

Gerência de Redes de Computadores

SNMP

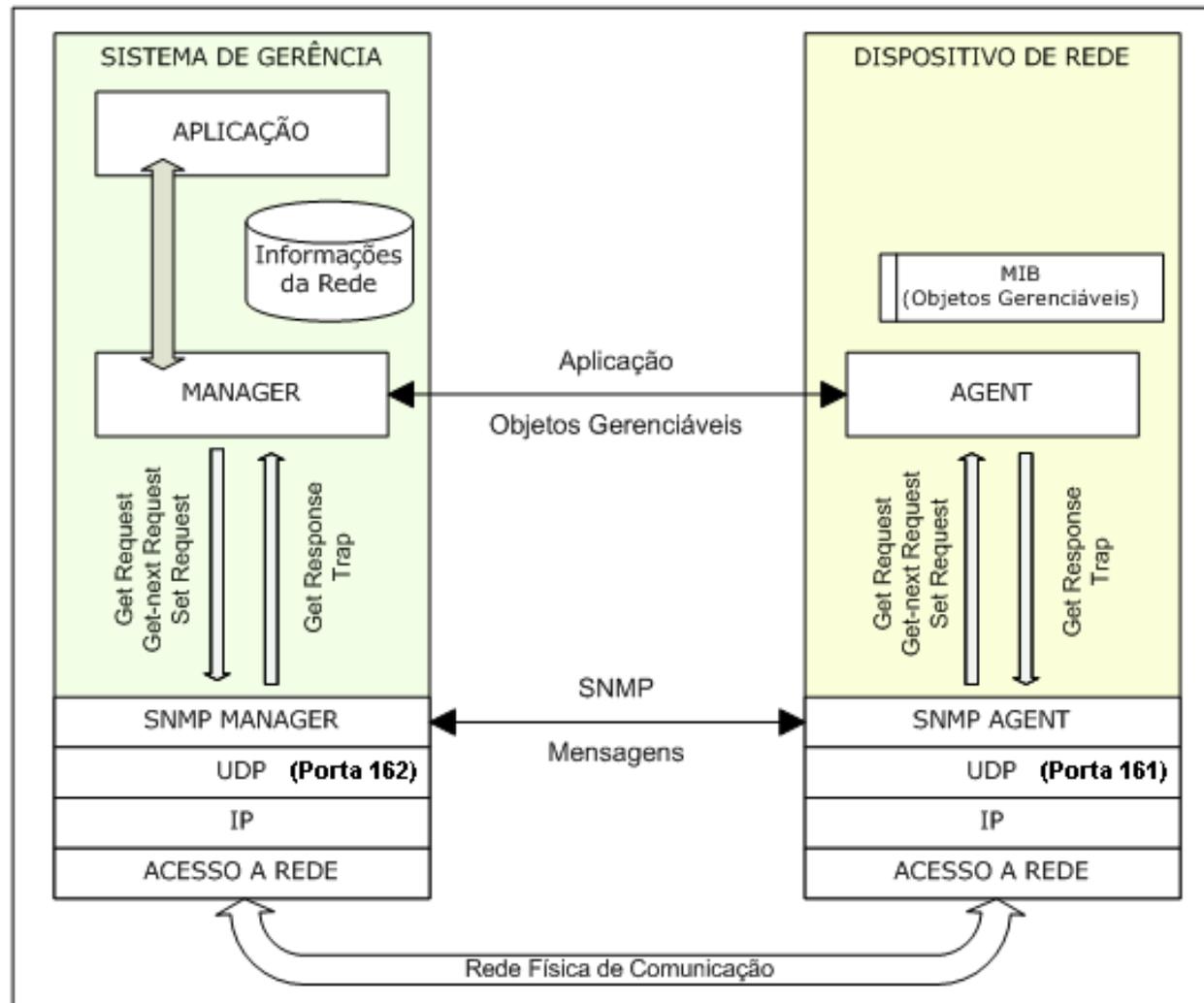
Prof. Alex Furtunato

alex.furtunato@ifrn.edu.br

SNMPv1

- Utiliza o protocolo UDP para transmissão dos dados
 - Agente escuta a porta 161
 - Gerente escuta a porta 162 para receber traps
- Segurança fraca, baseada em comunidade (community string)
 - Cada agente possui 3 comunidades: read-only, read-write e trap
 - Por padrão os equipamentos usam “public” e “private” para community

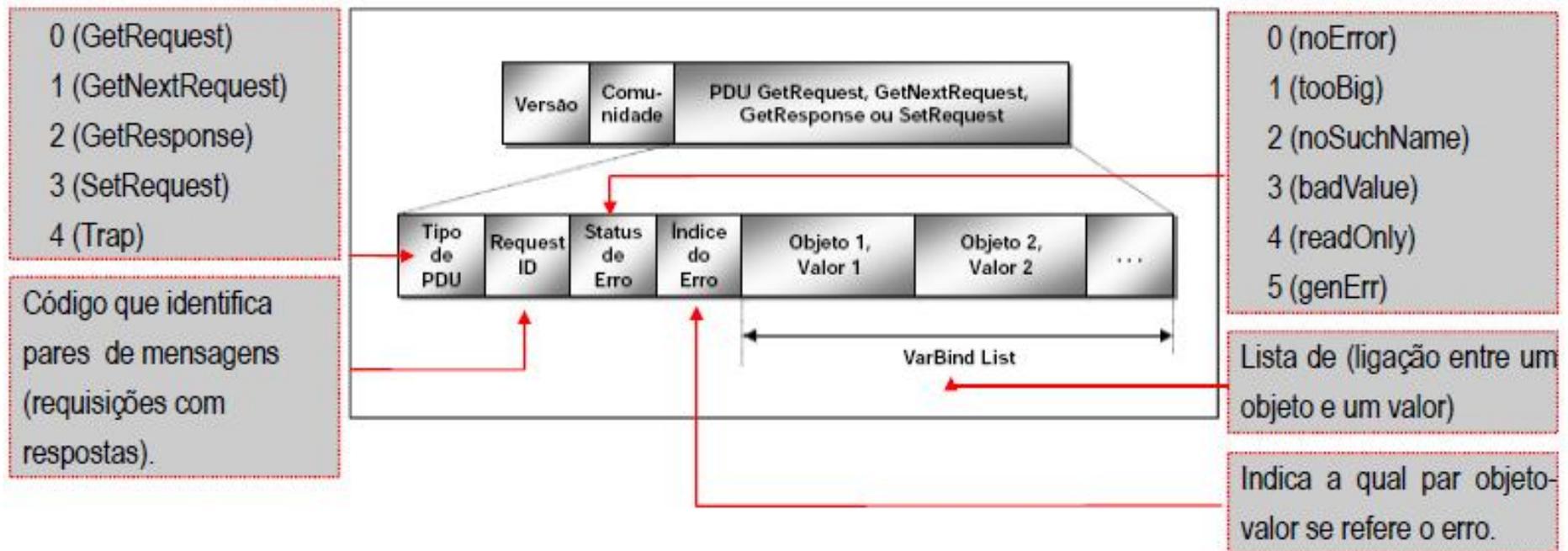
Comunicação SNMP



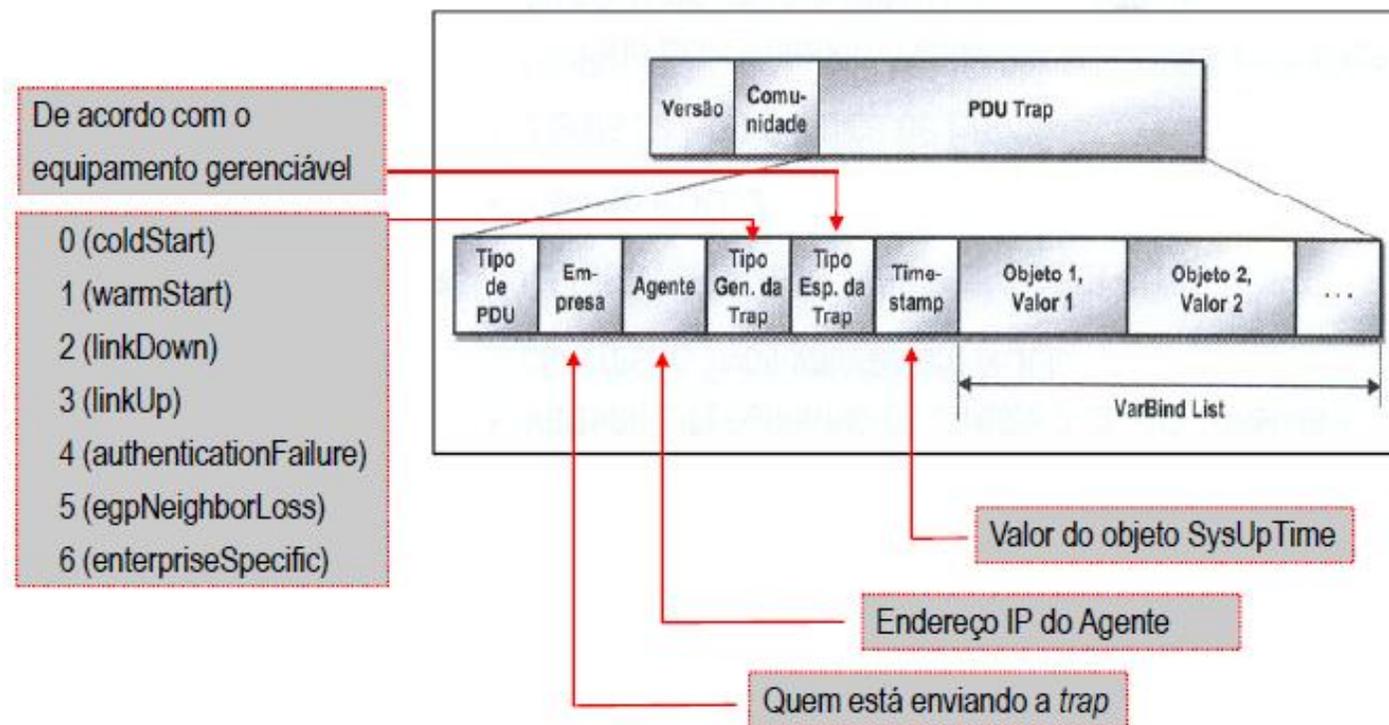
Mensagens SNMPv1

- GetRequest
- GetNextRequest
- GetResponse
- SetRequest
- Trap

PDU do SNMPv1



PDU do trap SNMPv1



Deficiências do SNMPv1

- Não é apropriado para o gerenciamento de redes grandes (polling performance)
- Autenticação fraca
- Modelo MIB limitado
- Não suporta comunicação gerente-gerente

SNMPv2

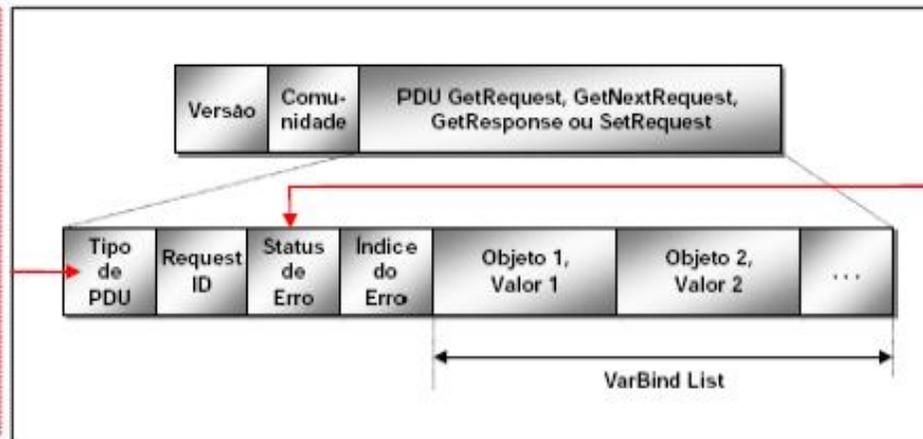
- Desenvolvido como uma solução intermediária
- Melhorias:
 - Operação com outros protocolos além de UDP
 - Suporte a comunicação gerente-gerente
 - Novo formato de trap
- Forma criadas duas versões:
 - SNMPv2p – baseado em parties (Complexo)
 - SNMPv2c – baseado em comunidade (Padrão)
 - SNMPv2u – baseado em usuários

Mensagens SNMPv2

- GetRequest
- GetNextRequest
- GetBulkRequest (SNMPv2 e SNMPv3)
- SetRequest
- GetResponse
- Trap
- Notification (SNMPv2 e SNMPv3)
- Inform (SNMPv2 e SNMPv3)
- Report (SNMPv2 e SNMPv3)

PDU do SNMPv2

- 0 (GetRequest)
- 1 (GetNextRequest)
- 2 (GetResponse)
- 3 (SetRequest)
- 4 (Trap)
- 5 (Get-Bulk-Request)
- 6 (Inform-Request)
- 7 (SNMPv2-Trap)



- 0 (noError)
- 1 (tooBig)
- 2 (noSuchName)
- 3 (badValue)
- 4 (readOnly)
- 5 (genErr)
- 6 (noaccess)
- 7 (wrongType)
- 8 (wrongLength)
- 9 (wrongEncoding)
- 10 (wrongValue)
- 11 (noCreation)
- 12 (inconsistentValue)
- 13 (resourceUnavailabe)
- 14 (commitFailed)
- 15 (undoFailed)
- 16 (authorizationError)
- 17 (inconsistentName)

GetRequest

- Enviada do Gerente para o agente solicitando dados de uma instância de objeto
- A identificação do objeto será no formato x.y, aonde, x é o ID do objeto e Y é a instância:
 - Para objetos escalares y é sempre 0
 - Em tabelas o y é a linha, que começa com 1
- Ex: (Utilizando o pacote Net-snmp)
snmpget cisco.rt.local 1.3.6.1.2.1.1.6.0
(Objeto sys.Location (.6), instância (.0))

GetNextRequest

- Permite recuperar um grupo de valores de objetos
- Utiliza-se da forma numérica em que os OIDs são organizados, incrementando o OID até receber uma mensagem de erro
- No pacote Net-snmp é o comando snmpwalk

GetBulkRequest

- A versão SNMPv2 implementa esse comando para pegar uma grande seção de uma tabela de uma só vez, sem erros
- Evita a ocorrência de erros por limitação do tamanho de retorno do agente
- Utiliza dois parâmetros para definir a quantidade máxima de objetos:
 - nonrepeaters
 - max-repetitions

SetRequest

- Utilizado para modificar o valor de um objeto gerenciado
- Somente os objetos definidos na MIB como *read-write* ou *write-only* podem ser utilizados nesse comando

GetResponse

- Comando enviado do agente para o gerente
- Resposta aos comandos get e set
- Retorna os dados requisitados pelo get ou se o comando set foi executado
- Utilizado também para responder ao comando get-next, indicando que existe mais variáveis a serem lidas

Trap

- O agente envia um trap para o gerente informando-o de algum evento, normalmente algum erro
- Normalmente é configurado no agente o destino do trap como o IP do gerente
- Identificado por códigos genéricos:
 - 0 – coldStart: Agente reinicializado
 - 1 – warmStart: Agente se reinicializou
 - 2 – linkDown: Interface mudou para estado down
 - 3 – linkUp: Interface mudou para estado up
 - 4 – authenticationFailure: Erro de autenticação
 - 5 – egpNeighborLoss: Vizinho egp ficou inativo
 - 6 – Trap específica dos fabricantes (idEmpresa.trapEspecifica)
- Normalmente as traps estão vinculadas a algum objeto da MIB que será utilizado para passar informações com a trap

InformRequest

- O mecanismo inform no SNMPv2 permite a comunicação entre os gerentes em uma rede
- Podes-se utilizar inform para substituir trap entre agente e o gerente. Nesse caso, o agente será informado do recebimento do inform por um response

Report

- A operação report foi definida no SNMPv2 mas nunca foi implementada nessa versão. Sua função seria relatar problemas relacionados ao processamento de mensagens SNMP e foi implementado no SNMPv3

SNMPv3

- Desenvolvido a partir de 1998
- Requisitos
 - Manter compatibilidade com versões anteriores
 - Resolver limitações das versões anteriores
 - Arquitetura modular
 - Manter o SNMP o mais simples possível
- USM (User-based Security Model)
 - DES, MD5 e SHA1
- VACM (View-based Access Control Model)
 - Controla quem pode e o que pode acessar
 - Views – Grupos/Objetos que podem ser acessados

Tipos de agentes

- Agentes extensíveis
 - Desenvolvido com arquitetura aberta, modular, permitindo adaptações
- Agentes monolíticos
 - Não extensíveis, otimizados para determinadas plataformas de hardware ou SO.
- Agentes proxies
 - Agente que não está dentro do sistema gerenciado. Utilizado para dispositivos que não têm suporte a SNMP ou a TCP/IP

Pacote Net-SNMP

- Pacote padrão no mundo linux
 - Debian: apt-get install snmp snmpd
- Composto de agente, aplicações de linha de comando e Biblioteca SNMP
- O agente é o daemon snmpd
- Arquivos de configuração do agentes:
 - /etc/snmp/snmpd.conf
- Arquivo de configuração do cliente:
 - /etc/snmp/snmp.conf
 - Define as mibs (para todas as mibs, deixa a linha "mibs:" comentada)
 - Ativa o repositório non-free no Source list do debia
 - Instala o script de download de mibs
 - Apt-get install snmp-mibs-downloader
 - Roda o comando de download:
 - %> download-mibs

Comandos do Net-SNMP

- snmpget
- snmpwalk
- snmptable
- snmpbulkget
- snmpdf
- snmpset
- snmptranslate
- snmptrap
- ...

Exercício SNMPv1

1. Instale o Net-snmp na maquina Debian:
 - `snmpd` e `snmp`
2. Configura o `sysContact` no arquivo de configuração do Agente
3. Utilizando o comando `snmpget` recupere a descrição do sistema, o Tempo de uso e o nome do Contato

Exercício SNMPv2

1. Altere a configuração do agente para a comunidade de leitura “ifrnpub” e para escrita como “ifrnpriv”
 - Linha que inicia com “com2sec”
2. Utilizado os comandos snmpbulkget e snmptable recupere os dados das interfaces
3. Altere os valor do Contato utilizado o comando snmpset e depois utilize o comando snmpget para testar