



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Gerência e Segurança de Redes

Modelos

filipe.raulino@ifrn.edu.br

SNMP e CMIP

- **SNMP x CMIP**

- O ambiente de gerenciamento OSI é composto por gerentes, agentes e objetos gerenciados.
- Um gerente transmite operações de gerenciamento aos agentes a fim de obter informações atualizadas sobre os objetos gerenciados e controlá-los.
- Um agente recebe as operações de gerenciamento emitidas pelo gerente e executa as ações necessárias sobre os objetos gerenciados.

CMIP

- **CMIP (Common Management Information Protocol)**
- CMIS -> define os serviços para operações de gerenciamento
- CMIP -> define procedures para a transmissão de informações de gerenciamento e define a sintaxe para o serviço de gerenciamento do CMIS.

As 11 PDUs que o CMIP utiliza:

- m-EventReport
- m-EventReport-Confirmed
- m-Get
- m-Linked-Reply
- m-Set
- m-Set-Confirmed
- m-Action
- m-Action-Confirmed
- m-Create
- m-Detete
- m-Cancel-Get-Confirmed

CMIP

Vantagens do CMIP

- O CMIP é um sistema muito mais seguro, como isto foi construído nos dispositivos de gerenciamento de segurança.
- O protocolo CMIP foi fundado por grandes corporações e governo.

Desvantagens do CMIP

- O protocolo CMIP utiliza muito mais recursos de sistema do que o SNMP.
- Isto significa que muito poucos sistemas tem capacidade para manipular uma implementação completa do CMIP.
- CMIP é muito difícil para programar, ele possui muitas variáveis dificultando para o programador o conhecimento de todas elas.

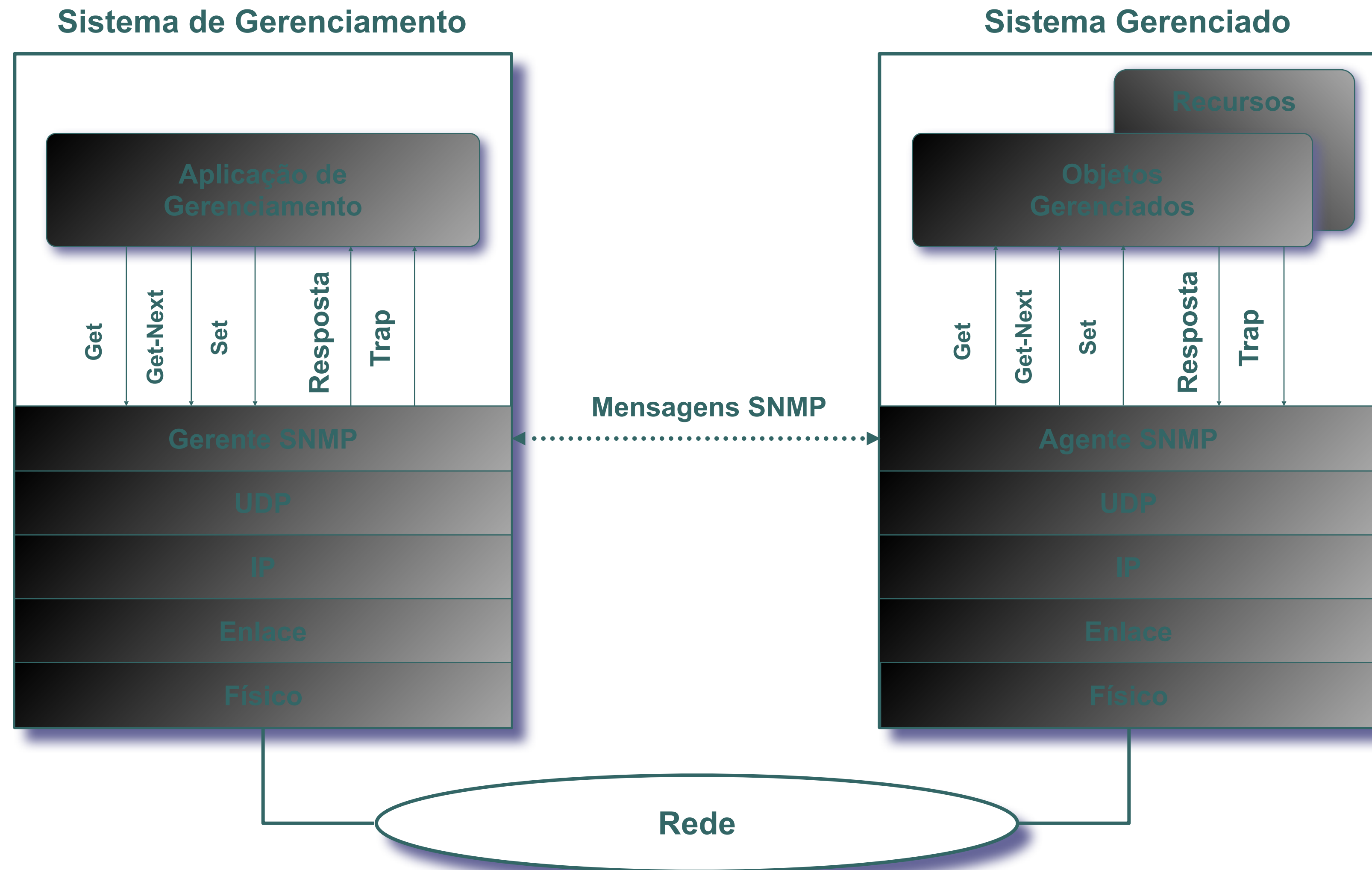
Comparação entre SNMP e CMIP

- O elemento SNMP agente é muito mais simples do que o CMIP
- As duas arquiteturas adotaram a abordagem orientada a objetos (MIB) para descrever e especificar as informações nela armazenadas.
- As operações definidas para o SNMPv1 restringem-se às operações simples do tipo get-and-set, com melhoras na definição do SNMPv2. O CMIP especifica um conjunto mais completo de operações
- Possibilidade de sincronizar operações realizadas sobre vários objetos.
- O SNMP é um protocolo não orientado a conexão e o CMIP é um protocolo orientado à conexão executado sobre toda a pilha de protocolos OSI de gerenciamento.
- O grande problema do CMIP é que se tornou um sistema muito grande e complexo que poucas redes conseguem suportá-lo.

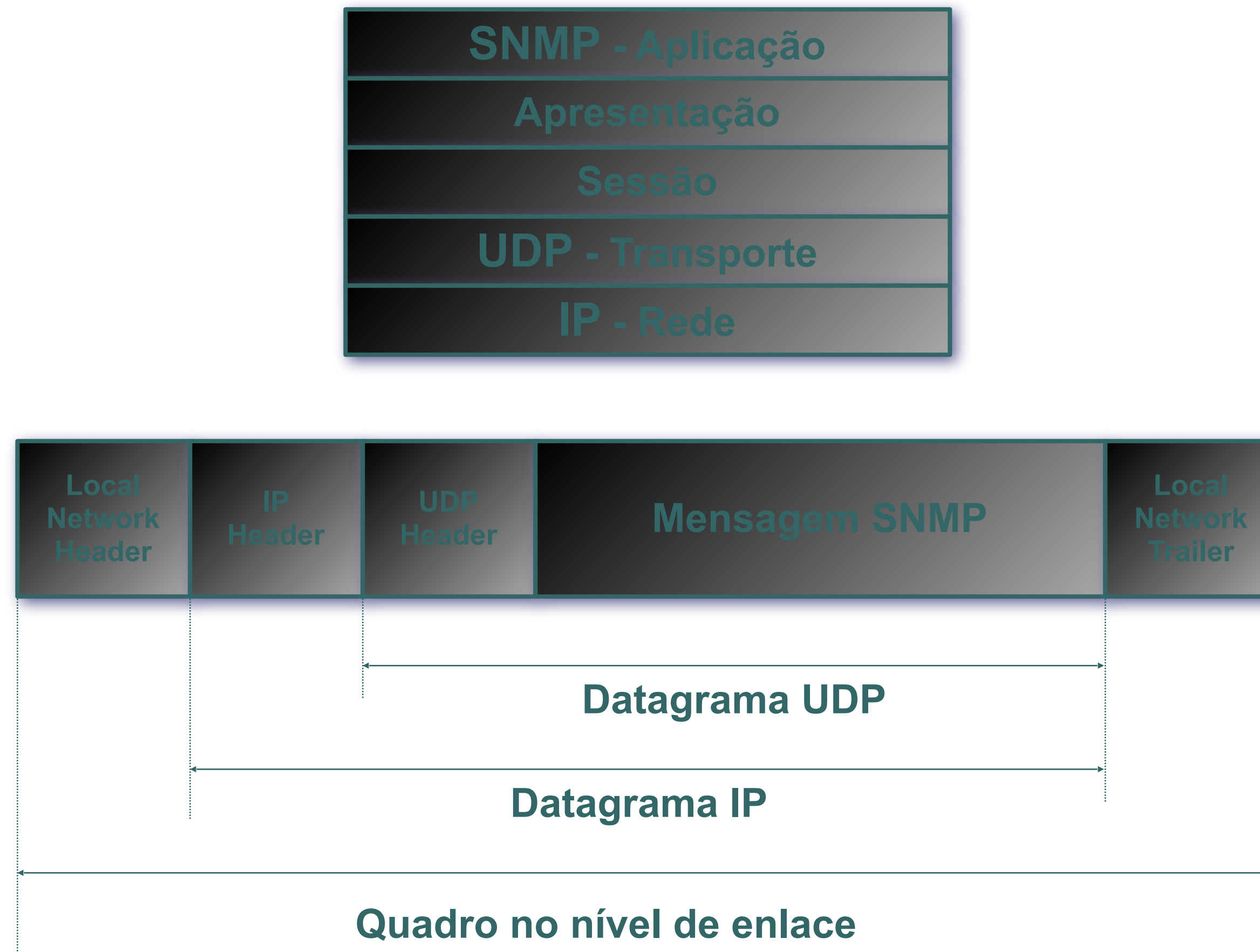
SNMP (*Simple Network Management Protocol*)

- Simples porque os recursos gerenciados necessitam de pouco processamento nas tarefas de gerenciamento; mínimo de software necessário
- Tarefas mais complexas de processamento e armazenagem de dados são de responsabilidade do sistema gerenciador
- Poucas funções de gerenciamento são pertinentes aos recursos gerenciados
- Para o protocolo ser simples existe um conjunto limitado de comandos e mensagens do protocolo possíveis

SNMP



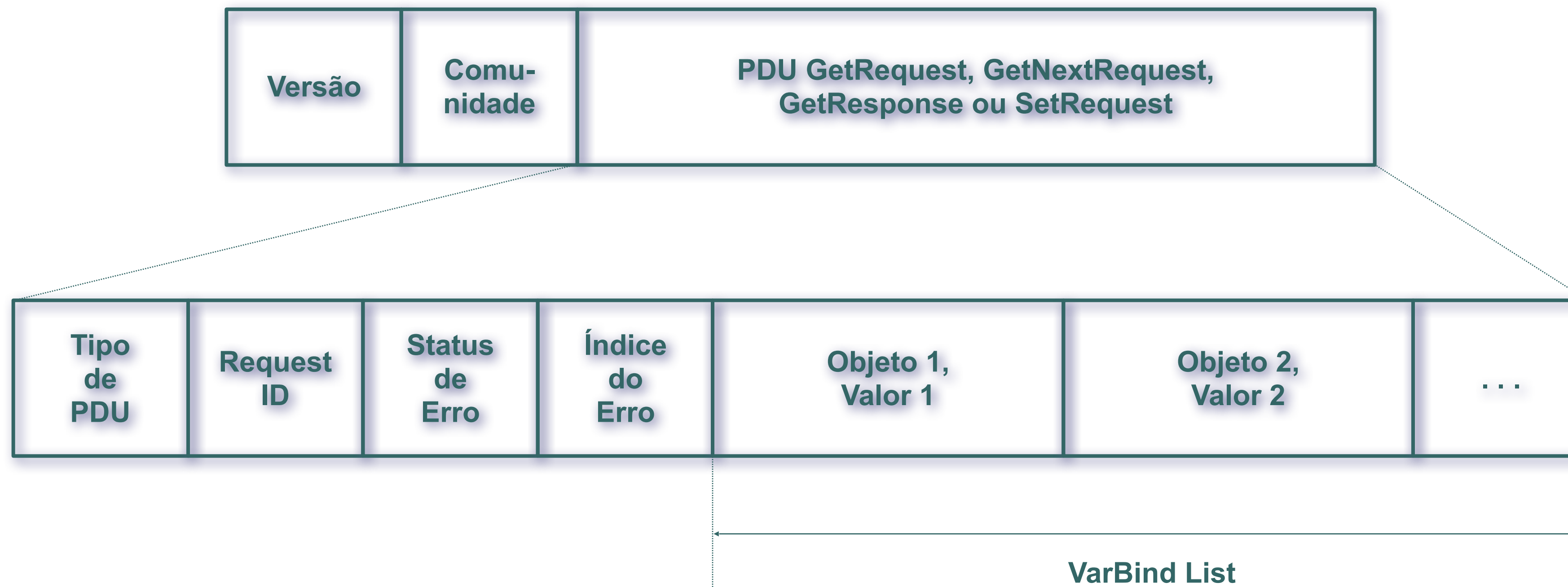
SNMP



SNMP Protocol Data Units (PDUs)

- Mensagem SNMP
 - Versão + Comunidade (header de autenticação)
 - PDU
- 5 tipos de PDUs
 - GetRequest
 - GetNextRequest
 - GetResponse
 - SetRequest
 - Trap

SNMP



- Campos
 - **Versão.** Para garantir que gerente e agente estão executando a mesma versão do protocolo. Mensagens com versões diferentes são descartadas.
 - **Comunidade.** Garante o acesso a um conjunto limitado de objetos da MIB. Caso exista diferenças na comunidade é emitido pelo agente uma *trap* que indica falha de autenticação
 - Caso a versão e comunidade estejam consistentes então é processada a PDU logo a seguir

- **Tipo de PDU.** Inteiro que identifica a operação a ser processada
 - 0 - GetRequest;
 - 1 - GetNextRequest;
 - 2 - GetResponse;
 - 3 - SetRequest;
 - 4 - Trap
- **Request ID.** Inteiro que identifica pares de mensagens SNMP entre agente e gerente.

- **Status de Erro.** Identifica operações executadas com sucesso ou um dos cinco erros previstos
 - 0 (**noError**) - Operação sem erros
 - 1 (**tooBig**) - O tamanho da PDU GetResponse excede um limite local
 - 2 (**noSuchName**) - Não existe objeto com o nome requisitado
 - 3 (**badValue**) - Uma PDU SetRequest contém uma variável de tipo, tamanho ou valor inconsistente
 - 4 (**readOnly**) - Uma PDU SetRequest foi enviada para alterar o valor de um objeto read-only
 - 5 (**genErr**) - Erro genérico

SNMP

- **Índice do Erro.** Indica a qual par objeto-valor, passado na PDU, se refere o erro
- **VarBind.** Ligação entre um objeto e um valor; **VarBind List:** lista destas ligações
- Em GetRequest e GetNextRequest os objetos possuem valores associados igual a **NULL** (tipo de dado especial de ASN.1)

SNMPv1

- Três tipos de dados simples são definidos na SMI SNMPv1:
 - *Integer*
 - *Octet strings*
 - *Object Ids*
- *Tipos de dados de Aplicação vasta:*
 - Endereços de rede
 - Contadores
 - Medidores
 - *Time ticks*
 - Opcacos
 - Inteiros(*integer*)
 - Inteiros sem sinal

SNMPv2

Adição de duas *PDU*s:

- *GETBULK REQUEST*
- *INFORM*

Três tipos de módulos de informação no *SMI*:

- Definições de objetos gerenciados relacionados
- Declarações de conformidade
- Declarações de capacidade

SNMPv3

- Atualização da segurança:
 - Criptografia das mensagens
 - Controle de acesso a objetos MIB
 - Autenticação da mensagem