**IOT – Infraestructuras i Operación de Telecomunicaciones**

*1 - Read the theoretical concepts of the SNMP lab session from API (pages 1-16). Prepare a list of concepts you do not understand, to discuss them during the lecture.*

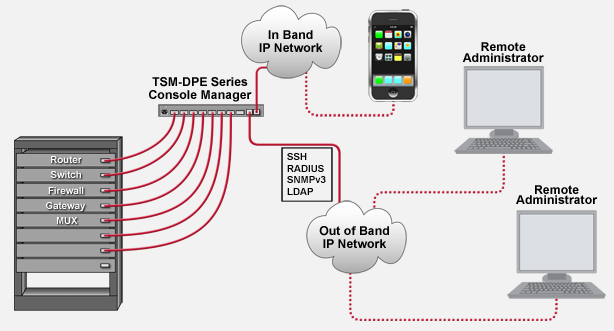
*2 - Read these parts of the "Network Monitoring and Management - Best Practices" from GEANT, and answer the following questions:*

1. *Summary & Introduction (1 page)*
2. *Chapter 1 (2 pages)*
   1. *Express graphically the difference between an in-band and an out-band monitoring/management system.*

**In-band management** implica el uso simultáneo de las interfaces y equipos de red con fines de producción de tráfico y de gestión. No requiere infraestructura física, pero por tanto presenta un menor nivel de seguridad ya que el tráfico de administración más sensible pasa también por el de producción a través de la misma infraestructura.

En posibles casos de congestión puede resultar difícil el acceso a los dispositivos que pueden eliminar el problema que lo produce.

**Out-band management (OOBM)** implica el uso de una infraestructura de red independiente y una interfaz independiente para fines de gestión, diferente de los dispositivos de red e interfaces utilizadas para la producción de tráfico. Se recomienda su uso para la gestión de redes en zonas donde los equipos y servidores se encuentren en el mismo recinto.

Nos ofrece más seguridad al tener una infraestructura de red independiente, pero esto implica mayores gastos. El acceso está activado aunque se produzcan problemas con algunos enlaces. En la Figura 1 podemos ver un esquema con las diferencias.

**Figura 1 – Esquema básico para ver las diferencias entre In-band y Out-band management**

1. *Chapter 4.5 - Device Monitoring Protocols (actually, it only mentions SNMP) (2 pages)*
   1. *What are the main security issues and problems of SNMP? How could you avoid them?*

El principal problema del protocolo SNMP es que está diseñado para colocar muy poca carga en la red. Es un protocolo sencillo porque utiliza unos tipos de datos no estructurados. Se utiliza básicamente con el protocolo de transporte UDP, no se recomienda utilizarlo con TCP (que también se puede utilizar) para redes muy grandes debido al gran número de conexiones necesarias que aumenta la cantidad de tráfico del enlace. Actualmente hay 2 versiones del protocolo SNMP: SNMP v2c y SNMP v3.

SNMP v2c realiza la autenticación utilizando una cadena de caracteres que se envía a través de la red como texto sin cifrar, entonces si alguien está haciendo algún ataque MITM (esnifando la red) puede descubrir este mensaje y poner en peligro el correcto funcionamiento de la red. El uso de esta variante se recomienda si los dispositivos no admiten SNMP v3, y el cifrado y protección se hace con otras herramientas.

SNMP v3 se creó a partir de las limitaciones de seguridad de SNMP v2c, por tanto introduce integridad del mensaje y autenticación entre las fuentes además de cifrar los paquetes.

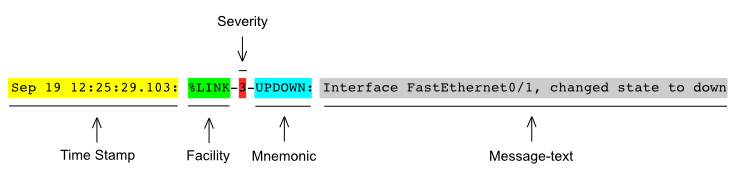
1. *Chapters 6.2, 6.3, 6.4, and 6.5 (3 pages)*
   1. *Which parameters do you think you will have to monitor in your project technical deployment? If they are not listed in the list of recommended variables, try to search which MIB includes them.*

Flujo de datos de la interfaz, carga del procesador y carga de la memoria. Estado de la interfaz y sus estadísticas. Lista de servicios iniciados en el servidor. Las bases estándar IETF MIB se encuentran bajo el nodo MIB-2 (.1.3.6.1.2.1) del árbol MIB. Algunas de las variables más frecuentemente utilizadas son las siguientes:

* Las interfaces (.1.3.6.1.2.1.2) – Toda la información sobre el estado de las interfaces en el dispositivo.
* ifMIB (.1.3.6.1.2.1.31) – ifMIB es una expansión de las interfaces MIB para 32 y 64 bits.
* TCP (.1.3.6.1.2.1.6) – Puedes encontrar los parámetros que describen las conexiones TCP.
* Host (.1.3.6.1.2.1.25) – La tabla de host contiene información sobre el estado del procesador y la memoria en los servidores.

1. *Chapter 7.1 - Just to understand what Syslog is (2 pages)*
   1. *Find an example of a Syslog record and briefly comment it.*

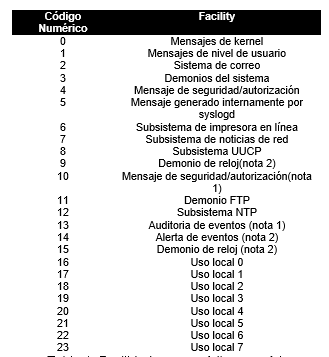
El protocol SysLog (Sistema Logger) se ha desarrollado como un mecanismo para la recopilación de información sobre los cambios y acontecimientos en los sistemas operativos Unix, y una de sus principales características muy útiles es la posibilidad de enviar la información a través de la red. Esto permite la recogida de los mensajes en un servidor central, que a su vez permite la detección más rápida y fácil de los problemas y sus posibles soluciones. SysLog utiliza el protocolo de transporte UDP y en la capa de aplicación no ofrece ningún mecanismo para proporcionar información sobre si el mensaje se transfiere correctamente a su destino, por tanto se puede decir que es poco fiable.

SysLog es un protocolo muy común para recopilar información sobre el estado del sistema. En la Figura 2 hay un ejemplo de mensaje SysLog.

**Figura 2 – Ejemplo de mensaje SysLog, con los principales campos**

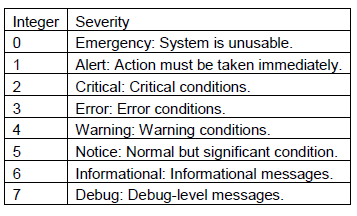
Como vemos los campos de la Figura 2, coinciden con todos los campos que describe el documento que también nombro a continuación.

**Facility:** Identifica el objeto que generó el mensaje, puede ser el sistema operativo, un proceso o una aplicación. La facility se presenta como un entero, y los valores que van del 0 al 15 están reservados para sistemas operativos UNIX, mientras que los valores que van del 16 al 23 se utilizan tradicionalmente para dispositivos de red. (Tabla 1).



**Tabla 1 – Facilities y sus códigos númericos respectivos**

**Severidad (Gravedad):** asume uno de los 8 valores enteros que describe la gravedad del problema actual (Tabla 2).



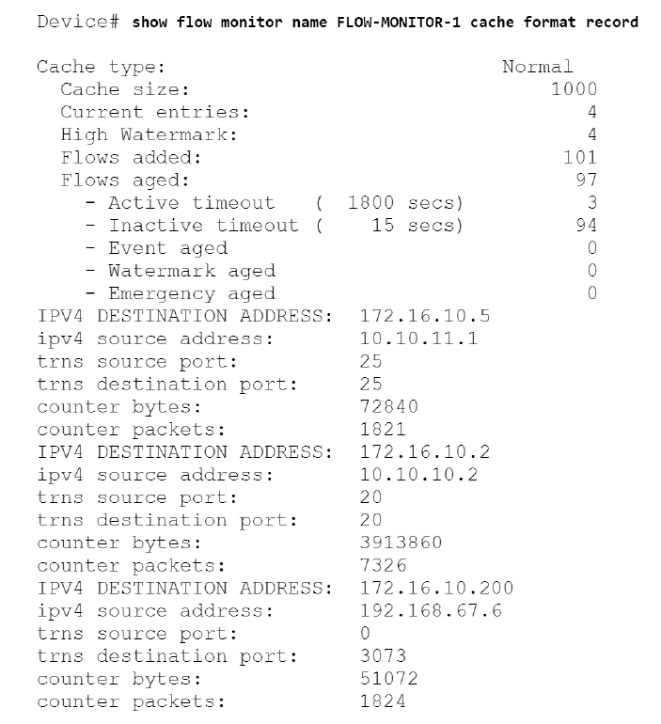
**Tabla 2 – Severidades y su código númerico respectivo**

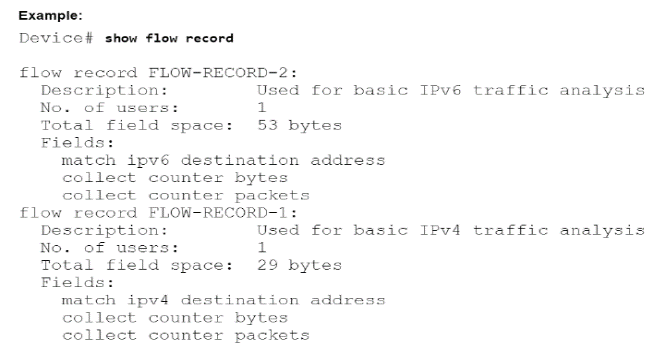
**Hostname:** contiene la dirección IP del dispositivo (interfaz) que envía los datos de SysLog.

**Timestamp:** proporciona información sobre el momento en que el mensaje SysLog se generó. Es recomendable utilizar el protocolo NTP para establecer una buena sincronización.

**Mensaje:** contiene el mensaje SysLog generado por el dispositivo y alguna información adicional sobre el proceso que generó el mensaje.

1. *Chapters 8.1, 8.2, 8.3 and 8.4 - Netflow (3 pages)*
   1. *Find an example of a Netflow analysis output record and briefly comment it.*

Netflow es uno de los protocolos más utilizados para la recolección de estadísticas de red y desarrollado por Cisco Systems Inc. La versión 9, a diferencia de la versión 5, oferta un formato de mensaje flexible y soporte para MPLS e IPv6.

Si por ejemplo utilizamos el comando “*show flow record*” en el terminal, podemos mostrar el estado actual del monitor de flujo que nosotros deseemos (Figura 3). Con el siguiente comando “*show flow monitor name FLOW-MONITOR-1 cache format record*” mostamos el estado, estadísticas y datos de flujo en la memoria caché para un determinado monitor de flujo (Figura 4).

**Figuras 3 (izq.) y 4 (der.) – Estado actual del monitor de flujo especificado, estadísticas y datos de flujo**

*3 - Take a look at the TF-NOC Survey document:*

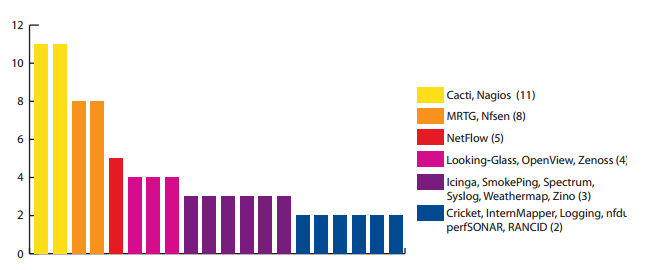
*3.1 Who has been asked?*

Metodología que se implementó para crear una visión visible de responsabilidades, para seguir un estándar/mejores prácticas/directrices que también son seguidas por el cliente (lengua común, seguridad) y para tener un mejor rendimiento. Mejora el soporte al usuario, permite la obtención de acreditación y fue una respuesta proactiva cuando la industria financiera cambió los diferentes requisitos.

*3.2 Identify the categories in which the tools have been categorized. Connect them with the concepts you learned in the GEANT document.*

Las diferentes herramientas NOC son las siguientes:

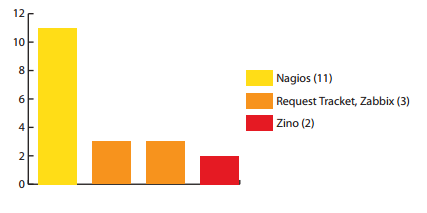
**1 - Monotorización**



**Gráfica 1 – Herramienta de monotorización**

Cada herramienta tiene los comentarios de las empresas que las hayan utilizado, pero todos coinciden que es una herramienta útil, práctica, sencilla de utilizar, tiene una interfaz bonita y amigable y, por último, es fiable.

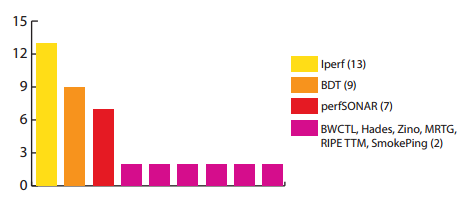
**2 - Gestión de problemas**



**Gráfica 2 – Herramienta de gestión de problemas**

Esta herramienta no presenta ningún tipo de comentario al respecto.

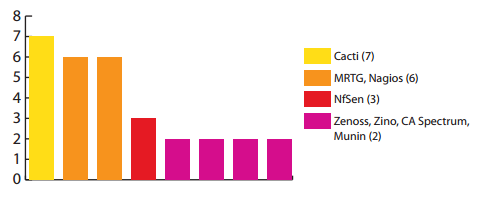
**3 – Gestión de rendimiento**



**Gráfica 3 – Herramienta de gestión de rendimiento**

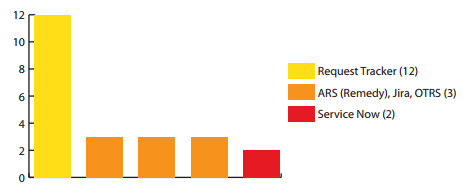
Comentarios: útil para para lidiar con los problemas de los clientes y fácil de utilizar y configurar. Algún organismo como IPerf dice que los usuarios requieren conocimientos previos.

**4 – Informes y estadísticas**



**Gráfica 4 – Herramienta de informes y estadísticas**

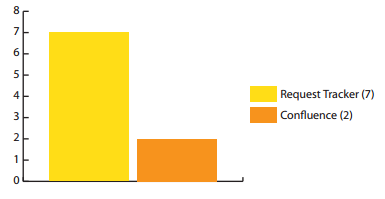
Comentarios: poco amigable para usuarios particulares, pero puede hacer cinetos de informes auto-configurados. Los archivos de texto sin formato, fáciles de adaptar. Muestra estadísticas sobre la utilización de ancho de banda.

**5 – Ticketing**

**Gráfica 5 – Herramienta de ticketing**

Comentarios: bajo mantenimiento, fiable y muy configurable. En cambio, no es muy eficiente, acceso a web bastante pobre y el buscador se puede mejorar.

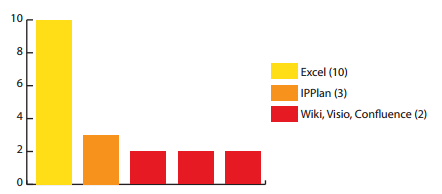
**6 – Cambio de gestión**



**Gráfica 6 – Herramienta de cambio de gestión**

Comentarios: fácil de configurar y administrar, bastante útil.

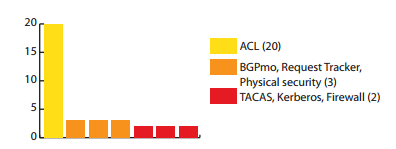
**7 – Gestión de recursos**



**Gráfica 7 – Herramienta de gestión de recursos**

Comentarios: fácil de utilizar, tienes que registrar todos los recursos. NO soporta IPv6.

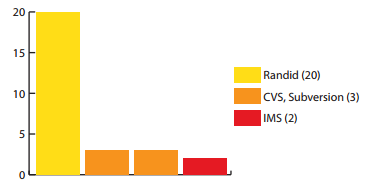
**8 – Gestión de seguridad**



**Gráfica 8 – Herramienta de gestión de seguridad**

Comentarios: le faltan bastantes cosas, no es suficiente.

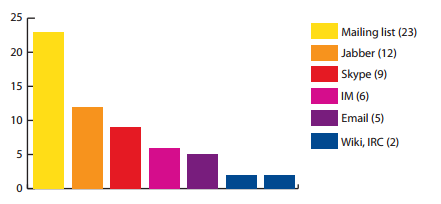
**9 – Configuración de gestión y backup**



**Gráfica 9 – Herramienta de configuración de gestión y backup**

Comentarios: fácil de usar y fiable. No hay medidas avanzadas y un poco de esfuerzo para el mantenimiento.

**10 – Comunicación, coordinación y chat**



**Gráfica 10 – Herramienta para la comunicación, coordinación y chat**

Comentarios: el uso de la característica de sala es muy útil. Si se va la luz, adiós herramienta.

*3.3 Which seem to be the most popular tools? Which aspects do they cover?*

1. Monitoreo: Cacti y Nagios.

2. Resolución de problemas: Nagios.

3. Rendimiento: Iperf.

4. Reporting: Cacti.

5. Ticketing: Request Tracker.

6. Change Management: Request Tracker.

7. Gestión de la configuración y backup: Randid.

8. Comunicación, coordinación, chat: Mailing list.

9. Documentación: Wiki.

10. Gestión de la seguridad: ACL.

11. Gestión de inventario: Excel.

12. Gestión de recursos: Excel.

13. Out-of-band access: Console Server.

14. Data aggregation, representation, visualisation: Cacti y Weatherma

*4 - Read the slides about Traffic Monitoring. Try to get a clear idea of the concepts presented.*