Gestão de redes e SNMP

Laboratório de Redes
2008/2009

Gestão de redes: Motivação

Num mundo perfeito as redes não necessitariam de gestão, simplesmente funcionariam

No entanto...

- O equipamento tende a avariar
- Alterações implicam configuração
- Alguém tem de pagar o uso
- Desempenho abaixo da expectativa
- Abusos...

Áreas de gestão

- Fault
- Configuration
- Accounting
- Performance
- Security

Áreas de gestão de redes – ISO

- Fault
  - Detecção, isolamento e correcção de comportamentos anormais
- Configuration
  - Localização e recolha de informação sobre os dispositivos
- Accounting
  - Medição da utilização da rede e imputação de custos aos utilizadores
- Performance
  - Recolha de estatísticas e avaliação do desempenho em condições normais e degradadas
- Security

Protocolos de gestão

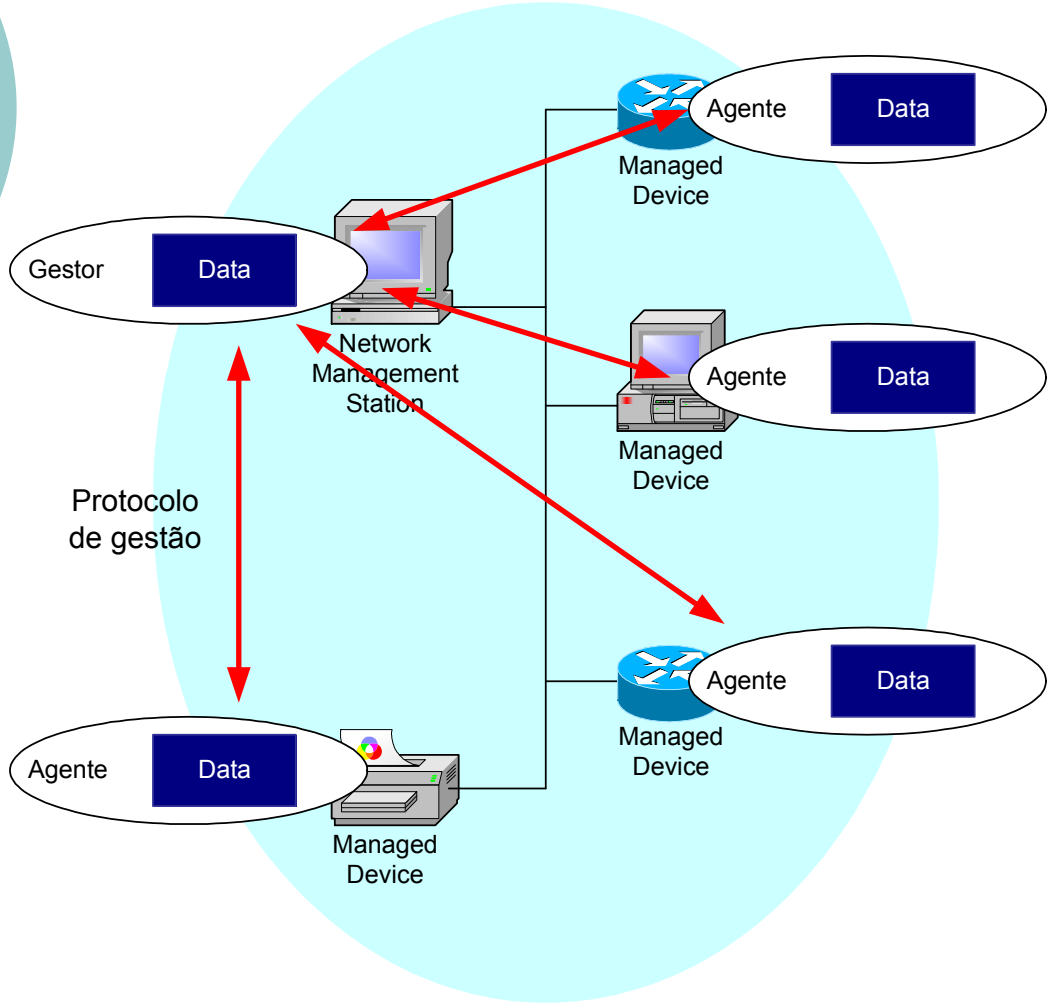
OSI CMIP

- Common Management Information Protocol
- Desenvolvido nos anos 80 como *o* protocolo unificador para gestão de redes
- Implementado muito lentamente...

SNMP

- Simple Network Management Protocol
- Origens na Internet (SGMP)
- Começou muito simples
- Rapidamente adoptado
- Crescimento em tamanho e complexidade
- Versão corrente: SNMPv3
- Protocolo *de facto* para gestão de redes

Gestão: Modelo-base

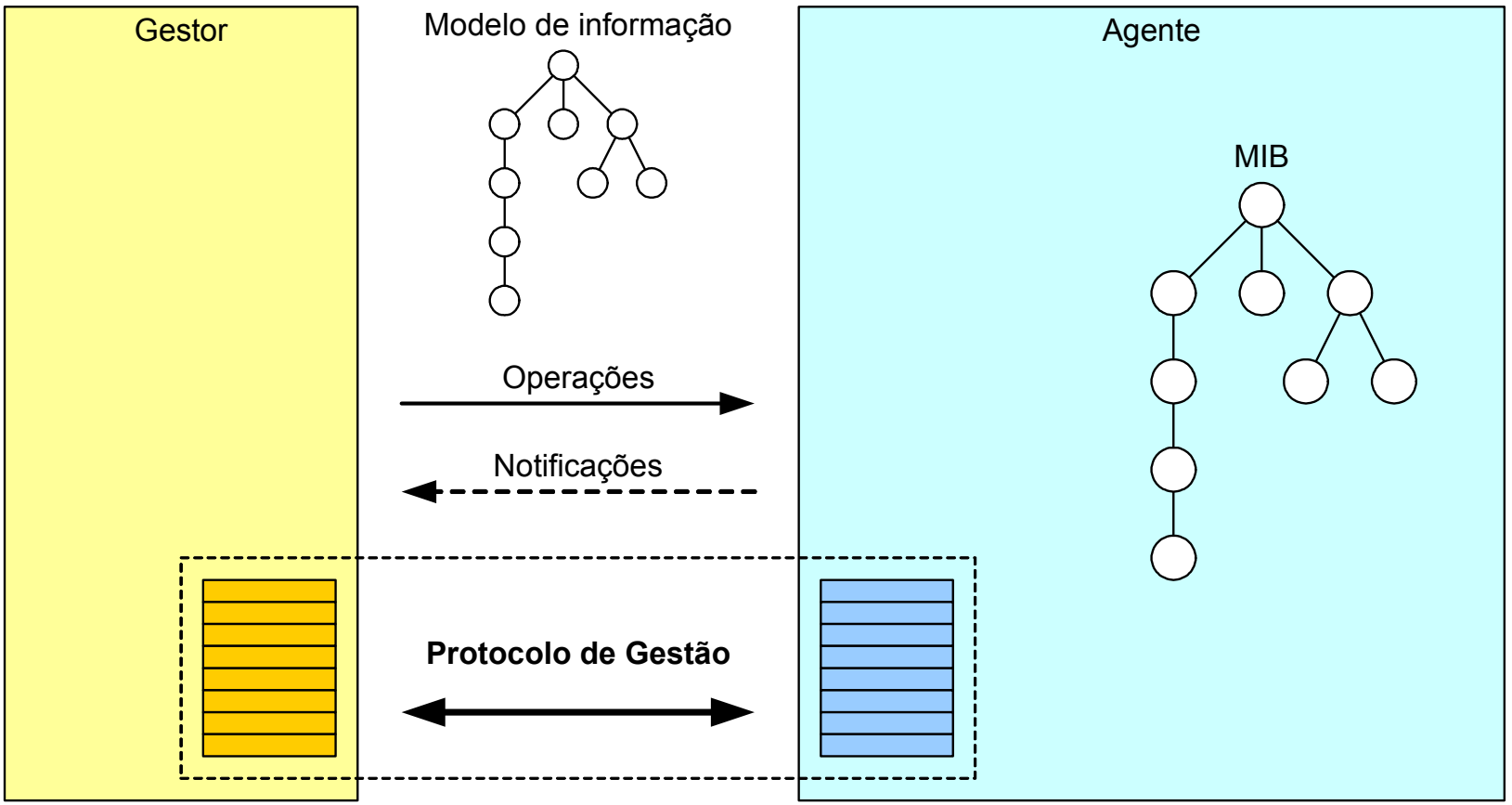


- Dispositivos geridos contêm objectos geridos cuja informação é recolhida numa Management Information Base (MIB)
- Gestor e agentes comunicam usando um protocolo de gestão

Paradigma Gestor/Agente

- Noção gestor/agente comum a todos os NMS (especialmente CMIP/SNMP)
- Corresponde a modelo cliente/servidor
  - Gestor ⇔ Cliente
  - Agente ⇔ Servidor
  - Muitos servidores e poucos clientes
- O agente opera sobre o dispositivo gerido
- O agente relata problemas ao gestor, permitindo-lhe ver e controlar toda a informação sobre o dispositivo gerido
- O gestor contém a inteligência para dar instruções aos agentes
- O gestor controla os agentes e administra o seu funcionamento

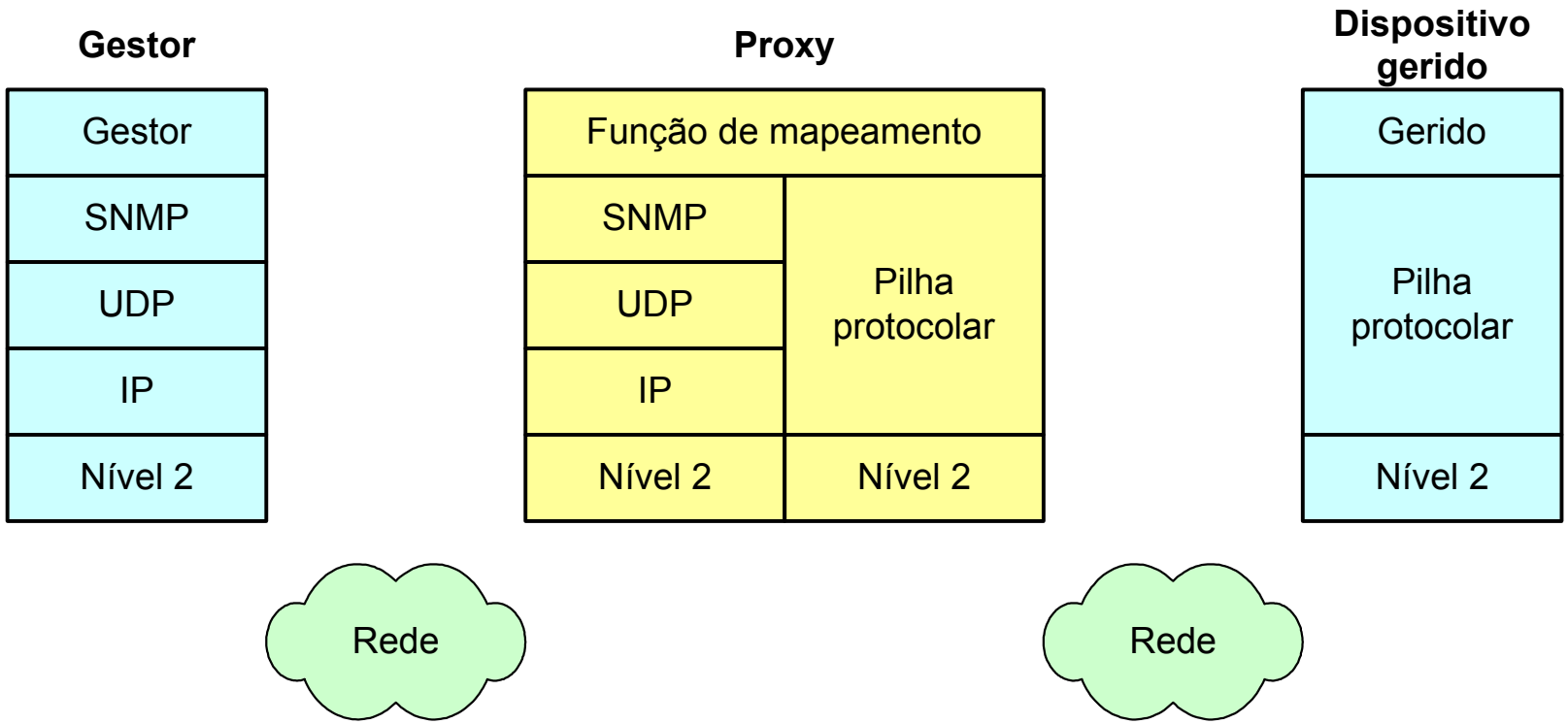
Modelo Gestor/Agente



Sistema de gestão SNMP

- Norma de facto para gestão de falhas
- Gestor SNMP + conjunto de MIBs
- Permite
  - Auto-descoberta de dispositivos na rede
  - Descoberta de falhas baseada em polling
  - Traps e gestão de eventos
  - Uso de proxies para dispositivos não-IP ou não-SNMP
  - Integração de múltiplas aplicações numa interface de gestão

Uso de proxy SNMP



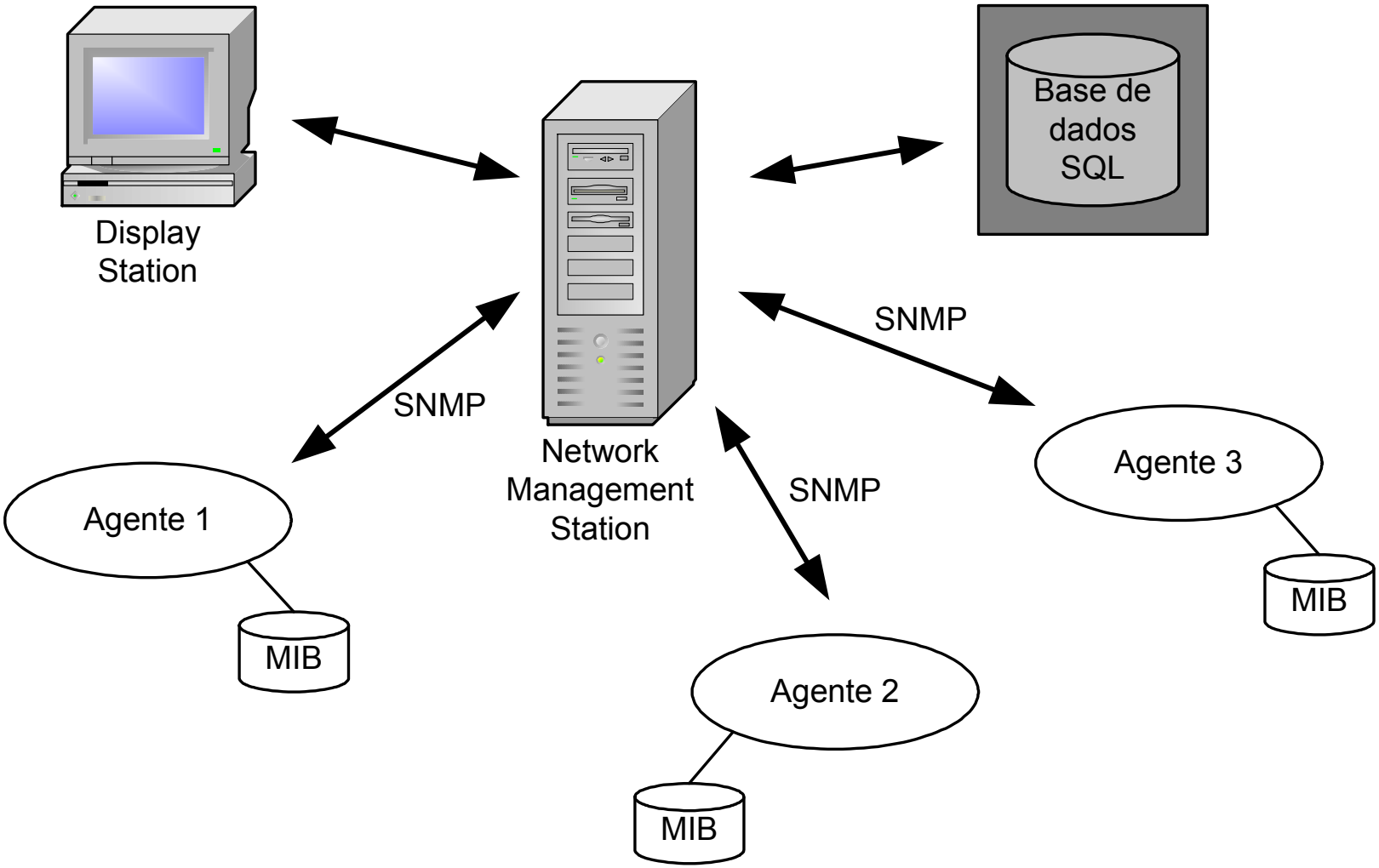
Sistema de gestão SNMP

- Um protocolo para todas as redes IP, independentemente da tecnologia nível 2
  - Funciona sobre UDP (connectionless)
- Vantagens
  - Permite gerir todas as redes
  - Uniformidade para o gestor
  - Permite gestão remota
- Desvantagens
  - Os protocolos de nível inferior têm que funcionar correctamente para entregar os pacotes de gestão
    - Se as tabelas de routing ficarem corrompidas deixa de poder usar-se

SNMP: 4 partes

- Management Information Base (MIB)
  - Base de dados distribuída com informação da rede – tabelas, campos e índices
- Structure of Management Information (SMI)
  - Linguagem de definição de dados para objectos das MIBs.
    - Uso de notação ASN.1 (BER)
- Protocolo SNMP
  - Estabelecimento de relações gestor ⇔ agente para troca de informação e comandos
- Segurança e Administração
  - Desenvolvidos recentemente, em particular no SNMPv3

Estrutura de gestão SNMP



ASN.1 – Abstract Syntax Notation

- Linguagem formal usada para descrever o que cada item é
  - "Pesada", mas essencial para suportar heterogeneidade
  - Frequente na Internet
- BER – Basic Encoding Rules
  - Especifica como transmitir dados ASN.1
  - Codificação TLV
    - Type (Tag) – Tipo de dados definido por ASN.1
    - Length – Comprimento dos dados em bytes
    - Value – Dados propriamente ditos, codificados de acordo com a sintaxe do ASN.1

ASN.1

Tipos de dados básicos

BOOLEAN(1)
INTEGER(2)
REAL(9)
    mantissa, base, expoente
BITSTRING(3), OCTETSTRING(4)
NULL(5)
ENUMERATED(10)

Exemplos:

```
brainDamaged ::= BOOLEAN
numberOfEmployees ::= INTEGER
avogadrosNumber ::= REAL(602,10,23)
sevenDeadlySins     ::= ENUMERATED {
    pride(1), envy(2), gluttony(3),
    avarice(4), lust(5), sloth(6),
    wrath(7)
}
```

Tipos de dados estruturados

SET(17)
SET OF(17)
SEQUENCE(16)
SEQUENCE OF(16)
CHOICE(11)
ANY

Exemplos:

```
messageBodyPart    ::= CHOICE {
    [0] IMPLICIT asciiText,
    [1] IMPLICIT telex
    ...etc... }
```

ASN.1

- Tipos de dados derivados: exemplos

Month ::= INTEGER (1..12)
Day ::= INTEGER (1..31)
Daily-temperatures ::= SEQUENCE SIZE (31) OF INTEGER

Name ::= PrintableString (SIZE (1..20))

- Tipos de tags
  - UNIVERSAL
    - Todos os tipos básicos
  - APPLICATION
    - Únicos para cada aplicação
  - CONTEXT-SPECIFIC
    - Únicos dentro de um outro tipo
  - PRIVATE

Basic Encoding Rules – BER

- Tag (type)
- Length
  - Definido (1 byte)
  - Indefinido (mais bytes)
- Value
  - Codificado conforme apropriado (ASN.1)

Exemplos:

Valor booleano verdadeiro

1	1	1

O inteiro -5 (complemento para 2)

2	1	11111011

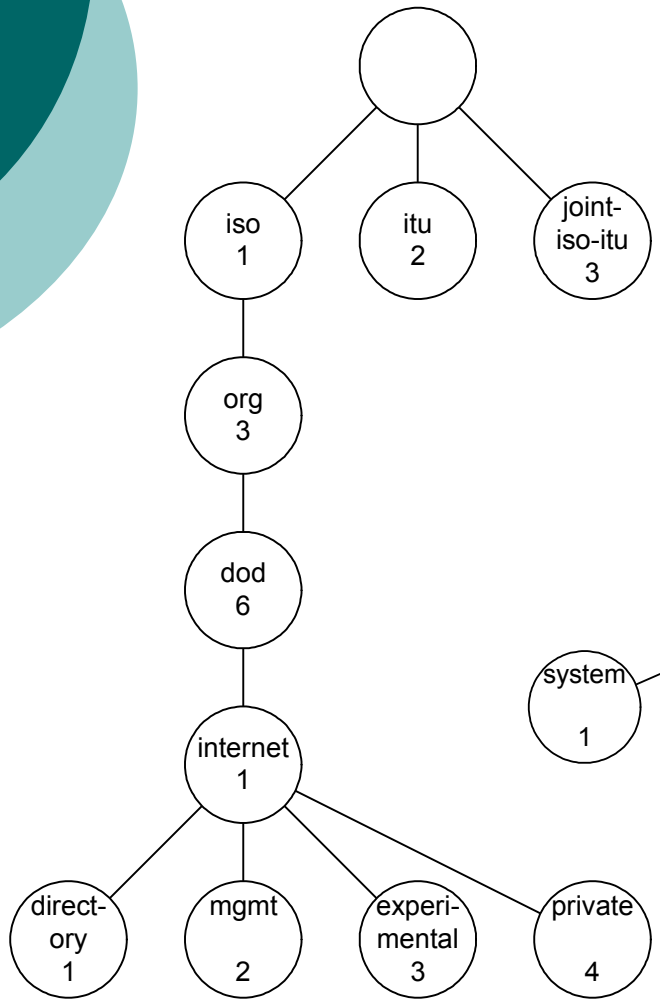
String “foo”

4	3	f	o	o

Structure of Management Information (SMI)

- Linguagem de definição de dados
- Usa ASN.1/BER
- Tipos de dados básicos (SMIv2)
  - INTEGER, Integer32, Unsigned32, OCTET STRING, OBJECT IDENTIFIED, IpAddress, Counter32, Counter64, Gauge32, TieTicks, Opaque
- Usada para definir MIBs
  - Estrutura em árvore
    - Nós identificados pelo Object ID (OID)
    - Nome associado
    - Exemplo:
      - 1.3.6.1.2.1.4.20 => ipAddrTable
  - Permite identificação unívoca de todo e qualquer objecto

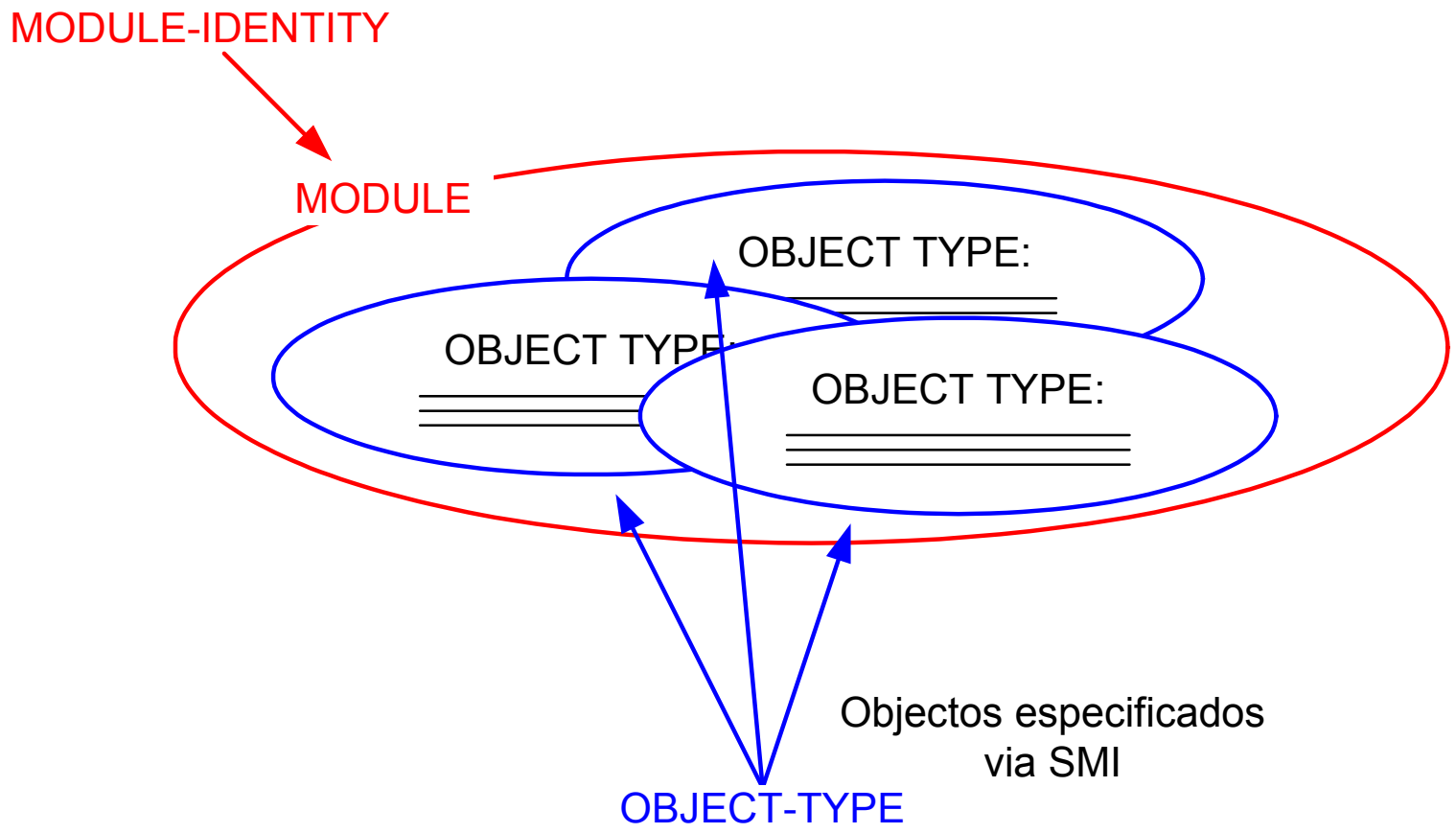
Estrutura e representação de MIBs



Management Information Base (MIB)

- Definidas usando SMI
- Usada para definir informação extraída dos dispositivos
- Conjunto de objectos geridos
  - Organização em árvore (OIDs)
  - Estrutura dos dados independente da implementação
    - Agente faz a conversão
- Tipos de módulos em MIBs
  - Standard
  - Experimental
  - Enterprise-specific (proprietárias)
- Algumas MIBs importantes
  - MIB-2 (MIB genérica TCP/IP)
  - RMON, RMON2 (Remote Monitoring)
    - Gestão não de um dispositivo mas da própria rede
    - Uso de probes

MIBs – Objectos e módulos



Exemplos de objectos e módulos

OBJECT-TYPE:
ipInDelivers

```
ipInDelivers OBJECT-TYPE
 SYNTAX  Counter32
 MAX-ACCESS  read-only
 STATUS  current
 DESCRIPTION
    "The total number of
    input datagrams
    successfully delivered to
    IP user-protocols
    (including ICMP)
::={ip 9}
```

MODULE-IDENTITY:
ipMIB

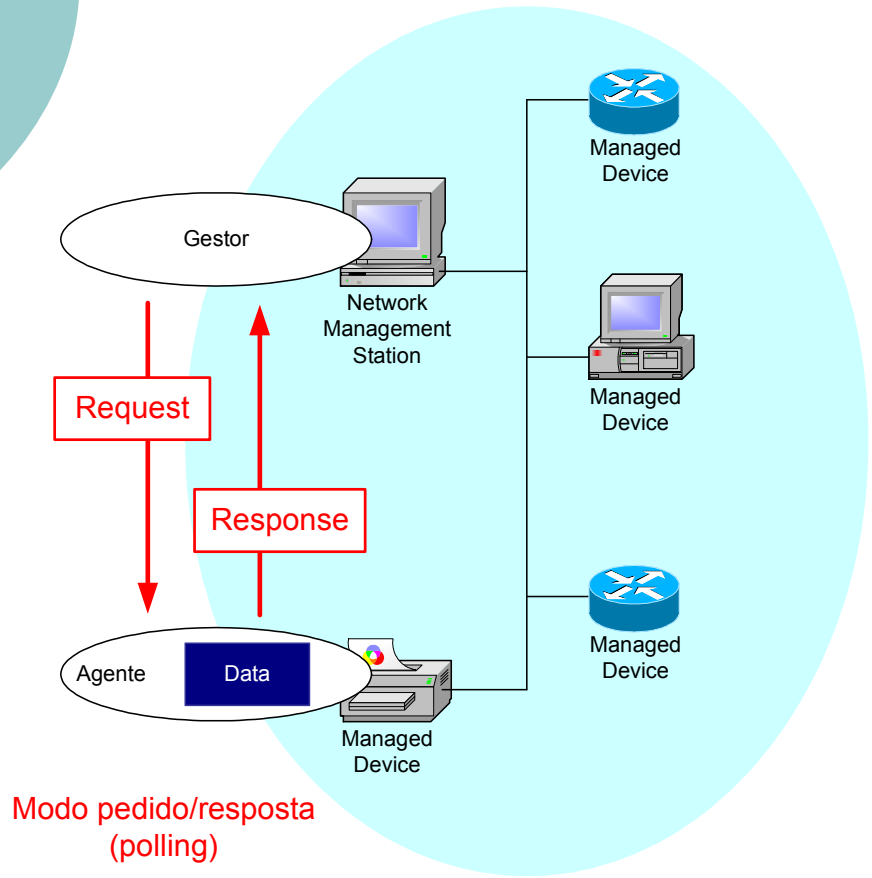
```
ipMIB MODULE-IDENTITY
 LAST-UPDATED "9411001000Z"
 ORGANIZATION "IETF SNMPv2
    Working Group"
 CONTACT-INFO "John Doe ....."
 DESCRIPTION
    "The MIB module for
    managing IP and ICMP
    implementations, but
    excluding their management
    of IP routes"
 REVISION "019331000Z"
 ........
::={mib-2 48}
```

Exemplo de MIB: Módulo UDP

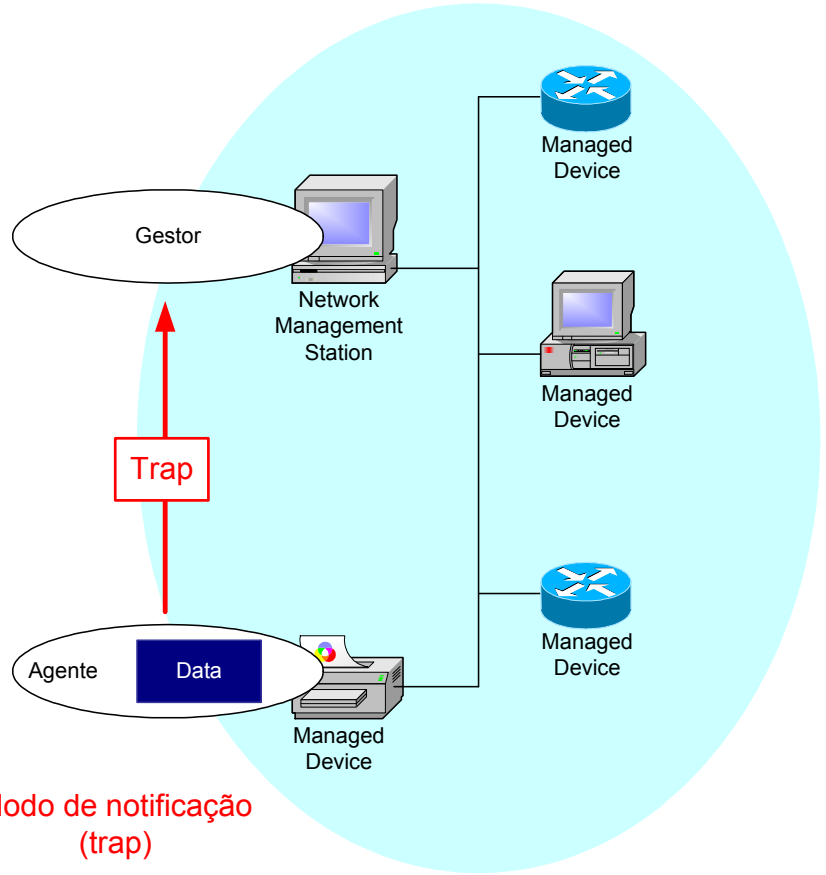
OID	Nome	Tipo	Comentários
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams no app at portl
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port in use by app, gives port # and IP address

Transferência de informação em SNMP

Dois mecanismos:



Modo pedido/resposta (polling)



Modo de notificação (trap)

SNMP: Polling

- Gestor interroga periodicamente o agente relativamente a nova informação
- Vantagens
  - O gestor controla completamente o dispositivo
  - O gestor conhece todos os detalhes da rede
- Desvantagens
  - Atraso entre a occorrência do evento e a sua detecção
  - Overhead de comunicação desnecessário:
    - Polling lento $\Rightarrow$ resposta lenta aos eventos
    - Polling rápido $\Rightarrow$ desperdício de largura de banda

SNMP: Traps

- Ocorrência de evento despoleta envio de trap
- Trap contém informação apropriada
  - Nome do dispositivo
  - Instante de ocorrência do evento
  - Tipo de evento
- Vantagem
  - A informação só é gerada quando necessário
- Desvantagens
  - Necessários mais recursos no dispositivo gerido
  - Se ocorrerem muitos eventos pode haver desperdício de LB (resolve-se com limiares)
  - Agente tem visão limitada da rede, pelo que o NMS pode já ter conhecimento dos eventos
- Traps + polling
  - Ocorrência de evento $\Rightarrow$ Envio de Trap
  - Gestor obtém mais informação por polling
  - Polling periódico como backup

SNMP: Tipos de mensagens

Tipo	Função
Get GetNext GetBulk (v2)	G➔A: pedido de dados (instância, próximo, bloco) GetNext permite walk
Inform (v2)	G➔G: valor da MIB
Set	G➔A: definição de valores (atómica)
Response	A➔G: valor (em resposta a um pedido)
Trap	A➔G: informa gestor de ocorrência de um evento

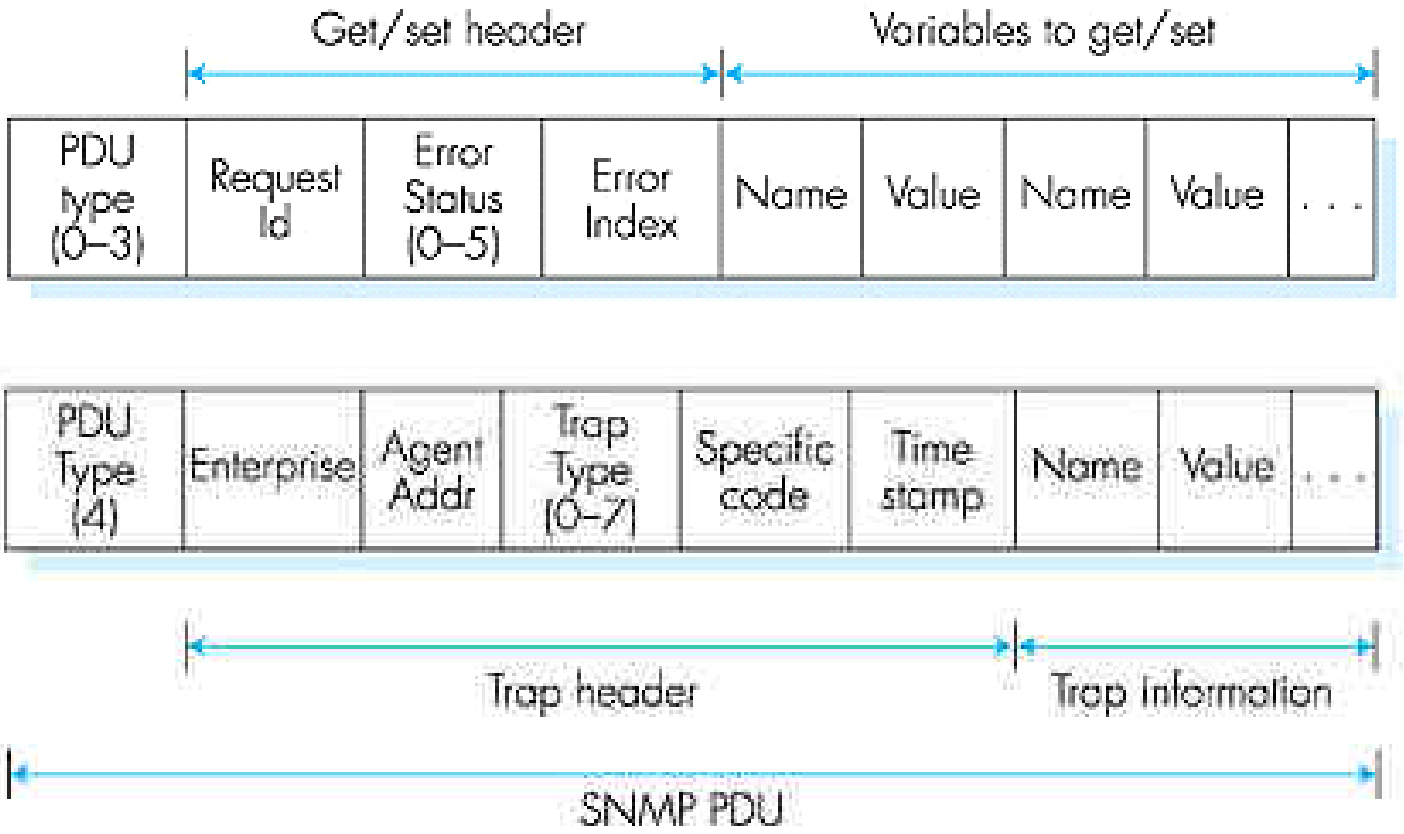
Mensagens SNMP

- Conteúdo
  - Versão
  - Community string (“password”)
  - Um ou mais PDUs SNMP
- PDU SNMP
  - Request ID (número de sequência)
  - Error Status
  - Error Index (se ≠ 0 indica o índice do OID que causou o erro)
  - Lista de OIDs e valores
    - Valores são Null para GETs
- Trap PDU
  - Enterprise (tipo de objecto que originou o trap)
  - Agent address (endereço do agente que o envia)
  - Generic trap type
  - Specific code
  - Time stamp
  - Lista de OIDs e valores (relevantes para o NMS)

SNMP: Formato das mensagens

Get, Set, Response

Trap



SNMP – Exemplo de mensagem

get-request para o objecto sysDescr (1.3.6.1.2.1.1.1)

```
   30      29      02     01    00
SEQUENCE len=41 INTEGER len=1 vers=0

   04     06   70  75  62  6C  69  63
string  len=6   p   u   b   l   i   c

   A0     1C    02     04   05 AE 56 02
getReq len=28 INTEGER len=4   -req ID-

   02     01    00      02     01   00
INTEGER len=1 status INTEGER len=1 index

   30      0E      30      0C   06   08
SEQUENCE len=14 SEQUENCE len=12 OID len=8

 2B  06  01  02  01  01  01  00
1.3 . 6 . 1 . 2 . 1 . 1 . 1 . 0

 05    00
NULL len=0
```

SNMP: Segurança e autenticação

- Na versão inicial, baseadas apenas na "community string"
  - Community strings identificam permissões: read-only ou read-write
    - Case-sensitive
  - Valores default
    - "public" ➔ read-only
    - "private" ➔ read-write
  - Circulam não-cifradas na rede...
- Novas versões (v2 e v3)
  - Controlo de acesso dependendo do utilizador
    - Agente mantém informação de direitos de acesso para diferentes utilizadores numa BD
    - BD acessível como objecto gerível
  - Suporte de cifragem – Uso de DES
  - Autenticação – Chave secreta partilhada
  - Protecçao contra repetições – Uso de *nounces*

MIBs e acesso SNMP

Categoria de acesso de MIB	Modo de acesso SNMP	
	Read-only	Read-write
Read-only	get, trap	get, trap
Read-write	get, trap	get, trap, set
Write-only	get, trap (depende da implementação)	get, trap, set (depende da implementação)
Not accessible	Inacessível	