas en TCP/IP: MIB-II
- **RFC 1215**, Marzo 1991 Definición de Traps para uso en SNMP
- **RFC 1902**, Enero 1996 Estructura de información de gestión SNMPv2
- **RFC 1903**, Enero 1996 Nomenclatura en SNMPv2
- **RFC 1904**, Enero 1996 Reglas de conformidad para SNMPv2
- **RFC 1905**, Enero 1996 Operaciones de protocolo SNMPv2
- **RFC 1906**, Enero 1996 Mapeados de transporte SNMPv2
- **RFC 1907**, Enero 1996 MIB para SNMPv2
- **RFC 1908**, Enero 1996 Compatibilidad entre las versiones 1 y 2 de SNMP
- **RFC 2271**, Enero, 1998 Arquitectura de las plataformas SNMP
- **RFC 2272**, Enero 1998 Procesamiento y envío de mensajes en SNMP
- Douglas R. Mauro, Kevin J. Schindt *Essential SNMP* (2nd ed.), Ed. O'Reilly & Associates
- Manuales de administración de Infovista: Server, VistaMart, VistaPortal
- Manuales de Administración de Netcool: Ómnibus, Precision, Webtop