ESPECIALIDAD FORMATIVA
GESTIÓN DE REDES DE VOZ Y DATOS

IFCM0310

UF1875: Gestión de recursos, servicios y de la red de comunicaciones

* Bibliografía usada en este documento:

UF1875: Gestión de recursos, servicios y de la red de comunicaciones, Autor: J. A. Jimenez Toro, EDITORIAL ELEARNING S.L. Edición: 5.0
Capturas de pantalla y textos electrónicos de varias web únicamente para ilustrar la actividad educativa

Luis Orlando Lázaro Medrano

Contenido

1. Gestión de recursos y servicios de la red de comunicaciones 1
1.1. Mapa de la red de comunicaciones. 1
1.2. Calidad de Servicio 2
El servidor de cola 8
Gestores de memoria 10
1.3. Centro de Gestión de Red, diseño y recursos implicados. 13
Componente Organizacional 15
Componente Funcional 17
1.4. Relación entre recursos y servicios 22
1.5. Herramientas para asignación de recursos: tipos y características 23
Sistema de Tickets 24
Sistema de órdenes de trabajo 24
Sistema de gestión de flujo de trabajo y motores de flujo de trabajo 24
1.6. Monitorización y rendimiento de servicios y recursos. 25
1.6.1. Clasificación de los sistemas de medida de consumos y rendimientos 26
1.6.2. Parámetros de rendimiento de los servicios ofrecidos en la red 28
Cacti 32
2. Gestión de redes de comunicaciones 43
2.1. Aspectos funcionales de la gestión de la red 43
Gestión de configuración 43
Gestión de fallos 44
Gestión de prestaciones 45
Gestión de contabilidad 45
Gestión de seguridad 46
2.2. Protocolo de gestión de red 48
CMIS/CMIP 49
SNMP 52
MIB 53
SMI 53
Syslog 57
Netconf 59
Protocolo TMN 61
2.3. Herramientas para la gestión de red 64
Cisco Prime. 65
HP IMC (Centro de administración inteligente). 67
Observer. 67
Tivoli NetView 68

Nagios 70
2.4. Supervisión red comunicaciones: tipos de incidencias, herramientas de notificación y alarmas..... 77
Tipo de Incidencias 77
2.5. Gestión centralizada y distribuida 82
Gestión centralizada 82
Gestión distribuida 82
2.6. Sistemas de gestión en operadores de telecomunicación 83
2.7. Los procesos de detección y diagnósticos de incidencias: herramientas específicas 86
Detección 86
Generación 87
Resolución 87
GLPI 89
2.8. Actualizaciones de software 97
RIS 99
OPSI 100
SpaceWalk 100
2.9. Planes de contingencias..... 101
Recursos y proceso vitales en la empresa 102
Análisis de riesgo 103
Protección de los puntos críticos..... 103
Estrategias y alternativas de recuperación 103
Equipos de trabajo y asignación de funciones 103
Pruebas del plan de contingencia..... 104
Manual de contingencia 104
Retroalimentación 105
Resumen 106

1. Gestión de recursos y servicios de la red de comunicaciones

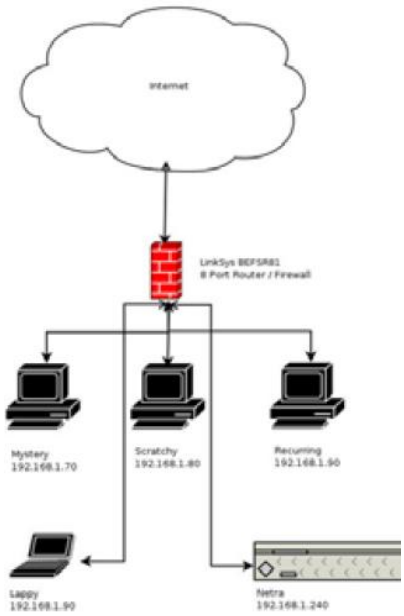
1.1. Mapa de la red de comunicaciones.

En toda red de comunicaciones para realizar diversas tareas de administración o realizar alguna tarea para reparar un error producido, necesitamos tener información de la red, ya sea información de localización física de los componentes como información lógica, como configuraciones.
Cuando se diseña una red de comunicaciones una forma de facilitar el trabajo es crear un mapa de red que es un documento gráfico donde se especifican los componentes de la red mediante una serie de elementos gráficos, este documento muestra de forma visual la organización de la red. En un mapa de red se debe incluir la siguiente información:

- Información física: donde especifica la ubicación física de todos los componentes; estaciones, router, switch, etc., como los enlaces (cableado) que existe entre los componentes de la red. Si la red está organizada en varias subredes o existe comunicación con otras redes, se especifica los dispositivos incluidos.
- Información lógica: información de configuración, como la dirección IP, MAC o cualquier otra información que lo identifique dentro de la red. Los nombres de los dispositivos, enlaces y subredes que componen la red, son incluidos en el diagrama.

Un mapa de red es un documento muy útil para el administrador, para conocer la organización de la red y en caso de algún problema localizar de forma más rápida el o los dispositivos involucrados. Un mapa de red permite examinar toda la red de forma visual y localizar un determinado componente de forma más rápida. Por ejemplo, si deseamos acceder a un determinado servidor para realizar diversas de tareas de administración, con el mapa de red podemos localizarlo rápidamente y conocer su dirección IP para poder acceder de forma remota, no debemos desplazarnos al servidor para acceder a él.

Hay varias herramientas que nos facilita la creación del mapa, este tipo de herramientas funcionan de dos maneras, con algunas herramientas creamos el mapa de red de forma manual, proporcionando diferentes opciones para la creación. Otro tipo de herramientas nos permiten crear el mapa de red de forma automática, se realiza un escaneo de la red, recoge información de la red y con la información obtenida el programa genera el mapa de red.
La primera categoría permite "dibujar" un mapa de red proporcionando diferentes conjuntos de figuras para los componentes de la red, solo tendremos que escoger las figuras, colocarlas y añadir información (IP, nombre, MAC, etc.), en redes grandes esta forma manual de generar un mapa de red puede resultar muy trabajosa.
Un ejemplo es el programa denominado Dia, un programa libre que nos permite realizar diferentes tipos de mapas proporcionando un conjunto de herramientas que nos ayudara para la creación del mapa de red y otro puede ser Draw.io que ya conocemos de sobra.



El segundo tipo de herramientas facilita mucho el proceso de crear el mapa de red, este tipo de programas escanean la red para hallar el esquema de la red, denominado topología, creando el mapa de forma automática con la información obtenida. Para el proceso de escaneo de la red, utilizan diversos protocolos que se encargan de obtener la información de los componentes de la red. Los protocolos más utilizados por este tipo de herramientas son:

- ⇨ **SNMP**: protocolo de la capa de aplicación utilizado para obtener información de diversos parámetros de los dispositivos de una red. Funciona mediante una serie de agentes instalados en los dispositivos gestionados por un gestor que monitorizan y recogen la información enviada por los agentes.
- ⇨ **RMON**: protocolo para monitorización utilizado en redes LAN, se puede considerar como sucesor de SNMP, definiendo un conjunto de funciones de comunicaciones. Utilizan un conjunto de monitores remotos y agentes de supervisión que pueden ser incluidos en los dispositivos gestionados. Este protocolo incluye un conjunto de objetos utilizados por los monitores.

- **CDP**: Protocolo de Descubrimiento de Cisco, protocolo desarrollado por la empresa Cisco System y utilizado en los equipos de esta empresa, como router o switch. Este protocolo funciona mediante la técnica de "descubrimiento de vecinos" este protocolo proporciona una alta independencia, tanto de los medios utilizados como de los protocolos de gestión.

También tenemos WMI desarrollado por Microsoft, que establece una serie de normas utilizadas para compartir información de administración, solo está disponible para redes Windows. WMI define una serie de propiedades independiente de la especificación donde este tipo de información puede ser compartida por las aplicaciones.

1.2. Calidad de Servicio.

QoS (Quality Of Service) sus siglas en inglés, especifica una serie de técnicas utilizadas para mejorar las capacidades de una red, modificando diversos parámetros de la red para mejora el rendimiento. Estas mejoras influyen en los servicios proporcionados por una red, si la red mejora su rendimiento los servicio que proporciona esa red también mejora su rendimiento. Estas técnicas funcionan bajo distintas tecnologías.

En la gran mayoría de los router implementan QoS que nos permite administrar el ancho de banda, como gestionar el tráfico, controlar el flujo de paquetes que entran y salen de la red según el tipo de paquetes u otro tipo de reglas.

Para aplicar QoS se deben medir un conjunto de parámetros como:

- **Ancho de banda**: cantidad de datos que es posible por unidad de tiempo. El objetivo es obtener el mayor ancho de banda posible, esto depende de múltiples factores, también es muy importante gestionar de forma óptima el ancho de banda para poder proporcionar múltiples servicios de forma correcta y que múltiples usuarios utilicen de forma concurrente los servicios de la red.
- **Retardo temporal y variación en el retardo (jitter)**: el primer factor implica que se produzcan retrasos en la comunicación, es la cantidad de tiempo que lleva transmitir un paquete desde un punto de la red a otro. El segundo factor, jitter, es definido como una fluctuación o variación en el tiempo de entrega de dos paquetes consecutivos (los milisegundos cuando hacemos ping), producida por varios factores como fallos en los enlaces, procesamiento lento de los paquetes en el router o retardo en la cola de los router. Estos dos factores perjudican mucho el rendimiento de la comunicación en la red y pueden afectar a cualquier servicio. Para un funcionamiento optimo estos dos factores deben tener un valor mínimo.
- **Pérdida de paquetes**: la información es transmitida mediante paquetes, si un paquete se pierde y no llega a su destino o es recibido con errores, se producen errores en la comunicación. Estos errores son producidos por diferentes motivos como:
  - Congestión en la red,
  - Fallos en los dispositivos de red.
  - Errores en las capas físicas.

Aplicando diferentes mecanismos, se puede conseguir que la tasa de error sea la mínima posible, aumentando la fiabilidad de la comunicación.

Para aplicar correctamente QoS en una red, hay que diseñar una política de prioridad de los servicios de la red. Dependiendo de las especificaciones de la red, algunos servicios serán más importantes que otros, dando una prioridad más alta a una serie de servicios con respecto a otros. QoS permite ofrecer diversos niveles de prioridad.

- Alta prioridad: asignando recursos para mejorar la calidad del servicio e incluso quitando recursos asignados a otros servicios con prioridad más baja.
- Baja prioridad: servicio de poca importancia en la red, algunos de sus recursos son asignados a otros servicios de prioridad alta.

Otro punto importante es saber cuándo aplicar QoS, primero debemos de estudiar qué tipo de tráfico se encuentra en la red. Podemos distinguir dos tipos de tráfico:

- Tráfico elástico: tráfico que puede ser ajustado fácilmente a las necesidades de la red, sin perjudicar al rendimiento de los servicios. Ejemplo de este tipo de tráfico es el generado por el protocolo TCP/IP.

- ⇨ Tráfico no elástico: tráfico que no permite una adaptación fácil a las necesidades de la red. Cualquier cambio que se produzca, afecta de forma negativa el rendimiento de la red y a los servicios. Ejemplo: tráfico en tiempo real, videoconferencia, VoIP, vídeo, etc.

Cada servicio tiene unos determinados requisitos QoS para obtener un óptimo funcionamiento en cada uno de ellos. Los requisitos son los comentados anteriormente; fiabilidad, retardo, jitter(variación de retardo) y ancho de banda. Un ejemplo de requisitos de QoS para diferentes servicios se muestra a continuación:

Servicio	Fiabilidad	Retardo	Jitter	Ancho de banda
Navegación Web	Alta	Medio	Alto	Bajo
Correo electrónico	Alta	Alto	Alto	Bajo
Telefonía	Media	Bajo	Bajo	Bajo
Video bajo demanda	Media	Alto	Medio	Medio
VoIP	Media	Alto	Medio	Alto
Videoconferencia	Media	Bajo	Bajo	Alto
Login remoto	Alta	Medio	Medio	Bajo

La fiabilidad influye si el servicio utiliza algún protocolo que proporciona seguridad en los datos, como TCP/IP, donde TCP se encarga de la seguridad de los datos transmitidos, realizando comprobaciones de datos en el destino. Algunos servicios que utilizan TCP son la navegación web, proporcionando fiabilidad de los datos transmitidos por la web.

Hay tres mecanismos para realizar QoS, para realizar una elección adecuada debemos tener en cuenta una serie de factores:

- ⇨ El problema que está intentando resolver, cada mecanismo está enfocado a un tipo de problema.
- ⇨ Cantidad de recursos disponibles, para saber cuántos recursos podemos asignar, algunos mecanismo requieren más recursos, conociendo los recursos disponibles, la elección del mecanismo a utilizar será más fácil.
- ⇨ La relación coste-beneficio, cada mecanismo tiene un coste y proporciona un beneficio, conocer la relación beneficio/coste será muy importante en el proceso de elección.

Para la realización de QoS en una red, se necesitan una serie de componentes.

- ⇨ Para aplicar QoS en una red se debe implementar una serie componentes como herramientas de gestión de colas, de planificación y espaciado de tráfico.
- ⇨ Técnicas de señalización de QoS, que permitirá conocer de forma eficiente lo que ocurre en los diferentes componentes de la red.
- ⇨ Funciones de gestión de QoS para controlar y administrar el tráfico.

Para cumplir los factores mostrados anteriormente, podemos distinguir tres tipos básicos de mecanismos.

- ⇨ Best Effort (BE): no realiza distinción entre los diferentes tipos de tráfico, cuando se produce congestión de tráfico simplemente aumenta el ancho de banda. Este mecanismo es utilizado en el protocolo TCP/IP. Como principal desventaja de este mecanismo es el alto coste que puede producir un aumento de ancho de banda de una red, como ventaja es la fácil implementación.
- ⇨ Servicios Integrados (IntServ): realiza una reserva extremo a extremo de recursos en los elementos que conforman la red. El tráfico que circula por la red se divide en diferentes flujos, creando un estado por cada tipo de flujo en cada nodo de la red que atraviese. Un protocolo de señalización, denominado RSVP, es el encargado de gestionar la reserva de recursos, señalar los flujos para su identificación y asignar de recursos necesarios. Para el correcto funcionamiento de IntServ necesita: crear, mantener y eliminar estados de los nodos de red, también implementa la comunicación de los nodos de red y equipos finales. Para cumplir esto, los equipos que actúen como nodos de red necesitan disponer de una serie de funcionalidades específicas, que deben ser implementadas por los fabricantes, con el

gasto que genera. Por ese motivo los fabricantes no han implementado este mecanismo en sus dispositivos y prácticamente no se utiliza. Otro punto a destacar es la sobrecarga que genera la reserva de recursos y la poca escalabilidad que proporciona.

- ⇨ Servicios Diferenciados (DiffServ): para evitar congestión en tráfico y garantizar QoS, este mecanismo permite que los dispositivos, como router o switch, tengan un comportamiento diferente en función del tipo de servicio que proporciona, permitiendo la coexistencia de diferentes servicios en la misma red. Esto se consigue, examinando el tráfico que genera un servicio y es marcado, este marca permite conocer de que servicio procede, ofreciendo un QoS diferente en función del marcado. Una ventaja, es que DiffServ es implementado dentro de los paquetes y no en los nodos de red, que permite tener servicios más escalables.

A continuación se explicara de forma mas detallada el mecanismo DiffServ, que es el más utilizado.
Como se ha mencionado anteriormente, este mecanismo realiza un marcado de los paquetes para realizar QoS en función de este. Para realizar esta tarea se añade al paquete un campo en la cabecera denominado DS, con la siguiente estructura.

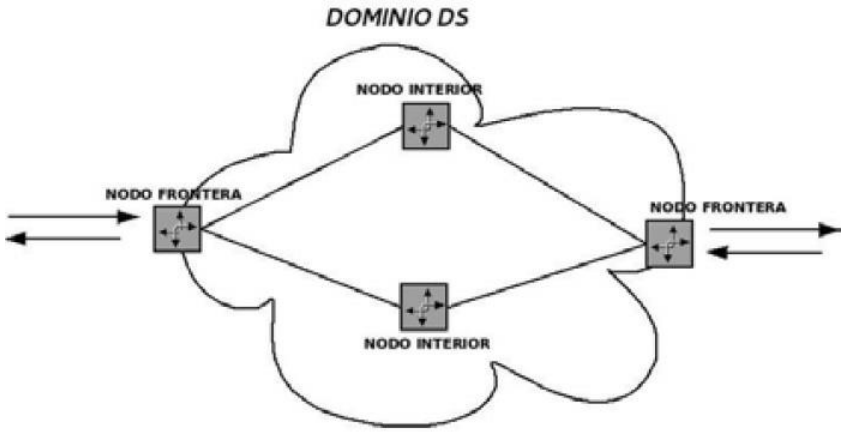
DSCP (6 bits)	Permite definir diferentes tipos de tráfico, máximo 64, mediante un código de 6 bits. Los valores se dividen en tres grupos: ⇨ Estándar. ⇨ Local/Experimental: Sólo válidos dentro de un dominio DS. ⇨ Reservado: Podrían ser estandarizados en el futuro.
ECN (2 bits)	Notifica situaciones de congestión, tiene cuatro valores: ⇨ 00: No hay congestión. ⇨ 10: ECN Capable Transport, desactiva ECT. ⇨ 01 : Activa el ECN Capable Transport (ECT), detectando una posible congestión ⇨ 11: congestión encontrada

En DiffServ existen tres tipos de servicios, cada uno de ellos proporciona una calidad de servicio. Estos tres tipos son:

- ⇨ Servicio Reenvío urgente (Expedited Forwarding o Premium): proporciona mayor calidad y equivale a ofrecer un servicio mediante una línea dedicada. Debe garantizar un caudal mínimo, proporciona pocas pérdidas, retardo y jitter. Este servicio es utilizado para VoIP o streaming de vídeo que necesitan una alta calidad en la transmisión un rendimiento óptimo.
- ⇨ Servicio Reenvío asegurado (Assured Forwarding): Proporciona un trato preferente, pero no garantiza ancho de banda, retardo, etc. En función del valor almacenado en el campo DSCP proporciona una prioridad de tráfico diferente, esto influirá en la posibilidad de que el servicio sea eliminado cuando se produzca una congestión en la red. Hay definidas cuatro posibles clases que tienen asignadas una cantidad de recursos (ancho de bando, espacio en buffers, etc.), cada clase es identificada por los tres primeros bits del DSCP y dentro de cada clase son especificadas tres categorías (alta, media y baja), que son identificadas por el cuarto y quinto bits. Estas categorías son utilizadas para especificar la prioridad de descarte en caso de congestión.
- ⇨ Servicio Por defecto (Best Effort): este servicio se caracteriza por tener a cero los tres primeros bits del DSCP. Este servicio no ofrece ningún tipo de garantía. No es necesario realizar cambios en la red.

La arquitectura de los Servicios Diferenciados DiffServ está basada en un modelo simple de clasificación de tráfico en la red, que es realizado en los límites de la red y asignado a diferentes grupos de tráfico de idéntico comportamiento. Cada comportamiento es identificado por un único DSCP. En el interior de la red, los paquetes se encaminan de acuerdo a un tratamiento particular, denominado comportamiento por saltos (PHB siglas en ingles) asociado al campo DS.
El componente principal de la arquitectura de los Servicio Diferenciados, DiffServ o DS, son los dominios o dominios DS. Este componente ha de ser entendido perfectamente para comprender el funcionamiento de los Servicios Diferenciados.
Un dominio DS está compuesto por una o más redes con una misma política de administración y un mismo PHB. Dentro de un dominio DS encontramos un grupo de nodos (nodos DS), en los límites del dominio son

definidos una serie de nodos frontera que son los encargados de la clasificación y marcado del tráfico de entrada al dominio.
Estos nodos frontera aseguran que los paquetes que entran al dominio estén marcados con un determinado PHB apropiado al dominio. Los nodos que están situados dentro del dominio, realizan el encaminamiento de los paquetes en función de su DSCP, dependiendo del marcado del paquete el nodo se comportará de manera diferente.



Los nodos frontera permiten la interconexión de varios dominios DS o con dominios que no soportan los Servicios Diferenciados. Deben ser capaces de aplicar un PHB apropiado a los paquetes basados en el campo DSCP. Además, puede ser necesario que apliquen mecanismo de adaptación del tráfico, definidas mediante un TCA (Traffic Conditioning Agreement), entre su dominio DS y los dominios DS conectados a él.
La interconexión entre dominio DS permite la comunicación de entre los dominios, los nodos frontera también actúan como nodos de Entrada/Salida al dominio.

- ⇨ Nodo entrada: encargado de comprobar que cualquier tráfico de entrada cumple con el TCA definido en el dominio.
- ⇨ Nodo salida: realiza una función de adaptación de tráfico para cumplir el TCA definido en el dominio.

Los nodos interiores solo están conectados con otros nodos interiores o con nodos frontera de su dominio. Estos nodos aplican el PHB apropiado a los paquetes basado en el DS, también deben realizar funciones de acondicionamiento de tráfico, aunque sus funciones son más limitadas que en el caso de los nodos fronteras.

Un acuerdo de nivel de servicio o Service Level Agreement (SLA), es un contrato escrito y firmado entre un proveedor de servicio y su cliente para marcar el nivel acordado de la calidad de dicho servicio. Un SLA es un documento donde especificar la clasificación del tráfico, las reglas de remarcado, los perfiles del tráfico y las acciones a llevar a cabo en los flujos de tráfico cuando éstos son adaptados o no a los perfiles dados.

Un dominio DS para su correcto funcionamiento necesita de una serie de componentes, estos componentes se resumen en dos:

- ⇨ Clasificador de paquetes.
- ⇨ Acondicionador de tráfico.

Un componente denominado clasificador es el encargado de realizar el proceso de clasificación del tráfico, realizando comprobaciones para que los paquetes cumplan determinadas reglas que son impuestas por un TCA determinado.
Existen dos tipos de clasificadores:

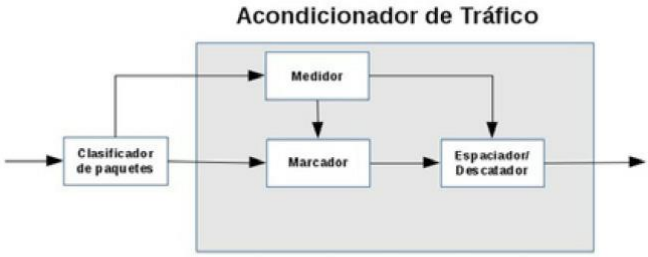
- ⇨ Clasificadores BA: realiza la clasificación de paquetes en función, y de forma exclusiva, del valor del campo DS solamente.
- ⇨ Clasificadores multicampo: clasifica los paquetes en función del valor de una combinación de campos de la cabecera.

Los clasificadores son utilizados para comprobar que los paquetes cumplen determinadas reglas. Los clasificadores deben configurar mediante diversos procedimientos que están cumpliendo las especificaciones del TCA apropiado. Además, los clasificadores deben autentificar la información que se usa para clasificar los paquetes.

TCA define un conjunto de reglas que son utilizadas para clasificar el tráfico, incluye un conjunto de parámetros como, perfiles de tráfico, marcados, descartes o cualquier otra acción que es aplicada al tráfico seleccionado.
Un perfil de tráfico especifica las propiedades de un flujo de tráfico seleccionado por un clasificador, especificando que reglas debe cumplir para ser incluido dentro de un perfil, si no cumple esas reglas no se considera que esta fuera del perfil.
Si un determinado flujo de tráfico se encuentra fuera de un perfil, se pueden aplicar un conjunto de acciones que permitan realizar una modificación del paquete para incluirlo dentro del perfil.
A los paquetes que están dentro del perfil se le permite el acceso al dominio DS sin realizar ningún procesamiento extra, en cambio a los paquetes que estén fuera del perfil son enviados a una cola hasta que cumpla las reglas especificadas en el perfil.
Cuando se cumplan las reglas del perfil, los paquetes serán validados por el perfil y pueden ser descartados o marcados con un nuevo código.
Un acondicionador (adaptador) de Tráfico pueden contener los siguientes elementos:

Medidor	Componente que gestiona (midiendo) el flujo de entrada de paquetes al acondicionador en función de los parámetros de velocidad de tráfico y en caso contrario, ejecutar alguna acción que corrija la velocidad del flujo de paquetes.
Marcador	Componente que realiza dos tareas, marcar un paquete en función del campo DSCP de su cabecera, modificando el comportamiento del paquete DS. Se puede configurar el marcado de varias formas, especificando una marca a un grupo de paquetes o marcar un paquete especifico. La otra tarea que puede realizar es dejar el paquete como esta sin realizar un proceso de marcado.
Espaciadores o Descartador	El espaciador retarda un paquete o un conjunto de ellos, hasta que cumpla con el perfil de tráfico exigido, para realizar esta tarea los paquetes son enviados a una cola finita. El descartador realiza un proceso de eliminación de aquellos paquetes que no cumplan con el perfil o que cumplen con un perfil de descartes.

Un clasificador realiza un proceso de selección de paquetes de un flujo de tráfico en función de ciertos parámetros incluidos dentro de la cabecera del paquete. Los paquetes son enviados al acondicionador, la entrada de paquetes al acondicionador son regulados por un medidor, los paquetes pueden ser marcados modificando su comportamiento o no marcados dejándolos igual que como han entrado en el acondicionador. Por último, los paquetes pueden ser espaciados, sufren un retardo enviándolos a una cola, o descartados en función de los requisitos del tráfico.
Los acondicionadores de tráfico son situados en los nodos frontera de un dominio DS, aunque se pueden situar en un enrutador o en el computador de un usuario, que permite estar más cerca de las fuentes de tráfico de la red.
Componentes del acondicionador de tráfico.



Los acondicionadores de tráfico y los clasificadores multicapa están generalmente localizados en los nodos frontera del dominio DS, pero pueden ser encontrados en nodos interiores de un dominio DS o en nodos dentro de un dominio no DS.

- ⇨ Nodos frontera de un dominio DS: son nodos que encontrados en los límites de un dominio, también son nodos de entrada/salida de un dominio, en ambos casos su función es clasificar, marcar o acondicionar un flujo de tráfico. El SLA es el encargado de especificar qué dominio tiene la responsabilidad de mapear los flujos de tráfico a los DS BA y acondicionarlos de acuerdo con el TCA apropiado. Sin embargo, un nodo DS de entrada debe asumir que el tráfico entrante puede no estar conforme con el TCA y debe estar preparado para aplicar el TCA de acuerdo con la política local. Si un nodo de ingreso está conectado a un dominio superior no capaz de DS, el nodo de ingreso DS debe poder cumplir con todas las funciones de condicionamiento de tráfico necesarias en el tráfico entrante.

- ⇨ Dentro del dominio origen: es un nodo que origina el tráfico y recibe un servicio particular. El tráfico originado en el dominio fuente a través de una frontera puede ser marcado por las fuentes de tráfico directamente o por medio de nodos intermediarios antes de que dejen el domino origen. Esto se conoce como "pre-marcado", que conlleva varias ventajas.
  - Es más fácil realizar la gestión del tráfico por parte del nodo
  - Permite realizar un premarcado al tráfico, permitiendo que la clasificación sea más simple.

  Los nodos frontera del dominio origen también pueden monitorizar el tráfico y aplicar diferentes políticas según las especificaciones del TCA.
- ⇨ Dominio no DS: Las fuentes de tráfico o nodos intermedios de un dominio no DS pueden realizar un proceso de adaptación del tráfico antes de alcanzar un nodo de entrada en un dominio DS.

Un PHB describe el comportamiento de un tráfico en función del encaminamiento a través de los nodos de un dominio y está asociado a un DS. Un clasificador BA clasifica los paquetes en función del valor en el campo DS, obteniendo un conjunto paquetes que llevan asociado en mismo valor DSCP. El PHB se refiere al tratamiento específico que reciben en un nodo los paquetes que corresponden a un tráfico clasificado por un BA concreto. Esto permite diferenciar los diferentes servicios asignándole un comportamiento en los nodos de un dominio.

PHB especifica una serie de operaciones (prioridad, programación, encolado o espaciado) de paquetes, de modo que un nodo realiza en algunos paquetes de un clasificador BA y debe estar conforme a un SLA o política definidas.

Hay varios tipos de PHB que son implementados en los nodos de un dominio DS.

Por defecto	Si un paquete llega a un nodo DS el valor de DSCP no está incluido en un PHB, se le asigna un PHB por defecto que especifica un valor de DSCP 000000 que corresponde a un comportamiento tipo Best Effort.
Selector de clase	Este tipo de PHB corresponde a valores DSCP xxx000, x es un valor entre 0 y 1, y proporciona compatibilidad con un diseño anterior denominado IP Precedence.
Encaminamiento asegurado	Proporciona un ancho de banda garantizado con pocas pérdidas, baja latencia y bajo jitter. Es el más indicado para aplicaciones que requieran una alta prioridad para el tráfico, utilizado para VoIP. El DSCP asignado es 101110.
Encaminamiento rápido	Define un método por el cual los clasificadores BA pueden recibir diferentes tipos de encaminamiento. Se denominan AF y hay cuatros clases; AF1, AF2, AF3 y AF4. A cada clase se le asigna una cantidad de ancho de banda.

En los nodos frontera e interiores de un dominio DS se llevan diversas funciones de encolamiento para realizar un proceso de adaptación en el tráfico entrante o saliente del domino. Además, en esta cola los nodos DS pueden definir un tratamiento particular que recibirán los paquetes de un flujo de tráfico.

Una congestión de red se produce cuando los paquetes llegan a un nodo más rápido de lo que pueden ser transmitidos, en el nodo se envían a una cola donde esperan ser transmitidos a su destino, para controlar la congestión de la red podemos utilizar dos componentes.

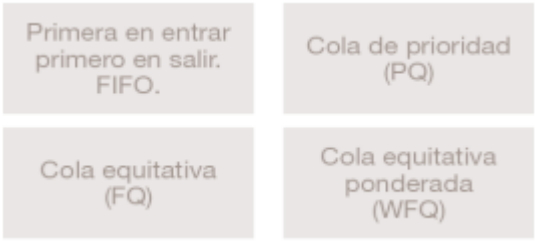
- ⇨ El servidor de cola: gestiona la cantidad de ancho de banda reservado para cada tipo de servicio en un nodo de salida. El servidor de la cola controla el acceso de los servicios a unos recursos disponibles de la red, decide qué paquetes son extraídos de una cola y cuando estos paquetes son preparados en el nodo para ser transmitidos a su destino.
- ⇨ El gestor de la memoria de la cola: controla el número de paquetes que hay dentro de la cola, especificando los paquetes que son descartados y cuando, este proceso se realizar cuando se produce una congestión e incluso puede ser realizado este proceso antes de que ocurra la congestión. El gestor de la memoria permite controlar el acceso de los servicios a los recursos disponibles en el nodo.

Aunque estos dos mecanismos están estrechamente relacionados, existen diferencias. La principal diferencia es el comportamiento de cada uno de ellos cuando se produce una congestión.

El servidor de cola controla la congestión gestionando el ancho de banda que reserva para cada servicio, mientras el gestor de memoria controla la congestión mediante la gestión de la longitud de la cola de paquetes, cuando se considera que la longitud de la cola es excesivamente alta, realiza un proceso descarte de paquetes.

El servidor de cola

El servidor de colas debe decidir que paquetes entran y salen de la cola, para realiza el proceso de elección de paquetes utiliza diversos varios algoritmos o estrategias.



FIFO (Primero en entrar, primero en salir)

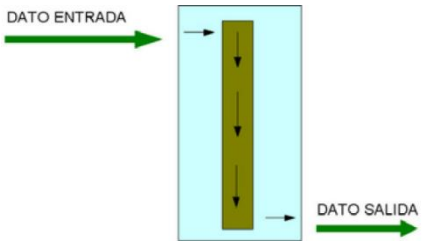
Todos los paquetes son tratados por igual, sirviendo los paquetes en el mismo orden en el que entraban en la cola (Primero en entrar, primero en salir). Es el mecanismo de encolamiento más simple. Como beneficios podemos encontrar:

- ⇨ Tiene una carga al sistema muy pequeña debido a su simplicidad, es el algoritmo con la menor carga de procesamiento.
- ⇨ Tiene un comportamiento muy predecible.

Como desventajas tenemos:

- ⇨ Como no realiza distinciones, no puede especificar un comportamiento diferente en función del tráfico, no implementa un sistema de prioridades.
- ⇨ Existe una sola cola y todos los flujos de tráfico son tratados de la misma forma, cualquier anomalía, por ejemplo un retardo, que se produzca debido a una congestión, afectara a todos los flujos por igual.
- ⇨ En FIFO se benefician más a los flujos UDP sobre los TCP. Esto es debido a que TCP implementa mecanismo de control para solucionar la congestión, reduciendo la tasa de transmisión. Mientras que las aplicaciones UDP no implementan este tipo de mecanismo y siempre transmiten con la misma tasa de transmisión. Este efecto produce que las aplicaciones TCP sufran retrasos que no sufren las aplicaciones UDP.
- ⇨ Cuando se produce un flujo de tráfico grande, puede consumir toda la memoria de la cola FIFO, produciendo que al resto del flujo se le niega el servicio, hasta que se vaya procesando el flujo en cola, liberando espacio. También provoca otro efectos colaterales como aumento del retardo, jitter y pérdidas.

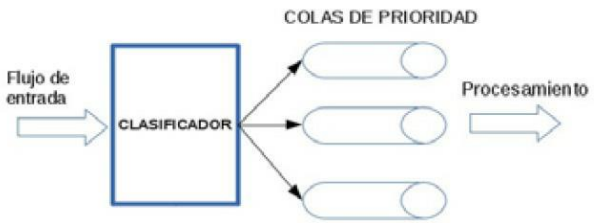
Las colas FIFO son simples, lo que implica que son fáciles de implementar, pero su rendimiento no es el más optimo comparado con otros mecanismos. Son utilizadas habitualmente como mecanismo por defecto en situaciones donde no hay ningún otro mecanismo configurado. En muchas ocasiones, son utilizadas en conjunto con otros mecanismos de encolamiento.



Cola de Prioridad (PQ)

En los Servicios Diferenciales, las colas PQ es un método fácil de implementar, frecuentemente utilizado como base para otros sistemas de encolamiento.

Su funcionamiento es el siguiente: primero realiza una clasificación de paquetes que se reciben y colocándolos en una de las varias colas disponibles en función de una prioridad asignada. Los paquetes solo se sirven de una determinada cola, escogiendo la cola con una prioridad mayor, dentro de cada cola se sirven mediante FIFO.



PQ ofrece varias ventajas.

- ⇨ Las colas PQ no proporciona mucha carga al sistema.
- ⇨ Utilizando la prioridad, permite asignar a diferentes flujos de tráfico un procesamiento diferente. Aquellos servicios que le afectan más el retardo se le asigna una prioridad alta.

PQ tiene varias desventajas.

- ⇨ Las colas con alta prioridad pueden acaparar de forma excesiva los recursos del sistema, esto se produce cuando existe mucho tráfico en estas colas, que pueden perjudicar a las colas con prioridades más bajas, con un retardo alto el tráfico que almacenan.
- ⇨ Si el tráfico de alta prioridad es muy alto, puede llenar la memoria asignadas a las colar y descartar todo el tráfico de prioridad baja por no tener memoria disponible.
- ⇨ Cualquier anomalía que afecte al tráfico de las colas con alta prioridad, afecta al tráfico de las colas de baja prioridad.

Hay dos tipos de funcionamiento para las colas PQ:

- ⇨ PQ estricto: Los paquetes con una prioridad más alta en la cola son servidos antes que paquetes en colas con más baja prioridad, siempre que haya un paquete de alta prioridad no se servirán paquetes de baja prioridad.
- ⇨ PQ controlado: Los paquetes con una prioridad más alta son servidos antes que paquetes en colas con prioridad más baja, siempre cuando el tráfico en la cola de mayor prioridad permanece por debajo de un umbral configurado por el usuario.

Cola Equitativa (FQ)

Todas las colas que se implementen que esta técnica, están diseñadas para que cada flujo de tráfico tenga una acceso justo (equitativo) a los recursos de la red y evitando que un flujo de tráfico consuma más ancho de banda del que le correspondería.

Su funcionamiento es el siguiente; primero clasifica los paquetes recibidos en función de diversas políticas y son asignadas a un cola, hay un número de colas FIFO configurables que tienen diversas prioridades.

Los paquetes almacenados en las distintas colas se van sirviendo mediante un mecanismo Round Robin.

Round Robin es un método para seleccionar cada uno de los elementos de un conjunto de manera equitativa y en un orden lógico, normalmente comenzando por el primero hasta llegar al último de la lista y empezando desde el principio.

FQ tiene una serie de ventajas y desventajas.

Ventajas

- ⇨ Las anomalías que se detecten en una cola solo perjudicará a esa cola, sin afectar a la calidad de servicio del resto de colas.
- ⇨ Si un flujo de tráfico realiza un consumo excesivo de recursos solo afectará a la cola donde esté almacenado, sin influir al resto de colas.

Desventajas

- ⇨ FQ solo se implementa mediante software y no en hardware.
- ⇨ FQ reserva la misma cantidad de ancho de banda para cada flujo. No permitiendo un ancho de banda diferente para un determinado flujo.
- ⇨ FQ funciona de forma óptima siempre que los paquetes almacenados en las colas tienen el mismo tamaño, asignándole el mismo ancho de banda, no funciona si los paquetes tienen diferentes tamaños.
- ⇨ FQ es sensible al orden de llegada de los paquetes.
- ⇨ FQ no es adecuado para servicios en tiempo real, como VoIP.
- ⇨ Existe una alta dependencia en función del mecanismo empleado para clasificar los paquetes.

Hay varias implementaciones donde se utiliza FQ.

- ⇨ FQ se aplica normalmente en las entradas de una red, donde los clientes se conectan con sus proveedores de servicio.
- ⇨ FQ proporciona un aislamiento ideal para flujos de tráfico individuales ya que en las entradas de la red de un cliente normal tiene un número de flujos limitado.
- ⇨ FQ basado en clases, clasifica los flujos de tráfico en un número de diferentes clases de servicio. Para cada clase de servicio se reserva un porcentaje del ancho de banda de salida configurado por el usuario y que depende de las especificaciones del servicio. Entonces hay una cola FQ para cada clase de

servicios. Como resultado, todos los flujos asignados a una clase de servicio, obtienen un reparto igual del conjunto de ancho de banda configurado para esa clase de tráfico en particular. Por ejemplo. Podemos reservar un porcentaje de ancho de banda de salida a un determinado servicio, como VoIP (30%) que requiere una cantidad de ancho de ancho alto para que el servicio sea estable y el resto del ancho de banda se le asigna al tráfico IP (70 %). Todos los flujos de VoIP que se reciban se le divide el ancho de banda en partes iguales dentro de ancho de banda asignado (30%).

Cola Equitativa Ponderada (WFQ)

WFQ es una solución basada en FQ que soluciona sus limitaciones. WFQ tiene varias colas que le asigna un peso, calculado mediante una fórmula, que es utilizado para la asignación del ancho de banda. Con esto se elimina una de las limitaciones de FQ, poder asignar diferentes ancho de banda a los flujos de tráfico.
Otra limitación de FQ es que elimina WFQ, soporta paquetes de tamaño variable en las colas. Esto impide, que los paquetes de mayor tamaño dispongan de mayor ancho de banda y que una paquete de menor tamaño se le asigne un ancho de banda mayor y no en función de su tamaño.
WFQ soporta la distribución equitativa del ancho de banda de paquetes de longitud variable mediante la aproximación a un sistema de procesador compartido generalizado (GPS siglas en ingles). Esta aproximación soporta la reserva de forma equitativa el ancho de banda, teniendo en cuenta la longitud del paquete.
Como resultado, en algún momento, cada cola recibe su porción del ancho de banda configurado.
Como ventajas WFQ tiene:

- ⇨ Cada servicio obtiene un ancho de banda garantizado.
- ⇨ Un reparto equitativo del ancho de banda, permite que el retardo sufrido en las colas sea mínimo.

WFQ tiene varias limitaciones.

- ⇨ No existe una implementación de WFQ mediante hardware, solo esta disponibles soluciones software. Al no existir soluciones hardware, el rendimiento es menor y las implementaciones son más complejas.
- ⇨ El algoritmo utilizado por WFQ es complejo y requiere un mantenimiento alto.
- ⇨ La escalabilidad que proporciona WFQ es baja, debido a su complejidad.

Las implementaciones de WFQ y sus aplicaciones:

- ⇨ WFQ se puede configurar para clasificar paquetes para un número de colas determinado.
- ⇨ WFQ permite al sistema servir un número limitado de colas que reciben un conjunto de flujos de tráfico. Para cada cola se reserva un porcentaje diferente del ancho de banda basándose en el peso que el sistema calcula para cada clase de servicio. Esta aproximación le permite al sistema reservar diferentes cantidades de ancho de banda a cada cola basándose en la política de QoS.
- ⇨ Una variación WFQ, Class-Based WFQ, se utiliza para servir un número limitado de colas que lleve un conjunto de flujos de tráfico. Para esta configuración las reglas de clasificación de paquetes definidas por el usuario asignan los paquetes a colas que tienen reservado un porcentaje del ancho de banda configurado por usuario. Esta aproximación permite determinar de manera precisa que paquetes se agrupan en una clase de servicio dada y especificar la cantidad exacta de ancho de banda reservado para cada clase de servicio.

Todas las colas tienen una memoria asignada donde almacenar los paquetes que va recibiendo, esta memoria está limitada y solo permite almacenar un número determinado de paquetes. Cuando el número de paquetes es mayor que la memoria disponible en esa cola, se produce una congestión, que debe ser evitado en una red.

Gestores de memoria

Para evitar la congestión se utilizan los gestores de memoria activa, que gestionan el uso de memoria de la cola. Cuando se produce un incremento en el uso de memoria muy alto, el gestor aplicará diferentes mecanismos para evitar el agotamiento de la memoria libre, produciendo una congestión. Actúa de forma activa antes de producirse la congestión.
Como ejemplo, para las redes IP tenemos dos mecanismos que permiten una gestión activa de la memoria de las colas:

- ⇨ Random Early Detection (RED), descarte aleatorio temprano.
- ⇨ Explicit Congestion Notification (ECN), notificación de congestión explicita.

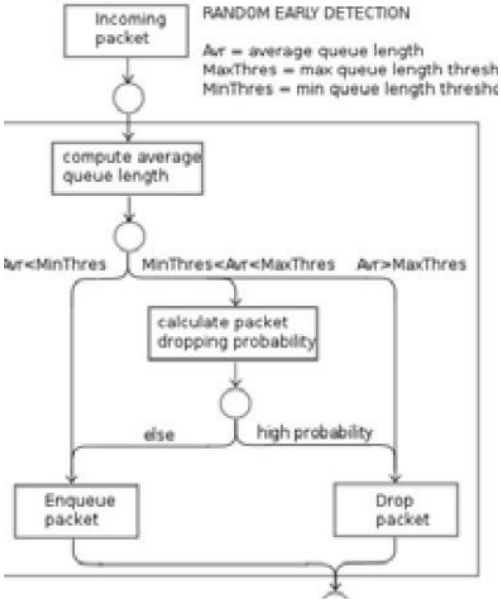
La gestión activa proporciona las siguientes ventajas:

- ⇨ Uso eficiente del ancho de banda de red.

- ⇨ Cuando se produce fluctuaciones momentáneas, la gestión activa permite absorberlas, evitando descartar paquetes.
- ⇨ La gestión activa permite controlar el tamaño de cola influyendo en el retardo de encolamiento.

El primer mecanismo de gestión activa de memoria que veremos es RED. Este mecanismo evita la congestión mediante el control del tamaño de la cola, notificando a los sistemas finales si deben finalizar el envío de los paquetes.
Cuando hay indicios de una posible congestión, debido a una bajada de los niveles de la memoria libre. Realiza un proceso de descartes de paquetes de forma aleatoria e informa al emisor que debe disminuir y adaptar su tasa de transmisión a la de la red, hasta que la memoria disponible alcance unos niveles de seguridad, evitando la congestión en la red.
En casos más extremos, el proceso de descarte se realiza de forma indiscriminada.

Funcionamiento de Random Early Detection, RED



RED controla el tamaño medio de la cola y define un rango, mediante un valor umbral máximo y mínimo, para controlar el proceso de descarte, que nos indica el estado de ocupación de la cola. Si el valor que define el estado de ocupación permanece por debajo del umbral máximo, los paquetes recibidos en la cola no serán descartados, si el valor excede el umbral máximo los paquetes serán descartados. Si el estado se encuentra entre el umbral máximo y el mínimo, los paquetes serán descartados en función de una probabilidad definida por el usuario. RED es configurado para que la ocupación media de la cola este entre el umbral máximo y mínimo.
El funcionamiento de RED es el siguiente; si la cola está vacía, el buffer está vacío, todos los paquetes entrantes se aceptan (el valor de ocupación estará por debajo del umbral mínimo),a medida de que la cola vaya recibiendo paquetes el valor de ocupación aumentara, aumentando la probabilidad de que un paquete entrante sea descartado será mayor(entre el umbral mínimo y máximo). Cuando la cola está llena (valor de ocupación por encima del umbral máximo), todos los paquetes entrantes serán descartados.
RED proporciona una serie de ventajas y desventajas, las ventajas que aporta RED son:

- ⇨ RED no requiere cambios en los protocolos TCP.
- ⇨ La política de descarte se realiza en función de la ocupación en la cola, esto proporciona un límite superior (valor umbral máximo) en la cola que indica cuando se realiza un descarte, que es muy útil para determinados protocolos de transporte.
- ⇨ Soporta tráfico en forma de ráfaga en una cola sin que se produzcan descartes.
- ⇨ La utilización de valores umbrales para controlar el uso de la cola, permite regular la cantidad de tráfico de forma más optima, haciendo un uso más eficiente de ancho de banda de salida.
- ⇨ Soporta el descarte equitativo de paquetes en múltiples flujos sin necesidad de que el dispositivo deba controlar la cantidad de tráfico que tiene cada flujo en una cola.

Respecto a las desventajas.

- ⇨ RED no permite de forma fácil prever su funcionamiento.
- ⇨ Para un funcionamiento óptimo, la configuración puede ser muy compleja.
- ⇨ El uso de RED no es recomendable para tráfico UDP o ICMP, muy utilizados en Internet.

Como RED calcula cuando se ha producido una congestión es el aspecto más importante, hay varias implementaciones que se diferencian en la forma de calcular el grado de ocupación de la cola.
Las diferentes variantes de RED. Las siglas corresponden a su nombre en inglés.

- ⇨ Descarte Aleatorio Anticipado (WRED)
  Permite asignar diferentes perfiles de descartes a diferentes tipos de tráfico, permitiendo un mayor control de las colas.
- ⇨ Descarte Aleatorio Anticipado de adaptación (ARED)
  Posee un algoritmo que permite elegir un descarte más o menos agresivo, basado en la observación de la longitud media de la cola. Se basa en el valor de la longitud media de la cola si oscila entre los valores umbrales máximo y mínimo, dependiendo donde se encuentre el valor. El algoritmo ARED actuará de una forma determinada (agresiva o conservadora).
- ⇨ Descarte Aleatorio Anticipado Robusto (RRED)
  Mejora el rendimiento de TCP contra ataques de tipo DOS, en concreto en una variante de este tipo de ataque denominado LDO. Permiten saturar determinados recursos. Este algoritmo está específicamente diseñado para la defensa de este tipo de ataques.

Uno de los elementos de los Servicios Diferenciados son los adaptadores (acondicionadores) de tráfico que actúan para adaptar el tráfico entrante conforme a las especificaciones de un dominio. Entre las diferentes operaciones que puede realizar un adaptador de tráfico, incluyen el control del tráfico o función policía (Traffic Policing).
El control de tráfico permite controlar la tasa máxima transmitida o recibida en un dispositivo y controlando el ancho de banda que es utilizado. El control de tráfico es configurado en las interfaces de los nodos que se encuentran en los extremos de la red que permiten tener un control fiable del tráfico que entra o sale de la red.
En la mayoría de las configuraciones de control de tráfico, el tráfico que cae dentro de los parámetros configurados es transmitido, mientras que si excede de los parámetros es descartado o transmitido con una prioridad diferente.
Para implementar el control de tráfico en una red se utilizan una serie de algoritmos, siendo el más conocido el algoritmo Token Bucket.
Token bucket es un mecanismo de control que controla cuando se puede transmitir paquetes basándose en la presencia de un token en una cubeta (un contenedor abstracto que mantiene agregado tráfico de red listo para ser transmitido). La cubeta contiene una serie de tokens, que representan una unidad de bytes o un solo paquete de un tamaño determinado. Cuando un tokens se retira de la cubeta, permite transmitir un paquete.
Cuando los tokens están disponibles, permite al flujo la transmisión de tráfico, si no hay tokens en la cubeta, el flujo no puede transmitir esos paquetes.
Token Bucket define una tasa de transferencia y está compuesto por tres componentes.

- ⇨ Tamaño de ráfaga: Especifica en bits por ráfaga que no exceder el tamaño de la cubeta.
- ⇨ Tasa media: Especifica cuantos datos pueden ser enviados o encaminados por unidad de tiempo.
- ⇨ Intervalo de tiempo: Especifica el quantum, pequeño intervalo de tiempo que se asigna, de tiempo en segundo por ráfaga.

Resumiendo todo lo anteriormente dicho sobre DiffServ, para proporcionar un buen servicio se deben cumplir los siguientes requisitos.

- ⇨ Todos los nodos por donde el tráfico se transmite deben ser nodos DS, en caso contrario no puede ser garantizado un servicio óptimo para todos los paquetes.
- ⇨ Cumplir la arquitectura de DiffServ: dominio, nodos fronteras e interiores.
- ⇨ Los dominios DS pueden comunicarse con otros dominios DS y dominio no DS, se deben establecer acuerdos para los diferentes dominios.

El principal problema que puede surgir es la comunicación con nodos no DS, las especificaciones son diferentes, como el campo DS y PHB. DiffServ depende de los mecanismos de reserva de recursos ofrecidos

por la implementación de los PHBs en los nodos. Las garantías del nivel de calidad de servicio pueden venirse abajo en el caso de que el tráfico transite por un nodo no DS o un dominio noDS.

1.3. Centro de Gestión de Red, diseño y recursos implicados.

Para la gestión de una red participan muchos componentes: elementos de red, herramientas de gestión protocolos de gestión, etc. Debe existir una organización donde de forma centralizada se gestione todos los componentes de una red, donde personal cualificado haga uso de todos los recursos para conseguir gestionar una red de forma eficiente.

Un centro de gestión de redes (CGR) o NOC (en inglés) es un lugar donde el personal técnico, utilizando una serie de herramientas específicas, realizan la gestión de todos los recursos de la red. Este tipo de centro solo es viable en grandes infraestructuras.

Un CGR está compuesto de una organización cuyo propósito es, utilizando su propia infraestructura, realizar una gestión lo más eficiente posible, consiguiendo que el funcionamiento de red mejore.

Esta organización debe tener cierta flexibilidad para adaptarse a los cambios que se produce en la red, aumentando la eficiencia en la gestión.

En un CGR se realizan una serie de tareas para la gestión de la red, las tareas que se incluyen son:

- ⇨ Seguimiento de los fallos de la red.
- ⇨ Control del rendimiento de la red, tomando todas las medidas necesarias que para que el servicio funcione, en caso necesario adoptando todas las medidas preventivas en caso de encontrar indicios de errores.
- ⇨ Diagnóstico de fallos e interrupciones de la comunicación si se producen, realizando una planificación para la reparación.
- ⇨ Planificación de la topología de red, el diseño de la red debe asegurarse que futuras modificaciones puedan ser implementadas sin mucha complejidad.
- ⇨ Planificación de mejoras de la red.
- ⇨ Actualizaciones de los componentes de la red, cualquier actualización del hardware o software de la red debe afectar lo menos posible funcionamiento de la red, evitando siempre que sea posible cualquier corte en el funcionamiento.

La organización que hay dentro de un CGR es la encargada de realizar un análisis de las tareas que debe realizar, especificando cuando se realizan las tareas y que recursos serán utilizados.

Una organización necesita una estructura que le permita ser más eficiente. Una posible estructura es mediante distintas unidades donde cada una de ellas se encarga de una función, creando diferentes unidades organizativas y cada una de ellas se encarga de distintas funciones.

Entre las funciones que se pueden incluir:

- ⇨ Planificación de la red, donde se realizan un análisis de uso de la red y el tráfico, también se encarga del funcionamiento de la red como de los servicios que proporcione.
- ⇨ Mantenimiento y supervisión de la red.
- ⇨ Administración de la red.
- ⇨ Gestión de clientes.
- ⇨ Gestión de software y hardware.

Cada unidad de organización tiene su propio personal que tiene asignadas una serie de funciones. Dentro del personal de la unidad, se incluyen.

- ⇨ Administradores de red.
- ⇨ Operadores de red.
- ⇨ Técnicos.
- ⇨ Personal de atención al cliente.

Las unidades no son totalmente independientes y debe existir comunicación entre las unidades, para algunas tareas esa comunicación es esencial. Por ejemplo, un usuario genera una incidencia en la red que es documentada por el personal de atención al cliente, que es comunicado a los técnicos para que la resuelvan que debe comunicar el personal de la red (operadores o administradores de red) cualquier cambio u operación que se realiza en la red. Como se ve, para esta tarea están involucrados personal de atención al cliente, técnicos y administradores, son necesarios para realizar de forma eficiente esa tarea.

La organización de un CGR y las unidades que se incluyen dependen de la infraestructura que se gestiona, la complejidad de la organización depende mucho del tamaño. En las empresas de telecomunicaciones que gestionan grandes redes está compuesta por una organización que involucra varios departamentos y un personal muy amplia, suele tener una estructura bastante compleja.
Un CGR no solamente se encarga de la gestión de red, sino que también puede contener parte de la infraestructura, convirtiéndose el mismo en un nodo de comunicación de la red.
Esta infraestructura debe tener un sitio dentro del CGR debidamente acondicionada, una habitación con la temperatura controlada donde colocar múltiples elementos de red y gran cantidad de cableado. El cableado, de hecho, es otro tema que puede convertirse rápidamente en un problema, debe estar perfectamente organizado, utilizando para ello lo que se denomina cable estructurado.
La gestión de la red debe ir acompañada de una buena gestión de las instalaciones realizando un seguimiento desde el punto de vista físico, mantenimiento de los cables, tanto de la red como de la instalación eléctrica. También es muy importante la seguridad del CGR, tanto del propio centro como del recinto donde se encuentra la infraestructura de red. Un acceso no autorizado a la red puede ser muy perjudicial, si no se han implementado los pertinentes controles para evitar cualquier intrusión no autorizada.
En infraestructuras muy grandes un CGR podría no ser suficiente, serán necesarios varios repartidos por la infraestructura de red. Cada CGR tendrá que coordinarse con el resto, aunque uno de ellos sea el principal y el resto serán utilizados como centros secundarios. En caso de fallo del CGR central, uno de los CGR secundarios lo reemplazará y convirtiéndose en CGR central, a la espera de resolver el fallo.
Un CGR dispone de una serie de recursos, divididos en tres categorías:

- ⇨ Métodos de gestión.
- ⇨ Recursos humanos.
- ⇨ Herramientas de gestión.
- ⇨ Métodos de gestión

Definen las pautas de comportamiento de los demás componentes del centro de gestión de red ante determinadas circunstancias.
Una gestión de red óptima proporciona una serie de características que nos permitirá mejorar la red, estas características que aporta son:

- ⇨ Control de activos.
- ⇨ Control de complejidad.
- ⇨ Mejorar el servicio.
- ⇨ Equilibrar necesidades.
- ⇨ Reducir los cortes en el funcionamiento.
- ⇨ Control de costes.

El objetivo que debe buscar y conseguir la gestión es:

- ⇨ Mejorar la disponibilidad de todos los elementos de red.
- ⇨ Uso de forma eficiente de los recursos.
- ⇨ Incrementar la efectividad.
- ⇨ Mejorar el rendimiento de todos los componentes.

Las funciones de gestión de red se dividen en dos grandes tareas:

- ⇨ **Monitorización**: Obtener información de la red.
  - Observar y analizar el funcionamiento de los componentes de la red.
  - Los componentes funcionales que están involucrados: prestaciones, fallos y costes.
- ⇨ **Control**: Tomar las medidas necesarias para obtener un rendimiento óptimo.
  - Modificar diversos parámetros de red.
  - Modificaciones de las configuraciones de los componentes de red, tanto hardware como software.
  - Los componentes funcionales que están involucrados: configuración y seguridad.

Las funciones de monitorización son denominadas funciones de lectura (leer datos), las funciones de control son denominadas funciones de escritura (escribir datos).
La monitorización se encarga de recoger información de los dispositivos de la red, los datos obtenidos se utilizarán para realizar un análisis para conocer el rendimiento de los componentes de la red.

Es muy importante obtener la información de forma estructura, hay diversos formatos de datos que permiten realizar el trabajo de análisis de forma más eficiente.
La monitorización tiene tres objetivos.

- ⇨ Identificación de la información: que información nos interesa monitorizar, conocer que componentes nos proporciona esa información.
- ⇨ Diseño de mecanismos de monitorización: como obtener la información de los componentes de la red, escoger que mecanismos serán utilizados para obtener la información.
- ⇨ Utilización de la información: que uso se va a dar de esta información, esta información puede ser utilizada para mejorar el funcionamiento de los componentes de la red.

La información a monitorizar se clasifica en varias categorías.

- ⇨ Estática: Información que cambia con muy poca frecuencia, un cambio en esta información puede ser un indicio de una anomalía en la red. Por ejemplo, un servidor web utilizado en una red proporciona el servicio a través del puerto 80 (habitualmente) y no suele ser cambiado.
- ⇨ Dinámica: Información relacionada con eventos en la red, cualquier información que se transmite por una red, cada paquete almacena información diferente.
- ⇨ Estadística: información que se utiliza para realiza diferentes gráficas para visualizar el rendimiento de un determinado dispositivo. Por ejemplo, cualquier dispositivo de una red, un servidor o router, se puede obtener la tasa de tráfico o la carga de su CPU.

La gestión de redes se basa en tres componentes básicos:

- ⇨ Componente organizacional
  Define la estructura para el proceso de gestión y la estrategia apropiada para llevarlo a cabo de acuerdo con las necesidades del negocio.
- ⇨ Componente técnico
  Define las herramientas a usar para realizar la función de gestión, y su implantación en la infraestructura.
- ⇨ Componente funcional
  Define las funciones de gestión que el componente organizacional debe ejecutar utilizando las herramientas de gestión.

Componente Organizacional

El componente organizacional se estructura en cuatro aspectos que realizan una serie de actividades, donde la responsabilidad de estas tareas se diferencia en función del tiempo de actuación.

- ⇨ Control operacional: Realiza actividades que son realizadas en un periodo muy corto de tiempo, se contabiliza el tiempo en horas.
- ⇨ Administración: Actividades realizas en un periodo corto de tiempo, se contabiliza en función de días.
- ⇨ Análisis: Actividades realizadas a medio plazo (meses).
- ⇨ Planificación: Actividades realizadas en periodo largo de plazo, se contabiliza en años.

Control operacional

Agrupa un conjunto de tareas cuyo objetivo es mantener un nivel óptimo de los servicios proporcionados por la red. El personal encargado de realizar estas tareas son los administradores de la red.
Para comprobar que las tareas realizadas no han producido errores y han sido ejecutadas de forma correcta, de forma periódica, se realizan una serie de análisis que permitirán a los administradores mejorar las eficiencias de esas tareas realizadas.
Entre las tareas a realizar por los administradores, podemos considerar:

- ⇨ Soporte a usuarios (Help Desk).
- ⇨ Recolección de datos sobre el rendimiento y utilización de la red.
- ⇨ Inicialización y parada de componentes de red.
- ⇨ Control sobre las modificaciones de las configuraciones de los componentes de la red.
- ⇨ Evaluación de alarmas.
- ⇨ Ejecución programada de pruebas preventivas.
- ⇨ Diagnóstico de problemas.

Administración

Realizar una serie de tareas que permite realizar un seguimiento de las tareas de control operacional, realizando una serie de informes, de forma periódica, que serán utilizados para realizar un análisis posterior que permitirá detectar errores y comprobar la eficiencia de las tareas realizadas.
Las actividades que se realizan:

- ⇨ Evaluación de la calidad del servicio, comprobar si los servicios funcionan de forma correcta.
- ⇨ Detección y aislamiento de fallos, permite controlar un error producido y no se ha propagado a otras partes de la red.
- ⇨ Evaluación de tráfico, comprobación de la tasa de tráfico que se transmite por la red.
- ⇨ Mantenimiento de registro histórico de problemas, permitirá tener un control de los errores producidos como las soluciones implementadas.
- ⇨ Mantenimiento de configuraciones, permite conocer las configuración de todos los componentes y realizar las oportunas modificación de configuración.
- ⇨ Contabilidad de red.
- ⇨ Control de acceso, conocer cuándo y quién accede a la red y sus servicios.

Análisis

Realiza un conjunto de actividades que permitan garantizar una buena calidad de servicio en función de una especificación definida, recopilando información de diferentes elementos sobre el funcionamiento de la red y realizando un análisis donde detectar posibles errores y escoger la solución más adecuada.
Entre las actividades que se realizan tenemos:

- ⇨ Definición de los parámetros de rendimiento para poder evaluar la calidad del servicio.
- ⇨ Análisis de la calidad del servicio.
- ⇨ Toma de decisiones para corregir problemas en la calidad del servicio.
- ⇨ Preparación de procedimientos para control operacional y administrativo

Planificación

Conjunto de actividades que se encargan de las decisiones dependientes del negocio al que se dedica la empresa, especifica las distintas características principales que debe tener la red en función de las características de la empresa.

- ⇨ Algunas tareas que se realizan:
- ⇨ Análisis de informes técnicos-económicos (anuales).
- ⇨ Establecimiento de política de telecomunicaciones.
- ⇨ Asignación de presupuesto.
- ⇨ Selección de criterios de distribución de costes o facturación.
- ⇨ Utilización de herramientas especializadas para simulación del ambiente de red y generar proyecciones de demanda de tráfico.
- ⇨ Planificación de la capacidad.

En el componente técnico utilizamos herramientas para la gestión de red, es donde se realiza la gestión de red propiamente dicha, incluyen la configuración e implantación en la infraestructura de red.

Monitorización

Con las herramientas de gestión se realiza la monitorización de la red, existen varios mecanismos de monitorización:

- ⇨ Sondeo o polling: Realiza accesos periódicos a la red y mediante un sondeo obtiene información de los componentes.
  Ventajas: simplicidad.
  Desventajas: tráfico excesivo generado con los sondeos periódicos.
- ⇨ Notificaciones: Los recursos envían mensajes (notificaciones) cuando se producen ciertos eventos configurables.
  Ventajas: el tráfico generado en mínimo.
  Desventajas: complejidad en la configuración, los nodos gestionados deben ser configurados, indicando con qué eventos envía las notificaciones.

- ⇨ Sondas: Es una combinación de los dos métodos anteriores.
  Ventajas: minimiza el tráfico y simplicidad.
  Desventajas: complejidad.

El método más utilizado por las herramientas de gestión es el último mecanismo. Sondas o Proxy.
En el mecanismo Sonda o Proxy, está compuesto por los siguientes componentes.

- ⇨ Gestor: Software disponible en la central de gestión y es el encargado de realizar la gestión de la red. Este software es la interfaz humana del sistema de gestión.
- ⇨ Agente: Software disponible en el dispositivo gestionado, tiene acceso a la información de gestión de los dispositivos e interactúa con el gestor para atender peticiones y generar eventos.
- ⇨ Proxy: Medio para proveer funcionalidad de gestión sobre dispositivos o elemento no compatibles mediante conversión de protocolos.

Un gestor es el encargado de recoger la información de los agentes ,que se encuentran en los dispositivos, a través de un protocolo de gestión. Los agentes se encuentran en un estado "pasivo" hasta que ocurre algún evento y envía una notificación al gestor, los agente almacenan información del dispositivo gestionado que puede ser pedida por un gestor.

Componente Funcional

El componente Funcional define las funciones de gestión que el componente organizacional debe ejecutar utilizando las herramientas de gestión. Estas funciones se engloban en 5 categorías:
En la unidad 2 se explicará con más detalle el aspecto funcional de la gestión de red, aquí se explicarán de forma resumida los aspectos más importantes.

Gestión de Configuración

Comprende tareas de mantenimiento de la configuración de la red en función del diseño de la red.
Algunas de las tareas que pueden incluirse:

- ⇨ Crear los diferentes parámetros de configuración del sistema.
- ⇨ Obtener información sobre el funcionamiento de la red.
- ⇨ Recoger avisos de cambios significativos.
- ⇨ Modificación en la configuración del sistema.
- ⇨ Gestión de inventario.
- ⇨ Gestión de incidencias.
- ⇨ Diseño de la red.

Gestión de Fallos

Comprende tareas relacionadas con los errores que se producen en una red. Algunas de las tareas incluidas en esta categoría:

- ⇨ Gestionar los registros de errores.
- ⇨ Realizar pruebas de diagnostico.
- ⇨ Resolución de errores.
- ⇨ Actuar en función de las incidencias recibidas.
- ⇨ Detectar y localizar fallos en la red.
- ⇨ Activar diferentes operativas para la resolución del fallo.

Gestión de Prestaciones

Gestionar diferentes medidas de parámetros de la red que servirán para garantizar unos niveles de rendimientos óptimos en función de las especificaciones de la red.

- ⇨ Obtener y gestionar información de diferentes estadísticas.
- ⇨ Determinar el nivel prestaciones esperado del sistema en función de diversos factores.
- ⇨ Gestionar los registros del estado del sistema.
- ⇨ Determinar los parámetros para realizar mediciones.
- ⇨ Establecimiento de valores umbrales para las mediciones.
- ⇨ Análisis de los datos obtenidos.

Gestión de contabilidad

Realiza diversas tareas relacionadas con la facturación y el coste de los recursos utilizados. Algunas de las funciones que se realizan.

- ⇨ Distribución de los recursos.
- ⇨ Control de los costes asociados al uso de los recursos.
- ⇨ Establecer límites de costes.
- ⇨ Informar de los costes a los usuarios y los recursos consumidos.
- ⇨ Gestión de facturas.
- ⇨ Integración con la contabilidad de la empresa.
- ⇨ Identificación de los costes.

Gestión de seguridad

Realiza diferentes tareas para proteger la red y la información transmitida.
Algunas de las tareas incluidas en esta categoría son:

- ⇨ Definir y controlar servicios y mecanismo de seguridad.
- ⇨ Control de acceso a los recursos de la red.
- ⇨ Protección del software instalado.
- ⇨ Definir diferentes políticas de seguridad para evitar accesos no autorizados.
- ⇨ Informar de los sucesos relativos a la seguridad del sistema.
- ⇨ Definición de alarmas de seguridad.
- ⇨ Protección de los usuarios de la red.
- ⇨ Examinar registro del sistema.
- ⇨ Distribuir la información de seguridad.

Recursos Humanos

Este tipo de recursos define al personal encargado del correcto funcionamiento del centro de gestión de red (CGR). Este personal está organizado en diferentes niveles en función de la responsabilidad atribuida, cada nivel tiene asignada una capacidad en la toma de decisiones. Esta capacidad tiene un componente jerárquico, el nivel más bajo no puede tomar muchas decisiones y en muchos casos dependerá de las decisiones que tomen los niveles mas alto.
Cada organización realiza una asignación de recursos de red al personal, creando diferentes perfiles que le asignarán una serie de tareas dentro de la gestión.
El modelo más utilizado es mediante diferentes niveles de soporte, cada nivel tiene un tipo de personal encargado de determinadas tareas.
Los niveles son:

- ⇨ Nivel 1 Operadores: también denominado Help Desk, se encargan del nivel más básico del soporte al usuario, resuelven incidencia de bajo nivel y requiere un conocimiento técnico bajo. Los operadores tienen un acceso limitado a los recursos de la red, principalmente recogen las incidencias de los usuarios e intentan resolverlas siguiendo una operativa definida, derivando la incidencia a un nivel superior en caso de no poder resolverla. Es el nivel más cercano a los usuarios y permiten obtener mucha información sobre una incidencia.
  Realizan tareas administrativas sencillas como:
  - Actualizaciones de software.
  - Arranque y parada de los componentes de la red.
  - Administración de ciertos dispositivos.
  - Recoger información de las alarmas.
  - Obtener información de los usuarios
  - Recoger datos sobre la utilización de los recursos de la red
- ⇨ Nivel 2 Administradores: Realizan tareas de administración de la red, el conocimiento del personal es un nivel medio. Realizan tareas control de la red y mantenimiento preventivo, utilizan herramientas para realizar diversas tareas como:
  - Gestión de inventario
  - Instalación de software y hardware.

- Gestión de configuraciones.
- Gestión de seguridad: control de acceso, etc.
- Mantenimiento de registro histórico de problemas.
- Evaluación de tráfico y calidad de servicio actuales.
- Generación de informes sobre el funcionamiento de la red.
- Análisis de datos, para conocer el rendimiento de la red.

⇨ Nivel 3 Analistas: Encargados de mantener la calidad de servicio en la red, realizando análisis periódicos de calidad. El conocimiento técnico del personal es alto y deben conocer con detalle todos los aspectos de la red. Pueden realizar las siguientes tareas.

- Elegir cual son los componentes que serán gestionados.
- Diseñar indicadores para conocer la calidad de servicio.
- Escoger los mecanismos que serán utilizados para controlar los componentes.
- Elegir métricas de rendimiento, medidas que permiten conocer el rendimiento de los componentes.
- Creación de las diversas operativas de actuación en función de diversos eventos
- Creación de manuales donde describen las diferentes operativas.
- Planificación de la evolución de la red.

⇨ Nivel 4 Planificadores: personal con sólidos conocimiento empresariales y habitualmente compuesto por personal no técnico. Encargado de la toma de decisiones relacionadas con el negocio donde trabaja la empresa. Entre las tareas que se pueden realizar:

- Generación de informes técnico-económico.
- Establecer políticas de control de costes.
- Crear políticas de facturación para los servicios proporcionados.
- Diseño y control del presupuesto para la red.
- Seleccionar los criterios económicos en la asignación de los recursos de la red.

Herramientas de Gestión

Todo CGR tiene instalado un conjunto de aplicaciones software que permitirán al personal realizar diversas tareas, entre las que se incluyen las herramientas de gestión. Para el personal de CGR (centro de gestión de redes) es necesario el uso de este tipo de herramientas, en redes grandes las herramientas de gestión son imprescindibles para realizar una gestión óptima. El número de componentes y la infraestructura compleja de este tipo de redes, crean un escenario perfecto para el uso de estas herramientas.

Las herramientas de gestión permiten la monitorización y control de los diversos de componentes de la red (software y hardware) como los servicios disponibles en la red. Los administradores utilizan estas herramientas como una interfaz para poder ejecutar diversas tareas, teniendo una visión global de red, mostrando todos los componentes de la red, como los enlaces, recursos implicando y los servicios proporcionados, obteniendo de forma simple mucha información de la red.

Los componentes hardware de la red se dividen en dos categorías:

⇨ Activos: dispositivos que envían regularmente información de estado al centro de gestión de red.

⇨ Pasivos: dispositivos que no envían información sobre su estado, son elementos utilizados para la conectividad de la red.

Las herramientas de gestión de redes están englobadas dentro de un sistema de gestión redes compuesto por una serie de componentes hardware y software.

Los componentes hardware se denominan nodos e incluyen software para realizar la gestión denominado entidad de gestión de red, NME siglas en inglés.

Un **NME** realiza las siguientes tareas:

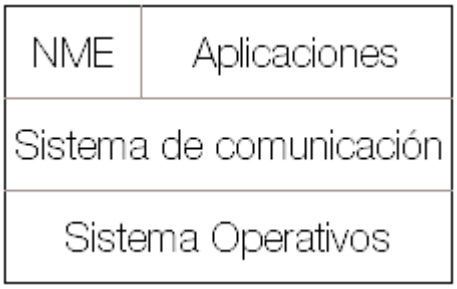
⇨ Recoge diversas estadísticas de los componentes de la red, como de la actividad de la red.

⇨ Almacena las estadísticas en el propio nodo.

⇨ Responde a comandos enviados por el CGR, como:

- Solicitud de estadísticas de un componente, enviándolas al CGR.
- Modificación de parámetros (ej. un temporizador usado en un protocolo).
- Proporcionar información de estado al CGR.
- Realización de pruebas.

Un nodo con un NME se denomina Agente.
Estructura de un nodo agente.



Entre todos los nodos disponibles de la red, se debe incluir (al menos uno) un nodo gestor, este nodo suele estar situado dentro de la infraestructura del CGR para permitir un mejor control de la red.
Un gestor incluye su propio NME, además incluye software denominado aplicación de gestión de red, NMA siglas en inglés, encargado de realizar las tareas de gestor.
Las tares que realiza el **NMA**.

- ⇨ Proporcionar una interfaz para que el administrador puede realizar diversas tareas de gestión.
- ⇨ Recibe las respuestas de los comandos enviados y ejecutados en un NME. Toda la comunicación es realizada a través de un protocolo de gestión de red, como por ejemplo SMNP.

En algunas redes es necesario que el nodo gestor sea redundante, la red contiene varios gestores donde solo uno funciona para la gestión de red, denominado nodo principal, y el resto actúa como un nodo gestor de reserva, recibe toda la información del nodo principal pero no realiza tareas de gestión como el nodo principal. Si en el nodo principal falla uno, de los nodos de reserva adquiere el rol de principal convirtiéndose en nodo principal y realizando las tareas de gestión de la red.
Estructura de un nodo gestor.

El componente software dentro de un CGR se puede dividir en tres categorías:

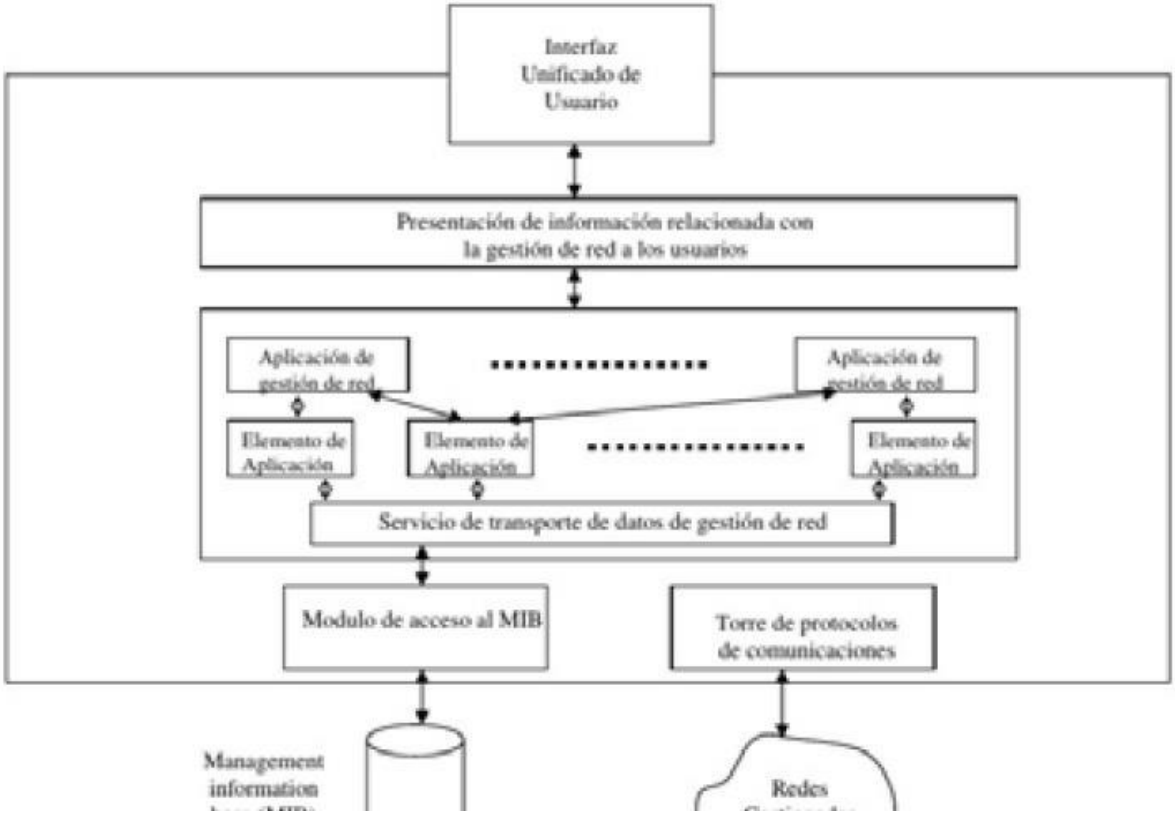
- ⇨ Software de interfaz: donde el administrador o un usuario autorizado puede visualizar de forma organizada y legible información recogida por los agentes. Este software es instalado en el gestor de red para monitorizar y controlar la red, permitiendo visualizar la información de los agentes en diferentes formatos (normalmente mediante una serie de gráficas), facilitando mucho la tarea de monitorización. También permite realizar tareas de pruebas, depuración y gestionar configuraciones de los componentes de la red. Esta interfaz es unificada, la misma para todos los nodos gestionados, también la interfaz es independiente del hardware, simplificando el proceso de monitorización.
- ⇨ Software de gestión de red: se encarga del control y monitorización de la red, todas las tareas relacionadas con la gestión de red. Está compuesto por tres niveles.
  - Aplicaciones: proporciona diversos servicios al usuario.
  - Elementos: implementa funciones básicas como generar una alarma, pueden ser compartidos por varias aplicaciones.
  - Servicio de transporte de datos: implementa el protocolo de comunicación utilizado entre los agentes y gestores, también proporciona una serie de funciones básicas para tareas de recogida, notificaciones, etc.
- ⇨ Software de soporte de gestión de red: se encarga del almacenamiento de los datos recogidos, utilizando un MIB, y la comunicación entre los elementos. El MIB almacena de forma jerarquizada la

información tanto del agente como del gestor. La información almacenada de un nodo es relativa a la gestión, configuración, comportamiento y diversos parámetros de control de un nodo. Para el gestor, contiene información del agente propio e información solicitada de los nodos que gestiona.

El funcionamiento de una herramienta de gestión, empieza en la interfaz de usuario que proporciona la herramienta donde el administrador gestiona la red, esta información será mostrada de forma unificada. Desde una consola de gestión el administrador podrá acceder a los gestores y agentes disponibles en el sistema, donde realizar diversas tareas de gestión en los nodos.

La información de los nodos es transmitida mediante un servicio de transporte para la gestión de red, un protocolo de gestión, y a través de un módulo de acceso es almacenada en una base datos MIB.

Mediante una serie de protocolos de comunicación la herramienta de gestión accede a las redes gestionadas.



La arquitectura mostrada anteriormente es un sistema centralizado, pero estos sistemas han ido evolucionando a sistemas distribuidos, este tipo de sistema implementa varias herramientas de control en la red.

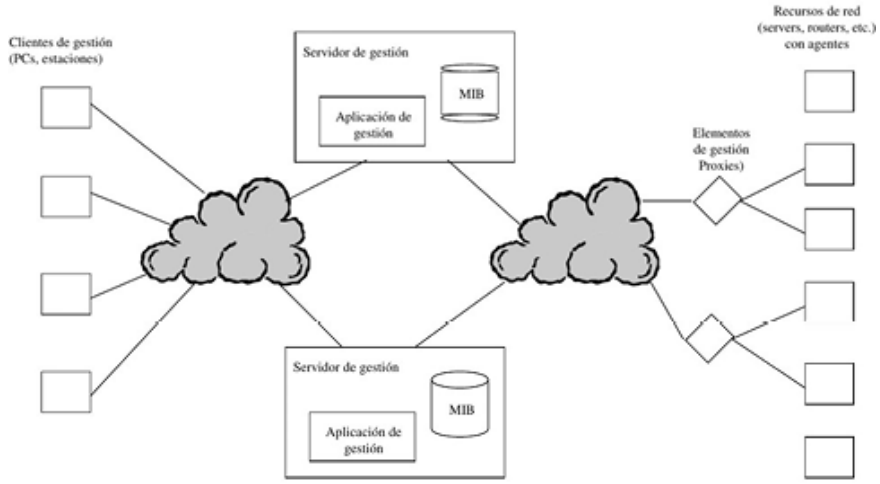
La gestión distribuida proporciona a una solución a diferentes problemas que surgen en la gestión centralizada:

- ⇨ Gestión de múltiples LAN.
- ⇨ Gestión más eficiente en entornos complejos.
- ⇨ Implantación de aplicaciones distribuidas.

La gestión distribuida simplemente sustituye un único nodo gestor en el CGR por múltiples nodos gestores que se encuentran en las LAN de la organización y trabajan de forma coordinadas entre ellas. Esto permite a los gestores de los departamentos mantener las redes, sistemas y aplicaciones de sus usuarios locales de forma más eficiente, simplificando la gestión. Toda la información de gestión puede ser enviada a un nodo central que servirá para tener una visión global de toda la red y poder realizar diversos análisis de comportamiento.

Para tener una arquitectura organizada con la gestión distribuida se utiliza una jerarquía, cada sistema de gestión tiene limitadas las funciones de control y monitorización en función de los recursos disponibles en la LAN que gestiona.

Una estación central tiene todas las funciones para la gestión de todos los recursos de la red, interactuando con las estaciones distribuidas para monitorizar y controlar su operación.



La gestión distribuida proporciona una serie de ventajas y mantiene las mismas ventajas.

- ⇨ Disminuye el tráfico de gestión de red.
- ⇨ Mayor escalabilidad, aumentar la potencia de la gestión solo se debe instalar mas hardware.
- ⇨ La gestión distribuida proporciona mayor fiabilidad, hay varias herramientas de gestión y en caso de fallo de una de ellas, otra herramienta de gestión puede incluir esos nodos en su gestión.

También tiene ciertas desventajas como:

- ⇨ Herramientas más complejas de utilizar.
- ⇨ Utilización de más recursos.

En una red es posible que algunos elementos de red no proporcionen un NME. Estos elementos no son soportados por el software de gestión, no cumplen los requisitos del software por diversas causas como pueden ser.

- ⇨ Antigüedad.
- ⇨ Hardware no soportado.
- ⇨ No tiene suficiente potencia.
- ⇨ No cumple los estándares.

Para solucionar este problema se utilizan un componente denominado proxies que permiten gestionar elementos de red no soportados por el software de gestión. El proxy conecta varios elementos gestionados y para obtener información del elemento, un gestor realiza una petición, un proxy la recoge y la envía al elemento correspondiente que envía una respuesta acorde con la petición recibida.

El proxy se encarga de realizar de todas las conversiones necesarias para que la información sea comprendida por el elemento y la respuesta debe ser convertida a un formato que el gestor entienda.

1.4. Relación entre recursos y servicios.

Una red ofrece una serie de servicios que son utilizados por los usuarios, estos servicios necesitan una serie de recursos para poder funcionar. Estos servicios son un producto ofrecido por una empresa y una serie de usuarios contratan estos servicios. Por ejemplo, los servicio que ofrecen una operadora de móviles a sus clientes.

Se establece una relación comercial entre la empresa proveedora y los clientes, que pagan por el producto y esperan recibir un servicio de calidad de acuerdo a lo especificado.

Los servicios de red poseen un factor muy configurable que permiten ajustarse a las necesidades del cliente, para obtener un nivel alto de satisfacción por parte del cliente.

Todo servicio de red debe cumplir una serie de propiedades para obtener un funcionamiento óptimo, estas propiedades son:

- ⇨ Rendimiento.
- ⇨ Capacidad.
- ⇨ Disponibilidad.

Estas propiedades se conocen como nivel de servicio y son una parte muy importante en la definición del servicio. Las especificaciones de un servicio respecto al nivel de servicio forman parte de un acuerdo de nivel de servicio o SLA (Service Level Agreement).

Un SLA define los términos técnicos del servicio que deben cumplir para su prestación y en caso de no cumplir el nivel de servicio acordado especifica qué tipo de operativas tendría el cliente disponible, como soporte técnico para solucionar el problema o una serie de bonificaciones para contentar al cliente por los inconvenientes producidos, en el SLA debe especificarse de forma clara los términos en que son aplicadas estas operativas. Resumiendo, un SLA especifica la relación comercial entre el usuario y la empresa que proporciona un servicio de red.

Un aspecto fundamental es la gestión del nivel de servicio, las empresas que proporciona un servicio debe de asegurar una calidad acorde a un nivel de servicio especificado. Este nivel debe ser lo suficientemente alto para que el nivel de satisfacción de los clientes también sea alto. El objetivo de la gestión es conseguir este nivel de satisfacción, si ese nivel no se consigue se puede perder el cliente, al no estar satisfecho por el servicio.

Para conseguir un nivel de servicio alto, la empresa proveedora del servicio de red utiliza una serie de recursos como pueden ser.

- ⇨ Dispositivos hardware: cualquier equipo como ordenadores, router, switch, etc.
- ⇨ Software: cualquier red necesita un conjunto de aplicaciones para poder funcionar correctamente como sistemas operativos, herramientas de gestión, herramientas de seguridad, etc.
- ⇨ Personal: es el encargado de realizar diversas tareas en la red, entre el personal tenernos: administradores de red y de sistemas, operadores, técnicos, etc.

Todos los recursos tienen un coste económico pero para asegurar un nivel de servicio especificado en el SLA requiere una inversión en diversas tareas.

- ⇨ Mantenimiento de la red: En cualquier red se requiere realizar diversas tareas de forma periódica para garantizar un buen rendimiento de los servicios de la red, comprobando que todos los componentes de la red funcionan de forma correcta. Esto implica una serie de costes en personal que se encargar de estas tareas.
- ⇨ Resolución de averías: Siempre surgirán averías en la red y esto tiene una serie de costes en personal, compra de equipos nuevos para sustituir equipos averiados u otros gastos que se generen.
- ⇨ Inversiones en la red: Otra serie de costes a tener en cuenta son para mejoras en la red para aumentar el nivel de calidad de un servicio. Estas mejoras también pueden permitir ampliar los servicios que proporciona la empresa.

La empresa debe decidir cómo y cuánto es el coste económico en recursos para que el servicio sea rentable para la empresa y el cliente deber estar satisfecho con el servicio. Si el gasto en recursos es alto el rendimiento del servicio será alto y el cliente estará satisfecho, pero para la empresa puede no ser rentable un gasto tan alto en los recursos asignados al servicio. Si el gasto en recursos es bajo, el rendimiento del servicio será bajo y el cliente puede no estar satisfecho con el servicio, con la posibilidad de dejar de ser cliente del servicio, aunque el gasto bajo en recursos puede ser muy rentable para la empresa.

El objetivo para la empresa es buscar un equilibrio entre el coste en recursos, dando un buen servicio al cliente, y la rentabilidad del servicio para la empresa.

1.5. Herramientas para asignación de recursos: tipos y características.

Para obtener un equilibrio entre el coste de los recursos y la rentabilidad, se deben utilizar los recursos de forma óptima. Cada servicio tiene asignado una serie de recursos que garanticen un correcto funcionamiento, si se excede en asignar recursos a un servicio puede ocurrir que nos encontremos con recursos que no se utilizan, pero si se asignan pocos recursos a un servicio, esto puede afectar de forma negativa al rendimiento del servicio.

Para saber los recursos que necesita un servicio, se deben tener en cuenta una serie de factores:

- ⇨ Número de usuario: la cantidad de usuarios que utilizan un servicio es proporcional a cantidad de recursos que se deben asignar.
- ⇨ Uso del servicio: el grado de uso del servicio influye en la cantidad de recursos, un servicio muy utilizado necesitara más recursos. Un corte de funcionamiento en un servicio muy utilizado por los clientes afectará de forma muy negativa en la satisfacción de los clientes.

- ⇨ Disponibilidad: define el grado de funcionamiento ininterrumpido que puede estar un servicio, una disponibilidad alta implica que un servicio funcione constantemente. La empresa debe analizar la disponibilidad de cada servicio, una mayor disponibilidad implica una mayor asignación de recursos.

Una asignación eficaz de los recursos influye de forma positiva en el funcionamiento de la red y de los servicios que ofrece. Hay disponible múltiples herramientas software que facilitan el proceso de asignación de recursos de forma eficaz.

Este tipo de herramientas permiten controlar los recursos asignados y su uso, realizando una asignación dinámica de recursos en función de ciertos parámetros, evitando que un servicio obtenga más recursos de los necesarios.

Las herramientas de asignación de recursos son clasificadas en tres categorías dependiendo de cómo realiza la asignación, estas categorías son:

- ⇨ Sistemas de tickets.
- ⇨ Sistemas de órdenes de trabajo.
- ⇨ Sistemas de gestión de flujo de trabajo y motores de flujo de trabajo.

Sistema de Tickets

Las herramientas basadas en un sistema de ticket realizan un seguimiento de los problemas que surgen en una red y como se están resolviendo. El componente principal de este sistema son los tickets que son utilizados para almacenar información acerca de los errores que se han producido en la red y permiten realizar un seguimiento de la resolución de estos problemas.

En muchos casos, los tickets son generados por los usuarios del servicio, que detectan y le afecta el error.

Otra forma de generar tickets, es por medio de aplicaciones que monitorizan la red y detectan un error en la red o en un servicio, todos los tickets creados recogen información del sistema para documentar el error y se le asigna un estado en función del estado de resolución del error, también los tickets puede tener una prioridad asignada en función de la importancia del error.

Un sistema de tickets, aparte de recoger información sobre un error, permite realizar una serie de acciones en función del error detectado. Por ejemplo, el sistema de tickets puede asignar automáticamente un problema a un técnico u otro personal que debe asumir la responsabilidad, o puede automáticamente escalar tickets que llevan demasiado tiempo para ser resueltos a un personal más especializado.

El sistema de tickets puede obtener estadísticas sobre el proceso de resolución y conocer el porcentaje de resolución de los errores en un tiempo determinado.

Sistema de órdenes de trabajo

Este tipo de sistemas son utilizados para la asignación y seguimiento de los trabajos de mantenimiento individuales en una red, ayudan a organizar y gestionar la fuerza de trabajo que las lleva a cabo.

A cada trabajo se le asigna una orden de trabajo a cuya resolución se le realiza un seguimiento, es similar a los sistemas de tickets.

Los sistemas de órdenes de trabajo ofrecen una gran variedad de funciones para capturar información sobre el proceso de resolución del error. Estas funciones permiten gestionar la asignación del trabajo a un personal, asegurándose que los todos los puestos de trabajo estén debidamente atendido. En general, permite conocer el trabajo que esta realizan el personal responsable del mantenimiento de la infraestructura de la red.

Sistema de gestión de flujo de trabajo y motores de flujo de trabajo

Un sistema de gestión de flujo de trabajo ayuda a controlar la ejecución de un proceso de resolución de un error, también denominado de flujo de trabajo. Un flujo de trabajo es básicamente un proceso predefinido o procedimiento que consta de varios pasos que pueden involucrar a diferente personal y organizaciones.

Los sistemas de gestión de flujo de trabajo se refieren a los procesos de negocio en general y no son específicos de gestión de la red. Sin embargo, pueden ser aplicados a la gestión de la red cuando los procesos y flujos de trabajo en cuestión influyen en el funcionamiento de una red.

Un sistema de gestión de flujo de trabajo ayuda a mantener un seguimiento de los pasos que deben realizar para la resolución de un error, asegurándose que el procedimiento predefinido se cumple.

Los flujos de trabajo son definidos usando un concepto llamado máquinas de estados finitos. Cada paso del procedimiento constituye un Estado, y las transiciones entre estados se producen de acuerdo con interfaces

bien definidas, y son realizadas en función de unos eventos definidos. Las tareas individuales luego se transfieren a través de estas máquinas de estados finitos, según corresponda, gestionando a través del núcleo del sistema de gestión de flujo de trabajo, también llamado el motor de flujo de trabajo.
Tanto los sistemas de tickets como los sistemas de órdenes de trabajo pueden ser considerados como ejemplos de flujos de trabajo especializados. Sin embargo, un sistema de gestión de flujo de trabajo es de carácter más general y altamente personalizable, para permitir la incorporación de cualquier tipo de flujo de trabajo.

1.6. Monitorización y rendimiento de servicios y recursos.

Todo proveedor de servicios de red necesita vigilar los servicios que proporciona y los recursos que utiliza, estos servicios deben proporcionar un rendimiento adecuado y utilizar recursos necesarios para que un buen rendimiento.
Los recursos generan una serie de gastos que son cubiertos mediante los ingresos de la empresa, que obtiene del pago de los clientes que utilizan los servicios de la red; también la empresa tiene otros gastos. No olvidemos que los proveedores de servicios en red son empresas que deben hacer negocio y que estos sean rentables.
La monitorización de servicios y recursos, permiten conocer el rendimiento de todos los servicios que se proporcionan y asignar los recursos necesarios en función del rendimiento que tiene un servicio, asignando más recursos en caso de que un servicio agote los recursos asignados. Una correcta monitorización consigue que el gasto en recursos sea el necesario para que el rendimiento sea optimo y los usuarios estén satisfecho con el servicio prestado.
Por ejemplo, para un servicio ADSL si la monitorización indica que hay una pérdida de rendimiento por una determinada causa y después de analizar la información obtenida, se detecta que hay un aumento de clientes que están saturando la central. Una posible solución sería asignar más recursos a esa central para que el rendimiento sea el adecuado.
Un rendimiento óptimo en los servicios hace aumentar la satisfacción de los clientes y mejora la imagen de la empresa, influyendo en la incorporación de nuevos clientes como en la retención de los clientes actuales e incluso puede ocurrir que los clientes soliciten otros servicios de la empresa, con aumento de ingreso que conlleva.
En la monitorización de los servicios y recursos, podemos obtener las siguientes funcionalidades:

- ⇨ Prevención de errores: cualquier comportamiento anómalo es detectado de forma temprana y permite actuar con más rapidez para resolver ese comportamiento, evitando que esa anomalía se convierta en un error grave.
- ⇨ Uso eficiente: `la monitorización permite conocer si un recurso o servicio está siendo utilizado de forma excesiva y actuar antes de que el servicio sufra una saturación. Permite prevenir el uso excesivo de un servicio.
- ⇨ Disponibilidad: podemos conocer cuánto tiempo lleva funcionando un servicio o recurso de forma ininterrumpida. Determinados servicios son considerados críticos y un corte en su funcionamiento puede provocar grandes pérdidas para la empresa, una correcta monitorización de un servicio permite prevenir un mal funcionamiento, aumentando la disponibilidad del servicio.
- ⇨ Carga de trabajo: conocer en qué momento un servicio o recurso es más utilizado y cuándo menos, podremos asignar más recursos en los momentos de uso más altos, evitando una saturación. Adaptando la cantidad de recursos asignados a un servicio en función de la carga de trabajo.
- ⇨ Rendimiento: conocer en todo momento el rendimiento de cada componente de la red, servicio, recursos, hardware, etc.
- ⇨ Ingresos: permite conocer los ingresos que genera cada cliente y servicios que proporciona la empresa.
- ⇨ Clientes: conocer el comportamiento de los clientes de la empresa.

Hay diferentes sistemas que permiten realizar la monitorización, podemos clasificarlos en tres tipos:

- ⇨ Sistemas de aprovisionamiento de servicios
  Este tipo de sistemas se utiliza en grandes proveedores de servicios, suelen ser aplicaciones muy complejas. Permite desplegar servicios sobre una red y es utilizado por empresas proveedores de servicios de red para el despliegue de sus redes. Este tipo de sistemas funcionan recibiendo una serie

de solicitudes de servicios, estas solicitudes indican una activación o desactivación de un servicio y son traducidas en una serie de órdenes enviadas a la red.
Permiten a los proveedores de servicio desplegar servicios en una escala muy grande, tienen una carga de trabajo muy alta, recibiendo un alto número de solicitudes de servicio cada día.
Habitualmente este tipo de sistemas son autónomos y no necesitan la intervención de un administrador, por esta razón no suelen proporcionar una interfaz gráfica y en los pocos casos que un administrador tenga que interactuar con el sistema, se proporciona un terminal de línea de comando de intervención humana. Por esta razón, en muchos casos solo proporcionan un terminal de comandos.
Este tipo de sistemas suele comunicarse con otros sistemas, como ejemplo cuando otros sistemas le envían solicitudes. Para establecer comunicación con otras aplicaciones, estos sistemas proporciona un API (Interfaz de Programación de Aplicaciones) que permiten programar cómo se realiza la comunicación con otros sistemas evitando la intervención humana.

- ⇨ Sistemas de gestión de orden de servicios

Los sistemas de gestión de orden de servicio permiten gestionar las órdenes de servicio que han sido enviadas por clientes de un servicio, el ámbito de uso son empresas proveedores de servicios (igual que con los sistemas de provisión de servicios). Este tipo de sistemas son una parte de un tipo de herramientas denominadas CRM, herramienta para administrar las relaciones con los clientes, que incluye un amplio conjunto de funciones, como pueden funciones de helpdesk.

- Identificación de equipos necesarios.
- Realización de controles de crédito del cliente.
- Programar el cumplimiento de las órdenes de servicio.
- Envío de solicitudes para activar los servicios de un sistema de abastecimiento de servicio.

El funcionamiento de este sistema está basado en el concepto de flujos de trabajo especializados, que es similar a las órdenes de trabajo o la gestión de tickets de problemas. Estos sistemas ayudan a los proveedores de servicios al seguimiento y cumplimiento de las órdenes de servicios, automatizando el proceso.
El procedimiento que se realiza para ejecutar una orden de servicio es el siguiente:
Los sistemas de aprovisionamiento de servicios y los sistemas de gestión tiene un funcionamiento similar, los dos utilizan el concepto de orden de servicio, pero en el segundo caso su funcionamiento se basa en el concepto de flujo de trabajo y su gestión, y en el primer caso se trata de una aplicación que realiza una comunicación con la red para configurarla.

- ⇨ Sistemas de facturación

Los proveedores de servicios de red reciben una serie ingresos de los clientes que utilizan sus servicios, estos ingresos permiten a un proveedor seguir proporcionando sus servicios a mas clientes o ampliar los servicios, como cualquier empresa obtener beneficio económico de los servicio que presta
Para gestionar los ingresos que reciben se utilizan los sistemas de facturación, este tipo de sistema son utilizados para conocer la facturación de la empresa, entre las funciones que desempeña tenemos:

- Conocer la contabilidad.
- Identifica los servicios prestados a los clientes.
- Define la tarificación de los servicios.
- Detección de fraudes.
- Control de los pagos de los clientes.
- Define las diferentes formas de pagos.
- Muestra estadísticas de los ingresos de cada uno de los servicios.

Los sistemas de facturación necesitan comunicarse con otras aplicaciones, en especial con el CRM de la empresa para los datos de clientes y poder facturar, conocer los pagos pendientes o los servicios contratados.

1.6.1. Clasificación de los sistemas de medida de consumos y rendimientos.

En toda red de comunicación se necesita medir diversos parámetros, que pueden ser divididos en dos tipos.

- ⇨ Consumos: estos parámetros permiten conocer el gasto que se realiza en la red. Entre los que hay que destacar el consumo de ancho de banda o el consumo eléctrico, estos dos parámetros son muy importantes. El consumo de ancho de banda óptimo permite que los servicios de la red funcionen

correctamente o detectar congestiones. Todos los componentes de la red se alimentan de electricidad y medir el consumo permite detectar diferente anomalías que pueden provocar fallos en los componentes de la red.

- ⇨ Rendimientos: estos parámetros permiten conocer el nivel de funcionamiento de los componentes tanto hardware como software, un buen rendimiento significa que el componente funciona de forma correcta y un mal rendimiento significa que componente tiene algún fallo en su funcionamiento. Respecto al hardware medir el tiempo de funcionamiento de diversos componentes , por ejemplo medir el tiempo que un disco duro accede a los sus datos, para el software medir el tiempo en que un determinado software procesa una determinada tarea.

Estos factores permiten conocer el funcionamiento de forma detallado de la red, mediante determinadas herramientas podemos realizar mediciones muy precisas en los diversos componentes de la red, que permitirán conocer al administrador el consumo en función de diversos parámetros, como el rendimiento de los componentes de la red.

Hay muchos parámetros que nos permitirán conocer el consumo de un dispositivo, el más representativo es el consumo eléctrico. Conociendo el consumo que se produce en la red, un administrador puede utilizar esta información para:

- ⇨ Si un dispositivo consume más electricidad de lo habitual, puede producirse una sobrecarga en el dispositivo que puede conllevar con una rotura, controlando el consumo eléctrico puede prevenirse.
- ⇨ Eficiencia energética, la electricidad conlleva un coste, si el consumo eléctrico se realiza de manera eficiente se producirá un ahorro en el consume y un menor coste. Realizando de forma periódica mediciones, el administrador conocerá los intervalos de tiempo donde más consumo se produce y cuando, pudiendo realizar los cambios pertinentes para adaptarse a eso periodos de consumo. También se puede utilizar dispositivos que consuman menos electricidad.
- ⇨ Controlar subidas y bajadas de tensión que pueden provocar fallos en los dispositivos. Hay dispositivos hardware como los SAI, que previenen estas situaciones.

Un factor a tener en cuenta, es la proporcionalidad entre consumo y potencia, las grandes redes consumen mucha electricidad, esto significa que las grandes infraestructuras requieren un gran consumo de electricidad, aunque no debe realizarse un desperdicio de la misma.

Otro tipo de consumo que debe medirse es el consumo de ancho de banda. En toda red de comunicación hay disponible un ancho de banda disponible, que influirá en la velocidad de transmisión de la información entre los dispositivos de la red. El uso del ancho de banda debe ser eficiente, de forma que todos los servicios y los clientes de la red puedan obtener adecuada en la red.

Para realizar esta tarea, son planificadas una serie de mediciones periódicas de diferentes parámetros permitirá conocer el uso del ancho de banda de la red y detectar posibles anomalías. Hay múltiples mediciones que se pueden realizar, entre los parámetros a monitorizar tenemos:

- ⇨ Tráfico entrante y saliente, existen diversas medidas como: Byte por segundo, paquetes o bit por segundo. Consiste en medir la cantidad información de entrada o de salida tanto en un red como un componente de ella.
- ⇨ Número de peticiones, pueden ser para un servidor web, base de datos u otro tipo de software. Permite conocer el uso que realiza un determinado software del ancho de banda de la red.

Otro punto a tener en cuenta, dentro de un sistema operativo se ejecuta un número de procesos, conocer el ancho de banda que utiliza cada proceso, nos permitirá saber si algún proceso realiza un uso no adecuado del ancho de banda e investigar las causas.

El ancho de banda es referido tanto para la transmisión de información en una red local como para Internet, el uso indebido del ancho perjudica a otros servicios. Debe realizarse un reparto del ancho de banda en función de varios criterios (equitativo o prioritario), cada cliente o servicio debe tener una parte del ancho de banda en función del criterio seleccionado.

Las mediciones de rendimientos consisten en monitorizar diversos parámetros, el rendimiento depende del componente, podemos diferenciar entre dos tipos.

- ⇨ Hardware. CPU, disco duro, memoria, interfaz de red, etc.
- ⇨ Software. Sistemas operativos, base de datos, servidores web, etc.

Respecto al hardware, se mide diversos componentes, entre los parámetros que se suelen medir tenemos.

- ⇨ Velocidad de funcionamiento, la velocidad de funcionamiento del componente nos indica el rendimiento.
- ⇨ Tiempo: un menor tiempo en realizar una determinada tareas nos indica un buen rendimiento para un hardware. Por ejemplo, el tiempo que tarda un disco duro en acceder a un determinado dato, un tiempo muy bajo indica un rendimiento alto.

Respecto al software, también se mide la velocidad y el tiempo para realizar determinadas tareas para saber su rendimiento, otros parámetros específicos para el software.

- ⇨ Procesamiento: la cantidad de trabajo (carga de trabajo) que es capaz de soportar un determinado software, permite conocer el rendimiento, mayor carga de trabajo mayor rendimiento. Dependiendo del software la carga de trabajo que medirá será diferente, para una servidor web será la cantidad de peticiones o para una servidor de base de datos la cantidad de consultas que soporta.

Estas mediciones pueden ser utilizadas para conocer el rendimiento de un determinado componente hardware/software antes de utilizarlo en un entorno de producción y conocer si el componente es adecuado para el entorno donde se va a utilizar.

Para realizar estas mediciones se pueden utilizar tanto componentes hardware como software, utilizan una serie monitores que consiste en un software que recopila la información para realizar las mediciones.

Los componentes hardware están compuestos de un software para medir en un hardware específico para esa tarea. Los componentes software son herramientas que son instaladas en el sistema que permiten realizar las mediciones. Los componentes hardware y software proporcionan un conjunto de métricas para realizar las mediciones.

Estos componentes pueden ser de dos tipos, en función de cómo realizar las mediciones, estos tipos son:

- ⇨ Centralizados: las mediciones son recogidas por un solo dispositivo.
- ⇨ Distribuidos: las mediciones son recogidas por varios dispositivos.

1.6.2. Parámetros de rendimiento de los servicios ofrecidos en la red

Un proveedor de red proporciona una serie de servicios a sus clientes. Estos servicios deben tener un óptimo rendimiento para conseguir un alto de grado de satisfacción por parte de los clientes, esta satisfacción permitirá que el cliente mantenga el servicio o contrate más servicios con el proveedor. Todo esto repercute de manera económica, mediante los ingresos por parte de los clientes, a la empresa y obteniendo un beneficio económico para el proveedor.

Todo servicio debe ser monitorizado por personal cualificado utilizando herramientas de gestión, esta monitorización permite conocer el estado del servicio y su rendimiento, actuando con rapidez en caso de fallo en un servicio.

Para medir el rendimiento de un servicio se debe realizar una serie de pasos.

- ⇨ Recolección de información.
- ⇨ Representación de los datos.
- ⇨ Análisis de datos.

Recolección de información

Para medir el rendimiento de un servicio se debe obtener información del servicio, escogiendo una serie de datos que permitirán saber cómo está funcionando un determinado servicio, este proceso se define como recopilación de información.

Con estos datos recopilados se puede calcular una serie de parámetros que serán utilizados para conocer de forma exacta el rendimiento del servicio, a esto se le denomina monitorizar un servicio.

Los servicios son ejecutados en una red, con lo que el rendimiento de la red afecta al rendimiento de los servicios, también se debe monitorizar diferentes parámetros de la red. Es muy importante monitorizar la red porque su rendimiento influirá mucho en la calidad del servicio y la satisfacción del cliente.

También el sistema, tanto hardware como software, donde se encuentre el servicio debe funcionar de manera correcta, el funcionamiento del sistema influye en el rendimiento del sistema. Cualquier error que se produzca en el sistema afectará negativamente al servicio. El sistema donde se encuentre el servicio debe ser monitorizado.

Por ejemplo, si un proveedor de servicio ofrece correo electrónico a sus clientes, este servicio deberá estar alojado en un equipo (ordenador) para su funcionamiento, se deberá monitorizar tanto los componentes

hardware (CPU, discos duros, memoria, etc.) como sus componentes software, servidor de correo electrónico.
La recopilación de datos para medir el rendimiento de una red se aplica a tres componentes que podemos dividir de la siguiente manera: rendimiento de red, rendimiento de sistemas y rendimiento de servicios. Cada uno de ellos, tendrá una serie de parámetros propios y algunos parámetros se pueden aplicar más generales.
Para el rendimiento de red se pueden monitorizar diferentes parámetros como:

- ⇨ Paquetes perdidos en la red.
- ⇨ Transferencia de paquetes.
- ⇨ Retardo producido.
- ⇨ Congestión en la red.
- ⇨ Velocidad de transmisión.

Para el rendimiento del sistema.

- ⇨ Carga de trabajo.
- ⇨ Memoria RAM disponibles.
- ⇨ Numero de procesos en ejecución.
- ⇨ Interfaces de red.
- ⇨ Disco duro.

Respecto al rendimiento del servicio, los parámetros a monitorizar dependerán del servicio, los parámetros para un servicio de base de datos son diferentes a los parámetros de un servidor web.
Para obtener esos datos, el administrador tiene disponible varias herramientas para obtener los parámetros de rendimiento.

- ⇨ Dependiendo del servicio o el sistema, puede incluir herramientas que proporciona información sobre su rendimiento. Por ejemplo, la base de datos MySQL incluye los “profiler” que proporciona información del rendimiento de las consultas de la base de datos en función de diversos parámetros (tiempo de ejecución, carga CPU, etc.).
- ⇨ Las herramientas de gestión, por ejemplo Nagios, proporcionan monitorización de diferentes parámetros, obteniendo una amplia variedad de información de servicios, red y sistemas.
- ⇨ Mediante protocolos de gestión, por ejemplo SNMP, podemos obtener diversos parámetros, estos protocolos pueden son utilizados por las herramientas de gestión.
- ⇨ Herramientas de generación gráficas como Cacti o Munin, que permiten visualizar los datos mediante una serie de gráficas, un administrador puede monitorizar diversos parámetros de un componente para conocer su rendimiento. Para obtener datos de los componente utiliza un protocolo de gestión como SNMP.

Representación de datos

La información obtenida puede tener un formato bastante inteligible, esta información debe ser convertida a un formato más legible para un administrador, que le permitirá realizar un análisis de los datos obtenidos de forma más sencilla.
Entre los formatos más utilizados se encuentran.

- ⇨ Gráficas: es una representación visual de los datos, utilizando diferentes tipos de gráficas (lineal, barras, circular, etc.). Este tipo de formato permite rápida visualización de los parámetros monitorizados y facilitan el análisis de los parámetros, es muy fácil detectar un bajada de rendimiento de un parámetro o un consumo excesivo de un recurso, con solo un vistazo a la gráfica correspondiente. Herramientas como Cacti o Munim permiten realizar gráficas de múltiples parámetros.
- ⇨ Tabular: representación de los datos en formato de tabla, si queremos representar parámetros donde conocer el valor exacto es conveniente, este tipo de formato es muy útil.
- ⇨ Otros formatos: como puede ser CSV o xls para hojas de cálculo, determinados programas incluyen su propio formato.

Análisis de datos

Con los datos obtenidos de los parámetros de un servicio, el siguiente paso será realizar un análisis de datos para conocer el rendimiento del servicio en un periodo de tiempo. Este análisis se puede realizar de forma manual -el administrador observando los datos mostrados determina el rendimiento-, o herramientas que se encargan de realizar el análisis de forma automática.

El resultado del análisis nos permitirá conocer si el servicio está funcionando con el rendimiento deseado o si hay alguna anomalía en el funcionamiento, en este caso se deberá aplicar las medidas adecuadas para obtener el rendimiento esperado.

El administrador necesita conocer cuál es el rendimiento adecuado para un servicio, debe tener en cuenta diversos factores.

- ⇨ Clientes que usen el servicio: el rendimiento de un servicio que usen millones de clientes no es el mismo que un servicio para cientos de clientes.
- ⇨ Recursos disponibles: los recursos que se tengan influirán en el rendimiento. El rendimiento de un servicio de Google, con muchos recursos disponibles, no puede ser el mismo que un servicio proporcionado por un servidor casero.
- ⇨ Tipo de red: la tecnología utilizada influye en el rendimiento, no es lo mismo ADSL o fibra óptica.
- ⇨ Ámbito: donde se proporciona el servicio, red local o Internet, el servicio es para un ámbito domestico o empresarial.

Teniendo en cuenta estos factores, un administrador puede conocer cuál es el rendimiento esperado para un determinado servicio. Conociendo el rendimiento del servicio y su posterior análisis podemos obtener información sobre su funcionamiento, saber si los recursos asignados al servicio son los adecuados, ver si se ha producido en algún momento saturación, conocer la carga de trabajo del servicio y si con los recursos disponibles se puede soportar, cuanto utilizan los clientes un servicio…etc

Conociendo lo anterior, el administrador debe escoger que tipo de parámetros de rendimiento que se van a monitorizar. Para escoger estos parámetros se utilizan diversas métricas de rendimiento de servicios, definiendo los aspectos claves que queremos medir.

Los servicios tienen una serie de factores que hay que tener en cuenta para medir sus rendimientos, estos factores son: tiempo de espera, disponibilidad, valor económico y uso:

- ⇨ Tiempo de espera: mide el tiempo que transcurre desde que un cliente realiza una petición a un servicio y la respuesta del servicio. Un tiempo de espera bajo es lo deseable.
- ⇨ Disponibilidad: un servicio debe estar en funcionamiento todo el tiempo, para que los clientes siempre puedan acceder al servicio, dependiendo de la importancia del servicio el grado de disponibilidad será diferente, aunque los deseable es un grado de disponibilidad alto.
- ⇨ Uso: otro aspecto que podemos medir es el uso de un servicio, cuantos clientes utilizan el servicio, a que hora, tiempo de uso por cliente, etc.
- ⇨ Valor económico: medición de un servicio en función de la economía de la empresa, gastos, ingresos que genera, ingresos por cliente, etc.

Métrica es una unidad de medida estándar que calcula un resultado.

El administrador puede escoger entre los factores expuestos, como medir el rendimiento de un servicio y escoger los parámetros de medición.

Hay que tener en cuenta que cada servicio tiene sus propios parámetros para medir su rendimiento.

Hay disponibles un conjunto parámetros que podemos utilizar para medir el rendimiento de un servicio.

- ⇨ Carga del servicio: Cantidad de procesos que ejecutan en un momento dado, mide el procesamiento que genera un servicio en función de tiempo.
- ⇨ Carga de usuario: La carga que genera cada usuario en los servicios. Nos permite conocer si algún usuario produce un exceso de carga en el servicios
- ⇨ Uso memoria: Cantidad de memoria utilizada por los servicios, nos permite conocer si el sistema tiene suficiente memoria para los servicios ofrecidos o si algún servicio realizar un uso excesivo de memoria.
- ⇨ Número de peticiones: Cantidad de peticiones que recibe un servicio, si recibe un número muy alto de peticiones puede hacer caer el servicio.
- ⇨ Usuarios por servicios: Cantidad de usuarios (clientes) que utilizan un servicio.
- ⇨ Ancho de banda: Mide la cantidad de ancho de banda que utilizan los cliente, podemos averiguar si el ancho de banda que tiene disponible un servicio es suficiente.

- ⇨ Tiempo de acceso: Tiempo que tarda un cliente en acceder a un servicio.
- ⇨ Tiempo de respuesta: Tiempo que tarda un servicio en responder.

Como se ha indicado anteriormente, cada servicio contiene una serie de parámetros propios que se utilizan para medir los servicios.
Por ejemplo para un servicio DNS, se mide una serie de parámetros del servidor DNS que ofrece el servicio.
Algunos de estos parámetros son:

- ⇨ Número de peticiones con éxito.
- ⇨ Número de peticiones que resultaron en una referencia.
- ⇨ Número de peticiones cuyo nombre no contenía el tipo de record consultado.
- ⇨ Número de peticiones cuyo nombre no existía.
- ⇨ Número de peticiones recursivas que requirieron el envío de una o más peticiones por el servidor.
- ⇨ Número de peticiones totales.

Todos estos valores nos permiten conocer el rendimiento real del servicio, incluso podemos generar una serie de estadísticas que nos ayudarán a conocer mejor el rendimiento del servicio.
Respecto al rendimiento de la red, podemos medir una serie de parámetros, entre los cuales tenemos:

- ⇨ Paquetes perdidos: Cantidad de paquetes que han sido enviados pero no han sido recibidos.
- ⇨ Retardo: Tiempo transcurrido en transmitir un paquete durante su trayecto completo.
- ⇨ Paquetes por segundo: Mide la velocidad de transmisión en paquetes por segundo.
- ⇨ Utilización del canal: Uso del canal de comunicación que se utiliza en la red.
- ⇨ Errores: Nos permite conoce la frecuencia en que se producen errores en la red.
- ⇨ Jitter: Nos muestra la frecuencia en que se produce jitter, que provoca retrasos de la señal.

Respecto a los sistemas, principalmente se mide el rendimiento de los componentes del sistema, entre los cuales tenemos.

- ⇨ Carga de CPU: Una carga alta de la CPU afecta negativamente al rendimiento del sistema.
- ⇨ Uso de memoria RAM: Nos permite conocer el uso de la RAM y la memoria disponible (libre).
- ⇨ Errores de paginación: Número de errores que se producen en el funcionamiento en la RAM.
- ⇨ Temperatura de CPU: Mide la temperatura de la CPU, si la temperatura es muy alta puede averiar la CPU.
- ⇨ Espacio disponible del disco duro: Muestra el espacio libre en el disco duro.
- ⇨ Uso de memoria virtual: Un uso alto de este tipo, perjudica el rendimiento del sistema e indica que la memoria RAM es insuficiente.
- ⇨ Iowat: Tiempo en que el software está en pausa hasta que tiene acceso al hardware.

Otra forma de conocer el rendimiento de un servicio "poniendo a prueba" es ejecutando una serie de pruebas con posible escenarios de trabajos. Existen diversas herramientas que proporcionan una batería de pruebas que comprobar el rendimiento, para ejecutar este tipo de pruebas el servicio no puede estar en producción, este tipo de pruebas influirá negativamente en el servicio si estuviera en funcionamiento.
Este tipo de pruebas nos permite conocer de antemano el rendimiento del servicio. Se pueden configurar las pruebas para que se asemejen al escenario donde el servicio va a funcionar, aunque no se puede simular el escenario real al cien por cien, si permite tener una aproximación del rendimiento.
El resultado de las pruebas nos permitirá conocer si la configuración del servicio es la adecuada para el escenario real donde el servicio funcionará. Si el resultado no es el esperado, se puede cambiar la configuración del servicio y volver a pasar las pruebas, este proceso se puede repetir hasta conseguir el resultado esperado.

Muchos servicios proporciona herramientas propias para comprobar su rendimiento, un conjunto de herramienta de rendimiento para diferentes servicios son:

Servicio	Herramientas
HTTP	ab comando para probar el rendimiento de un servidor web como Apache o Ngnix.
DNS	dig, Domain Name Speed Benchmark, permiten realizar consultas al DNS mostrando el tiempo que tardan y otro tipos de pruebas.
Base de datos	osdb o mysqlsap para MySQL, pgBench para postgresql
ADSL	Hay diversas herramientas, muchas de ellas son online, que permiten medir el rendimiento del ADSL, como ejemplo tenemos LineBenchmark o NetGauge.
Mail	mstone para diverso protocolos(POP,SMTP y IMAP), Smtp Open Relay Checker para SMTP

Existen herramientas de pruebas de rendimientos que funcionan para una variedad de servicios, un ejemplo es Apache JMeter que proporciona pruebas para HTTP, FTP, FTP, Mail (SMTP, POP3 y IMAP) y más servicios.
Como **ejemplo** de herramienta de prueba de rendimiento, veremos algunos ejemplos de ab (Apache Bench).
Esta herramienta viene incluida con el servidor web Apache, en Linux dependiendo de la distribución de Linux se encuentra en un paquete, httpd-tools en Centos/fedora o apache2-utils en debian. Para ejecutar una prueba se ejecuta el comando ab con una serie de opciones y una dirección, por ejemplo.

ab –n 100 –c 10 http://www.google.es/

Esta prueba ejecuta 100 peticiones a google.es (-n 100) con un máximo de 10 peticiones de forma concurrente. En el resultado se muestra diferente información como:
–Datos sobre la dirección indicada como el software servidor, el nombre y puerto.
–Número de peticiones resueltas.
–Cantidad de peticiones por segundo que el servidor pudo servir por segundo.
–Tiempo del Test.
–Tasa de transferencia.
–Porcentaje de conexiones.
La herramienta ab permite exportar los datos obtenidos en los resultados a otros formatos y visualizarlos con otros programas, como GNUplot o Excel. Utilizando la opción –g (formato GnuPlot) o –e (formato CSV) seguido por el nombre de fichero.

ab –n 100 –c 10-g resultado.dat http://www.google.es/

El resultado será exportado a un fichero resultado.dat, en formato GNUplot y poder realizar gráficas con ese programa.
También podemos generar un fichero html o php para testear cómo lo procesa Apache, hay disponibles por internet múltiples ejemplos de ficheros que podemos utilizar. El fichero debe ser copiado en la ruta de Apache.

ab -n 100 -c 10 -e resultado.dat http://debian.servidor/ejemplo.php

Los resultados obtenidos se refieren al procesamiento del fichero escogido.
Este método de probar el rendimiento es muy útil para comprobar cómo se comporta un servidor Apache en distintos escenarios. Por ejemplo, se puede crear un fichero con código php y acceso a una base de datos, para crear un escenario con acceso a una base de datos.

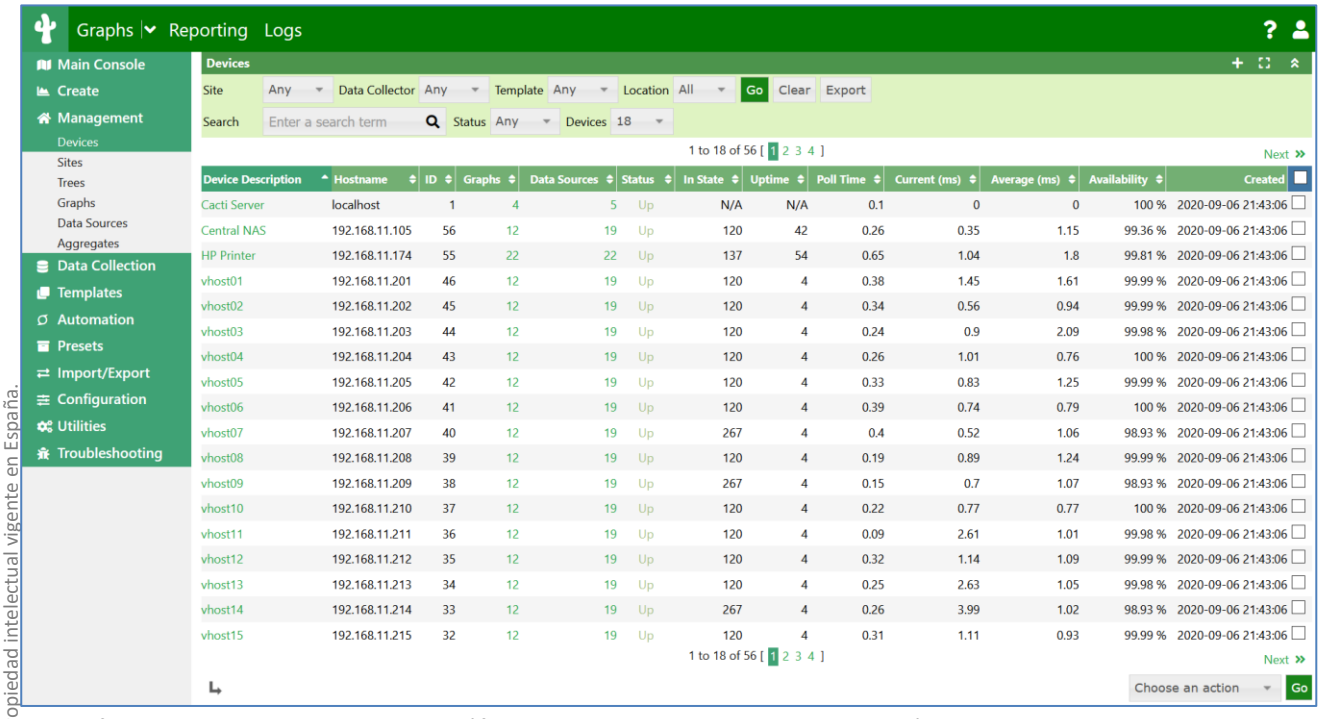
Cacti

Como parte **práctica**, un pequeño tutorial sobre un programa generador de gráficos en red denominado **Cacti**. Esta herramienta permite conocer el rendimiento de un componente de la red por medio de la visualización de múltiples parámetros por medio de una serie de gráficas. Un administrador analizando esas gráficas puede conocer el funcionamiento de la red y sus componentes.
Primero se explicará la instalación y una configuración básica para crear algunas gráficas. Este software permite generar gráficas de datos obtenidos, mediante la herramienta RRDtool, y proporciona múltiples métodos para recopilar de datos. Cacti proporciona una interfaz web donde se visualizan las gráficas creadas y permite realizar otras tareas de administración.

Cacti recopila información de forma periódica y los almacena en una base de datos, para generar una gráfica se debe escoger cuál es la fuente de datos donde se obtendrá la información para generar una gráfica. Esta herramienta de software libre está disponible para Windows y Linux, requiere una serie de requisitos como:
–Servidor web: soporta Apache, IIS o Ngnix.
–PHP: Cacti está desarrollado en PHP con lo que es necesario su instalación.
–Base de datos: requiere una base de datos donde se almacenarán los datos, MySQL es una buena opción.
–RRDtool: librería de perl utilizada para trabajar con los datos obtenidos y generar las gráficas.
–SNMP: debe estar instalado porque es el protocolo que Cacti utiliza para la obtención de datos.
La instalación es muy sencilla, para Linux hay disponibles paquetes para diversas distribuciones de Linux y en Windows descargar el fichero zip y seguir las instrucciones disponibles en la página web de Cacti **www.cacti.net**.
En el caso de instalar Cacti Debian, hay disponible un paquete que facilita la instalación.
apt-get install cacti
Instalará todos los requerimientos de Cacti.
Hace falta instalar SNMP, si no ha sido instalado anteriormente.
apt-get install smnp smnpd
A fin de obtener datos, en la instalación se ha creado un fichero de crontab, /etc/cron.d/cacti, donde se especifica la periodicidad de obtención de datos.
Con esto ha finalizado la instalación de Cacti, ahora se deberá ejecutar la interfaz web para configurar los diversos dispositivos de donde se obtendrán los datos y las gráficas que se van a generar.
Definición
Contrab es un fichero de configuración para el servicio cron, utilizado en sistemas Linux, que permite generar tareas (guiones), como ejecutar un comando, de forma periódica. Cada tarea definida se crea en una línea denominada trabajo, utilizando una sintaxis propia, el fichero contrab estará compuesto por una serie de líneas que representan a conjunto de trabajos que especifican una serie de tareas que se realizarán de forma periódica. Hay muchos manuales disponibles en internet, donde se explica la sintaxis utilizada, que es bastante simple.
Para visualizar la interfaz web de Cacti, abrimos el navegador e introducimos.

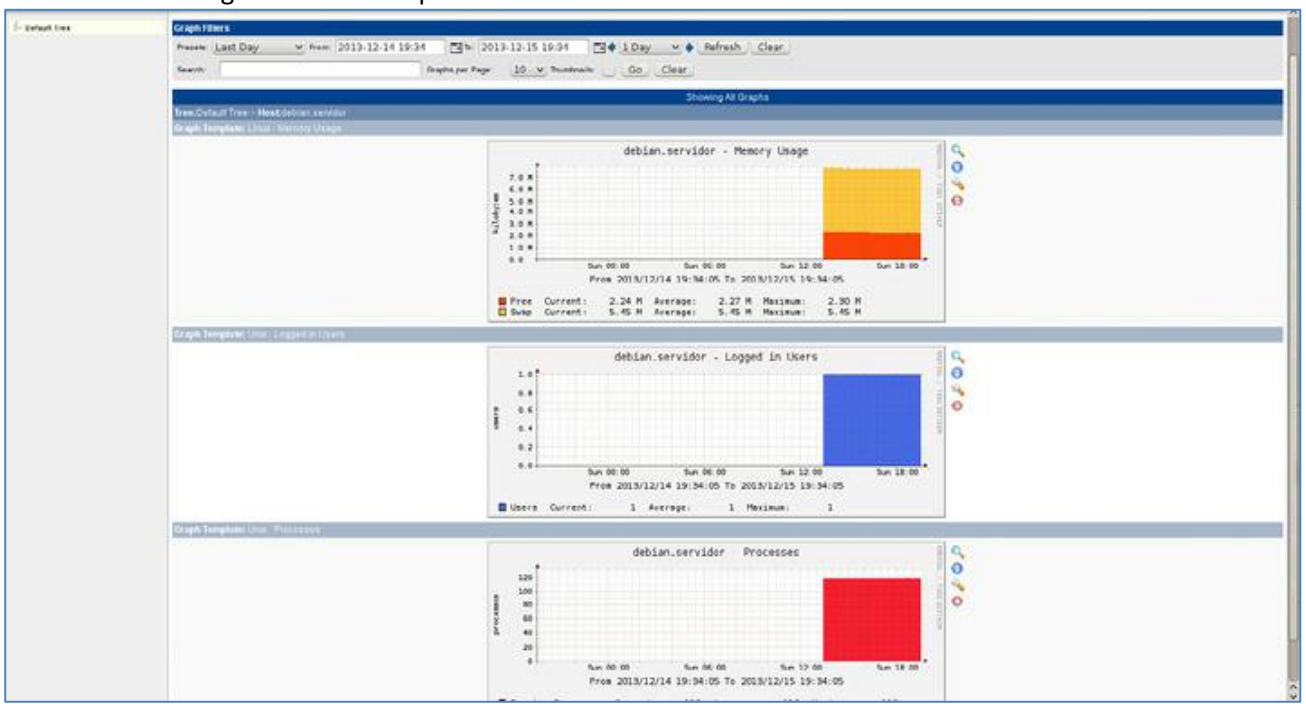
http://direcciónIP o nombre máquina/Cacti

Nos solicitará el usuario y contraseña de Cacti, especificado en el proceso de instalación. Mediante una serie de pasos, solicitando información en algunos pasos, se procederá a instalar Cacti, una vez ha finalizado la instalación se mostrará la interfaz de Cacti.



Por defecto Cacti crea una serie de gráficas para localhost, nombre de la máquina local donde se encuentra

Cacti instalado. Las gráficas creadas por defecto se muestran en la pestaña Graphs, pulsando en esa pestaña se verán todas las gráficas creadas por defecto.



Si la máquina tiene definido un nombre diferente a localhost, especificar ese nombre pulsando en la pestaña Console y en la columna de la derecha, escoger la opción Management->Device, donde aparecerá la lista de máquina que Cacti monitoriza. En este caso, solo aparece localhost, pulsamos en la siguiente ventana especificar los datos en Hostname y en Description.

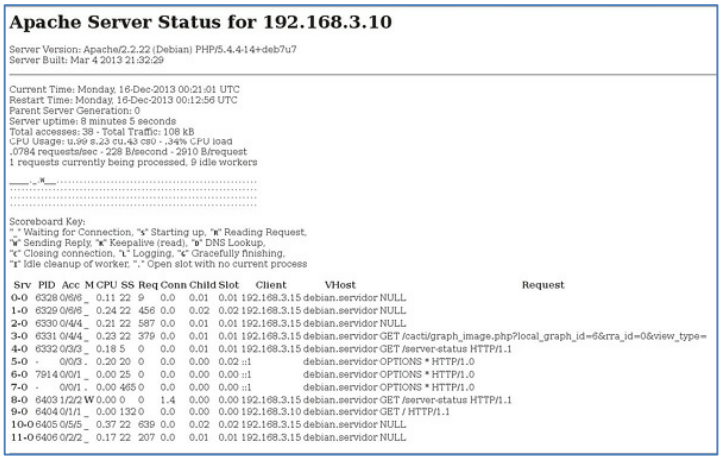
Para crear una nueva gráfica para monitorizar diversos parámetros de un servidor Apache, utilizaremos una plantilla de Cacti denominada apachestats, que proporciona diversas gráficas de diversos parámetros para un servidor Apache y utiliza un script denominado ws_apachestats. Tanto la plantilla como el script se pueden encontrar en los foros de Cacti.

Como requisito previo, es necesario activar el módulo de Apache mod_status, este módulo proporciona diferente información sobre el funcionamiento de Apache. En Debian este módulo viene cargado por defecto, para saber si el módulo esta en ejecución, comprobar si hay un fichero status.conf y status.load en /etc/apache2/mods-available. En caso contrario, el módulo no está cargado y hay que modificar la configuración de Apache para cargarlo.

Para comprobar que el módulo está cargado, abrir el navegador e indicar la siguiente dirección.

http://direcciónServidorApache/server-status

Mostrará una página con información de Apache.



Apache Server Status for 192.168.3.10

Server Version: Apache/2.2.22 (Debian) PHP/5.4.4-14+deb7u7
Server Built: Mar 4 2013 21:32:29

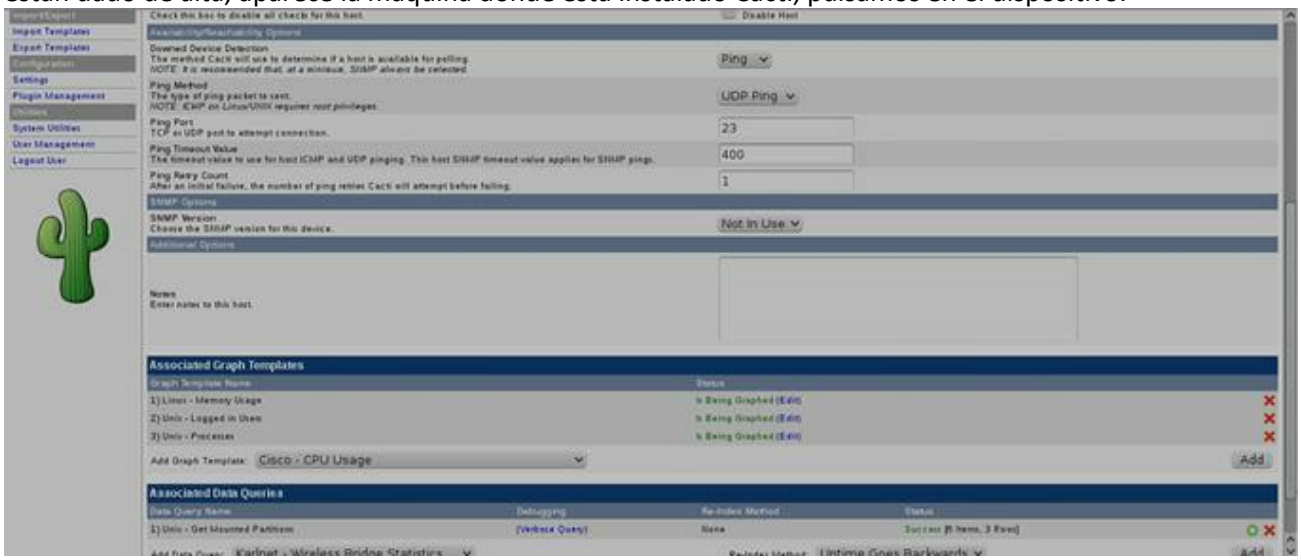
Current Time: Monday, 16-Dec-2013 00:21:01 UTC
Restart Time: Monday, 16-Dec-2013 00:12:56 UTC
Parent Server Generation: 0
Server uptime: 8 minutes 5 seconds
Total accesses: 38 - Total Traffic: 108 kB
CPU Usage: u.99 s.23 cu.43 cs0 - .34% CPU load
.0784 requests/sec - 228 B/second - 2910 B/request
1 requests currently being processed, 9 idle workers

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-0	6328	0/6/6	_	0.11	22	9	0.0	0.01	0.01	192.168.3.15	debian.servidor	NULL
1-0	6329	0/6/6	_	0.24	22	456	0.0	0.02	0.02	192.168.3.15	debian.servidor	NULL
2-0	6330	0/4/4	_	0.21	22	587	0.0	0.01	0.01	192.168.3.15	debian.servidor	NULL
3-0	6331	0/4/4	_	0.23	22	379	0.0	0.01	0.01	192.168.3.15	debian.servidor	GET /cacti/graph_image.php?local_graph_id=6&rra_id=0&view_type=
4-0	6332	0/3/3	_	0.18	5	0	0.0	0.01	0.01	192.168.3.15	debian.servidor	GET /server-status HTTP/1.1
5-0	-	0/0/3	.	0.20	20	0	0.0	0.00	0.02	::1	debian.servidor	OPTIONS * HTTP/1.0
6-0	7914	0/0/1	_	0.00	25	0	0.0	0.00	0.00	::1	debian.servidor	OPTIONS * HTTP/1.0
7-0	-	0/0/1	.	0.00	465	0	0.0	0.00	0.00	::1	debian.servidor	OPTIONS * HTTP/1.0
8-0	6403	1/2/2	W	0.00	0	0	1.4	0.00	0.00	192.168.3.15	debian.servidor	GET /server-status HTTP/1.1
9-0	6404	0/1/1	_	0.00	132	0	0.0	0.00	0.00	192.168.3.10	debian.servidor	GET / HTTP/1.1
10-0	6405	0/5/5	_	0.37	22	639	0.0	0.02	0.02	192.168.3.15	debian.servidor	NULL
11-0	6406	0/2/2	_	0.17	22	207	0.0	0.01	0.01	192.168.3.15	debian.servidor	NULL

La plantilla debe ser importada a Cacti, utilizar la opción Import Template en la sección Import/Export de la consola de Cacti y escoger la plantilla para importar.

Otro paso es copiar el scripts ws_apachestats al directorio donde Cacti almacena los scripts, que está situado en la ruta /usr/share/cacti/site/scripts/. Con el script copiado en la carpeta correspondiente, activar los permisos de ejecución del script en caso de no tenerlos activos.
Con la última operación, todos los requisitos se han cumplido, solo queda crear diversas gráficas para un servidor Apache.
Para crear gráficas, debemos escoger el host donde se encuentra el servidor Apache instalado y generar las gráficas para Apache utilizando las plantilla que se ha importado anteriormente.
Seleccionamos la máquina disponible, apartado Management->Devices, donde aparece, los dispositivos que están dado de alta, aparece la máquina donde está instalado Cacti, pulsamos en el dispositivo.



La información se muestra en varios apartados, buscar el apartado de gráficos asociados (Associated Graph Templates), en la opción Add Graph Template muestra una lista de las gráficas disponibles de las plantillas que contiene Cacti.
En la lista aparecen las gráficas disponibles para apachestats, las gráficas se identifican como Web server, escoger las gráficas y pulsar en el botón Add, aparecerán en la lista de las gráficas.
Estas gráficas todavía no muestran datos, deben crearse para el host, en la parte superior aparece la opción para crear las gráficas para el host, Create Graphs for this Host. Pulsando en la opción y tras marcar las graficas seleccionadas, pulsamos el botón de Create para crear las gráficas. En la siguiente ventana podemos escoger los colores que se mostrarán en las gráficas.
Las gráficas no mostrarán los datos hasta pasado un tiempo que pueda recopilar información, para ver las gráficas pulsar en la pestaña graphs.
Para generar más gráficas, se ha visto anteriormente que dentro del host hay un apartado de plantillas de gráficas asociadas (Associated Graph Templates) donde se despliega una lista de plantillas. En este caso solo se tendría que añadir la plantilla correspondiente y después crear la gráfica para este host, es el mismo proceso realizado anteriormente.
Para generar gráficas de otros servicios que no están disponibles en la lista de plantillas, puede buscarse la plantilla por internet. Hay varios sitios de internet donde hay disponibles un conjunto plantillas disponibles.
Un listado de plantillas y scripts para Cacti se puede encontrar en la siguiente página.

http://www.debianhelp.co.uk/cactitemplates.htm
http://forums.cacti.net/forum-12.html

El proceso de instalación de plantillas es el mismo.
–Importar la plantilla desde el panel de configuración de Cacti.
–Copiar el scripts php que acompaña en el directorio de scripts de cacti.
–Seleccionar la plantillas dentro del dispositivo
–Crear las gráficas, esperar un tiempo y comprobar si la gráfica muestra datos.
Las gráficas generadas son del equipo donde se encuentra cacti, pero también se pueden generar de otras máquinas remotas u otro tipo de dispositivos, como router o impresoras en red, como requisito para generar gráficas es que necesitan que soporten SNMP.

Para comprobar que tiene soporte para SNMP en un router, hay que entrar en el panel de configuración del router y buscar el soporte. Si tienen soporte, significa que tiene un agente SNMP instalado en el dispositivo, solo es necesario configurarlo para conectarlo a un gestor y obtener información sobre diversos parámetros y con esa información generar gráficas con Cacti.

Muchos de los router actuales proporcionan soporte para snmp, en algunos caso también para otros protocolos de gestión, dependiendo del router incluso pueden soportar tanto gestor como cliente de snmp.
Como ejemplo de cómo mostrar gráficas de un dispositivo remoto, se crearán varias gráficas de varios parámetros (CPU, memoria RAM y Red) de un equipo remoto (ordenador) utilizando snmp.
Lo primero es instalar snmp, en la máquina que tendrá el rol de gestor, será donde está instalado Cacti, y en la máquina que tendrá el rol de agente.
Para instalar el gestor será necesario instalar varios paquetes, en el servidor se necesitan los paquetes snmpd que instalar el gestor y para el agente el paquete será snmp.

apt-get install snmpd snmp

Editar el fichero de configuración en /etc/snmp/snmpd.conf, con unas pequeñas modificaciones adaptándolo a nuestras necesidades.
El fichero snmpd.conf incluye una configuración por defecto divida en varios partes, con una serie de comentarios bastante aclaratorios, en este caso se va a realizar unas pequeñas modificaciones del fichero para que funcione, las modificaciones a realizar.
–Comentar la línea AgentAddress udp:127.0.0.1:161.
–Comentar la línea rocommunity public default -V systemonly
–Añadir una línea en la sección Access control, rocomunity public 192.168.3.0/24, cambiar la dirección IP por la que corresponda para vuestra red.
–Dentro de la sección Active Monitoring descomentar la línea, trap2sink localhost public, esto especifica que la versión SNMP será 2c.
Se guarda el fichero con las modificaciones, se reinicia el servicio de smnp.

/etc/init.d/snmpd restart.

Verificar que todo funciona correctamente, utilizando el comando snmpwalk.

snmp-walk –v 2c –c comunidad direcciónIP

Si la máquina configurada con el gestor y agente tiene la dirección 192.168.3.10, entonces el comando será.

snmp-walk –v 2c –c public 192.168.3.10

Si todo funciona correctamente aparecerá información sobre la máquina por pantalla. Teniendo un gestor y cliente snmp en la máquina Debian funcionando y recopilando información.

Otra forma de realizar la configuración de snmpd es mediante el comando snmpconf que mediante una serie de preguntas ayuda en la creación del fichero de configuración, este comando se incluye en paquete snmp.
Para el siguiente escenario se va a configurar una máquina remota donde se instalará un agente snmp y la máquina con Debian donde está instalado el gestor de snmp.
Configurado el gestor en el servidor, queda instalar y configurar el agente en la máquina remota. Esta máquina tiene instalada una distribución de Linux (Fedora) y se encuentra en la misma red que el servidor, con la dirección IP 192.168.3.15.
Instalar el agente de snmp, está incluido en el paquete net-snmp.

yum install net-snmp

Para poder recoger información del equipo el servicio de snmp debe estar arrancado, en Fedora se debe ejecutar el siguiente comando.

service snmpd start

Ahora el servicio está ejecutándose y a la espera de peticiones de información por parte del gestor.

Instalado snmp en las dos máquinas queda el proceso de configuración.
En el proceso de instalación de Cacti en el servidor (Debian) se instalaron los paquetes de snmp, en este servidor es donde se configurará el gestor de snmp que se encargará de recoger información de la máquina remota.

En la máquina (Debian) donde va actuar como gestor de snmp, los ficheros de configuración de snmp se encuentran el directorio /etc/snmp/ donde existen tres ficheros:
–snmp.conf: este fichero de configuración contiene una serie de comentarios muy descriptivos, es utilizado para configurar el cliente de snmp, compuesto por el agente de snmp.
–snmpd.conf: fichero de configuración para el gestor de snmp, nos permite escoger con qué opciones arrancará el servicio de snmp (snmpd).
–Snmptrapd.conf: fichero de configuración para definir los trap de un agente -las trap notificaciones enviadas por un agente cuando surgen ciertos eventos-.

El servicio de snmp utiliza el puerto 161, este puerto debe estar abierto en la red para que el gestor y agente puedan comunicarse, también el servicio snmp (snmpd) debe estar en ejecución, con lo que es recomendable que el servicio se inicie de forma automática cuando arranque la máquina. En Debian con la instalación de los paquetes de snmp se configura para se inicie en el arranque del sistema, en Fedora se debe indicar con el comando systemctl enable snmpd.service.
Hay que configurar el gestor de snmp mediante el fichero snmpd, este fichero contiene muchos comentarios muy explicativos porque es bastante grande y su configuración puede resultar algo compleja.
Para el escenario donde se va a ejecutar, se va a crear un fichero nuevo snmpd.conf muy simple, con unas pocas directivas de configuración necesarias para poder monitorizar mediante snmp la máquina remota.
Lo primero es hacer una copia del fichero original snmpd.

mv snmpd.conf snmpd.example.conf

Realiza una copia del fichero original, con un nuevo nombre.
Crear un nuevo fichero nuevo snmpd.conf, utilizando nuestro editor favorito, en este fichero que en principio está en blanco, escribir las siguientes directivas de configuración.

com2sec local 127.0.0.1 public
com2sec redlocal 192.168.3.0/24 public
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local
group MyROGroup v1 redlocal
group MyROGroup v2c redlocal
group MyROGroup usm redlocal
view all included .1 80
access MyROGroup “” any noauth exact all none none
access MyRWGroup “” any noauth exact all all none
syslocation Linux (Debian), Debian.servidor
syscontact pepe <pepe@debian.servidor>

Aunque anteriormente se ha configurado el gestor en la máquina Debian realizando modificaciones el fichero original de snmpd. En este caso, se ha creado un fichero nuevo snmpd tanto en la máquina Debian (gestor) como en la máquina con Fedora(agente) para ver más opciones que pueden incluir el fichero snmpd.
Cada una de estas líneas define lo siguiente:
–com2sec local locahost public.
–com2sec relocal 192.168.3.0/24 public.
Define dos listas de control (ACL), que teniendo en cuenta la configuración de la red, define la especificaciones de la red que tendrá acceso el servicio snmpd, dirección o rango de IP (192.168.3.9/24) el nombre del ACL (localnet) y define una comunidad (public) que identifica el ACL. La otra ACL (local) es definida la el servidor local o localhost.

group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local
group MyROGroup v1 redlocal
group MyROGroup v2c redlocal

group MyROGroup usm redlocal

A cada ACL definida anteriormente se le asigna un grupo que indica el tipo de acceso, MyROGroup que es acceso de solo lectura y MyRWGroup que acceso de lectura/escritura. A continuación se especifica la versión del protocolo de snmp (v2c) y por útlimo, en nombre de la lista ACL.

view all included .1 80

Especifica la configuración para el MIB, donde se almacena la información obtenida, indica las ramas permitidas que el servicio snmpd puede ver.

access MyROGroup "" any noauth exact all none none

access MyRWGroup "" any noauth exact all all none

Especifica la política de acceso para cada grupo definido.

syslocation Linux (Debian), Debian.servidor

syscontact pepe <pepe@debian.servidor>

Especifica información del dispositivo y no influyen en la configuración, syslocation permite insertar información que describe al dispositivo y syscontact proporciona información de contacto.

Se ha creado el fichero de configuración para el gestor de snmp en la máquina Debian, ahora se configura el agente en la máquina Fedora. En este caso, solo existe un fichero de configuración snmpd.conf que será utilizado por el agente, el paquete de snmp instalado proporciona un fichero snmpd.conf con una configuración por defecto y con múltiples comentarios.

También se puede realizar el proceso anterior, crear una copia del fichero snmpd.conf original, crear una nuevo e insertar la misma configuración que ha sido descrita anteriormente.

Para comprobar que funciona correctamente, utilizar la herramienta snmpwalk que permite leer información de un agente snmp.

snmpwalk –v versionProtocoloSNMP direccionIP –c nombrecomunidad

Desde la máquina donde está el gestor instalado, especificamos.

snmpwalk –v 2c 192.168.3.15 –c public

Si muestra información del agente, todo está correcto, y en caso contrario algo ha fallado porque no existe comunicación entre el gestor y el cliente.

El escenario descrito es muy simple y la configuración utilizada tiene muy pocas directivas, como es de imaginar hay muchas opciones que se pueden incluir en fichero de configuración. Este ejemplo práctico es una pequeña muestra de los que puede hacer con snmp.

Ya tenemos configurado snmp y existe comunicación entre el gestor y el cliente, el siguiente paso es generar una serie de gráficas con Cacti para ver diversos parámetros de la máquina remota.

Otra forma de realizar pruebas con snmp, en vez de utilizar la herramienta snmpwalk, es mediante el paquete scli que proporciona una consola que permitirá obtener información de los agentes snmp.

Para instalarlo.

apt-get install scli

Para ejecutarlo.

scli ip_agente_snmp

Muestra la consola de scli con información del agente. Escribiendo el comando monitor veremos información del agente.

Para generar gráficas de la máquina remota en Cacti se debe generar un nuevo dispositivo (Device). Accedemos a Cacti con las credenciales correspondientes y en la pestaña Console, pulsamos en apartado Devices, sección Management, donde se muestra los dispositivos incluidos en Cacti. Para añadir un nuevo dispositivo, pulsar en Add que se encuentra en la parte superior.

En la siguiente ventana se podrá crear un dispositivo, presentando múltiples campos para rellenar. En este caso los campos a rellenar son:

- Description: nombre para el nuevo dispositivo, es el nombre que identificará al dispositivo en Cacti.
- Hostname: nombre del equipo en la red o dirección IP del dispositivo.
- Host Template: muestra una lista con diferentes tipos dispositivos, escoger el tipo ucd/net SNMP Host para un dispositivo gestionado por snmp.
- Number of Collection Threads: número de hilos concurrentes para usar con el poller, dejar por defecto (default).
- Disable Host: si está activo el dispositivo será desconectado para ser chequeado por Cacti.
- Downed Device Detection: Cacti tiene varios métodos para detectar los dispositivos, dependiendo del método escogido aparecerán diferentes opciones. En este caso, escoger Ping and SNMP Uptime, las opciones que aparecerán son:
    - Ping Method: Como realizar un ping, hay disponibles varios métodos; ICMP, UDP y TCP, estos dos últimos requieren especificar el puerto que se utiliza.
    - Ping Timeout Value: define el tiempo que transcurrido se considera que el host no está disponible.
    - Ping Retry Count: Número de reintentos que realiza un ping después de un fallo inicial.

Rellenar los campos con los datos del dispositivo y escoger la configuración adecuada para nuestra red.
En el siguiente apartado se debe especificar la versión del protocolo de SNMP, hay bastantes diferencias entre la versión 1 y 2, con la versión 3. En la configuración descrita anteriormente se ha utilizado la versión 2, con lo que se explicarán las opciones para la versión 2 (SNMP versión).
–SNMP Community: especificado en la configuración de snmpd.conf, donde se crean las listas de control, identifica un conjunto de gestores y clientes, está asociado a un ACL. Por defecto, el campo se rellena con public.
–SNMP Port: El protocolo snmp utiliza por defecto el puerto 161 para su funcionamiento. Si no se ha cambiado en la configuración el número del puerto, dejar el puerto por defecto en ese campo.
–SNMP Timeout: Define el tiempo, en milisegundos, que Cacti deberá esperar la respuesta, pasado ese tiempo se considera que se ha producido un error.
–Maximun OID's Per Get Request: número de OID, que representa una variable de un dispositivo que es leída por snmp, máximo que pueden ser obtenido por cada petición de snmp.

Con los datos de configuración del dispositivo introducidos, para crear el nuevo dispositivo se pulsa en el botón Add, creando un nuevo dispositivo y aparecerán dos nuevos apartados:
Associated Graph Template: apartado donde se añaden diversas gráficas para el dispositivo. Por defecto Cacti incluye varias gráficas en esta sección en función de la plantilla del dispositivo, para añadir más gráficas en la opción Add Graph Template muestra una lista con todas las gráficas disponibles. Hay disponibles por Internet múltiples plantillas de gráficas que pueden ser añadidas a Cacti .

Dependiendo del tipo de Host Template asignado al dispositivo, solo determinadas gráficas de la lista funcionarán de manera correcta, aunque en la lista se muestren todas las plantillas. Por ejemplo, si plantilla asignada es Cisco Router, las gráficas para ese tipo de plantillas aparecen con nombre de Cisco.

- Associated Data Queries: permite obtener diversos datos en función de las consultas que se realizan y con esos datos generar gráficas para monitorizar diversos parámetros. Por defecto, un dispositivo snmp genera dos Data Query.
    - SNMP - Interface Statistics: realiza consulta sobre datos estadísticos de las interfaces de red del dispositivo.
    - ucd/net - Get Monitored Partitions: permite monitorizar las particiones de disco duro del dispositivo.

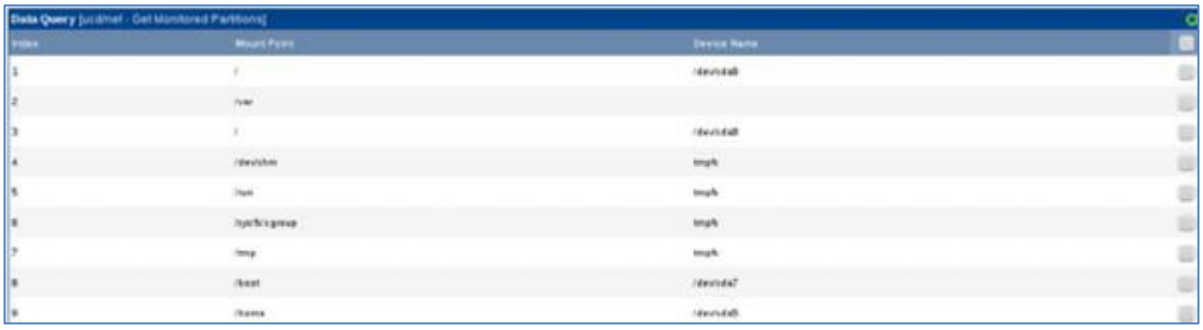
Igual que en las plantillas se pueden añadir nuevas Data Query al dispositivo en la opción Add Data Query.

Las gráficas no se han creado, en la columna Status de las plantillas de las gráficas indica que todavía no muestran datos. Para generar las gráficas, pulsar en Create Graphs for this Host, mostrando una nueva ventana donde seleccionar las gráficas.

La pantalla esta divida en dos zonas, la primera corresponde a las plantillas de gráficas seleccionadas (Graph Template), mostrando las tres plantillas escogidas, marcando cada plantilla para que pueda generar la gráfica.

La segunda zona muestra las gráficas correspondiente a los data query, el primero corresponde a la estadísticas de las interfaces de red por snmp (SNMP Interface Statistics), donde se muestran las interfaces de red disponibles en el dispositivo , pudiendo escoger que tipo de interfaz de red se va generar una gráfica. Dentro de la opción Selected a graph type hay disponibles diversos formatos para mostrar los datos de la gráfica.

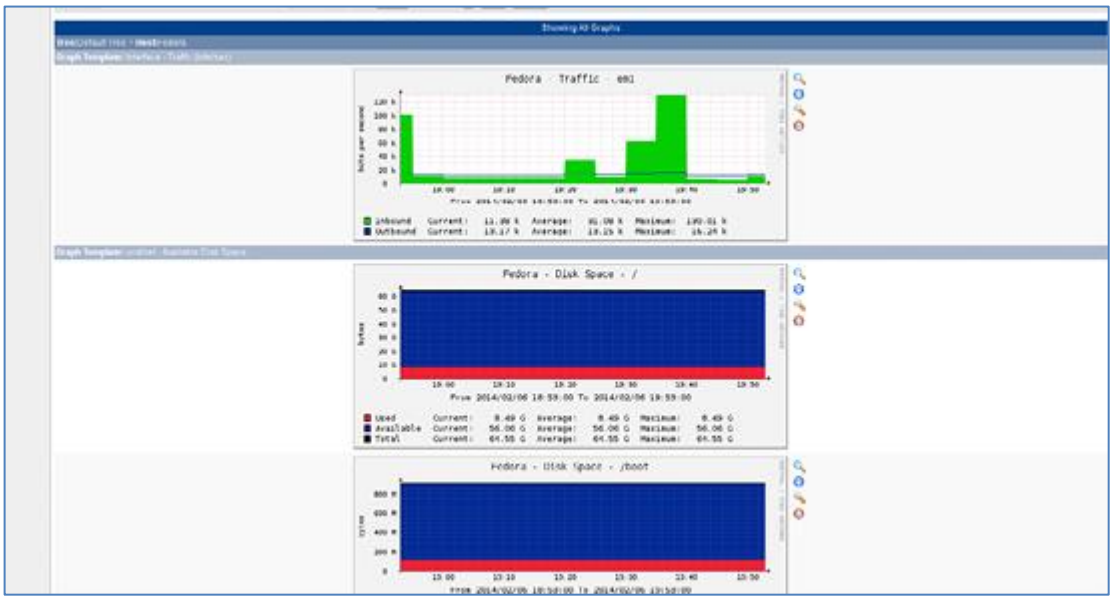
La otra Data Query mostrada, corresponde a las particiones del dispositivo (ucd/net - Get Monitored Partitions), donde muestra todas las particiones del dispositivos y escoger aquellas que no interesa monitorizar.



Seleccionar las gráficas que se desean generar y pulsar el botón Create para generarlas.

Con esto se han generado una serie de gráficas para una máquina remota utilizando snmp para obtener los datos.

Las gráficas están generadas pero no mostrarán información, Cacti recopila información cada cierto intervalo de tiempo, 5 minutos por defecto, por lo que se deberá esperar un tiempo para que empiece a mostrar datos en las gráficas.
Pasados unos minutos, las gráficas mostrarán los datos recopilados, para ver esos datos se debe pulsar en la pestaña de Cacti graphs (parte superior de la pantalla). En la ventana de las gráficas, hay una columna (Default Tree) donde aparecerán todos los dispositivos que Cacti genera gráficas. Es posible que la máquina remota no aparezca en la columna, solo aparecerá la primera máquina que se añadió que es donde está instalado Cacti.
Para añadir la máquina remota a la columna y poder visualizar las gráficas de una forma cómoda. Primero nos situamos en el apartado Devices donde aparecen todos los dispositivos y marcamos la máquina remota, escogemos una acción para esa máquina (Choose an action), seleccionar Place on a Tree (Default Tree) y pulsar en el botón de Go.
Añadir un dispositivo al Default Tree:
En la siguiente ventana dejamos las opciones por defecto y confirmamos pulsando en el botón de Continue.
Ahora tenemos en el Default Tree una nueva máquina, pulsamos en la pestaña graphs y en la columna aparecerá una nueva entrada. Pulsando en cada máquina se visualizan las gráficas generadas de cada dispositivo.
En la parte superior de la ventana se incluyen varios filtros (Preset) que permiten ver los datos generados en las gráficas en ciertos intervalos de tiempo, también se puede especificar una rango de fechas o realizar búsquedas.



En la parte derecha de cada gráfica aparece una serie de iconos que permiten realizar las siguientes tareas, de arriba abajo:
–Realiza un zoom en la gráfica, aumentando una zona de la gráfica para ver con más detalle, solo se tendrá que seleccionar, dibujando con el ratón un rectángulo, el área de la gráfica donde realizar el zoom. Las gráficas se dividen en múltiplos de 5 minutos.
–Exportación en formato CSV, descarga en formato CSV (valores separados por coma) los datos de la gráfica. Este formato es muy utilizado y es muy útil para generar informes.
–Permite ver las propiedades, como se ha generado la gráfica y el comando con todas las opciones que se han utilizado.
–Nos sitúa al comienzo de la página, visualizando la primera gráfica.
También si pulsamos en cualquier gráfica, mostrará la misma gráfica en diversos intervalos de tiempo.
–Diaria (Daily): con intervalo de tiempo de 5 minutos.
–Semanal (Weekly): con un intervalo de 30 minutos.
–Mensual (Monthly): con un intervalo de 2 horas.
–Anual (Year): con un intervalo de 1 día.

Cuando pulsamos en la pestaña graphs, aparecen en la parte izquierda de la página cuatro pestañas que permitirán realizar diversas tareas relacionadas con las gráficas.
Estas pestañas son las siguientes.

- Settings
  Permite configurar diversos aspectos de las gráficas por defecto, como pueden ser: el tamaño de las gráficas, el intervalo de tiempo, el modo de vista, etc.
- Tree Mode
  Es la vista por defecto que aparece cuando pulsamos en la pestaña graphs, se ha explicado anteriormente.
- List mode
  Permite visualizar un conjunto de gráficas, muestra una lista con todas las gráficas de todos los dispositivos, marcamos las gráficas que deseamos visualizar y pulsamos al botón View. Mostrará en la misma página todas las gráficas seleccionadas.
- Preview Mode
  Visualiza todas las gráficas en unas páginas, a diferencia del Tree Mode, este modo visualiza las gráficas en varias columnas, facilitando la visualización en el caso de tener muchas gráficas. En la parte superior hay disponibles varias opciones de filtros de visualización.

Con esto finaliza el pequeño tutorial de Cacti, este programa solo tiene la funcionalidad de generación de gráficas y siendo una herramienta cuya curva de aprendizaje no es alta. Aunque algunos aspectos, como la configuración de snmp, pueden ser algo complejos.
Hay disponibles por internet muchas plantillas que permitirán generar gráficas de múltiples dispositivos de manera sencilla, estas plantillas son relativamente fáciles de instalar e utilizar.
Cacti es muy útil en conjunción otras herramientas de gestión, por ejemplo **Nagios**, algunas de las alternativas a esta herramienta son; Munin o MRTG.

2. Gestión de redes de comunicaciones

2.1. Aspectos funcionales de la gestión de la red

El componente funcional se encarga de definir un conjunto de competencia. La organización ISO agrupa estas competencias en cinco grandes aéreas funcionales.
–Gestión de configuraciones: mantener información sobre el diseño de la red.
–Gestión de fallos: detectar, aislar y solucionar errores.
–Gestión de prestaciones: disponibilidad y uso.
–Gestión de contabilidad: recursos usados y facturación.
–Gestión de seguridad: registro de eventos y protección.
Los usuarios de la red tienen sus propias expectativas. La calidad de servicio vendrá determinada por el cumplimiento de estas y las áreas funcionales ayudaran al cumplimiento.

Gestión de configuración
Es el proceso de obtención de datos de la red y la utilización de los mismos para incorporar, mantener y retirar los diferentes componentes o recursos que integran la red. Consiste en la realización de tres tareas fundamentales:

- ⇨ Recolección de datos sobre el estado de la red. Para ello generalmente se emplean dos tipos de herramientas que funcionan de forma automática:
  - o Herramientas de autodescubrimiento (auto-discovery): mediante un sondeo realizado de forma periódica por la red, averigua qué elementos están activos y cuáles son sus características.
  - o Herramientas de autotopología (auto-mapping): descubre cómo están interconectados los distintos elementos de la red, mostrando la información obtenida mediante un mapa topológico.
- ⇨ Cambio en la configuración de los recursos.
- ⇨ Almacenamiento de los datos de configuración: los datos obtenidos han de ser almacenados para obtener el inventario de red.

En la gestión de configuraciones, es donde se crea un SLA con el cliente, definido anteriormente en el apartado anterior. Este documento estaría compuesto de las siguientes partes.
–Identificación de las partes contractuales.
–Identificación del trabajo a realizar.
–Objetivos de niveles de servicio.
–Niveles de servicio proporcionados.
–Multas por incumplimiento.
–Fecha de caducidad.
–Cláusulas de renegociación.
–Prestaciones actuales proporcionadas.

La gestión de configuración se realizan una serie de tareas que definen una serie de funciones que se dividen en dos categorías: funciones de monitorización o funciones de control, cada función engloba una serie de tareas.

- ⇨ Funciones de control:
  Definición de la información de configuración.
  Establecimiento y modificación de valores de atributos:
  Establecimiento y modificación de relaciones.
  Operaciones de inicialización y apagado de la red.
  Distribución de software.
- ⇨ Funciones de monitorización:
  Examen de valores y relaciones.
  Informes sobre el estado de la configuración.

La información de configuración describe el funcionamiento y estado de los recursos de la red, con esta información el administrador tendrá una especificación del recurso y conocerá todas sus características, que están definidas por una serie de atributos.
Esta información es muy importante y debe ser almacenada para no sufrir pérdidas, el almacenamiento puede utilizar las siguientes estructuras:
–Lista de datos: donde almacenar un conjunto de valores.
–Una base de datos orientada a objetos: cada elemento es definido por un objeto que está constituido por un conjunto de atributos para definen las características del objeto y una serie de comportamiento asociados al objeto que indican las acciones que puede realizar.
–Base de datos relacional: la información se estructura en una serie de tablas donde cada fila representa a un elemento y está definido por una serie de campos, de manera opcional se pueden definir relaciones entre las tablas.
–Esta información esta accesible por el gestor y disponible para el administrador para que pueda realizar diferentes tareas de administración en la red. Entre las tareas que puede realizar.
–Especificar nuevos atributos a un agente o modificar atributos de un agente.
–Definir nuevos tipos de datos o tipos de objetos que podrán ser utilizados por los elementos de la red.
–Acceso remoto a los agentes a través del gestor, el administrador podrá acceder al agente para realizar tareas administrativas.
Todas las modificaciones realizadas en la configuración de los agentes serán modificadas en la base de datos correspondiente, pudiendo modificar su comportamiento y esto puede producir un cambio en el manejo de un recurso.
El administrador puede insertar valores por defecto predefinidos (estados por defecto, características operativas, etc.) en un sistema completo, un nodo concreto o un nivel determinado.
Una relación describe una asociación, conexión o condición que existe entre un recurso o componente de la red. La gestión de configuración debe permitir la creación, modificación o eliminación de estas relaciones sin afectar a la red.
Otra operación que realiza la gestión de configuración es incluir un mecanismo que permita al administrador inicializar o apagar la red, parte de una red o solo un recurso de la red. La inicialización incluye verificar que todos los atributos y relaciones se han establecido adecuadamente, notificando al administrador que algún recurso, atributo o relación necesita ser establecido y validar los comandos de inicialización del administrador. El apagado de la red, requiere disponer de mecanismos para solicitar determinadas estadísticas o información de estado antes de que finalice la operación de apagado.
La gestión de configuración debe permitir distribuir software a los sistemas finales (servidores, terminales, etc.) y sistemas intermedios (bridges, routers, etc.). Para ello se debe disponer de facilidades que permitan: solicitudes de carga de software, transmisión de las versiones de software especificadas y actualización de la configuración de los sistemas.
Además de ejecutables, también se pueden distribuir tablas y otros datos que controlen el comportamiento de un nodo, como las tablas de encaminamiento, necesitando un mecanismo de control de versiones de software que permita cargar diferentes versiones de software o tablas de encaminamiento en base a determinadas condiciones, tal como tasas de error.

Gestión de fallos

Es el proceso de detección de los errores y buscar la solución más adecuada, también se deben identificar las causas del fallo para corregirlos. El objetivo de la gestión fallos es mantener un nivel servicio optimo, para conseguir este objetivo se realiza dos tipos de gestiones.
–Gestión proactiva: evitar fallos antes de que sucedan, realizando una serie de pruebas y analizando la información recibida, buscando el posible origen de fallos. Para detectar estos fallos, se realizan una serie de mecanismos como: creación de valores umbrales en determinados parámetros, cuando el valor umbral es sobrepasado automáticamente se envía una notificación al personal encargado.
–Gestión reactiva: El fallo se ha producido y el objetivo es resolverlo lo antes posible para evitar consecuencias mayores en la red. La rapidez en la resolución se consigue utilizando diversos mecanismos para optimizar el proceso de reparación

Cuando un fallo es descubierto o una posible anomalía en el funcionamiento, es generada una incidencia que almacena toda la información disponible sobre el fallo o anomalía, para ayudar en el proceso de resolución. Toda incidencia pasa por una serie de estados denominados ciclo de vida, estos estados son:

–Detección del fallo: una serie de alarmas son activadas cuando se produce un error, estas alarmas pueden ser activadas por un usuario, abriendo una incidencia, o generadas por herramientas de monitorización que envían una notificación al personal encargado, cuando se activa una alarma.

–Aislamiento del fallo: cuando se detecta un fallo, aislar el componente donde ha surgido el error para que no se propague por el resto de la red, incluso puede ser necesario reconfigurar la red. Hay que informar a los usuarios del fallo para evitar molestias.

–Diagnosis del fallo: realizar un estudio del fallo para encontrar las posibles causas y encontrar la solución adecuada:

–Elaboración de una hipótesis. Con los datos y el estudio realizado, que posibles soluciones tenemos.

–Verificación de la hipótesis. Probar las posibles soluciones y comprobar cuál de ellas tiene la mejor respuesta.

–Resolución del fallo. Escogida la solución más óptima, que ha sido probada para comprobar que funciona. Conviene documentar la solución encontrada para posibles usos futuros.

Gestión de prestaciones

Realiza un proceso de medición del rendimiento de la red para garantizar unos niveles adecuados de rendimientos. Las mediciones se realizan a través de una serie de indicadores que comprueban los niveles de rendimientos acordados.

Los indicadores se dividen en dos categorías:

- ⇨ Medidas orientadas a servicios: permiten mantener los niveles de determinados servicios para conseguir la satisfacción de los clientes. Tenemos varios indicadores.
  - Disponibilidad. Porcentaje de tiempo de una red, dispositivo o aplicación está en funcionamiento y disponible para el usuario.
  - Tiempo de respuesta. Cuánto tarda en aparecer la respuesta en el terminal del usuario cuando éste realiza una acción.
  - Fiabilidad. Porcentaje de tiempo en el que no han ocurrido errores en la transmisión y entrega de información.
- ⇨ Medidas orientadas a eficiencia: medidas que permiten mantener los niveles de satisfacción anteriores al mínimo coste posible. Tenemos varios indicadores.
  - Throughtput. La tasa a la que ocurren los eventos a nivel de aplicación.
  - Utilización. Porcentaje de la capacidad teórica de un recurso que se está utilizando, también denominado nivel de uso.

La disponibilidad depende de la aplicación, puede ser un factor muy importante, por ejemplo en las aplicaciones de bases de datos requieren una alta disponibilidad para tener accesos a los datos que se almacenan en ella.

En redes, la disponibilidad depende mucho de la fiabilidad de sus componentes, si los componentes son muy fiables, prácticamente no fallan y la red siempre estará disponible (alta disponibilidad). Para medir la fiabilidad de un componente se calcula la probabilidad de que realice la función esperada durante un tiempo especificado bajo determinadas condiciones sin producirse errores.

La fiabilidad se expresa por los fabricantes de componentes por su MTBF, que expresa el tiempo transcurrido entre dos fallos.

Para aumentar la disponibilidad podemos realizar ciertas tareas:

–Controlar las configuraciones, una mala configuración puede afectar a un componente.

–Redundancia, algunos componente pueden estar duplicados y en caso de fallo de uno, no afecte al sistema.

–Analizar los datos obtenidos para encontrar problemas de rendimiento en un componente

–Establecer unos límites de rendimiento.

Gestión de contabilidad

Mide el grado de utilización de los recursos y la facturación. Las principales tareas que se realizan.

–Identificación de Componentes de Coste.

–Establecimiento de políticas de tarificación.
–Definición de procedimientos para tarificación.
–Gestión de facturas
–Integración con la contabilidad empresarial.
El objetivo que se pretende alcanzar con una gestión de contabilidad es distribuir la utilización de los recursos entre los distintos usuarios. El uso de determinados recursos puede conllevar un coste alto, el uso equitativo de este recurso hace que todos los usuario tengan acceso a él , la relación coste-utilización será optima. También detectar el abuso provocado por un uso excesivo de un recurso por parte de un usuario, cuando el uso de un recurso sobreexplotado por un usuario, el resto de usuario tendrán un acceso deficiente o incluso no tendrán acceso.
Para cumplir los objetivos planteados se utilizan herramientas especializadas que monitorizan la utilización de los recursos. Estas herramientas obtienen una serie de datos y proporcionan una serie de estadísticas, con esos datos se generan una serie de gráficas que facilitan a los administradores el trabajo de monitorización, visualizando de una manera rápida el uso excesivo de un recurso. Se pueden programar la graficas, cuando llegues a un determinado nivel que activen un alarma.

Gestión de seguridad
Implementan una serie de funciones que proporcionan protección continuada de la red y sus componentes, la seguridad deberá tener en cuenta los siguientes factores:
–Acceso a las redes.
–Acceso a los sistemas.
–Acceso a la información en tránsito
Funciones que se deben realizar en la gestión de seguridad:
–Definición de análisis de riesgos y política de seguridad.
–Implantación de servicios de seguridad e infraestructura asociada.
–Definición de alarmas, registros e informes de seguridad.
Para realizar una buena gestión de seguridad se debe entender lo que implica tener una buena seguridad.

La seguridad implica una serie de aspectos:
–Privacidad: La información debe estar accesible para lectura sólo a persones autorizadas. Los accesos incluyen: leer visualizar, imprimir, o incluso revelar la propia existencia del trabajo.
–Integridad: los recursos deben ser modificables sólo por usuarios autorizados. Las modificaciones incluyen: escribir, modificar, eliminar y crear.
–Disponibilidad: los recursos deben estar disponibles solo a los usuario autorizados.
En la gestión de seguridad debemos realizar una serie de actuaciones para mantener segura nuestra red, estas actividades se pueden resumir:
–Defender: utilizar diferentes mecanismos que dificulten los ataques a la red. Reforzar la defensas en caso de múltiples ataques.
–Asegurar: realizar diferentes tareas que permitan disminuir las consecuencias de un ataque.
–Denunciar: identificar las causas y causantes cuando se produce un ataque.
Para la realización de una correcta gestión de seguridad, conviene tener en cuenta dos aspectos.

- ⇨ Activos: diferentes elementos que posee o usa una organización y pueden ser el destino de un posible ataque, podemos incluir como activos de una organización:
  - Recursos físicos: equipos informáticos, router, etc.
  - Uso de recursos: un ataque puede realizar un uso de indebido de algún recurso de la red, por ejemplo usar la Wifi de la empresa sin autorización.
  - Información almacenada: uno de los activos más importantes en una organización es la información que maneja, un posible robo de información puede ser muy perjudicial.
  - Información en tránsito: la información que es transmitida por la red puede ser objeto de un espionaje mediante herramientas especificas (sniffer).
  - Personal: cualquier tipo de persona que trabaja o está relacionada con una organización.
- ⇨ Imagen y reputación: una bajada de la imagen o reputación puede perjudicar en otros aspectos de una organización.

Una lista de posibles amenazas a una organización nos proporcionará una valiosa información para una buena gestión de seguridad. Podemos dividir las amenazas en dos categorías.

Amenazas físicas	Diferentes formas de fallos provocados por agentes externos como pueden ser: Suministro eléctricos. Fallos hardware. Catástrofes naturales. Incendio. Agua. Personal. Temperatura y humedad.
Amenazas lógicas	Diferentes formas de realizar ataques a diferentes componentes software a través de diferentes técnicas y utilizando software para ese propósito. Una lista de posibles amenazas. Acceso no autorizado. Intrusiones. Virus. Ingeniería social. Errores de software. Errores de usuarios.

Para mantener una buena seguridad debemos realizar diversas tareas que podemos englobar en tres categorías.
–Mantenimiento de la información de seguridad.
–Control de acceso a losa recursos.
–Control del proceso de cifrado.

Mantenimiento de la información de la seguridad

Todo sistema contiene información relativa a su seguridad, estos elementos son varios y se pueden resumir:
–Contraseñas: los usuarios del sistema conviene que tengan una contraseña para acceder al sistema, algunos programa necesitan de una contraseña para acceder.
–Permisos: diferentes componente del sistema tiene unos permisos asignados, como ficheros, programas o recursos
–Información de autenticación: es la información que se genera para autorizar el acceso a un componente del sistema.
–Parámetros de configuración de servicios de seguridad: todo sistema incluye un serie de componente de seguridad, como un cortafuego.
La gestión de seguridad debe registrar la actividad que se genera en la red, para detectar intentos de ataques, o ataques conseguidos. Esto incluye las siguientes funciones:
–Log de eventos.
–Monitorización de registros de seguridad.
–Monitorización de utilización y usuarios de recursos de seguridad.
–Avisos de violaciones de seguridad.
–Recepción de avisos de violaciones de seguridad.
–Mantener y examinar logs de seguridad.
–Mantener backups de los datos referentes a seguridad.
–Mantener perfiles de usuarios y utilizaciones para recursos específicos para permitir la verificación del cumplimiento de las políticas de seguridad definidas.

Control de acceso a los recursos

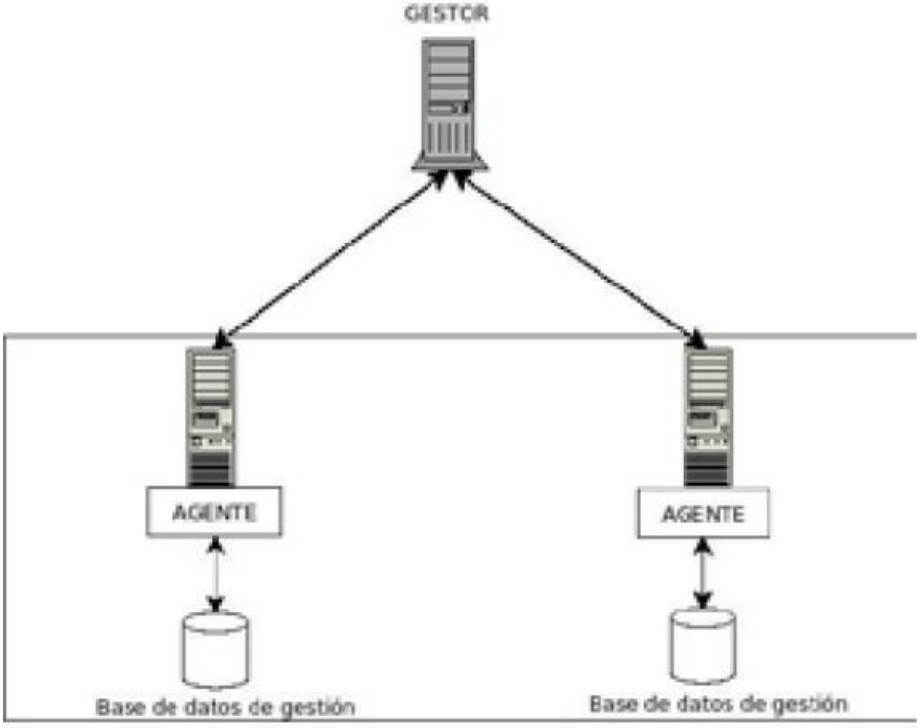
Consiste en la autenticación y autorización de acceso a recursos. Para ello hay que mantener perfiles de usuarios y de utilización para recursos específicos, estableciendo prioridades de acceso.
Definir una política para realizar un control acceso de los recursos de red de forma adecuada, utilizando herramientas para analizar y controlar el uso legítimo de la red.

Control del proceso de cifrado

La información transmitida por la red entre agentes y gestores debe ser cifrado, si se considera necesario, para impedir el acceso a personas no autorizadas. Este cifrado proporciona una capa de seguridad a la información aunque aumenta la complejidad y requiere un procesamiento extra para el cifrado. En esta categoría se deberá escoger el algoritmo de cifrado más adecuado y el mecanismo de distribución de las claves en función de la configuración de la red.

2.2. Protocolo de gestión de red

Un protocolo de gestión proporciona un conjunto de reglas de comunicación entre un gestor y un conjunto de agentes. En un protocolo se definen diversos aspectos de la gestión como:
–Tipos de mensajes y operaciones.
–Seguridad (autenticación, privacidad).
–Manejo de secuencias.
El funcionamiento de un protocolo de gestión es el siguiente. Los agentes localizados en los dispositivos gestionados, son sondeados periódicamente por la entidad gestora



Podemos dividir los protocolos de gestión en dos categorías en función del tipo de red que gestiona
Los protocolos de gestión que son implementados en redes de computadores hay varios, pero aquí nos enfocaremos en dos protocolos:

- ⇨ CMIS/CMIP: protocolo de gestión que se basa en el modelo ISO creado por la organización OSI, es utilizado en ambientes empresariales debido a un diseño robusto.
- ⇨ SNMP: es el estándar para la familia TCP/IP, protocolo de gestión muy utilizado por múltiples herramientas para conocer los componentes de los dispositivos, también es incluido en determinado hardware, entre las herramientas que lo utilizan tenemos.
  - Herramientas de monitorización.
  - Herramientas de generación de mapas de red.
  - Herramientas de inventario.
  - Herramientas de generación de gráficas de red.

Y Para las redes de telecomunicaciones

- ⇨ TMN: protocolo definido por la organización ITU-T como un sistema abierto de una red comunicaciones, también en parte está basado en el modelo ISO.

CMIS/CMIP

Es un protocolo de gestión de red definido en la capa de aplicación del modelo OSI. Permite gestionar equipos de red locales y remotos, tanto en entornos privados y públicos.

Está compuesto de dos elementos:

–CMIS: Servicio de administración de información común, servicio especificado por el organismo ITU que es empleado para la administración de elementos de red. Define una interfaz de servicio que es implementado por el protocolo CMIP.

–CMIP: Protocolo de administración de información común, es el protocolo de gestión de red, proporciona una implementación de los servicios definidos por CMIS, permitiendo la comunicación entre las aplicaciones de gestión y los agentes.

Las características de CMIS/CMIP:

–Utiliza gestores y agentes que se comunican a través de CMIS/CMIP.

–El modelo de datos se basa en objetos, los dispositivos de una red son descritos mediante objetos, utilizando la notación ASN.1, donde existen clases, instancias, herencia, etc.

–Utiliza una base de datos jerárquica, denominada MIB, donde es almacenada la información de los dispositivos gestionados en forma de objetos.

Las características del protocolo CMIP:

- ⇨ Su funcionamiento se basa en un mecanismo de sondeo, un gestor realiza accesos periódicos para obtener información de los agentes que monitoriza.
- ⇨ Confirmación de las peticiones por parte de los clientes.
- ⇨ El agente es el encargado de monitorizar los recursos.
- ⇨ Estructura distribuida.
- ⇨ La comunicación con los agentes está orientada a conexión.
- ⇨ CMIS proporciona una serie de servicios que son transmitidos por CMIP, estos son:
  - M-GET: Un gestor obtiene información de un agente.
  - M-SET: Un gestor modifica información de un agente.
  - M-CREATE: Añade nuevas instancias de objetos gestionados.
  - M-ACTION: Usado por un gestor para invocar un procedimiento predefinido especificado como parte de un objeto de un agente.
  - M-EVENT_REPORT: Permite al agente enviar eventos y alarmas.
  - M-DELETE: Elimina uno o más objetos.
  - M-CANCEL-GET: Finaliza una operación GET larga.

El protocolo CMIP proporciona una serie de ventajas como:

–Los objetos almacenados en el MIB proporcionan información que permiten ser utilizada para realizar diversas tareas.

–Autenticación, cifrado y registro de seguridad.

–Permite enviar datos de cualquier tamaño o complejidad al enviarlos como objetos.

Como desventajas de CMIP:

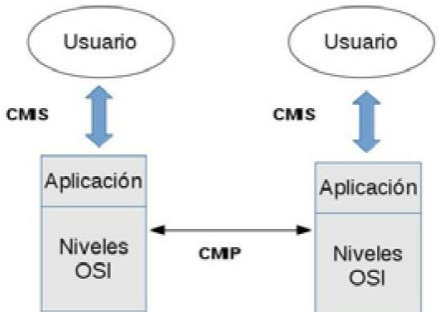
–Consume muchos recursos.

–Especificaciones complejas, por lo que dificulta la programación.

–Implementación costosa, tanto a nivel de hardware como software.

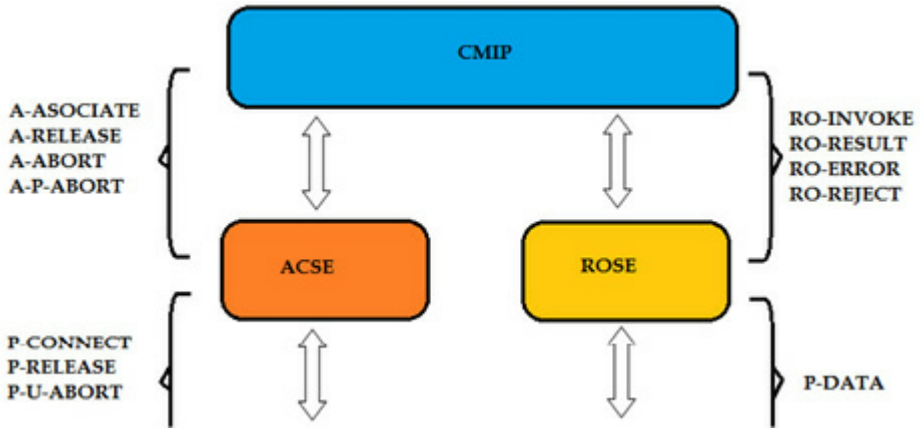
–Variables complejas.

Uso de CMIS/CMIP



El modelo de arquitectura CMIS está compuesto por los siguientes elementos:
–Aplicación de gestión de sistemas (SMAP): software instalado en el dispositivo gestionado que implementa las funciones de gestión para ese sistema. Tiene acceso a los parámetros del sistema y puede gestionar todos los aspectos del sistema y coordinarse con SMAP de otros sistemas.
–Entidad de aplicación de gestión de sistemas (SMAE): Entidad de nivel de aplicación. Se encarga del intercambio de gestión con SMAE de otros nodos, también se comunica con el SMAP. Para el intercambio de información utiliza el protocolo CMIP.
Base de información de gestión (MIB): base de datos donde se almacena información del estado de los dispositivos.
Dentro de CMIP tenemos un conjunto de protocolos de aplicación. Para dar un servicio más general, aparte de la gestión de sistema, CMIP trabaja en asociación con otros protocolos, los cuales son:
–ACSE: Elemento de servicio de control de asociación, es un protocolo que establece y libera asociaciones entre entidades de aplicación. El establecimiento lo puede realizar el agente o el administrador y durante el proceso se intercambian los títulos de la entidad de aplicación para identificarse, junto a los nombres de contexto de aplicación.
–ROSE: Elemento de servicio para operaciones remotas, protocolo encargado de las llamadas a procedimiento remotos, permite la invocación de una operación en un sistema remoto.
Específicos para la gestión de red, tenemos los siguientes protocolos.
–SMASE: implementa funciones básicas de gestión en las aéreas de gestión de fallos, contabilidad, configuración, prestaciones y seguridad. Proporciona servicios al gestor de red y a las aplicaciones de red, por ejemplo da servicio a SMAP.
–CMISE: proporciona funciones básicas de gestión a las 5 áreas funcionales. El SMASE delega en este elemento aquellas funciones que requieren comunicaciones con otros sistemas. Hace uso de los servicios proporcionados por ACSE y ROSE.
El protocolo ACSE proporciona una serie de servicios que son utilizados por el administrador, estos servicios son.
–A-ASSOCIATE: servicio confirmado requerido para iniciar la asociación entre entidades de aplicación.
–A-RELEASE: servicio confirmado implementado para liberar una asociación entre entidades de aplicación sin pérdida de información.
–A-ABORT: servicio no confirmado que causa la liberación anormal de una asociación con una posible pérdida de información.
–A-P-ABORT: servicio iniciado por el proveedor que indica la liberación anormal de la asociación del servicio de presentación con posible pérdida de información.

El protocolo ROSE proporciona una serie de servicio a CSMISE:
–RO-INVOKE: servicio no confirmado usado por un usuario de ROSE, para invocar que una operación sea realizado por un ROSE remoto.
–RO-RESULT: servicio no confirmado que un ROSE invocado usa para contestar a una previa indicación RO-INVOKE: en el caso de que se haya realizado con éxito.
–RO-ERROR: servicio no confirmado que es usado por un usuario de ROSE invocado para contestar a una previa indicación RO-INVOKE, en el caso de que haya fracasado.
–RO-REJECT, servicio no confirmado utilizado por un usuario de ROSE para rechazar una petición.
Los servicios que proporcionan los protocolos ACSE y ROSE, se comunican por CMIP y al servicio de presentación.



El protocolo CMIP proporciona una serie de servicios por medio de CMISE, estos servicios se pueden resumir en tres tipos.

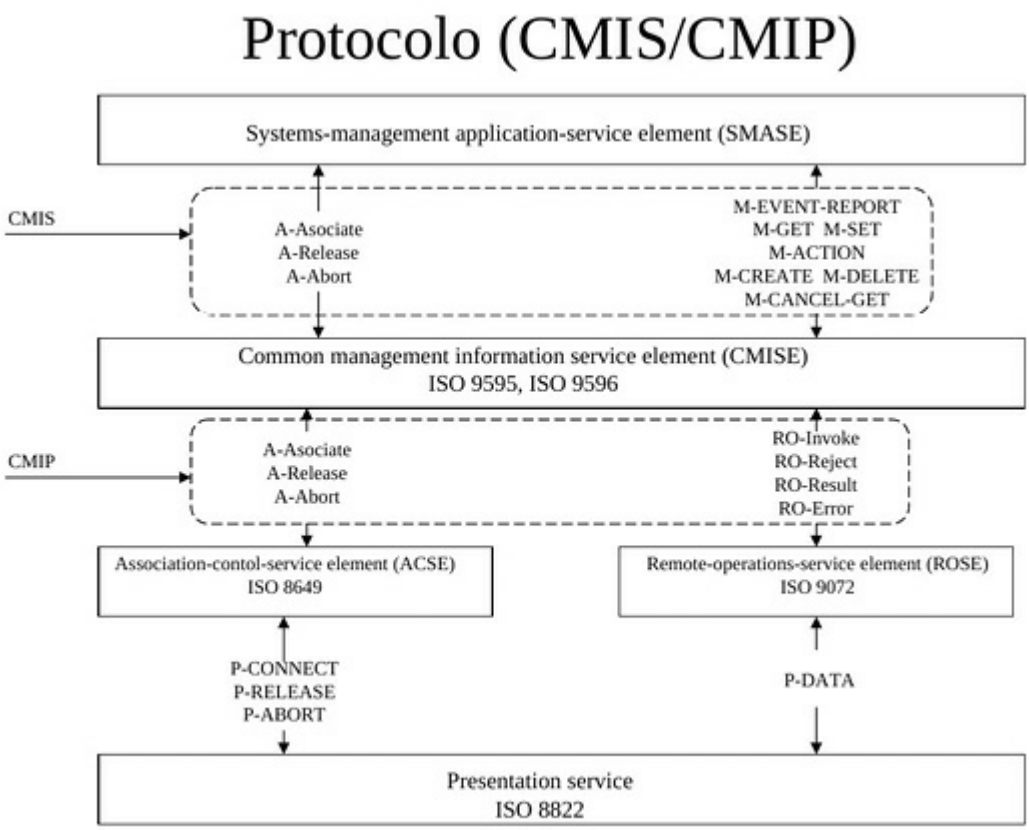
Manejo de datos: proporciona servicios que utiliza el administrador para solicitar y alterar información de los recursos del agente.

Informe de sucesos: servicio que es empleado por el agente para informar al administrador.

Control directo: servicio empleado por el administrador.

El intercambio de información se realiza mediante CMISE puede ser especificado en dos partes. Por una parte, tenemos el acceso de usuario mediante una interfaz mediante CMIS. El protocolo que se utiliza para la transmisión de la información se denomina CMIP, donde se especifica el formato y los procedimientos asociados.

El CMIS proporciona 7 servicios para realizar operaciones de gestión mediante primitivas de servicio. Además los usuarios necesitan establecer asociaciones entre CMISEs para poder realizar operaciones de gestión. Para ello existen 3 primitivas que proporciona el ACSE y que pasan de manera transparente el CMISE.



SNMP

Protocolo Simple de Gestión de Red (Simple Network Management Protocol), es un protocolo para intercambio de información entre dispositivos de una red, y conocer el estado de los dispositivos. SNMP fue publicado inicialmente en 1989 aunque empezó a ser utilizado por aplicaciones a partir de 1990.

SNMP es un protocolo estándar de la familia de TCP/IP, permite a los administradores de red realizar un conjunto de funciones como:

–Supervisar la operación de la red.
–Configurar los equipos.
–Encontrar y resolver fallos.
–Analizar las prestaciones de los equipos.

Para funcionar SNMP consta de tres elementos:

–La base de Información de gestión (MIB).
–La estructura de gestión de la Información (SMI).
–El protocolo de gestión de red simple (SNMP).

Hay varias versiones disponibles SNMP v1 (versión 1), SNMP v2 (versión 2) y SNMP v3 (versión 3). Este protocolo está compuesto por los siguientes elementos.

- ⇨ Administrador
  Situado en el equipo donde gestiona la red, recibirá la información de los dispositivos.
- ⇨ Agentes
  Situados en los dispositivos (nodos) que van a ser gestionados, recogen información del nodo y la envía al administrador.
- ⇨ Sistemas administradores en red (NMS)
  Ejecuta aplicaciones que monitorizan y controlan en los dispositivos gestionados, al menos debe existir un NMS en la red gestionada.

Para los dispositivos que no soportan SNMP se utilizan los agentes proxy, vistos en el apartado de CMIS/CMIP, que son encargados de realizar las conversiones necesarias para realizar una comunicación entre un gestor y un agente sin soporte SNMP.

En el protocolo SNMP se establece una comunicación entre el administrador y los agentes, que es realizada mediante una serie de mensajes que son enviados mediante protocolo UDP, servicio no orientado a conexión, lo que evita mecanismo de control y recuperación. El protocolo SNMP utiliza los puertos UDP, 161 donde realiza las transmisiones normales y 162 se utiliza para los mensajes de tipo Trap o interrupción.

MIB

SNMP define un estándar separado para los datos gestionados por el protocolo. La información del estado de los dispositivos es almacenada en una base de datos denominada Base de Información de Gestión (MIB), que es almacenada de forma jerárquica con una estructura en forma de árbol, esta información es utilizada por SNMP. Los MIB contienen información de los dispositivos administrados, como información del estado y es actualizada por los agentes de SNMP.

La versión MIB utilizada por el protocolo SNMP se denomina MIB-II (versión), es la que se explicará en este apartado, aunque sea nombrada como MIB, también existe una versión MIB.

En un MIB se almacena la información mediante objetos que definen algún tipo de información y con sus correspondientes valores asignados, estos objetos son representados en una estructura de árbol, mediante los nodos hojas. Estos objetos representan un número de características de un dispositivo administrado.

El formato de cada objeto de un MIB está especificado mediante un subconjunto de la notación ASN.1 que es una notación estándar ISO que permite describir de forma flexible diferentes estructuras de datos de forma independiente de la plataforma.

Para definir un objeto en MIB se utiliza la anotación ASN.1, utilizando una plantilla que debe especificar los siguientes puntos:

- ⇨ Object-type: Debe contener el nombre del tipo de objeto con su correspondiente identificador de objeto.
- ⇨ Syntax: Sintaxis abstracta de ASN.1 que define la sintaxis del objeto.
- ⇨ Definition: Descripción textual del tipo de objeto. Las implementaciones de los distintos fabricantes deben garantizar que se cumple esta definición.
- ⇨ Access: Restricciones de acceso al objeto.
- ⇨ Status: Indica si el objeto es obligatorio para todo nodo, opcional o bien si está obsoleto y se mantiene solo por compatibilidad.

Un elemento de red puede implementar más de un MIB diferente con diferentes informaciones, y de hecho algunos MIBs concretos son de implementación obligatoria según las especificaciones de SNMP.

El MIB-II que incluye información genérica sobre un nodo SNMP y contiene, entre otros, los siguientes subárboles de información:

–System: Información genérica del nodo (nombre de máquina, ubicación física, etc.).
–Interfaces: Número de interfaces de red en el nodo, y parámetros de cada una.
–TCP/IP: Parámetros de funcionamiento de los protocolos de la pila TCP/IP (TCP, UDP, IP, ICMP, etc.).
–SNMP: Parámetros e información de estado del propio protocolo SNMP.
–Transmission: Información sobre el medio físico de transmisión asociado a cada interfaz.

Si bien MIB-II es el único MIB obligatorio en cualquier dispositivo SNMP, existen conjuntos estándar adicionales para otras tecnologías. Algunos de los más utilizados son:

–MIB-ATM.
–MIB-Frame Relay.
–MIB-DNS.
–Host Resources MIB: En el caso de que el elemento de red sea un PC, permite monitorizar aspectos locales de la máquina (uso de CPU, espacio libre en disco, número de usuarios, etc.).
–RMON: Conjunto de estadísticas que se van generando con el tráfico de paquetes, y que permiten hacer un estudio global de la red.

SMI

SMNP utiliza un subconjunto de ASN.1 que se conoce como SMI (estructura de gestión de información), que se utiliza para definir la estructura de un MIB. SMI define las entradas de una MIB y presenta una estructura en forma de árbol de global para la información de administración, convenciones, sintaxis y las reglas de construcción de un MIB.

SMI solo permite utilizar datos simples para definir un MIB, mediante diversas técnicas permite:
–Define la estructura de un MIB.
–Definición de un objeto en MIB, incluyendo la sintaxis y asignación de valores para cada objeto.
–Codificar el valor de los objetos.

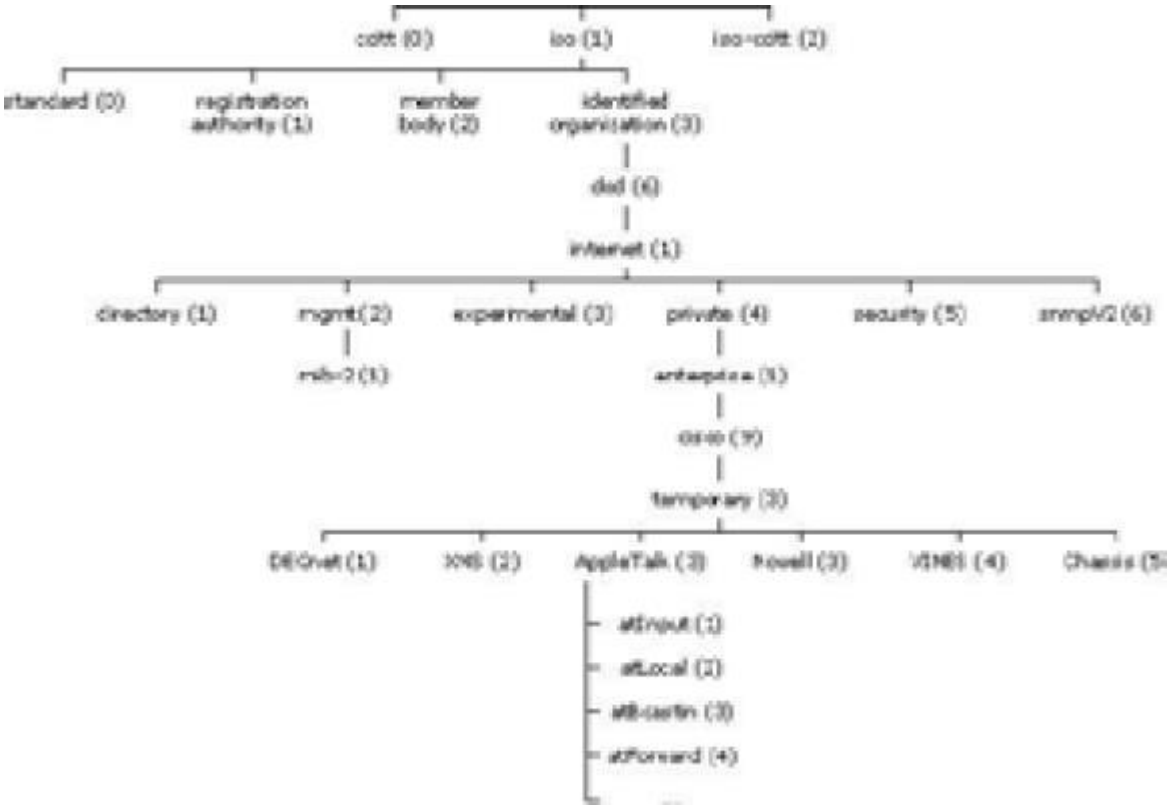
SMI establece el nombre de cada objeto administrado en MIB, así como la sintaxis y codificación. El nombre del objeto se denomina OID (identificador de objeto) que identifica de forma unívoca el objeto. La sintaxis de un objeto define el tipo de dato, la codificación describe como se envía la información incluida en los objetos entre un origen y un destino.
Los tipos de datos que son definidos por SMI, pertenece a los tipos especificados por la norma ASN.1 (notación sintáctica abstracta). Los tipos definidos en SMI son:
–Integer: representa valores enteros sin restricciones.
–Octet String: es una cadena de 0 o más bytes.
–Object identifier: Identificador de cada uno de los objetos definidos en la MIB, normalmente se denomina OID.
–Null: representa que la variable no tiene ningún valor.

También define un conjunto de estructura como son:
–Sequence: estructura donde los datos se codifican como una secuencia de datos.
–Sequence of: define un vector donde todos los elementos son del mismo tipo de datos.
–SMI también proporciona una serie de tipos de datos predefinidos que utilizan los tipos mencionados anteriormente. Algunos de estos tipos.
–NetworkAddress: es un selector que permite seleccionar varios formatos de direcciones.Inicialmente sólo IpAddress.[eliminado en v2].
–IpAddress: STRING de 4 octetos (dirección IP versión 4).
–Counter: entero no negativo que sólo puede incrementarse hasta llegar al valor máximo, en el que vuelve a 0. Valor máximo: 32 bits.
–Gauge: entero no negativo que puede ser incrementarse o decrementarse. No puede superar el valor máximo: 32 bits.
–TimeTicks: entero no negativo que expresa el tiempo en centésimas de segundo desde un determinado momento.
–Opaque: datos arbitrarios codificados como OCTET STRING.
Además de su formato, cada objeto del MIB tendrá asociada una regla de codificación, que especifica cómo transformar el tipo abstracto a flujo de bits para su transmisión por la red, de forma que todos los elementos de la red codifiquen igual los diferentes objetos y no haya problemas en la comunicación.
De todos los tipos de datos de un MIB, los identificadores de objetos o OID (Object identifier) son el elemento básico para la construcción de la MIB. Es un tipo de datos que especifica un objeto.
Los identificadores de objetos tienen las siguientes características:
–Es único y su valor es una secuencia de números enteros.
–Un grupo de objetos definidos formará un estructura en árbol. Los objetos concretos estarán en las hojas del árbol.
Los OID definidos para un objeto es único solo en la jerarquía de MIB que lo almacena, por ejemplo un OID sería:

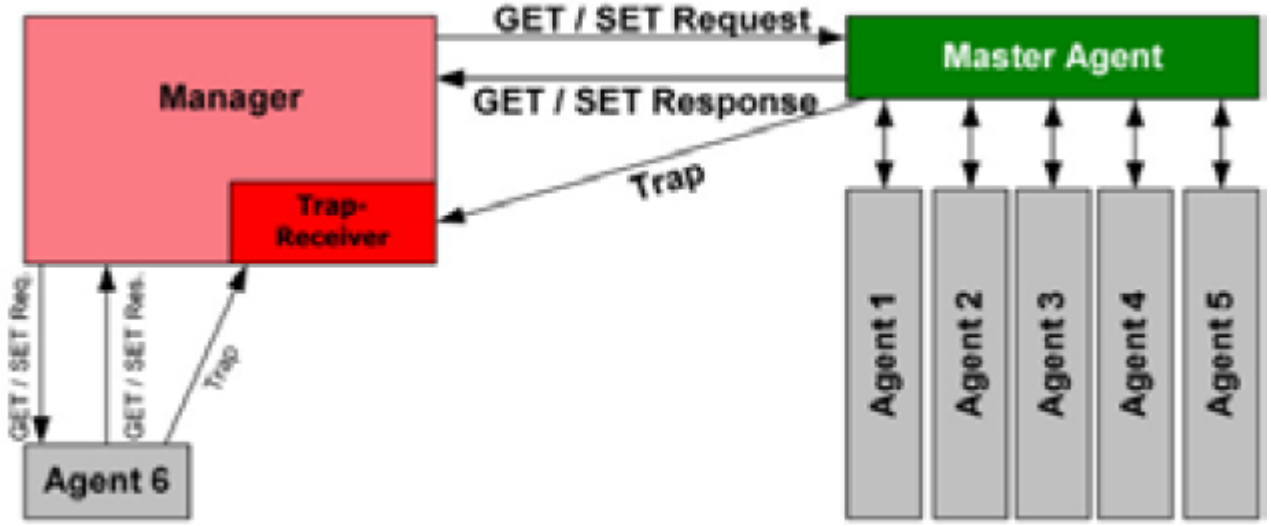
.1.3.6.1.2.1.1.3.0

Este OID representa una variable que está almacenada en el MIB.
Existen herramientas que permiten buscar OID dentro de un MIB o realizar otras operaciones, en Linux tenemos el paquete net-snmp-utils, que proporciona un conjunto de herramienta de terminal para SNMP que permiten realizar operaciones sobre un MIB. También existen herramientas gráficas como MIB Browser que permite realizar búsquedas y otras tareas de manera gráfica en un MIB.

Estructura en árbol de un MIB.



Para obtener la información de los dispositivos, SNMP puede realizar esta acción de dos maneras:
–Sondeo (Polling): Es el modo normal de funcionamiento, se basa en un concepto de Preguntas y Respuestas. El nodo administrador envía una solicitud a un agente pidiendo información o mandándole actualizar su estado, los agentes envían información al nodo administrador como respuesta o una confirmación de una acción solicitada. Este modo tiene como desventaja que puede incrementar el tráfico de la red perjudicando el rendimiento.
–Interrupción (Trap): un agente manda la información al nodo administrador puntualmente, ante una situación predeterminada, estas situaciones son configurables.
Funcionamiento de SNMP.



SNMP realiza intercambio de información de forma estructurada, este intercambio es realizado a través de una serie de mensajes, que tienen una estructura compuesta por tres campos:
–Versión: número de versión del protocolo SNMP.
–Comunidad: Nombre de comunidad del agente SNMP definido en el agente, se utiliza para la autenticación.

–PDU SNMP: Contenido de la unidad de datos del protocolo, depende de la operación que se ejecute. Este campo tiene la siguiente estructura.

·Tipo: especifica que operación realiza.

·Identificador: número que es utilizado para el intercambio de información entre el administrador y los agentes.

·Estado de error: utilizado para un determinado tipo de mensajes, proporciona información sobre el tipo de error producido. Puede contener el siguiente conjunto de valores.

›0. No hay error.
›1. PDU demasiado grande.
›2. No existe esa variable.
›3. Valor incorrecto.
›4. El valor es de solo lectura.
›5. Error genérico.

Enlazado de variables: serie de nombres de variables con sus valores correspondientes.

Con la estructura explicada anteriormente, son construidos una serie de mensajes para el intercambio de información.

Existen algunas variantes de SNMP que mejoran algunos aspectos, una de las más conocidas es RMON, monitorización de redes remotas, que permite monitorizar una red al completo y también a dispositivos de forma individual, como sucede con SMNP.

Proporciona un MIB que amplía las funcionalidades de MIB-II utilizado en SNMP, como obtener información de la propia red. Realiza consultas mediante una serie sondas utilizando los mensajes de SNMP, pero el funcionamiento se diferencia en los siguientes puntos.

–El procesamiento de la información es más complejo que en SMNP, almacena mucha más información.

–La información se envía bajo demanda al gestor.

RMON se centra en el análisis del tráfico de la red y no en el estado de dispositivo, como realiza SNMP.

El MIB de RMON es definido como una extensión del MIB-II de SNMP y añade nuevos grupos, como:

–Statistics: estadísticas de la red.

–History: almacena un conjunto de estadísticas seleccionadas en un tiempo determinado (histórico).

–Alarm: Define los valores máximos o mínimos (umbrales), si esos valores son superados se dispara una alarma.

–Matrix: Matriz donde se almacena el tráfico enviado-recibido por los dispositivos de la red.

–Filter: Filtros para determinar qué tipos de paquetes serán capturados para su análisis.

–Capture: Paquetes capturados por los filtros.

–Event: Registro de alarmas generadas.

–Token Ring: Datos de monitorización para redes Token Ring.

Existe una segunda versión, RMON v2, que añade nuevas funcionalidades, que aparte de monitorizar a nivel de enlace, incluye monitorización niveles superiores del modelo OSI. Para realizar estas nuevas tareas, incluye nuevos grupos:

–Genera estadísticas para nivel superiores, como nivel de red y aplicaciones.

–Agrupa las estadísticas en función del protocolo.

–Mecanismo para configuración remota de las sondas.

También existen extensiones para RMON, como SMON que es utilizado para monitorización de redes conmutadas, redes no Ethernet. Este tipo de redes presentan una serie de características que la diferencian de las redes Ethernet. Para monitorizar este tipo de redes, presenta una serie de características, como son:

–Replicación de puertos.

–Permite monitorizar tráfico de un sub-segmento de red.

El uso de RMON presenta una serie de ventajas, algunas de estas se presentan a continuación.

⇨ Operaciones fuera de línea (offline)
Si se produce un fallo de conexión entre el agente (monitor RMON) y el gestor, el agente seguirá recolectando información sobre la red. Cuando el fallo se ha arreglado y la conexión se restablecido, el monitor enviara toda la información al gestor. En RMON se envía la información bajo demanda, no necesita una orden del gestor para que el monitor recoja información de la red.

- ⇨ Detección y reporte de fallos
  Proporciona monitoreo preventivo, detecta un fallo antes de que se produzca. El monitor puede configurarse para detectar determinadas situaciones y si ocurre, que envíe una notificación al gestor.
- ⇨ Datos con valor agregados
  Un monitor puede analizar la información que recolecta de la red donde se encuentra. Esta tarea permite tener más control sobre la red y ahorra en número de gestores que son necesarios para una determinada red.
- ⇨ Múltiples gestores de red
  Un monitor puede ser configurado para que funcione correctamente con múltiples gestores de red, aumenta la fiabilidad. Si un gestor falla, el monitor puede enviar los datos recogidos a otro gestor.

Syslog

Syslog proviene del mundo de los servidores y se ha vuelto muy popular como mecanismo sencillo para que los nodos puedan transmitir de forma asíncrona mensajes de eventos, hoy en día la mayoría de los nodos disponen de su implementación.

Como su nombre indica, el propósito de syslog es escribir mensajes de sistema en un fichero de registro (log) donde un operador de red o una aplicación pueda acceder para su análisis y procesado. Si en vez de enviar los mensajes de sistema en un fichero se envían a un gestor, el propio gestor tendría la información en tiempo real de cuándo ocurren los eventos, sin necesidad de tener que monitorizar el fichero.

En general, los nodos con syslog implementado notifican excesivamente con eventos de todo tipo y en algunos casos con mensajes sin importancia. Aunque todos los mensajes que genera syslog proporcionan un registro general de la actividad del nodo. Incluso, bajo ciertas circunstancias, el poder leer todas las trazas de la actividad del nodo puede ser muy valioso a la hora de hacer algún tipo de diagnóstico, sobretodo en el caso de problemas, como degradación de servicio o vulnerabilidades de seguridad.

La práctica en un gran operador de telecomunicaciones es registrar todo pero notificar solo los eventos importantes.

El protocolo proporciona una estructura para los mensajes compuesta por una cabecera, parte opcional de datos estructurados y un mensaje:

Cabecera						Datos Estructurados			Mensaje
Prioridad	Versión	Marca de tiempo (Timestamp)	Nombre del host	Nombre de aplicación	Identificador de mensaje	SDE1	…	SDEn	Mensaje

La cabecera incluye los siguientes campos

- ⇨ Prioridad: facilita la categorización de los mensajes de acuerdo con algún criterio. Está compuesto por un código de gravedad y otro de facilidad. La gravedad es un número del 0 al 7, siendo cero el más grave, cada número especifica un grado de gravedad.
  0: Emergencia: sistema inutilizable.
  1: Alerta: tomar acciones a corto plazo
  2: Crítica: situación muy peligrosa
  3: Error: se ha producido un error en el sistema
  4: Aviso: se he producido una situación no esperada
  5: Notificación: sistema funciona pero se ha producido una situación anómala
  6: Información: mensajes de información del sistema
  7: Depuración: mensajes de depuración.

La facilidad es un código numérico que define diferentes tipos de mensaje en función de unos criterios. Para calcular la prioridad se realiza la siguiente formula.

Prioridad = (facilidad * 8) + gravedad

Los códigos numéricos asignados a la facilidad son:

0	Mensajes del kernel	12	Subsistema NTP
1	Mensajes a nivel de usuario	13	Log de auditorías
2	Mensajes de corro	14	Log de alertas
3	Demonios del sistema	15	Demonio de hora
4	Mensajes de seguridad	16	Uso local 0
5	Mensajes por syslogd	17	Uso local 1
6	Subsistema de impresión	18	Uso local 2
7	Subsistema de red	19	Uso local 3
8	Subsistema UUCP	20	Uso local 4
9	Demonio de hora	21	Uso local 5
10	Mensajes de seguridad	22	Uso local 6
11	Demonio FTP	23	Uso local 7

–Versión del protocolo Syslog.
–Marca de tiempo, especifica la hora del mensaje.
–Nombre de Host, nombre del sistema que ha enviado el mensaje de syslog.
–Nombre de la aplicación, especifica la aplicación con su ID de proceso que ha enviado el mensaje de Syslog.
–Identificador asociado al mensaje que lo identifica.
Los datos estructurados permiten añadir parámetros adicionales, extendiendo la funcionalidad de un mensaje de syslog. Utilizando estos campos cualquiera puede definir extensiones del protocolo syslog sin que pierda interoperabilidad con el protocolo.
La parte del mensaje en donde es almacenado el propio mensaje, no tiene un formato propio que defina la información que almacena. En esta parte, contiene información del mensaje como quien ha generado el mensaje, esta información es situada al principio del campo (32 primeros caracteres) y el resto es utilizado para almacenar el propio mensaje.
Al no especificar un formato, puede haber diferencias en la estructura de los mensajes dependiendo de los fabricantes. Esto es debido a que syslog en principio no fue un estándar y surgieron varias modificaciones en el formato de mensaje, aunque esto fue solucionado con posterioridad cuando se definió un norma que especifica el protocolo syslog como estándar.
El funcionamiento de Syslog implica dos componentes que utilizan el intercambio de mensajes, tenemos:
–Syslog sender: envía mensajes a syslog.
–Syslog receiver: recibe los mensajes.
Estos componentes suelen estar asociados a un agente y gestor, pero pueden funcionar en otros tipos escenarios, como los siguientes:
–Los dos componentes (sender y receiver) se encuentran en el mismo nodo, generando un fichero local en el nodo donde un registro almacena los mensajes que han sido generados.
–Un host almacena de forma centralizada los registros, recibe los mensajes de syslog de varios nodos. Si una aplicación necesita acceder a los mensajes de syslog de un nodo, accederá al host central. Este escenario reduce la carga en los nodos individuales y también reduce la gestión de syslog, pero puede aumentar el tráfico en la red.

Netconf

Protocolo que utiliza mecanismo RPC, con arquitectura cliente/servidor que interactúa con mensajes XML, se encarga de realizar las transacciones con validaciones y rollback, utilizando diversos protocolos de transporte como SSH o TLS.

Fue desarrollado por la IETF en 2006 y revisado en 2011, está diseñado específicamente para la gestión de configuraciones, proporcionando un serie de mecanismos para realizar diversas operaciones como: instalación, modificación y borrado de configuraciones.

Este protocolo tiene un ámbito más limitado, configuraciones, y no es un protocolo de gestión con funciones de supervisión, puede complementar con otros protocolos, como SNMP, que suplan estas funcionalidades.

RPC (Remote Procedure Call) o Llamada a Procedimiento Remoto, es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.

El hecho de que Netconf esté diseñado para la configuración de los nodos no significa que no pueda ser utilizado o expandido para otros fines. De hecho, ya permite la recuperación de la información de estado, aunque no constituya la función central. Por ahora, sin embargo, Netconf es el mejor posicionado en el apartado de gestión de la configuración y llena el vacío dejado por SNMP.

Netconf está basado en la noción de que la información de configuración de los nodos puede ser entendida y manejada como si estuviese contenida en un almacén de datos que a su vez puede manejarse como un archivo. En esencia, un almacén de datos corresponde al fichero de configuración del dispositivo con el conjunto de sentencias de configuración que deben ser ejecutadas para modificar su estado al deseado.

Netconf proporciona un conjunto de operaciones para la gestión del almacén de datos. Con algunas diferencias, se asemeja al MIB de protocolo SMNP.

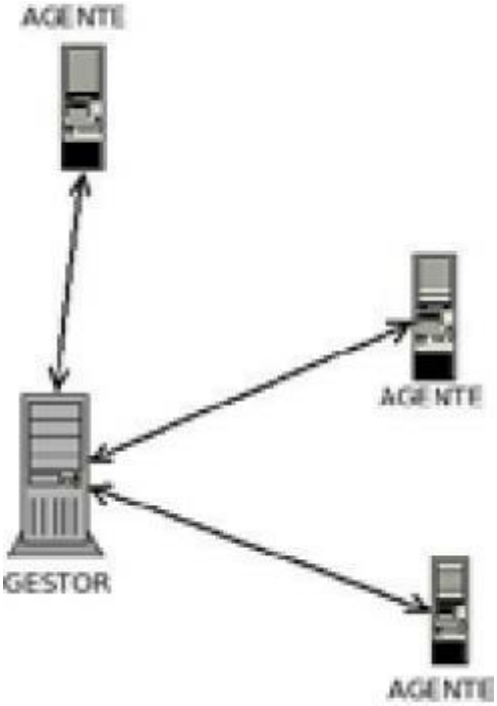
Netconf permite que los datos almacenados dentro del almacén de datos estén organizados jerárquicamente en forma de árbol. La información que tiene relación esta agrupada, esto facilita el acceso de la información por parte de cualquier aplicación. Así, el manejo de los almacenes de datos es aún más fácil porque no siempre es necesario manipularlo completo sino por partes. Con esta organización, las operaciones pueden aplicarse a subárboles individuales, correspondientes a las distintas subconfiguraciones, en vez de a la configuración en su totalidad.

Una característica destacada de Netconf es el uso de XML como lenguaje para las operaciones, que permite la representación de la información de una manera estructurada.

Los documentos XML contienen etiquetas que se utilizan para delimitar las diferentes piezas de información en un fichero. Las etiquetas se definen por los usuarios, que pueden asociar etiquetas diferentes, con una semántica diferente.

Cuando la información se codifica en XML, se traduce en un documento XML. Esto significa que en Netconf, cada petición y cada respuesta se codifican como un documento XML que se envían entre el gestor y el agente. Este documento contiene la información sobre qué operación se ha solicitado, qué parámetros lleva y los contenidos del almacena de datos que van como parte. Netconf también define las etiquetas necesarias junto con las plantillas de los documentos que corresponden a las distintas operaciones o mensajes.

La arquitectura de Netconf es definida en cuatro capas.



–Capa de protocolo de transporte: esta capa proporciona un camino de comunicación entre el cliente y el servidor. Netconf especifica los requisitos que debe cumplir, pero no incluye un mecanismo propio, para realizar esta tarea se utilizan protocolos como SSH o SSL.
–Capa RPC: proporciona primitivas que permite a los gestores invocar funciones en los agentes usando patrones de peticiones-respuesta.
–Capa de operaciones: define un conjunto de operaciones básicas del protocolo invocadas por RPC con parámetros codificados en XML.
–Capa de contenido: define la estructura utilizada para los datos de configuración, estado y notificaciones.
–El funcionamiento de Netconf es el siguiente, cuando se quiere establecer una sesión Netconf, primero se debe definir el canal de transporte y una vez definido se abre la sesión. Tanto el cliente como el servidor deben enviarse una lista con las funcionalidades, que son las operaciones permitidas, que soportan cada uno de ellos, solo se utilizarán aquellas funcionalidades que ambos soporten. Esto se realiza mediante mensajes XML, también es enviada información adicional necesaria para una comunicación correcta.
Una vez finalizado el intercambio de información el cliente está preparado para recibir las peticiones del servidor y el cliente a enviar las respuestas al servidor.
Netconf proporciona una serie de operaciones para realizar la gestión, estas operaciones forman parte del protocolo base que proporciona una serie de capacidades, también existen un conjunto de operaciones adicionales mediante una serie de extensiones a las operaciones del protocolo base, aunque estas operaciones son opcionales, como ejemplo de operaciones opcionales tenemos xpath y valídate. Este conjunto de operaciones adicionales son acordadas en el establecimiento de la sesión de Netconf.

- ⇨ Get-config: Recupera información de un archivo de configuración de un nodo.
- ⇨ Get: Se utiliza para recuperar cualquier tipo de información, es una generalización de la operación anterior.
- ⇨ Edit-config: Modifica la configuración de un nodo, los cambios se especifican en una serie de parámetros que se incluye en la operación.
- ⇨ Copy-config: Modifica la configuración de un nodo, pero a diferencia de la operación, reemplaza toda la configuración.
- ⇨ Delete-config: Borra una configuración que no está utilizando el nodo en ese momento.
- ⇨ Lock y unlock: Permiten al gestor tener acceso en exclusiva a la configuración.
- ⇨ Close-session: Cierra una sesión, respetando cualquier operación que aún estuviese ejecutándose.
- ⇨ Kill-session: Termina una sesión de manera inmediata, sin importar las operaciones en ejecución.

Cada una de las operaciones descritas en la tabla, incluye una serie de parámetros para su ejecución.

Protocolo TMN

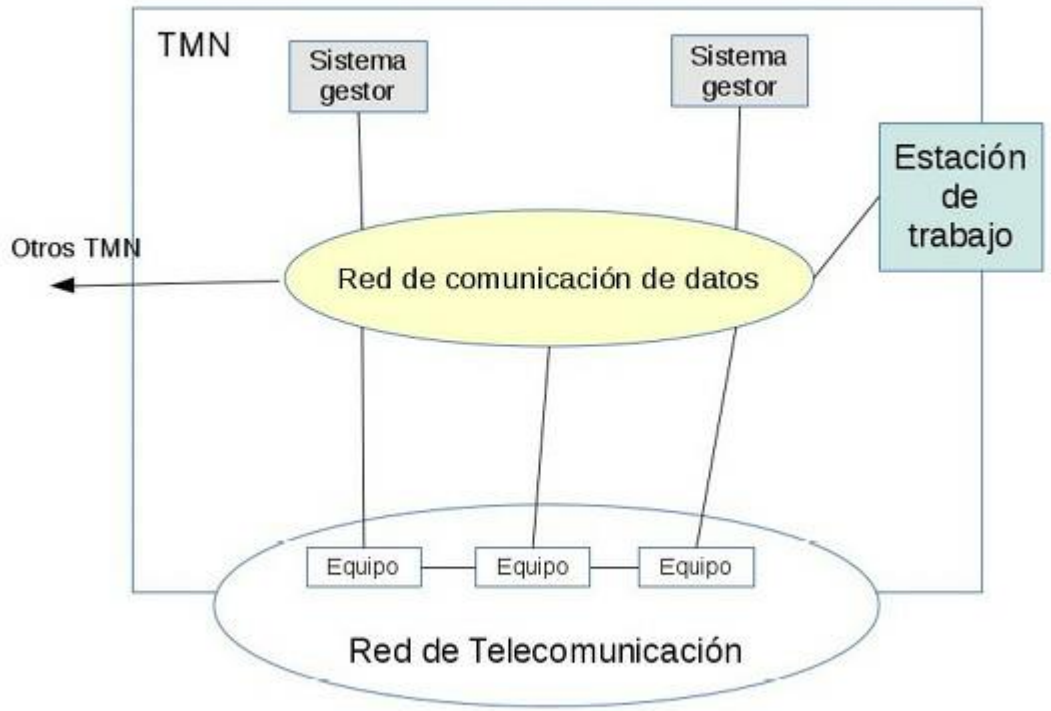
TMN (Red de gestión de telecomunicaciones) es un protocolo definido ITU-I para la gestión de sistemas abiertos en una red de telecomunicaciones. El objetivo es proporcionar una estructura de red organizada para conseguir la interconexión de los diversos tipos de Sistemas de Operación y equipos de telecomunicación usando una arquitectura estándar e interfaces normalizadas.

En el protocolo TMN, la gestión se realiza mediante un conjunto de sistemas interconectados a los elementos gestionados mediante una red, esta red de gestión puede no usar los mismos medios de transmisión que la red gestionada. En resumen, para el utilizar el protocolo TMN se diseña una red que permite gestionar diferentes tipos de redes.

El protocolo TMN puede hacer uso de parte de la red telecomunicación para sus propias comunicaciones, un conjunto de sistemas gestor se encarga de realizar la mayor parte de las funciones de gestión, incluso es posible que una función de gestión sea realizada por múltiples sistemas gestor.

La red comunicación se utiliza para el intercambio de información de gestión entre los sistemas, también se utiliza la red comunicación para conectarse o otros dominios TMN.

El diseño de TMN permite ser utilizado para la gestión de redes analógicos-digitales, redes telefónicas, redes LAN-WAN, redes móviles, etc.



La arquitectura TMN está diseñada para que varios sistemas que interactúan entre ellos para conseguir un efecto coordinado sobre la red. La arquitectura TMN está compuesta por:

Arquitectura funcional: Describe una distribución de la funcionalidad de gestión TMN mediante una serie de bloques funcionales.

Arquitectura física: Define cómo estas funciones de gestión pueden ser implementadas dentro de un equipo físico.

Arquitectura de información: Define el formato de la información que se transmite entre los dispositivos.

Arquitectura organizativa o lógica: Implementa una relación jerárquica entre los sistemas gestor donde a cada sistema gestor se la asignan diferentes responsabilidades, esto proporciona un modelo de gestión más estructurado.

En la arquitectura funcional se definen un conjunto de bloques funcionales, donde a cada uno se le asigna una responsabilidad. Los bloques funcionales son:
–Bloque funcional de sistema de Operación (OSF): funciones de un gestor, procesa la información de gestión para la red de comunicaciones.
–Bloque funcional de elementos de red (NEF): funcionalidades de los equipos de la red que le permiten funcionar como agentes de gestión.
–Bloque funcional de estación de trabajo (WSF): proporciona una interfaz al usuario, permite conectar al usuario con el sistema de operaciones para interpretar la información de gestión de TMN.
–Bloque funcional adaptador (QAF): permite gestionar elementos de red que no sean TMN, incorporándolo como entidades NEF u OSF.
–Bloque funcional de mediación (MF): Actúa sobre la información que llega de los NEF y de los QAF para adaptarla, filtrarla y condensarla adecuándola al formato utilizado por los OSF.
En una implementación TMN no es necesario definir todos los bloques funcionales, en la configuración pueden definir varios bloques funcionales del mismo tipo.
La arquitectura funcional define una serie de puntos de referencia que identifican la información entre los bloques funcionales. Hay cinco tipos de puntos de referencia, tres tipos se definen dentro de TMN son los puntos: q, f y x. Los otros dos puntos están fuera de TMN y están parcialmente definidos, son los puntos g y m.

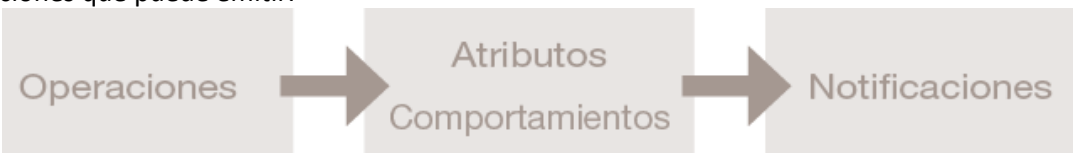
	NEF	OSF	MF	QAF	WSF	no-TMN
NEF		q	q			
OSF	q	q,x	q		f	
QAF		q	q			m
MF	q	q	q	q	f	
WSF		f	f			g
no-TMN				m	g	

La arquitectura física define como implementar los elementos descritos en la arquitectura funcional en bloques físicos:
–NE: elemento de red.
–OS: sistema de operación.
–WS: estación de trabajo.
–MD: dispositivo de mediación:
–QA: adaptador Q.
–DCN: red de comunicación de datos.
Existe una relación entre los bloques físicos y bloques funcionales (OSF, NEF, WSF, QAF y MF), a los primeros se implementan funcionalidades descritas por los segundos.

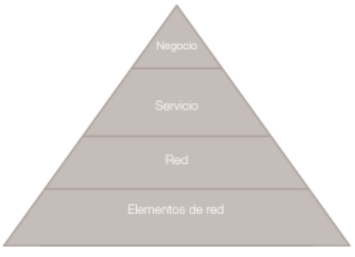
	NEF	MF	QAF	OSF	WSF
NE	O	opcional	opcional	opcional	opcional
MD		O	opcional	opcional	opcional
QA			O		
OS		opcional	opcional	O	
WS					O

Las relaciones pueden ser obligatorias (O), la funcionalidad especificada se implementa en el dispositivo correspondiente. Pero los dispositivos, de forma opcional, puede tener otro tipo de funcionalidades.
Los bloques físicos se conectan mediante interfaces que es una implementación de un punto de referencia que une a dos bloques funcionales. Los puntos de referencia g y m no pertenecen a TMN y tiene una interfaz asignada.
Las interfaces se comunican usando CMIP sobre la pila OSI.

Las interfaces tienen asignados una serie de letras mayúsculas, que corresponden a la letra del punto de referencia que implementa.
–Interfaz Q: implementa al punto de referencia q, es la interfaz más utilizada en TMN y define un perfil OSI completo.
–Interfaz F: implementa el punto de referencia f, define las funciones de la interfaz, pero no un protocolo para la misma.
–Interfaz X: implementa al punto de referencia x,, implica estrictas condiciones de seguridad.
En la arquitectura de información de gestión se pueden considerar:
–El modelo de información de gestión se realiza mediante orientación a objetos, de esta forma realiza una abstracción de los gestión de red. La información se modela mediante objetos gestionados.
–Utiliza un modelo agente-gestor, el intercambio de información se realiza mediante un protocolo estándar.
Un objeto gestionado es la vista conceptual de un recurso a gestionar, ya sea físico o lógico, los recursos son representados por uno o varios objetos. Para que el sistema de gestión controle un recurso debe tener un objeto asignado, los recursos que no tengan objetos no existen para el sistema de gestión.
Un objeto está compuesto:
–Atributos definidos en el objeto.
–Operaciones que podemos realizar con él.
–Comportamiento que presenta.
–Notificaciones que puede emitir.



Para definir se utilizan GDMO (Guías para la definición de objetos de Administración) que proporcionan un sintaxis con la que se especifican las MIB de los equipos TMN.
El modelo agente-gestor es utilizado para el intercambio de información entre procesos de gestión en TMN, los dos papeles tienen diferentes responsabilidades:
–Gestor: inicia las operaciones de gestión y recibe las notificaciones de los agentes, deben ser instalados en los dispositivos donde se recogerá la información.
–Agente: se encarga de los objetos gestionados que tengan asociados, responde a las operaciones indicadas por el gestor y envía las notificaciones correspondientes al gestor. Debe ser instalado en los dispositivos que van a ser monitorizados.
El protocolo utilizado para el intercambio de información entre agentes y gestores es CMIP, que es un protocolo estándar. Los mensajes que se envían a través de CMIP se realizan por medio de servicios que proporciona CMIS.
Anteriormente se explico el protocolo CMIP/CMIS de manera más detallada.
La arquitectura organizativa o lógica de TMN está basada en el modelo FCPAS de la organización OSI, este modelo está compuesto por las siguientes categorías.
–Gestión de fallos.
–Gestión de la configuración.
–Gestión de la facturación.
–Gestión de las prestaciones.
–Gestión de la seguridad.
Cada una de estas categorías está estructurada por medio de una serie de capas que corresponden a diferentes niveles de abstracción, también denominadas niveles lógicos.



El nivel de abstracción aumenta conforme se va bajando de nivel en la pirámide.

Capa Elemento de red

Esta capa incluye funciones propias de los elementos individuales, controla y coordina un subconjunto de elementos de red. Se encarga de todos los aspectos relacionados con los dispositivos físicos de la red como elementos individuales.
Permite administrar un conjunto de elemento de red, ofreciendo una visión de la red. Proporciona todo tipo de información de los elementos de red en un formato para TMN. También proporciona una interfaz de adaptación para elementos que no soporten TMN.
Esta capa es la encargada de mantener un serie de datos estadísticos, registros y otros datos acerca de un conjunto de elementos de red.

Capa de red

Proporciona una visión en conjunto de la red, utilizando las vistas individuales de la capa anterior. Se encarga del control y coordinación desde el punto de vista de la red. Las funciones que realiza son:
–Suministro, cese o modificación de servicios de red.
–Mantenimiento de la capacidad de la red, optimizando el funcionamiento en caso necesario.
–Detección de errores.
–Mantenimiento de datos estadísticos y registros de red.

Capa de servicio

Esta capa está relacionada con la gestión de aquellos aspectos que pueden ser directamente observados por los usuarios de la red de telecomunicaciones. Estos usuarios pueden ser usuarios finales, empresas o proveedores de servicios.
A los usuarios no se le permite ver la estructura interna de red y no pueden realizar tareas de administración directamente de los elementos de red. Las funciones asignadas.
–Interacción entre servicios.
–Gestión calidad de servicio, QoS.
–Relaciones con el usuario o proveedores de servicios.
–Mantenimiento de datos estadísticos.
–Contabilidad de uso de los recursos.

Capa de Negocio

Esta capa incluye las estrategias de negocios que definen las acciones para conseguir el retorno de la inversión, considerando la responsabilidad global sobre la administración de la organización. Las funciona que puede incluir.
–Soporte para proceso de toma de decisiones de inversión y utilización óptima.
–Soporte de gestión de presupuesto de telecomunicaciones.
–Soporte de suministro y demanda de mano de obra.
–Mantenimiento de datos agregados sobre la empresa.

2.3. Herramientas para la gestión de red

Para realizar una correcta gestión de una red hay disponibles un conjunto de herramientas software que ayudan al administrador a realizar una gestión óptima de la red.
Para escoger que tipo de herramienta es la más adecuada en función de una serie de parámetros.

- ⇨ El tamaño de la red: influye en la herramienta que podemos escoger. No tiene las mismas necesidades una gran red que un red para un pequeña empresa, también influye el coste de la herramientas, mucho mayor en herramientas para grandes redes, y los requisitos para utilizar esas herramientas.
- ⇨ Necesidades: que parámetros de gestión debe ser controlados en función de los servicios que proporciona la red. Identificando las aéreas donde es necesaria la gestión de redes.
- ⇨ Tecnologías: dependiendo de la tecnologías que se utilizan en la red y la arquitectura, se debe tener en cuenta para la elección de la herramientas de gestión.

Las herramientas de gestión de red proporcionan al administrador una serie funcionalidades, algunas de estas funcionalidades son:

- ⇨ Descubrimiento de la topología: saber la estructura de la red (topología), que tipos de dispositivos lo componen y mostrarlo de forma gráfica. Esta funcionalidad se realiza de forma automática por la herramienta de gestión.
- ⇨ Herramientas de diagnósticos de la red: realiza un serie de sondeos periódicos para buscar e identificar fallos en la red, también recopila información sobre el error para encontrar la solución más adecuada.
- ⇨ Herramientas de seguridad: proporcionan diferentes herramientas que aseguren la red de posibles ataques, uso indebido de los recursos, accesos no autorizados u otro tipo de acciones que perjudiquen el rendimiento de la red.
- ⇨ Monitorización y control de la red: vigilar diversos parámetros de la red y en función de unos valores configurados, generar notificaciones o alarmas para determinados eventos.
- ⇨ Ejecución de comandos remotos: permitir que un administrador o la propia herramienta, realizar diversas tareas de administración en equipos remotos.
- ⇨ Gestión de MIB: gestionar el funcionamiento de la base de datos donde se almacena datos de gestión (MIB).
- ⇨ Visualización de los datos de gestión: se realiza mediante diversas tipos de gráficas.

Todas las funcionalidades descritas anteriormente pueden incluirse en una sola herramienta de gestión, denominadas soluciones completas, donde incluyen un conjunto de herramientas integradas y cada una se encarga de un conjunto de tareas, también proporciona una administración y configuración centralizadas. Pero también podemos tener un conjunto de herramientas que por separadas realizan su tarea y utilizando un formato de datos común poder integrarlas entre ellas, esta última opción proporciona más versatilidad pero la administración puede resultar compleja.

Las herramientas de gestión incluyen una serie de características.

- ⇨ Incluye una interfaz de gráfica de usuario.
- ⇨ Exportación de los datos de gestión en diferentes formatos.
- ⇨ Configuración de parámetros de gestión de forma centralizada mediante una interfaz.
- ⇨ Gestión proactiva, identificar problemas potenciales analizando los datos recogidos.
- ⇨ Tolerancia a fallos planificando copias de seguridad de la información de gestión.

Hay empresas de dispositivos de red que proporcionan su propio software de gestión, también hay software de gestión que funciona en múltiples dispositivos hardware, se denominan herramientas de gestión multifabricante.

El funcionamiento de las herramientas de gestión consiste en uno o varios equipos donde realizar la gestión (gestores) y un conjunto de clientes que tienen instalado un software configurado en los dispositivos que queremos controlar (agentes). Para acceder al gestor el software de gestión proporciona una interfaz web donde realizar todas las tareas de mantenimiento y monitorización de la red. Esta interfaz web permite al administrador acceso remoto desde cualquier equipo de la red al servidor donde está instalado el gestor.

La comunicación entre el gestor y los agentes utiliza algunos de los protocolos de comunicación explicados anteriormente, como SNMP, cada software de gestión tiene disponible un conjunto de herramientas para realizar las tareas de gestión de red.

Como soluciones software completas para la gestión de una red, tenemos:

Cisco Prime.

Cisco Prime es una familia de diferentes productos desarrollados por Cisco, empresa especializada en soluciones de redes, proporciona diferentes productos para administrar redes y los servicios que proporciona. Dependiendo de diferentes aspectos como el tipo de red, hardware disponible o los servicios que proporciona la red hay un producto de Cisco específico.

Para la gestión de redes, algunos de los productos disponibles.

Cisco Prime Collaboration

Simplifica la gestión de redes de Comunicaciones Unificadas de Cisco y colaboración mediante vídeo.

Ayuda a garantizar una alta calidad de servicio, un mínimo de interrupciones del sistema y la resolución a tiempo de problemas.
Agiliza las implementaciones de Comunicaciones Unificadas de Cisco en instalaciones y reduce el tiempo y el conocimiento necesario para gestionar los cambios en la red.
Reduce el coste total de oportunidad mediante herramientas y procesos automatizados de aprovisionamiento y control.

Cisco Prime Infrastructure

Habilita la gestión convergente de ciclos de vida útil del acceso fijo e inalámbrico para las redes de campus y sucursales.
Proporciona visibilidad de garantía de las aplicaciones y resolución de problemas a fin de optimizar la experiencia del usuario.
Acelera la implementación de nuevos dispositivos, servicios de red y acceso seguro unificado.
Simplifica las auditorías de cumplimiento de la normativa con respecto a los reglamentos y las mejores prácticas del sector.

Cisco Prime Home

Gestión remota automatizada de dispositivos domésticos conectados, además de aprovisionamiento, configuración y actualizaciones de software sin intervención del usuario
Diagnóstico y resolución de problemas en tiempo real tanto para proveedores de servicios como para consumidores
Aumento de los ingresos a través de servicios para el consumidor, que incluyen Wi-Fi gestionada, firewall gestionado y controles parentales
Motor de análisis para disponer de una mayor visibilidad del uso y las características de la red doméstica

Como software de gestión de Cisco, veremos de ejemplo las características técnicas Cisco Prime Infraestructure. Una solución software que se integra con diversos dispositivos hardware. Entre las características disponibles tenemos:
–Soporta el protocolo SMNP como CDP (Cisco Discover Protocol), que es un protocolo de gestión propietario de Cisco, para descubrir la topología de red.
–Gestión de inventarios tanto de dispositivos Cisco como de otras compañías y de forma automática notifica los cambios que se produzcan.
– Monitorización mediante agentes.
– Política de QoS y realiza monitorización sobre esas políticas.
–Genera SLA.
–Analiza los paquetes de red.
–Y múltiples funcionalidades más.
Todo esto mediante una interfaz gráfica que facilita el trabajo del administrador.

HP IMC (Centro de administración inteligente).

Hewlett Packard (HP) es una empresa tecnológica que proporciona múltiples servicios y hardware para diferentes sectores.

Dentro de la gestión de redes incluye varias familias de productos en función del cliente, para la gestión de redes proporciona un conjunto de herramientas denominada HP IMC que tiene dos versiones: Estándar y Enterprise.

La versión estándar HP IMC es una solución de gestión integral e independiente que ofrece funciones de gestión integradas y por módulos para errores, configuración, contabilidad, rendimiento y necesidades de seguridad. El diseño del software IMC Standard se basa en una arquitectura orientada a servicios (SOA) mediante un modelo de flujo de aplicaciones empresariales a modo de núcleo que permite una gestión totalmente integrada de los recursos, servicios y usuarios. El software IMC permite gestionar dispositivos de HP y de terceros, y es compatible con los sistemas operativos Microsoft® Windows® y Linux.

Las principales características de gestión que incluye:

–Integra de forma coherente la gestión de errores, la configuración de elementos y la supervisión de redes, desde un punto de visión central. Compatibilidad integrada con dispositivos de otros fabricantes para permitir a los administradores de red gestionar de forma centralizada todos los elementos de la red, con una variedad de tareas automatizadas, que incluyen detección, categorización, configuraciones básicas e imágenes de software.

–Arquitectura modular: Se pueden añadir nuevos módulos para aumentar las capacidades de gestión de la red.

–Mejoras de actualizaciones instantáneas: el software IMC Standard proporciona ahora la disponibilidad de notificación y descarga de los últimos parches de IMC.

–Gestión de virtualización: Ofrece el conocimiento y la gestión de redes virtuales y reduce la complejidad de la migración al adaptar y automatizar las políticas de red con imágenes virtuales, soporta vMware, Hyper-V y KVM.

–Modelos de implementación, muy flexibles y escalables.

Observer.

Obsever es un producto de la empresa Network Instruments para la gestión de redes.

http://www.networkinstruments.com/products/observer/index.php

Está disponible para sistemas operativos Windows, soporta tanto redes LAN como conmutadas.

Proporciona un monitor de red con capacidades de análisis de datos, análisis de prestaciones y diagnóstico de problemas, soportando 740 protocolos, lista de protocolos. Está compuesto por dos componentes:

–Componente de recolección de datos, que reúne información acerca de los datos que fluyen por un segmento LAN o un conmutador.

–Componente de análisis, que decodifica, trata y visualiza los datos obtenidos por la(s) sonda(s).

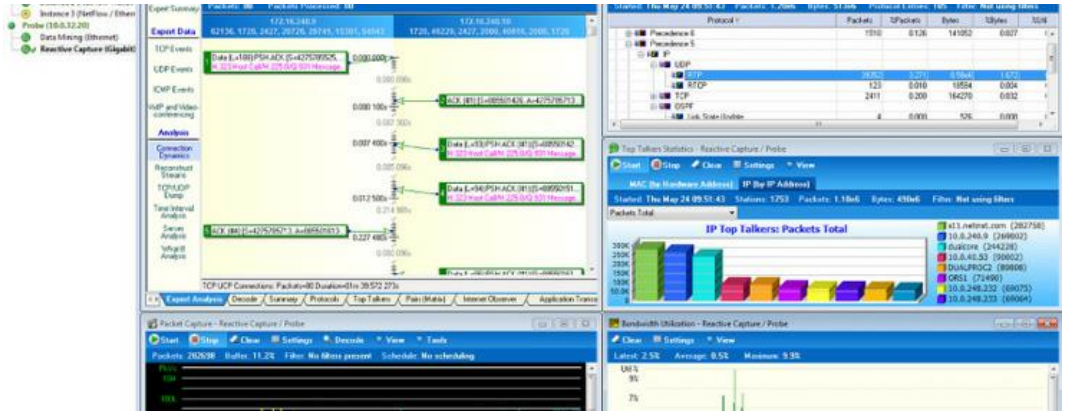
Observer monitoriza el segmento de red o conmutador al que se conecta el PC donde está instalado. Para monitorizar otros segmentos o conmutadores, se deben añadir sondas adicionales (Distributed Observer).

–Sondas específicas de Observer.

–Sondas de SNMP, RMON, RMON mejoradas.

–Posibilidad de incluir gestor de MIBs (compilador).

–Posibilidad de incluir acceso vía web.



Tivoli NetView

Tivoli NetView es una herramienta de gestión distribuida de redes que pertenece a la empresa IBM.
http://www-03.ibm.com/software/products/es/tivnetv/
Esta herramienta descubre redes TCP/IP mostrando su topología, monitoriza el estado de la red y recopila información datos sobre el rendimientos, para identificar de forma rápida los fallos de la red.
Utilice esta solución de gestión de red distribuida escalable para medir la disponibilidad y proporcionar aislamiento de fallos para la gestión de problemas.
–Administrar áreas de la red que están segmentadas por firewalls muy restrictivos.
–Compartimentar o restringir las acciones del operador y puntos de vista de la red.
–Mantener el inventario de dispositivos de gestión de activos.
–Disfrutar de la sencillez de uso de la consola Web que forma parte de este software de gestión de red para completar las tareas de administración.
–Elaborar informes sobre las tendencias de la red y analizar los datos de la red.
Las soluciones descritas anteriormente son soluciones completas que integran un conjunto de herramientas para diferentes servicios, están diseñadas para ambientes más empresariales y su coste puede ser alto para otro tipo de ambientes. También existen otros tipos de herramientas más específicas para diversas tareas de gestión de red, que integradas entre ellas proporcionan una funcionalidad similar a las soluciones completas.

Una lista de algunas herramientas.

- ⇨ Topología de red
  Herramientas para mostrar la topología de una red, ya sea de forma automática o manual. Ejemplo del primer tipo tenemos Network Topology Mapper de Solarwinds o Zenmap, ejemplo del segundo tipo es Microsoft Visio.
- ⇨ Gráficas de red
  Herramienta que recoge datos de diferentes parámetros de un dispositivo y muestra esos datos en diferentes gráficas. Como ejemplo tenemos Cacti, Munin o Monitorix.
- ⇨ Gestión de software
  Herramienta que permiten realizar actualización de software de forma remota en una red, también gestionan la instalación en múltiples equipos de una red. Como ejemplo tenemos opsi, Spacewalk, M23, OpenGnSys.
- ⇨ Gestión de inventario
  Herramientas para llevar un control de los dispositivos que componen la red y almacenar información de sus características, estas herramientas pueden tener funcionalidades incluidas en el apartado anterior. Como ejemplo tenemos GLPI o OCS Inventory
- ⇨ Gestión de configuración
  Herramientas que nos permiten administrar la configuración de diversos sistemas. Ejemplos: Puppet o Chef.
- ⇨ Acceso remoto
  Herramientas para acceder a un equipo de forma remota. Ejemplos: Putty, SSH, Mosh, Teamviewer o VNC.
- ⇨ Ejecución de comandos remotos
  Herramientas para ejecutar comandos en un equipo o un conjunto de equipos de forma remota. Como ejemplos tenemos Fabric o Ansible.
- ⇨ Gestión de fallos
  Herramientas para administrar las incidencias que surgen en Mantis o Trac.
- ⇨ HelpDesk
  Herramientas permite tener un servicio técnico que ayude a resolver los problemas de los usuarios de la red. Como ejemplos tenemos OTRS, RT -Request Tracker-.
- ⇨ Monitorización de redes
  Herramientas para monitorizar los dispositivos de una red, dispone de múltiples servicio para la monitorización y gestión de una red. Como ejemplos tenemos Nagios, Zabbix o Zenytal.

- ⇨ Gestión de seguridad
  Herramientas que ayudan a los administradores de red en la seguridad de los equipos, detección de intrusos y prevención. Como ejemplo tenemos la herramienta OSSIM.

Las herramientas explicadas en la tabla anterior pueden trabajar de forma conjunta en una red, como ventaja a las soluciones completas.

–Menor coste: muchas de las herramientas mostradas son gratuitas.

–Requisitos: Son herramientas utilizadas en redes de menor tamaño, aunque algunas herramientas pueden ser utilizadas en grandes redes, y los recursos que utilizan son menores.

–Versatilidad: podemos escoger que herramienta es la más adecuada para nuestra red. Las soluciones completas tienen una arquitectura modular que nos permite quitar o añadir funcionalidades mediante módulos, incluso podemos integrar software externo, pero no es tan versátil como utilizar herramientas específicas que permiten un grado de combinación más alto.

–Software libre: Gran parte de las herramientas descritas en la tabla son software libre, en contraposición con las soluciones completas que son software propietario. El software libre tiene algunas ventajas, como la disponibilidad del código fuente, que permite personalizar la aplicación a nuestras necesidades.

–Hardware: algunas de las soluciones completas están optimizadas para el hardware de la compañía y requiere altos requisitos hardware. En cambio, las herramientas específicas no requieren unos requisitos de hardware altos.

También las herramientas específicas tienen una serie de desventajas en comparación con las soluciones completas.

–Integración: las soluciones completas las herramientas que proporcionan están diseñadas para trabajar como un conjunto, por eso tiene una mayor integración. Las herramientas específicas que funcionan de forma independientes, aunque pueden comunicarse entre ellas utilizando diferentes mecanismos, el nivel de integración de mucho menor.

–Administración centralizada: las soluciones completas proporcionan una interfaz centralizada, en la mayoría de los casos son interfaz web, donde realizar tareas de administración. Las herramientas especificas tienen su propia interfaz de administración, aunque algunos casos pueden integrarse, en otros tendremos varias interfaces de administración. También existen herramientas que no proporcionan una interfaz de administración.

–Soporte: Aunque las herramientas específicas proporcionan un soporte muy bueno. Las soluciones completas han sido desarrolladas por grandes empresas (HP, Cisco, IBM, etc.) el soporte es más especializado.

Nagios

Como parte práctica, veremos un ejemplo de herramienta de gestión, nos centraremos en la configuración de esta herramienta y los servicios que puede proporcionar. Esta herramienta es Nagios.

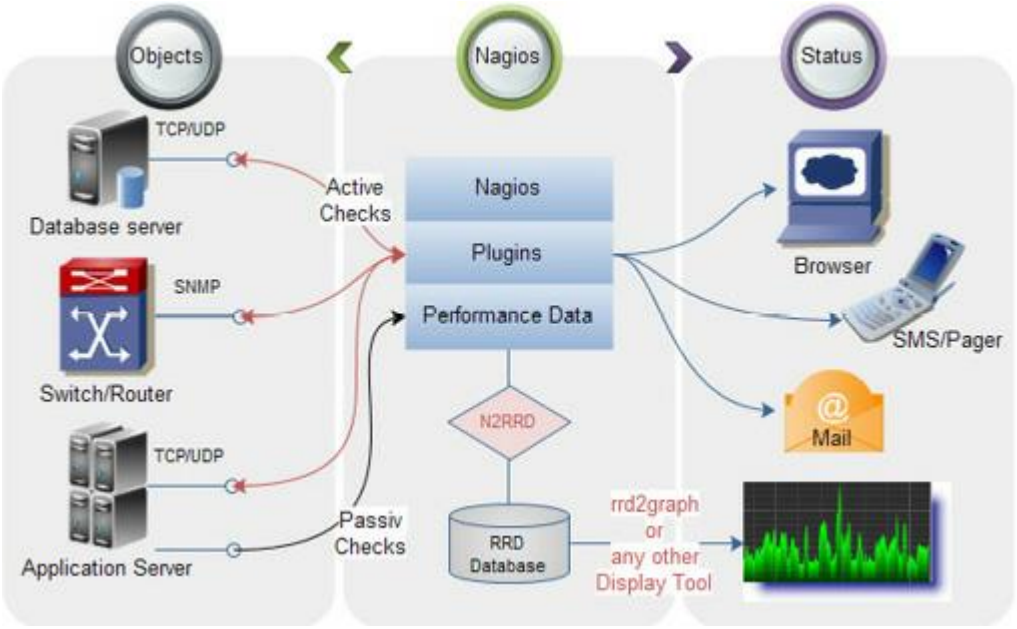
Nagios es una herramienta de monitorización de redes de código abierto para hardware y servicios software, generando alertas en función de una serie de parámetros configurables. Dispone de un conjunto muy extenso de plugins que permiten aumentar la funcionalidad, también permite integrarse como herramienta, por medio de plugin.

La gestión de la red es realizada mediante una interfaz web donde podremos monitorizar distintos parámetros de los dispositivos de una red por medio de distintos protocolos, como SNMP.

En la parte práctica se explicara cómo realizar las siguientes tareas:

–Monitorizar el estado de un cliente Linux.
–Monitorizar el estado de un cliente Windows.
–Monitorización por SNMP.
–Instalación y configuración de plugins de Nagios.
–Generación de gráficas con PNP4Nagios.

El funcionamiento de Nagios sigue un diseño de Gestor-Agente, donde en el equipo donde está instalado Nagios (gestor) controla un conjunto de agentes instalados en dispositivos hardware.



Nagios proporciona un potente sistema de plugin, otras características a destacar:

–Soporte de varios sistemas operativos, se pueden monitorizar recursos en sistemas Windows, Linux o Mac.
–Soporte de diferente hardware que incluyan SMNP.
–Genera notificaciones de múltiples formas (correo electrónico, SMS, mensajería, etc).
–Monitorización remota mediante SSL o SSH.
–Generación de informes y gráficas de rendimiento de la red u otros parámetros.
–Interfaz web de monitorización, posibilidad de sustituir la interfaz web de monitorización proporcionada por software de terceros (como ejemplo Centreon).
–Soporte para resolución de problemas de forma proactiva.
–Posibilidad de definir manejadores de eventos, que permiten reiniciar servicios o aplicaciones en caso de fallos.
–Monitorización de diferentes servicios.
–Fácilmente escalable.

En este ejemplo veremos cómo configurar Nagios para monitorizar una pequeña red. Veremos:

Instalación

La instalación de Nagios se realizara en equipo de con Linux, en la mayoría de distribuciones de Linux se encuentra este software en sus repositorios.

Para instalar Nagios solo necesitamos instalar los paquetes de nagios y como requisito es necesario tener instalado un servidor web Apache.
Para simplificar, en fedora.

yum install nagios

Instalar todos los paquetes de Nagios y sus dependencias.
Arrancar el servicio de Nagios y Apache

service start nagios
service start httpd

A continuación crear una contraseña para el usuario nagiosadmin, que es el usuario administrador que Nagios ha creado en el proceso de instalación.

htpasswd -c /etc/nagios/passwd nagiosadmin

Crear usuario y grupos necesarios para el correcto funcionamiento de Nagios.

groupadd nagios
adduser nagios -g nagios
passwd nagios
usermod -G nagios nagios
usermod -G apache,nagios apache

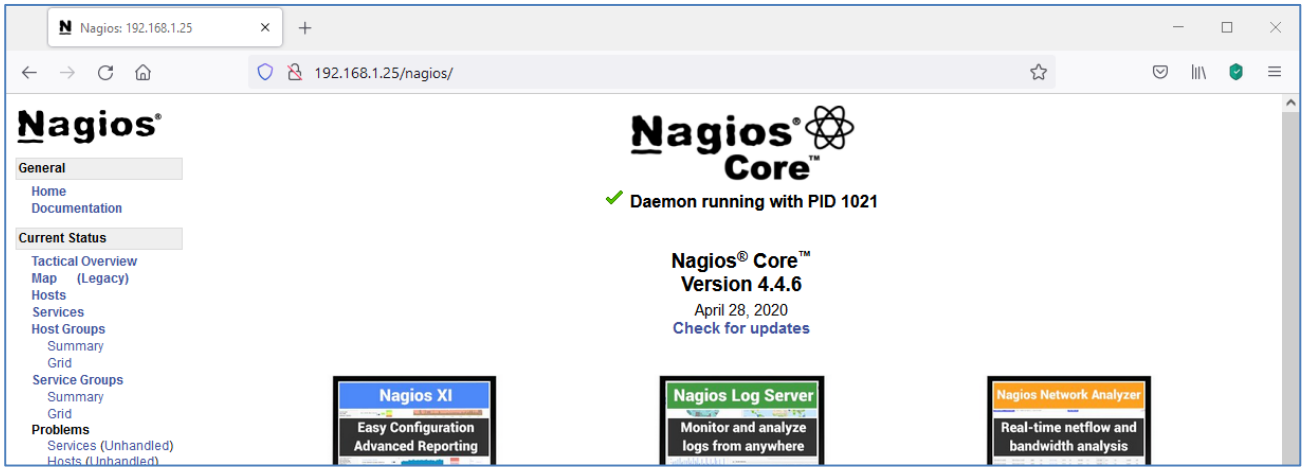
Es posible que los usuarios y los grupos se hayan creado en proceso de instalación del paquete de Nagios.
Nagios proporciona un archivo de configuración denominado nagios.cfg, para comprobar que el archivo de configuración es correcto, realizando una comprobación de la configuración, ejecutar.

nagios -v /etc/nagios/nagios.cfg

Realizar esto después de cualquier cambio en el fichero de configuración.
Si no muestra errores, la configuración es correcta finalizando la instalación de Nagios, solo queda acceder a la interfaz web de Nagios.
Abrimos un navegador y especificamos la siguiente dirección.

http://direcciónIP/nagios

La dirección corresponde al equipo donde esté instalado Nagios, solicita usuario y contraseña, ingresamos con los datos del usuario administrador de Nagios denominada nagiosadmin e introducimos su contraseña, si la contraseña es correcta mostrará la pantalla principal de Nagios:



La pantalla está dividida en dos partes, una columna a la izquierda donde mostrará todas las opciones disponibles y una parte central que mostrará los datos en función de la opción escogida.

Topología de red

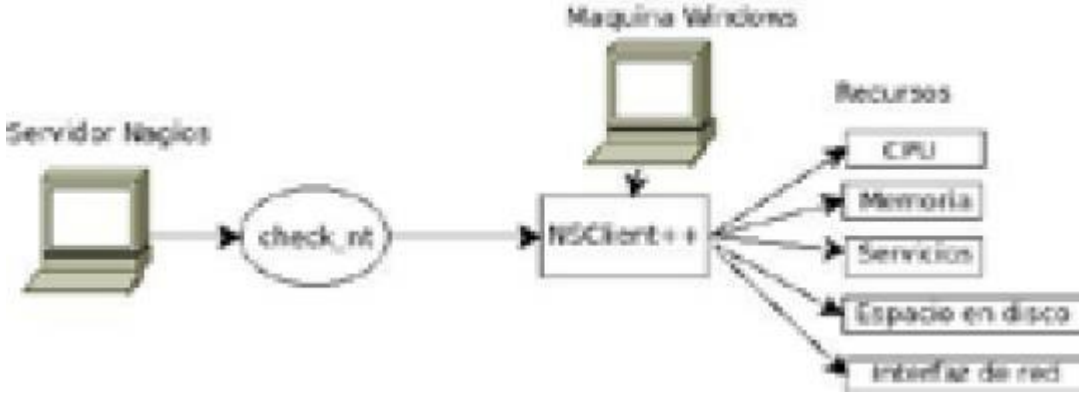
Nagios automáticamente sondea toda la red y muestra un mapa de red con la topología de red, solo debemos pulsar en la opción Map y mostrara los dispositivos. En este caso, solo mostrará un nodo denominado localhost que corresponde al equipo donde se encuentra Nagios instalado.
Este nodo tiene una serie de servicios y parámetros monitorizados por defecto, si pulsamos en el nodo podremos verlos. Para cambiar la información de este nodo, poniendo el nombre del equipo y la dirección IP, en el /etc/nagios hay un directorio objects, en este directorio tenemos ficheros de configuración que nos pueden servir de ejemplo.

El directorio objects muestra diferentes ficheros de configuración de definición de objetos, los objetos definen parámetros que queremos monitorizar. Una lista de algunos objetos que podemos definir.
–Equipos (host).
–Grupos de equipos (hostgroup).
–Servicios (service).
–Comandos (command).

Aquí encontramos un fichero localhost.cfg, que es un fichero de ejemplo que se utiliza como plantilla y es utilizado por defecto en Nagios, define el nodo que es mostrado en el mapa de red. Si abrimos el fichero con nuestro editor de texto favorito, veremos una estructura muy simple y bien documentada, compuesta por un conjunto de directiva "define", utilizadas para definir objetos.
La primera parte del archivo especifica la definición del host (host definition), vemos una directiva "define" donde define el nombre del dispositivo y dirección IP, modificamos esa información por la del equipo.
En el siguiente "define" modificamos la opción "members" por el nombre del equipo que ha sido definido anteriormente. En los siguientes "define" modificar el parámetro host_name por la información correcta.
De esta forma, ahora tenemos el nodo con información correcta de nuestro equipo y en el mapa de red ya no aparece localhost.

Configuración de agentes

Vamos añadir un nuevo equipo a Nagios, un equipo con Windows. Para realizar esto es necesario un paquete denominado nrpe que permite ejecutar plugins de Nagios en otras máquinas, permitiendo monitorizar equipos con Windows mediante la instalación de un cliente. Para realizar esto el paquete nrpe incluye un plugin denominado check_nt para comunicarnos con un cliente en Windows.



Nagios, a través del plugis check_nt, se comunica con un cliente en la máquina Windows denominado NSClient++, este software se comporta como un agente que recopila información de los recursos de la máquina y lo envía al gestor. Los recursos que monitoriza Nagios de un cliente Windows deben especificarse previamente en un fichero de configuración.
También podemos monitorizar utilizando el protocolo SNMP, aunque requiere la instalación del cliente SMNP y una configuración un poco diferente.
Tenemos Nagios instalado en un equipo, hace falta instalar el cliente para Windows denominado NSClient++ en http://nsclient.org/nscp/ podemos descargarlo, que nos permitirá monitorizar un equipo en Windows desde Nagios.
Después de instalar el cliente, tenemos que modificar los archivos de configuración correspondientes, para configurar un cliente Windows existe un fichero de configuración denominado windows.cfg, este fichero nos servirá de plantilla. Abrimos este fichero, vemos un conjunto de directivas "define" que definen una serie de objetos, el primer "define" es para definir el host de Windows, modificar los valores dirección IP (address) y nombre del equipo (host_name) con los valores de la máquina de Windows. Después modificar el resto de define el parámetro host_name con el valor asignado anteriormente.
Nos vamos al interfaz web y pulsamos en el apartado Map y vemos que existe un nuevo nodo que corresponde a la máquina de Windows.

Para añadir nuevos nodos, tendremos que crear un fichero de configuración por cada nodo a monitorizar, con la extensión cfg, podemos utilizar los ficheros de ejemplos como plantillas o crear nuevos ficheros desde cero. Después en el fichero nagios.cfg especificar dónde se encuentran esos ficheros, el fichero nagios.cfg se encuentra documentado con varios ejemplos que nos servirán para saber cómo realizar esta tarea.
Dentro de los ficheros de configuración especificamos los datos del nodo y los recursos que deben ser monitorizados de ese nodo. Cada nodo tendrá un conjunto de directivas define donde especificaremos la información del nodo y sus recursos.
Nagios proporciona un conjunto de objetos con diferentes características y que ayudará en el proceso de monitorización. Cada objeto describirá una componente y unas propiedades.

Definición de objetos

Como se ha explicado anteriormente, se define un conjunto de objetos; en los nodos que han sido creado se ha utilizado los ficheros windows.cfg y localhost.cfg como plantilla para definir nuestros nodos. En estos dos ficheros hay una serie de objetos creados, tenemos objetos host, hostgroup y service.

- ⇨ host
  Define un equipo físico.
- ⇨ hostgroup
  Define un conjunto de equipos físicos, se utiliza para agrupar un conjunto de host, simplificando la configuración.
- ⇨ service
  Define un "servicio" que se ejecuta en un equipos y que pretende monitorizar, los servicios están asociados a los host y pueden ser
  Atributos del host como: CPU, memoria, disco duro disponible, etc.
  Servicios que se ejecutan en un host (HTTP, POP3, FTP, SSH, etc.).
  Otros cosas asociadas al host como registros DNS.

Existen más tipos de objetos que pueden ser añadidos al fichero de configuración. El resto de objetos que podemos crear son:
–servicegroup.
–command.
–contact.
–contactgroup.
–timeperiod.
–servicedependency.
–serviceescalation.
–hostdependency.
–hostescalation.
Como ejemplo crearemos un objeto de tipo servicio para monitorizar el uso memoria RAM en el equipo local de Nagios y otro objeto servicio que monitorice el tráfico de red en el equipo Windows.
Primero configuremos un servicio para monitorizar la memoria RAM del equipo de Linux.
Como se ha comentado antes, Nagios incluye un conjunto de plugins, el paquete Nagios-plugins que en la instalación de Nagios se ha instalado como dependencia. Algunos de esos plugins son utilizados en los ficheros localhost.cfg y windows.cfg, en las directivas define definen algunos servicios que utilizan esos plugins.
Como no existe un plugin en el paquete Nagios-plugins para monitorizar la memoria RAM, debemos buscar uno e instalarlo en el sistema. Hay muchos plugins para monitorizar memoria RAM, se ha utilizado check_memory.pl que es un script creado en perl.
Descargamos el fichero y los situamos en la carpeta de plugins de Nagios (/usr/lib64/nagios/plugins) o en la carpeta que queramos.
El plugin check_memory.pl se encuentra en:
https://www.monitoringexchange.org/inventory/Check-Plugins/Operating-Systems/Linux/check_memory
Información sobre cómo utilizar el plugin.
http://blog.christosoft.de/2013/01/nagios-icinga-memory-usage/

Ahora debemos configurar Nagios para utilizar el plugin, primero debe indicarse cómo va ejecutarse check_memory. Utilizamos el fichero commands.cfg, en este fichero definimos los comandos, que es uno de objetos disponibles en Nagios, la directiva "define" seria de esta manera.

```
define command{
        command_name check_memory
        command_line perl /usr/lib64/nagios/plugins/check_memory.pl -w $ARG1$ -c $ARG2$
}
```

Define un comando con el nombre check_memory, este comando es un script de perl y con el parámetro command_line indicamos cómo se ejecuta el comando y especificando los argumentos, si los tuviera. Este comando especifica dos argumentos:

- ⇨ w: indica un aviso "warning", define un valor limite en porcentaje y se activa cuando la memoria libre supera ese límite.
- ⇨ c: índice un aviso "critical", define un valor limite en porcentaje y se activa cuando la memoria libre supera ese límite.

Para que este plugins funcione requiere que el sistema tenga el comando free, lo más seguro es que ya esté instalado, y el paquete perl-Nagios-Plugin.

El siguiente paso es definir un servicio que utilice este plugin y especificar los valores a los argumentos. En el fichero localhost.cfg creamos una nueva definición.

```
define service{
        use local-service
        host_name fedora.portatil
        service_description RAM disponible
        check_command check_memory!20%!10%
}
```

Hay parámetros en común con el resto de las definiciones que aparecen en el fichero localhost.cfg, los parámetros que se especifican.

- ⇨ use
  Especifica el nombre de la plantilla de servicio que se usa.
- ⇨ host_name
  Especifica al host (equipo) donde se aplica este servicio.
- ⇨ service_description
  Nombre que identifica el servicio, este nombre es utilizado en la interfaz web de Nagios para identificarlos.
- ⇨ check_command
  Especifica cómo se ejecuta el plugin y los valores que tiene cada argumento.

El plugin activa un aviso de tipo warning si la memoria disponible es menor al 20% de la memoria disponible y un aviso de tipo critical si la memoria disponible es del 10% de la memoria disponible.

Reiniciamos Nagios para que el plugin entre en funcionamiento, en la interfaz web en el apartado Service veremos en nuevo plugin activo con el nombre de RAM disponible.

Service Status Details For Host 'fedora.portatil'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
fedora.portatil	Current Load	OK	11-19-2013 21:08:17	1d 22h 6m 53s	1/4	OK - load average: 2.98, 1.92, 1.41
	Current Users	OK	11-19-2013 21:04:13	1d 22h 6m 15s	1/4	USERS OK - 2 users currently logged in
	PING	OK	11-19-2013 21:06:05	1d 22h 5m 0s	1/4	PING OK - Packet loss = 0%, RTA = 0.12 ms
	RAM disponible	OK	11-19-2013 21:07:01	0d 3h 12m 42s	1/4	CHECK_MEMORY OK - 1179M free
	Root Partition	OK	11-19-2013 21:07:57	1d 22h 4m 23s	1/4	DISK OK - free space: / 59018 MB (89% inode=96%):
	SSH	OK	11-19-2013 21:03:53	0d 3h 18m 30s	1/4	SSH OK - OpenSSH_6.3 (protocol 2.0)
	Swap Usage	OK	11-19-2013 21:05:35	1d 22h 3m 8s	1/4	SWAP OK - 100% free (7397 MB out of 7397 MB)
	Total Processes	OK	11-19-2013 21:03:45	1d 22h 2m 30s	1/4	PROCS OK: 191 processes with STATE = RSZDT

Results 1 - 8 of 8 Matching Services

Para el equipo con Windows se va a instalar un plugin que monitorice el tráfico de red. Dentro del paquete nagios-plugin, incluye un plugin check_nt se puede obtener información del tráfico de red, los valores que se obtienen son muy limitados y no permite obtener múltiples valores de tráfico de red de un equipo.

Hay un plugin denominado check_win_net_usage.sh que permite monitorizar diferentes valores del tráfico de red. Utiliza como base el plugin check_nt y permite aumentar sus funcionalidades, también se necesita el

cliente NSClient++ en el equipo Windows. Este plugin por defecto tiene configurado la ruta /usr/local/Nagios/libexec, se deberá modificar la ruta si no es correcta. Para realizar esta tareas, abrir el fichero con un editor, buscar el parámetro pluginlocation y especificar la ruta correcta (/usr/lib64/nagios/plugins).

Definir el comando en commands.cfg.

```
define command {
command_name check_win_net_usage
command_line $USER1$/check_win_net_usage.sh -H $HOSTADDRESS$ -i $ARG1$ -o KB $ARG2$
}
```

Define un objeto command con el nombre check_win_net_usage y especifica el comando con sus argumentos.

A continuación, definir el servicio en el fichero windows.cfg

```
define service{
use generic-service
host_name win-PC
service_description Trafico red
check_command check_win_net_usage!"Gigabit Ethernet Broadcom NetXtreme"
}
```

Debemos especificar la interfaz de red de la máquina de Windows que se va a monitorizar.

En la interfaz web de Nagios en el apartado Service, escogemos la máquina con Windows (win-PC), vemos el listado con los servicios monitorizados y veremos el servicio nuevo denominado Tráfico red.

View Service Status Detail For All Hosts

Service Status Details For Host 'win-PC'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
win-PC	C:\ Drive Space	OK	11-20-2013 13:12:51	0d 12h 5m 7s	1/3	c: - total: 297,99 Gb - used: 47,65 Gb (16%) - free 250,35 Gb (84%)
	CPU Load	OK	11-20-2013 13:13:49	0d 12h 1m 56s	1/3	CPU Load 12% (5 min average)
	Explorer	OK	11-20-2013 13:14:48	0d 12h 4m 0s	1/3	explorer.exe: Running
	Memory Usage	OK	11-20-2013 13:15:47	0d 12h 3m 4s	1/3	Memory usage: total:7675,09 Mb - used: 1589,67 Mb (21%) - free: 6085,
	NSClient++ Version	OK	11-20-2013 13:16:45	0d 12h 4m 8s	1/3	NSClient++ 0,4,1,102 2013-07-15
	Trafico red	OK	11-20-2013 13:21:09	0d 12h 5m 23s	1/3	Network OK - 224 KBytes received/sec, 0 KBytes sent/sec
	Uptime	OK	11-20-2013 13:20:43	0d 0h 41m 50s	1/3	System Uptime - 0 day(s) 1 hour(s) 43 minute(s)

Results 1 - 7 of 7 Matching Services

Generación de gráficas

Nagios no incluye la generación de gráficas por defecto y necesita algún programa externo para esa tarea. Hay múltiples herramientas que pueden ser integradas con Nagios, tenemos PNP4Nagios, Munin o Cacti.

En este caso, se ha escogido PNP4nagios que está muy bien integrado y es fácil de instalar, utiliza la librería rrdtool para generar datos para las gráficas. Para la instalación, utilizando el gestor de paquetes de la distribución de Linux (yum, apt-get) descargar el paquete PNP4Nagios y las dependencias que requiera. Con el paquete instalado y sus dependencias, toca configurar las gráficas que queremos ver.

PNP4Nagios obtiene los datos de los diferentes plugins instalados en Nagios y genera una serie de gráficas con esos datos. También podemos definir una serie de enlaces en Nagios para cada servicio y host monitorizado.

Para configurar PHP4Nagios.

–Modificar el parámetro del fichero /etc/default/npcd, run="yes".

–En el fichero /etc/nagios3/nagios.cfg establecer el parametro process_performance_data=1.

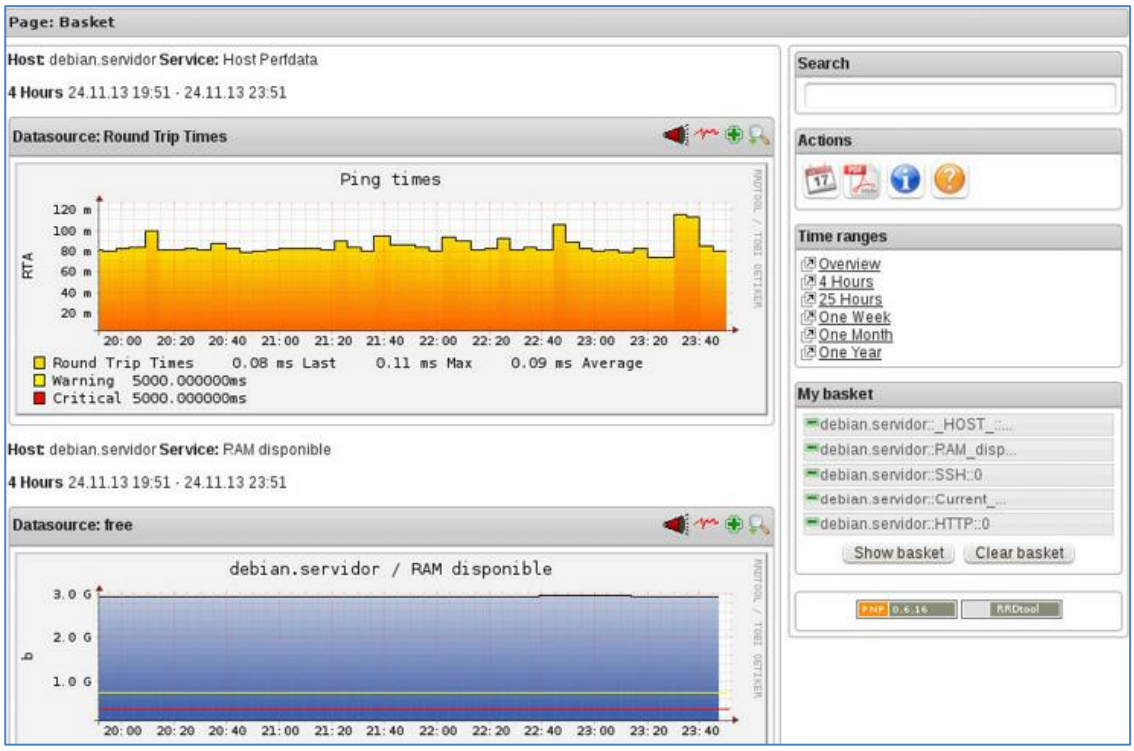
–Añadir broker_module=/usr/lib/pnp4nagios/npcdmod.o config_line=/etc/pnp4nagios/npcd.cfg

–Ejecutar servicio npcd start (requiere permisos de root).

–Reiniciar Nagios,service nagios3 restart.

Introducir en un navegador la siguiente URL.

http://direccion_ip_servidor_nagios/pnp4nagios



Para añadir un enlace en cada servicio y host desde la interfaz web de Nagios para tener acceso a las gráficas de forma más cómoda, debemos configurar una propiedad denominada action_url.

La forma más cómoda de configurar esa propiedad es a través de las plantillas que proporciona Nagios y no tener que configurar todos los hosts que tengamos monitorizados. La primera plantilla corresponde a la utilizada por los host (generic-host) que dependiendo de la distribución de Linux tiene diferentes rutas, en Debian /etc/nagios3/conf.d/generic-host_nagios2.cfg k y agregar:

action_url /pnp4nagios/graph?host=$HOSTNAME$&srv=$SERVICEDESC$

El resultado en la interfaz web de Nagios es un Nuevo icono en el apartado Host, cada máquina monitorizada tendrá su enlace a las gráficas.

La segunda plantilla corresponde a la plantilla para los servicios (generic-service), igual que para los host dependiendo de la distribución de Linux la ruta será diferente, en Debian /etc/nagios3/conf.d/generic-host_nagios2.cfg y añadir la siguiente línea:

action_url /pnp4nagios/graph?host=$HOSTNAME$&srv=$SERVICEDESC$

El resultado es parecido que para los Host, un Nuevo icono en cada servicio que enlaza a una gráfica del servicio.

Se ha visto un pequeño repaso sobre Nagios, diferentes configuraciones para monitorizar un par de equipos, evidentemente Nagios proporciona muchas más funcionalidades. Podíamos haber realizado la monitorización mediante SMNP, aunque la configuración puede resultar más compleja.
Mediante plugins se puede ampliar la funcionalidad de Nagios, permite integrarse con otro software visto anteriormente como HP Openview o Tivoli, también podemos almacenar los datos en una base de datos, con NDOUtils se pueden almacenar en MySQL.
Nagios puede resultar difícil de configurar, para ayudar en la configuración existen diversos programas como Lilac, NagiosQL o Centreon que permiten realizar la configuración de forma más fácil.
Por último, recordar que Nagios es software libre con licencia GPLv2.

2.4. Supervisión red comunicaciones: tipos de incidencias, herramientas de notificación y alarmas

La supervisión y mantenimiento de una red de comunicaciones debe incluir la capacidad de determinar los parámetros de conexión y configuración de los elementos de la red, incluyendo la capacidad para supervisar características de funcionamiento de los elementos de la red para reconocer averías dentro de la red de comunicaciones.
Cuando se produce un error en la red debe seguirse una serie de procedimientos en función del tipo de error, se debe registrar todo el proceso por el técnico desde que se produce el error hasta que se solucione.
Es muy importante tener bien definido todo el proceso de reparación, aunque debe permitirse cierta flexibilidad en el procedimiento, y estar bien documentado.
La supervisión de la red debe realizarse de forma no intrusiva, que no afecte al correcto funcionamiento de la red y no afecte a los usuarios. Esta supervisión puede realizarse de forma "manual" mediante una serie de revisiones por parte de los técnicos de los diferentes elementos de la red, o de forma automática mediante herramientas de monitorización, como Nagios que hemos visto anteriormente. También se puede realizarse una combinación de ambos tipos, una serie de revisiones por medio de técnicos y mediante una herramienta de monitorización.
Esta última opción es la más recomendable y la más eficiente, aunque tiene unos costes más altos.

Tipo de Incidencias

Una red de comunicaciones proporciona una serie de servicios a distintos usuarios, el correcto funcionamiento de estos servicios es primordial y cualquier anomalía que se produzca en un servicio produce molestia a los usuarios. El objetivo del personal encargado en la administración de una red es el correcto funcionamiento y si se produce un error que sea solucionado lo antes posible, perjudicando lo menos posible a los usuarios.
Cuando se produce algún error, es generada una incidencia donde se almacena información del error, también denominado parte de incidencia, como puede ser: descripción del error, lugar, usuario (si lo ha generado algún usuario), causas, etc.
Tipos de incidencias:
–Incidencias físicas.
–Incidencias de red.
–Incidencias de usuarios.
–Incidencias de servicios.
–Incidencias ambientales.
–Incidencias de seguridad.
Cada incidencia engloba un conjunto de errores y existen varios tipos.

Incidencias físicas

Este tipo de incidencia se generan por errores que se producen en componentes de hardware como pueden ser:
–Elementos de un computador como: CPU, Discos duros, Monitor, memoria RAM, etc.
–Dispositivos de red como router, switch, Gateway, etc.
–Medios de transmisión (cables).
Los síntomas para este tipo de incidencias pueden ser: pérdidas de rendimiento en un servicio, corte de conexión o de servicios.

Generalmente, para solucionar la incidencia se reemplaza el dispositivo o componente dañado porque en muchos casos el dispositivo no se puede reparar o el coste de la reparación es muy alto.
Para evitar los problemas que surgen con este tipo de incidencias, se incluye redundancia en aquellos dispositivos, que por su importancia en la red, no pueden dejar de funcionar.
Incidencias de red
Este tipo de incidencias se asocian al funcionamiento de la red y no se incluyen los fallos físicos. Se incluyen diversos errores como:
–Pérdidas de la señal de comunicación.
–Pérdidas de rendimientos en servicios de red.
–Baja velocidad de transmisión.
–Retardo en la comunicación.
Las incidencias generadas afectan a software de la red y hay disponibles herramientas software para comprobar diversos parámetros de la red. Las posibles soluciones para este tipo de incidencias pueden ser:
–Cambios en la configuración: la incidencia se ha generado por una mala configuración de software, modificando a una configuración óptima la incidencia se debe resolver.
–Actualizaciones de software: algunos errores que se producen se pueden solucionar realizando actualizaciones que mejoran tanto en seguridad (arreglos de bugs, vulnerabilidades, etc.) como en rendimientos el software. También se deben instalar los parches que proporcionan los fabricantes.

Incidencias de usuarios

Este tipo de incidencia afectan a los usuarios utilizando los servicios que proporcionan, tanto como errores que sufren los usuarios como ayuda para el manejo de un servicio. Las incidencias que se generan no son exclusivamente fallos o errores, también pueden incluir ayuda para configuraciones o dudas sobre el uso de servicios. Se pueden generar incidencias para determinadas situaciones como por ejemplo:
–Configuraciones: un usuario necesita ayuda para realiza una determinada configuración de un servicios.
–Averías: fallo que se produce en la red o un servicio que afecta al usuario.
–Peticiones de ayuda: cuando un usuario no sabe realizar una determinada tarea o tienes algún tipo de duda sobre el servicio.
–Mal uso de servicios: determinados usuarios abusan o utilizan de forma inadecuada un servicio de la red.
Las causas de este tipo de incidencia son muy muchas, pueden derivar a otro tipo de incidencia, y se debe obtener la máxima información posible del usuario que ha generado la incidencia, esta información será muy útil para conocer las causas del error y encontrar la mejor solución.

Incidencias de servicio

Están asociados al mal funcionamiento de los servicios que proporciona la red, dependiendo del servicio los errores que pueden surgir son diferentes. Podemos considerar de forma general los siguientes errores:
–Cortes de servicios.
–Pérdidas de rendimiento.
–Baja velocidad del servicio.
Dependiendo del servicio hay disponibles diversas herramientas que ayudan a encontrar los errores que han generado la incidencia. Las posibles soluciones son muy diversas, dependiendo del servicio, pero podemos implementar redundancia en los servicios, aunque el coste puede ser alto.

Incidencias ambientales

Este tipo de incidencia se asocia a factores ambientales que pueden influir en el rendimiento de la red. Los errores que pueden producirse son:
–Inundaciones.
–Fuego.
–Altas temperaturas.
Este tipo de incidencias afectan a los dispositivos hardware y para evitarlos hay soluciones como: controlar la temperatura con sistemas de climatización, habitaciones ignífugas o sistemas de extinción para el fuego.
El factor ambiental que más produce son las altas temperaturas porque afectan a todos los dispositivos hardware y dependiendo del hardware, tendrá un umbral máximo de temperatura. La mayoría del hardware permite monitorizar la temperatura y controlarla mediante sistemas de refrigeración externos

(aire acondicionado) o incluidos en el hardware, existen desde ventiladores, de diversos tamaños y potencia, hasta sistemas de refrigeración por agua.

Incidencias de seguridad

Las incidencias de este tipo son generadas cuando surgen fallos de seguridad, podemos considerar los siguientes errores:
–Accesos no autorizados: aprovechándose de vulnerabilidades en el software o por medio de otras técnicas (ingeniería social, phishing, etc.).
–Programas maliciosos como virus, troyanos, gusanos, etc.
–Intrusiones externas, un atacante desde fuera de la red tiene control sobre dispositivos de la red.
–Acceso físico no autorizado: una persona no autorizada accede a sitios importantes para la red, como por ejemplo acceder al lugar donde se encuentran los servidores de una red.
Para evitar este tipo de incidencias se puede realizar las siguientes tareas:
–Instalación de software de seguridad: como cortafuegos, antivirus, IDS, etc.
–Permisos de usuarios: definir un conjunto de permisos que asigna una serie de privilegios, que serán asignado a los usuarios de la red.
–Política de contraseña: Cualquier contraseña utilizada en el red debe ser robusta y se debe obligar a utilizar contraseñas que cumplan ciertos requisitos como:
·Longitud adecuada: debe evitar contraseñas de poca longitud porque pueden ser descubiertas mediante técnicas de “fuerza bruta”.
·Aleatoria: que no incluya información que pueda descubrirse fácilmente (cumpleaños, nombres, etc.) y debe utilizar diversos caracteres (números, letras y símbolos) tanto en mayúsculas como minúsculas.
Control de acceso físico: Hay determinados sitios que se debe vigilar el acceso de personas, para ello se deben implementar diferentes métodos de acceso como: tarjetas, cámaras o sistemas biométricos para impedir el acceso a personal no autorizado. Estos sitios albergan sistemas que debido a su importancia deben ser controlados.
Cuando se produce una incidencia y se asigna un administrador u operador, puede tener asignada una prioridad que indica su gravedad y la rapidez con que debe ser resuelta, porque afecta al funcionamiento de la red de forma muy negativa.
La prioridad se divide en diferentes categorías en función de la importancia, mayor gravedad a menor gravedad, tenemos:

- ⇨ Critico: Define una pérdida total de un servicio o recurso, tiene una prioridad máxima y debe ser solucionado en un corto periodo de tiempo, disponiendo de todos los recursos disponibles y el tiempo que sea necesario para resolver la incidencia.
- ⇨ Mayor: Define un error grave que afecta de forma parcial a un recurso o servicio, aunque no supone un corte total en el funcionamiento, afecta de forma considerable el rendimiento. La prioridad que se le asigna es menor y debe ser notificado de forma inmediata. Este tipo de incidente debe estar vigilado de forma constante para que la incidencia no suba de nivel y resolverlo lo antes posible. Se le asignan recursos de forma exclusiva pero por un tiempo limitado
- ⇨ Medio: Define un error que no implica mucha gravedad, pero si no es resuelto a medio plazo puede serlo. El peligro de este tipo de incidencia es su “potencial de peligrosidad” sino es resuelto a medio plazo. No se le asignan recursos de forma exclusiva pero tiene los recursos necesarios para resolverlos.
- ⇨ Bajo: Define un error que no afecta de forma sustancial a los recursos o servicios de una red. Tienen una prioridad baja y se resolverá cuando hay recursos libres.

Pueden existir otras categorías, esto depende de la operativa de la empresa.

Herramientas de notificación y alarmas

Cuando se produce un error en la red, debe generarse una incidencia para que el personal correspondiente pueda resolver el error que se ha producido lo antes posible.
Para facilitar el trabajo de generación de una incidencia, hay disponible una serie de herramientas de notificación y alarmas, el proceso que genera este tipo de herramientas puede ser resumido:
Error > Alarma > Notificación > Incidencia

En este tipo de herramientas el administrador configura una serie de alarmas asignadas a un recuso o servicio de la red, con una serie de valores umbrales. Cuando un valor umbral es sobrepasado activa una alarma que genera una notificación y es enviada al administrador u otro personal que corresponda. La notificación es enviada por un canal de comunicación (email, SMS, sistema de mensajería u otro canal) que previamente ha sido configurado, la notificación incluye información especifica de la alarma que ha sido activada.

Este tipo de herramientas son imprescindible para una correcta gestión de una red y conlleva una serie de ventajas:

–Acelera la resolución de problemas: Los errores se detectan de forma muy rápida, en el momento que ocurren, y al disponer de toda la información necesaria, el tiempo de resolución es menor.

–Minimiza el tiempo de caída o pérdida de rendimiento: Si los errores son detectados rápidamente y el tiempo para resolver la avería es menor. Como consecuencia el impacto que se produce en la red es mínimo.

–Menor utilización del soporte: La herramientas de notificación y alarmas permiten prevenir posibles errores graves, reduciendo las pérdidas de servicio y de rendimiento en la red. Influyendo en el uso del soporte técnico que disminuye.

–Mejora la disponibilidad de la red: Si la red tiene menos errores o estos errores no afectan de forma significativa al rendimiento de la red, el tiempo de disponibilidad de los servicios y recursos de la red será mayor.

–Aumento de la capacidad de respuesta: las alarmas y notificaciones permiten conocer lo antes posible un error en la error y actuar de forma rápida en la resolución. Esto consigue un tiempo de respuesta menor.

–Prevención de errores: Este tipo de herramientas permiten actuar en una incidencia antes de que se convierte en un error grave cuyas consecuencias en la red sean mayores. También nos permite detectar anomalías en la red, actuando antes de que se conviertan en un problema más grave.

–Reducción de costes: Tanto en coste de horas de trabajo del personal técnico, como de recursos.

–Mejor información: Las herramientas de notificación y alarmas generan información del error, ahorrando tiempo al personal técnico que podrá encontrar antes las causas del error y tardará menos tiempo en encontrar una solución.

Cuando es generada una incidencia, el administrador debe analizar la información disponible y comprobar qué tipo de anomalía se ha producido.

El administrador debe ejecutar una serie de pruebas para confirmar el tipo de incidencia, puede ejecutar un tipo de pruebas específico para ese tipo, si el administrador conoce el tipo de incidencia. En caso contrario, ejecutara un conjunto de pruebas mas genérico.

Si es confirmado el tipo de incidencia, el administrador podrá descubrir de forma más fácil las causas de la incidencia y encontrar una solución de forma más eficiente.

Podemos distinguir varias tipos de pruebas:

–Pruebas de conectividad física: Verifican que los medios de transmisión funcionan correctamente. En algunos casos, el error es producido por fallos en los medios de transmisión, como rotura de cables o fallo en los conectores. Un fallo en el medio de transmisión provoca que un elemento de la red no funcione correctamente y puede parecer que el error ha sido producido en el elemento de red. Para realizar este tipo de pruebas se utilizan herramientas como Tester de cables para comprobar diferentes tipos de cables.

–Pruebas de conectividad lógica: Se encargan de verificar la comunicación entre los elementos de red a nivel de software. Descartado el error de los medios de transmisión, debemos comprobar si la comunicación se realiza de forma correcta, analizando diversos parámetros de comunicación y comprobando que los valores obtenidos son los esperados. Hay múltiples herramientas que verifican la comunicación como: ping, traceroute o dig.

–Prueba de rendimiento: Comprueban que el funcionamiento es acorde a lo esperado, realizando varias medidas de diversos parámetros y analizando los valores obtenidos podemos conocer el rendimiento de la red, verificando si es el rendimiento óptimo o no. Las pruebas de rendimiento pueden ser ejecutadas por los servicios que proporciona la red, elementos hardware (CPU, RAM), medios de transmisión, etc. Este tipo de pruebas también pueden ser ejecutadas para comprobar la capacidad de procesamiento de un dispositivo y para conocer cuál es su umbral máximo de funcionamiento.

–Pruebas de seguridad: Verifican la seguridad de la red, comprueban que no se han producido accesos no autorizados u otros errores de seguridad, también comprueban la vulnerabilidad del sistema y los dispositivos de la red. Es importante realizar este tipo de prueba periódicamente.
Toda las pruebas son aconsejables realizarlas de forma periódica, incluso tener un calendario de pruebas, para prevenir errores. Para cada incidencia debe ejecutarse una prueba, por ejemplo si hay problemas de conexión de red ejecutar una prueba de conectividad física sería la primera opción, si la prueba no da resultado se ejecutarían otro tipos de pruebas. En algunos casos, es difícil identificar el error y dependerá del técnico o administrador de red que tipo de pruebas ejecutar.
Una herramienta de notificación y alarmas debe contener una serie de características que deben tener en cuenta a la hora de implementar una herramienta de este tipo en una red.
–Integración con herramientas especificas de seguridad y detección de vulnerabilidades.
–Alarmas basadas en valores umbrales.
–Reenvío de alarmas a otros sistemas.
–Posibilidad de realizar análisis para identificar las causas de un error.
Otras características que deben ser tenidas en cuenta, aunque son comunes con otras herramientas, es que tiene una curva de aprendizaje baja (fácil de usar), esto implica un nivel alto de usabilidad. También es aconsejable que sea modular para poder ampliar sus capacidades fácilmente.
Este tipo de herramientas envían información por la red, tanto para monitorizar las alarmas configuradas como en el envío de notificaciones, es conveniente que no genere mucho tráfico para no saturar la red.
Las herramientas para gestionar alarmas y notificaciones están integradas en herramientas de monitorización que controlan los servicios y recursos de una red, también se denominan herramientas de gestión.
Una alarma se asigna a un recurso o servicio y es configurada en el equipo donde se encuentra la herramienta de gestión (servidor). Se configurarán las alarmas con una serie de valores umbrales, si un valor umbral es superado se activará una alarma. Cada alarma tendrá configurada una notificación, cuando una alarma es activada la notificación será enviada, la notificación podrá tener diferentes canales de comunicación en función de la alarma. Por ejemplo, para las alarmas que se activen cuando se produce un error grave, se envía una notificación por SMS y correo electrónico al administrador, pero si se activa una alarma de un error menos grave se envía un mensaje por el sistema de mensajería interna.
Mediante un software denominado agente, que es utilizado por la herramienta de gestión para monitorizar dispositivos, crea una comunicación entre el servidor y los agentes que comprobarán de forma periódica si alguna alarma ha sido activada.
Anteriormente se han visto diversas herramientas de monitorización (Nagios, Zabbix o Pandora FMS), y como ejemplo se ha visto la configuración de Nagios.
Nagios monitoriza dispositivos (host) o un servicio (service) y crea alarmas para cada uno de ellos. Cada servicio o host es determinado por dos componentes:
–El estado del servicio o host: OK, Warning, Critical, etc.
–El tipo de estado: Soft o Hard.
Nagios chequea un service o host un número determinado de veces (4 por defecto) antes de considerar que se ha producido un error, de esta forma se evitan los falsos positivos. Dependiendo en qué número de reintento se encuentra el chequeo el servicio puede estar en estado soft o hard.
–SOFT: es producido cuando el chequeo de un servicio o host nos devuelve un “non-OK” pero aún no ha sido (re)chequeado el número de veces que ha sido configurado.
–HARD: es producido cuando el chequeo de un servicio o host es un “non-OK” y ya ha sido (re)chequeado el número de veces configurado.
Para las notificaciones debemos especificar qué mecanismo utilizar, habitualmente se utiliza el email pero también se puede utilizar SMS o mensajería instantánea.
Para las notificaciones por email, lo primero será configurar los contactos que pueden recibir las notificaciones y los datos necesarios, como el email. Crear un objeto de Nagios contacto o grupo de contacto para definirlo en Nagios.
Otro requisito para las notificaciones por email es la instalación y configuración de un servidor de correo, como sendmail o postfix, esto puede resultar más complejo dependiendo de la configuración de la red.

Por último, especificar qué servicios o parámetros monitorizados enviarán una notificación, cuándo se debe enviar y a quién.

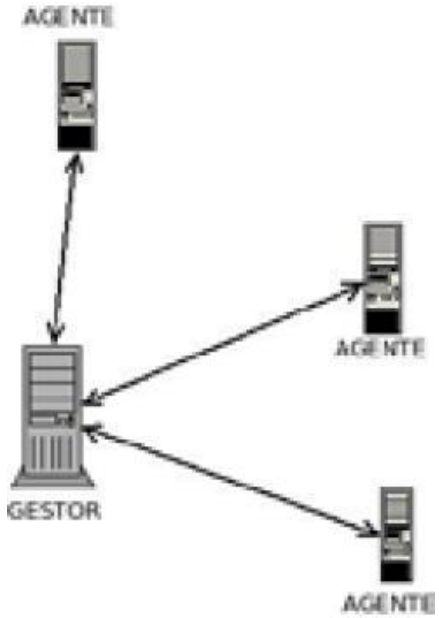
2.5. Gestión centralizada y distribuida

Anteriormente se han visto las herramientas de gestión, como Nagios, pero debe decidirse cómo funcionan dentro de la red, qué tipo de instalación se realiza.
Hay dos tipos, en función de la configuración utilizada para la gestión:

Gestión centralizada

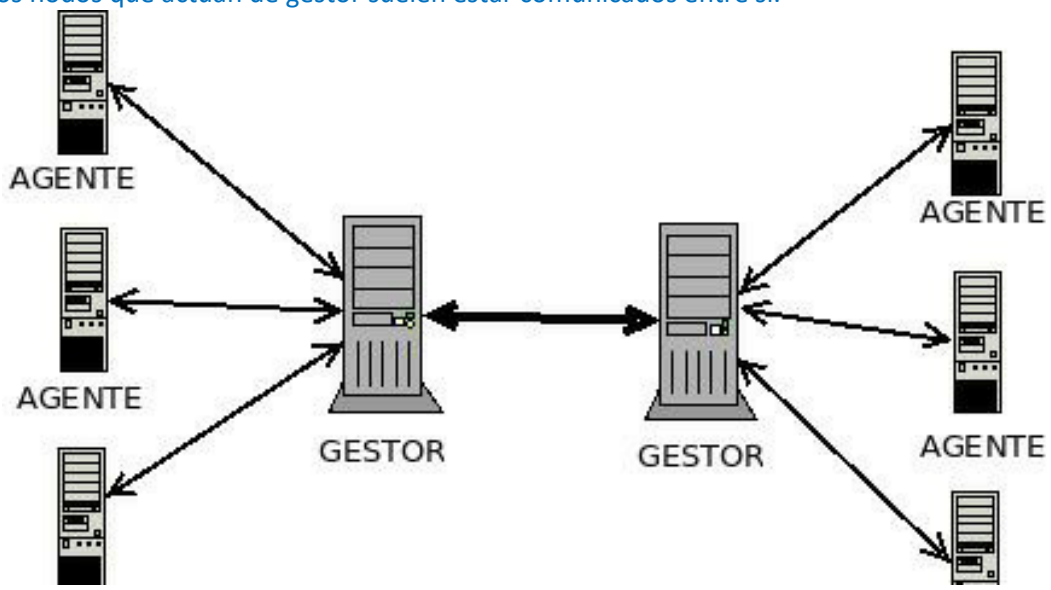
Un **nodo central (gestor) monitoriza un conjunto de clientes** por medio de agentes que recompila información de diversos parámetros del cliente y la envían al gestor, también el gestor puede solicitar información a los agentes.

Las herramientas de gestión que implementan esta tipo de esquema, son más fáciles de configurar, solo hay un nodo gestor y un conjunto de agentes. Esto implica que el mantenimiento es más simple que otros esquemas, otra ventaja es el coste debido a esta simplicidad en este esquema.
Como desventajas tenemos:
–Fallo en el gestor: si falla el nodo gestor la herramienta de gestión deja de funcionar, este esquema tiene como punto débil la disponibilidad de un solo nodo.
–Recursos: si el conjunto de agentes es muy grande, el nodo gestor puede llegar a sufrir saturación en su funcionamiento.
–Escalabilidad: si aumentan los agentes que monitoriza el gestor y como solo hay un nodo central disponible, para aumentar la capacidad del gestor es aumentando la potencia del hardware. Con el esquema centralizado no se pueden añadir más nodos gestores.
Para infraestructuras de tamaño pequeño/medio este tipo de esquema puede ser muy útil, la configuración y el mantenimiento es más simple que en el esquema distribuido, siempre que el número de agentes y la información de gestión que maneja no sea muy elevada.

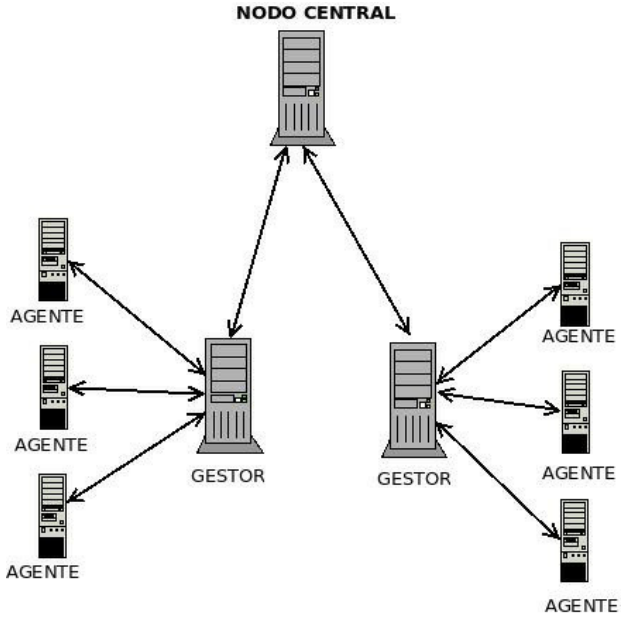


Gestión distribuida

Un conjunto de nodos realizan las tareas de gestión actuando como gestores, cada nodo puede estar encargado de un conjunto de agentes, otra opción es que cada nodo se encarga de determinadas tareas de gestión. Los nodos que actúan de gestor suelen estar comunicados entre sí.



La red es gestionada por un conjunto de nodos gestores, esto proporciona mas disponibilidad, si un nodo gestor falla, el resto de nodos gestor siguen funcionando y monitorizando la red. El resto de nodos gestores pueden monitorizar los agentes del nodo caído.



Las herramientas de gestión que utilizan un esquema de gestión distribuida proporcionan más fiabilidad en la gestión, un fallo en un gestor no implica que la herramienta deje de monitorizar.
Como desventajas tenemos:
–Configuración más compleja, hay disponibles un conjunto de gestores que deben comunicarse entre ellos para saber cuando un gestor ha fallado.
–Recursos altos, existen varios nodos gestores que necesitan un requerimiento hardware altos.
–Mantenimiento más complejos, deben controlar varios nodos gestores.
La gestión distribuida es utilizada en grandes infraestructura de red donde hay disponibles un conjunto de dispositivos muy elevado a monitorizar. Este tipo de infraestructuras tienen una organización compleja donde un esquema distribuido facilita la monitorización de los recursos de la red.
Una variación de la gestión distribuida es recoger información de los nodos gestores a un nodo central, este esquema denominado gestión mixta, facilita la monitorización de todos los gestores, también permite gestionar las configuración de cada uno de los gestores de forma más fácil.
Este nodo central almacena la configuración de cada nodo gestor y en caso de fallo en el nodo gestor, como un fallo de hardware. Después de la reparación del nodo gestor, desde el nodo central importar la configuración del gestor, ahorrando mucho tiempo en la configuración.
Este tipo esquema es utilizado los CGR, centro de gestión de red, donde de forma centralizada poder monitorizar todos los nodos gestores y los agentes que incluyen.

2.6. Sistemas de gestión en operadores de telecomunicación

Una operadora de telecomunicación dispone de una red extensa con múltiples dispositivos que están incluidas en varias subredes. Toda la gestión está centralizada en uno a varios CGR, centro de gestión de redes, donde un equipo de personas con diversas funciones se encargan de realizar la gestión de la infraestructura de la operadora.
Una operadora de telecomunicación puede estar compuesta de diversas redes con diferentes tecnologías, dependiendo de los servicios que proporciona y entre las que podemos destacar:
–Internet: proporciona acceso a internet a sus clientes, utilizan protocolos propios de internet como TCP/IP o DNS.
–Teléfono: proporciona acceso a llamadas de teléfono entre los clientes, tanto de forma analógica como digital, mediante VoIP, en este caso los protocolos utilizados para internet.

–Móvil: proporciona a los clientes servicios de telefonía móvil tanto de voz como de datos. Existen diversos tipos de redes que se diferencian en la velocidad de envío de datos y poder acceder a Internet desde el móvil, entre las redes más usadas para los datos.
–GRPS.
–3G.
–4G.
–LTE.
Algunas operadoras proporcionan servicios de televisión, pero normalmente se ofrecen a través de Internet utilizando los protocolos TCP/IP.
Aunque una operadora de telecomunicación ofrece diversos servicios con diferentes tecnologías y dispone de diferentes redes, en la actualidad estos servicios están convergiendo a servicios digitales que utilizan protocolos como TCP/IP. Un ejemplo, es ofrecer servicios de telefonía por VoIP en vez de utilizar la telefonía "clásica" analógica.
Las operadoras de telecomunicaciones disponen de uno, o varios, CGR donde utilizan diversas herramientas de gestión, estas herramientas deben tener en cuenta la infraestructura de la operadora, entre los aspectos que debe ser tenidos en cuenta son:
–Tipo de red: dependiendo de la red; telefónica, móvil o Internet, la gestión y los parámetros a monitorizar son diferentes.
–Componentes físicos: cada tipo de red puede utilizar diversos componentes como: fibra óptica, cable coaxial o par trenzado. Cada unos de ellos utiliza dispositivos específicos como router, switch o cable-módem.
–Protocolos: cada red y tecnologías empleadas utilizan una serie de protocolos. Hay que tener en cuenta esto para realizar una correcta monitorización de la infraestructura.
No es lo mismo monitorizar una red de una pequeña empresa con unas decenas de dispositivos, que una infraestructura de un operadora de telecomunicaciones con miles o cientos de miles de dispositivos. Los factores que se deben tener en cuenta para el correcto funcionamiento del la infraestructura son:
Infraestructura de operadora de telecomunicaciones: disponibilidad, rendimiento, escalabilidad y seguridad.
Estos factores expuestos, deben ser cumplidos en la red de la operadora con el mayor grado posible, estos factores no pueden cumplirse al cien por cien. Una correcta gestión de la red ayudará a cumplir mayormente estos factores.
Una explicación más detallada se muestra a continuación.
–Disponibilidad: la red de un operador debe estar siempre en funcionamiento (siempre disponible), cualquier caída en el funcionamiento afecta de forma negativa, como pérdida de clientes y bajada en los ingresos económicos de la operadora. La disponibilidad muestra el tiempo de funcionamiento entre caída, generalmente este dato se muestra como un porcentaje de tiempo en funcionamiento.
–Rendimiento: un operador proporciona una serie de servicios a un sus clientes, estos servicios deben funcionar de forma correcta y cumpliendo con las condiciones que el cliente a contratado. Es muy importante que la red de la operadora y los servicios tengan un funcionamiento óptimo, consiguiendo que los clientes estén satisfechos.
–Escalabilidad: cuando un servicio recibe una carga de trabajo elevada de forma inesperada, el servicio debe ser capaz de soportar esa carga y si con los recursos disponibles no puede soportar esa carga, que sea más fácil añadir recursos al servicio sin que sufra pérdida de rendimiento. La escalabilidad mide el grado de adaptación de un servicio a un aumento de carga de trabajo. Un servicio poco escalable implica que un aumento en la carga de trabajo sufre una pérdida de rendimiento, incluso una caída.
–Seguridad: los servicios y la red de un operador debe ser segura para sus clientes, no sufrir ataques externos que afecten al rendimiento y a los datos de los clientes. Una correcta gestión puede detectar posibles ataques y tomar acciones necesarias para evitar un mayor daño.
Una operadora de telecomunicaciones necesitará un conjunto de herramientas de gestión que monitorizan las diferentes redes que posea, esto depende de los servicios que ofrezca. Entre las redes que puede monitorizar están.
–Red telefónica: el operador puede ofrecer Internet, mediante diversas tecnologías como ADSL, RDSI o FFTH, y utilizando diferentes medios de transmisión como fibra óptica, cable coaxial o par trenzado.
También ofrece servicio de telefonía, tanto analógica (red telefónica conmutada) como digital (VoIP).

–Red móvil: el operador ofrece servicios de telefonía móvil, mediante diversas tecnologías, el servicio distingue dos categorías:
·Servicio de Voz.
·Servicio de datos.
–Televisión: el operador ofrece servicios de Televisión mediante distintas tecnologías (cable o satélite), otro servicios que puede proporciona es video bajo demanda, aunque habitualmente se utiliza Internet para ofreces este servicio.
Cada red utiliza herramientas de gestión específicas, en apartados anteriores se ha visto distintas herramientas de gestión que son utilizadas para gestionar servicios de acceso a Internet (ADSL, vídeo bajo demanda o VoIP), entre las herramientas que se han descrito tenemos:
–Nagios.
–Cisco Prime.
–HP IMC
Los servicios de telefonía "clásica" utilizan comunicación analógica, por ese motivo no existen herramientas de gestión como en el caso de la comunicación digital. La gestión de este tipo de servicios se realiza principalmente en las propias centrales telefónicas, donde los técnicos utilizando una serie de herramientas específicas para comprueban el estado de la señal telefónica.
Con el cambio progresivo en la red telefónica del par trenzado por otros medios de transmisión como la fibra óptica, que implica el cambio a una comunicación digital. Esto provocará un cambio en la gestión de las redes y la disponibilidad de múltiples herramientas.
Hay diferentes arquitecturas de redes móviles con sus propias tecnologías y servicios. A lo largo del tiempo, los servicios y las tecnologías han ido evolucionando en las redes móviles, esta evolución es descrita mediante diversas generaciones, actualmente está implementándose la cuarta generación 4G.
Las generaciones son las siguientes:
1º -> Analógica
2º -> Digital: GSM, GRPS, EGDE
3º -> Digital: WCDMA, UMTS
3.5º -> UMTS/HSPA/HSPA
4º -> LTE, LTE advanced
Los servicios que proporciona cada una de las generaciones, principalmente son voz y datos, aunque algunas generaciones permiten ofrecer otro tipo como televisión. En cada generación la velocidad de transmisión aumenta considerablemente, en 4G permite una velocidad de 150 megabits por segundo.
En las redes móviles, los sistemas de gestión deben monitorizar un conjunto de dispositivos tanto para la transmisión de voz como los datos, entre los dispositivos tenemos:
–Equipos de acceso al servicio.
–Enrutadores.
–Conmutadores.
–Equipos de transmisión.
Para dispositivos móviles, existe una categoría de software que permite administrar y monitorizar este tipo de dispositivos denominados Administradores de dispositivos móviles, en inglés Mobile Device Management (MDM). Este tipo de software es utilizado principalmente por grandes empresas para sus redes privadas.
Los sistemas de gestión utilizados en los operadores se dividen en dos partes:
–Hardware: equipos que monitorizan diversos parámetros de la red.
–Software: aplicaciones instaladas en el centro de gestión de red de la operadora.
Hay diversas empresas que proporcionan este tipo de sistemas, tanto hardware como software, entre las que podemos encontrar:
–HP.
–Cisco.
–Siemens.
–NEC.
–Alcatel-Lucent.
–Ericsson.

En las grandes operadoras suele ser habitual, tener un sistema de gestión propio, desarrollado por la propia operadora o por una empresa externa con las especificaciones de la operadora. Esto es debido a que sus redes son muy extensas y complejas, con un sistema propio es más fácil implementar las particularidades de sus redes que utilizando un sistema comercial que será más complejo realizar una adaptación y posiblemente más caro, porque debería ser personalizado para adaptarlo a sus redes.
Para la gestión utilizan protocolos específicos para telecomunicaciones, como TMN u otros protocolos propietarios. Otros protocolos como SNMP se utilizan para los servicios que utilizan el protocolo IP como VoIP, ADSL, Vídeo bajo demanda, etc.

2.7. Los procesos de detección y diagnósticos de incidencias: herramientas específicas

En una empresa que dispongan de una red propia u ofrecen servicios en una red pública, como Internet, surgen diversos incidentes en el funcionamiento de la red, entre las cuales podemos considerar.
–Fallos de hardware/software.
–Fallos de seguridad.
–Anomalías en la red.
–Bajadas de rendimiento.
Cualquier incidente que implique un mal funcionamiento de la red, puede ser considerado como una incidencia.
Cuando surge en la red una incidencia se debe reportar y enviarla al personal que administra la red, esta incidencia debe contener información sobre ella, esta información será muy útil para diagnosticar la causa de la incidencia y resolverla.
Hay software que ayuda en el proceso de generar la incidencia y el posterior seguimiento, este tipo de software asigna una serie de estados a la incidencia en función del estado de resolución.
Cuando es generada una incidencia se desarrolla todo un proceso, incluso empieza antes de la generación y que finaliza con la resolución de la incidencia. Estos pasos se pueden resumir en:
–Detección.
–Generación.
–Resolución.
Cada paso del proceso puede ser dividido en varias tareas.
En el apartado 2.1 de este módulo se explica con más detalle las incidencias y el proceso de generación.

Detección

Para generar una incidencia antes ha surgido un suceso que la ha provocado, este incidente debe ser detectado, hay varias formas de detección:
–Detección por usuario: un usuario o cliente de la red, informa de un incidente al personal de soporte técnico y otro personal técnico.
–Detección por software: algún software que monitoriza la red detecta el incidente y envía información al personal correspondiente.
–Detección por hardware: algunos dispositivos de la red pueden detectar incidente en su propio funcionamiento o en el funcionamiento de la red, recopilando información del incidente y enviándola.
Deben existir diversas maneras de enviar la información del incidente, asegurando que siempre habrá un canal disponible para el envío de la información, entre los canales más utilizados son:
–Teléfono.
–SMS.
–Correo electrónico.
–Mensajería.
–Redes sociales.
Dependiendo del incidente, la información puede ser recibida por personal de soporte técnico, operadores de red o administradores dependiendo de la operativa utilizada en la empresa.
Es muy importante recopilar información sobre el suceso antes de generar la incidencia, esta información será incluida en la incidencia será de mucha utilidad para su resolución, entre las diferentes formas:
–Usuarios o clientes: en este caso la información obtenida no será muy técnica, generalmente será una descripción del incidente y las consecuencias en el funcionamiento. En ocasiones los usuarios son los

primeros en detectar el incidente y su información permitirá tomar medidas de forma rápida para resolución.

–Ficheros log: El funcionamiento del software y todas las acciones que han ocurrido son almacenadas en log que registra todo los eventos producidos. Cualquier sistema operativo tiene un conjunto de log y mucho software proporciona su propio log. La información proporcionada por un log puede ser muy técnica y en un formato poco legible, necesitando una conversión a un formato más legible.
–Monitorización: las herramientas de monitorización configuradas para alertar cuando detectan diversos eventos en la red, enviando información del evento que ha activado la alerta. Este tipo de información es técnica y legible.

Generación
Con la información recopilada del incidente, el siguiente paso es generar una incidencia, que debe ser rellenada por personal cualificado, esta tarea suele ser asignada:
–Personal de soporte.
–Operadores de red.
–Administradores.
En el sistema es muy habitual que los clientes no tengan permisos para rellenar una incidencia, aunque como se ha visto anteriormente si pueden notificarlas.
La estructura de una incidencia depende mucho de la empresa, aunque hay una serie de campos que podemos considerar imprescindibles. Una incidencia debe tener cierta información para cumplir con su objetivo, debemos tener el cuenta ciertos parámetros.

- ⇨ Identificador: Cada incidencia debe tener algún código que la identifica.
- ⇨ Asignación: Una incidencia debe ser asignada, por ejemplo a un técnico, quien es el encargado de la resolución.
- ⇨ Estado: Cada incidencia se le asigna un estado que servirá para realizar un seguimiento de la incidencia, los estados asignados dependerá de la operativa que se utiliza en la empresa.
- ⇨ Descripción: Información adicional sobre el incidente para ayudar en la resolución

Estos campos son considerados imprescindibles en toda incidencia, otra información que puede ser incluida como;
–Prioridad.
–Fecha límite para resolverla.
–Tipo.
–Fecha y hora.
–Lugar donde se ha producido.
–Nombre de la persona que ha rellenado la incidencia o escalado de una incidencia.
El escalado de una incidencia consiste en trasladar una incidencia a otro departamento, generalmente con personal especializado, esto depende del tipo de incidencia que se ha generado y la dificultad de esta.

Resolución
Una incidencia ha sido generada con información de un incidente que se ha producido, el siguiente paso sería resolver la incidencia con ayuda de la información que ha sido proporcionada y el conjunto de recursos asignados.
Dentro de un operador de telecomunicaciones las incidencias suelen ser generadas por el personal de soporte técnico que intentan resolverlas y en caso contrario derivarla a otro departamento, esto depende de la operativa utilizada por el operador.
Para resolver una incidencia son necesarios una serie de recursos, entre los que consideramos.
–Información: que está incluida en la incidencia generada.
–Personal: tipo de personal y cuanto personal es necesario para la resolución.
–Hardware: para la resolución de una incidencia es necesario el cambio de algún dispositivo hardware.
–Software: para resolución de determinadas incidencias es necesario la instalación o actualización de software.

Los recursos en cualquier empresa son limitados y deben ser utilizados de forma eficiente, por este motivo las incidencias suelen incluir un campo de prioridad donde en función de la prioridad asignada indica la importancia de la incidencia y rapidez que debe ser resuelta.
El campo de prioridad es definido con diversos grados, depende de la operadora cuántos grados son definidos, una prioridad alta permite asignar más recursos y por más tiempo que una prioridad baja. Con la prioridad se pueden administrar los recursos limitados de forma eficiente asignándola a aquellas incidencias que más afectan al funcionamiento de una red.
El personal técnico recibe una incidencia, el siguiente paso es diagnosticar el error con la información proporcionada. Estudiando el incidente que se describe, el técnico puede descubrir la causa que ha originado la incidencia, haciendo uso de un conjunto de herramientas.
Existen varios tipos de fallos, entre los que podemos considerar.

- ⇨ Seguridad: Detectado una acceso no autorizado al sistema, rompiendo la seguridad del sistema.
- ⇨ Rendimiento: El funcionamiento de la red no es óptimo, afectando a la calidad de los servicios ofrecidos, pueden existir diversas causas para este tipo de fallo.
- ⇨ Hardware: Fallo en algún dispositivo de la red, que puede ser desde una bajada de rendimiento hasta la rotura del dispositivo.
- ⇨ Software: Igual que el tipo anterior pero desde el punto de vista de software.

Cada tipo de error implica una resolución diferente, para los fallos de software y hardware, la sustitución del componente averiado suele ser la solución más sencilla, aunque puede provocar una parada en los servicios del operador, con el perjuicio económico que implica. Esta solución sería la última opción.
Para los fallos de seguridad, la solución consiste en detectar el componente donde se encuentra el fallo de seguridad y repararlo. Entre las opciones que se suelen utilizan tenemos:
–Actualizar el componente donde se encuentra el fallo.
–Sustitución de hardware por otro más seguro.
–Implementar medidas de seguridad que aumenten la seguridad del sistema.
Respecto a los fallos de rendimiento, este tipo de fallo puede ser generado por múltiples causas:
–Malfuncionamiento en un componente hardware o software.
–Congestión en la red.
–Uso incorrecto de los recursos de la red.
–Un ataque desde el exterior, como un DDOS.
–Elevada carga de trabajo.
Este tipo de fallos se propagan por la red de forma muy rápida, un problema de rendimiento en un componente de la red puede afectar de forma muy rápida el resto de la red. Una buena medida sería aislar los componentes con bajo rendimiento, de esta forma se restringe los componentes que se deben analizar para encontrar el origen de la bajada de rendimiento.
Este tipo de fallos puede derivar en algunos de los fallos vistos anteriormente, un dispositivo que ha sufrido una pérdida de rendimiento y la causa puede ser que debido a un fallo de seguridad un atacante ha tomado el control de forma remota. Las posibles soluciones son cualquiera de las vistas anteriormente.
Otro mecanismo utilizado por los técnicos para el diagnóstico de incidencia es la reproducción del incidente en sus equipos. Si el personal técnico posee un laboratorio de pruebas donde poder reproducir el incidente que describe la incidencia, si se consigue, esto proporciona una buena base de información que puede ser utilizada para escoger la mejor solución para la incidencia. Este mecanismo es utilizado por grandes empresas que poseen los recursos necesarios para disponer un laboratorio de pruebas.
En muchas ocasiones para una incidencia existen varias soluciones, el personal técnico debe escoger la mejor solución y que resuelva la incidencia de forma óptima. Para la elección es necesario probar las soluciones y probarlas en un entorno seguro, no es recomendable realizar pruebas en un entorno en producción. Después de un análisis de los resultados de la pruebas escoger la solución optima.
El personal técnico ha escogido la solución óptima, la solución es implementada en el entorno en producción y funciona de forma correcta, con lo que la incidencia se ha resuelto, a esto se denomina cerrar la incidencia.
Tanto la solución como la incidencia debe ser documentada por los técnicos, con esto se crea una base de conocimiento que puede ser consultada en futuras incidencias. Entre los datos que conviene documentar, tenemos:

–Descripción del incidente.
–Causa o causas que la provocado la incidencia.
–Efectos que ha provocado.
–Solución implementada.
–Posibles soluciones alternativas.

Esta base de conocimiento con las incidencias cerradas, debe estar disponible para todo el personal técnico para su consulta, proporcionando una considerable ahorro de tiempo en la resolución de futuras incidencias.
Cuando se genera una incidencia, el personal técnico puede consultar esta base de información que puede proporcionar una información muy valiosa, donde encontrar si la incidencia ha sido generada anteriormente, describiendo la solución utilizada, como incidencias que guarden cierta similitud con la nueva incidencia.

GLPI
Como ejemplo de herramienta de generación de incidencia se mostrará **GLPI**.
GPLI es una herramienta código abierto desarrollada en PHP, cuyos requisitos son los mismos que para cualquier aplicación web, Apache y MySQL. Está disponible para Windows y Linux.
Como funcionalidades principales tiene:

- ⇨ Gestión de inventario software/hardware.
- ⇨ Gestión de incidencia: generación y seguimiento de tickets, peticiones de usuario…
- ⇨ Gestión de empresa: gestión de contactos, proveedores, contratos, documentos y presupuestos.

En este caso solo veremos el módulo de soporte, GPLI permite realizar soporte técnico a usuarios (HelpDesk), entre las características tenemos:
–Generación de incidencias,.
–Estadísticas.
–Seguimiento de incidencias.
–Planificación de intervenciones.
–Base de datos de conocimiento
Pantalla donde se muestra los datos de una incidencia.

Summary

	Date	Description	Duration	Planning	Author	Private
253	2008-06-15 20:55:45	followup 0 qipimoa67tue8nx8	1 Hour(s)	None	admin0 name admin0 firstname	No
1476	2008-04-10 00:14:11	Attribution du ticket: admin0 name admin0 firstname -> glpi	0 Minute(s)	None	glpi	No

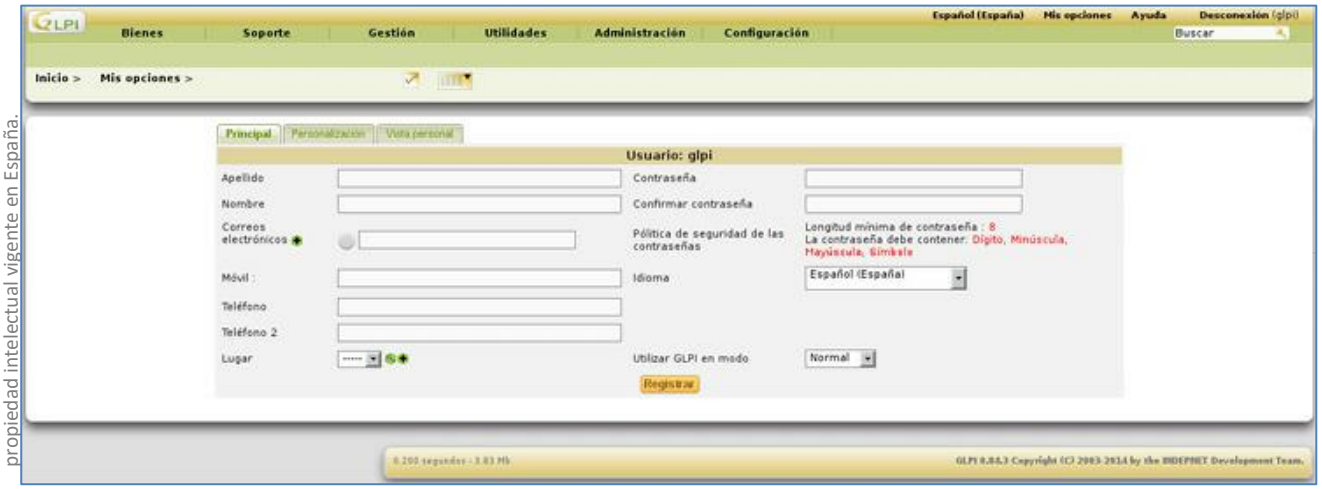
Instalación de GLPI

La instalación de GLPI es bastante fácil, necesitamos bajar el programa desde la página web (https://glpi-project.org/es/). En algunas distribuciones de Linux, como Fedora o Debian, se encuentra disponible en sus repositorios, aunque es posible que no sea la última versión disponible en su página web.
El archivo descargado deberá subirse al directorio de Apache y abrir un navegador con la ruta http://IPservidor/glpi, especificando la dirección o nombre del equipo donde se ha instalado GLPI.
Si el programa se ha descargado desde su página web, cuando se ejecuta por primera vez, ejecutará un asistente de configuración y al finalizar mostrará la pantalla de login.
Pantalla de login en GLPI

Si se ha descargado desde un repositorio de Linux, el asistente no aparece y directamente aparecerá la pantalla de login.
Las credenciales por defecto son:

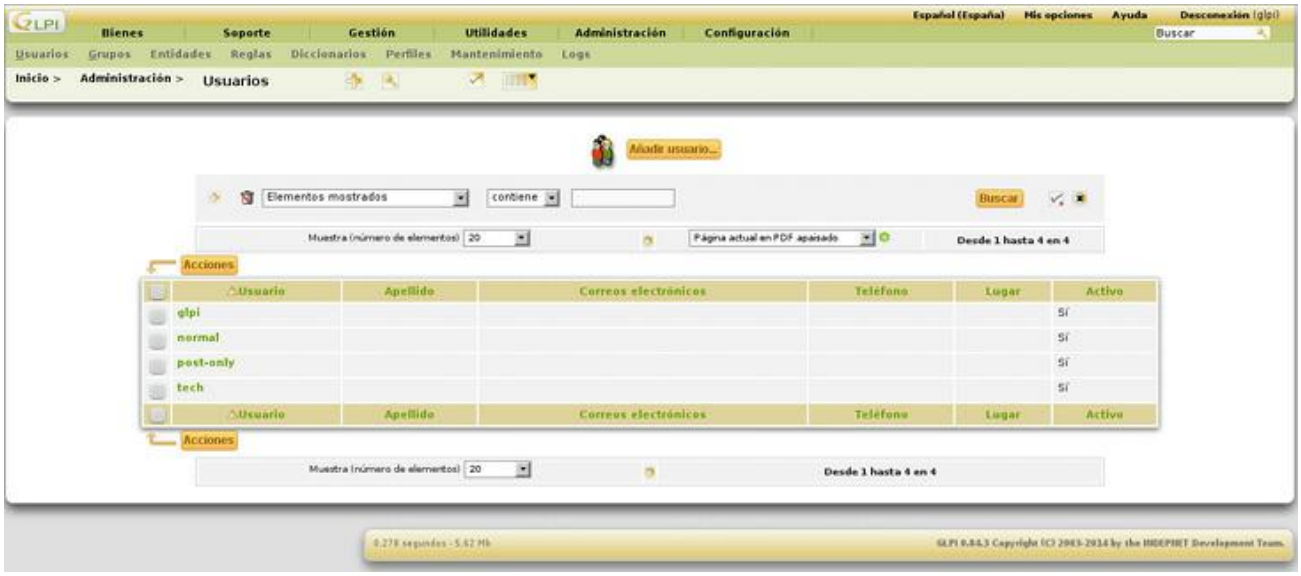
Login: glpi
Password: glpi

La versión de GLPI que será instalada es 0.84.3 en Debian Wheezy.
La pantalla principal está organizada en varias pestañas y en la parte superior los diferentes módulos disponibles y cada uno de ellos dispone de un menú desplegable. Cada módulo se encarga de un área de gestión.
–Bienes: donde realizar tareas de inventario de dispositivos.
–Soporte: soporte de usuario (Helpdesk), el área que utilizaremos.
–Gestión: encargada de la parte más empresarial.
–Utilidades: gestión sobre un conjunto de aplicaciones: advertencia, base de conocimiento, RSS, reservas y informes.
–Administración: para gestionar diferentes componentes del programa.
–Configuración: nos permite configurar cualquier aspecto del programa.
La primera tarea a realizar es cambiar la contraseña del usuario, una notificación nos indica que cambiemos la contraseña de los usuarios, pulsamos en la opción Mis opciones y muestra los datos del usuario actual.
Preferencias del usuario



Donde introducir los datos del usuario, en este caso cambiar la contraseña del usuario con los requisitos que se indican, introducir la contraseña y pulsar en Registrar.
Para comprobar el cambio de contraseña, pulsar en Desconexión, ingresar con el mismo usuario y la nueva contraseña.

Por defecto, GLPI crea una serie de usuarios:
–Normal: tiene acceso a los datos solo para lectura y generar incidencias.
–Post-only: permite generar incidencias en la interfaz, los clientes pueden generar incidencias con este usuario.
–Técnico (tech): tiene acceso a los datos en modo escritura/lectura, puede generar, modificar y borrar incidencia, este usuario es especifico para usuarios que habitualmente utilizan la aplicación. La mayoría de tareas de administración no podrán realizarlas.
–Administrador (glpi): permite gestionar todos los aspectos de la aplicación, tiene permiso para realizar todas las tareas en la aplicación.
Es recomendable cambiar la contraseña de todos los usuarios por defecto.
Para obtener la interfaz web en español, hay que pulsar en la opción de preferencias (settings) que se encuentra en la parte superior derecha, donde aparecerá la preferencias del usuario y modificar la opción de idioma a Español (España).
Para ver un listado de todos los usuarios de la aplicación, dentro del menú Administración existe la opción Usuarios.
Lista de usuarios en GLPI.



Muestra una lista con los usuarios disponibles en el sistema, si pulsamos en el nombre del usuario muestra una ventana donde añadir o modificar los datos de ese usuario. Para añadir un nuevo usuario hay disponible un botón de Añadir usuario.
También existe un apartado donde buscar un usuario por diferentes criterios de búsqueda, se puede buscar por diferentes campos del usuario, dependiendo del campo existen una serie de opciones (contiene, no es, es, etc.) para afinar en la búsqueda.
Podemos añadir más criterios de búsquedas pulsando en la opción Añadir criterio de búsqueda representado por un icono con el símbolo “+”.
En la parte superior se puede ver el camino recorrido para llegar en la pantalla actual, Inicio->Administración->Usuarios. Puede utilizarse para moverse por la interfaz.
Si pulsamos en Inicio, volvemos a pantalla principal del usuario, donde divido por pestañas, muestra diferentes vistas diferentes tareas del usuario.

Pantalla de inicio

Incidencias

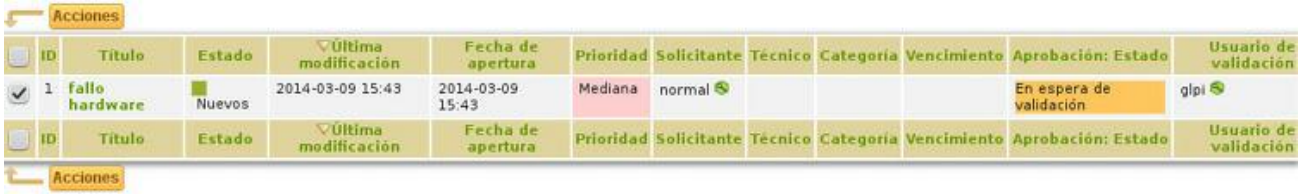
GLPI proporciona las herramientas necesarias para realizar funciones de HelpDesk o soporte a usuario. Entre otras funcionalidades los usuarios de HelpDesk pueden generar incidencias y enviarlas a otros usuarios.
Por ejemplo vamos a generar una incidencia por un operador que será recibida por un técnico.
Para el rol de operador utilizaremos el usuario normal, ingresamos en GLPI con el usuario normal y su contraseña, creada anteriormente. Este usuario solo puede realizar determinada tareas en la interfaz, como generar incidencias.
Nos situamos en Soporte->Incidencias.
En la parte superior hay disponibles un conjunto de iconos y uno de ellos, símbolo "+", sirve para crear una incidencia
Pantalla para generar una incidencia.

Algunos campos de la incidencia no pueden ser rellenados por el usuario normal y es responsabilidad de otros usuarios.
Los campos disponibles para el usuario normal.
–Tipo -disponibles dos opciones-: incidencias donde describir un incidente ocurrido y solicitud donde pedir algún tipo de servicio.
–Categoría: cada incidencia o solicitud se pueden englobar dentro de una categoría que deben ser generadas por un usuario con ese permiso.
–Asignada a: permite asignar la incidencia a otro usuario, por defecto el usuario normal no puede realizar una asignación a otro usuario.

–Urgencia: permite asignar un grado de urgencia a la incidencia, dependiendo de la urgencia asignada, los campo Impacto y Prioridad serán modificados.
–Solicitud de validación: permite que la incidencia deba ser revisada y validada por otro usuario, el usuario normal solo tiene permiso para enviarla al usuario glpi (administrador).
–Título: especificar un título para la incidencia.
–Descripción: rellenamos con información de la incidencia.
–Fichero: podemos adjuntar un fichero, como por ejemplo el log de un determinado componente.
Como ejemplo, se genera un incidencia con urgencia mediana de un fallo hardware que debe ser validada por el usuario glpi, el cliente ha indicado que el disco duro hace un ruido muy raro y no arranca el equipo.
Pulsando en Añadir.
Una nueva incidencia ha sido generada, en el apartado Inicio podemos ver que hay una incidencia en curso.
Pueden generarse nuevos usuarios o modificar el nombre de los usuarios por defecto para cumplir los requisitos de nuestra empresa. En este caso vamos a utilizar los creados por defecto y asignarle un determinado rol para el ejemplo mostrado.
La incidencia debe ser validada por el usuario glpi, este usuario deberá validar la incidencia para que siga el proceso.
Pantalla inicio del usuario glpi

El usuario glpi en su pantalla inicio mostrará una notificación indicando que hay una incidencia que debe ser validada, si pulsamos en la notificación, mostrará la incidencia con su datos.

Incidencia que espera validación.



Podemos añadir una acción a la incidencia a escoger entre una lista, marcar la incidencia y pulsar en el botón Acciones, mostrará una nueva pantalla con una lista de acciones a realizar sobre la incidencia, estas acciones son:
–Actualizar: para modificar algún dato de la incidencia.
–Tirar a la papelera: para borrar la incidencia, moviéndola a la papelera.
–Añadir un Documento.
–Eliminar un documento: esta eliminación será permanente.
–Añadir un nuevo seguimiento: permite que un usuario pueda saber el estado de la incidencia y todas las modificaciones que han sido realizadas. Este seguimiento puede ser realizado por diferente métodos.
–Añadir una nueva tarea.
–Solicitud de validación.
–Añadir un actor: permite añadir un usuario con un rol determinando, tenemos los siguientes roles:
·Solicitante: usuario o grupo que puede generar una incidencia.
·Supervisor: usuario o grupo que gestionar una incidencia.
·Asignada a: usuario o grupo que recibe la incidencia para resolverla.
Para validar una incidencia por parte del usuario glpi, pulsamos en la incidencia (título).

Datos de una incidencia

El usuario glpi tiene más permisos, puede realizar más acciones en la incidencia. Entre las acciones que puede realizar distintas al usuario normal.

–Vencimiento: asignar un fecha límite para la resolución de la incidencia, también se le puede asignar un ANS (acuerdo de nivel de servicio) o SLA, que indicará la fecha de vencimiento acordada entre el cliente y la empresa.

–Estado: asignar un estado a la incidencia, por defecto es nueva, indicando que la incidencia es nueva, el resto de estados son:

·En curso (asignada): la incidencia está en proceso de resolución y asignada al personal correspondiente.

·En curso (planificada): ha sido asignada y tiene planificada una actuación.

·Espera: la actuación correspondiente está en curso y en espera de resultados.

·Terminado: la actuación ha finalizado.

·Cerrado: la incidencia ha sido cerrada, que significa que se ha resuelto y no se realizan más actuaciones sobre ella.

–Origen de la solicitud: donde proviene la incidencia, indica el mecanismo origen de la incidencia; Helpdesk, Directa, Email, Teléfono, Escrito u otro, también el usuario glpi puede añadir nuevos mecanismos pulsando en el icono con el símbolo “+”.

·Aprobación: apartado donde validar las incidencias, está compuesto por varias opciones:

·En espera de aprobación: en espera de aprobar o rechazar la incidencia.

·Rechazado.

·Aprobado.

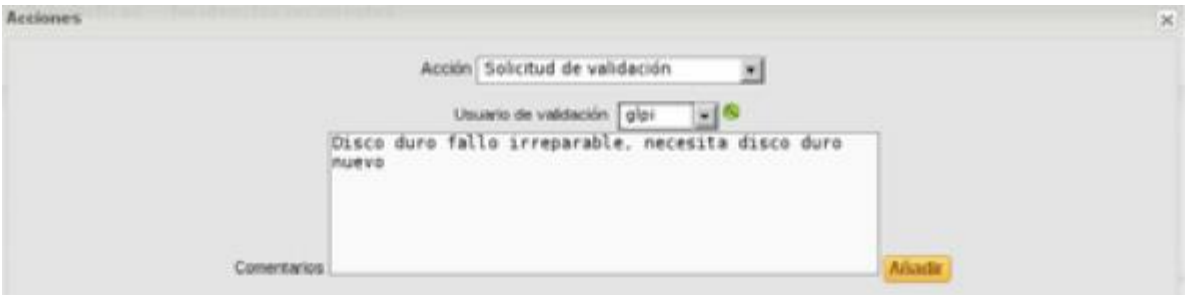
·No está sujeto a validación.

–Lugar: específica la localización donde se ha producido la incidencia, por defecto está vacío y el usuario glpi puede crear un lugar. Para crear un lugar pulsar en icono “+”.

Pantalla para crear un lugar.

Donde se especifica:
·Nombre: para identificar la localización.
·Debajo de: especificar donde se encuentra dentro de la organización de la empresa.
·Código de oficina.
·Nº de código:
·Comentarios: para añadir datos a la localización.
–Actor: donde se puede ver cuáles son los actores de la incidencia (Solicitante, Supervisor y Asignada), para añadir actores pulsar en icono "+" en cada una de las categorías.
–Documento asociado: adjuntar un documento relacionado con la incidencia.
–Incidencias relacionadas: indicar si la incidencia está relacionada con otra, indicando el ID (identificador) de la incidencia.
–Añadir nuevo seguimiento: algunas veces se indica cómo va el proceso de resolución de la incidencia, indicando una pequeña descripción.
El estado de la incidencia pasará a en curso (asignada), la incidencia en aprobación será Aceptada y el lugar será en Oficina, debe ser creado anteriormente, el supervisor será glpi y la incidencia será asignada a tech.
La incidencia deberá ser registrada, pulsando en el botón Registrar.
En la pantalla de inicio del usuario glpi muestra la incidencia en seguimiento, debido a que es el supervisor de la incidencia.
Como la incidencia ha sido asignada al usuario tech, este usuario tendrá la incidencia en su pantalla inicio.
Pantalla de inicio del usuario tech

El técnico procesa la incidencia, cambia el estado a planificado indicando que va concertar una cita con el cliente para revisar el equipo, añadiendo un nuevo seguimiento para indicar que ha concertado la cita. De esta forma el supervisor podrá saber cómo va la incidencia.
El técnico se ha desplazado a la oficina y comprueba que el disco duro está dañado y debe ser reemplazado, pero necesita la aprobación del supervisor para instalar el nuevo disco duro.
Abre la incidencia y modifica el estado lo cambia a En espera, añade un nueva Acción del tipo Solicitud de validación para el usuario glpi indicando el motivo.
Solicitud de una validación



En la pantalla inicio del usuario glpi mostrará una incidencia que espera ser aprobada. Nos situamos en el apartado de Incidencias y pulsamos en la pestañas validaciones¸ donde muestra la validaciones, tanto las aprobadas como las que están a la espera de validar.

Pulsamos en la incidencia que está a la espera de validar, modificar el estado de la validación a Aceptado y escribir una comentario (opcional) para la validación.

Validación de una incidencia

Por último, registrar la validación, modificando el estado de validación a aceptada. En la pantalla inicio de glpi desaparecerá la notificación de validación.

El técnico tiene la aprobación y procede a sustituir el disco duro al cliente, instalando el sistema operativo de nuevo y los datos para el cliente. Modifica el estado de la incidencia a Terminado.

Añade un nuevo seguimiento indicando las tareas realizadas.

Por último el usuario glpi (supervisor) visualiza la incidencia y comprueba el seguimiento, como no hay noticias del cliente de nuevo se considera que la incidencia se ha solucionado con éxito, modifica el estado de la incidencia a cerrado. En la pantalla de inicio de glpi,desaparecerá la notificación de la incidencia.

Dentro del apartado incidencia, está compuesto por una serie de pestañas que realizan diversas tareas, en el proceso anterior se ha utilizado las pestañas Seguimientos y Validaciones.

Las pestañas presentes en el apartado de incidencias (tabla en la siguiente página).

Pestaña	Descripción	Usuarios autorizados
Seguimientos	Permite conocer los pasos que se van ejecutando para resolver la incidencia.	Todos
Validaciones	La incidencia necesita la aprobación de otro usuario.	Administrador, técnico y normal.
Tareas	Permite añadir una tarea que debe ser realizada para una incidencia.	Administrador, técnico y normal.
Solución	Permite dar una solución por parte de otro usuario o de la base de conocimiento, el usuario que tenga asignada la incidencia deberá aprobar o rechazar la solución.	Administrador, técnico y normal.
Estadísticas	Muestra estadísticas por diversos criterios.	Todos
Costes	Asigna una serie de costes para resolver la incidencia, cada intervención puede generar una serie de costes.	Administrador y técnico.
Documentos	Adjunta documentos a la incidencia.	Administrador, técnico y normal.
Problemas	Asigna un problema surgido en la incidencia.	Administrador y técnico.
Histórico	Muestra todos los eventos producidos en una incidencia.	Todos
Todos	Muestra la información de todas las pestañas de una incidencia en la misma pantalla.	Todos

Dentro de GLPI se ha visto la parte de soporte y solo un pequeña parte de todas las funcionalidades que proporciona, también hay disponibles otros módulo, como Inventario o Gestión, que no se han comentado. GLPI dispone un amplio catálogo de plugins para los diversos módulos que permiten aumentar o añadir funcionalidades.

2.8. Actualizaciones de software

Toda red está compuesta por un conjunto de software instalado en diversos componentes y este software no está libre de errores. Las empresas desarrolladoras de software proporcionan un conjunto de actualizaciones de software que mejoran su rendimiento.

Las actualizaciones de software debe ser un punto crítico para cualquier administrador de una red, todo el software debe estar actualizado a su última versión disponible.

Las actualizaciones de software proporcionan las siguientes funcionalidades:

–Mejoras en el rendimiento: esto se consigue reparando fallos que provocaban una pérdida de rendimiento o implementando mejoras que en el rendimiento del software.

–Eliminación de agujeros de seguridad: muchas actualizaciones reparan errores en el software que permitían accesos no autorizados u otro tipo de fallos de seguridad.

–Corrección de errores: ningún software está libre de errores, las actualizaciones corrigen los errores descubiertos.

–Aspecto visual: determinadas actualizaciones, sobre todo en aquellas que implican un cambio de versión, modifica la interfaz gráfica del software.

–Cambios en el funcionamiento: introduce variaciones o cambios completos en el funcionamiento, esto suele realizarse en cambios versiones.

Algunas actualizaciones implican incompatibilidades con funcionalidades disponibles en versiones inferiores, esto puede resultar perjudicial para determinados usuarios que utilizaban esas funcionalidades y no la encuentran en versiones actualizadas.

Algunas actualizaciones implican una adaptación de uso por parte de los usuarios, produciendo algún conflicto por parte de los usuarios descontentos con el cambio, aunque esto cambios impliquen una mejora en el funcionamiento.

Otro aspecto a tener en cuenta, en determinados sistemas (como Linux) las aplicaciones tienen una series dependencia y su funcionamiento depende de otras aplicaciones. Cuando actualizamos un determinado programa, puede afectar a sus dependencias y provocar un conflicto de dependencias, impidiendo una correcta actualización.

El proceso de actualización implica una carga de trabajo adicional en el equipo que puede afectar a su rendimiento. El administrador debe definir una política de actualizaciones, teniendo en cuenta diversos aspectos:

–Cuándo realizar las actualizaciones: escoger la fecha y hora para realizar las actualizaciones para que afecten lo menos posible al rendimiento del equipo y la red.

–Qué componentes actualizar: escoger con qué frecuencia realizar la actualización, depende del componente la frecuencia de las actualizaciones será diferente. Por ejemplo, para un servidor web en producción las actualizaciones serán más espaciadas, para no afectar a su rendimiento.
–Qué tipo de actualizaciones: existen diversos tipos de actualizaciones, por ejemplo actualizaciones de seguridad o críticas. Dependiendo del software es aconsejable aplicar solo un tipo de actualizaciones, como solo actualizaciones de seguridad, para no afectar al rendimiento. En otro tipo de software es aconsejable aplicar todo tipo de actualizaciones.
Una buena política de actualizaciones, aumenta la seguridad del sistema y otros factores como usabilidad, rendimiento o fiabilidad.
Dentro de las actualizaciones podemos considerar dos tipos.
–Locales: la orden de realizar las actualizaciones se realiza dentro del sistema.
–Remotas: la orden se realiza desde un ordenador distinto y de forma remota.

Las actualizaciones locales son realizadas por el usuario administrador del equipo, las actualizaciones remotas son ejecutadas por un administrador desde su equipo. Las actualizaciones remotas son una tarea realizada por los administradores de red para actualizar un conjunto de equipos en una red de una manera fácil.
La ejecución de una actualización se puede realizar de dos formas:
–Automáticas: un software de actualizaciones se ejecuta de forma periódica.
–Manuales: la ejecución de la actualización se realiza de forma manual.
Las actualizaciones automáticas deben ser programadas, indicando la periodicidad (diario, semanal o mensual) de ejecución y especificar la hora. Las actualizaciones manuales, el administrador decide cuando ejecutarlas.
Dependiendo del componente, hay disponible solo actualizaciones de forma manual, debido a que el proceso de actualización es un proceso delicado y preciso una supervisión. Por ejemplo, actualizar el firmware de un router.
En otros casos, las actualizaciones automáticas no son recomendables, por ejemplo en un servicio que se encuentra en producción, como un servidor de correo. El proceso de actualización debe ser supervisado por el administrador para evitar problemas con el funcionamiento del servidor y solo aplicar aquellas actualizaciones críticas o de seguridad.
Los sistemas operativos proporcionan software que permite actualizar los componentes del sistema, pudiendo escoger entre una ejecución manual o automática.
También existen actualizaciones para software donde el proceso de actualización es realizado de forma automática y transparente para el usuario. Por ejemplo, Firefox o Google Chrome, es actualizado sin que el usuario intervenga y la actualización será aplicada en el siguiente arranque, este mecanismo es denominado actualizaciones silenciosas.
Otro tipo de actualizaciones para software, aparece una notificación indicando que hay una nueva actualización, el usuario deberá aceptar y el proceso de actualización comenzará. Un ejemplo de este tipo de actualización es utilizado para actualizar la máquina virtual de java.
En cualquier red, hay múltiples equipos que deben ser actualizados, el administrador dispone de herramientas para realizar actualizaciones remotas de un conjunto de equipos, sin tener que desplazarse donde se encuentren los equipos. El administrador de red controla de forma estricta las configuraciones y el software instalado, esto facilita la actualización remota de múltiples equipos.
Las herramientas de actualizaciones remotas proporcionan las siguientes ventajas:
–Ahorro de tiempo: todos los equipos ejecutan las actualizaciones al mismo tiempo.
–Control del software instalado: este tipo de software dispone de un inventario del software instalado en los equipos.
–Seguridad: el administrador de red ejecuta las actualizaciones de forma periódica y es el encargado de gestionar todas las actualizaciones, quitando la responsabilidad de las actualizaciones a los usuarios.
–Gestión de actualizaciones: se puede decidir organizar las actualizaciones por grupos dependiendo de diversos parámetros y ejecutar las actualizaciones cuando sea más oportuno en la red.
Hay diferentes formas de realizar las actualizaciones remotas, entre las cuales tenemos.

–Programando las actualizaciones, en un periodo determinado la herramienta de actualización lanza el comando para actualizar a todos los equipos que controla.
–Las actualizaciones son descargadas en un servidor y distribuidas al resto de los equipos.
Hay disponibles otro tipo de herramientas que permite de forma centralizada gestionar configuraciones de múltiples dispositivos, como ejemplo tenemos Puppet o Chef. Estas herramientas utilizan una arquitectura Servidor/Cliente, donde en el servidor almacena las configuraciones que deben cumplir los clientes, entre esas configuraciones permite comprobar si el equipo esta actualizado y en caso contrario ejecutar la actualización desde el servidor.
Con este tipo de herramientas no solo permite realizar actualizaciones, también permite realizar instalaciones de forma remota. Por ejemplo, instalar un determinado software de forma remota en un conjunto de equipos, también permite instalar un sistema operativo en un conjunto de equipos.
Esto implica un ahorro grande de tiempo, con las instalaciones remotas evita tener que realizar en cada equipo una instalación local, otras ventajas que implica son:
–Inventario de los equipos: permite conocer el software instalado en cada equipo y poder gestionar actualizaciones.
–Despliegue: mediante una instalación remota del sistema operativo y de diversos software, permite preparar múltiples equipos para su uso de forma más rápida.
–Centralización de copias: para la instalación remota en múltiples equipos solo necesita una copia del software en un servidor.
El uso de este tipo de herramientas también implica una serie de desventajas:
–Complejidad: este tipo de herramientas requieren configurar la red para su correcto funcionamiento y su instalación en algunos casos puede ser bastante compleja.
–Tráfico en la red: las instalaciones remotas provocan mucho tráfico en la red debido a la instalación es enviada a múltiples equipos por la red. Por este motivo, este tipo de instalaciones deben ser realizada cuando no haya usuarios en la red o haya muy poco uso en la red.
La instalación de este tipo de herramientas requiere una serie de requisitos:
–Los equipos deben estar en red y accesibles desde el equipo remoto.
–La seguridad debe permitir el acceso, si hay un cortafuego debe permitir el acceso.
–Para determinadas funcionalidades presentes en este tipo de herramientas, debe tener activados en el equipo algunas opciones como PXE o DHCP.
–Tener el software almacenado y accesible en un equipo desde donde se realizaran la instalación.
En grandes infraestructuras de red, este tipo de herramientas son imprescindibles para el administrador de red. Dentro del CGR de la empresa pueden realizarse instalaciones a múltiples equipos, sin que el personal técnico deba desplazarse para realizar las instalaciones, con el ahorro tiempo y recursos que implica.
Hay disponible un abanico de herramientas de gestión de instalaciones remotas, este tipo de herramientas dispone de muchas más funcionalidades, a parte de las instalaciones.
Este tipo de herramienta utiliza una arquitectura servidor/cliente, donde el servidor ejecuta la herramienta que gestión y administra a múltiples clientes.

RIS

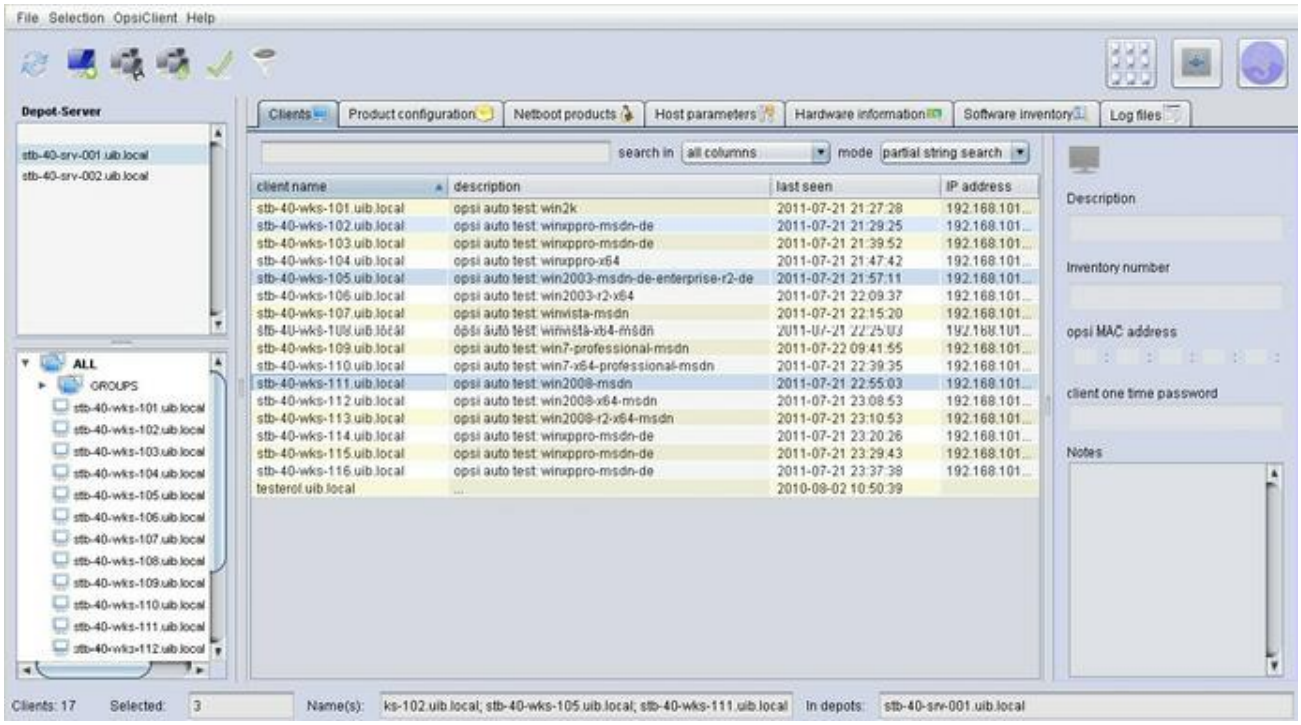
Herramienta incluida en sistemas Windows Server, donde un servidor con una imagen en el disco duro de un sistema Windows permite instalarlo de forma remota en múltiples equipos. Permite realizar instalaciones de forma desatendidas mediante un archivo de configuración con los datos para la instalación.

Mediante el uso PXE permite realizar arranque remoto en los equipos, con DHCP asignarle una IP para realizar la instalación, también permite distribuir los controladores.
A partir del Windows Server 2003 Service Pack 2 fue sustituido por WDS.
WDS es una herramienta que utilizada para el despliegue de los sistemas Windows Vista/7/Server 2008, permite la automatización del despliegue en los clientes, utilizando un formato de imagen especifico denominado Windows Imaging Format (WIM).
Mediante una serie de archivos (guiones) WDS permite almacenar y destruir paquetes de instalación basados en imágenes WIM, para que el despliegue sea compatible con IP multicast y pueda gestionar paquetes de 32 o 64 bits.

OPSI

Herramienta de administración de clientes Windows, esta herramienta permite administrar un conjunto de clientes en Windows desde un servidor Linux. Entre Las funcionalidades que dispone.

–Instalación de sistemas operativos de forma desatendida o mediante una imagen.
–Instalación remota de software.
–Gestión de actualizaciones.
–Inventario de hardware y software.
–Administración de licencias.
–Gestión de clientes con OPSI.



OPSI requiere la instalación de un pequeño programa en los clientes Windows, denominado Agente, este programa se comunica con el servidor de OPSI para poder administrarlo mediante una consola Web. Para realizar instalación remotas requiere tener software compatible, hay disponible diversas páginas donde descargarse software compatible. OPSI incluye un lenguaje script para convertir cualquier software a software compatible con OPSI.

Hay disponible un conjunto de módulos que proporcionan la empresa desarrolladora de OPSI mediante la cofinanciación, cuando un módulo es completamente financiado es liberado de forma gratuita.

Los módulos disponibles son los siguientes:

–Administración de perfiles de usuarios.
–Soporte para MySQL.
–Conector para Nagios.
–Soporte para WAN.
–Soporte para UEFI/GPT.
–Backup de la imagen en local.

En el plan de desarrollo está previsto el soporte de clientes Linux en un futuro.

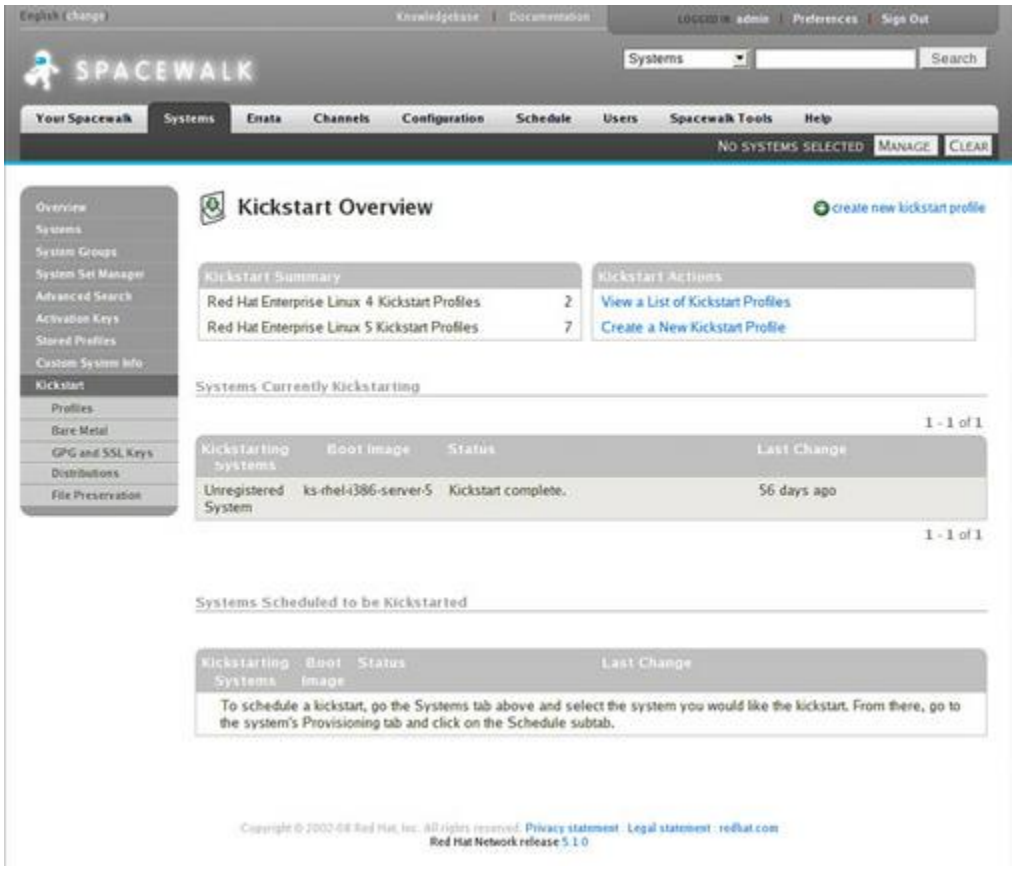
SpaceWalk

Es una herramienta desarrollada por RedHat y es la versión de código abierto del servicio Satellite de RedHat, esta mantenida por la comunidad y RedHat, la comunidad también es el encargado de dar soporte a esta herramienta.

SpaceWalk es un sistema que permite la distribución de paquetes a diversos clientes y la automatización del proceso de instalación o actualización, otras funciones que incluye son:

–Inventario de los equipos, tanto software como hardware.
–Utilizando la herramienta Kickstart (provisión de sistemas), permite realizar instalaciones desatendidas.

–Administración y despliegue de archivos de configuración.
–Permite diversos grados de agrupación: por paquetes, repositorios y clientes.
–Monitorización de los sistemas y ejecución de comandos remotos.
–Soporte para KVM, permite provisionamiento de máquinas virtuales.
Provisión de sistemas con Kickstart



Spacewalk proporciona una interfaz web para su administración, también proporciona una serie de comandos para ejecutar en un terminal.
El servidor debe cumplir unos requisitos software para la instalación, estos requisitos son:
–Java.
–Python.
–Tomcat.
–Postgresql, aunque puede utilizar otras base de datos.
Para los clientes no existen requisitos, solo es necesario un terminal para ejecutar varios comandos.
Los clientes son añadidos al servidor mediante una clave que debe generarse y activarse, cada cliente debe tener una clave que es activada para ser identificado y evitar confusiones sobre los paquetes que son instalados en un cliente.
Los repositorios son almacenados en canales y los clientes pueden suscribirse a uno o varios. Los clientes pueden descargar o actualizar los paquetes de forma automática o el administrador desde el servidor puede ejecutarlas, en concreto puede programar cuando Spacewalk las ejecuta, hacia un cliente.
Esta herramienta permite distinguir entre diferentes roles, entre usuarios y administradores, definiendo las acciones que puede realizar un administrador.
La documentación para esta herramienta está disponible en su página web, consta de una wiki y diversos manuales.

2.9. Planes de contingencias

Toda infraestructura de red debe estar correctamente monitorizada para detectar posibles fallos y poder repararlos antes que se convierta en algo más grave, generando incidencias para facilitar el proceso de resolución y documentar la solución encontrada para crear una base de conocimiento.

Pero por diferentes motivos, es posible que pueda afectar a un servicio de forma más grave, incluso puede provocar un fallo total en todos los servicios de la empresa. Esto provoca un grave perjuicio económico y debe ser reparado los antes posible para restablecer todos los servicios, disponiendo de un plan que indica una serie de pasos para reanudar lo antes posible todos los servicios.
Este plan debe estar bien documentado y comunicado a todas las partes de la organización para que sepan cual es papel y que acciones deben ejecutar cuando se activa. A este plan se denomina un plan de continuidad, que describe el procedimiento a seguir para reanudar el funcionamiento de un sistema informático, en la empresa deben existir varios planes de continuidad que describan diversos procedimientos en función del proceso que se debe reanudar.
Todos los planes de continuidad deben estar englobados en un documento de manera organizada, este documento se denomina plan de contingencia, que periódicamente debe ser revisado para incluir las actualizaciones producidas en el sistema.
Un plan de contingencia debe cubrir tres aéreas.
–Incluir una un plan de respaldo y recuperación que permiten reanudar un servicio evitando interrupciones o reinicios. Para conseguir esto existen herramientas de altas disponibilidad para diversos servicios que proporciona una capa de redundancia.
–Describir todas las posibles opciones para que el sistema siga funcionando en cualquier aunque las instalaciones habituales no estén disponibles.
–Proporcionar continuidad en el negocio que la empresa incluso cuando se produzcan interrupciones.

Un plan de contingencia debe tener en cuenta los siguientes aspectos:
–Un servicio siempre debe estar disponible y funcionar de manera óptima.
–Para ofrecer este servicio se necesita una infraestructura.
–El negocio de la empresa es obtener beneficios con los servicios que proporcionan.
–Estos servicios deben tener una calidad definida en el contrato del cliente.
Un plan de contingencia es desarrollado mediante un proyecto de elaboración, donde se especifican los procedimientos operativos que deben ser aplicados en caso de producirse determinados eventos, estableciendo un plan de acción con anterioridad es un facto determinantes para dar una respuesta rápida y eficaz.
Para elaborar un plan de contingencia correctamente, se deben incluir diversos puntos a tener en cuenta en la elaboración.
–Recursos y procesos virales de contingencia.
–Análisis de riesgo.
–Protección de los puntos críticos.
–Estrategias y alternativas de recuperación.
–Equipos de trabajo y asignación de funciones.
–Pruebas del plan de contingencia.
–Manual de contingencia.
–Retroalimentación.
La elaboración de un plan de contingencia debe tener en cuenta los puntos descritos, que pueden ser diferentes en cada empresa. El personal técnico será el encargado de definir esos puntos de forma correcta. A continuación se explicará con más detalle cada uno de los puntos.

Recursos y proceso vitales en la empresa
Toda empresa tiene una serie de procesos y recursos que se consideran críticos por diversos factores, un fallo puede ser muy perjudicial para la empresa. Identificar esos recursos y procesos e incluirlos en el plan de contingencia es un aspecto muy importante en el proceso de elaboración del plan.
Los responsables de la elaboración del plan de contingencia deben examinar todos los recursos disponibles y los procesos para comprobar su importancia en el modelo de negocio de la empresa. Para conocer ese grado de importancia se pueden tener en cuenta los siguientes factores.
–Cómo afecta al modelo de negocio si se produce un fallo.
–Coste económico para la reparación.
–Tiempo de reparación.

–Grado de dependencia.
Si un recurso falla y afecta de forma grave al modelo de negocio, la reparación tiene un alto coste económico, tiempo de reparación alto y muchos recursos dependen de él. Ese recurso indudablemente se considerará crítico, pero esto puede que no sea tan fácil para otros recursos. Los responsables deben ponderar cada uno de esos factores para obtener el grado de crítico que tiene un proceso o recurso cuando falla, deben obtener un conjunto reducido de componentes críticos.

Análisis de riesgo
Cualquier empresa está expuesta a un conjunto de interrupciones o desastres que causan un impacto negativo en el modelo de negocio. Estos desastres provocan interrupciones durante un periodo de tiempo en los servicios que proporciona la empresa.
Un estudio de este tipo de desastres a los que puede enfrentase la empresa debe ser tenido en cuenta en la elaboración del plan de contingencia.
Existen diversos tipos de desastres en función de la causa que los provoca, tenemos:
–Falta de servicio, esto puede ser provocado por falta de energía, corte comunicaciones, fallo hardware, etc.
–Causas naturales como incendios, inundaciones, terremotos, etc.
–Situaciones de alto riego, engloba diversas acciones como ataques informáticos, virus informáticos, accesos no autorizados, etc.
Estudiar qué tipo de desastres pueden ocurrir tanto en los servicios como en las instalaciones y tenerlos en cuenta en el plan de contingencia. Conocer cómo impactarán los desastres que pueden afectar a la empresa, se podrá realizar un análisis de los riesgos que existen en la infraestructura, en los servicios y las operaciones de la empresa.
Para todo este proceso es necesario conocer de forma detallada toda la estructura de la empresa, negocio y todos los componentes involucrados en la empresa. Para realizar este punto deben involucrarse diversos departamentos de la empresa para proporcionar la información necesaria.

Protección de los puntos críticos
Conociendo los puntos críticos y los riesgos, ahora queda cómo proteger los puntos críticos para minimizar los riesgos. En este punto se debe describir diversas recomendaciones para proteger estos puntos críticos, entre las recomendaciones podemos considerar:
–Realizar copias de seguridad de los datos, es aconsejable tener una copia de los datos fuera del sistema, para que en caso de fallo del sistema no afecte también la copia.
–Redundancia de los servicios críticos, también dispone de hardware redundante.
–Fuente energía alternativas, como generadores.
–Tener personal extra para casos de desastres.

Estrategias y alternativas de recuperación
Si las medidas de protección fallan, se deben especificar diversas alternativas para recuperar el sistema, tener un plan B. Tener definido un conjunto de estrategias de recuperación que definan una serie de procedimientos y dependiendo de un conjunto de factores elegir una estrategia u otra.
Entre los factores que podemos encontrar tenemos:
–Coste.
–Seguridad.
–Tiempo de recuperación.
–Los procesos o aplicaciones afectadas qué nivel crítico tienen.
–Recursos.
–Personal.
Dependiendo del tamaño de la empresa (pequeña, mediana y grande), existen muchas alternativas de estrategias de recuperación. Para las grandes existen más diferencias, ya que todas las estrategias implican una sede remota, en las pequeñas y mediana empresa debido a su coste hace inviable esta opción.

Equipos de trabajo y asignación de funciones
Para ejecutar un plan de contingencia es necesario una serie de recursos y uno de los principales son los recursos humanos. Para una ejecución eficaz es necesario establecer un serie de grupos de trabajo y

asignarles una serie de funciones y a las personas que integran el grupo también se le asignan una funciones.
Dentro de cada departamento debe existir una persona (coordinador) que será el encargado de establecer que recursos y procesos son considerados críticos dentro del grupo de trabajo, coordinándose con otros grupos de trabajo para efectuar una ejecución más eficaz.
Otro tipo de grupos que se deben crear son aquellos que solo entrarían en acción cuando se realiza un proceso de recuperación. Dentro de la empresa hay determinados servicios que con proporcionados por empresas externas, como electricidad o comunicaciones, los grupos de recuperación deben estar entrenados correctamente para realizar una comunicación rápida con el personal de estas empresas externas y que el tiempo de recuperación sea mínimo.
Por ejemplo, si se produce un corte en el suministro eléctrico, el grupo de trabajo encargado de la recuperación debe tener una operativa describiendo a que número llamar o como comunicarse con la empresa que proporciona el suministro eléctrico. En algunas ocasiones las empresas externas suelen asignar personal específico a la empresa, con lo que la comunicación es más eficaz, debido a que ese personal específico conoce de necesidades de la empresa.
Todos los grupos de trabajo deben tener muy clara sus funciones y como actuar ante una situación de riesgo, debiendo tener un entrenamiento adecuado, los grupos de recuperación deben actuar rápidamente porque el tiempo que tarden será decisivo en la recuperación de los servicios de las empresas.
El personal debe conocer las funciones del grupo al que pertenecen y del resto de grupo, sobretodo de aquellos que tengan una relación directa. Debe existir una persona o varias encargadas de gestionar a todos los grupos,

Pruebas del plan de contingencia

Todo plan de contingencia debe ser probado para comprobar que funciona en caso de algún desastre en la empresa y la recuperación de los servicios funciona correctamente. Podría realizarse una serie de simulacros antes aprobar el plan de contingencia, pero para mejor resultado es conveniente realizar pruebas, se pueden hacer de dos maneras:
–Pruebas parciales: son ejecutadas para comprobar ciertas aéreas del plan de contingencia, este tipo de pruebas no afectan mucho al funcionamiento de los servicios, siempre que estén planificadas correctamente y sean aplicadas en a pequeña escala.
–Pruebas totales: comprueba el funcionamiento del plan de contingencia de forma global, realizando un análisis de todos los puntos del plan. Este tipo de pruebas afectan al funcionamiento de los servicios de la empresa, con lo cual se debe realizar en un entorno que no esté en producción.
Lo más recomendable es realizar los dos tipos de pruebas para comprobar el funcionamiento del plan de contingencia, aunque a distinto intervalos de tiempo. De forma periódica realizar pruebas parciales en determinadas aéreas, de forma más habitual en aquellas que sean críticas, y en un periodo de tiempo más espaciado una prueba total.
Una prueba real debe evaluar los siguientes puntos:
–Comprobar que la información contenida en el plan es correcta.
–Comportamiento del personal.
–Comunicación entre el personal de contingencia y empresas externas.
–Capacidad de recuperación.
–Rendimiento de la empresa después de una recuperación.

Manual de contingencia

Con los puntos anteriores se obtiene información muy valiosa como:
–Cuáles son los recursos críticos.
–Riesgos en el modelo de negocio de la empresa.
–Impacto en el empresa en caso de fallo.
–Organización de los recursos humanos.
–Operativas de recuperación.
–Comunicación con las empresas externas.
–Etc.

Con toda la información se debe elaborar un documento donde plasmar todo lo aprendido de los puntos anteriores, este documento se denomina manual de contingencia que documenta todos los puntos anteriores

Retroalimentación

Las empresas evolucionan y sus modelos de negocio, lo que en la actualidad puede considerarse crítico, en un futuro puede no serlo. Todo plan de contingencia debe tener en cuenta esa evolución, actualizando la información y operaciones para cumplir los nuevos requisitos.

Resumen

Mapa de Red
Protocolos de Gestión de Red: SNMTP, RMON…
QoS: Ancho de banda, retardo temporal, jitter y pérdida de paquetes
Tráfico Elástico y No Elástico
Service Level Agreement (SLA)
Gestión de Colas: FIFO (1º entrar 1º Salir) y luego por Prioridades con algoritmos o no de equidad
Centro de gestión de redes (CGR) o NOC (en inglés), concepto, funcionamiento
Para llevar a cabo las tareas de Gestión de la red usamos herramientas, como GLPI y Nagios para monitorización.
Las herramientas de monitorización utilizan Agentes: NME en los clientes y NMA en el servidor (Nagios)
Con las herramientas de monitorización queremos medir consumos (gasto de disco, memoria...) y rendimiento (velocidad de procesos…)
Gestión centralizada y distribuida
GLPI: Herramienta para la gestión de Inventario, Tickets y gestión de empresa: proveedores, contactos… y dentro se puede dar soporte a usuarios mediante helpdesk, FAQ
RIS es una herramienta incluida en sistemas windows server que permite realizar instalaciones remotas en múltiples equipos windows