

Administración de redes y SNMP

Sebastián Castro A.

CC50P

2006/2

Administración de Redes

- ♦ La administración de redes va más allá del control de los recursos
- ♦ Consiste principalmente de cuatro funciones:
 - Operación
 - Administración
 - Mantenición
 - Aprovisionamiento

Problemas Típicos

- ◆ El problema más común y más serio es la falla de conectividad.
 - Cae en la categoría de “administración de falla”.
 - Por falla en un nodo, equipamiento o error de procedimiento.
 - Situaciones temporales como sobrecarga.
 - Fallas eléctricas: configuraciones en uso y por omisión
- ◆ Problemas de rendimiento.
- ◆ Problemas de seguridad.

Desafíos

- ♦ Administrar la infraestructura de comunicación Y los sistemas que generan información.
- ♦ Mantenerse actualizado en el avance de la tecnología.
- ♦ Análisis de problemas, en base a conocimiento e intuición.
- ♦ Anticipar las demandas de los clientes.
- ♦ Adquisición de recursos.

Desafíos

- ◆ Crecimiento sustentable de la red (escalabilidad y mantenibilidad)
- ◆ Regular el ambiente entre cliente y servidor.
- ◆ Trabajar con tecnologías emergentes.
- ◆ Mantener la confiabilidad (cambios, actualizaciones).
- ◆ Diagnosticar problemas o fallas de modo transparente.
- ◆ Análisis de costo e inversión.
- ◆ Determinación de responsabilidades en situaciones de falla.
- ◆ Mantener la topología lo más simple posible: principio KISS.

NMS

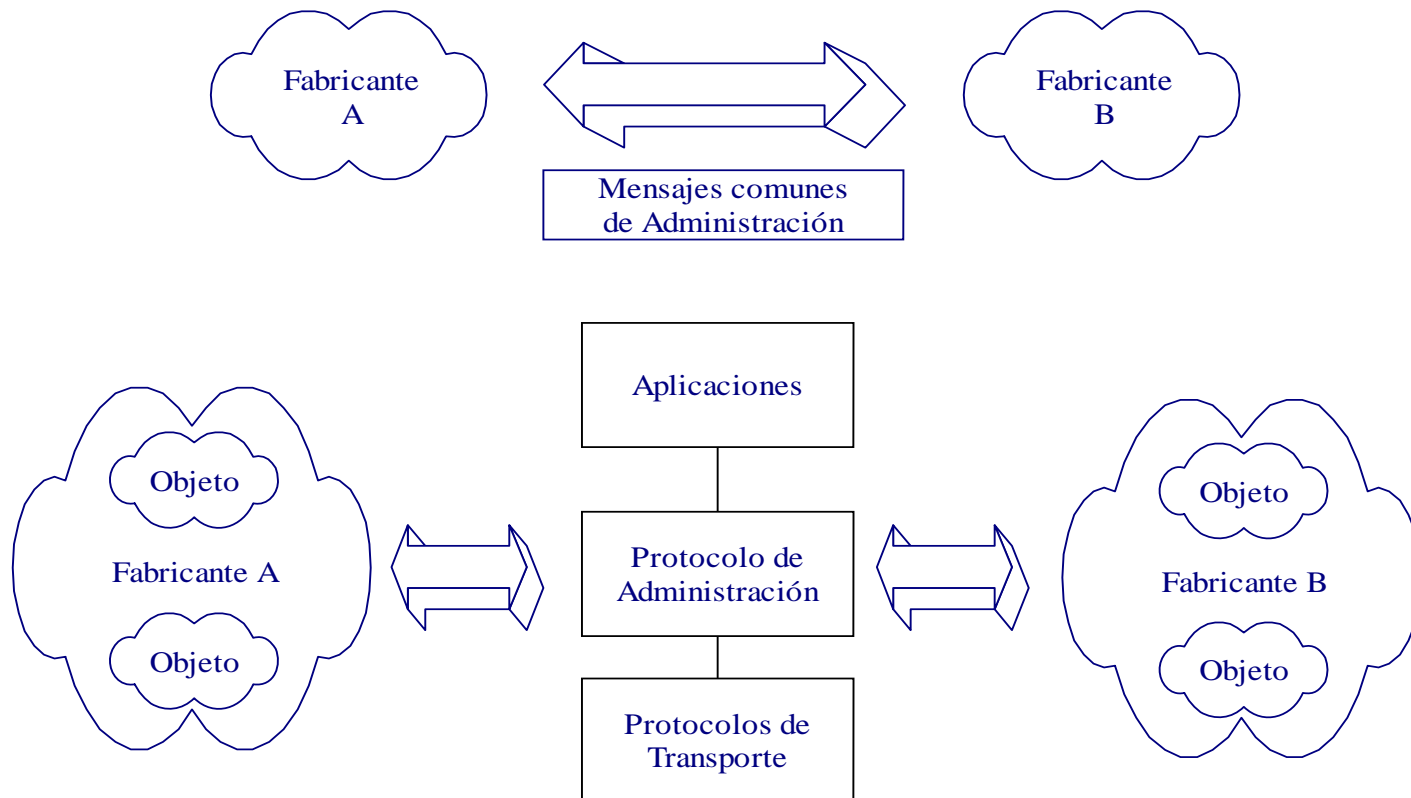
- ◆ Network Management System
- ◆ Se necesita para:
 - Administración proactiva.
 - Diagnóstico de problemas.
 - Análisis estadístico del rendimiento.
 - Para eliminar cuellos de botella.
 - Formalizar una práctica manual.

Principios de Administración

◆ Introducción

- La red se compone de componentes y sus interconexiones.
- Los fabricantes de los componentes son los mejores calificados para desarrollar un sistema los administre.
- En una gran compañía, es muy fácil encontrar componentes de diversos fabricantes, por lo sería fácil encontrar un sistema de administración por cada fabricante.
- Se hace necesaria entonces la existencia de un sistema de administración común.

Principios de Administración

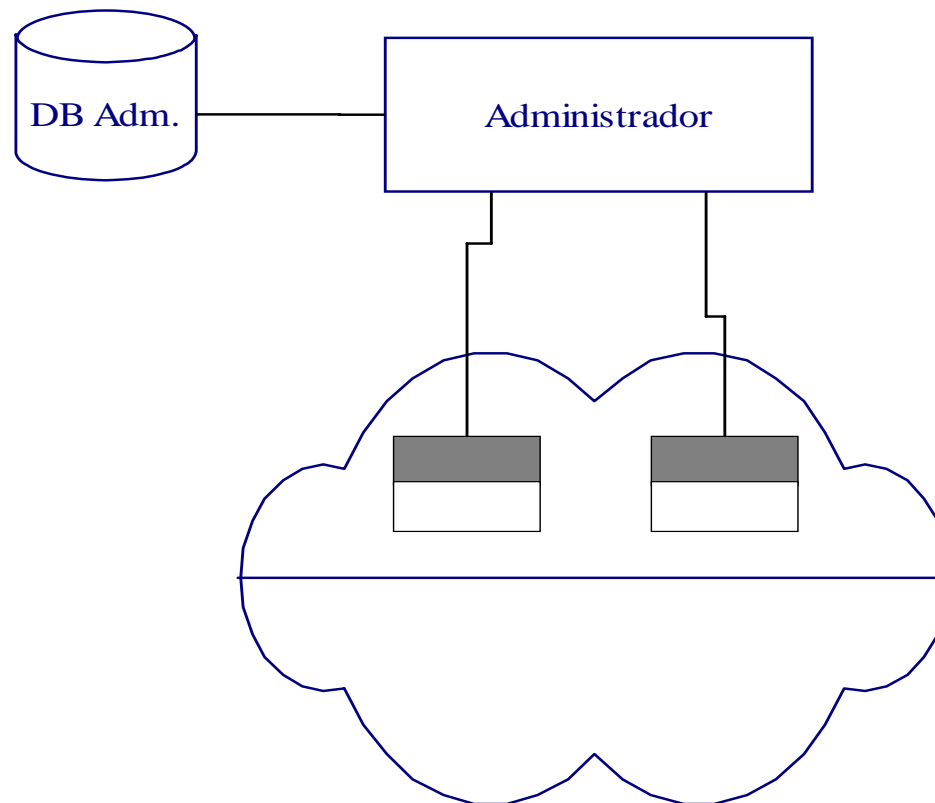


Estándares de Administración

- ◆ Existen diferentes estándares para la administración de redes.
 - CMIP, Common Management Information Protocol, protocolo de OSI.
 - TMN, Telecommunications Management Network está diseñado para administrar redes de telecomunicaciones y es el estándar de ITU.
 - SNMP, Simple Network Management Protocol, es el estándar de la IETF y se utiliza en todas las redes que utilizan los protocolos de Internet.
 - Es el protocolo más implementado y ampliamente utilizado, debido a la simpleza de su concepción.
 - Administración basada en Web, de reciente aparición. Existen dos tecnologías en uso: Web-Based Enterprise Management (WBEM) y Java Management Extensions (JMX)

Modelo Organizacional

♦ Modelo de dos capas



Modelo Organizacional

- ◆ Modelo de dos capas
 - Esta compuesto de “elementos de red” como hosts, hubs, bridges, switches, routers y otros. Pueden ser clasificados en **administrables** y **no administrables**. Aquellos administrables tienen un proceso de administración corriendo dentro de ellos llamado **agente**. Generalmente éstos tienen un costo mayor con respecto a los no administrables.

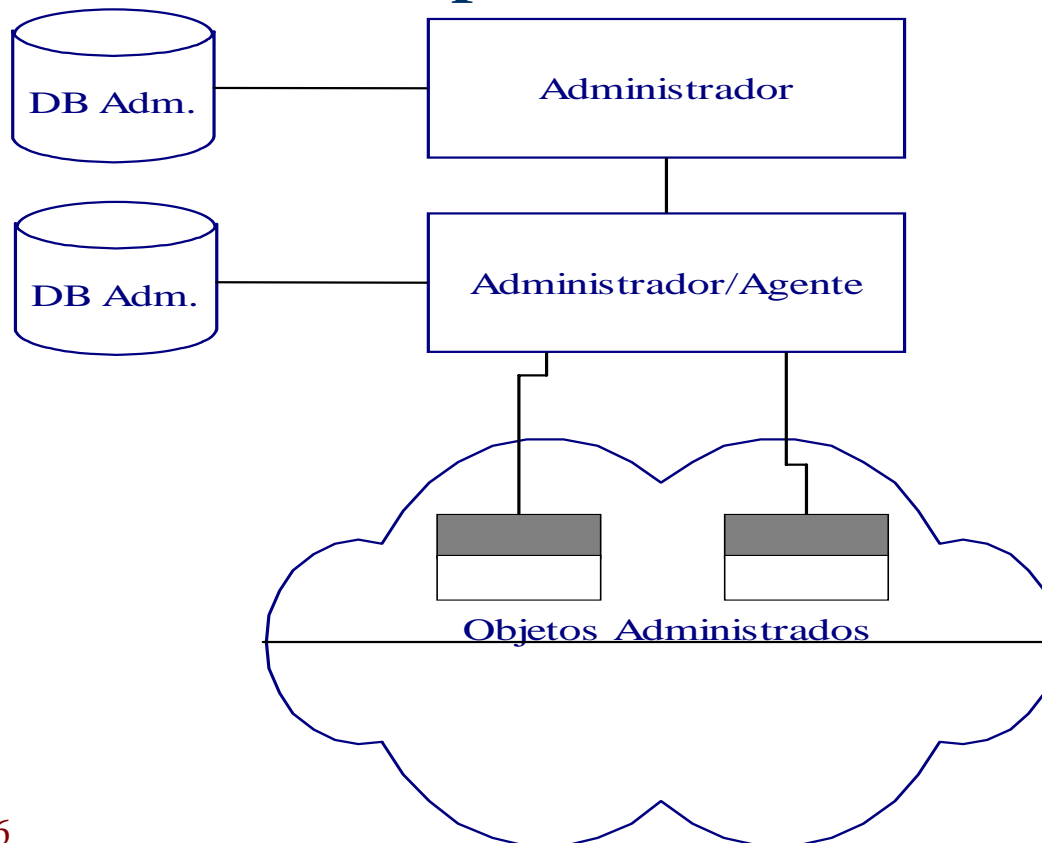
Modelo Organizacional

◆ Modelo de dos capas

- El agente mantiene información acerca del elemento que “administra”.
- El **administrador** controla el elemento administrado. Éste consulta al agente y recibe información, se procesa y luego se almacena en la **base de datos de administración**.
- El agente también puede enviar información de alarma ante ciertos eventos (sin que el administrador lo solicite).

Modelo Organizacional

♦ Modelo de tres capas



Modelo de Información

- ◆ Modelo de Información
 - Preocupado de la estructura y almacenaje de la información.
 - Representación de los objetos y la información relevante para su administración.
 - La industria usa el “Structure of Management Information” (SMI) para definir la sintaxis y la semántica de la información almacenada en el MIB.

Modelo de Información

◆ MIB

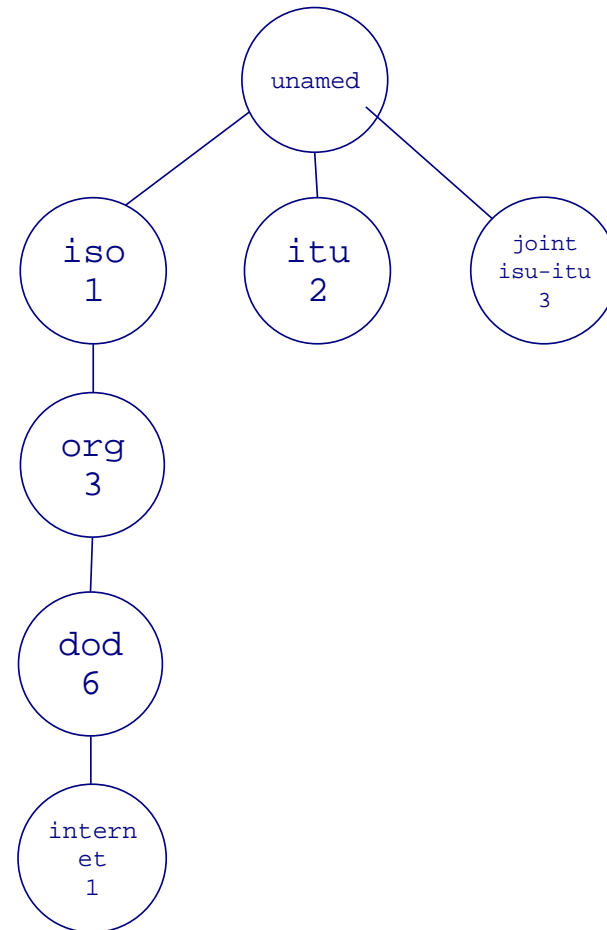
- Management Information Base
- Define las variables que residen en el nodo administrado.
- Definido de acuerdo a las reglas del SMI.
- Cada objeto administrado es descrito usando un identificador de objeto (OID) definido en el SMI.

Modelo de Información

- ◆ Los objetos administrados se definen unívocamente mediante una estructura de árbol.
- ◆ Existe un nodo raíz (root) y nodos bien definidos que depende directamente de él.
- ◆ La estructura ha sido definida por la OSI, donde la raíz no tiene un nombre específico.
- ◆ La raíz tiene tres hijos: **iso**, de la International Standards Organization; **itu**, de la International Telecommunications Union y **iso-it** para los objetos acordados en conjunto.

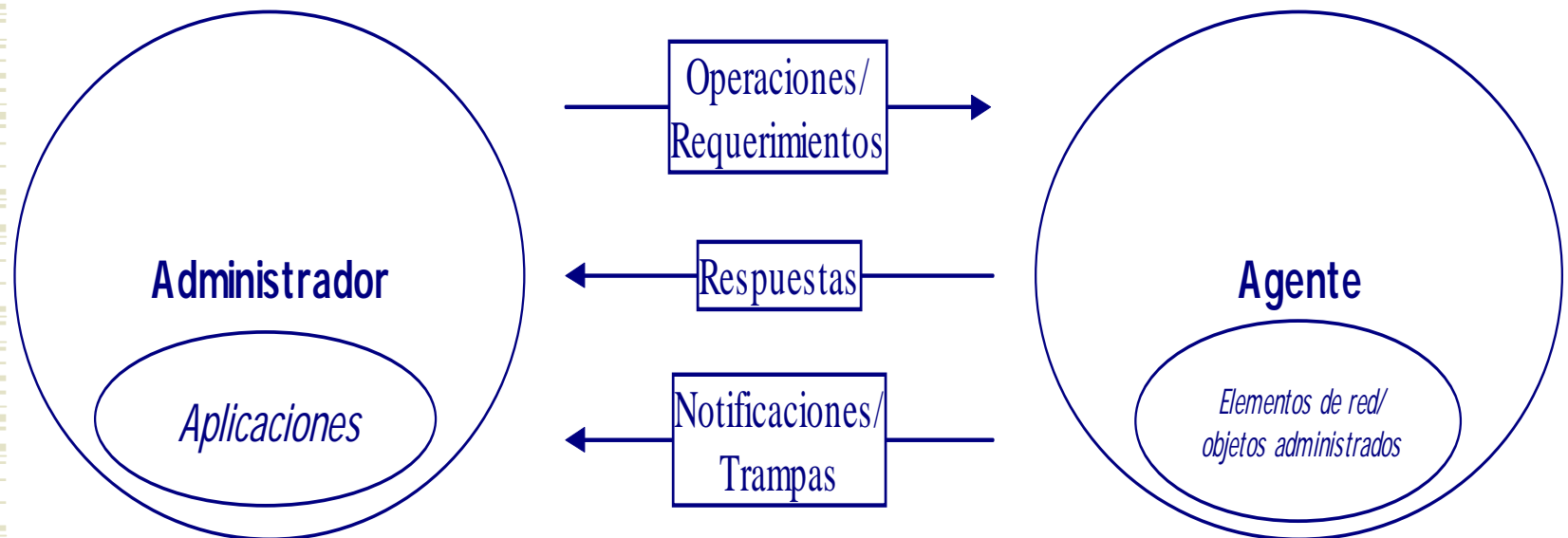
Modelo de Información

- **Dod** se refiere al “Department of Defense”.
- Todos los objetos asociados a Internet contiene en su identificación el mismo sufijo (1.3.6.1).



Modelo de Comunicación

- ◆ Entre las dos entidades involucradas tenemos los siguientes intercambios.



Modelo de Comunicación

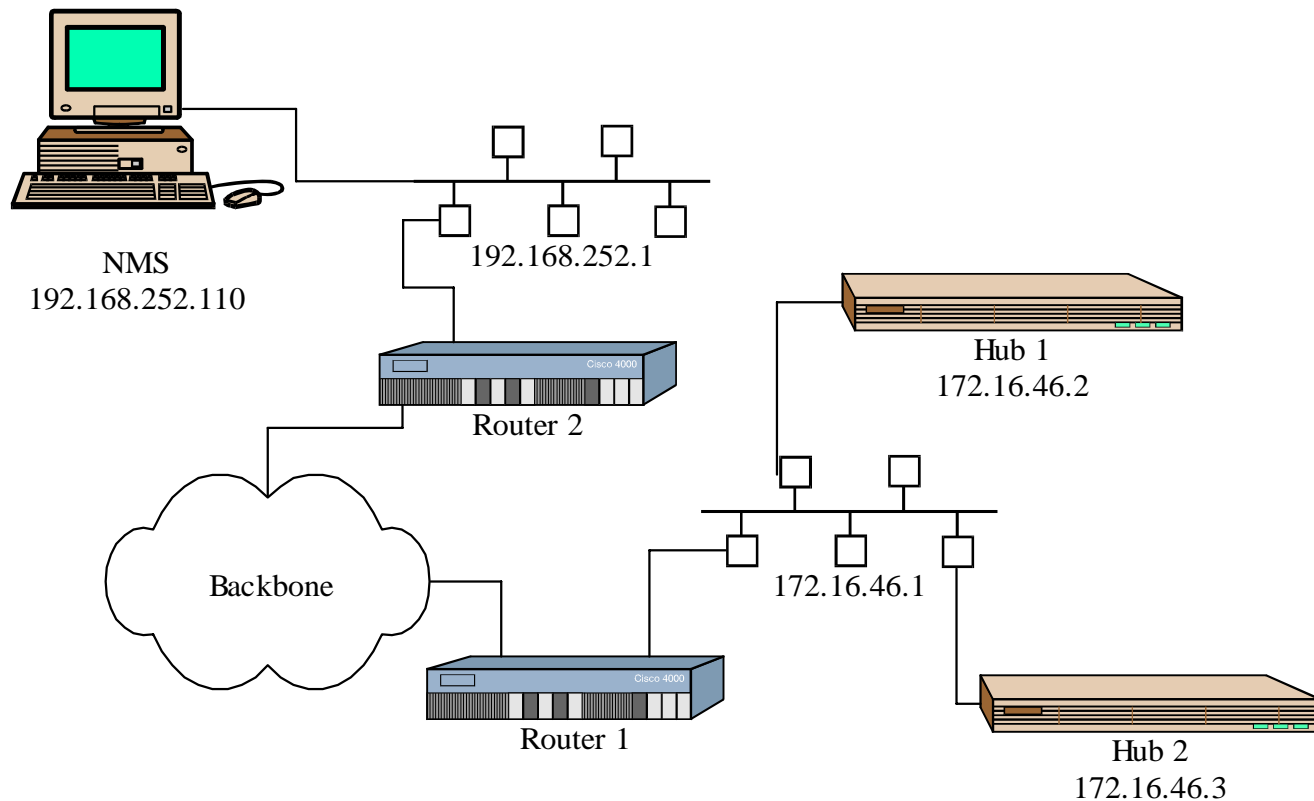
- La aplicación en el administrador envía **requerimientos** al agente.
- El agente ejecuta el requerimiento en el elemento de red y devuelve una **respuesta** al administrador.
- Las **notificaciones** y **trampas** son mensajes no solicitados, generadas por el agente.
- El modelo Internet utiliza SNMP y UDP/IP.

SNMP

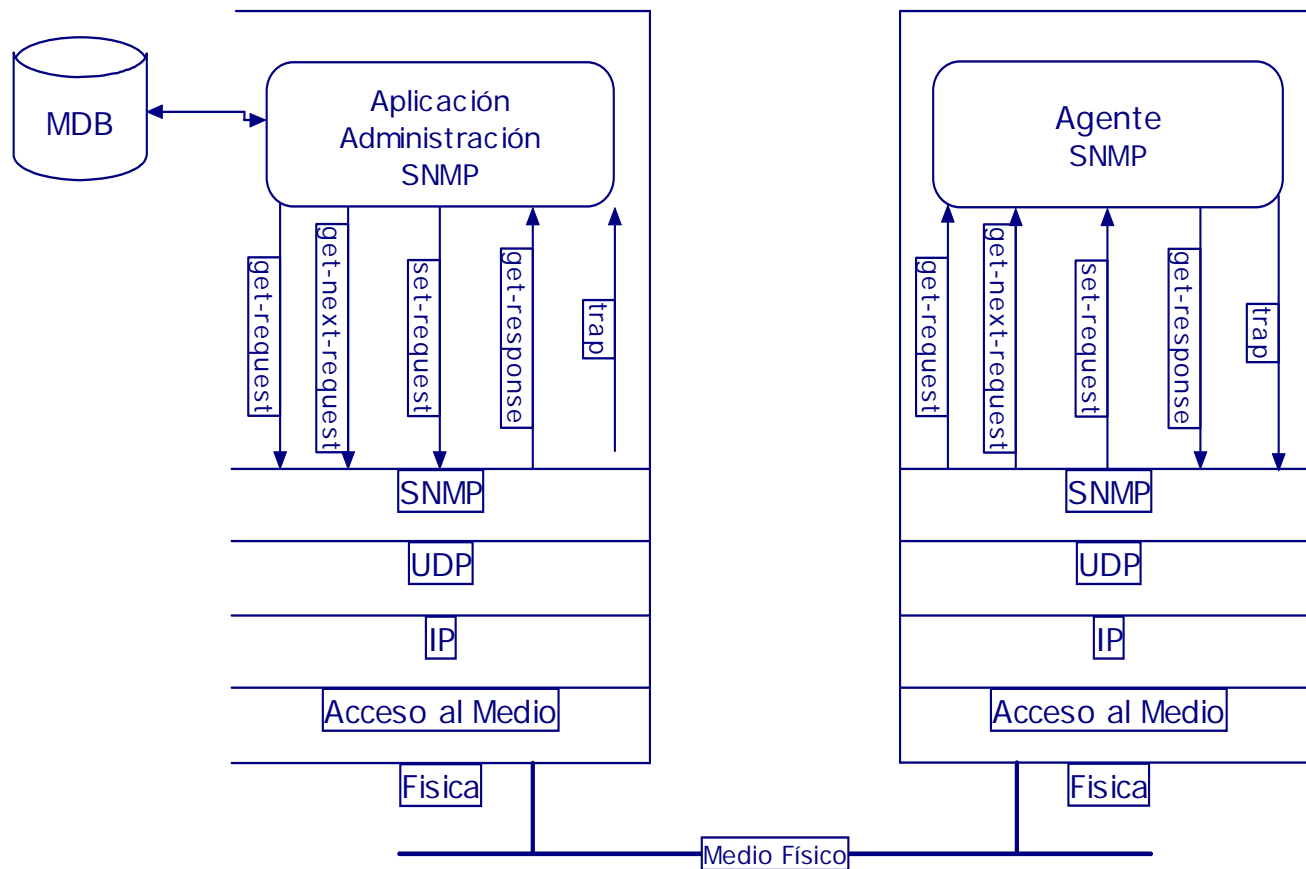
- ◆ Simple Network Management Protocol
 - Conocido como el protocolo de administración de Internet.
 - Es simple comparado con otros protocolos, pero visto desde sí mismo no es tan simple.
 - La mayoría de los componentes de red tienen agentes SNMP internos, que permiten ser integrados a un sistema de administración.
 - Nacido en 1970, existen tres versiones del protocolo y se denominan SNMPv1, SNMPv2 y SNMPv3.
 - El modelo de información de SNMP comprende el SMI y el MIB. SMI está definido utilizando ASN.1.

SNMP

♦ Ejemplo de una red administrada



SNMP (Arquitectura)



SNMP

- El protocolo está diseñado para que sea simple, y su éxito lo ha demostrado.
- La comunicación entre las entidades se lleva a cabo a través de **mensajes de protocolo**.
- Tres de ellos (get-request, get-next-request y set-request) son utilizados por el administrador.
- Los otros dos (get-response y trap) son generados por el agente.

SNMP

◆ Detalle de los mensajes

- **Get-request** es generado por el administrador cuando solicita el valor de un objeto.
- **Get-next-request** o simplemente get-next, se utiliza para solicitar el siguiente valor de un objeto. Se utiliza cuando un objeto contiene una lista de valores. Por ejemplo, una tabla de rutas.
- **Set-request** es generado por el administrador para definir o reiniciar el valor de un objeto variable. Los parámetros configurables se definen usando este mensaje.

SNMP

◆ Detalle de los mensajes

- **Get-response** es generado por el agente y sólo en respuesta a un get-request, get-next o set-request originado por el administrador.
- **Trap** es un mensaje no solicitado generado por el agente, sin intervención del administrador. Ocurren cuando el agente detecta la ocurrencia de un parámetro predefinido. Así, un agente puede enviar traps cuando una interfaz se desconecta y luego vuelve a conectarse o cuando un parámetro supera un límite previamente definido.

SNMP

- El Administrador mantiene una base de datos con la información que recibe de parte de los agentes en los objetos administrados. Ésta base es dinámica y puede ser almacenada en cualquier arquitectura de base de datos elegida por los implementadores.
- Por otro lado, mantiene el MIB asociado al objeto en cuestión, que le permite conocer el detalle del objeto. El MIB es estático.

SNMP

◆ MIB

■ MIB I

- 114 objetos estándar.
- Los objetos incluidos son considerados esenciales para la administración de fallas o configuración.

■ MIB II

- Extiende MIB I
- 185 objetos definidos.

■ Otros MIB

- RMON

■ MIB Proprietarios

- Extensiones a los MIB estándar generados por los fabricantes.

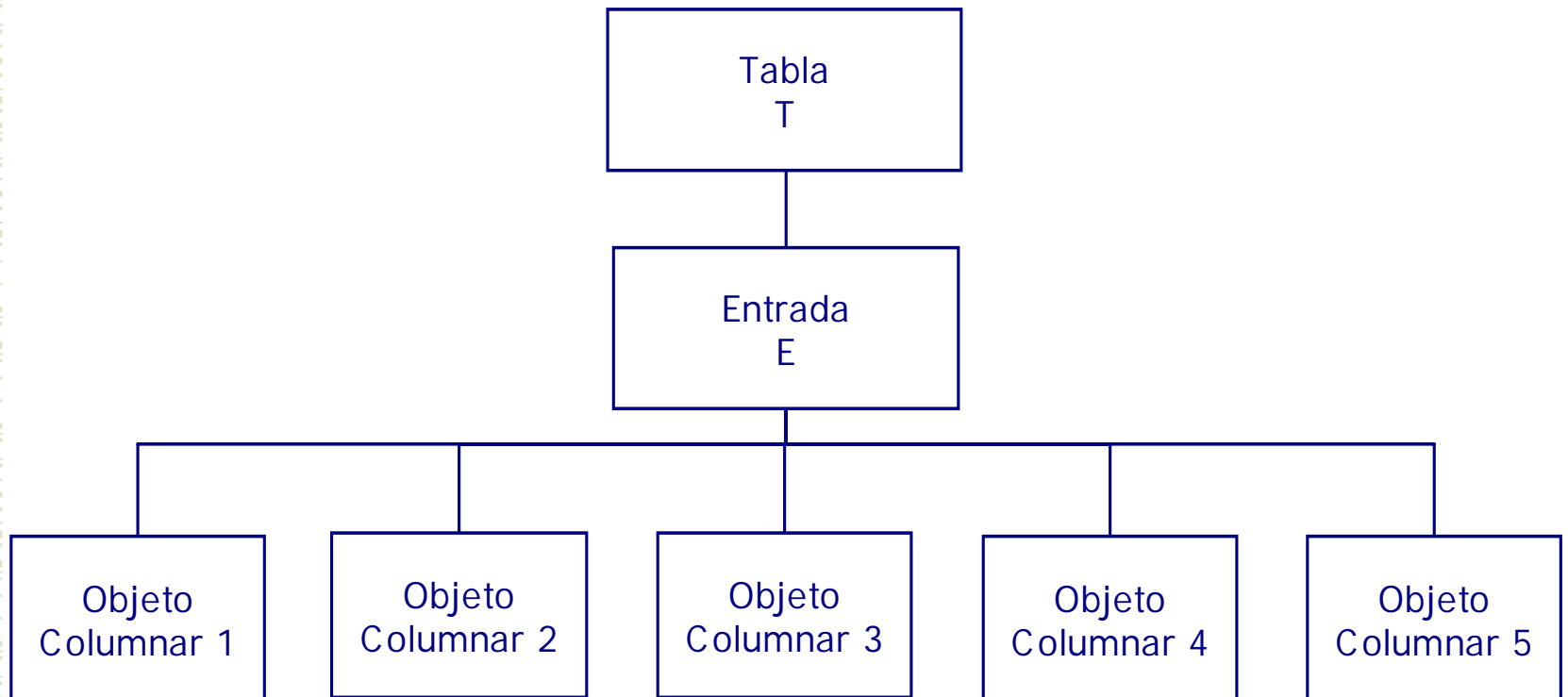
SNMP

◆ MIB

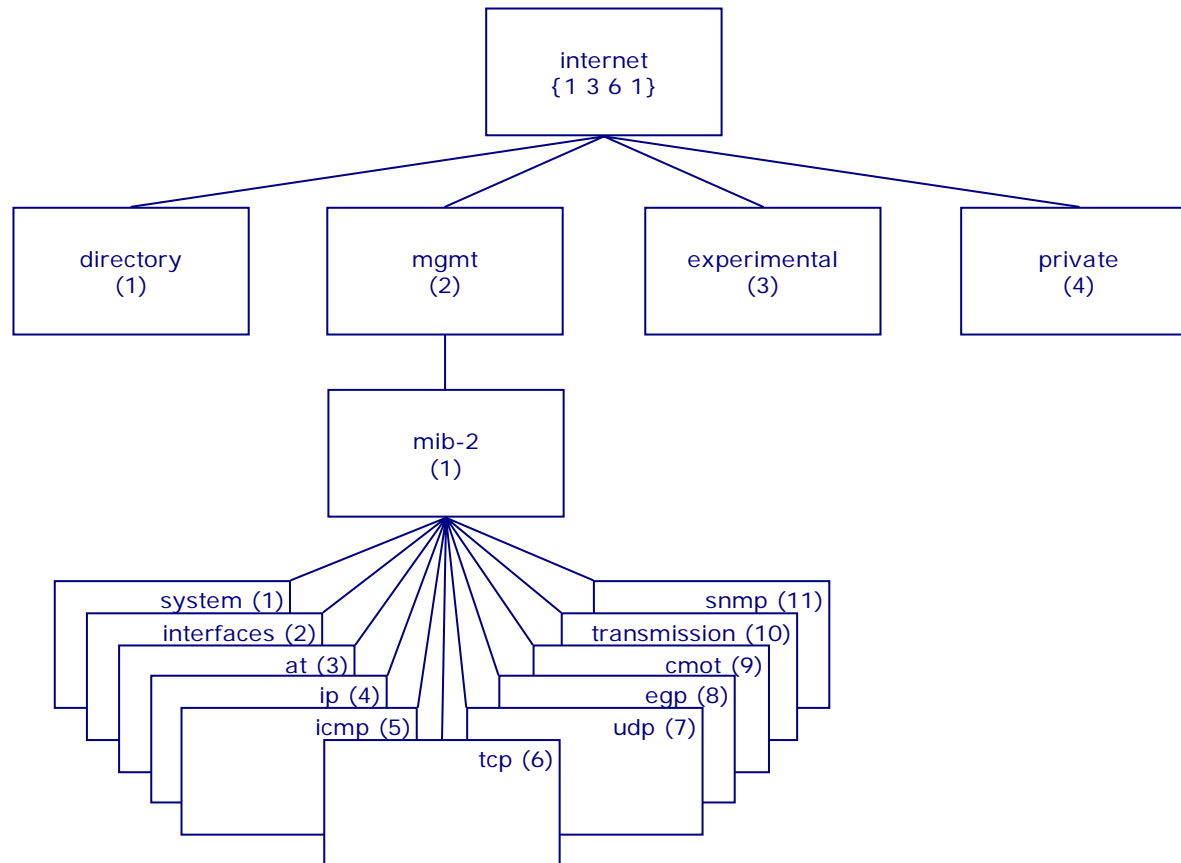
- Existen objetos administrados del tipo escalar y del tipo compuesto.
- El valor de un objeto escalar se obtiene al consultar por OID.0
- El valor de un objeto compuesto, que generalmente corresponde a una tabla, no se puede obtener. Es necesario conocer su estructura interna para consultarlo.
 - Si se conoce el OID de una tabla, obtener el valor de un campo de la tabla se hace consultando por OID.E.C.I, donde:
 - ◆ E indica el número asignado a la entrada, generalmente 1.
 - ◆ C indica el número asignado al campo dentro de cada fila.
 - ◆ I indica el valor del índice de la fila deseada (que depende de la estructura de la tabla en cuestión).

SNMP

♦ Ejemplo de objeto agregado



SNMP



SNMP

◆ System

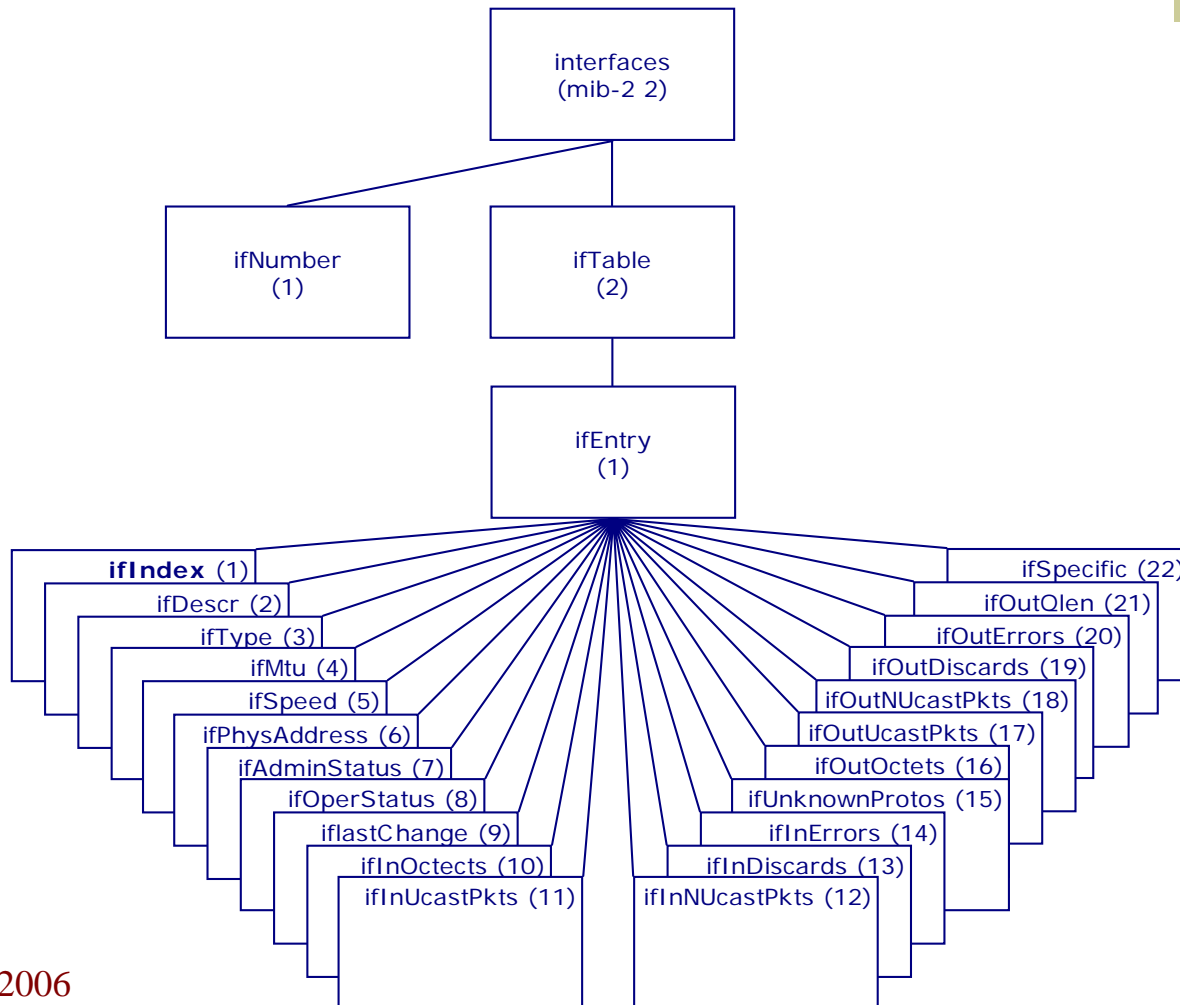
Entidad	OID	Descripción
sysDescr	system 1	Descripción Textual
sysObjectID	system 2	OBJECT IDENTIFIER de la entidad
sysUpTime	system 3	Tiempo desde el último reset (en centenas de segundo)
sysContact	system 4	Persona de contacto
sysName	system 5	Nombre del sistema
sysLocation	system 6	Ubicación física
sysServices	system 7	Valor que indica la capa de servicios provista

SNMP

■ Interfaces

- Contiene los objetos asociados a las interfaces del sistema.
- Si hay más de una, el grupo describe los parámetros asociados a cada interface.
- Especifica el número de interfaces en un componente y los objetos asociados a cada interface. Para ello, contiene dos nodos: *ifNumber* con el número de interfaces y *ifTable* con la lista de las interfaces y sus detalles.

SNMP



SNMP

■ Interfaces

- El campo *ifIndex* sirve de índice en el objeto agregado *ifTable*.
- Un ejemplo de uso del MIB Interfaces es la medida de la tasa de tráfico entrante y saliente para una interfaz específica. Utilizando *get-request* y dado un *ifIndex*, podemos averiguar el número de paquetes unicast entrando (*ifInUcastPkts*) y saliendo (*ifOutUcastPkts*) cada segundo. Como obtenemos un número siempre creciente, es necesario calcular la diferencia entre dos lecturas para determinar la tasa.

SNMP

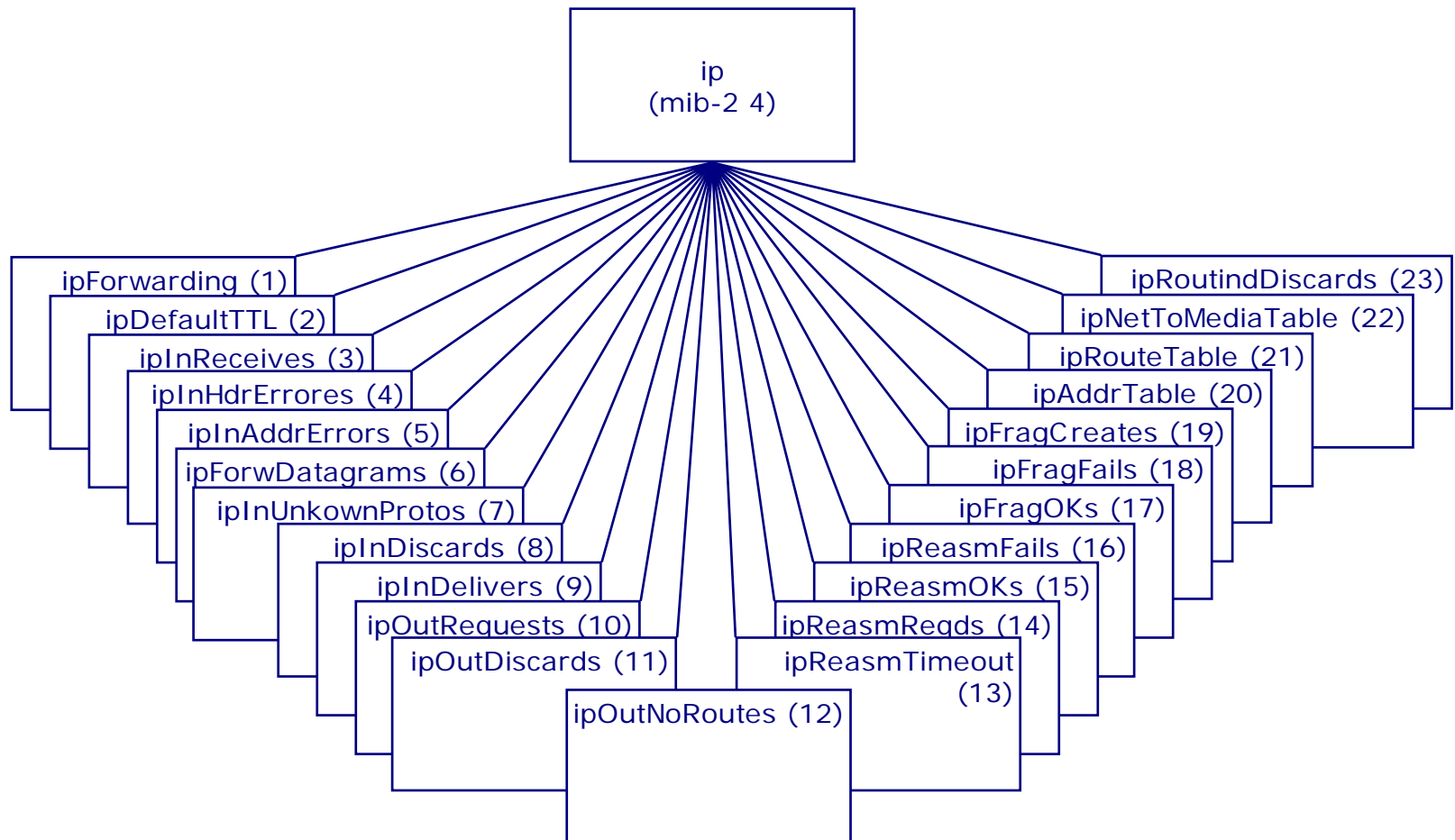
- Address Translation (at)
 - Consiste en una tabla que convierte las direcciones de red en direcciones físicas.
 - En el caso de Ethernet, se refiere al caché de ARP del aparato.
 - En MIB-II cada grupo de protocolo tiene su propia tabla de traducción, por lo que éste grupo se encuentra deprecado y sólo se mantiene por compatibilidad con MIB-I.

SNMP

■ IP

- Internet utiliza el protocolo IP como protocolo de red. El grupo IP tiene la información de los parámetros del protocolo.
- Además tiene la tabla que reemplaza a “Address Translation”.
- Los routers periódicamente ejecutan algún algoritmo de ruteo que actualiza su tabla de rutas, elementos que se encuentran definidos como objetos en este grupo.
- El grupo IP define todos los parámetros necesarios para el nodo de manera de manejar adecuadamente la capa IP.

SNMP



SNMP

■ IP

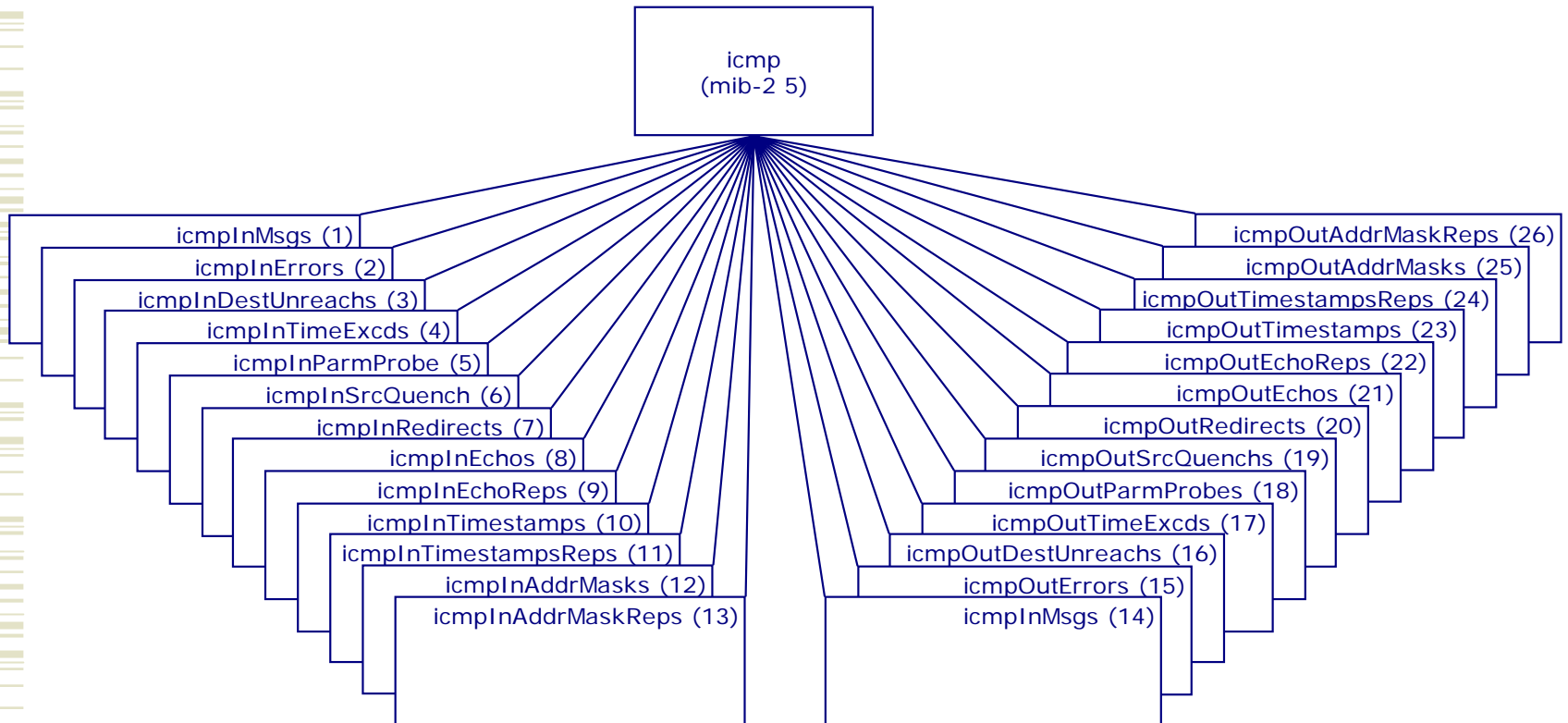
- El grupo contiene tres tablas: IP Address, IP routing e IP Address Translation.
- Se puede utilizar la información de ésta grupo para verificar si un elemento de red esta actuando como router (*ipForwarding*) o para medir el número de datagramas IP con errores (*ipInAddrErrors*).
- La tabla “IP routing” contiene una entrada por cada ruta conocida en el elemento. Permite hasta cinco rutas diferentes hacia el mismo destino.
- La tabla “IP Address Translation” contiene las relaciones entre las direcciones IP y las direcciones físicas de las interfaces.

SNMP

■ ICMP

- Cubre todos los parámetros asociados al protocolo.
- Recordar que es parte integrante del protocolo TCP/IP.
- Contiene las estadísticas asociadas a los mensajes de control ICMP.
- Todos son contadores de sólo lecturas.
- Por ejemplo, se puede utilizar para tener una estadística del número de *requests* de ping enviados (*icmpOutEcho*). Recordar que los mensajes de ping salientes corresponden a ICMP Echo Request.

SNMP

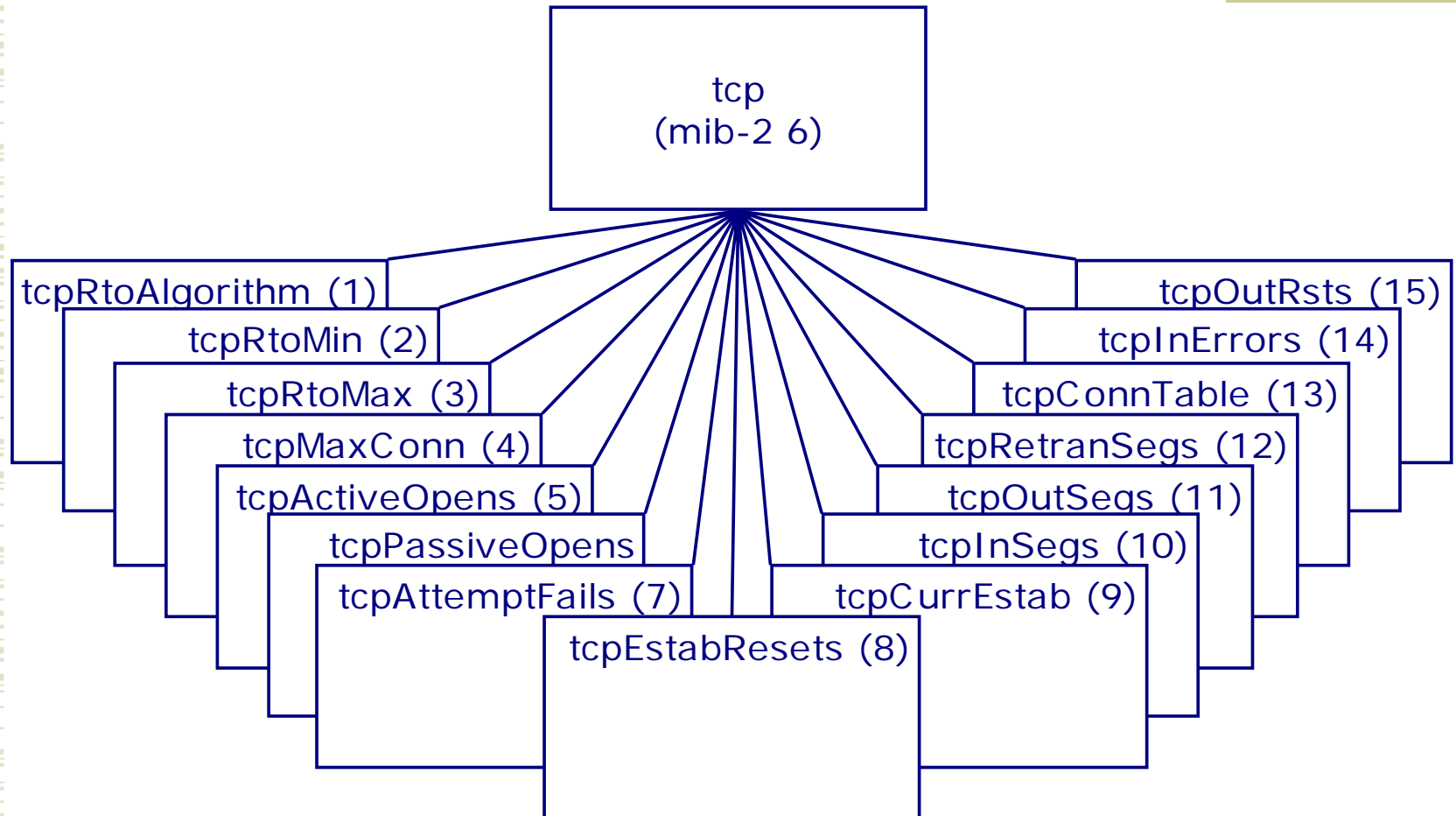


SNMP

■ TCP

- La capa de transporte de Internet define TCP y UDP.
- Este grupo sólo incluye lo relacionado con TCP (el siguiente grupo es de UDP).
- Contiene una tabla: “TCP Connection”, que detalla todas las sesiones TCP activas, con sus direcciones y puertos locales y remotos.

SNMP

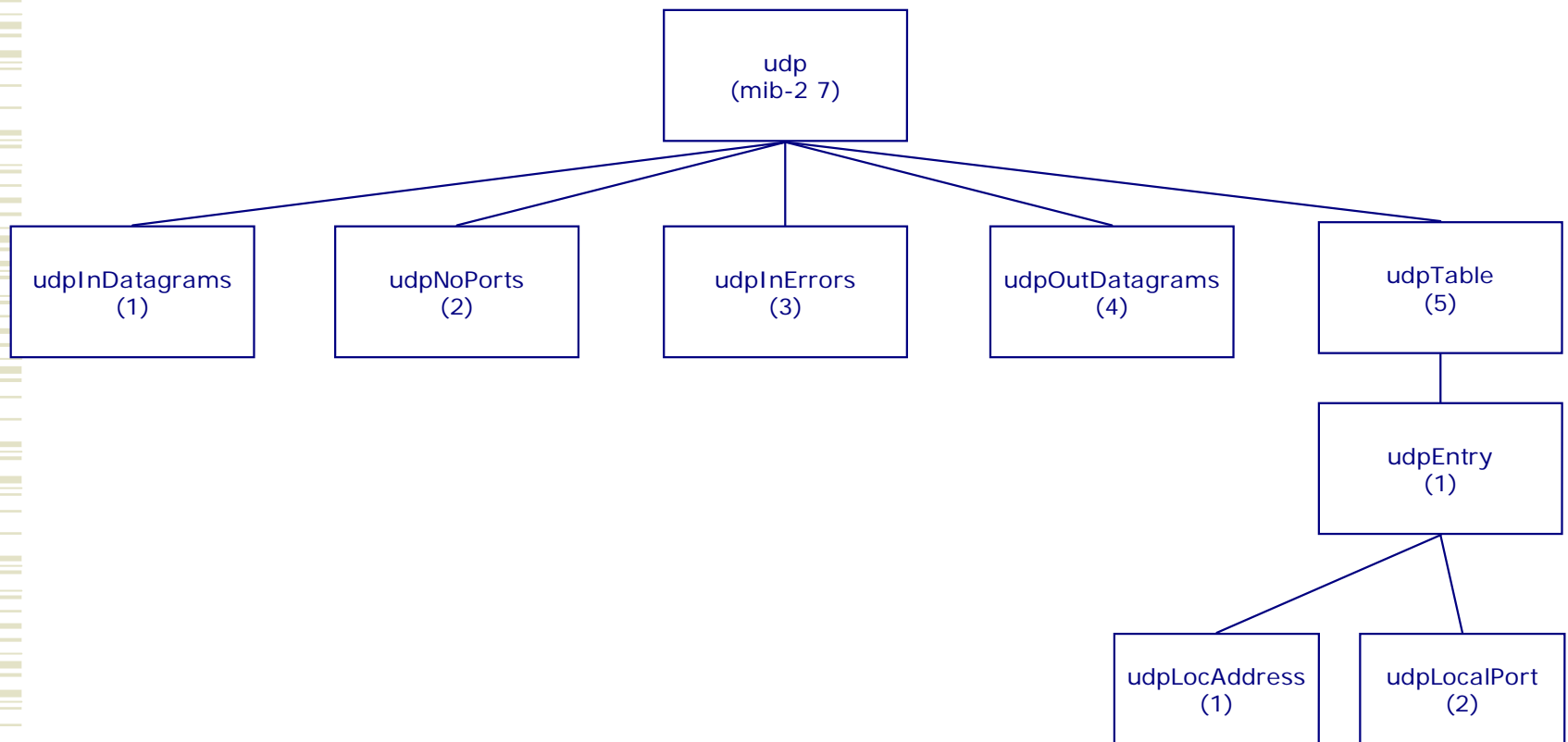


SNMP

■ UDP

- Mantiene información acerca del protocolo UDP.
- Contiene principalmente la tabla “UDP Listener”, con información acerca de los puertos aceptando datagramas UDP.

SNMP



SNMPv1

◆ Modelo Administrativo

- Un administrador y un agente forman una **comunidad**, que se identifica con un string (denominado “community string”).
- Así, un administrador puede tener ciertos privilegios sobre el agente y otro administrador puede tener privilegios diferentes al primero.
- Existe un esquema de autenticación entre los administradores y los agentes, basados en el *community string*.

SNMPv1

◆ Modelo Administrativo

- Un elemento de red comprende muchos objetos administrados, públicos y privados.
- Aún así, un agente puede tener permitido ver sólo un subconjunto de los objetos administrados. Esto es conocido como una **vista MIB**.
- Junto con la “vista”, cada comunidad tiene asociado un **modo de acceso**, ya sea READ-ONLY o READ-WRITE.
- Un par (vista MIB, modo de acceso) constituye un “perfil de comunidad”.
- El “perfil de comunidad” combinado con el modo de acceso de un objeto administrado determinan las operaciones que puede realizar un agente sobre él.