

**Instituto Politecnico Nacional**

**ESCOM “ESCUELA SUPERIOR DE CÓMPUTO”**

*ADMINISTRACIÓN DE SERVICIOS EN RED*

*DISEÑO DE UNA RED FCAPS*

PROFE: RICARDO MARTÍNEZ ROSALES

ALUMNOS: Rojas Alvarado Luis Enrique

Miranda Sandoval Mario A

Hernández Escobedo Fernando

GRUPO: 4CM1

**Gestión de fallos**

¿Tiene la organización un ping poller que considere una falla cuando un dispositivo no responde a un ping? ¿Se monitorizan los traps SNMP, y traps específicos son considerados como fallas? ¿Se monitorizan los registros del sistema (syslog) y mensajes específicos dan lugar a una falla? ¿Se supervisa el estado del hardware del dispositivo y se consideran fallas por eventos como falla en el suministro de energía, falla del sistema redundante, temperatura del dispositivo, etc.? ¿Se envían los fallos al sistema de servicio de atención y se administran mediante un proceso de gestión de incidentes?

1. Un ping poller es un sistema automático que interroga a todos los dispositivos de la organización haciéndo ping y que garantiza que toda la topología funciona y tienen un rendimiento óptimo, detectando paquetes perdidos o latencia en la comunicación de los dispositivos.
2. Por otro lado, el Protocolo Simple de Administración de Red o SNMP (en inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más. Nos permitirá supervisar el funcionamiento de la red, buscar y resolver sus problemas.

Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP.

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el siguiente formato:



* Versión: Número de versión de protocolo que se está utilizando (por ejemplo 0 para SNMPv1, 1 para SNMPv2c, 2 para SNMPv2p y SNMPv2u, 3 para SNMPv3, ...).
* Comunidad: Nombre o palabra clave que se usa para la autenticación. Generalmente existe una comunidad de lectura llamada "public" y una comunidad de escritura llamada "private".
* SNMP PDU: Contenido de la Unidad de Datos de Protocolo, el que depende de la operación que se ejecute.

Los mensajes GetRequest, GetNextRequest, SetRequest y GetResponse utilizan la siguiente estructura en el campo SNMP PDU:

* Identificador: Es un número utilizado por el NMS y el agente para enviar solicitudes y respuesta diferentes en forma simultánea;
* Estado e índice de error: Sólo se usan en los mensajes GetResponse´(en las consultas siempre se utiliza cero). El campo "índice de error" sólo se usa cuando "estado de error" es distinto de 0 y posee el objetivo de proporcionar información adicional sobre la causa del problema. El campo "estado de error" puede tener los siguientes valores:

0: No hay error;

1: Demasiado grande;

2: No existe esa variable;

3: Valor incorrecto;

4: El valor es de solo lectura;

5: Error genérico.

* Enlazado de variables: Es una serie de nombres de variables con sus valores correspondientes (codificados en ASN.1).

GetRequest: A través de este mensaje el NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre. En respuesta el agente envía una respuesta indicando el éxito o fracaso de la petición. Si la petición fue correcta, el mensaje resultante también contendrá el valor del objeto solicitado. Este mensaje puede ser usado para recoger un valor de un objeto, o varios valores de varios objetos, a través del uso de listas.

GetNextRequest: Este mensaje es usado para recorrer una tabla de objetos. Una vez que se ha usado un mensaje GetRequest para recoger el valor de un objeto, puede ser utilizado el mensaje GetNextRequest para repetir la operación con el siguiente objeto de la tabla. Siempre el resultado de la operación anterior será utilizado para la nueva consulta. De esta forma un NMS puede recorrer una tabla de longitud variable hasta que haya extraído toda la información para cada fila existente.

SetRequest: Este tipo de mensaje es utilizado por el NMS para solicitar a un agente modificar valores de objetos. Para realizar esta operación el NMS envía al agente una lista de nombres de objetos con sus correspondientes valores.

GetResponse: Este mensaje es usado por el agente para responder un mensaje GetRequest, GetNextRequest, o SetRequest. En el campo "Identificador de Request" lleva el mismo identificador que el "request" al que está respondiendo.

Trap: Una trap es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración. El formato de la PDU es diferente:



* Enterprise: Identificación del subsistema de gestión que ha emitido el trap;
* Dirección del agente: Dirección IP del agente que ha emitido el trap;
* Tipo genérico de trap:
  + Cold start (0): Indica que el agente ha sido inicializado o reinicializado;
  + Warm start (1): Indica que la configuración del agente ha cambiado;
  + Link down (2): Indica que una interfaz de comunicación se encuentra fuera de servicio (inactiva);
  + Link up (3): Indica que una interfaz de comunicación se encuentra en servicio (activa);
  + Authentication failure (4): Indica que el agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad);
  + EGP neighbor loss (5): Indica que en sistemas en que los routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio;
  + Enterprise (6): En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.
* Tipo específico de trap: Es usado para traps privados (de fabricantes), así como para precisar la información de un determinado trap genérico;
* Timestamp: Indica el tiempo que ha transcurrido entre la reinicialización del agente y la generación del trap;
* Enlazado de variables: Se utiliza para proporcionar información adicional sobre la causa del mensaje.

GetBulkRequest: Este mensaje es usado por un NMS que utiliza la versión 2 o 3 del protocolo SNMP típicamente cuando es requerida una larga transmisión de datos, tal como la recuperación de largas tablas. En este sentido es similar al mensaje GetNextRequest usado en la versión 1 del protocolo, sin embargo, GetBulkRequest es un mensaje que implica un método mucho más rápido y eficiente, ya que a través de un solo mensaje es posible solicitar la totalidad de la tabla.

InformRequest: Un NMS que utiliza la versión 2 o 3 del protocolo SNMP transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados, utilizando el protocolo de nivel 4(OSI) TCP, y enviara el InformRequest hasta que tenga un acuse de recibo. [1]

1. Syslog es el acrónimo de System Logging Protocol, que significa protocolo de registro del sistema. Se trata de un protocolo estándar utilizado para enviar mensajes de registro o eventos del sistema a un servidor específico, llamado servidor de syslog. El syslog se utiliza principalmente para recopilar varios registros de dispositivos de diversas máquinas diferentes en una ubicación central para la supervisión y su análisis.

El protocolo está habilitado en la mayoría de equipos de red, como *routers*, *switches*, cortafuegos e incluso en algunas impresoras y escáneres. Además, syslog está disponible en sistemas basados en Linux/Unix y en muchos servidores web como Apache. Syslog no está instalado de manera predeterminada en los sistemas Windows, que usan su propio registro de eventos; si bien es capaz de reenviarlos a través de herramientas de terceros u otras configuraciones utilizando el protocolo Syslog.

El protocolo está habilitado en la mayoría de equipos de red, como routers, switches, cortafuegos e incluso en algunas impresoras y escáneres. Además, syslog está disponible en sistemas basados en Linux/Unix y en muchos servidores web como Apache. Syslog no está instalado de manera predeterminada en los sistemas Windows, que usan su propio registro de eventos; si bien es capaz de reenviarlos a través de herramientas de terceros u otras configuraciones utilizando el protocolo Syslog.

1. Free Windows Admin Tools ofrece tres herramientas: Remote Task Manager, Remote Device Manager y Remote Desktop Connection. Remote Device Manager te muestra información sobre los componentes de hardware de cada computadora. Te servirá para hacer un inventario del hardware disponible sin desplazarte físicamente. Pruebas de Diagnóstico.- Diseñar y realizar pruebas que apoyen la localización de una falla (Pruebas de conectividad física, pruebas de conectividad lógica, pruebas de medición).
2. Administración de Reportes.- Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

El ciclo de vida de la administración de reportes se divide en 4 áreas:

Creación de Reportes.- Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema en la red.

Seguimiento a Reporte.- La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte.

Manejo de Reportes.- El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso.

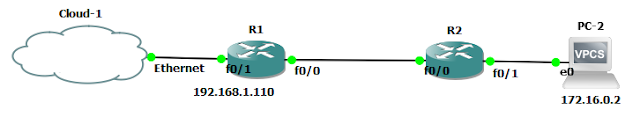
Finalización de Reportes.- Una vez que el problema reportado ha sido solucionado, el administrador del sistema de reportes, debe dar por cerrado el reporte.

**Gestión contable**

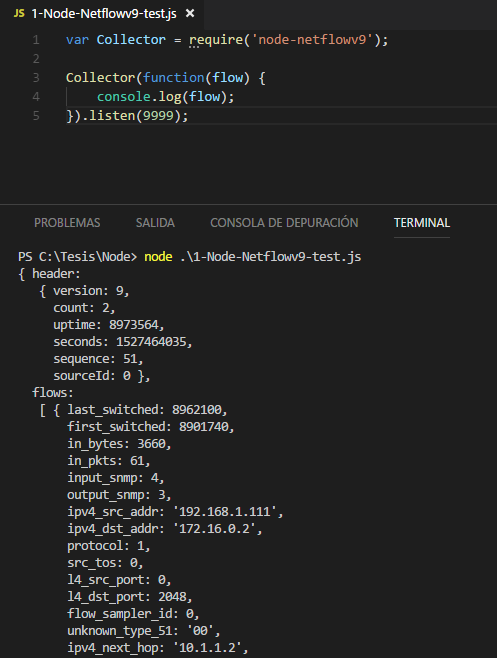
¿Está habilitada la exportación de NetFlow o equivalente en todos los dispositivos? ¿Se recogen y almacenan datos NetFlow o equivalentes? ¿Se clasifican los datos almacenados según el tipo de servicio o la aplicación? ¿Pueden los datos recopilados ser atribuidos a usuarios o grupos de usuarios específicos? ¿Se hacen ajustes contables por violaciones de SLA?

1. El primer paso hacia la administración de contabilidad apropiada es medir la utilización de los recursos de red importantísimos. La utilización de los recursos de red se puede medir usando las características de contabilidad IP NetFlow de Cisco y de Cisco.

NetFlow (flujo de red) es una tecnología de medición de lado de entrada que permite capturar los datos requeridos para aplicaciones de planificación, supervisión y contabilidad de redes. El Netflow se debe desplegar en los interfaces del borde/del router de la agregación para los proveedores de servicio o los interfaces del router de acceso a WAN para los clientes de la empresa.

 **enable**

configure terminal  
  interface FastEthernet0/1  
    ip route-cache flow  
    exit  
ip flow-export destination 192.168.1.111 9999  
ip flow-export source FastEthernet0/1  
ip flow-export version 9  
ip flow-cache timeout active 1  
ip flow-cache timeout inactive 15  
exit  
write



1. Un Service Level Agreement (SLA) es un contrato que describe el nivel de servicio que un cliente espera de su proveedor.

# **Referencias**

|  |  |
| --- | --- |
| [1] | L. T. Rocamora, «Servicios de Red e Internet,» 2 Febrero 2015. [En línea]. Available: https://es.slideshare.net/Lord\_LT/prctica-snmp-servicios-de-red. [Último acceso: 2 Noviembre 2020]. |
| [2] | A. Telesis, «Ping Polling,» [En línea]. Available: https://www.alliedtelesis.com/sites/default/files/documents/feature-guides/ping\_polling\_feature\_overview\_guide\_revb.pdf. [Último acceso: 2 Noviembre 2020]. |
| [3] | PAESSLER, «It Explained: Syslog,» [En línea]. Available: https://www.es.paessler.com/it-explained/syslog. [Último acceso: 2 Noviembre 2020]. |
| [4] | B. It, «Blue It,» 6 Abril 2017. [En línea]. Available: https://blueit.com.ec/blog/item/225-administrar\_hadware\_software.html. [Último acceso: 2 Noviembre 2020]. |
| [5] | S. O. V. Manuel‎, «Mi sitio personal,» [En línea]. Available: https://sites.google.com/a/itdurango.edu.mx/10040372/home/administracion-de-redes/unidad-i. [Último acceso: 2 Noviembre 2020]. |
| [6] | Anonimous, «Desde otra perspectiva,» 27 Mayo 2018. [En línea]. Available: http://solarisdmt.blogspot.com/2018/05/gns3-configuracion-basica-de-netflow-y.html. [Último acceso: 2 Noviembre 2020]. |
| [7] | Cisco, «Sistema de administración de red: Informe oficial de Mejores Prácticas,» 10 Agosto 2018. [En línea]. Available: https://www.cisco.com/c/es\_mx/support/docs/availability/high-availability/15114-NMS-bestpractice.html. [Último acceso: 2 Noviembre 2020]. |