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)
Santiago Ricci (sricci@unlu.edu.ar)
Alejandro Iglesias (aaiglesias@unlu.edu.ar)
Mauro Meloni (maurom@unlu.edu.ar)
Marcelo Fernandez (fernandezm@unlu.edu.ar)

- 2020 -

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

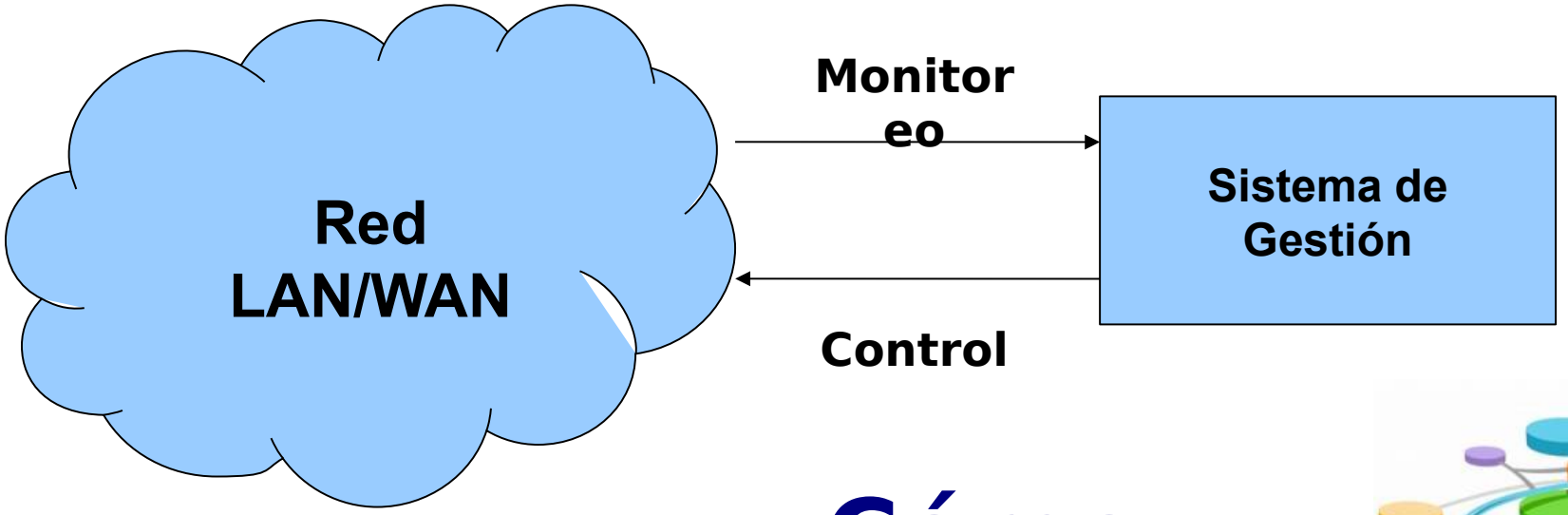
Definición

"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 ?

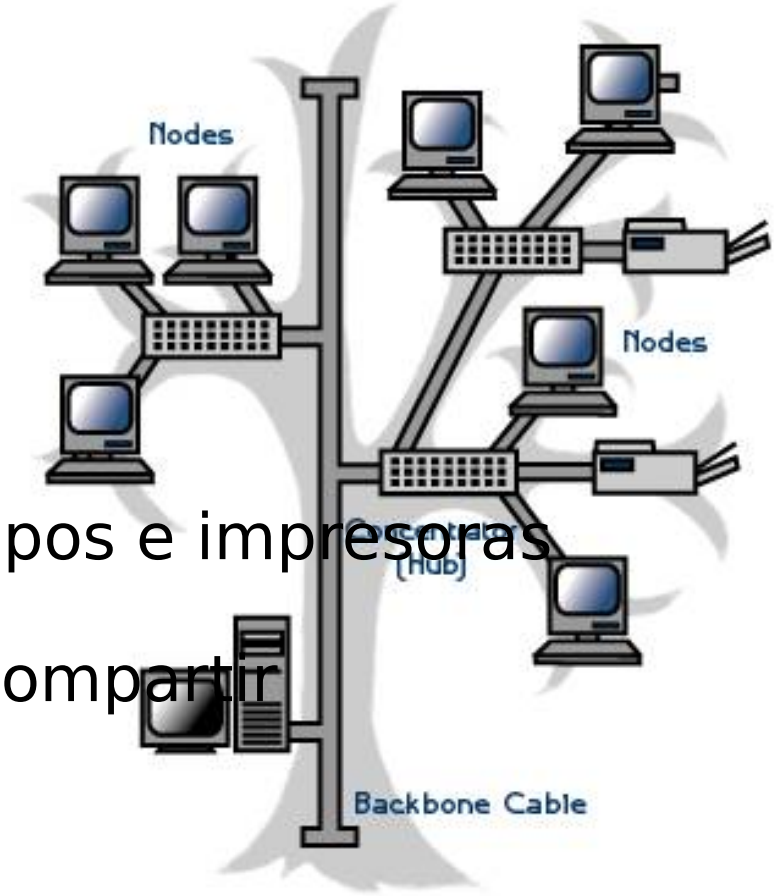
Introducción

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...

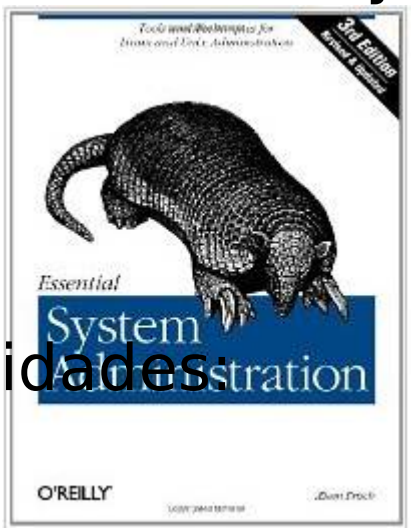
Hay cuestiones de mantenimiento a tener en cuenta

- ¿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

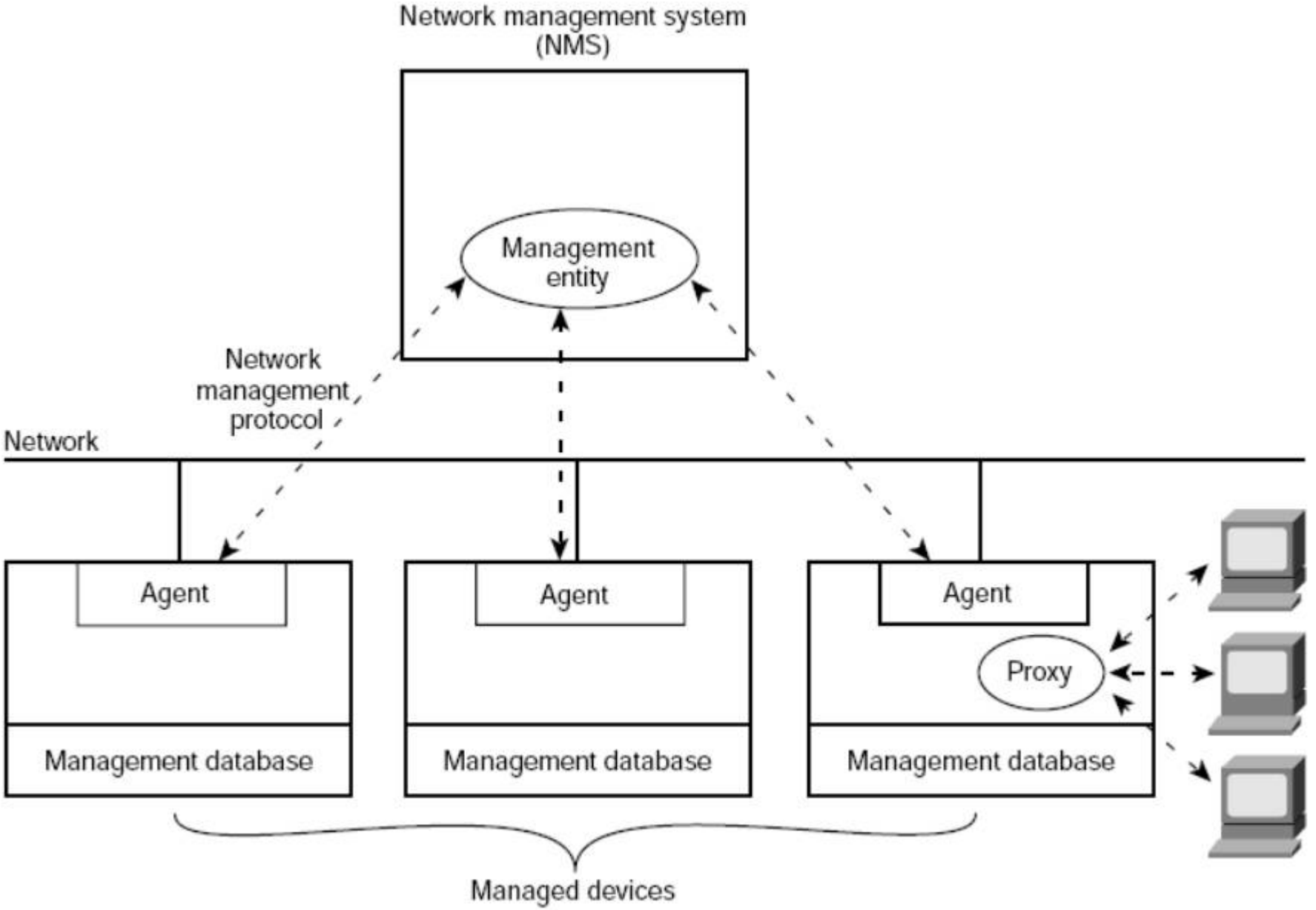
Monitoreo (Funciones de “lectura”)

- Observar y analizar el estado y comportamiento de la configuración de red y sus componentes.
- Incluye: prestaciones, fallas y costos.

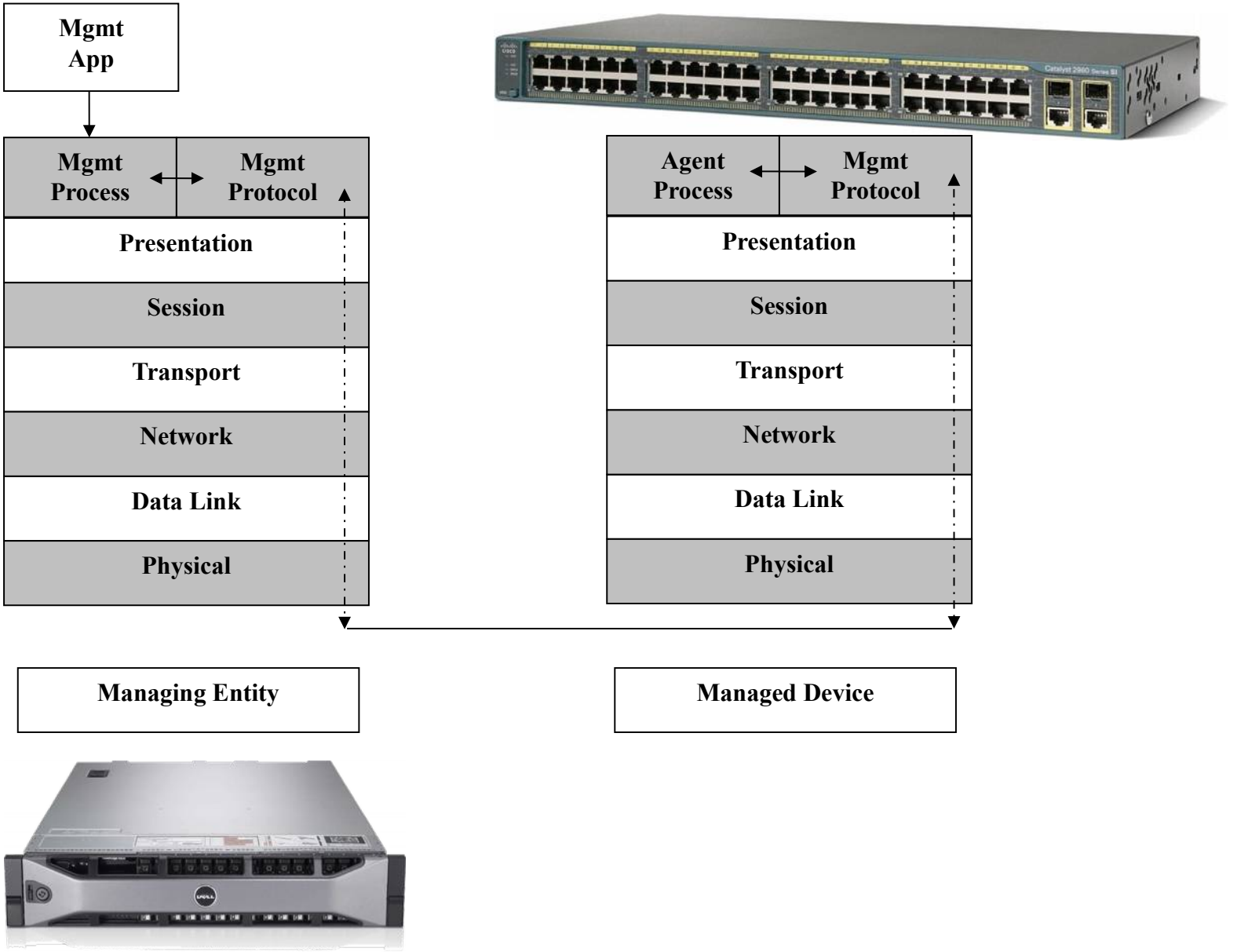
Control (Funciones de “escritura”)

- Alterar parámetros de los componentes de la red
- Incluye: configuración y seguridad

Escenario


Network management system
(NMS)
Management
entity
Network
management
protocol
Network
Agent
Agent
Agent
Proxy
Management database
Management database
Management database
Managed devices

En OSI


Mgmt App
Mgmt Process
Mgmt Protocol
Presentation
Session
Transport
Network
Data Link
Physical
Agent Process
Mgmt Protocol
Presentation
Session
Transport
Network
Data Link
Physical
Managing Entity
Managed Device

Cuestiones

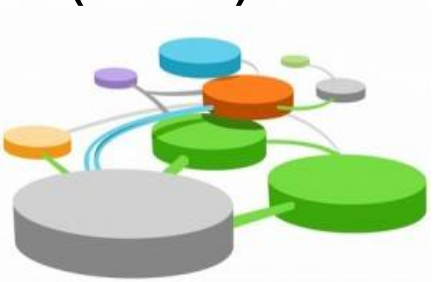
Existe un ***overhead*** en términos de:

- Ciclos de CPU usados para generar y procesar los mensajes
- Habitualmente se requiere una Entidad Gestora (“Managing Entity”) dedicada.
- Se utiliza ancho de banda 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**: wireless, direcciones.
- **Servicios**: www, dns, mail, etc.
- **Requerimientos de BW**: audio, video, downloading.
- **Facilidades**: BW constante, múltiples proveedores.
- **Seguridad**: ubicación de proxies, Cortafuegos (FireWalls), Sistemas de detección de intrusiones (IDSs).



Políticas

Ejemplos de “algunas” cuestiones a analizar

- 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: cuánto, cuándo, dónde?
- 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...

ISO

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**

FCAPS Gestión de Fallas

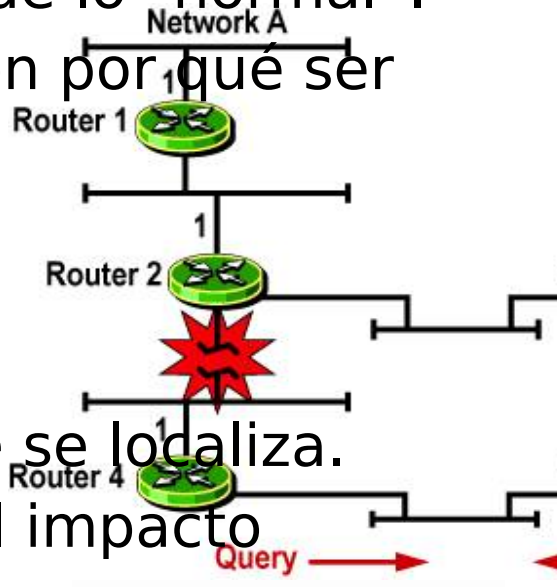
Engloba funciones para monitorear la red a fin de garantizar que
todo funcione correctamente. Abarca la atención y el procesamiento
de alarmas, pero también otras funciones tales como el diagnóstico y
la resolución de problemas.

- 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.

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.

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

Critical	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.
Major	A device is completely down or in danger of going down. Attention needs to be paid to this problem immediately.
Minor	A part of a device (a service, and interface, a power supply, etc.) has stopped functioning. The device needs attention.
Warning	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.
Indeterminate	No Severity could be associated with this alarm.
Normal	Informational message. No action required.
Cleared	This alarm indicates that a prior error condition has been corrected and service is restored

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 testing
- 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

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

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

Qué se puede "gestionar"?

- Habilitar/deshabilitar puertos/dispositivos
- Redireccionar tráfico
- Configurar tablas de rutas
- 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...

por ej: nodo puede actuar como router o como host

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

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.

FCAPS Gestión de la Contabilidad

Recolectar info de los dispositivos de la red

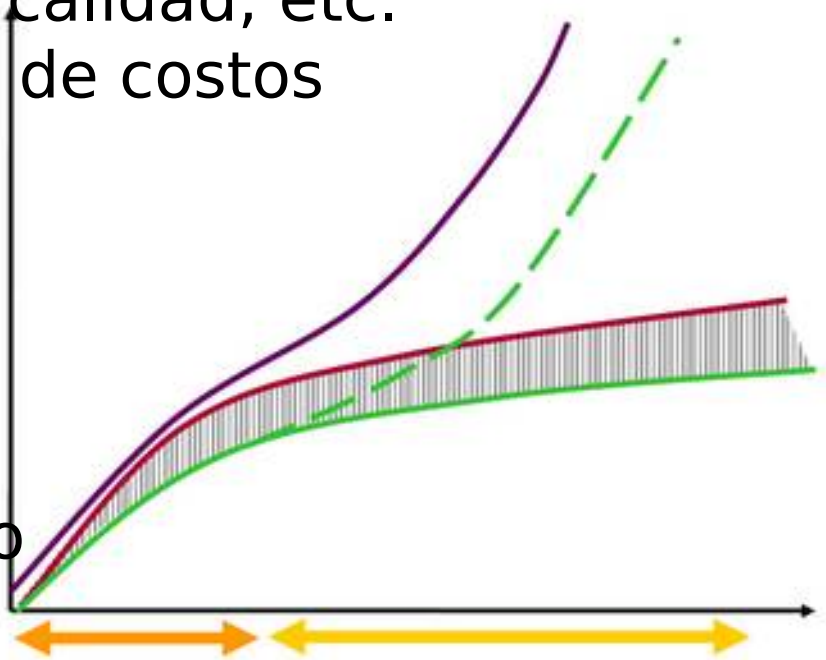
- Uso de recursos por impacto de costo
- Establecer “quotas”

Establecer “cargos” por uso

- Establecer medidas de costo (número de transacciones, paquetes, bytes, etc.), volumen o calidad, etc.
- Establecer claramente las políticas de costos

Analizar

- Uso vs cuotas
- Dominios de “cargos”
- Crear gráficas de tendencias
- Tratar de hacer predicciones de uso
- Proyectar costos futuros



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

FCAPS Gestión de la Performance

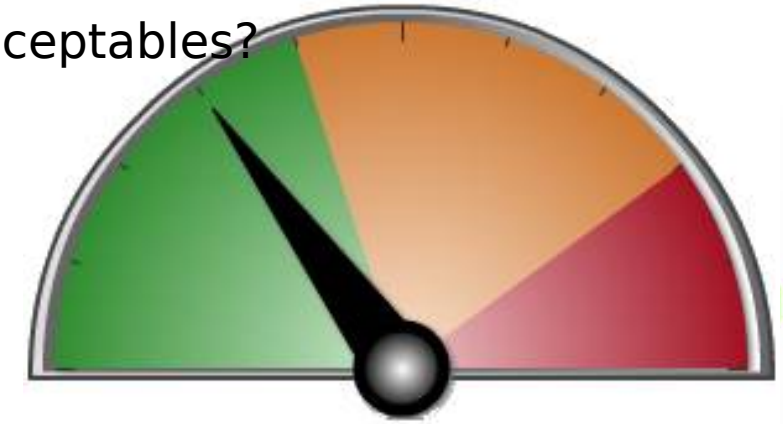
"Las redes modernas están compuestas de muchos componentes que se comunican y comparten datos y recursos. La efectividad de una aplicación depende cada vez más de unas prestaciones adecuadas de la red"

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?



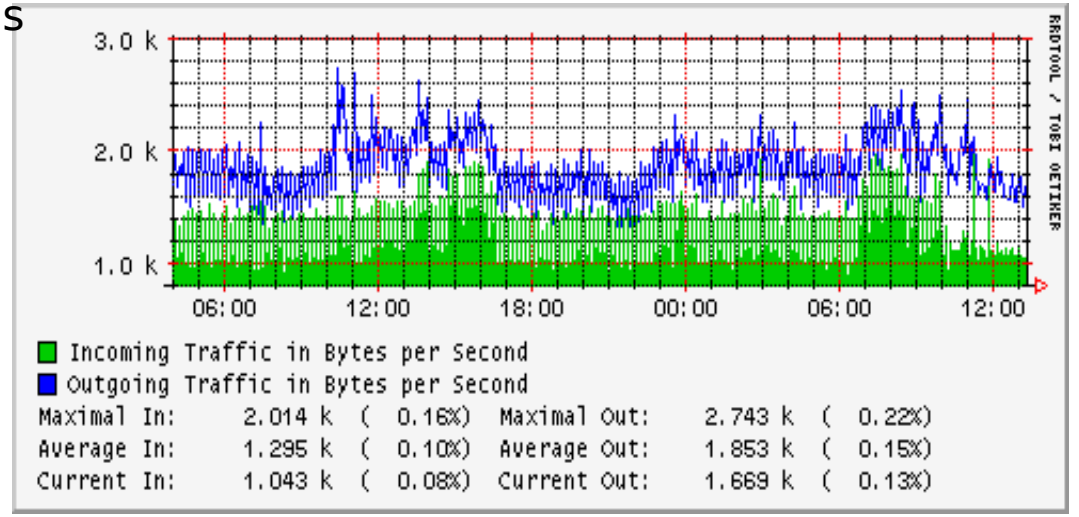
Requiere:

- 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...

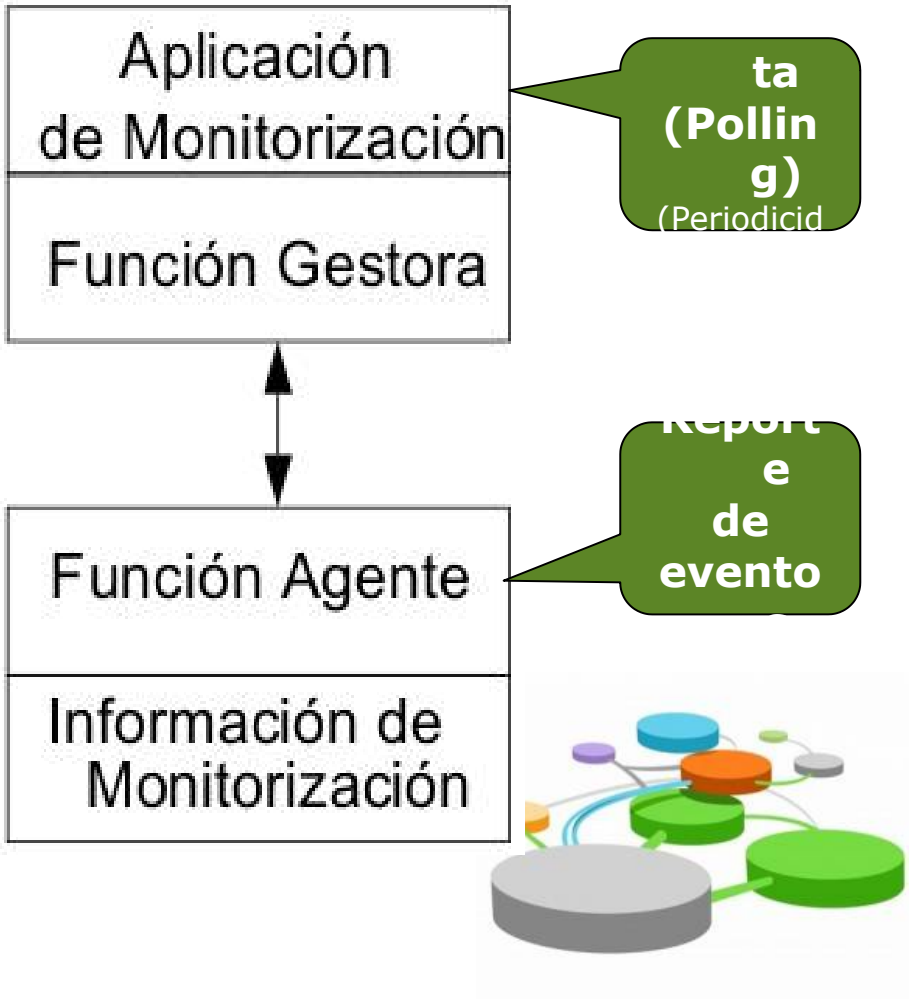
Performance
- Tiempos de respuesta
- Uso de CPU
- Tamaños de las colas

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.

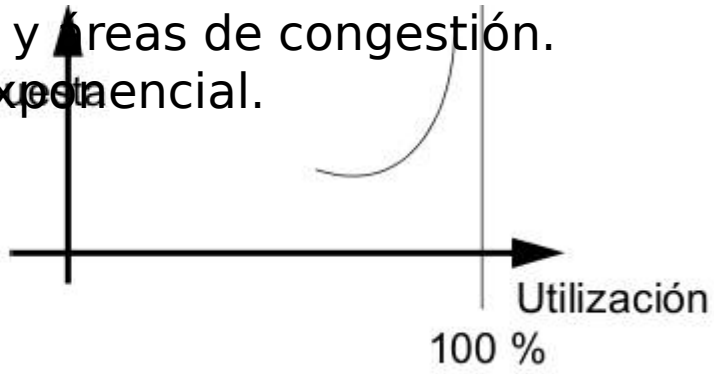
$$Disponibilidad = \frac{MTBF}{MTBF + MTTR}$$

- **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

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” a 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 mecanis- mos de seguridad (protocolos, cifrado, software, etc).
- Control de acceso (ACLs).
- Prevención de incidentes.
- Auditoría de eventos.

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

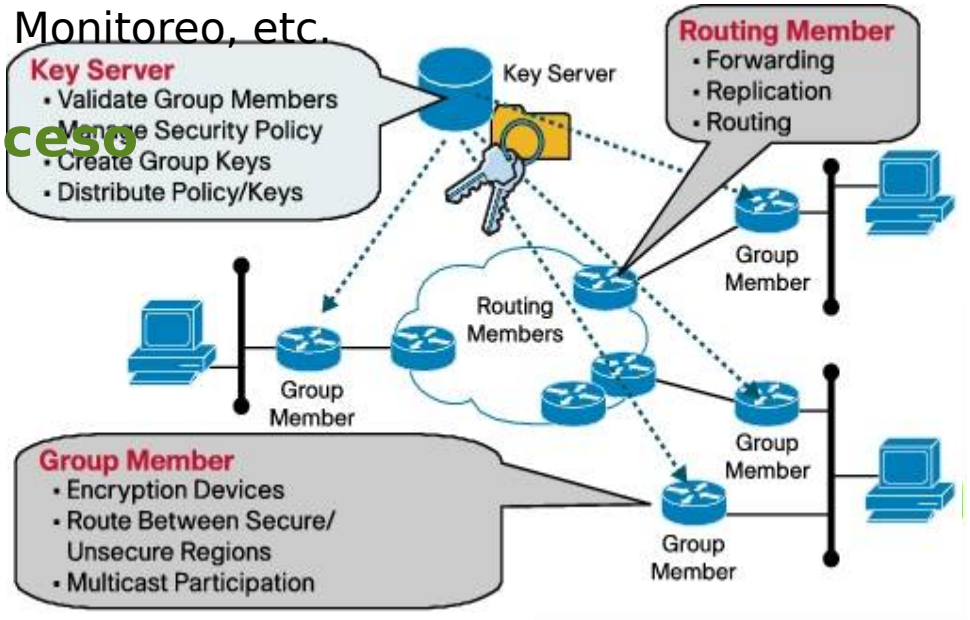
- En los servicios: mail, www, FTP, Rlogin, RPC, Monitoreo, etc.

Aplicar métodos de control de acceso

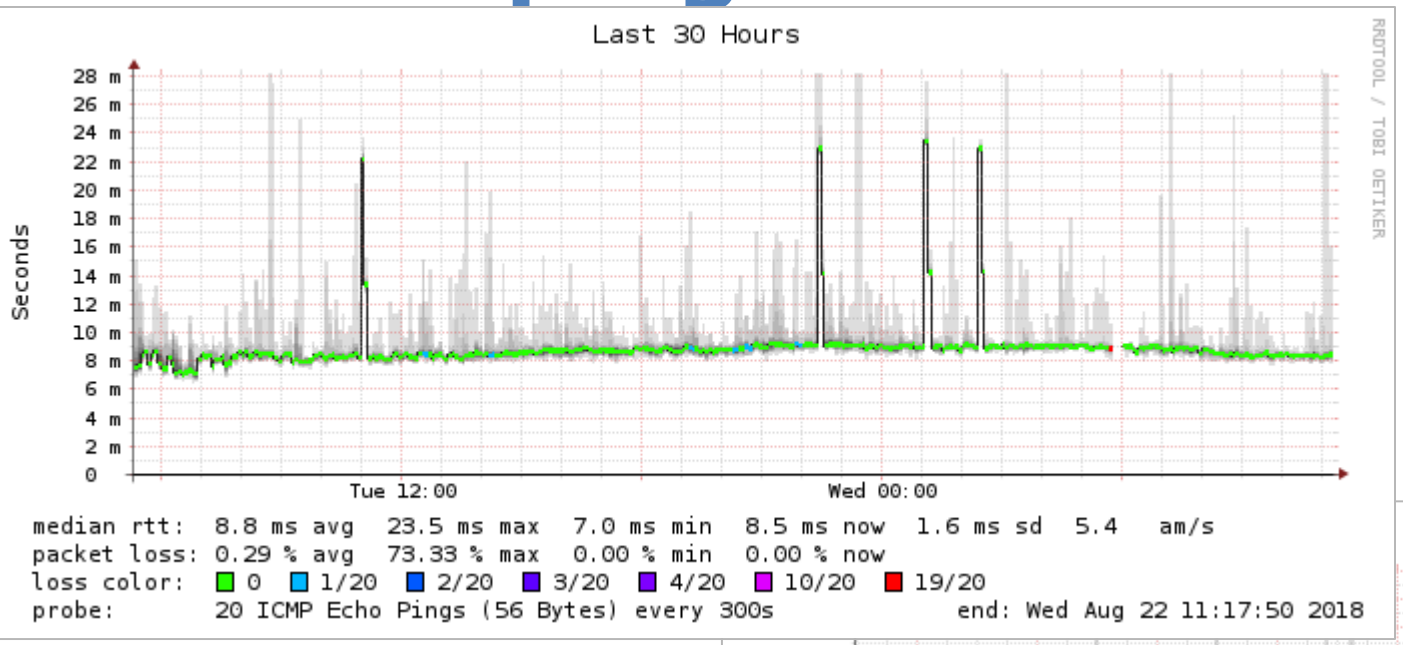
- Criptografía
- Filtrado de paquetes en routers/firewalls
- Source host/user authentication

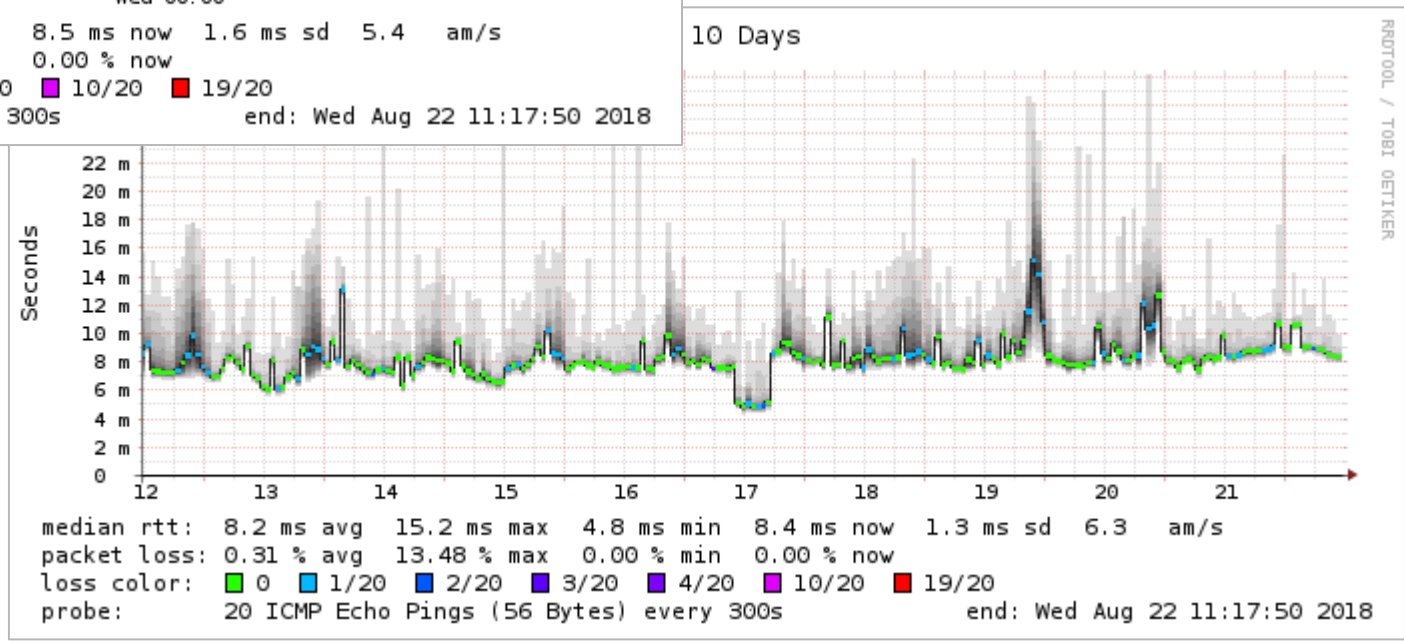
Mantenimiento

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



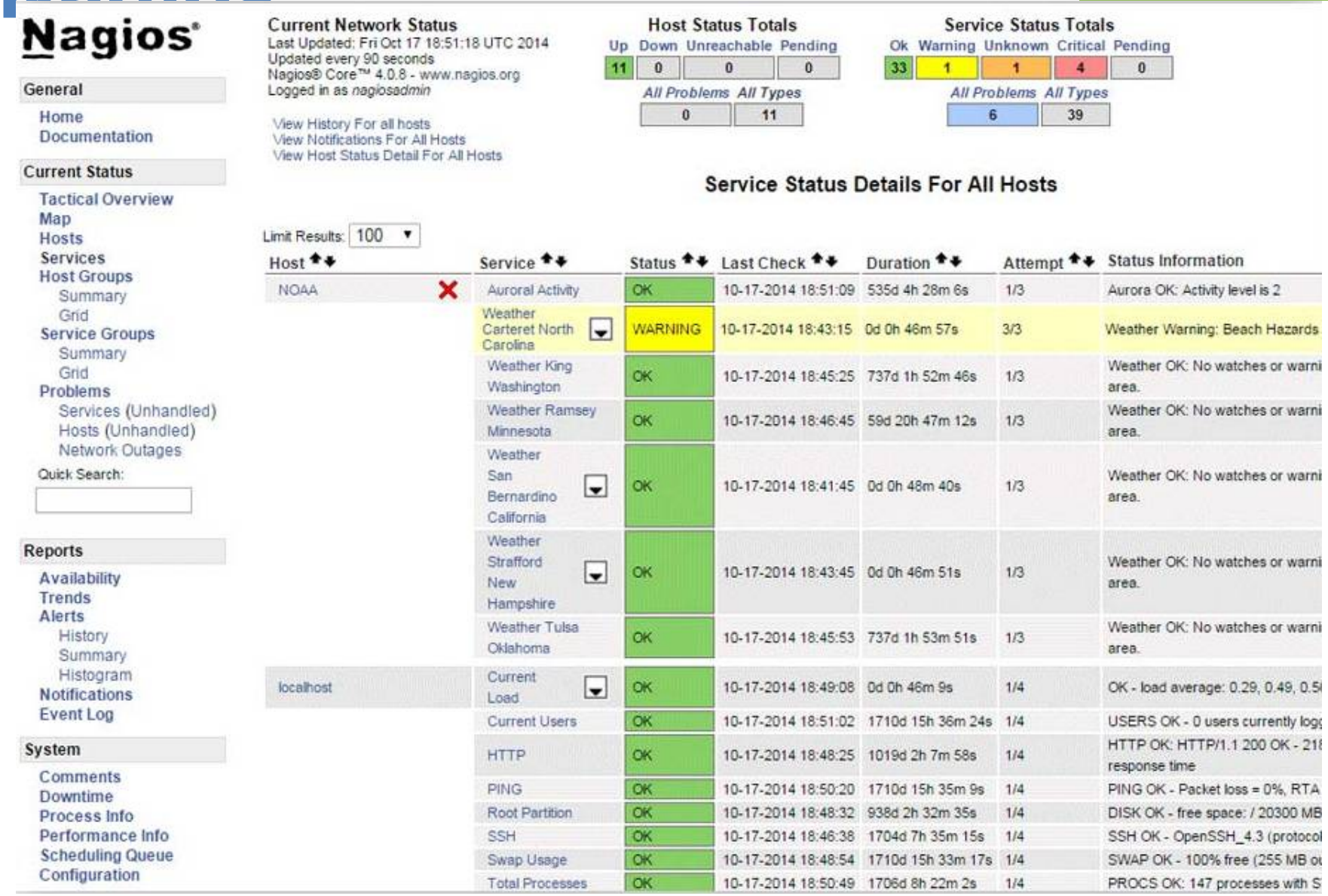
Soft para Monitoreo: Smokeping





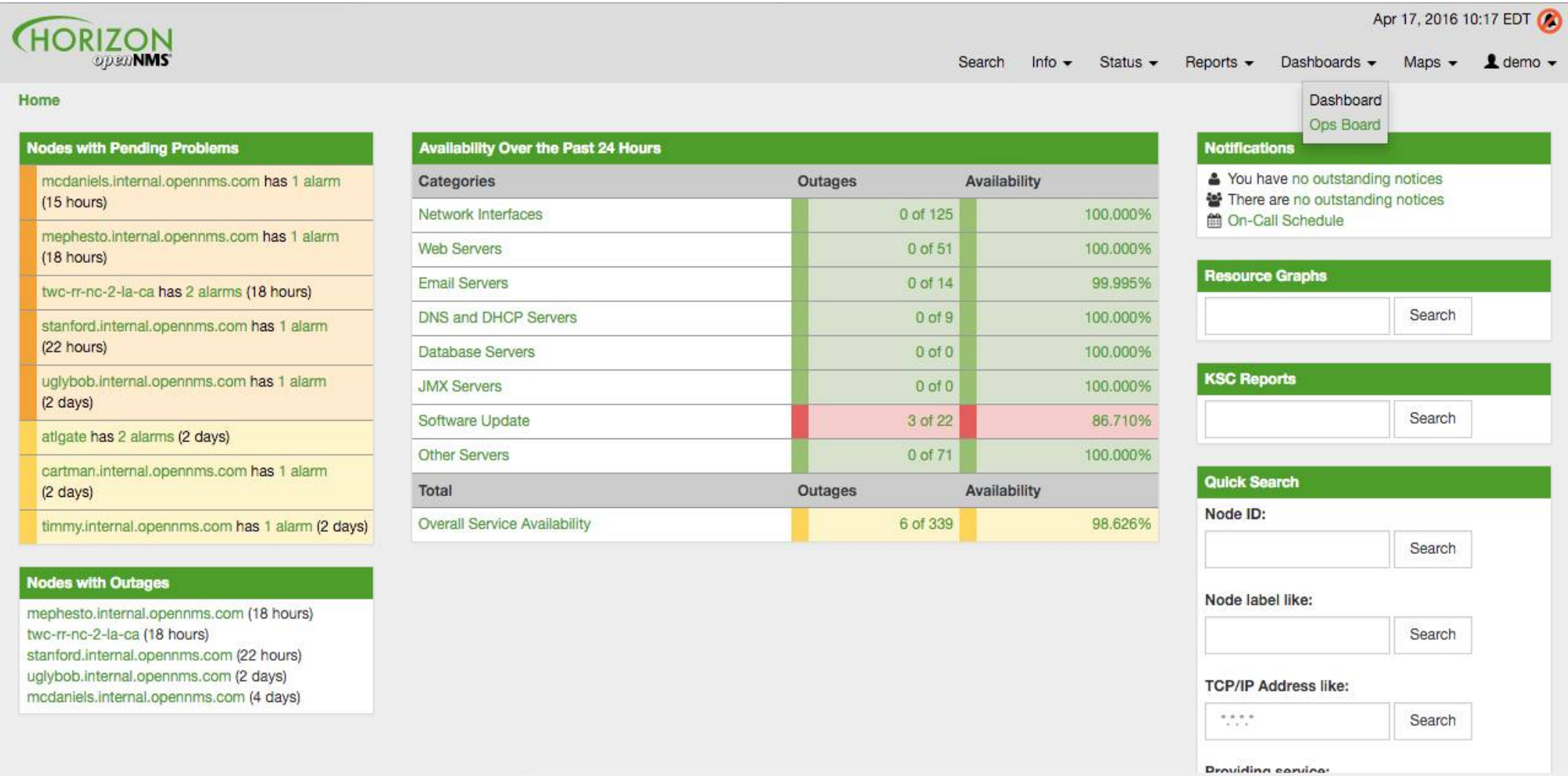
Smokeping UCDavis:
http://smokeping.ucdavis.edu/cgi-bin/smokeping.fcgi?target=Campus.Border

Soft para Monitoreo: Nagios



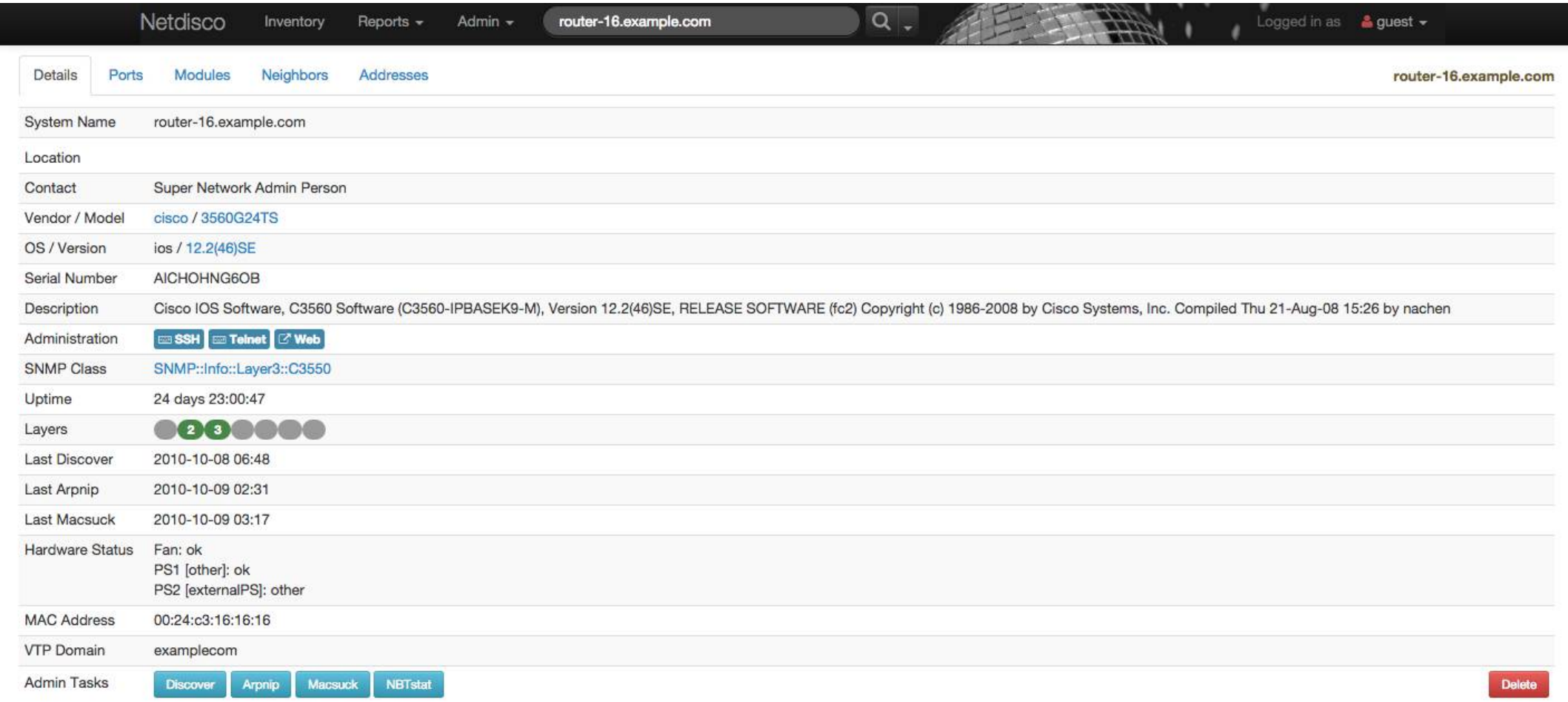
Demo online: http://nagioscore.demos.nagios.com/

Soft para Monitoreo: OpenNMS



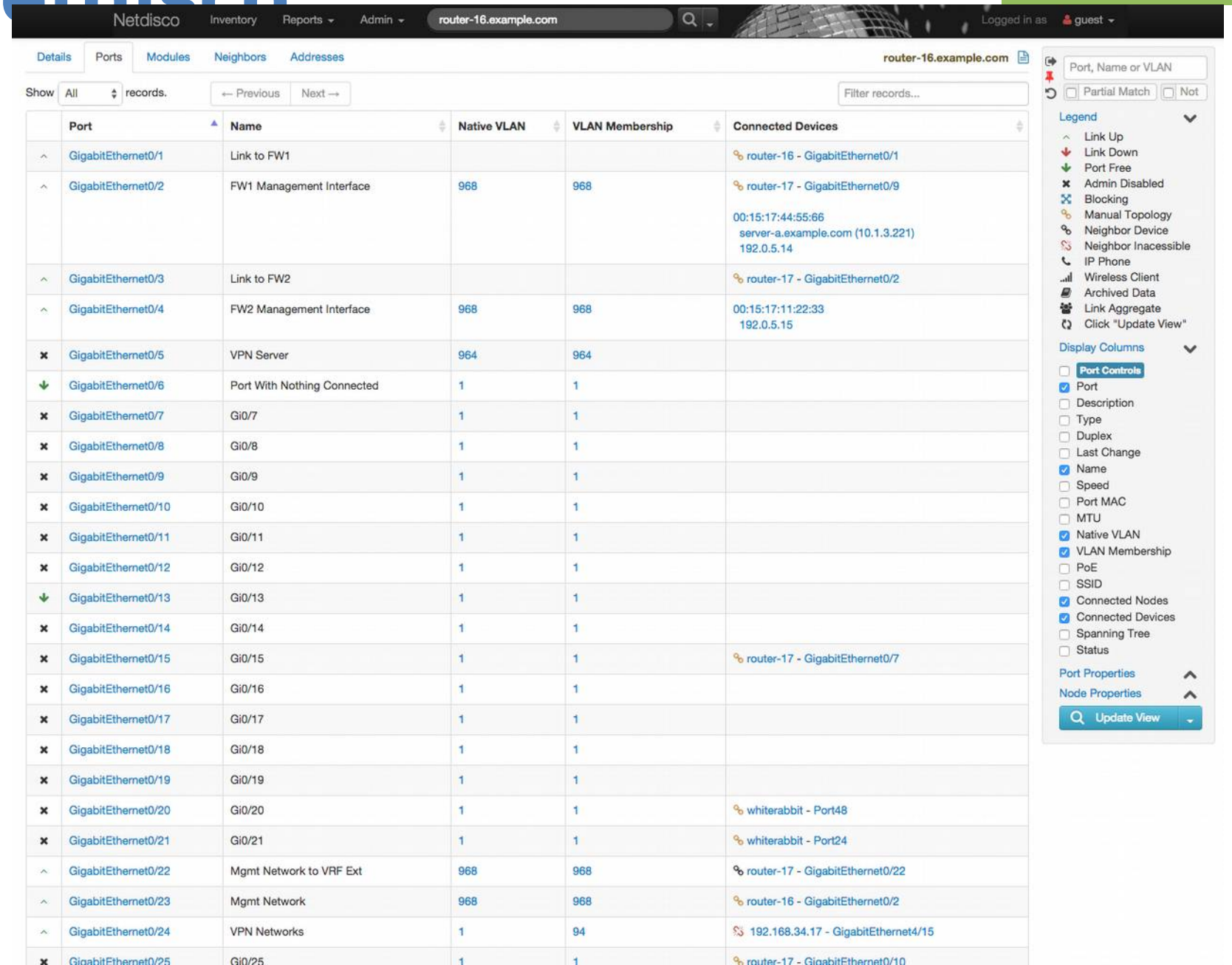
Demo online: https://demo.opennms.org

Soft para Discovery: Netdisco

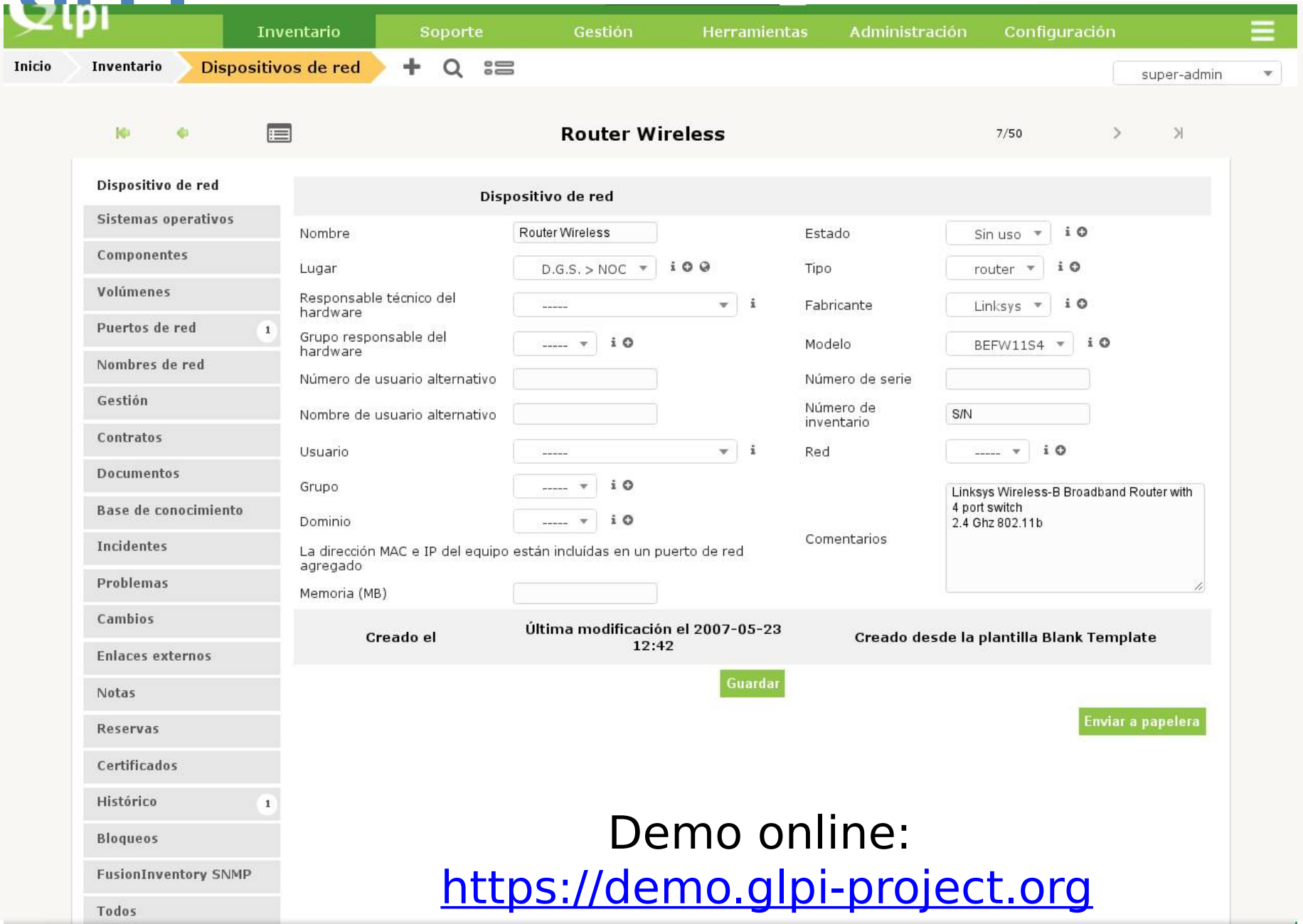


Demo online: https://netdisco2-demo.herokuapp.com/

Soft para Discovery: Netdisco

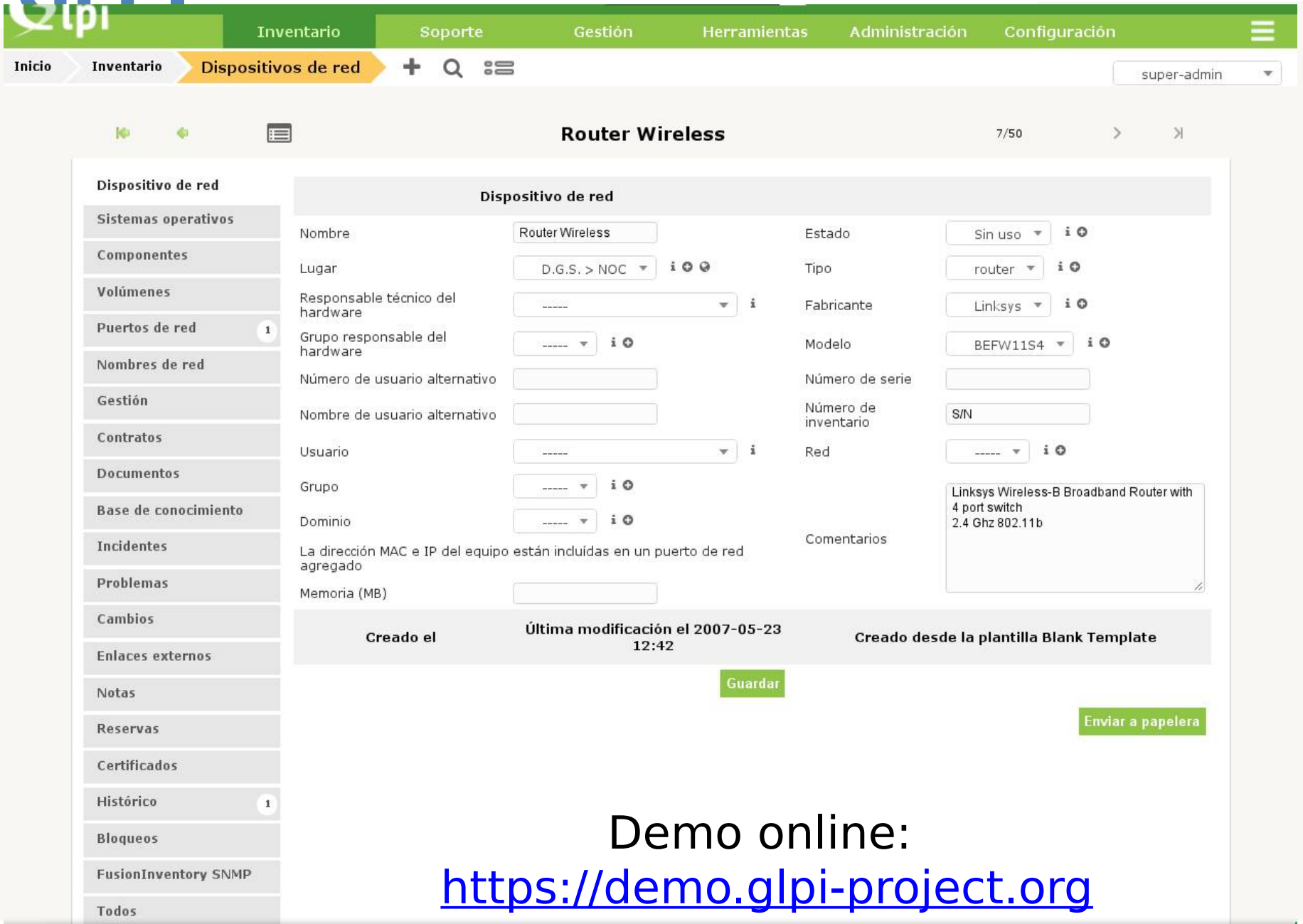


Soft para Inventario: GLPI



Demo online:
https://demo.glpi-project.org

Soft para Issue Tracking: GLPI



Demo online:
https://demo.glpi-project.org

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”

Próxima: Protocolo SNMP