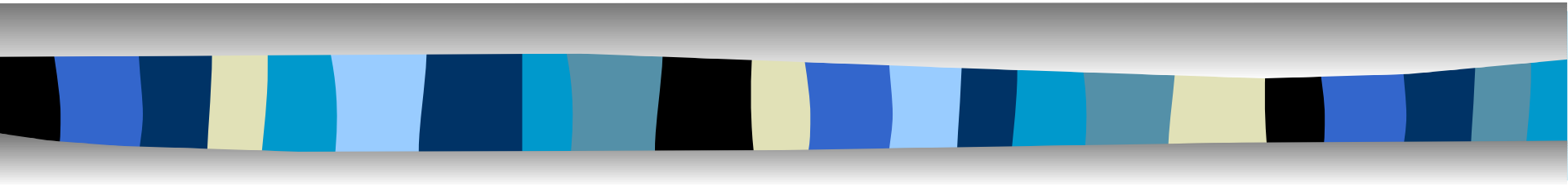
Gerência de Redes
Aula 04 - O protocolo SNMP



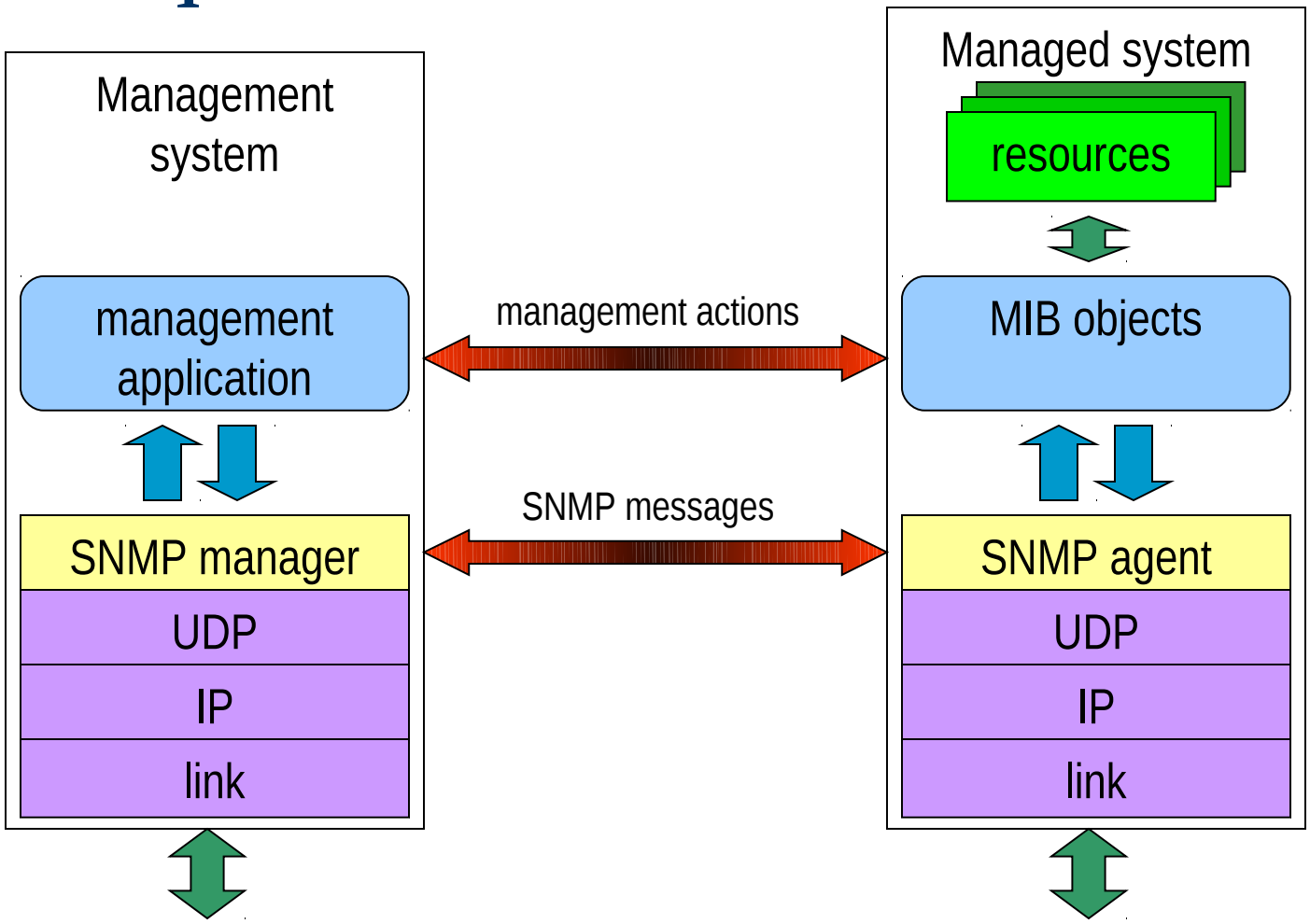
Prof. Carlos Maziero, PhD

DAINF – Departamento Acadêmico de Informática
UTFPR – Universidade Tecnológica Federal do Paraná

O protocolo SNMP

- Veicula informações de gerência
  - transporte de valores das MIBs
- Interações sem conexão
  - Mensagens em UDP/IP
  - portas 161 e 162
  - pacotes de tamanho variável
- Mensagens auto-contidas
  - formato Type - Length - Value

A arquitetura SNMP



Histórico do SNMP

- 1989: SNMP v1
- 1992: Remote Monitoring - RMON
- 1993: SNMP v2
- 1996: SNMP v2c (Community Security)
- 1996: MIB RMON v2
- 1998: SNMP v3 (User Security Model)

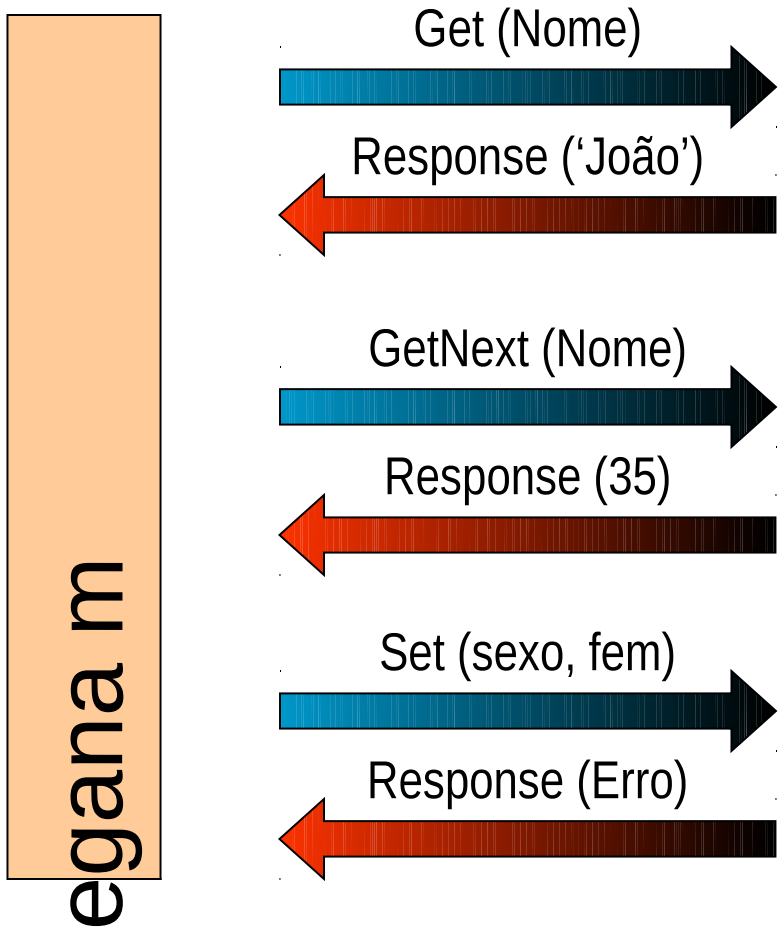
Operações básicas SNMP

- GET
- GET-NEXT
  - gerente busca informações dos agentes
  - acessos em leitura às MIBs
- SET
  - gerente modifica informações dos agentes
  - acessos em escrita às MIBs
- TRAP
  - agentes enviam informações não solicitadas aos gerentes, informado eventos importantes

Restrições das operações

- Permitem somente inspeção e/ou alteração de variáveis
- A estrutura da MIB não pode ser alterada pelas operações
- Somente podem ser acessados valores escalares em cada operação

Exemplo de uso



SNMP Agent MIB

pessoa.nome = João
pessoa.idade = 35
pessoa.sexo = masc

Modelo de segurança SNMP

- Modelo mais comum: SNMP V2C
- Baseado no conceito de comunidade
- Uma comunidade define:
  - método para autenticar acesso (senha)
  - visibilidade da MIB
  - privilégios de acesso à MIB
- Cada dispositivo implementa uma ou mais comunidades
- Comunidade default: “public”

Serviço de autenticação

- Cada mensagem SNMP é autenticada
  - Nome da comunidade serve de senha
  - Sistema de segurança frágil e limitado
- Muitas vezes a operação SET é proibida
- Certos dispositivos regulam acesso usando:
  - nome da comunidade
  - número IP do(s) gerente(s)

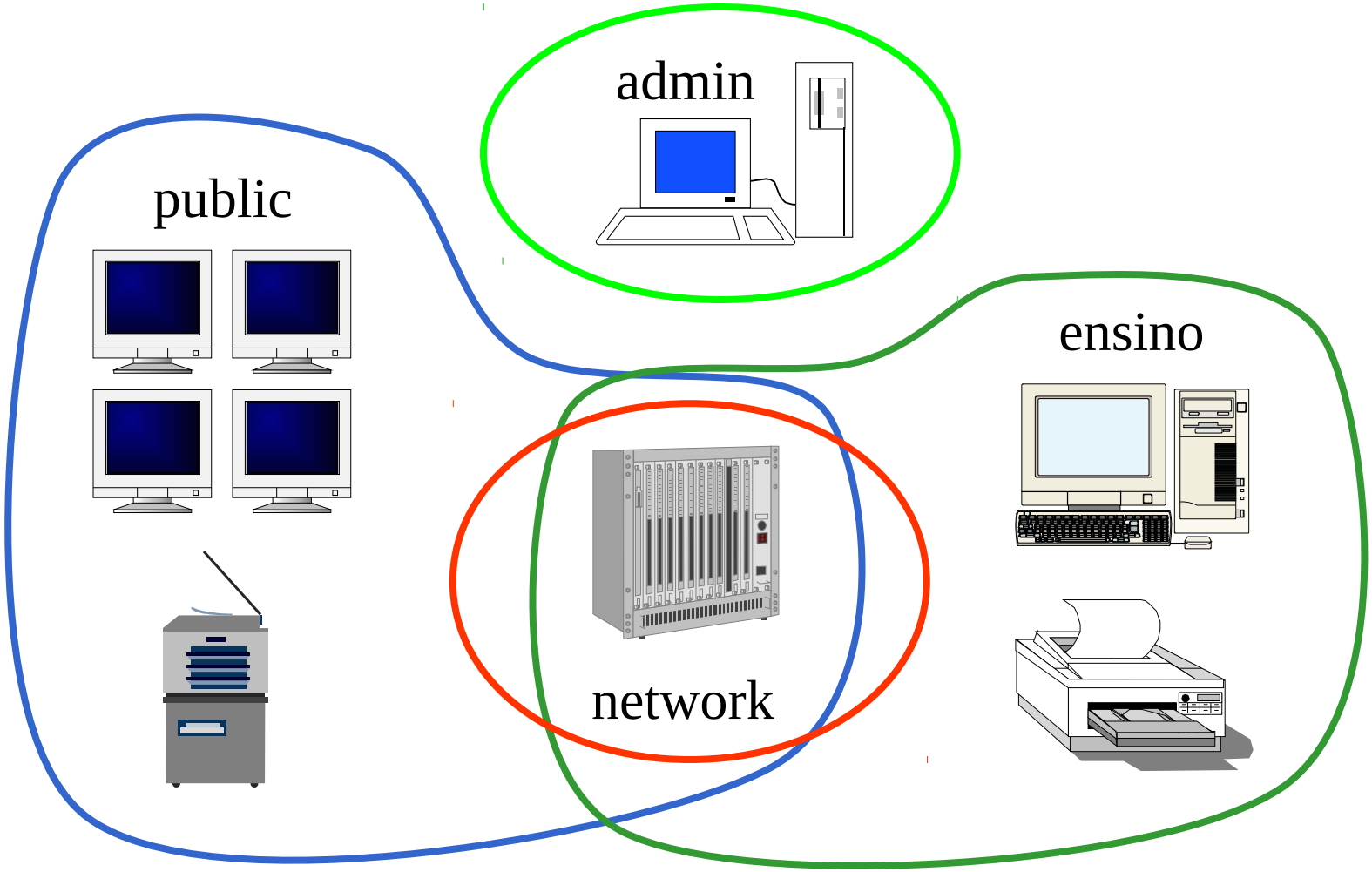
Política de acesso

- Aspectos da política de acesso:
  - **visão da MIB**: que partes da MIB podem ser acessadas.
  - **Modo de acesso**: pode ser em leitura ou leitura/escrita.
  - Ambas definem um perfil "**perfil de comunidade**".
  - O modo de acesso não deve conflitar com os campos ACCESS definidos na MIB.
- Um dispositivo pode implementar várias comunidades, com diversas políticas de acesso.

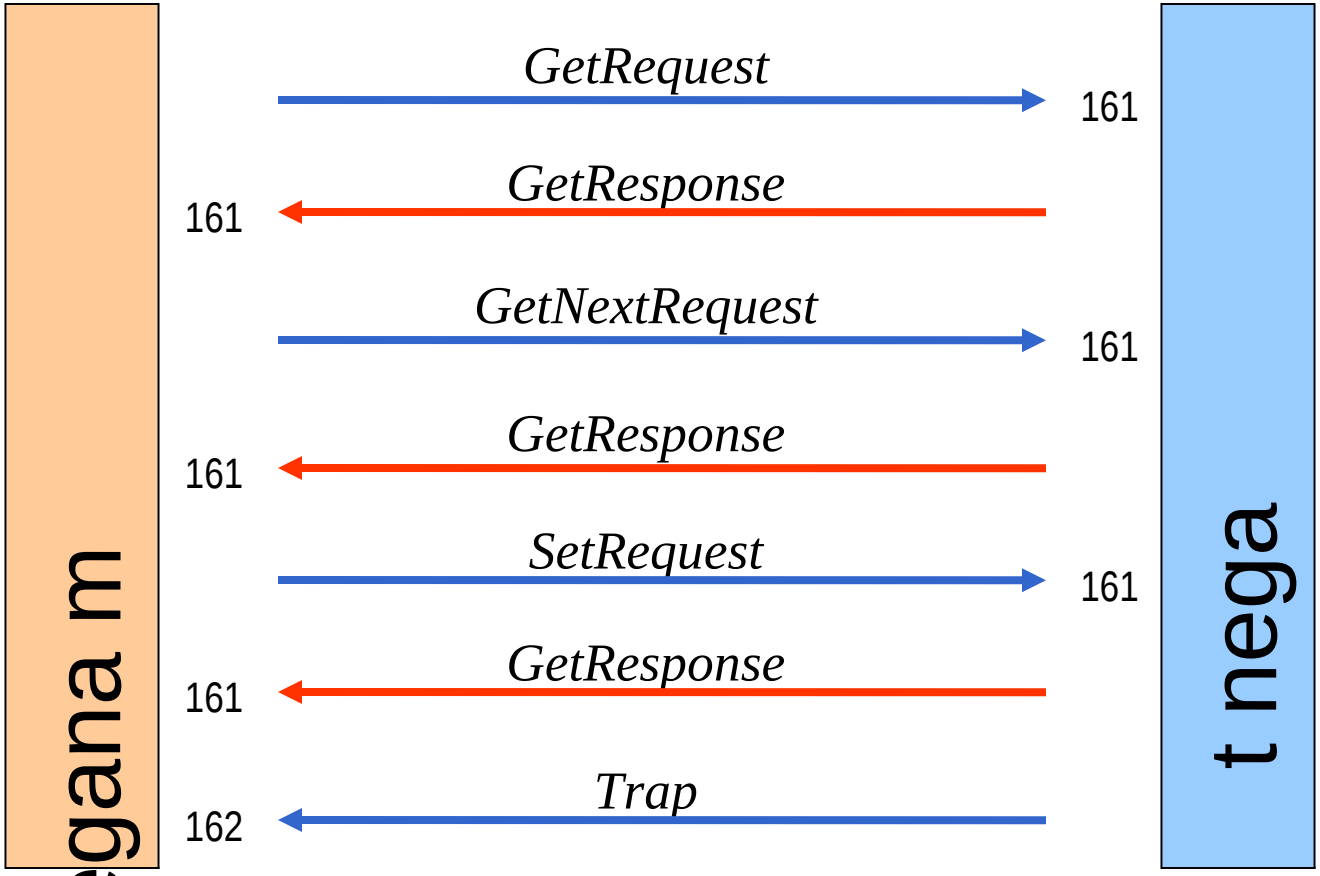
Acesso SNMP X acesso MIB

MIB ACCESS	SNMP access control: READ-ONLY	SNMP access control: READ-WRITE
read-only	*available for GET & TRAP operations*	
read-write	*available for GET & TRAP operations,*	*available for GET SET TRAP operations*
write-only	*available for GET & TRAP operations, but value is implementation specific*	*available for GET SET & TRAP operations, but value is implementation specific for GET & TRAP*
not accessible	*unavailable*	

Exemplo de comunidades

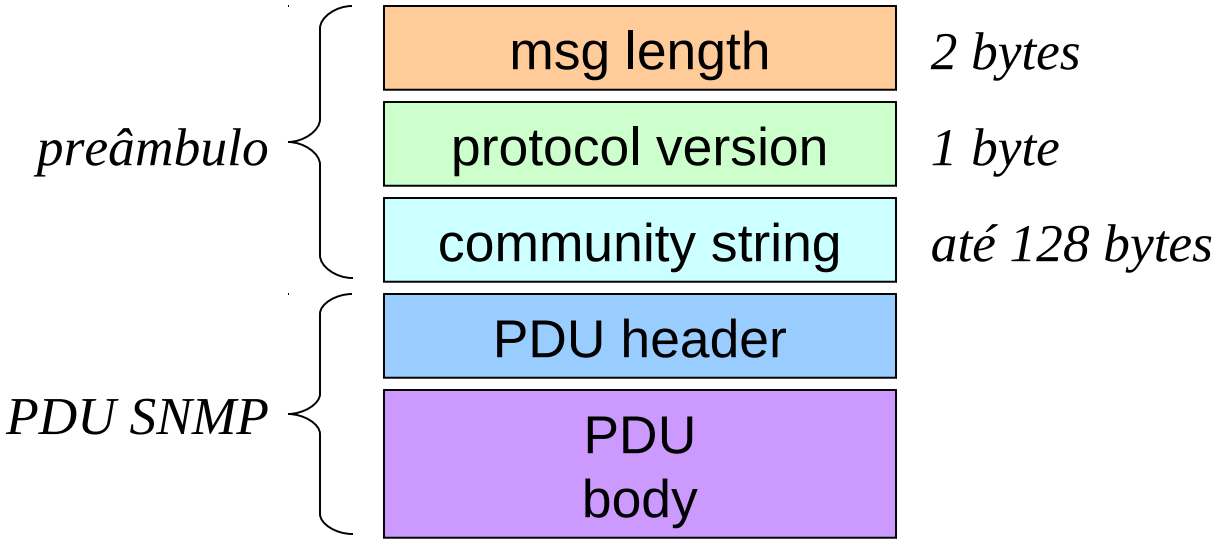


As PDUs SNMP

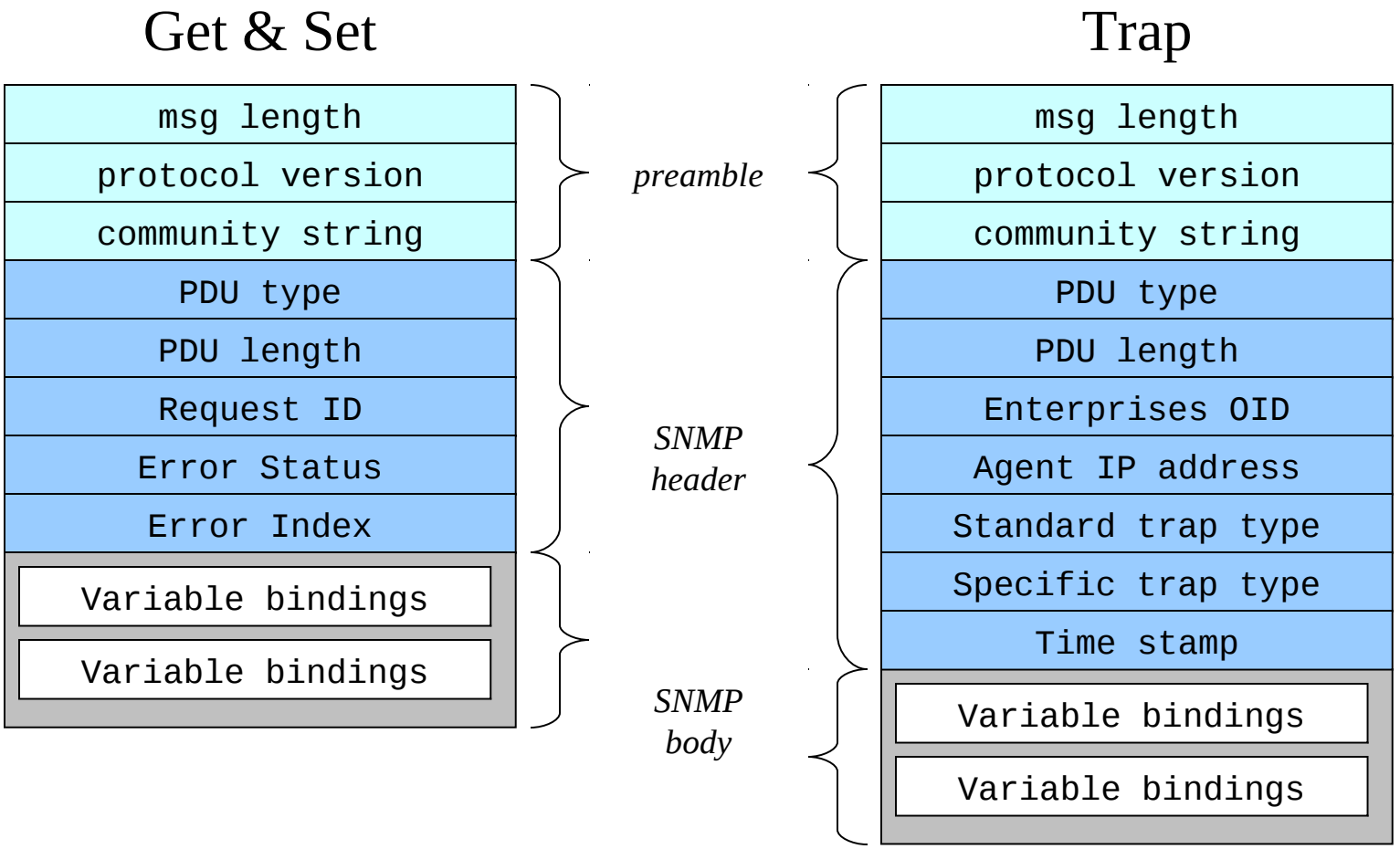

r egana m
t nega
GetRequest
161
GetResponse
161
GetNextRequest
161
GetResponse
161
SetRequest
161
GetResponse
161
Trap
162

Uma mensagem SNMP

- Conteúdo codificado via BER
- Geralmente limitada a < 484 bytes



Estrutura das PDUs SNMP



Preâmbulo e cabeçalho

- Versão
  - 0: SNMPv1, 1: SNMPv2, ...
- Tipo de PDU
  - 0: getRequest
  - 1: getNextRequest
  - 2: getResponse
  - 3: setRequest
  - 4: trap
- Request ID
  - valor numérico usado para casar pedidos e respostas

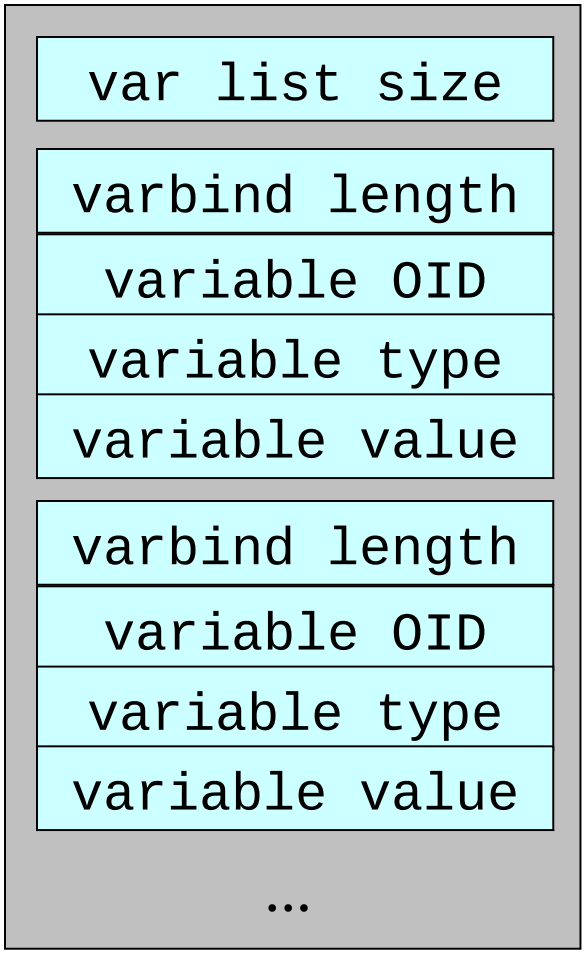
Códigos de erro

- Error Status:

  0: *noError*: sucesso na operação
  1: *tooBig*: resposta muito grande para enviar
  2: *noSuchName*: *OID* não suportado pelo agente
  3: *badValue*: valor incorreto para operação *set*
  4: *readOnly*: tentativa de escrita inválida
  5: *genErr*: erro não relacionado ao protocolo

- Error index:
  - indica qual variável listada na PDU causou o erro.

Conteúdo das mensagens



41
23
1.3.6.1.2.1.1.2.0
2
1.3.6.1.4.1.311.1.1.3.2
14
1.3.6.1.2.1.7.4.0
65
250

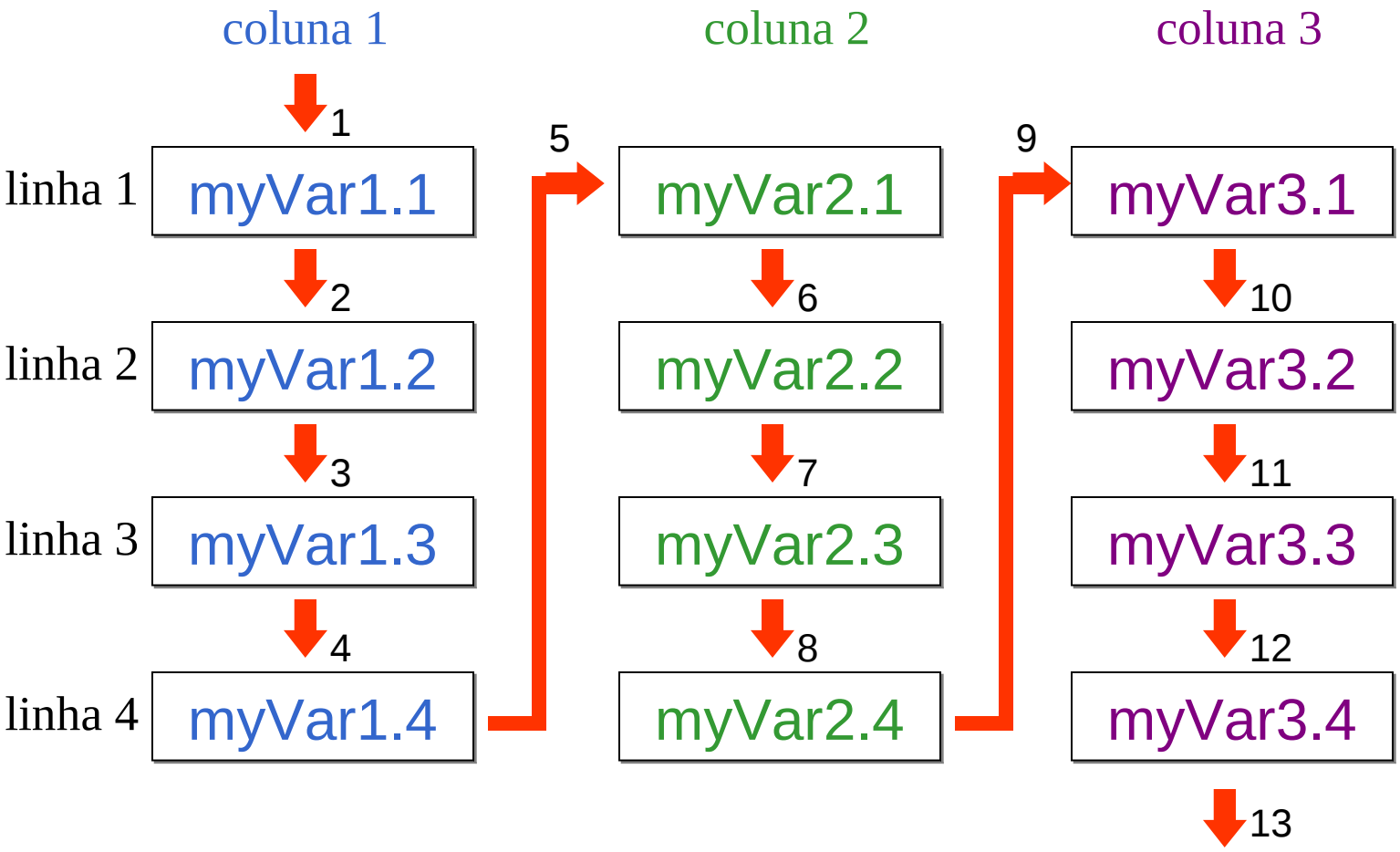
A operação *GetNext*

- Busca próximo elemento na MIB
  - Usa ordem lexicográfica
    - 1.3.6.1.2.1.1.4
    - 1.3.6.1.2.1.1.4.0
    - 1.3.6.1.2.1.1.5.0
    - ...
- Serve para:
    - passear na MIB (descoberta da estrutura)
    - buscar dados em tabelas

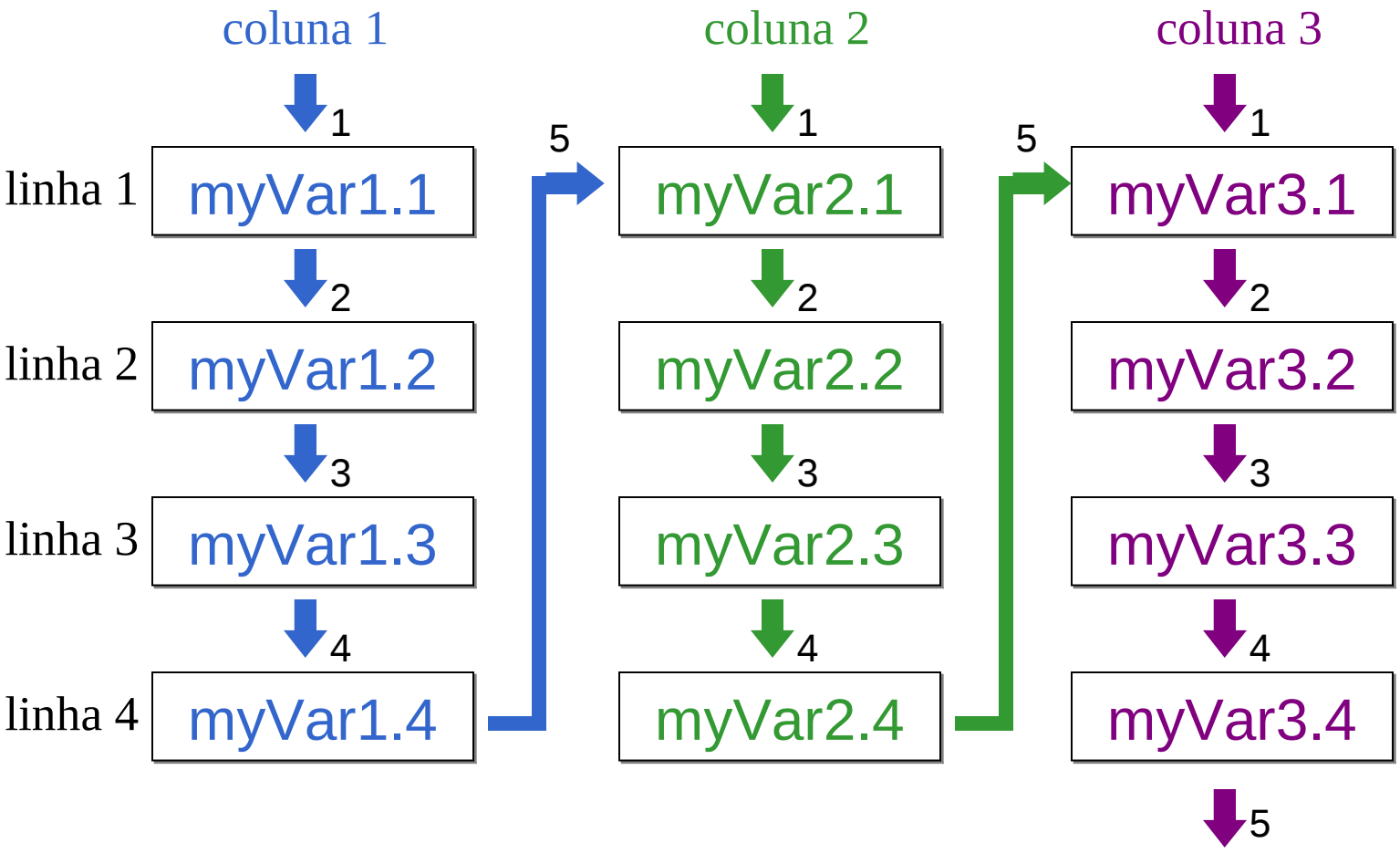
Exemplo de passeio na MIB

```
snmpgetnext sigma.pucpr.br public system
   system.sysDescr.0 = OCTET STRING: "Image: rel/11.02 Created ..."
snmpgetnext sigma.pucpr.br public system.sysDescr.0
   system.sysObjectID.0 = OBJECT IDENTIFIER: enterprises.18.3
snmpgetnext sigma.pucpr.br public system.sysObjectID.0
   system.sysUpTime.0 = Timeticks: (2703290) 7:30:32
snmpgetnext sigma.pucpr.br public system.sysUpTime.0
   system.sysContact.0 = OCTET STRING: "Jurandir - RIEP"
snmpgetnext sigma.pucpr.br public system.sysContact.0
   system.sysName.0 = OCTET STRING: "BLN - PUC-PR"
snmpgetnext sigma.pucpr.br public system.sysName.0
   system.sysLocation.0 = OCTET STRING: "Biblioteca Central - Campus I"
snmpgetnext sigma.pucpr.br public system.sysLocation.0
   system.sysServices.0 = INTEGER: 78
snmpgetnext sigma.pucpr.br public system.sysServices.0
   interfaces.ifNumber.0 = INTEGER: 1
...
```

Percurso seqüencial



Percurso paralelo



Exemplo: uma tabela fictícia

animalTable.animalEntry

animalIndex	*animalName*
1	Cow
4	Mouse
7	Horse
9	Dog

Percorrendo a tabela (1)

- getNextRequest 1:
  - OID:`animalTable.animalEntry`
  - Value: `NULL`
  - OID:`animalTable.animalEntry.animalName`
  - value: `NULL`
- getNextResponse 1:
  - OID:`animalTable.animalEntry.1`
  - Value: `1`
  - OID:`animalTable.animalEntry.animalName.1`
  - Value: “`Cow`”

Percorrendo a tabela (2)

- getNextRequest 2:
  - OID:`animalTable.animalEntry.1`
  - Value: `NULL`
  - OID:`animalTable.animalEntry.animalName.1`
  - value: `NULL`

- getNextResponse 2:
  - OID:`animalTable.animalEntry.4`
  - Value: `4`
  - OID:`animalTable.animalEntry.animalName.4`
  - Value: “`Mouse`”

Traps em SNMP

- Mensagens enviadas pelo agente
- Não são respostas a pedidos
- Representam eventos anormais
- Classificam-se em:
  - genéricos: presentes na MIB padrão
  - específicos: definidos na MIB “enterprises”

Traps genéricos

- *coldStart*:
  - o dispositivo foi ligado
  - configuração local pode ter sido alterada
  - informa ao gerente sobre sua existência
- *warmStart*:
  - o dispositivo foi reinicializado
  - configuração local não foi alterada
- *linkDown*:
  - link ou porta de comunicação ligada ao nó falhou

Traps genéricos (2)

- *linkUp*:
  - link ou porta local foi (re)ativada.
- *authenticationFailure*:
  - o dispositivo recebeu msg SNMP não autorizada
  - comunidade não reconhecida
  - número IP de gerente inválido
- *egpNeighborLoss*:
  - *Exterior Gateway Protocol* falhou no nó
  - normalmente usado em roteadores

SNMP e Windows

- Suporte a SNMP no Windows:
  - Serviço Win32 opcional
  - Windows NT: agente e/ou gerente
  - Windows 95/98: somente agente
  - Somente SNMPv1
- No Windows NT 5.0:
  - integração completa ao modelo SNMP
  - suporte completo a SNMP v1 e SNMP v2c
  - API WinSNMP engloba MGMT-API
  - IP helper API
  - Conjunto maior de MIBs (host, forwarding, ...)

SNMPv2

- Definido em 1993 (RFC)
- Suporte flexível:
  - gerência centralizada
  - gerência distribuída
- Modificações mais significativas:
  - estrutura de informação (SMI)
  - interações “gerente a gerente”
  - operações do protocolo

SMI em SNMPv2

- Super-conjunto da SMI em SNMPv1
- Especificação e documentação mais elaboradas dos objetos da MIB
- Novos conceitos:
  - definições de novos objetos
  - tabelas conceituais
  - novas definições de notificações
  - módulos de informação

Definições de objetos

- Melhor definição de OBJECT-TYPE
- Novos tipos de dados:
  - Counter32
  - Unsigned64
- Remoção de ambigüidades de SNMPv1
- Novas interpretações de alguns tipos:
  - Gauge32
  - Counter64

Cláusula MAX ACCESS

- Similar a ACCESS, enfatizando que o acesso não pode ser modificado por configuração do agente
- Níveis de acesso:
  - not accessible
  - accessible for notify
  - read only
  - read-write
  - read-create (tabelas conceituais)

Cláusula STATUS

- Novos status:
  - current
  - deprecated
  - obsolete
- Desaparecem:
  - mandatory
  - optional

Tabelas

- Duas categorias de tabelas:
  - estrutura fixa
  - estrutura alterável
- Criação/deleção de linhas
  - operações pelo gerente, via SNMP
  - extremamente complexo e controverso
  - segue o modelo adotado em RMON

O protocolo SNMPv2

- Três formas de interação
  - manager to agent, request/response
  - agento to manager, unconfirmed
  - manager to manager, request/response

- o último é definido em SNMPv2

PDUs SNMPv2

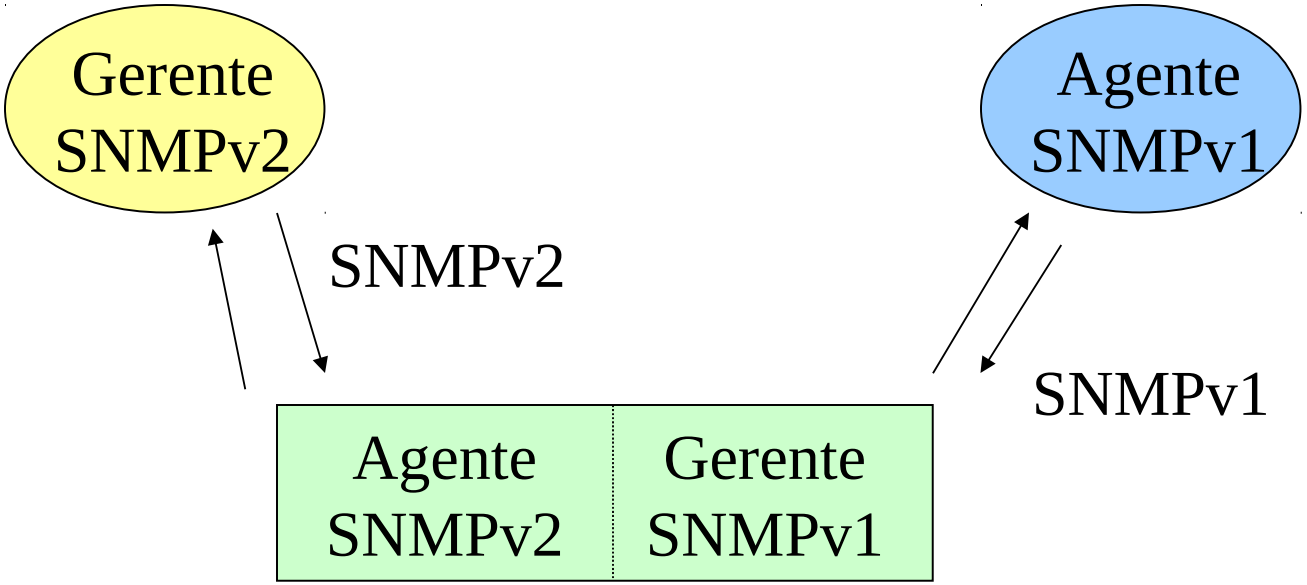
- GetRequest, GetNextRequest
  - similar à de SNMPv1
  - resposta não é mais atômica
- SetRequest
  - idem
- GetBulkRequest
  - busca de grandes blocos de dados
  - equivale a um GetNextRequest múltiplo

PDUs SNMPv2

- InformRequest
  - comunicação entre gerentes
  - enviado pelo gerente que deseja enviar a informação
  - resposta ResponsePDU sem conteúdo.
- ReportPDU
  - não utilizada (abandonada nas RFCs)

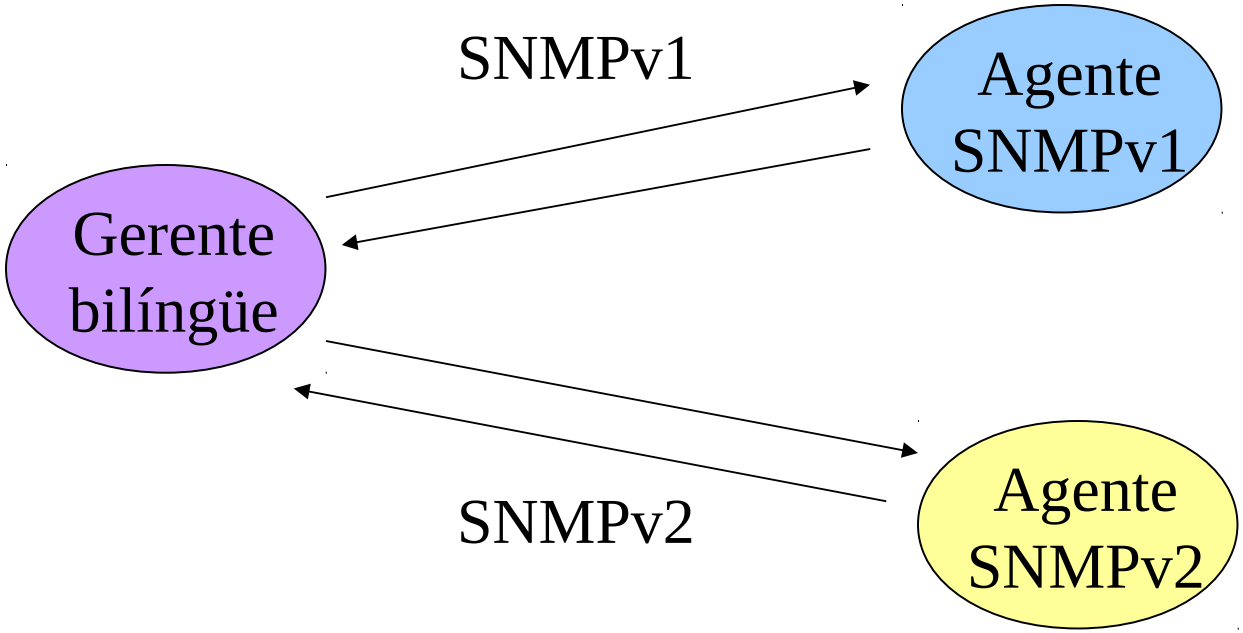
Coexistência de SNMPv1 e v2

- Por proxies SNMP



Coexistência de SNMPv1 e v2

- Por gerentes bilíngues



Leitura complementar

- Capítulo 4 do “*Murray*”
- Capítulo 4 do “*Miller*”
- Capítulo 7 do “*Stallings*”