Práctica con Net-SNMP

Carlos Armas
Roundtrip Networks

Hervey Allen
NSRC

Preparado con materiales de:

Carlos Vicente
Servicios de Red/Universidad de Oregon

Contenido

- Utilizar el paquete *Net-SNMP* para obtener el valor de algunas variables comunes en dispositivos como enrutadores, switches, etc.
  - Configuración del agente SNMP en un servidor Unix/Linux
  - Instalación de MIBs populares
  - Comandos
    - snmpget,
    - snmpset,
    - snmpwalk,
    - snmptable,
    - snmpbulkwalk
  - Algunos scripts simples y útiles utilizando net-snmp
- Utilización de un Navegador de MIBs (*mbrowse*)

Instalación

- Preferiblemente utilizar los paquetes incluídos en su distribución:

 # apt-get install snmp (Ubuntu)
 # apt-get install snmpd (Ubuntu)

 # yum install net-snmp (Fedora)

snmp - SNMP (Simple Network Management Protocol) applications
snmpd - SNMP (Simple Network Management Protocol) agents

Instalación

- Si no, también es posible compilar el código fuente:
  - Disponible en: http://net-snmp.sourceforge.net

```
# tar xvzf net-snmp-5.4.2.1.tar.gz
# cd net-snmp-5.4.2.1/
# make
# make install
```

Instalación de MIBs

- Varios de los mayores fabricants (Cisco, HP, etc.) distribuyen sus MIBs privadas, junto con las MIBs estándar.
- Si se mezclan estas distribuciones, se termina con MIBs repetidas y a veces incompatibles, lo cual causa muchos errores al cargar
- Sería necesario editar manualmente cada vez :-(

Netdisco MIBs

- Una opción es utilizar la distribución de MIBs de Netdisco (sólo las MIBs, no el software)
- Contiene MIBs estándar, y algunas de las más relevantes para
  - Cisco
  - Extreme
  - HP
  - Net-SNMP
  - Nortel
- Incluye scripts para facilitar la inclusión de MIBs de otros fabricantes

Instalación de MIBs

- En www.netdisco.org sección 'Download'
  - Descargar y desempacar
  - 'netdisco-mibs-0.7.tar.gz' en
    `/usr/local/netdisco/mibs`
  - Copiar la configuración para Net-SNMP
    - **cp mibs/snmp.conf /etc/snmp/**
  - En situaciones de la vida real, es preferible editar este archivo para eliminar los fabricantes que no le interesen (opcional)

Configuración MIBs (opcional)

- **`vi /etc/snmp/snmp.conf`**
- Buscar la línea 'mibdirs'
  - Cada categoría tiene un directorio
  - Eliminar de la lista los directorios que no necesite
  - Esto agiliza la carga de las mibs cada vez que se ejecute uno de los utilitarios

Configuración del Agente (snmpd)

- MUY útil
  - Permite extraer estadísticas de prácticamente todo:
    - Tráfico, Carga del CPU, Memoria, etc.
    - Permite agregar variables propias bajo la MIB de net-snmp, con valores extraídos de scripts escritos por usted
      - Esto es muy flexible
  - Genera *traps* para los eventos más comunes:
    - Carga sobrepasa umbral, etc
    - Se 'muere' un proceso
  - Tiene la gran ventaja de ser estándar, por lo que podemos utilizar cualquier herramienta gestora que soporte SNMP
- Se configura editando el archivo
  - **/etc/snmp/snmpd.conf**

Configuración del Agente

```
syslocation ColNodo Data Center
syscontact  info@colnodo.apc.org

rocommunity  public 192.168.0.0/20

trapcommunity  public

trap2sink  192.168.1.10 public

proc  mysqld
proc  apache2
proc  sendmail
proc  sshd

disk  / 10%

load 15 10 10

agentSecName internal
rouser internal

# Nota: Sólo funciona si está compilado con DISMAN-EVENT-MIB
defaultMonitors yes
```

Configuración del Agente

- Iniciar el programa residente (daemon)

```
# /etc/init.d/snmpd start
```

- Asegurarse de que esté activo

```
# ps -fe |grep snmpd
# snmpwalk -v 2c -c public localhost
```

Herramientas de encuesta en linea de comandos: Parámetros comunes

- **#man snmpcmd**
  - -c Nombre de la comunidad
  - -v Versión (1, 2c, 3)
  - -m Lista de módulos MIB a incluir
  - -M Lista de directorios con módulos MIB a incluir
  - -r Número de intentos (retries)
  - -t Tiempo de espera
  - -O Opciones de salida
    - -On : Imprimir en forma numérica (no traducir nombres de variables)

snmptranslate

- Permite traducir un OID a un nombre:

```
# snmptranslate .1.3.6.1.2.1.2.2.1.2
IF-MIB::ifDescr
```

- Opciones interesantes: -Td, -Tp

snmpget

- Usar cuando se sabe exactamente el nombre o el OID de la variable
  - ¿Cuánto tiempo ha estado encendido el equipo?

```
#snmpget -v 2c -c public <dirección ip> System.sysUpTime.0
```

snmpwalk

- Cuando se quiere ver un grupo de variables
  - Mirar las descripciones de las interfaces:

```
#snmpwalk -v 2c -c public <dirección ip> ifDescr
```

  - Mirar los contadores de entrada y salida (en octetos)

```
#snmpwalk -v 2c -c public <dirección ip> ifInOctets
#snmpwalk -v 2c -c public <dirección ip> ifOutOctets
```

snmpwalk

- Cuando no sabemos el nombre exacto de la variable
  - Guardar la salida de la MIB-II completa en un archivo de texto

```
snmpwalk -v 2c -c public <dirección ip> > snmp.txt
```

snmpbulkwalk

- Igual que *snmpwalk*, pero utiliza la operación *get-bulk* de SNMP
  - Solicitar la tabla de ARP:

```
#snmpbulkwalk -c public -v2c <direccion-ip> atPhysAddress
```

snmptable

- Cuando se sabe que un grupo de variables tienen estructura de tabla
  - La tabla de direcciones IP

```
#snmptable -v2c -c public <dirección ip> -Ov ipAddrTable
```

snmpset

- Requiere una *comunidad* con permisos de escritura
  - Muy inseguro en SNMPv1 y SNMPv2!

```
snmpset -c private -v 1 switch1 system.sysContact.0 snoc@igc.org
```

Algunos scripts útiles

Carlos Vicente ha puesto a disposición pública algunos utilitarios:

http://ns.uoregon.edu/~cvicente/download

switchportstats

- Provee una tabla ASCII con los valores de las variables más relevantes por interfaz

```
# switchportstats sw1
Port Admin  Oper   Mbs     InUpkts   InNUpkts   InErrors    OutUpkts   OutNUpkts
  1    up    up   100    31865539   36044466          0    23569440      224780
  2    up    up   100       17742       9168          0      174581     1364722
  3    up    up   100    22225470      46703          0    10525934    17436432
  4    up  down    10      196348      28687          0      651716     3728124
  5    up  down    10          78         25          0       15436         758
  6    up  down    10           0          0          0           0           0
  7    up  down    10        6580         19          0        6596        2059
  8    up  down    10     1029510       6285         13     2078635     1091331
 92    up  down     0           0          0          0           0           0
 93    up    up     0    55341274   36135353         13    37022345    23848206
 94    up  down     0           0          0          0           0           0
```

tablediff

Usage:

#tablediff [-i|--interval <seconds>] [-n|--nodiff] [-h|--help] [-e|--exclude <col1,col2,...>] <program>

Takes a table from another program's output and displays values repeatedly every given seconds. Optionally, shows increments instead of absolute values (default).

1) Program's output must be in table form
2) -n causes the actual values to be displayed, instead of deltas
3) -e excludes columns from delta calculations. Column list must be comma-separated.

Example:
tablediff -i 5 -e 1,2,3,4 switchportstats switch1

macsuck

- Extrae la tabla de MAC-a-puerto (forwarding table) de un switch

```
# macsuck test-switch
00602E011AD6    193     Trk1
00096E0852DE    125     F5
00304883A95F    74      D2
00304827FFBB    76      D4
00E08156DD59    74      D2
0019B9C9ABD3    170     H2
001111EAAEAA    74      D2
000E0C5A6235    77      D5
0004239E342C    173     H5
0007EB2F75C7    43      B19
0002B39A0684    74      D2
00AA00308E36    18      A18
001D09045026    74      D2
0018F362C681    77      D5
0015172D6836    23      A23
001372334064    74      D2
000A9C513A8F    5       A5
003048273F96    41      B17
```

arpsuck

- Extraer la tabla de ARP

```
# arpsuck test-switch
10.82.50.2       00D00195E001    2264    A
10.82.50.3       00D00195DC02    2264    A
10.82.50.5       0010DCCC6D05    2264    A
10.82.50.20      0001E7C93A03    4300    loopback interface
192.168.60.1     00005E000102    264     B
192.168.60.2     00D00195E006    264     C
192.168.60.3     00D00195DC07    264     C
192.168.60.19    00A069001349    264     D
192.168.60.21    00304827FFBB    264     E
192.168.60.51    0010DC74CCA2    264     F
192.168.60.72    000785804234    264     G
192.168.60.84    0019D16A5F66    264     H
192.168.60.91    00188B48D293    264     I
192.168.60.177   00A0C9F1A968    264     J
```

Navegadores de MIBs

- Difícil localizar variables
  - En qué parte de la jerarquía se debe buscar?
  - Difícil de interpretar resultados de *snmpwalk*

- Per tenemos navegadores de MIBs!
  - Interfaz gráfico
  - Presentación jerárquica
  - Descripciones de las variables y los módulos
  - Interfaz de búsquedas

Mbrowse

- Es un navegador MIB que utiliza Net-SNMP
- Es código abierto (open source)
- Disponible en
  - http://www.kill-9.org/mbrowse/

- Tiene bookmarks! ☺

Net-SNMP GUI package

- Es un navegador MIB que utiliza Net-SNMP
- Es código abierto (open source)
- Instalación en Fedora:

  #yum install net-snmp-gui

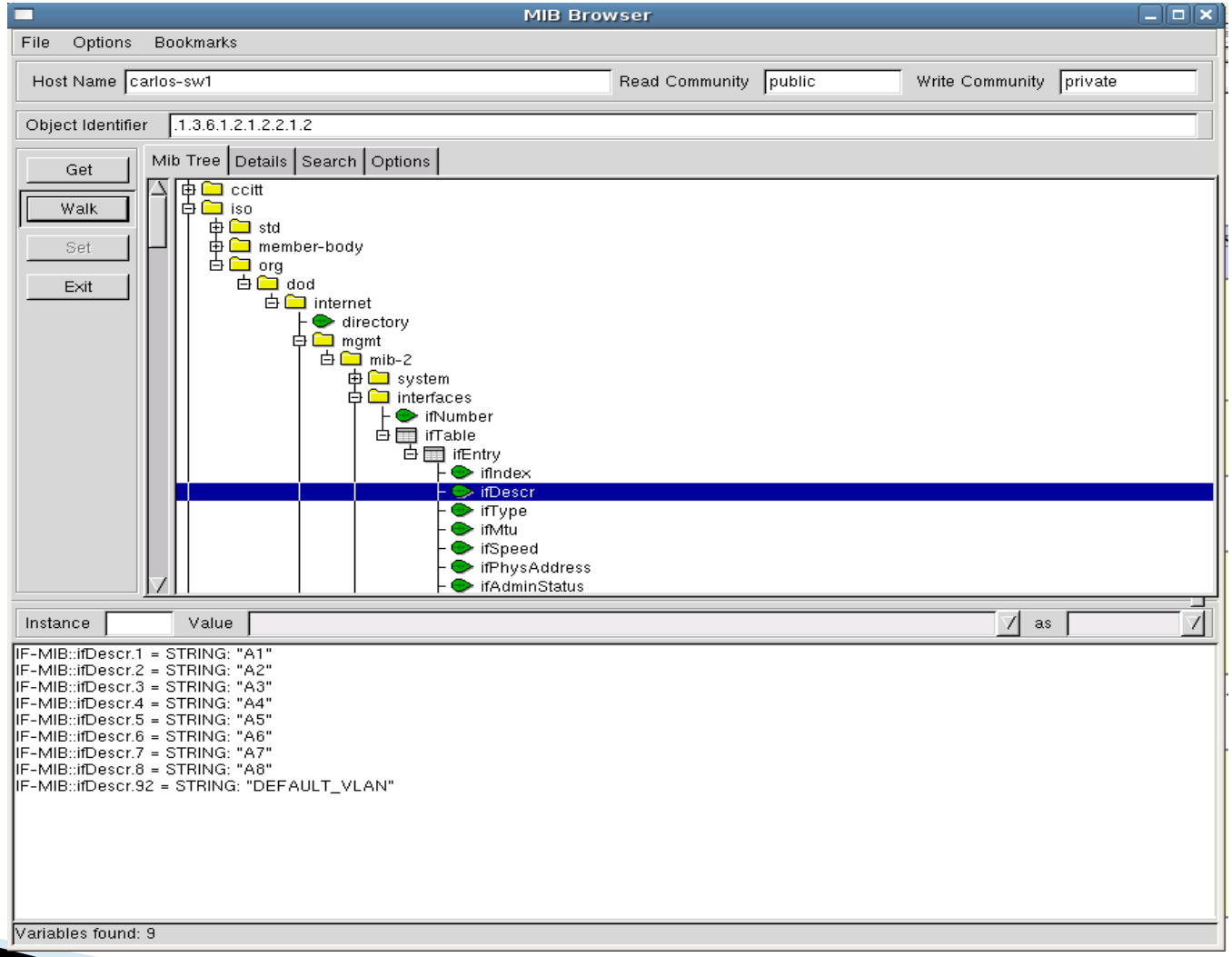
  #tk-mib

Mbrowse: Instalación

- En Ubuntu:
  - apt-get install mbrowse
- También puede compilarse directamente del código fuente:

```
# wget http://www.kill-9.org/mbrowse/mbrowse-0.3.1.tar.gz
# tar xzvf mbrose-0.3.1.tar.gz
# cd mbrowse-0.3.1/
# ./configure
# make
# make install
```

Mbrowse


MIB Browser
File
Options
Bookmarks
Host Name
carlos-sw1
Read Community
public
Write Community
private
Object Identifier
.1.3.6.1.2.1.2.2.1.2
Get
Walk
Set
Exit
Mib Tree
Details
Search
Options
ccitt
iso
std
member-body
org
dod
internet
directory
mgmt
mib-2
system
interfaces
ifNumber
ifTable
ifEntry
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
ifAdminStatus
Instance
Value
as
IF-MIB::ifDescr.1 = STRING: "A1"
IF-MIB::ifDescr.2 = STRING: "A2"
IF-MIB::ifDescr.3 = STRING: "A3"
IF-MIB::ifDescr.4 = STRING: "A4"
IF-MIB::ifDescr.5 = STRING: "A5"
IF-MIB::ifDescr.6 = STRING: "A6"
IF-MIB::ifDescr.7 = STRING: "A7"
IF-MIB::ifDescr.8 = STRING: "A8"
IF-MIB::ifDescr.92 = STRING: "DEFAULT_VLAN"
Variables found: 9

Ejercicios

- Utilizando las herramientas vistas en clase:
  - Encontrar y visualizar las descripciones de las interfaces de enrutadores del laboratorio
  - Determinar la utilización (en bytes) de las unidades de almacenamiento locales en los servidores
  - Cuánto tiempo han estado funcionando los siguientes equipos?
    - SW1, Firewall, SW2, R1, R2, R3?
  - Ver diagrama de topología de la red!