

# Capítulo 15

Monitorização da Rede.

Simple Network Management Protocol (SNMP).

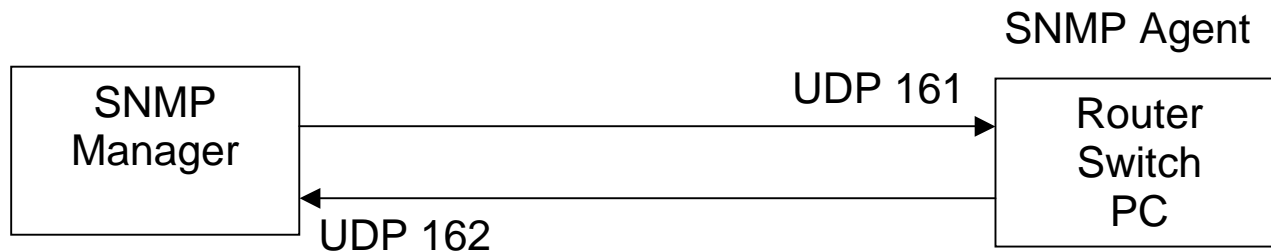
---

- Uma das mais importantes tarefas de um administrador de uma rede informática é monitorizar o tráfego na rede,
- Detectar perdas de conectividade, saturação de tráfego e ataques (Denial of service - DoS)
- O protocolo SNMP é o protocolo standard para monitorizar remotamente dispositivos de rede (routers e switches)

# Cliente-Servidor

---

- Funciona no paradigma cliente-servidor (Manager-Agent)
- Protocolo UDP portas 161 e 162



# Versões SNMP

---

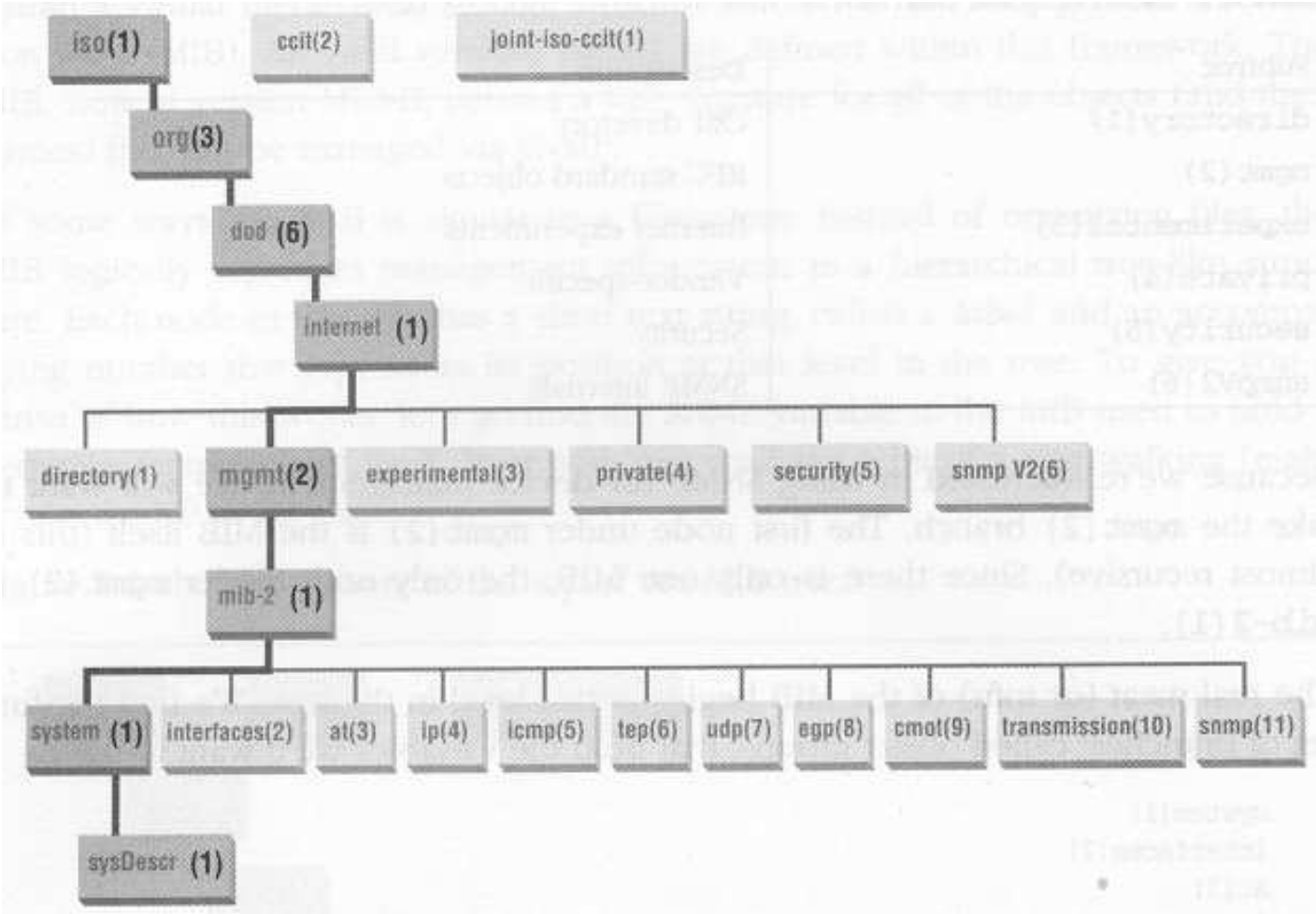
- SNMPv1
- SNMPv2c
- SNMPv3
  
- Versão 1 é a mais utilizada
- Versão 3 oferece mais segurança (criptação dos dados)

# Management Information Base (MIB)

---

- Todas as variáveis SNMP existem numa base de dados com uma estrutura hierárquica - Management Information Base (MIB)
- As variáveis podem ser inteiros, strings, identificadores de objectos (OID) e valores nulos

# Management Information Base (MIB) #2



# Management Information Base (MIB) #3

---

- MIB é similar a uma estrutura de directorios, mas em vez de organizar ficheiros o MIB organiza informação (variaveis)
- Cada nodo na arvore tem um label (texto) e um numero inteiro
- Exemplos:

Directory(1)

Mgmt(2)

Experimental(3)

Private(4)

# OID - Object identifier #1

---

- O OID é o conjunto de numeros separados por pontos que identifica um nodo na estrutura

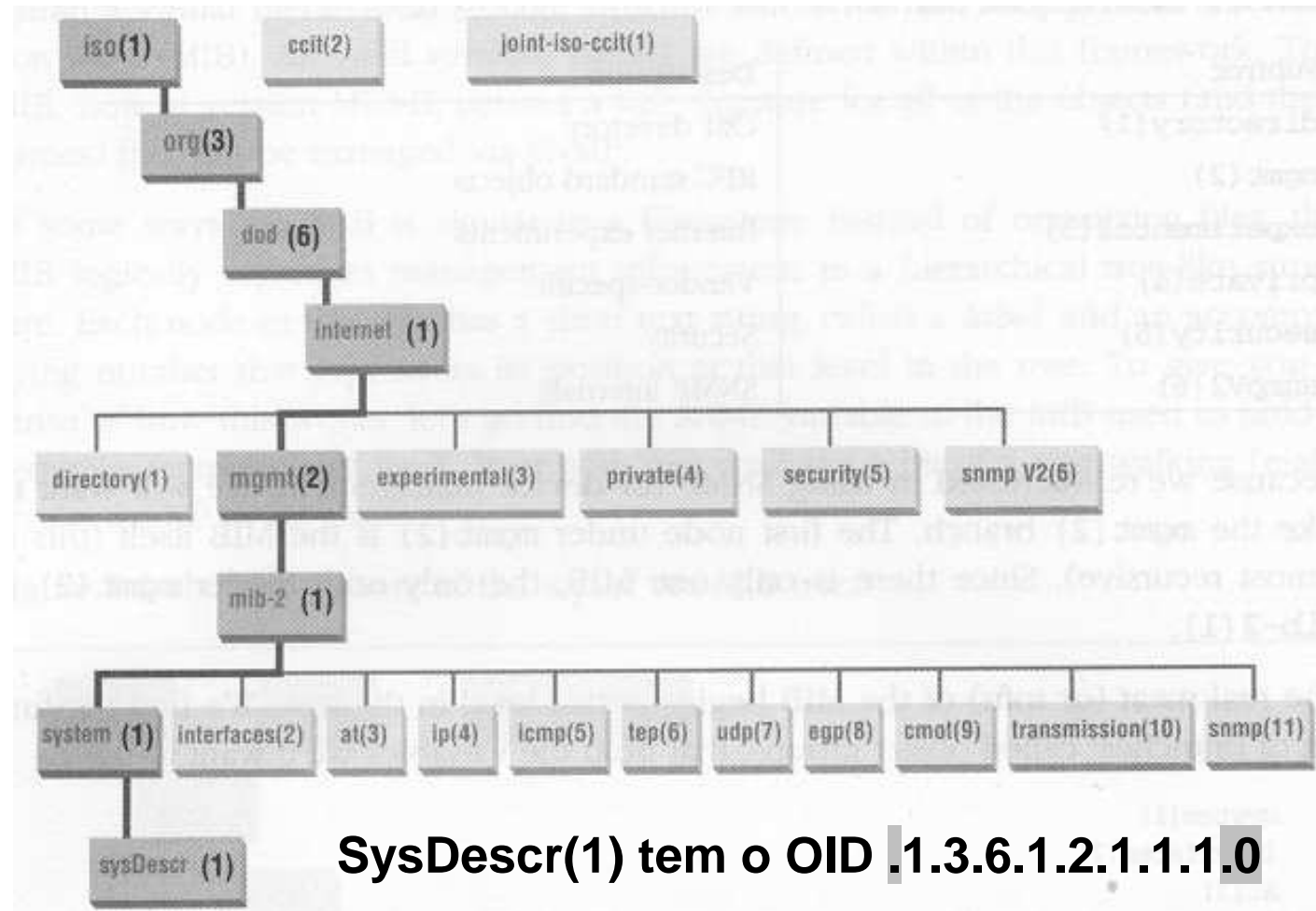
- Exemplo de um OID:

**SysDescr(1) tem o OID `1.3.6.1.2.1.1.1.0`**

- Notas:

- O zero final indica o valor da variavel
- sem o ponto inicial o OID não começa na raiz mas a partir do nodo mib-2

# OID - Object identifier #2





## OID - Object identifier #3

---

Exemplo:

```
jbastos@australia:~$ snmpget -v 2c -c public router1  
.1.3.6.1.2.1.1.1.0
```

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux router1  
2.4.33.3 #1 Fri Oct 20 01:11:49 WEST 2006 i586
```

```
jbastos@australia:~$ snmpget -v 2c -c public router1  
.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0
```

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux router1  
2.4.33.3 #1 Fri Oct 20 01:11:49 WEST 2006 i586
```

```
jbastos@australia:~$ snmpget -v 2c -c public router1  
system.sysDescr.0
```

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux router1  
2.4.33.3 #1 Fri Oct 20 01:11:49 WEST 2006 i586
```

# SNMP community

---

Communities são uma forma de agrupar SNMP agents com as mesmas restrições de acesso

Funcionam como pseudo-passwords

Exemplo:

```
jbastos@australia:~$ snmpget -v 2c -c public router1  
system.sysUpTime.0
```

# Mensagens (comandos net-snmp) SNMP

---

GET (snmpget)

GET-NEXT (snmpgetnext)

GET-RESPONSE

SET (snmpset)

TRAP (snmptrap)

# snmpget

---

```
jbastos@australia:~$ snmpget -v 2c -c public router1  
system.sysUpTime.0
```

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (95014248) 10  
days, 23:55:42.48
```

# snmpgetnext

---

```
jbastos@australia:~$ snmpgetnext -v 2c -c public router1  
ip.ipRouteTable.ipRouteEntry.ipRouteDest
```

```
RFC1213-MIB::ipRouteDest.0.0.0.0 = IPAddress: 0.0.0.0
```

```
jbastos@australia:~$ snmpgetnext -v 2c -c public router1  
ip.ipRouteTable.ipRouteEntry.ipRouteDest.0.0.0.0
```

```
RFC1213-MIB::ipRouteDest.10.10.20.0 = IPAddress:  
10.10.20.0
```

```
jbastos@australia:~$ snmpgetnext -v 2c -c public router1  
ip.ipRouteTable.ipRouteEntry.ipRouteDest.10.10.20.0
```

```
RFC1213-MIB::ipRouteDest.10.10.80.0 = IPAddress:  
10.10.80.0
```

# snmpwalk

---

```
jbastos@australia:~$ snmpwalk -v 2c -c public router1  
ipRouteDest
```

```
RFC1213-MIB::ipRouteDest.0.0.0.0 = IPAddress: 0.0.0.0  
RFC1213-MIB::ipRouteDest.10.10.20.0 = IPAddress: 10.10.20.0  
RFC1213-MIB::ipRouteDest.10.10.80.0 = IPAddress: 10.10.80.0  
RFC1213-MIB::ipRouteDest.10.11.0.0 = IPAddress: 10.11.0.0  
RFC1213-MIB::ipRouteDest.193.136.224.0 = IPAddress: 193.136.224.0
```

# snmpset

---

```
jbastos@australia:~$ snmpget -v 2c -c public router1  
system.sysLocation.0
```

```
SNMPv2-MIB::sysLocation.0 = STRING: Unknown (configure  
/etc/snmp/snmpd.local.conf)
```

```
jbastos@australia:~$ snmpset -v 2c -c private router1  
system.sysLocation.0 s "Faro - Portugal"
```

```
SNMPv2-MIB::sysLocation.0 = STRING: Faro - Portugal
```

# snmptrap

---

- Traps são utilizadas pelos agents para informar a management station (manager) de condições anormais (overload etc)

```
snmptrap -v 1 -c public manager sysLocation.0 s  
"temperature alarm!"
```

- O manager tem que estar a correr o serviço "snmptrapd" para receber as mensagens de "trap":

```
SNMPv2-MIB::sysLocation.0 = STRING: temperature  
alarm!
```



# IReasoning MIB Browser

The screenshot shows the iReasoning MIB Browser interface. At the top, there is a menu bar with 'File', 'Edit', 'Operations', 'Tools', 'Bookmarks', and 'Help'. Below the menu bar, the 'Address' field is set to '10.10.22.162' and the 'OID' field is set to '5.116.101.109.1.3.6.1.2.1.1.0'. The 'Operations' dropdown is set to 'Walk'. A 'Go' button is visible to the right of the dropdown.

The main interface is divided into two panes. The left pane, titled 'SNMP MIBs', contains a 'MIB Tree' with a tree view showing folders for 'RFC1213-MIB.iso.org.dod.internet.mgmt.mib' and 'HOST-RESOURCES-MIB.iso.org.dod.internet'. The right pane, titled 'Result Table', displays a table of system information.

Name/OID	Value	Type
sysDescr.0	Linux router1 2.4.33.3 #1 Fri Oct 20 01:11:49 WEST 2006 i...	OctetString
sysObjectID.0	.1.3.6.1.4.1.2021.250.10	OID
sysUpTime.0	283 hours 24 minutes 21 seconds	TimeTicks
sysContact.0	Root <root@localhost> (configure /etc/snmp/snmpd.local.c...	OctetString
sysName.0	router1	OctetString
sysLocation.0	Unknown (configure /etc/snmp/snmpd.local.conf)	OctetString
.1.3.6.1.2.1.1.8.0	0 millisecond	TimeTicks
.1.3.6.1.2.1.1.9....	.1.3.6.1.2.1.31	OID
.1.3.6.1.2.1.1.9....	.1.3.6.1.6.3.1	OID
.1.3.6.1.2.1.1.9....	.1.3.6.1.2.1.49	OID
.1.3.6.1.2.1.1.9....	.1.3.6.1.2.1.4	OID
.1.3.6.1.2.1.1.9....	.1.3.6.1.2.1.50	OID
.1.3.6.1.2.1.1.9....	.1.3.6.1.6.3.16.2.2.1	OID
.1.3.6.1.2.1.1.9....	.1.3.6.1.6.3.10.3.1.1	OID
.1.3.6.1.2.1.1.9....	.1.3.6.1.6.3.11.3.1.1	OID
.1.3.6.1.2.1.1.9....	.1.3.6.1.6.3.15.2.1.1	OID
.1.3.6.1.2.1.1.9....	The MIB module to describe generic objects for network inte...	OctetString
.1.3.6.1.2.1.1.9....	The MIB module for SNMPv2 entities	OctetString
.1.3.6.1.2.1.1.9....	The MIB module for managing TCP implementations	OctetString
.1.3.6.1.2.1.1.9....	The MIB module for managing IP and ICMP implementations	OctetString
.1.3.6.1.2.1.1.9....	The MIB module for managing UDP implementations	OctetString
.1.3.6.1.2.1.1.9....	View-based Access Control Model for SNMP.	OctetString
.1.3.6.1.2.1.1.9....	The SNMP Management Architecture MIB.	OctetString
.1.3.6.1.2.1.1.9....	The MIB for Message Processing and Dispatching.	OctetString
.1.3.6.1.2.1.1.9....	The management information definitions for the SNMP User-...	OctetString
.1.3.6.1.2.1.1.9....	0 millisecond	TimeTicks
.1.3.6.1.2.1.1.9....	0 millisecond	TimeTicks
.1.3.6.1.2.1.1.9....	0 millisecond	TimeTicks

At the bottom of the window, there is a status bar showing the current OID '.1.3.6.1.6.3.16.1.5.2.1.6.6.115.121.115.116.101.109.1.3.6.1.2.1.1.0', the time '1:23:45 PM', and the memory usage '15M of 15M'.

# MRTG Traffic Grapher

