



**Administración y Gestión de Redes**  
Lic. en Sistemas de Información

**Laboratorio de REDES**  
Recuperación de Información  
y Estudios de la Web



# Introducción a la Gestión de Redes

## Equipo docente:

Fernando Lorge ([florge@unlu.edu.ar](mailto:florge@unlu.edu.ar))  
Santiago Ricci ([sricci@unlu.edu.ar](mailto:sricci@unlu.edu.ar))  
Alejandro Iglesias ([aaiglesias@unlu.edu.ar](mailto:aaiglesias@unlu.edu.ar))  
Mauro Meloni ([maurom@unlu.edu.ar](mailto:maurom@unlu.edu.ar))  
Patricio Torres ([ptorres@unlu.edu.ar](mailto:ptorres@unlu.edu.ar))

# Presentación

- Objetivos
- Temas principales
- Intro a la gestión de redes/motivación/definiciones
- Modelo de gestión/estándares/protocolos
- Configuración y contabilidad
- Rendimiento
- Seguridad
- Casos de estudio y aplicaciones



# Definición

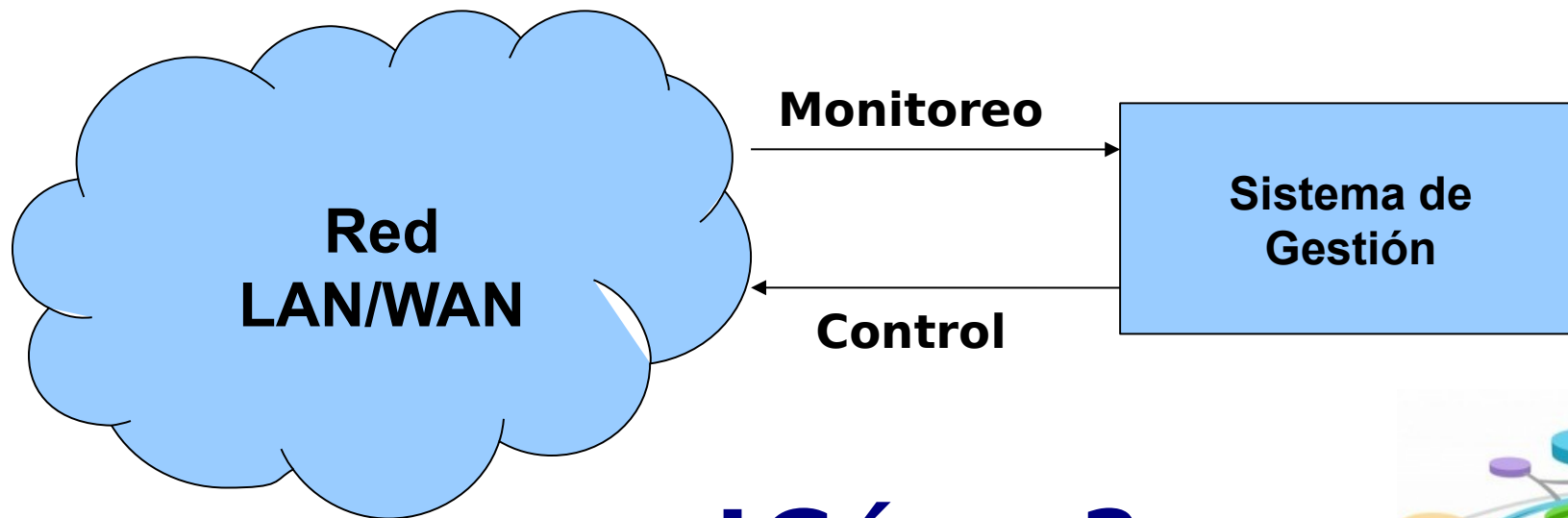
“La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para **monitorizar, probar, sondear, configurar, analizar, evaluar y controlar** los **recursos de la red** para conseguir los requerimientos de tiempo real, desempeño operacional y calidad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

*T.Saydam and T. Magedanz, “From Networks and Network Management into Service and Service Management”, Journal of Networks and Systems Management, Vol 4, No. 4 (Dic 1996).*



# Definición

“Realizar tareas de **inicialización, monitoreo y control** de una red de comunicaciones con el objetivo de que ésta cumpla los **requisitos de los usuarios** para los que fue construida.”



## ¿Cómo?



# Introducción

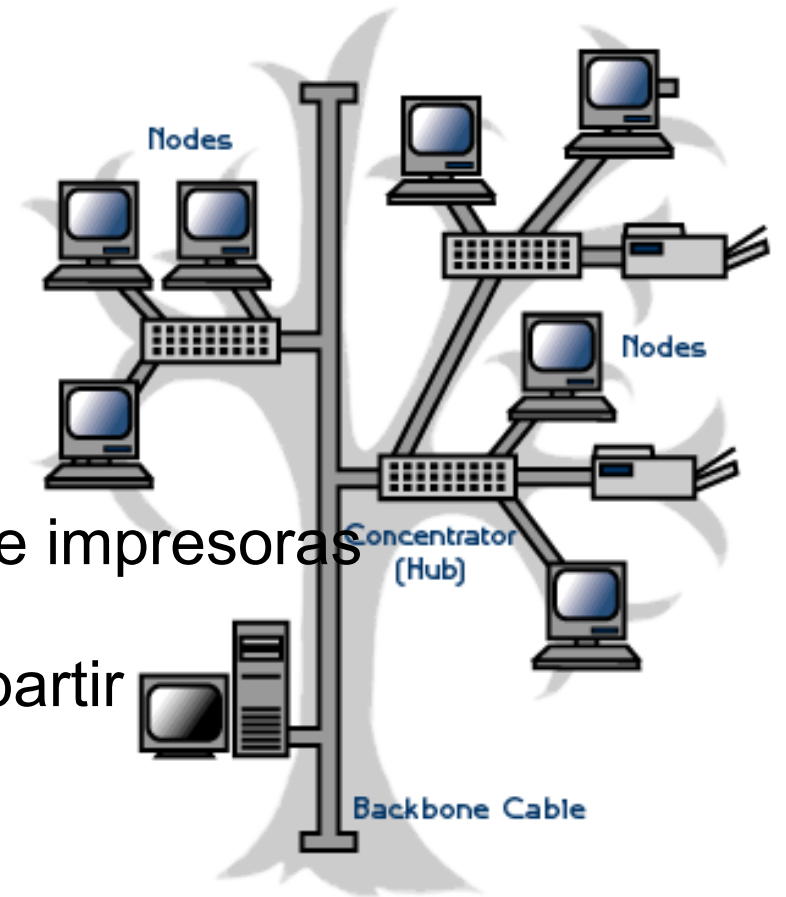
## Inicios

Las redes eran locales y pequeñas.

## Tareas

- Instalación de componentes: equipos e impresoras
- Configuración: NICs, protocolos, compartir impresora/disco
- Testeo: PING era suficiente
- Otros: hubs, switches, routers, cableado

**Fácil de manejar!!!**



# Introducción

Pero...

Hay cuestiones de mantenimiento a tener en cuenta

- ¿Cómo optimizar la **performance**?
- ¿Cómo manejar **fallas** y **cambios** en la red?
- ¿Cómo extender la **capacidad** de la red?
- ¿Cómo extender la **cobertura** de la red?
- ¿Cómo contabilizar el **uso**?
- ¿Cómo resolver cuestiones de **seguridad**?



# Introducción

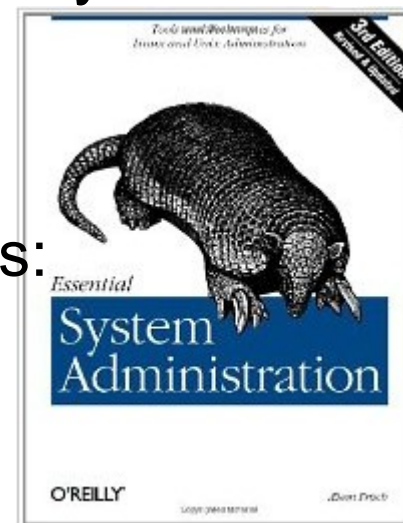
## En el pasado...

El “administrador” tomaba todas las responsabilidades y tareas

## En la actualidad...

Las tareas se encuentran divididas en especialidades:

- Servers admin
- System admin
- Network admin
- Especialista de seguridad



# Introducción

## **NOC – Network Operations Center**

(Centro de Operaciones de Red)

### **Funciones**

- Monitoreo y gestión de la red.
- Información sobre la disponibilidad actual, histórica y planeada de los componentes/sistemas.
- Estado de la red y estadísticas de operación.
- Monitoreo y gestión de fallas.





# Introducción

**Gestión = Monitoreo + Control**

**Monitoreo** (Funciones de “lectura”)

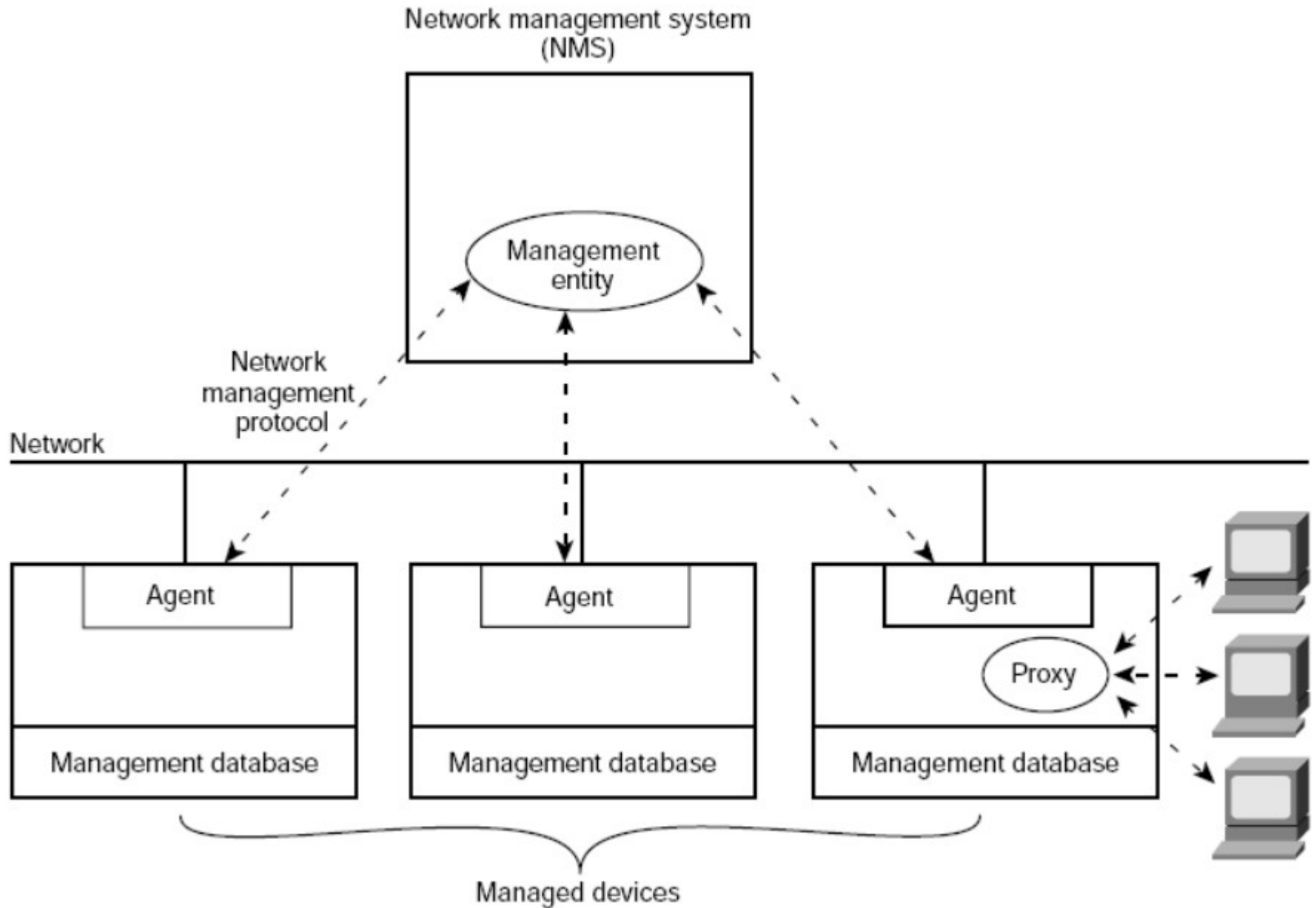
- Observar y analizar el estado y comportamiento de la configuración de red y sus componentes.

**Control** (Funciones de “escritura”)

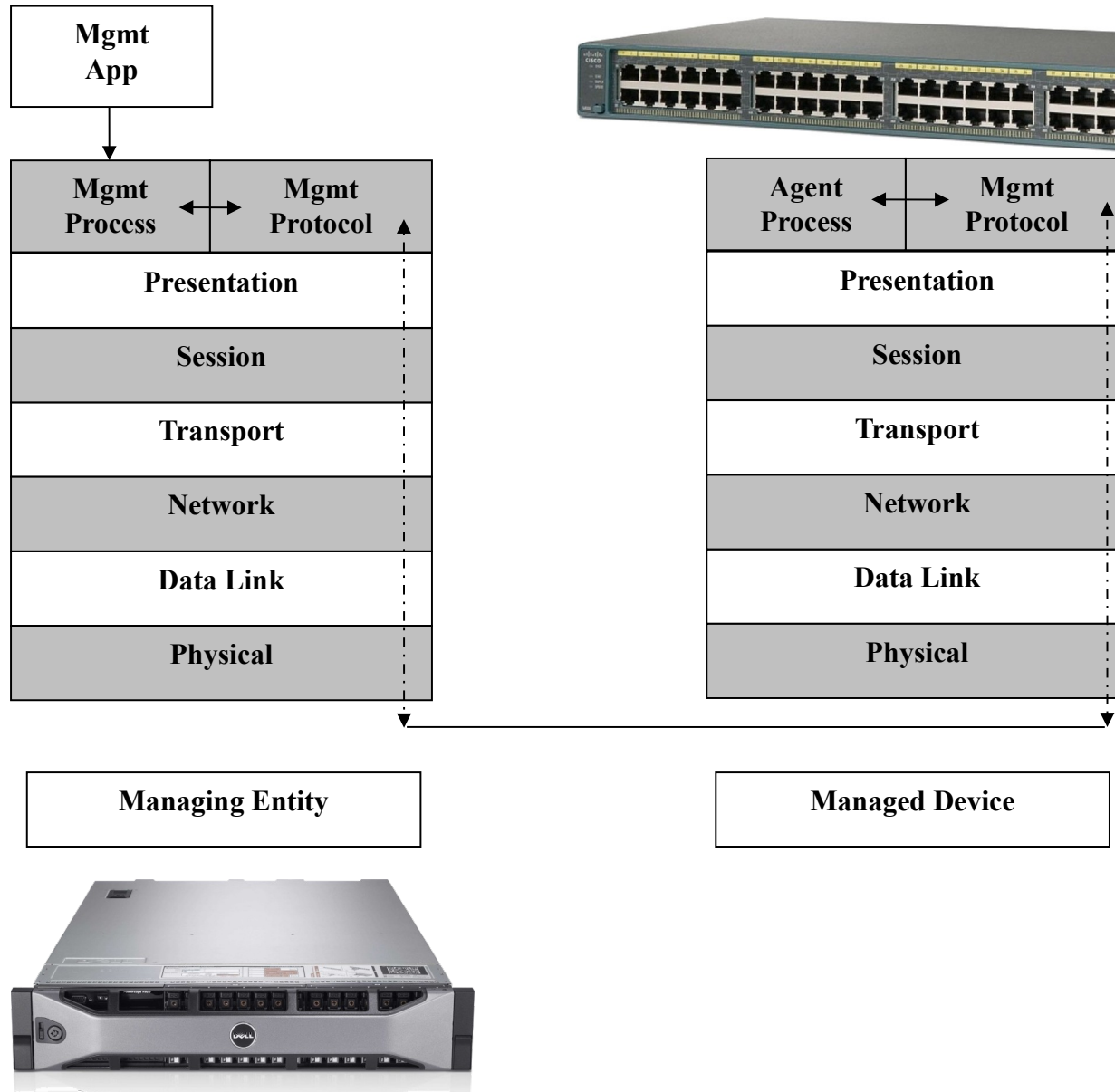
- Alterar parámetros de los componentes de la red



# Escenario



# En OSI



# Cuestiones

Existe un ***overhead*** en términos de:

- Ciclos de CPU usados para generar y procesar los mensajes
- Habitualmente se requiere una Entidad Gestora (“Managing Entity”) dedicada.
- Se utiliza tasa de transferencia para enviar/recibir mensajes

**Tiene que ser un balance  
entre costo y beneficio!**



# A tener en cuenta...

- **Distribución geográfica (Niveles)**: global, nacional, local, organizacional, departamental, etc.
- **Subredes**: routers, switches y otros dispositivos.
- **Conectividad**: enlaces punto a punto, wireless, internet, etc
- **Servicios**: www, dns, mail, aplicaciones, db, etc.
- **Requerimientos de BW**: audio, video, downloading, backups...
- **Facilidades**: BW constante, múltiples proveedores.
- **Seguridad**: ubicación de proxies, Cortafuegos (FireWalls), Sistemas de detección de intrusiones (IDSs).



# A tener en cuenta...

- Tráfico
- ¿Qué es crucial? (servicios) y qué no lo es
- Cuántos paquetes de control acepto en la red
- Cuáles son los umbrales de alarma
- Backups: qué respaldar, cuándo, dónde, por cuanto tiempo?
- Testeo de aplicaciones
- Actualizaciones de software
- Tipos de servicio requeridos
- Niveles de seguridad requeridos
- Requerimientos de seguridad en FW
- Necesidad de IDSs
- Permisos de usuarios
- etc, etc, etc...



Normas de gestión de sistemas

Agrupadas en

- **Funciones de Gestión**
- **Objetos Gestionados**
- **Servicios y Protocolos de Aplicación**



# ISO - FCAPS

La ISO definió 5 áreas funcionales para ordenar/organizar la gestión de una red ([FCAPS](#))

## ● **Gestión de Fallas**

Prevención, detección y respuesta ante algún “comportamiento” anormal.

## ● **Gestión de la Configuración**

Configuración de equipos (local o remotamente) y servicios (ej. DNS).

## ● **Gestión de la Contabilidad (Accounting)**

Medir el uso de los recursos para una mejor distribución de costos.

## ● **Gestión de la Performance (calidad de funcionamiento)**

Optimización del funcionamiento: tiempos de respuesta, utilización, error rate...

## ● **Gestión de la Seguridad**

Control de acceso/uso de recursos de la red.





# FCAPS Gestión de Fallas

Engloba funciones para monitorear la red a fin de garantizar que **todo funcione correctamente**. Abarca la atención y el procesamiento de alarmas, pero también otras funciones tales como el diagnóstico y la resolución de problemas.

- Ejecución de **pruebas periódicas**.
- **Detección, diagnóstico y solución** de fallas - Análisis de causa raíz.
- Filtrado y **correlación** de eventos y alarmas.
- **Mantenimiento de históricos** de alarma y estado de los sistemas.
- Registro y **seguimiento de reparaciones** y pedidos (issue tracking)
- **Gestión proactiva** de fallas (mantenimiento preventivo)



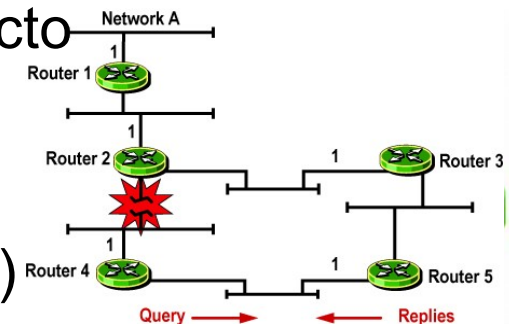
# FCAPS Gestión de Fallas

## Falla

- Es una situación que **requiere de algún tipo de acción** para que sea corregida y el sistema vuelva al funcionamiento normal.
- Es descubierta debido a la imposibilidad de operar correctamente o porque genera una cantidad de errores fuera de lo “normal”.
- Los errores ocurren ocasionalmente y no tienen por qué ser fallas (ej. todo enlace tiene una tasa de error).

## Cuando ocurre una falla...

- Diagnosticar y determinar rápidamente dónde se localiza.
- Aislar la red, reconfigurándola de forma que el impacto sea lo menor posible.
- Resolver el problema para que la red vuelva a su estado inicial (puede requerir cambiar componentes)



# Fallas - Requisitos de los usuarios

- Esperan soluciones **rápidas y seguras**.
- **Toleran fallas ocasionales**, pero esperan estar informados de manera inmediata de la falla y de su rápida solución.



Entonces,

- Se necesitan funciones muy rápidas de detección y diagnóstico.
  - Se puede minimizar el impacto utilizando componentes y rutas redundantes.
  - Después de corregir la falla, el servicio debe asegurar que se ha resuelto de verdad, y no se han introducido nuevos problemas (*control y seguimiento de fallas*).
- **Esperan** estar informados del estado de la red, incluyendo paradas de mantenimiento programadas y no programadas.



# Alarmas

- Mensajes que indican una condición de alerta:
  - UPS: **On battery power in response to an input power problem**
  - Nagios: **\*\* PROBLEM Host Alert: rtw0057 is DOWN \*\***
  - Arpwatch: **flip flop (192.168.0.101) eth1**
  - Traps SNMP
- Generados por un evento particular (p.ej. enlace caído) o superación de umbrales en parámetros monitoreados (% uso CPU, temperaturas, etc.)



# ISO X.733 Alarm reporting function

Información asociada a mensajes de alerta:

- Tipo de evento
- Tiempo del evento
- Clase y ejemplar de objeto gestionado (Sistema afectado)
- Probable causa
- Nivel de gravedad
- Situación de respaldo
- Indicación de tendencia
- Información de umbral
- Alarmas correlacionadas
- Acción recomendada para su resolución
- Información adicional
- ...



# Alarmas - Niveles de severidad

## IETF RFC 5424 The Syslog Protocol - Severidad:

- 0 EMERGENCY: system is unusable
- 1 ALERT: action must be taken immediately (requiere acción inmediata)
- 2 CRITICAL: critical conditions (requiere acción humana)
- 3 ERROR: error conditions
- 4 WARN(ING): warning conditions (falló, pero puede continuar)
- 5 NOTICE: normal but significant condition
- 6 INFO(RMATIONAL): informational messages
- 7 DEBUG: debug-level messages (usualmente desactivados)

## UIT-T X.733: Gravedad percibida:

Indeterminado  
Eliminado  
Aviso  
Crítico  
Mayor  
Menor



# Niveles de alarma en OpenNMS

<b>Critical</b>	This alarm means numerous devices on the network are affected by the alarm. Everyone who can should stop what they are doing and focus on fixing the problem.
<b>Major</b>	A device is completely down or in danger of going down. Attention needs to be paid to this problem immediately.
<b>Minor</b>	A part of a device (a service, and interface, a power supply, etc.) has stopped functioning. The device needs attention.
<b>Warning</b>	An alarm has occurred that may require action. This severity can also be used to indicate a condition that should be noted (logged) but does not require direct action.
<b>Indeterminate</b>	No Severity could be associated with this alarm.
<b>Normal</b>	Informational message. No action required.
<b>Cleared</b>	This alarm indicates that a prior error condition has been corrected and service is restored

# Niveles de alarma en Zabbix

SEVERITY	DEFINITION	COLOR
Not classified	Unknown severity.	Gray
Information	For information purposes.	Light blue
Warning	Be warned.	Yellow
Average	Average problem.	Orange
High	Something important has happened.	Light red
Disaster	Disaster. Financial losses, etc.	Red



# Alarma en SmokePing

Sat Jun 4 10:44:56 2016

Alert "bigloss" is active for target=World.Google

Pattern

-----  
==0%,==0%,==0%,==0%,>0%,>0%,>0%

Data (old --> now)

-----  
loss: 0%, 0%, 0%, 0%, 100%, 5%, 100%  
rtt: 31ms, 31ms, 31ms, 31ms, U, 107ms, U

Comment

-----  
suddenly there is packet loss



# FCAPS Gestión de Fallas

## Realizar testeos

- Conexiones físicas (herramientas necesarias)
- Conexiones lógicas (software). ping, traceroute, wget, iperf, etc.

## Priorizar fallas

- Definir el orden en que deben ser resueltas
- Utilizar mensajes de gestión in-band para aprender sobre fallas importantes
- Identificar los eventos que causan mensajes de falla
- Identificar qué dispositivos deben ser “encuestados” y a qué intervalos
- Identificar qué parámetros de los dispositivos deben ser recolectados y con qué frecuencia
- Priorizar los mensajes a almacenar en la BD para análisis futuro

## Informar

- A los usuarios, así como también los tiempos de solución del inconveniente

## Hacer reportes

- Hacer informes periódicos sobre fallas y tiempos de solución
- Establecer si existen motivos recurrentes
- Tratar de definir políticas de prevención



# FCAPS Gestión de la Configuración

Implica **proveer y modificar la configuración de los equipos y dispositivos** en la red, tanto la incorporación y establecimiento inicial de uno nuevo, como los cambios continuos de configuración que se requieran.

- **Configuración de recursos** administrados, ya sean equipos de red o servicios que se ejecutan en la red.
- **Auditoría periódica** de la red para (re)descubrir lo que hay en ella.
- **Sincronización** de la información almacenada en el sistema de gestión (inventario) contra lo que realmente existe en la red.
- Realización de **copias de seguridad** de la configuración de red, dispositivos y restauración en caso de fallas.
- Administración del SW que se ejecuta en equipos de red.



# FCAPS Gestión de la Configuración

## Dispositivos y red

- Selección de los componentes correctos
- Definición del despliegue del sistema de cableado
- Seteo de los parámetros de las interfaces
- Direcciones de red

## Qué se puede “gestionar”?

- Habilitar/deshabilitar puertos/dispositivos
- Configurar tablas de rutas
- Redireccionar tráfico
- Configurar parámetros de seguridad
- Llevar inventario (manual y/o automático → NMS)
  - Cables, dispositivos, software, SO, utilidades, drivers, versiones, aplicaciones, vendedor, red, subred, direcciones...
- Manejo de parches
- Etc, etc, etc...

*“Se ocupa de inicializar la red, mantener, añadir y actualizar el estado de los componentes y las relaciones entre dichos componentes”*



# FCAPS Gestión de la Contabilidad

La función de Contabilidad (Accounting) se ocupa de recopilar y registrar datos sobre **cómo se usa la red** y sobre el **consumo de sus servicios por parte de los usuarios** finales. Esto implica:

- Registrar el consumo de recursos (tasa de transferencia, disco, etc).
- Informar a los usuarios de costos ocasionados o recursos consumidos
- Permitir el establecimiento de límites de contabilidad y asociar calendarios de tarifas a la utilización de recursos.
- Permitir la combinación de costos cuando se invoquen múltiples recursos para alcanzar un objetivo de comunicación dado.

Fundamental para organizaciones que deben facturar el uso de los recursos o servicios.

(Puede requerirse contabilidad en real-time)



# FCAPS Gestión de la Contabilidad

En muchas organizaciones, diferentes divisiones, centros de gasto o proyectos, son facturados por el uso de los servicios de red.

**Aunque esto no ocurra**, es necesario mantener información sobre el uso de los recursos de red por usuarios o tipos de usuarios:

- Determinados usuarios pueden estar abusando de sus privilegios de acceso y cargar la red afectando a los demás.
- Los usuarios pueden hacer un uso ineficiente de la red, y el gestor puede ayudar a cambiar procedimientos para mejorar la efectividad.
- Conocer en detalle las actividades de los usuarios es muy útil para planificar el crecimiento adecuado de la red.



# FCAPS Gestión de la Performance

Consiste en **recopilar estadísticas** de la red con el objetivo de **evaluar el rendimiento** para luego modificar la red en consecuencia (gestión de configuración).

Engloba las siguientes actividades:

- Reunir información estadística y generar informes de tendencia.
- Mantener y examinar registros históricos de estados de sistemas.
- Determinar periódicamente el rendimiento del sistema en condiciones naturales y artificiales.
- Cambiar los modos de operación del sistema con el fin de efectuar actividades de gestión del funcionamiento.



# FCAPS Gestión de la Performance

*“Las redes modernas están compuestas de muchos componentes que se comunican y comparten datos y recursos. La efectividad de una aplicación depende cada vez más de unas prestaciones adecuadas de la red”*

## Dos categorías funcionales principales

- **Monitoreo** → Seguimiento de la actividad de la red
- **Control** → Realización de ajustes para mejorar las prestaciones.

## Cuestiones:

- ¿Cuál es el nivel de utilización de la capacidad?
- ¿Hay excesivo tráfico?
- ¿Las prestaciones se han reducido a niveles inaceptables?
- ¿Hay cuellos de botella?
- ¿Está aumentando el tiempo de respuesta?

## Requiere:

- Identificar los valores relevantes a monitorizar
- Definir las métricas adecuadas

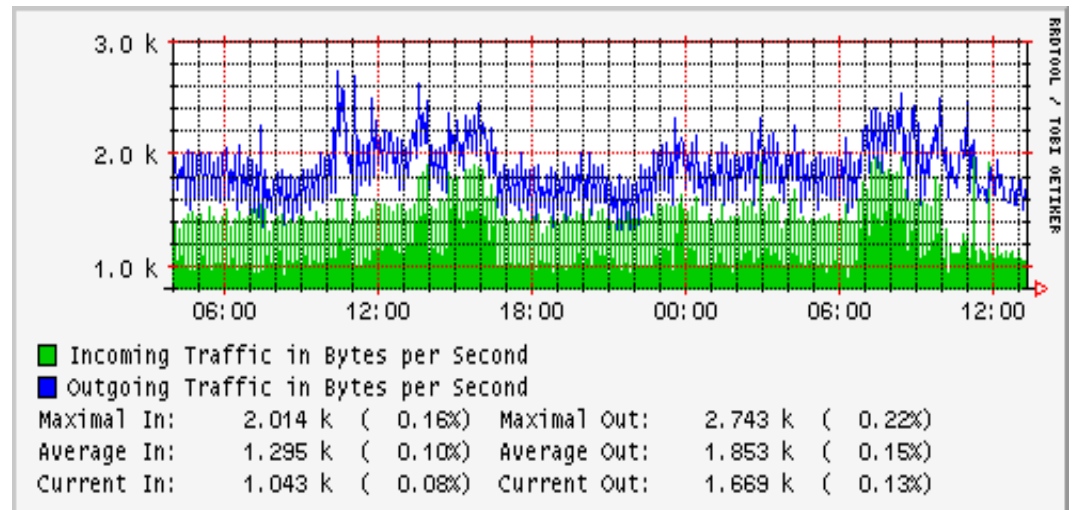




# FCAPS Gestión de la Performance

## Recolectar datos de uso (Baseline)

- Medir la utilización de un enlace
- Contar la cantidad de paquetes Rx/Tx por dispositivo
- Medir uso de CPU/memoria, long de colas
- Medir el tiempo total de respuesta



## Recolectar datos históricos

- Medir la utilización y el tiempo total de respuesta en diferentes momentos del día (y sobre un período extendido)

## Capacity Planning

- Detectar tendencias (ej., observando gráficas) para proyectar el costo de una expansión



# Métricas

Ejemplos de “algunas” variables a considerar

## Confiabilidad

- Tasa de errores
- Paquetes perdidos
- Fallas de los enlaces

## Disponibilidad

- Tiempo medio entre fallos (MTBF) de la red, subred, componentes, servicios...

## Performance

- Tiempos de respuesta
- Uso de CPU
- Tamaños de las colas

## Throughput

- Bytes/segundo
- Mensajes/segundo



# Información de Monitoreo

- **Estática:** Características de un elemento/dispositivo de la red. Ejemplo: cantidad y velocidad de las interfaces de un switch.
- **Dinámica:** Relacionada con eventos en la red. Ejemplo: Tx/Rx de paquetes.
- **Estadística:** resultado de la agregación de información dinámica. Ejemplo: Tasa media de paquetes Tx por un nodo

## Modelo gestor-agente



# Monitoreo de prestaciones

**Dificultad:** Seleccionar los indicadores apropiados (hay métricas no comparables, no todos los fabricantes de equipos soportan las mismas).

## Indicadores orientados al Servicio (calidad del servicio)

- **Disponibilidad** Porcentaje de tiempo que un elemento de red, componente, aplicación está disponible para el usuario.
- **Tiempo de respuesta** Tiempo que el usuario debe esperar la respuesta a una acción iniciada por él.
- **Fiabilidad** Porcentaje de tiempo sin errores en la transmisión y entrega de la información.

## Indicadores orientados a la Eficiencia (costo de “esa” calidad)

- **Throughput** Tasa de ocurrencia de eventos de usuario: generación de transacciones, mensajes.
- **Utilización** Porcentaje actualmente utilizado de la capacidad teórica total de un recurso.



# Monitoreo

- **Disponibilidad:**

Sobre todos los componentes de la red. Es muy difícil establecer un “número” único.

$$Disponibilidad = \frac{MTBF}{MTBF + MTTR}$$

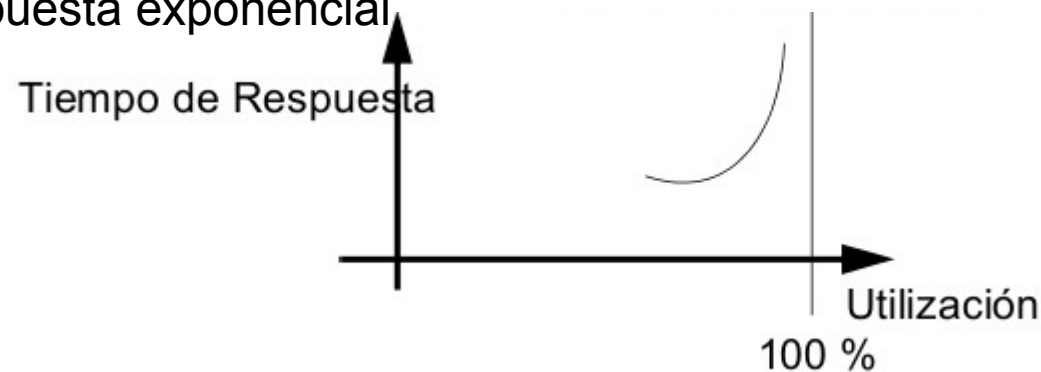
- **Tiempo de respuesta:** Realizar mediciones separadas para detectar “cuellos de botella”

- **Fiabilidad:** Analizar tasa de paquetes corruptos

- **Throughput:** Nos ayuda a prever posibles problemas de prestaciones como consecuencia de incrementos de la demanda

- **Utilización:** Se trata de detectar cuellos de botella y áreas de congestión.

Alto grado de utilización → tiempo de respuesta exponencial



# Monitoreo

## Algunos problemas

### ● Fallas inobservables

- Puede que sean muy puntuales y menores o porque el equipo en cuestión no dispone de mecanismos para detectar ese error. Por ejemplo, un microcorte del enlace.

### ● Fallas parcialmente observables

- Lo observado no es suficiente para diagnosticar la causa. Por ejemplo, un ráfaga de tramas dañadas que generan retransmisiones puntuales.

### ● Incertidumbre en la observación

- Aunque haya observaciones muy detalladas, puede que exista incertidumbre acerca de la causa. Por ejemplo, un nodo que no responde un ping, ¿necesariamente falló?



# Monitoreo

## ¿Cómo se hace?

### - Protocolos específicos

SNMP, CMIP, ICMP, CDP, LLDP...

### - Herramientas (semi) automáticas, NMS, SIEM, IDS...

OpenNMS (demo online: <http://demo.opennms.org>)

Observium (demo online: <http://demo.observium.org>)

OSSIM, Snort, Nagios, Cacti, Zabbix, Munin, Nfsen, RDDTool, Ganglia, MRTG, OpenVAS, Logstash...

Propietarias...



# FCAPS Gestión de la Performance

## Establecer umbrales de notificación

- “Encuestar” los dispositivos administrados por valores críticos de los parámetros
- Establecer los intervalos de encuesta
- Establecer alarmas
- Tomar una acción cuando se dispara un alarma

## Construir BD de dispositivos

- Analizar los datos off-line
- Con información de parámetros monitoreados, umbrales, tiempos
- Establecer necesidades de upgrades

## Ejecutar simulaciones de la red

- Desarrollar un modelo de la red
- Usar los datos recolectados como parámetros del modelo para optimizar performance

## Latencia

- Tiempo de respuesta entre petición/response





# FCAPS Gestión de la Seguridad

## Seguridad de la Red

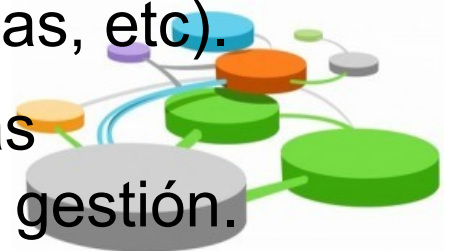
Asegurar la protección de la información en un sistema de red contra accesos no autorizados, modificaciones, destrucción...

- Políticas y proced de seguridad.
- Implementación de mecanismos de seguridad (protocolos, cifrado, software, etc).
- Control de acceso (ACLs).
- Prevención de incidentes.
- Auditoría de eventos.
- Detección y respuesta.

## Seguridad de la Gestión de Red

Asegurar que las operaciones de gestión son en sí mismas seguras.

- Seguridad del NOC.
- Seguridad de los mensajes de gestión (monitoreo / control).
- Seguridad física (conexión, cableado, oficinas, etc).
- Seguridad de las aplicaciones de gestión.



# FCAPS Gestión de la Seguridad

Las “tres A”

## Autenticación

- Establecer que algo/alguien es auténtico, que es cierto/real.
- Identidad y credenciales que la acreditan.

## Autorización

- Proceso por el cual se asegura que los recursos sólo sean accedidos (utilizados, modificados...) sólo por aquellos a quienes se les ha otorgado el permiso de hacerlo.

## Contabilidad (Accounting)

- Realizar seguimiento de la utilización de los recursos por parte de los usuarios (pero esto es de la otra función).



Protocolos: RADIUS, TACACS, DIAMETER, Kerberos, ... SAML ...

# FCAPS Gestión de la Seguridad

## Técnicas básicas

- Identificar hosts y la información sensible en cada caso
- Gestionar passwords
- Asignar permisos de usuario
- Almacenar y analizar intentos de login fallidos
- Establecer restricciones de acceso remoto
- Limitar la vista de la red
- Seguir hora y origen de los accesos remotos a servidores

## Identificar métodos de acceso

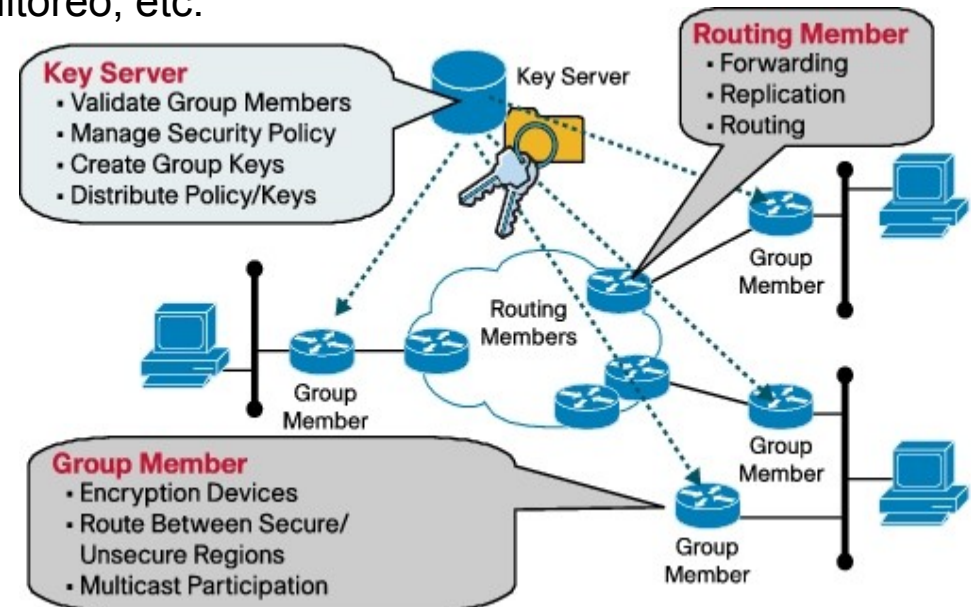
- En los servicios: mail, www, FTP, Rlogin, RPC, Monitoreo, etc.

## Aplicar métodos de control de acceso

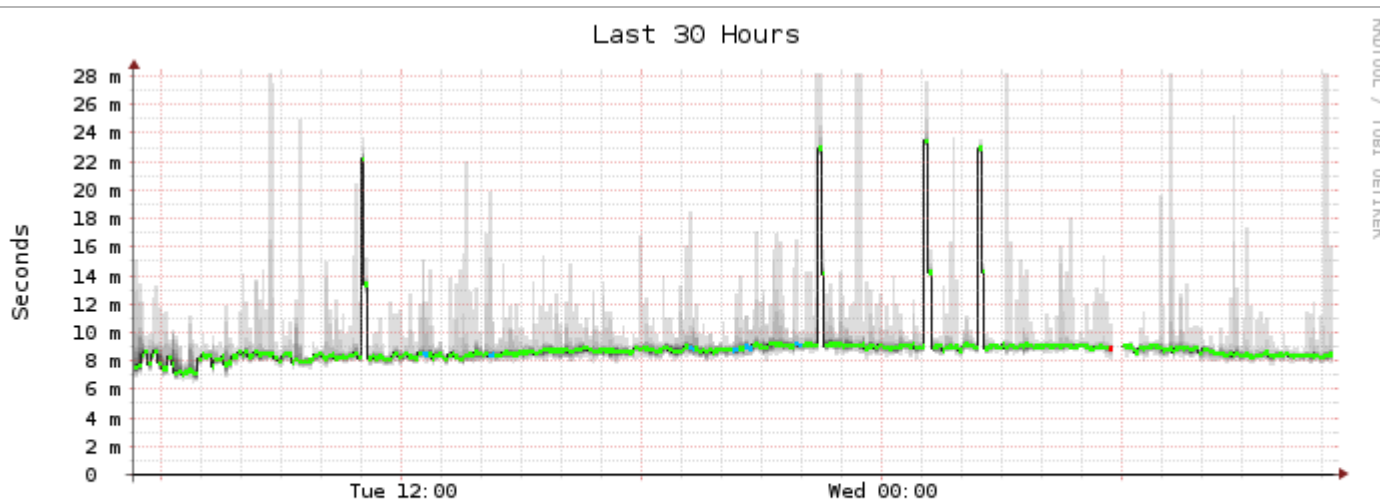
- Criptografía
- Filtrado de paquetes en routers/firewalls
- Source host/user authentication

## Mantenimiento

- Auditar actividad en puntos de acceso
- Ejecutar simulación de ataques
- Tratar de detectar intrusos

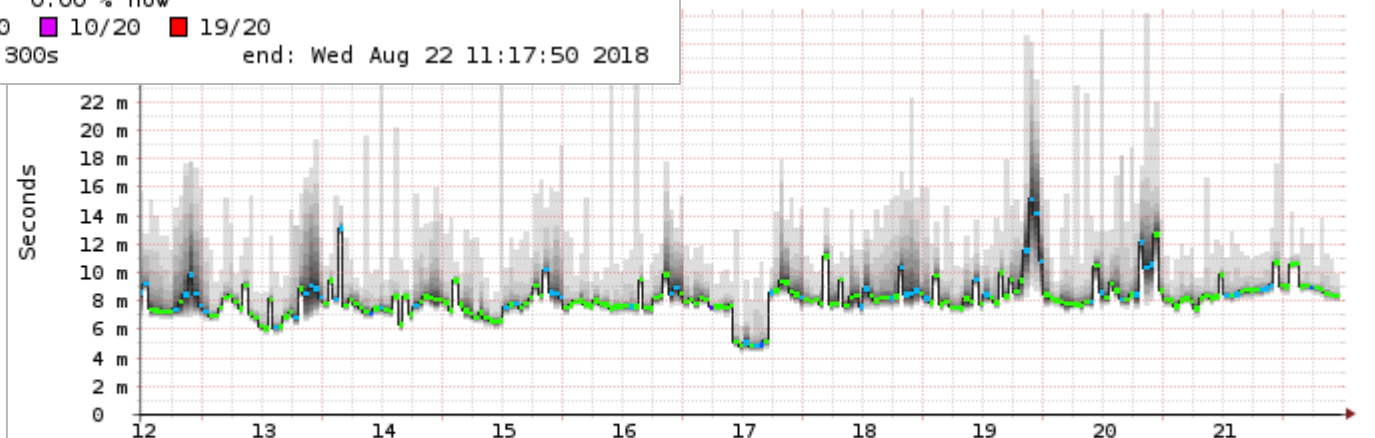


# Soft para Monitoreo: Smokeping



median rtt: 8.8 ms avg 23.5 ms max 7.0 ms min 8.5 ms now 1.6 ms sd 5.4 am/s  
packet loss: 0.29 % avg 73.33 % max 0.00 % min 0.00 % now  
loss color: 0 1/20 2/20 3/20 4/20 10/20 19/20  
probe: 20 ICMP Echo Pings (56 Bytes) every 300s end: Wed Aug 22 11:17:50 2018

10 Days



median rtt: 8.2 ms avg 15.2 ms max 4.8 ms min 8.4 ms now 1.3 ms sd 6.3 am/s  
packet loss: 0.31 % avg 13.48 % max 0.00 % min 0.00 % now  
loss color: 0 1/20 2/20 3/20 4/20 10/20 19/20  
probe: 20 ICMP Echo Pings (56 Bytes) every 300s end: Wed Aug 22 11:17:50 2018

Smokeping UC Davis: <http://smokeping.ucdavis.edu/cgi-bin/smokeping.fcgi?target=Campus.Border>

# Soft para Monitoreo: Nagios

## Nagios®

### Current Network Status

Last Updated: Fri Oct 17 18:51:18 UTC 2014  
 Updated every 90 seconds  
 Nagios® Core™ 4.0.8 - www.nagios.org  
 Logged in as nagiosadmin

### Host Status Totals

Up	Down	Unreachable	Pending
11	0	0	0
All Problems		All Types	
0		11	

### Service Status Totals

Ok	Warning	Unknown	Critical	Pending
33	1	1	4	0
All Problems		All Types		
6		39		

### General

Home  
 Documentation

### Current Status

Tactical Overview  
 Map  
 Hosts  
 Services  
 Host Groups  
 Summary  
 Grid  
 Service Groups  
 Summary  
 Grid  
 Problems  
 Services (Unhandled)  
 Hosts (Unhandled)  
 Network Outages

Quick Search:

### Reports

Availability  
 Trends  
 Alerts  
 History  
 Summary  
 Histogram  
 Notifications  
 Event Log

### System

Comments  
 Downtime  
 Process Info  
 Performance Info  
 Scheduling Queue  
 Configuration

### Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
NOAA	Auroral Activity	OK	10-17-2014 18:51:09	535d 4h 28m 6s	1/3	Aurora OK: Activity level is 2
	Weather Carteret North Carolina	WARNING	10-17-2014 18:43:15	0d 0h 46m 57s	3/3	Weather Warning: Beach Hazards
	Weather King Washington	OK	10-17-2014 18:45:25	737d 1h 52m 46s	1/3	Weather OK: No watches or warni area.
	Weather Ramsey Minnesota	OK	10-17-2014 18:46:45	59d 20h 47m 12s	1/3	Weather OK: No watches or warni area.
	Weather San Bernardino California	OK	10-17-2014 18:41:45	0d 0h 48m 40s	1/3	Weather OK: No watches or warni area.
	Weather Strafford New Hampshire	OK	10-17-2014 18:43:45	0d 0h 46m 51s	1/3	Weather OK: No watches or warni area.
	Weather Tulsa Oklahoma	OK	10-17-2014 18:45:53	737d 1h 53m 51s	1/3	Weather OK: No watches or warni area.
localhost	Current Load	OK	10-17-2014 18:49:08	0d 0h 46m 9s	1/4	OK - load average: 0.29, 0.49, 0.51
	Current Users	OK	10-17-2014 18:51:02	1710d 15h 36m 24s	1/4	USERS OK - 0 users currently logg
	HTTP	OK	10-17-2014 18:48:25	1019d 2h 7m 58s	1/4	HTTP OK: HTTP/1.1 200 OK - 211 response time
	PING	OK	10-17-2014 18:50:20	1710d 15h 35m 9s	1/4	PING OK - Packet loss = 0%, RTA
	Root Partition	OK	10-17-2014 18:48:32	938d 2h 32m 35s	1/4	DISK OK - free space: / 20300 MB
	SSH	OK	10-17-2014 18:46:38	1704d 7h 35m 15s	1/4	SSH OK - OpenSSH_4.3 (protocol
	Swap Usage	OK	10-17-2014 18:48:54	1710d 15h 33m 17s	1/4	SWAP OK - 100% free (255 MB of
Total Processes	OK	10-17-2014 18:50:49	1706d 8h 22m 2s	1/4	PROCS OK: 147 processes with S	

Demo online: <http://nagioscore.demos.nagios.com/>

# Soft para Monitoreo: OpenNMS

Apr 17, 2016 10:17 EDT



Search Info Status Reports Dashboards Maps demo

Dashboard  
Ops Board

Home

## Nodes with Pending Problems

- mcdaniels.internal.opennms.com has 1 alarm (15 hours)
- mephesto.internal.opennms.com has 1 alarm (18 hours)
- twc-rr-nc-2-la-ca has 2 alarms (18 hours)
- stanford.internal.opennms.com has 1 alarm (22 hours)
- uglybob.internal.opennms.com has 1 alarm (2 days)
- atlgate has 2 alarms (2 days)
- cartman.internal.opennms.com has 1 alarm (2 days)
- timmy.internal.opennms.com has 1 alarm (2 days)

## Nodes with Outages

- mephesto.internal.opennms.com (18 hours)
- twc-rr-nc-2-la-ca (18 hours)
- stanford.internal.opennms.com (22 hours)
- uglybob.internal.opennms.com (2 days)
- mcdaniels.internal.opennms.com (4 days)

## Availability Over the Past 24 Hours

Categories	Outages	Availability
Network Interfaces	0 of 125	100.000%
Web Servers	0 of 51	100.000%
Email Servers	0 of 14	99.995%
DNS and DHCP Servers	0 of 9	100.000%
Database Servers	0 of 0	100.000%
JMX Servers	0 of 0	100.000%
Software Update	3 of 22	86.710%
Other Servers	0 of 71	100.000%
<b>Total</b>	<b>Outages</b>	<b>Availability</b>
Overall Service Availability	6 of 339	98.626%

## Notifications

- You have no outstanding notices
- There are no outstanding notices
- On-Call Schedule

## Resource Graphs

## KSC Reports

## Quick Search

Node ID:

Node label like:

TCP/IP Address like:

Providing service:

Demo online: <https://demo.opennms.org>

# Soft para Monitoreo: Zabbix



Demo video: <https://www.zabbix.com/la/demo>

# Soft para Discovery: Netdisco

Netdisco

Inventory

Reports ▾

Admin ▾

router-16.example.com



Logged in as guest ▾

Details **Ports** Modules Neighbors Addresses

router-16.example.com

System Name	router-16.example.com
Location	
Contact	Super Network Admin Person
Vendor / Model	<a href="#">cisco / 3560G24TS</a>
OS / Version	<a href="#">ios / 12.2(46)SE</a>
Serial Number	AICHOHNG6OB
Description	Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(46)SE, RELEASE SOFTWARE (fc2) Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Thu 21-Aug-08 15:26 by nachen
Administration	<a href="#">SSH</a> <a href="#">Telnet</a> <a href="#">Web</a>
SNMP Class	<a href="#">SNMP::Info::Layer3::C3550</a>
Uptime	24 days 23:00:47
Layers	
Last Discover	2010-10-08 06:48
Last Arpnip	2010-10-09 02:31
Last Macsuck	2010-10-09 03:17
Hardware Status	Fan: ok PS1 [other]: ok PS2 [externalPS]: other
MAC Address	00:24:c3:16:16:16
VTP Domain	examplecom
Admin Tasks	<a href="#">Discover</a> <a href="#">Arpnip</a> <a href="#">Macsuck</a> <a href="#">NBTstat</a> <a href="#">Delete</a>

Demo online: <https://netdisco2-demo.herokuapp.com/>



# Soft para Discovery: Netdisco

Netdisco Inventory Reports Admin router-16.example.com Logged in as guest

router-16.example.com

Details Ports Modules Neighbors Addresses

Show All records. Filter records...

Port	Name	Native VLAN	VLAN Membership	Connected Devices
GigabitEthernet0/1	Link to FW1			router-16 - GigabitEthernet0/1
GigabitEthernet0/2	FW1 Management Interface	968	968	router-17 - GigabitEthernet0/9 00:15:17:44:55:66 server-a.example.com (10.1.3.221) 192.0.5.14
GigabitEthernet0/3	Link to FW2			router-17 - GigabitEthernet0/2
GigabitEthernet0/4	FW2 Management Interface	968	968	00:15:17:11:22:33 192.0.5.15
GigabitEthernet0/5	VPN Server	964	964	
GigabitEthernet0/6	Port With Nothing Connected	1	1	
GigabitEthernet0/7	Gi0/7	1	1	
GigabitEthernet0/8	Gi0/8	1	1	
GigabitEthernet0/9	Gi0/9	1	1	
GigabitEthernet0/10	Gi0/10	1	1	
GigabitEthernet0/11	Gi0/11	1	1	
GigabitEthernet0/12	Gi0/12	1	1	
GigabitEthernet0/13	Gi0/13	1	1	
GigabitEthernet0/14	Gi0/14	1	1	
GigabitEthernet0/15	Gi0/15	1	1	router-17 - GigabitEthernet0/7
GigabitEthernet0/16	Gi0/16	1	1	
GigabitEthernet0/17	Gi0/17	1	1	
GigabitEthernet0/18	Gi0/18	1	1	
GigabitEthernet0/19	Gi0/19	1	1	
GigabitEthernet0/20	Gi0/20	1	1	whiterabbit - Port48
GigabitEthernet0/21	Gi0/21	1	1	whiterabbit - Port24
GigabitEthernet0/22	Mgmt Network to VRF Ext	968	968	router-17 - GigabitEthernet0/22
GigabitEthernet0/23	Mgmt Network	968	968	router-16 - GigabitEthernet0/2
GigabitEthernet0/24	VPN Networks	1	94	192.168.34.17 - GigabitEthernet4/15
GigabitEthernet0/25	Gi0/25	1	1	router-17 - GigabitEthernet0/10

**Legend**

- Link Up
- Link Down
- Port Free
- Admin Disabled
- Blocking
- Manual Topology
- Neighbor Device
- Neighbor Inaccessible
- IP Phone
- Wireless Client
- Archived Data
- Link Aggregate
- Click "Update View"

**Display Columns**

- Port Controls
- Port
- Description
- Type
- Duplex
- Last Change
- Name
- Speed
- Port MAC
- MTU
- Native VLAN
- VLAN Membership
- PoE
- SSID
- Connected Nodes
- Connected Devices
- Spanning Tree
- Status

Port Properties

Node Properties

Update View

# Soft para Inventario: GLPI

### Router Wireless 7/50

<b>Dispositivo de red</b>	<b>Dispositivo de red</b>	
<b>Sistemas operativos</b>	Nombre Router Wireless	Estado Sin uso ⓘ
<b>Componentes</b>	Lugar D.G.S. > NOC ⓘ	Tipo router ⓘ
<b>Volúmenes</b>	Responsable técnico del hardware ----- ⓘ	Fabricante Linksys ⓘ
<b>Puertos de red 1</b>	Grupo responsable del hardware ----- ⓘ	Modelo BEFW11S4 ⓘ
<b>Nombres de red</b>	Número de usuario alternativo	Número de serie
<b>Gestión</b>	Nombre de usuario alternativo	Número de inventario S/N
<b>Contratos</b>	Usuario ----- ⓘ	Red ----- ⓘ
<b>Documentos</b>	Grupo ----- ⓘ	Comentarios Linksys Wireless-B Broadband Router with 4 port switch 2.4 Ghz 802.11b
<b>Base de conocimiento</b>	Dominio ----- ⓘ	
<b>Incidentes</b>	La dirección MAC e IP del equipo están incluídas en un puerto de red agregado	
<b>Problemas</b>	Memoria (MB)	
<b>Cambios</b>	<b>Creado el</b>	<b>Última modificación el 2007-05-23 12:42</b>
<b>Enlaces externos</b>		<b>Creado desde la plantilla Blank Template</b>

Guardar

Enviar a papelera

<https://glpi-project.org>

# Soft para Issue Tracking: GLPI

### Router Wireless 7/50

<b>Dispositivo de red</b>	<b>Dispositivo de red</b>	
<b>Sistemas operativos</b>	Nombre Router Wireless	Estado Sin uso ⓘ
<b>Componentes</b>	Lugar D.G.S. > NOC ⓘ	Tipo router ⓘ
<b>Volúmenes</b>	Responsable técnico del hardware ----- ⓘ	Fabricante Linksys ⓘ
<b>Puertos de red 1</b>	Grupo responsable del hardware ----- ⓘ	Modelo BEFW11S4 ⓘ
<b>Nombres de red</b>	Número de usuario alternativo	Número de serie
<b>Gestión</b>	Nombre de usuario alternativo	Número de inventario S/N
<b>Contratos</b>	Usuario ----- ⓘ	Red ----- ⓘ
<b>Documentos</b>	Grupo ----- ⓘ	Comentarios Linksys Wireless-B Broadband Router with 4 port switch 2.4 Ghz 802.11b
<b>Base de conocimiento</b>	Dominio ----- ⓘ	
<b>Incidentes</b>	La dirección MAC e IP del equipo están incluídas en un puerto de red agregado	
<b>Problemas</b>	Memoria (MB)	
<b>Cambios</b>	<b>Creado el</b>	<b>Última modificación el 2007-05-23 12:42</b>
<b>Enlaces externos</b>		<b>Creado desde la plantilla Blank Template</b>

Guardar

Enviar a papelera

- Sistemas operativos
- Componentes
- Volúmenes
- Puertos de red 1
- Nombres de red
- Gestión
- Contratos
- Documentos
- Base de conocimiento
- Incidentes
- Problemas
- Cambios
- Enlaces externos
- Notas
- Reservas
- Certificados
- Histórico 1
- Bloqueos
- FusionInventory SNMP
- Todos

# Bibliografía

- MAURO, D., SCHMIDT, K., 2005, Essential SNMP (2nd ed). O'Reilly Media. Capítulo 1. "Introduction to SNMP and Network Management" (págs. 1-10; omitir sección "Change Management")
- CLEEM, A. 2007. Network Management Fundamentals. CISCO Press. Capítulo 5. "Management Functions and Reference Models: Getting Organized" (págs. 129-166)
- OPPENHEIMER, P., 2011, Top-Down Network Design (3d ed). CISCO Press. Capítulo 9. "Developing Network Management Strategies" (págs. 263-278)
- UIT-T Rec X.700 (FCAPS), X.701, X.733
- RFC 5424 "The Syslog Protocol"

