SNMP

GRUPO 5:

MARTÍN DOS SANTOS MORAES

JONATHAN MAIA

ARIEL RAMIREZ

LUIS JURADO TAPIA

INTRODUCCIÓN SNMP

- IETF(Internet Engenering Task Force)
- Sus fines

INTRODUCCIÓN SNMP

- Fue Desarrolado por el IETF (Internet Engineering task force) por allá en los 90´con el fin de facilitar en gestionamiento de redes.

CONCEPTOS BÁSICOS

- Simple Network Management Protocol
- Compuesto de un conjunto normas para la gestión de red
- TCP/IP
- ¿Qué permite hacer este protocolo?

CONCEPTOS BÁSICOS

- SNMP o Simple Network Management Protocol (Protocolo de simple administración de red) se compone de un conjunto de normas para la gestión de la red, incluyendo una capa de aplicación del protocolo, una base de datos de esquema y un conjunto de objetos de datos, es decir, en simples palabras es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de los protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar, resolver sus problemas y planear su crecimiento.

DISPOSITIVOS QUE SOPORTAN SNMP

- Routers
- Swich
- Servidores
- Impresoras
- Pc´s de escritorio
- Y muchos mas…

EJEMPLOS DE SNMP

- En router: Interfaces activos, velocidad de sus enlaces , números de errores, bytes emitidos, bytes recibidos ,etc.
- En una impresora: Se termino el papel, no hay mas tinta, etc.
- En modem: la perdida de conexión , etc.
- En swich: Bocas conectadas, desconectar bocas, si la maquina esta infectada de virus, etc.

VERSIONES

- SNMPv1
- SNMPv2
- SNMPv3

COMPONENTES BÁSICOS

- Dispositivos Administrados
- Agentes
- Sistemas Administradores de red (NMS´s)

DISPOSITIVOS ADMINISTRADOS

- 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 NMS´s usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers , servidores de acceso, swiches , bridges, hubs, computadores o impresoras.

AGENTE

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

UN SISTEMA ADMINISTRADOR DE RED (NMS)

- Ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS´s proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o mas NMS´s deben existir en cualquier red administrada.

COMANDOS BÁSICOS

- El comando de lectura
- El comando de escritura
- El comando de notificación
- Las operaciones transversales

EL COMANDO DE LECTURA

- Es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son matenidas por los dispositivos administrados.

EL COMANDO DE ESCRITURA

- Es usado por NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados .

EL COMANDO DE NOTIFICACIÓN

- Es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS

OPERACIONES TRANSVERSALES

- Son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables, como por ejemplo , una tabla de rutas.

BASE DE INFORMACIÓN DE ADMINISTRACIÓN SNMP (MIB)

- Router, servidores, hubs.
- Objetos administrados
- MIB

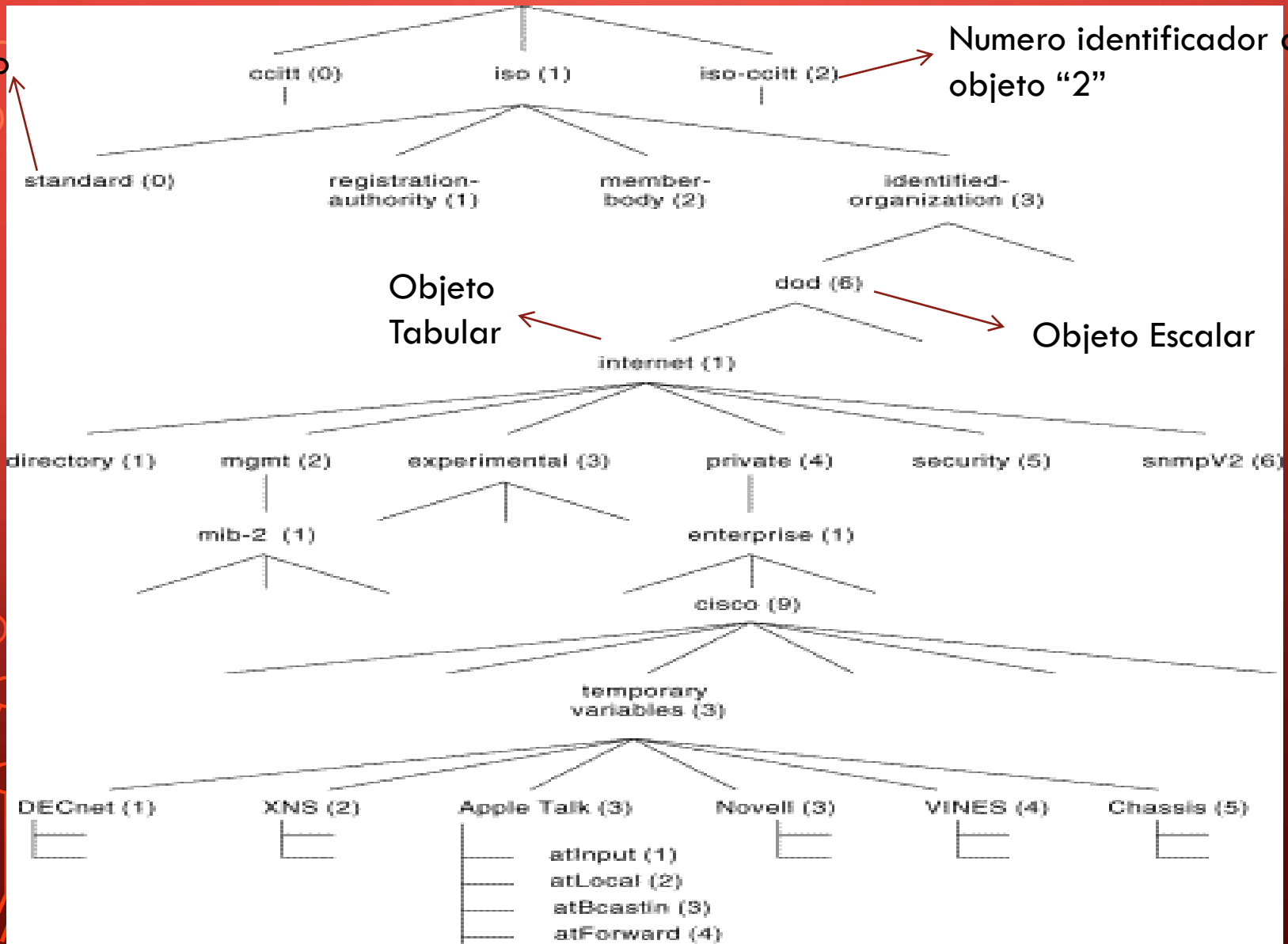
OBJETOS ADMINISTRADOS

- Objeto MIB, objeto, o MIB
- Escalares
- Tabulares
- Identificador de objeto

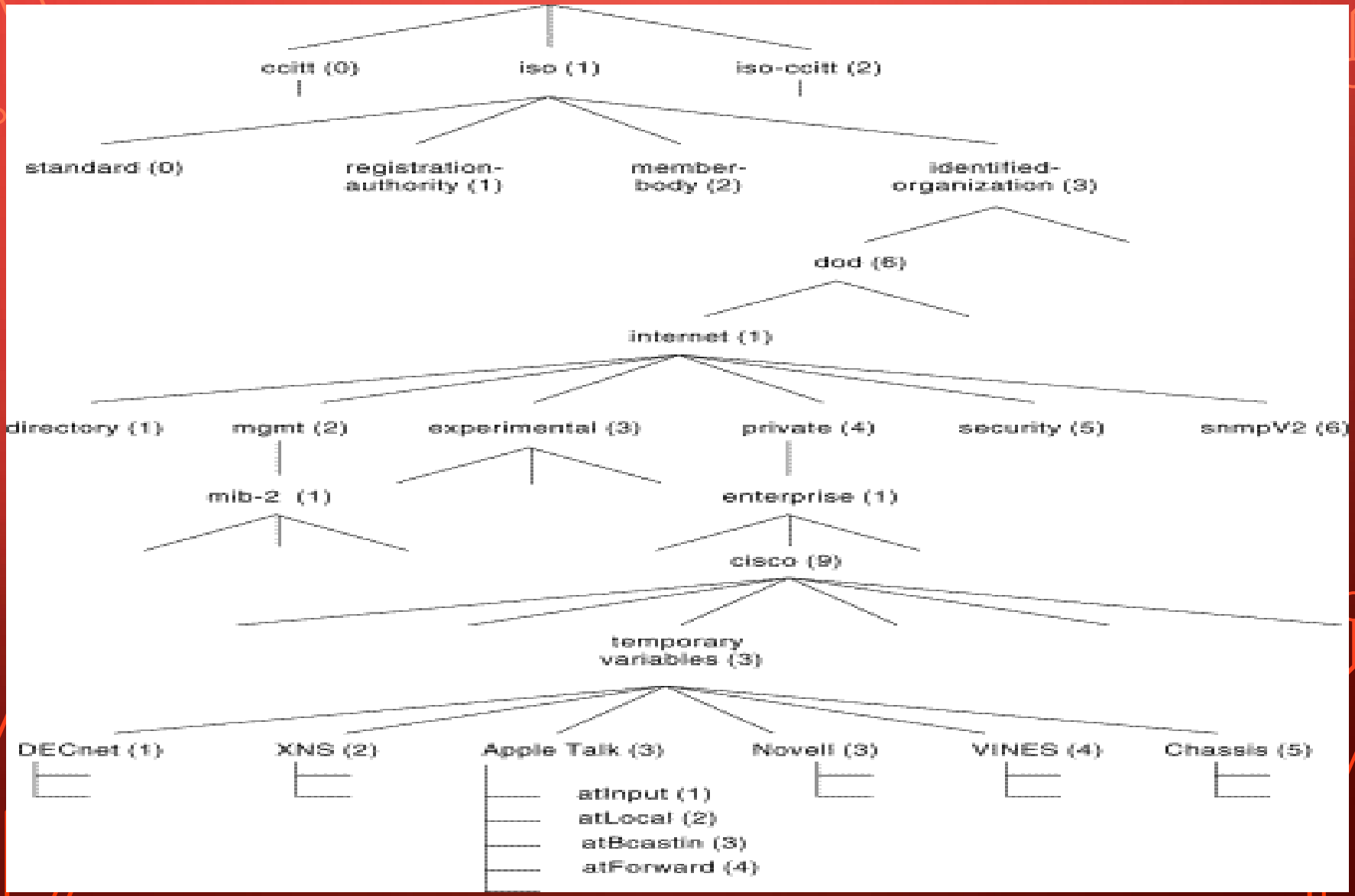
OID´S

- Object Identifiers
- ¿Qué es un OID?
- Por ejemplo 1.3.6.1
- ¿Cómo se organizan los OID´s?

ÁRBOL MIB


Objeto
Numero identificador de objeto "2"
ccitt (0)
iso (1)
iso-ccitt (2)
standard (0)
registration-authority (1)
member-body (2)
identified-organization (3)
Objeto Tabular
dod (6)
Objeto Escalar
internet (1)
directory (1)
mgmt (2)
experimental (3)
private (4)
security (5)
snmpV2 (6)
mib-2 (1)
enterprise (1)
cisco (9)
temporary variables (3)
DECnet (1)
XNS (2)
Apple Talk (3)
Novell (3)
VINES (4)
Chassis (5)
atInput (1)
atLocal (2)
atBcastin (3)
atForward (4)

ÁRBOL MIB


ccitt (0)
iso (1)
iso-ccitt (2)
standard (0)
registration-authority (1)
member-body (2)
identified-organization (3)
dod (6)
internet (1)
directory (1)
mgmt (2)
experimental (3)
private (4)
security (5)
snmpV2 (6)
mib-2 (1)
enterprise (1)
cisco (9)
temporary variables (3)
DECnet (1)
XNS (2)
Apple Talk (3)
Novell (3)
VINES (4)
Chassis (5)
atInput (1)
atLocal (2)
atBcastIn (3)
atForward (4)

EJEMPLOS

- “directory” se encuentra en el nodo 1.3.6.1.1 del árbol.

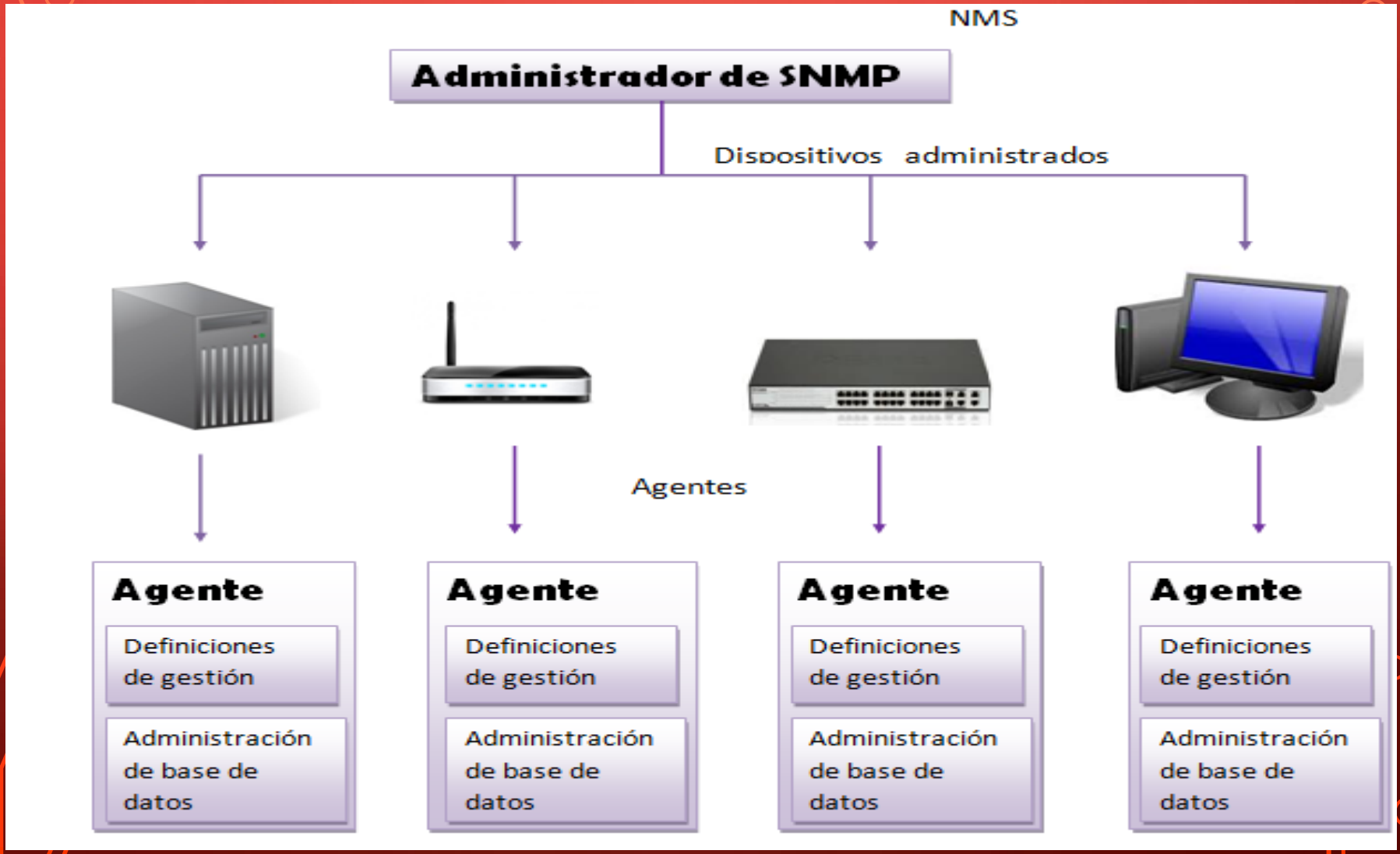
EJEMPLOS

- “directory” se encuentra en el nodo 1.3.6.1.1 del árbol.
- ¿A qué nodo del árbol me estoy refiriendo si tengo este OID? 1.3.6.1.4.1

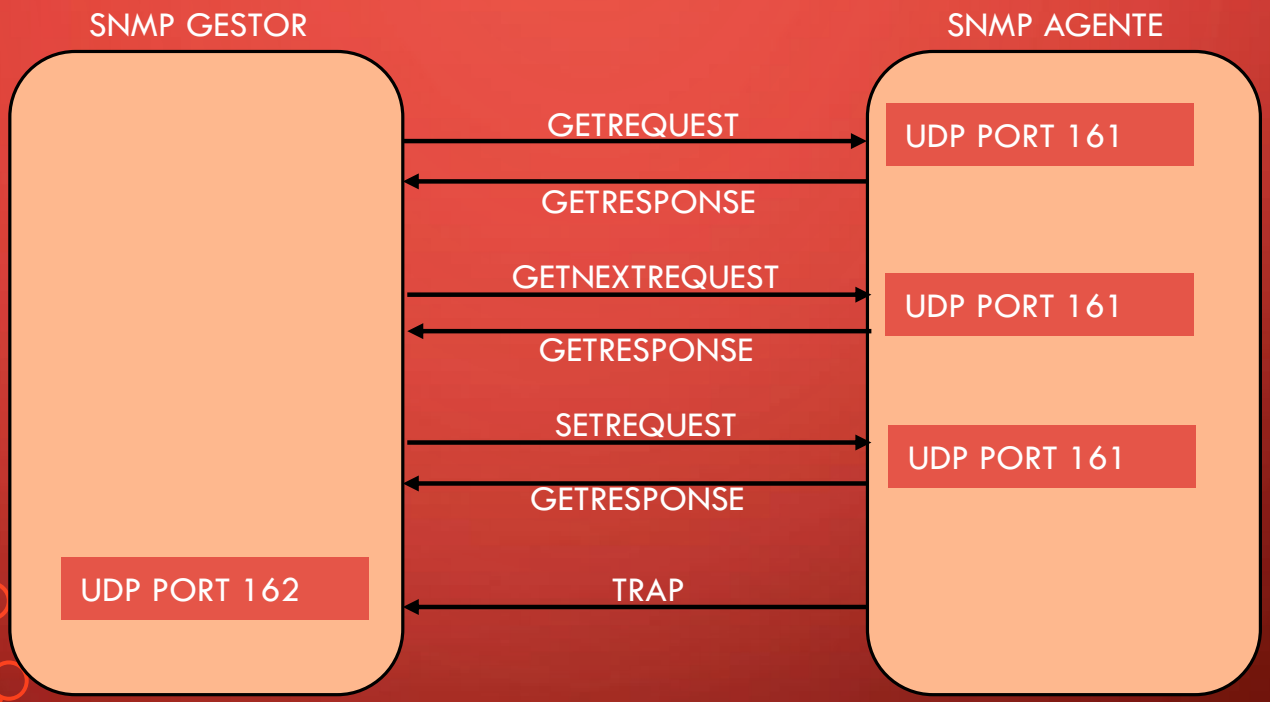
EJEMPLOS

- “directory” se encuentra en el nodo 1.3.6.1.1 del árbol.
- ¿A qué nodo del árbol me estoy refiriendo si tengo este OID? 1.3.6.1.4.1
- ✓ “enterprise”

ESQUEMA DE ADMINISTRACIÓN DE RED

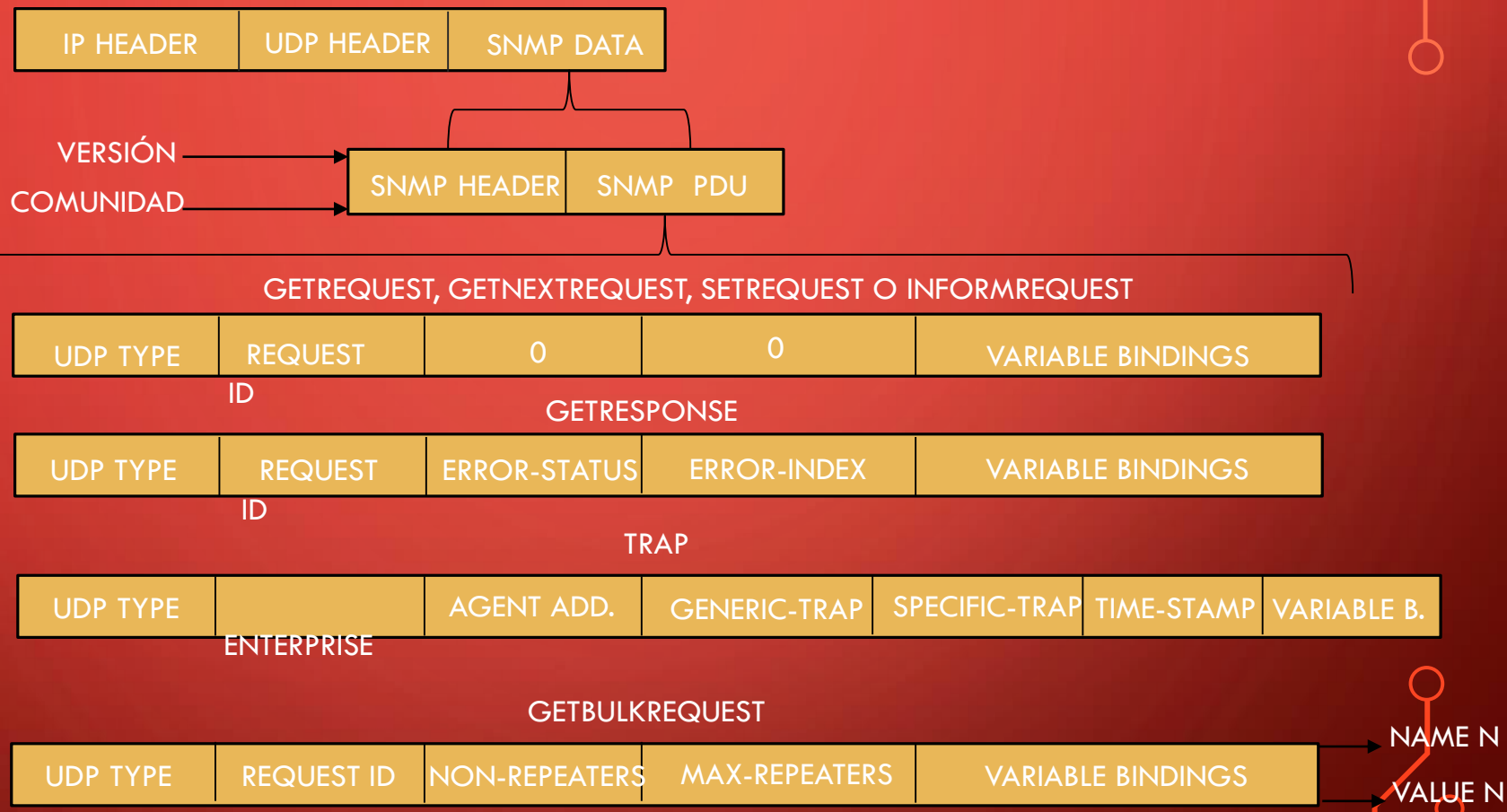


DETALLES DEL PROTOCOLO



DETALLES DEL PROTOCOLO

- **SNMP opera en la capa de aplicación del conjunto de protocolos de Internet. El agente SNMP recibe solicitudes en el puerto UDP 161. El administrador puede enviar solicitudes de cualquier puerto de origen disponible para el puerto 161 en el agente. La respuesta del agente será enviado de vuelta al puerto de origen en el gestor. El administrador recibe notificaciones en el puerto 162. El agente puede generar notificaciones desde cualquier puerto disponible. SNMPv1 especifica cinco centrales unidades de datos de protocolo (PDU). Otros dos PDU, GetBulkRequest e InformRequest se añadieron en SNMPv2 y prorrogados a SNMPv3.**


IP HEADER
UDP HEADER
SNMP DATA
VERSIÓN
COMUNIDAD
SNMP HEADER
SNMP PDU
GETREQUEST, GETNEXTREQUEST, SETREQUEST O INFORMREQUEST
UDP TYPE
REQUEST ID
0
0
VARIABLE BINDINGS
GETRESPONSE
UDP TYPE
REQUEST ID
ERROR-STATUS
ERROR-INDEX
VARIABLE BINDINGS
TRAP
UDP TYPE
ENTERPRISE
AGENT ADD.
GENERIC-TRAP
SPECIFIC-TRAP
TIME-STAMP
VARIABLE B.
GETBULKREQUEST
UDP TYPE
REQUEST ID
NON-REPEATERS
MAX-REPEATERS
VARIABLE BINDINGS
NAME N
VALUE N

-IP header: Contiene la IP del dispositivo al que queremos comunicarnos.
-UDP header: Contiene los puertos de origen y destino.
-SNMP header: Contiene la versión del SNMP (SNMPv1, SNMPv2, SNMPv3) y la comunidad (privada o pública).
-SNMP PDU: Indica el contenido de la PDU, el que depende de la operación que se ejecute, que puede ser algún tipo de request, get o un trap.
-PDU Type:

PDU TYPE VALUE	PDU TYPE
0	GETREQUEST
1	GETNEXREQUEST
2	GETRESPONSE
3	SETREQUEST
5	GETBULKREQUEST
6	INFORMREQUEST
7	TRAP

-Request ID: Usado para distinguir una solicitud con una ID, entre las demás solicitudes.

-Error-Status: Indica que ha habido una excepción mientras se procesaba una solicitud.

STATUS VALUE	ERROR CODE	DESCRIPCIÓN
0	noERROR	No tiene error
1	tooBIG	Demaciado grande
2	noSuchName	No existe esa variable
3	badValue	Valor incorrecto
4	readOnly	Valor de solo lectura
5	genError	Error genérico

-Error Index: Cuando el error-status es diferente de cero puede proporcionar información adicional indicando que variable causa la excepción.

-Variable Bindings: Una lista de nombre de variables con sus correspondientes valores. Normalmente contiene los datos solicitados por una operación get o trap.

-SNMP Trap:

-PDU Type: Trap.

-Enterprise: Identificación del subsistema de gestión que ha emitido el trap.

-Agent Address: Indica la dirección IP del agente que emite el trap.

-Generic Trap:

(0)Cold Start: Indica que el agente ha sido inicializado o reiniciado.

(1)Warm Start: Indica que la configuración del agente ha cambiado.

(2)Link Down: Indica que una interfaz de comunicación se encuentra fuera de servicio (inactiva).

(3)Link Up: Indica que una interfaz de comunicación se encuentra en servicio (activa).

(4)Authentication Failure: Indica que el agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad).

(5)EGP Neighbor Loss: Indica que en sistemas en que los routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio.

(6)Enterprise: En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.

-Specific Trap: Es usado para traps privados, así como para precisar la información de un determinado trap genérico.

-Time Stamp: Indica el tiempo que ha transcurrido entre la re inicialización del agente y la generación del trap.

-Variable Vinculables: Se utiliza para proporcionar información adicional sobre la causa del mensaje.

-GETBULKREQUEST PDU:

-No Repetir: el número de objetos que sólo se espera para devolver una sola instancia, no varias instancias. Los gestores solicitan con frecuencia el valor de sysUpTime y sólo quieren esa instancia, más una lista de otros objetos.

-Máxima Repeticiones: el número de objetos que deben ser devueltos para todos los OID de repetición. El Agente debe truncar la lista para algo más corto si es que no encaja dentro del tamaño máximo de mensaje apoyado por el generador de comandos o el agente.

MENSAJES SNMP

- **Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión.**

TIPOS DE MENSAJES:

-GetRequest: Se envía desde el gestor hacia el agente para recuperar el valor de una variable. En respuesta el agente responde indicando el éxito o el fracaso de la petición.

-GetNextRequest: **Este mensaje es usado para recorrer una tabla de objetos. 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. Siempre el resultado de la operación anterior será utilizado para la nueva consulta. 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. Para realizar esta operación el NMS envía al agente una lista de nombres de objetos con sus correspondientes valores.

-GetResponse: Este mensaje es usado por el Agente para responder un GetRequest, GetNextRequest, o SetRequest. En el campo "Request ID" lleva el mismo identificador que el "request" al que está respondiendo.

-Trap: Un Trap es generado por el Agente para reportar ciertas condiciones y cambios de estado al gestor.

-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 transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados, utilizando el protocolo de nivel 4 TCP, y enviara el InformRequest hasta que tenga un acuse de recibo.

VERSIONES SNMP

- SNMPv1
- SNMPv2
  - SNMPv2c
- SNMPv3

SNMPV1

- Solución temporal
- Mensajes PDU
  - GetRequest
  - GetNextRequest
  - GetResponse
  - SetRequest
  - Traps
- Cadena de Comunidad o SNMP

SNMPV1

- Cadena de Comunidad o SNMP:

  Es básicamente una contraseña que identifica a un usuario como miembro de su comunidad. ¿Por qué comunidad? Porque SNMP identifica a un grupo de elementos de la red, junto con sus sistemas de gestión como una “comunidad”. Cuando un usuario inicia sesión, la cadena de comunidad indica que está autorizado a la red y esto le da acceso total a la red y sus elementos.

SNMPV1

- RFC 1155
- RFC 1156
- RFC 1157

Más adelante RFC 1213

SNMPV1

- RFC 1155: Estructura e identificación de gestión para internet basadas en TCP/IP.
- RFC 1156: Base de Información de Gestión (MIB-1) para la gestión de la red basada en TCP/IP.
- RFC 1557: un protocolo simple de red.

Más adelante RFC 1213 que tiene MIB-2

SNMPV2

- Mejoras en comunicación, rendimiento, seguridad, entre otras.
- Mensajes PDU
  - GetBulkRequest
  - InformRequest
- RFC 1441 – RFC 1452

SNMPV2C

- Seguridad de comunidad
- Sistema de gestión de red bilingüe
- Agentes Proxys
- RFC 1901 – RFC 1908; RFC 2576

SNMPV2C

- Sistema de gestión de red bilingüe:

  Soporta tanto la versión 1 como la versión 2

SNMPV2C

- Sistema de gestión de red bilingüe:

  Soporta tanto la versión 1 como la versión 2

- Una entidad se pone en contacto con una agente.
- El NMS examina la información almacenada en una base de datos local para saber que versión es.
- Cuando el NMS identifica la versión, este se comunica con el agente usando la versión adecuada.

SNMPV2C

- Agentes Proxy
  - Recopila datos de dispositivos que no soportan SNMP
  - Recopila datos de la versión 1

SNMPV2C

- Agentes Proxy
  - Recopila datos de dispositivos que no soportan SNMP

SNMPV2C

- Agentes Proxy
  - Recopila datos de dispositivos que no soportan SNMP

SNMPV2C

➢ Agentes Proxy

- Recopila datos de la versión 1
  - Un NMS de la versión 2 pública un comando destinado a un agente de la versión 1.
  - El NMS envía un mensaje SNMP hacia el agente proxy de la versión 2.
  - El agente proxy reenvía mensajes Get, GetNext y Set sin cambios hacia un agente de la versión 1.
  - Los mensajes GetBulk son convertidos por el agente proxy a mensajes GetNext y luego se envían al agente de la versión 1.
  - El agente proxy mapea los mensajes Traps de la versión 1 hacia los mensajes Traps de la versión 2 y luego se los transmite al NMS.

IMPLICACIONES DE SEGURIDAD

- No hay cifrado
- UDP
- Configuración de gran alcance
- SANS

IMPLICACIONES DE SEGURIDAD

- Las versiones 1 y 2 están sujetas a la detección de paquetes de la cadena de comunidad de texto claro desde el trafico de la red, debido a que no implementan el cifrado.
- SNMP utiliza UDP por lo que es más vulnerable a los ataques de suplantación de IP. Por lo tanto, están sujetas a pasar por las listas de acceso de dispositivos que son implementadas para restringir el acceso a SNMP. Aunque en la versión 3 ya se debe prevenir estos ataques.

IMPLICACIONES DE SEGURIDAD

- La configuración de gran alcance no son usualmente utilizados, en parte a la falta de seguridad de en las versiones anteriores a la versión 3 y también porque muchos dispositivos no son capaces de ser configurados a través de los cambios individuales de objetos MIB.
- SNMP encabeza la lista de problemas comunes de configuración predeterminada del SANS con el tema de las cadenas de comunidades.

SNMPV3

- Integridad del mensaje
- Autenticación
- Confidencialidad

SNMPV3

- Integridad del mensaje: asegura que el mensaje no haya sido violado durante la transmisión
- Autenticación: verifica si el mensaje proviene de una fuente valida
- Confidencialidad: encripta el contenido del paquete para impedir la obtención de una fuente no autorizada

SNMPV3

- Modificación de la información
- Mascaras
- Mensajes corrientes de modificación
- Divulgación

SNMPV3

- Modificación de la información: protección contra entidades no autorizadas que alteran en tránsito los mensajes generados por un principal autorizado.
- Mascaras: protección contra las operaciones de gestión no autorizadas por algún director al asumir la identidad de otra principal que cuenta con las autorizaciones correspondientes.
- Mensajes corrientes de modificación: protección contra mensajes que consiguen maliciosamente reordenado, retrasado o reproducción para efectuar las operaciones de gestión autorizadas.
- Divulgación: protección contra escuchas en los intercambios entre los motores de SNMP.

SNMPV3

- Identificación de las entidades
- Soporte para los modelos de seguridad

SNMPV3

- Identificación de las entidades: cada entidad tiene un identificador llamado snmpEngineID y la comunicación es solo posible si la entidad conoce la entidad de su interlocutor. Los Traps son excepciones a esta regla
- Soporte para los modelos de seguridad: se puede definir la política de seguridad dentro de un dominio administrativo o intranet. Contiene las especificaciones para la USM

SNMPV3

- Comunicación sin autenticación y sin privacidad (noAuthNoPriv)
- La comunicación con la autenticación y sin privacidad (authNoPriv)
- La comunicación con la autenticación y la privacidad (authPriv)
- Definición de diferentes protocolos de autenticación y privacidad

SNMPV3

- Definición de un procedimiento de descubrimiento
- Definición del procedimiento de sincronización de hora
- Definición del marco MIB SNMP
- Definición de las MIB USM
- Definición de las MIB VACM

APLICACIONES

- Descubre automáticamente y mapea hasta 1500 dispositivos con IP habilitado
- Monitorea y reporta el estado de los dispositivos y enlaces claves
- Recomienda optimizaciones
- Mapea conexiones puerto a puerto
- Envía eventos y alarmas vía e-mail, beeper o mensajes SMS

DESCUBRIMIENTO AUTOMATICO

- Es una función de los Sistemas de Monitoreo
- Recolecta datos de los dispositivos

MONITOREO DE RED

- Es una herramienta de los sistemas de Administración de redes, que permite supervisar dispositivos y/o servicios de una red en búsqueda de componentes defectuosos

MONITOREO RED

- TIPOS DE MONITOREO:

  ACTIVO

  PASIVO (SNMP)

MRTG: MULTI ROUTER TRAFFIC GRAPHER

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, y ofrecen una visión en tiempo real del tráfico.

MRTG está escrito en el Perl y C y trabaja bajo UNIX y el NT.

MRTG: MULTI ROUTER TRAFFIC GRAPHER

MRTG es un script en Perl que utiliza SNMP para leer cualquiera de **los parámetros ifInOctets y ifOutOctets** 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: MULTI ROUTER TRAFFIC GRAPHER

- **Scripts**:

  Cfgmaker

  Indexmaker

  Mrtg

MRTG: MULTI ROUTER TRAFFIC GRAPHER

- Ejemplos:
- *C:\mrtg\bin perl cfgmaker public@192.168.0.1 –global "WorkDir: c:\mrtg" –output prueba.cfg*
- *C:\mrtg\bin perl indexmaker –output prueba.html prueba.cfg*
- *C:\mrtg\bin perl mrtg prueba.cfg*

REFERENCIA

- http://enredados2012.blogspot.com.ar/2012/10/tutorial-de-monitoreo-mrtg.html
- http://oss.oetiker.ch/mrtg
- informatica.uv.es/it3guia/ARS/apuntes/snmp.ppt
- http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol