
# UNIVERSIDAD DEL AZUAY

## Facultad de Ciencias de la Administración

## Escuela de Ingeniería de Sistemas

***"Gestión de monitoreo de redes mediante la herramienta Galileo en la Universidad del Azuay"***

Trabajo de Graduación previo a la obtención del
Título de Ingeniero de Sistemas

Director:

Ing. Pablo Esquivel León

Autores:

Sara Paola López Quezada

Diego Felipe Merchán Flores

Cuenca – Ecuador

2006

## INDICE GENERAL

**CAPITULO V**



**CAPITULO VI**



**CAPITULO VII**



**CAPITULO VIII**



**CAPITULO XI**

**CAPITULO X**

**AGRADECIMIENTO**

En primer lugar queremos agradecer a Dios por la oportunidad que nos brinda para culminar con éxito este trabajo.

Así mismo a nuestros padres, Marcia y Alfredo, Beatriz y Raúl, por dejarnos la educación como su mejor herencia, por su invalorado apoyo con ejemplo de valores de amor, responsabilidad, trabajo y honestidad. Por todo su sacrificio y amparo con nuestros hijos y nosotros mismos.

Finalmente deseamos expresar nuestro agradecimiento más sincero al Ing. Pablo Ronco de la Universidad de Buenos Aires, por su ayuda en la preparación de esta monografía. Además, agradecemos especialmente al Ing. Pablo Esquivel, quien supo apoyarnos técnica y profesionalmente con mucha paciencia, preocupación y dedicación.

**Los autores**

**DEDICATORIA**

A Dios por darme la vida, guiar e iluminar mi camino y sobre todo por permitirme disfrutar mis logros junto a mis hijos Paola y Julián

A mi esposo, por ser un gran compañero y amigo.

A mis padres, quienes han sido ejemplo en mi vida.

A mi segunda madre Patricia, quién con su amor y cariño me dio mucho valor para alcanzar mis metas.

A mis suegros, que sin su apoyo no hubiera podido conseguir ningún logro, con el cuidado de mi bebé

**Paola**

**DEDICATORIA**

Este trabajo se lo dedico entero a mis hijos, Paola Gabriela y Diego Julián, por el inmenso amor que siento por ellos por ser las personas, junto al de mi esposa Paola, más importantes en mi vida.

A mis padres por guiarme toda su vida mostrándome los objetivos que son los verdaderos ingredientes que dan propósito a mi vida.

**Felipe**

## RESPONSABILIDAD

Todas las ideas, contenido y opiniones vertidas en éste trabajo son de exclusiva responsabilidad de los autores.

| | |
|---|---|
| Paola López de Merchán | Felipe Merchán Flores |

## INDICE DE ILUSTRACIONES

## Resumen

Presentamos a Galileo un Sistema de Monitoreo administrado, el que utiliza una herramienta simple que provee información sobre la red. Emite alertas ante ciertos eventos que pueden comprometer la disponibilidad de los servicios y permite reaccionar a tiempo para contrarrestarlos. Realiza la recolección donde podemos visualizar los datos necesarios para la gestión de performance. Con él podemos obtener vistas del estado actual y reciente de la infraestructura de servicios y redes de información. Planificar el incremento del hardware y software. Obtener variedad de mediciones y análisis de los dispositivos seleccionados. Contar con reportes periódicos de disponibilidad y de perfomance.

Galileo brinda visibilidad del estado de la infraestructura del cliente, permite accionar proactivamente para evitar problemas, evaluar la capacidad de sus recursos para brindar servicios y planificar su necesidad futura

## Abstract

Galileo is an Administration Monitoring System which utilizes a simple tool to provide information about your network and send event-related alerts befote they compromise the availability of services, providing a proactive response. The system collects all the necesary information in order to monitor the network performance, monitor the current information system and services infraestructure, perform hardware and software upgrade planning, and obtain availabilty and performance reports.

Galileo provides a view of the current system infraestructure, allows to act proactively to avoid system downtime, and evaluates the current resource capacity in order to forecast upcoming service needs.

# CAPITULO I

# INTRODUCCIÓN GENERAL

En este siglo de grandes avances tecnológicos, en donde el uso de las computadoras ha sido generalizado. Las redes de computadoras han tenido un crecimiento sostenido en los últimos años, en donde cada vez un mayor número de empresas e instituciones educativas, dependen gran número de sus procesos y operatividad a estas.

Esta creciente expansión de las redes de comunicaciones ha hecho necesario la adopción y el desarrollo de herramientas de seguridad que protejan tanto los datos transmitidos como el acceso a los elementos de la red de los posibles ataques que pueda sufrir.

La administración de redes se está convirtiendo en una creciente y compleja tarea debido a la variedad de tipos de red y a la integración de diferentes medios de comunicación. A medida que las redes se vuelven más grandes, más complejas y más heterogéneas, el costo de su administración aumenta. En tal situación, son necesarias herramientas automáticas para dar el soporte requerido por administradores humanos, recolectando información acerca del estatus y el comportamiento de los elementos de red.

Ahora ya no se trata solo de mantener operativos los nodos como si de entes individuales se tratase, el nuevo objetivo debe ser mantener el sistema como un todo, como un solo ente. Se trata de nuestro mundo artificial en el que las iteraciones entre los distintos nodos se vuelven mucho más ricas y complicadas

Cualquier red corporativa debe estar correctamente administrada con el objetivo de asegurar a sus usuarios su utilización. QoS es una tecnología que permite garantizar a los clientes de red el correcto funcionamiento de la misma, por otra parte, la monitorización del tráfico nos servirá para evitar problemas, o en el peor de los casos, para ayudarnos a solucionarlos.

## *1.1 Generalidades de Galileo*

**Qué es Galileo ?**

Galileo es un sistema de monitoreo que permite conocer el estado actual e histórico de los equipos y servicios monitoreados.

El acceso a esta información se realiza mediante un browser o un llamado telefónico.

Con Galileo Ud. puede:

- Enviar mensajes de alarma frente a fallas en los equipos monitoreados en distintos formatos: mail, mensajes de audio, pager, llamado telefónico.

- Recibir alarmas generadas por Galileo permitiéndole actuar antes que las fallas sean percibidas por los usuarios.

- Correlacionar los datos recolectados y determinar las posibles causas de las fallas.

- Generar reportes de disponibilidad automáticos con los datos recolectados.

- Verificar el cumplimiento de los niveles de servicios acordados con sus proveedores o clientes.

- Dimensionar los recursos de red y planificar su crecimiento “capacity planning”, es decir que Ud. puede estimar la tendencia de las variables monitoreadas y así evitar fallas antes de que los recursos se saturen.

## *1.2 Ingreso al sistema*

El acceso al sistema se realiza mediante un “browser” que soporte HTTPS (Internet Explorer, Mozilla Firefox, Netscape, etc). En la barra de direcciones deberá ingresar un URL como el siguiente.

https://”nombre o ip del servidor”; Ejemplo: https://172.16.1.169

En ese instante, el servidor Galileo presentará un certificado de clave pública que le garantiza la autenticidad de la información al usuario.


**Figura 1-1** Certificado de Autenticidad

Acepte el certificado generado por UyR Consultores.

Luego, en la ventana de autenticación, ingrese su nombre de usuario y contraseña. Estos fueron creados por el administrador del servicio Galileo.

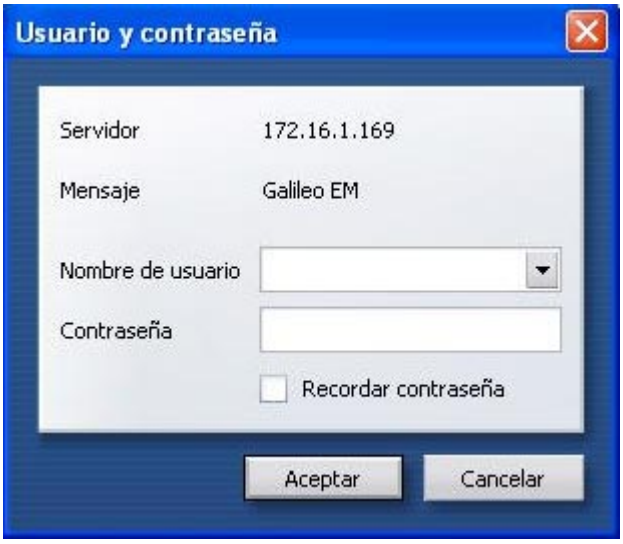



**Figura 1-2** Registro de usuario

Si la autenticación se realiza satisfactoriamente, Usted accederá a la pantalla principal del sistema.

**NOTA:**

En adelante llamaremos nodo a todo equipo monitoreado por Galileo

## 1.3 Pantalla Principal

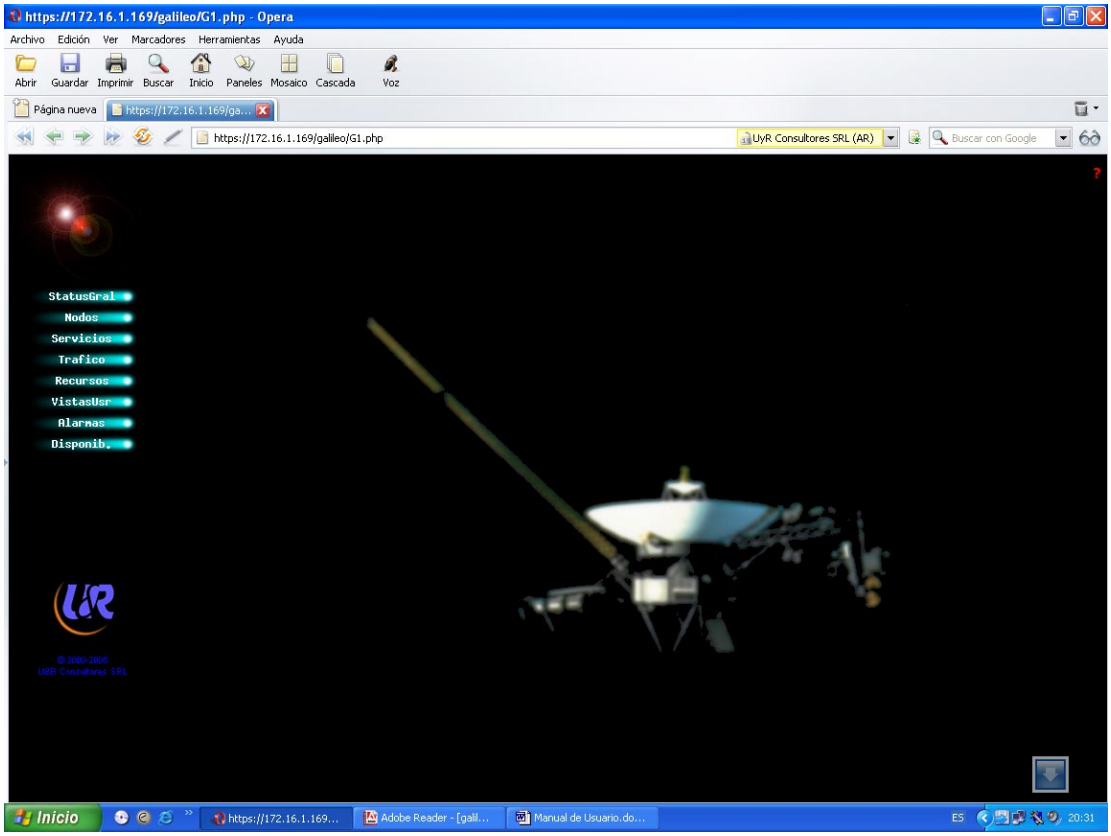



**Figura 1-3** Pantalla principal de Galileo

La pantalla de Galileo se encuentra dividida en tres regiones, una central, donde se presenta la información; una sobre el margen izquierdo, en la que el usuario accede a las distintas secciones; y una superior, en la que se escoge la vista de una sección.

## *1.4 Barra de Secciones*

En la columna de la izquierda se encuentran una serie de opciones que permiten seleccionar las distintas secciones del sistema que ofrece Galileo.

| | |
|---|---|
| **Estado General** | • Se presenta información consolidada del estado actual de todos los nodos.<br>• No se muestra histórico<br>• No se muestran los valores medidos |
| **Nodos** | • Se presenta información estática detallada de los mismos.<br>• No se muestra estado actual<br>• No se muestra histórico<br>• No se muestran los valores medidos |
| **Servicios** | • Se presentan los valores medidos sobre los servicios monitoreados.<br>• Se muestra el estado actual<br>• Se muestra información histórica en forma gráfica<br>• Se muestra el valor de la última medición |
| **Tráfico** | • Se presentan los valores medidos de cantidad y composición de tráfico y tiempo de respuesta sobre los enlaces monitoreados.<br>• Se muestra el estado actual<br>• Se muestra información histórica en forma gráfica<br>• Se muestra el valor de la última medición |
| **Recursos** | • Se presentan los valores medidos referidos a los recursos de los distintos nodos de la red. (Espacio en disco, utilización de procesador, memoria RAM disponible, etc)<br>• Se muestra el estado actual<br>• Se muestra información histórica en forma gráfica<br>• Se muestra el valor de la última medición |

| | |
|---|---|
| **Vistas de Usuarios** | • Sección en la que el usuario puede crear múltiples vistas. Permite agrupar la visualización diferentes variables relacionadas según el criterio del usuario en una única vista.<br>• Permite correlacionar distintas variables |
| **Alarmas** | • Sección que permite ver las alarmas y agruparlas según el tiempo |
| **Disponibilidad** | • Se muestra la disponibilidad de los nodos y sus respectivos servicios y recursos |

## *1.5 Barra de Vistas*


**Figura 1-5** Barra de Vistas

Según la sección que se trate, la barra de vistas dispondrá de 1 o mas botones. Esta barra se utiliza principalmente para especificar una vista dentro de una sección, Ejemplo. Visualizar la vista de “memoria RAM” dentro de la sección “recursos”.

## *1.6 Aumento del detalle de la información visualizada*

Para cada una de las vistas se pueden definir distintos niveles de detalle. Hay varios modos de aumentar el detalle de la información que muestra Galileo.

Uno es usando los botones de “**detalle”** junto a la barra de vistas, que está sobre el sector superior derecho de la pantalla de Galileo.

El nivel 0 es el que se muestra siempre por defecto, las vistas 1 y 2 agregan sucesivamente más información.

Otro modo es haciendo “clic” sobre alguno de los íconos que representa el nodo del que deseamos tener mas detalle. Primero mostrará solamente dicho icono con mayor información en modo texto, si hacemos “clic” nuevamente sobre el icono, se despliega a la derecha un gráfico que muestra el comportamiento en función del tiempo. Si volvemos a hacer “clic” sobre el gráfico, se obtiene un zoom del mismo.

Cuando estamos viendo el gráfico, en la parte superior derecha de la pantalla aparecen las siguientes opciones:

**Vista** con valores de 0 a 4: Los distintos valores de la vista se corresponden con el intervalo de tiempo que se mostrará en el gráfico.

| Vista | Período visible | Intervalo entre muestras |
|---|---|---|
| 1 | Últimas 24 horas | 3 minutos |
| 2 | Últimas 200 horas (≈1 semana) | 30 minutos |
| 3 | Últimas 800 horas (≈1 mes) | 2 horas |
| 4 | Últimos 400 días (≈1 año) | 1 día |

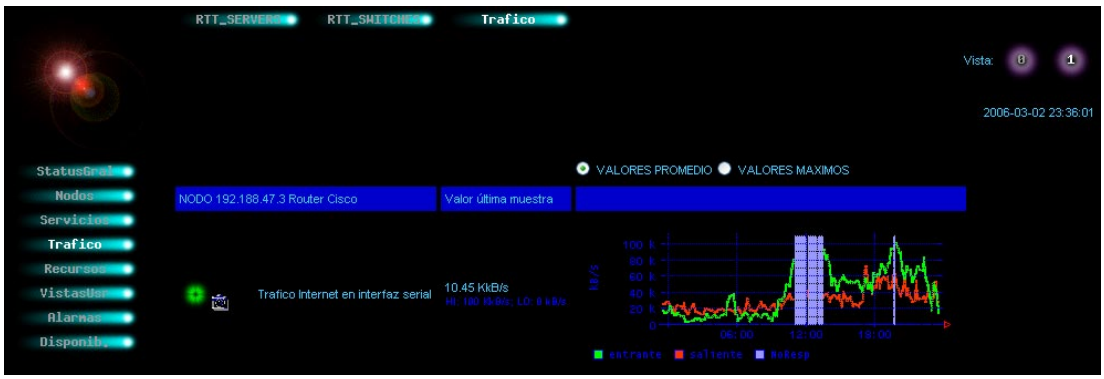



**Figura 1-6** Vista 1 Tráfico de Internet en interfaz serial

En los gráficos pueden aparecer zonas sin información en color gris o azul.

El color gris indica que Galileo durante dicho período no estuvo en condiciones de monitorear dicha variable o estuvo deshabilitada dicha recolección.

Las zonas en azul indican que la variable monitoreada no pudo ser leída, por ejemplo porque el nodo a monitorear estaba apagado, fuera de la red u otro problema que impide leer dichas variables dentro de los “timeouts” previstos.

## *1.7 Reportes, Disponibilidad y Gráficos*

Las opciones **PDF, DISP, DISP2 y Graf** que aparecen en las vistas, en la parte superior derecha, nos permiten:

- **DISP** muestra la disponibilidad de los nodos y con las vistas 0, 1 y 2 podemos visualizar sucesivamente más información. Al hacer click sobre éste icono, el mismo cambia por Graf.

- **DISP2** muestra la disponibilidad de los nodos de la vista y se configura el intervalo de tiempo y el criterio para determinar la no disponibilidad (OOS, LIMITHI, LIMITLO).

- **PDF** genera el reporte de lo que vemos en pantalla (Disponibilidad o Gráfico) y lo guarda en un archivo con formato pdf.

- **Graf** muestra los gráficos de las variables mostradas. Esta opción no se ve normalmente en el menú ya que es la vista por defecto. Al hacer click sobre éste icono, el mismo cambia por DISP.


**Figura 1-7** Gráficos Vista 1 en Switches

# CAPITULO II

## Estado General

Seleccionando el ítem **StatusGral** se accederá a la sección de “Estado General”. En esta pantalla se representa información de estado actual de todos los nodos monitoreados, permitiendo detectar fácilmente si hay algún problema o situación de alarma.

Para cada nodo, se indica el nombre y se incluye una barra de estado.

Utilizando una representación gráfica y numérica, esta barra representa la cantidad y los estados de las variables monitoreadas del nodo. El tamaño de franjas de la barra de estados será proporcional a la cantidad de variables que se encuentran en cada uno de los estados

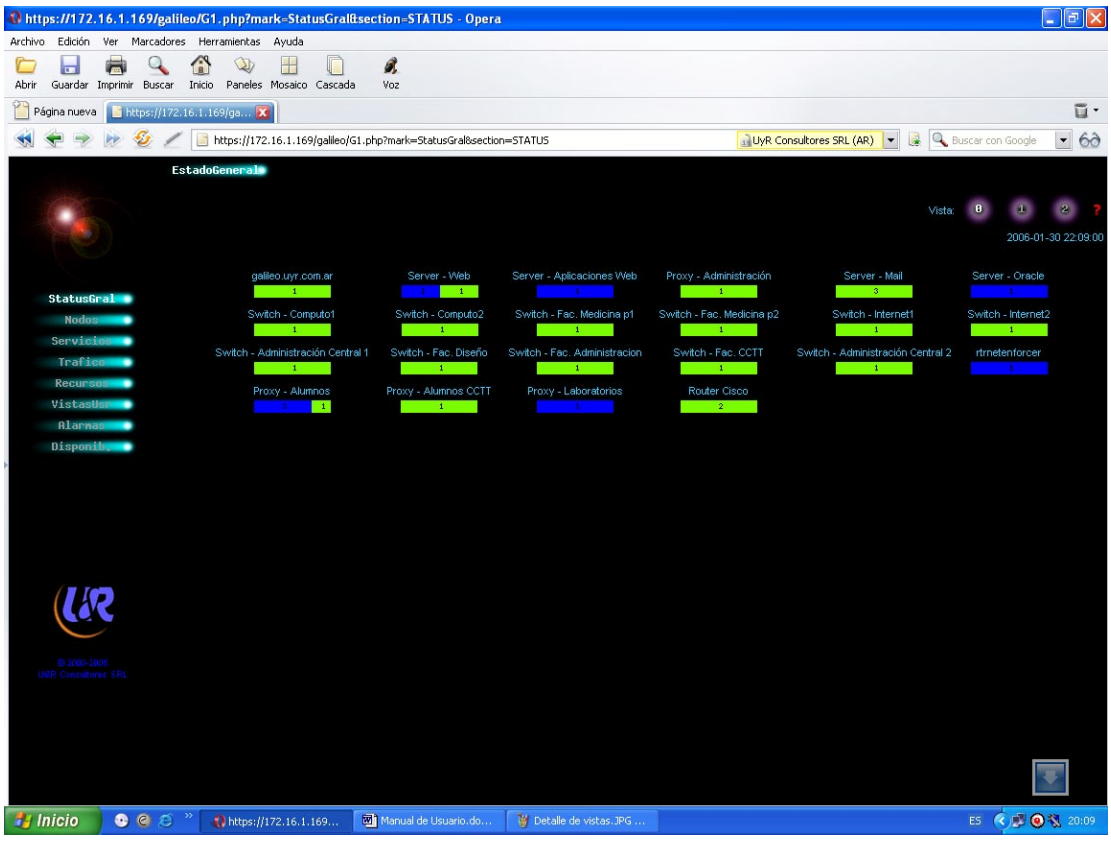



**Figura 2-1** Estado General de los nodos del campus

## *ESTADO NORMAL*

Si aparece una franja verde con un número adentro indica la cantidad de variables que se encuentran en una situación normal.

## *ESTADO DE FALLA*

Si aparece una franja roja con un número adentro indica la cantidad de variables que se encuentran fuera de rango. Es decir, que el valor actual de la variable esta por encima del umbral superior, o por debajo del umbral inferior definido.

## *ESTADO DE NO DISPONIBILIDAD*

Si aparece una franja azul con un número adentro indica la cantidad de variables que se encuentran fuera del “alcance” de Galileo. Es decir, la estación de monitoreo no puede medir la variable correspondiente.

Ejemplo: Nodo en el cual se monitorean 18 variables. 8 se encuentran NORMAL, 7 NO DISPONIBLES y 3 en FALLA

# CAPITULO III

## Nodos

Un nodo es un equipo que está siendo monitoreado por Galileo.
Los nodos pueden agruparse por región geográfica, función u otra característica.
Este agrupamiento lo realiza, a pedido del cliente, el administrador o proveedor del Galileo y no es modificable desde la interfaz de usuario.

Al seleccionar un grupo desde el menú superior horizontal, se muestra un detalle de los nodos que conforman dicho grupo, como ser nombre, función, dirección IP, sistema operativo y estado actual de las variables que se están monitoreando en dicho nodo.

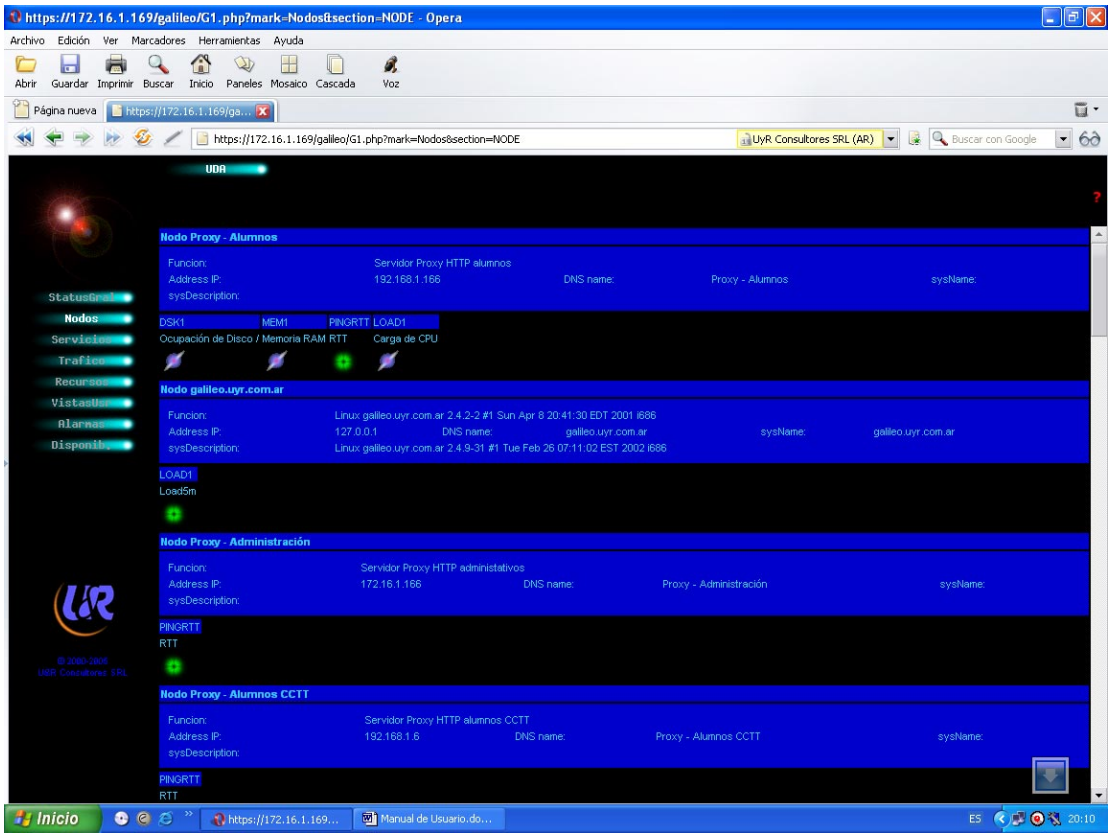



**Figura 3-1** Detalle de nodos

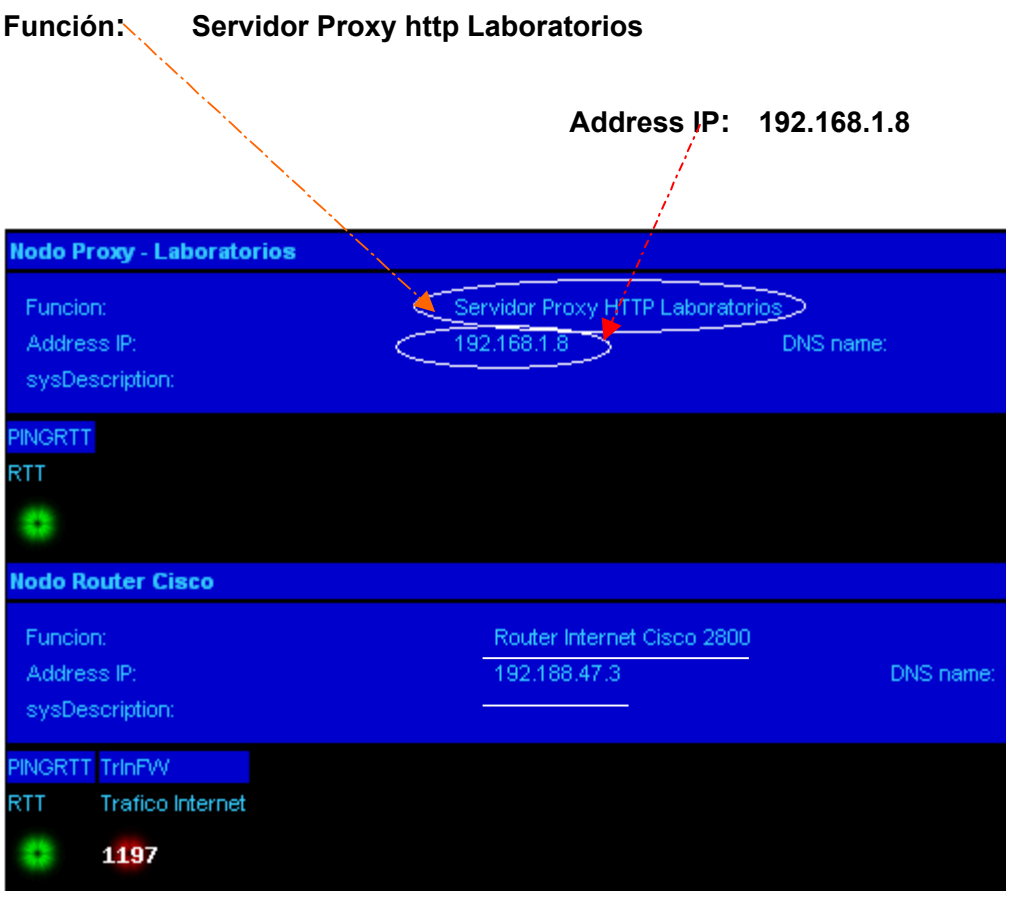



**Figura 3-2** Nombre o Función y Dirección IP de cada nodo

El ingreso de ésta información es directo en la base de datos Galileo, en la tabla Server.

Ver el Anexo A, que muestra la BD completa.

## *3.1 Reporte Ejemplo*

En la ilustración siguiente podemos mostrar la disponibilidad del nodo Proxy – Laboratorios atendiendo a un criterio de selección, de 09:00 a 18:00, de Lunes a Viernes durante el mes de Febrero de 2006.


**Figura 3-3** Personalización de reporte para un nodo

Se puede interpretar como cuatro eventos registrados en la variable levantada RTT (Round Trip Time) en el modo Proxy – Laboratorios en los criterios antes descritos.

Este reporte lo podremos obtener con la opción DISP2 revisado en la opción Reportes, disponibilidad y gráficos del capítulo primero. Contamos además con la opción de generar un documento en formato .PDF para almacenarlo para posteriores revisiones.

# CAPITULO IV

## Servicios

Esta opción permite tener una vista de los nodos monitoreados en función de los servicios que se prestan, como ser WEB, SMTP.

El servicio a visualizar se selecciona desde el menú superior horizontal, luego se puede modificar la vista con las opciones 0, 1, 2 y 3, ampliar los gráficos haciendo click sobre los mismos, o generar los reportes con la opción PDF en conjunto con DISP2.

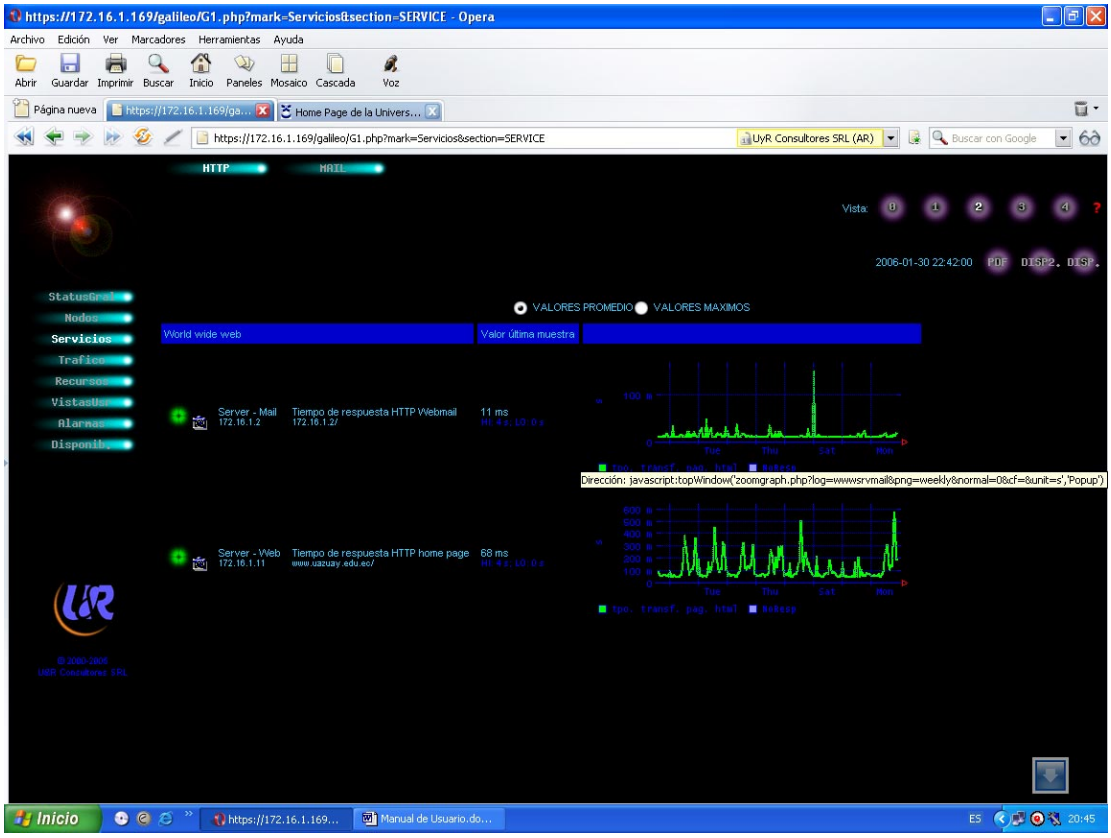



**Figura 4-1** Detalle de Servicios Http

En la siguiente pantalla se puede observar que la última muestra del tiempo de respuesta SMTP del nodo Server – mail es de 3.47 ms, es decir dentro del umbral permitido HI: 1 s; LO: 0 s

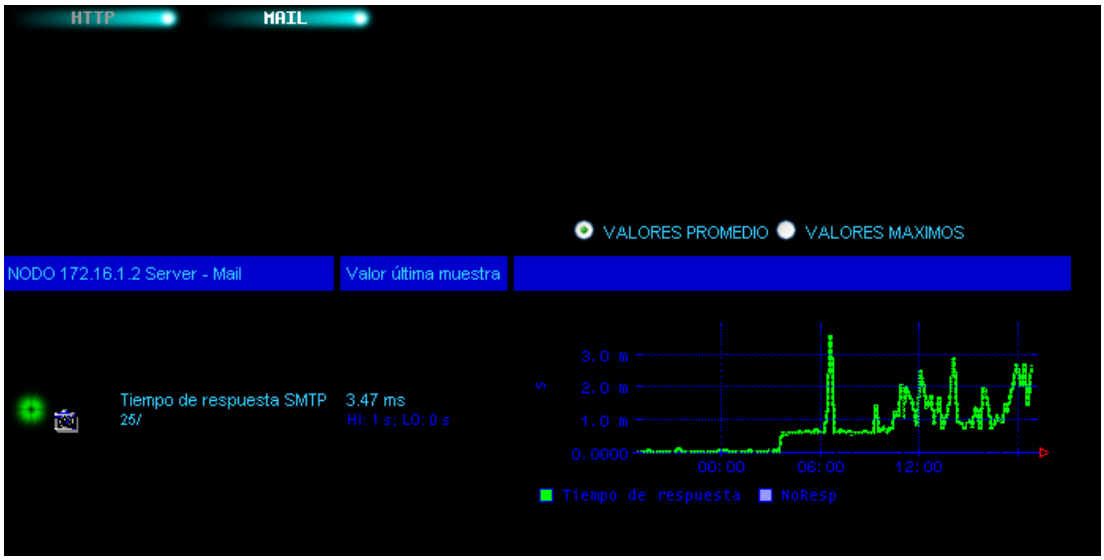



**Figura 4-2** Detalle de Servicios Server-Mail

# CAPITULO V

# Tráfico

Esta opción permite tener una vista de los nodos monitoreados en función del tráfico en sus interfaces de red.

El tipo de tráfico a visualizar se selecciona desde el menú superior horizontal, con las opciones Netflows, TrafIF, TrCircFR y TrafFS (pueden no estar visibles las cuatro opciones, o estar con nombres configurables)

Luego se puede modificar la vista con las opciones 0, 1, 2 y 3, ampliar los gráficos haciendo click sobre los mismos, o generar los reportes con la opción PDF en conjunto con DISP y Graf.

***5.1 Netflows*** permite identificar el tráfico discriminando por protocolo, por ejemplo podemos ver el tráfico debido a dns, http, https, imap, mail, netbios, snmp.

También nos muestra el tráfico total y un gráfico con el aporte porcentual de cada uno en el total.


**Figura 5-1** Tráfico en los nodos Switches

***5.2 TraflF*** nos permite ver el total de tráfico entrante y saliente en cada una de las interfaces de cada nodo monitoreado. También podemos ver la diferencia entre el tráfico entrante y saliente del firewall.


**Figura 5-2** Tráfico entrante y saliente en interfaz serial

***5.3 TrCircFR*** permite ver el tráfico de los circuitos de Frame Relay

***5.4 TrafFS*** permite ver el tráfico en los file servers

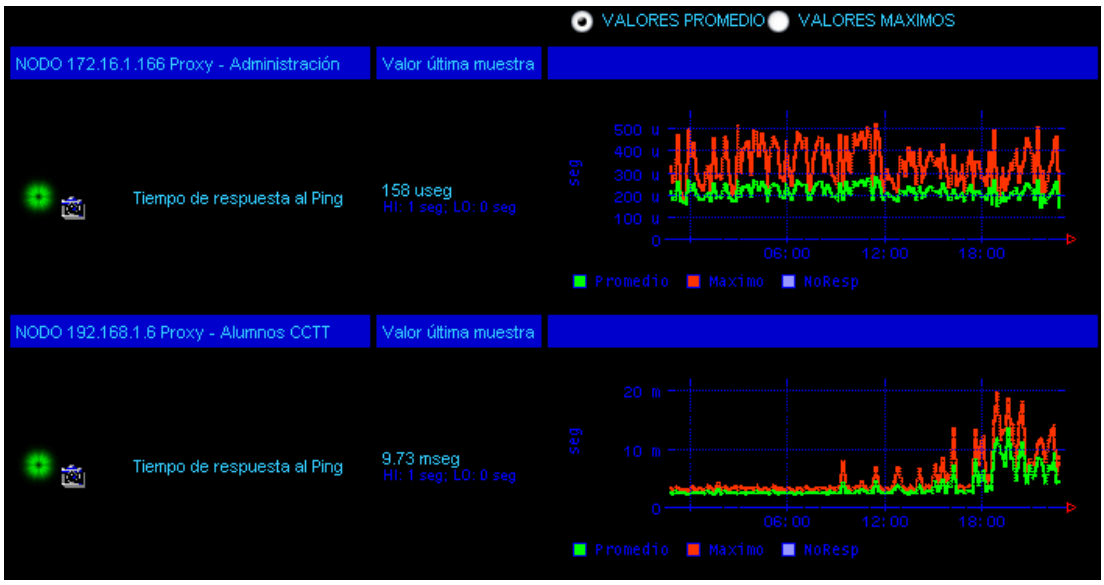



**Figura 5-3** Tráfico en los nodos servers

## 5.5 Reporte Ejemplo

En la ilustración siguiente podemos mostrar la disponibilidad del nodo Router – Cisco atendiendo al tiempo de respuesta en el mes de Febrero de 2006, de donde se han obtenido 20 eventos

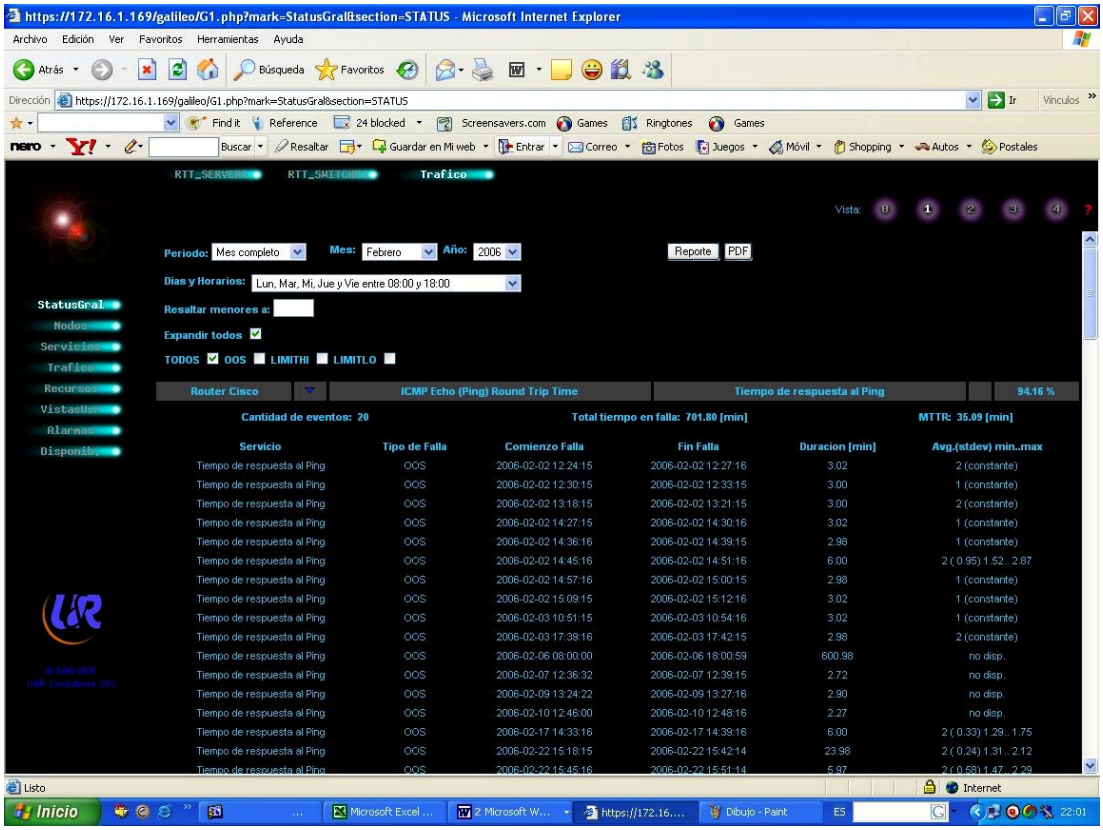



**Figura 5-4** Reportes por criterios

# CAPITULO VI

## Recursos

Esta opción permite tener una vista del estado de los recursos de los nodos monitoreados.

El tipo de recurso a visualizar se selecciona desde el menú superior horizontal, luego se puede modificar la vista con las opciones 0, 1, 2, 3 y 4 ampliar los gráficos haciendo click sobre los mismos, o generar los reportes con la opción PDF en conjunto con DISP2 y Graf.


**Figura 6-1** Carga del Procesador del en nodo Galileo.uyr.com.ar

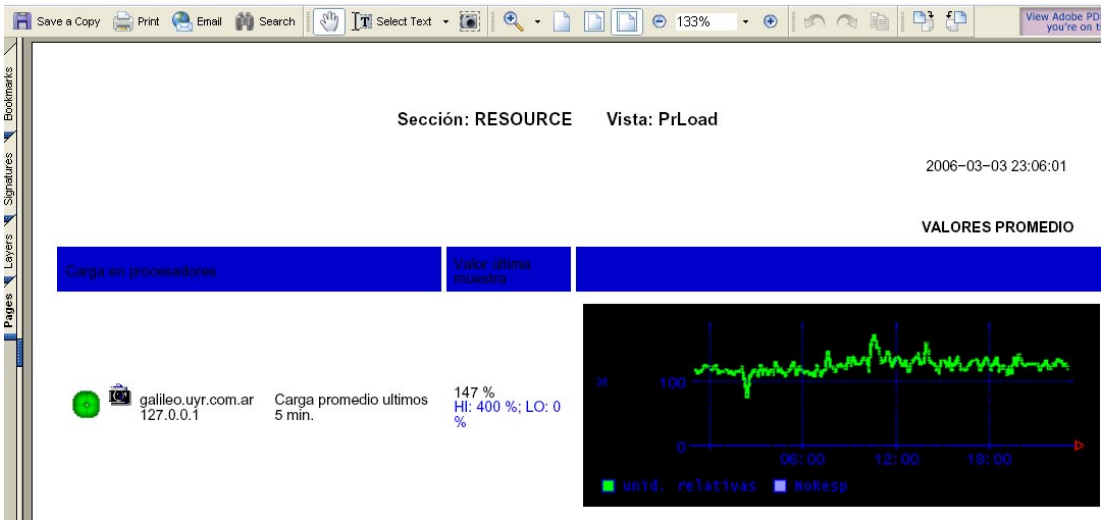



**Figura 6-2** Reporte generado con la opción PDF

Los recursos están agrupados bajo los siguientes menús:

DISK_OCUP, MEMORIA_DISP, Proc, UPS y CPU_SERVERS.

Se pueden agregar o sacar otros menús, es parte de la configuración).

***6.1 DISK_OCUP*** muestra el espacio libre y utilizado en cada partición de disco de los nodos monitoreados. Es útil para ver el crecimiento gradual de los datos y poder predecir en que momento nos quedaremos sin espacio en disco.

***6.2 MEMORIA_DISP*** muestra la memoria Virtual o Física disponible o ocupada, dependiendo de la plataforma en la que se muestrea.

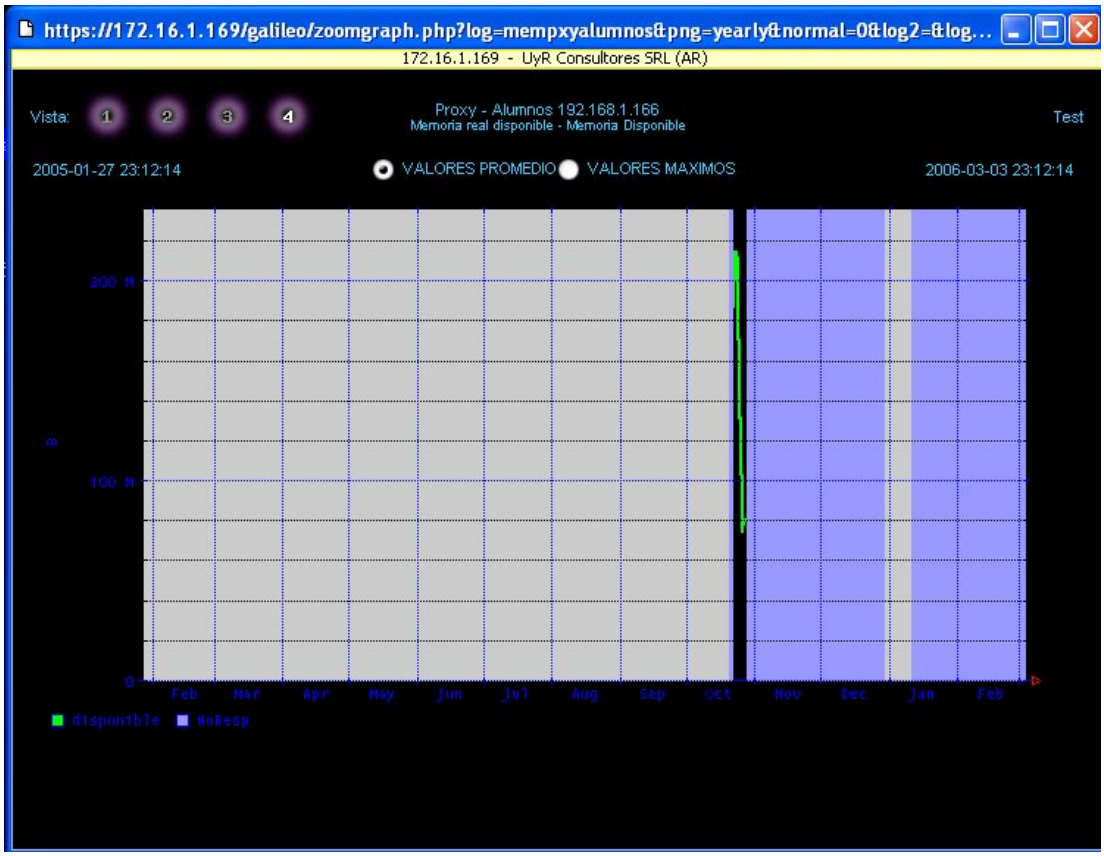



**Figura 6-3** Memoria disponible del Proxy alumnos de un año

En la imagen anterior el color gris indica que Galileo durante dicho período no estuvo en condiciones de monitorear dicha variable y la zona azul indica que la variable monitoreada no pudo ser leída, el nodo estuvo apagado o fuera de red

***6.3 Proc*** muestra procesos y la cantidad de los mismos, por ejemplo la cantidad de procesos http que están corriendo en un servidor. Se pueden muestrear varios proceso por nodo.

***6.4 UPS*** muestra el porcentaje de carga y el tiempo remanente de cada una de las UPS monitoreadas.

***6.5 CPU_SERVERS*** muestra la cantidad media de procesos en la “run queue” del procesador de cada uno de los nodos monitoreados o la utilización del CPU dependiendo de la plataforma. En el primer caso, este valor sirve para estimar la carga de los procesadores.

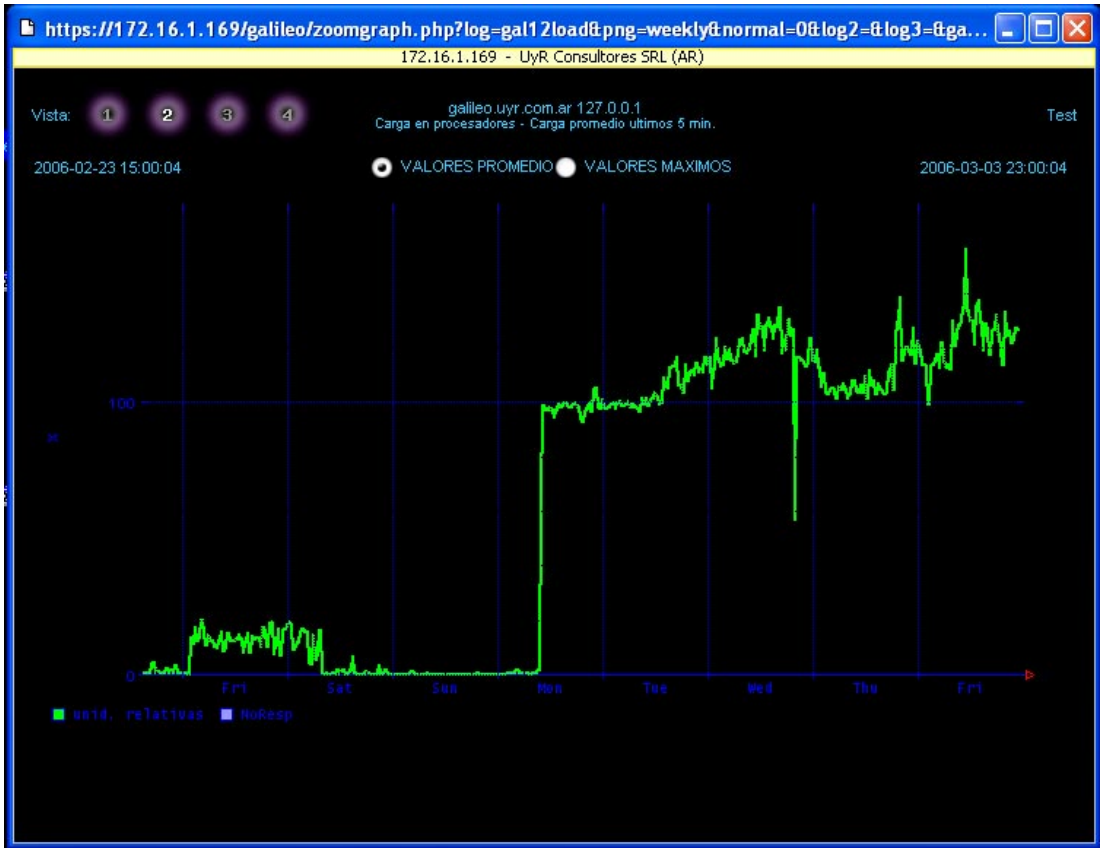



**Figura 6-4** Gráfico de carga del Procesador en una semana

# CAPITULO VII

# Vistas de Usuario

La opción **VistasUsr** permite crear vistas propias a cada usuario de Galileo.
Un mismo usuario puede tener varias vistas distintas según sus necesidades.

A medida que se van agregando vistas de usuario, se va ampliando el menú superior horizontal, incorporando las recientemente creadas.

Las vistas creadas se seleccionan desde el menú superior horizontal, luego se puede modificar la vista de las variables mostradas con las opciones 0, 1, 2 y 3, ampliar los gráficos haciendo click sobre los mismos, o generar los reportes con la opción PDF en conjunto con DISP y Graf.

## *7.1 Como crear una vista de usuario*

En los menús Servicios, Tráfico y Recursos aparecen, en la vista 0, un “check box” junto a cada una de las variables monitoreadas. Son éstas variables las que podrán incorporarse en las vistas de usuario.

Se ingresa a Servicios, Tráfico y Recursos sucesivamente haciendo un click en el checkbox de cada variable que nos interesa ver desde la vista que vamos a crear.

Luego de seleccionadas las variables, se hace click sobre el botón **AGREGAR** que aparece a la derecha de la pantalla. Esta operación va recolectando las variables de nuestro interés.

Luego, en el menú **VistasUsr**, hacemos click sobre **Usuario** en el menú superior horizontal, completamos el nombre de la nueva vista en la ventana que aparece a la derecha bajo SALVAR COMO y luego hacemos click sobre **SALVAR COMO**.
A partir de este momento ya aparecerá en el menú superior horizontal la nueva vista.

### 7.1.1 Ejemplo de creación de vistas de usuario

La primera pantalla muestra la vista previa que tenemos sobre **VistasUsr** antes de crear la vista de usuario.

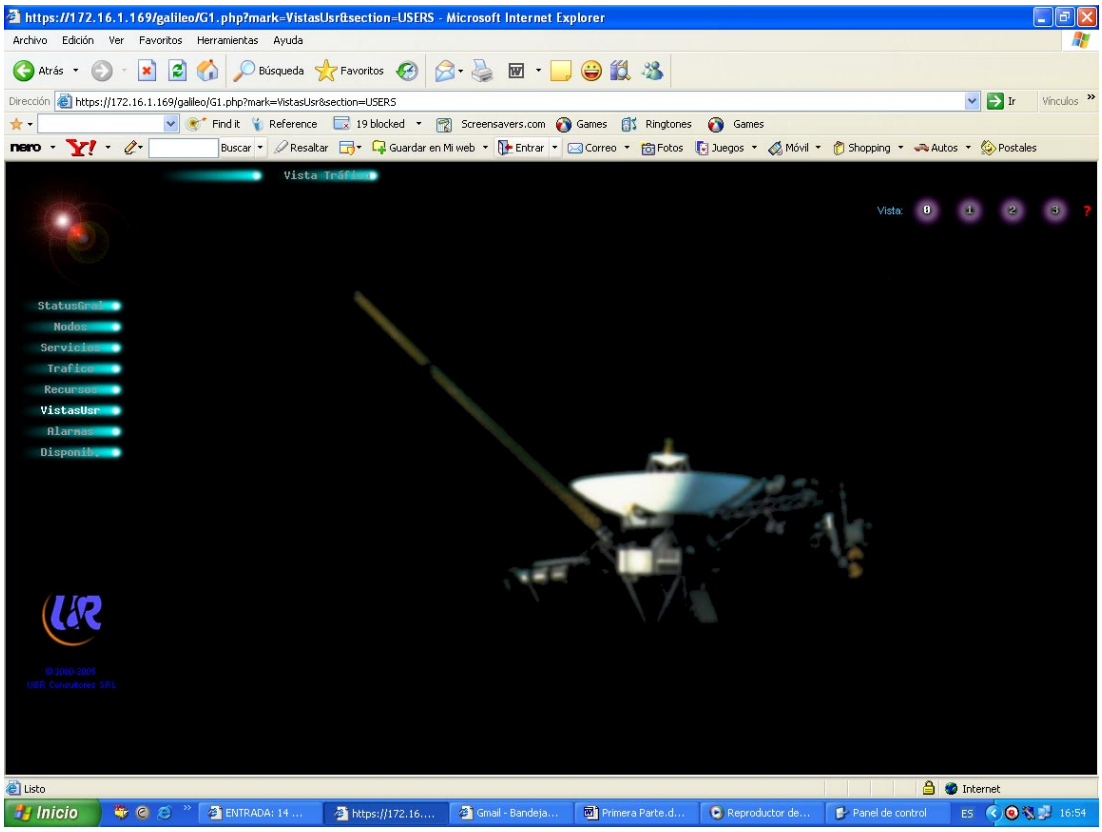



**Figura 7-1** Pantalla de Vista de usuario

Primero vamos a **Tráfico** (En la vista "0") y seleccionamos la variable, Rtt_Switches y luego con un click sobre el Check Box del nodo Switch– Internet1,


**Figura 7-2** Selección de tráfico del nodo Switch – Internet1


Click en Agregar

Igualmente seleccionamos el Check Box del nodo Router Cisco de la variable Tráfico, para obtener un detalle de este nodo en el mismo reporte.


**Figura 7-3** Selección de tráfico del nodo Router Cisco

Lo mismo podemos hacer con los servicios www (World wide web) con las variables correspondientes

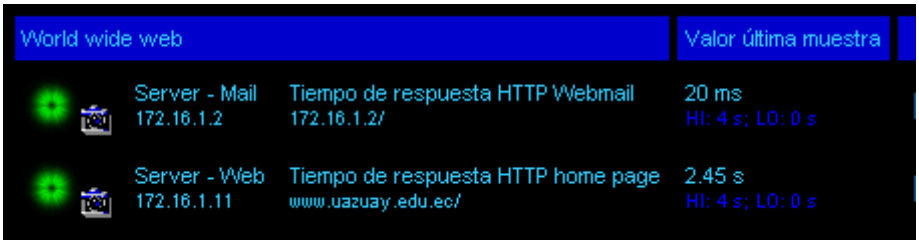
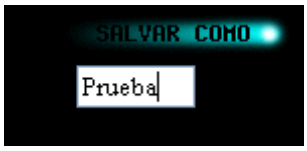




**Figura 7-4** Selección de servicios www

Luego vamos a **VistasUsr** -> **Usuario**, completamos el nombre de la vista (Vista Tráfico) y oprimimos **SALVAR COMO**


**Figura 7-5** Visualización de las variables seleccionadas




Finalmente aparece en el menú superior horizontal la nueva vista de usuario.

## *7.2* Otras opciones del menú vistas de usuario

Las opciones **ACTUALIZAR**, **VACIAR** y **ELIMINAR** que aparecen a la derecha de la pantalla permiten lo siguiente:

### 7.2.1 ACTUALIZAR

Permite quitar de la vista aquellas variables que no estén marcadas en el check box.

Para quitar de una vista a una variable, debemos quitar el tilde haciendo click en el check box correspondiente y luego hacer click en **ACTUALIZAR.**

Esta opción NO permite quitar todas las variables de la vista, siempre queda al menos una variable en la vista.

### 7.2.2 VACIAR

Permite quitar todas las variables de una vista sin necesidad de hacer click sobre los check box.

### 7.2.3 ELIMINAR

Permite eliminar la vista de usuario.

## *7.3 Utilidades de las vistas de usuario*

Las vistas de usuario facilitan las siguientes tareas:

- correlacionar datos que normalmente se ven en menúes diferentes
- confeccionar reportes de un grupo limitado de variables
- ver en una sola pantalla las variables que son de mayor interés
- al poder tener varias vistas, cada una puede servir a un fin específico

# CAPITULO VIII

# Alarmas

Esta sección permite ver las alarmas y agruparlas según el tiempo que las mismas llevan en dicho estado.

El menú superior horizontal muestra 3 opciones: Vigentes, 1hora y 2horas

## *8.1 Vigentes*

Muestra todas las alarmas

## *8.2 1hora*

Muestra aquellas alarmas que están hace más de una hora

## *8.3 2horas*

Muestra aquellas alarmas que están hace más de dos hora

Por lo tanto, si estado de alarma se resuelve dentro de la primera hora, esta alarma no se reflejará en los menúes de 1hora y 2horas.

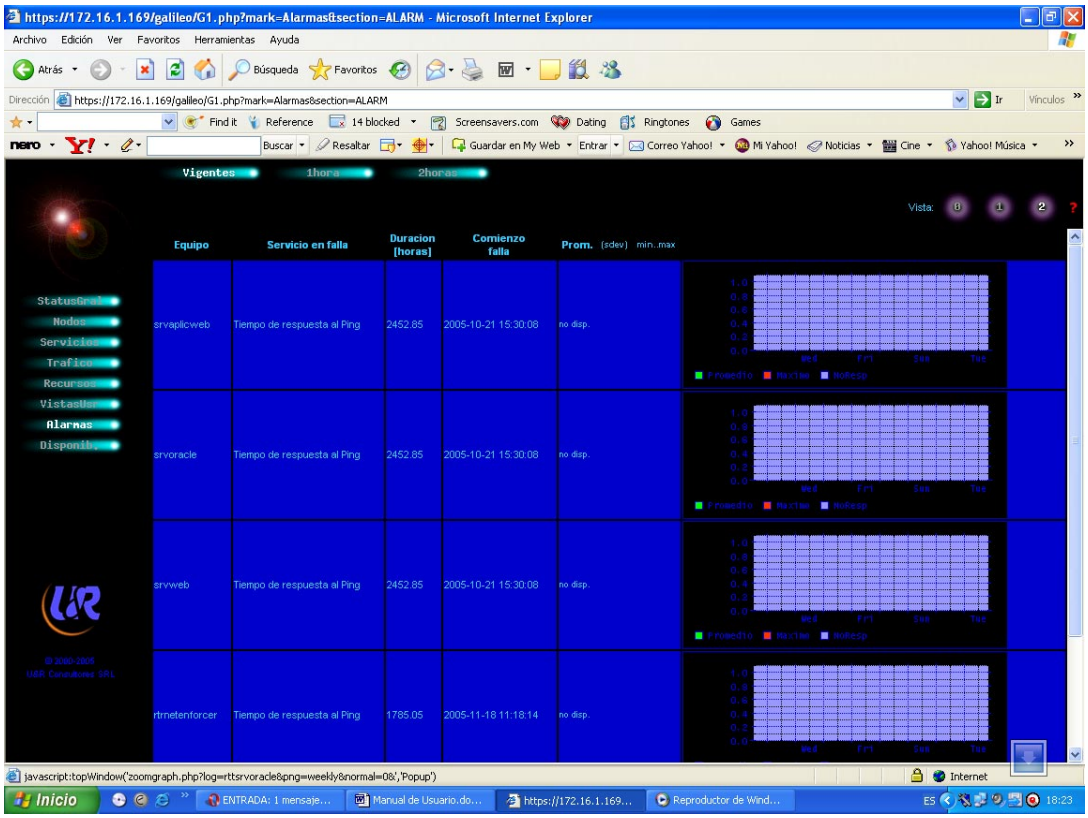



**Figura 8-1** Vista de la pantalla de **Alarmas** -> **Vigentes**

En la pantalla de ejemplo vemos que las variables están en situación de alarma y también podemos ver el gráfico de dicha variable (vista 2).

Nota: Esta función prácticamente no se la utiliza, inicialmente tenía otro objetivo la que ha dejado de existir.

# CAPITULO XI

## Disponibilidad

Este menú muestra la disponibilidad de los nodos y sus respectivos servicios y recursos.

El menú superior horizontal permite ver la disponibilidad de los últimos 10, 30 o 90 días.

Con las vistas 0, 1 y 2 podemos ampliar el nivel de detalle a visualizar

Con el botón **PDF** podemos generar un archivo con la información de disponibilidad.

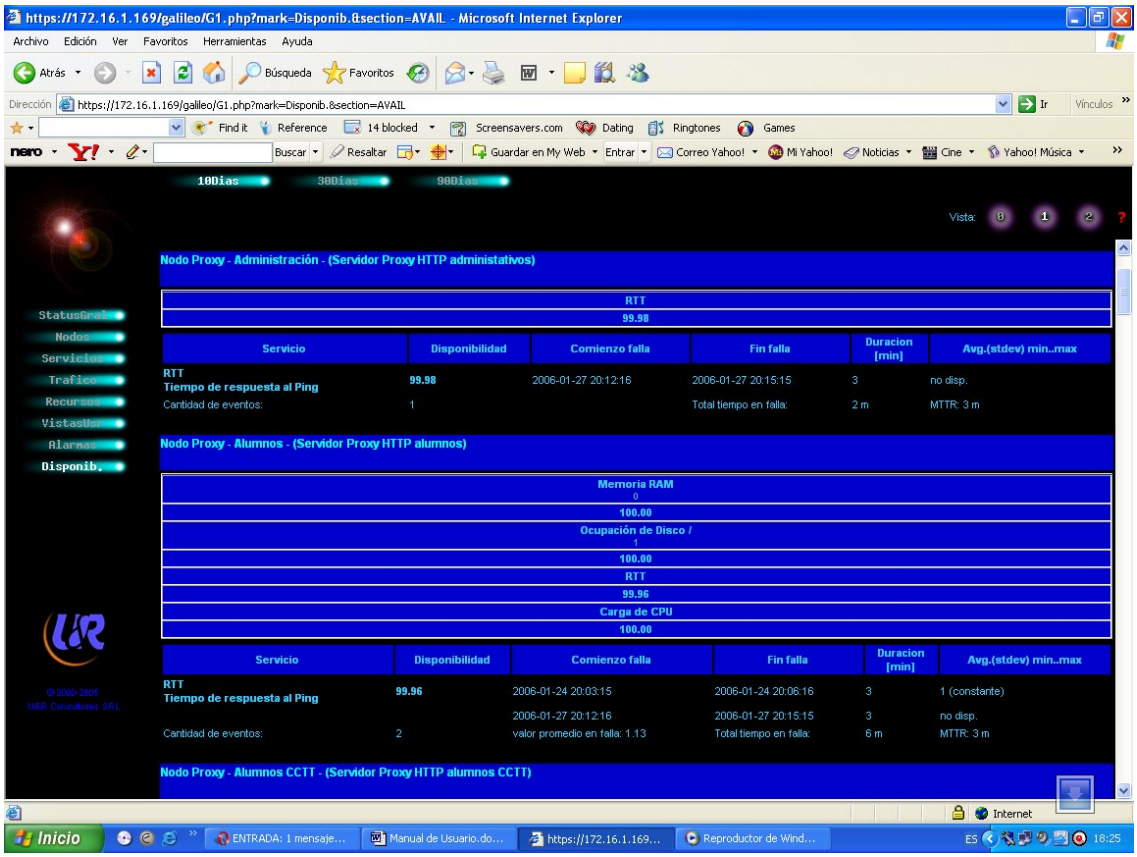



**Figura 9-1** Disponibilidad de los nodos

# CAPITULO X

# ADMINISTRACIÓN Y CONFIGURACIÓN

La administración del sistema de “Monitoreo Administrado Galileo” es en forma manual, al momento no existe un ambiente desarrollado para su configuración, toda la administración es remota, vía https, en donde un equipo de desarrollo que reside en Buenos Aires - Argentina, tiene privilegios para levantar gestionar variables de servicios y/o recursos. Esto se lo hace manipulando directamente la base de datos, mediante phpMyAdmin 2.2.7, el que sirve de gestor con la base de datos MySql 3.23.56.

## *10.1 Arquitectura*

Galileo tiene dos partes prácticamente independientes:

- Subsistema de muestreo
- Subsistema de presentación y control

Toda la configuración y la mayor parte del estado de Galileo se guardan en una base de datos SQL, implementada con mysql. Esta BD es accedida por ambas partes de Galileo.

### 10.1.1 Subsistema de muestreo

A intervalos regulares de tiempo el cron daemon activa un programa php que consulta la base de datos, y en función de su contenido genera un archivo de configuración.

A continuación dicho programa envía un sonido al device de audio, y luego llama al programa mrtg, escrito en perl. El mrtg efectúa todos los muestreos en función de su archivo de configuración.

De esta manera, el mrtg muestrea lo que ha sido configurado en la BD sql.

Nosotros usamos tres de estos programas: un muestreador de dns servers llamado gDnsProbe, uno para servicios http llamado gWgetProbe y otro que realiza ping llamado gPingProbe. En los dos primeros casos los muestreadores obtienen el tiempo de respuesta del servicio, en el caso del muestreador que realiza ping devuelve el promedio y el peor valor de una secuencia de muestras, cuando no se recibe respuesta se devuelve una indicación de no accesibilidad. Este último caso se representa por un valor -1.

EL programa mrtg permite activar el mecanismo de alarmas y/o almacenar los valores de las muestras en la BD sql.

Actualmente la alarma se genera cuando el valor de la muestra cruza un threshold (fuera de rango) hacia un valor peor. Peor significa que se aparta del óptimo, especificado en la BD sql en el campo bestlevel. Cuando una alarma se dispara, se produce un trap snmp dirigido al mismo galileo.

El mrtg inserta el valor muestreado en un archivo de tipo RRD (round robin database). Estos archivos se manipulan y mantienen los valores muestreados con distintas granularidades temporales. Cada variable muestreada tiene un archivo rrd asociado. Todos los archivos rrd se encuentran en el directorio /var/galileo. Todos los gráficos que muestra galileo salen exclusivamente de los datos contenidos en estos rrd.

### 10.1.2 Subsistema de presentación

Galileo utiliza un esquema de doble menu y vistas.

En la barra vertical izquierda existe un menu que permite seleccionar lo que llamaremos un viewgroup. El usuario selecciona un viewgroup, y los miembros del viewgroup (que llamaremos views) aparecen en el menú superior.

Cuando el usuario presiona el cartel del view, el sistema envia el view al sector inferior derecho de la pantalla (el frame mas grande).

Los views tienen modificadores: los números del 0 al 4 que aparecen a la derecha del menu superior. Estos modificadores sirven para variar en cierta medida la cantidad, el detalle o la granularidad temporal de los gráficos o datos que proporciona el view.

En la tabla viewgroups hay un entry para cada uno de ellos, y en la viewitems existen tres campos view, section y samplerid, cada entry en esta tabla indica que variable se debe incluir en esa view y section (viewgroup).

## *10.2 Disposición de archivos*

Todos los archivos relacionados con Galileo se encuentran en el directorio /usr/local/galileo. Dentro de este, hay 5 subdirectorios:

**bin**, donde están los programas ejecutables (ya sean estos scripts o binarios);
**etc,** donde están archivos de configuración,
**www,** donde se encuentra la totalidad del árbol accesible mediante el http daemon
El contenido de este árbol es mayormente archivos php, que se interpretan al ser accedidos. Esto los convierte en ejecutables, pero que no están en bin.
**doc,** allí se ubicará el manual cuando esté hecho.
**mibs,** allí se ubican las mibs accesibles al snmp.

## *10.3 Administración y configuración de Galileo*

El menú de configuración se accede a través del URL
https://<server fqdn>/galileo/admin.php

En este menú se incluyen las siguientes opciones:

**10.3.1 Objetos:** para modificar los objetos (modifican las tablas server y server_service) y para administrar las distintas vistas

**10.3.2 AdminBD:** para acceder directamente a la guia de manejo de la BD (usar con cuidado).

**10.3.3 Tts:** (time to sample) para inspeccionar el tiempo necesario para una ronda de muestreo de Galileo. Este tiempo debe ser muy inferior al intervalo de muestreo de 3 minutos

**10.3.4 Usuarios:**Un item para agregar usuarios al sistema (los usuarios de galileo se registran en la BD pero no en el UNIX). Para agregar un usuario, insertar un registro con el username y el password, usando para éste la función encrypt de mysql. Por ejemplo:

```
INSERT INTO user_data (username, passwd)
  VALUES ('pepe', encrypt('noteladire') );
```

Un item para bajar el certificado de la Aut. Certificante de UyR, para autenticar automáticamente las conexiones https.

**10.3.3 Packs**: espacio para colocar archivos útiles que el server pueda almacenar. Por ejemplo, allí se coloca el ejecutable del putty para Windows, que permite acceder al server mediante ssh.

La configuración de las variables a muestrear se realiza insertando registros en las tablas “server”, “service” y “server_service”

En la primera van los datos que caracterizan al nodo a muestrear, fundamentalmente el address de IP y el nombre del elemento administrado.

| name | abrev | ipaddr | comment |
|---|---|---|---|
| galileo.uyr.com.ar | galileo | 127.0.0.1 | Linux galileo.uyr.com.ar 2.4.2-2 #1 Sun A |
| Server - Web | srvweb | 172.16.1.11 | Servidor de HTTP |
| Server - Aplicaciones Web | srvaplicweb | 172.16.1.12 | Servidor de HTTP de aplicaciones WEB |
| Proxy - Administración | pxyadmin | 172.16.1.166 | Servidor Proxy HTTP administativos |
| Server - Mail | srvmail | 172.16.1.2 | Servidor de e-mail |
| Server - Oracle | srvoracle | 172.16.1.9 | Servidor de aplicaciones Oracle |
| Switch - Computo1 | swcomputo1 | 172.16.2.1 | Switch 3com 4228 |
| Switch - Computo2 | swcomputo2 | 172.16.2.10 | Switch 3com 4228 |
| Switch - Fac. Medicina p1 | swfacmedip1 | 172.16.2.11 | Switch 3com 4228 |
| Switch - Fac. Medicina p2 | swfacmedip2 | 172.16.2.12 | Switch 3com 4228 |
| Switch - Internet1 | swinternet1 | 172.16.2.2 | Switch 3com 4228 |
| Switch - Internet2 | swinternet2 | 172.16.2.3 | Switch 3com 4228 |
| Switch - Administración Central 1 | swadmcent1 | 172.16.2.4 | Switch 3com 4228 |
| Switch - Fac. Diseño | swfacdise | 172.16.2.5 | Switch 3com 4228 |
| Switch - Fac. Administracion | swfacadmin | 172.16.2.6 | Switch 3com 4228 |
| Switch - Fac. CCTT | swfaccctt | 172.16.2.8 | Switch 3com 4228 |
| Switch - Administración Central 2 | swadmcent2 | 172.16.2.9 | Switch 3com 4228 |
| rtrnetenforcer | rtrnetenforcer | 192.168.1.1 | Administrador de Ancho de Banda |
| Proxy - Alumnos | pxyalumnos | 192.168.1.166 | Servidor Proxy HTTP alumnos |
| Proxy - Alumnos CCTT | pxyalumnoscctt | 192.168.1.6 | Servidor Proxy HTTP alumnos CCTT |
| Proxy - Laboratorios | pxylab | 192.168.1.8 | Servidor Proxy HTTP Laboratorios |
| Router Cisco | rtrcisco | 192.188.47.3 | Router Internet Cisco 2800 |

La segunda tabla (service) se usa para definir el tipo de variable (cómo se obtiene: por snmp, por wget, por el probe de dns o el de ping), el oid basico (sin incluir ids de instancia).

| name | abrev | comment | samplertype | unitname |
|---|---|---|---|---|
| BytesPerd | BytesPerd | Diferencia de bytes/seg | dif | B/s |
| dnsa1 | DNSa | DNS autoritativo | dns | s |
| dnsc1 | DNSc | DNS cache | dns | s |
| lnxdsk1 | DSK1 | Ocupacion disco | oid | B |
| ntdsk1 | DSK3 | Ocupacion disco (NT4) | oid | MB |
| Flows | flows | Netflows | flows | B/s |
| iisbt | iisbt | Bytes transferidos por IIS | oid | b. |
| iisft | iisft | Files transferidos por IIS | oid | f. |
| Tiempo desde ultima | KPA | Periodo recepcion keepalives | keepa | [m] |
| lnxload1 | LOAD1 | Carga en procesadores | oid | % |
| Variable controlada r | MAN | Estado variable controlada manualmente | manual | |
| lnxmem1 | MEM1 | Memoria real disponible | oid | B |
| ntmpag | ntmpag | NT MemoryPagesPerSec | oid | p/s |
| ntppni | ntppni | NT %ProcessorNotIdle / %ProcNotIdleInUserMode | oid | % |
| ntpwsvb | ntpwsvb | NT IIS process: Working set, Virtual bytes | oid | [bytes] |
| Ping Round Trip Tim | PINGRTT | ICMP Echo (Ping) Round Trip Time | ping | seg |
| lnxproc1 | PROC1 | Daemons en ejecucion | oid | procs |
| SAMBA | SMB | Filesharing netbios (SAMBA) | NULL | NULL |
| SAMBAP | SPR | PrintSharing netbios (SAMBA) | NULL | NULL |
| SQlQuery | SQL | Consulta SQL | sql | ms |
| stoused | stoused | Ocupacion disco (alloc.units) | oid | GB |
| TBA | TBA | Temperatura ambiente | temp | oC |
| TCP Probe | TCP | Tiempo de respuesta | tcp | s |
| frCircuitOctets | TrCircFR | Trafico en circuito frame relay | oid | kB/s |
| Trafico en interfaz | TrInFW | Trafico en interfaz | oid | kB/s |
| UPS | UPS | APC UPS probe | oid | % |
| UPS100 | UPS100 | upsSecondsOnBattery | oid | s |
| UPS2 | UPS2 | APC UPS slave probe | oid | % |
| WWW | WWW | World wide web | wget | s |
| WWWs | WWWs | World wide web seguro (https) | wget | s |

La tercera (server_service) contiene los datos asociados a la instancia particular (el instance id, valores máximos, threshold para alarmas, etc.).

| samplerid | scale | credential | enabled | server | service | abrev | thresmax | thresmin | maxvalue | laststatus | level |
|---|---|---|---|---|---|---|---|---|---|---|---|
| cpupxyalumnos | 0.01 | uda-snmp | Y | 192.168.1.166 | LOAD1 | Carga de CPU | 4 | 0 | 100 | N/A | -1 |
| dsk1pxyalumnos | 0.001 | uda-snmp | Y | 192.168.1.166 | DSK1 | Ocupación de Disco / | 1,00E+08 | 100000 | 1,00E+08 | N/A | -1 |
| gal12load | 0.01 | asate | Y | 127.0.0.1 | LOAD1 | Load5m | 4 | 0 | 100 | OK | 0.16 |
| mempxyalumnos | 0.001 | uda-snmp | Y | 192.168.1.166 | MEM1 | Memoria RAM | 1,00E+06 | 10000 | 1,00E+06 | N/A | -1 |
| rttpxyadmin | 1000 | | Y | 172.16.1.166 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 0.45 |
| rttpxyalumnos | 1000 | | Y | 192.168.1.166 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 1.839 |
| rttpxyalumnoscctt | 1000 | | Y | 192.168.1.6 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 4.097 |
| rttpxylab | 1000 | | Y | 192.168.1.8 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 3.309 |
| rttrtrcisco | 1000 | | Y | 192.188.47.3 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 3.118 |
| rttrtmetenforcer | 1000 | | Y | 192.168.1.1 | PINGRTT | RTT | 1000 | 0 | 100 | N/A | -1 |
| rttsrvaplicweb | 1000 | | Y | 172.16.1.12 | PINGRTT | RTT | 1000 | 0 | 100 | N/A | -1 |
| rttsrvmail | 1000 | | Y | 172.16.1.2 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 0.178 |
| rttsrvoracle | 1000 | | Y | 172.16.1.9 | PINGRTT | RTT | 1000 | 0 | 100 | N/A | -1 |
| rttsrvweb | 1000 | | Y | 172.16.1.11 | PINGRTT | RTT | 1000 | 0 | 100 | N/A | -1 |
| rttswadmcent1 | 1000 | | Y | 172.16.2.4 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 3.526 |
| rttswadmcent2 | 1000 | | Y | 172.16.2.9 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 2.702 |
| rttswcomputo1 | 1000 | | Y | 172.16.2.1 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 2.67 |
| rttswcomputo2 | 1000 | | Y | 172.16.2.10 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 5.561 |
| rttswfacadmin1 | 1000 | | Y | 172.16.2.6 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 2.38 |
| rttswfaccctt | 1000 | | Y | 172.16.2.8 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 3.459 |
| rttswfacdise1 | 1000 | | Y | 172.16.2.5 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 3.607 |
| rttswfacmedicp1 | 1000 | | Y | 172.16.2.11 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 17.336 |
| rttswfacmedicp2 | 1000 | | Y | 172.16.2.12 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 19.965 |
| rttswinternet1 | 1000 | | Y | 172.16.2.2 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 3.288 |
| rttswinternet2 | 1000 | | Y | 172.16.2.3 | PINGRTT | RTT | 1000 | 0 | 100 | OK | 4.153 |
| smtpsrvmail | 1000 | | Y | 172.16.1.2 | TCP | Servicio SMTP | 1000 | 0 | 100 | OK | 0.3201 |
| trfrtrcisco | 1 | uda-snmp | Y | 192.188.47.3 | TrInFW | Trafico Internet | 100000 | 0 | 100000 | OK | 82915.9 |
| wwwsrvmail | 1 | | Y | 172.16.1.2 | WWW | Webmail www.uazuay.edu.ec | 4 | 0 | 100 | OK | 0.011 |
| wwwsrvweb | 1 | | Y | 172.16.1.11 | WWW | Home page www.uazuay.edu.ec | 4 | 0 | 100 | OK | 0.222 |

Ver el Anexo A, que muestra la BD completa.

# CONCLUSIONES

Cabe destacar que no se ha tenido la oportunidad de dar mantenimiento (alta, baja y ajuste de nuevos elementos a administrar) ni emplear variables de monitoreo limitándonos a manipular lo existente. Además no existe un ambiente desarrollado para su administración.

La sección de Alarmas inicialmente ha tenido otra función que por el momento no se la utiliza, es por ello que no alcanza a mostrar información relevante.

Con Galileo, los Resúmenes nos permite visualizar el estado de la totalidad de la infraestructura mediante un golpe de vista los que se renuevan periódicamente, además de todo el entorno gráfico que nos permiten percibir la situación real de la infraestructura y establecer tendencias. Para todas las variables se almacenan promedios diarios, semanales, mensuales y anuales, con distinta granularidad.

Con la vista de los nodos del campus podemos conocer las características importantes y funciones que desempeña cada equipo monitoreado.

Además hemos sistematizado algunas otras características atendiendo su utilidad

## Garantiza los servicios en la red informática

Permite controlar y medir términos de:

- Disponibilidad
- Tiempos de respuesta
- Utilización
- Facilita el diagnóstico y la planificación
- Controla y mide el tráfico de enlaces

## Reducir costos por incremento de la eficiencia y la productividad

Aislamiento y prevención de los “cuellos de botella”

Maximiza la disponibilidad de los sistemas

Simplifica y centraliza la administración de redes

Análisis del pasado, presente y futuro de la performance del ambiente de tecnologías de la información

## Mantenimiento

Requiere mantenimiento posterior frecuente

Ata / Baja / Ajuste ante nuevos elementos a administrar

Reconfiguración de niveles de alarmas

Requiere esfuerzo para producir reportes

Requiere de interpretación de los datos

## Necesidad de mantener la plataforma funcionando

La falta de mantenimiento causa que la plataforma sea cada vez menos útil

La falta de utilidad causa que la plataforma caiga en desuso

Si la función de management no se lleva a cabo, la infraestructura es más vulnerable y el servicio se compromete

# Recomendaciones

Galileo nos brinda la oportunidad de visualizar el estado total de la infraestructura además de un entorno gráfico donde podemos percibir su situación real, pero si la función management no se lleva a cabo puede caer en desuso volviéndose cada vez menos útil.

En esta plataforma de monitoreo existen todavía algunas fallas al momento de interpretar los reportes por lo que se sugiere una periódica actualización, se tiene entendido que este update corrige algunas falencias tales como presentar disponibilidades 100% cuando este no le responde a Galileo.

Consideramos una herramienta importante los reportes de disponibilidad de nodos de acuerdo a intervalos de tiempo y criterios, los que me permite documentar un historial de eventos para cada elemento de la red que necesite.

Es recomendable también que el estudio de esta herramienta parta de las fuentes, como funciona, su administración, detalle de bases de datos, herramientas utilizadas para su creación además del estudio del protocolo SNMP (Simple Network Management Protocol), protocolo definido por los comités técnicos de Internet para ser utilizado como una herramienta de gestión de los distintos dispositivos en cualquier red.

## Anexo A

Structure for table **alarm**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| alarm | primary key | cod | integer (11) |
| | | server | char (50) |

Structure for table **availty**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| availty | primary key | cod | integer (5) |
| | | status | char (20) |
| | | tstart | date time |
| | | tstop | date time |
| | | failtype | char (10) |
| | key | samplerid | char (40) |
| | | sampleavg | float |
| | | samplesdev | float |
| | | samplemin | float |
| | | samplemax | float |
| | | nsamples | integer (11) |
| | | duration | integer (11) |

Structure for table **confitems**

| TABLA | CAMPO | TIPO |
|---|---|---|
| confitems | fieldname | varchar (255) |
| | inputtag | varchar (255) |
| | help varchar | varchar (255) |
| | seq int | integer (11) |
| | service | varchar (255) |
| | label | varchar (255) |
| | required | char (1) |
| | confset | varchar (255) |

Structure for table **db**

| TABLA | CAMPO | TIPO |
|---|---|---|
| db | abrev | varchar (50) |
| | dbname | varchar (50) |
| | cfgfile | varchar (255) |

Structure for table **frameitems**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| frameitems | unique key prim | frame | char (10) |
| | | type | char (10) |
| | unique key prim | seq | integer (11) |
| | | item | char (255) |

Structure for table **galiconf**

| TABLA | CAMPO | TIPO |
|---|---|---|
| galiconf | parm | char (50) |
| | pval | char (255) |
| | pdefault | char (255) |

Structure for table **groupitems**

| TABLA | CAMPO | TIPO |
|---|---|---|
| groupitems | name | char (255) |
| | viewgroup | char (255) |
| | type | char (255) |
| | seq | integer (11) |
| | selector | char (255) |
| | maxcolumns | integer (11) |

Structure for table **menuitems**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| menuitems | primary key | cod | integer (11) |
| | | menu | varchar (10) |
| | | seq | integer (11) |
| | | label | varchar (50) |
| | | abrev | varchar (50) |
| | | alt | varchar (50) |
| | | icon | varchar (50) |
| | | color | varchar (10) |
| | | size | varchar (5) |
| | | url | varchar (250) |
| | | target | varchar (50) |

Structure for table **oid**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| oid | primary key | cod | char (100) |
| | | denom | char (255) |
| | | ogroup | char (10) |

Structure for table **oidgroup**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| oidgroup | primary key | cod | char (10) |
| | | denom | char (255) |

Structure for table **sampler**

| TABLA | CAMPO | TIPO |
|---|---|---|
| sampler | tstart | date time |
| | tstop | date time |
| | duration | integer (11) |
| | period | integer (11) |

Structure for table **samplertype**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| samplertype | primary key | cod | char (10) |
| | | denom | char (255) |

Structure for table **server**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| server | primary key | ipaddr | char (20) |
| | | name | char (50) |
| | | abrev | char (50) |
| | | comment | char (255) |
| | | seq | integer (11) |
| | | syslocation | char (255) |
| | | sysname | char (255) |
| | | sysdescr | char (255) |
| | | tstamp | timestamp (14) |
| | | monitored | char (10) |
| | | incview | char (255) |

Structure for table **server_service**

| TABLA | LLAVE | CAMPO | TIPO | |
|---|---|---|---|---|
| server_service | primary key | samplerid | varchar (50) | |
| | | parm1 | varchar (255) | |
| | | parm2 | varchar (255) | |
| | | scale | float | |
| | | interv | float | |
| | | randze | char (1) | |
| | | credential | varchar (255) | |
| | | enabled | char (1) | |
| | | handler | varchar (50) | default '14all.cgi' |
| | | type | varchar (50) | |
| | | alert | varchar (50) | |
| | | server | varchar (50) | |
| | | service | varchar (50) | |
| | | seq | integer (11) | |
| | | abrev | varchar (50) | |
| | | comment | varchar (50) | |
| | | bestlevel | float | |
| | | thresmax | float | |
| | | thresmin | float | |
| | | maxvalue | float | |
| | | laststatus | varchar (50) | |
| | | level | float | |
| | | stamp | timestamp (14) | |
| | | slope | float | |
| | | rawsample | double | |
| | | hostview | varchar (50) | |

Structure for table **service**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| service | | name | varchar (50) |
| | primary key | abrev | varchar (50) |
| | | comment | varchar (255) |
| | | samplertype | varchar (10) |
| | | unitname | varchar (50) |
| | | parmOID1 | varchar (255) |
| | | parmOID2 | varchar (255) |
| | | seq | integer (11) |
| | | cod | integer (11) |
| | | gauge | char (1) |
| | | absolute | char (1) |
| | | magnit1 | varchar (255) |
| | | magnit2 | varchar (255) |

Structure for table **user_info**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| user_info | primary key | user_name | char (30) |
| | | user_passwd | char (20) |
| | | user_group | char (10) |

Structure for table **viewgroup**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| viewgroup | | name | varchar (50) |
| | primary key | abrev | varchar (50) |
| | | comment | varchar (50) |
| | primary key | section | varchar (50) |
| | | seq | integer (11) |
| | | viewhandler | varchar (255) |
| | | numdetails | integer (11) |
| | | typesel1 | varchar (50) |
| | | typesel2 | varchar (50) |
| | | typesel3 | varchar (50) |
| | | groupby | varchar (50) |

Structure for table **viewitems**

| TABLA | LLAVE | CAMPO | TIPO |
|---|---|---|---|
| viewitems | primary key | view | varchar (50) |
| | primary key | section | varchar (50) |
| | primary key | samplerid | varchar (50) |

# BIBLIOGRAFIA


1. Galileo Estación de monitoreo Configuración
   Autor: U&R Consultores
   Publicación: 2003-03-12

2. https://172.16.1.169/galileo/G1.php
   Servidor Galileo de la Uda
   Fecha de Ingreso: 20/Ene/2006

3. http://www.uyr.com.ar/typo3/
   Galileo, servicio de red administrado
   Fecha de Ingreso: 15/Ene/2006

4. http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/index.php
   Portal de los Ingenieros en Informática
   Fecha de Ingreso: 12/Dic/2005

5. http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/
   Guía de Administración con redes en Linux
   Fecha de Ingreso: 12/Dic/2005

6. http://www.mty.itesm.mx/dgi/programas/msc/promocion/node8.html
   Administración de Redes
   Fecha de Ingreso: 12/Dic/2005

7. http://www.microsoft.com/spanish/MSDN/estudiantes/redes/gestion/default.asp
   Microsoft MSDN Estudiantes
   Fecha de Ingreso: 12/Dic/2005

8. http://www.gestiopolis.com/recursos/documentos/fulldocs/ger/adredesis.htm
   Administración de redes con enfoque de Ingeniería Social
   Fecha de Ingreso: 12/Dic/2005

9. http://www.itlp.edu.mx/publica/tutoriales/telepro/t7_4.htm
   Tutorial de Teleproceso
   Fecha de Ingreso: 12/Dic/2005

**UNIVERSIDAD DEL AZUAY**

**FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN**

**ESCUELA DE INGENIERÍA DE SISTEMAS**

**MONOGRAFÍA PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERO DE SISTEMAS**

**TEMA**

***"GESTIÓN DE MONITOREO DE REDES MEDIANTE LA HERRAMIENTA GALILEO EN LA UNIVERSIDAD DEL AZUAY"***

**INTEGRANTES:**

**Sara Paola López Q.**
**Diego Felipe Merchán F.**

**Cuenca, 20 de Diciembre del 2005**

Cuenca, 20 de Diciembre de 2005

**Señor Economista**
**Luís Mario Cabrera**
**DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN DE LA UNIVERSIDAD DEL AZUAY**
**Ciudad**

Señor Decano:

Nosotros, Sara Paola López Quezada y Diego Felipe Merchán Flores, estudiantes de la Escuela de Ingeniería de Sistemas, nos dirigimos a usted y por su digno intermedio al Honorable Consejo de la Facultad, para solicitarle la aprobación del Diseño de la Monografía con el tema: *"GESTIÓN DE MONITOREO DE REDES MEDIANTE LA HERRAMIENTA GALILEO EN LA UNIVERSIDAD DEL AZUAY",* requisito previo a la obtención del Título de Ingeniero de Sistemas para los estudiantes que han realizado el Curso de Graduación en la Universidad del Azuay – Cuenca, así como la designación del Director.

El Diseño de la Monografía cuenta con el informe favorable del Director de Escuela Ing. Oswaldo Merchán y del Ing. Pablo Esquivel profesor de la Facultad.

Por la favorable acogida que brinde a la presente, anticipamos nuestros agradecimientos,

**Atentamente,**

**Paola López Q.** **Felipe Merchán F.**

Cuenca, 20 de Diciembre de 2005

**Señor Economista**
**Luís Mario Cabrera**
**DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN DE LA UNIVERSIDAD DEL AZUAY**
**Ciudad**

Señor Decano:

Quienes suscribimos comunicamos a usted que hemos procedido a revisar el Diseño de la Monografía presentado por la Sra. Sara Paola López Q. y el Sr. Felipe Merchán F., estudiantes de la Escuela de Ingeniería de Sistemas, con el tema: *"GESTIÓN DE MONITOREO DE REDES MEDIANTE LA HERRAMIENTA GALILEO EN LA UNIVERSIDAD DEL AZUAY",* como requisito previo a la obtención del Título de Ingenieros de Sistemas, sobre la base del cual emitimos un informe favorable y salvando su mejor criterio, se recomienda su aprobación.

**Atentamente,**

**Ing. Oswaldo Merchán M.**
**Director de Escuela**

**Ing. Pablo Esquivel L.**
**Profesor**

# DISEÑO DE MONOGRAFÍA

## 1. Título del proyecto

*"GESTIÓN DE MONITOREO DE REDES MEDIANTE LA HERRAMIENTA GALILEO EN LA UNIVERSIDAD DEL AZUAY"*

## 2. Selección y delimitación del tema

**Contenido:** El tema se desarrollará en el área de investigación y configuración de la aplicación Galileo mediante el servicio de Internet https.
**Espacio:** El presente proyecto se realizará en la ciudad de Cuenca
**Tiempo:** El proyecto abarcará un plazo de 6 semanas.

## 3. Descripción del objetivo de estudio

El objetivo es el de investigar y analizar el funcionamiento de una aplicación de monitoreo de redes denominada Galileo, instalada en un equipo servidor de la Universidad del Azuay, para poder llegar a demostrar con una aplicación práctica todo el rendimiento que nos pueda prometer.

## 4. Resumen del proyecto

El trabajo que se presenta es una aplicación denominada GALILEO que fue instalada en el departamento de redes internas de la Universidad del Azuay, un sistema de monitoreo que permite conocer el estado actual e histórico de los equipos y servicios monitoreados, el acceso a esta información se realiza mediante un browser. Este permite enviar mensajes de alarma frente a fallas en los equipos monitoreados. Además correlacionar los datos recolectados y determinar las causas de las fallas. Se pueden generar reportes automáticos con los datos recolectados por Galileo. Sirve como herramienta donde se puede ver la tendencia de las variables monitoreadas y evitar fallas antes que las mismas se produzcan.

## 5. Introducción

En este siglo de grandes avances tecnológicos, en donde el uso de las computadoras ha sido generalizado. Las redes de computadoras han tenido un crecimiento sostenido en los últimos años, en donde cada vez un mayor número de empresas e instituciones educativas, dependen gran número de sus procesos y operatividad a estas.

Esta creciente expansión de las redes de comunicaciones ha hecho necesario la adopción y el desarrollo de herramientas de seguridad que protejan tanto los datos transmitidos como el acceso a los elementos de la red de los posibles ataques que pueda sufrir.

La administración de redes se está convirtiendo en una creciente y compleja tarea debido a la variedad de tipos de red y a la integración de diferentes medios de comunicación. A medida que las redes se vuelven más grandes, más complejas y más heterogéneas, el costo de su administración aumenta. En tal situación, son necesarias herramientas automáticas para dar el soporte requerido por administradores humanos, recolectando información acerca del estatus y el comportamiento de los elementos de red.

Ahora ya no se trata solo de mantener operativos los nodos como su de entes individuales se tratase, el nuevo objetivo debe ser mantener el sistema como un todo, como un solo ente. Se trata de nuestro mundo artificial en el que las iteraciones entre los distintos nodos se vuelven mucho más ricas y complicadas

## 6. Situación actual y futura

**Situación Actual**

En la actualidad esta aplicación Galileo está instalada en una computadora del departamento de redes internas de la UDA, con una interfase de red monitoreando el estado los equipos. Al momento no reporta ningún tipo de información por falta de su gestión.

**Situación Futura**

Se planea obtener el mayor provecho de esta herramienta que permite conocer el estado actual e histórico de los equipos y servicios monitoreados, de donde obtendremos parámetros para actuar frente a fallas, determinar sus causas y evitarlas antes de que se produzcan

## 7. Justificación e impacto

**Justificación**

La decisión de abarcar este tema fue por la necesidad de gestionar esta herramienta de monitoreo Galileo instalada por la empresa Argentina U&R Consultores SRL, con el que se pretende llevar un control sobre todos los nodos del campus Universitario y así poder planear acciones en caso de fallas de los equipos monitoreados.

**Impacto Tecnológico**

El impacto tecnológico de la nueva herramienta de monitoreo que se necesita debe ser capaz de ir más allá de la mera administración para proporcionar una gestión totalmente autónoma, capaz de adaptarse a la situación en la que se encuentre el sistema en cada momento.

# 8. Objetivos

**Objetivo General**

- Monitorear los nodos del campus de la Universidad del Azuay mediante la herramienta Galileo.

**Objetivo Específico**

- Averiguar el estado actual de los equipos
- Visualizar todos los nodos (equipos) que están siendo monitoreados
- Obtener una vista de los nodos monitoreados en función de los servicios que prestan y del tráfico en sus interfaces de red
- Obtener una vista del estado de los recursos de los nodos monitoreados
- Crear vistas propias a cada usuario de Galileo
- Ver las alarmas y agruparlas
- Mostrar la disponibilidad de los nodos
- Manual de Uso

# 9. Marco Teórico

Para poder aplicar nuestro proyecto hemos visto la necesidad de tener conocimiento de los siguientes conceptos:

**Monitorización**

La monitorización de red permite solucionar y prevenir muchos de los problemas que pueden presentarse en la administración de la misma: cuellos de botella, sobrecarga de usuarios, intrusiones, etc. Por lo tanto, es importante estar siempre informado de los datos que circulan por nuestro sistema.

**Procesos distribuidos**

Las aplicaciones distribuidas se basan en los conceptos de cooperación y compartición de recursos a través de la red. Una aplicación distribuida es una aplicación que utiliza o accede a recursos de varios sistemas.

Un sistema distribuido puede construirse de forma que sea más fiable que un sistema centralizado, al no depender de un solo nodo y facilitar la replicación de funciones y de datos en los distintos nodos de la red

**Gestión de red**

Al incrementarse la complejidad de las redes se hace necesario el disponer de potentes sistemas de gestión de red que proporcionen herramientas que permitan a los administradores un control relativamente sencillo de todas las operaciones relacionadas con las redes.

Cualquier red corporativa debe estar correctamente administrada con el objetivo de asegurar a sus usuarios su utilización. QoS es una tecnología que permite garantizar a los clientes de red el correcto funcionamiento de la misma, por otra parte, la monitorización del tráfico nos servirá para evitar problemas, o en el peor de los casos, para ayudarnos a solucionarlos.

**Seguridad en las redes**

Evidentemente las redes, como otros sistemas son susceptibles a múltiples ataques que pueden distorsionar el efecto de la información transmitida o capturarla simplemente. Al aumentar la complejidad de las redes se hace cada vez más patente la necesidad de articular mecanismos de seguridad y protección.

## 10. Contenidos

Puntos a analizar en este contenido:

**1 Introducción General**
- **1.1** Generalidades de Galileo
- **1.2** Ingreso al sistema
- **1.3** Pantalla Principal

**2 Estado General**
- **2.1** Aumento del detalle de la información visualizada
- **2.2** Botones de vista
- **2.3** Reportes, Disponibilidad y Gráficos

**3 Nodos**
- **3.1** Función
- **3.2** Dirección IP

**4 Servicios**
- **4.1** http
- **4.2** Mail
- **4.3** Botones de vista
- **4.4** Reportes, Disponibilidad y Gráficos

**5 Trafico**

- **5.1** Servers
- **5.2** Switches
- **5.3** Tráfico
- **5.4** Botones de vista
- **5.5** Reportes, Disponibilidad y Gráficos

**6 Recursos**

- **6.1** Ocupación de disco
- **6.2** Carga de procesadores
- **6.3** Memoria real disponible
- **6.4** Botones de vista
- **6.5** Reportes, Disponibilidad y Gráficos

**7 Vistas de usuario**

- **7.1** Crear vistas distintas de usuario
- **7.2** Utilidades de las vistas de usuario
- **7.3** Botones de vista
- **7.4** Reportes, Disponibilidad y Gráficos

**8 Alarmas**

- **8.1** Vigentes
- **8.2** Una Hora
- **8.3** Dos Horas
- **8.4** Botones de vista

**9 Disponibilidad**

- **9.1** 10 días
- **9.2** 30 días
- **9.3** 90 días
- **9.4** Botones de vista
- **9.5** Reportes

## 11. Procedimientos metodológicos

Para la recopilación de la información nos basaremos en:

- Investigación en Internet
- Envíos de material fuente vía correo electrónico por U&R Consultores
- Exploración de aplicación Galileo

## 12. Recursos humanos y técnicos

**Recursos Humanos**

El presente proyecto se hará con la participación del siguiente grupo humano:

| | |
|---|---|
| Investigadores y Desarrolladores: | Sara Paola López Quezada |
| | Diego Felipe Merchán Flores |

Asesoramiento en el proyecto: Ing. Pablo Ronco
Ing. Pablo Esquivel
Ing. Oswaldo Merchán

**Recursos Materiales**

Hardware: El hardware mínimo que se requiere es:
Servidor:

Procesador Intel Pentium IV
Disco Duro: 80 Gb
Ram: 1Gb

Cliente:

Computadores superiores a procesadores Pentium II

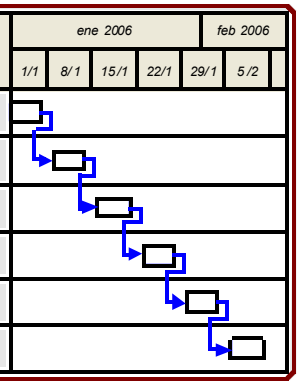
Software:

Sistema Operativo Windows / Linux
Internet Explorer 6.0 / Opera 8.5
Microsoft Office Xp

## 13. Cronograma de actividades

El siguiente cronograma de actividades lo definimos en período de semanas

| Id. | Tareas | Comienzo | Fin | Duraci–n |
|---|---|---|---|---|
| 1 | Estados y Generalidades | 02/01/2006 | 06/01/2006 | 1s |
| 2 | Estudio de Nodos y Servicios | 09/01/2006 | 13/01/2006 | 1s |
| 3 | Estudio de Tr‡fico y Recursos | 16/01/2006 | 20/01/2006 | 1s |
| 4 | Estudio de Vistas de Usuario | 23/01/2006 | 27/01/2006 | 1s |
| 5 | Revisi–n de alarmas y disponibilidad | 30/01/2006 | 03/02/2006 | 1s |
| 6 | Documentaci–n de Sistema | 06/02/2006 | 10/02/2006 | 1s |



## 14. Bibliografía

http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/index.php
Portal de los Ingenieros en Informática
Fecha de Ingreso: 12/Dic/05

http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/
Guía de Administración con redes en Linux
Fecha de Ingreso: 12/Dic/05

http://www.mty.itesm.mx/dgi/programas/msc/promocion/node8.html
Administración de Redes
Fecha de Ingreso: 12/Dic/05

http://www.microsoft.com/spanish/MSDN/estudiantes/redes/gestion/default.asp
Microsoft MSDN Estudiantes
Fecha de Ingreso: 12/Dic/05

http://www.gestiopolis.com/recursos/documentos/fulldocs/ger/adredesis.htm
Administración de redes con enfoque de Ingeniería Social
Fecha de Ingreso: 12/Dic/05

http://www.itlp.edu.mx/publica/tutoriales/telepro/t7_4.htm
Tutorial de Teleproceso
Fecha de Ingreso: 12/Dic/05