

# SNMP

**(SIMPLE NETWORK MANAGEMENT PROTOCOL)**

# Integrantes

- ❖ Chuquimia, Clever
- ❖ Zapatero, Noel
- ❖ Acevedo, Jorge

# Temas a Tratar

- Componentes Básicos de SNMP
- MIB (Management Information Base)
- Gestión SNMP
- Interoperabilidad
- Formatos de Mensaje
- Compendio de Traps y Mensajes

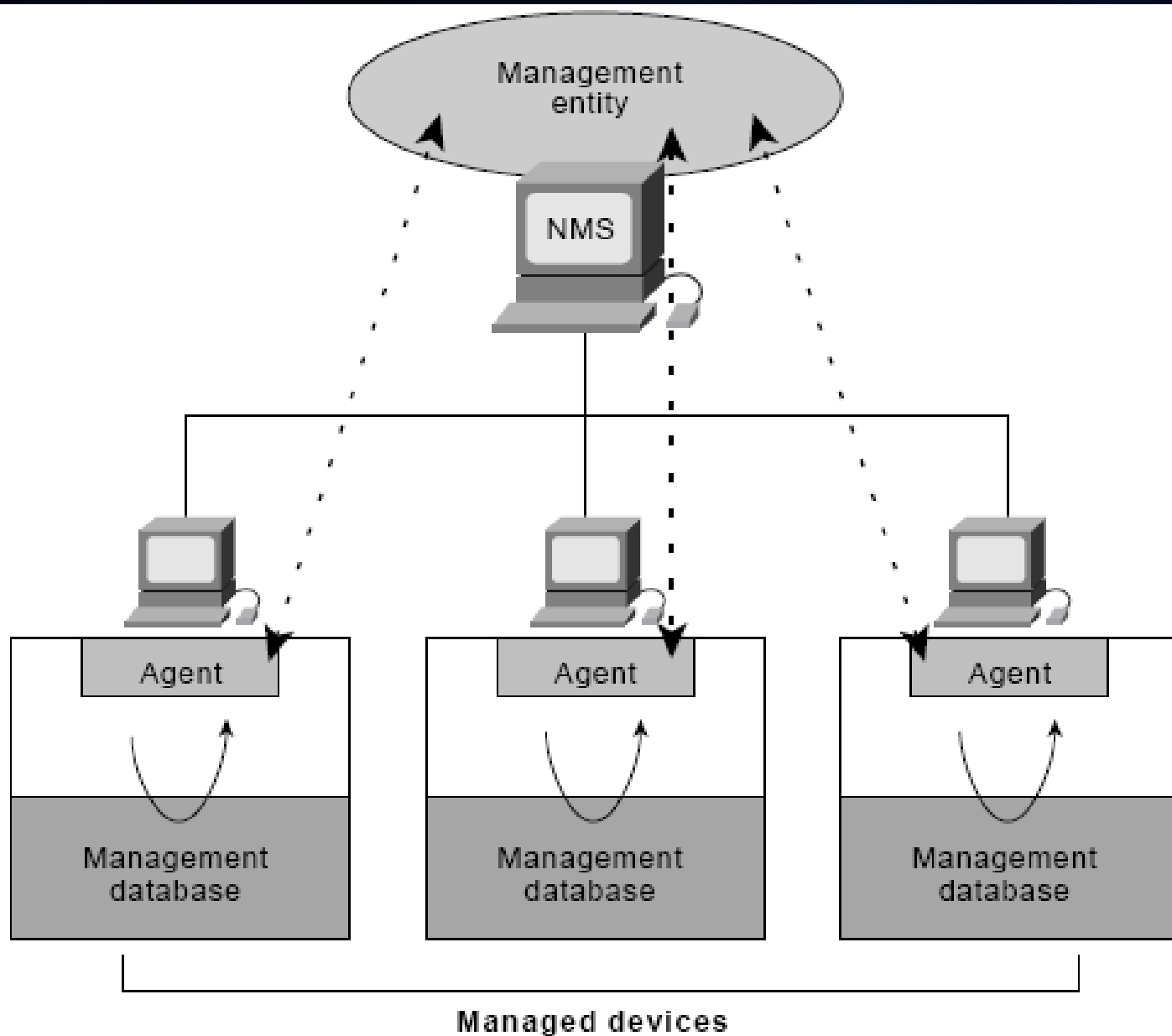
# Breve Reseña

- Sólo contaban con herramientas de gestión de red como:
  - ICMP
  - PING (Packet Internet Gruper)
  - Trace-Route

# Componentes Básicos de SNMP

Una red administrada con SNMP consiste de tres componentes fundamentales:

- Dispositivos administrados. **Managed Devices (MD)**
- Agentes. **Agent**
- Administrador de sistemas en **NMS**  
la Red.



# Comandos Básicos SNMP

Los *Dispositivos administrados* (MD) son supervisados y controlados utilizando 4 comandos SNMP básicos:

- **Read** (utilizado por los NMS)
- **Write** (utilizado por los NMS)
- **Trap** (utilizado por los MD)
- **Operaciones de recorrido (Traversal Operations)**  
(utilizadas por los NMS)

# Management Information Base (MIB)

- Es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red.

## La definición del tipo de objeto consta de cinco campos:

- **Objeto:** nombre textual, para el tipo del objeto, junto con su correspondiente OID, definido abajo (el OID se escribe al final de la definición del objeto).
- **Sintaxis:** la sintaxis abstracta para el tipo de objeto. Las opciones son SimpleSyntax (entero, octeto de caracteres, identificador de objeto, Null), ApplicationSyntax (dirección de red, contador, escala) u otro tipo de sintaxis de aplicación.
- **Definición:** descripción textual de la semántica del tipo.
- **Acceso:** sólo lectura, sólo escritura, lectura - escritura o inaccesible.
- **Status:** obligatorio, opcional u obsoleto.

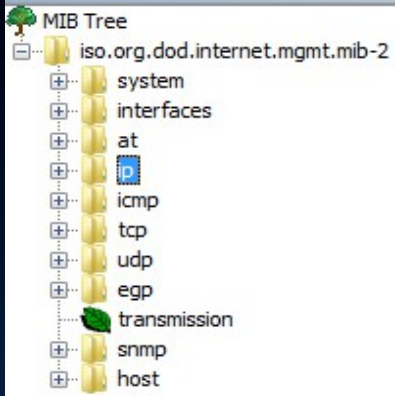
# Tipos de nodos

Existen dos tipos de nodos que conforman una MIB: estructurales y de información.

- Los **nodos estructurales** sólo tienen descrita su posición en el árbol. Son "ramas". Por ejemplo:

ip OBJECT IDENTIFIER ::= { 1 3 6 1 2 1 4 }

SNMP MIBs



Name	ip
OID	.1.3.6.1.2.1.4
MIB	RFC1213-MIB
Syntax	
Access	
Status	
DefVal	
Indexes	
Descr	

- Los **nodos con información** son nodos "hoja". De ellos no cuelga ningún otro nodo. Estos nodos están basados en la macro OBJECT TYPE, por ejemplo:

ipInReceives      OBJECT TYPE

SYNTAX            Counter

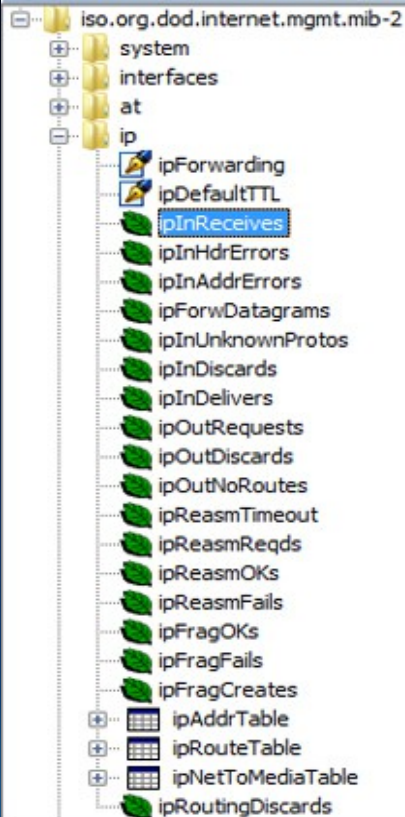
ACCESS            read-only

STATUS            mandatory

DESCRIPTION      "El número total de datagramas de entrada recibido de las interfaces, incluyendo los recibidos por error."

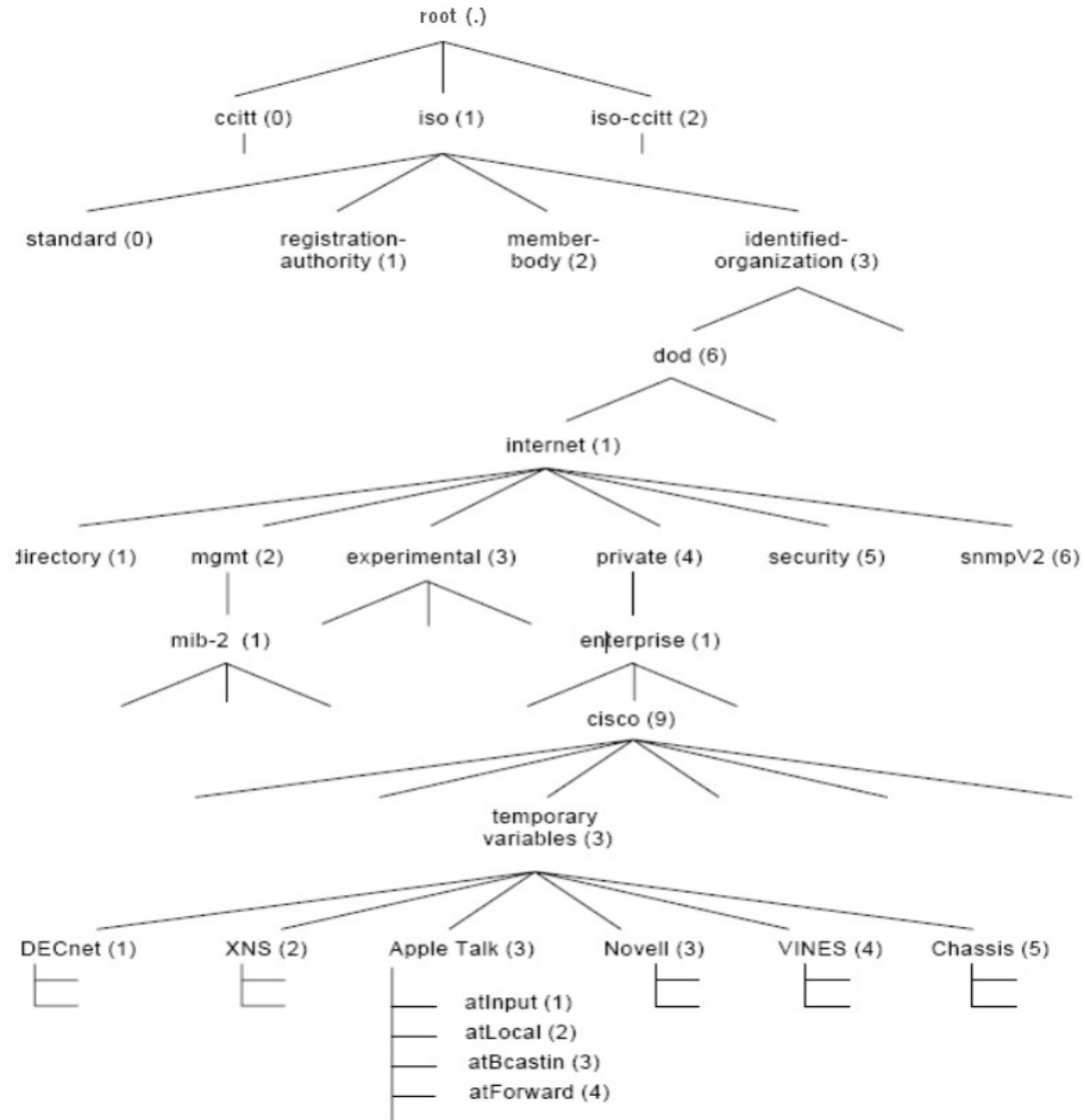
::= { ip 3 }

## SNMP MIBs



Name	ipInReceives
OID	.1.3.6.1.2.1.4.3
MIB	RFC1213-MIB
Syntax	COUNTER
Access	read-only
Status	mandatory
DefVal	
Indexes	
Descr	The total number of input datagrams received from interfaces, including those received in error .

# Ejemplo de árbol MIB

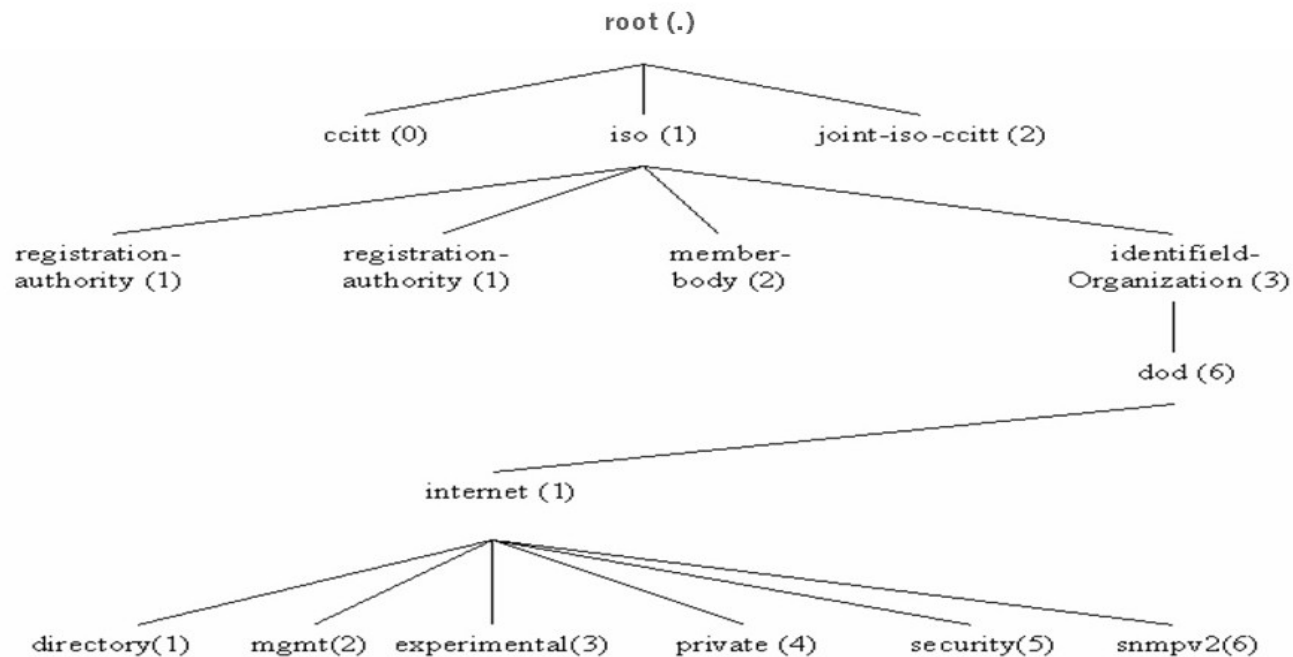


Tomamos como objeto administrado atForward (4) que podría ser identificado por el OID (identificador del objeto):

**Iso.identified-organization.dod.internet.private.enterprise.AppleTalk.atForward**

O por el descriptor de objeto equivalente:

**.1.3.6.1.4.1.9.3.3.4**



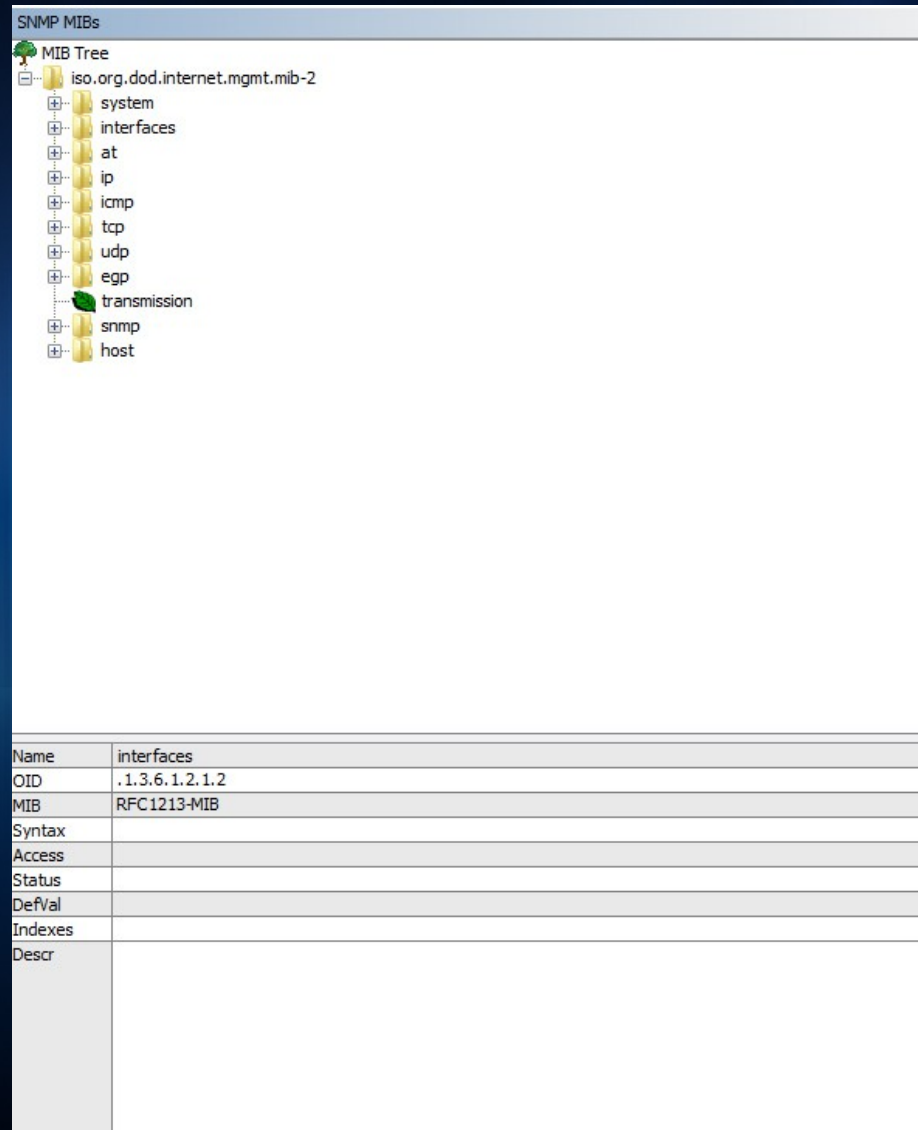
La ubicación sería:

***.iso.org.dod.internet.mgmt***

O de la forma numérica:

***.1.3.6.1.2***

# MIB-II se compone de los siguientes nodos estructurales:



SNMP MIBs

MIB Tree

- iso.org.dod.internet.mgmt.mib-2
  - system
  - interfaces
  - at
  - ip
  - icmp
  - tcp
  - udp
  - egg
  - transmission
  - snmp
  - host

Name	interfaces
OID	.1.3.6.1.2.1.2
MIB	RFC1213-MIB
Syntax	
Access	
Status	
DefVal	
Indexes	
Descr	

# Operaciones del Protocolo SNMP

SNMP es un protocolo simple de petición o solicitud / respuesta.

Se pueden utilizar las siguientes operaciones del protocolo:

- **Get**
- **GetNext**
- **Set**
- **Trap**

La versión SNMP V2 define 2 nuevas operaciones de protocolo:

- **GetBulk**
- **Inform**

# Interoperabilidad SNMP

- \*Estrategias de Coexistencia
- \*Diferencias entre SNMPv1 y SNMPv2  
(Headers y PDU)

# Incompatibilidad

- Existen 2 grandes incompatibilidades entre SNMPv1 y SNMPv2:
  - Formato de los Mensajes
  - Operaciones de Protocolo

Por eso la Internet Engineering Task Force generó el RFC 1908 en la que proponía dos estrategias de coexistencia entre ambas versiones de SNMP

# Estrategias

- ❖ Agentes Proxy: Un agente de SNMPv2 actúa como Agente Proxy en función de los dispositivos administrados en SNMPv1.
- ❖ Administración de Sistema Bilingüe: El NMS(o Administrador) cuenta con una base de datos en donde se detalla que versión de SNMP se debe utilizar en cada situación.

# Diferencias en los Mensajes



- Message Header: Tanto en SNMPv1 como en SNMPv2 se componen de la misma forma:
  - Version Number (número de Versión de SNMP)
  - Community Name (Dominio administrativo; es una forma débil de autenticación)

<b>PDU Type</b>	<b>Request ID</b>	<b>Error Status</b>	<b>Error Index</b>	<b>Object 1 Value 1</b>	<b>Object 2 Value 2</b>	<b>Object X Value X</b>
-----------------	-------------------	---------------------	--------------------	-----------------------------	-----------------------------	-----------------------------

### **Enlaces Variables**

- PDU (Protocol Data Unit): A pesar de tener un formato similar, SNMPv2 incorpora nuevos mensajes, por lo que estos poseen una estructura diferente. Los PDU tanto de SNMPv1 y SNMPv2 son de longitud variable según lo establecido por la ASN.1 (norma de sintaxis para representar datos, independiente de la maquina que se este usando). Cada campo refiere a:

- PDU Type: Especifica el tipo de PDU transmitida.
- Request ID: Asocia el SNMP con las respuestas recibidas.
- Error Status: Indica uno de la serie de errores y tipos de errores. Solo las operaciones de respuestas llenan este campo, el resto lo llenan con 0.
- Error Index: Asocia el error con una instancia particular. Solo las operaciones de respuestas llenan este campo, el resto lo llenan con 0.
- Enlaces Variables: Es el campo en donde va la data. Cada enlace asocia un objeto particular con un valor.

# Valores de Error Status y Error Index

- 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

PDU Type	Request ID	Non Repeaters	Max Repetitions	Object 1 Value 1	Object 2 Value 2
----------	------------	---------------	-----------------	---------------------	---------------------

### Enlaces Variables

- PDU GetBulk (SNMPv2): GetBulk es un mensaje implementado en SNMPv2 y cuenta con una estructura diferente:
  - PDU Type: Identifica el tipo como GetBulk.
  - Request ID: Asocia SNMP con las respuestas.
  - Non Repeaters: Especifica el numero de instancias de objetos en los campos de Enlaces Variables que no deberían ser recuperados mas que una vez desde el inicio de la petición
  - Max Repetitions: Especifica el numero máximo de veces que el resto de los objetos de Enlaces Variables (excepto los Non Repeaters) pueden ser recuperados.

Enterprise	Agent Address	Generic Trap Type	Specific Trap Code	Time Stamp	Object 1 Value 1	Object 2 Value 2	Object X Value X
------------	---------------	-------------------	--------------------	------------	------------------	------------------	------------------

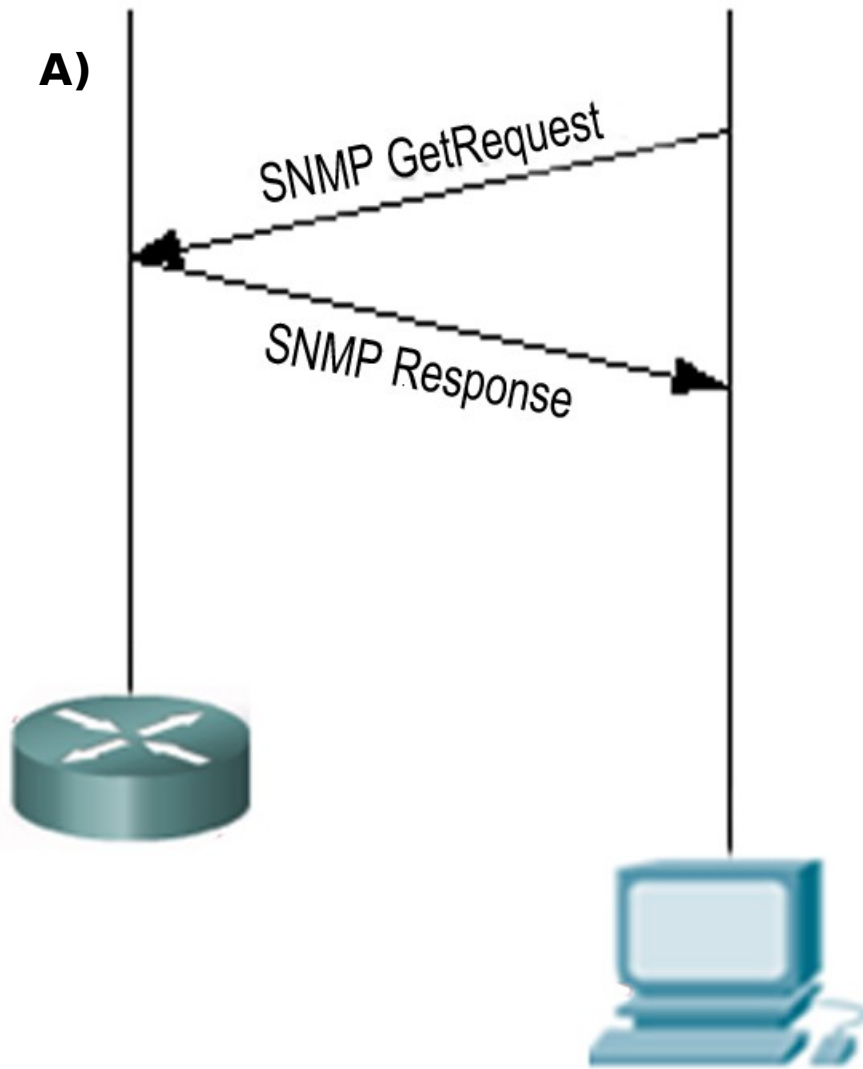
## Enlaces Variables

- PDU Trap: Los traps tanto en SNMPv1 y SNMPv2 tienen un formato diferente al resto, pero iguales entre si:
  - Enterprise: Identifica el tipo de objetos administrados que generan los traps.
  - Agent Address: Provee la dirección de los objetos administrados (dirección IP).
  - Generic Trap Type: Numero de tipo de trap genérico.
  - Specific Trap Code: Numero de código de trap específico.
  - Time Stamp: Provee la cantidad de tiempo transcurrido entre la última conexión realizada y la generación del trap.

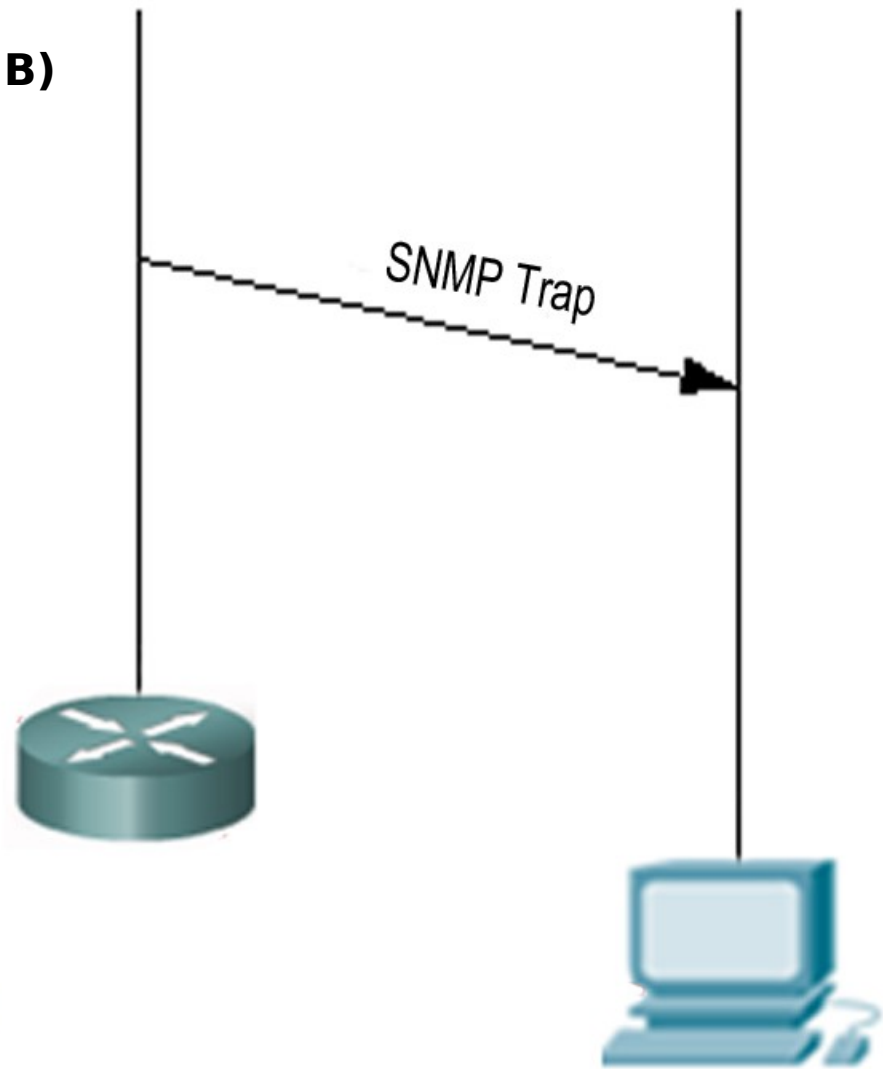
# SNMP TRAPS

- SNMP Traps le permite a un agente notificar a la estación de gestión NMS eventos significantes por medio de mensajes no solicitados SNMP.

**A)**



**B)**



# Utilización de TRAPS

- ❖ Si un administrador de redes es responsable de un gran número de dispositivos y cada dispositivo tiene un gran número de objetos, no es práctico para el obtener o solicitar información desde cada objeto en cada dispositivo. La solución es que cada agente del MD notifique al NMS enviando mensajes Traps sobre eventos relevantes en cada dispositivo y sus objetos.
- ❖ Después de recibir el evento, el administrador lo despliega y puede elegir tomar una acción basada en el evento o puede registrarlo directamente desde el MD y tener una mejor comprensión del evento.

# Mensajes

- Para realizar las operaciones de administración, el protocolo SNMP utiliza un servicio no orientado a conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes.
- Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el siguiente formato:

**Message Header:**  
**Version / Comunidad**

**SNMP PDU:**  
**Get/GetNext/Set/  
GetBulk/Inform**

# Tipos de Request

**GetRequest** : 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.

**GetNextRequest**: 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. 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.

**GetResponse:** Este mensaje es usado por el agente para responder un mensaje GetRequest, GetNextRequest, o SetRequest.

**GetBulkRequest:** 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 ó 3 del protocolo SNMP transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados.