Gestión de redes con Necromantux

Ana Saiz García
<*ana{arroba}gpul{punto}org*>

VI Jornadas sobre Software Libre
A Coruña, 28 de Abril de 2006

Guión

- Introducción a la gestión de redes
- Conceptos básicos de SNMP
  - Introducción
  - Modelo de información
  - Protocolo
  - Control de acceso
- Gestión de red con Necromantux
  - Conectándonos a la red
  - Gestión con SNMP
  - Gestión con otras herramientas incluidas en Necromantux

Introducción a la gestión de redes (I)

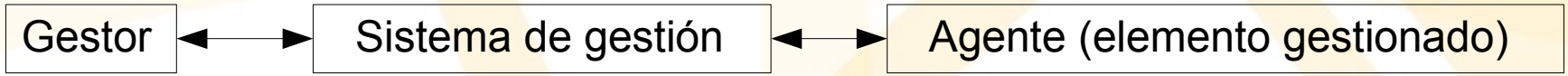
- **Definición**: Planificación, organización, supervisión y control de elementos de comunicación (dispositivos, sistemas o redes) para garantizar un nivel de servicio de acuerdo a un coste.
- **Objetivo**: aproximar la utilización al 100%, mejorando disponibilidad y rendimiento.
- **Métodos**:
  - ***Monitorización***:observación y análisis del estado y comportamiento de los equipos de la red
  - ***Control***: modificación de parámetros en los equipos de la red gestionada

Introducción a la gestión de redes (y II)

- Áreas funcionales (ISO):
  - Supervisión y fallos
  - Contabilidad
  - Prestaciones

  Monitorización
  - Configuración
  - Seguridad

  Control
- Componentes:



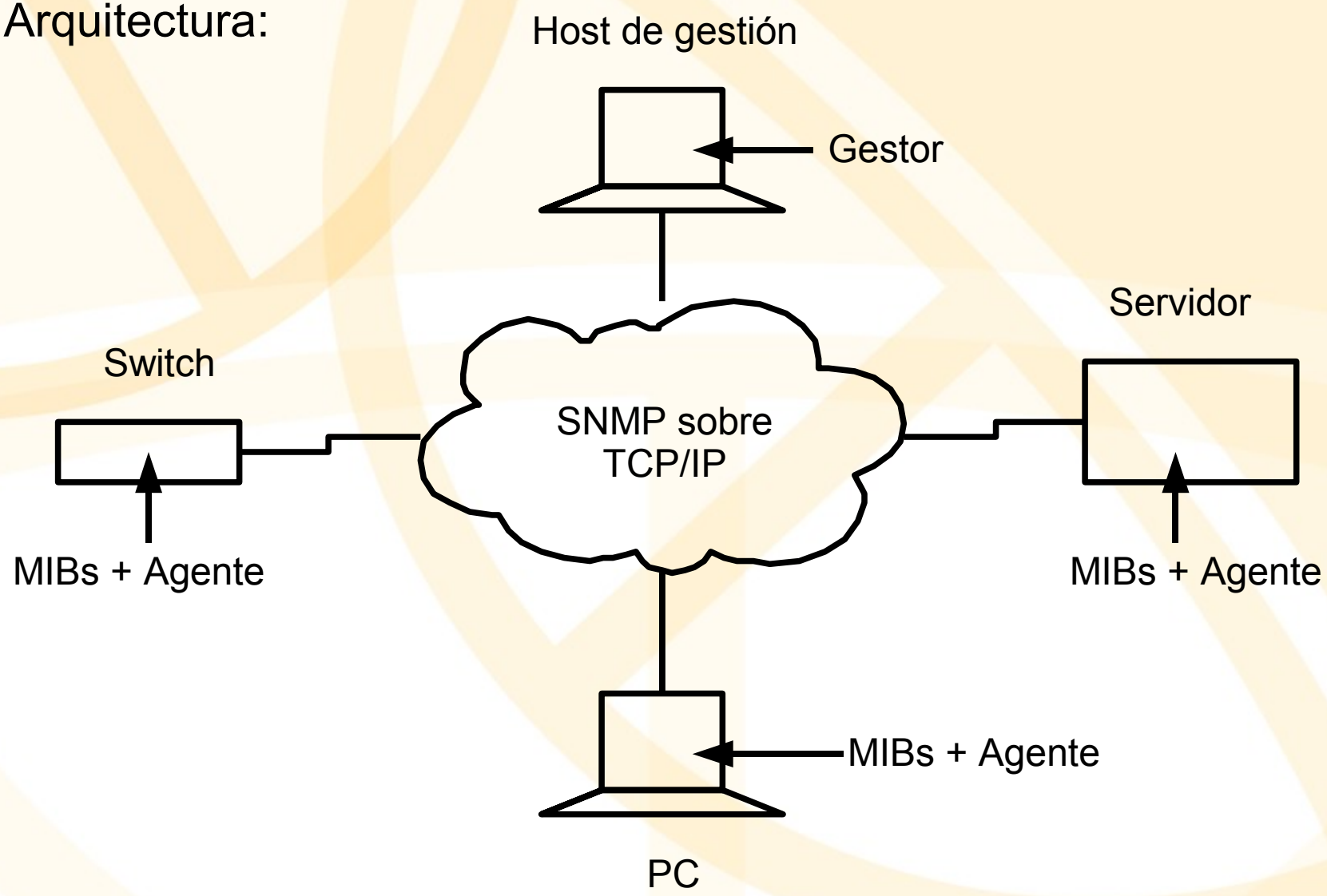
- Mecanismos de monitorización
  - Sondeo (*polling*): Gestor → Agente
  - Notificaciones (*event reporting*): Agente → Gestor
  - Mixtos: elemento intermedio que sondea al agente y notifica al gestor

Conceptos básicos de SNMP
Introducción (I)

- **SNMP**: *Simple Network Management Protocol*
  - Estándar para gestionar remotamente dispositivos conectados en red mediante un conjunto de operaciones simples (1988)
  - Se puede gestionar cualquier dispositivo que contenga el software adecuado para la recogida de información SNMP (agente)
  - v1 (RFC1157), v2 (RFC1901-1908), v3 (mayor seguridad) (RFC2271-2275)
- **SMI**: *Structure of Management Information* (RFC1155)
  - Cómo definir los objetos gestionados y su comportamiento
- **MIB***: Management Information Base* (RFC1156,1213)
  - Base de datos de los objetos gestionados a los que tiene acceso el agente
  - Un agente puede implementar varias MIBs concretas, pero todos implementan una general (MIB-II)

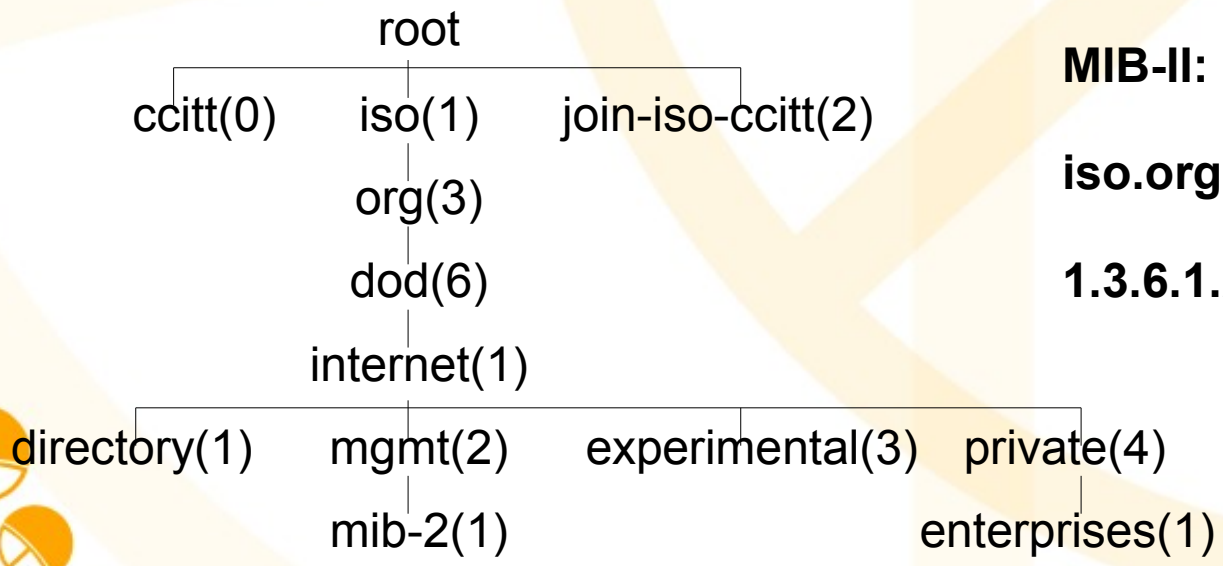
Conceptos básicos de SNMP
Introducción (y II)

- Arquitectura:



Conceptos básicos de SNMP
Modelo de información (I)

- **OIDs**: Identificadores de objetos (*Object Identifiers*)
  - Numéricos o textuales
  - Referencian recursos del sistema remoto para gestionarlos
- **Árbol OIDs**:
  - Árbol jerárquico
  - Definido por una secuencia de números enternos no negativos separados por un punto (.)



MIB-II:

iso.org.dod.internet.mgmt.mib-2

1.3.6.1.2.1

Conceptos básicos de SNMP
Modelo de información (II)

- **Grupos de MIB-II** (Todo dispositivo que soporte SNMP, soporta MIB-II)
  - **system (1)**: información sobre el sistema en el que está el agente
  - **interfaces (2)**: información sobre cada interfaz en un dispositivo de red
  - **at (3)**: obsoleto
  - **ip (4)**: información sobre IP, incluyendo encaminamiento (*routing*)
  - **icmp (5)**: información sobre ICMP (errores, mensajes descartados...)
  - **tcp (6)**: información sobre TCP, incluyendo tablas de conexiones
  - **udp (7)**: información sobre UDP (datagramas recibidos, erróneos...)
  - **egp (8)**: información sobre EGP
  - **cmot (9)**: vacío, se mantiene por razones históricas
  - **transmission (10)**: vacío, grupos específicos para medios de transmisión
  - **snmp (11)**: información sobre rendimiento de SNMP

Conceptos básicos de SNMP
Modelo de información (III)

- **Cómo se refieren los objetos**
  - **Instancias:** un único objeto puede tener múltiples instancias, y es a las que se accede.
  - Tipos de objeto: **tabulares** y **escalares**
  - **Tablas:**
    - Cada fila se identifica por el objeto *Entry: Table.Entry*
    - Cada columna define un objeto columnar, n: *Table.Entry.n*
    - Cada columna tiene una instancia por cada fila de la tabla => valor del objeto
    - Índices: simples o compuestos
    - Identificación de la instancia: identificación del objeto columnar + valor del índice en la fila
  - **Objetos escalares:**
    - Tienen una única instancia, y se identifica con el OID del objeto concatenado con .0

Conceptos básicos de SNMP
Modelo de información (IV)

- **Ejemplos**
  - **Escalar:** nombre del sistema: *system.sysName.0*
  - **Tabla:** Tabla de conexiones TCP: *tcp.tcpConnTable* (1.3.6.1.2.1.6.13)

tcpConnState (1)	tcpConnLocalAddress (2)	tcpConnLocalPort (3)	tcpConnRemAddress (4)	tcpConnRemPort (5)
3	192.168.1.2	12	192.168.1.100	18
2	192.168.1.2	32	192.168.1.50	99

tcp.tcpConnTable.tcpConnEntry (1.3.6.1.2.1.6.13.1)

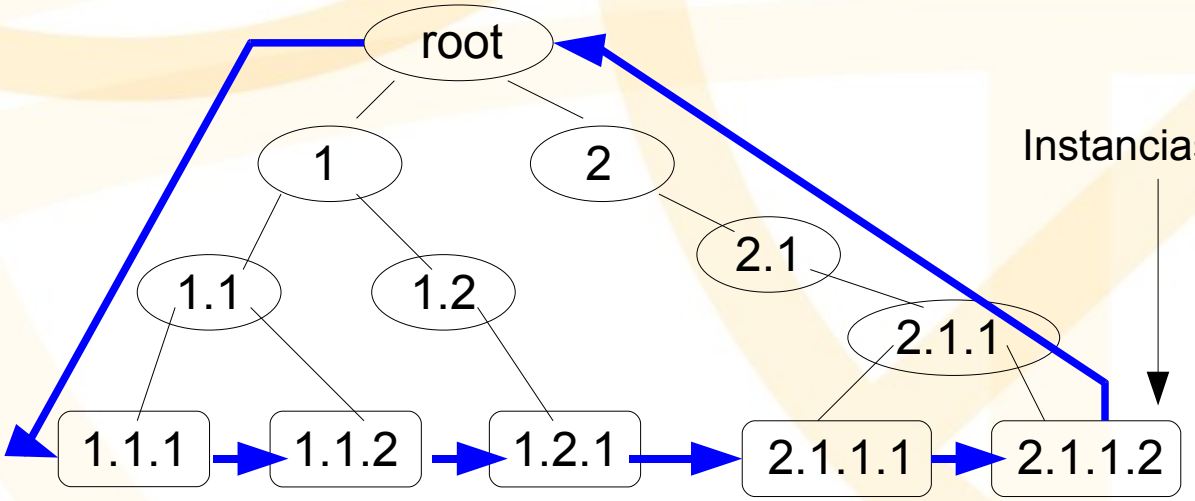
índice compuesto:
tcpConnLocalAddress.tcpConnLocalPort.tcpConnRemAddress.tcpConnRemPort

1ª fila, 2ª columna:
tcp.tcpConnTable.tcpConnEntry.**tcpConnLocalAddress**.192.168.1.2.12.192.168.1.100.18

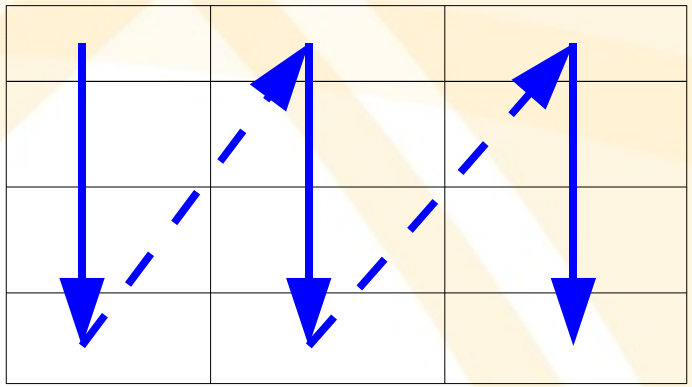
objeto fila | objeto columnar | índice (compuesto)

Conceptos básicos de SNMP
Modelo de información (y V)

- **Orden lexicográfico**
  - Permite acceso secuencial a los datos
    - Para cuando no se conoce la estructura de la vista a la que tiene acceso el agente
    - Para recorrer tablas



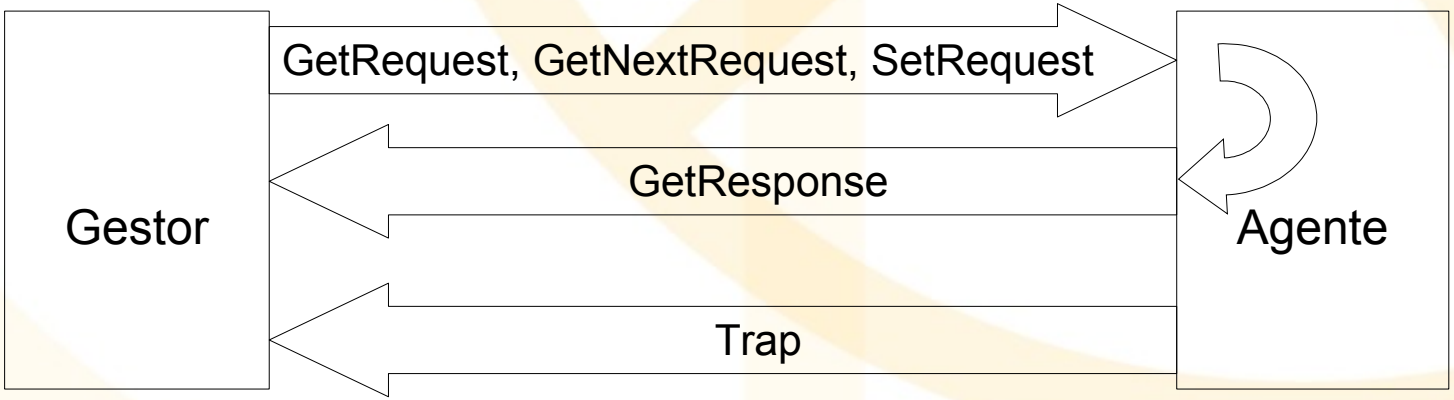
Árbol de objetos escalares



Tabla

Conceptos básicos de SNMP
Protocolo

- SNMP a nivel de aplicación sobre UDP: no conectivo, no fiable, baja sobrecarga. Puertos 161 (agente) y 162 (gestor)
- **Operaciones**
  - **GetRequest:** Gestor pide valores específicos de la MIB al Agente
  - **GetNextRequest**: Gestor pide valor del objeto siguiente a uno dado, siguiendo el orden lexicográfico
  - **GetResponse**: Agente devuelve los valores solicitados al Gestor
  - **SetRequest**: Gestor asigna un valor a un objeto en el sistema del Agente
  - **Trap**: Agente informa de un suceso inusual predefinido



Conceptos básicos de SNMP
Control de acceso

- Sistema gestionado => controles sobre su MIB:
  - *Política de **autenticación***:
    - Limita el acceso de los gestores
    - **Comunidad** (*community*): valor secreto compartido entre gestor y agente (password)
  - *Políticas de **acceso***:
    - distintos accesos para distintos gestores
    - **Vistas**: subconjuntos de objetos que pueden ser accedidos por determinados gestores
    - Cada comunidad tiene asociado un modo de acceso (lectura-escritura (rw), o sólo lectura (ro)) sobre cada vista

Gestión de red con Necromantux

- Conectándonos a la red
- Gestión con SNMP
  - Preparación
  - Net-SNMP
  - Tkined
    - Descubrimiento de la red
    - Consultas
    - Monitorización
- Gestión con otras herramientas incluidas en Necromantux
  - Descubrir la red
  - Sniffing
  - Análisis del flujo de datos
  - Otras herramientas

Gestión de red con Necromantux
Conectándonos a la red (I)

- **Opción A: Nigromante**:
  1) Botón derecho... Wizards... Nigromante
  2) Seleccionar 1: Configuración manual de la red
  3) Seleccionar interfaz
  4) ¿Configurar con DHCP?
     - Aceptar => Conectados a la red
     - Cancelar => Introducimos nosotros los datos:

       (1)Dirección IP *(ej, 192.168.1.50)*

       (2)Dirección Broadcast *(ej, 192.168.1.255)*

       (3)Máscara de red *(ej, clase C, 255.255.255.0)*

       (4)¿Configurar Gateway? Sí => introducir IP Gateway

       (5)¿Configurar DNS? Sí => introducir IP DNS

       => Conectados a la red

Gestión de red con Necromantux
Conectándonos a la red (y II)

- **Opción B: Manualmente**
  - Con DHCP:
    - **`#dhclient <interfaz>`** (ej, `#dhclient eth0`)
  - Sin DHCP:
    - **`#ifconfig <interfaz> <ip> netmask <máscara>`**

    (ej, `#ifconfig eth0 192.168.1.50 netmask 255.255.255.0`)
    - **`#route add default gw <ip_gateway>`**

    (ej, `#route add default gw 192.168.1.1`)

- Para probar que estamos conectados, ping a alguna de las máquinas que sepamos que están en la red (ej, `#ping 192.168.1.35`)

Gestión de red con Necromantux
Gestión con SNMP: Preparación

- Sistema a gestionar => Agente SNMP instalado (snmpd)
  - Fichero de configuración: **`/etc/snmp/snmpd.conf`**
    - Información del sistema:
      - `syslocation localhost`
      - `syscontact root@localhost`
      - `sysservices 79`
    - Información de control de accesos (comunidades, vistas)
      - `rocommunity necromantux`
  - Arrancar el agente:

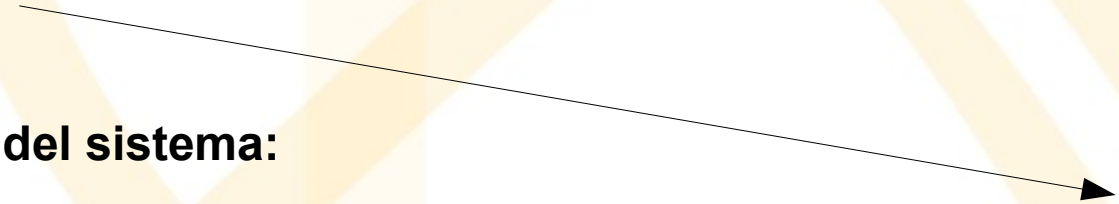
    `#/etc/init.d/snmpd start`

Gestión de red con Necromantux
Gestión con SNMP: Net-SNMP (I)

- Suite de aplicaciones para implementar SNMPv1, v2 y v3
- Utilizaremos **SNMPv1**: necesitamos autenticarnos con la **comunidad**

1) Recuperación del valor de un objeto dado: **snmpget**

```
#snmpget -v<versión> -c<comunidad> <IPagente>
  <OIDinstancia(!)>
```



Ejemplo: Información del sistema:

```
#snmpget -v1 -c necromantux 192.168.1.35 system.sysName.0
#snmpget -v1 -c necromantux 192.168.1.35 system.sysLocation.0
#snmpget -v1 -c necromantux 192.168.1.35 system.sysContact.0
#snmpget -v1 -c necromantux 192.168.1.35 system.sysServices.0
```

Gestión de red con Necromantux
Gestión con SNMP: Net-SNMP (II)

2) Modificación del valor de un objeto dado: **snmpset**

```
#snmpset -v<versión> -c<comunidad> <IPagente>
  <OIDinstancia> <tipo de objeto> <valor>
```

- Puede que el valor no pueda modificarse, porque:
  - el objeto está definido como de sólo lectura
  - no está permitida la escritura a nuestro gestor

Ejemplo: Información de contacto del sistema

```
#snmpset -v1 -c necromantux 192.168.1.35 system.sysContact.0
  s ana@localhost
```

s indica que el valor a modificar es un String

Gestión de red con Necromantux
Gestión con SNMP: Net-SNMP (III)

2) Recorrido por un árbol de objetos o una tabla:

2.1) Objeto a objeto: **snmpgetnext**

```
#snmpgetnext -v<versión> -c<comunidad> <IPagente>
  <OIDinstancia>
```

- OIDinstancia es el OID de la instancia anterior, en orden lexicográfico, a la que queremos consultar

Ejemplo: tabla de interfaces

```
#snmpgetnext -v1 -c necromantux 192.168.1.35
  interfaces.ifTable.ifEntry.0 => devuelve valor de ifIndex.1

#snmpgetnext -v1 -c necromantux 192.168.1.35
  interfaces.ifTable.ifEntry.ifIndex.1 => devuelve valor de
  ifIndex.2

...
```

Gestión de red con Necromantux
Gestión con SNMP: Net-SNMP (IV)

2.2) Tabla o subárbol completo: **snmpwalk**

```
#snmpwalk -v<versión> -c<comunidad> <IPagente>
  <OIDinstancia>
```

Ejemplo: tabla de interfaces

```
#snmpwalk -v1 -c necromantux 192.168.1.35 interfaces.ifTable
```

Ejemplo: tabla de conexiones TCP

```
#snmpwalk -v1 -c necromantux 192.168.1.35 tcp.tcpConnTable
```

- Si abrimos una nueva conexión TCP (ssh, http...) y volvemos a consultar, aparecen nuevas filas en la tabla

Gestión de red con Necromantux
Gestión con SNMP: Tkined (I)

- Aplicación gráfica para análisis y monitorización
- Botón derecho... Redes... Tkined
- Para habilitar aplicaciones: *Tools...* aplicación que queramos

1) Descubrimiento de la red: **IP Discover**
   - *Tools... IP Discover*
   - *IP Discover... Set Parameters* -> opciones, para que sea más rápido y sólo descubra los equipos adyacentes al nuestro:
     - *ICMP retries* = 1
     - *ICMP timeout* = 1
     - *Delay between ICMP packets* = 1
     - *Max length of a route* = 1
   - *IP Discover... Discover IP Network* => introducir IP de la red (ej, *192.168.1*)
   - Mover los nodos: pulsando CTRL o botón central del ratón
   - Se pueden cambiar los nombres y los iconos

Gestión de red con Necromantux
Gestión con SNMP: Tkined (II)

2) Consultas de objetos SNMP: **SNMP Browser**

- *Tools... SNMP Browser*
- *SNMP Browser... Set Parameter*s -> opciones de la consulta SNMP:
  - community: comunidad para autenticarnos ante el agente (ej, *necromantux*)
- *SNMP Browser... MIB Browser* -> nos permite navegar por la MIB
- *SNMP Browser... MIB-2...* grupo al que pertenece el objeto que queremos consultar... objeto a consultar (escalar o tabla)
- Ejemplos:
  - *SNMP Browser... MIB-2... system... system.Contact*
  - *SNMP Browser... MIB-2... interfaces... ifTable*
  - *SNMP Browser... MIB-2... tcp... tcpConnTable*
- Aparece una nueva ventana con los valores de los objetos consultados

Gestión de red con Necromantux
Gestión con SNMP: Tkined (III)

3) Monitorización: **IP Monitor, SNMP Monitor**

- *Tools... IP Monitor...*
  - *IP Monitor... Check Reachability*
    - Monitorizar alcanzabilidad de los equipos
    - Si uno deja de ser alcanzable, parpadea y muestra “unreachable”
  - En *IP Monitor... Set Parameters* modificamos el intervalo de monitorización [s]
- *Tools... SNMP Monitor*
  - *SNMP Monitor... Set SNMP Parameter* -> community: comunidad para autenticarnos ante el agente (ej, *necromantux*)
  - *SNMP Monitor... Set Monitor Parameter* -> intervalo, gráfica
  - *SNMP Monitor... Interface utilization* -> estadísticas de uso de las interfaces de red
  - *SNMP Monitor... Monitor variable* -> monitorizamos el objeto que queramos, introduciendo su OID
    - *SNMP Monitor... Modify Monitor Job* -> cambiar intervalo, umbrales para alarmas, salida de la alarma, o matar el monitor

Gestión de red con Necromantux
Gestión con SNMP: Tkined (IV)

3) Monitorización: **SNMP Monitor**:

Ejemplos: monitorización de parámetros de red

- Cantidad de datagramas IP recibidos
  - Monitorizar *ip.ipInReceives.0*
  - *SNMP Monitor... Modify Monitor Job*
    - Establecer un umbral para un máximo de datagramas por unidad de tiempo
    - Establecer salida de la alarma con gráfico (graph) y texto (text)
  - Si se supera el umbral, la gráfica parpadeará y aparecerá un aviso en una ventana nueva
- Cantidad de mensajes descartados en un interfaz de red
  - Consultar la tabla de interfaces: *SNMP Browser... MIB-2... interfaces... ifTable*
  - Buscar el índice del interfaz que nos interese (**N**)
  - Monitorizar *interfaces.ifTable.ifEntry.ifInDiscards.**N*** o *interfaces.ifTable.ifEntry.ifOutDiscards.**N***
  - Establecer un umbral, por ejemplo si se superan X descartes cada minuto

Gestión de red con Necromantux
Gestión con SNMP: Tkined (y V)

3) Monitorización: **SNMP Monitor**:

Ejemplos: monitorización de recursos del equipo (Grupo *Host Resources*, RFC2790)

- Cantidad de memoria utilizada en el equipo
  - Consultar la tabla de almacenamiento del grupo Host Resources: *SNMP Browser... MIB-2... host... hrStorage... hrStorageTable*
  - Buscar el índice de la memoria del equipo (ej, **2**)
  - Monitorizar *host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageUsed.**2***
  - Consultar *host.hrStorageTable.hrStorageEntry.hrStorageSize.**2***
  - Establecer umbral inferior al tamaño de la memoria, para que avise antes de que vaya a alcanzarse
- Procesos corriendo en el sistema
  - *SNMP Browser... MIB-2... host... hrSystem... hrSystemMaxProcesses* -> máximo de procesos que admite el sistema (si no lo hay, vale 0)
  - Suponiendo que lo hubiera, monitorizar *host.hrSystem.hrSystemProcesses.0*
  - Poner un umbral anterior al máximo de procesos que admite el sistema, para que nos avise antes de que se alcance

Gestión de red con Necromantux
Otras herramientas incluidas en Necromantux (I)

1) Descubriendo la red: **nmap**

- Recorre rangos de direcciones
- informa de qué hosts están levantados, sus puertos abiertos y otras opciones (sistema operativo, versión de los servicios...)
- **`#nmap <IPSubred>`**
- Ejemplo:
  - `#nmap 192.168.1.0/24`
  - `#nmap -sV 192.168.1.0/24` -> versiones de los servicios
  - `#nmap -O 192.168.1.0/24` -> sistema operativo
- Versión gráfica: **nmapfe** -> *Botón derecho... Redes... Nmap*

=> Podemos conocer la estructura de la red a la que nos enfrentamos

Gestión de red con Necromantux
Otras herramientas incluidas en Necromantux (II)

2) Análisis del tráfico de la red *(Sniffing)*: **tcpdump, ethereal**

- Asumir el tráfico de la red para inspeccionar su contenido
- No sólo para *crackers*, útil para detección de problemas en las conexiones
- Topologías ethernet en bus: todo el tráfico circula por toda la red => colocar una máquina en modo promíscuo que capture todo el tráfico

a) **tcpdump**

- Aplicación en línea de comandos
- Muy potente pero compleja, conocimientos avanzados para interpretar los datos
- **`#tcpdump -v -i <interfaz>`**
- Ejemplo:
  - `#tcpdump -v -i eth0`

Gestión de red con Necromantux
Otras herramientas incluidas en Necromantux (III)

2) Análisis del tráfico de la red *(Sniffing)*: **tcpdump, ethereal**

b) **ethereal**

- Aplicación gráfica: *Botón derecho... Redes... Ethereal*
- Interfaz más agradable y análisis de los datos más sencillo que en tcpdump
- Capturar tráfico: *Capture... Start*, y elegimos interfaz
- Detenemos la captura cuando consideremos que tenemos datos suficientes
- Aparecen registros de las conexiones y los paquetes obtenidos
- Pinchando en cada uno => detalles:
  - Tiempos
  - Protocolos, se pueden ver en detalle
  - Contenido
  - Direcciones de origen y destino...
- Se puede guardar la captura

Gestión de red con Necromantux
Otras herramientas incluidas en Necromantux (IV)

2) Análisis del flujo de datos: **ethstatus, iptraf**

- En algunos casos no es necesario ver el contenido del tráfico, sólo la cantidad y forma del flujo de datos

a) **ethstatus**

- Información (algo pobre) sobre el interfaz: cantidades de tráfico, velocidades...
- **`#ethstatus`**

b) **iptraf**

- Analiza el tráfico IP sobre una interfaz
- Estadísticas de una interfaz, más vistoso que ethstatus
- Estadísticas del flujo de datos (protocolos, tamaño de paquetes...), sin preocuparse por el contenido
- **`#iptraf`**

Gestión de red con Necromantux
Otras herramientas incluidas en Necromantux (y V)

3) Otras herramientas: **mtr, bing**

a) **mtr**

- Máquinas por las que circula un paquete hasta llegar a su destino
- **#mtr <IP_destino>**
- Ejemplo:
  - `#mtr 192.168.1.50`

b) **bing**

- Ancho de banda entre dos puntos de la red
- Las estadísticas aparecen al pararlo
- **#bing <IP_origen> <IP_destino>**
- Ejemplo:
  - `#bing 192.168.1.35 192.168.1.50`

Referencias

- Teoría SNMP:
  - *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2.* William Stallings. Addison Wesley Professional.
  - *Essential SNMP.* Douglas Mauro, Kevin Schmidt. O'Reilly
- Otras herramientas de Necromantux:
  - *Auditoría y Gestión de Red con Necromantux Live CD.* David Fernández Vaamonde.Revista Mundo Linux, nº 80 (Julio 2005)
  - Páginas *man* de las herramientas
- RFCs:
  - 1157 (SNMP), 1155 (SMI), 1156 y 1213 (MIB), 2790 (Host Resources-MIB)
- Net-SNMP:
  - http://www.net-snmp.org/
- Tkined:
  - http://www.eng.auburn.edu/users/doug/tkined.html
- Esta charla estará en http://ana.saizgarcia.net/charlas