Gestión y Monitorización de Redes
Introducción a SNMP

Network Startup Resource Center
www.nsrc.org

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Resumen

- Qué es SNMP?
- Sondeo y consulta
- OIDs y MIBs
- Notificationes
- SNMPv3

Qué es SNMP?

SNMP – Simple Network Management Protocol (Protocolo Simple para la Gestión de Redes)

- Protocolo estructurado, información estructurada
- Para consultar el estado de los dispositivos de la red y recibir notificaciones
- También puede ser utilizado para cambiar el estado del dispositivo.
- Estandard definido, muchas herramientas lo utilizan
- Soportado en la mayoria del equipamiento de red
- Transporte : UDP puertos 161 y 162 (notificaciones)

Utilizando SNMP

Consultas frecuentes:

- Bytes In/Out de una interfaz, errors
- Carga del CPU
- Cantidad de tiempo activo (Uptime)
- Temperatura u otros OIDs específicos de algunos fabricantes.

Para los nodos *hosts* (servidores o computadoras)

- Espacio en disco
- Programas instalados
- Procesos en ejecución
- ...

Windows y UNIX tienen agentes SNMP

Versiones de SNMP

v1 (1988) Especificación Original
- Histórica

v2 (1996) Standard fallido
- Seguridad + nuevos tipos de datos + nuevos operadores
- Contadores de 64-bit, get-bulk, notificaciones v2
- Se introduce el modelo de control de acceso basado en vistas (VACM: View based control access model)
- Histórica, no se aplicaron las definiciones actuales

v2c (1996) Estandard *De facto*
- Typos de datos y operadores v2
- Seguridad v1(cadena de texto basada en la *comunidad*) (modelo simple de seguridad)
- Histórica

v3 (1998) Seguridad mejorada
- Seguridad basada en usuarios y vistas (USM/VACM)
- Estandard de internet completo

We will use SNMP v2c and v3 in this class

Roles SNMP

Terminología—Se va a utilizar Gestor (Manager) y Agente (Agent)

Gestor / Manager (La estación de trabajo para monitoreo)

- Algunas veces definida como: el cliente SNMP
- SNMPv3 lo define como: el Generador de Comandos y Receptor de Notificaciones

Agente / Agent (se ejecuta en los dispositivos de red/servidores)

- Algunas veces se define como: Servidor SNMP
- SNMPv3 lo define como: la entidad que responde a los comandos y origina las notificaciones

Cómo funciona SNMP?

Operadores Básicos

- **get** (manager -> agent)
  - Realiza una consulta para obtener un valor
- **getnext** (manager -> agent)
  - Obtiene el siguiente valor (ej. Lista de valores de una tabla)
- **getresponse** (agent -> manager)
  - Respuesta a **get**, **getnext**, o **set**, incluye los errores
- **set** (manager -> agent)
  - Define un valor o ejecuta una acción
- **trap** (agent -> manager)
  - Notificación emitida desde el equipo (linea interrumpida, temperatura por encima de un valor, ...)

Cómo funciona SNMP?

Basado en consulta/respuesta

- El monitoreo generalmente utiliza **get, getnext, getbulk**
- Cambiar el estado utiliza: **set**
- La respuesta siempre es: **getresponse**
- **getbulk** requiere v2c o v3

Las notificaciones son emitidas como **traps** o **informs**

- **traps** son “no reconocidas”
- **informs** son “reconocidas” (v2c, v3)
- Utilice **traps** con formato v2c
- Nadie utiliza **informs**

La base de datos SNMP

La información de un dispositivo está disponible en la MIB (Management Information Base / Base de datos de Información de Gestión)

- SNMP utiliza Object Identifiers (OIDs) / Identificadores de Objetos para organizar la información
- OIDs son claves para identificar cada elemento de datos
- OIDs están organizados en una estructura de árbol que compone la MIB
- Los ficheros MIB documentan partes de la Management Information Base en un dispositivo.

OIDs

OID: Object Identifier / Identificador de Objeto

- Una clave única para seleccionar un elemento de datos específico en el dispositivo
- La misma información siempre se encontrará en el mismo OID. Así de simple!
- Un OID es una cadena de números variables ej.

```
.1.3.6.1.2.1.1.3
```

- Organizada jerárquicamente en un árbol para asegurar que sea único (*similar a DNS*)

Si las direcciones de correo fueran OIDs

user@nsrc.org

sería algo como lo siguiente:

user@nsrc.enterprises.private.internet.dod.org.iso

user@99999.1.4.1.6.3.1

exceptuando que invertimos el orden, poniendo primero iso(1):

.1.3.6.1.4.1.99999.117.115.101.114

Atienda a los valores después de 99999—se deletrea “user” utilizando el código ascii en notación decimal!

No se preocupe respecto a la complicada definición del árbol de OIDs. Lo que interesa es que los OIDs son únicos.

- Asegura que los fabricantes no tienen OIDs repetidos
- El número de OID es lo que se transmite por la red.

OIDs y ficheros MIB

Se lee de izquierda a derecha

Los elementos de OID separados por '.'

```
.1.3.6.1.4.1.9. ...
```

Cada OID esta asocidado es un etiqueta (label)

```
.1.3.6.1.2.1.1.5 => sysName
```

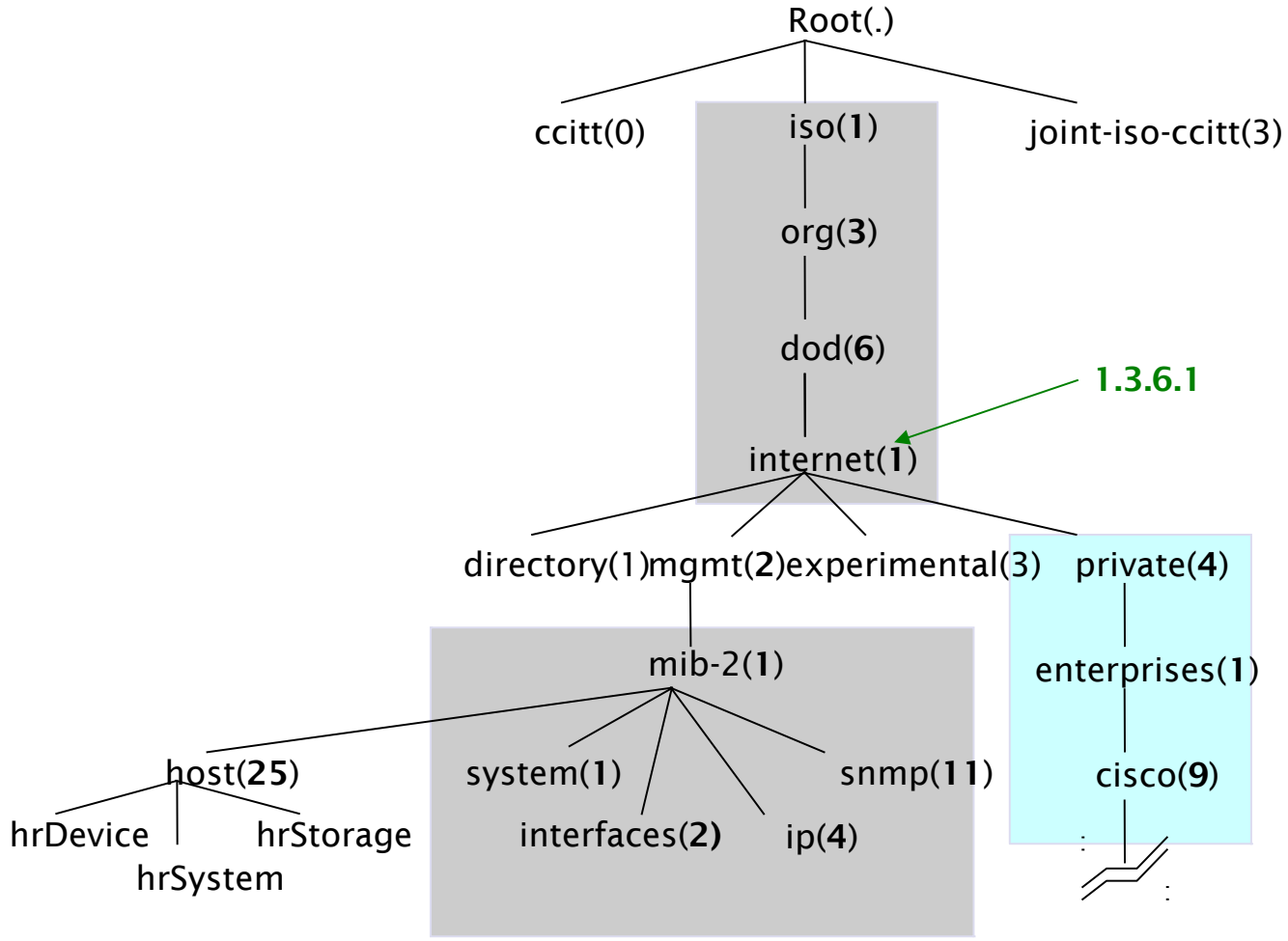
La dirección completa:

```
.iso.org.dod.internet.mgmt.mib-
2.system.sysName
```

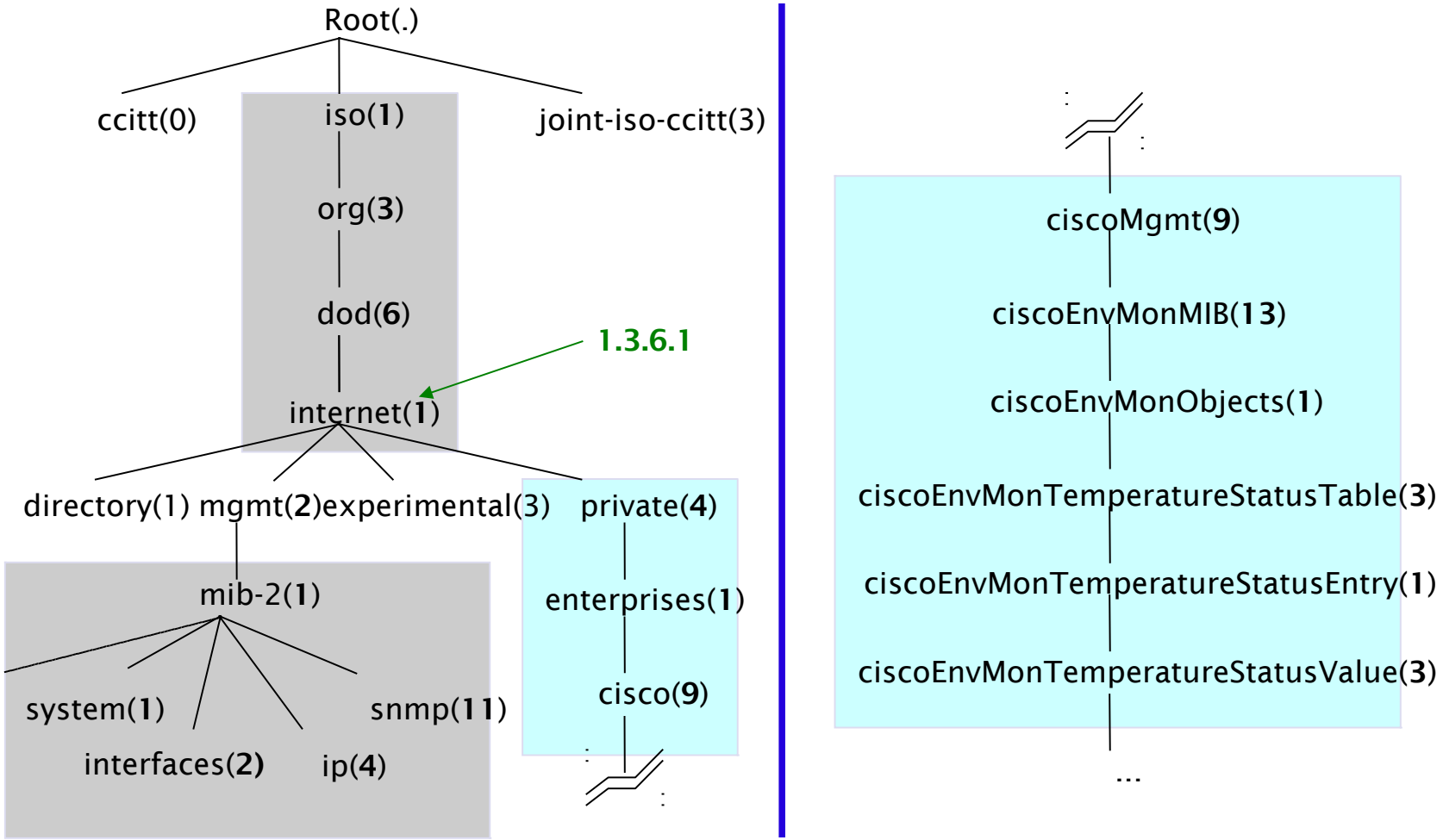
Como convertir de OIDs a etiquetas (y vice versa)?

- Utilizando los ficheros MIB!

El árbol MIB


Root(.)
ccitt(0)
iso(1)
joint-iso-ccitt(3)
org(3)
dod(6)
1.3.6.1
internet(1)
directory(1)
mgmt(2)
experimental(3)
private(4)
mib-2(1)
enterprises(1)
host(25)
system(1)
snmp(11)
cisco(9)
hrDevice
hrStorage
interfaces(2)
ip(4)
hrSystem

El árbol MIB


Root(.)
ccitt(0)
iso(1)
joint-iso-ccitt(3)
org(3)
dod(6)
1.3.6.1
internet(1)
directory(1)
mgmt(2)
experimental(3)
private(4)
mib-2(1)
enterprises(1)
system(1)
snmp(11)
cisco(9)
interfaces(2)
ip(4)
ciscoMgmt(9)
ciscoEnvMonMIB(13)
ciscoEnvMonObjects(1)
ciscoEnvMonTemperatureStatusTable(3)
ciscoEnvMonTemperatureStatusEntry(1)
ciscoEnvMonTemperatureStatusValue(3)
...

Algunas partes del árbol MIB

La MIB Internet, `.1.3.6.1`, tiene solo dos ramas de interés:

- Standard MIBs / MIBs estandar

  `.1.3.6.1.2.1` = `.iso.org.dod.internet.mgmt.mib-2`

- Vendor-specific (proprietary) MIBs / Específicas del fabricante

  `.1.3.6.1.4.1` = `.iso.org.dod.internet.private.enterprises`

La IEEE tiene MIBs de interés en tres partes del árbol:

- IEEE 802 MIBs, incluyendo LLDP

  `.1.0.8802` = `.iso.standard.iso8802`

- IEEE 802.3 MIBs, incluyendo LAG

  `.1.2.840.10006` = `.iso.member-body.us.ieee802dot3`

- IEEE 802.11 MIBs para comunicación inalámbrica / wireless

  `.1.2.840.10036` = `.iso.member-body.us.ieee802dot11`

Ficheros MIB

Los ficheros MIB, definen los objetos que pueden ser consultados, incluyendo:

- Nombre de objeto / Object name
- Descripción de objeto / Object description
- Tipo de datos / Data type (integer, text, list)

Los ficheros MIB están definidos como texto estructurado

- Utilizan un subconjunto de definiciones ASN.1 llamado Structure of Management Information (SMI)

Los ficheros MIB estandar incluyen:

- MIB-II – (RFC1213) – subgrupo de MIBs
- HOST-RESOURCES-MIB (RFC2790)

Ejemplo MIB

```
sysUpTime OBJECT-TYPE
              SYNTAX TimeTicks
              ACCESS read-only
              STATUS mandatory
              DESCRIPTION
                      "The time (in hundredths of a second) since the
                      network management portion of the system was last
                      re-initialized."
              ::= { system 3 }
```

`sysUpTime OBJECT-TYPE`

This defines the object called `sysUpTime`.

`SYNTAX TimeTicks`

This object is of the type `TimeTicks`. Object types are specified in the SMI we mentioned a moment ago.

`ACCESS read-only`

This object can only be read via SNMP (i.e., **get**, **getnext**); it cannot be changed (i.e., **set**).

`STATUS mandatory`

This object must be implemented in any SNMP agent.

`DESCRIPTION`

A description of the object

`::= { system 3 }`

The `sysUpTime` object is the third branch off of the `system` object group tree.

Ficheros MIB

Los ficheros MIB permiten interpretan un valor que se obtiene de un agente (a partir de una consulta)

- Por ejemplo, el estado para el ventilador puede ser:
  - `1, 2, 3, 4, 5, or 6`
  - Qué significa esto?
- Consulte convencion textual (textual convention o (tc)) en el fichero MIB

Muestra de MIB

```
CiscoEnvMonState ::= TEXTUAL-CONVENTION
        STATUS current
        DESCRIPTION
                "Represents the state of a device being monitored.
                 Valid values are:

                 normal(1):          the environment is good, such as low
                                     temperature.

                 warning(2):         the environment is bad, such as
temperature
                                     above normal operation range but not too
                                     high.

                 critical(3):        the environment is very bad, such as
                                     temperature much higher than normal
                                     operation limit.

                 shutdown(4):        the environment is the worst, the system
                                     should be shutdown immediately.

                 notPresent(5):      the environmental monitor is not present,
                                     such as temperature sensors do not exist.

                 notFunctioning(6): the environmental monitor does not
                                     function properly, such as a temperature
                                     sensor generates a abnormal data like
                                     1000 C.
```

Seguridad en SNMP

SNMP version 1 y 2c son inseguros

SNMP version 3 fue creado para solucionar eso

La autenticación SNMPv3 está basada en un usuario

- "User-based Security Model" (USM) / Modelo de Seguridad basado en Usuario
  - Autenticidad e integridad
  - Las claves son utilizadas para que los usuarios y mensajes tengan firmas digitales generadas con funciones hash (MD5 or SHA)
  - Privacidad
  - Los mensajes pueden ser encriptados con algoritmos de llave privada (DES or AES)
  - Validación temporal
  - Utiliza un reloj sincronizado con una ventana de 150 segundos y chequeo de secuencia

Niveles de Seguridad SNMPv3

noAuthNoPriv

- Sin autenticación ni privacidad

authNoPriv

- Autenticación sin privacidad

authPriv

- Autenticación con privacidad

Configuración SNMP en Cisco

Solo lectura / Read-only

```
snmp-server community NetManage RO
```

- Habilita SNMPv1 y v2c

```
snmp-server group ReadGroup v3 auth
snmp-server user admin ReadGroup v3 auth sha NetManage
```

- Autenticación SNMPv3 sin encriptación

Lectura-Escritura / Read-write

```
snmp-server group WriteGroup v3 auth write v1default
snmp-server user admin-rw WriteGroup v3 auth sha NetManage priv aes 128 NetWrite
```

- Cisco permite consultas authNoPriv y authPriv con ese usuario
- Se puede definir tambien un usuario “solo lectura” sin encriptación (priv)
- Preste atención que se recomienda el uso de SNMP version 3 si desea tener acceso de escritura utilizando el operador **set**

Configuración Net-SNMP

Adicione la definicion de “comunidad” editando el fichero `/etc/snmp/snmpd.conf` con la siguiente información:

```
rocommunity NetManage  10.10.0.0/16
```

Adicione el usuario SNMPv3

```
# service snmpd stop
# net-snmp-create-v3-user -a SHA -A NetManage admin
# service snmpd start
```

Edite el fichero de configuración de usuario `~/.snmp/snmp.conf`

```
defVersion 3
defCommunity NetManage
defSecurityName admin
defSecurityLevel authNoPriv
defAuthPassphrase NetManage
defAuthType SHA
```

Consultando un agente SNMP

Utilizando las herramientas del paquete Net-SNMP...

Los comandos de consulta mas utilizados:

- `snmpget`
- `snmpwalk`
- `snmpbulkwalk` (requires v2c or v3)
- `snmpstatus`
- `snmptable`

Sintaxis:

```
snmpXXX -v1 -c<community> host [OID]
snmpXXX -v2c -c<community> host [OID]
snmpXXX -v3 -lauthNoPriv -u<user> -aSHA -A<pass> host [OID}
```

Sin embargo, como se ha configurado el fichero snmp.conf, todo puede ser aun más fácil

```
snmpxxx host [OID]
```

- También, si desea forzar el uso de la version v2c:

```
snmpxxx -v2c host [OID]
```

Consultando un agente SNMP

Algunos ejemplos:

```
snmpstatus 10.10.0.254
snmpget 10.10.0.254 ifNumber.0
snmpwalk -v2c 10.10.0.254 ifDescr
```

Consultando un agente SNMP

Comunidad / Community:

- Una cadena de texto de ”seguridad” (contraseña) para definir si el gestor que realiza la consulta tendrá permisos de RO (solo-lectura / read-only) o RW (lectura-escritura / read-write)
- Esta es la forma más simple de autenticación SNMP

OID

- Un valor, por ejemplo, `.1.3.6.1.2.1.1.5.0`
- O su nombre / etiqueta equivalente: `sysName.0`

Preguntemos por el nombre del sistema (utilizando la OID anterior)

- Por qué escribir el `.0`? Qué ha notado?

Consultas utilizando snmp.conf

Dos consultas:

```
# snmpwalk 10.10.0.252 sysUpTime
DISMAN-EVENT-MIB::sysUpTimeInstance =
Timeticks: (1946738) 5:24:27.38
# snmpwalk -v2c 3 10.10.0.252 sysUpTime
DISMAN-EVENT-MIB::sysUpTimeInstance =
Timeticks: (1953429) 5:25:34.29
```

La primera utilizando SNMPv3 como estaba definido en snmp.conf, la segunda especificando SNMPv2c y utilizando la cadena de seguridad de snmp.conf.

Consulta fallida...Por qué?

Dos respuestas:

```
# snmpget -v1 10.10.0.252 ifHCInOctets.1
Error in packet
Reason: (noSuchName) There is no such variable name in this MIB.
Failed object: IF-MIB::ifHCInOctets.1

# snmpget 10.10.0.252 ifHCInOctets.1
IF-MIB::ifHCInOctets.1 = Counter64: 475028252
```

Por qué? Atienda al tipo de dato: Counter64. Los contadores de 64-bit son solo soportados en SNMPv2c y v3.

Los contadores de 64-bit son importantes, porque en las interfaces Gigabit los contadores de 32-bit (ifInOctets) pueden resetearse (llegar a conteo maximo y regresar a 0) en 34 segundos.

Cuan rápido se puede resetear un contador 32-bit en 10G?

Falla SNMP: sin respuesta?

El dispositivo puede estar apagado o desconectado

El dispositivo puede no tener el agente SNMP en ejecución

El dispositivo puede estar configurado con una palabra de seguridad diferente

El dispositivo puede estar configurado para no aceptar consultas SNMP desde la dirección IP del gestor que está utilizando

En todos estos casos, no se obtendrá respuesta

Buenas prácticas SNMP

- Proteja el tráfico y acceso SNMP:
  - VLAN de Gestión de la Red
  - Listas de Acceso
  - Utilice SNMPv3 con autenticación para consultas y cambios de configuración (**set**) cuando sea posible
- Utilice notificaciones (traps) SNMPv2c
  - Mejor estructuradas que las notificaciones v1
  - Tiempos mas precisos
- No provoque sobrecarga innecesariamente
  - Solo consulte los agente tan rápido como lo necesite
  - Es posible que se incremente la carga del CPU debido a las consultas en algunos dispositivos y se afecten otros procesos
  - No tiene sentido consultar cada 5 segundos si el dispotivos actualiza el constador cada 10 segundos

A continuación en las prácticas...

- Utilizar `snmpwalk`, `snmpget`
- Fichero de configuración: `/etc/snmp/snmp.conf`

- Ejecturar el agente SNMP en Linux (daemon)
- Fichero de configuración: `/etc/snmp/snmpd.conf`

- Cargar las MIBs

Referencias

Essential SNMP (O'Reilly Books) Douglas Mauro, Kevin Schmidt

- http://www.amazon.com/Essential-Second-Edition-Douglas-Mauro/dp/0596008406

Wikipedia

- http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

MIB/OID Browser

- http://oid-info.com/

Cisco SNMP on IOS, MIB tools, and MIB/OID browser

- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/command/nm-snmp-cr-book.html
- http://tools.cisco.com/ITDIT/MIBS/servlet/index
- http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&substep=2&translate=Translate&tree=NO

Open Source Java MIB Browser

- http://www.dwipal.com/mibbrowser.htm

SNMP Link – collection of SNMP resources

- http://www.snmplink.org/

Net-SNMP Open Source SNMP tools

- http://net-snmp.sourceforge.net/

Integration with Nagios

- https://web.archive.org/web/20100614010336/http://www.cisl.ucar.edu/nets/tools/nagios/SNMP-traps.html

Versiones SNMP

v1 Especificacion original

RFCs 1155,1157,1213

v2 Seguridad+nuevos tipos de datos +nuevos operadores

RFCs 901,1909-1910,2011,2576,2578-2580,3416-3418

v2c Estandar de facto

Documented in RFC 3584

v3 Seguridad robusta: USM/VACM

RFCs 3411-3415,3417-3418,3826,5343,5345,5590

RFC 3584 especifica coexistencia entre versiones