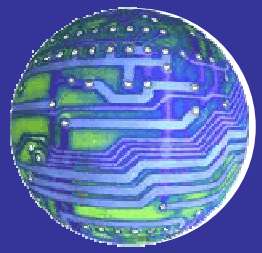
Departamento de Electrónica - UTFSM



SNMP: Simple Network Management Protocol

Patricio E. Valle Vidal
pvalle@elo.utfsm.cl

Profesor: Tomás Arredondo V.

20 de Agosto 2007 : Redes de Computadores I (ELO-322)

CONTENIDOS

- Problema
- Introducción
- Objetivos
- Propuesta SNMP
  - Arquitectura
  - Cuatro llaves fundamentales
  - Métodos de adquisición
  - Encapsulación
  - SNMPv1, SNMPv2c y SNMPv3
  - Seguridad y control de seguridad
  - Administración distribuída
  - Protocolo AgentX
- Conclusión

PROBLEMA

- La complejidad de una red de datos puede sufrir bajas en su eficiencia y productividad.
  - Identificación de recursos crítico.
- Incosistencia de datos en la red.
  - Información sensible es transmitida.
- Balanceo de necesidades: funcionamiento, disponibilidad, seguridad, costo, etc.

INTRODUCCIÓN

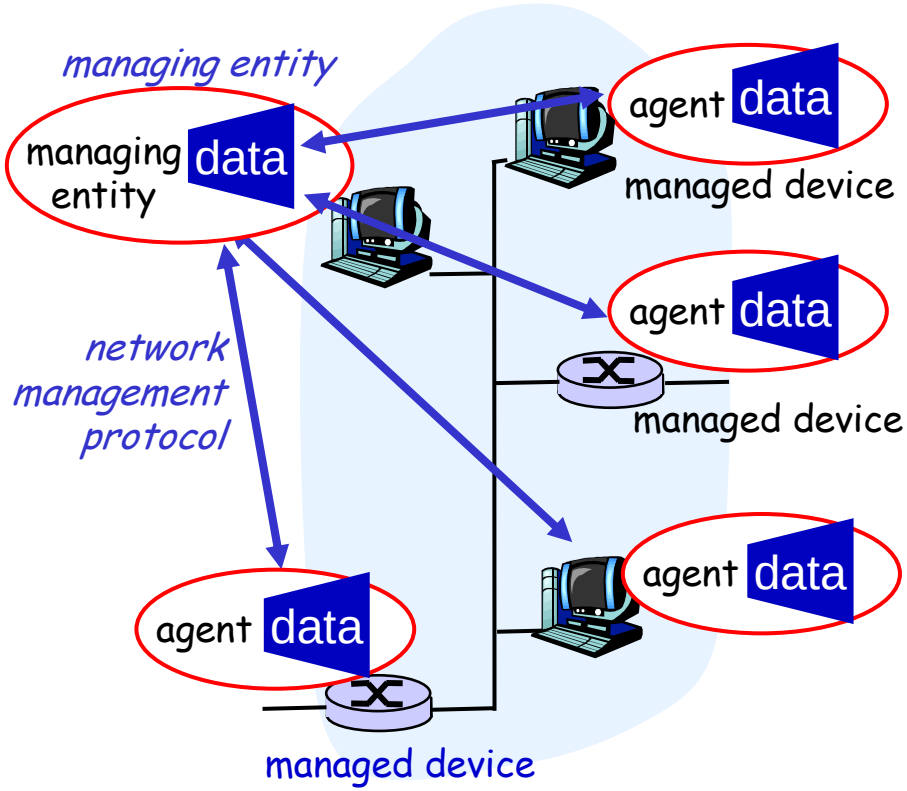
- Administración de una red de computadores:
  - Cinco áreas funcionales según The International Organization for Standarization (ISO).
    - Fallas
      - ❑ Detección y solución.
    - Seguridad
      - ❑ Control de acceso a la información de red.
    - Configuración
      - ❑ Administración de cambios
    - Funcionamiento
      - ❑ Medidas desempeño de hardware/software.
    - Descripción
      - ❑ Mapeo de recursos de red a identidades del cliente.

PROPUESTA SNMP

- SNMP: Simple Network Management Protocol.
- Permite la obtención de estadísticas, estados de red, etc.
- Define un mecanismo de administración remota para equipos de red (routers, bridges, etc.).
- Principio fundamental: toda la administración de equipos esta realizada por la manipulación de variables.
- Propuesta
  - Medios estándares para especificar las cantidades reconocidas por los dispositivos.
  - Protocolo para consultar, retornar y notificar cambios de las variables.

SNMP: ARQUITECTURA

- Una red SNMP consiste de 3 componentes principales
  - Recursos administrados
  - Agentes
  - Sistemas de administración de red (NMS)
- Un recurso administrado es un nodo en la red SNMP y contiene al agente SNMP.
- El NMS crea una conexión virtual hacia el agente SNMP.
- EL agente provee de información al NMS sobre su estado en la red.



SNMP: CUATRO LLAVES FUNDAMENTALES

- Management Information Base (MIB)
  - Almacenamiento distribuido de información sobre datos de administración de red.
- Sintaxis usada para especificar un MIB
  - SMIv2 (Structure of Management Information).
- Protocolo SNMP
  - Protocolo para el intercambio de datos entre agente y entidad administradora.
- Seguridad, capacidades de administración
  - Mayor adición en SNMPv3.

MANAGEMENT INFORMATION BASE (MIB)

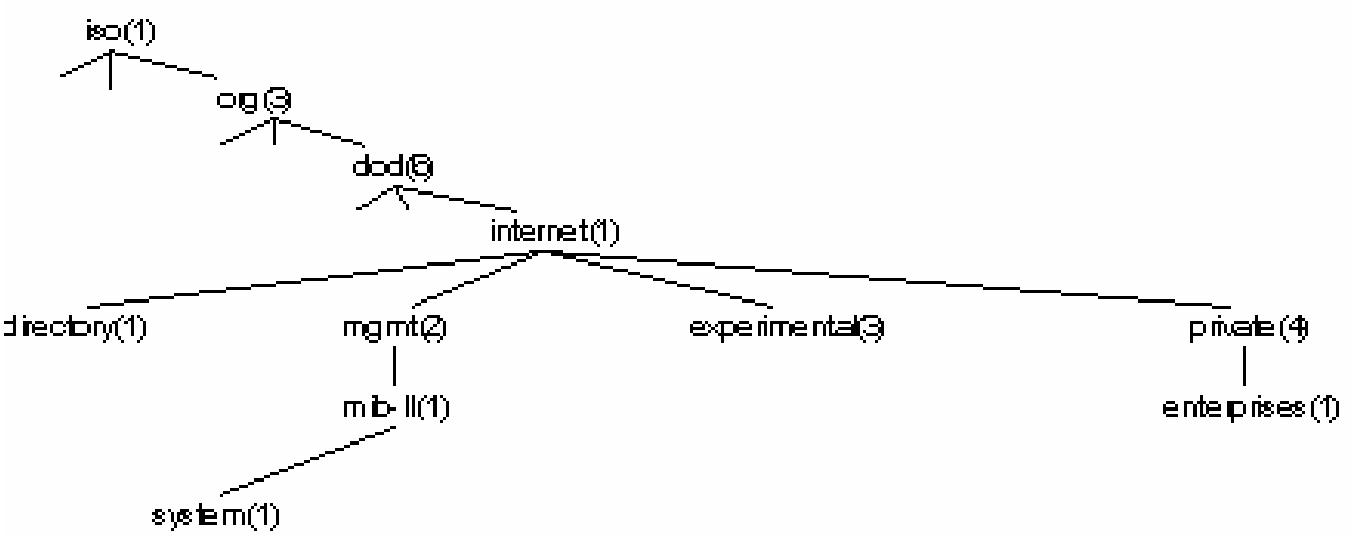
- Un MIB está constituído por un conjunto de objetos administrados mas sus atributos.
- MIBs son creados usando sintaxis SMIv2.
- La información en la MIB está organizada jerarquicamente.
- Los objetos administrados son descritos de dos formas diferentes:
  - Nombres
  - Identificadores
- El MIB tiene una rama privada
  - Ejemplo: LM-Sensors, Asterisk.

STRUCTURE OF MANAGEMENT INFORMATION (SMIv2)

- SMIv2 define las reglas para crear MIBs y está basado en variables de tipos simples.
  - Basado en subconjunto extendido de ASN.1
- Características de las variables definidas por SMI
  - Cada variable tiene un tipo de dato ASN.1
    - INTEGER, OCTET STRING, OBJECT IDENTIFIER, NULL, etc.
  - No implementa estructuras de datos y operaciones complejas.
  - Las variables son escalares (un instancia) o columnas en una tabla de dos dimensiones (cero o varias variables).

IDENTIFICADORES DE OBJETO (ASN.1)

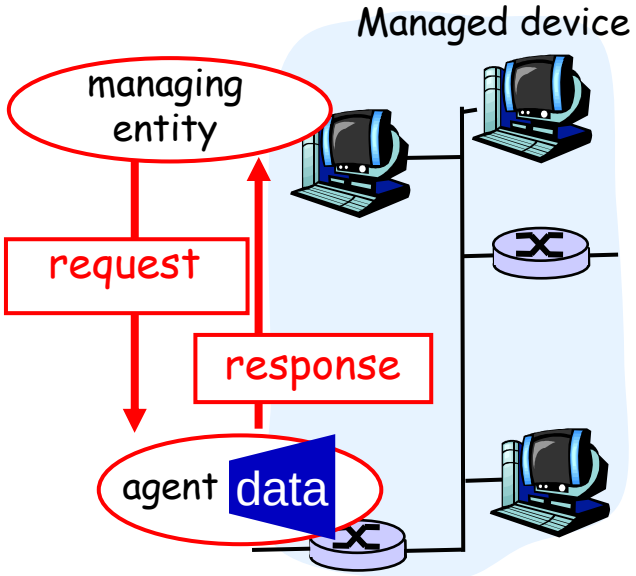
- Variables identificadas por un string único de dígitos.
  - Ejemplo: 1.3.6.1.4.1.3.5.1.1
  - El espacio de nombres es jerarquico.
- Variables descritas mediante el uso de alias (dentro del MIB).
  - Ejemplo: **ifNumber ::= {interfaces 1}**
  - **Interfaces** fue previamente definida en MIB como 1.3.6.1.2.1.2 así: ifNumber = 1.3.6.1.2.1.2.1

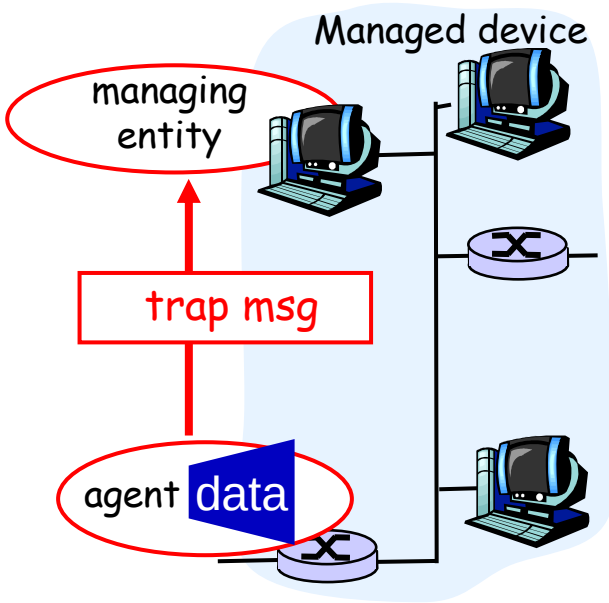


The Global MIB Tree

SNMP: MÉTODOS DE ADQUISICIÓN

- Existen dos formas para obtener información desde SNMP.
  - Notificaciones (Traps)
    - Si un evento ocurre en un equipo administrado una notificación es enviada a la estación.
    - Una notificación contiene:
      - Nombre del equipo de red.
      - El tiempo de disparo del evento.
      - Tipo de evento.
  - Consultas
    - La estación periodicamente consulta por información al equipo de red.
    - Ventaja: Mantiene en conocimiento el estado del equipo.
    - Desventaja: Retardos desde cuando un evento ocurre a cuando es notificado.
      - Cortos intervalos: BW desperdiciado.
      - Largos intervalos: Respuesta a eventos demasiado lentos.

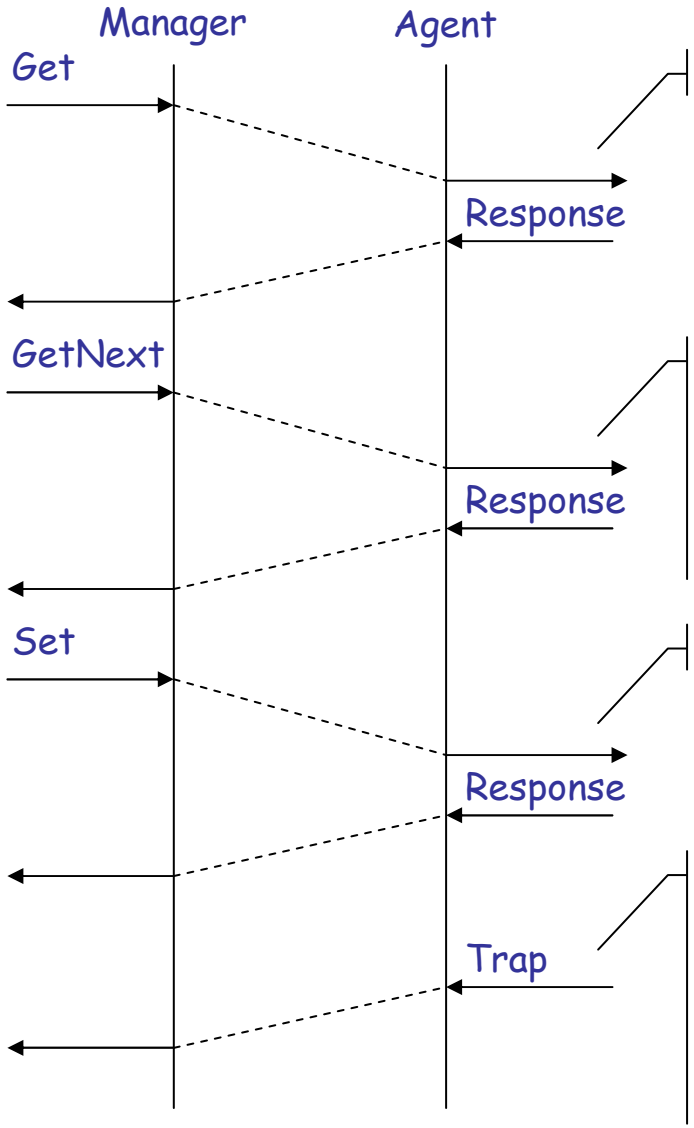




SNMP: ENCAPSULACIÓN

- UDP
  - Agente: puerto 161.
  - Entidad administradora: puerto 162.
- La entrega de información es importante, principalmente en caso de altas perdidas.
  - Congestión.
  - Operaciones impropias.
- TCP no es conveniente (aunque sea soportado, particularmente para SNMPv3 en sus operaciones de escritura).

SNMPv1



Para leer una o más variables

Recupera el nombre y valor de la próxima instancia del objeto.
Esta operación es usada para descubrir estructuras y leer tablas MIB.
Usando múltiples/sucesivas operaciones GetNext es posible leer el MIB completo sin conocer su estructura.

Escribe valores de una o más instancias.

Es sólo la operación Agent → Manager; es un evento asincrónico.
El agente puede emitir un evento e informar a una central. Sin embargo, el mensaje recibido no tiene retorno (acknowledge), por lo que puede haber pérdida del mensaje.
Aunque los Traps se usan, las consultas siguen siendo necesarias (Ej. cuando el agente está caído).

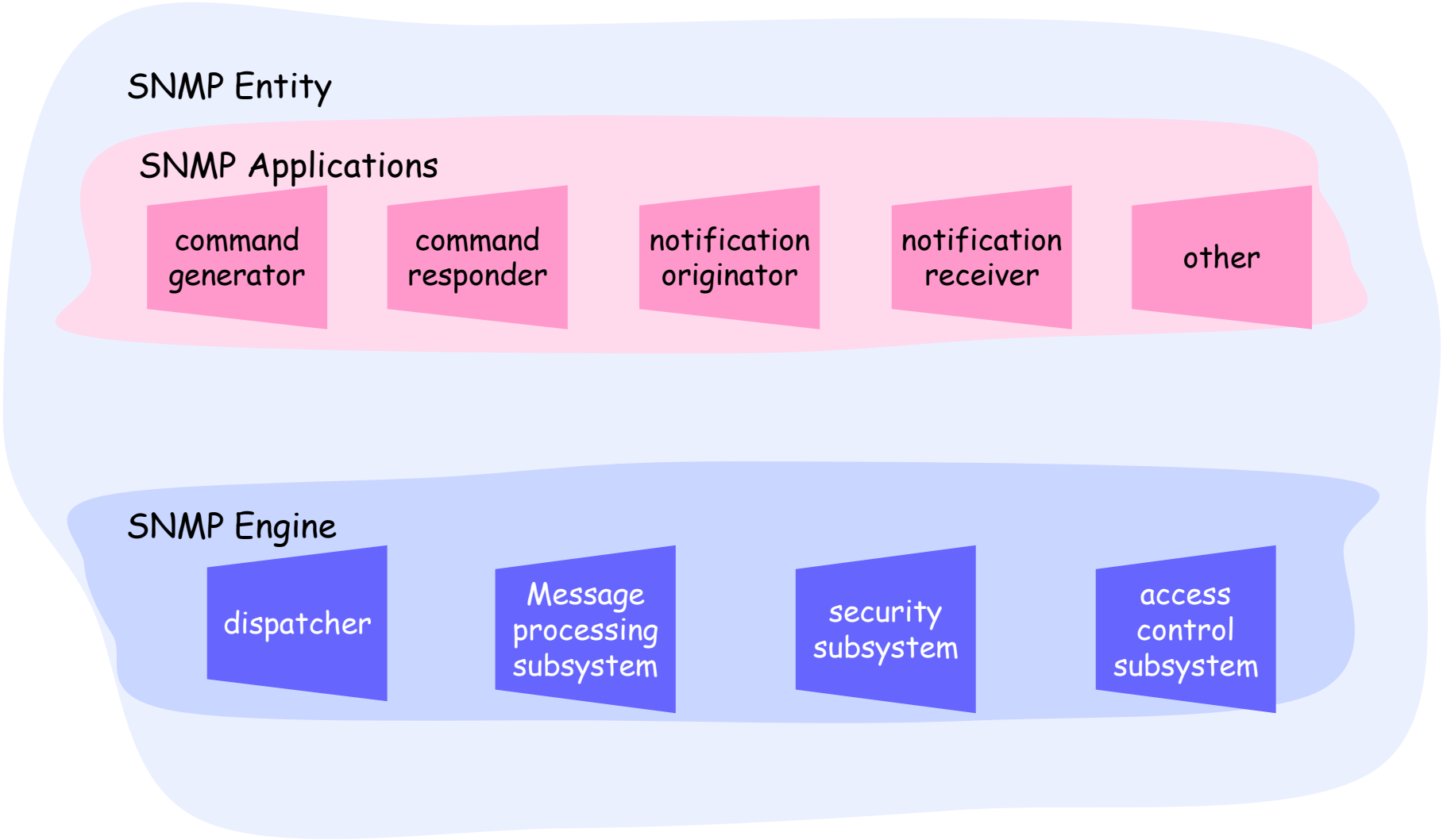
SNMPv2c

- Incluye las funciones básicas de SNMPv1
  - Puede coexistir con SNMPv1
- Tipos nuevos de mensajes
  - Recupera información de administración de gran tamaño usando pocos recursos de red (GetBulk)
- Soporte multi-protocolo estandarizado
  - El mundo en su mayoría es IP.
- Seguridad planeada pero disminuida
  - La “C” indica seguridad basado en comunidades

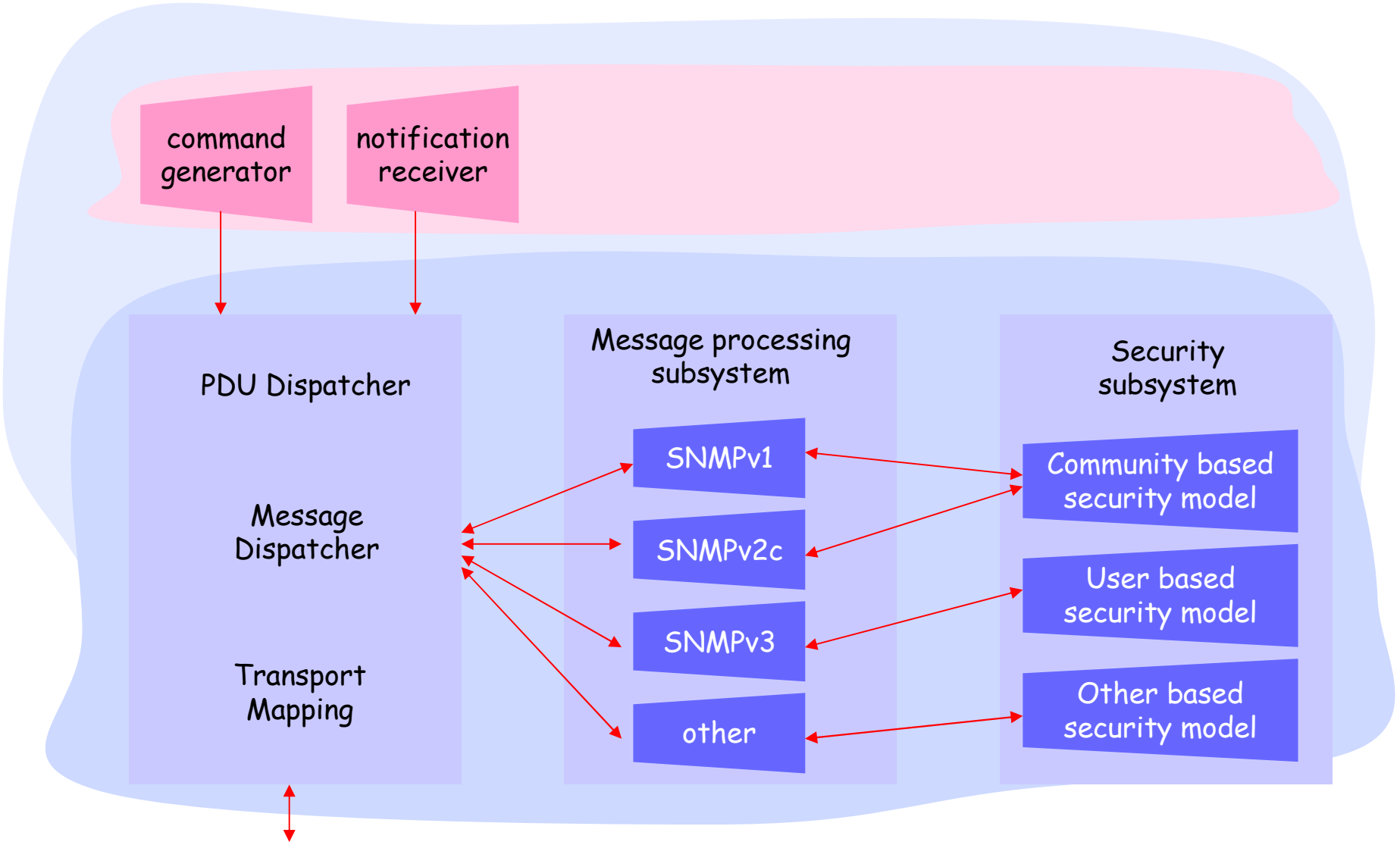
SNMPV3

- Seguridad de SNMP completada
- Agentes y administradores son denominadas entidades SNMP
- Una entidad contiene un motor SNMP
- Todas las aplicaciones SNMP están dentro de la entidad SNMP
  - Generadores de consultas.
  - Respondedoras de consultas.
  - Originadores de notificación.
  - Recibidoras de notificación.
  - Proxy

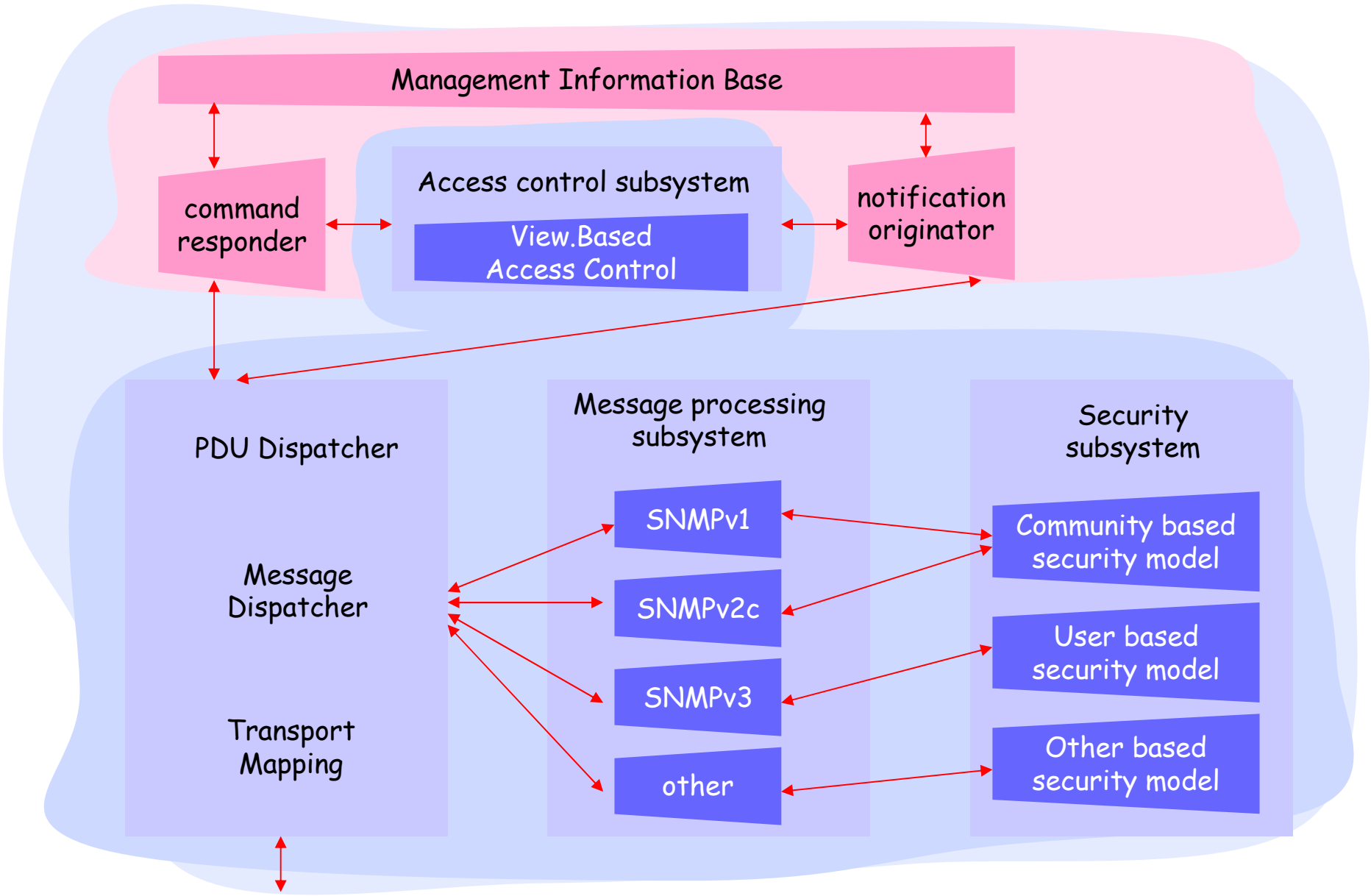
SNMPv3: ARQUITECTURA



SNMPv3: ARQUITECTURA DE UN NMS



SNMPv3: ARQUITECTURA DE UN AGENTE

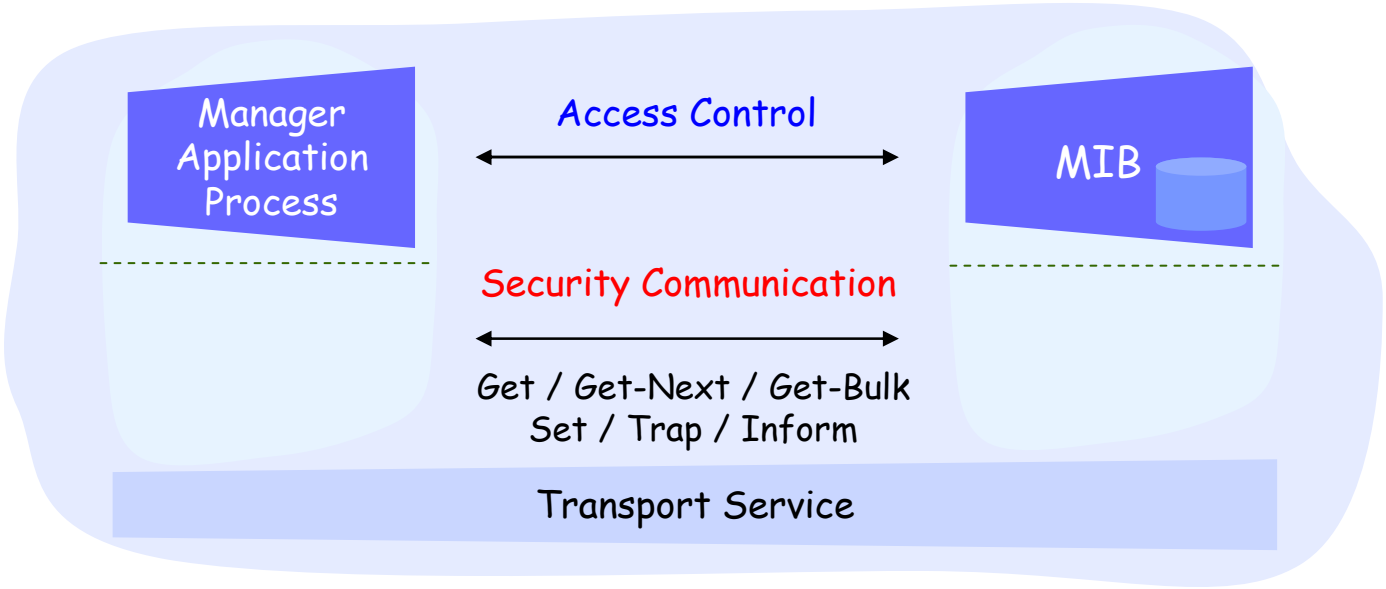


SNMP: SEGURIDAD

- Mensajes de Integridad
  - Evitar la manipulación del mensaje.
- Autentificación
  - El origen es una fuente válida.
  - Protocolo de autentificación
    - HMAC-MD5-96
    - HMAC-SHA-96
- Encriptación
  - Información oculta.
  - Protocolos de encriptación
    - CBC-DES
- 3 niveles de seguridad
  - noAuthNoPriv, authNoPriv, authPriv.
- 2 modelos de seguridad
  - Community-Based Security Model
  - User-Based Security Model

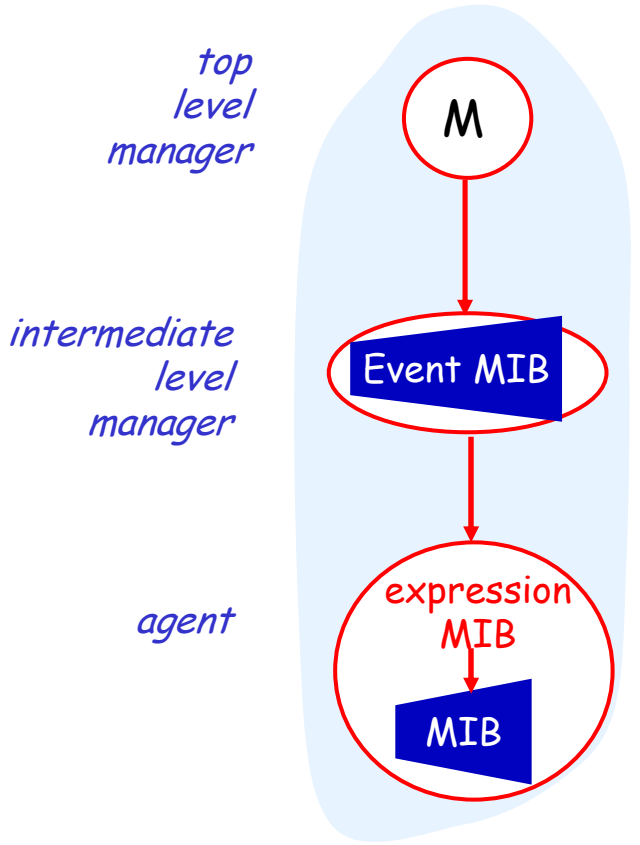
SNMP: CONTROL DE ACCESO

- Fundamentos de la seguridad en SNMPv3
  - Cada usuario pertenece a un grupo
  - Un grupo define sus políticas de acceso para sus usuarios.
  - Políticas de acceso: ¿Qué objetos MIB pueden ser accedidos para; lectura, escritura y notificación?.
  - Un grupo define el nivel y modelo de seguridad para sus usuarios.
- View-Based Access Control Model



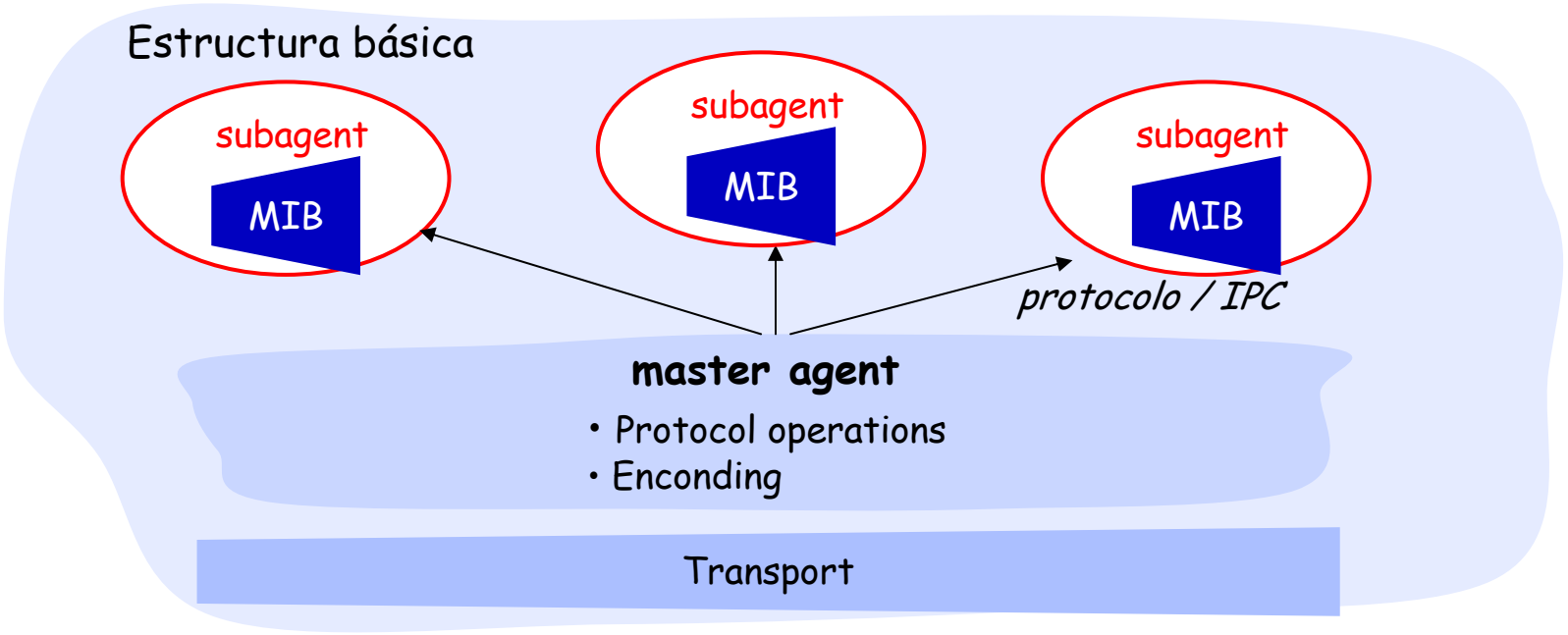
ADMINISTRACIÓN DISTRIBUIDA

- Basado en MIB
- Expresiones MIB
  - Las entradas son variables de un MIB (local)
  - Opera sobre valores absolutos y deltas.
  - Conjunto completo de expresiones.
  - La salida es almacenada en un tabla de valores.
  - Esta tabla podría servir como entrada para otras expresiones MIB.
- Eventos MIB
  - La entrada son variables de un MIB (remoto).
  - Activaciones sobre cambios en objetos MIB especificados.
  - Genera una notificación o conjunto de operaciones SET.



AGENTX: EXTENSIÓN DE UN AGENTE

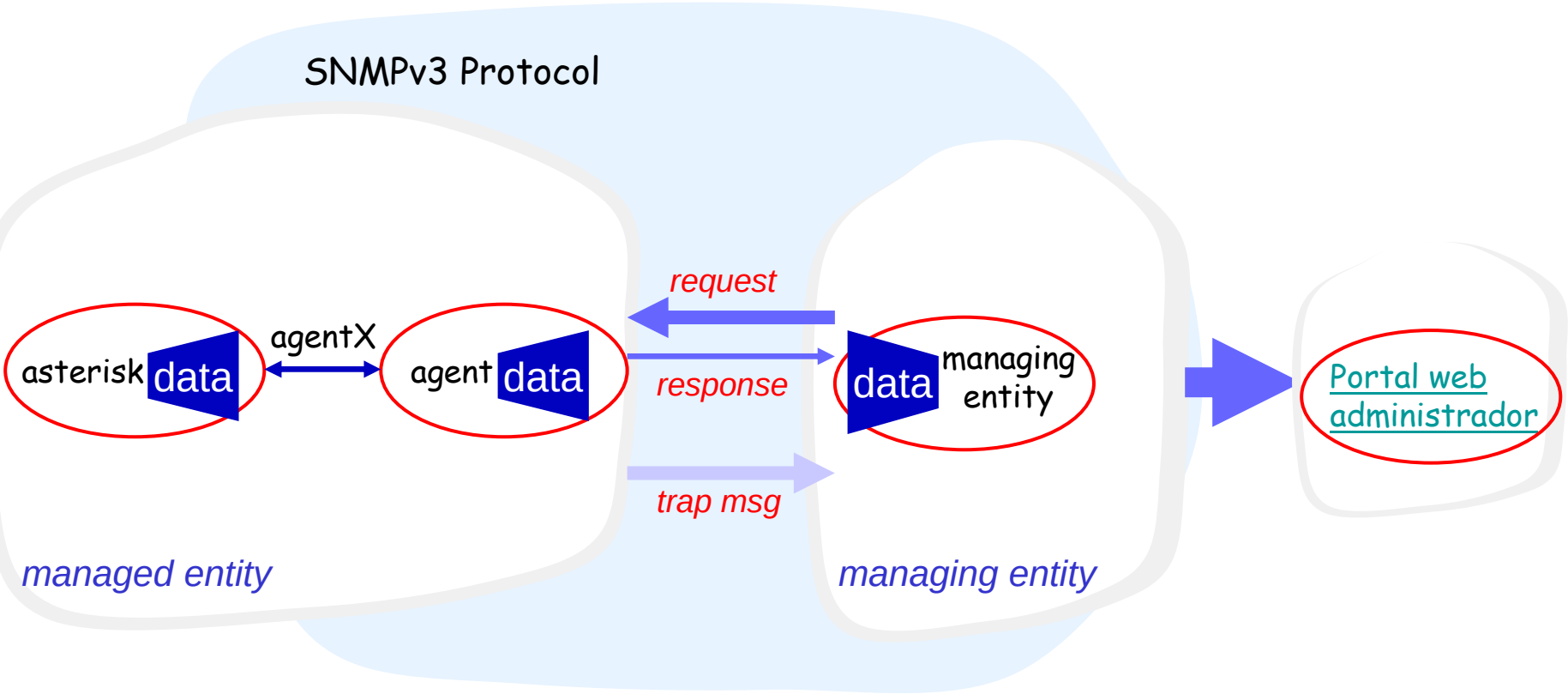
- Facilita la extensión de agentes SNMP con nuevos módulos MIB.
- Separa el motor SNMP de la implementación MIB.
- Permite la adición dinámica de nuevas implementaciones de módulos MIB.
- Los agentes extensibles deben ser transparentes.



CONCLUSIONES

- Un equipo pude ser administrado vía SNMP para servicios específicos, sin la necesidad de que el agente interactúe directamente con ellos.
  - Mapeo de valores a objetos MIB.
- La simplicidad de mantenerse informado de la situación actual de los servicios que entrega una red.
  - Es posible ocultar información sobre estadísticas.
  - Monitoreo de recursos estratégicos.
- El reconocimiento de fallas por parte de un agente en un equipo administrado permite liberar la carga de la estación y de la red (ancho banda).

ESQUEMA FUNCIONAL



CONSULTAS