SNMP

Claudia Inostroza
Cinostro@reuna.cl
Albert Astudillo
aastudillo@reuna.cl

Managua 05 y 06 de Diciembre de 2011

Agenda

- Qué es SNMP?
- Componentes
- Comandos
- Versiones
- OIDs
- MIBs
- Snmpwalk

Qué es SNMP?

- SNMP Protocolo Simple de Gestion de Red. Estándar reconocido, se encuentra presente en la mayoría de los equipos de red
- Basado en Encuesta/Respuesta: **GET / SET**
- Jerarquía de Árbol
- Para el monitoreo se utiliza principalmente GET
- Se consulta el estado de ”Identificadores de Objeto” (OIDs) Concepto de MIBs (Base de Informacion de Gestion)
- Existen definiciones estándares y específicas de proveedores.
- Como transporte utiliza UDP con el puerto 161

Componentes de SNMP

- Dispositivos Administrados
  - Elementos de red (switch, bridge, router), servidores.
- Agentes
  - Elementos de software que residentes en los equipos administrados que se encargan de almacenar información.
- Sistemas administradores de red (NMS)
  - Equipos que consultan y administran la información entregada por los agentes.

Comandos SNMP

- GET (entidad gestora -> agente)
  - Encuesta, solicitando un valor
- GET-NEXT (entidad gestora -> agente)
  - Solicitando valor siguiente (recursivo, para listas)
- GET-RESPONSE(agente -> entidad gestora)
  - Respuesta a GET/SET, o error
- SET(entidad gestora -> agente)
  - Setear un valor, or ejecutar accion
- TRAP(agente -> entidad gestora)
  - Notificación espontánea de incidente (falla de línea, temperatura por encima de límite, etc ...)

Versiones

- V1 (1988) RFC1155, RFC1156, RFC1157
- V2 RFC1901 ... RFC1908 + RFC2578. Extiende v1, nuevos tipos de datos, métodos de recuperación de datos mejorados (GETBULK)
- La versión más usada es v2c (carece de método de alta seguridad)
- V3 RFC3411 ... RFC3418 (alta seguridad)
- Típicamente se usa SNMPv2 (v2c)

Version 1

- Utiliza un método muy simple de autenticación, basado en 'comunidades'
- Provee los siguientes tipos de operaciones:
  - GET(petición de un valor)
  - GET-NEXT(petición del valor siguiente en la tabla)
  - GET-RESPONSE (respuesta al get o set)
  - SET-REQUEST(petición de escritura)
  - TRAP (alarma espontánea enviada por el agente)

Version 2

- Contiene una serie de mejoras
- Tipos de datos
  - Counter64
  - Cadenas de bits
  - Direcciones de red (además de IP)
- Operaciones
  - GetBulk
  - Inform
- No es lo suficientemente seguro ya que continua utilizando como esquema de seguridad las comunidades
- La versión mas utilizada es la 2c

- Principalmente, resuelve los problemas de seguridad de versiones anteriores:
  - ¿El mensaje solicitando una operación ha sido alterado? ¿Ha llegado en el momento adecuado?
  - ¿Quién solicitó la operación?
  - ¿A qué objetos se accederá en esta operación?
  - ¿Qué privilegios tiene el solicitante sobre los objetos en cuestión?

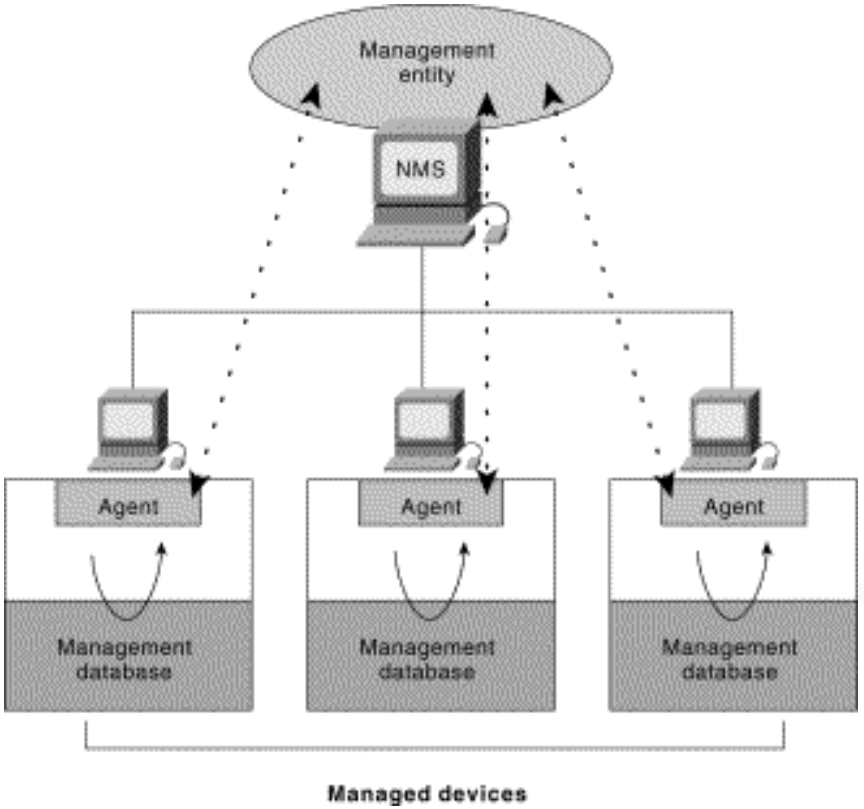
Cómo se comunican?

- El protocolo de gestión provee las reglas de comunicación entre los NMS y los dispositivos administrados.

- Define entre otros:
  - Tipos de mensajes (pregunta y respuesta)
  - Seguridad de acceso, y datos (autenticación, privacidad)

En resumen

- Los agentes localizados en los dispositivos gestionados, son consultados periódicamente por el NMS, utilizando el protocolo de gestión



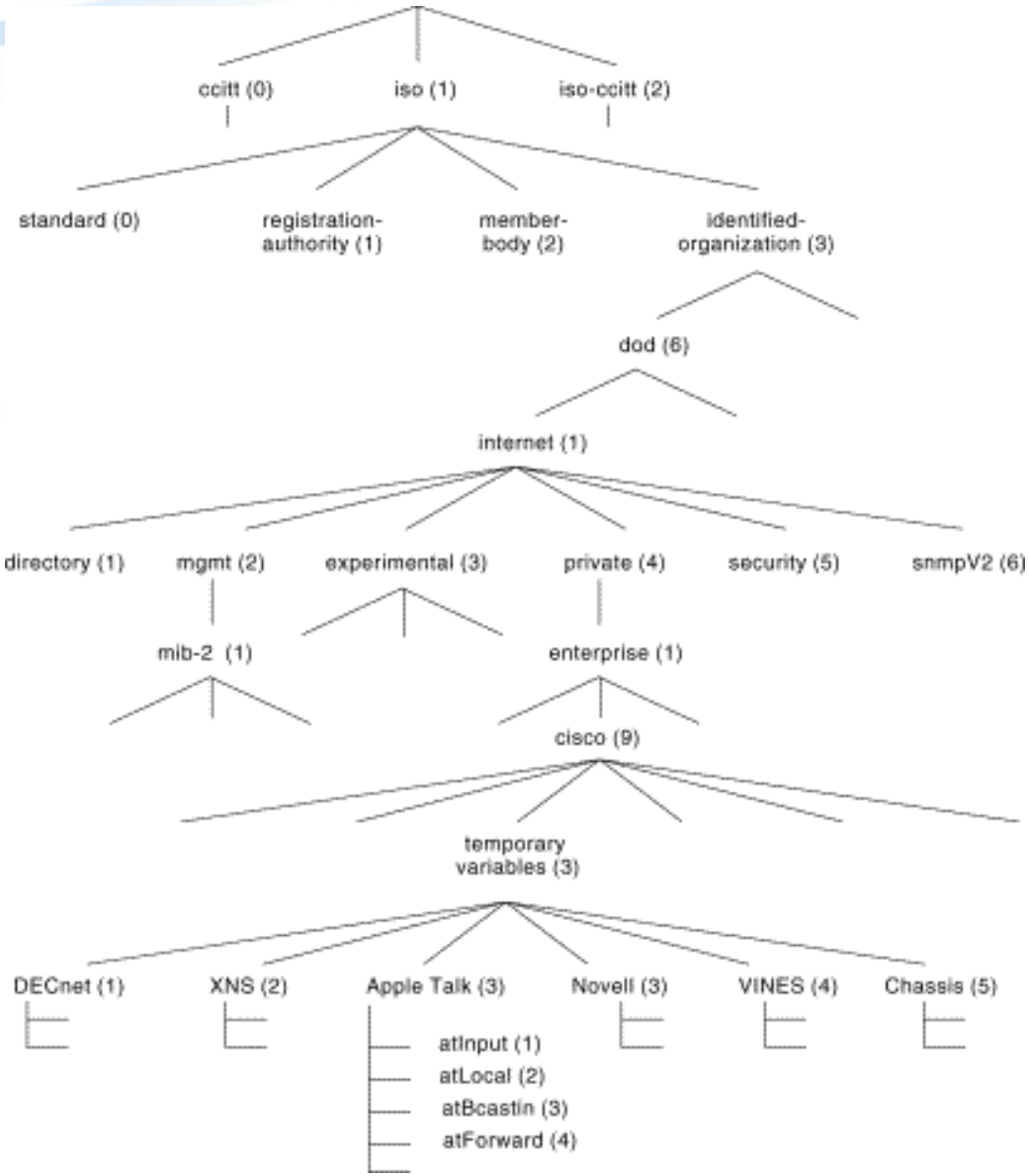
Tipos de datos en respuesta

- Integer: Entero de 32 bits
- Octet String: Cadena de bytes (2^16)
- Counter32: Entero de 32 bits que se incrementa
- Counter64: Entero de 64 bits que se incrementa
- Gauge32: Entero de 32 bits que no se incrementa
- TimeTicks: Tiempo medido en centésimas de segundo desde algún momento determinado

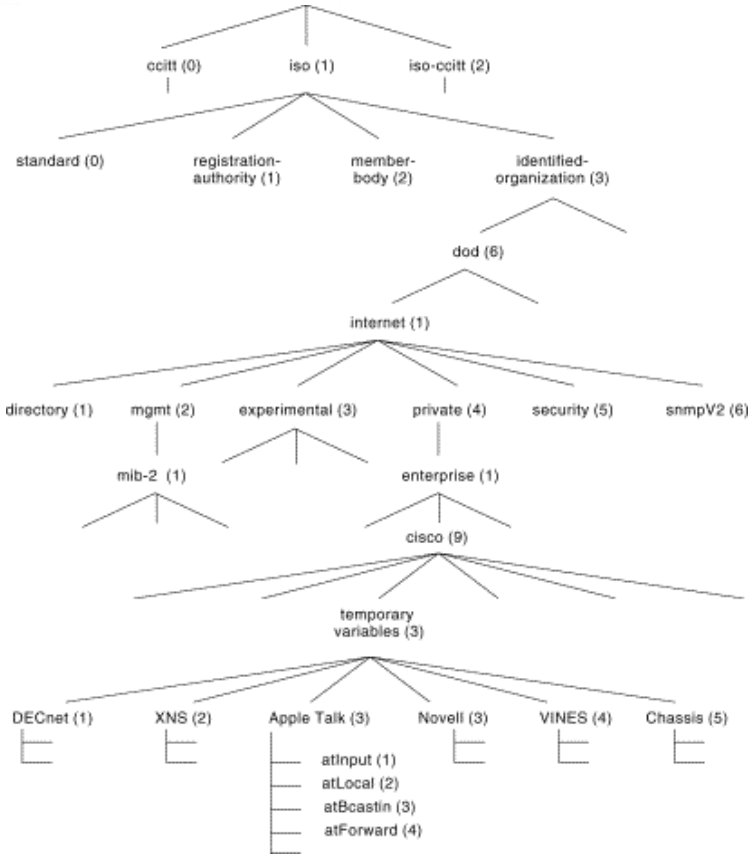
Management Information Base (MIB)

- Agrupación de objetos de gestión en módulos
- Hay cientos de módulos estándar definidos por la IETF
- Existen muchos módulos privados definidos y registrados por fabricantes para la gestión de sus equipos
- Muchas veces, los fabricantes indican información estándar sólo en sus módulos privados, lo cual hace muy difícil la utilización de herramientas comunes para gestionar redes heterogéneas

Àrbol 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)

Árbol Mib



Equivale:
.iso.org.dod.internet.private.enterprise.cisco.temporary.tmpappletalk.atForward
O también: .1.3.6.1.4.1.9.3.3.4

SnmpWalk

- Herramienta utilizada para hacer un barrido de todos los OID's dentro de una MIB.
- Es recomendable, para este fin, utilizar herramientas anexas como SNMPBrowsers, ya que ordenan los valores resultantes.
- Es posible utilizar esta herramienta en servidores Unix mediante el siguiente comando:

- Snmpwalk –c public –v 2c.

Referencias

- RFCs 1157, 1901, 1905, 2570, 2574
- Computer Networking: A Top-Down Approach Featuring the Internet. James F. Kurose.
- Internetworking with TCP/IP, Vol1: Principles, Protocols and Architectures. Douglas Comer.
- The Simple Times www.simple-times.org
- Essential SNMP (O'Reilly Books) Douglas Mauro, Kevin Schmidt


REUNA
Ciencia y
Educación en Red