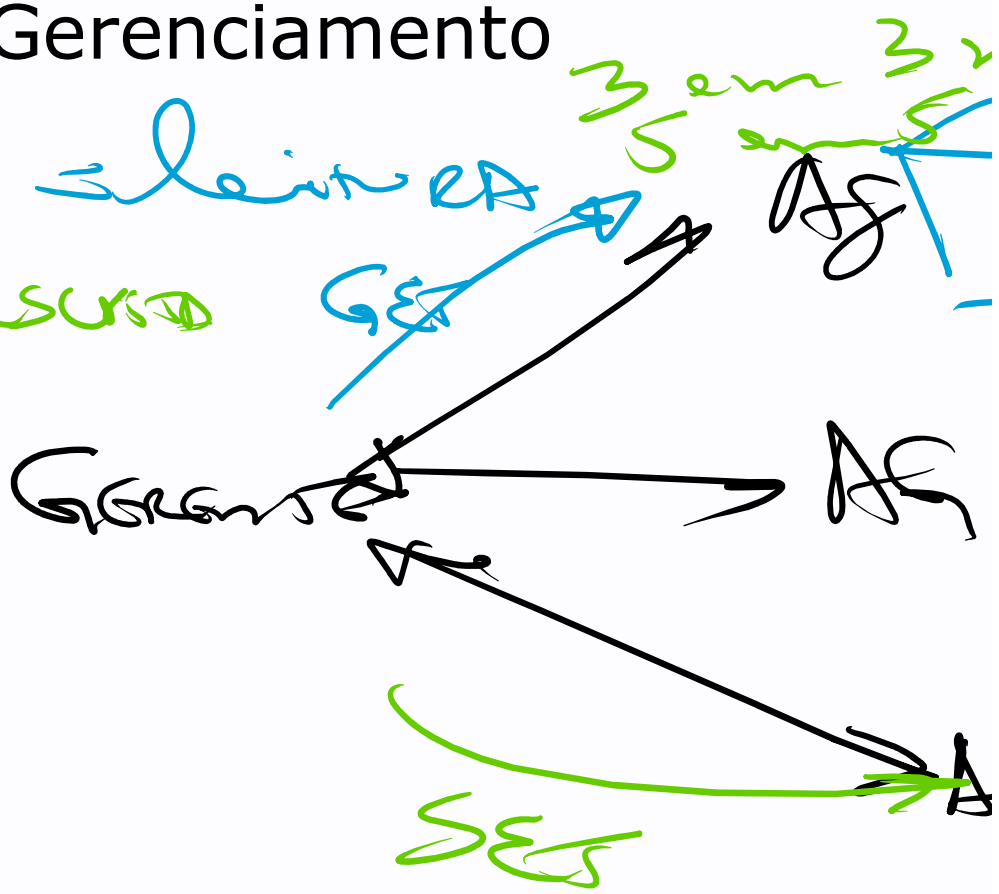
PUC Minas

Monitoração e Controle

- Funções de Gerenciamento
- Monitoração
- Controle
- Resumo



Funções de Gerenciamento

PUC Minas

As funções de gerenciamento de rede podem ser agrupadas sem duas categorias:

Monitoração de rede e controle de rede.

- A monitoração da rede está relacionada com a tarefa de observação de seus componentes; é uma função de "leitura".

- O controle da rede é uma função de "escrita" e está relacionada com a tarefa de alteração de valores de parâmetros e execução de determinadas ações.

PUC Minas

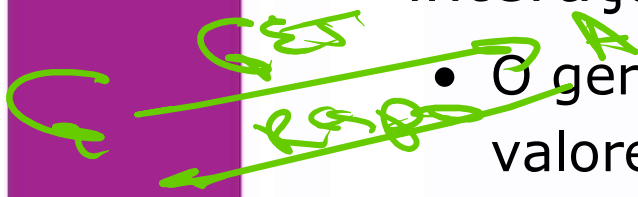
Monitoração (1)

- Consiste na observação de informações relevantes ao gerenciamento, classificadas em três categorias:
  - **Estática:** Caracteriza a configuração atual e os elementos na atual configuração, tais como o número e identificação de portas em um roteador.
  - **Dinâmica:** Relacionada com os eventos na rede, tais como a transmissão de um pacote na rede.
  - **Estatística:** Pode ser derivada de informações dinâmicas; ex. Média de pacotes por unidade de tempos em um determinado sistema.

Monitoração (2)

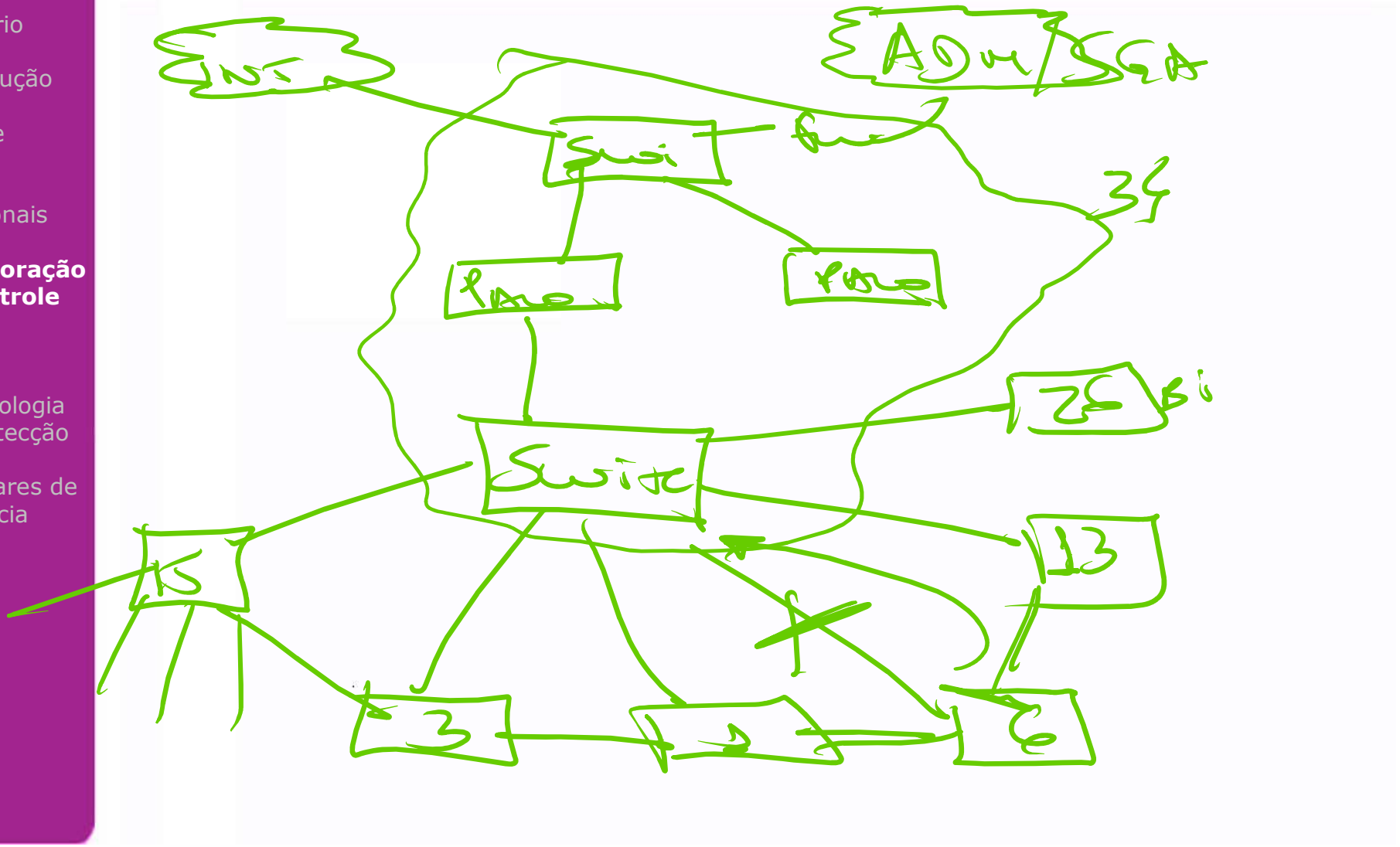
PUC Minas

- A informação de gerenciamento é coletada e armazenada por agentes e repassada para um ou mais gerentes.
- Duas técnicas podem ser utilizadas na comunicação entre agentes e gerentes: **polling e event-reporting.**
- A técnica de **polling** consiste em uma interação do tipo **request/response**.
  - O gerente pode solicitar a um agente o envio de valores de diversos elementos de informação.
  - O agente responde com os valores constantes em sua MIB



Monitoração (3)

- Na técnica de **event-reporting**, a iniciativa é do agente.
  - O gerente fica na escuta, esperando pela chegada de informações.
  - Um agente pode gerar um relatório periodicamente para fornecer ao gerente o seu estado atual.
  - A periodicidade do relatório pode ser configurada previamente pelo gerente.
  - Um agente também pode enviar um relatório quando ocorre um evento significativo ou não usual.



Monitoração (4)

PUC Minas

Simple Network Manage Protocol

- Tanto o **polling** quanto o **event-reporting** são usados nos sistemas de gerenciamento, porém a ênfase dada a cada um dos métodos difere muito entre sistemas.
- Em sistemas de gerenciamento de redes de telecomunicações, a ênfase maior é dada para o método de **event-reporting**.
- Em contraste, o modelo **SNMP dá pouca importância ao event-reporting**. O modelo OSI fica entre estes dois extremos.

Monitoração (5)

A escolha da ênfase depende dos seguintes fatores:

- A quantidade de tráfego gerada por cada método;
- Robustez em situações críticas;
- O tempo entre ocorrência do evento e a notificação ao gerente;
- A quantidade de processamento nos equipamentos gerenciados;
- A problemática referente à transferência confiável versus transferência não confiável;
- As aplicações de monitoração de rede suportadas;
- As considerações referentes ao caso em que um equipamento falhe antes de enviar um relatório.

Controle (1)

- Refere-se à modificação de parâmetros e à execução de ações em um sistema remoto. Todas as cinco áreas funcionais de gerenciamento (falhas, desempenho, contabilização, configuração e segurança), envolvem monitoração e controle.

- A ênfase nas três primeiras destas áreas, tem sido na monitoração, enquanto que nas duas últimas, o controle tem sido mais enfatizado.

Controle (2)

O controle de configuração inclui as seguintes funções:

- Definição da informação de configuração – recursos e atributos dos recursos sujeitos ao gerenciamento
- Atribuições e modificação de valores de atributos;
- Definição e modificação de relacionamentos entre recursos ou componentes da rede;
- Inicialização e terminação de operações de rede;
- Distribuição de software;
- Exame de valores e relacionamentos;
- Relatórios de status de configuração;

Controle (3)

- O controle de segurança é relativo à segurança dos recursos sob gerenciamento, incluindo o próprio sistema de gerenciamento.
- Os principais objetivos em termos de segurança, são relativos à confidencialidade, integridade e disponibilidade.
- **As principais ameaças à segurança referem-se à interrupção, interceptação, modificação e mascaramento.**

Controle (4)

As funções de gerenciamento de segurança podem ser agrupadas em três categorias:

- manutenção da informação de segurança
- controle de acesso aos recursos
- controle do processo de criptografia

Resumo

Classificação da informação

- Estática (ex. A localização e o responsável por um determinado equipamento)
- Dinâmica (ex. Estado de uma interface de rede)
- Estatística (ex. Quantidade média de pacotes transmitidos por hora)

Técnicas para coleta de informações

- Polling e Event Reporting

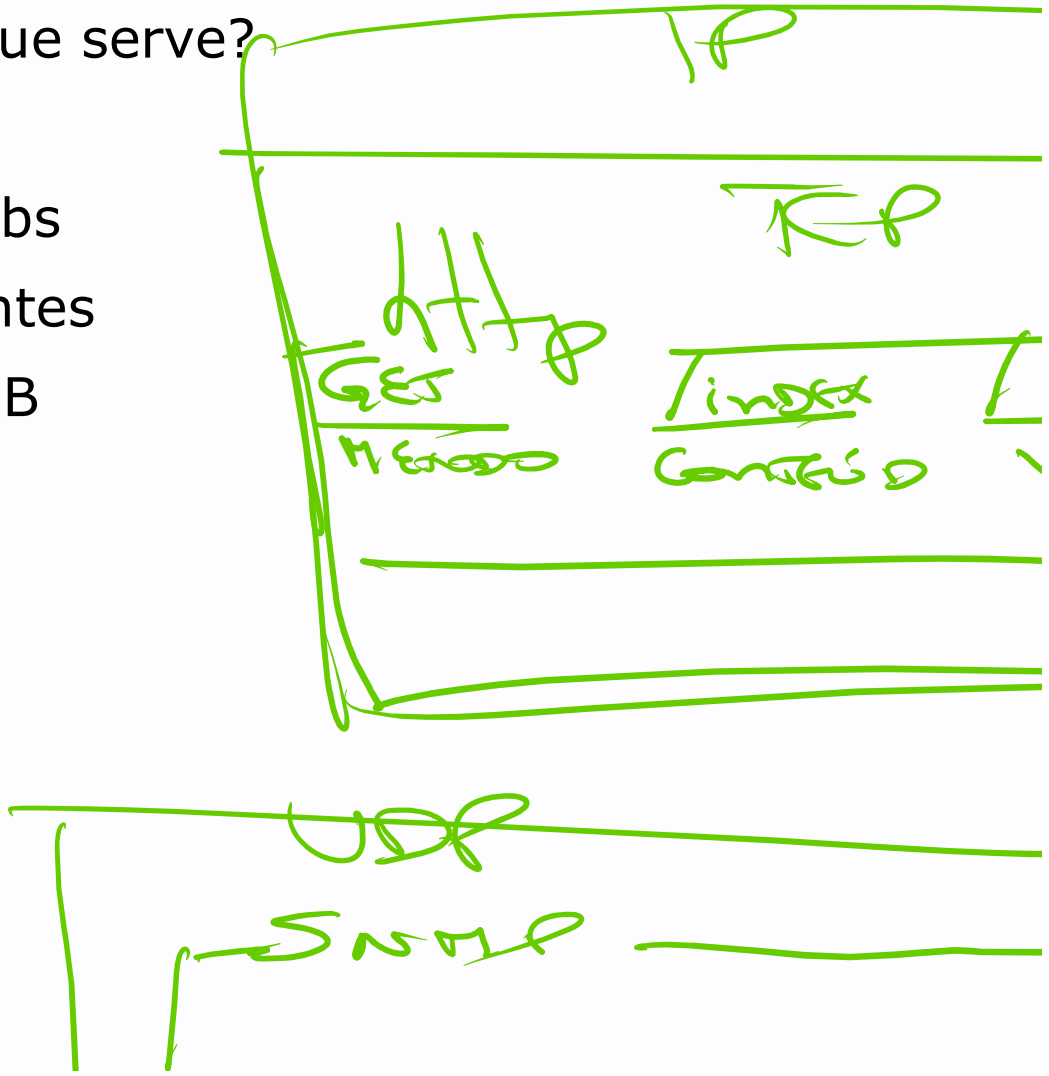
Controle de redes

- Controle de configuração (ex. Distribuição de sw)
- Controle de segurança
- Tipos de ameaças

PUC Minas

SNMP

- O que é? Para que serve?
- SMI e MIB
- RFC e Outras Mibs
- Gerentes e Agentes
- Host resouce MIB
- UDP
- Comunidades
- OID
- Operações
- SNMPv3
- RMON



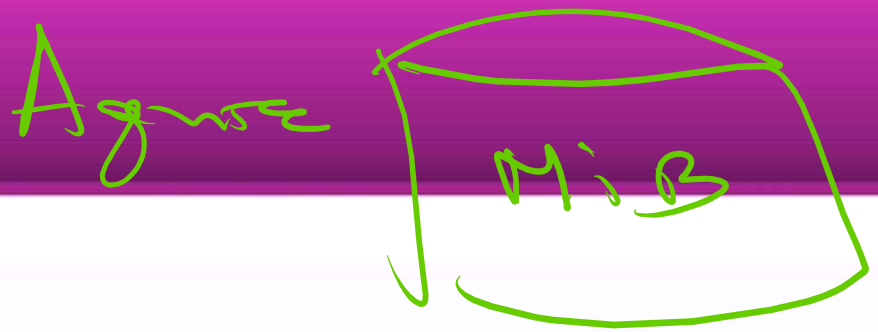
O que é?

- **Simple Network Management Protocol (SNMP)** é um protocolo de gerenciamento de dispositivos que atua na camada de aplicação da pilha TCP/IP.
- O SNMP foi lançado em 1988 para atender a necessidade crescente de padronização do gerenciamento de dispositivos IP.
- Sucedeu o Simple Gateway Management Protocol (SGMP) anteriormente definido na RFC 1028 de 1987 que tinha sido desenvolvido para gerenciar roteadores da Internet.

Para que serve?

- **Apesar de ter sido desenvolvido, inicialmente, para gerenciar dispositivos de rede, pode gerenciar sistemas (Unix, Windows, Linux,...), impressoras, modem, fontes de energia e muito mais.**
- É possível gerenciar qualquer dispositivo que execute um software (agente) que permita a recuperação de informações de acordo com o protocolo SNMP. Isso inclui não só dispositivos de hardware, mas softwares como SGBDs, servidores web e de aplicações.

MIB



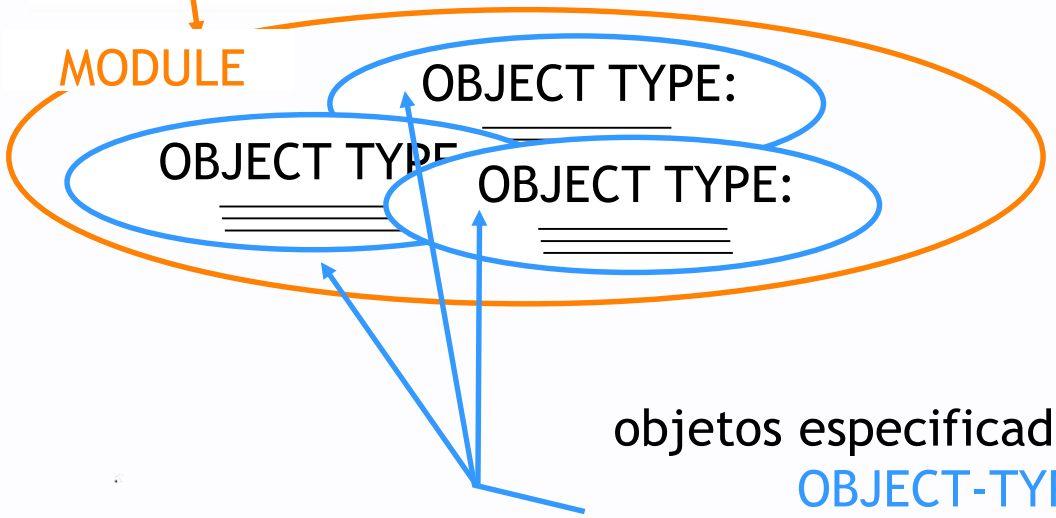
- Um agente tem uma lista dos objetos por ele suportados (exemplos: status da interface do roteador, taxa de utilização do processador, memória disponível)
- Management Information Base (MIB) é **uma base de dados de objetos gerenciados que o agente tem acesso**
- A MIB é uma base de dados, cuja estrutura é especificada pelo padrão SMI

MIB

Um módulo MIB é especificado pela SMI como:

MODULE-IDENTITY

(100 MIBs padronizadas, mais proprietárias)



objetos especificados via construção OBJECT-TYPE da SMI

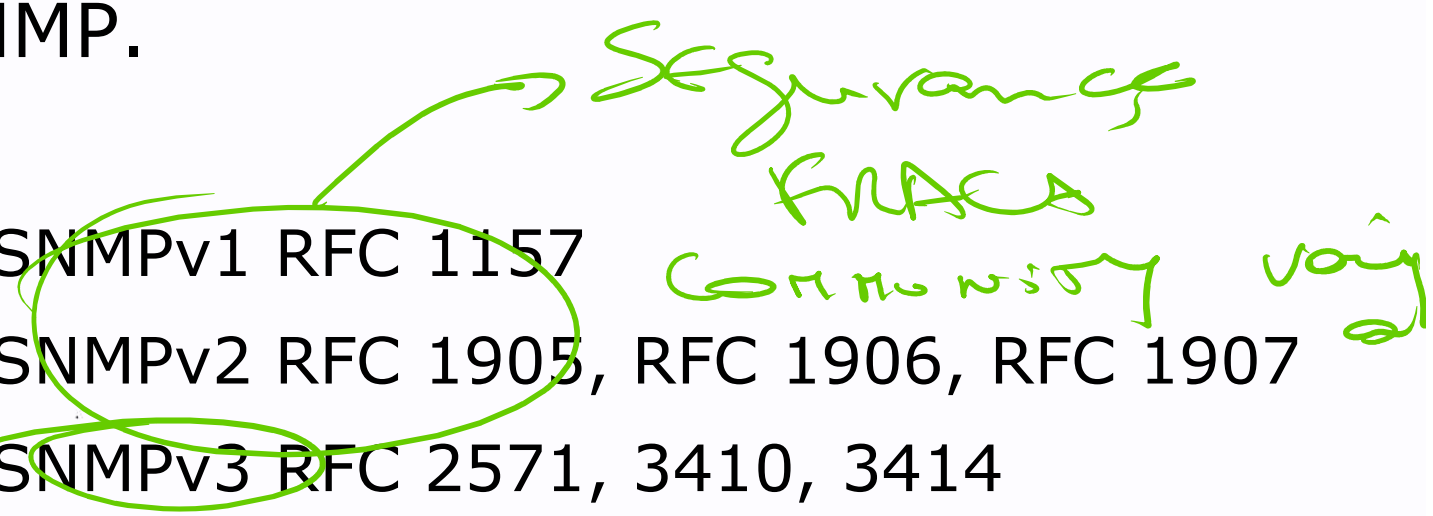
Structure of Management Information (SMI)

PUC Minas

- São as regras para se definir objetos gerenciados e respectivos comportamentos
- **Todo tipo de informação solicitado pela NMS, como status e/ou estatísticas, são definidos em uma MIB**
- Um agente pode implementar algumas ou **várias MIBs**, mas todos implementam uma específica chamada MIB-II (RFC 1213)

RFCs

- Internet Engineering Task Force (IETF) é responsável pela definição de protocolos padrão que controlam o tráfego na Internet, o que inclui o SNMP.



  - SNMPv1 RFC 1157
  - SNMPv2 RFC 1905, RFC 1906, RFC 1907
  - SNMPv3 RFC 2571, 3410, 3414
  - http://www.ietf.org/rfc.html

Outras MIBs

- Um fornecedor pode definir uma MIB exclusiva como um diferencial para o seu produto
- Essas MIBs podem oferecer informações mais consistentes para o gerenciamento do dispositivo do fabricante que não estão cobertas na MIB padrão
- O carregamento de uma nova MIB na NMS não garante que as informações serão fornecidas pelo agente.
- O agente só fornece as informações para as quais ele foi programado, portanto procure as MIBs fornecidas pelo fabricante do dispositivo

Gerentes e Agentes

- Network Management Station (NMS) ou Gerente solicita informações continuamente dos agentes (polling)
- O agente responde à solicitação da NMS
- A NMS recebe traps enviados por agentes a qualquer momento
- Traps assíncronos informam se algo aconteceu no dispositivo
- O agente pode ser implementado como um serviço (daemon) ou como parte do sistema operacional

Host Resource MIB (1)

- A host resource MIB fornece um conjunto de objetos para auxiliar o gerenciamento de recursos dos diversos sistemas operacionais
- Informações como capacidade de disco, processos em execução, números de usuários concorrentes, podem ser definidas nessa MIB
- Host resource MIB está definida na RFC 2790

Host Resource MIB (2)

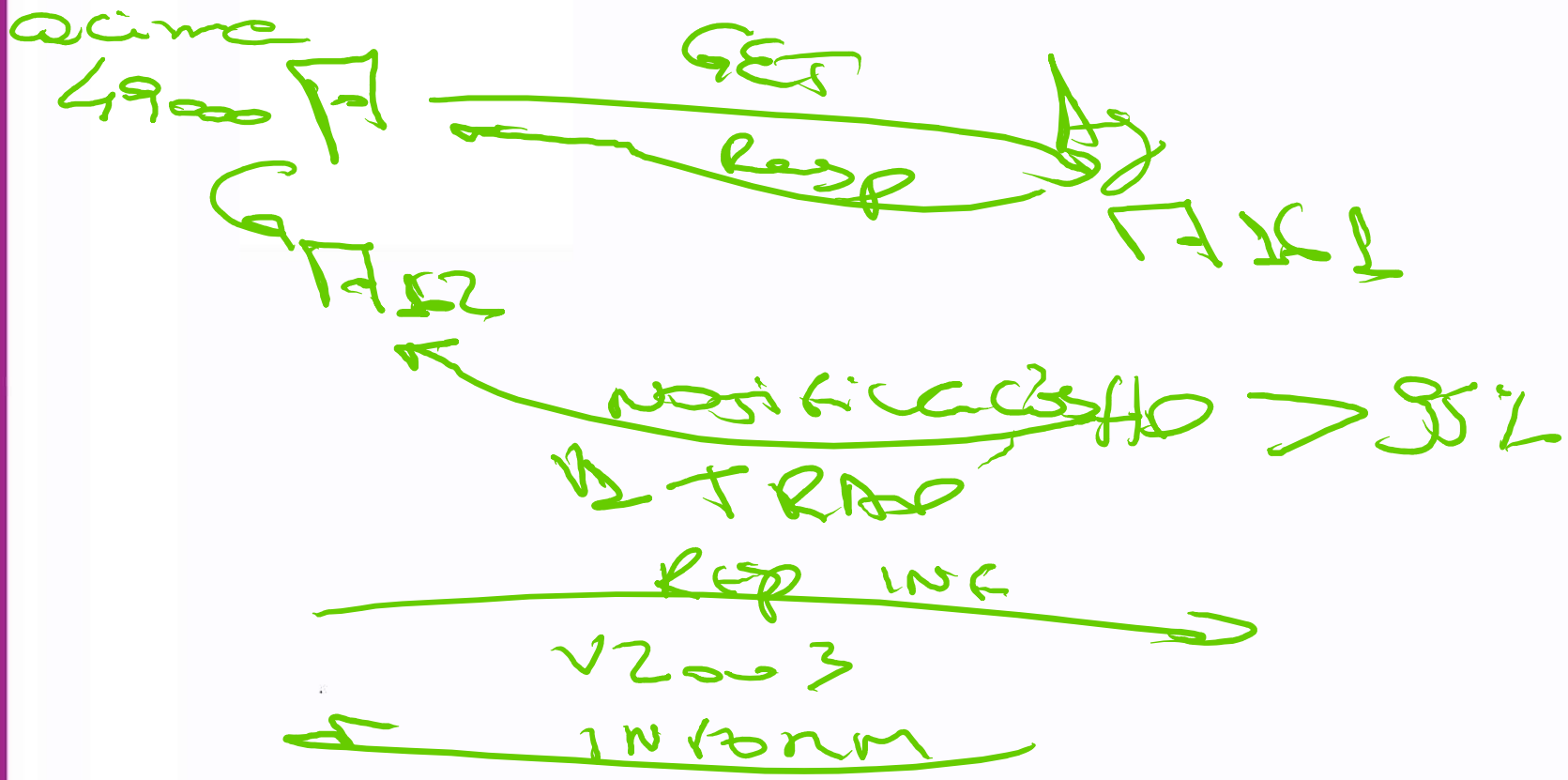
- A Host Resource MIB é importante para o gerenciamento da rede, mas nem todo agente implementa essa MIB
  - hrSystem: Objetos pertencentes ao sistema
  - hrStorage e hrDevice: armazenamento e sistemas de arquivos
  - hrSWRun: Softwares em execução
  - hrSWRunPerf: Aspectos de desempenho de softwares
  - hrSWInstalled: Softwares instalados

UDP

O SNMP usa o UDP como protocolo de transporte:

- Utiliza a porta 161 para envio e recebimento de informações no Agente
- Utiliza a porta 162 no gerente para recebimento de traps de dispositivos gerenciados

O recebimento de traps não é confirmado, na versão 2 no v3 existe o INFORM.



Comunidades (1)

- O SNMPv1 e SNMPv2 usa o conceito de comunidades para definir uma certa confiabilidade entre estação de gerência (NMS) e o agente.
- Um agente é configurado com três nomes de comunidade associadas a: read-only, read-write e trap.
- Se a NMS informa a comunidade read-only, terá acesso somente de leitura podendo, portanto, solicitar informações do agente, mas não enviar informações a ele.

Comunidades (2)

PUC Minas

- Informando a **string (comunidade)** read-write é possível enviar uma solicitação de alteração ao agente
- A string associada à permissão de trap possibilita que a NMS receba as notificações enviadas pelo agente
- Como as strings de comunidade trafegam como texto livre, isso facilita a interceptação dessas strings

- **SNMPv3 trata disso**

SNMP v1
- Comunidades
- Lista de Comandos
- E erros possíveis

SNMP v2
+ SNMP v1
+ Comandos
+ Lista genérica erros

SNMP v3
+ SNMP v2 + Criptografia
+ Visão

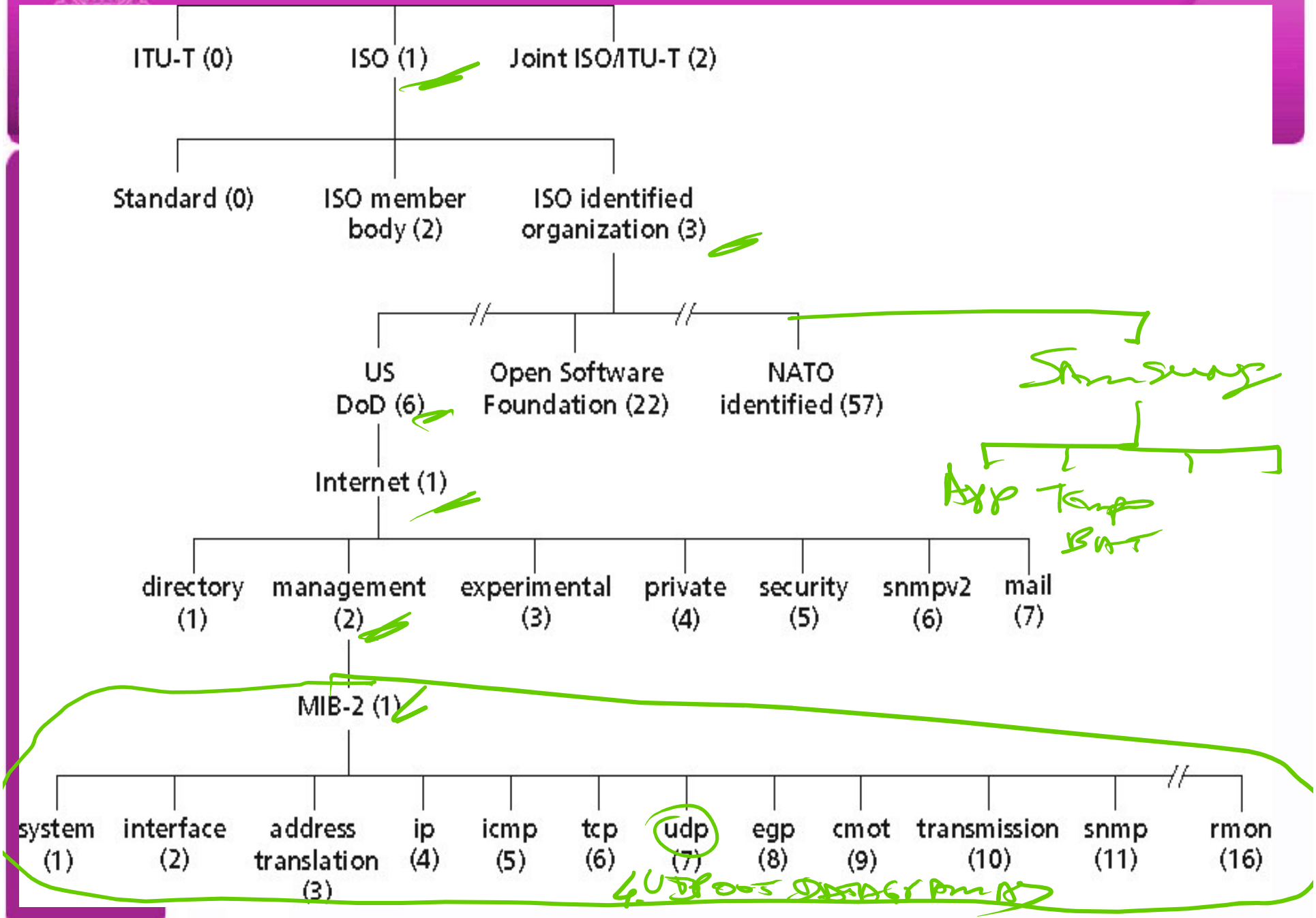
OID (1)

- SMIv1 (RFC 1155) define exatamente como os objetos gerenciados são nomeados e especifica os respectivos tipos de dados.
- A definição dos objetos gerenciados pode ser dividida em três partes:
  - Nome ou identificados do Objeto (OID – Objeto Identifier): Define exclusivamente um objeto gerenciado.
  - Tipo e sintaxe: Definida em Abstract Syntax Notation One (ASN.1)
  - Codificação: Codificada em Basic Encoding Rules (BER)

OID (2)

Object ID	Nome	Tipo	Comentários
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	número total de da **entregues** nes
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	número de datag com app destino in
1.3.6.1.2.1.7.3	UDPInErrors	Counter32	número de datagra entregues por outr
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	número de datagra enviados
1.3.6.1.2.1.7.5	udpTable		SEQUENCE uma linha uso por uma aplicaç o número da porta endereço l

porta em


ITU-T (0)
ISO (1)
Joint ISO/ITU-T (2)
Standard (0)
ISO member body (2)
ISO identified organization (3)
US DoD (6)
Open Software Foundation (22)
NATO identified (57)
Internet (1)
directory (1)
management (2)
experimental (3)
private (4)
security (5)
snmpv2 (6)
mail (7)
MIB-2 (1)
system (1)
interface (2)
address translation (3)
ip (4)
icmp (5)
tcp (6)
udp (7)
egp (8)
cmot (9)
transmission (10)
snmp (11)
rmon (16)

Operações (1)

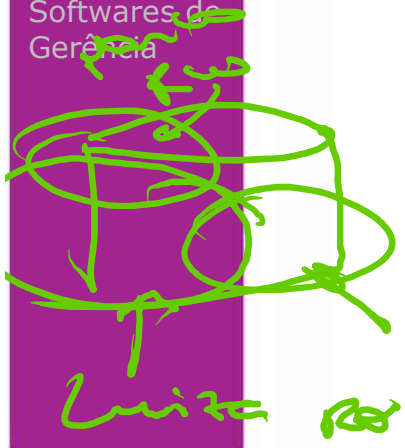
- Existe um formato (PDU) padrão para cada operação:
  - get
  - get-next
  - get-bulk (SNMPv2 e SNMPv3)
  - set
  - get-response
  - trap
  - notification (SNMPv2 e SNMPv3)
  - inform (SNMPv2 e SNMPv3)
  - report (SNMPv2 e SNMPv3)

Operações - Trap (2)

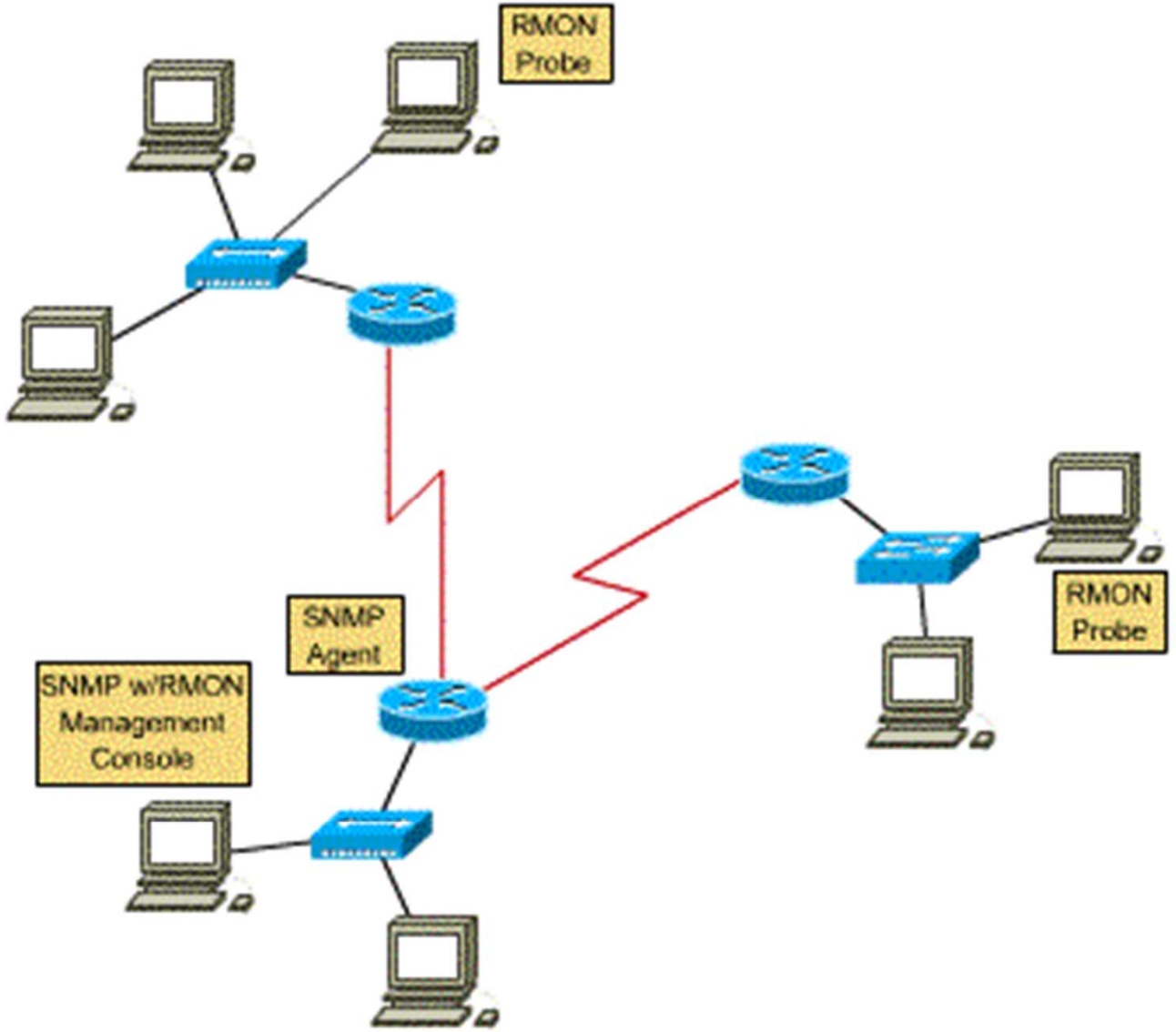
- Um meio do agente informar a NMS que aconteceu algo errado.
- Existem 6 tipos genéricos de trap:
  - coldStart(0)
  - warmStart(1)
  - linkDown (2)
  - linkUP (3)
  - authenticationFailure(4)
  - egpNeighborLoss(5)
  - enterpriseSpecific(6)

SNMPv3

- Criptografia: mensagem SNMP criptografada com DES
- Autenticação: calcular, enviar MIC(m,k): calcula hash (MIC) sobre a mensagem (m), com chave secreta compartilhada (k)
- Proteção contra playback: usar nonce
- Controle de acesso baseado em visões
  - A entidade SNMP mantém uma base de dados de direitos de acesso e regras para vários usuários
  - A própria base de dados é acessível como um objeto gerenciado!



Network With RMON Probes



RMON (2)

Objetivos do Monitoramento Remoto

Coleta de dados de valor agregado

Detectar e relatar problemas

Utilização de múltiplos gerentes

Propiciar operação off-line

Monitoramento preemptivo

RMON 2

Atua a partir da camada de rede