UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SISTEMA DE MONITORIZACIÓN DE ALARMAS DE EQUIPOS DE RED MEDIANTE LA SUITE DE PRODUCTOS IBM TIVOLI NETCOOL

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ALFONSO TORRES ROMERO

PROMOCIÓN
2004 – II

LIMA – PERÚ
2009

SISTEMA DE MONITORIZACIÓN DE ALARMAS DE EQUIPOS DE RED MEDIANTE LA SUITE DE PRODUCTOS IBM TIVOLI NETCOOL

Dedico este trabajo a:
Mi familia por su incondicional
apoyo y dedicación.

SUMARIO

Con el constante crecimiento que experimentan las redes en cuanto a fabricantes, dispositivos y tecnologías, se hace cada vez más difícil la operación y monitorización de las mismas. Esta situación plantea a los ingenieros de red, serios desafíos en el mantenimiento del servicio y en el tiempo de atención de las averías.

Es debido a esta problemática que surge la necesidad para las operadoras de implementar sistemas de monitorización de alarmas de equipos de red que permitan obtener una rápida detección de averías y fallos con el fin de mejorar el servicio que ofrecen y disminuir los tiempos de diagnóstico y solución de problemas.

El presente trabajo pretende describir la implementación de un sistema real de monitorización de alarmas de red mediante la suite de productos IBM TIVOLI NETCOOL. Se tomó en cuenta la solución de IBM por ser una de las mejores en el mercado actual y la más utilizada por los proveedores de servicios, más de 1000 proveedores, incluyendo todos los top 20 confían en TIVOLI NETCOOL para asegurar que sus servicios más críticos funcionen según los más altos estándares.

ÍNDICE

SUMARIO		**V**
ÍNDICE		**VI**
PRÓLOGO		**1**
CAPÍTULO I		**2**
1	**MARCO TEÓRICO CONCEPTUAL**	**2**
1.1	Breve historia de la gestión de alarmas	2
1.2	Arquitecturas de gestión tradicionales	5
1.2.1	Modelo OSI	7
1.2.2	Modelo TMN	9
1.2.3	Modelo Internet	12
1.3	Protocolos de gestión de redes	13
1.3.1	CMIP	14
1.3.2	SNMP	16
1.3.3	SNMP v2	21
1.3.4	SNMP v3	22
1.3.5	RMON	22
1.3.6	RMON 2	24
1.3.7	SYSLOG	25
CAPÍTULO II		**28**
2	**SOLUCIÓN IBM TIVOLI NETCOOL**	**28**
2.1	Descripción de la solución	28
2.2	Arquitectura de productos	29
2.2.1	Capa de Colecta	29
2.2.2	Capa de Agregación	31
2.2.3	Capa de Visualización	31
2.3	Ventajas y Beneficios	32
CAPÍTULO III		**34**
3	**IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE ALARMAS**	**34**
3.1	Análisis de la problemática en la gestión de alarmas	34
3.1.1	Descripción del problema	34
3.1.2	Antecedentes del problema	35

3.2	Descripción de la red TEA	35
3.2.1	Red de acceso	35
3.2.2	Red de transporte	36
3.2.3	Red de núcleo (core IP/MPLS)	36
3.3	Funcionamiento del servicio de acceso	36
3.3.1	Escenarios de acceso	38
3.3.2	VPN (Virtual Private Network)	39
3.4	Lista de equipos	39
3.5	Fundamentos productos IBM TIVOLI NETCOOL	40
3.5.1	Netcool® Omnibus™	40
3.5.2	Netcool® Impact™	46
3.5.3	Netcool® Reporter™	47
3.5.4	Netcool® Webtop™	47
3.6	Puesta en marcha	49
3.6.1	Estructura Física (Hardware)	49
3.6.2	Estructura Lógica	50
3.6.3	Visualización de eventos	51
3.6.4	Tratamiento y Correlación de eventos	54
3.6.5	Almacenamiento de eventos	56
3.7	Pruebas y Testeos	56
3.8	Resultados Obtenidos	57
3.9	Análisis de Costos	60
CONCLUSIONES		**63**
BIBLIOGRAFÍA		**64**

PRÓLOGO

La gestión y monitorización de alarmas ha cambiado mucho durante los últimos años, debido principalmente a muchos factores tales como: el creciente número de equipos y tecnologías de diferentes fabricantes, la dispersión geográfica de la red, la inserción de nuevos servicios y la necesidad de disminuir los costos de operación y mantenimiento.

A raíz de ello, la monitorización de alarmas de red apunta actualmente no sólo a la simple detección de averías y fallos en la red sino también a la reacción automática cuando se producen dichas alarmas y al suministro adecuado de informaciones y recomendaciones para su rápida solución.

La solución TIVOLI NETCOOL de IBM, además de plantear un entorno global centralizado de monitorización en tiempo real para las alarmas de equipos de red (que pueden ser de diferentes tecnologías y fabricantes), ofrece una serie de mecanismos y automatismos de correlación, aislamiento y resolución de fallos que permiten a las empresas proveedoras de servicios de red, resolver rápidamente los problemas más críticos de la red, optimizando la disponibilidad y flexibilidad del servicio.

En el capítulo I se ofrece una visión general de los sistemas de gestión de alarmas de red, la historia y evolución de estos sistemas, las arquitecturas de gestión tradicionales, los protocolos de gestión más utilizados y el estado actual de estos sistemas desde el punto de vista tanto de sistema como en alcance tecnológico.

En el capítulo II se explica la solución TIVOLI NETCOOL que ofrece IBM a las empresas proveedoras de servicios de red, empresas de telecomunicaciones y empresas orientadas a negocios de TI (Tecnologías de la información) para la monitorización de las alarmas de sus equipos de red.

Finalmente en el capítulo III se describe la implementación del sistema de monitorización de alarmas de equipos de red, desarrollado para Telefónica Empresas Argentina (TEA), la estructura física utilizada (hardware), la estructura lógica (productos TIVOLI NETCOL), análisis de costos, el plan de pruebas realizado y los resultados obtenidos.

Antes de terminar, quisiera agradecer al equipo del proyecto SIGRES TEA (Sistema Integral de Gestión de Redes y Servicios para Telefónica Empresas Argentina), módulo de fallas (alarmas), por todo el esfuerzo y dedicación desplegada así como también a mi familia por estar conmigo desde siempre, sin ellos no sería lo que soy. A todos ¡Gracias!

CAPÍTULO I
MARCO TEÓRICO CONCEPTUAL

En el presente capítulo se describe la evolución y situación actual en la que se encuentra la gestión de alarmas, así como también el funcionamiento de los principales protocolos utilizados en los sistemas de gestión (por ejemplo CMIP, SNMP, SYSLOG, etc)

1.1 Breve historia de la gestión de alarmas

El progreso tecnológico que ha tenido hasta la fecha la gestión de redes y por ende la monitorización de alarmas de red, se debe principalmente a la evolución propia de las redes de telecomunicaciones, generada a partir de la necesidad básica de compartir información y procesos con usuarios remotos.

Estas primeras redes de telecomunicaciones se caracterizaban por tener un reducido número de nodos y cada uno de ellos su propio administrador; cuando surgía algún problema que afectara a más de un nodo, los administradores correspondientes se ponían en contacto para juntos solucionarlo. A este primer modo de gestión de red mostrado en la Figura 1.1, se le denominó "Gestión Autónoma".

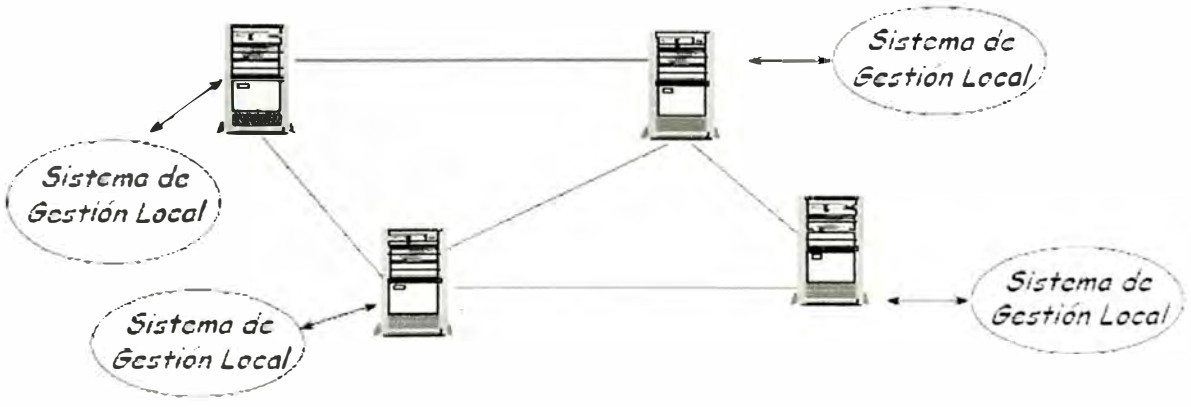


Figura 1.1.- Sistema de Gestión Autónoma

Con el crecimiento del número de nodos, la solución anterior ya no fue eficaz. Por ello a principios de los ochenta aparecieron aplicaciones que brindaban la posibilidad de la supervisión remota de los nodos por lo que la gestión se centralizó, consolidando toda la monitorización de la red en un solo nodo. Sin embargo, cada una de estas aplicaciones sólo servían para redes que estuvieran compuestas por equipos de un mismo fabricante.

Como se muestra en la Figura 1.2, a este modo de gestión, se le denominó "Gestión Homogénea".

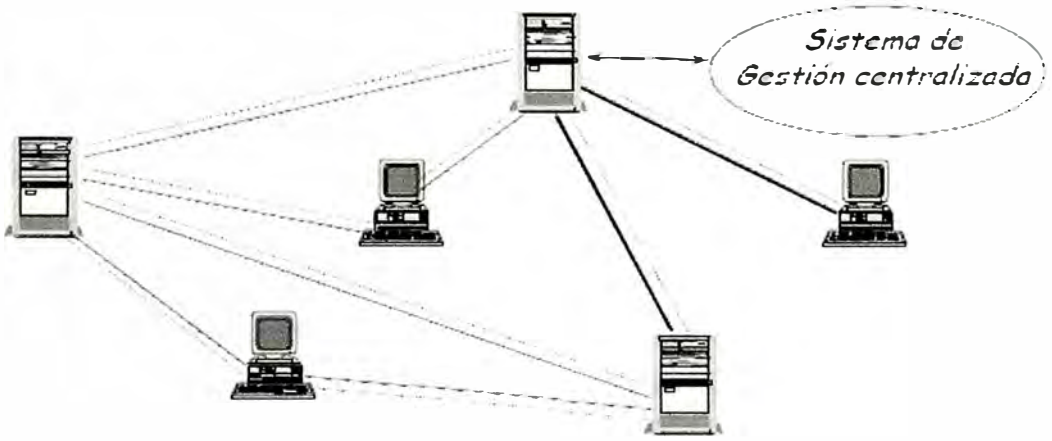


Figura 1.2.- Sistema de Gestión Homogénea

Más adelante con el crecimiento de las redes (conexión de redes locales con redes de área extendida) y la proliferación de varios equipos de interconexión de red de diferentes fabricantes, cada fabricante con sus propios programas de gestión e interfaces de usuario, es de esta manera como muestra la Figura 1.3 que se da inicio a la llamada "Gestión Heterogénea".

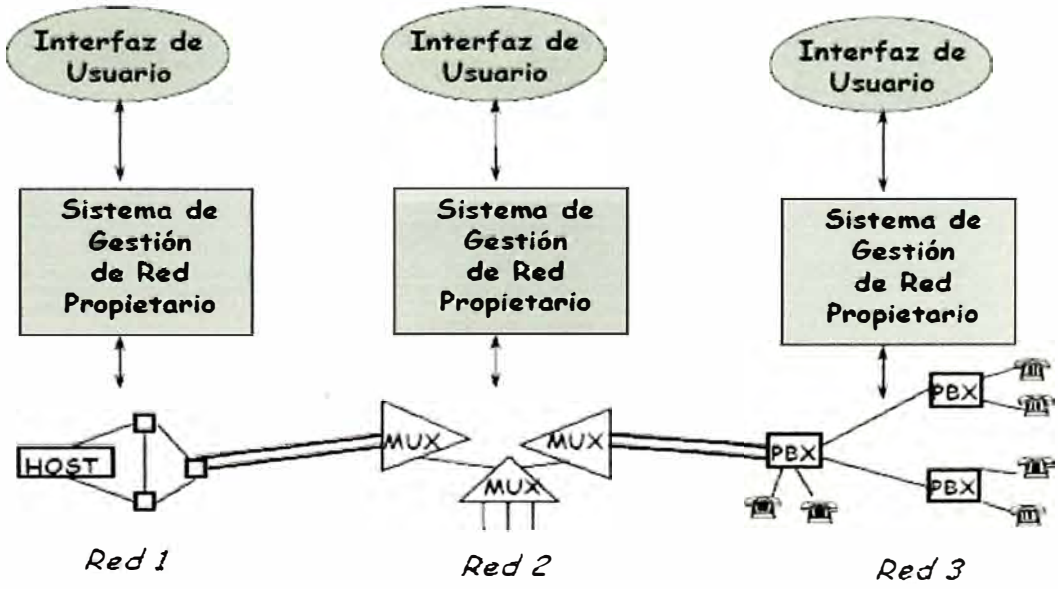


Figura 1.3.- Sistema de Gestión Heterogénea

El uso de este modo de gestión trajo consigo numerosas dificultades para los operadores, de las cuales se cita: la multiplicidad de interfaces de usuario, los distintos programas de aplicación con funcionalidad similar, la duplicidad y posible inconsistencia de la información almacenada en las bases de datos, etc.

Todo ello conllevó al planteamiento y desarrollo de una nueva solución, la denominada "Gestión Integrada" mostrada en la Figura 1.4. En este modo de gestión se normalizan las comunicaciones con la especificación de un protocolo entre elemento de red y centro de gestión como por ejemplo CMIP (Common Management Information Protocol – Protocolo de administración de información común) y SNMP (Simple Network Management Protocol – Protocolo simple de administración de red) y se normaliza la información permitiendo que el centro de gestión pueda conocer las propiedades de gestión de los elementos de red bajo una definición sintácticamente uniforme de ellos.
Los modelos de gestión normalizados tradicionales más importantes para este tipo de gestión heterogénea son: el modelo de gestión OSI (Open Systems Interconnection – Interconexión de sistemas abiertos) de ISO (International Organization for Standardization - Organización Internacional para la Normalización) con el protocolo CMIP, el modelo TMN (Telecommunications Network Management Red de gestión de telecomunicaciones) de la ITU-T (Internacional Telecommunications Union – Unión internacional de telecomunicaciones) y el modelo de gestión Internet IETF (Internet Engineering Task Force - Grupo de Trabajo en Ingeniería de Internet), basado en el protocolo SNMP. Recientemente, han adquirido importancia el modelo de gestión por agentes inteligentes y la gestión por webs.

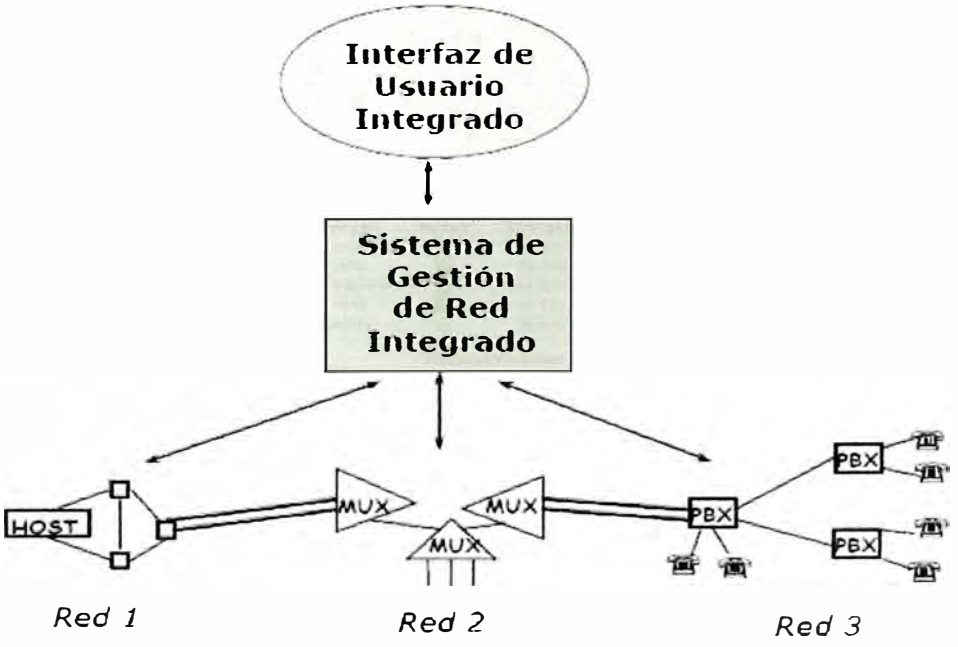


Figura 1.4.- Sistema de Gestión Integrada

De esta manera se llega a la última etapa en la evolución de los sistemas de gestión, las llamadas "Plataformas de Gestión". Estas plataformas utilizan una integración de aplicaciones para poder adaptarse al entorno cambiante y complejo de los elementos de

red que se quieran gestionar. Entre las aplicaciones más usuales que se incorporan, destacan: el discover, que permite autodescubrir equipos y topologías de la red; la programación de sondeos de variables de la MIB (Management Information Base) para el protocolo SNMP; la programación de acciones ante alarmas y finalmente, los visualizadores gráficos de alarmas.

Estas plataformas de gestión posibilitan un mayor grado de integración multifabricante que cualquier esquema gestor de gestores ya que las interacciones con otros sistemas de gestión de diferentes fabricantes se realizan a través de interfaces de programación de aplicaciones estándares (API) y un conjunto estándar de definiciones de datos de gestión.

En la Figura 1.5, se muestra la plataforma de gestión TIVOLI NETCOOL de IBM, otras plataformas de gestión conocidas, figuran: HPOV (OpenView Network Management Server) de Hewlett Packard, NetExpert de Objective Systems Integrators, etc.

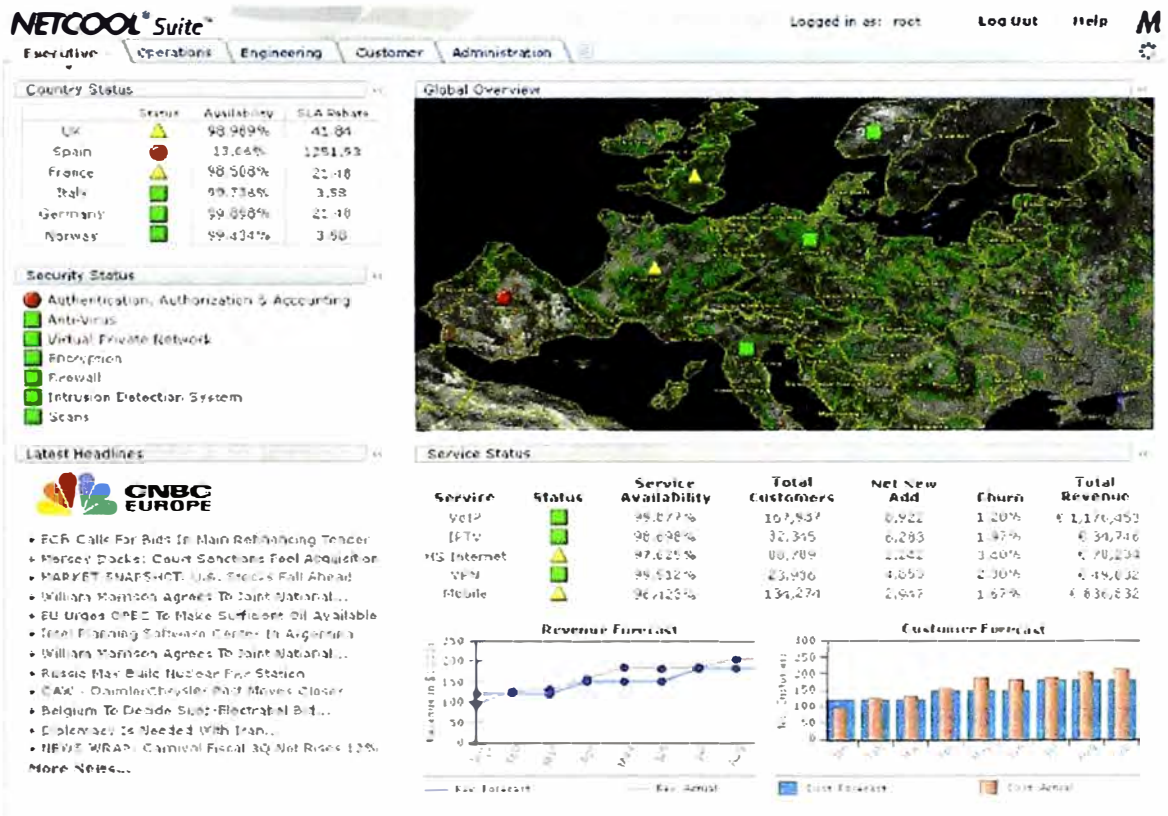


Figura 1.5.- Plataforma de Gestión

1.2 Arquitecturas de gestión tradicionales

La ISO (International Organization for Standardization – Organización internacional para la normalización) define la gestión de red como: "El conjunto de elementos de control y supervisión de los recursos que permiten que la comunicación tenga lugar sobre la red".

En su mayoría, los sistemas de gestión utilizan una estructura básica, conocida por paradigma gestor-agente, cuyo esquema queda reflejado en la Figura 1.6.

Figura 1.6.- Paradigma Gestor-Agente

Los elementos de un sistema de gestión bajo este paradigma son:

- Objeto gestionado: representa cualquier dispositivo físico o lógico de la red y el equipamiento lógico relacionado con él que permita su gestión.
- Agente: es el equipamiento lógico de gestión que muchas veces reside en el objeto gestionado.
- Protocolo: utilizado por el agente para pasar información entre el objeto gestionado y el gestor o estación de gestión.
- Objeto ajeno: se define como un objeto gestionable que utiliza un protocolo ajeno, es decir un protocolo distinto al que utiliza el gestor.
- Agente conversor: actúa de conversor entre el protocolo ajeno y el protocolo utilizado por el gestor.
- Gestor o Estación de gestión: está formada por varios módulos o programas corriendo en una estación de trabajo u ordenador personal.

El principio de funcionamiento reside en el intercambio de información de gestión entre el gestor y los objetos gestionados. Habitualmente, los agentes mantienen en cada objeto gestionado información acerca del estado y las características de funcionamiento de un determinado recurso de la red. El gestor pide al agente, a través de un protocolo de gestión de red, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales, podrá conocer el estado del recurso y podrá influir en su comportamiento. Cuando se produce alguna situación anómala en un recurso gestionado, los agentes, sin

necesidad de ser invocados por el gestor, emiten los denominados eventos o notificaciones que son enviados a un gestor para que el sistema de gestión pueda actuar en consecuencia.

A continuación se describen las tres principales arquitecturas de gestión tradicionales:

- Modelo de gestión OSI
- Modelo de gestión TMN
- Modelo de gestión en Internet

1.2.1 Modelo OSI

El modelo OSI denominado también "OSI System Management", es el conjunto de muchos estándares desarrollados conjuntamente por ISO y la CCITT (Consultative Committee for International Telegraphy and Telephony – Comité Consultivo Internacional Telegráfico y Telefónico) para la gestión de redes OSI. Este modelo de gestión incluye:

- Un conjunto de aplicaciones de propósito general, Ejemplo SMAP (System Management Application Process – Aplicación de gestión de sistemas)
- Una especificación de estructura de objetos, SMI (Structure of Management Information – Estructura de información de gestión)
- Un servicio de gestión, CMIS (Common Management Information Service)
- Un protocolo de gestión, CMIP (Common Management Information Protocol)

Un equipo gestionado dentro del entorno OSI seguirá el modelo de arquitectura que se muestra en la Figura 1.7.

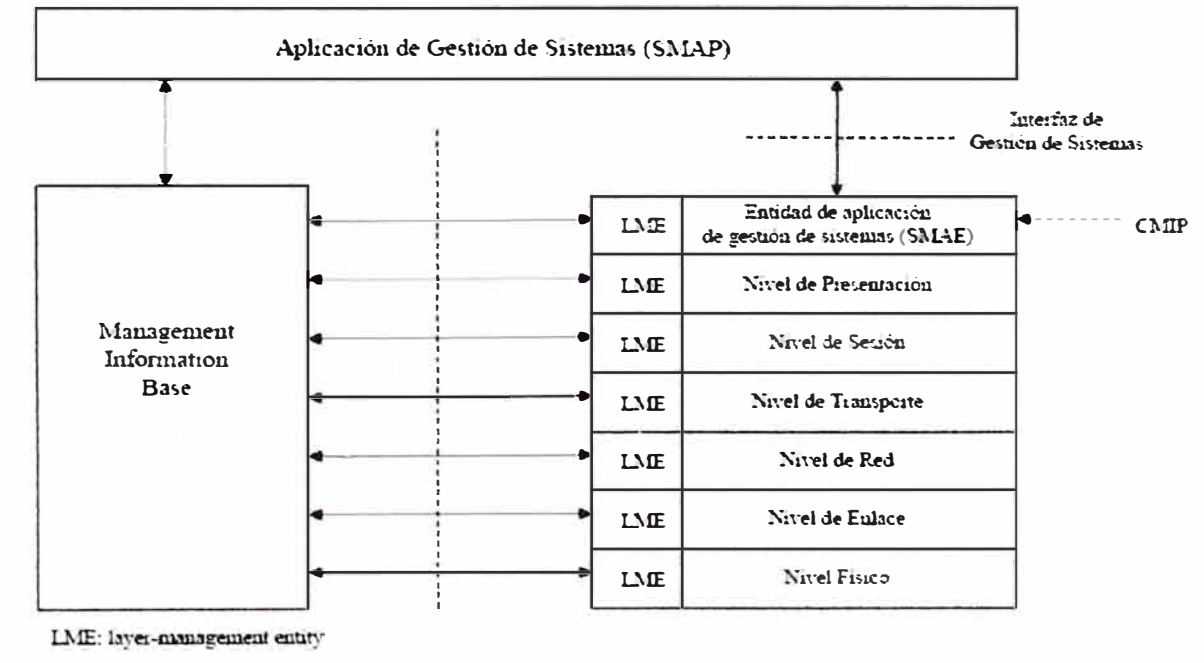


Figura 1.7.- Arquitectura OSI (CMIS)

Los elementos clave de este modelo de arquitectura son:

- Aplicación de gestión de sistemas SMAP: Software local de un equipo (sistema) gestionado que implementa las funciones de gestión para ese sistema (host, router, etc.) Tiene acceso a los parámetros del sistema y puede, por tanto, gestionar todos los aspectos del sistema y coordinarse con SMAPs de otros sistemas.
- Entidad de aplicación de gestión de sistemas SMAE (System Management Application Entity): Entidad de nivel de aplicación responsable del intercambio de información de gestión con SMAEs de otros nodos, especialmente con el sistema que hace las funciones de centro de control de red. Para esta función se utiliza un protocolo normalizado (CMIP)
- Entidad de gestión de nivel o capa LME (Layer Management Entity): Proporciona funciones de gestión específicas de cada capa del modelo OSI.
- Base de información de gestión MIB (Management Information Base).

Todos los elementos descritos en la arquitectura, deben existir en cada uno de los elementos a gestionar en el sistema (red). El SMAP puede tomar el papel de agente o de gestor. El papel de gestor corresponde a los centros de control de red, y el de agente a los sistemas gestionados.

La Figura 1.8 muestra la comunicación Gestor-Agente en OSI, donde el gestor solicita información o solicita la ejecución de comandos a los sistemas gestionados.

El agente interacciona con el gestor y es responsable de administrar los objetos de su sistema. El flujo normal de información de gestión y control entre el gestor y el agente se realiza mediante el protocolo CMIP, perteneciente al nivel de aplicación OSI.

El protocolo permite que un sistema se pueda configurar para que opere como gestor o como agente. La mayoría de las realizaciones prácticas de sistemas gestionados se configuran con unos pocos sistemas operando en modo gestor, controlando las actividades de un gran número de sistemas operando en modo agente.

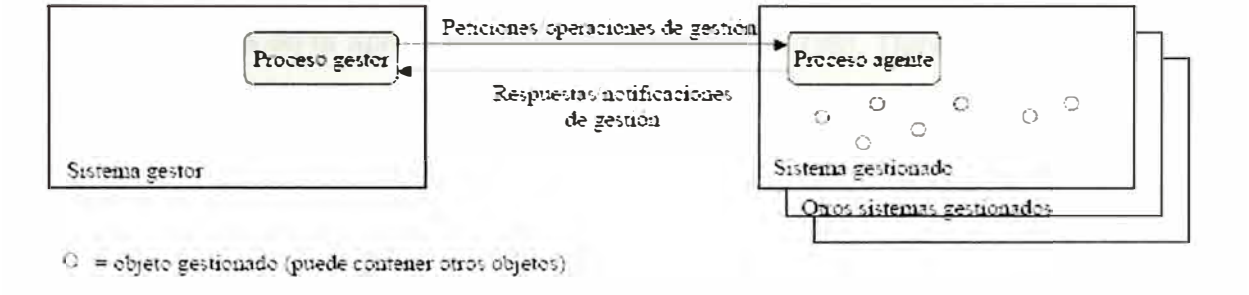


Figura 1.8.- Comunicación gestor-agente en OSI

La Estructura de la Información de Gestión (SMI), define la estructura lógica de la información de gestión OSI. Establece las reglas para nombrar a los objetos gestionables y a sus atributos. Define un conjunto de subclases y tipos de atributos que son en principio aplicables a todos los tipos de clases de objetos gestionables.
La Base de Información de Gestión (MIB), representa la información que se está utilizando, modificando o transfiriendo en la arquitectura de los protocolos de gestión OSI. La MIB conoce todos los objetos gestionables y sus atributos. No es necesario que este centralizada físicamente en un lugar concreto, puede estar distribuida a través del sistema y en cada uno de sus niveles.
CMIS (Common Management Information Services - Servicios de Información Común de Gestión) es un conjunto de reglas que identifican las funciones de una interfaz OSI entre aplicaciones, utilizado por cada aplicación para intercambiar información y parámetros. CMIS define la estructura de la información que es necesaria para describir el entorno. Prácticamente todas las actividades de la gestión de red OSI están basadas en las primitivas de servicio CMIS, entre las principales, se tiene:

- M-EVENT-REPORT: usado por un agente para notificar la ocurrencia de un evento a un gestor.
- M-GET: Usado por un gestor para obtener información de un agente.
- M-SET: Usado por un gestor para modificar información de un agente.
- M-ACTION: Usado por un gestor para invocar un procedimiento predefinido especificado como parte de un objeto de un agente. La petición indica el tipo de acción y los parámetros de entrada.
- M-CREATE: Usado para crear una nueva instancia de una clase de objetos.
- M-DELETE: Usado para eliminar uno o más objetos.
- M-CANCEL-GET: Usado para finalizar una operación GET larga.

1.2.2 Modelo TMN

La TMN (Telecommunications Management Network) presenta un modelo real, orientado a objeto, actualizado y ampliamente aplicable, definido por un número de estándares y basado sobre el modelo de comunicaciones de siete capas OSI.
Como consecuencia de la aplicación de la arquitectura de OSI, TMN es bastante similar a la gestión de red OSI basada en CMIP. Sin embargo, no son idénticos: TMN ha sido desarrollado para su proyección al futuro (los servicios de gestión OSI pueden ser considerados como un sub-set de servicios TMN)
Las recomendaciones que regulan la TMN son las de la serie M.3XXX de la ITU-T. En estas recomendaciones se definen los siguientes modelos y arquitecturas:

Arquitectura física: proporciona la manera de transportar la información de los procesos relacionados con la gestión de las redes de telecomunicaciones. Los componentes que forman esta arquitectura física son los siguientes:

- Sistemas de operaciones (OS)
- Redes de comunicaciones de datos (DCN)
- Dispositivos mediadores (MD)
- Estaciones de trabajo (WS)
- Elementos de red (NE)
- Adaptadores Q (QA).

Las interfaces TMN se basan en el modelo de referencia OSI (ITU-T X.200):

- Interfaz Qx: es una interfaz apropiada para pequeños elementos de red que requieran unas pocas funciones OAM (Operation, Administration and Mainenance) utilizadas con gran frecuencia. Utilizada normalmente por los NEs y MDs más complejos.
- Interfaz Q3: soporta un complejo conjunto de funciones y requiere el servicio de bastantes protocolos para poderlas ofrecer. Para las OSs y los NEs se encuentra especificada en los documentos T1.204-1989 y T1.208-1989 de ANSI.
- Interfaz X: soporta el conjunto de funciones para la interconexión de diferentes OSs, ya sea entre entornos de TMNs o no. Requiere de las 7 capas de OSI, según está definido en la normativa T1.217 de ANSI. Los mensajes y protocolos definidos para la interfaz X podrían usarse igualmente en la interfaz Q3.
- Interfaz F: soporta el conjunto de funciones para la interconexión de estaciones de trabajo con componentes físicos de la red de comunicaciones que contengan las OSF (Operations Systems Function, son procesos de Información de dirección para supervisar, controlar, y coordinar funciones de telecomunicaciones) o las MF (Mediation Function, conforme a la información adjunta bloques funcionales).

Modelo organizativo: definido por la ITU-T, establece las siguientes capas:

- Capa de gestión comercial, incluye la completa gestión de la explotación de la red, incluyendo contabilidad, gestión y administración, basándose en las entradas procedentes de las capas de gestión de servicios y de gestión de red.
- Capa de gestión de servicios, incluye las funciones que proporcionan un manejo eficiente de las conexiones entre los puntos finales de la red, asegurando un óptimo aprovisionamiento y configuración de los servicios prestados a los usuarios.

- Capa de gestión de red, incluye el control, supervisión, coordinación y configuración de grupos de elementos de red constituyendo redes y subredes para la realización de una conexión.
- Capa de gestión de elementos de red, incluye la gestión remota e individual de cualquier elemento de red que se precise para el establecimiento de conexiones entre dos puntos finales para proporcionar un servicio dado. Este nivel proporcionará funciones de gestión para monitorizar y controlar elementos de gestión individuales en la capa de elemento de red.
- Capa de elementos de red, incluye las funciones que proporcionan información en formato TMN del equipamiento de red así como las funciones de adaptación para proporcionar interfaces TMN a elementos de red no-TMN.

Modelo funcional: se compone de Bloques de Servicios, Componentes y Funciones de gestión. La idea consiste en descomponer las funcionalidades de mayor a menor nivel en bloques re-aprovechables (según las necesidades desde el punto de vista de los operadores).

Modelo de información: define el formato de la información que se transmite entre los bloques funcionales. La Figura 1.9 muestra el esquema de una red TMN.

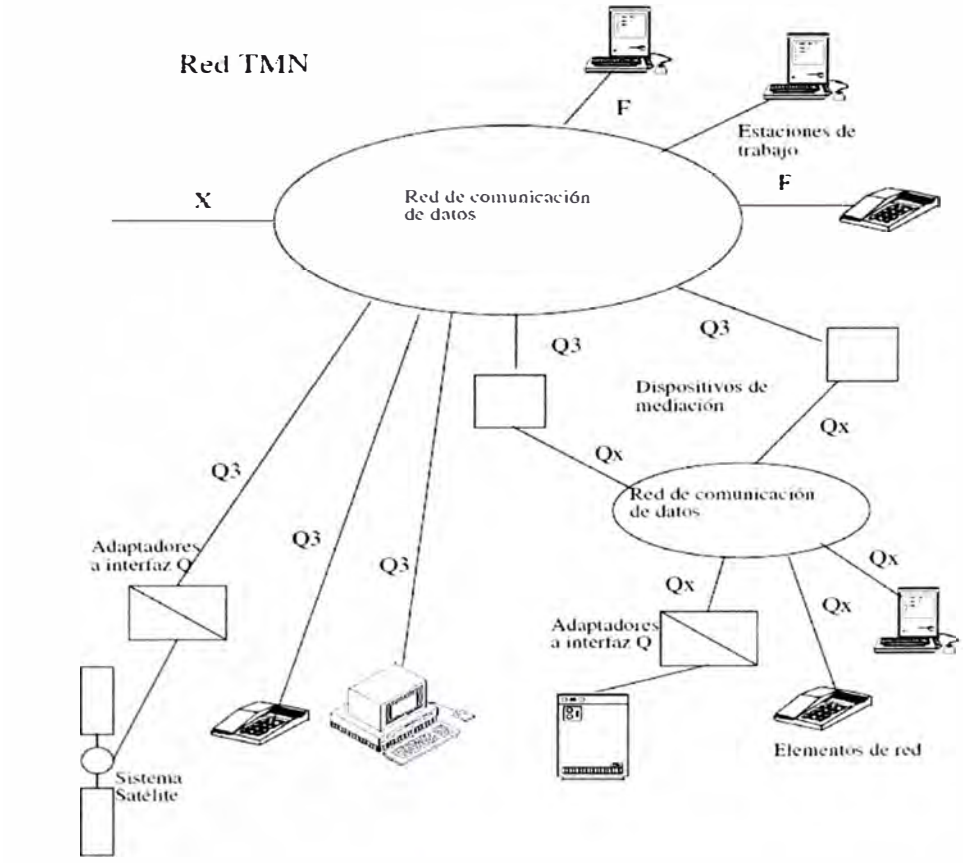


Figura 1.9.- Red TMN

Las recomendaciones para la red TMN son las siguientes:

- M.3000. Introducción a la recomendación TMN.
- M.3010. Principios para una red de gestión de telecomunicaciones.
- M.3020. Metodología para la especificación de la interfaz TMN.
- M.3100. Modelo de información de elementos de red genéricos.
- M.3101. Requerimientos para conformar objetos gestionados en TMN M.3100.
- M.3180. Catálogo de información de gestión TMN.
- M.3200. Introducción a los servicios de gestión TMN.
- M.3300. Capacidades de gestión TMN presentadas en la interfaz F.
- M.3400. Funciones de gestión TMN.
- M.xfunc. Servicios de gestión TMN y funciones para la interfaz X.
- M.xinfo. Identificación de la información que se intercambia vía la interfaz X para diferentes casos de acceso.

1.2.3 Modelo Internet

En 1988, el IAB (Internet Activities Board, Comité de Actividades Inter-red) determinó la estrategia de gestión para TCP/IP (Transfer Control Protocol/Internet Protocol). Esto significó el nacimiento de dos esfuerzos paralelos: la solución a corto plazo, SNMP, y la solución eventual a largo plazo, CMOT (CMIP Over TCP/IP, CMIP sobre TCP/IP)

CMOT pretendía implantar los estándares del modelo de gestión OSI en el entorno Internet (TCP/IP). CMOT tuvo que afrontar los problemas derivados de la demora en la aparición de especificaciones y la ausencia de implementaciones prácticas. Como consecuencia de ello, la iniciativa CMOT fue paralizada en 1992.

SNMP es una extensión del protocolo de gestión de red para gateways SGMP (Simple Gateway Monitoring Protocol – Protocolo simple de monitorización para gateways) que se convirtió en 1989 en el estándar recomendado por Internet. Está dirigido a proporcionar una gestión de red centralizada que permita la observación, el control y la gestión de las instalaciones. Utilizando SNMP, un administrador de red puede direccionar preguntas y comandos a los dispositivos de la red. (CMIP para la gestión OSI y SNMP para la gestión Internet).

Al convertirse TCP/IP en el estándar de facto en redes de ordenadores, SNMP se ha convertido en otro estándar de facto, pero con muchas limitaciones. En Agosto de 1988 se publican las primeras recomendaciones: SNMP, SMI y MIB. Son revisadas en 1991 las recomendaciones SNMP y MIB, dando lugar, esta última, a la recomendación MIB II. A partir de esta fecha comienza el desarrollo de MIBs particulares por parte de los fabricantes. En Mayo de 1993 aparece SNMPv2 y en Febrero de 1998 SNMPv3 para

suplir las deficiencias en cuanto a seguridad y funcionalidad se refiere. El marco de trabajo de SNMP está basado en tres documentos:

- Structure of Management Information (SMI).- RFC 1155.
- Management Information Base (MIB).- RFC 1213

Algunas de las funciones que proporciona SNMP son:

- Supervisión del rendimiento de la red y su estado.
- Control de los parámetros de operación.
- Obtención de informes de fallos.
- Análisis de fallos.

Los sistemas de gestión de Internet están formados por cuatro elementos básicos: Gestores, Agentes, MIB y el protocolo de información de intercambio SNMP.

- Agente: equipamiento lógico alojado en un dispositivo gestionable de la red. Almacena datos de gestión y responde a las peticiones sobre dichos datos.
- Gestor: equipamiento lógico alojado en la estación de gestión de red. Tiene la capacidad de preguntar a los agentes utilizando diferentes comandos SNMP (PUT, GET, etc).
- MIB (Management Information Base): base de datos virtual de los objetos gestionables, accesible por un agente, que puede ser manipulada vía SNMP para realizar la gestión de red.
- El protocolo SNMP realiza las funciones descritas anteriormente llevando información de gestión entre los gestores y los agentes.

Existe un tipo de agente que permite la gestión de partes de la red que no comparten el modelo de gestión de Internet. Son los llamados Agentes Proxy. Estos agentes proxy proporcionan una funcionalidad de conversión del modelo de información y del protocolo.

1.3 Protocolos de gestión de redes

Los protocolos de gestión de red proveen las reglas de comunicación entre el gestor y los agentes de gestión. Estos protocolos a su vez soportan las funciones necesarias para monitorizar, controlar y coordinar los objetos gestionados. Entre los principales protocolos utilizados en la gestión de redes, se tiene:

- CMIS/CMIP
- SNMP, SNMPv2, SNMPv3
- RMON, RMON2
- SYSLOG

1.3.1 CMIP

CMIP fue diseñado teniendo en cuenta a SNMP solucionando los errores y fallos que tenía SNMP y volviéndose un gestor de red mucho más detallado. Su diseño es similar a SNMP por lo que se usan PDUs (Protocol Data Unit) como 'variables' para monitorizar la red. En CMIP las variables son unas estructuras de datos complejas con muchos atributos, que incluyen:

- Variables de atributos: Representan las características de las variables.
- Variables de comportamiento: Qué acciones puede realizar.
- Notificaciones: la variable genera una indicación de evento cuando ocurre un determinado hecho.

La arquitectura CMIP provee un modo de que la información de control y de mantenimiento pueda ser intercambiada entre un gestor y un elemento remoto de red. En efecto, los procesos de aplicación llamados gestores residen en las estaciones de gestión mientras que los procesos de aplicación llamados agentes, residen en los elementos de red.

CMIP define una relación igual a igual entre el gestor y el agente incluyendo lo que se refiere al establecimiento y cierre de conexión, y a la dirección de la información de gestión. Las operaciones CMIS (Common Management Information Services) se pueden originar tanto en los gestores como en agentes, permitiendo relaciones simétricas o asimétricas entre los procesos de gestión. Sin embargo, la mayor parte de los dispositivos contienen las aplicaciones que sólo le permiten hacer de agente. La serie CMIP está compuesta por 6 protocolos que se esquematizan en la Tabla 1.1.

Tabla 1.1.- Suite de protocolos CMIP

<table>
<tr><td colspan="2">Procesos de Administración de Aplicaciones</td></tr>
<tr><td colspan="2">CMISE
ISO 9595/9596</td></tr>
<tr><td>ACSE ISO
8649/8650</td><td>ROSE ISO DIS
9072-1/2</td></tr>
<tr><td colspan="2">ISO Presentación
ISO</td></tr>
<tr><td colspan="2">ISO Sesión
ISO</td></tr>
<tr><td colspan="2">ISO Transporte
ISO</td></tr>
</table>

Como se puede ver en la Tabla 1.1, un sistema CMIP debe implementar una serie de protocolos de los cuales el CMISE (Elemento CMIS) es el que trabaja mano a mano con CMIP: todas las operaciones de gestión de red que crea CMISE, el CMIP las mapea en una operación en el CMIP remoto. Para comunicarse entre sí dos entidades de aplicación pares del administrador y del agente se utilizan APDU´s (Application Protocol Data Units – Unidad de datos de protocolo de aplicación). Como hemos visto, CMIP está compuesto de los protocolos OSI que siguen:

ACSE (Association Control Service Element - Elemento de servicio de control de asociación): se utiliza para establecer y liberar asociaciones entre entidades de aplicación. El establecimiento lo puede realizar el agente o el administrador, y durante el proceso se intercambian los títulos de la entidad de aplicación para identificarse, y los nombres del contexto de aplicación para establecer un contexto de aplicación. Servicios que ACSE proporciona a CMISE:

- A-ASSOCIATE, servicio confirmado utilizado para inicializar la asociación entre entidades de aplicación.
- A-RELEASE, servicio confirmado usado para liberar una asociación entre entidades de aplicación sin pérdida de información.
- A-ABORT, servicio no confirmado que causa la liberación anormal de una asociación con una posible pérdida de información.
- A-P-ABORT, servicio iniciado por el proveedor que indica la liberación anormal de la asociación del servicio de presentación con posible pérdida de información.

ROSE (Remote Operation Service Element – Elemento de Servicio de Operación Remota): es el equivalente OSI a una llamada de un procedimiento remoto. ROSE permite la invocación de una operación en un sistema remoto. CMIP usa los servicios orientados a conexión proporcionados por ROSE para todas las peticiones, respuestas y respuestas de error. Servicios que ROSE proporciona a CMISE:

- RO-INVOKE, servicio no confirmado que es usado por un usuario de ROSE para invocar que una operación sea realizada por un ROSE invocado remoto.
- RO-RESULT, servicio no confirmado que un ROSE invocado usa para contestar a una previa indicación RO-INVOKE en el caso de que se haya realizado con éxito.
- RO-ERROR, servicio no confirmado que es usado por un usuario de ROSE invocado para contestar a una previa indicación RO-INVOKE en el caso de que haya fracasado.
- RO-REJECT, servicio no confirmado utilizado por un usuario de ROSE para rechazar una petición (indicación RO-INVOKE) del otro.

CMISE (Common Management Information Service Element – Elemento CMIS): proporciona los servicios básicos de administración confirmados y no confirmados para reportar eventos y manipular datos de administración. CMISE hace uso de los servicios proporcionados por ROSE y ACSE. Servicios de CMISE: se denominan unidades funcionales y se resumen en la tabla siguiente las denominadas 'stand alone' (luego hay otras tres más). El número que sigue a cada unidad funcional está definido por el CMIP. También se especifica en cada caso si se trata de servicio confirmado o no confirmado.

1.3.2 SNMP

El protocolo SNMP (RFC 1157) surge a partir del protocolo SGMP para gestión de routers IP. El Simple Network Management Protocol (SNMP) es un protocolo de aplicación que ofrece servicios de gestión de red al conjunto de protocolos Internet. SNMP define una arquitectura basada en cliente-servidor, como se muestra en la Figura 1.10.

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

SNMP permite también extensiones de esta MIB a agentes particulares para el uso de MIB privadas.

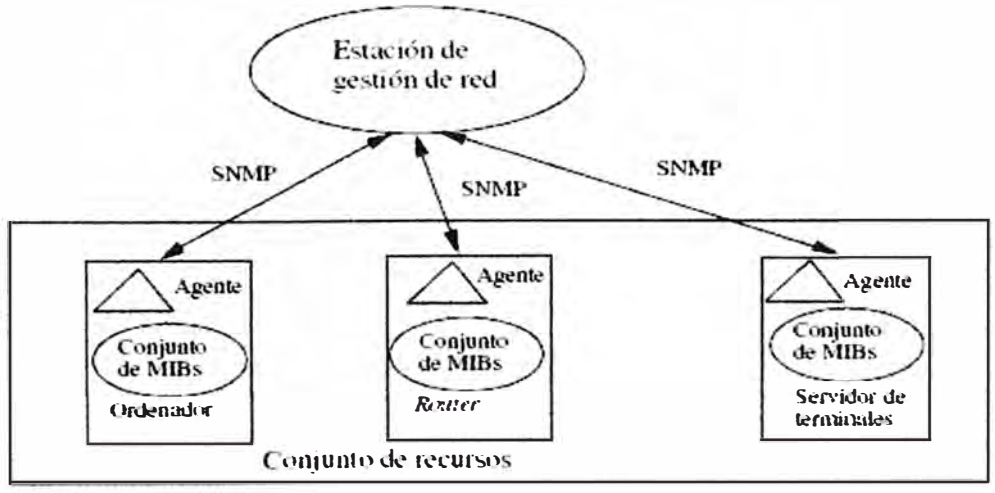


Figura 1.10.- Arquitectura SNMP

El marco de trabajo del protocolo SNMP se basa esencialmente en tres documentos:

- Structure of Management Information (SMI): RFC1155.
- Management Information Base (MIB): RFC 1156, RFC 1213.
- Simple Network Management Protocol (SNMP): RFC 1157.
- Otros documentos adicionales como el RFC 1212 (Concise MIB definitions)

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

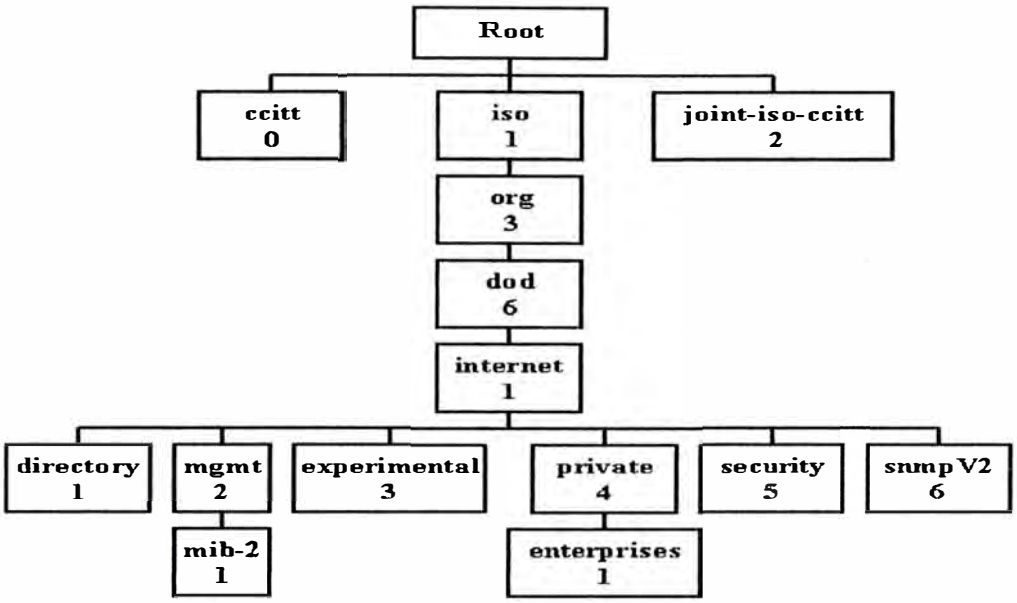


Figura 1.11.- Árbol OID

Como se muestra en la Figura 1.11, los OIDs no son más que una secuencia de enteros no negativos separados por un punto que forman un árbol. Este árbol, denominado de registro, está estandarizado a nivel mundial. Por ejemplo, el OID: 1.3.6.1.1 identifica el objeto que se encontraría si, comenzando en el root, se pasa a la rama 3, después a la 6, a la 1 y finalmente a la rama 1.

La torre de comunicaciones SNMP se apoya en la estructura de protocolos TCP/IP de Internet que se muestra en la Figura 1.12.

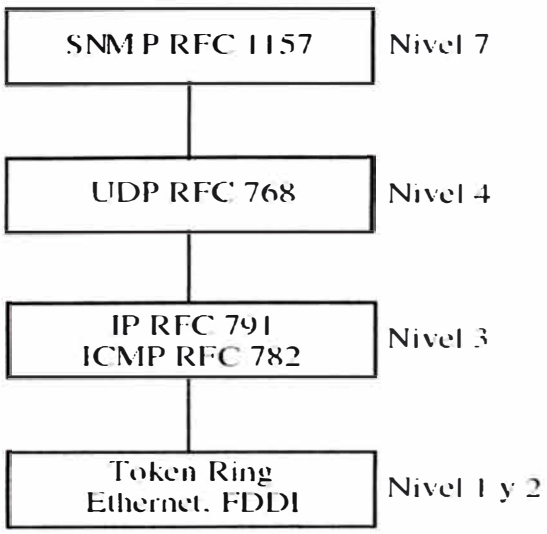


Figura 1.12.- Torre de protocolos en internet

SNMP, si bien es un protocolo abierto, también puede utilizar un agente proxy para gestionar sistemas propietarios. Cabe destacar también que en SNMP la comunicación con los agentes no está orientada a conexión y que al ser un protocolo basado en UDP/IP no garantiza la llegada de los mensajes TRAP a destino, con lo que tienen que integrarse mecanismos especiales en capas superiores para evitar estas deficiencias.

Entre los tipos de operaciones permisibles con SNMP, se tiene:

- GetRequest: petición de valores específicos de la MIB.
- GetNextRequest: proporciona un medio para moverse por la MIB. Petición del objeto siguiente a uno dado de la MIB (orden lexicográfico).
- GetResponse: devuelve los valores solicitados por las operaciones anteriores.
- SetRequest: permite asignar un valor a una variable. Debido a posibles problemas de seguridad esta función suele estar desactivada.
- Traps: son mensajes especiales que permiten a los agentes informar al gestor de sucesos inusuales y/o alarmas sucedidos en el objeto gestionado. (por ejemplo: ColdStart, WarmStart, LinkDown, LinkUp, AuthenticationFailure, etc).

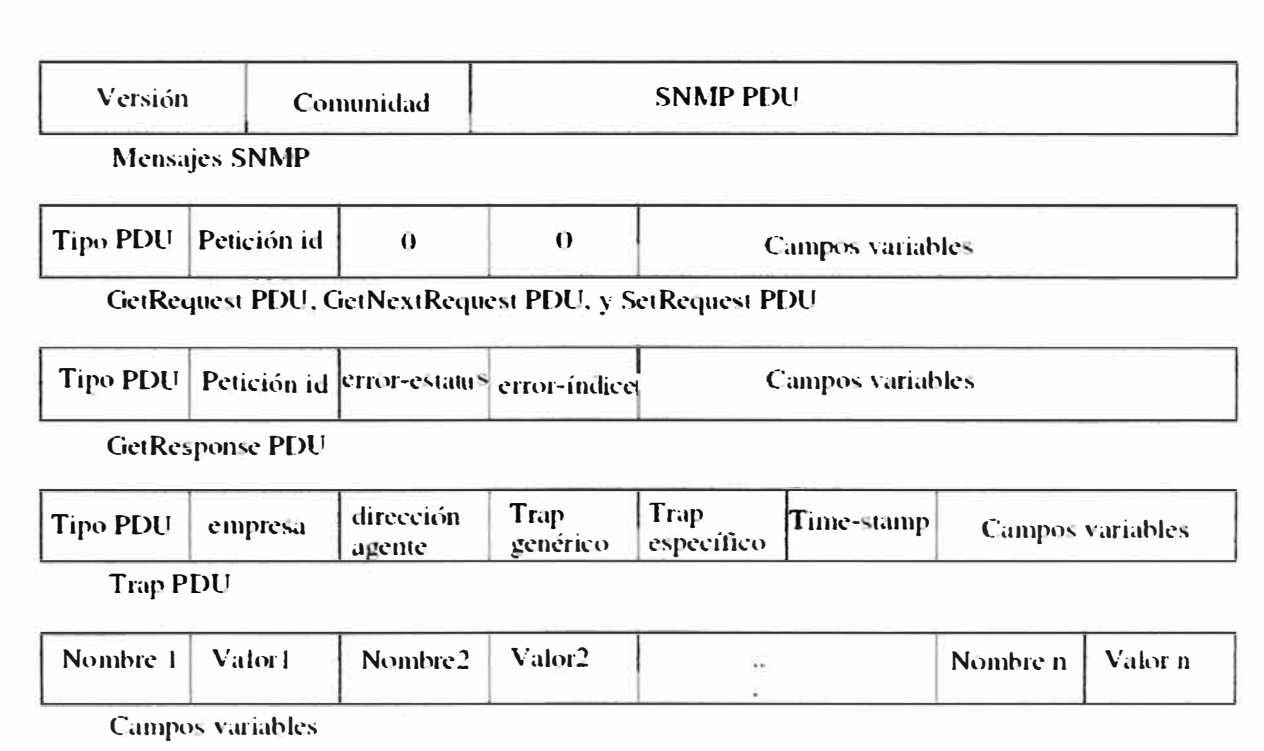


Figura 1.13.- Formatos PDU

La Figura 1.13, muestra los formatos de los PDU de las diferentes operaciones existentes en SNMP. Para las operaciones GetRequest, GetNextRequest y SetRequest, el esquema de mensaje es el mismo. Para el caso de los traps se incluyen en el mensaje, la dirección del agente (dirección IP), el tipo de trap que puede ser genérico (en la Tabla 1.2 se

muestran los valores de traps genéricos) o específico de cada fabricante, el timestamp que indica el tiempo que ha transcurrido entre la reinicialización del agente y la generación del trap, y finalmente los campos variables que permiten añadir más información al evento (se construyen con el número de OID seguido de su valor asignado)

Tabla 1.2.- Tipos de traps genéricos

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 se encuentra fuera de servicio (inactiva).
Link up (3)	Indica que una interfaz de comunicación se encuentra en servicio (activa).
Authentication failure (4)	Indica que el agente ha recibido un requerimiento de un NMS (Estación de gestión de red) no autorizado (normalmente controlado por una comunidad).
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 (6)	En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores (traps específicos)

A continuación, en la Figura 1.14, se describe la secuencia de eventos que se produce en la emisión y recepción de un mensaje SNMP por parte de una entidad de gestión.

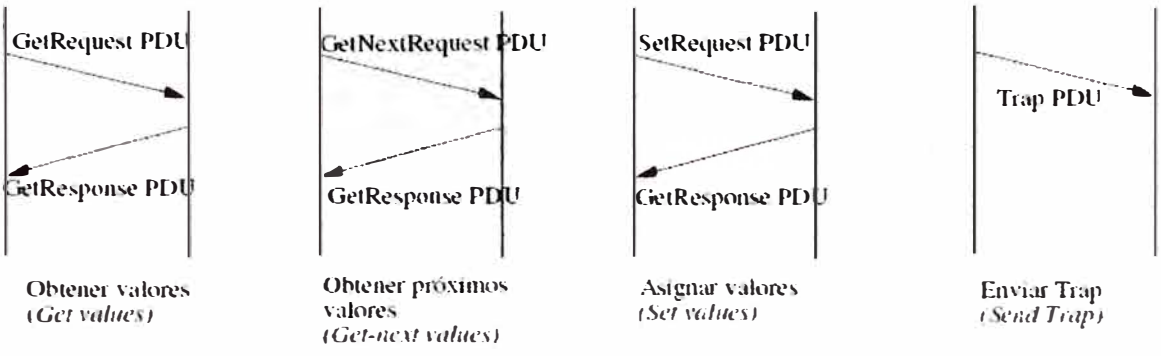


Figura 1.14.- Secuencias de PDUs en el protocolo SNMP

Secuencia de transmisión de un mensaje SNMP:

- Construcción de la PDU, usando estructuras ASN.1.
- La PDU se procesa por el servicio de autenticación junto a las direcciones correspondientes.
- La entidad de protocolo construye el mensaje, consistiendo de una versión de campo, el nombre de la comunidad y el resultado del paso dos.
- Este nuevo objeto ASN.1 es entonces codificado, usando las reglas de codificación básicas y pasado al servicio de transporte.

Secuencia de recepción de un mensaje SNMP:

- Chequeo básico de la sintaxis del mensaje, descartándolo si es erróneo.
- Verificación del número de versión. Se descarta el mensaje si no es coherente.
- La entidad de protocolo pasa al usuario, la porción PDU del mensaje y las direcciones de transporte de emisor y receptor al servicio de autenticación. Si la autenticación falla, el servicio de autenticación señaliza a la entidad de protocolos SNMP, para que genere una Trap y descarte el mensaje. Si la autenticación tiene éxito, el servicio de autenticación devuelve la PDU en la forma de objeto ASN.1 definido en RFC 1157.
- La entidad de protocolo hace un chequeo básico de la sintaxis del mensaje, descartándolo si es erróneo. En cualquier caso, la comunidad nombrada con la adecuada política de acceso SNMP seleccionada finalmente procesa la PDU.

Comparaciones SNMP y CMIP:

Algunas comparaciones entre los protocolos SNMP y CMIP:

- En cuanto a modelo de datos de instrumentación, el protocolo SNMP se representa a través de variables, tablas, traps etc. mientras que CMIP utiliza un modelo de objetos extendido.
- Respecto a identificación de nombres de datos gestionados, SNMP hace uso de un árbol de directorios estático y CMIP hace uso de un árbol de directorios dinámico.
- A nivel operacional, el protocolo CMIP se basa en una arquitectura jerárquicamente distribuida, lo que permite que el número de objetos supervisados sea mayor que en el protocolo SNMP que al ser de tipo centralizado, viene limitado por la capacidad tecnológica de las plataformas de gestión. De todas formas, hay que decir a favor del protocolo SNMP que es más simple y que el personal requerido para su mantenimiento se reduce.

- A nivel funcional, SNMP está basado en técnicas de sondeo, mientras que CMIP utiliza una técnica basada en eventos. Esto permite a CMIP ser más eficiente que SNMP en el control de grandes redes.
- CMIP es un protocolo orientado a conexión mientras que SNMP no lo es. Esto significa que la carga de proceso de SNMP es reducida, pero cuando se envía un mensaje nunca se puede asegurar que el mensaje llega a su destino. La seguridad de los datos no es prioritaria para SNMP.
- A nivel de implementación, hay que decir que un agente CMIP ocupa unos 400 Kbytes o más mientras que un agente SNMP ocupa de 20 Kbytes a 60 Kbytes. También, el costo de procesado y de la misma aplicación es más elevado en una plataforma CMIP.
- En cuanto al soporte por parte de fabricantes, el protocolo SNMP es el utilizado por la gran mayoría de fabricantes y clientes, y existe una multitud de productos comerciales. Los gastos de mantenimiento también suelen ser menores en SNMP al ser más simple y tener una mayor base comercial.
- Finalmente, el protocolo CMIP permite más extensiones, es más escalable, permite la herencia de atributos y es más flexible que el protocolo SNMP.

1.3.3 SNMP v2

Este protocolo de gestión se definió en 1993, es una versión más avanzada del SNMP.
SNMP v2 aporta una serie de ventajas respecto a la primera versión, entre las cuales pueden destacarse:

- Permite una mayor eficiencia en la transferencia de información.
- Admite mecanismos de seguridad como la autentificación y el cifrado frente al SNMP (no implementados).
- Permite la comunicación entre estaciones de gestión.
- Parte de un modelo de comunicaciones extendido considerablemente.
- Permite una señalización extendida de errores.
- Permite el uso de varios servicios de transporte.

El sistema basado en SNMP v2 soluciona muchos de los problemas de su anterior versión, SNMP; sin embargo, su mayor complejidad está coartando su desarrollo.
El protocolo SNMP v2, que incluye los mensajes de la primera versión, dispone de los siguientes tipos de mensajes adicionales:

- GetBulkRequest: petición de múltiples valores.
- InformRequest: transmite información no solicitada (gestor a gestor).

La Figura 1.15 muestra el formato de los mensajes de las operaciones en SNMP v2, similar a la versión anterior, se incluye la nueva operación GetBulkRequest.

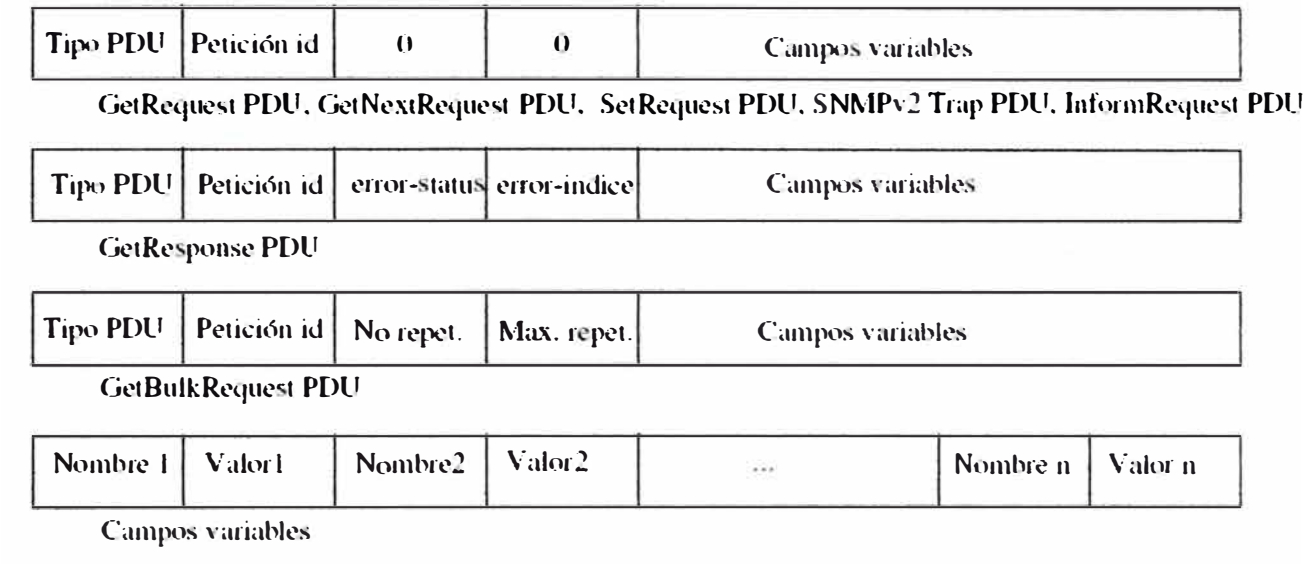


Figura 1.15.- Formatos SNMPv2

Sin embargo, a pesar de sus mejoras se quedó corto en cuanto a seguridad (sigue utilizando el esquema de comunidades como medio de autenticación) lo que propició el desarrollo de una nueva versión SNMPv3.

1.3.4 SNMP v3

El protocolo SNMP v3 es una evolución de la serie de modelos de gestión vistos anteriormente. La arquitectura de seguridad se diseñó para adaptar diferentes modelos de seguridad. El modelo más común es basado en usuarios (User-based Security Model, o USM) e incluye:

- Autenticidad e Integridad: Se utilizan claves por usuario y los mensajes van acompañados de huellas digitales generadas con una función hash (MD5 o SHA)
- Privacidad: Los mensajes pueden ser cifrados con un algoritmo de clave secreta (CBC-DES)
- Validez temporal: Utiliza relojes sincronizados y una ventana de 150 segundos con chequeo de secuencia

1.3.5 RMON

El Remote Network-Monitoring (RMON), especificado en 1994, define una MIB para permitir la monitorización remota, y proporciona al gestor de red información vital acerca de la interconexión con otras redes.

Mientras que el protocolo SNMP se diseñó en función de una arquitectura de polling pasivo, el RMON permite al usuario el uso de agentes "inteligentes" que responden de acuerdo con acontecimientos excepcionales. Esto reduce el tráfico asociado con la red de gestión, mientras que permite al equipo remoto alertar a la plataforma de gestión SNMP cuando ocurre algún problema.

Entre las características principales cabe destacar:

- Operación off-line: pueden interrumpirse procesos de polling mientras el monitor sigue funcionando siempre.
- Monitorización preventiva: en caso de sistemas bien dimensionados, se puede enviar periódicamente información de estatus de la red a fin de prevenir posibles problemas.
- Detección de problemas y generación de informes: disposición de sondas activas.
- Datos de valor añadido: el monitor de redes puede realizar análisis específicos de la información de su red que no son accesibles con métodos directos (sólo hasta nivel MAC).
- Múltiples gestores: RMON permite la estructura de plataformas gestoras dispuestas de forma distribuida y jerárquica.

Uno de los principales alicientes del estándar RMON es el de proporcionar una arquitectura distribuida, frente al carácter centralizado del protocolo SNMP.

Las funciones MIB asociadas a RMON1 entran dentro los siguientes grupos:

Actividades a nivel de aplicación

- Filter: mecanismo de selección de paquetes de acuerdo a un determinado criterio.
- Packet capture: colección de paquetes y mecanismos de carga a través de criterios de filtrado.
- Events: mecanismo de control para acciones disparadas por una alarma.

Estadísticas de host

- Host: descubrimiento y estadísticas de hosts por direcciones MAC.
- Host Top N: estadísticas ordenadas por dirección MAC.
- Matrix: seguimiento de la conversación entre dos hosts.

Otros grupos

- Statistics: tráfico LAN acumulado y estadísticas de errores.
- History: estadísticas de muestreo de intervalo para análisis de tendencias.
- Alarms: niveles de disparo.
- Token Ring: 4 parámetros de las redes token-ring.

Finalmente se puede añadir que una red con sonda RMON (agente RMON): reduce el tráfico de gestión ya que analiza el tráfico, las alarmas, etc. y procesa toda la información de la red, mandando únicamente los datos significativos a la estación de gestión (p.e. estadísticas).
Y una red sin sonda RMON: se caracteriza por realizarse un polling continuo de la estación de gestión al monitor. La estación de gestión ha de procesar toda la información lo que provoca un mayor tráfico de gestión.

1.3.6 RMON 2

RMON 2 aparece como especificación RFC en 1996 como una extensión de RMON. RMON 2 añade respecto a la versión uno, la decodificación de paquetes entre los niveles 3 y 7 del modelo OSI. Ello trae consigo las siguientes consecuencias:

- Una sonda RMON2 puede monitorizar tráfico de acuerdo con protocolos de nivel de red y direcciones, incluido el Internet Protocol (IP). Esto permite a la sonda observar más allá de los segmentos LAN, a los cuales está conectado, y ver el tráfico entrante/saliente a la LAN vía routers (nodos específicos). Aplicable a la gestión de interconexión de redes.
- A causa de que la sonda RMON 2 puede decodificar y monitorizar tráfico a nivel de aplicación, tal como email, transferencia de ficheros, y protocolos WWW, la sonda puede grabar tráfico a y desde hosts para determinadas aplicaciones.

RMON 2 introduce, además, dos nuevas funcionalidades que mejoran el protocolo RMON: el uso de objetos indexados que no son parte de la tabla que éstos indexan, y el uso de indexado de filtro temporal.

Los grupos MIB que incorpora RMON 2, respecto a la versión anterior, son los siguientes:

- Protocol Discovery
- Protocol Distribution
- Adress Mapping
- Network Layer Host
- Network Layer Matrix
- Application Layer Host
- Application Layer Matrix
- User History
- Probe Configuration
- RMON Conformance

1.3.7 SYSLOG

El protocolo syslog definido en la RFC 3164, fue escrito por Eric Allman. Este protocolo provee el transporte que permite a los dispositivos enviar mensajes de notificación a través de las redes IP hacia las colectoras de mensajes también conocidos como servidores syslog.

En un sistema operativo UNIX, el "kernel" y otros componentes internos generan mensajes y alamas. Estos mensajes son típicamente almacenados en un "file system" (fichero de sistema) o reenviados a otro dispositivo en la forma de mensajes syslog.

El demonio interno llamado "syslogd" gestiona el proceso syslog. Este demonio es una parte integral de la mayoría de distribuciones UNIX/LINUX y no necesita ser descargado o instalado. Syslog provee un punto central de colección y procesamiento de los "logs" del sistema. Estos logs son usados para tareas de auditorias y troubleshooting (localización de fallas y averías).

Por ejemplo cuando un hacker bloquea un sistema, esta actividad es logeada y escrita en los mensajes syslog, por lo que estos mensajes pueden ser de mucha ayuda a los operadores y/o administradores de red para entender el ataque, identificar el daño y arreglar el sistema.

Syslog utiliza el protocolo UDP (User Datagram Protocol) por el puerto 514 en formato de texto plano. Aunque syslog tiene algunos problemas de seguridad, su sencillez ha hecho que muchos dispositivos y/o elementos de red lo implementen, tanto para enviar como para recibir. Eso hace posible integrar mensajes de varios tipos de sistemas en un solo repositorio central.

El tamaño del paquete syslog está limitado a 1024 bytes y posee los siguientes componentes: Facility, Severity, Hostname, Timestamp y Message, que a continuación, se describen:

- Facility, Los mensajes del syslog son categorizadas en base a las fuentes que las generan. Estas fuentes pueden ser el sistema operativo, el proceso, o una aplicación. Estas categorías llamadas "Facility" son representadas por números enteros, según las indicaciones de la Tabla 1.3. Los facilitys de uso local no son reservadas y están disponibles para el uso general. Por lo tanto, los procesos y las aplicaciones que no han preasignado valores de facility pueden elegir una de las ocho facilitys de uso local. Como tal, los dispositivos de Cisco utilizan uno de los facilitys de uso local para enviar mensajes del syslog (por ejemplo los switches CatOS y los concentradores VPN 3000 utilizan el facility de uso local 7 y los Cisco PIX firewalls usan el facility de uso local 4 por defecto para enviar sus mensajes syslog)

Tabla 1.3.- Lista de Facility

0	Mensajes del kernel.
1	Mensajes del nivel de usuario.
2	Sistema de correo.
3	Demonios de sistema.
4	Seguridad/Autorización.
5	Mensajes generados internamente por syslogd.
6	Subsistema de impresión.
7	Subsistema de noticias sobre la red.
8	Subsistema UUCP.
9	Demonio de reloj.
10	Seguridad/Autorización.
11	Demonio de FTP.
12	Subsistema de NTP.
13	Inspección del registro.
14	Alerta sobre el registro.
15	Demonio de reloj.
16	Uso local 0
17	Uso local 1
18	Uso local 2
19	Uso local 3
20	Uso local 4
21	Uso local 5
22	Uso local 6
23	Uso local 7

- Severity, La fuente o facility que genera el mensaje syslog también específica la severidad del mensaje usando un simple dígito entero (A menor valor del entero, aumenta el nivel de la alarma, es decir se hace más crítica), como se muestra en la Tabla 1.4.

Tabla 1.4.- Lista de Severidad

0	Emergencia: el sistema está inutilizable.
1	Alerta: se debe actuar inmediatamente.
2	Crítico: condiciones críticas.
3	Error: condiciones de error.
4	Peligro (warning): condiciones de peligro.
5	Aviso (notice): normal, pero condiciones notables.
6	Información: mensajes informativos.
7	Depuración (debug): mensajes de bajo nivel.

- Hostname, el campo "hostname" consiste en el nombre del host (configurado en el mismo host) o la dirección IP. En dispositivos como routers o firewalls que poseen multiples interfaces, syslog utiliza la dirección IP de la interfaz de donde el mensaje fue transmitido.
- Timestamp, este campo es el tiempo que tiene localmente el dispositivo cuando el mensaje fue generado, bajo el formato MMM DD HH:MM:SS.
- Message, este campo viene a ser el texto del mensaje syslog con cierta información adicional sobre los procesos que generaron el mensaje. Un ejemplo de estos mensajes son los generados por los dispositivos Cisco IOS, los cuales comienzan con el signo porcentaje (%) y usan el siguiente formato:

  %FACILITY-SEVERITY-MNEMONIC-MESSAGE_TEXT:
  - FACILITY: se refiere a la fuente del mensaje como un dispositivo de hardware, un protocolo o un modulo de software de sitema. Tener en cuenta que este FACILITY es especificado por Cisco y es sólo relevante en el mensaje y es diferente con el FACILITY definido en la RFC 3164.
  - SEVERITY: similar a la severidad definida en la tabla 2.3.
  - MNEMONIC: es un código de especificación de dispositivo que identifica únicamente al mensaje.
  - MESSAGE_TEXT: es el texto que describe al mensaje y puede contener detalles como número de puertos y direcciones de red.

Como resumen, en este capítulo se ha mostrado la evolución y situación actual de la gestión de alarmas, así como también, la variedad de protocolos más utilizados en las principales plataformas de gestión actuales, analizando sus funcionalidades y algunas comparaciones entre ellos.

CAPÍTULO II
SOLUCIÓN IBM TIVOLI NETCOOL

En el presente capítulo se describe la solución TIVOLI NETCOOL de IBM para las operadoras y empresas proveedoras de servicios de red, explicando a su vez la arquitectura de sus productos, sus fundamentos básicos y las ventajas y beneficios que brinda.

2.1 Descripción de la solución

Dado que la principal causa de los problemas que aquejan a las operadoras y proveedores de servicios de red es la falta de un sistema que unifique la monitorización de alarmas de todos los equipos de red y facilite la gestión de estos equipos, se propone la solución TIVOLI NETCOOL de IBM.

Esta solución está basada en la suite de productos TIVOLI NETCOOL de IBM que ofrecen varias herramientas para la gestión centralizada de alarmas en tiempo real y soluciones para la garantía de servicios, las cuales se ajustan con las necesidades actuales de las empresas de telecomunicaciones, operadoras, proveedores de servicios de red y empresas orientadas a negocios de TI (Tecnologías de la información) en general.

La solución TIVOLI NETCOOL permite a las compañías de telecomunicaciones, a los proveedores de servicios de Internet (ISP) y a todo tipo de empresas que ofrezca servicios de red, garantizar a sus clientes, los tiempos previstos de operación de sus servicios y aplicaciones de red, es decir garantiza la disponibilidad del servicio.

La plataforma TIVOLI NETCOOL supervisa el estado de la red en busca de posibles incidencias, alertas o disfunciones, de tal forma que posibilite la adaptación de la red a las necesidades de sus clientes.

A través de NETCOOL, los operadores de los centros de operaciones de red pueden comprobar gráficamente y en tiempo real qué ocurre en el interior de la red, lo que les permite responder y solucionar los problemas antes de que se produzcan cortes de servicio (up time).

TIVOLI NETCOOL está basada en una arquitectura abierta y permite ajustarse a cualquier entorno de red, desde entornos heterogéneos distribuidos a sistemas heredados y equipos de voz. Finalmente lo más importante, ofrece a las empresas, la

posibilidad de adaptar y configurar el sistema de monitorización a medida, personalizando la solución de acuerdo a sus necesidades específicas y requerimientos particulares.

2.2 Arquitectura de productos

La arquitectura de productos TIVOLI NETCOOL, que componen la solución a implementar y que se muestra en la Figura 2.1, está dividida en 3 capas:

- Capa de Colecta.
- Capa de Agregación.
- Capa de Visualización

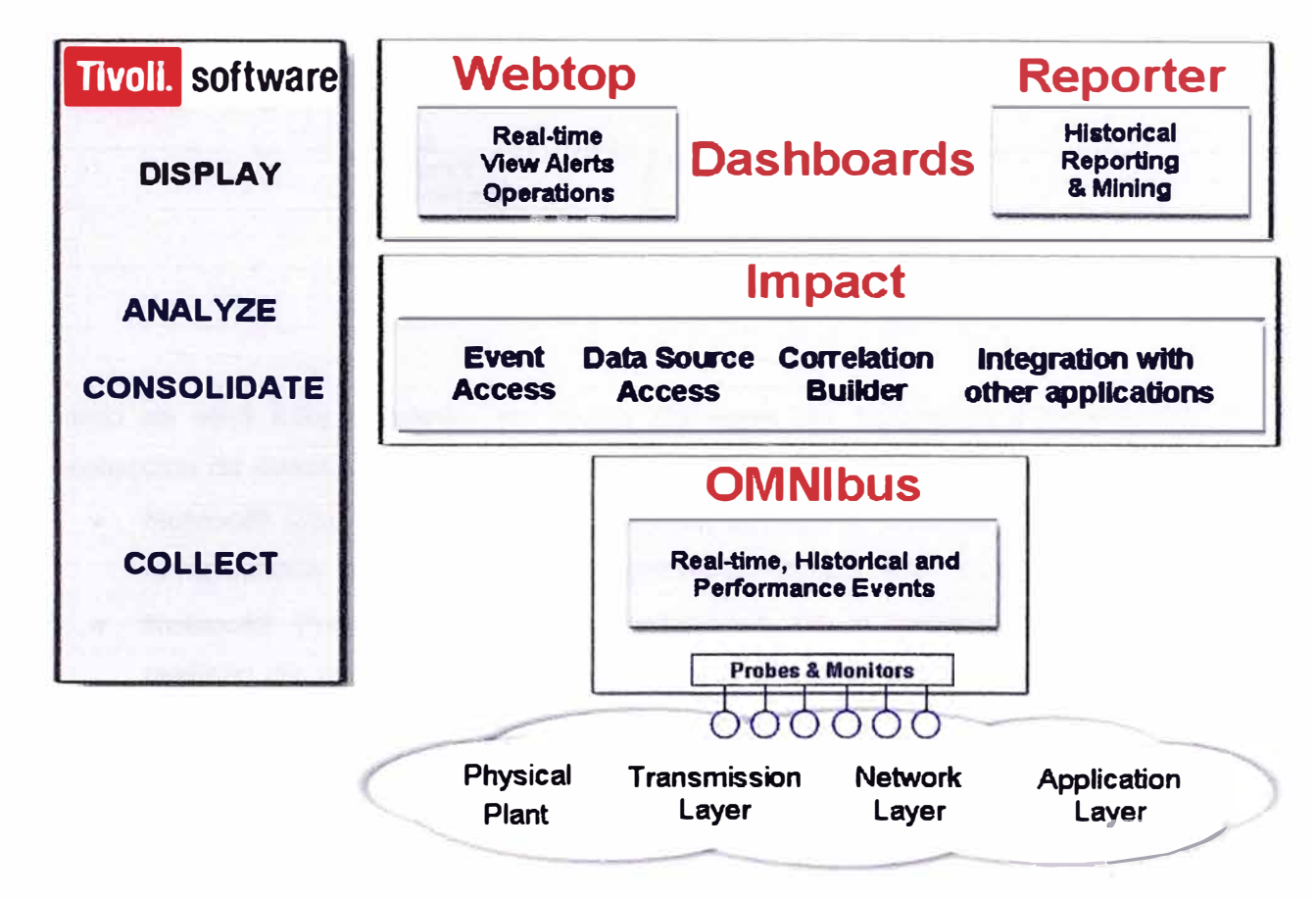


Figura 2.1.- Arquitectura de productos TIVOLI NETCOOL

2.2.1 Capa de Colecta

La capa de Colecta, está basada en el aplicativo Netcool® Omnibus™, tiene como función, la monitorización de los elementos de red y la recolección de los eventos en la red por medio de sondas especializadas (probes) par su posterior almacenamiento (repositorio centralizado de las alarmas). A continuación, en la Figura 2.2 se muestra la arquitectura de la capa de colecta.

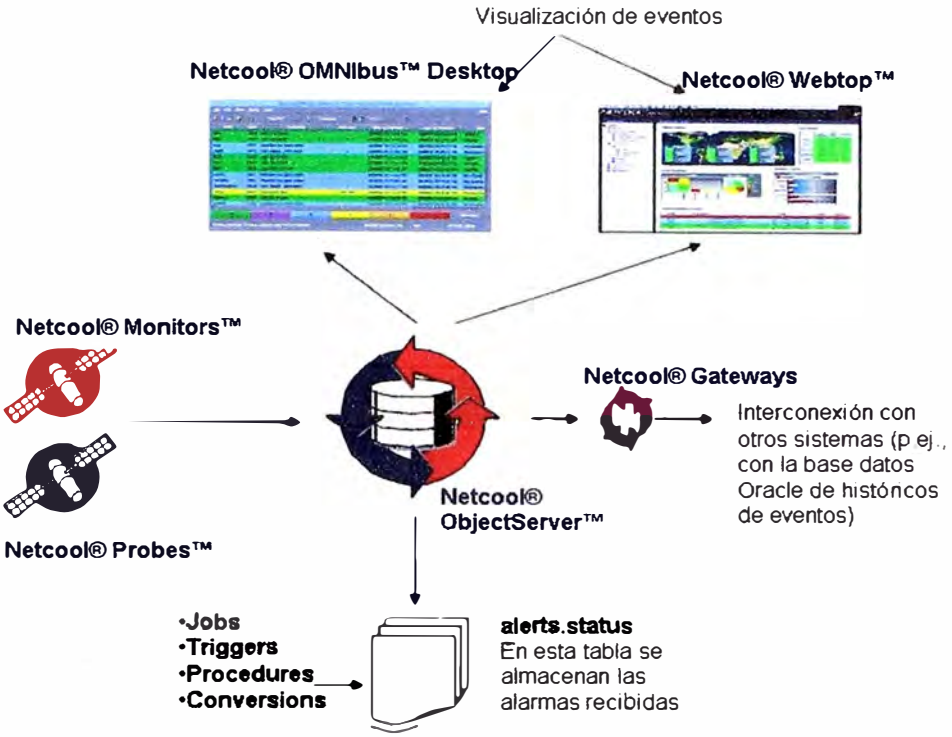


Figura 2.2.- Arquitectura de la capa de Colecta

Como se verá más adelante, se puede distinguir los siguientes componentes en la recolección de eventos:

- Netcool® ObjectServer™, es el corazón de todo el sistema de gestión, mantiene el repositorio centralizado de las alarmas en tiempo real.
- Netcool® Probes™ (Sondas), encargados de la recolección de eventos, lo realizan de manera pasiva, es decir reciben los eventos desde los gestores de equipos o directamente desde los equipos de red.
- Netcool® Monitors™, encargados también de la recolección de eventos, lo realizan de manera activa mediante el testeo periódico de servicios, existen 2 tipos: ISM (Internet Service Monitor – Monitor de servicios de Internet) para los servicios de Internet (DNS, HTTP, etc) y SSM (System Service Monitor – Monitor de servicios de sistema) monitoriza parámetros de sistema por ejemplo: memoria utilizada, capacidad en disco, procesos en ejecución, etc.
- Netcool® Gateways™, encargados para la interconexión entre ObjectServers (FailOver, en caso el ObjectServer primario se encuentra indisponible, el secundario toma el lugar de este automáticamente), con bases de datos como Oracle, par lo cual se utiliza el Gateway Oracle del Netcool® Reporter™.
- Netcool® Omnibus™ Desktop, para la visualización de las alarmas de manera nativa, en el mismo servidor donde está instalado el ObjectServer.

2.2.2 Capa de Agregación

La capa de Agregación, donde se realiza el análisis y consolidación de los eventos, así como también la integración a otros sistemas y/o aplicaciones como por ejemplo al bus EAI (Enterprise Application Integration – Integración de aplicaciones de empresa) basado en la aplicación comercial IBM WebSphere MQ. La herramienta principal en esta capa es el Netcool® Impact™, como se muestra en la Figura 2.3.

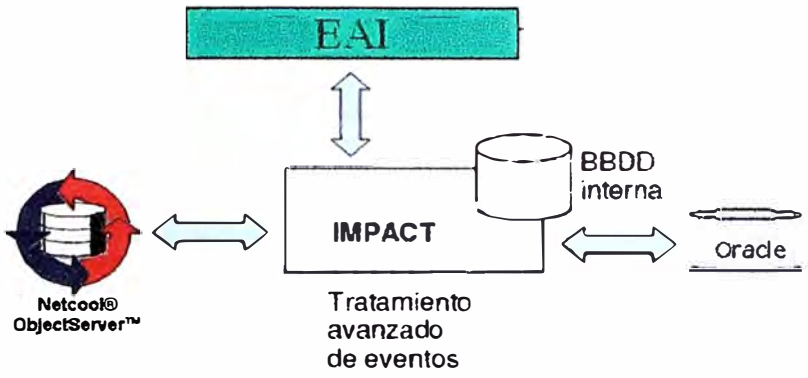


Figura 2.3.- Arquitectura Capa de Agregación

2.2.3 Capa de Visualización

La capa de Visualización, basada en los aplicativos Netcool® Reporter™ (para el almacenamiento del histórico de las alarmas y los informes estadísticos de las mismas) y Netcool® Webtop™ (para la presentación de las alarmas en una interfaz web). En la Figura 2.4 se muestra la arquitectura de la capa de visualización.

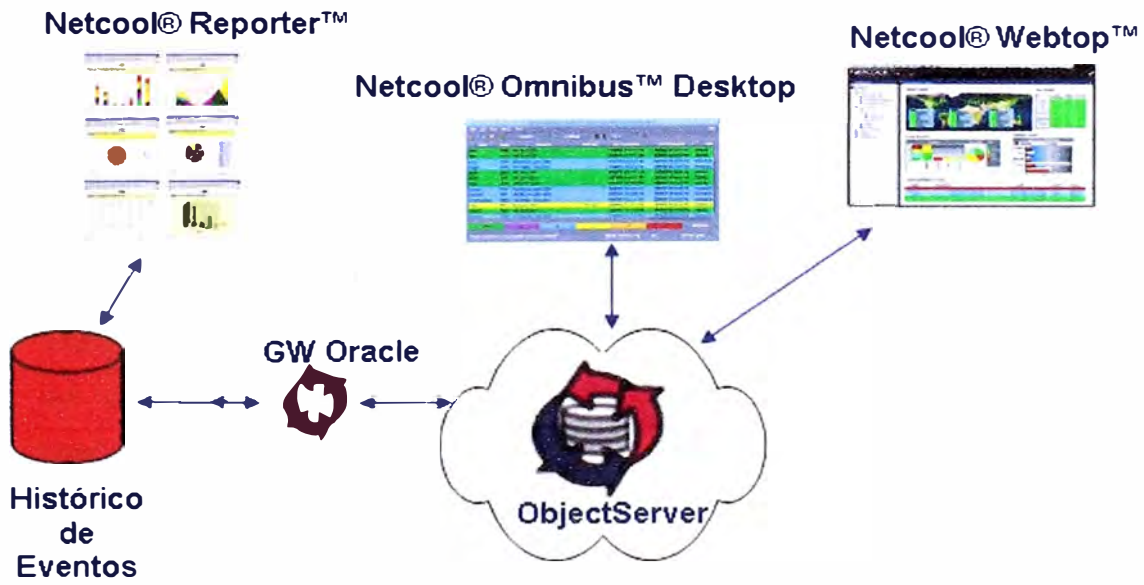


Figura 2.4.- Arquitectura Capa de Visualización

Se puede resumir la solución TIVOLI NETCOOL, de la siguiente manera:
La recolección de eventos se puede dar de dos maneras: pasiva o activa. La recolección pasiva es realizada por sondas (probes), las cuales reciben los eventos de los gestores de red o directamente de los propios elementos de red. La recolección activa en cambio es realizada por los monitores ISM y SSM, los cuales se encargan de realizar testeos periódicos (polling) tanto a los servicios de Internet (DNS, HTTP, etc) como a los servidores donde corren dichos servicios, respectivamente.
Los eventos recibidos por las probes y monitores son enviados al repositorio centralizado de alarmas (Object Server) para su futuro tratamiento y enriquecimiento de información en la capa de Agregación que a su vez brinda la posibilidad de integración a otros sistemas.
El ObjectServer trabaja sólo con los eventos actuales (on-line) para que se disponga de la información de los históricos de eventos, las alarmas son enviadas a medida que llegan a una base de datos Oracle externa, esta función es realizada por el Gateway Reporter que es una herramienta que viene incluida dentro del aplicativo Netcool® Reporter™ quien a su vez se encarga de generar los informes de eventos que serán visualizados por los usuarios a través de la interfaz web proporcionada por Netcool® Webtop™, en dicha interfaz también se visualizan las alarmas disponibles en el Object Server.

2.3 VENTAJAS Y BENEFICIOS

Entre las principales ventajas y beneficios que ofrece TIVOLI NETCOOL se encuentran:

- Un punto central de gestión de las operaciones de red y de TI (Tecnologías de la Información), incluyendo aplicaciones empresariales, dispositivos de red, protocolos de Internet, dispositivos de seguridad, etc.
- Optimiza la disponibilidad y flexibilidad del servicio a través de funciones automatizadas de correlación, aislamiento y resolución que le permiten identificar y resolver rápidamente los problemas más críticos del servicio.
- Consolidación de datos, aumento de información de las alarmas con datos obtenidos de bases de datos de otros sistemas y viceversa.
- Visualización web de las alarmas, con vistas de servicios e informes estadísticos del histórico de alarmas.
- Notificación automática de los eventos a los operadores y a los técnicos designados, mediante correo electrónico o mensajes de texto SMS.
- Soporte a estándares actuales y en evolución, incluidos ITIL (Biblioteca de Infraestructura de Tecnologías de Información), IPv4 e IPv6.

- Agilidad personalizable para recopilar sucesos empresariales y tecnológicos de más de 1.000 fuentes en tiempo real.

En este capítulo se ha descrito la solución TIVOLI NETCOOL de IBM, explicando el funcionamiento de la solución y los aplicativos que forman parte de ella. Lo mostrado en este capítulo es la base para el diseño e implementación de un sistema de monitorización de alarmas utilizando la suite TIVOLI NETCOOL.

CAPÍTULO III
IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE ALARMAS

Una vez concluida la explicación de los aplicativos TIVOLI NETCOOL en el capítulo II, el presente capítulo se encargará de describir la implementación de un sistema de monitoreo de alarmas de equipos de red, tomando como referencia la red de Telefónica Empresas de Argentina (TEA), el presente sistema tiene como principal función la gestión de los servicios de acceso a Internet que ofrece la empresa a través de su red.

3.1 Análisis de la problemática en la gestión de alarmas

Antes de describir la implementación del sistema de monitorización de alarmas, se pasará a realizar un análisis global del problema que tienen hoy en día, las empresas de telecomunicaciones y empresas proveedoras de servicios de red en general, en la gestión de sus alarmas de red.

3.1.1 Descripción del problema

La gestión de alarmas de los equipos de red se ha convertido a lo largo de los años en una tarea estratégica y de vital importancia para las operadoras y compañías proveedoras de servicios, debido principalmente al rol que juega en el buen funcionamiento de la red y en la calidad del servicio proporcionado. Sin embargo debido al constante crecimiento de las redes tanto en tamaño (interconexión de redes, aumento de equipos de diferentes fabricantes) como en complejidad (mayor número de sistemas de gestión propietarios) no tardaron en aparecer los siguientes problemas en las operadoras:

- Incremento en los tiempos de diagnostico y solución de problemas.
- Perdidas en el rendimiento y disponibilidad del servicio.
- Mayor dificultad al introducir nuevos servicios.
- Aumento en los costos de operación y mantenimiento.

A raíz de ello, surge la necesidad en las operadoras de reemplazar y/o integrar los obsoletos sistemas de gestión de alarmas propietarios a un nuevo sistema capaz de unificar la monitorización de las alarmas de los equipos y satisfacer las nuevas necesidades del operador.

Es en este sentido, que se plantea implementar un sistema de monitorización, basado en los productos TIVOLI NETCOOL de IBM ya que además de ser una de las mejores soluciones disponibles en el mercado de plataformas de gestión, es la solución escogida y recomendada por las operadoras líderes en el mundo.

3.1.2 Antecedentes del problema

El progreso tecnológico de las redes de comunicación de datos en los últimos años ha conducido al desarrollo de los sistemas de gestión de alarmas en diferentes organizaciones.

El abaratamiento de los costos en el diseño y desarrollo de estas redes y el aumento de las capacidades de procesamiento, condujeron a muchas organizaciones a migrar sus actuales sistemas de información de arquitecturas centralizadas a arquitecturas distribuidas, dispersas geográficamente.

En este sentido las redes surgieron como medio de interconectar diferentes equipos (de diversos fabricantes) instalados remotamente unos de otros, ofreciendo capacidades de acceso a servicios de otras redes, como por ejemplo: capacidades adicionales de proceso, accesos a bases de datos internacionales, etc.

La existencia de dichos equipos dispersos sobre los que se implementan e interconectan todas estas redes para el acceso a servicios avanzados de telecomunicaciones y la exigencia cada vez mayor de los clientes por servicios de mejor calidad y menor precio impulsa a las empresas a disponer de sistemas de gestión única para toda la red en lugar de sistemas de gestión de alarmas individualizada y/o fragmentada, especialmente cuando se trata de redes a gran escala y con aplicaciones de servicios críticos.

3.2 Descripción de la red TEA

La red de Telefónica Empresas de Argentina (TEA) que se muestra en la Figura 3.1, se divide en 3 secciones:

- Red de acceso.
- Red de transporte.
- Red de núcleo (core IP/MPLS).

3.2.1 Red de acceso

La red de acceso, abarca desde los routers Cisco (Serie 800, 1600, 1700, 2500, etc) que se encuentran en el lado del cliente CPE (Customer Premise Equipment – Equipo local de cliente) hasta los equipos Path Newbridge y los modems satelitales iDirect que proporcionan la interfaz entre el CPE con la red de transporte.

3.2.2 Red de transporte

La red de transporte, basada en la tecnología ATM (Asynchronous Transfer Mode – Modo de transferencia asíncrona) comprende los equipos switch BPX de Cisco y los switch multiservicio Passport y DPN de Nortel.

3.2.3 Red de núcleo (core IP/MPLS)

La red de núcleo (backbone), basado en la tecnología IP/MPLS comprende los equipos PE (provider equipment) que proveen el acceso al core IP/MPLS y los equipos P (providers) que son los que operan en el core IP/MPLS y permiten la interconexión con las redes de otros proveedores (ISP)

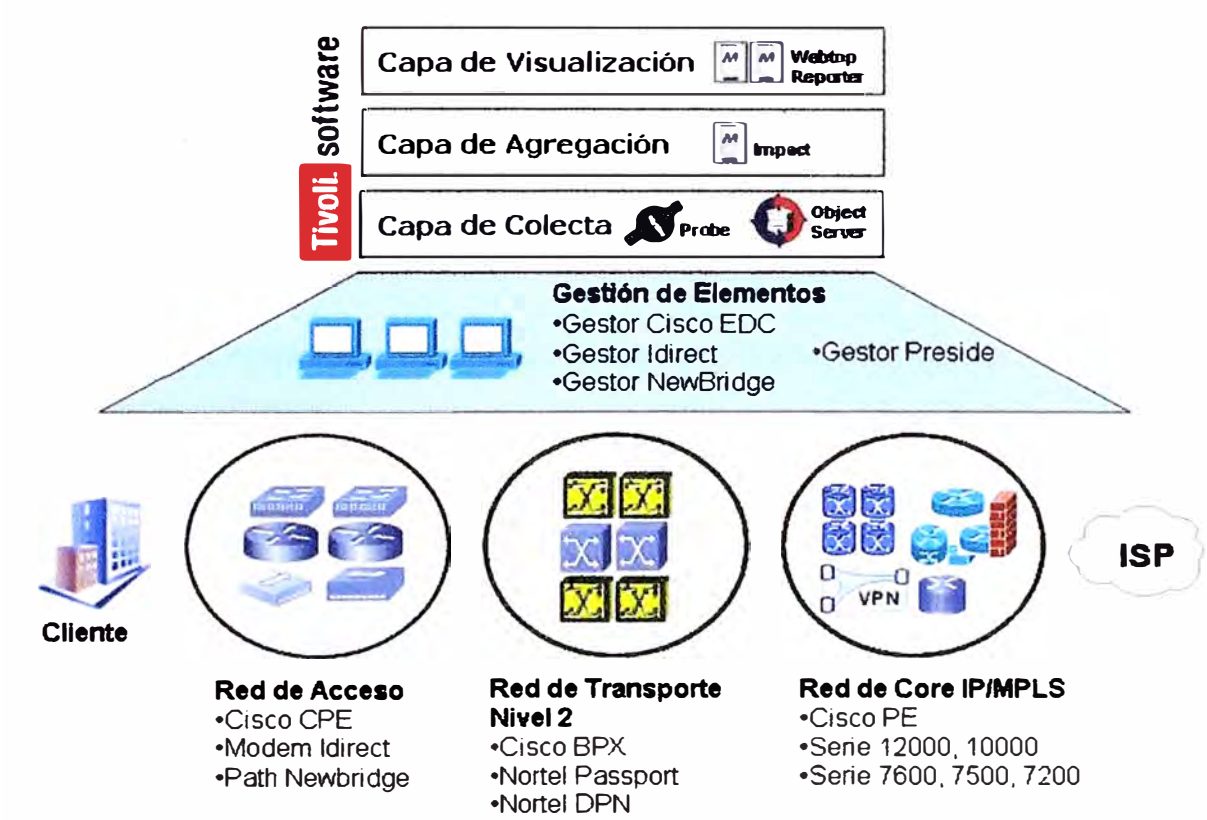


Figura 3.1.- Arquitectura de la red de TEA

3.3 Funcionamiento del servicio de acceso

El servicio de acceso a Internet que provee TEA, hace referencia a los siguientes conceptos:

Número de Referencia, hace referencia a un servicio y tiene vinculado uno o varios números de orden (OSE). La referencia se vincula a un acceso de cliente comprendiendo el tramo que va desde el CPE de cliente hasta el PE.

Número de Orden de Servicio, en adelante OSE (Orden de Servicio), se asocia a cada uno de los siguientes elementos de red

- Interfaz física/lógica del CPE; en el caso de que un CPE tenga varios números de Referencia asociados, cada uno de ellos referenciaría a interfaces diferentes dentro del mismo CPE (ejemplo: Supongamos que un CPE1 tiene asociados dos números de Referencia X e Y, en cada uno de ellos el OSE que se asocia al CPE hará referencia a interfaces físicas/lógicas diferentes, por ejemplo Serial0/0.20 y Serial0/1.24)
- PATH; se pueden presentar una doble casuística: PATH Newbridge y PATH Satelital (en este escenario, las alarmas que se reciban de los módems del entorno iDirect estarán vinculadas a este OSE).
- Interfaz física/lógica del elemento de transporte de nivel 2, las casuísticas contempladas son (en todas los casos se trata de la interfaz del lado del CPE): Interfaces físico/lógicas ATM, Interfaces físico/lógicas FR e Interfaces físico/lógicas X.25.
- Interfaz física/lógica del PE

En la Figura 3.2 mostrada a continuación, quedan plasmados cada uno de los conceptos anteriormente indicados:

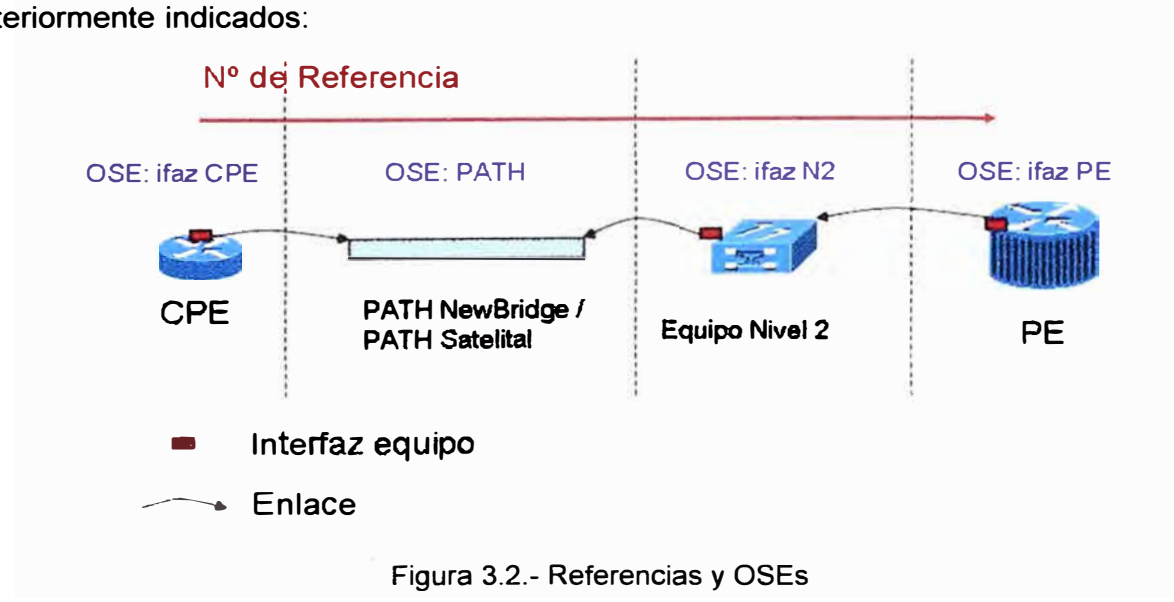


Figura 3.2.- Referencias y OSEs

A nivel de elementos de red se establece la siguiente categorización:

- CPE: equipos de cliente
- Transporte físico de Nivel 1: Path Newbridge / Path Satelital
- Transporte Nivel 2: equipos de transporte hasta PE
- PE: equipo de acceso a Core IP/MPLS
- P: equipo de Core IP/MPLS

3.3.1 Escenarios de acceso

Se contemplan dos tipos de escenarios de acceso, CPE gestionado lejano y CPE gestionado cercano, desde el CPE al PE:

- CPE Gestionado Lejano, como se muestra en el Figura 3.3, este tipo de acceso tiene asociado un único número de Referencia y cuatro OSEs: una interfaz física/lógica del CPE, PATH Newbridge o Satelital, una interfaz física/lógica del elemento de transporte de nivel 2 (ATM, FR o x.25) y una interfaz física/lógica del PE.

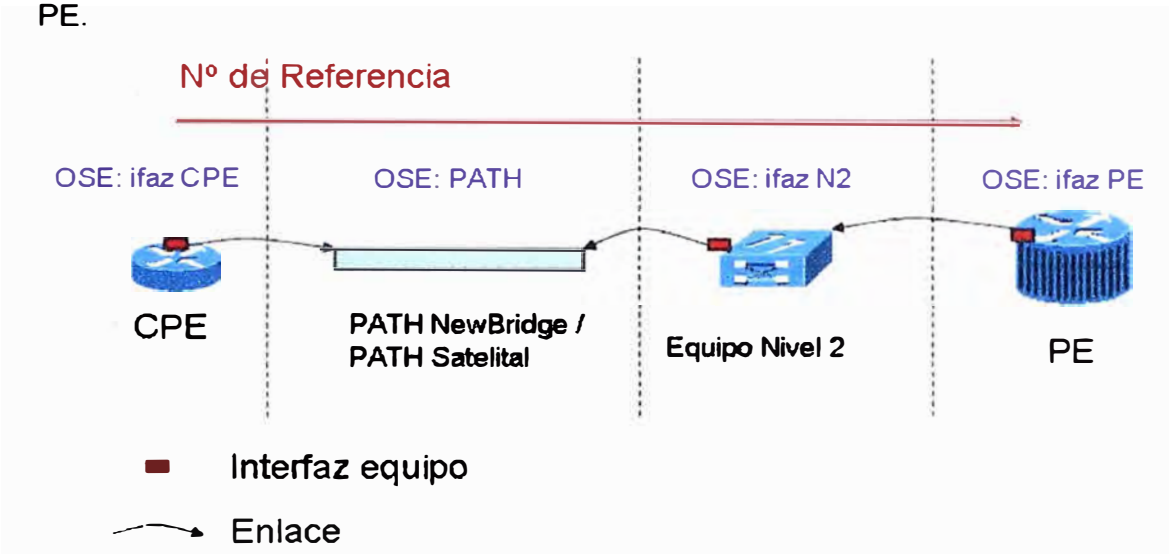


Figura 3.3.- CPE gestionado lejano

- CPE Gestionado Cercano, como se muestra en la Figura 3.4, este tipo de acceso tiene asociado un único número de Referencia y tres OSEs: una interfaz física/lógica del CPE, una interfaz física/lógica del elemento de transporte de nivel 2 (ATM, FR o x.25) y una interfaz física/lógica del PE.

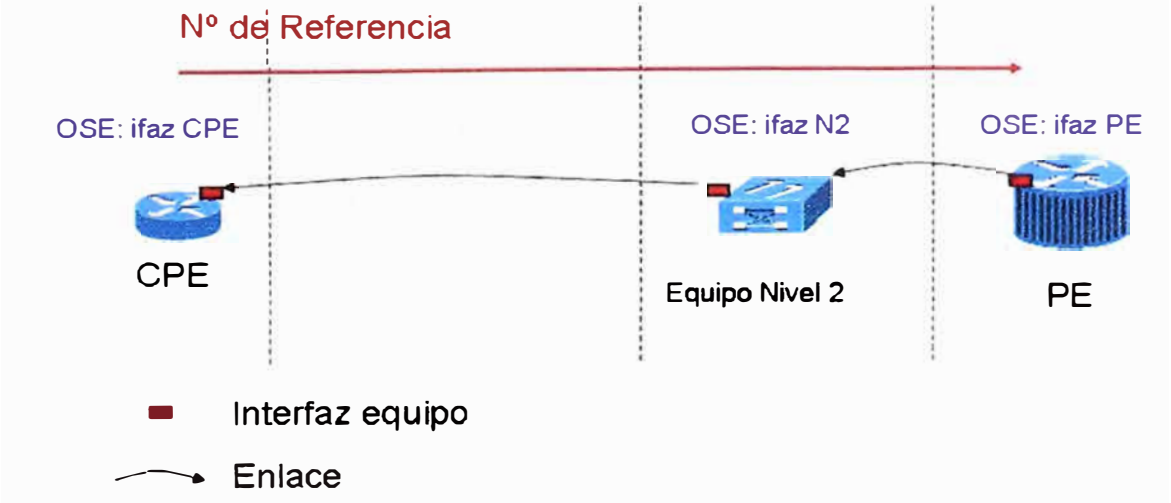


Figura 3.4.- CPE gestionado cercano

3.3.2 VPN (Virtual Private Network)

Las redes privadas virtuales, son utilizadas por TEA principalmente para brindar conectividad a las empresas (cliente) desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etc) utilizando Internet como vínculo de acceso, logrando proporcionar un nivel de acceso comparable al de la red local.

Cada VPN de TEA posee a nivel de servicio varios números de Referencias, cada referencia esta asociado a uno de los accesos y a X OSEs en función del tipo de acceso definido en el apartado 3.3.1.

3.4 Lista de equipos

La lista de equipos que conforman la red que se va a monitorizar se muestra en la Tabla 3.1.

Tabla 3.1.- Lista de equipos

EQUIPOS	RED	CATEGORÍA
Cisco 805 Cisco 1600 Cisco 1700 Cisco 2500 Cisco 2600 Cisco 2920 Cisco 3000 Cisco 3600 Cisco 3700 Cisco 3810 Cisco 4500 Cisco 7200	Acceso EDC	CPE
iDirect 3000 iDirect 5000 iDirect 7000	Acceso Satelital	PATH (transporte de nivel 1)
Alcatel 3640 Alcatel 7470	Transporte Newbridge	PATH (transport de nivel 1)
BPX	Transporte ATM (PATH ATM - Red BPX)	N2 (transporte de nivel 2)
Nortel Passport 7440 Nortel Passport 7480	Transporte FR/X.25/ATM (PATH FR/X.25/ATM - Red Passport)	N2 (transporte de nivel 2)
DPN	Transporte FR/X.25 (PATH FR/X.25 – Red DPN)	N2 (transporte de nivel 2)
Cisco 12000 Cisco 10000 Cisco 7600 Cisco 7500 Cisco 7200	Core IP/MPLS	PE / P

3.5 Fundamentos productos IBM TIVOLI NETCOOL

La lista de productos IBM TIVOLI NETCOOL que forman parte de la solución a implementar son:

- Netcool® Omnibus™
- Netcool® Impact™
- Netcool® Reporter™
- Netcool® Webtop™

3.5.1 Netcool® Omnibus™

Esta herramienta tiene como función principal centralizar la recolección y almacenamiento de eventos y/o alarmas en el sistema, consta de los siguientes componentes, mostrados en la Figura 3.5.

- Netcool® ObjectServer™
- Netcool® Probes™ (Sondas)
- Netcool® ISM™ (Internet Service Monitor)
- Netcool® SSM™ (System Service Monitor)

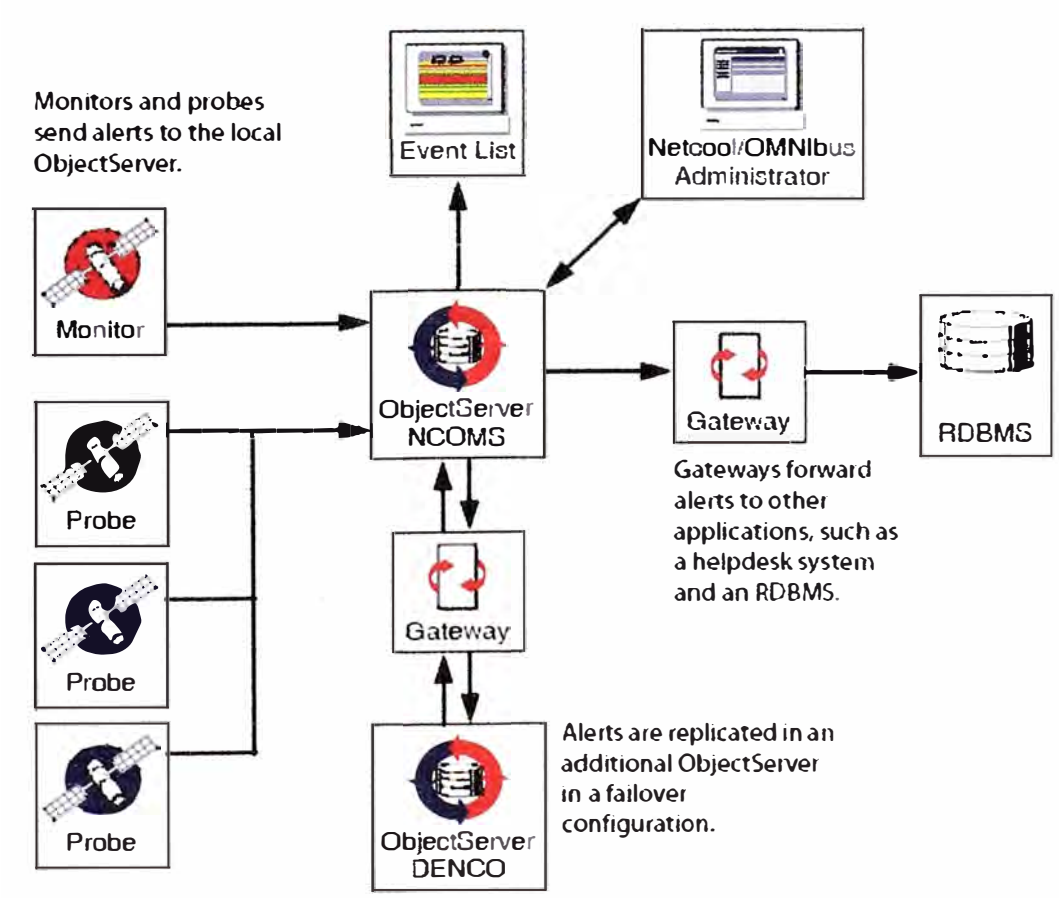


Figura 3.5.- Arquitectura Netcool® Omnibus™

a) Netcool® ObjectServer™

El ObjectServer puede ser comprendido como una base de datos Sybase que contiene todos los eventos que en el momento están afectando a la red, cada evento es representado por un registro SQL (Structured Query Language – Lenguaje de consulta estructurado). Las propiedades principales del Netcool® ObjectServer™ son:

- Base de Datos residente en memoria.
  - Acceso rápido.
  - Formato homogéneo de eventos.
- Recibe los eventos que le envían las Netcool® Probes™ y los Netcool® Monitors (ISM y SSM)
- Realiza el procesado básico de los eventos recibidos (automatizaciones, procedures y tools).
- Transfiere los eventos recibidos a otros componentes usando Netcool® Gateways (por ejemplo el Gateway de Oracle)
- Despliega los eventos y/o alarmas al usuario final usando diferentes interfaces:
  - Nativa destinada a los administradores (Netcool® Omnibus™ Desktop).
  - Web destinada a los operadores (Netcool® Webtop™).

La base de datos en memoria permite un acceso muy rápido a la información, Las sondas y monitores introducen los eventos recolectados de la red en la BBDD en memoria que es el núcleo del módulo de alarmas de SIGRES. El resto de componentes conecta con esta base de datos del ObjectServer para operaciones de R/W (lectura/escritura).
Los gateways son usados para transferir datos de un Object Server a otros componentes Netcool (por ejemplo, la base de datos Oracle que se usa como almacenamiento de históricos).
La visualización de eventos se realiza de dos formas, una mediante una consola nativa en Unix (Desktop) que está destinada principalmente a la administración de la herramienta, y un servidor Web (Webtop), que permite visualizar todas las alarmas mediante un navegador web. Con Webtop, además de las listas de eventos es posible ver mapas, gráficos estadísticos, y acceder a reportes de la BBDD de históricos, así como a mapas topológicos. Webtop posee una consola de administración, accesible solo para usuarios administradores.

b) Netcool® Probes™ (Sondas)

Las Netcool® Probes™ son procesos (programas binarios) que recolectan la información procedente de los equipos activos de red o de sistemas de gestión propietarios y la

envían al Netcool® ObjetServer™. "Traducen" la información, que envían al formato de alarma normalizada que posteriormente será mostrada a los operadores. En la Figura 3.6 se muestra el proceso de recolección de eventos.

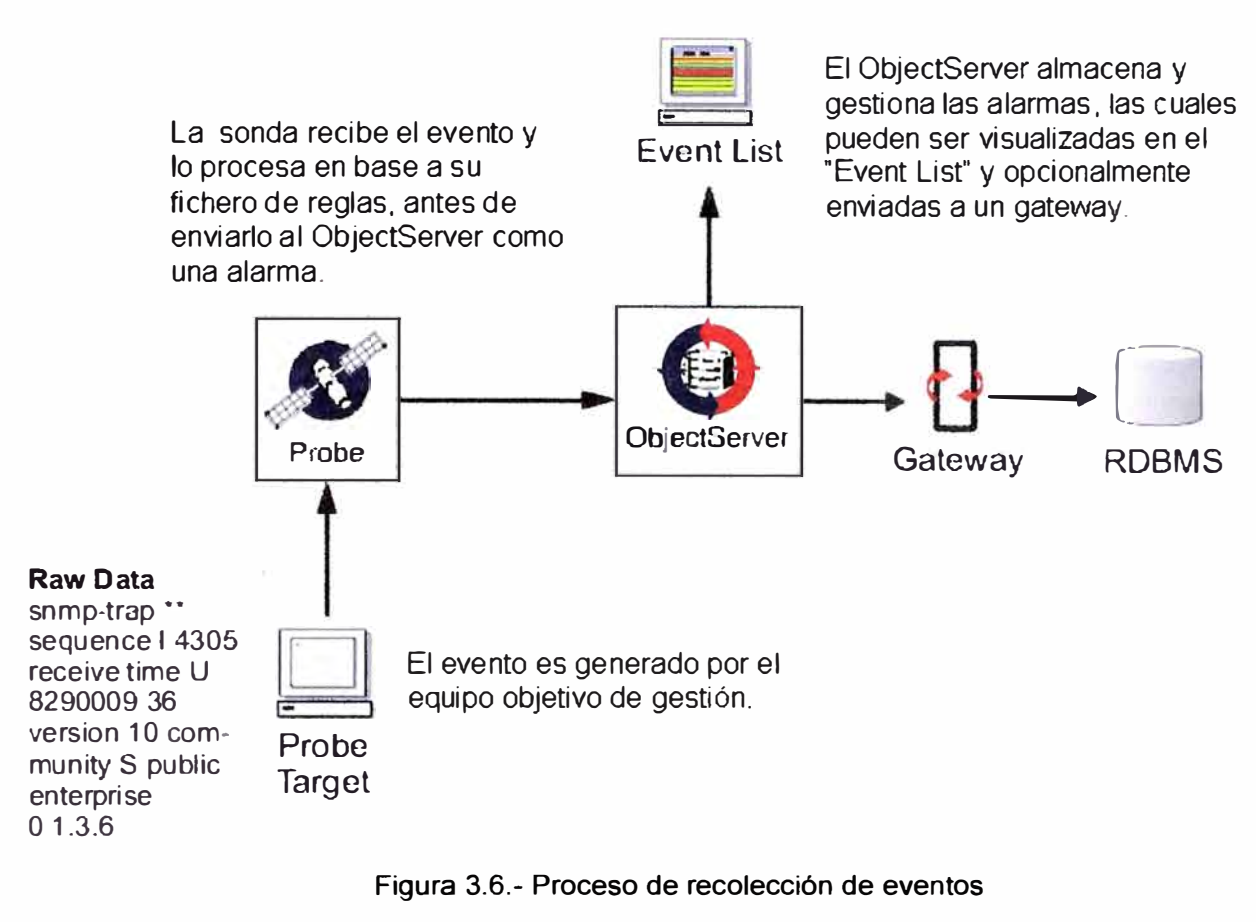


Figura 3.6.- Proceso de recolección de eventos

Las probes pueden instalarse en el mismo servidor donde se instala el ObjectServer o en un servidor remoto, son además, el primer nivel de procesado de eventos.

El sentido de las probes, es obtener la información de los eventos de una fuente (gestores propietarios o los mismos elementos de red), transformarlos en el formato de evento común y enviarlos al ObjectServer.

Cuando la probe recibe una cadena de datos, particiona esa cadena en elementos individuales (tokens $), con los cuales construye el evento. La probe o sonda utiliza un archivo de reglas donde se define la asignación de estos elementos 'particionados' a los campos de evento que se volcarán en la tabia "alerts.status" (tabla donde se almacenan las alarmas).

En el fichero de reglas se puede añadir también información extra al evento y realizar operaciones matemáticas.

Dependiendo del origen de los datos se utiliza un tipo de probe u otra, para nuestra solución, se utilizan 3 tipos de probes GLF (para la recolección de eventos desde ficheros

de log), SYSLOG (para la recolección de eventos desde mensajes syslog) y MTTRAPD (para la recolección de eventos desde traps SNMP), como se muestra en la Figura 3.7.

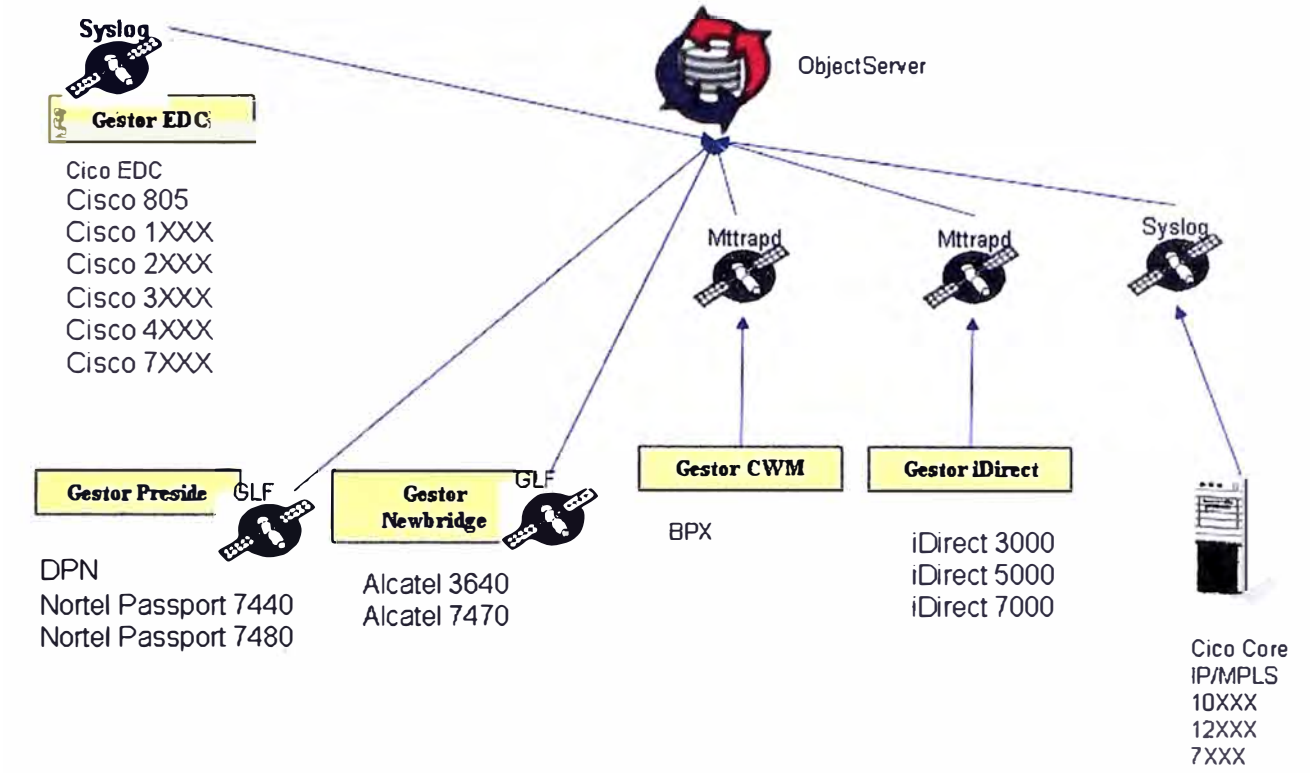


Figura 3.7.- Clasificación de plataforma por tipo de sonda

En la Figura 3.8 se muestra, el modo de operación de una probe, la cual puede dividirse en cinco etapas:

- **1.- Inicialización:** La probe se conecta al ObjectServer, identificando el formato de la tabla "alerts.status". Se leen y analizan los ficheros props y rules de la probe y esta queda preparada para recibir los eventos.
- **2.- Recuperación de Eventos:** La probe recupera los eventos de la fuente de datos. Esta operación puede realizarse a través de un API, leyendo un archivo de log o conectándose a un puerto serie, por ejemplo.
- **3.- Partición:** La probe particiona la cadena de datos del evento en elementos individuales (tokens $), los cuales son utilizados en el archivo de reglas.
- **4.- Archivo de Reglas (Rules File):** Una vez que la probe ha particionado la cadena de datos del evento, el evento es analizado por el archivo de reglas, donde se fijan los valores de los campos (@) de las alarmas.
- **5.- Envío de Evento:** El último paso consiste en enviar el evento al ObjectServer, asegurándose de que dicho evento es recibido. Si ocurriese cualquier problema durante el envío, la probe almacenará el evento en un archivo a la espera de recuperar la conexión con el ObjectServer para poder enviarlo nuevamente.

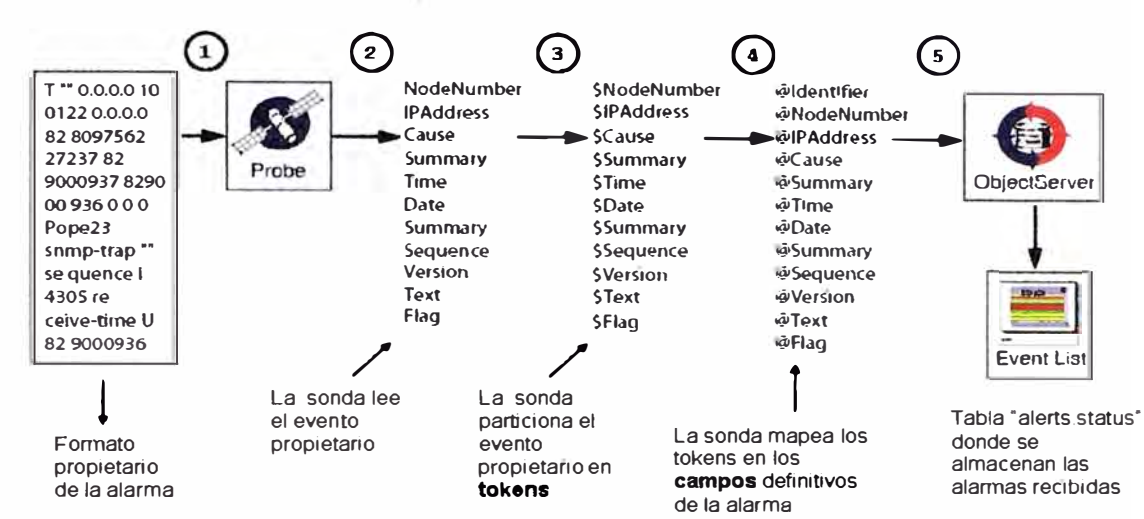


Figura 3.8.- Modo de operación de una probe

c) Netcool® ISM™ (Internet Service Monitor)

Los monitores ISM permiten la monitorización de los servicios de Internet comportandose como un usuario final, es decir realizan testeos como si fuera un usuario tratando de utilizar el servicio. En la Figura 3.9 se muestra su tipo de monitorización.

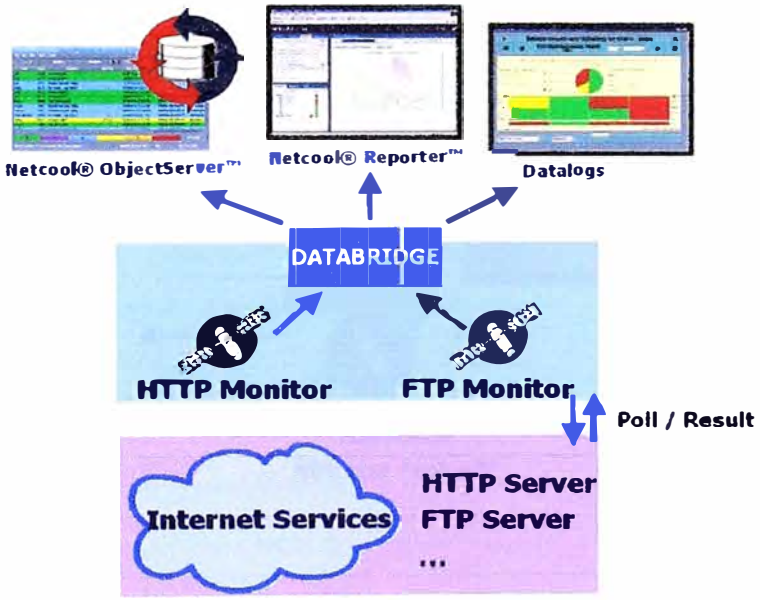


Figura 3.9.- Monitorización ISM

Propiedades principales del Netcool® ISM™ (Internet Service Monitor):

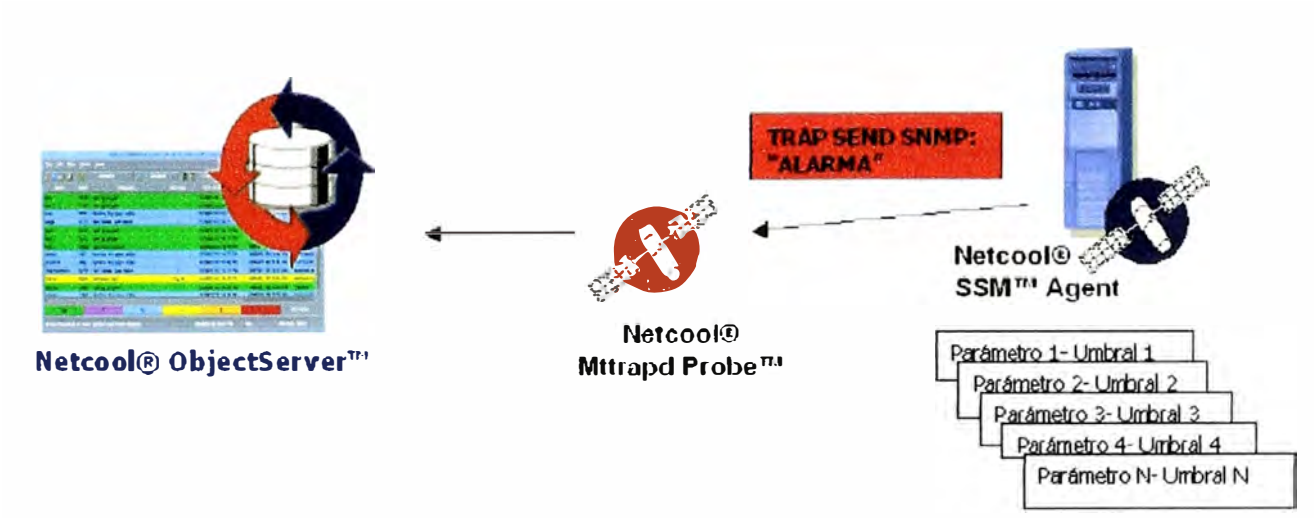
- Procesos (programas binarios) que realizan la monitorización de servicios IP.
- Los Netcool® ISM™ Monitors, se diferencian por el tipo de protocolo a monitorear (HTTP, ICMP, LDAP, RADIUS, etc).
- Componentes activos: realizan tests periódicos sobre los servidores que ofrecen los servicios a monitorizar.

- El resultado de dichas pruebas es utilizado para:
  - Generar alarmas que se envían al Netcool® ObjectServer™.
  - Información del estado de servicio, datalogs.
- Los Netcool® ISM™ Monitors permiten la visualización del estado actual e histórico de los servicios monitorizados.

En resumen se puede decir que la herramienta Netcool® ISM™ es una aplicación diseñada para monitorizar la confiabilidad, tiempo de respuesta y funcionamiento de los servicios de Internet como Aplicaciones Web, E-mail, DNS, FTP, HTTP, etc.

d) Netcool® SSM™ (System Service Monitor)

Netcool® SSM™ es una aplicación que mide la disponibilidad y rendimiento de los servidores y las aplicaciones que se ejecutan en dichos sistemas.
Netcool® SSM™ monitoriza los cambios en las condiciones de la configuración, estado de las aplicaciones y ficheros del sistema. Cuando se sobrepasan unos determinados umbrales (threshold) de funcionamiento previamente establecidos, se genera una alarma que será enviada al ObjectServer, tal como se muestra en la Figura 3.10.



Una vez superado uno de los umbrales definidos en Netcool® SSM™ Agent dentro del dispositivo, se genera un send trap hacia el Netcool® ObjectServer™, el cual se encargara de almacenar, deduplicar, y correlacionar el evento y/o alarma reportada por el SSM™ Agent. Este evento y/o alarma podrá ser observado por el operador a través de interfase Web de la solución Netcool® Webtop™.

Figura 3.10.- Monitorización SSM

Netcool® SSM™ está compuesto por los siguientes elementos:

- El agente maestro: más conocido como agente, constituye la base del Netcool® SSM™. El agente se instala en las máquinas que se desea monitorizar. Su función principal es la de proveer la plataforma para los subagentes.
- Subagentes y módulos MIB: la capacidad de monitoreo está implementada en los subagentes y las MIBs. Las MIBs (Management Information Base) constituyen la base de datos de las configuraciones realizadas y las métricas obtenidas de los parámetros y aplicaciones del sistema. Los subagentes constituyen la interface SNMP que se encarga de realizar el monitoreo y las medidas de los parámetros definidos en los módulos MIB asociados. Los subagentes son cargados y ejecutados por medio del agente maestro. Algunos de los parámetros por defecto que se monitorizan son: estrés de procesos, carga de disco, ocupación de CPU, estado de dispositivos e interfaces, errores en interfaces, etc.

3.5.2 Netcool® Impact™

Netcool® Impact™ es la principal herramienta de análisis y correlación de datos para la suite de productos Netcool. Utilizado principalmente para personalizar y mejorar el rendimiento del ObjectServer haciendo posible el enriquecimiento de eventos y la integración con otros sistemas como bases de datos (Oracle), sistemas de mensajería (EAI – MQSeries), aplicaciones de inventario, etc. Impact puede enriquecer y actualizar un determinado evento con información contenida en su base de datos interna o en otras bases de datos como Oracle por ejemplo. En la Figura 3.11 se muestra el esquema Netcool® Impact™ con la integración a otros aplicativos y/o base de datos.

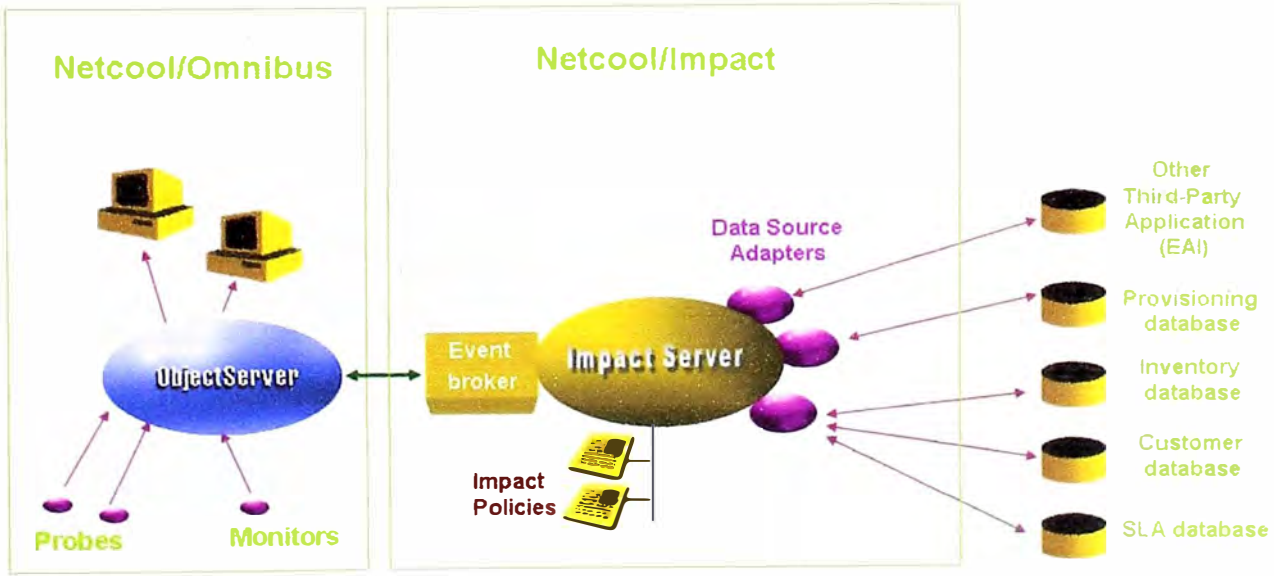


Figura 3.11.- Esquema Netcool® Impact™

3.5.3 Netcool® Reporter™

Netcool® Reporter™, es una aplicación cliente servidor basada en web que proporciona funcionalidades de creación, diseño y vista de reportes sobre la base de datos Oracle (histórico de alarmas), es posible generar informes de históricos de eventos y/o alarmas en base a los registros almacenados en una Base de Datos Oracle. Los reportes definidos y generados pueden ser integrados en la herramienta de contenidos web Netcool® Webtop™. Reporter proporciona una capacidad histórica de almacenamiento de reportes configurable de acuerdo a la capacidad en disco del servidor.

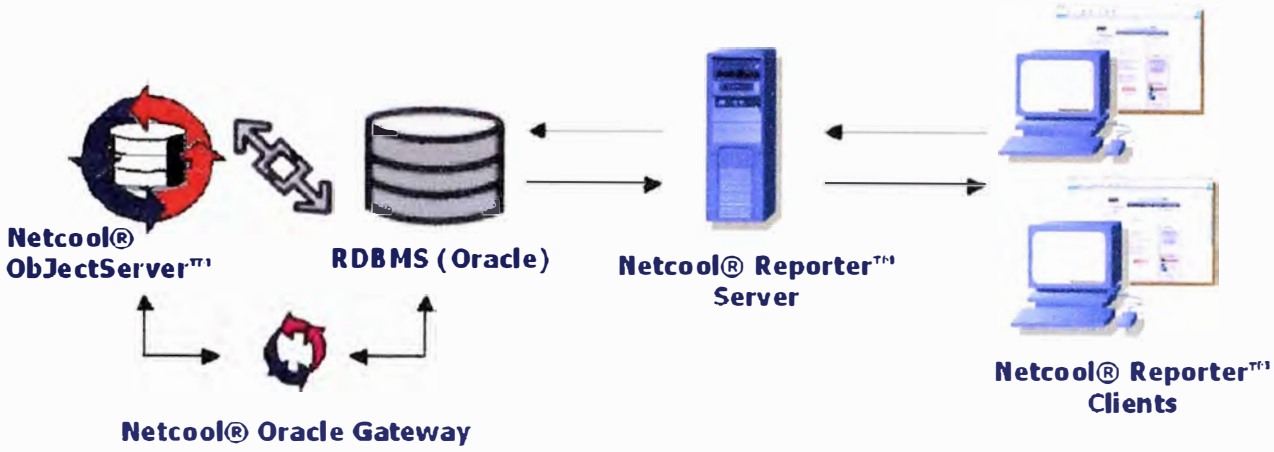


Figura 3.12.- Esquema de funcionamiento Netcool® Reporter™

En la Figura 3.12, se muestra el funcionamiento de Netcool® Reporter™; los eventos recolectados por las probes son inicialmente almacenados en el ObjectServer, a su vez almacenados en la Base de Datos Oracle, mediante el gateway oracle de Netcool® Reporter™.

En la web de Supervisión Netcool® Webtop™ se realizan consultas desde el servidor de Reporter hacia la Oracle DB (DataBase – Base de datos). La creación de cada reporte es configurable por usuario y se realiza mediante una fácil herramienta de elaboración de sentencias por medio de una interfaz gráfica propietaria de Netcool® Reporter™. La base de datos del entorno de TEA está en una configuración cluster lo que garantiza una alta disponibilidad del recurso.

3.5.4 Netcool® Webtop™

Netcool® Webtop™, es el servidor de contenidos que ofrece una interfaz web para el acceso a los servicios de supervisión de alarmas. Es la herramienta principal que usarán los operadores de supervisión y clientes en su actividad diaria cuyo esquema general se muestra en la Figura 3.13. El módulo Webtop edita las alarmas de Omnibus a través de un navegador web y permite que ciertos usuarios las manipulen, mediante listas de

eventos activos (ACL). El servidor de Webtop publica las alarmas sobre el protocolo HTTP, de manera que puedan consultarse a través de cualquier navegador soportado. De esta forma los operadores pueden monitorizar alarmas de su red vía web.

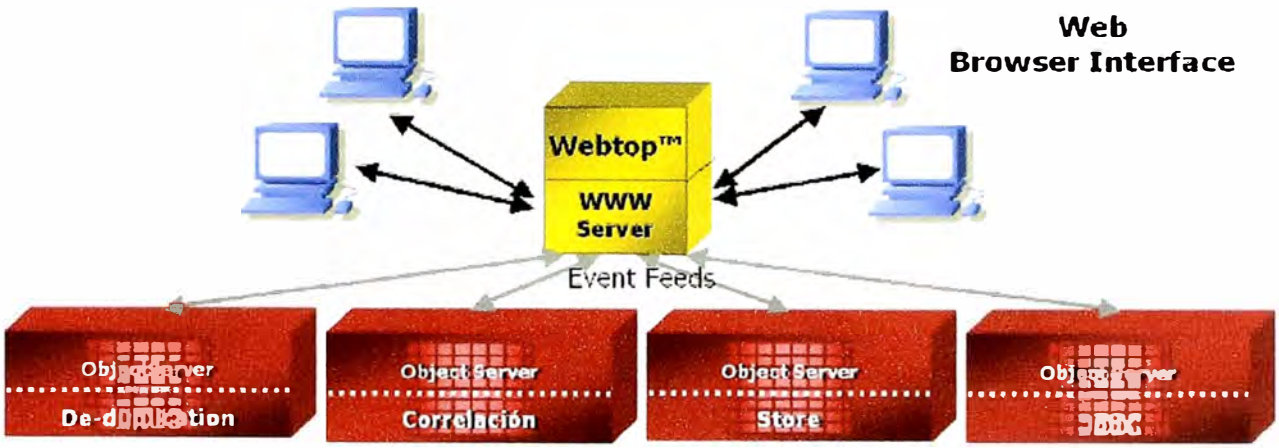


Figura 3.13.- Esquema general Netcool® Webtop™

La Figura 3.14 muestra un AEL (Active Event List - Listado de eventos), que es la ventana donde se visualizan las alarmas, en base a una jerarquía de colores, donde las alarmas de color rojo son aquellas de mayor relevancia y de severidad "crítica", las de color naranja son aquellas de severidad "mayor", las de color amarillo con severidad "menor", las de azul con severidad de "advertencia", las de color morado son aquellas indeterminadas o meramente informativas y finalmente las de color verde que son aquellas que notifican la solución de algún fallo en la red.

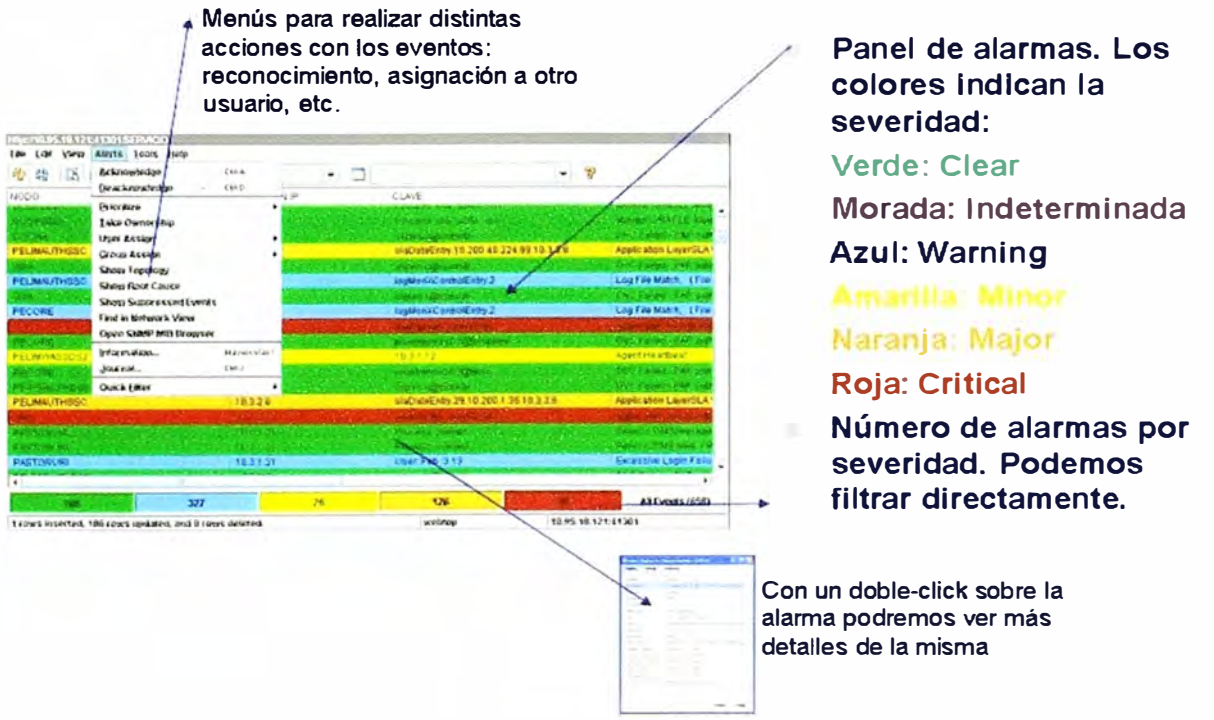


Figura 3.14.- Propiedades del listado de eventos

3.6 Puesta en marcha

A continuación se muestra en la Figura 3.15, el esquema integrado de todos los aplicativos que componen la solución:

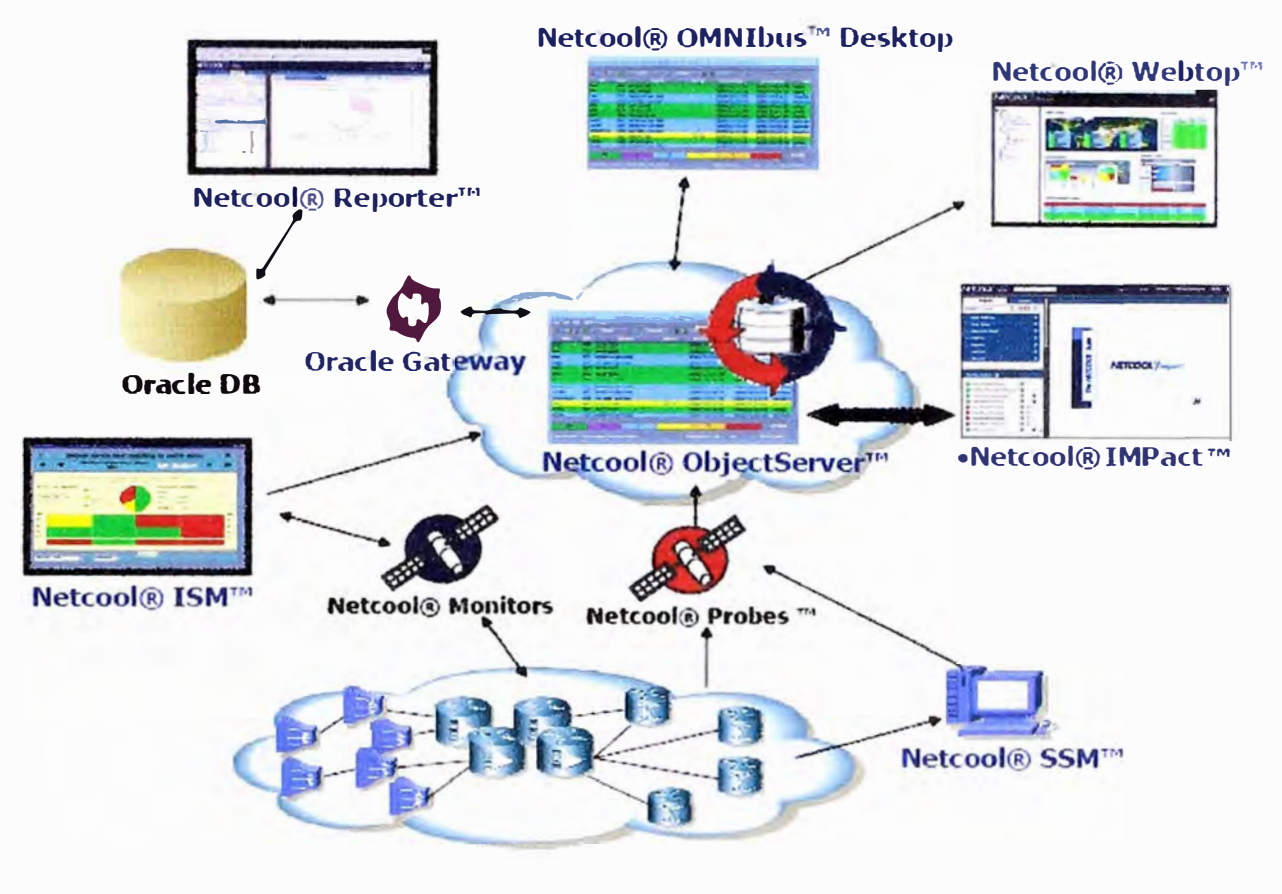


Figura 3.15.- Esquema integrado de los aplicativos

3.6.1 Estructura Física (Hardware)

A continuación se detallan las máquinas que componen la estructura física de la solución TIVOLI NETCOOL y los componentes instalados en cada una de ellas.

En la Figura 3.16 se muestran los cuatro servidores Sun Fire T2000, que se utilizarán en la solución. Todos con procesadores 8x1GHz de doble núcleo, memoria RAM de 8GB y disco duro de 4x73GB, los cuales garantizarán un buen desempeño de las aplicaciones.

- En la primera máquina (epnet01) se instala el ObjectServer y el Servidor de licencias, el cual se instala por defecto conjuntamente con el ObjectServer, esta herramienta es la responsable de administrar las licencias utilizadas por los aplicativos.
- En la segunda máquina (epnet02) se instalan las probes (glf, mttrapd y syslog)
- En la tercera máquina se instala Netcool® Impact™.
- Y finalmente en la cuarta máquina se instalan Reporter, Webtop, GW Oracle y la base de datos Oracle.

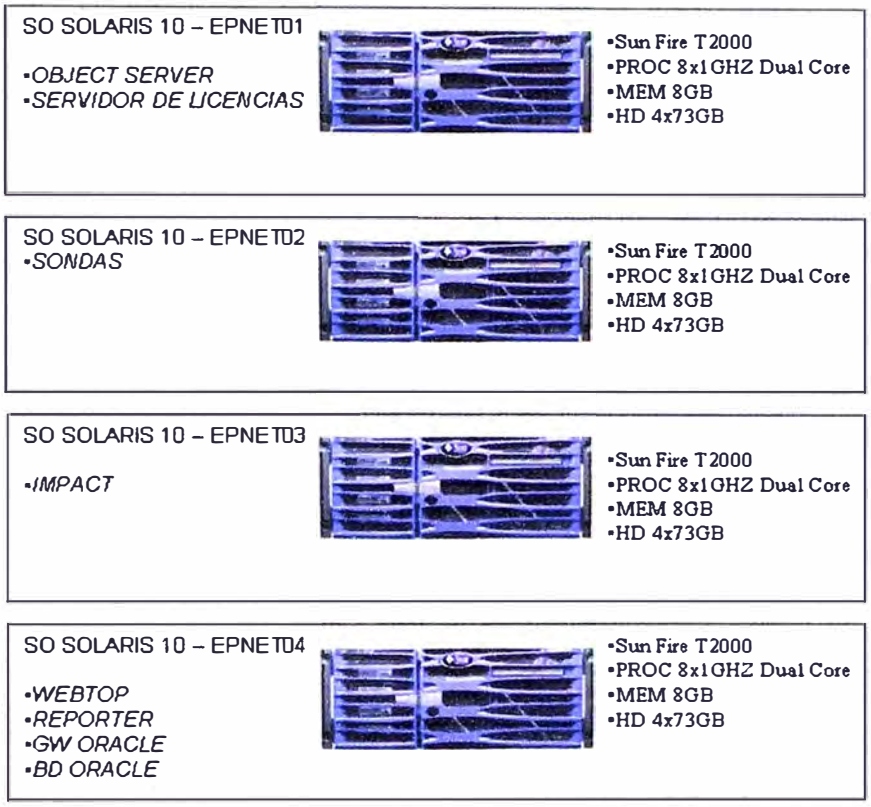


Figura 3.16.- Servidores Sun para los aplicativos TIVOLI NETCOOL

3.6.2 Estructura Lógica

A continuación, en la Figura 3.17 se observa, los entornos monitorizados y los equipos que monitorizan cada probe (sonda):

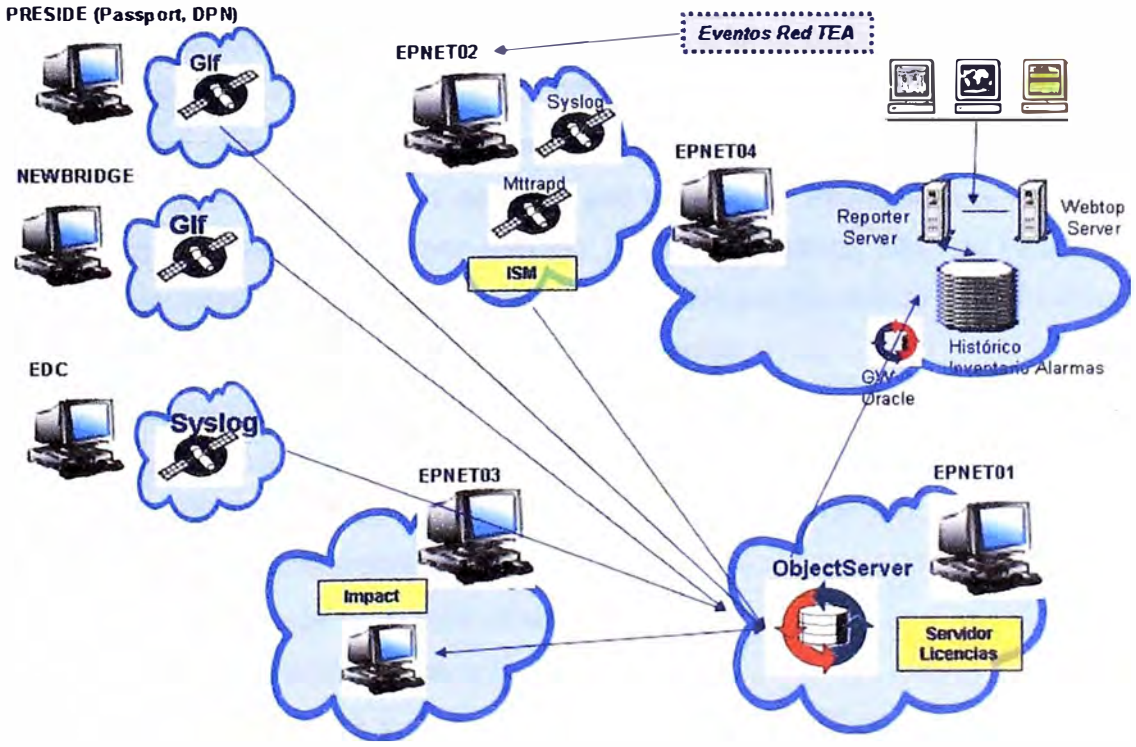


Figura 3.17.- Estructura Software

La sonda GLF instalada en el gestor PRESIDE recolecta los eventos de los equipos Nortel passport y DPN de Nortel enviados por el gestor, desde el fichero de log "presideAlarms".
La sonda GLF instalada en el gestor Newbridge recibe los eventos de estos equipos provenientes del gestor desde el fichero de log "newBridgeLog"
La sonda syslog instalada en el gestor EDC recolecta los eventos de los routers CPE mediante mensajes syslog almacenados en el gestor.
La sonda mttrapd instalada en la máquina epnet02 recolecta los eventos de los modems satelitales (Idirect) y de los equipos Cisco BPX vía traps SNMP.
La sonda syslog instalada en la máquina epnet02 recibe los eventos de los routers Cisco (PE / P) mediante mensajes syslog enviados a la máquina epnet02.

3.6.3 Visualización de eventos

A continuación, se describen los campos más importantes que aparecen en los eventos y/o alarmas:

- Identifier: Es la clave para la deduplicación de los eventos y/o alarmas como se verá más adelante. Está compuesto por el nombre de la instancia del Netcool ObjectServer, que para el caso de TEA es "TEA", con otros cinco campos de la Base de Datos residente en memoria. Identifier = "TEA" :: NEName :: AlertKey :: AlertGroup :: ObjectType :: Type
- NEName: Nombre del equipo donde se origina el evento y/o alarma.
- NEAddress: Dirección IP del equipo donde se origina el evento y/o alarma.
- Node: Dirección IP del equipo que notifica o envía el evento y/o alarma.
- NodeAlias: Dirección IP del equipo que notifica o envía el evento y/o alarma (en caso de que el evento sea enviado por un Gestor Propietario la IP del Gestor aparecerá en este campo, por ejemplo: N2000 de Huawei, NMS de Alcatel, etc.).
- Manager: nombre de la sonda, "@", nombre del equipo donde se esta ejecutando el Netcool Probe: Ejemplo: mttrapd@sg-fa-ccol02
- Agent: Gestor de red o en su defecto nombre de equipo.
- AlertKey: Si para la visualización y procesamiento del evento y/o alarma es necesaria la parte afectada, esta será ubicada en este campo.
- AlertGroup: Tipo de problema, nivel 1.
- ObjectType: Tipo de problema, nivel 2.
- Summary: Descripción del evento y/o alarma.
- LastOcurrence: Fecha y hora en que se recibió el último evento notificando el problema. Vale la pena aclarar que este dato se ingresa internamente a la Base

de Datos en formato timestamp (UNIX), y al momento de ser visualizado a través de un Netcool Event List, se muestra en un formato DD-MM-YYY HH:MM:SS AM/PM.

- FirstOccurrence: Primera vez que se notificó el evento y/o alarma. También se ingresa internamente a la Base de Datos en formato timestamp (UNIX), y al momento de ser visualizado a través de un Netcool Event List, se muestra en un formato DD-MM-YYY HH:MM:SS AM/PM.
- StateChange: Fecha y hora de la última modificación realizada en la alarma. También se ingresa internamente a la Base de Datos en formato timestamp (UNIX), y al momento de ser visualizado a través de un Netcool Event List, se muestra en un formato DD-MM-YYY HH:MM:SS AM/PM.
- Tally: Número de veces que se recibió el evento y/o alarma.
- Type: Tipo de evento, si el campo type es de valor 0 indica que es un evento informativo, si es 1 indica que es un evento problema y si es 2 indica que es un evento resolución.
- OwnerUID: Usuario propietario del evento y/o alarma.
- OwnerGID: Grupo propietario del evento y/o alarma.
- Severity: severidad del evento y/o alarma. 0,1,2,3,4,5 indican Clear, Indeterminate, Warning, Minor, Mayor, Critical respectivamente.
- Grade: Indica cuantas veces se ha recibido el evento y/o alarma problema y a continuación el evento y/o alarma resolución. Este campo es útil para identificar problemas intermitentes en la red.
- Technology: Indica el dispositivo o elemento que generó la alarma: Ej.: Acceso – Cisco, Acceso - Newbridge, IP – Cisco, etc.
- AdditionalInfo: Información adicional del evento y/o alarma.
- InvName: Nombre del equipo en inventario (Información enriquecida a través de Netcool Impact)
- NEModelID: Descripción del hardware y software del equipo (Modelo – Versión,
- Información enriquecida a través de automatización de Netcool OMNIbus)
- NetworkName: Descripción de la red donde se ubica el equipo que esta reportando el evento y/o alarma (Información enriquecida a través de automatización de Netcool OMNIbus, Ejemplo: ATM, CORE IP, etc.
- Location: Ubicación geográfica del equipo (Area1/Area2/Area3), Información enriquecida a través de Netcool Impact.
- Customer: Nombre o razón social del cliente afectado por la alarma.

Las listas de eventos (Event List's) de Netcool® Webtop™ pueden ser configuradas para ver unos u otros campos de un evento y/o alarma, estos campos hacen referencia a la tabla "alerts.status" de la Base de Datos residente en memoria (Netcool® ObjectServer™). Desde la herramienta Netcool® Webtop™ hacemos clic en un componente que despliega una lista de eventos (AEL Active Event List), la lista de eventos se abrirá con la vista que hubiera asociado al componente. Desde una lista de eventos, se accede a la ventana de vistas, como se muestra en la Figura 3.18.

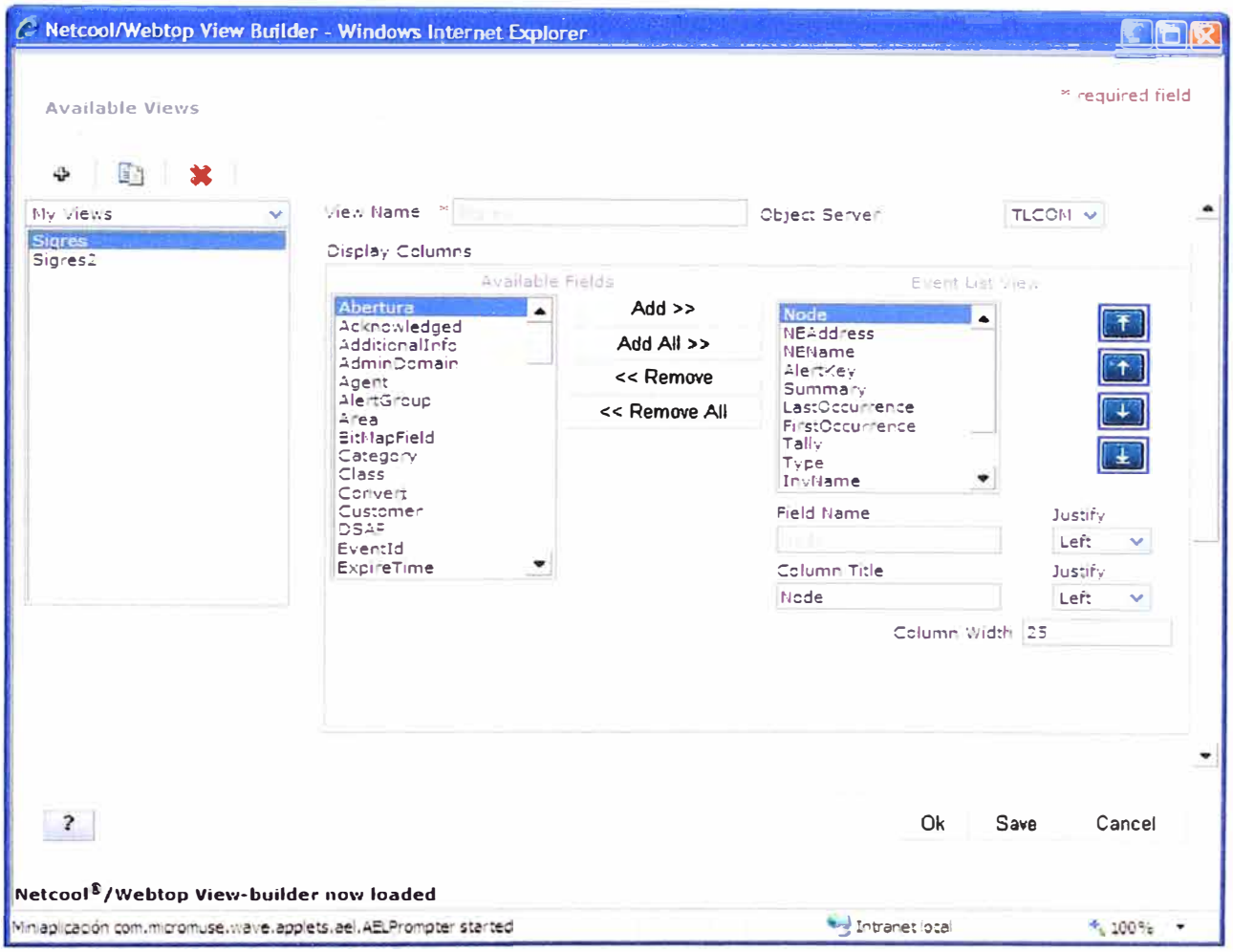


Figura 3.18.- Configuración de una Vista básica de AEL

Los filtros permiten definir qué alarmas se mostrarán en la lista de eventos de Netcool® Webtop™. Podemos utilizar un filtro vacío, en cuyo caso se mostrarían todas las alarmas contenidas en el Netcool® ObjectServer™, o podemos utilizar filtros para que muestren, por ejemplo, sólo las alarmas de un determinado equipo, o de una determinada tecnología. También se pueden utilizar filtros complejos que requieran varias condiciones. Desde la herramienta Netcool® Webtop™ hacemos clic en un componente que despliega una lista de eventos (AEL Active Event List), la lista de eventos se abrirá con el filtro que

hubiera asociado al componente. Desde una lista de eventos, se accede a la ventana de filtros, como se muestra en la Figura 3.19:

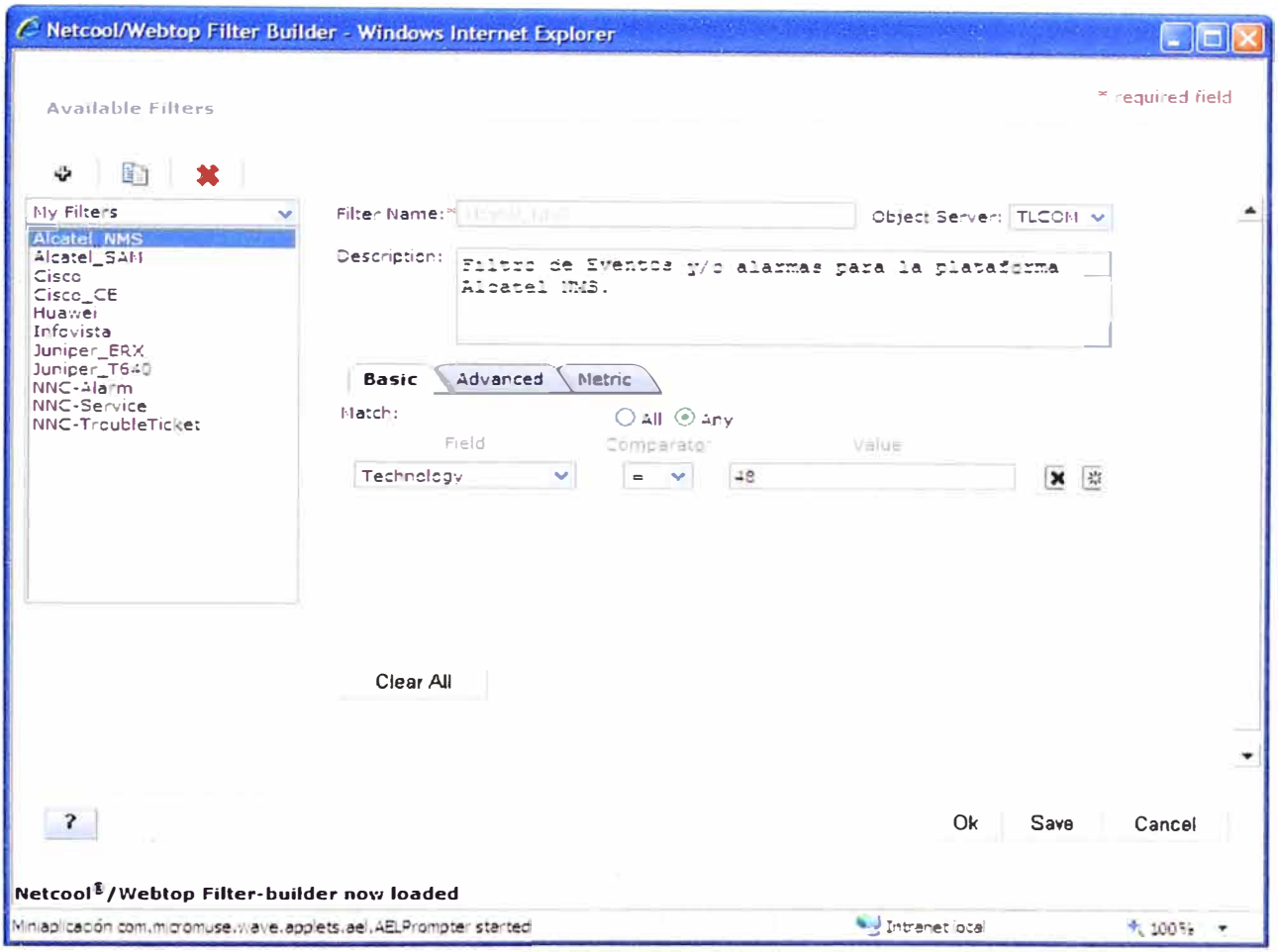


Figura 3.19.- Ventana de Filtros

3.6.4 Tratamiento y Correlación de eventos

Deduplicación, cuando un dispositivo tiene un problema, envía a través de un snmp trap, o un fichero de log, un evento y/o alarma notificando este problema; en muchas ocasiones envía repetidamente el mismo snmp trap y/o mensaje de log. Por ejemplo, un dispositivo que tenga un problema con su ventilador de CPU puede enviar un snmp trap notificando este problema cada 5 segundos. En caso de que el problema no se pudiera solucionar con rapidez se generaría un elevado volumen de alarmas en el sistema que dificultaría la consulta del estado de la red a través de Netcool® Webtop™.

Para evitar este problema, el Netcool® ObjectServer™ no crea una nueva alarma si ya había una "equivalente"; incrementa en uno (1) el campo Tally (Count). Así, este campo nos indica cuantas veces se ha producido o notificado el mismo problema. El campo Identifier de un evento y/o alarma es el que determina si se crea, o no, una nueva alarma

y/o evento. En caso de que el nuevo evento y/o alarma candidata a ingresar en el sistema contenga un identificador igual que el de otra ya existente dentro de la Base de Datos residente en memoria, en lugar de crearse esta nueva alarma, se actualiza la ya existente con la información de la nueva, y se incrementa en uno el campo Tally (tabla alerts.status Netcool® ObjectServer™), columna Count en las AEL (Active Event List) de Netcool® Webtop™, tal como se muestra en la Figura 3.20.

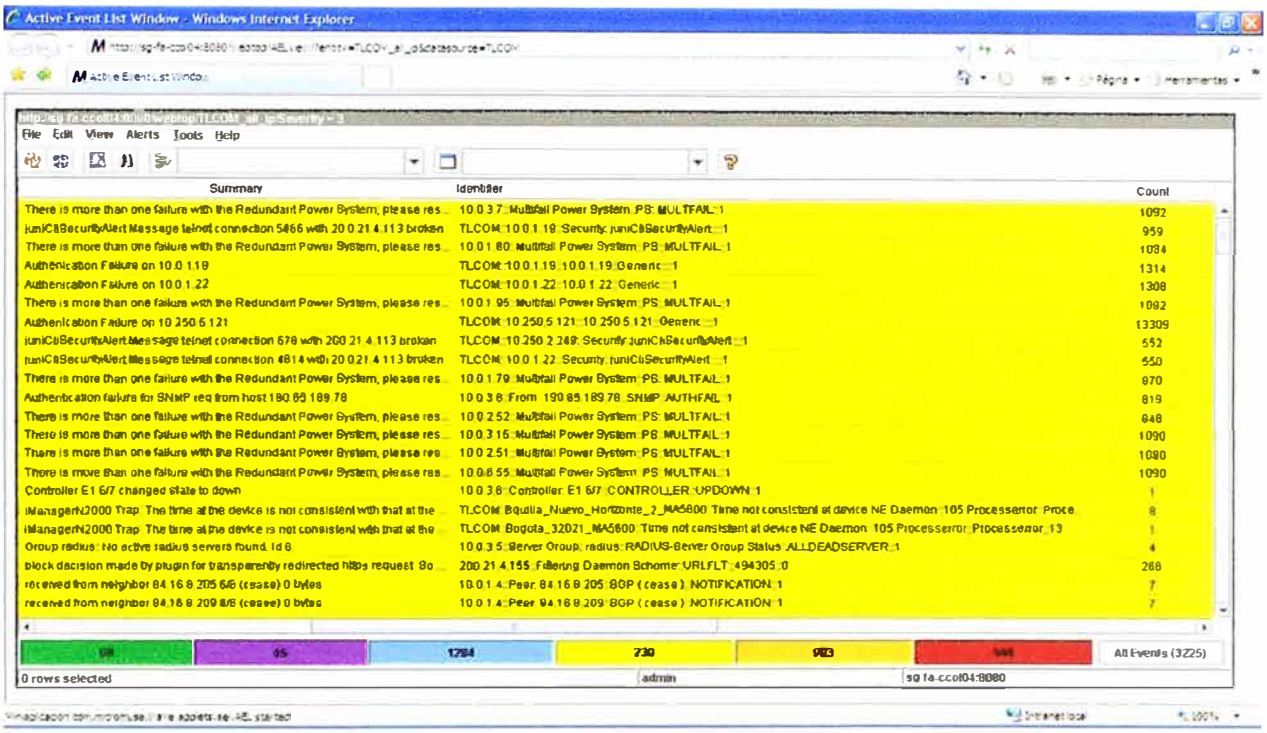


Figura 3.20.- Número de ocurrencias de un equipo

Dentro del sistema están continuamente corriendo una serie de automatizaciones. Una de ellas (Generic_Clear_Sigres) se encarga de correlacionar los eventos y/o alarmas, de forma que cuando llega una alarma resolución, se aplican los siguientes cambios a su correspondiente alarma problema:

- Severidad = 0. Se actualiza la severidad del evento y/o alarma para indicar que el problema ha cesado o se ha solucionado.
- Grade = Grade + 1. Se genera un contador para saber cuantas veces el evento y/o alarma ha sido correlacionado.
- SummaryClear = Summary del evento y/o alarma resolución. El campo es actualizado con la descripción del evento y/o alarma resolución.
- LastOccurrence = LastOccurrence del evento y/o alarma resolución. El campo es actualizado con la fecha y hora del evento y/o alarma resolución.

El evento y/o alarma resolución se actualiza con Aknowledge = 1, indicando que la alarma de resolución ya ha sido actualizada en su respectiva alarma problema.

Existen algunas excepciones a esta fase, como es el escenario de las alarmas enviadas al Netcool® ObjectServer™ por la herramienta Netcool® SSM™. En estos casos no se recibe una alarma tipo resolución (Type = 2), y la resolución del problema se realiza mediante una automatización. El sistema comprueba el estado de los elementos con una periodicidad determinada, generando una nueva alarma cada vez que el estado del elemento no es correcto. Si transcurrido ese periodo de tiempo no vuelve a llegar esa alarma, entonces el problema se ha solucionado. Esta es la filosofía en que se basan este tipo de automatizaciones, y para implementarla comprueban el campo LastOcurrence de la tabla "alerts.status", el cual nos indica el momento en que se recibió la última alarma.

3.6.5 Almacenamiento de eventos

Una vez que un problema se ha solucionado, las alarmas que nos indicaban la existencia de este problema permanecerán en el sistema durante un tiempo determinado antes de ser borradas. Las condiciones que han de darse para el borrado del evento y/o alarma son:

- Una vez transcurridos cinco (5) minutos o más desde que llegó la última alarma y se encuentra resuelta (Severidad = 0) sin haber sido asignada a ningún usuario o grupo (Automatización Delete_Clears_Sigres).
- Una vez transcurrido 24 horas o más desde que llegó la última alarma y esta no ha sido asignada a ningún usuario o grupo (automatización Delete 24_old).

Las alarmas serán borradas si se cumplen las condiciones de alguno de los dos puntos anteriores. Una vez borradas las alarmas no volverán a ser visibles a través de la herramienta Netcool® Webtop™, pero sí mediante informes de históricos proporcionados por la herramienta Netcool® Reporter™, debido a que estos eventos son almacenados en un repositorio de Base de Datos Oracle. Estas automatizaciones se realizan dentro del ObjecServer utilizando mecanismos de base de datos basado en SQL (Structured Query Language – Lenguaje de peticiones estructuradas) como son triggers y procedures.

3.7 Pruebas y Testeos

Las pruebas y testeos del sistema siguen un plan de trabajo, que consta de los siguientes procedimientos:

- Procedimiento 1: Recepción de los eventos de todas las tecnologías de equipos en el ObjectServer (router Cisco CPE, NewBridge, Idirect, BPX, Nortel Passport, DPN, router Cisco PE, etc)

- Procedimiento 2: Correlación básica y borrado de eventos.
- Procedimiento 3: Enriquecimiento de alarmas e Integración al bus EAI vía Netcool® Impact™.
- Procedimiento 4: Generación de informes de históricos de eventos y visualización de alarmas via Netcool® Webtop™.
- Procedimiento 5: Comprobación de alarmas de pérdidas de conectividad.

Dado que no se dispuso de un ambiente específico para pruebas de sistemas, las pruebas se realizaron sobre el mismo ambiente de producción. Sin embargo, al utilizar el mismo ambiente de producción para las pruebas, los eventos simulados introducidos que no corresponden a la red ni a la situación real, podrían ocasionar confusiones a los operadores de red. Para minimizar ese impacto, el personal involucrado en las pruebas de certificación se encargó de realizar, el borrado de las alarmas generadas mediante simulación una vez realizada la prueba, enviando eventos de "clear" para los mismos elementos sobre los que se generó la alarma.

En el ambiente de producción se recibieron simultáneamente:

- Eventos reales de la red de producción.
- Eventos reales recibidos de equipos de laboratorio.
- Eventos simulados vía scripts.
- El estado comercial del servicio.

3.8 Resultados Obtenidos

La Figura 3.21, muestra la pantalla de acceso: URL: http://epnet04:8080

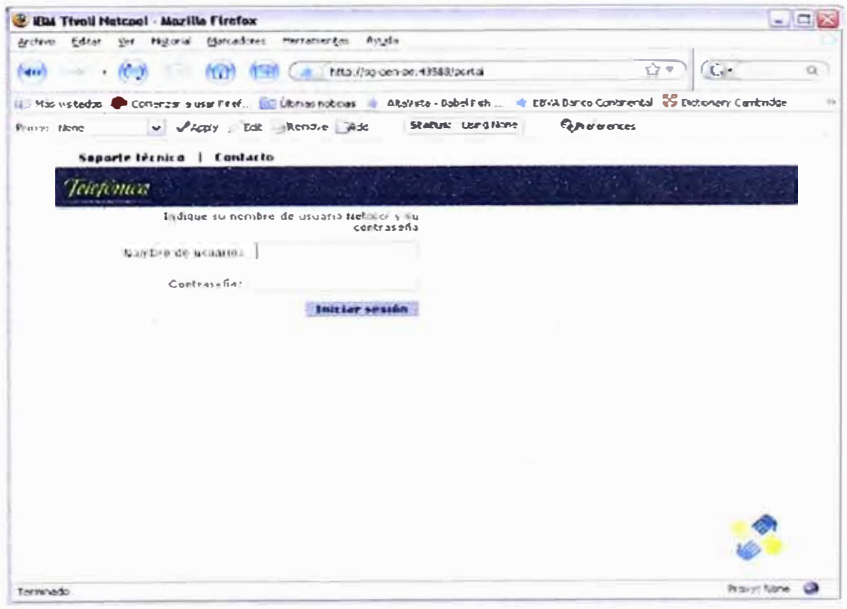


Figura 3.21.- Pantalla de Acceso a Netcool® Webtop™

La Figura 3.22 muestra la pantalla de inicio del operador, con el resumen ejecutivo de la gestión de la red a lo largo de todo el territorio argentino.

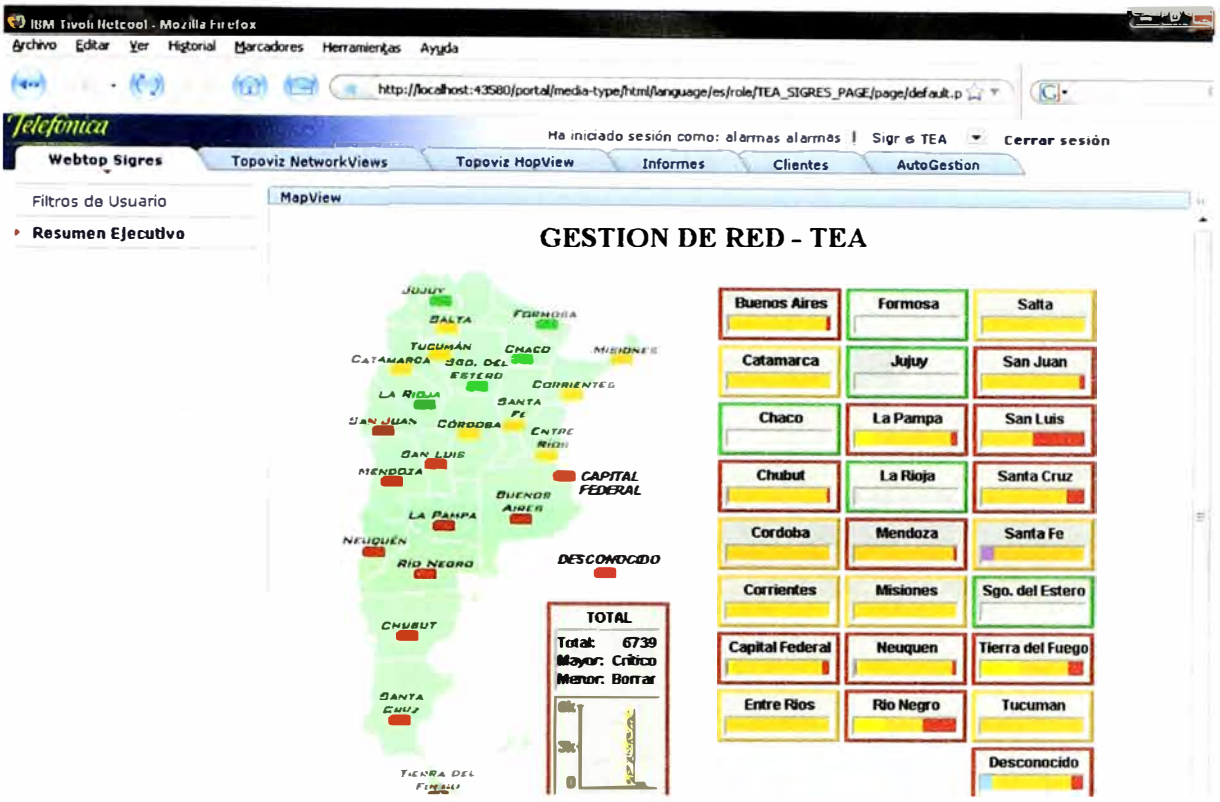


Figura 3.22.- Resumen Ejecutivo Argentina

La Figura 3.23 muestra la pantalla de visualización de un cliente de Telefónica Empresas con el listado de todas sus referencias asignadas.

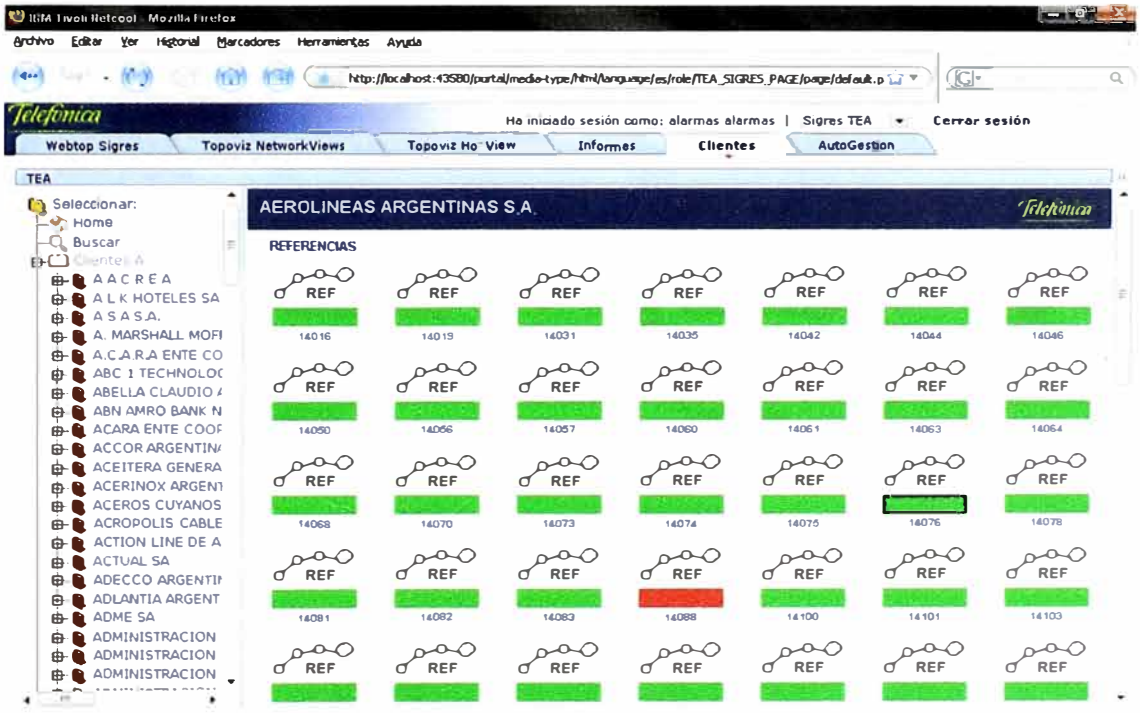


Figura 3.23.- Lista de referencias asignadas a un cliente.

La Figura 3.24, muestra la pantalla de visualización de una referencia del tipo CPE gestionado lejano.

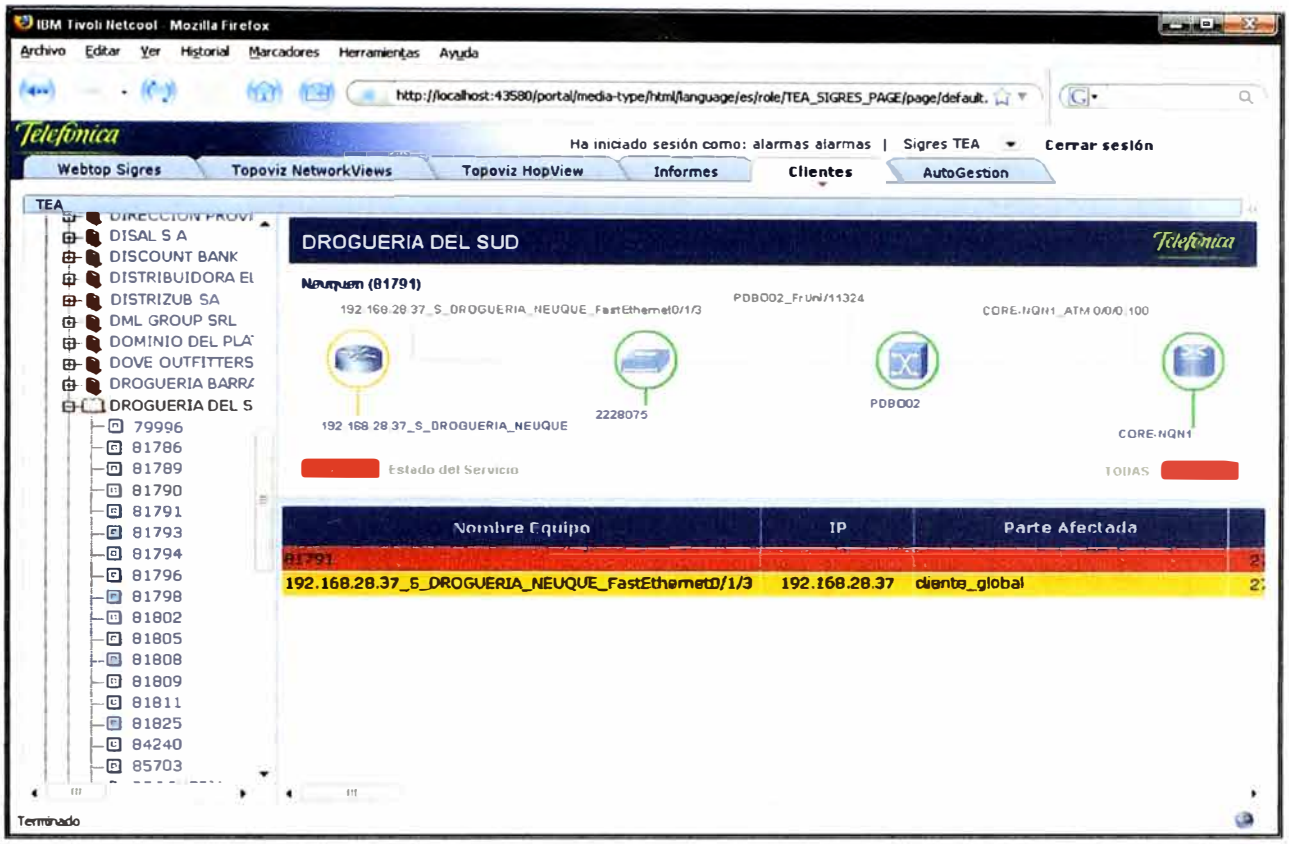


Figura 3.24.- Visualización de Referencia.

La Figura 3.25 muestra la pantalla de Informes de históricos de eventos:

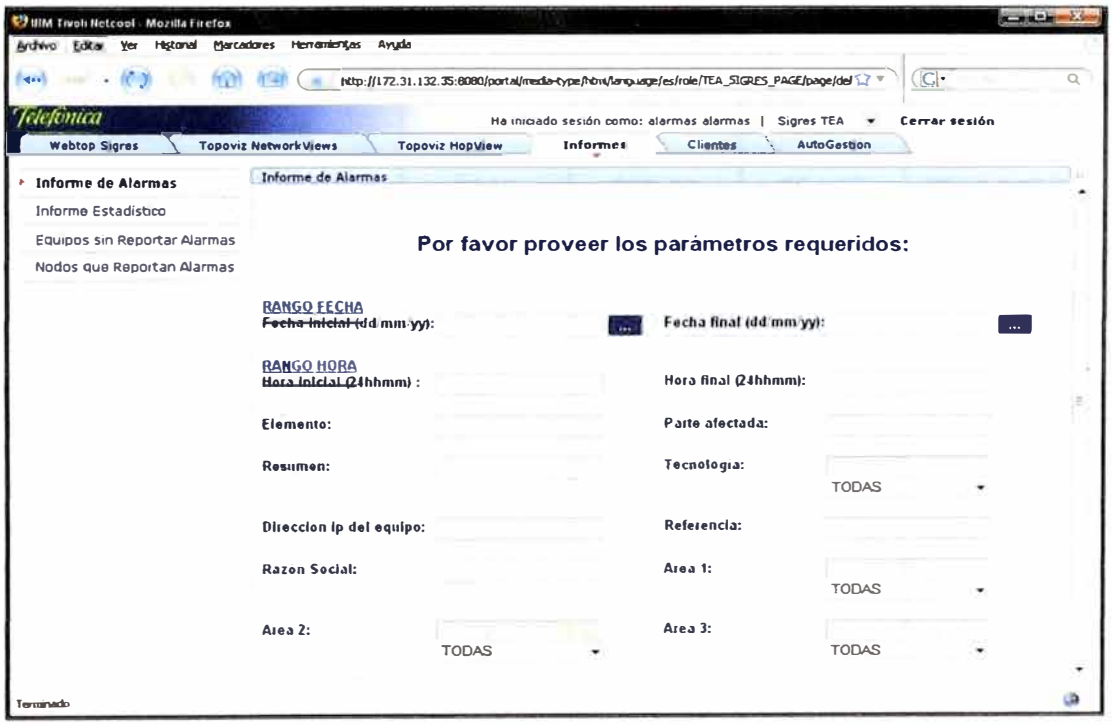


Figura 3.25.- Visualización de informes.

3.9 Análisis de Costos

La Cotización que IBM ofrece a sus clientes con los precios de sus productos, se muestra en la Tabla 3.2 y la Tabla 3.3.

Tabla 3.2.- Cotización de Costos para Telefónica Data

NUMERO DE PARTE	DESCRIPCION	VU o Cantidaes	PRECIO Lista		PRECIO Desc
Consolidación de Eventos Core (Omnibus)					
D60WZLL	IBM Tivoli Netcool/OMNIbus Base per Install License + SW Maintenance 12 Months	1	$60,375.00	$48,058.50	$48,058.50
Interface Web Unica (WebTop)					
D60WQLL	IBM Tivoli Netcool/Webtop per Install License + SW Maintenance 12 Months	1	$1,150.00	$915.40	$915.40
D6136LL	IBM Tivoli Netcool/Webtop Concurrent User License + SW Maintenance 12 Months	22	$5,750.00	$4,577.00	$100,694.00
D6138LL	IBM Tivoli Netcool/Webtop Limited Use Concurrent User License + SW Maintenance 12 Months	60	$517.50	$411.93	$24,715.80
Consolidación de Eventos Core (Probes de integración de eventos)					
D60X2LL	IBM Tivoli Netcool/OMNIbus Probe Tier 1 per Resource Value Unit License + SW Maintenance 12 Months	3945	$69.00	$54.92	$216,659.40
D60X2LL	IBM Tivoli Netcool/OMNIbus Probe Tier 1 per Resource Value Unit License + SW Maintenance 12 Months	2000	$69.00	$54.92	$138,000.00
D60X5LL	IBM TIVOLI NETCOOL/OMNIBUS PROBE TIER 3 PER RESOURCE VALUE UNIT LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTH	1	$21,850.00	$17,392.60	$21,850.00

Tabla 3.3.- Cotización de Costos para Telefónica Data

NUMERO DE PARTE	DESCRIPCION	VU o Cantidaes	PRECIO Lista		PRECIO Desc
Reporteador de Gestión de Fallas (Reporter)					
D60WULL	IBM Tivoli Netcool/Reporter Base per Install License + SW Maintenance 12 Months	1	$41,400.00	$32,954.40	$32,954.40
D60WSLL	IBM Tivoli Netcool/Reporter Tier 1 per Resource Value Unit License + SW Maintenance 12 Months	1	$5,002.50	$3,982.45	$3,982.45
Gateways de Interconexión (los de interconexión de Omnibus están incluidos)					
D60YFLL	IBM TIVOLI NETCOOL/OMNIBUS GATEWAY TIER 1 PER CONNECTION LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	1	$27,600.00	$21,969.60	$21,969.60
Monitoreo de Sistemas y servicios de Internet					
D59D0LL	IBM TIVOLI COMPOSITE APPLICATION MANAGER FOR INTERNET SERVICE MONITORING PROTOCOL LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	10	$12,190.00	$9,703.70	$9,703.70
D561YLL	IBM TIVOLI MONITORING 10 PROCESSOR VALUE UNITS (PVUS) LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	5000	$85.39	$67.97	$33,985.00
			TOTAL		**$653,488.25**

Como se observa de las tablas, el costo total asciende a 653'488,25 dólares americanos sin incluir IVA (impuestos de valor agregado), si bien es un gasto considerable para la empresa, bien vale la pena la inversión.

A continuación, se citan algunos motivos que justifican, el porqué de la inversión:

- Mejor servicio: Los usuarios esperan igual o mejor servicio a medida que la información y los recursos informáticos crecen y se distribuyen.
- Control de recursos estratégicos de la empresa: Las redes y servicios se han vuelto vitales para las empresas. Sin un control efectivo o se consiguen los resultados esperados de ellas.
- Control de la complejidad: El crecimiento de las redes, usuarios, interfaces, protocolos y vendedores complican la gestión.
- Balance de necesidades: Las organizaciones tienen diversos usuarios con diferentes necesidades y niveles de soporte, con requisitos específicos de prestaciones, disponibilidad y seguridad.
- Reducción de tiempos de no funcionamiento: Cuanto más vital se vuelve la red, más debe aproximarse su disponibilidad al 100% del tiempo
- Control de costos: Se debe controlar la red para cubrir las necesidades de los usuarios a un coste razonable.

En este último capítulo, se mostró la implementación de un sistema de monitorización de alarmas, se observaron los resultados obtenidos y el tipo de equipos que requiere la solución como también un análisis de los costos implica la adquisición de los aplicativos TIVOLI NETCOOL.

CONCLUSIONES

Luego de describir la implementación de un sistema de monitorización de alarmas de red y destacar la necesidad que tienen las operadoras de tener implementado un sistema capaz de garantizar la disponibilidad en todo momento del servicio que brindan, se llegan a las siguientes conclusiones:

[1] La gestión de alarmas de red es una necesidad primordial en las organizaciones.

[2] De la gestión de alarmas, se espera que:

- Asegure un servicio casi continuo a los usuarios finales descrito por la disponibilidad y velocidad de respuesta, sin que se vean afectados por las actualizaciones tecnológicas en la red.
- Incremente el desempeño de una red con el empleo de la mejor tecnología de redes, recursos humanos adecuados, métodos de trabajo probados y herramientas integradas que automaticen las operaciones de gestión.
- Controle los costos dedicados a las comunicaciones y a la seguridad de la información.

[3] La ejecución de un proyecto como el implementado en el informe, requiere:

- Esfuerzo conjunto de las áreas Informática y Operaciones, mas los grupos de Planeación, Ingeniería, I&D (Investigación y Desarrollo), Mercadeo y Desarrollo de productos.
- Cooperación estrecha con los suministradores.
- Adopción de interfaces comunes en áreas de interés entre proveedores de servicios y con clientes.

BIBLIOGRAFÍA

[1] Antoni Barba Marti, "Gestión de Redes", ediciones UPC, Septiembre 1999.

[2] Andrew S. Tanenbaum, "Redes de computadoras", Prentice Hall, Inc 2003.

[3] William Stallings, "The Practical Guide to Network Managment Standards", Addison Wesley 1998.

[4] Kornel Terplan, "Communication Network Management", Prentice Hall, Inc 1992.

[5] SNMP RFC 1157, 1901, 1905, 2570, 2574, http://www.ietf.org/rfc.html.

[6] Anand Deveriya, "Network Administrators Survival Guide", Cisco Press, Septiembre 2005.

[7] Netcool, http://www-01.ibm.com/software/tivoli/welcome/netcool/index.html.

[8] IBM, - "Tivoli Netcool/OMNIbus v 7.2.1, Administration Guide", IBM 2008.

[9] IBM, - "Tivoli Netcool/OMNIbus v 7.2.1, User's Guide", IBM 2008.

[10] IBM, - "Tivoli Netcool/OMNIbus v 7.2.1, Quick Start Guide", IBM 2008, disponible en URL http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcoolOMNIbus.doc_7.2.1/welcome.htm

[11] IBM, - "Tivoli Netcool / Impact v4.0.1, Administration Guide", IBM 2007.

[12] IBM, - "Tivoli Netcool / Impact v4.0.1, User Interface Guide", IBM 2007.

[13] IBM, - "Tivoli Netcool / Impact v4.0.1, Solutions Guide", IBM 2007.

[14] IBM, - "Tivoli Netcool / Reporter v2.2, Administration Guide", IBM 2008.

[15] IBM, - "Tivoli Netcool / Reporter v2.2, User Guide", IBM 2008, disponible en URL http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcoolreporter.doc_2.2/welcome.htm

[16] IBM, - "Tivoli Netcool / Webtop v2.1, Administration Guide", IBM 2007.

[17] IBM, - "Tivoli Netcool / Webtop v2.1, Quick Start Guide", IBM 2007, disponible en URL http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcoolwt.doc/welcome.htm