Capítulo 15

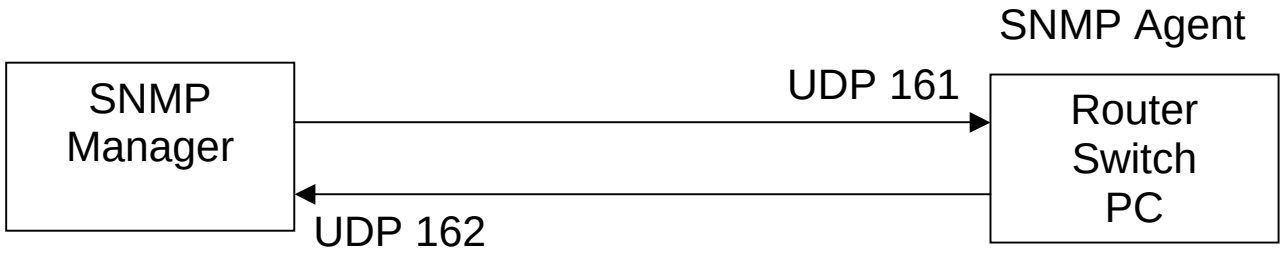
Monitorização da Rede.

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

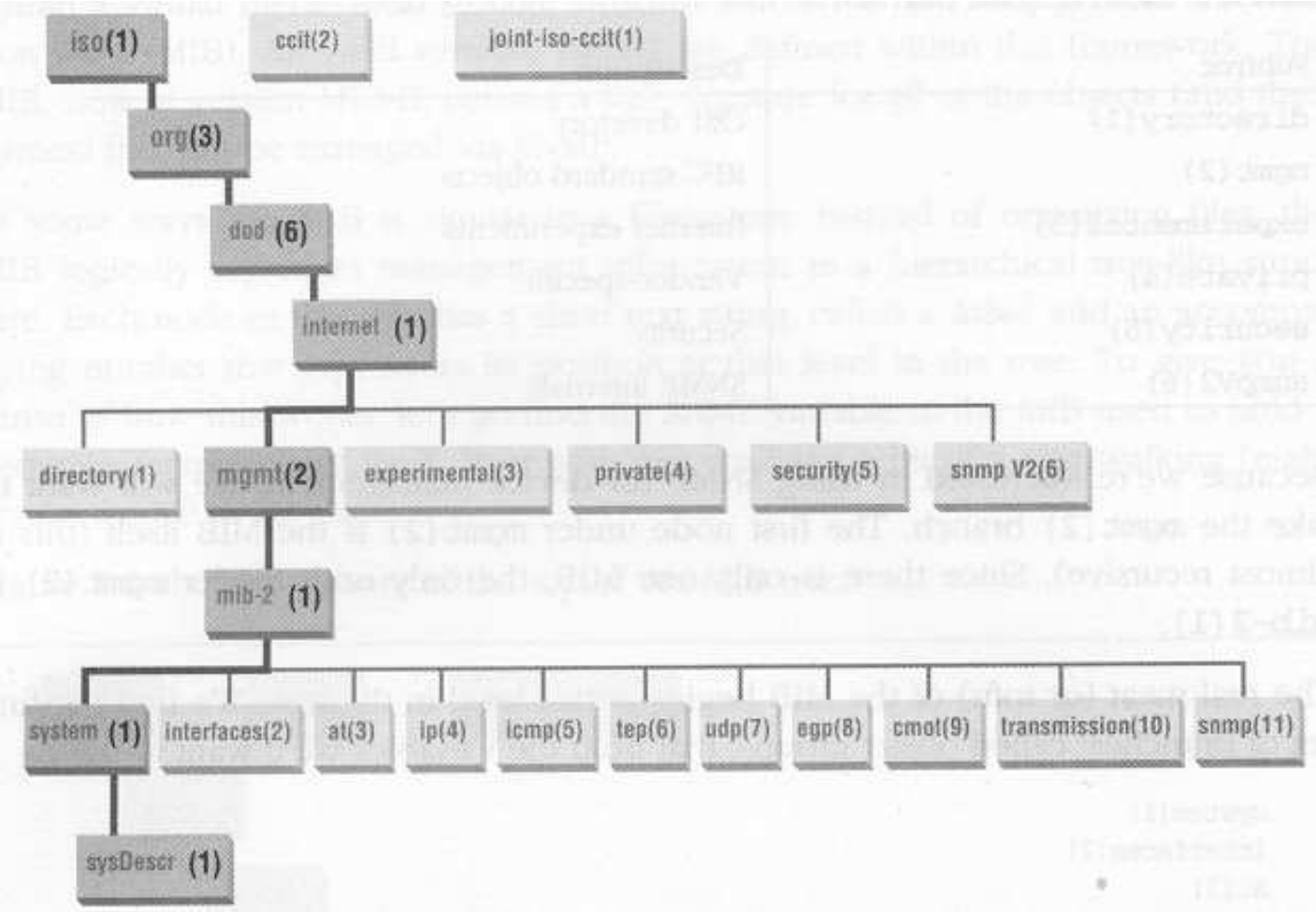
- SNMPv1
- SNMPv2c
- SNMPv3

- Versão 1 é a mais utilizada
- Versão 3 oferece mais segurança (encriptação dos dados)

Management Information Base (MIB)

- Todas as variaveis SNMP existem numa base de dados com uma estrutura hierarquica - Management Information Base (MIB)
- As variaveis 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)
```

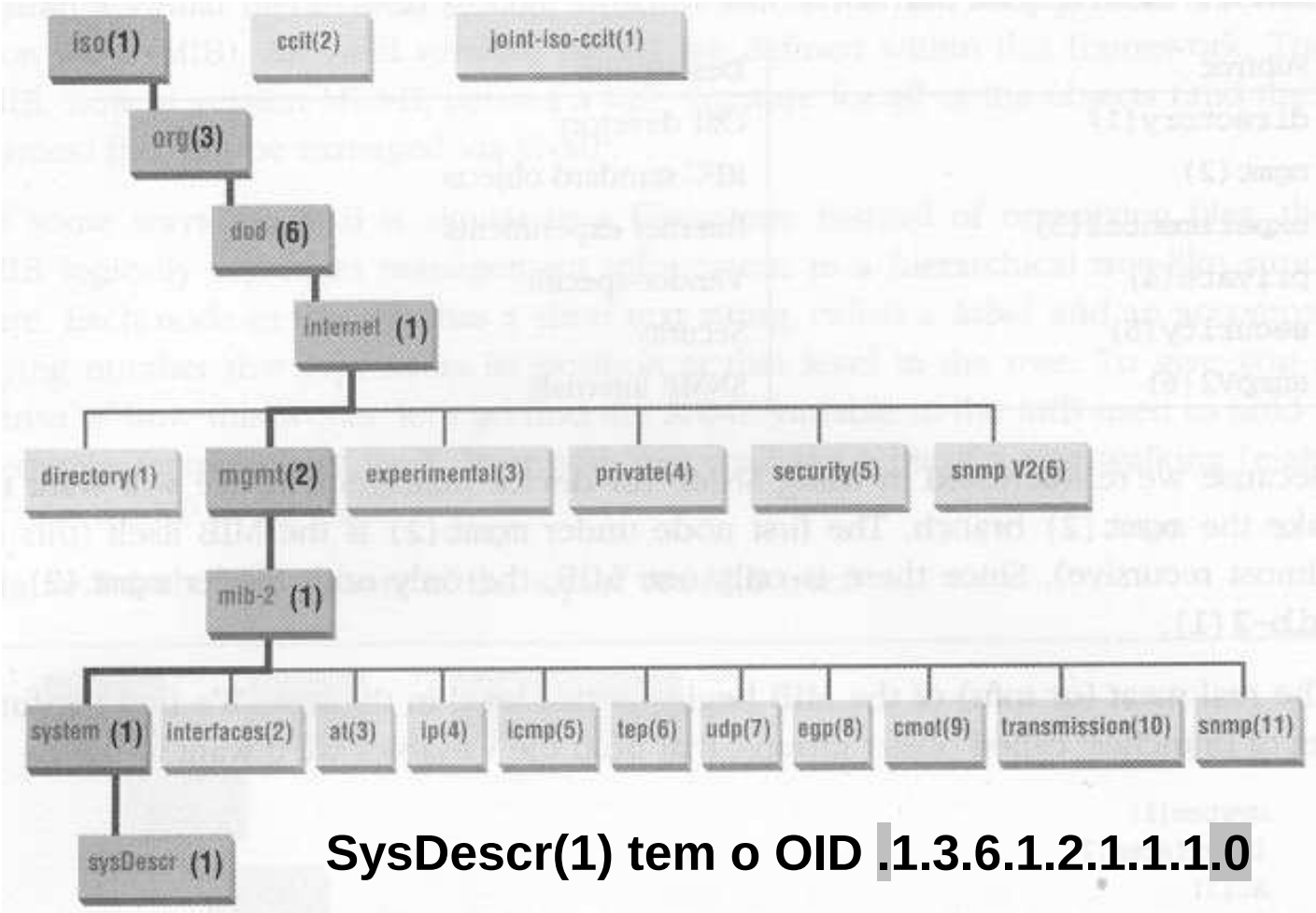
OID - Object identifier #1

- **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



SysDescr(1) tem o OID .1.3.6.1.2.1.1.1.0

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

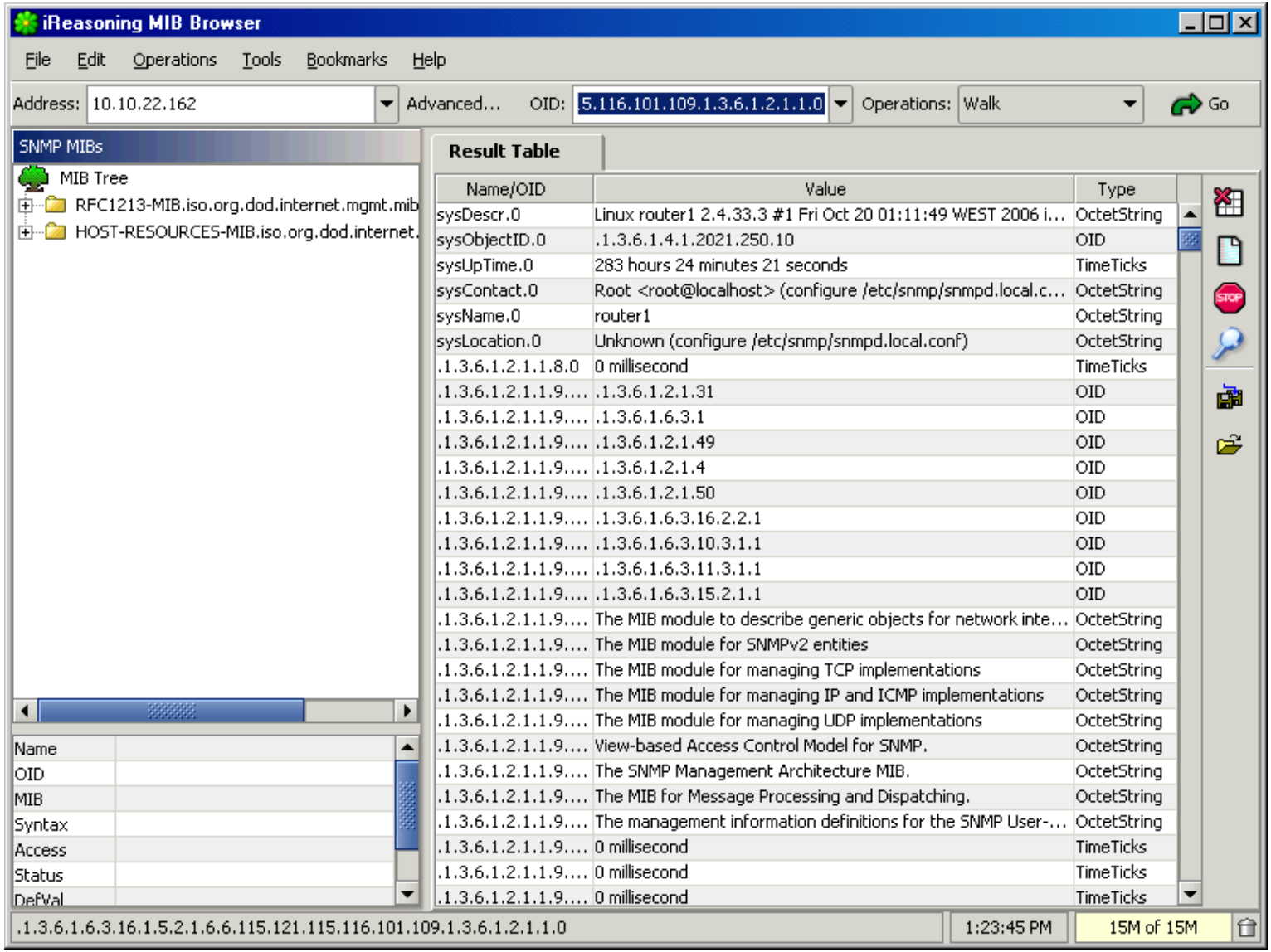
- Traps são utilizadas pelos agents para informar a management station (manager) de condições anormais (overload etc)

```
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



MRTG Traffic Grapher