



Redes de Datos II

Servicios TCP/IP III

Network Management

- Cubre aspectos de:
 - Configuración
 - Control
 - Monitoreo
- Necesidad de acceder a diferentes niveles del equipamiento y funcionalidad de la red.
- Diversidad de los mismos.

Metodologías

- Interfaz por línea de comandos(CLI).
- Dependiente del dispositivo.
- Conexión directa con el dispositivo.
- Conexión remota a través de Telnet.
- Configuración descargable por medio de archivos(TFTP).
- Terminal Servers para el caso de redes complejas.

Metodologías

- Interfaz gráfica (GUI).
- Operación directa o remota.
- Más independiente del dispositivo.
- Comandos GUI mapeados a comandos CLI.
- Menor nivel de detalle.

Una única aplicación para administrar la red!

Propuestas en TCP/IP

- Internet Advisory Board (IAB)
 - Normas para TCP/IP y arquitectura ISO
- SNMP: comprende el uso del Protocolo Simple para Administración de la Red (Simple Network Management Protocol, SNMP)
- TCP/IP(CMOT): comprende las normas OSI para administración de la red:
 - Servicios Comunes de Información sobre la Administración (Common Management Information Services, CMIS)
 - Protocolo Común de Información sobre la Administración (Common Management Information Protocol, CMIP).
 - "Common Management Information Services and protocol Over TCP/IP(CMOT)".

SNMP

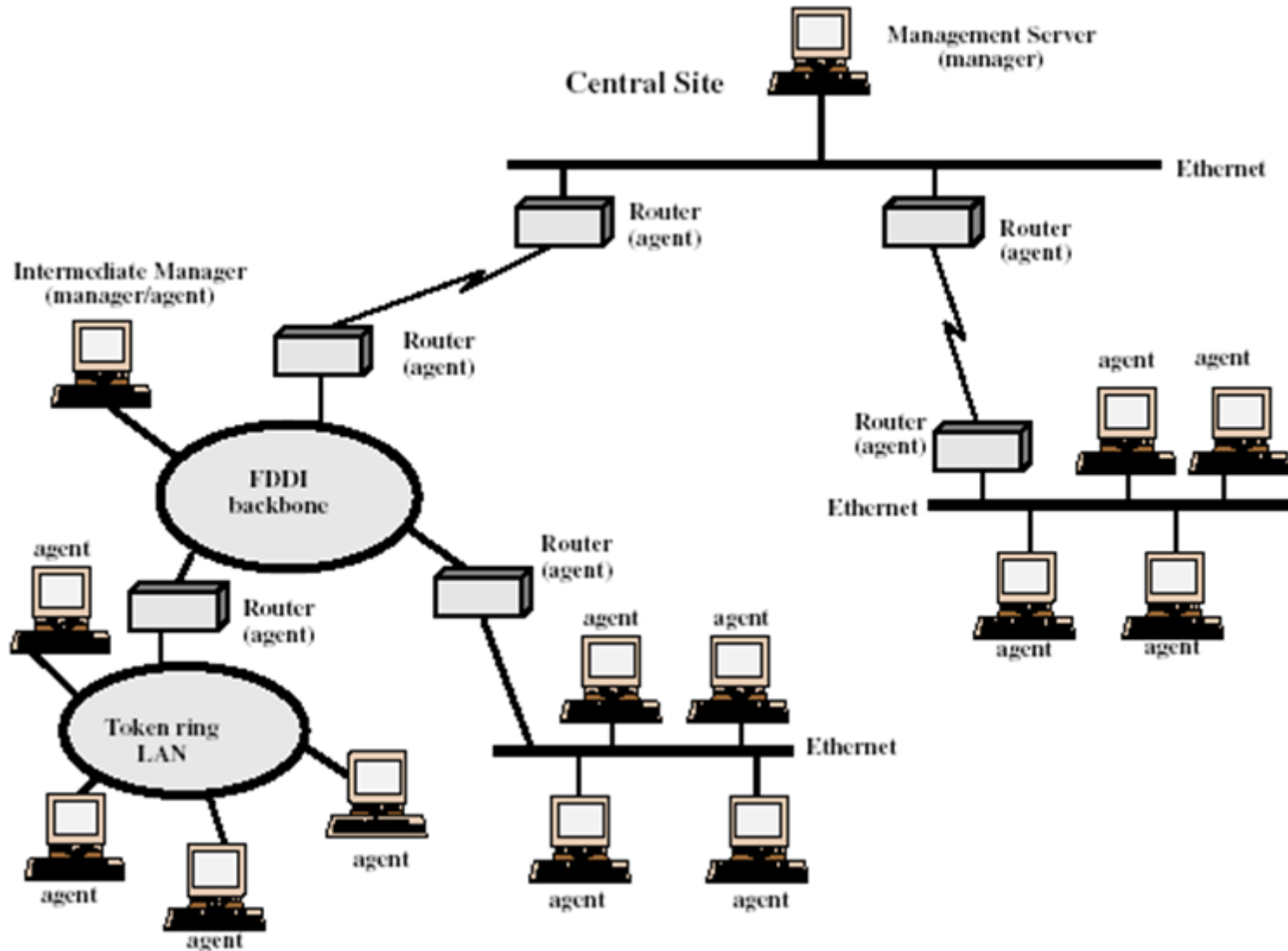
- Actúa a nivel de aplicación para consultar a los diferentes dispositivos (routers, switches, hubs, hosts, modems, impresoras, etc).
- Cada equipo conectado a la red ejecuta procesos (agentes), para realizar una administración tanto remota como local.
 - Actualizan variables (especie de histórico), que máquinas remotas pueden consultar.
 - router: interfaces activas, velocidad de enlaces errores, bytes transmitidos/recibidos.
 - impresora: que se terminó el papel, ...
 - modem: la pérdida de conexión, etc
 - switch: ports conectados, acciones de control por IP duplicados,etc.

La Arquitectura de Administración de Red se compone de cuatro componentes principales:

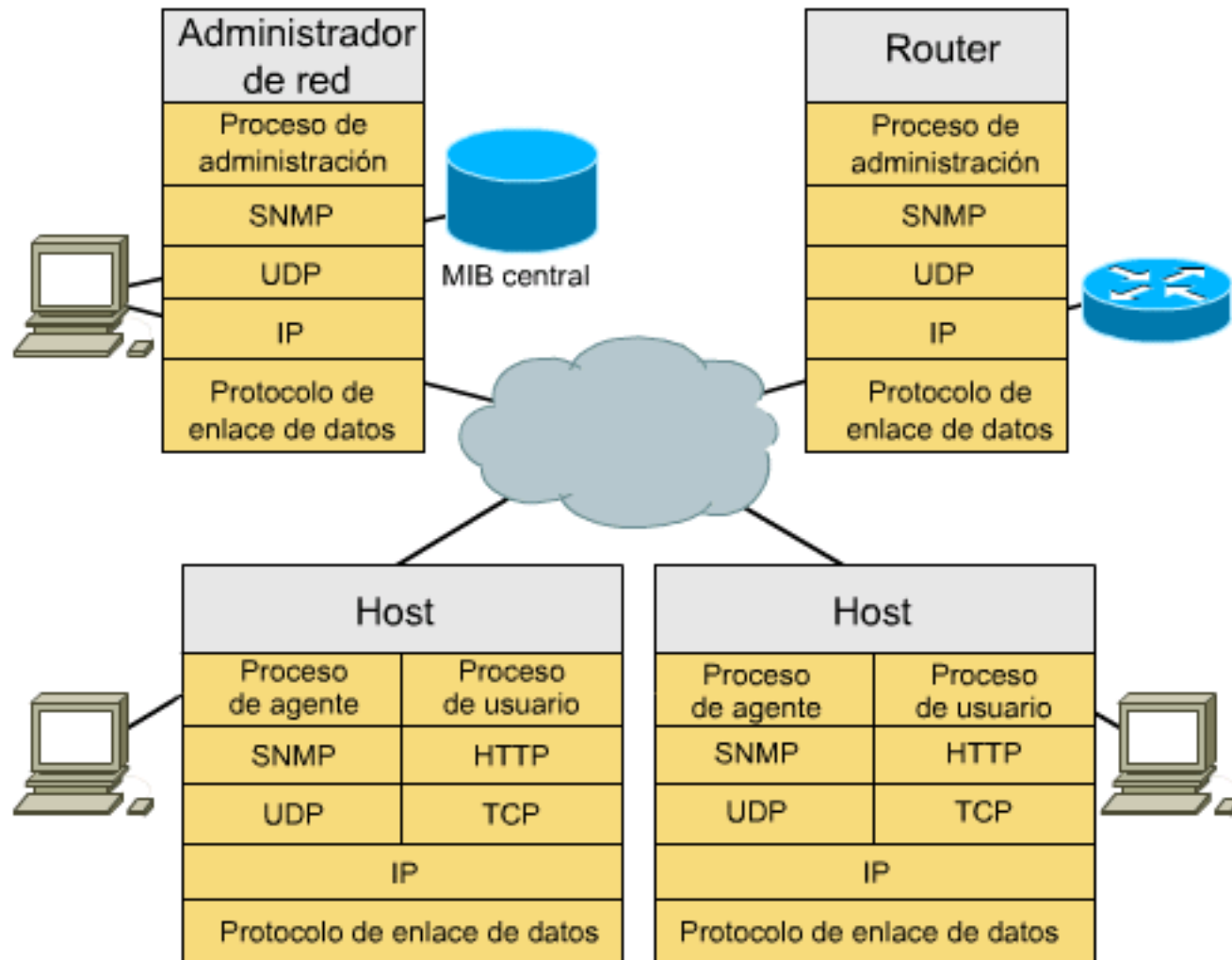
- estación de administración
- agente de administración del dispositivo administrado
- base de información de administración,
- protocolo de administración.

SNMP facilita la comunicación entre la estación administradora y el agente de un dispositivo de red (o nodo administrado), permitiendo que los agentes transmitan datos estadísticos (*variables*) a través de la red a la estación de administración.

Arquitectura



Arquitectura – Detalle Funcional



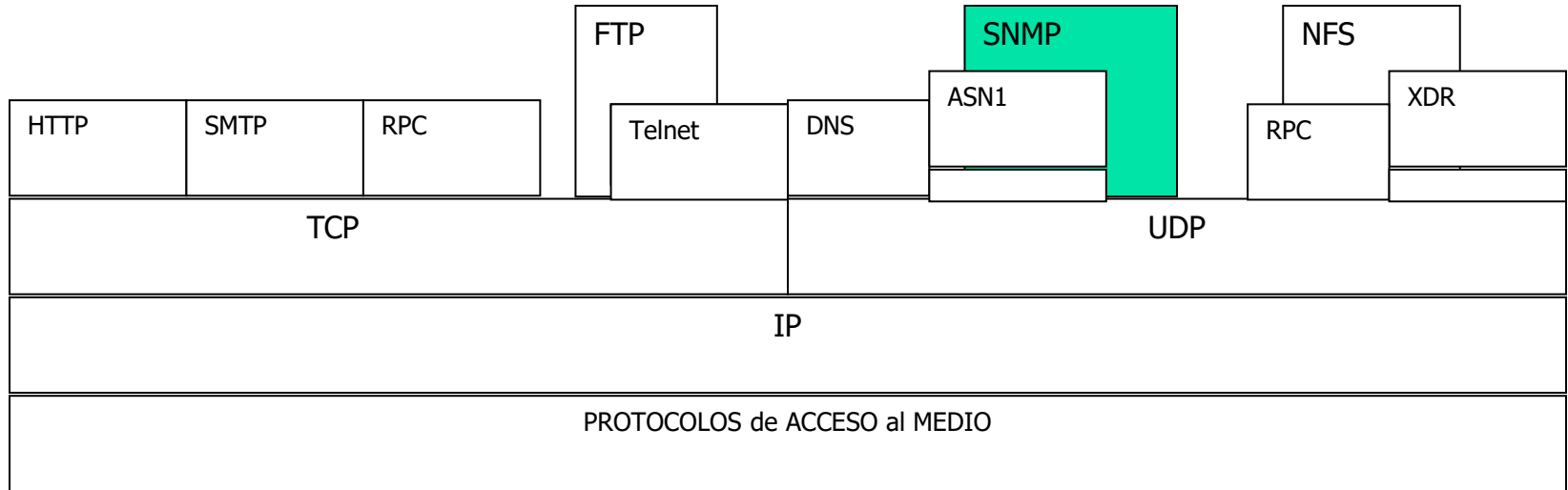
Funcionamiento

- Pregunta:
 - La estación administradora envía solicitud a un agente pidiéndole información o mandándole actualizar su estado. Este método se conoce como sondeo.
- Respuesta:
 - La información recibida del agente.
- El problema del sondeo es que se incrementa con los nodos administrados y en ocasiones puede llegar a perjudicar el rendimiento de la red.
- Interrupción:
 - El agente envía la información al nodo administrador ante una situación predeterminada, por ejemplo una anomalía detectada en la red.

SNMP – Protocolo

- Es independiente del protocolo de nivel de red.
- Se encapsula en UDP o TCP, pero por norma general, en UDP, ports 161 y 162.
 - 161 se utiliza para las transmisiones normales de comando SNMP
 - 162 se utiliza para los mensajes de tipo “trap” o interrupción.

Stack de protocolos



- Formato de representación de la información:
Abstract Syntax Notation.1 (ASN1)

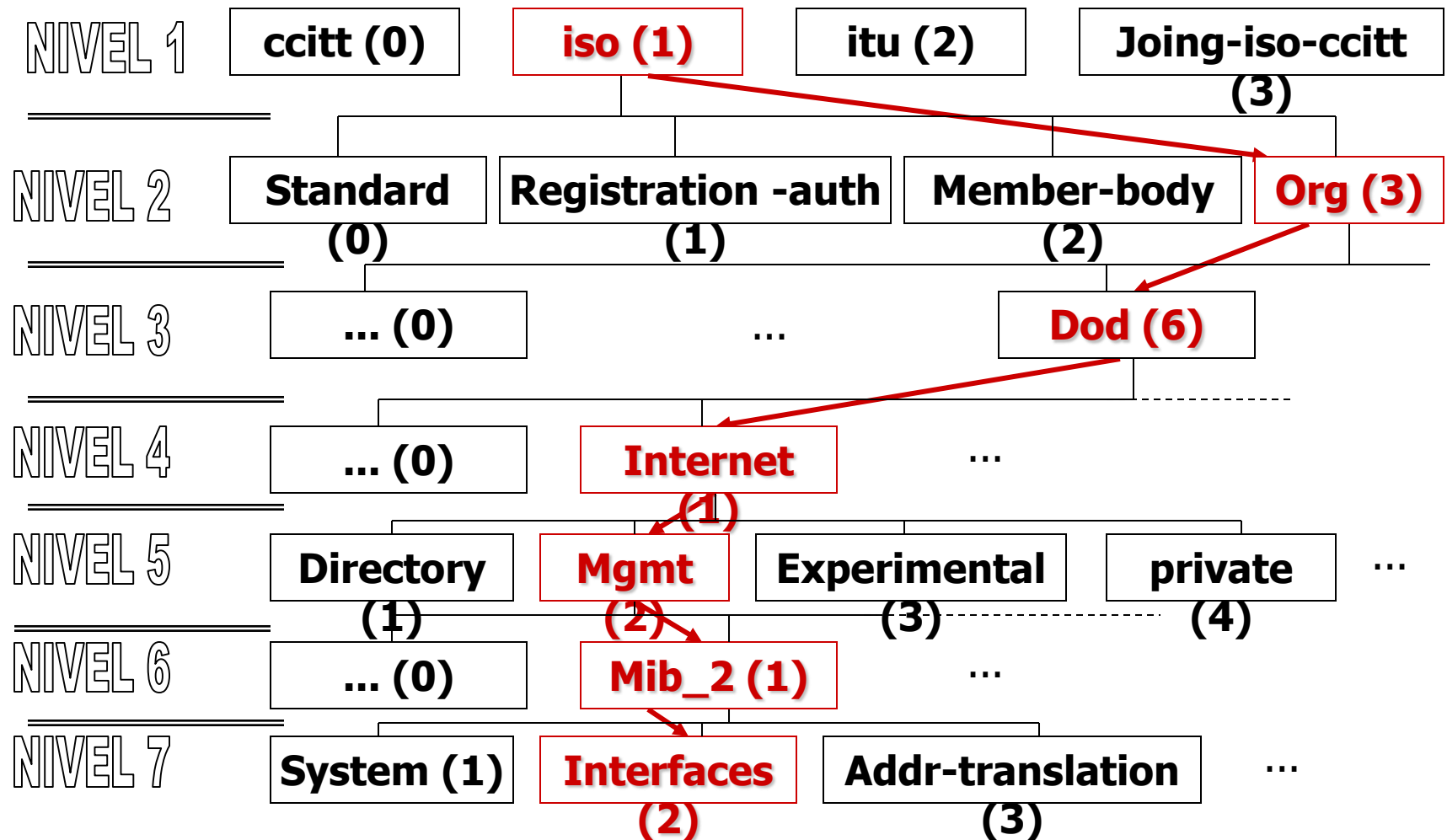
SNMP – Componentes

- Nodos administrados que ejecutan agentes SNMP y estación administradora.
- Estructura e identificación de la información sobre la administración (SMI) : Una especificación que permite definir las entradas en una MIB.
- Base de información de la administración (MIB) :
 - Una base de datos relacional (organizada por objetos (o variables) y sus atributos (o valores)) que contiene información del estado y es actualizada por los agentes.
- SNMP: El método de comunicación entre los dispositivos administrados y los servidores.

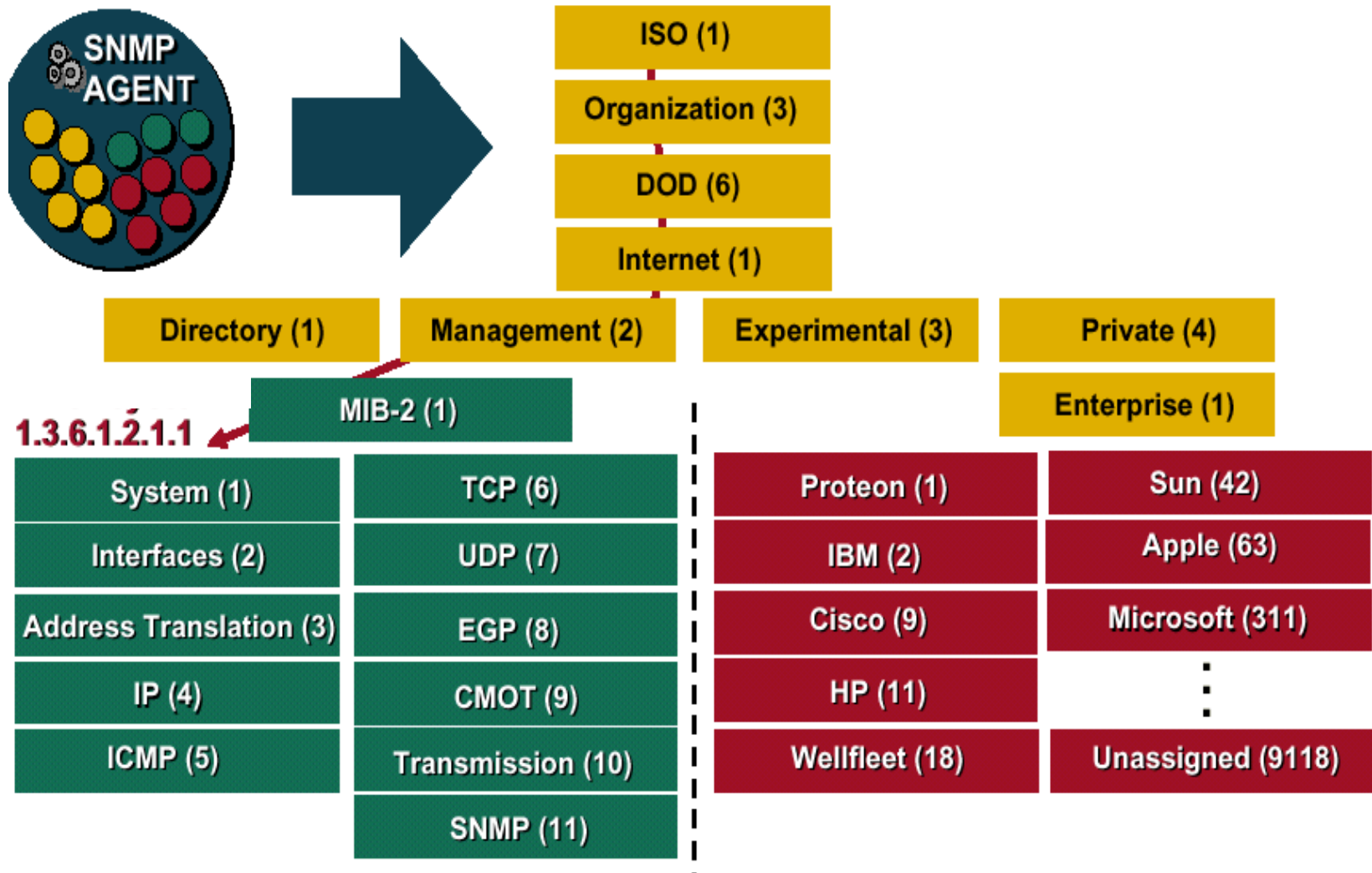
Structure Management Information (SMI)

- Estructura en forma de árbol global para la información de administración, convenciones, sintaxis y las reglas para la construcción de MIBs.
- La MIB está organizada en niveles, que a su vez lo hace en módulos que contienen grupos de variables de interrelacion
 - La estructura SMI guarda similitud con el DNS y sus zonas de autoridad, o variables definidas por cada fabricante.
- Ejemplo de GRUPOS de variables en MIB-2 en la SMI: System (identifica el hw y sw), AT (traducción de dirección de Ethernet a IP), IP (contador de paquetes, fragmentación), ICMP (contador de cada tipo de mensaje ICMP), TCP y UDP (conexiones abiertas TCP), EGP (estadística de protocolo externo)

Acceso a MIB-2.Interfaces



Detaille de MIB-2



iso.org.dod.internet.mgmt.mib_2.interfaces.iftable.ifEntry.variable.puerto

su equivalente

.1.3.6.1.2.1.2.2.1.variable.puerto

- Este formato para la representación de variables puede ser expresadas tanto en ASCII como números separados por puntos, en una notación intermedia entre ASCII y ASN1 conocida como OID (Object Identifier) o descriptor.
- En esta notación inicialmente se identifica el organismo de estandarización, ISO y dentro de éste está ORG y dentro DOD (Departament of Defense), donde la primera rama del árbol desde DOD es Internet.
- Así sucesivamente hasta especificar la variable (u objeto) y el puerto a consultar.

Objetos para monitoreo de Ethernet

- ifOperStatus:
 - Nos indica el estado operacional de un determinado enlace.
- ifAdminStatus:
 - Se utiliza para cambiar el estado operacional de un enlace. Únicamente es accesible por el administrador de la red.
- ifInErrors:
 - Nos indica el número de paquetes entrantes en los que el agente ha encontrado algún tipo de error.
- ifInDiscards:
 - El número de paquetes entrantes que el agente ha seleccionado para ser eliminados. No necesariamente son solo los que contienen errores. Una razón para eliminar paquetes suele ser liberar espacio en los buffers de entrada.
- ifInOctets:
 - Indica el número total de bytes recibidos en el enlace.

Objetos para monitoreo de Ethernet...

■ ifOutErrors:

- Indica el número total de paquetes que no han podido ser enviados por causa de un error.

■ ifOutDiscards:

- El número de paquetes salientes que el agente ha seleccionado para ser eliminados. Además de aquellos que contienen algún error, también se eliminan para liberar espacio en los buffers de salida.

■ ifOutOctets:

- El número total de octetos transmitidos fuera del enlace.

■ ifSpeed:

- Nos da una estimación del ancho de banda actual que dispone el enlace en bits por segundo. En aquellos enlaces en los que el ancho de banda no varíe o en los que no sea posible hacer una aproximación exacta, este objeto suele contener el ancho de banda nominal.

La base de información de administración tiene una estructura de base de datos (según SMI) y reside en cada dispositivo administrado.

La base de datos contiene una serie de objetos (variables), que son datos sobre recursos reunidos en el dispositivo administrado.

Objeto – Variable

- Parámetro que corresponde a un grupo del dispositivo administrado: ***System, AT, IP, TCP, UDP, EGP, ...***
- Posee atributos (o valores) que representan el estado del objeto
- Los únicos métodos que operan sobre los atributos son **escribir y leer**
- La sintaxis utilizada para representar la información es ASN.1
- Es un subconjunto de SMI

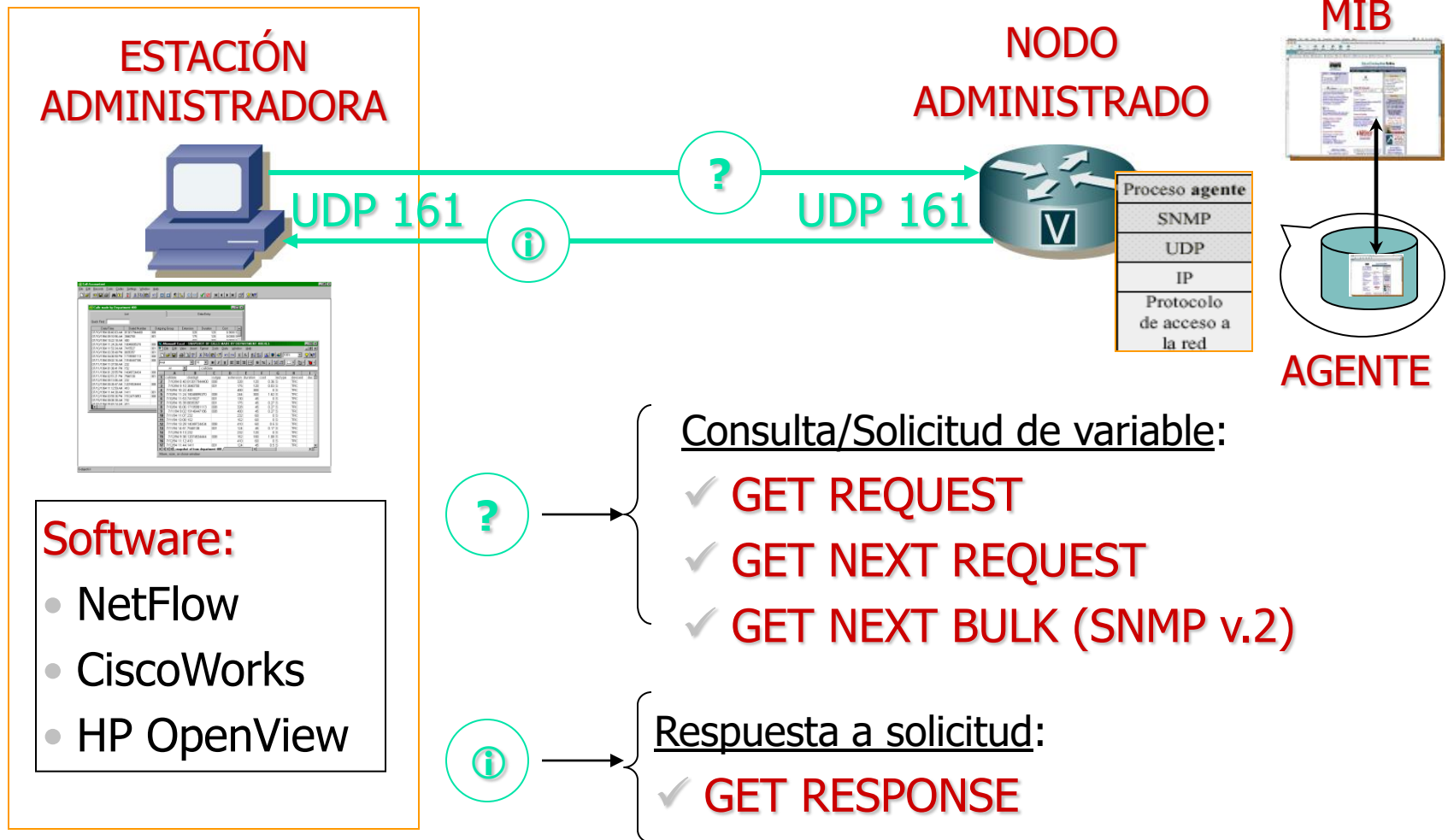
Agentes

- Los periféricos que tienen integradas las capacidades para SNMP corren un paquete pequeño de software agente para administración (generalmente de 64kb), cargado como parte de un ciclo de arranque o guardado en la memoria fija (firmware) del dispositivo.
- Estos dispositivos que tienen agentes SNMP se dice que se trata de dispositivos o nodos administrados.
- No todos los nodos son agentes, ni pueden serlo.
- Agente apoderado (o proxy): gestiona los dispositivos que no pueden ejecutar un agente local.
 - Localización: externo al dispositivo administrado.

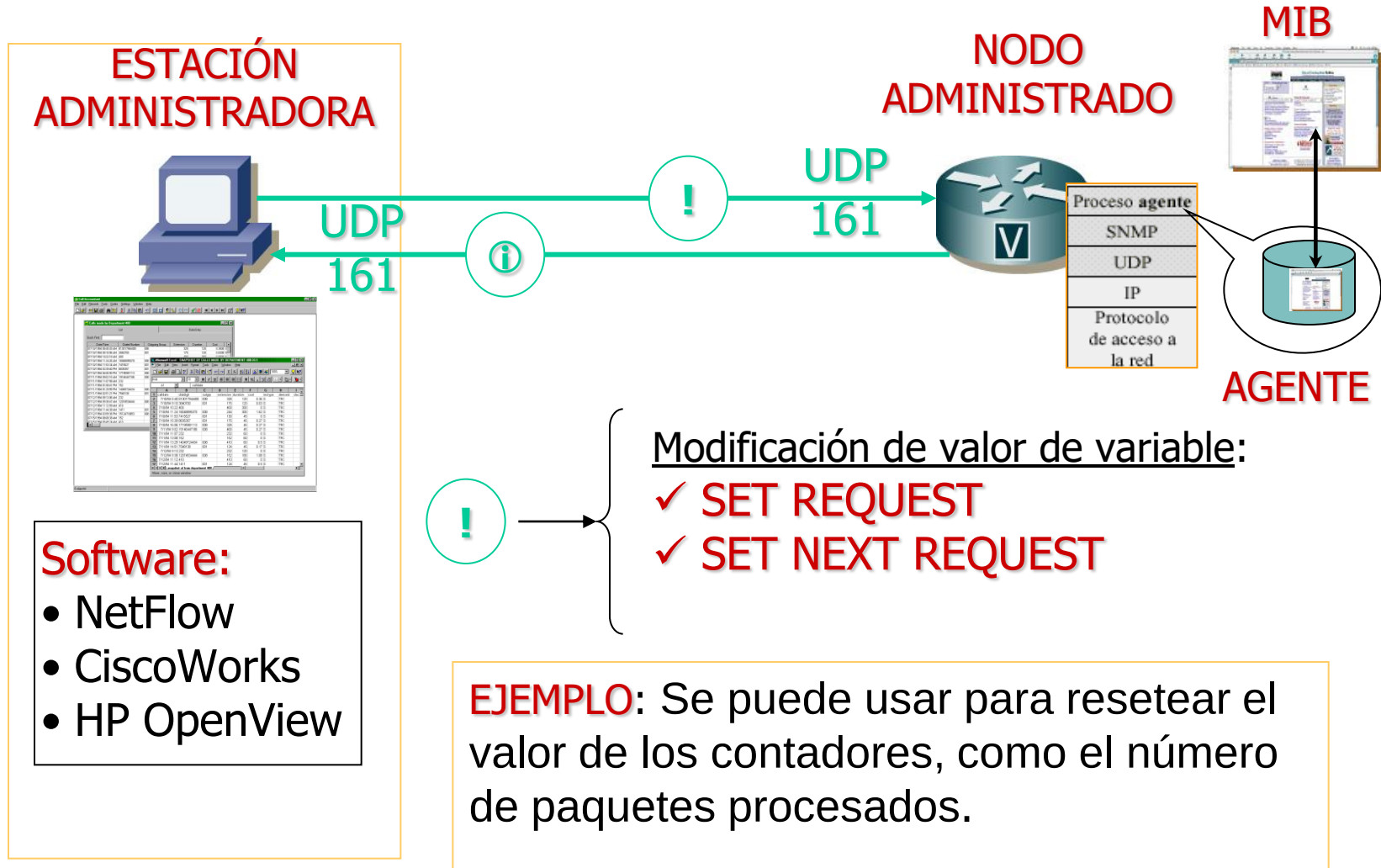
Agentes...

- Los dispositivos administrados por SNMP (puentes, routers, hubs y switches) se comunican con el software servidor SNMP que está localizado en cualquier parte de la red.
- El agente de administración responde a la estación de administración de dos maneras:
 - Mediante sondeo o pooling: la estación de administración requiere datos desde el agente y el agente responde con los datos solicitados
 - Por interrupción: tal que se establecen umbrales (límites superiores o inferiores) en el dispositivo administrado y si se supera este umbral en el dispositivo, envía un mensaje de alerta a la estación de administración.
- En ocasiones se puede combinar ambos métodos, conocido como sondeo dirigido a interrupción.

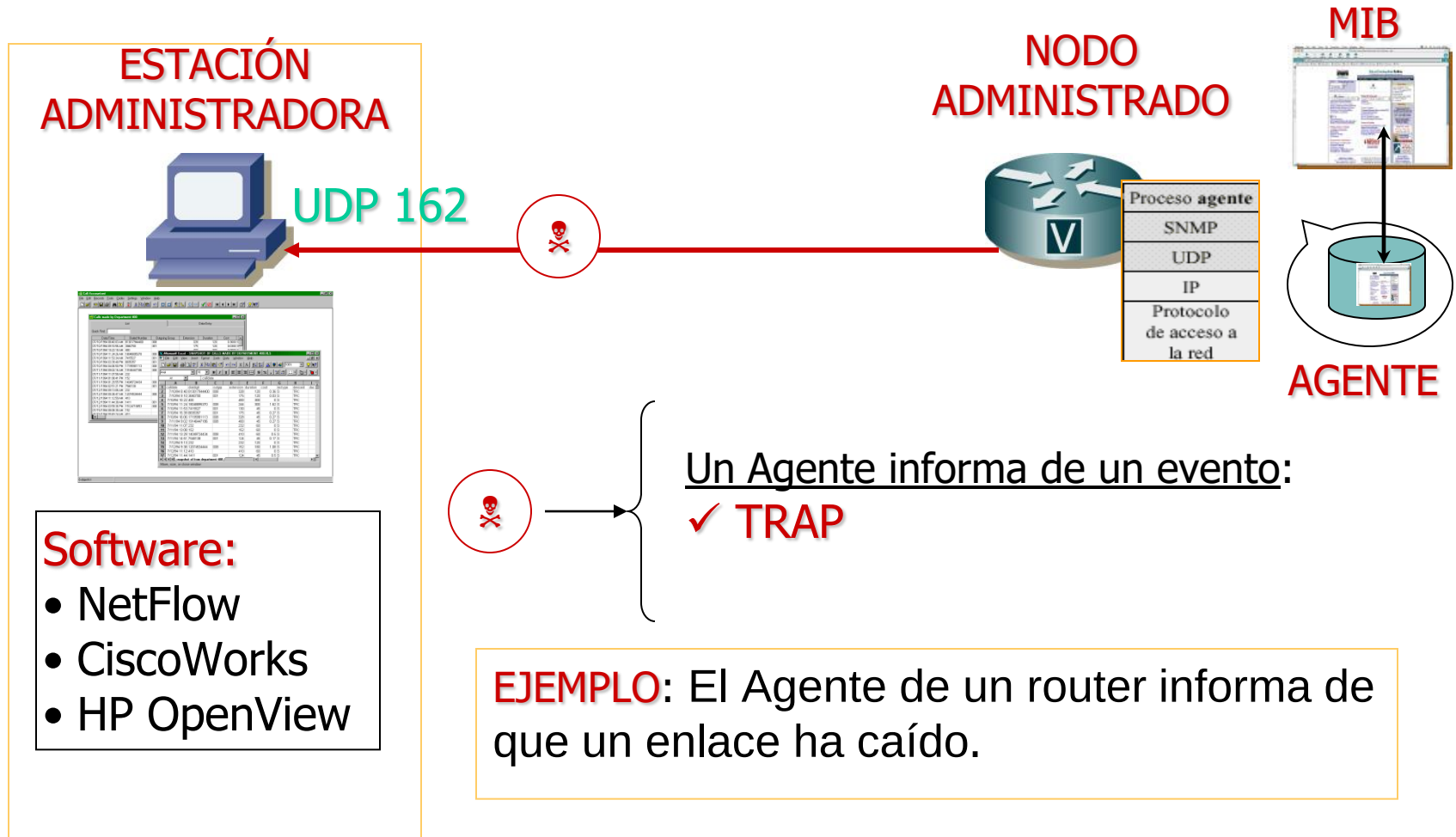
SNMP en acción



SNMP en acción...



SNMP – Traps



SNMP – Primitivas

1. GET REQUEST
2. GET NEXT REQUEST
3. GET BULK REQUEST (en SNMP v2)
4. SET REQUEST
5. SET NEXT REQUEST
6. GET RESPONSE
7. TRAP
8. INFORM REQUEST (en SNMP v2)

Primitivas

- Get Request
 - Solicita uno o mas (lista) atributos (valores) de un objeto (o variable).
 - Transmitida por el nodo administrador
 - Recibida por el agente que contesta
- Get Next Request
 - Solicita el siguiente atributo de un objeto
 - Transmitida por el nodo administrador
 - Recibida por el agente que contesta
- Get Bulk Request
 - Solicita un conjunto amplio de atributos en vez de solicitar uno a uno
 - Transmitida por el nodo administrador
 - Recibida por el agente

Primitivas...

- Set Request
 - Actualiza uno o varios atributos de un objeto
 - Transmitida por el nodo administrador
 - Recibida por el agente
- Set Next Request
 - Actualiza el siguiente atributo de un objeto
 - Transmitida por el nodo administrador
 - Recibida por el agente

Primitivas...

- Get Response
 - Devuelve los atributos solicitados
 - Transmitida por el agente
 - Recibida por el nodo administrador
- Trap
 - Informa fallos como la pérdida de comunicación con un vecino
 - Transmitida por el agente
 - Recibida por el nodo administrador

Primitivas...

- Inform Request
 - Describe la base local de información de gestión MIB para intercambiar información nodos de administración entre sí
 - Transmitida por el nodo administrador
 - Recibida por otro nodo administrador

- Operaciones con grandes volúmenes: se incorpora una PDU GetBulkRequest.
 - Esta PDU proporciona a las estaciones administradoras la posibilidad de trabajar con grandes cantidades de datos, de una sola vez, como grandes tablas.
- Comunicación entre administradores:
 - Inform_Request PDU, facilita la comunicación entre diferentes estaciones administradoras, permitiendo la existencia de jerarquías que son necesarias en sistemas muy complejos.

- Mejoras en las adquisiciones:
 - En versión 1 cuando una de las variables en la lista de un comando GET fallaba, hacía que todo el comando fallara, obligando a eliminar esta variable de la lista y volver a consultar. En SNMPv2 este procesamiento es automático, y el error se indica en el valor de retorno de la variable.
- Mejoras en monitorización remota:
 - En redes que no están conectadas directamente a la estación de administración.

- Definido básicamente para suplir deficiencias de seguridad de v1 y v2.
- Provee 3 servicios:
 - Autenticación.
 - Privacía.
 - Control de acceso.

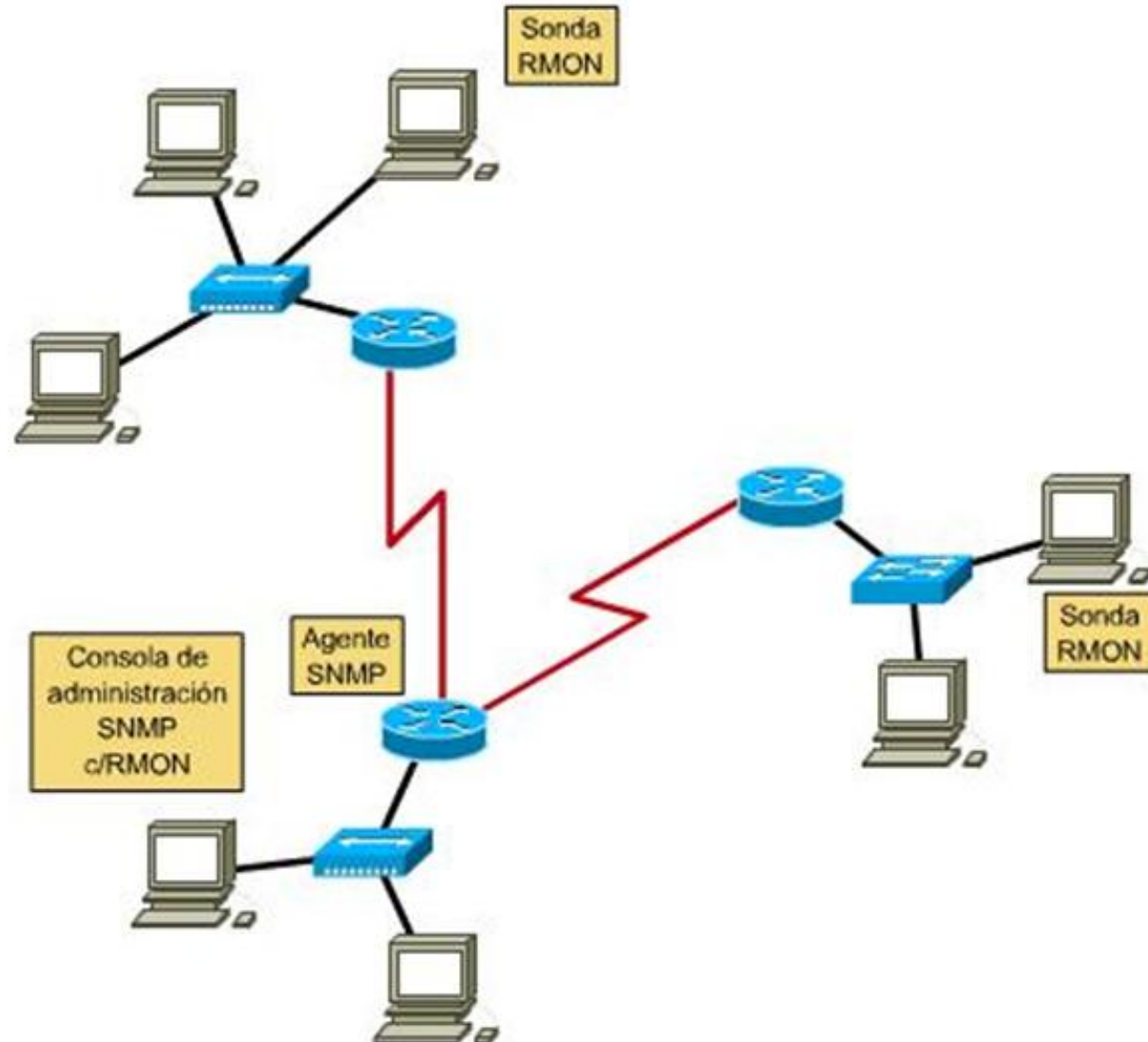
SNMP – Limitaciones

- SNMP gestiona dispositivos individuales, pero no permite diagnosticar fallos en un red remota u otro segmento de red.
- Para ello, el software de monitorización debe trasladarse a cada segmento de red.
- Esto se puede resolver mediante el uso de agentes en los segmentos remotos de red, utilizando equipos especiales o bien ordenadores de propósito general, llamados sondas RMON (Remote MONitor)

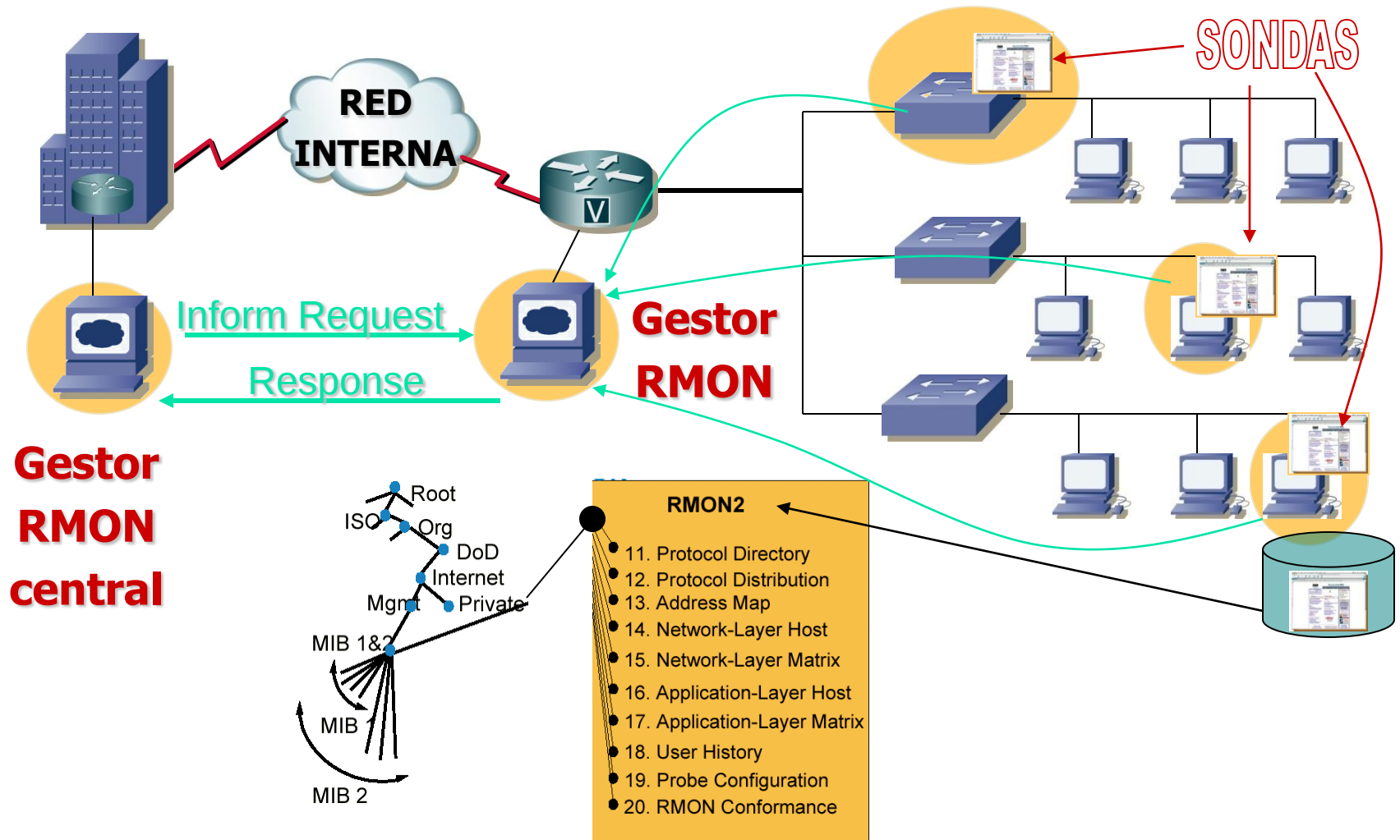
Remote MONitor

- Una de las mejoras principales de SNMP se denomina Monitoreo Remoto (RMON).
- Las extensiones de RMON a SNMP brindan la capacidad para observar la red como un todo, aunque esté distribuida, en contraste con el análisis de dispositivos individuales, declarándose para ello una MIB especial para guardar información de monitorización de un segmento de red diferente. La MIB asociada es 1.3.6.1.2.1.16
- Las sondas RMON recopilan información y tiene la misma función que un agente SNMP, transmitiendo la información periódicamente. Además, pueden procesar la información a enviar a la estación de administrador.
- La RMON está localizada en cada segmento de red y pueden introducirse en un host, en un switch, en un router o en un dispositivo específico para ello. Además, permite añadir redundancia a la administración de la red, ya que RMON permite volcar los datos a varias consolas de administración.
- La RMON1 trabaja en información de capa 1 y 2.
- La RMON2 trabaja en información de capa 3 y superiores.

SNMP con RMON



Funcionamiento de RMON

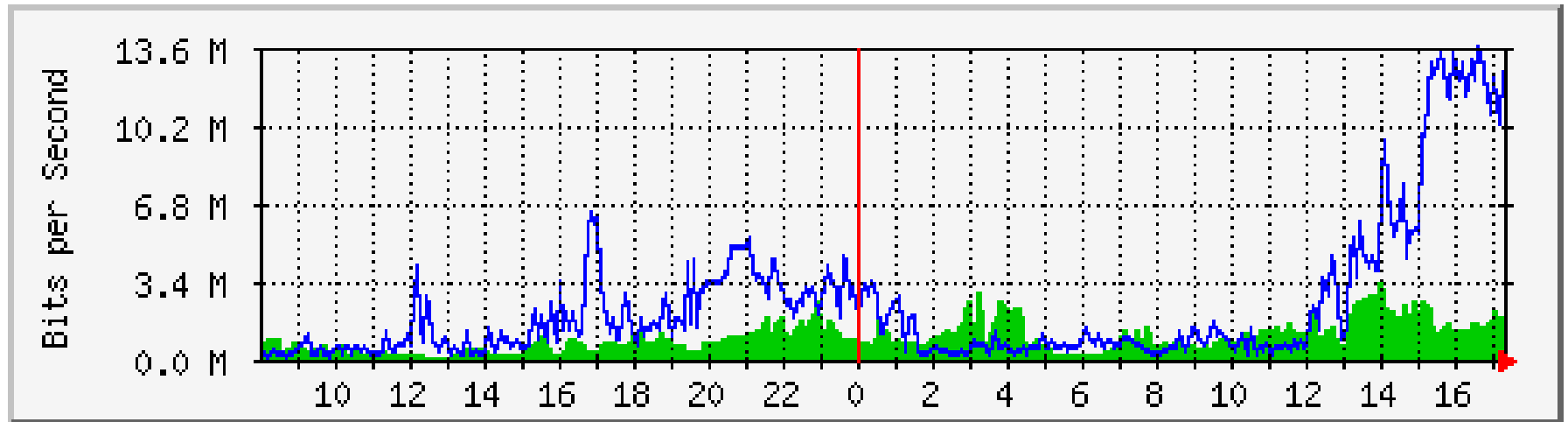


- *Multi Router Traffic Grapher* (MRTG) es una herramienta para monitorización de tráfico en las redes y sus enlaces tanto internos como externos.
- MRTG genera páginas HTML con imágenes PNG, que ofrecen una visión en tiempo real del tráfico.
- MRTG está escrito en el Perl y C.

MRTG...

- MRTG es un script en Perl que utiliza SNMP para leer cualquiera de los atributos de los objetos (contadores) de los routers y un programa rápido en C que procesa la información para visualizarla gráficamente en tiempo real.
- Además, MRTG guarda la información por semanas, meses y años, monitorización hasta 200 enlaces.
- MRTG se utiliza generalmente para monitorizar la carga del sistema, sesiones establecidas, tráfico, errores, etc

MRTG...



RFCs(164 Nov. 2018) SNMP

Number	Title	Authors	Date	More Info	Status
RFC 3411 STD 62	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	D. Harrington, R. Presuhn, B. Wijnen	December 2002	Obsoletes RFC 2571, Updated by RFC 5343,RFC 5590	Internet Standard
RFC 3412 STD 62	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	J. Case, D. Harrington, R. Presuhn, B. Wijnen	December 2002	Obsoletes RFC 2572, Updated by RFC 5590	Internet Standard
RFC 3413 STD 62	Simple Network Management Protocol (SNMP) Applications	D. Levi, P. Meyer, B. Stewart	December 2002	Obsoletes RFC 2573,Errata	Internet Standard
RFC 3414 STD 62	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	U. Blumenthal, B. Wijnen	December 2002	Obsoletes RFC 2574, Updated by RFC 5590,Errata	Internet Standard

RFCs SNMP

Number	Title	Authors	Date	More Info	Status
RFC 3415, STD 62	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)	B. Wijnen, R. Presuhn, K. McCloghrie	December 2002	Obsoletes RFC 2575,Errata	Internet Standard
RFC 3416, STD 62	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)	R. Presuhn, Ed.	December 2002	Obsoletes RFC 1905,Errata	Internet Standard
RFC 3417, STD 62	Transport Mappings for the Simple Network Management Protocol (SNMP)	R. Presuhn, Ed.	December 2002	Obsoletes RFC 1906, Updated by RFC 4789,RFC 5590	Internet Standard
RFC 3418, STD 62	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)	R. Presuhn, Ed.	December 2002	Obsoletes RFC 1907,Errata	Internet Standard
<u>RFC 5590</u>	Transport Subsystem for the Simple Network Management Protocol (SNMP)	D. Harrington, J. Schoenwaelder	June 2009	Updates RFC 3411 , RFC 3412 , RFC 3414 , RFC 3417	Draft Standard (was published as Proposed Standard)

RFCs SNMP

Number	Title	Authors	Date	More Info	Status
RFC 6353	Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)	W. Hardaker	July 2011	Obsoletes RFC 5953	Draft Standard
RFC 6765	xDSL Multi-Pair Bonding (G.Bond) MIB	E. Beili, M. Morgenstern	February 2013	Errata	Proposed Standard
RFC 6766	xDSL Multi-Pair Bonding Using Time-Division Inverse Multiplexing (G.Bond/TDIM) MIB	E. Beili	February 2013	Errata	Proposed Standard
RFC 6767	Ethernet-Based xDSL Multi-Pair Bonding (G.Bond/Ethernet) MIB	E. Beili, M. Morgenstern	February 2013	Errata	Proposed Standard
RFC 6768	ATM-Based xDSL Bonded Interfaces MIB	E. Beili	February 2013	Errata	Proposed Standard

RFCs SNMP

Number	Title	Authors	Date	More Info	Status
RFC 6933	Entity MIB (Version 4)	A. Bierman, D. Romascanu, J. Quittek, M. Chandramouli	May 2013	Errata, Obsoletes RFC 4133	Proposed Standard
RFC 7241	The IEEE 802/IETF Relationship	S. Dawkins, P. Thaler, D. Romascanu, B. Aboba, Ed.	July 2014	Errata, Obsoletes RFC 4441	Informational
RFC 7407	A YANG Data Model for SNMP Configuration	M. Bjorklund, J. Schoenwaelder	December 2014	Errata	Proposed Standard
RFC 7630	HMAC-SHA-2 Authentication Protocols in the User-based Security Model (USM) for SNMPv3	J. Merkle, Ed., M. Lochter	October 2015	Errata, Obsoleted by RFC 7860	Proposed Standard
RFC 7860	HMAC-SHA-2 Authentication Protocols in User-Based Security Model (USM) for SNMPv3	J. Merkle, Ed., M. Lochter	April 2016	Obsoletes RFC 7630	Proposed Standard
RFC 8038	Exporting MIB Variables Using the IP Flow Information Export (IPFIX) Protocol	P. Aitken, Ed., B. Claise, S. B S, C. McDowall, J. Schoenwaelder	May 2017		Proposed Standard