Protocolos de gerência

- **SNMP**
  - *Simple Network Management Protocol*
  - Criado pela IETF em 1988
  - Projetado para monitorar redes simples
  - Dominante em redes TCP/IP
- **CMIP**
  - *Common Management Information Protocol*
  - Proposto pela ISO no início dos anos 90
  - Controle (complexo) de redes complexas
  - Muito presente em redes de telefonia

Gerenciamento TCP/IP

- SNMP - *Simple Network Management Protocol*
  - RFC1155 *Structure and Identification of Management Information for TCP/IP-based internets*
  - RFC 1156 - *Management Information Base Network Management of TCP/IP-based internets*
  - RFC 1157 - *A Simple Network Management Protocol*
  - RFC 1213 - *Management Information Base Network Management of TCP/IP-based internets: MIB-II*
- RMON - *Remote Network Monitoring*
  - RFC1271 e depois RFC 1757

Informações de gerência

- **MIB**
  - *Management Information Base*
  - Dados mantidos pelos elementos gerenciados
  - Informação com estrutura hierárquica
- **SMI**
  - *Structure of Management Information*
  - Define notações, formatos, tipos, nomes, ...
  - Usa como base a notação formal ASN.1

SNMP

- Voltado à monitoração de redes simples
  - Pode ser embutido em hardware simples
  - Muito usado em redes TCP/IP
- Comandos e tipos de dados fixos
  - Poucos tipos de mensagens
  - estrutura bastante simples
- Usa UDP/IP
  - baixo nível de tráfego de gerência
  - protocolo de transporte sem conexão
  - não confiável (perda de pacotes)
- Comandos e respostas assíncronas

Limitações de SNMP

- **Falta de segurança**
  - esquema de autenticação trivial
  - limitações no uso do método SET
- **Ineficiência**
  - esquema de eventos limitado e fixo
  - operação baseada em pooling
  - comandos transportam poucos dados
- **Falta de funções específicas**
  - MIB com estrutura fixa
  - Falta de comandos de controle
  - Falta de comunicação entre gerenciadores
- **Não confiável**
  - baseado em UDP/IP
  - traps sem reconhecimento

Gerenciamento TCP/IP

- SNMPv2
  - RFC1442 Structure of Management Information for Version 2 of SNMP
  - RFC1448 Protocol Operations for Version 2 of SNMP
- SNMPv3
  - 1998
  - Principal característica: Segurança

Protocolo SNMP

- Simple Network Management Protocol
- Estrutura de Informação de Gerência (SMI) - ASN.1 (Abstract Syntax Notation One) / Macro OBJECT-TYPE
- Protocolo - ASN.1 / BER (Basic Enconding Rules) via UDP/IP

ASN.1

- Linguagem formal para definição de sintaxe de abstrata (ISO)
- SNMP usa um subconjunto de tipos ASN.1, bem como a macro OBJECT -TYPE para a especificação da MIB
  - Integer
  - Octet String
  - Display String
  - Object Identifier
  - Sequence
  - Sequence of

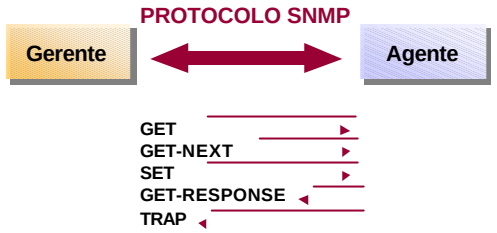
BER

- Regras que geram a sintaxe de transferência
- Tipos codificados em três campos: rótulo, tipo & valor

```
ex::= sequence {                    dados:
      nome OCTET STRING,             { adao, 45 }
      idade INTEGER
}
```

dados codificados: 30 07 02 04 04 A D A O 02 01 45

Protocolo



O protocolo SNMP é transportado pelo protocolo UDP

Comandos SNMP

- **GET**
  - ler valor de um objeto gerenciável
  - somente lê valores isolados (sem agrupamentos)
- **GET-NEXT**
  - ler próximo valor em objeto gerenciável
- **SET**
  - setar valor em objeto gerenciável
  - considerado pouco seguro
- **TRAP**
  - indicação assíncrona de ocorrência de evento

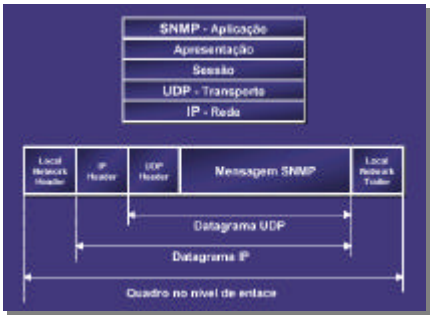
SNMP over UDP

TRAPS

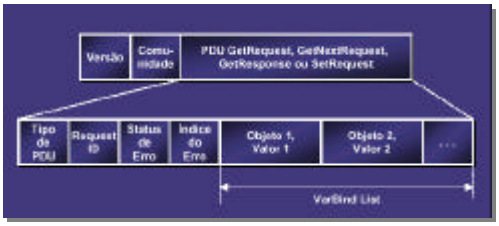
- Mensagens não solicitadas geradas por um agente SNMP

COLDSART
WARMSTART
LINK DOWN
LINK UP
FAILURE OF AUTHENTICATION
EXTERIOR GATEWAY PROTOCOL NEIGHBOR LOSS
ENTERPRISE-SPECIFIC

PDU´s SNMP



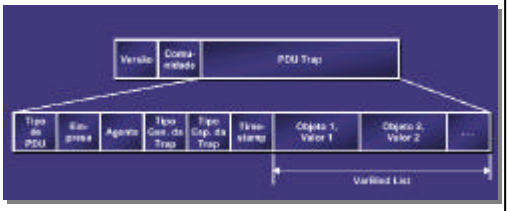
Get, Get-Next, Set, Get-Response



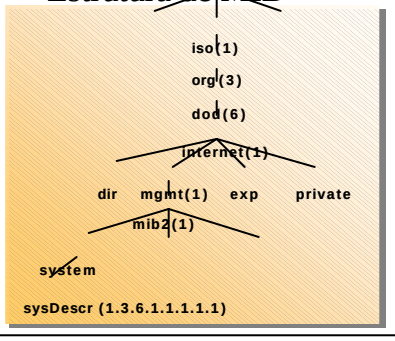
Erros

- Erros retornados por agentes SNMP
  - 0 (noError)
  - 1 (tooBig)
  - 2 (noSuchName)
  - 3 (badValue)
  - 4 (readOnly)
  - 5 (genError)
- Índice do Erro
  - Indica a qual variável se refere o erro

Traps



Estrutura de MIB



Macro OBJECT-TYPE

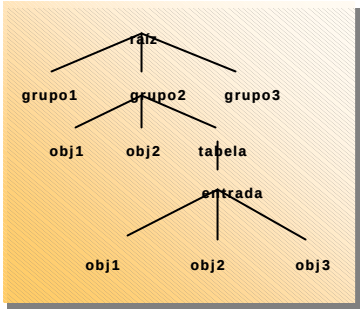
```
sysLocation OBJECT-TYPE
        SYNTAX   Display String (size (0 .. 255))
        ACCESS   read-write
        STATUS    mandatory
        DESCRIPTION " ------ "
        ::= { system 6 }
```

Macro OBJECT-TYPE

```
ipRoutingTable OBJECT-TYPE
        SYNTAX Sequence of
    IpRouteEntry
        ACCESS read-write
        STATUS mandatory
        ::= { ipRoutingTable 1 }

ipRouteEntry OBJECT-TYPE
        SYNTAX IpRouteEntry
        ACCESS read-write
        STATUS mandatory
```

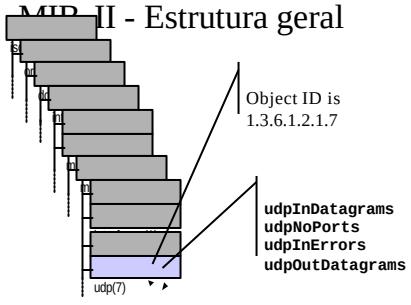
Organização da MIB



MIB II - Grupos de Objetos

- System
- Interfaces
- AT
- IP
- ICMP
- TCP
- UDP
- EGP
- Transmission
- SNMP

MIB II - Estrutura geral



Outras MIBs

- Servidor Novell
- Clientes
- UPS
- Hosts
- PU e LUs SNA
- Aplicações distribuídas
- Cafeteiras, torradeiras etc...

Operação SNMP

- ID do obejto + ID da instância
- Objetos folha (.0)
  - ex.: GET sysDescr.0
    - GET 1.3.6.1.1.1.1.1.0
- Objetos como campo de uma tabelas (.chave)
  - ex.: GET ipRouteNextHop.143.54.1.0
    - GET 1.3.6.1.1.1.5.7.143.54.1.0

Objetos Relevantes ao Gerenciamento de Falhas

Grupo SYSTEM

sysDescr	descrição do sistema
sysLocation	localização física do sistema
sysContact	pessoa responsável pelo sistema
sysName	nome do sistema

Objetos Relevantes ao Gerenciamento de Falhas

GRUPO INTERFACES

Dados sobre cada interface específico do dispositivo

ifTable	tabela com informações sobr todos os interfaces
ifEntry	linha com informações sobre um interface
ifNumber	número de interfaces

Objetos Relevantes ao Gerenciamento de Configuração

Grupo INTERFACES

ifDescr	nome do interface
ifType	tipo do interface
ifMTU	máximo tamanho de datagrama
ifSpeed	velocidade do interface (BPS)
ifAdminStatus	up/down/test

Objetos Relevantes ao Gerenciamento de Performance

ifInDiscards	taxa de entradas descartadas
ifOutDiscards	taxa de transmissões descartadas
ifInErrors	taxa de erros de entrada
ifOutErrors	taxa de erros em transmissões
ifInOctets	taxa de bytes recebidos
ifInUcastPkts	taxa de pacotes unidirecionados recebidos
ifOutUcastPkts	taxa de pacotes

Exemplo

```
penta% snmpi -a routcv
snmpi> bulk system
snmpi: 3 rows retrieved in 0.643473 seconds during 8 iterations
snmpi: threads: at most 2 active, total of 6 created, and 5 did nothing
snmpi: messages: 9 requests sent, along with 0 retries
snmpi: 9 responses rcvd, along with 0 duplicates
snmpi: timeouts: min=0.082 fin=0.082 max=2.000 seconds
```

Exemplo

```
penta% snmpi -a tchepoa.ufrgs.br
snmpi> get sysDescr.0
sysDescr.0="GS Software (GS3-BFX), Version 9.0(2), SOFTWARE
Copyright (c) 1986-1992 by cisco Systems, Inc.
Compiled Thu 03-Sep-92 11:13 by mlw"

snmpi> get ifNumber.0
ifNumber.0=16

snmpi> get ifDescr.4
ifDescr.4="Serial1"
snmpi> get ifOperStatus.4
ifOperStatus.4=up(1)
snmpi> get ipRouteNextHop.0.0.0.0
ipRouteNextHop.0.0.0.0=143.54.1.125
```

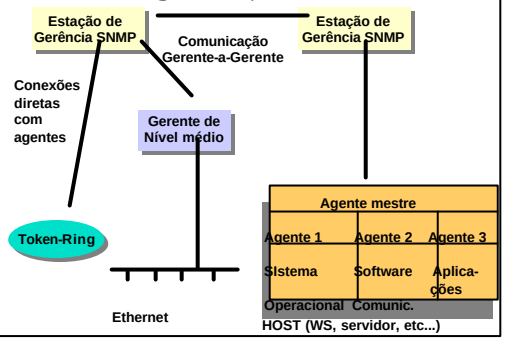
Exemplo

```
snmpi> bulk ifDescr, ifType
snmpi: 13 rows retrieved in 0.337115 seconds during 9 iterations
snmpi: threads: atmost 4 active, total of 10 created, and 6 did nothing
snmpi: messages: 23 requests sent, along with 0 retries
snmpi:           23 responses rcvd, along with 0 duplicates
snmpi: timeouts: min=0.057 fin=0.070 max=2.000 seconds
row     ifDescr ifType
1       "Ethernet0"     ethernet-csmacd(6)
2       "Serial0"       propPointToPointSerial(22)
3       "Ethernet1"     ethernet-csmacd(6)
4       "Serial1"       propPointToPointSerial(22)
12      "Serial9"       ppp(23)
5       "Serial2"       propPointToPointSerial(22)
13      "Serial10"      propPointToPointSerial(22)
6       "Serial3"       propPointToPointSerial(22)
7       "Serial4"       rfc877-x25(5)
```

SNMPv2

- Gerenciar recursos arbitrários e não apenas recursos de rede (aplicações, sistemas e comunicação gerente-a-gerente)
- Continua simples e rápido
- Incorpora segurança
- Funciona sobre TCP/IP, OSI e outros protocolos
- Interopera com plataformas SNMP
- Gerenciamento hierárquico

SNMPv2



Operações SNMPv2

- GetRequest
- GetNextRequest
- SetRequest
- Response
- Trap
- GetBulkRequest
- InformRequest

SNMPv2

- SNMPv2 : utilização do protocolo *Manager-to-Manager*
- Alarmes e eventos
- *Party* : segurança
- Segurança
  - mecanismo de autenticação
  - privacidade (criptografia)
  - controle de acesso (por tipo de acesso)

SNMPv3

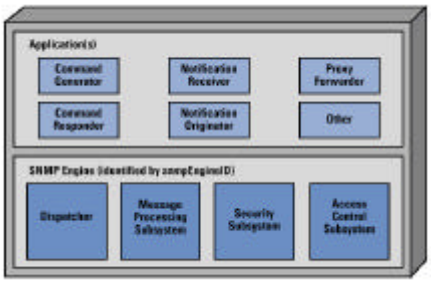
- Apelo do SNMP é a sua simplicidade
- Conjunto de *Proposed Standards* em Janeiro de 1998

RFC	Title
2271	An Architecture for Describing SNMP Management Frameworks
2272	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
2273	SNMPv3 Applications
2274	User-Based Security Model for SNMPv3
2275	View-Based Access Control Model (VACM) for SNMP

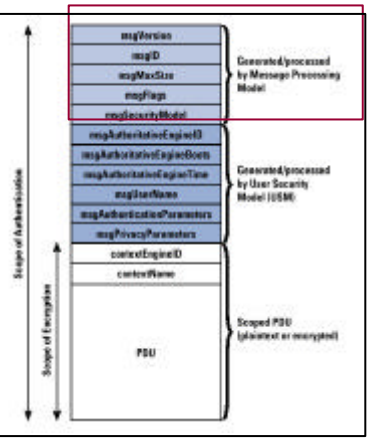
Segurança no SNMPv3

- Principais características do SNMPv3
  - Autenticação Digital
  - C[illegible]

Arquitetura SNMPv3



PDU SNMP v3



User-Based Security Model (USM)

- Definido na RFC 2274
  - Autenticação: provê integridade de dados e autenticação da origem
    - MD5 ou SHA-1
  - *Timeliness*: protege contra atrasos e/ou *replay*
  - Privacidade: provê criptografia de dados
    - CBC (Chiper Block Chaining)
  - Formato da Mensagem: define o formato dos parâmetros de segurança da PDU
  - *Discovery*: obtenção de informações sobe outras SNMP *engines*
  - *Key Management*: define os procedimentos para geração de chaves.

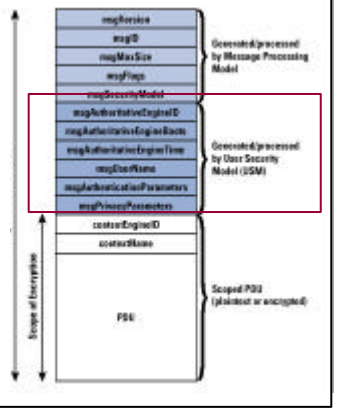
USM – Entidade Autoritativa

- Transmissores ou Receptores são definidos como entidades autoritativas, de acordo com as seguintes regras:
  - Quando uma mensagem SNMP contém um *payload* que espera por uma reposta, o receptor desta mensagem é autoritativo
    - Get, Get-nest, GetBulk, Set e Inform
  - Quando uma mensagem SNMP contém um Quando uma mensagem SNMP contém um *payload* que não espera por uma reposta, a entdade origem da PDU é autoritativa
    - Trap, Respose e Report

USM - ...

- A designação de autoridade serve a dois propósitos:
  - O *timeliness* da mensagem é determinado com respeito ao *clock* mantido pela *engine* autoritativa. Assim a entidade não autoritativa pode sincronizar seu *clock* com a entidade autoritativa
  - O processo de localização de chaves habilita o armazenamento das chaves em uma única *engine*
- Métodos de Criptografia
  - Chave compartilhada
  - 2 chaves
    - *Authkey*
    - *PrivKey*

Parâmetros do USM



Criptografia de Dados

- Usa o CBC
  - Chave *privKey* de 16 bytes
    - Utiliza-se os 8 primeiros bytes para o DES, pois ele necessita de 56 bits
  - Vetor de Inicialização de 64 bits
    - Os 8 bytes restantes da *privkey* são usados para o pre-IV
    - Para garantir que dois IV diferentes são utilizados dois "textos" diferentes, codificados com a mesma chave, é produzido um valor "salteado" de 8 bytes.
    - Executa-se um XOR entre o valor salteado e o pre-IV para gerar o novo IV

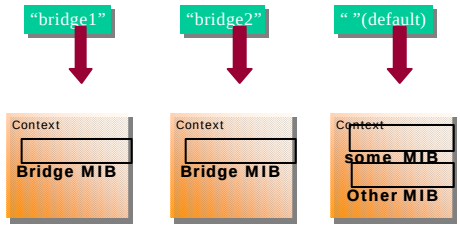
View Access Control Model

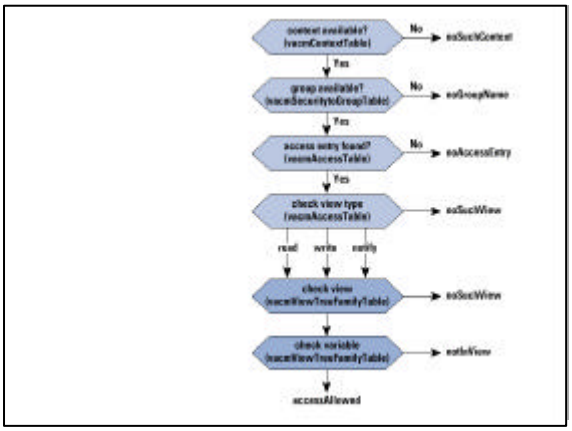
- Este modelo tem duas características importantes
  - Determina se o acesso a um objeto gerenciado de uma MIB Local é permitido
  - Faz uso da MIB que define a política de controle de acesso para um agente
- Elementos
  - *Groups*
  - *Security level*
  - *Context*
  - *MIB views*
  - *Access policy*

Elementos

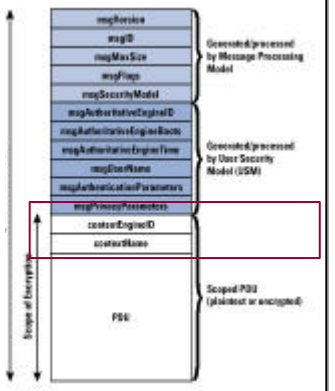
- *Groups*
  - Zero ou mais tuplas
    <***securityModel, securityName***>
- *Contexts*
  - É o nome de um subconjunto de instâncias de objeto da MIB Local
  - Conceito relacionado a controle de acesso
  - Uma instância de objeto ou objeto pode estar associado a mais de um contexto
  - Para identificar uma instância individualmente deve-se usar o *contextName* e o *contextEngineID*

Contexto - Exemplo





Parâmetros do VACM



Extensões de SNMP

- RMON - Remote Network Monitoring
  - extensão da MIB-II para gerência
  - Facilidades para monitoração e coleta
  - “Remendo” sobre SNMP e MIB
- RMON-2
  - Coleta de informações mais abrangente
- SNMP-V2
  - estrutura de segurança melhorada
  - comunicação entre gerentes (método **`inform`**)
  - MIB e SMI aumentadas: novos tipos de dados