PONTIFICIA **UNIVERSIDAD CATÓLICA** DEL PERÚ

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DEL CENTRO DE OPERACIÓN Y GESTIÓN DE LA RED ACADÉMICA PERUANA EN SOFTWARE LIBRE

TESIS PARA OPTAR EL TÍTULO DE

INGENIERO DE LAS TELECOMUNICACIONES

PRESENTADO POR

Arturo Díaz Rosemberg

LIMA – PERÚ

2007

RESUMEN

El objetivo general de esta tesis es contar con una herramienta que permita conocer el rendimiento de la Red Académica Peruana-RAAP y a partir de este conocimiento poder tomar decisiones de gestión. Esta red soporta protocolos avanzados, como IPv6, y está implementado con la arquitectura MPLS para ofrecer alta calidad de servicio a las aplicaciones de tiempo real.

Se analiza todo lo relacionado con el manejo apropiado de la red RAAP y, partiendo de esto, el trabajo se centra en el desarrollo de una plataforma para el monitoreo y gestión de esta red. Esta plataforma está basada en software libre en su totalidad y está diseñada para ser modular y adaptable para soportar posibles mejoras.

Dentro de la tesis se incluye el estudio de la estructura de la red académica, conceptos generales de gestión de redes, así como la configuración y una presentación de las interfaces de la implementación final.

A mi madre.

AGRADECIMIENTOS

A mis padres y hermanos por la educación y el invalorable apoyo que siempre me han brindado.

A todos los profesores de Telecomunicaciones, de los cuales he aprendido mucho. Especialmente a mi asesor, el Ingeniero Daniel Díaz y al Ingeniero David Chávez por su apoyo en este y otros proyectos.

A Pame por el cariño y compañía que siempre me da. A Diego por las ideas y colaboración. A Julio, Carlos, Diego M. y todos mis compañeros de especialidad, pues con ellos estos últimos ciclos han sido únicos.

Finalmente a todos los involucrados con el software libre, por dedicar su tiempo a los proyectos y compartir sus conocimientos con todas las personas.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABLAS

Glosario

ALICE	América Latina Interconectada con Europa.
APAN	Asia-Pacific Advance Network.
ARPANET	Advanced Research Projects Agency Network.
ASN	Abstract Syntax Notation.
CCITT	Consultative Committee for International Telegraphy and Telephony.
CLARA	Cooperación Latino Americana de Redes Avanzadas.
CLI	Command Line Interface.
DANTE	Delivery of Advance Network Technology to Europe.
DOD	Department of Defense (de los Estados Unidos).
Gbps	Gigabit por segundo.
IANA	Internet Assigned Numbers Authority.
IP	Internet Protocol.
IPv4	Internet Protocol versión 4.
IPv6	Internet Protocol versión 6.
ISO	International Standards Organization.
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector.
MIB	Management Information Base.
MPLS	Multiprotocol Label Switching.
NAT	Network Address Translation.
NBAR	Network-Based Application Recognition.
NMS	Network Management System.

NREN	National Research and Education Network.
OID	Object Identifier.
QoS	Quality of Service.
SLA	Service Level Agreement.
SGMP	Simple Gateway Management Protocol.
SMI	Structure of Management Information.
SNMP	Simple Network Management Protocol
TdP	Telefónica del Perú.
UPS	Uninterruptible Power Supply.
RAAP	Red Académica Peruana.
RRA	Round Robin Archive.
RRD	Round Robin Database.

Capítulo 1: Planteamiento del proyecto

1.1. Introducción

Las telecomunicaciones y en particular el campo de las redes de datos son áreas de constante desarrollo e innovación, en la actualidad la gran mayoría de empresas y entidades educativas utilizan redes de datos como base para sus comunicaciones y como plataforma para brindar servicios. Además, las redes de datos facilitan conexiones con sitios remotos, intercambio de información, enlaces internacionales, entre otras facilidades.

Cuando se piensa en redes de datos es inevitable pensar en la Internet, red que empezó uniendo universidades y centros de investigación en Estados Unidos y que ahora cubre prácticamente todo el mundo [BOL81][DOM2001]. Esta red sirve de plataforma a muchos negocios y se ha vuelto eminentemente

comercial, es por eso que desde hace unos años se vio la necesidad de disponer de una red paralela que vuelva a estar dedicada a la investigación y a la prueba de nuevas tecnologías de manera exclusiva. Actualmente existen iniciativas ya implementadas de redes académicas, que cuentan con mayores anchos de banda y tecnologías aún no disponibles en la Internet comercial, tales como: IPv6, multicast, etcétera.

En el caso del Perú existe la Red Académica Peruana, conocida como RAAP [RAAP2003] la cual interconecta a universidades y centros de investigación, y permite además comunicación con las redes académicas internacionales.

La utilización de la RAAP se encuentra en constante crecimiento, y se prevé también la inclusión de nuevos miembros, todo esto hace necesario que cuente con un sistema de monitoreo y gestión.

Para esto se debe seleccionar el software a utilizar y adaptarlo a las necesidades de la RAAP, de forma que permita optimizar el uso de los recursos con los que se cuenta y detectar posibles fallas de manera rápida, para poder garantizar un funcionamiento fluido de la red y sus equipos.

1.2. Objetivos

- Diseñar e implementar una plataforma de monitoreo y gestión de la Red Académica Peruana

- Permitir conocer cuantitativamente el rendimiento de la red y su evolución.
- Permitir tomar algunas acciones de control o gestión.

Para poder implementar el centro de gestión de la RAAP se debe conocer el uso que se le da a la red actualmente y como se espera que este evolucione; además, siendo esta una red que soporta los protocolos IPv4 e IPv6, debe contar con herramientas de gestión acordes a esta realidad.

Esta plataforma debe ser capaz de monitorear equipos de la red y servidores, generando alarmas en caso se encuentre algún problema.

Además debe permitir que el administrador pueda tomar medidas correctivas de manera remota, buscando así una pronta solución del problema.

Por otro lado como consecuencia de la implementación de este sistema, se podrá estudiar el tráfico actual de la red e incluso podrá servir de apoyo a las investigaciones que se lleven a cabo utilizando la infraestructura de la RAAP.

Capítulo 2: Estudio del escenario a gestionar

2.1. Redes académicas

Por encargo del Departamento de Defensa de los Estados Unidos, se creó a finales de 1969 la red ARPANET (Advanced Research Projects Agency Network), uniendo inicialmente el Instituto de Investigación de Stanford (SRI), la Universidad de UTAH así como dos campus de la Universidad California: Los Ángeles (UCLA) y Santa Bárbara (UCSB); poco a poco se fueron uniendo más centros de investigación en Estados Unidos [BOL81] La Figura 2.1 se ilustra los primeros centros interconectados a través de la red ARPANET. El objetivo de esta red era servir como medio de comunicación entre diversos organismos de Estados Unidos. En un inicio utilizó computadoras denominadas *Interface*

Message Processor, con módems conectados a líneas dedicadas de 50 Kbps [WWW14].

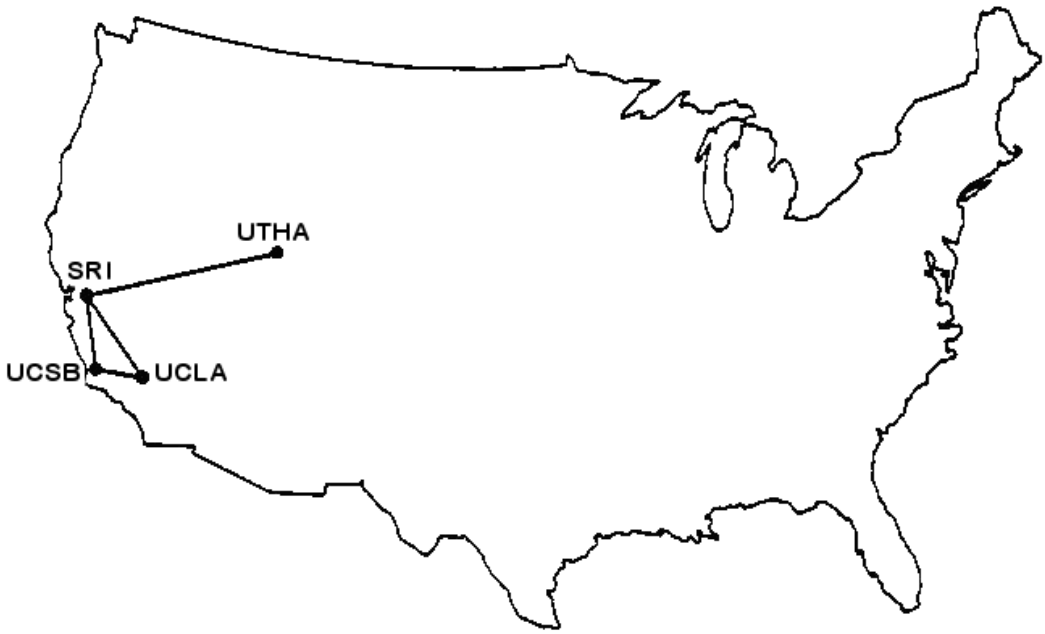

Figura 2.1 Mapa ARPANET (diciembre de 1969)
Basado en: "ARPANET Completion Report" [BOL81]

Definitivamente esta red ha evolucionado mucho en estos últimos 37 años y según estadísticas de la CIA [CIA2006] la red sobrepasa los mil millones de usuarios. Cabe resaltar que conforme iban aumentando los usuarios, los intereses dejaron de ser puramente académicos y se volvieron en gran medida comerciales.

A raíz de eso, en distintos países ha surgido la iniciativa de crear redes, una vez más, dedicadas únicamente al entorno académico y la investigación. En general a estas redes se les denomina NREN (Nacional Research and Education Network) y se encuentran interconectadas a nivel de continentes y a todo el mundo.

Entre las redes más destacadas se puede citar a:

- Abilene, en Norte América. Formada por el consorcio Internet2 y agrupa más de 220 universidades e instituciones, con enlaces de hasta 10 Gbps [WWW1]. Su topología se ilustra en la Figura 2.2.

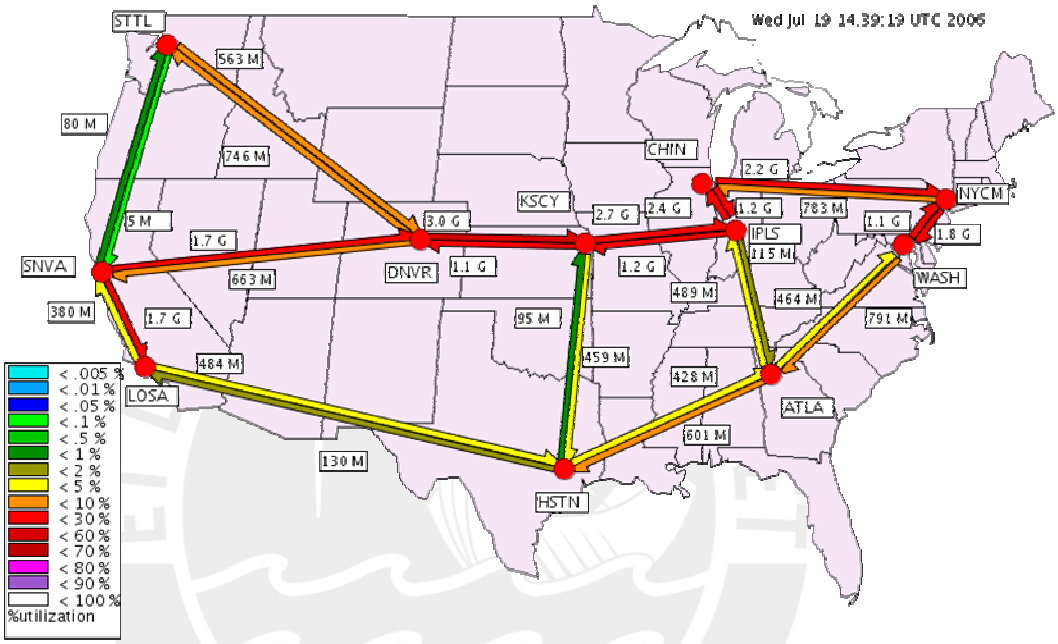

Figura 2.2 Backbone de Abilene
Fuente: Abilene Home, [WWW1]

- GÉANT2, en Europa. Construida y operada por DANTE (Delivery of Advance Network Technology to Europe). Esta forma un *backbone* que conecta las NREN de 30 países alrededor de Europa como RedIRIS en España, UKERNA en el Reino Unido, entre otras [WWW2]. La topología puede ser vista en la Figura 2.3.

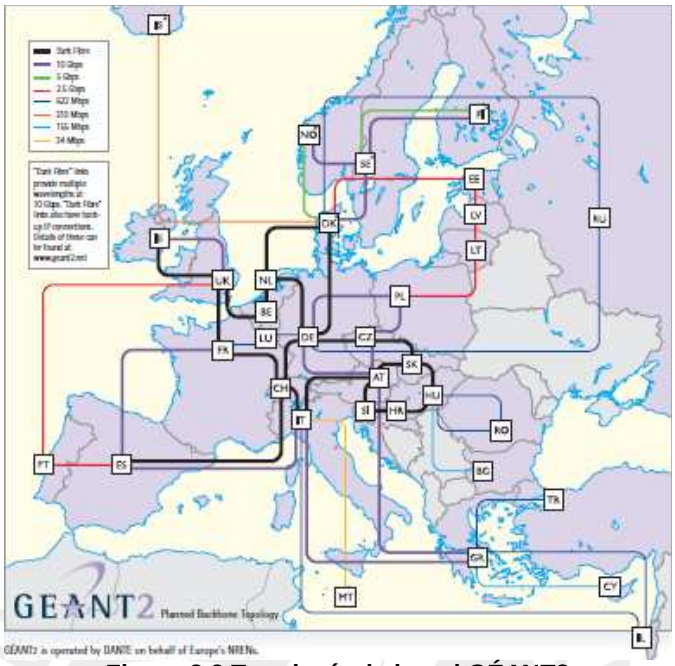

Figura 2.3 Topología de la red GÉANT2
Fuente: GÉANT2 topology [WWW5]

- APAN (*Asia-Pacific Advance Network*), en Asia. Une NRENs en Asia y Oceanía, como AARNet en Australia, APAN-JP en Japón, entre otras redes [WWW3] (Figura 2.4).

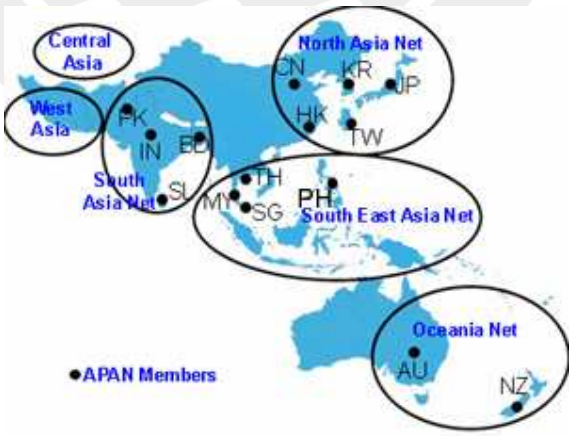

Figura 2.4 Países miembros de la APAN
Fuente: APAN Homepage [WWW3]

- CLARA (Cooperación Latinoamericana de Redes Avanzadas). Une los NRENs de Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, México, Nicaragua, Panamá, Perú, Uruguay y Venezuela. Clara nace gracias al proyecto ALICE (América Latina Interconectada con Europa), mediante el cual la comisión Europea firmó un contrato de 12.5 millones de Euros para la creación de esta red y su conexión con Europa y el resto del mundo [WWW4] como se ilustra en la Figura 2.5.

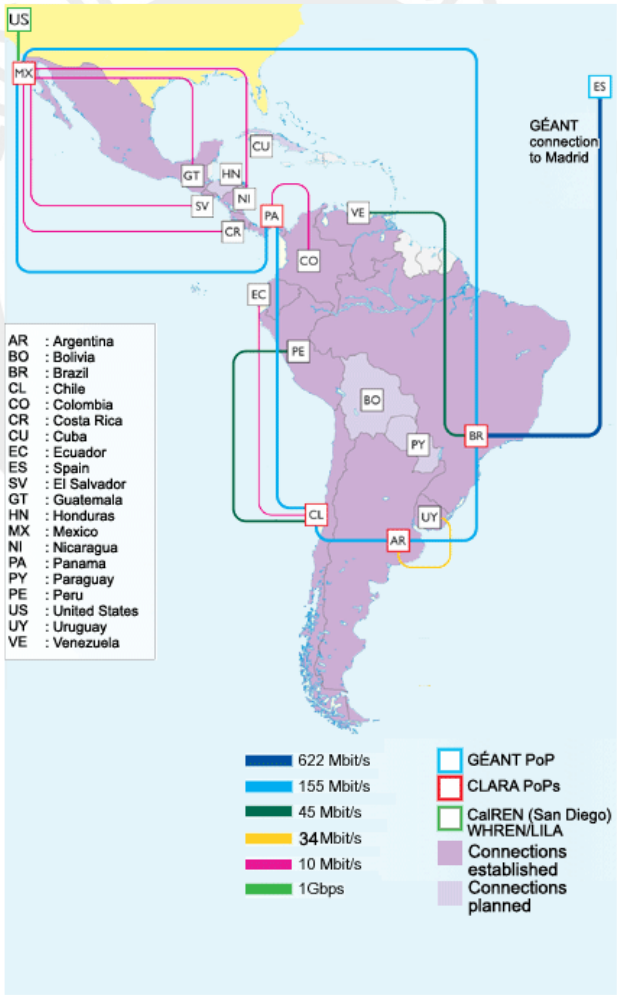

Figura 2.5 Topología de la red CLARA
Fuente: Mapa de la topología de RedCLARA [WWW6]

2.2. La RAAP

La RAAP es la NREN peruana, está en funcionamiento desde abril del 2005. El objetivo de esta red es:

> *"…desarrollar una infraestructura basada en tecnologías de comunicaciones avanzadas, que permita integrar universidades y centros de investigación en todo el país entre sí y con el resto del mundo, facilitando así el desarrollo de proyectos multidisciplinarios, descentralizados y colaborativos, orientados a la investigación, la innovación y la educación."*
>
> RAAP - [WWW8]

En general el fin de este NREN es actuar como soporte para el uso compartido de datos de carácter científico, servicios de colaboración, tratamiento de grandes cantidades de datos. Permitiendo la interconexión de instituciones a nivel nacional e internacional [WWW7].

2.2.1. Estructura de la RAAP

Actualmente la RAAP cuenta con nueve miembros:

- Pontificia Universidad Católica del Perú (PUCP).
- Universidad Nacional Mayor de San Marcos (UNMSM).
- Universidad Nacional de Ingeniería (UNI).
- Universidad Nacional Agraria de la Molina (UNALM).
- Universidad Peruana Cayetano Heredia (UPCH).

- Instituto Peruano de Energía Nuclear (IPEN).
- Instituto Nacional de Investigación y Capacitación de Telecomunicaciones (INICTEL-UNI).
- Universidad Ricardo Palma (URP).
- Universidad Católica Santa María (UCSM).

Estos puntos se encuentran interconectados, brindando a cada sitio remoto enlaces virtuales hacia todos los otros sitios, formando una topología en *mesh.* A la fecha, estos enlaces entre los puntos son líneas dedicadas, arrendadas a Telefónica del Perú (TdP), quien forma la red utilizando circuitos virtuales implementados con MPLS[1] (*Multiprotocol Label Switching*) dando a cada enlace, actualmente, un ancho de banda de 10 Mbps. Existe la posibilidad de que, en el futuro, otros operadores se unan a la RAAP ofreciendo también interconexión.

Desde el nodo ubicado en la PUCP sale el enlace de fibra óptica hacia el nodo de CLARA en Chile, permitiendo comunicar a la RAAP con el resto de las NRENs que forman parte de CLARA y desde ahí al resto del mundo. CLARA utiliza un enlace desde el nodo en México hacia Albilene (Internet2) y otro desde el nodo en Brasil hacia GÉANT2.

En una primera instancia la RAAP contó con IPv4 (*Internet Protocol version 4*), pero desde sus inicios se apuntaba a brindar soporte a IPv6 (*Internet Protocol*

[1] El MPLS es una tecnología de transporte de datos que opera entre las capas 2 y 3 del modelo de referencia OSI. El estándar está definido en la RFC3031

version 6), utilizando para ello una configuración *dual stack*[2], este se empezó a implementar en julio de 2006.

2.2.2. Distribución de direcciones IP

Desde un inicio se planteó la distribución de direcciones públicas únicas sin utilizar *Network Address Translators* (NATs) dentro de la red. Además se realizó un plan de numeración para la implementación de IPv6.

2.2.2.1. Direcciones IPv4

Se planteó la distribución de dos redes Clase C distribuidas en nueve subredes diferentes, una para cada sitio, como se muestra en la Tabla 2-1.

Tabla 2-1 - Distribución de direcciones IPv4 en la RAAP

Institución	IP WAN	Subred Asignada	IP Gateway
PUCP	10.129.215.174	200.37.45.0/26	200.37.45.1
INICTEL	10.160.215.162	200.37.45.64/26	200.37.45.65
UNMSM	10.129.215.178	200.37.45.128/26	200.37.45.129
IPEN	10.160.215.166	200.37.45.192/26	200.37.45.193
UPCH	10.129.215.190	200.37.46.0/26	200.37.46.1
UNALM	10.128.215.162	200.37.46.64/26	200.37.46.65
UNI	10.128.215.174	200.37.46.128/26	200.37.46.129
URP	10.160.215.170	200.37.46.192/28	200.37.46.193
UCSM	10.208.215.166	200.37.46.208/28	200.37.46.209

En todos los casos al *router* que da acceso a cada LAN a la RAAP se le asigna la primera dirección de cada subred.

Además, como se observa en la Tabla 2-1 en la WAN TdP se utilizan direcciones pertenecientes a una red Clase A privada.

[2] Mas información sobre técnicas de transición de IPv4 a IPv6 puede ser encontrada en [TAM2004]

2.2.2.2. Direcciones IPv6

La RAAP planteó una forma de distribución que beneficie el enrutamiento jerárquico, tomando en cuenta no solo a los actuales sitios, sino previendo todo tipo de instituciones académicas que pueden llegar a ser miembros de la RAAP. Las direcciones para los sitios que actualmente forman la RAAP son mostradas en la Tabla 2-2.

Tabla 2-2 Distribución de direcciones IPv6 para los actuales miembros de la RAAP

Institución	IP WAN	Subred Asignada	IP Gateway
PUCP		2001:13A0:1041::/48	2001:13A0:1041::1
INICTEL	2001:13A0:7F1F::F2	2001:13A0:1061::/48	2001:13A0:1061::1
UNMSM	2001:13A0:7F1F:: 2	2001:13A0:1021::/48	2001:13A0:1021::1
IPEN	2001:13A0:7F1F::FA	2001:13A0:1062::/48	2001:13A0:1062::1
UPCH	2001:13A0:7F1F::22	2001:13A0:1042::/48	2001:13A0:1042::1
UNALM	2001:13A0:7F1F::12	2001:13A0:1023::/48	2001:13A0:1023::1
UNI	2001:13A0:7F1F:: A	2001:13A0:1022::/48	2001:13A0:1022::1
URP			
UCSM			

Como se observa en la Tabla 2-2, la PUCP, la URP, y la UCSM, aún no tienen asignadas direcciones para su enlace WAN, puesto que estas no cuentan aún con conectividad para este protocolo, sin embargo dentro de la distribución ya se les ha asignado una subred.

2.2.3. Utilización actual y futura

El principal uso que se le da a la red en la actualidad es su utilización para videoconferencias de tipo académico, tanto a nivel local, como internacional, dado el gran ancho de banda y la baja latencia se han logrado conexiones de gran calidad con puntos alrededor del mundo. Dentro de estos eventos se

puede destacar el del 13 de marzo del 2006 denominado “Cruzando el Atlántico con la Nueva Internet”, en el cual participaron más de 20 puntos de alrededor del mundo [WWW9].

Por otro lado, la red se utiliza para mover grandes cantidades de información cuyo traslado tomaría mucho tiempo a nivel de la Internet comercial. Además la baja latencia también beneficia a la ejecución de escritorios remotos y aplicaciones distribuidas.

Se prevé que la utilización de la red en lo que respecta a videoconferencia siga en aumento y que a esto se le sumen tráficos de *streaming* y grandes cantidades de datos para análisis científico.

2.2.4. Necesidades del centro de gestión

Este centro de gestión debe medir constantemente la utilización de la red, su rendimiento y facilitar la detección de problemas. Las herramientas utilizadas para el centro de gestión soportan IPv4 e IPv6 que son los protocolos con los que trabaja la RAAP.

Por otro lado las computadoras conectadas a la RAAP cuentan con diversos sistemas operativos, diferentes distribuciones de Linux y en algunos casos Windows, por ello es necesario un sistema que sea multiplataforma.

Además, si bien es cierto la implementación del centro de gestión es centralizada en un servidor, es imprescindible que cualquier miembro de la RAAP pueda acceder a algún tipo de información desde su ubicación; es por ello que se prefiere una interfaz que permita la administración remota.

Capítulo 3: Gestión de redes

3.1. Definición

La gestión de redes es un concepto bastante general, que implica la utilización de herramientas para ayudar en el manejo de dispositivos, sistemas y redes. [MAUD2005]

Según Sayman [SAY1996]: *"La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable".*

3.2. Antecedentes

Conforme el campo de las redes avanzaba y crecía tanto en tamaño como en complejidad se vio la necesidad de contar con un sistema para su administración, localización de fallos, estudio de rendimiento, entre otros.

En la actualidad existe más de un protocolo dedicado a la gestión de redes, desde estándares propietarios como NBAR de Cisco y por otro lado protocolos completamente abiertos como el SNMP. Al ser este accesible a cualquier persona o empresa este último está mucho más difundido y se puede encontrar todo tipo de equipos que lo implementan.

Dentro del contexto de una red se puede administrar los equipos encargados de su funcionamiento como concentradores (*hubs*), conmutadores (*switches*) y enrutadores (*routers*), así como equipos servidores y los servicios que corren dentro de ellos (Web, correo, DNS). Además también es posible incluir dentro de la administración otros equipos adicionales, como los UPS, controladores de temperatura, etcétera.

3.3. Modelo para la gestión de redes

Se analizará un modelo propuesto por la ISO, en este se definen los objetivos que debe seguir un administrador para gestionar su red de manera integral. El modelo es un modelo de referencia, lo cual implica que, debe ser adaptado a

nuestro entorno en función a las necesidades específicas de la red a gestionar, poniendo énfasis en ciertos puntos [WAL2000] [MAUD2005] [WWW23].

Este modelo es también comúnmente conocido como FCAPS, por las siglas de sus áreas funcionales en inglés (*Fault-Management, Configuration, Accounting, Performance, Security)*.

3.3.1.1. Gestión de fallas

Lo ideal al tener una red es que siempre esté disponible y que en caso ocurra una falla esta pueda ser detectada y que se envíe una alerta para su corrección. El problema debe ser reconocido, aislado, corregido y lo ideal es también tener un registro de lo sucedido y de la solución tomada.

3.3.1.2. Gestión de configuraciones

El objetivo de esta categoría es tener información sobre cada dispositivo de la red en lo que respecta a sus capacidades y a su actual configuración, así como llevar un control de los cambios que ocurran.

3.3.1.3. Gestión de contabilidad

En esta categoría tiene por objetivo asegurar que los recursos de la red están siendo correctamente utilizados y conocer quién los utiliza.

Esto puede ser visto desde dos puntos de vista, en el caso de sistemas cuya utilización involucra un pago, se debe poner énfasis en que cada usuario no supere sus cuotas permitidas, además de llevar un control de lo que se debe cobrar. Por otro lado se debe administrar el acceso de los usuarios a los recursos, por medio del establecimiento de permisos y contraseñas.

3.3.1.4. Gestión de performance

Dentro de lo que es la performance, se debe poder observar y analizar la utilización de la red, de manera que se pueda determinar el estado y eficiencia de la misma, así como el poder definir tendencias y poder preparar los requerimientos de la red en un futuro.

Además del ancho de banda utilizado puede ser conveniente analizar parámetros tales como tasas de error, paquetes eliminados, tiempos de latencia, entre otros. Deber ser posible definir límites, que de ser sobrepasados generen una alerta.

3.3.1.5. Gestión de seguridad

La seguridad por un lado está relacionada con la contabilidad en lo que se refiere al acceso a los recursos. Pero además implica la protección frente a ataques externos por parte de personas ajenas a la red. Esto puede implicar la

utilización de *firewalls*, sistemas de detección y prevención de intrusos así como antivirus.

3.4. Protocolos de gestión de redes

3.4.1. SNMP

SNMP son las siglas de "Simple Network Management Protocol", es un protocolo que permite realizar la gestión remota de dispositivos. El predecesor de SNMP, SGMP (*Simple Gateway Management Protocol*) fue diseñado para administrar *routers*, pero SNMP puede administrar prácticamente cualquier dispositivo, utilizando para ello comandos para obtener información y para modificar la información.

Este protocolo ha sido definido por la IETF, para lo cual ha publicado una serie de RFCs, detallados en la Tabla 3-1.

Tabla 3-1 Relación de RFCs para las distintas versiones del SNMP

Versión	RFCs
SNMPv1	1157
SNMPv2p	1441, 1452
SNMPv2c	3416, 3417, 3418
SNMPv3	3410, 3411, 3412, 3413, 3414, 3415, 3416, 3417, 3418, 2576

La primera versión de SNMP es la más antigua y básica, su principal limitación es que la seguridad se provee por comunidades, que son *passwords* sin ningún tipo de encriptación, esto se trató de resolver proporcionando una seguridad más fuerte en la versión 2p de este protocolo (SNMPv2p), pero este esquema, bastante más complicado de implementar, no fue adoptado por muchos

fabricantes. Esta versión además proveía nuevas funciones para aumentar la eficiencia cuando se trabaja con cantidades grandes de datos, rescatando estas ventaja y volviendo a la autenticación basad en comunidades, se introdujo la versión 2c (SNMPv2c). Existen además otras dos versiones de SNMP la SNMPv2* y la SNMPv2u, pero no han sido muy difundidas. En general cuando se habla de SNMPv2 se hace referencia a SNMPv2c.

Actualmente, la versión 3 (SNMPv3) es reconocida como el estándar de la IETF desde el 2004, lo principal en ella es la seguridad, por lo cual este protocolo está diseñado para proveer: Autenticación, Privacidad, Autorización y control de acceso.

Existen dos aspectos a resaltar en lo concerniente a estas versiones, el primero es que todas pueden ser soportadas de manera simultánea, como lo describe el RFC3584[3]. Por otro lado, si bien el RFC1157 que describe el SNMPv1 está ya archivado como histórico, este protocolo es el más utilizado actualmente [MOD2003], a pesar de las falencias de seguridad mencionadas anteriormente.

3.4.1.1. Arquitectura del sistema SNMP

Por la forma en la que el protocolo está implementado, se distinguen dos entidades: estaciones administradoras y elementos de la red [RFC1157]. Una estación administradora es un servidor que, por medio de un programa, realiza

[3] RFC3584: *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.*

la gestión de los dispositivos por medio de comandos y consultas SNMP. El programa que realiza la gestión es denominado NMS (*Network Management System*). Por otro lado en los elementos a administrar residen los agentes, que son los que responden los mensajes y realizan las acciones indicadas por el NMS.

En la Figura 3.1 se muestra un ejemplo de red gestionada utilizando SNMP, cabe resaltar que los elementos a gestionar pueden encontrarse en la misma LAN así como en la WAN o en otras LANs a las que el NMS tenga acceso, incluso dentro del mismo servidor es posible tener el NMS y un agente, es decir el servidor se puede gestionar a sí mismo.

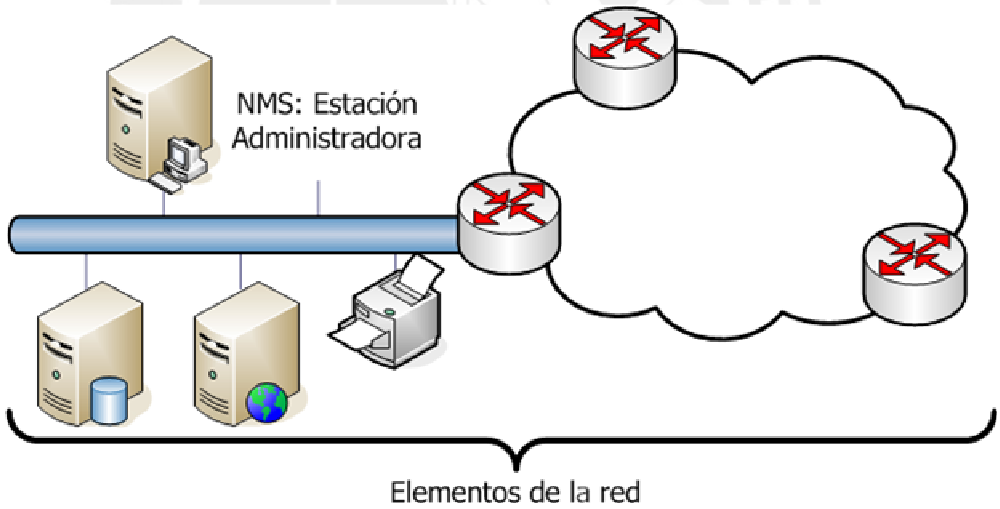

Figura 3.1 NMS y los elementos de la red

Entre el NMS y los agentes se intercambian tres tipos básicos de mensajes, mostrados en la Figura 3.2. La dupla *query/response* corresponden al *pooling* o sondeo que realiza el NMS de manera periódica y a la respectiva respuesta. El *trap* corresponde a un mensaje no solicitado por el NMS que puede mandar el

agente en caso ocurra un evento determinado, por ejemplo, la desconexión de una interfaz en un *router*. Una cosa a considerar es que si bien el *pooling* es usualmente periódico, al igual que el *trap* es de naturaleza asíncrona, ya que no tiene un tiempo determinado de inicio y el agente debe estar preparado para responder *queries* o generar *traps* en cualquier momento.

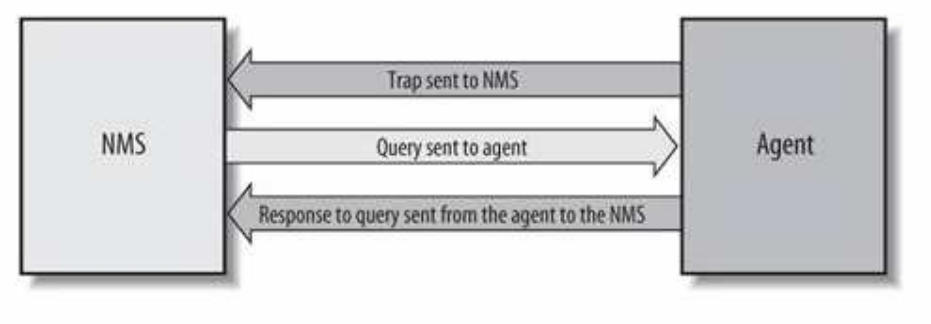

Figura 3.2 Mensajes entre el NMS y el Agente
Fuente: Essential SNMP, 2nd Edition [MAUD2005]

3.4.1.2. Datagrama SNMP

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

3.4.1.3. ASN.1

El *Abstract Syntax Notation One* (ANS.1) es un estándar de la ISO y la ITU-T para describir mensajes a ser intercambiados entre aplicaciones. Provee un conjunto de reglas para describir la estructura de los objetos. SNMP utiliza un subconjunto de las reglas definidas por este estándar, para la definición de cómo se van a representar y transmitir los datos.

3.4.1.4. SMI

La *Structure of Management Information* (SMI) define el nombre y tipo de datos de los objetos gestionables. Cada objeto a gestionar tiene tres atributos:

- El nombre u OID (Object Identifier) el cual define de manera unívoca cada objeto.
- Tipo y sintaxis: Para esto se utiliza la ASN.1, de manera que la sintaxis sea universal y no haya problema al comunicar sistemas diferentes.
- Codificación: Se define como se codifican y decodifican los objetos en una cadena de octetos, de manera que no haya problema al transmitirlos.

3.4.1.5. MIB

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

En la Figura 3.3, se muestra la estructura de la MIB-2, su posición dentro del árbol y los objetos administrables dentro de esta.

La jerarquía se inicia en la raíz, desde la cual se dividen tres ramas, una para los objetos administrados por la ITU-T, antes CCITT, la segunda para los administrados por la ISO y la tercera para los de administración conjunta.

Dentro de la rama de la ISO, la tercera subdivisión corresponde a organizaciones, como se mencionó en el Capítulo 2, la Internet nace por un proyecto del departamento de defensa de los Estados Unidos, es por ello que su OID se encuentra dentro de DOD (*Department of Defense*). Debajo del subárbol Internet, existen ramas relacionadas a administración de redes y SNMP, estos subárboles son administrados por la IANA.

Son de especial interés el mgmt.mib-2 y el private.enterprises, en el primero se define la MIB estándar de Internet, y el segundo es proporcionado a empresas para que puedan registrar OIDs particulares para ser utilizados en soluciones propias de hardware o software. La estructura puede ser vista en la figura 3.3.

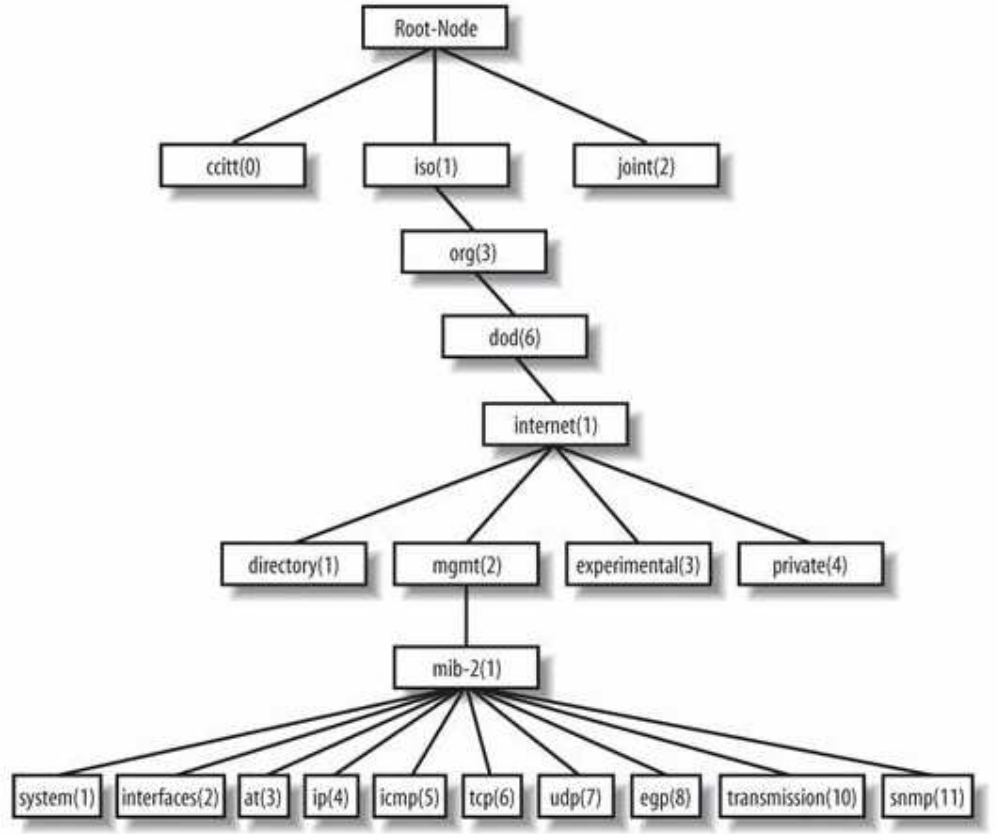

Figura 3.3 Estructura jerárquica de la MIB-II
Fuente: Essential SNMP, 2nd Edition [MAUD2005]

3.4.1.6. OID

Los OIDs (Object IDentifier) es la dirección de una variable o nodo dentro de la estructura de alguna MIB, está constituida por números enteros positivos separados por puntos. Por ejemplo el nodo system es: .1.3.6.1.2.1.1

Se debe notar el punto inicial que corresponde a la raíz. Además, el valor de los objetos se referencia por un sufijo, según el tipo de dato que retorna, así un valor único, como un entero o una cadena de caracteres, es referenciado por

un 0 y un objeto con múltiples entradas, como una tabla, se utilizan sufijos distintos de cero para cada entrada.

3.4.2. RMON

RMON (Remote MONitoring) es un estándar para la gestión que define grupos para el monitoreo de distintos requerimientos de la red, general alertas, etc. Implementa una MIB con un agente que corre en determinados dispositivos, denominados, monitores o sondas, para poder tener estadísticas completas es necesario contar con uno de estos dispositivos en cada segmento de red.

Los objetivos definidos en el [RFC2021] son:

- El dispositivo almacena información y estadísticas aún cuando la estación gestora no se encuentre operando, o no se encuentre en constante comunicación.
- El monitoreo es continuo ya que se da en el mismo agente, además provee facilidades para ver información histórica y la posibilidad de alertar de fallas en el momento que estas ocurren.
- La sonda puede ser configurada para detectar anomalías específicas e informar de estas.
- Como el monitor está en el mismo segmento de red que los equipos que monitorea puede recuperar información que el gestor difícilmente podría obtener de otra forma. Por ejemplo, identificar el *host* que genera más tráfico.

- En caso se tengan múltiples gestores, RMON da la posibilidad de que la información se procese y/o almacene en este agente, evitando repetir tareas en los distintos gestores.

3.4.3. NBAR

NBAR (Network-Based Application Recognition) es un mecanismo integrado en las últimas versiones del IOS de algunos *switches* y *routers* CISCO[4]. Este clasifica los flujos de información que pasan por los equipos, buscando identificar el protocolo y la aplicación que los genera. Para ello, se basa en el análisis del primer paquete del flujo, dentro del cual analiza los puertos de origen y destino, además de la información dentro del paquete mismo.

Con esta información se pueden establecer políticas de QoS priorizando aplicaciones importantes para la red [WWW17]. También gracias a esto se puede obtener estadísticas de la utilización del ancho de banda disponible según protocolos o aplicaciones. Además es posible reconocer patrones de virus o troyanos de manera que no ingresen a la red, por ejemplo el gusano "Code Red" [WWW20].

[4] La lista completa puede ser encontrada en [WWW15]

3.5. Software para administración

Dentro de lo que se refiere a la administración de redes existen múltiples implementaciones de sistemas de tipo comercial y libre, muchos de ellos se enfocan a necesidades específicas del administrador de redes y otros son más generales. En las siguientes secciones se presenta una revisión breve de las principales características de las aplicaciones más conocidas.

3.5.1. Software comercial

Si bien la tesis se orienta a una implementación utilizando herramientas de software libre, es importante analizar las opciones que ofrece el mundo comercial de manera que se identifique algunas características con las que convendría contar.

3.5.1.1. HP Openview

"HP OpenView es un conjunto de soluciones de software, amplio y modular para gerenciar y optimizar los servicios de TI e infraestructura de voz y datos" [WWW10]

Esta solución está compuesta de muchas partes que en conjunto consideran todas las necesidades que un administrador de redes pueda tener. Dentro de los productos, se encuentran:

- Network Node Manager (NNM)
- Customer Views (CV)
- Services Information Portal (SIP)

Es de especial interés para el presente estudio el NNM, pues es el que se encarga de la administración de dispositivos SNMP, provee además capacidades para el descubrimiento de equipos y la posibilidad de mostrar gráficas topológicas. [ZIT2004]

El NNM descubre todos los elementos a los que tiene acceso y los agrega a la topología, muestra además un sistema de alertas de los que tiene configurados. Dentro de la topología conforme se navega al segmento de red que se quiere observar, es posible tomar más acciones sobre los *host*, como observar alarmas específicas, monitorear interfaces, realizar conexiones telnet, entre otras.

Si bien este es un sistema muy completo su implementación implica un costo bastante elevado. Además el software necesita una máquina relativamente poderosa[5] para funcionar sin problemas. En la Figura 3.4 se muestra una de las interfaces que grafica una red, se pueden observar los distintos tipos de dispositivos y los diferentes segmentos de red, haciendo clic sobre alguno, se pasaría a observar con mayor detalle los equipos presentes en este segmento, en la parte superior se muestra el manú con distintas opciones para la visualización y configuración.

[5] El DataSheet del NNM [WWW21] recomienda como mínimo 1 GB de RAM y 912 MB de HD.

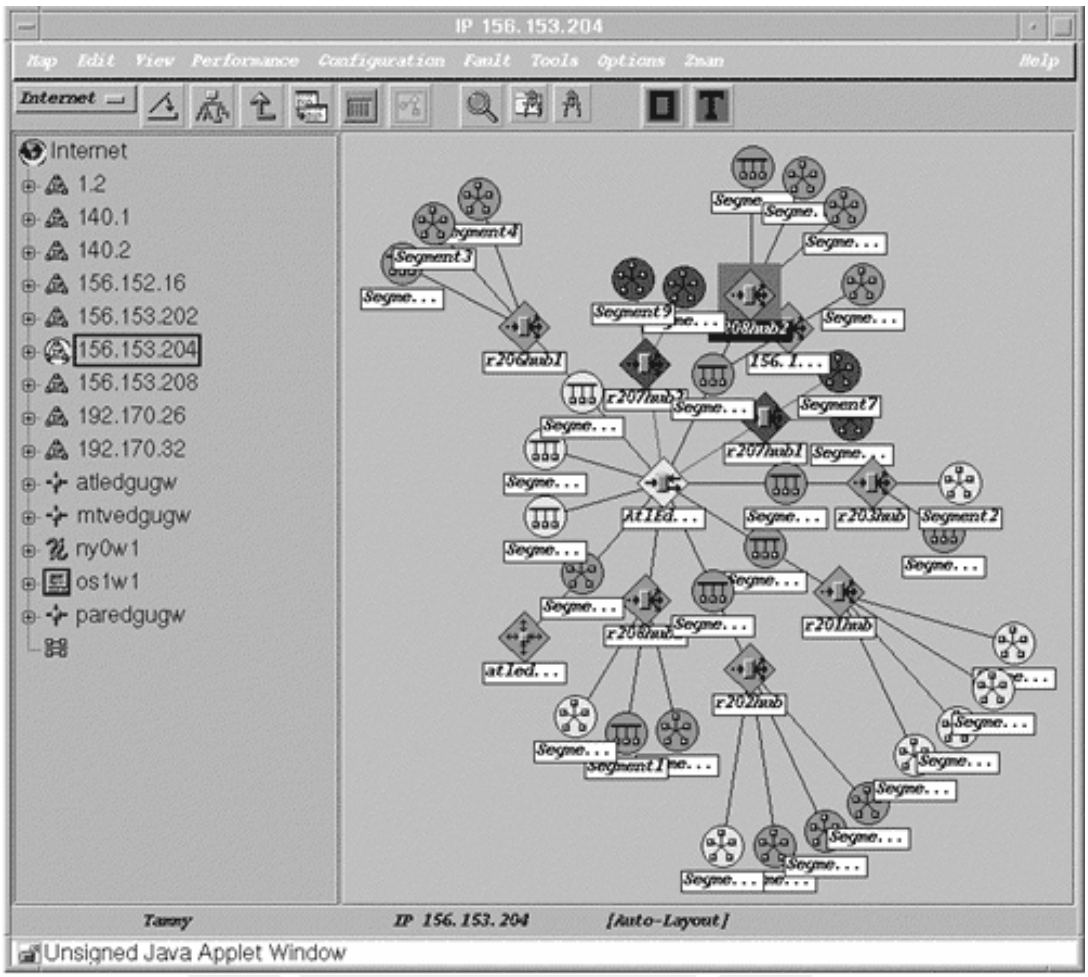

Figura 3.4 Gráfico de una red en HP OpenView
Fuente: HP OpenView System Administration Handbook [ZIT2004]

3.5.1.2. IBM Tivoli

De manera similar al HP OpenView, el IBM Tivoli es una solución extensa, la presente comparación será enfocada en el Monitoring, el cual "…*proporciona funciones de supervisión para los recursos esenciales del sistema a fin de detectar los cuellos de botella y los problemas potenciales, así como recuperarse automáticamente de situaciones críticas*." [WWW11]

Este software cuenta con una interfaz Web que permite visualizar datos de manera remota, supervisa programas en servidores, aplicaciones, bases de datos y software intermedio. En la Figura 3.5 se muestra la interfaz con diversas estadísticas de un dispositivo, como estado del CPU, capacidad disponible en los discos duros, estado de la memoria RAM y virtual.

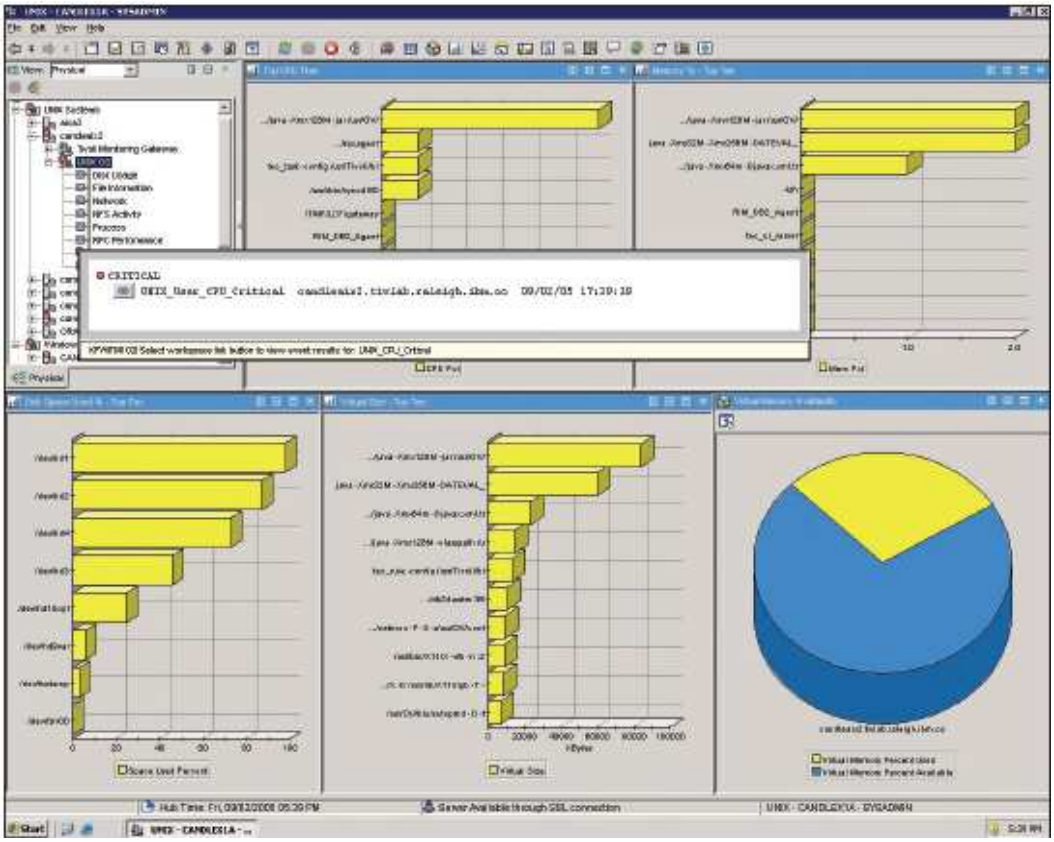

Figura 3.5 Tivoli Monitoring, monitoreo de un sistema operativo UNIX
Fuente: IBM Tivoli Monitoring datasheet [IBM2006]

3.5.1.3. Solarwinds Orion Network Performance Monitor

Este es un sistema, basado completamente en Web, orientado al manejo de fallas y performance, utiliza SNMP para analizar datos de *routers*, *switches*, servidores, etcétera. El sistema corre sobre Windows 2000 o 2003 Server lo

que incrementa el costo de licencias. La Figura 3.6 muestra interfaces para el monitoreo de un *switch*, en esta se observan estadístivas de tiempos de respuesta y pérdida de paquetes, así como de utilización de memoria y CPU. Las estadísticas son dadas en forma de instrumentos de medición para la última medición y como gráficos para observar datos históricos.

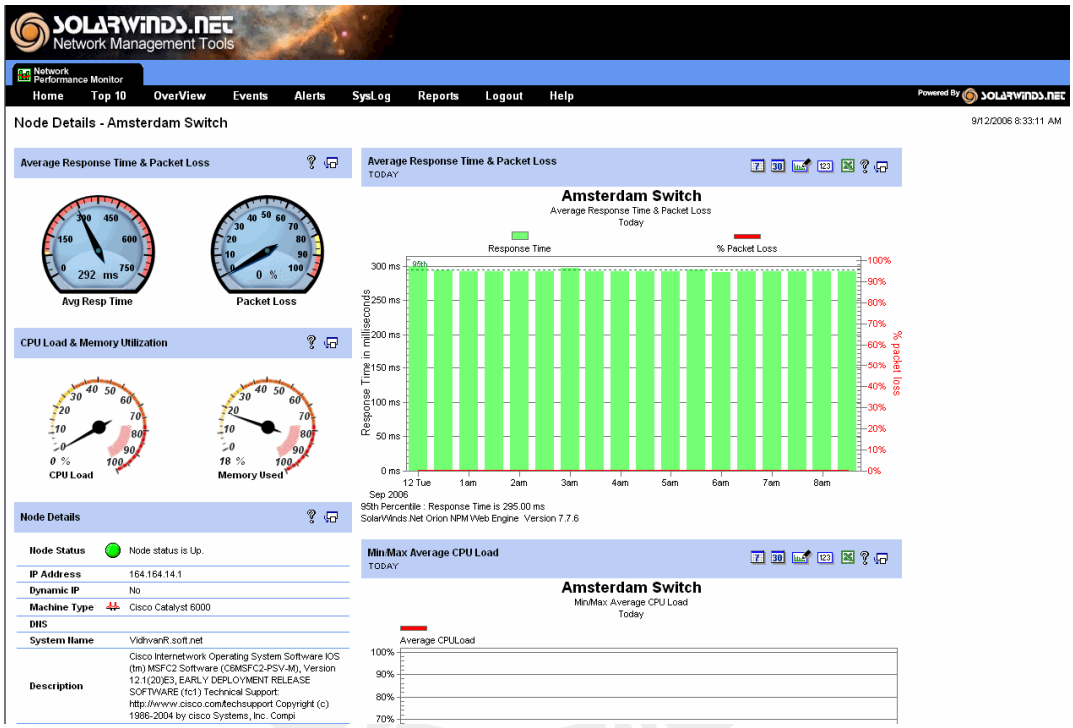

Figura 3.6 SolarWinds manejo de eventos y alertas
Fuente: SolarWinds datasheet [SOL2006]

3.5.2. Software libre

Se entiende por software libre, el software que puede ser copiado, modificado y redistribuido sin costo alguno. Lo cual trae consigo muchas ventajas, entre las cuales destaca el no tener que pagar ningún tipo de licencia, la posibilidad de ver el código fuente y realizar modificaciones, por ejemplo, para adaptar algo a necesidades específicas.

Es común encontrar comunidades detrás de cada producto de software libre, estas proveen soporte para el mismo así como un constante desarrollo de nuevas versiones, parches de seguridad o de corrección de errores. La mayoría de comunidades son tan libres como el software, por lo que cualquier persona con conocimientos y tiempo puede aportar para el desarrollo o para la depuración de errores. Además, es común encontrar al creador o creadores del software respondiendo preguntas en los foros [CHA2003] [DUD2006].

3.5.2.1. MRTG

El Multi Router Traffic Grapher, es un software que permite realizar gráficas de dispositivos SNMP, de manera que se pueda analizar la performance, las tendencias, entre otras cosas. Está escrito en Perl y funciona tanto en Linux como en Windows. [OET2006a].

El programa puede generar páginas HTML con los gráficos como figuras GIF, estas son similares a la mostrada en la Figura 3.7, en la cual se muestra un gráfico de estadísticas de tráfico entrante (verde) y saliente (línea azul).

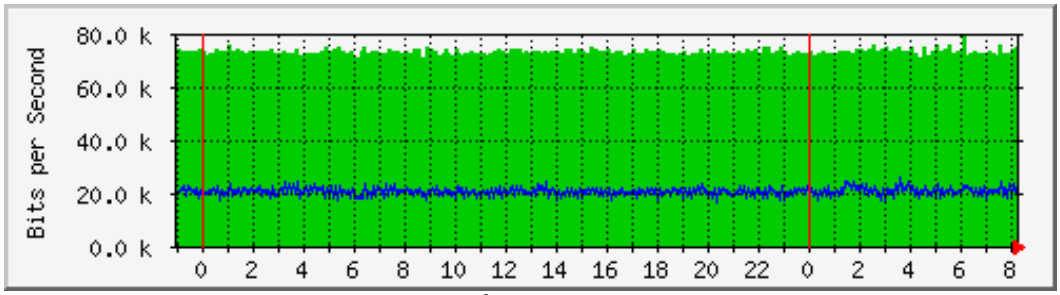

Figura 3.7 Gráfica utilizando MTRG

3.5.2.2. RRDTools

RRDTools (Round Robin Database Tools) es un software libre del mismo autor del MRTG, está orientado al almacenamiento de datos y la generación de gráficos basados en estos. Provee un motor de bases de datos cíclicas, es decir trabaja con una cantidad fija de datos y cuando todos los registros se llenan se escribe sobre el dato más antiguo. Esto proporciona una estructura de datos fija cuyo tamaño y resolución serán definidos al crearla. Se puede establecer más de una base de datos para cada dispositivo a monitorear de manera que se mantengan promedios a diferentes resoluciones para una misma información [BOA] [OET2006b].

El RDDTools, además provee capacidades para graficar en función a los datos almacenados, como se muestra en la Figura 3.8, en dicha figura se muestran diversas fuentes graficadas en distintos colores.

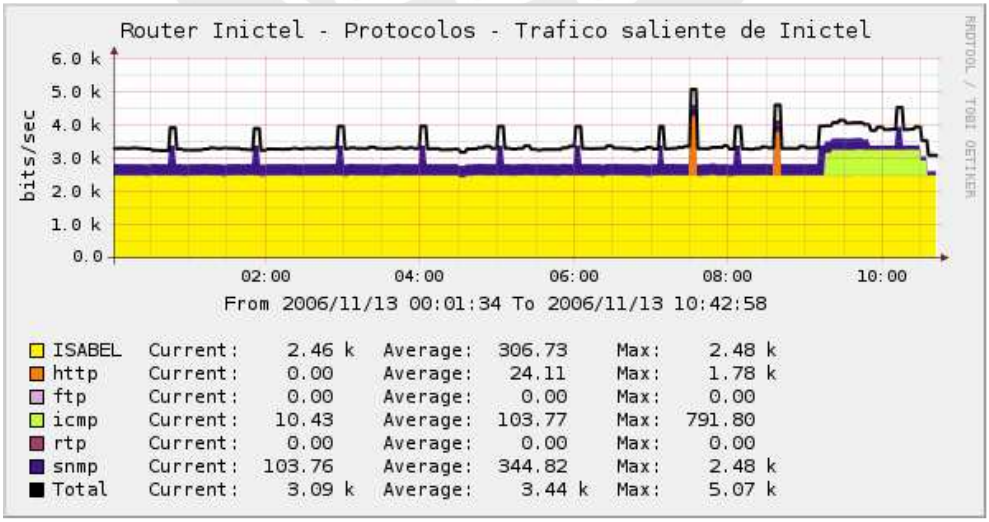

Figura 3.8 Gráfica usando RRDTools

3.5.2.3. SmokePing

Este es un programa escrito en Perl, para medir la latencia en un enlace. Utiliza RRDTools, para graficar y los datos son guardados en RRDs. Con esto se puede observar tendencias en latencia y pérdida de paquetes, permite además configurar alarmas en función a límites o patrones. En la Figura 3.9 se muestra un gráfica de tiempos de respuesta, y debajo estadísticas de pérdidas de paquetes [OET2006c] [SWR] .

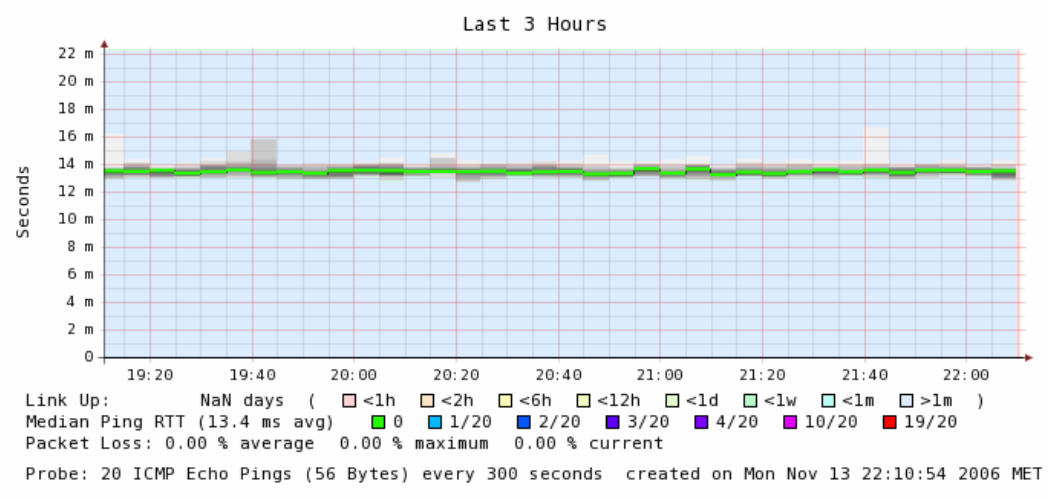

Figura 3.9 Gráfica de SmokePing

3.5.2.4. Cacti

Cacti es una interfaz Web, escrita en PHP, que hace uso del RRDTools, provee todo un conjunto de programas para hacer el sondeo así como *scripts* para equipos específicos y plantillas para diversos tipos de gráficos y equipos. Incluye además el manejo de usuarios, y a cada cual se le puede asignar diferentes permisos para ver o para crear nuevos gráficos.

Está escrito en PHP, y es posible implementarlo en Linux, Solaris, BSD, e incluso Windows [BEI] [CAL].

Cuenta con una arquitectura de *plugins* que puede ser instalada de manera opcional, esta proporciona nuevas funcionalidades, por ejemplo definir límites y alertas cuando estos sean alcanzados, permitir descubrir nuevos dispositivos, mostrar mapas de red, etcétera [WWW12]. La interfaz por defecto es mostrada en la Figura 3.10, a la izquiera se muestran las opciones de configuración y en la parte superior los botones de navegación para ir a la sección donde se muestran los gráficos por dispositivo.

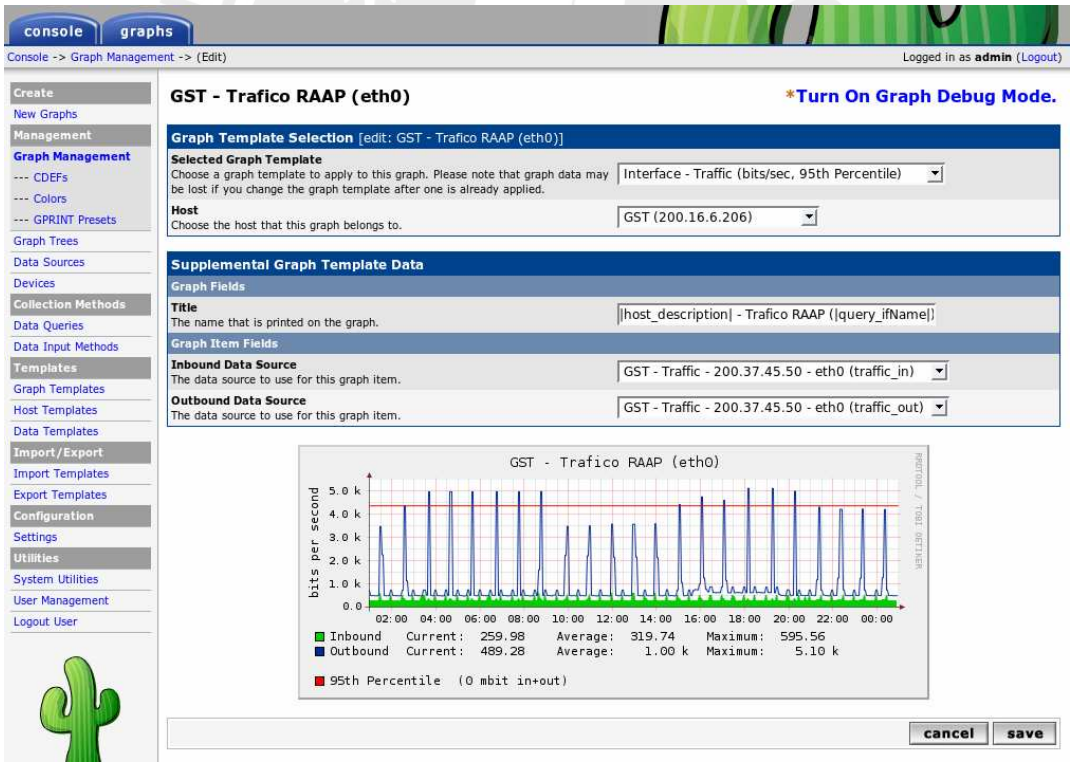

Figura 3.10 Interfaz de Cacti

3.5.2.5. Nagios

Nagios es un programa para el monitoreo de redes, equipos y servicios. Está escrito en C y puede ser instalado en Linux y algunas variantes de Unix. Nagios está diseñado para monitorear una sistema poniendo énfasis en los servicios que corren sobre él, y alertar en caso ocurra un error. El monitoreo se realiza mediante SNMP y scripts. Cuenta con un gran número de *plugins*, que permiten adicionar funcionalidades, por ejemplo el NRPE (Nagios Remote Plugin Executor) que permite ejecutar *scripts* de manera remota en los *host* monitoreados. Dentro de cada servidor se puede monitorear el estado de servidores de correo, servidores Web, manejadores de bases de datos, entre otros servicios. Así como llevar registro de la utilización del ancho de banda, utilización del disco duro y otras estadísticas [BUC] [WEH2006].

Además puede ser configurado para tomar acciones ante un problema, de forma que a la vez que se generan alertas, se pueda realizar una acción concreta, por ejemplo, reiniciar un demonio. Asimismo permite establecer formas de monitoreo jerárquico lo cual es muy ventajoso en entornos con una gran cantidad de equipos [ROB2005].

En la Figura 3.11 se muestra la interfaz de un mapa de red, a la izquierda se encuentran las opciones para otras visualizaciones, tales como estadísticas históricas, estado de los servicios, entre otras opciones.

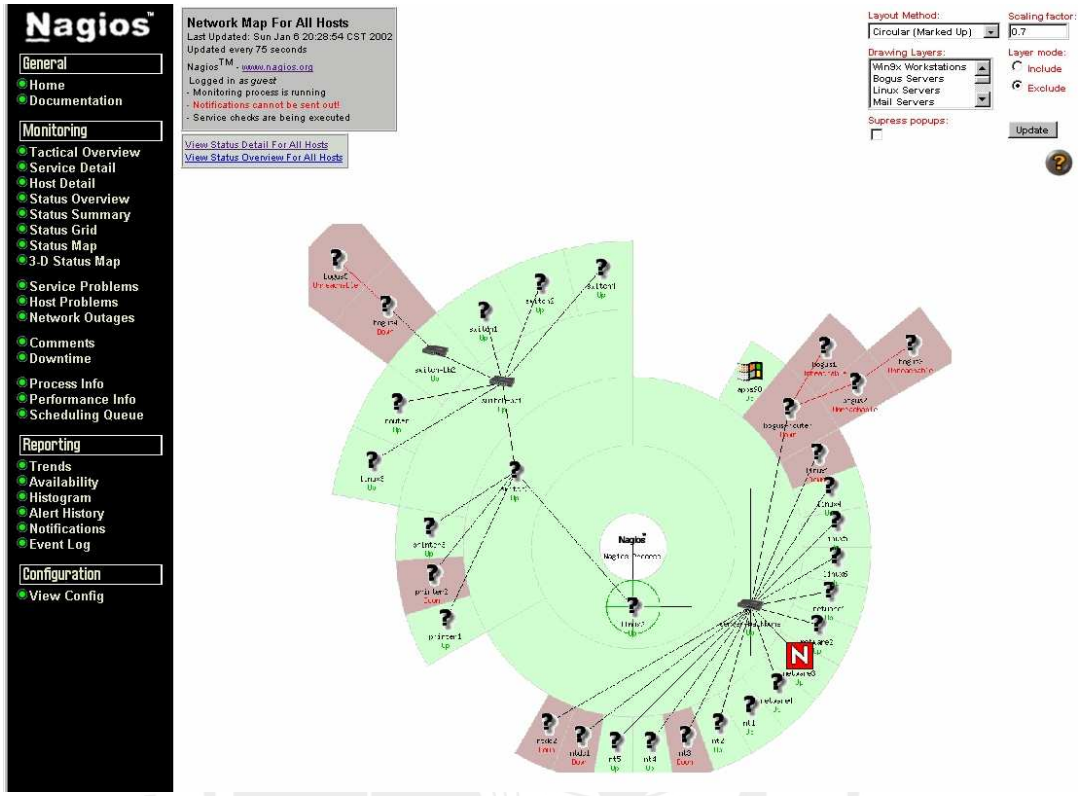

Figura 3.11 Nagios
Fuente: Página oficial de Nagios [WWW16]

3.5.2.6. OpenNMS

OpenNMS apunta a ser un sistema completo comparable al HP OpenView o IBM Tivoli, está escrito principalmente en Java, se enfoca principalmente en el monitoreo de servicio, de forma similar al Nagios, para esto simula un usuario accediendo a los servicios, por ejemplo para un servidor Web pide una página, para un servidor de correos manda un correo, etcétera [TAB2005].

Se enfoca en cubrir todas las áreas del modelo OSI para la gestión de redes, algunas por defecto y otras mediante integración con otras herramientas.

Cuenta con un modelo de monitoreo distribuido, que permite realizar eficientemente el monitoreo de redes de gran tamaño.

La Figura 3.12 muestra la disponibilidad de cada dispositivo y si es que hay alguna notificación importante, con los enlaces en la barra superior se puede acceder a las demás interfaces que permiten observar gráficos, notificaciones, mapas de red y estadísticas en general.

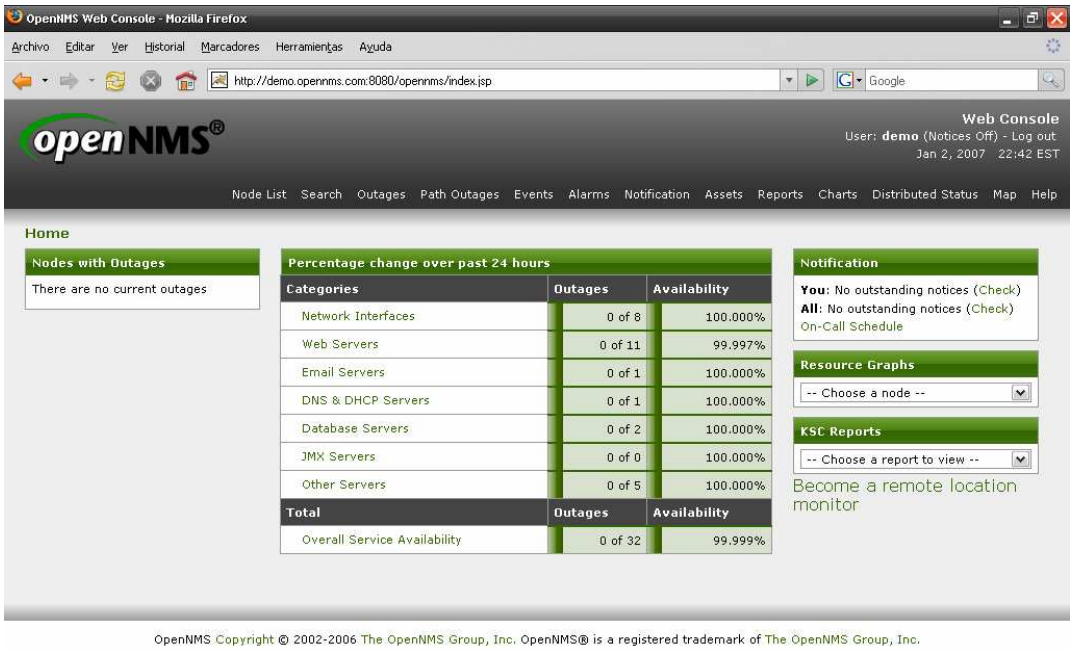

Figura 3.12 OpenNMS
Fuente: OpenNMS demo [WWW18]

Capítulo 4: Diseño e implementación del NOC

4.1. Sistema a implementar

El sistema pone énfasis en el principal problema actual que tiene la RAAP que es la medición de la utilización de sus enlaces, con este sistema es posible realizar pruebas de performance, observar la utilización de los enlaces, constatar el correcto funcionamiento de los equipos, así como constatar que el proveedor cumple con los SLA.

Una característica importante es que el sistema debe ser capaz de monitorear el tráfico en IPv6 ya que la red lo soporta y la RAAP promueve activamente su utilización.

Además se debe contar con un sistema de alarmas que alerten a la persona encargada en caso de que ocurra algún problema con la red o un servidor, de forma que la interfaz del sistema no tenga que estar siendo revisada en todo momento.

Finalmente el sistema debe ser lo suficientemente flexible como para agregar nuevos módulos para necesidades futuras. Entre los módulos adicionales, podemos destacar la posibilidad de disgregar tráfico en función del protocolo, utilizando para esto NBAR dado que los *routers* del *backbone* de la RAAP son marca Cisco y cuentan con esta capacidad. También se da la posibilidad de realizar modificaciones de manera remota en la configuración en los equipos ya sea por medio de Telnet o SSH, entendiendo por equipos tanto *routers*, como servidores o cualquier otro dispositivo configurable por estos medios.

Se eligió una interfaz basada en Web, pues permite el acceso a la información de manera remota, el servidor desde donde se corre el sistema debe contar con dos interfaces, de forma que la información pueda ser vista desde una computadora con conexión exclusiva a la RAAP como desde cualquier computadora conectada al Internet convencional. Esta interfaz debe proveer maneras de visualizar el estado general de la red, las mediciones de tráfico y observar el tráfico y estadísticas en cada dispositivo.

4.2. Herramientas utilizadas

Las herramientas utilizadas para la implementación son:

- Sistema operativo GNU/Linux Ubuntu Server Dapper Drake 6.06.1 LTS

El Linux provee un sistema operativo estable sin ningún tipo de costos por licencias. En particular este sistema operativo está basado en Debian que cuenta con software moderno y una comunidad de desarrolladores muy activa, además cuenta con la opción de tener soporte comercial.

La versión elegida tiene la particularidad adicional de que es denominada LTS(Long Term Support) puesto que va a proveer un tiempo de soporte de 5 años en la versión de servidores, con lo cual se garantiza que posibles errores o fallas de seguridad serán corregidas por todo este periodo.

- Apache 2.0.55

Este es un servidor de HTTP para múltiples plataformas, que actualmente es el servidor más usado en Internet, según Netcratf, es utilizado por más del 60% de los sitios Web [WWW19]. Se utilizó la versión 2 pues presenta algunas mejoras, incluyendo el soporte para IPv6. [MALD2005] [WWW13]

- PHP 5.1.6

Es un lenguaje libre, multiplataforma, principalmente utilizado para la programación de *scripting* en el servidor. En este caso fue usado como módulo del Apache 2 para la compilación en tiempo real de páginas Web dinámicas. La versión 5.1.6 es la versión disponible en los repositorios del sistema operativo elegido y funciona sin problemas con el resto de programas seleccionados, además según sus creadores esta versión cuenta con mejoras de performance [WWW22].

- Java

Utilizado para soportar applets independientemente del sistema operativo que seste usando. Es un requisito de la máquina donde se ejecuta el applet solo en caso se desee utilizar el módulo de configuración remota. El sistema ha sido probado con las versiones 1.4, 1.5 y 1.6 corriendo en Windows y Linux.

- Perl5

Usado para el desarrollo de *scripts*, en este caso fue usado principalmente para la conexión con *routers* para la obtención de información.

- GIMP 2.2.13

El GIMP (GNU Image Manipulation Program) es un programa libre para creación y edición de imágenes, fue creado como una alternativa libre al photoshop. Dentro del desarrollo fue utilizado para la creación y edición de gráficos a ser utilizados en el sistema, como por ejemplo los logos, botones, etcétera.

- Cacti 0.8.6h:

Se utilizó Cacti 0.8.6h ya que era la ultima versión estable al momento de la implementación, la versión 0.9 se encontraba en beta al momento de la redacción de esta tesis, pero es recomendable utilizar esta versión pues ya ha pasado gran tiempo en prueba y utilización en distintos tipos de entornos.

- Plugin Architecture 0.9:

Para extender las funcionalidades del Cacti se utilizó este *framework* haciendo más uniforme y sencilla la instalación de distintos módulos al Cacti, además utilizándolo se tiene una referencia para los módulos a crear dentro del sistema y hace posible que estos sean independientes de la instalación del *core*, además permite prescindir de algunos de ellos sin afectar el resto del sistema.

- PHP Network Weathermap 0.82

Es una utilidad para crear y visualizar mapas de redes, dentro de estos se puede observar la utilización de los enlaces, vinculándolos a datos de RRDs, de forma que la información se actualice automáticamente.

- Thold 0.3

Plugin para definir límites en cada gráfico, de manera que, en caso alguno de estos sea sobrepasado, se pueda enviar una alerta por correo.

- Manage 0.4.2

Plugin para el Cacti que permite mostrar el estado actual de los dispositivos monitoreados en una pantalla. Además es posible observar el estado de los servicios dentro de cada uno de estos dispositivos.

En caso ocurra un error con un dispositivo o servicio se envía una alerta por correo electrónico.

- Discovery 0.6

Plugin para monitorear si es que dentro de determinadas subredes se encuentran nuevos equipos, además es posible ver si es que estos tienen SNMP habilitado, siempre y cuando conozcamos la comunidad.

- Syslog_ng

Sistema para gestionar *logs*, permitiendo su exportación y recepción de *logs* remotos.

- Haloe 0.4

Interfaz Web para revisar *logs* almacenados en una base de datos.

- Update 0.3

Plugin para revisar si existen actualizaciones de la arquitectura de plugins o de algún plugin.

- Telnet+SSH+Terminal 2.6

Applet en Java que permite estableces sesiones remotas de Telnet o SSH.

4.3. Implementación del NOC

Cacti fue elegido como base dado que provee capacidades de manejo gráfico de la información así como una base largamente probada, pues utiliza RRDtools. Por defecto incluye interfaces de autenticación y formas de

configurar permisos para acceso a sitios específicos según el usuario. Además provee la capacidad para adicionar nuevas plantillas y definir nuevos gráficos. Antes de instalar el Cacti, se debe contar con una base de datos (MySQL en este caso), un servidor Web (Apache) y el PHP.

Es recomendable realizar de manera independiente, la instalación y configuración de la base de datos, para definir la contraseña de root así como los permisos de conexión.

La instalación del Cacti se llevó a cabo utilizando el administrador de paquetes de Ubuntu, ya que tiene consideraciones adicionales de seguridad sobre el código disponible desde la Web de Cacti. Por ejemplo, la contraseña de la base de datos se encuentra en un archivo separado con permisos de solo lectura, mientras que en la versión estándar está incluida en el archivo de configuración general. Adicionalmente incluye los nuevos parches para el Cacti.

Habilitando y configurando el SNMP en los equipos a monitorear se pudo probar las primeras gráficas, luego de definir el tipo de dispositivo en el Cacti y crear los gráficos deseados.

Sobre el Cacti se ha desarrollado una plataforma para adicionar *plugins*, si bien esta aún no forma parte de la versión oficial, se espera que en la próxima versión lo haga, además ya existe una gran variedad de *plugins* escritos.

Esta plataforma determina una forma estándar para escribir nuevas interfaces e incorporarlas al sistema, manteniendo la independencia del módulo, de manera que todos los archivos de este se encuentren separados y la parte central del sistema no tenga que ser modificada, además los módulos pueden ser activados y desactivados sin afectar al resto del sistema.

La instalación de esta plataforma puede darse de dos maneras, sobrescribiendo los archivos o aplicando parches. Dado que los archivos usados son algo diferentes a los originales, se optó por aplicar el parche, el cual falla en el fichero que guarda la contraseña de la base de datos, por lo que luego de hacer una comparación se hizo un parche manual para ese archivo en particular.

Una vez que la plataforma de *plugins* estuvo en funcionamiento, se procedió a la instalación, configuración y activación de *plugins*. En el caso del Thold se definió los límites y las opciones de de alerta. Para el Discovery, se configuró el intervalo de monitoreo y las subredes a monitorear.

Para obtener los mapas de la red es necesario instalar el PHP Weathermap y configurarlo, además de establecer los permisos necesarios a los archivos de configuración, la creación de los mapas se llevó a cabo con ayuda de un editor gráfico en fase de prueba y con la manipulación directa de los archivos de configuración de cada mapa. Además dentro de cada mapa se definieron vínculos específicos que permitan que estos interactúen entre ellos y con otras

partes de sistema, logrando así que, por ejemplo, haciendo clic en un *router* se pueda entrar a la consola de Telnet, o que un mapa pueda vincular a otro mapa para ver con mas detalle algunos enlaces, creado la sensación de haber realizado un acercamiento.

Para poder realizar la configuración remota de los dispositivos se utilizó el Telnet+SSH+Terminal, el cual es una aplicación escrita en Java que realiza una conexión con un dispositivo utilizando Telnet o SSH, esta aplicación fue primero integrada a una página Web como *applet* y luego fue convertida a un *plugin*, siguiendo los lineamientos de la arquitectura y manteniendo además un diseño uniforme. Es necesario notar que, por restricciones de seguridad, el programa no puede realizar conexiones remotas a una máquina que no sea el servidor Web, por ello fue necesario utilizar un Proxy para que redirija conexiones locales a los IPs de dispositivos en la red.

Para poder realizar el almacenamiento centralizado de *logs* se instaló y configuró el syslog_ng en el sistema gestor determinando aquellos *logs* que se almacenarán en la base de datos e indicándole que escuche un puerto para poder recibir *logs* remotos. Los equipos que enviarán sus *logs* deben ser configurados indicando la dirección a la que estos deben ser enviados.

Los *logs* serán mostrados en la interfaz Web y además se pueden configurar opciones de alerta, por ejemplo vía *mail*. Este mismo sistema puede ser utilizado para recibir *traps* y configurar alertas.

4.4. Esquema

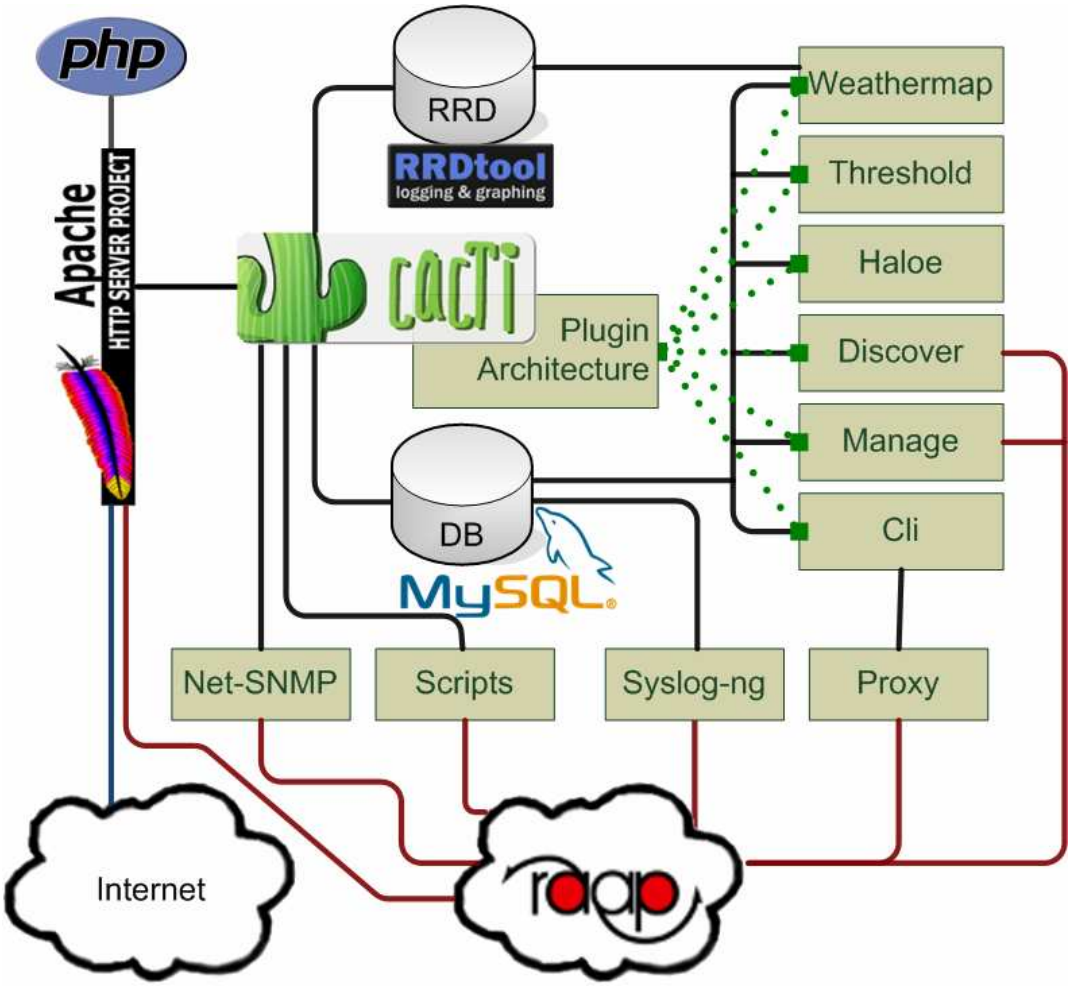

Figura 4.1 Esquema del sistema

La Figura 4.1 muestra un esquema general del sistema.

Un usuario puede acceder al sistema desde cualquier computadora conectada a Internet o a la RAAP, la comunicación se hace por http, utilizando como servidor al Apache, las páginas dinámicas son procesadas por el módulo de PHP.

El Cacti maneja la interacción del sistema en sí, empezando por la pantalla para autenticación y la autorización para el manejo de acceso a las diferentes interfaces. Internamente el Cacti se encarga del sondeo de los dispositivos, este se da utilizando Net-SNMP y además *scripts*, los resultados obtenidos del sondeo son almacenados en archivos de bases de datos cíclicas (RRA), manejadas con el RRDTools, el cual también se encarga de generar las gráficas.

Los parámetros de la configuración del Cacti y de la mayor parte del sistema son almacenados como entradas en una base de datos relacional, en este caso MySQL. La misma base de datos sirve para almacenar los *logs* del sistema, ya sea del servidor local, como los exportados de dispositivos y otros servidores.

Los *plugins* interactúan con el Cacti gracias al *plugin architecture*, que permite que se integren funcionalidades manteniendo cada módulo separado. El *weathermap* utilizado para la generación de mapas de red interactúa directamente con los datos de los RRAs, para la generación de las imágenes, y con el Cacti para que estas sean mostradas como parte del sistema. El Haloe, se encarga de mostrar vía Web los registros obtenidos vía el syslog_ng y almacenados en la base de datos. Los *plugins* Discover y Manage además interactúan con los dispositivos directamente, en el caso de Discover este realiza *pings* para determinar la existencia de nuevos dispositivos dentro de las subredes, además analiza si estos cuentan con SNMP habilitado, por otro lado el Manage revisa el estado de los dispositivos y de los servicios que corren en

ellos, para esto debe interactuar con la red puesto que revisa el estado de los puertos.

El CLI también debe interactuar con la red, ya que este *plugin* permite la configuración de los equipos, pero por restricciones de seguridad impuestas por el Java este *applet* no puede realizar conexiones directamente a otros dispositivos que no sean el servidor Web, es por esto que dentro del servidor se implementa una especie de *proxy* o *relay* que redirecciona las conexiones lo cual permite además que se realicen conexiones a dispositivos en la RAAP desde un equipo conectado a Internet.

4.5. Características del sistema

4.5.1. Monitoreo de IPv6

Es necesario distinguir el tráfico correspondiente a cada protocolo, de forma que se pueda observar activamente el proceso de migración y la utilización del nuevo protocolo.

Actualmente no existe una implementación de MIB de Cisco que permita hacer esta distinción, sin embargo dentro de la consola de configuración existen comandos que pueden proporcionar esta información, por ejemplo el *show interfaces accounting*, mostrado en la Figura 4.2.

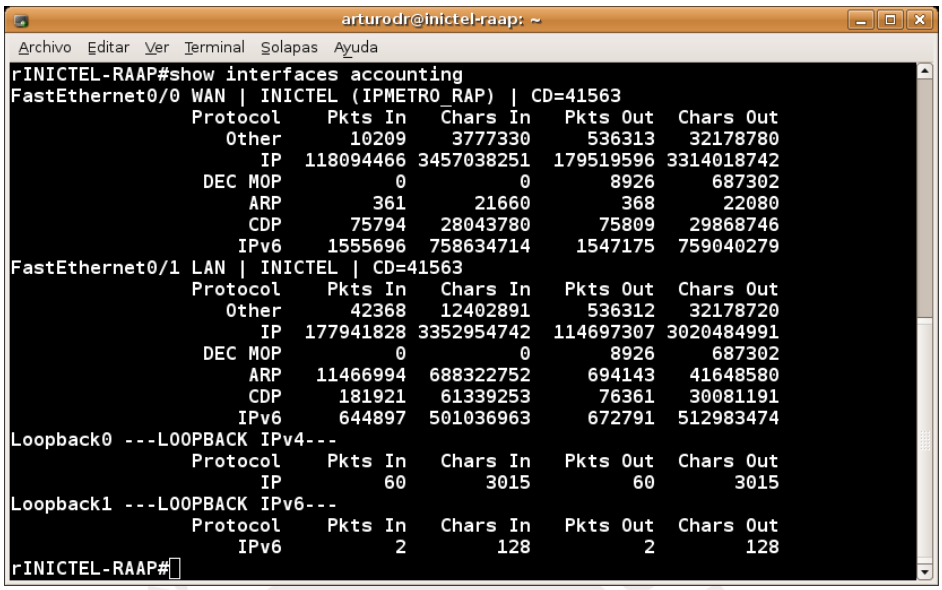

Figura 4.2 Comando show interfaces accouting en el router del Inictel

Por ello, se desarrolló un script en Perl, que se conecte a cada router, ejecute ese comando, interprete los resultados y devuelva los valores requeridos, de forma que teniendo estos datos, podamos calcular la tasa de transferencia en cada período de muestreo y con esto poder realizar gráficas dentro del sistema, como la que se muestra en la Figura 4.3.

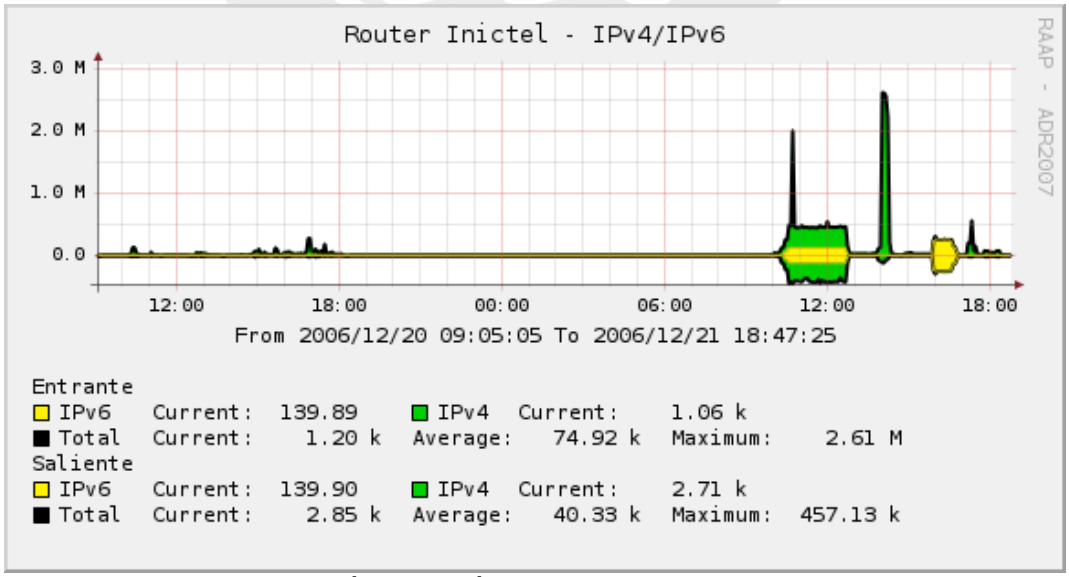

Figura 4.3 Gráfica del tráfico correspondiente a IPv4 e IPv6

4.5.2. Clasificación del tráfico por tipo de protocolo

Por la red pasan distintos tipos de gráficos, por lo que es conveniente clasificarlos y mostrar que tipo de tráfico está pasando por los enlaces. Para poder realizar esto se utilizó NBAR, protocolo mencionado en la sección 3.4.3, la configuración seguida en los routers es mostrada en el Anexo A. El sistema fue adaptado para que reconozca los distintos protocolos, y que los grafique tal como se muestra en la Figura 4.4.

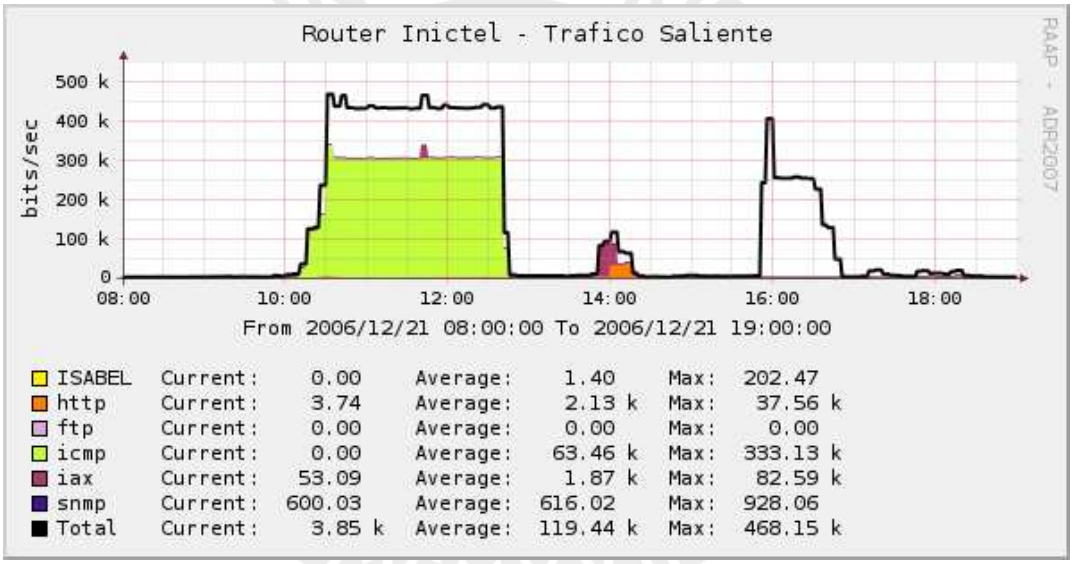

Figura 4.4 Muestra de diferentes protocolos utilizando NBAR.

4.5.3. Monitoreo de la plataforma de videoconferencias

La plataforma de videoconferencia Isabel constituye actualmente uno de los principales usos de la RAAP, y su utilización va en aumento para todo tipo de eventos, tanto a nivel local, como internacional. Por esto el monitoreo de la utilización de este programa es fundamental para la red, dentro del sistema desarrollado se consideran dos aspectos, el monitoreo del estado del servidor y el ancho de banda utilizado por la plataforma.

4.5.3.1. Monitoreo del estado del servidor

Se analizó la utilización de puertos de este servidor con ayuda del *nmap* y las conexiones con el *wireshark*. En base a eso se determinó que cuando este está en ejecución en modo de MCU, escucha las conexiones por el puerto 53020. Teniendo en cuenta esta información se configuró el sistema para que verifique el estado de ese puerto y que además lo asocie a la aplicación Isabel, tal como se muestra en la Figura 4.5.

Figura 4.5 Estado del servidor Isabel

4.5.3.2. Monitoreo de la utilización de la red

Se buscó determinar cuánto del tráfico en la red corresponde a este tipo de aplicación, para esto se configuró el NBAR de los *routers*, para que detecten el tráfico por el rango de puertos que utiliza Isabel, tanto de TCP como en UDP, de forma que lo catalogue como una aplicación particular. Por otro lado se configuró el sistema para que este tráfico sea asociado a la aplicación y pueda ser diferenciado en gráficos, como el que se muestra en la Figura 4.6.

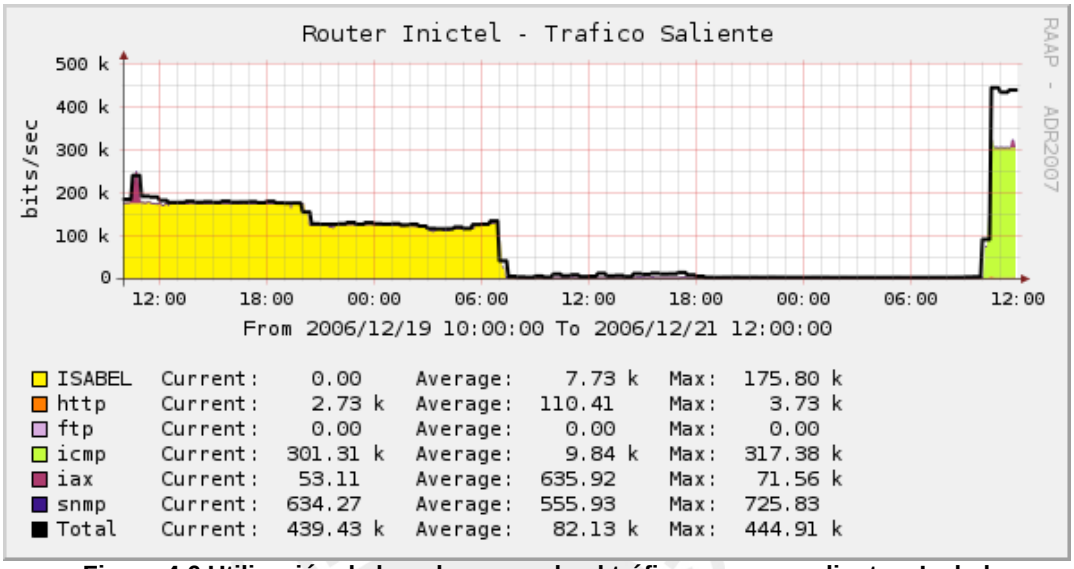

Figura 4.6 Utilización de la red separando el tráfico correspondiente a Isabel

4.5.4. Monitoreo del servidor de VoIP

Dado que dentro de la RAAP se está implementando un sistema de VoIP [QUI2007], que daría servicio a los sitios que conforman la red, se consideró necesario adaptar el sistema para obtener el estado del servidor y estadísticas del mismo.

Dentro del proyecto de implantación de este servidor, se eligió trabajar con Asterisk 1.0.11, esta versión no incluye ninguna forma directa para el monitoreo por SNMP, por lo que se decidió definir una MIB e implementar los *scripts* que permitan obtener estadísticas del funcionamiento del servidor. Los detalles de esta implementación se encuentran en el Anexo B.

Luego de realizar esta adaptación se logró el monitoreo del servidor Asterisk utilizando SNMP. Dentro de las estadísticas se consideró el número de clientes conectados y desconectados para los protocolos SIP e IAX, así como las

llamadas que se están realizando, con estos datos, se eleboraron las gráficas mostradas en las Figuras 4.7, 4.8 y 4.9.

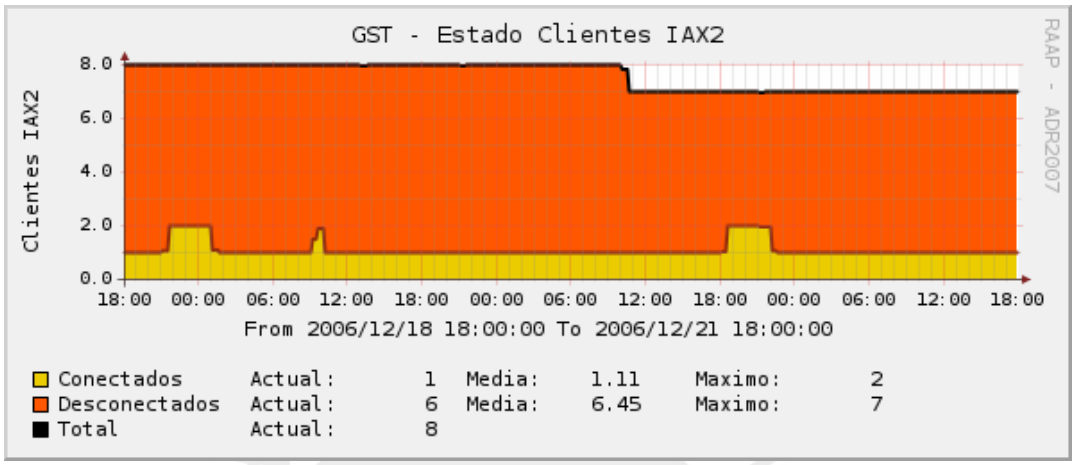

Figura 4.7 Estado de los clientes SIP

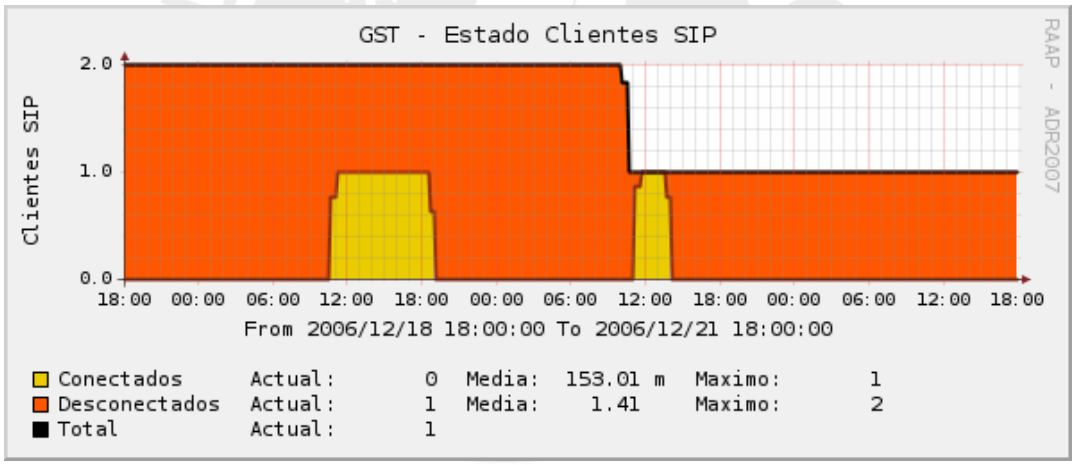

Figura 4.8 Estado de los clientes IAX

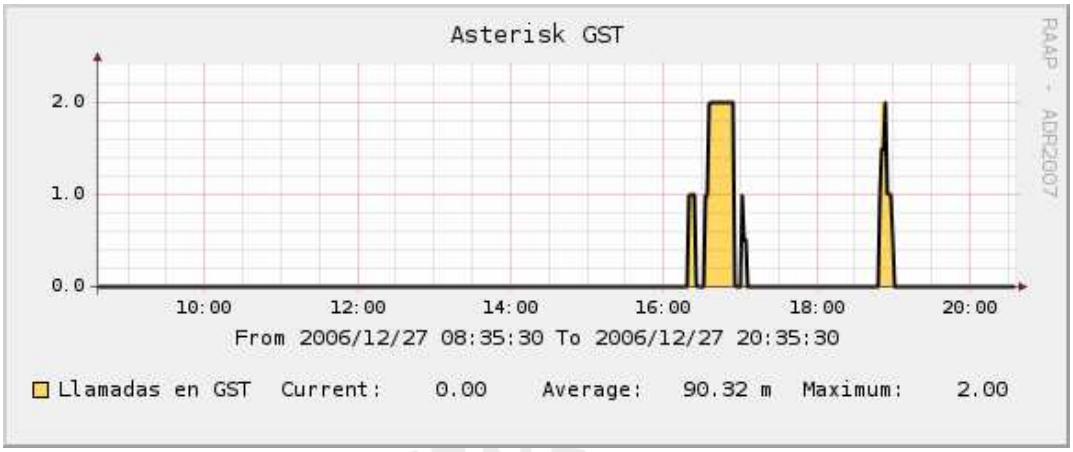

Figura 4.9 Llamadas realizadas usando el servidor

4.5.5. Customización de gráficos de red

Se configuraron gráficos de la RAAP, siguiendo la topología de la misma. Estos gráficos permiten observar el tráfico actual de todos los sitios en gráficos funcionales. La información de los enlaces corresponde a los últimos datos almacenados en las RRAs, además con ayuda de librerías en *javascript* se puede mostrar la información histórica al poner el puntero del mouse sobre el enlace, como se observa en la Figura 4.10.

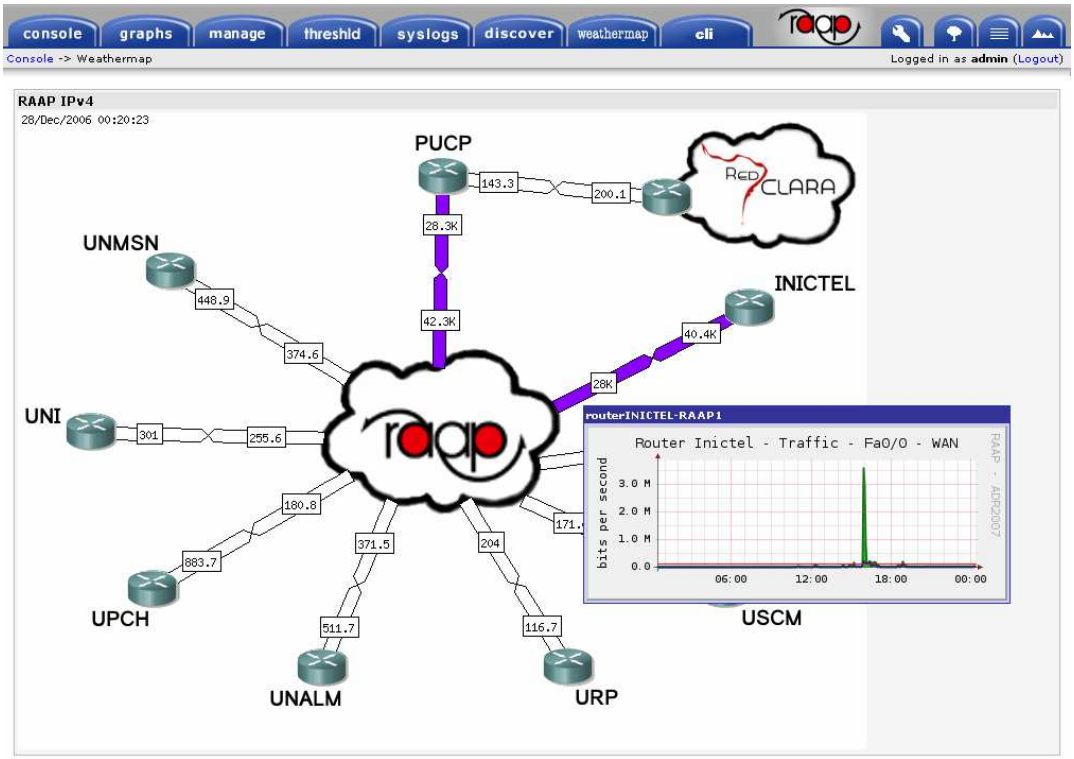

Figura 4.10 Mapa de la RAAP

Además se puede configurar el mapa para que al hacer clic sobre un nodo se muestre otro mapa o alguna otra funcionalidad, como la configuración por Telnet, para diferenciar que acción se llevaría a cabo, se utilizan mensajes de ayuda utilizando las mismas librerías de *javascript* mencionadas anteriormente, como se muestra en la Figura 4.11.

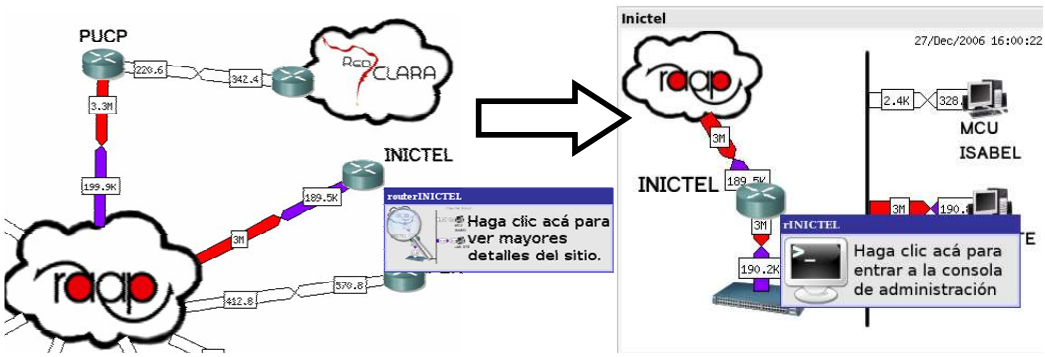

Figura 4.11 Facilidades de la interfaz de mapas de red

4.5.6. Exportación de *logs* de los equipos

Los *logs* de sistema pueden contener información importante para el administrador, sin embargo típicamente esta información se almacena de forma local en archivos de texto plano, lo cual hace tediosa su revisión, especialmente cuando la red está conformada por diversos dispositivos.

Buscando simplificar esta situación, se configuró un sistema que permite el almacenamiento centralizado de los logs en una base de datos (Figura 4.12), de forma que estos puedan ser manipulados más fácilmente, además se implementó un módulo, que hace posible la exploración de estos logs vía Web, permitiendo además filtrarlos según diversos criterios, tales como: dispositivo que los origina, prioridad, fecha, etcétera.

←T→	facility	priority	date	time	host	message	seq
☐ ✎ ✕	cron	info	2006-12-16	23:50:01	gst	/USR/SBIN/CRON[3664]: (root) CMD (/usr/share/cacti...	17
☐ ✎ ✕	ftp	info	2006-12-16	23:50:23	gst	pure-ftpd: (?@gst.telecom.pucp.edu.pe) [INFO] New ...	73
☐ ✎ ✕	mail	info	2006-12-16	23:50:23	gst	postfix/smtpd[3823]: connect from gst.telecom.pucp...	82
☐ ✎ ✕	mail	info	2006-12-16	23:50:23	gst	postfix/smtpd[3823]: lost connection after CONNECT...	84
☐ ✎ ✕	mail	info	2006-12-16	23:50:23	gst	postfix/smtpd[3823]: disconnect from gst.telecom.p...	85
☐ ✎ ✕	ftp	info	2006-12-16	23:50:23	gst	pure-ftpd: (?@gst.telecom.pucp.edu.pe) [INFO] Logo...	282
☐ ✎ ✕	cron	info	2006-12-16	23:55:01	gst	/USR/SBIN/CRON[4150]: (root) CMD (/usr/share/cacti...	474
☐ ✎ ✕	mail	warning	2006-12-24	21:06:05	gst	postfix/smtpd[27230]: warning: Illegal address syn...	4264
☐ ✎ ✕	ftp	info	2006-12-16	23:55:23	gst	pure-ftpd: (?@gst.telecom.pucp.edu.pe) [INFO] New ...	525

Figura 4.12 Vista de los logs almacenado en una base de datos

4.5.7. Backup del sistema

Dado que dentro del sistema se guardan estadísticas de toda la red y por todas las modificaciones y añadiduras hechas al código original de los programas, así como los *scripts*, es necesario contar con un respaldo, de manera que en caso de falla los datos se puedan recuperar y pueda continuar el funcionamiento del sistema. La información a resguardar se divide en archivos en los directorios correspondientes a los programas, *scripts*, registros en la base de datos MySQL y los resultados de los sondeos guardados en RRAs. Se realizó un *script* que realice el *dump* de las tablas de la base de datos que contiene la configuración del sistema, y que reúne los archivos necesarios, los comprime y almacena en el disco duro con la fecha de realización del *backup*. Se programó la ejecución automática de este *script* una vez al día. Además, para mayor seguridad el archivo generado es exportado por FTP a otro servidor.

Cada archivo ocupa alrededor de 3MB, por lo que para evitar que el espacio se consuma innecesariamente, se eliminan los registros antiguos.

4.6. Interfaces

Como se mencionó en la sección anterior la interfaz del sistema es Web, por lo que puede ser accedida utilizando cualquier navegador gráfico[6] en cualquier

[6] Ha sido probado en Firefox 1.5 y 2.0, Internet Explorer 6.0 y 7.0

sistema operativo[7]. Las figuras mostradas fueron tomadas de un Firefox 2.0 corriendo sobre un sistema operativo GNU/Linux Kubuntu 6.10.

La primera pantalla es la de autenticación y autorización de usuario (Figura 4.13). La identidad del usuario se verifica por la contraseña asignada, además las secciones del sistema a las que se tendrá acceso dependen del usuario que ingrese y sus permisos previamente definidos.

Figura 4.13 Pantalla de autenticación y autorización

Una vez que se a accedido al sistema lo siguiente es la pantalla de bienvenida, dentro de esta se puede observar la cantidad de errores actuales detectados. En la Figura 4.14 se muestra la pantalla cuando no hay ningún error, además se proveen vínculos a las distintas secciones del sistema, con una pequeña explicación.

[7] Para las pruebas se ha utilizado principalmente GNU/Linux Kubuntu 6.10 y Microsoft Windows XP SP2, pero también se ha probado el funcionamiento en otras versiones de Linux, y Windows.

Figura 4.14 Pantalla de bienvenida

La Figura 4.15 muestra la interfaz de gráficos, esta posee tres formas de visualización:

- Vista del árbol.
- Lista, para seleccionar gráficos específicos.
- Página donde se muestran los gráficos seleccionados en la lista.

En la figura 4.14 también se muestra la pantalla del árbol, dentro del sistema se ha definido el árbol RAAP, que contiene los equipos monitoreados agrupados en función de la entidad donde se encuentran.

Dentro de esta interfaz se pueden apreciar los gráficos de tráficos de IPv4, IPv6, la separación de tráfico según en protocolo y todos los gráficos mencionados en la sección anterior.

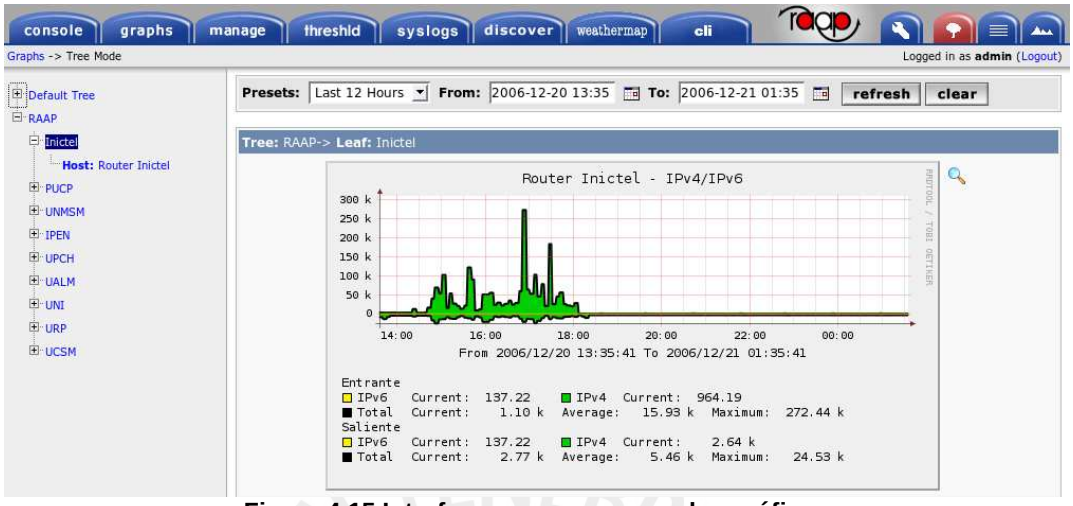

Figura 4.15 Interfaz para navegar por los gráficos

Dentro de la vista de los gráficos se puede configurar la forma en la que se mostrarán los gráficos (Figura 4.16), esta opción se encuentra en la pestaña *settings*, representada por una llave de tuercas. Cada usuario tiene la capacidad de establecer sus preferencias.

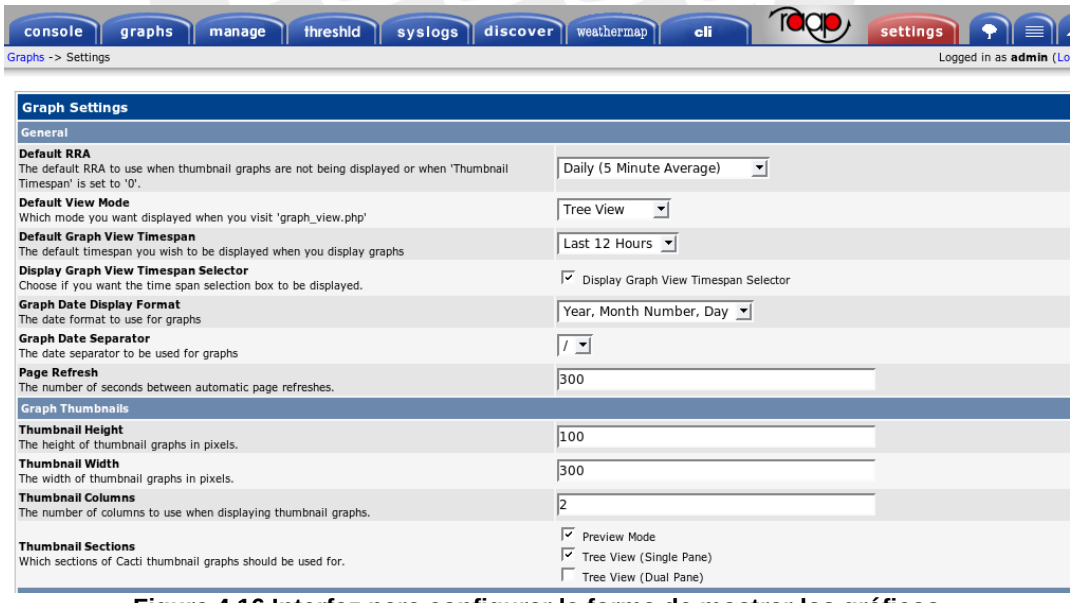

Figura 4.16 Interfaz para configurar la forma de mostrar los gráficos

La interfaz Manage, permite observar el estado de los dispositivos que conforman la red, y de los servicios que corren en estos (Figura 4.17),

mostrando alertas cuando ocurre algún error, además estas alertas son enviadas por correo electrónico.

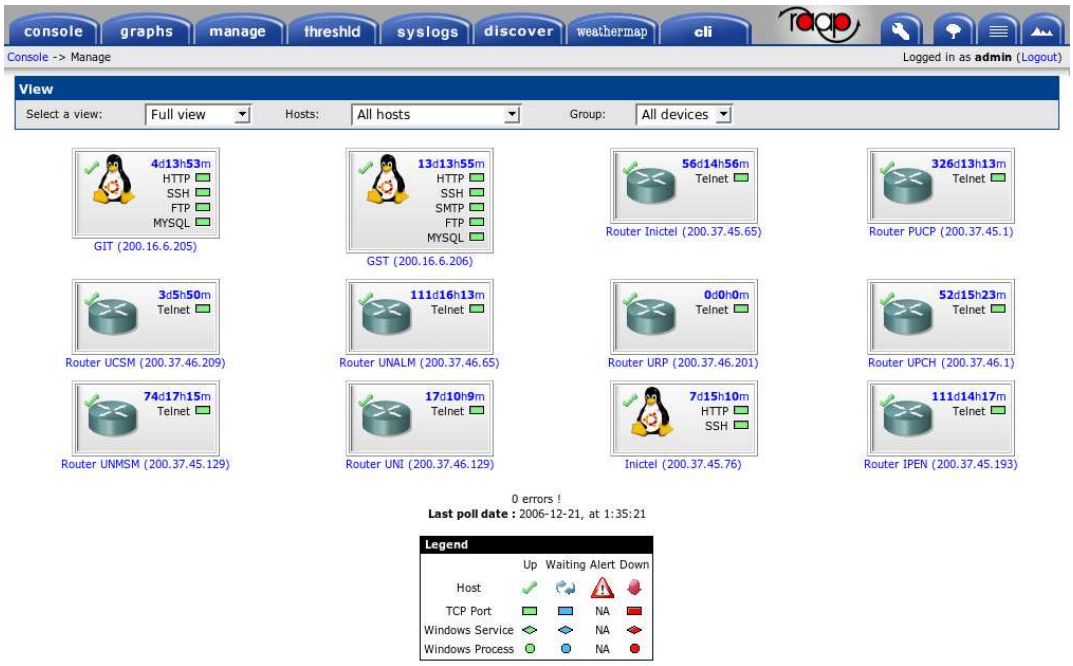

Figura 4.17 Interfaz para mostrar el estado de los dispositivos

En envío por correo electrónico permite que, a través del uso de programas adicionales, como el GTalk en Windows (Figura 4.18), se obtengan alertas de forma prácticamente automática, sin necesidad de observar la interfaz, en Linux las posibilidades son aún mayores.

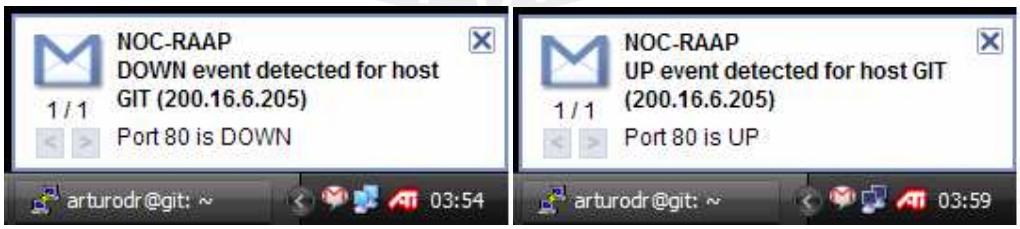

Figura 4.18 Ejemplo de alertas

La interfaz *threshold*, permite establecer límites, para cualquier parte del sistema que esté siendo monitoreada. En caso cualquier límite sea sobrepasado se generará una alerta que, al igual que en el caso anterior, será

enviada por correo electrónico. Esto permite establecer un monitoreo más preciso, ya que pueden existir problemas que no implican la caída de un enlace o servicio, por ejemplo un disco duro en un servidor está lleno, el CPU de un *router* está sobrecargado, la central está recibiendo muchas llamadas, etcétera.

Cada alerta es configurable, pudiéndose definir límites superiores, inferiores, límites que toman en cuenta valores anteriores o valores absolutos, alertas solo si la condición se mantiene un tiempo determinado, así como la posibilidad de comunicar la situación a una persona diferente para cada tipo de alerta. La interfaz en la que se observa si algún límite ha sido sobrepasado es mostrada en la Figura 4.19.

Figura 4.19 Revisión del estado de los límites definidos

La sección *syslog*, permite el análisis de registros del sistema, así como de registros de sistemas remotos, clasificando cada registro según su nivel de

prioridad y permitiendo diferentes criterios para filtrarlos (Figura 4.20). Permite además que cierto tipo de alertas sean enviadas por correo electrónico.

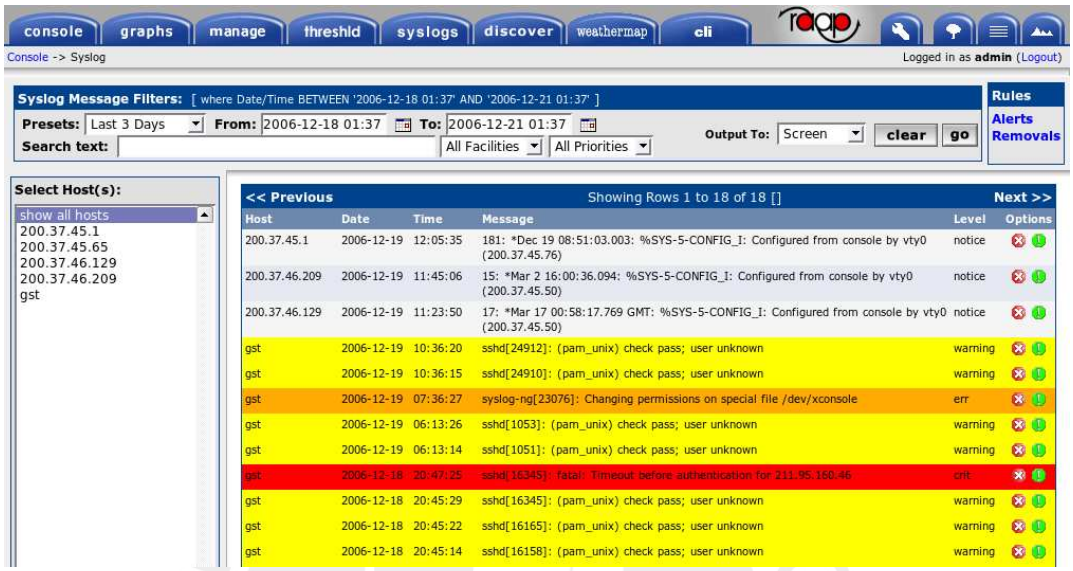

Figura 4.20 Interfaz para revisar los logs de los dispositivos

La interfaz *discover* permite observar que equipos se encuentran en la red, permitiendo que en caso no formen parte de los dispositivos actualmente monitoreados estos puedan ser agregados al registro (Figura 4.21).

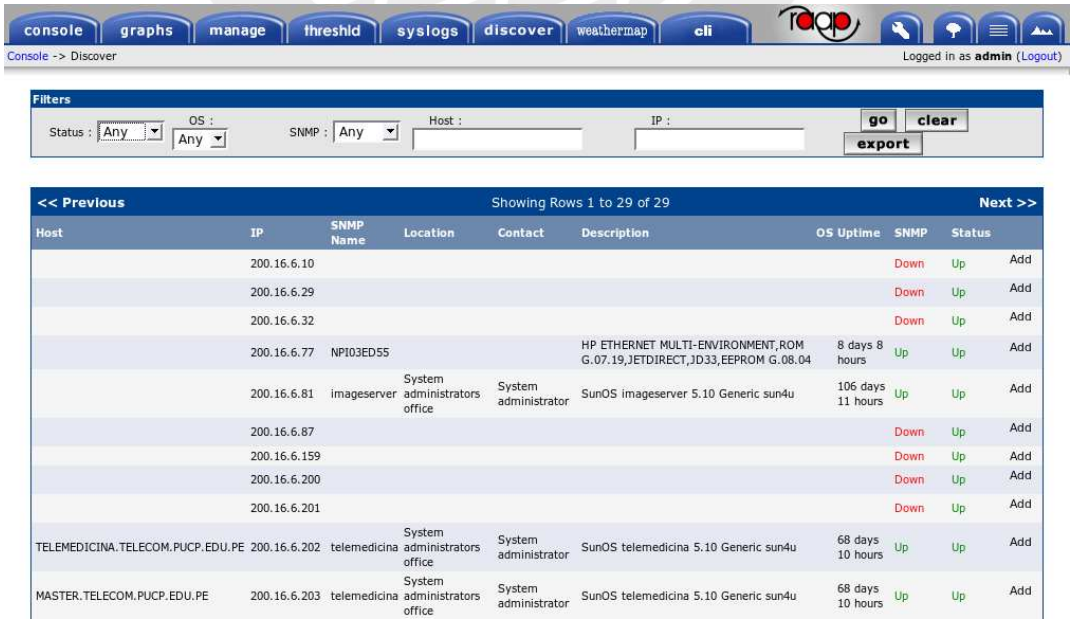

Figura 4.21 Interfaz para el descubrimiento de equipos

La interfaz weathermap hace posible que se vea de forma gráfica el estado de los enlaces de la red, posicionando el puntero sobre algún enlace se mostrarán las estadísticas de ese enlace para las últimas 24 horas (Figura 4.22), además si se hace clic sobre el enlace, se mostrarán estadísticas del día, semana, mes y año.

Por otro lado, haciendo clic sobre el *router* del sitio, se accede a un mapa mas detallado, o si es que estamos en la pantalla con mayor detalle para este dispositivo, se puede entrar a la consola para su configuración.

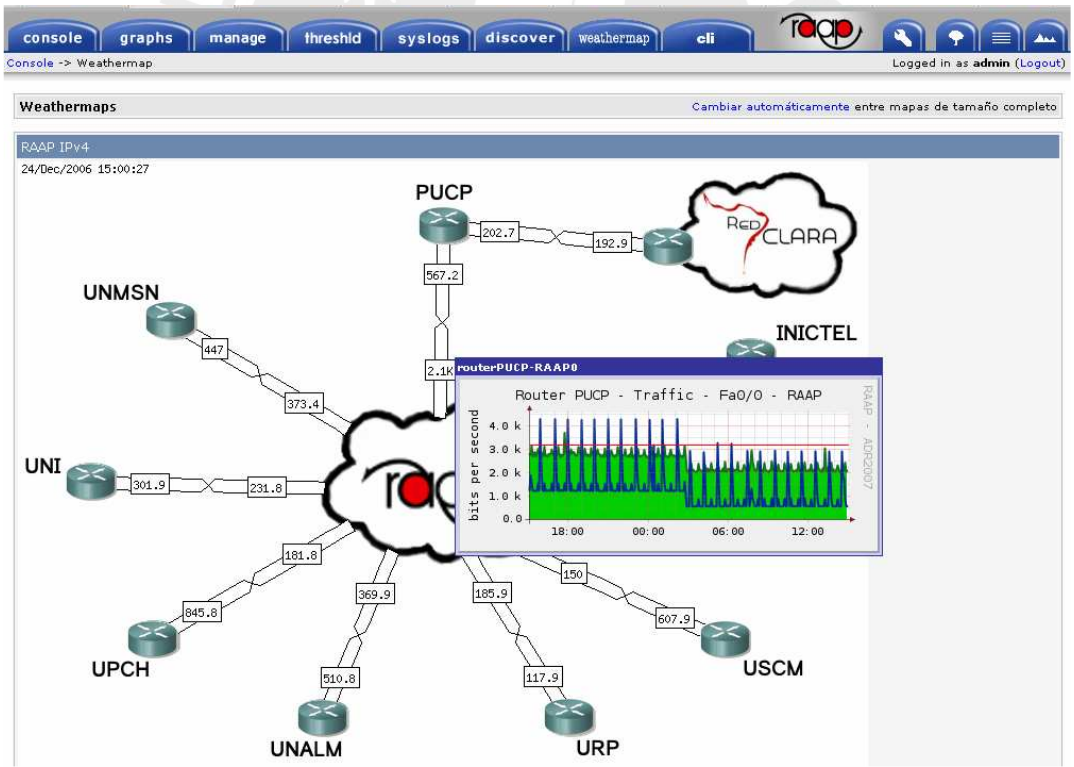

Figura 4.22 Interfaz para ver los mapas de red

La última interfaz es la de configuración de dispositivos, mostrada en la Figura 4.23. Esta interfaz un *applet* en Java que permite entrar a la consola del

dispositivo, ya sea para modificar alguna configuración, ver alguna estadística específica o tomar alguna decisión de gestión, por ejemplo modificar los anchos de banda para algunos parámetros de QoS.

El proporcionar una interfaz para la modificación de la configuración de los equipos implica que esta solo debe ser accesible a personas autorizadas, en ese sentido se han tomado precauciones de seguridad, para que se acceda a esta interfaz, el usuario debe estar autenticado en el sistema, además el administrador debe haberle concedido permisos específicos y la persona debe poseer los *passwords* del equipo en sí.

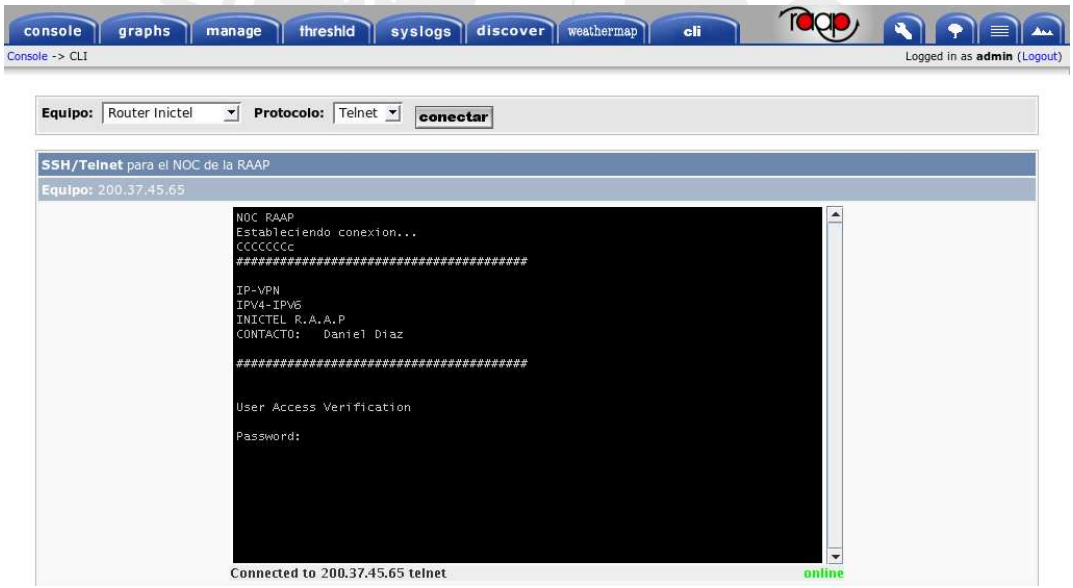

Figura 4.23 Interfaz para la configuración de equipos

4.7. Utilización del sistema

El sistema se encuentra en prueba desde comienzos de septiembre del 2006, implementado en un servidor de la Pontificia Universidad Católica del Perú (PUCP). Su aplicación directa es el monitoreo del estado de equipos que

conforman la RAAP, pero al ser modular y adaptable, es posible aplicarlo al monitoreo de cualquier red o servicios dentro de una institución o empresa.

Además puede ser adaptado como plataforma de apoyo a la educación de temas relacionados a redes y gestión, como ejemplo de esto se realizó una prueba durante un laboratorio del curso de Redes de Banda Ancha correspondiente a la especialidad de Ingeniería de las Telecomunicaciones de la PUCP. Asimismo podría ser utilizado como apoyo a la educación a distancia de cursos similares. Finalmente el sistema puede servir de apoyo a investigaciones de tecnologías relacionadas a las redes, como ingeniería de tráfico, análisis de protocolos, comparación de *codecs*, etcétera.

Capítulo 5: Conclusiones y Recomendaciones

5.1. Conclusiones

- Se analizaron las características de la RAAP, y en función a ellas, se diseñó e implementó un sistema para su monitoreo y gestión.
- El sistema permite obtener y almacenar estadísticas del rendimiento de la red, observando sus características actuales y su evolución histórica.
- El sistema hace posible monitorear el estado de los equipos y los servicios que corren en ellos, generando una alarma en caso ocurra un error.
- El sistema permite realizar cambios en los equipos, para efectuar alguna modificación en la configuración o corregir un estado erróneo.
- El sistema ha sido implementado utilizando software libre, esto proporciona ahorros en licencias y además la posibilidad de modificar el código para adaptar los programas a necesidades específicas.

- El sistema es modular, lo cual hace posible que sea adaptado conforme las necesidades de la RAAP evolucionen. Además puede ser adecuado al monitoreo de diversos escenarios e incluso a aplicaciones del tipo educativo.

5.2. Recomendaciones

El sistema es bastante completo para las necesidades actuales y las que puedan emerger a corto plazo, sin embargo se le pueden incluir nuevas características, como trabajos a futuro, entre estas se puede destacar:

- Análisis de flujos tomados de NetFlow. Esto permitiría un mejor estudio de la utilización de la red, pudiendo observar mejor como se distribuye el tráfico entre los dispositivos, esto será más relevante conforme se encuentren más terminales conectados a la red.
- Generación de reportes mensuales automáticos de estadísticas de utilización.
- Generación de alertas vía mensajes de texto a un celular. Con este sistema en caso ocurra un error, la persona indicada podría ser alertada de una forma más rápida lo cual contribuiría a que los tiempos de reparación se reduzcan, aumentando la disponibilidad del sistema.
- Despliege de un esquema de redundancia para el gestor. De esta forma se evitaría la perdida de algún dato en caso de falla.

Estas características no son fundamentales, pero permitirían una mejor respuesta, así como una plataforma más adecuada conforme la RAAP crezca y el tráfico dentro de ella aumente.

Además se recomienda estudiar otros esquemas de gestión de redes y la compatibilidad que podrían tener con el esquema actual.

REFERENCIAS

[BEI] Berry I., *"Cacti manual"*, www.cacti.net/downloads/docs/pdf/manual/pdf

[BOA] Bogaerdt A., "RRDtool tutorial", oss.oetiker.ch/rrdtool/tut/rrdtutorial.en.html

[BOL81] Bolt, Beranek y Newman, "ARPANET COMPLETION REPORT", 1981

[BUC] Burgess C., 2006, *"The Nagios Book"*, *Prerelease05012006*, www.nagiosbook.org

[CAL] Carter L., "Installation HOW-TO for Linux", www.cacti.net/downloads/docs/contrib/Cacti-Linux-How-To.pdf

[CIA2006] CIA "The World Factbook", 2006, https://www.cia.gov/cia/publications/factbook/

[CHA2003] Chalmers A., "Using open-source and inexpensive tools to cut management costs", ServerWorld, Abril del 2003 página 12.

[DOM2001] Dodge, M., Kitchin, R., "Atlas of Cyberspace", Addison Wesley, Agosto del 2001.

[DUD2006] Dubie D., "Open source management arrives", Network World, Mayo del 2006, página 8

[FEJ2005] Feldman J., "Get a Jump on Network Management", Network Computing, Octubre del 2005 páginas 67, 68 y 69.

[IBM2006] IBM, Tivoli Monitoring Datasheet, ftp://ftp.software.ibm.com/software/tivoli/datasheets/ITM-61-datasheet-final-Aug706.pdf

[MALD2005] Malone D, Murphy N, “IPv6 Network Administration”, O’Reilly, Estados Unidos, 2005, 306 páginas.

[MAUD2005] Mauro D, Schmidt K, “Essential SNMP”, 2nd Edition O’Reilly, Estados Unidos, 2005, 460 páginas.

[MOD2003] Molta, D., “Monitoring and Managing IP Networks”, http://web.syr.edu/~djmolta/ist452/ch_11.ppt

[MOS2003] Morris S, “Network Management, MIBs and MPLS: Principles, Desing and Implementation”, Addison Wesley, Estados Unidos, 2003, 416 páginas.

[OET2006a] Oetiker T., “MRTG Documentation” http://oss.oetiker.ch/mrtg/doc/index.en.html

[OET2006b] Oetiker T., “RRDtool Documentation”, http://oss.oetiker.ch/rrdtool/doc/index.en.html

[OET2006c] Oetiker T., Niko Tyni, “Smoke Ping Documentation”, http://oss.oetiker.ch/smokeping/doc/index.en.html

[QUI2007] Quintana D. Tesis de grado: “Diseño e implementación de una red de telefonía IP con software libre en la RAAP.”, Perú, 2007.

[RAAP2003] Estatutos de la Red Académica Peruana, marzo del 2003.

[RFC1157] Case J., Fedor M., *et al*, SNMP, 1990. http://tools.ietf.org/html/rfc1157

[RFC2021] Waldbusser S., Remote Network Monitoring Management Information Base Version 2 using SMIv2, 1997. http://tools.ietf.org/html/rfc2021

[RFC3031] Rosen E., Viswanathan A., Callon R., MPLS, 2001. http://tools.ietf.org/html/rfc3031

[ROB2005] Benedito R., Tesis de grado: "Gerência e Monitoramento de redes de computadores com o software livre Nagios", Belém, 2005.

[SAY1996] Sayman T., Magedanz T., "From Networks and Network Management into Services and Services Management", Journal of Networks and System Management, Vol4 No 4, 1996.

[SOL2006] SolarWinds, Orion datasheet, http://www.solarwinds.net/PDF/OrionNPM.pdf

[SWR] Sweeney R., "Monitoring your enterprise PACS with Nagios, Cacti and Smokeping". http://people.ee.ethz.ch/~oetiker/webtools/smokeping/pub/contrib/EnterprisePACSMonitoringwithNagiosSmokepingandCacti.pdf

[TAB2005] Taurus, B., "Enterprise-Wide Network Management with OpenNMS," O'Relly Network, 9 de agosto del 2005. http://www.oreillynet.com/pub/a/sysadmin/2005/09/08/openn ms.html

[TAM2004] Tatipamula M., Grossetete P., ESACI H.," IPv6 Integration and Coexistence Strategies for Next-Generation Networks", IEEE Communications Magazine, enero del 2004

[WAL2000] Walker, B. "The art of Production Environment Engineering" Sun BluePrints Online, junio del 2000. http://www.sun.com/blueprints/0600/prodeng.pdf

[WEH2006] Holger Weiss, 2006, "Official Nagios Documentation", http://nagios.sourceforge.net/download/contrib/documentation/english/Nagios_2_0_Docs.pdf

[ZIT2004] Zitello T., Williams D., Weber P., "HP OpenView System Administration Handbook: Network Node Manager, Customer Views, Service Information Portal, HP OpenView Operations", Prentice Hall PTR, Agosto del 2004.

Referencias a páginas Web

[WWW1] "About Abilene" http://abilene.internet2.edu/about

[WWW2] "GÉANT Home" http://www.geant.net

[WWW3] APAN http://www.apan.net/

[WWW4] CLARA www.redclara.net/01.htm

[WWW5] "GÉANT topology" http://www.geant2.net/upload/pdf/665_GN2_Topology_May_065_final.pdf

[WWW6] Mapa de la Topología de RedCLARA http://www.redclara.net/03/04.htm

[WWW7] RAAP http://www.raap.org.pe

[WWW8] "La Red Académica Peruana (RAAP)" Editorial del IPv6 Task Force Perú http://www.pe.ipv6tf.org/editorial/20051019

[WWW9] Quemada J., "Isabel Plaza" noticia sobre el evento "Cruzando el Atlántico con la Nueva Internet" http://isabel.dit.upm.es/index.php?option=com_content&task=view&id=34&Itemid=2

[WWW10] HP, Gestión de los Sistemas de Información, http://h20219.www2.hp.com/PublicSector/cache/107561-0-0-140-470.html

[WWW11] Tivoli Monitoring, http://www-306.ibm.com/software/info/ecatalog/es_ES/products/U106183E34344S82.html

[WWW12] Cacti Forums, http://forums.cacti.net/

[WWW13] Overview of new features in Apache 2.0, http://httpd.apache.org/docs/2.2/new_features_2_0.html

[WWW14] Artículo en Wikipedia: ARPA http://en.wikipedia.org/wiki/Advanced_Research_Projects_Agency_Network

[WWW15] Cisco, Network-Based Application Recognition and Distributed Network-Based Application Recognition http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hqos_c/part05/ch05/hdtnbara.pdf

[WWW16] "Official Nagios website", http://nagios.org/

[WWW17] Cisco, “Enterprise QoS Solution Reference Network Design Guide”. http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a008049b062.pdf

[WWW18] OpenNMS demo, http://demo.opennms.com:8080/opennms

[WWW19] Netcraft September 2006 Web Server Survey, http://news.netcraft.com/archives/2006/09/05/september_2006_web_server_survey.html

[WWW20] Cisco, “Using Network-Based Application Recognition and ACLs for Blocking the "Code Red" Worm” http://www.cisco.com/warp/public/63/nbar_acl_codered.pdf

[WWW21] HP, “HP OpenView Network Node Manager Advanced Edition 7.51 software Data sheet” http://h20229.www2.hp.com/products/nnm/ds/nnm_ae_ds.pdf

[WWW22] PHP, “Migrating from PHP 4 to PHP 5”, http://www.php.net/manual/en/migration5.php

[WWW23] FururеSoft Whitepaper: “FCAPS”, http://www.futsoft.com/pdf/fcapswp.pdf

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DEL CENTRO DE OPERACIÓN Y GESTIÓN DE LA RED ACADÉMICA PERUANA EN SOFTWARE LIBRE

TESIS PARA OPTAR EL TÍTULO DE

INGENIERO DE LAS TELECOMUNICACIONES

PRESENTADO POR

Arturo Díaz Rosemberg

LIMA – PERÚ

2007

Anexo A: Configuración de los routers

En este anexo se tratará la configuración realizada en cada router del backbone de la RAAP y el método seguido para simplificar esta configuración.

A.1 Configuración realizada

Los routers ya cuentan con una configuración en lo concerniente a la conectividad y passwords de acceso vía Telnet. La configuración que se muestra a continuación corresponde a lo necesario para que los routers interactúen correctamente con el NMS.

A.1.1 SNMP

Para poder acceder a la información de los routers se está utilizando el protocolo SNMPv1, para agregar seguridad al sistema el IP del NMS ha sido añadido a un access-list, de forma que solo este host pueda efectuar consultas,

además la comunidad creada es de solo lectura. Los comandos se muestran en la tabla A-1.

Tabla A-1 Configuración del servidor SNMP y la lista de acceso

```
rINICTELRAAP(config)#access-list 50 permit 200.37.45.50
rINICTELRAAP(config)#snmp-server community public RO 50
rINICTELRAAP(config)#snmp-server enable informs
```

Para la configuración de los traps se indica el IP del NMS y que tipo de traps recibe, luego se configura el router para que genere esos traps. La configuración hecha es la mostrada en la tabla A-2.

Tabla A-2 Configuración de las traps

```
rINICTEL-RAAP(config)#snmp-server host 200.37.45.50 traps 1 config tty
syslog
rINICTEL-RAAP(config)#snmp-server enable traps config
rINICTEL-RAAP(config)#snmp-server enable traps tty
rINICTEL-RAAP(config)#snmp-server enable traps syslog
```

A.1.2 NBAR

El NBAR hace posible acceder a datos de que tipo de tráfico está pasando por las interfaces y a que tasa de bits. En necesario habilitar el NBAR en cada interfaz del router, tal como se muestra en la tabla A-3.

Tabla A-3 Configuración del NBAR

```
rINICTEL-RAAP(config)#interface FastEthernet0/0
rINICTEL-RAAP(config-if)#ip nbar protocol-discovery

rINICTEL-RAAP(config)#interface FastEthernet0/1
rINICTEL-RAAP(config-if)#ip nbar protocol-discovery
```

En NBAR reconoce flujos de aplicaciones como HTTP, FTP, SNMP, entre otras, sin embargo puede ser configurado para que reconozca otros flujos, en este caso, es de especial interés reconocer el flujo del protocolo IAX, utilizado

en las troncales de VoIP así como el de la plataforma de video conferencias Isabel.

Para el caso del protocolo IAX todo el tráfico viaja por un mismo puerto UDP, la versión uno utiliza el puerto 5036 y la segunda y última versión utiliza el puerto 4569, los comandos entrados son los mostrados en la tabla A-4.

Tabla A-4 Configuración de reconocimiento de IAX con NBAR

```
rINICTEL-RAAP(config)#ip nbar port-map custom-02 udp 5036 4569
```

Para la plataforma Isabel se utilice un rango de Puerto TCP y UDP, para manejar la sesión y para el envío de los datos en sí. Los comandos necesarios se muestran en la tabla A-5.

Tabla A-5 Configuración para el reconocimiento del tráfico de la plataforma Isabel con NBAR

```
rINICTEL-RAAP(config)#ip nbar port-map custom-01 udp 53020 53021 53022
53023 53024 53025 53026 53027 53028 53029 53030 53031 53032
rINICTEL-RAAP(config)#ip nbar port-map custom-01 tcp 53009 53010 53011
53012 53013 53014 53015 53016 53017 53018 53019 53020 53021 53022
53023
```

A.1.3 Administración remota de logs

En el NMS se ha configurado una base de datos que tendrá los *logs* de los equipos y que generará alertas en caso ocurra un error. Para que el sistema funcione todos los equipos deben enviar sus *logs* a este servidor. En cada router se debe configurar la interfaz que originará los *logs*, y el IP del servidor al que será enviado. La configuración seguida es la mostrada en la Tabla A-6.

Tabla A-6 Configuración de la exportación de los logs

```
rINICTEL-RAAP(config)#logging source-interface FastEthernet0/1
rINICTEL-RAAP(config)#logging 200.37.45.50
```

A.2 Automatización de la configuración

Dado que la configuración era similar para los nueve *routers*, y todos estos cuentan con acceso vía Telnet, se optó por utilizar un *script* que se conecte a cada equipo y realice la configuración cambiando los parámetros necesarios para cada router. El *script*, mostrado en la tabla A-7, fue realizado utilizando Perl, dado que provee métodos para una fácil interacción con los *routers*.

Tabla A-7 Script para la configuración de los routers

```
#!/usr/bin/perl

use Net::Telnet::Cisco;

#Verifica los argumentos, por defecto apunta al router INICTEL
if($#ARGV>=0) {$host=$ARGV[0];} else {$host=1;}

#Relación de nombres
@router =
('PUCP','INICTEL','UNMSN','IPEN','UPCH','UNALM','UNI','URP','UCSM');

#Relación de IPs:
@ip =
('200.37.45.1','200.37.45.65','200.37.45.129','200.37.45.193','200.37.
46.1','200.37.46.65','200.37.46.129','200.37.46.201','200.37.46.209');

#Relación de passwords
@pass=('***', '***', '***', '***', '***', '***', '***', '***', '***');

@fecha = localtime(time);
$anio = $fecha[5]+1900;
$mes = $fecha[4]+1;
$fecha[1];
$fechaf = sprintf "$anio%02d%02d%02d%02d", $mes, $fecha[3], $fecha[2],
$fecha[1];

for ($host=1; $host<10; $host++) {
        printf "- Router %-7s: ",$router[$host];
                #Nueva sesión y logueo
                $sesion = Net::Telnet::Cisco->new(Host => $ip[$host]);
                $sesion->login('login', '***');
                # Entrar a modo privilegiado
                if ($sesion->enable("$pass[$host]") ) {

print "\n  Configurando: ";

print $sesion->cmd('configure terminal');

print "Custom port-maps ";
print $sesion->cmd('ip nbar port-map custom-02 udp 5036 4569');
print $sesion->cmd('ip nbar port-map custom-01 udp 53020 53021 53022
53023 53024 53025 53026 53027 53028 53029 53030 53031 53032');
print $sesion->cmd('ip nbar port-map custom-01 tcp 53009 53010 53011
53012 53013 53014 53015 53016 53017 53018 53019 53020 53021 53022
53023');

print "Access-list ";
print $sesion->cmd('access-list 50 permit 200.37.45.50');
```

```
print "SNMP ";
print $sesion->cmd("snmp-server community pc$router[$host] RO 50");
print $sesion->cmd('snmp-server enable informs');
print $sesion->cmd('snmp-server host 200.37.45.50 traps 1 config tty
syslog');
print $sesion->cmd('snmp-server enable traps config');
print $sesion->cmd('snmp-server enable traps tty');
print $sesion->cmd('snmp-server enable traps syslog');

print "NBAR ";
print $sesion->cmd('interface FastEthernet0/0');
print $sesion->cmd('ip nbar protocol-discovery');
print $sesion->cmd('interface FastEthernet0/1');
print $sesion->cmd('ip nbar protocol-discovery');

print "Logs ";
print $sesion->cmd('logging source-interface FastEthernet0/1');
print $sesion->cmd('logging 200.37.45.50');

print "\n";
print $sesion->cmd("exit\nexit");

        print "\nObteniendo configuración...";
                #Comando a ejecutar
                @int_acc = $sesion->cmd('show running-config');
                #Esto imprimiria todo el resultado
        print "ok  Guardando...";
                open (ARCHIVO, ">conf/$router[$host]_$fechaf.conf") ||
die("No se puede abrir el archivo");
                print ARCHIVO "@int_acc";
                close (ARCHIVO);
        print "ok\n";
                } else {warn "Error: " . $session->errmsg;}
                $sesion->close;
}
```

Anexo B: Monitoreo de un servidor Asterisk

En este anexo se mostrarán los pasos seguidos para lograr el monitoreo del servidor de VoIP.

B.1 Planteamiento del sistema

El sistema consta de un servidor NET-SNMP al cual se le ha añadido una MIB, definida utilizando el lenguaje ASN.1. Se debe tener en cuenta que el demonio snmpd debe estar funcionando en la misma computadora que el ASTERISK para que este pueda acceder a la información deseada.

Para que el NET-SNMP pueda obtener la información del ASTERISK necesitará ejecutar *scripts* con privilegios de administrador, esto no resulta práctico por consideraciones de seguridad, por esto este ejecutará a un archivo

binario que a su vez llamará al *script* propiamente dicho. El archivo binario, programado en C, tiene habilitado el SETUID, de forma que este proceso será ejecutado como el *owner* del mismo, en este caso el *root*.

Esto será integrado al resto del sistema, siguiendo la base del Cacti.

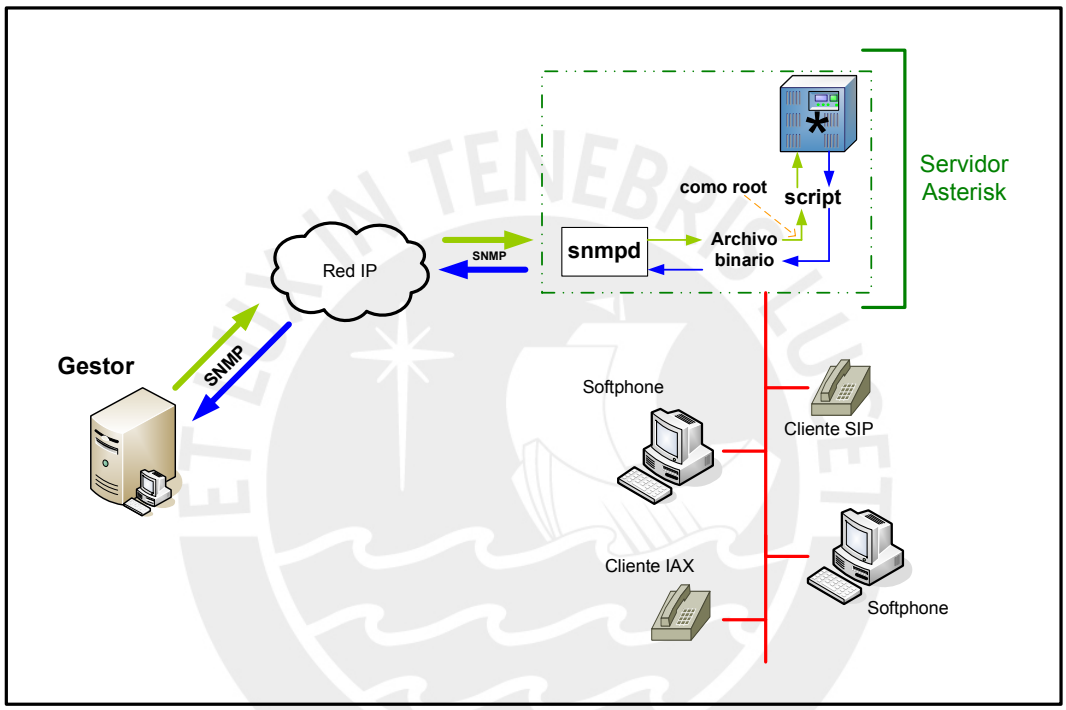

Figura B.1 Esquema del sistema de monitoreo del servidor Asterisk

B.2 Configuración seguida

El objetivo es monitorear el servidor VoIP de la RAAP, por lo que el trabajo se basa en el sistema descrito en [QUI2007]. Este es un Asterisk 1.0.11 basado en Rapid Xorcom, esta versión no cuenta con soporte SNMP, por lo que se definió una MIB para obtener los datos de los parámetros a monitorear.

La MIB, provee la estructura y las direcciones (OIDs) que utilizaremos, en este caso ha sido definida dentro de enterprises, y sigue la estructura mostrada en la figura A.2.

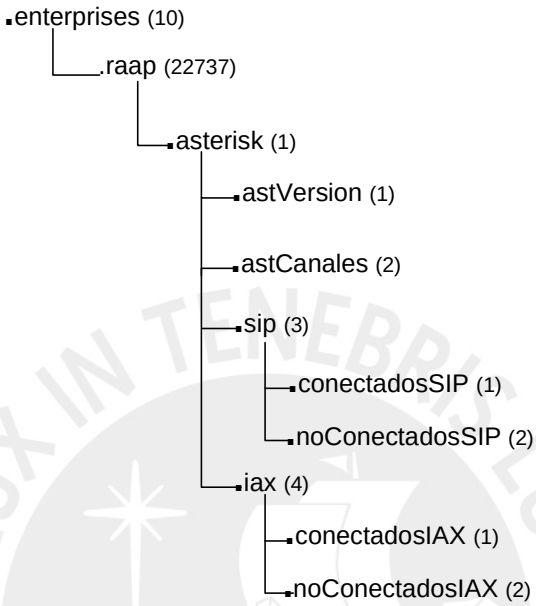

Figura B.2 Estructura de la MIB a definir

Para esto se utilizó la siguiente definición:

Tabla B-1 Definición de la MIB

```
RAAP-MIB DEFINITIONS ::= BEGIN

IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, enterprises
                                FROM SNMPv2-SMI
        OBJECT-GROUP            FROM SNMPv2-CONF


raap MODULE-IDENTITY
        LAST-UPDATED "200612050000Z" - 5/dic/2006
        ORGANIZATION "PUCP"
        CONTACT-INFO "Arturo"
        DESCRIPTION  "MIB para gestionar un servidor Asterisk"
        REVISION     "200612050000Z" -- 5/dic/2006
        DESCRIPTION  "Revision final"
        ::= { enterprises 22737}

asterisk        OBJECT IDENTIFIER ::= {raap 1}
raapMIBConformance OBJECT IDENTIFIER ::= { raap 2 }
sip             OBJECT IDENTIFIER ::= {asterisk 3}
iax             OBJECT IDENTIFIER ::= {asterisk 4}

astVersion OBJECT-TYPE
        SYNTAX Octect String
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "Este es un objeto que devuelve la version del
Asterisk"
        ::= {asterisk 1}
```

```
astCanales OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "Este es un objeto que devuelve el numero de
canales utilizandos actualmente"
        ::= {asterisk 2}

conectadosSIP OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "Este es un objeto que devuelve el numero de
clientes SIP conectados"
        ::= {sip 1}

noConectadosSIP OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION  "Este es un objeto que devuelve el numero de
clientes SIP NO conectados"
        ::= {sip 2}

conectadosIAX OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "Este es un objeto que devuelve el numero de
clientes IAX conectados"
        ::= {iax 1}

noConectadosIAX OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "Este es un objeto que devuelve el numero de
clientes IAX NO conectados"
        ::= {iax 2}


raapMIBGroup      OBJECT IDENTIFIER
                            ::= { raapMIBConformance 1 }

grupoRaap OBJECT-GROUP
    OBJECTS {
        astVersion,
        conectadosSIP,
        noConectadosSIP,
        conectadosIAX,
        noConectadosIAX
    }
    STATUS       current
    DESCRIPTION
        "Objetos para el monitoreo de Asterisk"
    ::= { raapMIBGroup 1 }

END
```

Teniendo la MIB ya es posible traducir los OIDs, con lo siguiente probamos su correcto funcionamiento:

Tabla B-2 Prueba de la utilización de la MIB

```
arturodr@gst:~$ snmptranslate -m ALL -On -IR astVersion
.1.3.6.1.4.1.22737.1.1
arturodr@gst:~$ snmptranslate -m ALL -On -IR astCanales
.1.3.6.1.4.1.22737.1.2
arturodr@gst:~$ snmptranslate -m ALL -On -IR conectadosSIP
.1.3.6.1.4.1.22737.1.3.1
arturodr@gst:~$ snmptranslate -m ALL -On -IR noConectadosSIP
.1.3.6.1.4.1.22737.1.3.2
arturodr@gst:~$ snmptranslate -m ALL -On -IR conectadosIAX
.1.3.6.1.4.1.22737.1.4.1
arturodr@gst:~$ snmptranslate -m ALL -On -IR noConectadosIAX
.1.3.6.1.4.1.22737.1.4.2
```

Una vez que todos los OIDs son traducidos, es necesario relacionar estos OIDs con los scripts correspondientes. Esta configuración se realiza en el /etc/snmp/snmpd.conf

Tabla B-3 Configuración de la relación de los OIDs con los scripts

```
pass .1.3.6.1.4.1.22737.1.1
      /usr/share/cacti/site/scripts/raap/astVersion
pass .1.3.6.1.4.1.22737.1.2
      /usr/share/cacti/site/scripts/raao/astCanales
pass .1.3.6.1.4.1.22737.1.3.1
      /usr/share/cacti/site/scripts/raap/conectadosSIP
pass .1.3.6.1.4.1.22737.1.3.2
      /usr/share/cacti/site/scripts/raap/noConectadosSIP
pass .1.3.6.1.4.1.22737.1.4.1
      /usr/share/cacti/site/scripts/raap/conectadosIAX
pass .1.3.6.1.4.1.22737.1.4.2
      /usr/share/cacti/site/scripts/raap/noConectadosIAX
```

Dentro de cada ejecutable se realiza una llamada a un script correspondiente, tomaremos como ejemplo la realización del script de llamadas:

Tabla B-4 Programa en C que llama al script

```
#include <unistd.h>
#include <stdlib.h>
#include <stdio.h>

int main() {
        execl("/usr/share/cacti/site/scripts/raap/astCanales.sh",
NULL);
        return 1;
}
```

Este archivo es compilado y se genera un ejecutable:

Tabla B-5 Generación del ejecutable

```
$ sudo gcc astCanales.c -o astCanales
```

a este ejecutable debemos ejecutarlo como root sin importar el usuario que lo invoque, para esto el owner del fichero debe ser root y se debe activar el SETIUD:

Tabla B-6 Configuración del SEIUD

```
$ sudo chown root astCanales
$ sudo chmod 4711 astCanales
```

Por otro lado el *script* invocado debe devolver, el valor de las llamadas, para esto realiza una conexión al asterisk que está corriendo en la máquina y ejecuta el comando *show channels*, cabe resaltar que este comando devolverá mas información que no es necesaria para este caso, por lo que se ejecutan filtros de forma que solo nos quedemos con las porción que nos interesa. De forma adicional se debe devolver el OID y el tipo de dato que se está retornando. Finalmente el *script* queda de la siguiente manera:

Tabla B-7 Script para la obtención de los datos

```
#!/bin/sh
PATH=/usr/bin:/usr/sbin:/bin:/sbin
echo ".1.3.6.1.4.1.22737.1.2"
echo "Integer32"
asterisk -rx "show channels" | tail -1 | head -1 | cut -f 1 -d " "
```

Ahora haciendo un snmpget al *host*, este devolverá la cantidad de llamadas en ese momento. Para poder utilizar los nombres de los OIDs debemos hacer que se tomen en cuenta todas las MIB, de la siguiente forma:

Tabla B-8 Variable para exportar todos los MIBs

```
$ export MIBS=ALL
```

Luego de esto ya es posible realizar consultas de forma normal, por ejemplo:

Tabla B-9 Prueba utilizando snmpget

```
$ snmpget -v 1 -c public localhost astCanales
RAAP-MIB::astCanales = INTEGER: 1
```