Gestión de Redes: Protocolo SNMP

Ing. Pedro Escudero

Telf: 0994667184
Mail: pedro.escudero@unach.edu.ec
Web: https://www.researchgate.net/profile/Pedro-Escudero-3/research

Abril - 2025

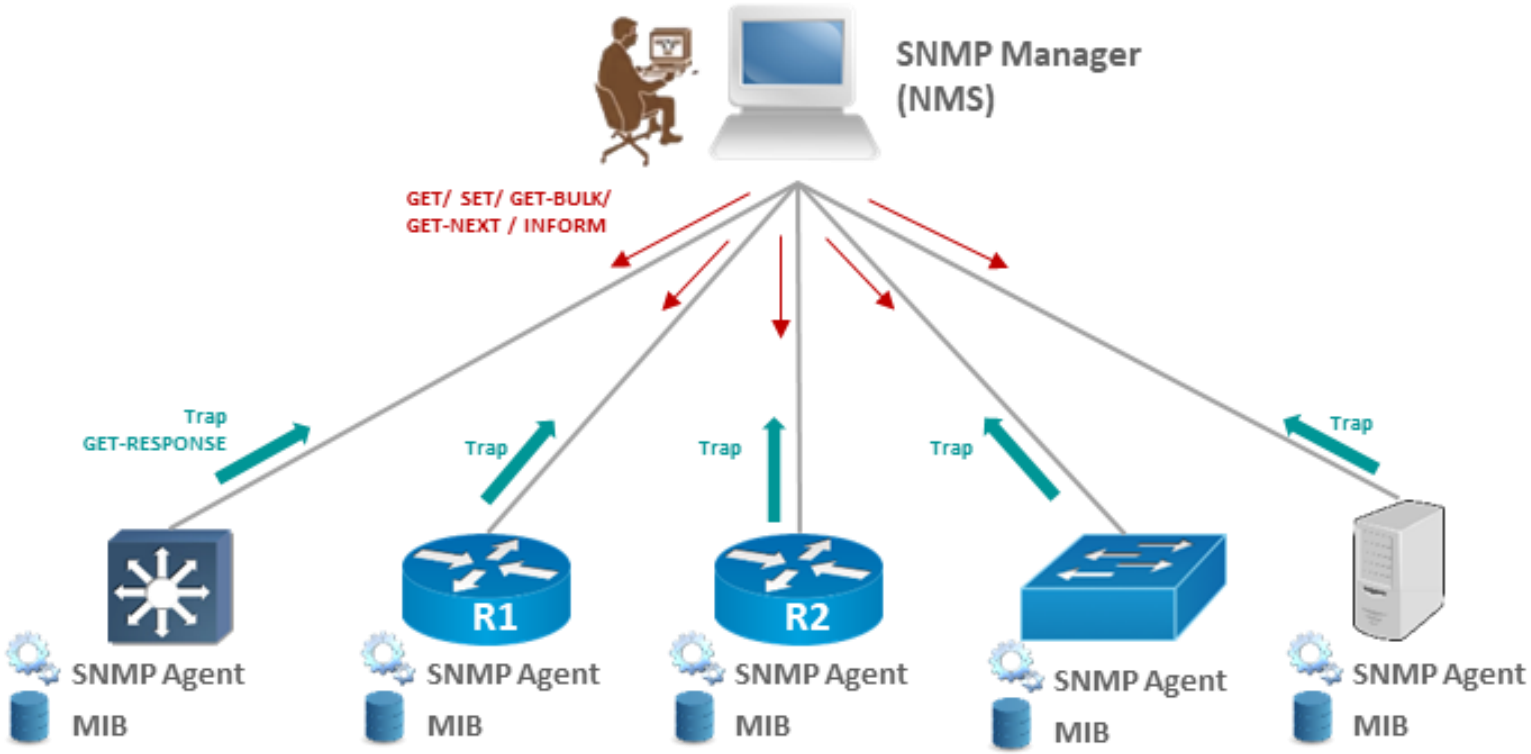
Contenido

1. Introducción

Introducción

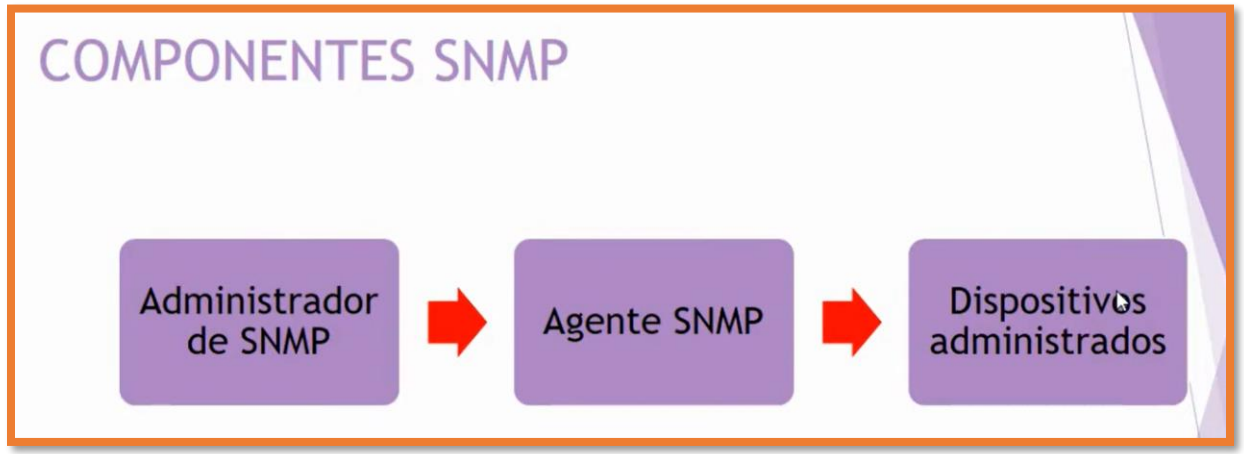
SNMP

- Simple Network Management Protocol (SNMP) es un protocolo de gestión de red muy utilizado, que permite *obtener información de dispositivos de red, memoria libre, uso de la CPU, detección de errores, establecer alarmas, estado de funcionamiento, etc.*



- Protocolo de gestión de red
- En mayo de 1990 se publicó la primera versión SNMP, en el RFC 1157
- Protocolo estándar de la capa de aplicación
- Para el transporte de los paquetes se prevé el protocolo sin UDP
- Utiliza el Puerto por defecto 161 y 162
- Monitoreo de carga de CPU, I/O interface, espacio en disco, temperature, entre otros

- **Introducción**



2. Conceptos Básicos

• Conceptos Básicos

Componentes básicos:
Una red administrada a través de SNMP consta de tres componentes clave:
- Sistemas administradores de red (Network Management System, NMS);
- Dispositivos administrados
- Agentes

Funciones de los componentes:

Un sistema administrado de red (NMS) ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS proporcionan volumen de los recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.

Un dispositivo administrado es un dispositivo que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NM's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, seitches, bridges, hubs, computadores o impresoras.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee conocimiento local de la informacion de administración (memoria libre, número de paquetes IP recibidos, rutas, etc.), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

- **Conceptos Básicos**

Dispositivos administrados

- Puede ser cualquier dispositivo de red, router, swicth, firefall, impresora, ups, balanceadores de carga, sensor de temperatura.
- Puede ser cualquier servidor, físico o virtual.
- Cualquier sistema operativo.
- Puede ser cualquier dispositivo con una IP y un agente SNMP.

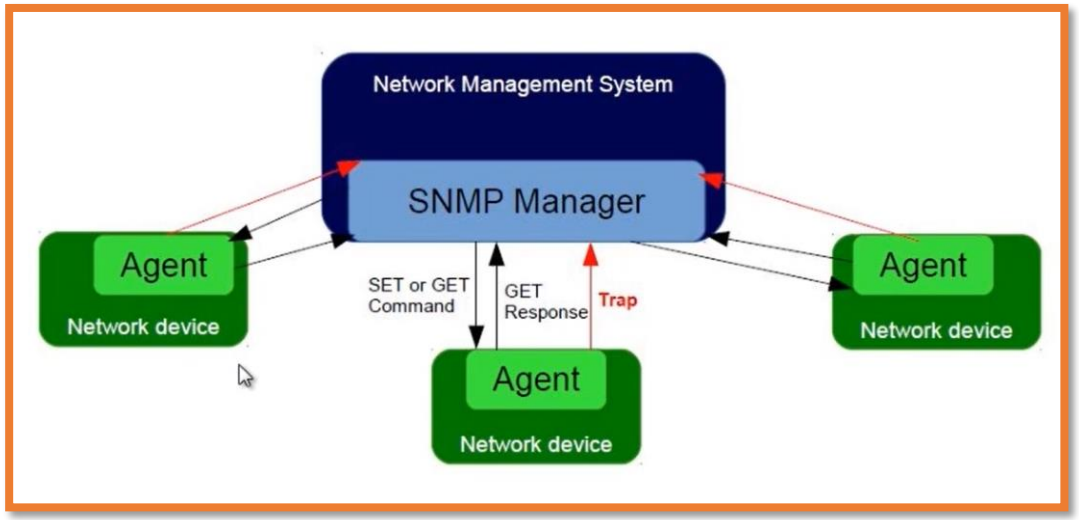
Agente SNMP

- Cada fabricante de dispositivo configura el agente SNMP en el dispositivo administrado.
- Recolecta información administrativa sobre su entorno local.
- Almacena y recupera información administrativa tal como se definió en la base de datos MIB.
- Indica al administrador cuando se produce un evento.
- Ejem: Dispositivo Windows, Unix, cisco.

Administrador de SNMP

- Recolectar información administrativa de los agentes SNMP de los dispositivos administrados y almacenarla de una manera mas legible, puede ser cualquier protocolo de monitoreo de red como OpManager, solarwinds o puede ser cualquier solución de monitoreo de red como NMS o EMS.
- NMS: sistema administrador de red.
- EMS: sistema de gestión de elementos.

• Conceptos Básicos



MIB Management information base

OID Object Identifier

Dispositivo Gestor (Servidor) de SNMP.

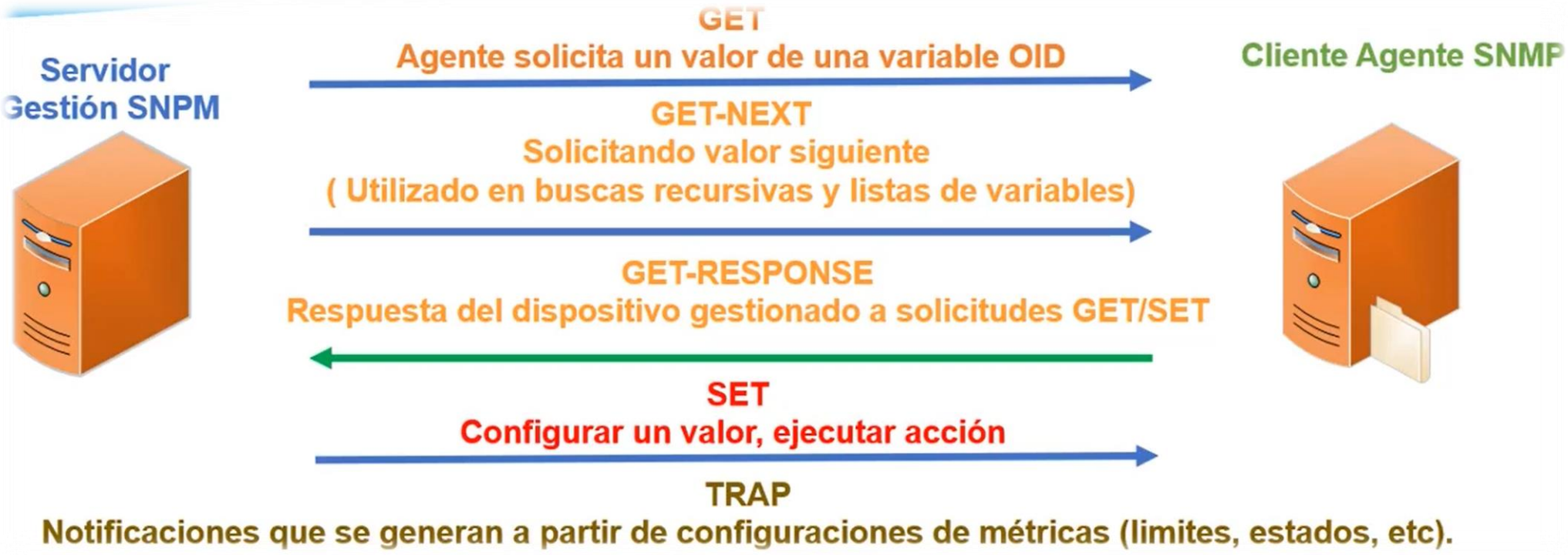
Recopila o setea configuraciones de los equipos gestionados o agentes SNMP.

Agente SNMP (Dispositivo gestionado):

Entrega información a solicitudes del servidor, de sus componentes internos a nivel de software y hardware.

- **Conceptos Básicos**

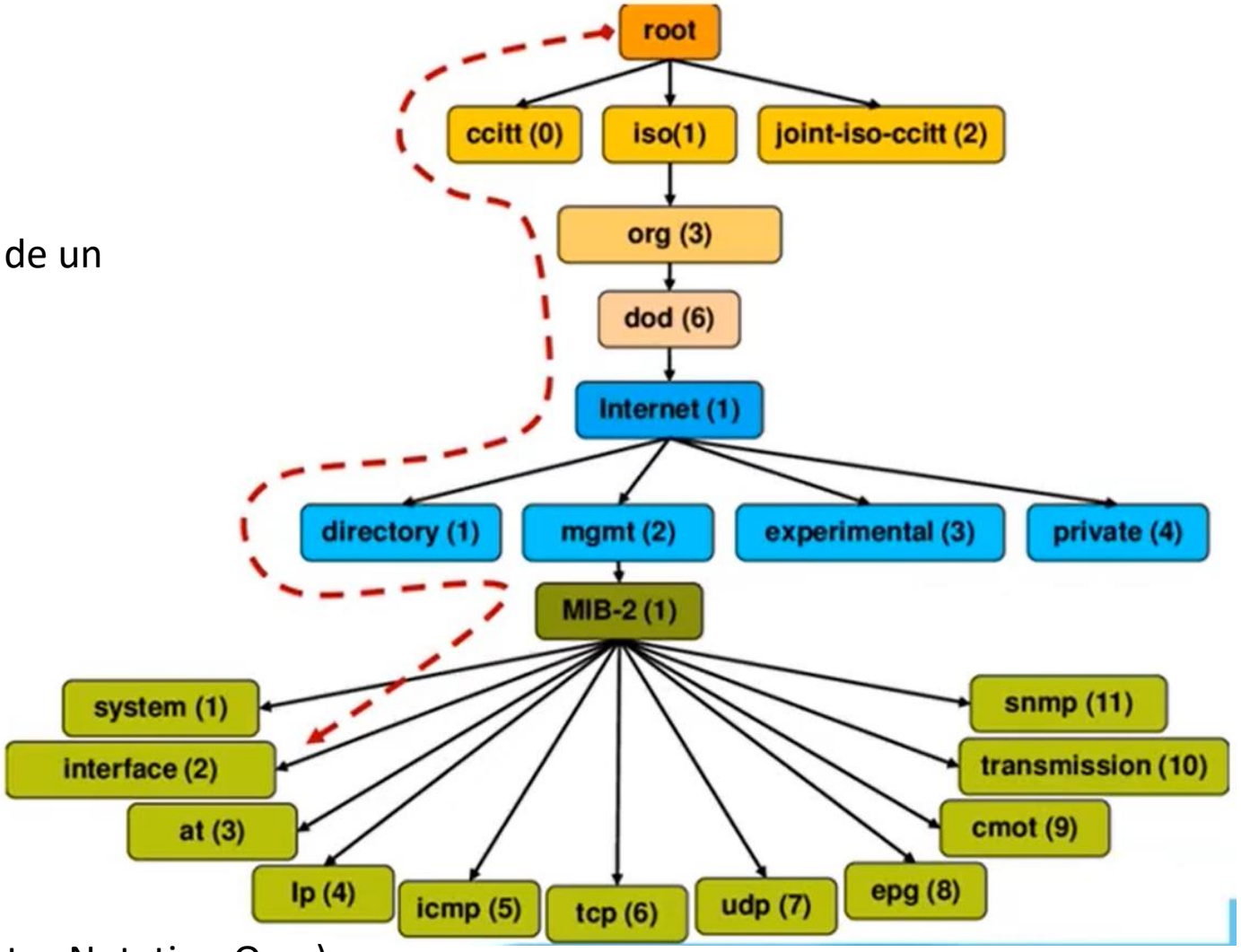
Interacciones de Protocolo



• Conceptos Básicos

Identificadores de Objetos (OID)

Cadena de números que representan la ubicación de un objeto propio del dispositivo gestionado.
Se lee de izquierda a derecha
Ej. 1.3.5.3.2.1
Números jerárquicos similares a DNS



Management Information Base (MIB)

Definen objetos que se puede encuestar
Definidos por:
- Nombre de objeto
- Descripción de objeto
- Tipo de dato

Los archivos tienen estructura ASN.1 (Abstract Syntax Notation.One)
Los MIB estándar incluyen:
- MIB-II-(RFC1213)-un grupo de MIBs secundarios.
- HOST-RESOURCES-MIB (RFC2790)

3. Versiones

- **Versiones**

NORMA	ALIAS	VENTAJAS	DESVENTAJAS
SNMP		▸ Parte de la plataforma TCP/IP. ▸ Norma abierta. ▸ Trabaja con bases de datos MIB definidas.	▸ Excesivo número de peticiones. ▸ Sin comunicación de administrador a administrador. ▸ Sólo soporta TCP/IP. ▸ Sin seguridad.
SNMP2	▸ SMP ▸ SNMP seguro	▸ Soporta recuperación masiva. ▸ Soporta comunicación de administrador a administrador. ▸ Soporta múltiples protocolos. ▸ Proporciona seguridad. ▸ Permite configuración remota.	▸ Nunca se implementó debido a desacuerdos entre las entidades normativas.
SNMP2 Actualizado	▸ SNMP2t ▸ SNMP2c ▸ SNMP1.5	▸ Presumiblemente más fácil de implementar, debido a la remoción de las características de seguridad.	▸ Sin característica de seguridad. ▸ Sin comunicación de administrador a administrador. ▸ Sin configuración remota.
SNMP3	▸ SNMP2	▸ Añade las características de seguridad dentro del SNMP2.	▸ Falta de soporte de las organizaciones normativas. ▸ Se ofrece soluciones propietarias de vendedores.

- **Ambientes de trabajo**

Ambiente de trabajo de la herramienta PRTG.

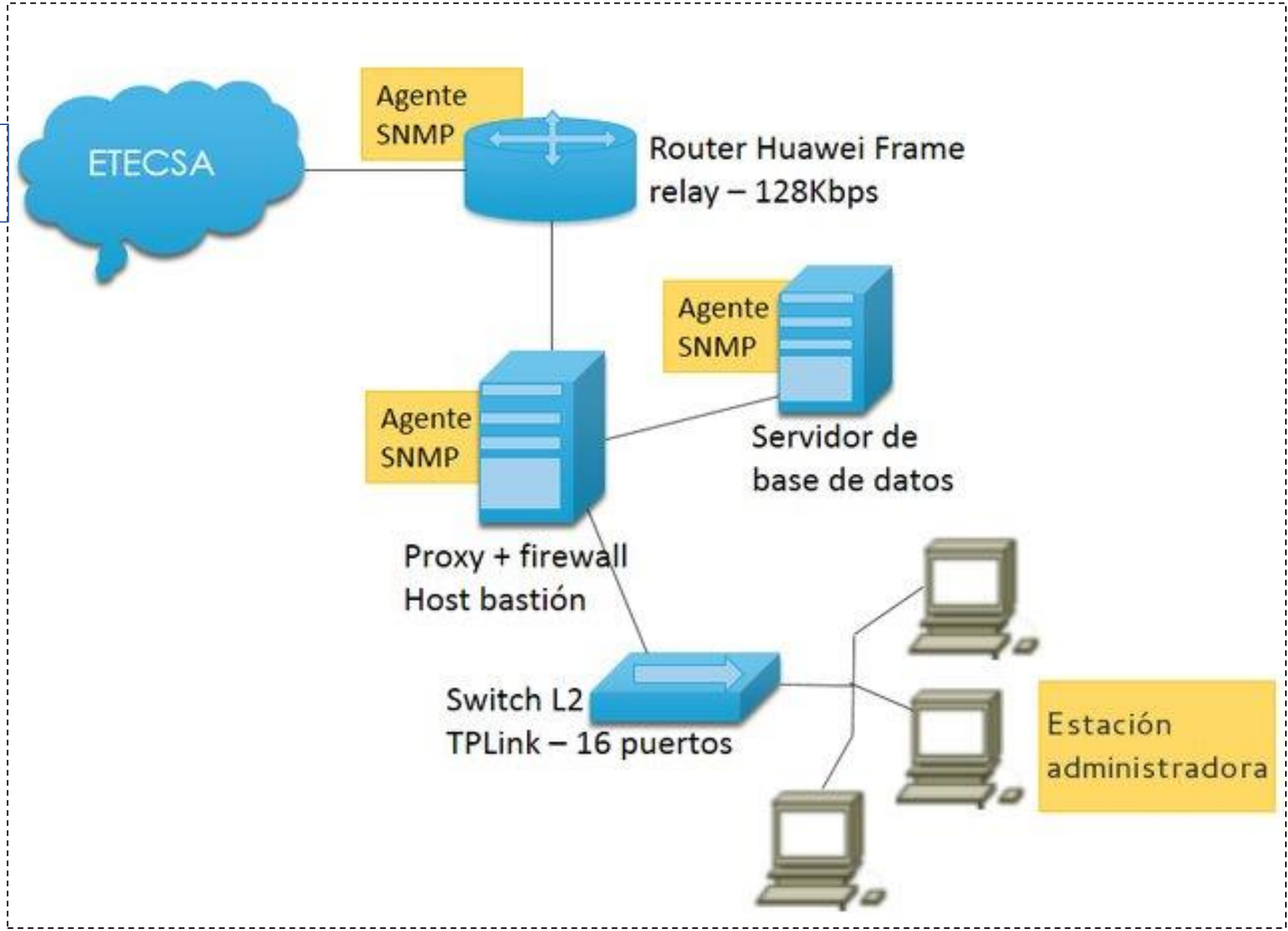
- **Ambientes de trabajo**

Ambiente de trabajo de la herramienta Nagios.

4. Entornos de comunicación seguros

- **Datos**

Ejemplo de Red real de empresa



Integridad de datos

- Nivel crítico
- Nivel alto
- Nivel Intermedio
- Nivel bajo

• Entornos de cx seguros

Integridad de datos

Nivel crítico

Datos financieros de una empresa

- Datos dificiles de verificar
- Pérdida de registros de tráfico en un alto porcentaje
- Registros de eventos de red incompletos o ausentes
- Latencias

Nivel alto

Comercio electrónico y análisis:

- Se validan todos los datos
- Los datos se verifican para proporcionar confiabilidad
- Los ejemplos incluyen las bases de datos de las organizaciones

Nivel intermedio

Ventas en línea y motores de búsqueda:

- Se realiza poca verificación
- Los datos no son completamente confiables
- Los datos se recopilan mediante formularios divulgados públicamente

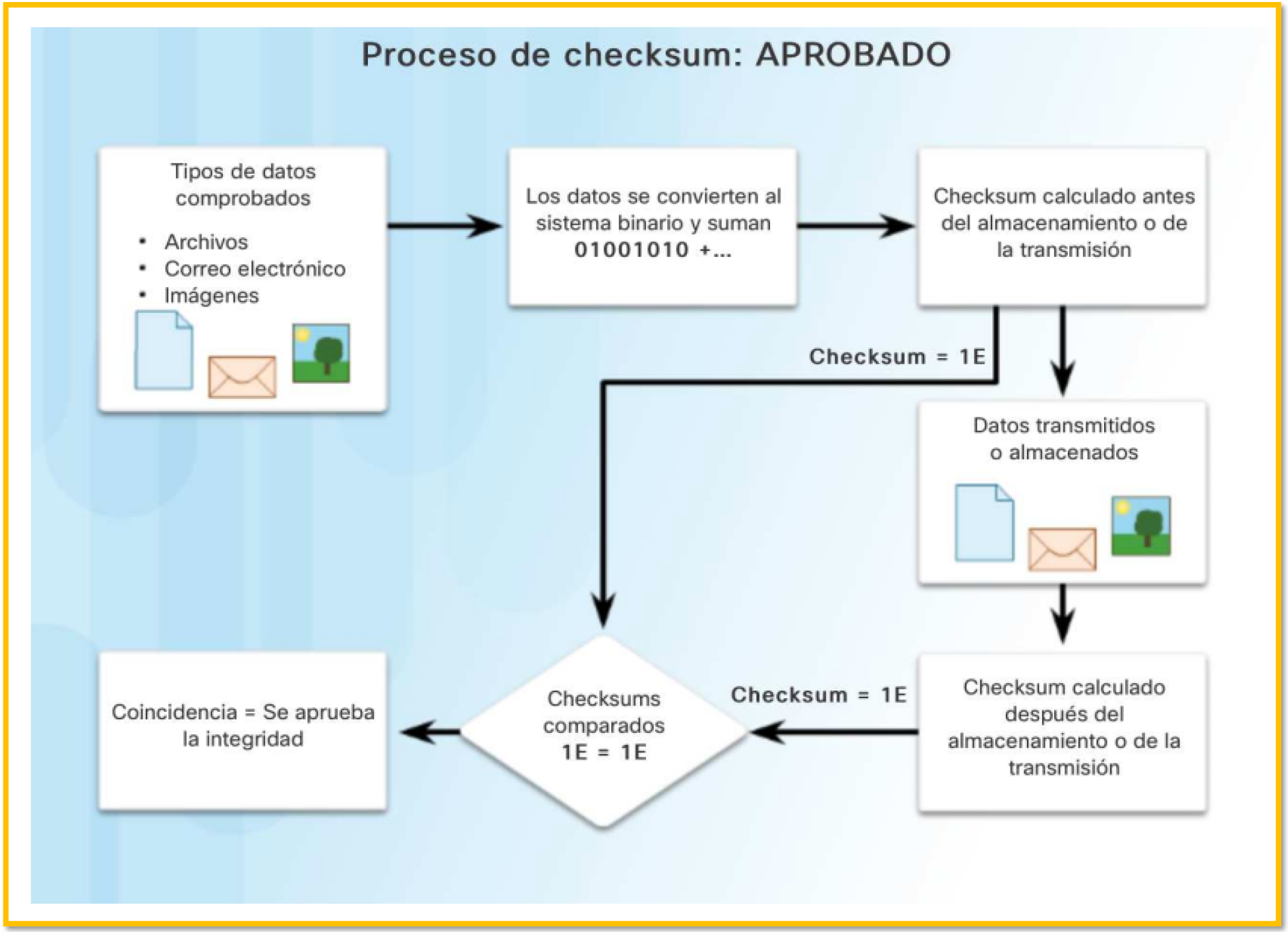
Nivel bajo

Blogs y sitios de publicaciones personales:

- Los datos no pueden verificarse
- Bajo nivel de confianza en el contenido
- Los ejemplos incluyen la opinión pública y la contribución abierta

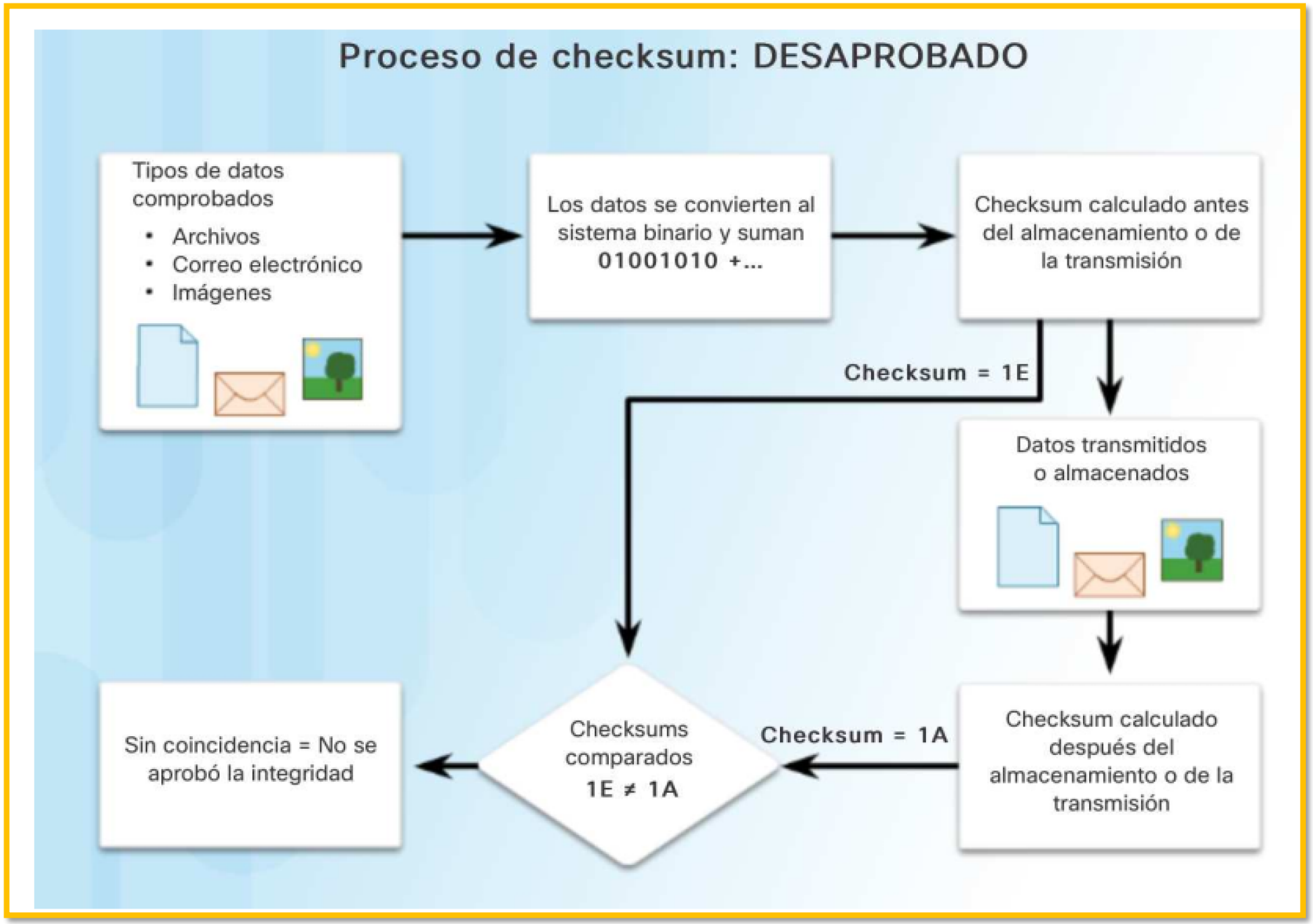
- **Entornos**

Verificación de Identidad



- **Entornos**

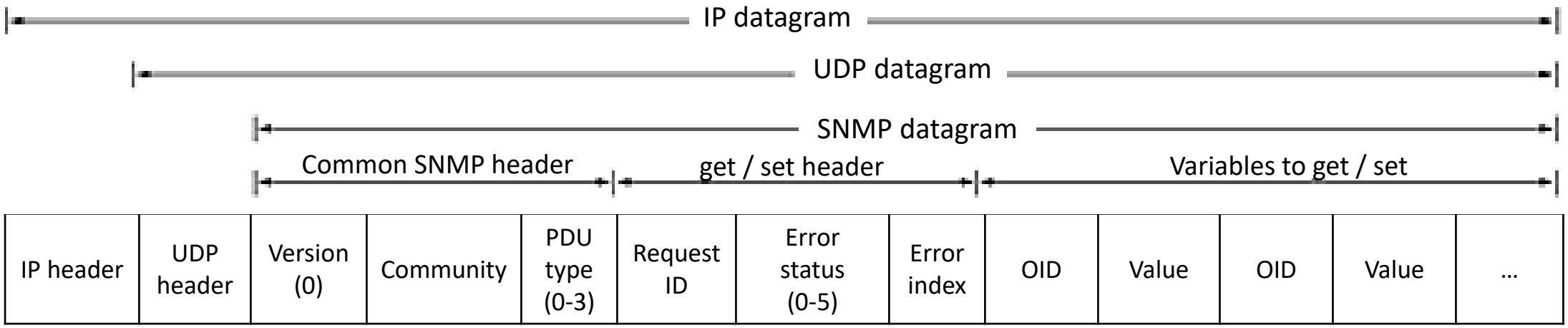
Verificación de Identidad



5. Estructura SNMP

• Estructura SNMP

The SNMP data packet is enclosed in the UDP data packet, which is enclosed in the IP data packet.



• Mediation Protocol

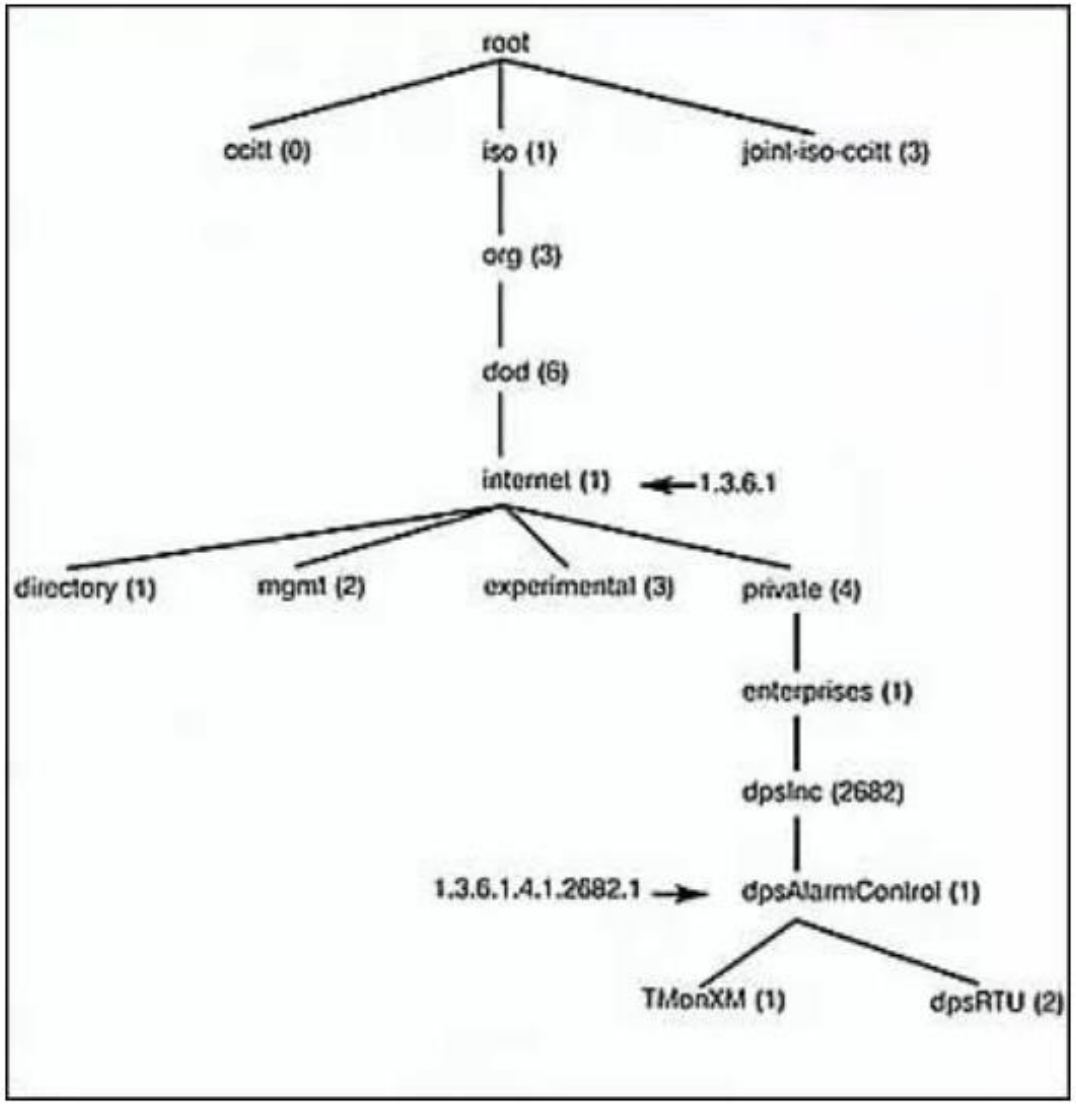
The concept of protocol mediation in the context of SNMP involves integrating various network monitoring and management protocols into a unified system, allowing different types of equipment and software to communicate effectively. Protocol mediation serves as a bridge that converts data and alarms from various proprietary or outdated protocols into a standard format like SNMP traps or TL1 messages, which can then be managed from a central SNMP or TL1 manager..

https://www.dpstele.com/snmp/implementation/equipment-mediated.php

• Mediation Protocol

Each element in the SNMP world is addressed with an Object Identifier (OID). These are long strings of dot-separated numbers. They look something like extra-long IP addresses (ex."1.3.6.1.4.1.2682.1.2.102").

And just like an IP address, each additional number adds detail. The first several numbers are always the same for SNMP devices. In the example above, "1.3.6.1.4.1..." means only "enterprise SNMP equipment". The last few numbers mean "DPS Telecom" (the manufacturer of this agent)



The MIB tree is a visual representation of how OIDs are formed.

• Tareas

- **Leer hasta la página 22**
  - **Libro:** https://openaccess.uoc.edu/bitstream/10609/75226/2/Control%20y%20gesti%C3%B3n%20de%20redes_M%C3%B3dulo%204_Gesti%C3%B3n%20de%20red.pdf

- **Realizar la práctica de configuración básica de SNMP.**
  - Usar todo lo que crea necesario (simulador, red de laboratorio, etc.).

  Link:
  https://www.sapalomera.cat/moodlecf/RS/4/course/files/8.2.2.4%20Lab%20-%20Configuring%20SNMP.pdf

Mail: pedro.escudero@unach.edu.ec
Telf: 0994667184