
## Gestión de Redes

# Introducción a SNMP

# Contenido

- Que es SNMP?
- Solicitudes y Consultas
- OIDs y MIBs
- Traps
- SNMPv3 (Opcional)

# Qué es SNMP?

SNMP – Protocolo Simple de Gestión de Red

- Estandar reconocido, muchas herramientas disponibles
- Presente en cualquier dispositivo de red (decente)

Basado en Solicitud/Respuesta: **GET / SET**

- GET se usa para monitoreo
- ”Identificadores de Objeto” (OIDs)
- El clave para identificar cada dato en las respuestas

Concepto de MIBs (Base de Informacion de Gestion)

- Se define una coleccion de OIDs

# Qué es SNMP?

Encuestas tipicas

- Bytes Adentro/Fuera (I/O) por un interfaz, errores
- Carga de CPU
- Tiempo arriba (Uptime)
- Temperatura o otros OIDs especificos a vendidores

Por clientes (servidores o desktops)

- Espacio del disco duro
- Software instalado
- Procesos corriendo
- ...

Windows y UNIX tienen agentes de SNMP

# Qué es SNMP?

- UDP protocolo UDP, puerto 161
- Diferentes versiones
  - v1 (1988) – RFC1155, RFC1156, RFC1157
    - Especificación original
  - v2 – RFC1901 ... RFC1908 + RFC2578
    - Nuevos tipos de datos, métodos de recopilación 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), y a veces v3

# Roles de SNMP

La *entidad gestora*

Recopila y presenta la información de dispositivos y servidores

El *dispositivo gestionado*

- Contiene un agente de gestión que responde a las encuestas de la entidad gestora
- Qué tipo de información?
  - ✓ Los objetos gestionados pueden ser muy variados:
    Carga del CPU, estado de una interfaz de red, espacio en disco duro, entre muchas otras…

# Como Funciona?

## Comandos Basicos

**GET** ←→ **entidad gestora -> agente**

Solicitud de valor de variable únice

**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**

Configurar un valor, o ejecutar acción

**TRAP** ←→ **agente -> entidad gestora**

Notificación espontánea de incidente (falla de línea, temperatura por encima de límite, etc ...)

# OIDs and MIBs

## OID: Identificadores de Objeto

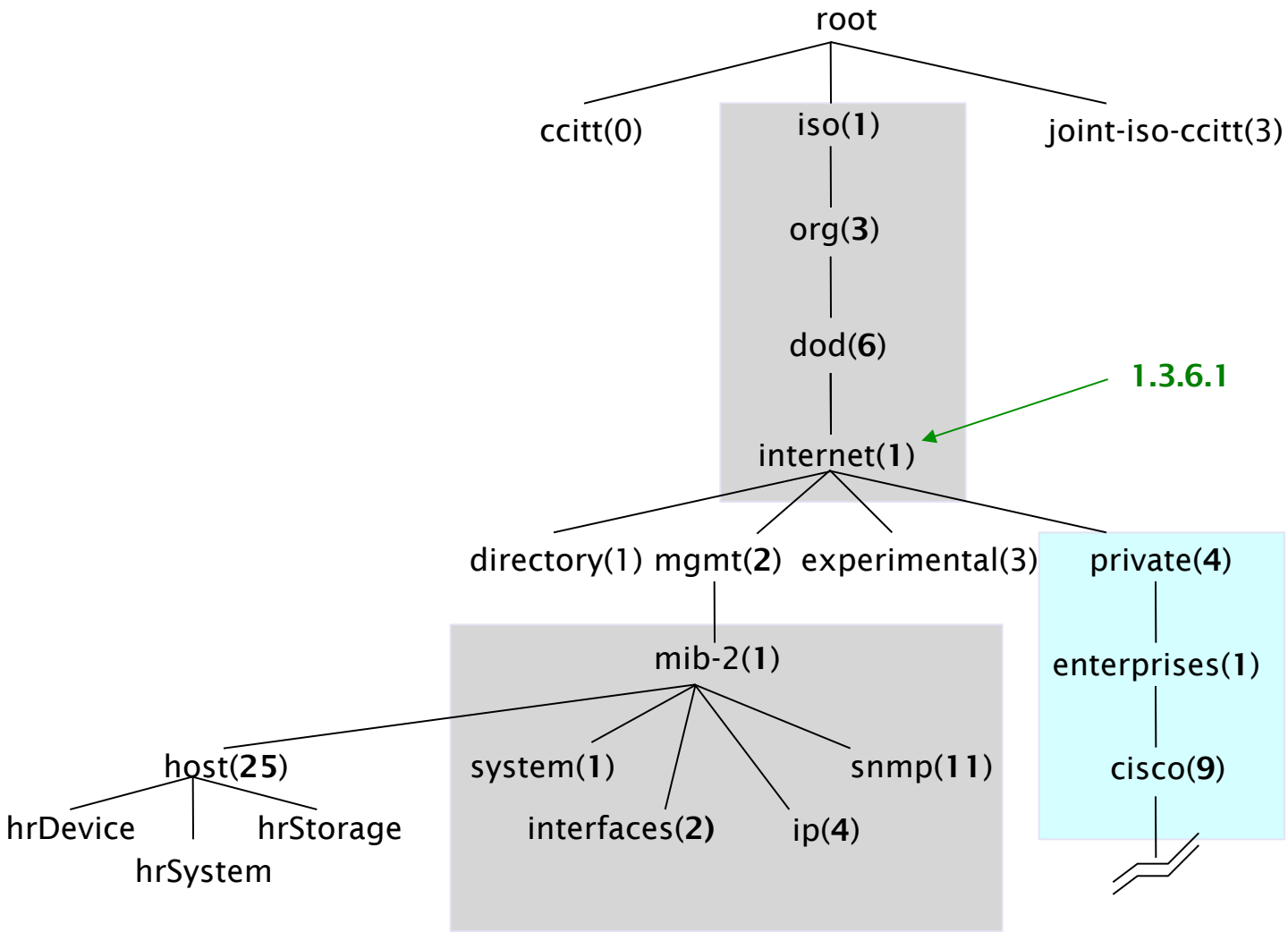
- Una llave unica para seleccionar un objeto particular en el dispositivo
- La misma informacion siempre se encuentra en el mismo OID. Esto es simple!
- Un OID es una cadena de tamaño variable de numeros, ej. 1.3.6.1.2.1.1.3
- Proporcianados en forma jerárquica en un arbol para asegurar que sean unicos (similar a DNS)

## MIB: Base de Información de Gestión

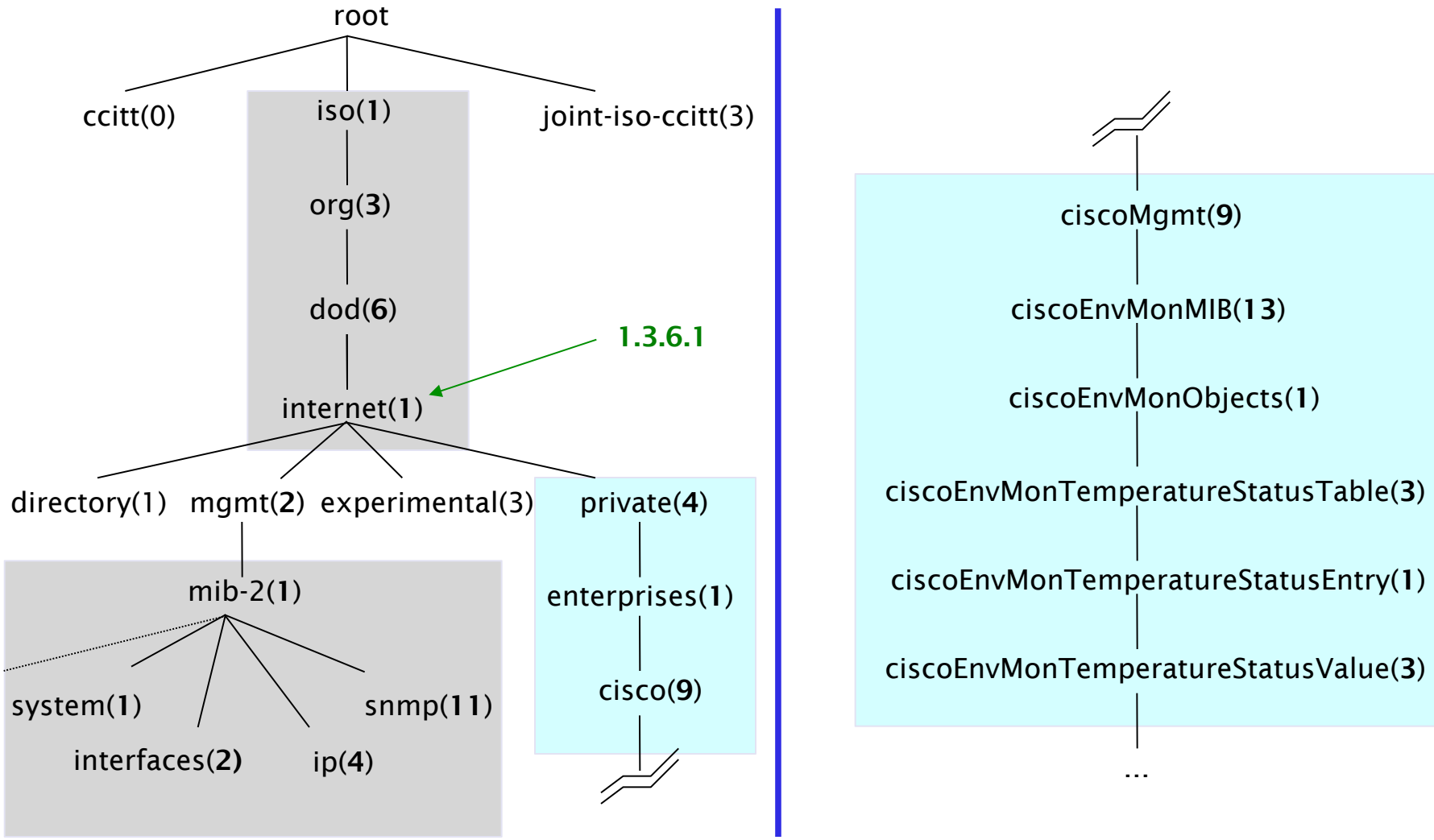
(Management Information Base)

- Una coleccion de OIDs relacionados
- Una corelacion de OIDs numericos a nombres legibles

# Arbol 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
hrSystem
interfaces(2)
ip(4)

# Arbol 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)
...

# Si direcciones de correo fueran OIDs

user@nsrc.org

*hubiera sido algo paracido como:*

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

user@99999.1.4.1.6.3.1

*pero que escribimos el parte mas arriba por el lado izquierdo:*

1.3.6.1.4.1.99999.117.115.101.114

- No se preocupa por el Arbol con muchos ramos. Que importa es que los OIDs son unicos.
- Asegura que los vendedores no tengan OIDs en conflicto.
- Que el OID numerico es que esta mandado a la red en el alambre

# El MIB de Internet

- **directory**(1) directorio OSI
- **mgmt**(2) objetos de estanderes RFC*
- **experimental**(3) experimentos Internet
- **private**(4) Especifico a los vendedores*
- **security**(5) Seguridad
- **snmpV2**(6) interno a SNMP

* Realmente solo hay dos ramas de interés:

1.3.6.1.2.1 = MIBs estandares

1.3.6.1.4.1 = MIB especificos a los vendedores

# OIDs y MIBs

- Lealos desde el izquierdo hacia derecha
- Componientes de OID separados por '.'
  - `1.3.6.1.4.1.9. ...`
- Cada OID corresponde a una ficha:
  - `.1.3.6.1.2.1.1.5 => sysName`
- El sendero completo:
  - `.iso.org.dod.internet.mgmt.mib-2.system.sysName`
- Como convertimos desde OIDs a Fichas (y vice versa)?
  - Use los archivos de MIBs!

# Archivos de MIB

- Archivos de MIBs definan objetos de que se puede encuestar, incluyendo:
  - Nombre de objeto
  - Descripcion de objeto
  - Tipo de dato (integer, texto, lista)
- Los archivos son texto con estructura, usando ASN.1
- Los MIBs estanderes incluyen:
  - MIB-II – (RFC1213) – un grupo de MIBs segundarios
  - HOST-RESOURCES-MIB (RFC2790)

# MIBs - Ejemplo

```
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-request`); it cannot be changed (i.e., `set-request`).

**`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.

# Archivos de MIB - 2

Archivos de MIBs, tambien, lo hacen posibles de interpretar un valor devuelto de un agente.

- Por ejemplo, el estatus de un ventilador podria ser 1,2,3,4,5,6 – que significa esto?

# MIBs - Muestra

```
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.
```

# Euncuestando un agente SNMP

Algunos comandos tipico para encuestar:

- `snmpget`
- `snmpwalk`
- `snmpstatus`
- `snmptable`

**Sintaxis**:

```
snmpXXX -c community -v1 host [oid]
snmpXXX -c community -v2c host [oid]
```

# Euncuestando un agente SNMP

## Un ejemplo

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

# Euncuestando un agente SNMP

Communidad:

- Texto de seguridad (clave / password) para definir si la entidad gestora tendra acceso R/O (solo leer) o R/W (leer y escribir).
- Esto es la forma mas simple de autenticacion de SNMP

OID

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

Preguntamos por el nombre del sistem (usando el OID de arriba)

- Porque el .0? Que notas?

# Falla SNMP: no respuesta?

- El dispositivo puede ser fuera linea o inalcanzable
- El dispositivo puede no tener un agente de SNMP
- El dispositivo puede estar configurado con otro texto de comunidad
- El dispositivo puede estar configurado para rechazar encuestas de SNMP desde su direccion de IP

*En todos de estes casos no va a recibir respuesta*

# Proxímo en nuestra practica

- Usando snmpwalk, snmpget
  - Archivo de configuracion: `/etc/snmp/`**`snmp.`**`conf`
- Corriendo el agente de Linux *(daemon)*
  - Archivo de configuracion: `/etc/snmp/`**`snmpd.`**`conf`
- Cargando MIBs
- Configurar SNMPv3 (opcional)

# Referencias


- ***Essential SNMP*** (Libros de O'Reilly)  Douglas Mauro, Kevin Schmi
- **SNMP Basico en Cisco**
  http://www.cisco.com/warp/public/535/3.html
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm
- **Wikipedia:**
  http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- ***IP Monitor*** **un Navegador de MIBs**
  http://support.ipmonitor.com/mibs_byoidtree.aspx
  **Navegador Cisco de MIB:**
  http://tools.cisco.com/Support/SNMP/do/BrowseOID.do
- **Navegador de MIB de Java de Fuente Abierto**
  http://www.kill-9.org/mbrowse
  http://www.dwipal.com/mibbrowser.htm (Java)
- ***SNMP Link*** **– Un coleccion de Recursos SNMP**
  http://www.snmplink.org/
- ***Net-SNMP*** **–  Herramientas de Fuente Abierto de SNMP**
  http://net-snmp.sourceforge.net/
- **Integrando con Nagios:**
  http://www.cisl.ucar.edu/nets/tools/nagios/SNMP-traps.html

# Materias Opcionales

## SNMP Versión 3

# SNMP y Seguridad

- SNMP versiones 1 y 2c son inseguros
- SNMP versión 3 creado para resolver esto

**Componientes**

- Mandador (Controlador de Mensajes)
- Sistema segundaria de procesar mensajes
- Sistema segundaria de seguridad
- Sistema segundaria de control de acceso

# SNMP versión 3 (SNMPv3)

El modulo mas comun esta basado en usuario o un “Modelo de Seguridad de Usuario”

- **La autenticidad y la integridad:** Las claves son usadas para los usuarios y los mensajes tienen firmas digitales generadas con una función hash (MD5 o SHA)
- **Privacidad:** Mensajes pueden estar encifrados con algoritmos como DES, de una clave secreta (privada).
- **Validez temporal:** Utiliza un reloj sincronizado con una ventana de 150 segundos con la comprobación secuencial.

# Niveles de Seguridad

**noAuthPriv**

- No autenticación, no privacidad

**authNoPriv**

- Autenticación sin privacidad

**authPriv**

- Autenticación con privacidad

# Configuración Cisco SNMPv3

```
snmp-server view  vista-ro   internet  included
snmp-server group ReadGroup  v3 auth read vista-ro
snmp-server user  admin ReadGroup v3 auth md5  xk122r56
```

O, como alternativo:

```
snmp-server user  admin  ReadGroup v3 auth md5 xk122r56
   priv des56 D4sd#rr56
```

# Configuración Net-SNMP SNMPv3

```
# apt-get install snmp snmpd
# net-snmp-config --create-snmpv3-user -a "xk122r56" admin
  /usr/sbin/snmpd
# snmpwalk -v3 -u admin -l authNoPriv -a MD5 -A "xk122r56”
    127.0.0.1
```