5º curso de Ingeniería de Telecomunicación
Asignatura: Gestión de Red
Práctica 3

Estudio de los formatos de los mensajes del protocolo SNMP

OBJETIVOS DE LA PRÁCTICA

Los principales objetivos de esta práctica son:

- Familiarizarse con el manejo de un analizador de red.
- Generar las diferentes primitivas del protocolo de gestión SNMP.
- Estudiar los formatos de los mensajes SNMP(RFC 1157).

INTRODUCCIÓN

1. Formato de las Tramas SNMP

SNMP permite el intercambio de información a través de la red entre la estación de gestión y el agente en forma de mensajes SNMP. Cada mensaje incluye un número de versión que indica la versión de SNMP, un nombre de comunidad utilizado en el intercambio, y uno de los cinco tipos de PDU's definidos: GetRequest, GetNextRequest, SetRequest, GetResponse y Trap.

Las tramas tienen el siguiente formato:

Versión	Comunidad	SNMP PDU

Donde:
Versión indica la versión del protocolo. RFC 1157 es versión 1.
Comunidad es el nombre de la comunidad y sirve para autentificar el mensaje SNMP.

PDU SNMP depende del tipo de operación a realizar. Este puede ser:

- **Si se trata de GetRequest, GetNextRequest o SetRequest tendremos:**

PDU type	Request Id	0	0	Variable Bindings

PDU type: indica el tipo de PDU,
Request Id: se utiliza para diferenciar las distintas peticiones, añadiendo a cada una de ellas un único identificador.
Variable Bindings: es una lista de nombres de variables y sus correspondientes valores. En algunos casos (GetRequest), el valor de las mismas es NULL. En el caso de las Traps,

proporcionan información adicional relativa a la Trap, dependiendo el significado de este campo de cada implementación en particular.

- **Si se trata de GetResponse :**

PDU type	Request Id	Error-status	Error-index	Variable Bindings

Error-status: se utiliza para indicar que a ocurrido una excepción durante el procesamiento de una petición. Sus valores posibles son: **noError**(0), **tooBig**(1), **noSuchName**(2), **badValue**(3), **readOnly**(4), **genErr**(5).
Error-index: cuando el campo **Error-status** es distinto de 0, puede proporcionar información adicional indicando la variable que causó la excepción.

- **Si se trata de un Trap:**

PDU type	Enterprise	agent-addr	generic-trap	specific-trap	timestamp	Variable Bindings

Enterprise: Identifica el subsistema de gestión de red que ha emitido el Trap.
Agent-addr. : Dirección IP del agente que generó el Trap.
Generic-trap: Tipo de Trap genérico predefinido. Puede ser:

- **coldStart**(0): el agente se ha reinicializado, de forma que se puede alterar la configuración de los agentes o la implementación del protocolo. Típicamente reinicio por caída del sistema.
- **warmStart**(1):la entidad emisora SNMP se ha reinicializado sin haberse alterado la configuración de los Agentes ni la implementación del protocolo. Usualmente es una rutina de tipo restart.
- **linkDown**(2): señaliza un fallo en alguno de los enlaces de comunicación del Agente. El primer elemento en el campo Variable-Bindings indicará el interfaz en cuestión.
- **linkUp**(3): señaliza el restablecimiento de uno de los enlaces de comunicación del Agente. El primer elemento en el campo Variable-Bindings indicará el interfaz en cuestión.
- **authentificationFailure**(4): indica que la entidad emisora del Trap ha recibido un mensaje en el que ha fallado la autentificación.
- **egpNeighborLoss**(5): indica que un EGP (External Gateway Protocol) vecino, para el cual la entidad emisora tenía asociado otro EGP, ha sido desmarcado y la relación entre ambos EGPs ha finalizado.
- **enterpriseSpecific**(6): significa que la entidad emisora reconoce que algún evento específico del fabricante ha ocurrido. El campo specific-trap indica el tipo de Trap.
- **Specific-trap**: código de Trap específico e indica de una forma más específica la naturaleza del Trap.

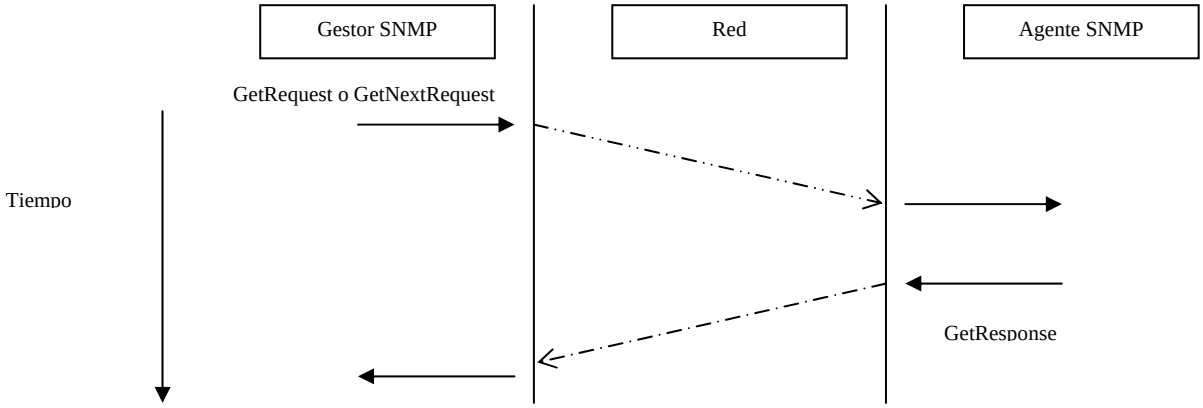
Timestamp: Tiempo transcurrido entre la última reinicialización de la entidad de red y la generación del trap.

2. Transacciones SNMP.

Como hemos comentado anteriormente las operaciones básicas en SNMP son:

- De obtención de datos: **GetRequest**, **GetNextRequest**;
- De modificación: **SetRequest**;
- De aviso: **Trap**.

Ejemplo de la transacción de obtención de datos:



DESARROLLO DE LA PRACTICA

1. Generación y captura de transacciones SNMP.

- Con la ayuda de una aplicación que realice la función gestora, estudiar como efectuar los distintos tipos de transacciones SNMP posibles sobre un agente accesible en el laboratorio. (**GetRequest, GetNextRequest, SetRequest, Trap).**
- Realizar dichas transacciones, y capturarlas en el analizador de red de cada puesto de trabajo, para su posterior análisis.

2. Responder a las siguientes preguntas

a) ¿Qué protocolos intervienen en generación y envío de una transacción SNMP?

b) ¿Qué puertos UDP se utilizan en las transacciones de petición o modificación de datos, en el agente y en el gestor? y ¿en las de aviso? Realiza un dibujo explicativo.

c) En una trama GetRequest ¿cuál es la utilidad del campo Request- Id?

d) En una transacción de petición de datos de un agente, ¿qué valor tiene el campo Variable-Bindings, en la trama GetRequest?

e) Describe una petición de un GetNextRequest realizada a un objeto de tipo estructural de la MIB de un agente.

f) Analiza una transacción de modificación y compara los campos Variable-Bindings de la petición (al agente) y la respuesta (del agente).

g) Intenta capturar o generar una transacción de aviso (Trap), y analiza sus campos.