SSC-0158
Computação em Nuvem

Aula 11 – Monitoração, Gerência, Protocolos e Ferramentas

Prof. Julio Cezar Estrella
jcezar@icmc.usp.br

O que é monitoração?

“Observar em determinado período de tempo se as condições de um objeto/equipamento está dentro dos padrões”

Porque monitorar?

- Determinar partes mais utilizadas do sistema;
- Determinar Gargalos de Desempenho;
- Ajustar Parâmetros de Configurações de Hardware;
- Caracterizar Carga de Trabalho que o sistema pode suportar, devido a variabilidade computacional;

Ferramentas (Algumas)

- DSTAT
- Sysstat
- Zabbix

DSTAT

- Combinação do vmstat, iostat, ifstat, netstat é muito mais…
- Disponível para:
  - Red Hat Enterprise Linux / CentOS
  - Fedora
  - Gentoo
  - OpenSUSE
  - Debian
  - Mandriva
  - Caos
  - Ubuntu Breezy
  - Linspire
  - Sourcemage
  - Rpath
  - PLD Linux
  - Slackware
  - Tiny Core Linux

FONTE: http://dag.wiee.rs/home-made/dstat/

Zabbix

- Um software gratuito de código fonte aberto, com sistema de monitoramento distribuídos, capaz de monitorar a disponibilidade e desempenho da infraestruturade redes e aplicações
- http://www.zabbix.com

Gerência

- **Gerência** → Métodos para planejar, configurar, controlar, monitorar, corrigir falhas e administrar redes de computadores
  - **Modelo Gerente-Agente**
    - nós gerenciáveis – 1 ou mais nós gerenciáveis
    - estrutura de informação de gerenciamento – SMI (regras de descrição dos objetos)
    - base de informações de gerenciamento – MIB (conjunto de informações de gerenciamento)
    - operações de gerenciamento – primitivas para manipulação via usuários.

Gerência

- **Gerenciamento de rede:**

“Inclui a disponibilização, a integração e a coordenação de elementos de hardware, software e humanos para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável.”

[Saydam, 1996]

Gerência

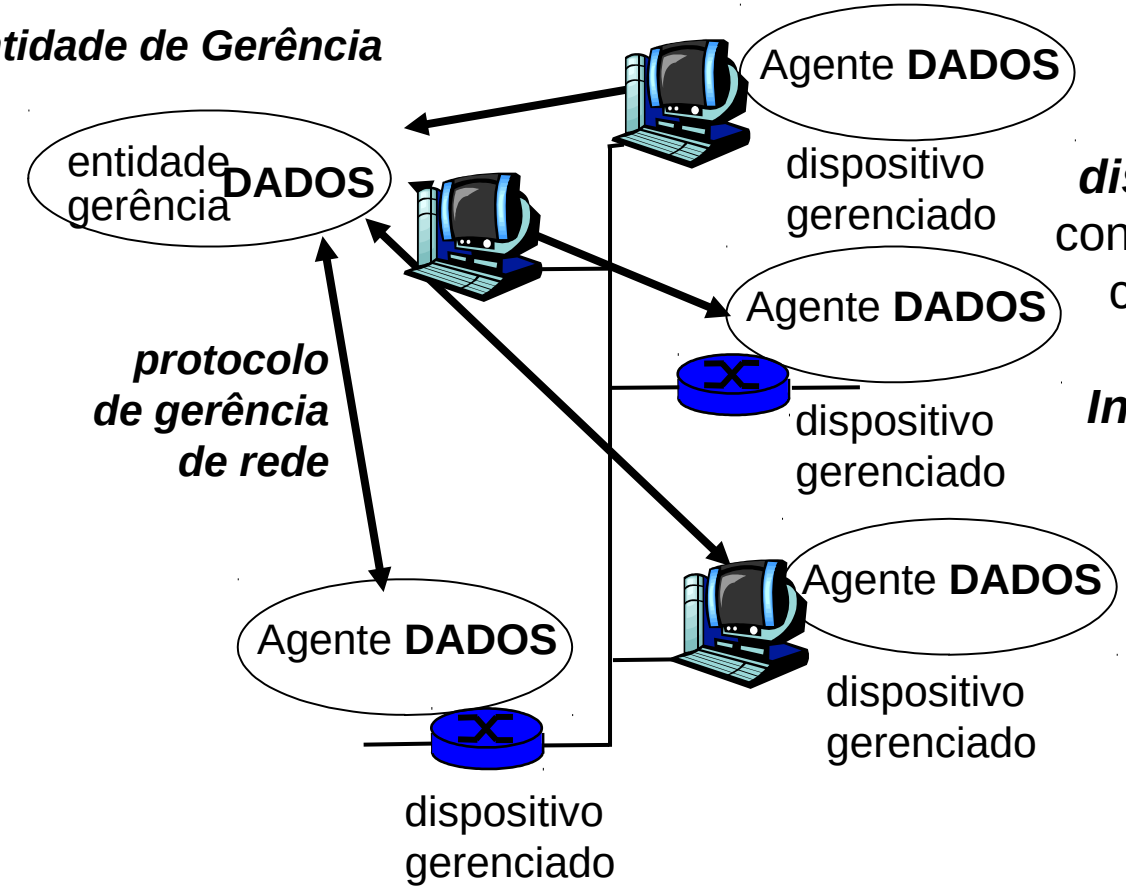
- Sistemas autônomos (i.é., “rede”): centenas ou milhares de componentes de hw/sw interagindo.
- Outros sistemas complexos que necessitam de monitoração e controle:
  - Aeronave.
  - usina nuclear.
  - Outros?
- Gerência de rede inclui instalação, integração e coordenação de elementos de hardware, software e humanos para monitorar, testar, checar, configurar, analisar, avaliar e controlar a rede e recursos destes elementos para atingir os requisitos de tempo real, desempenho operacional e Qualidade de Serviço a um custo razoável.

Gerência

- A *International Organization for Standardization* (ISO) definiu as principais áreas de gerenciamento de rede.

- A divisão proposta engloba as seguintes áreas:
  - Gerência de falhas;
  - Gerência de contabilização;
  - Gerência de configuração;
  - Gerência de segurança;
  - Gerência de desempenho.

Infraestrutura para Gerência de Redes



dispositivos gerenciados contêm ***objetos gerenciados*** cujos dados são reunidos numa ***Base de Informações de Gerência (MIB)***

Padrões de Gerenciamento

- OSI CMIP - Common management information protocol:
  - Projetado nos anos 80: considerado o padrão de gerenciamento por excelência.
  - Padronização lenta demais.
  -
- SNMP: Simple Network Management Protocol:
  - Origem na Internet (SGMP).
  - Começou simples.
  - Desenvolvido e adotado rapidamente.
  - Crescimento: em tamanho (abrangência) e complexidade.
  - Atualmente: SNMP V3.
  - Padrão de fato para gerenciamento de redes.

Protocolo de Gerenciamento

- SNMP é o padrão para protocolo de gerência mais popular.
- Foi o padrão adotado por vários fabricantes e operadoras.
- Define como funciona a arquitetura de gerenciamento de redes TCP/IP.
- É simples para ser implementado em todo tipo de equipamentos e flexível o bastante para aceitar futuras modificações.
- É o protocolo de gerenciamento da arquitetura TCP/IP. Define como funciona a arquitetura de gerenciamento Internet.

Protocolo de Gerenciamento

- Protocolo assíncrono de requisição e reposta (*request/response*)
- Único requisito de transporte do SNMP é um serviço de transporte sem conexão
- Permite a uma NMS centralizada consultar agentes para obter e modificar informações nas MIBs

Protocolo SNMP

O SNMP é um protocolo de gerência utilizado para obter informações de servidores SNMP - agentes espalhados em uma rede baseada na pilha de protocolos TCP/IP.

Protocolo SNMP – Visão Geral

1. Management Information Base (MIB):
   - Base de dados distribuída com dados de gerenciamento de rede.
2. Structure of Management Information (SMI):
   - Linguagem de definição para objetos da MIB.
3. Protocolo SNMP:
   - Transporta informações e comandos sobre objetos entre o gerenciador e o elemento gerenciado.
4. Segurança, capacidades administrativas.

SMI

- Structure of Management Information (SMI)
  - Finalidade: definir bem e sem ambigüidade a sintaxe e semântica dos dados de gerência.
  - tipos básicos de dados
    - Formato genérico dos dados.
  - TIPO DO OBJETO
    - tipo dos dados, status, semântica do objeto gerenciado
  - IDENTIDADE DO MÓDULO
    - agrupa objetos relacionados em módulos MIB

Protocolo SNMP

- Duas formas de transportar info das MIBs e comandos:
  - Polling: “Entidade de Gerência” interroga cada “dispositivo gerenciado” e recebe as infos das MIBs. Usa a Tabela de Polling.
  - Trap: “Dispositivo gerenciado” percebe um evento gerenciado que atingiu os limites de variação estabelecidos previamente e envia info da MIB à “Entidade de Gerência”.

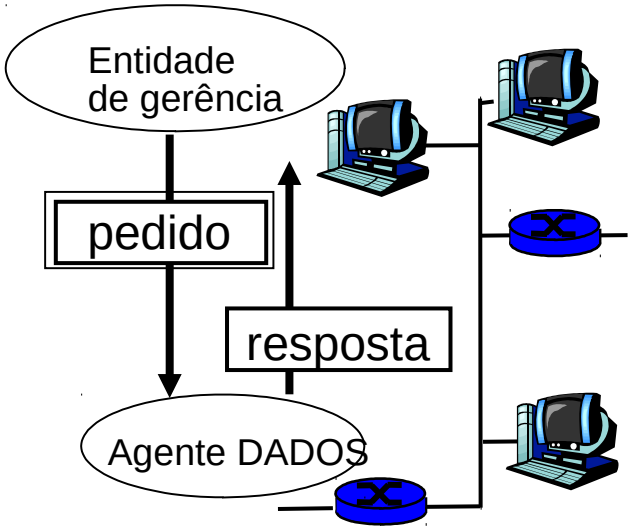
ANS.1

- ASN.1 (Abstract Syntax Notation One)
  - Linguagem formal para definição de sintaxe abstrata (ISO) (descrição dos dados)
- 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

Protocolo SNMP

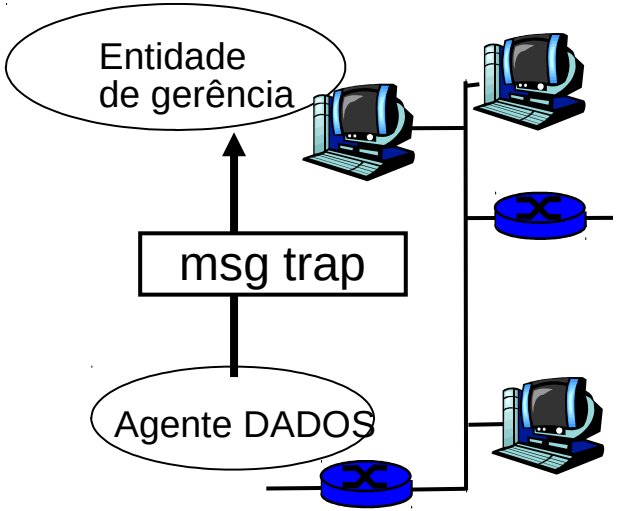
- No SNMP os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP, para enviar e receber suas mensagens através da rede.

Protocolo SNMP



Dipositivo Gerenciado.

Modo pedido/resposta (Polling)



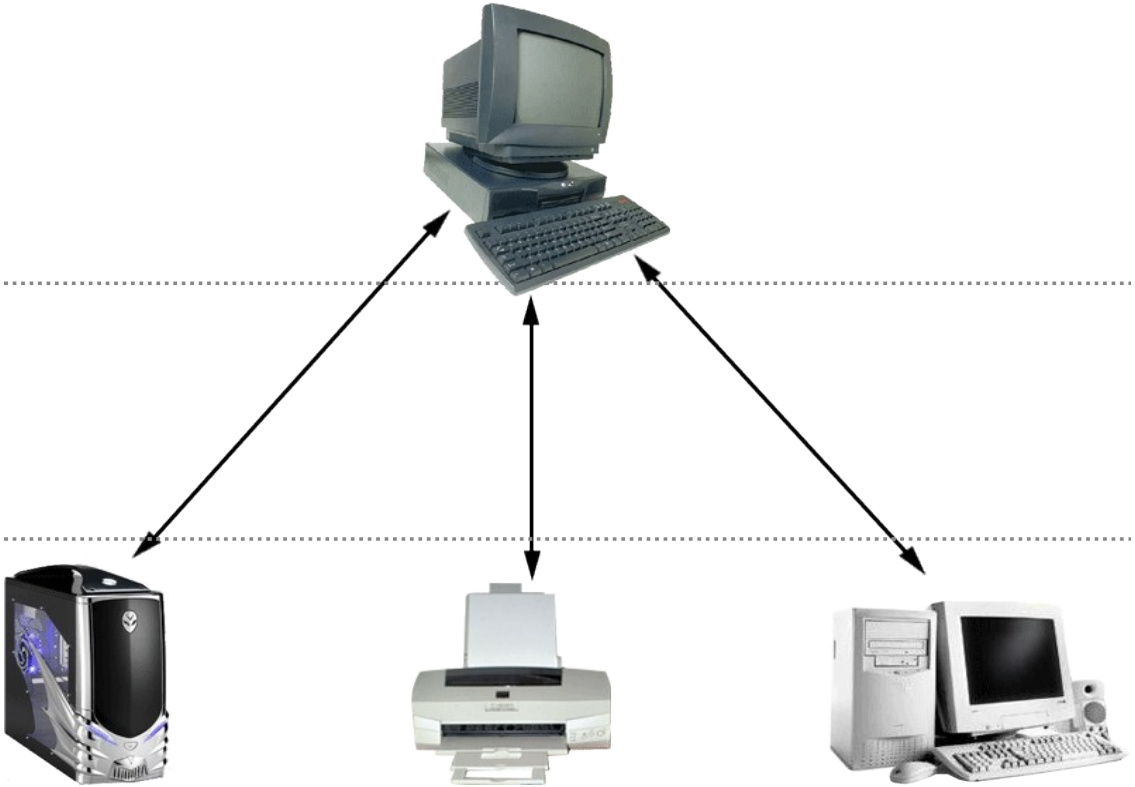
Dispositivo Gerenciado

modo interrupção (TRAP)

Segurança e Administração

- Criptografia: mensagem SNMP criptografada com DES.
- Autenticação
- Proteção contra playback: usa Nonce.
- Controle de acesso baseado em visões (Comunidades):
  - 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.

O que monitorar?



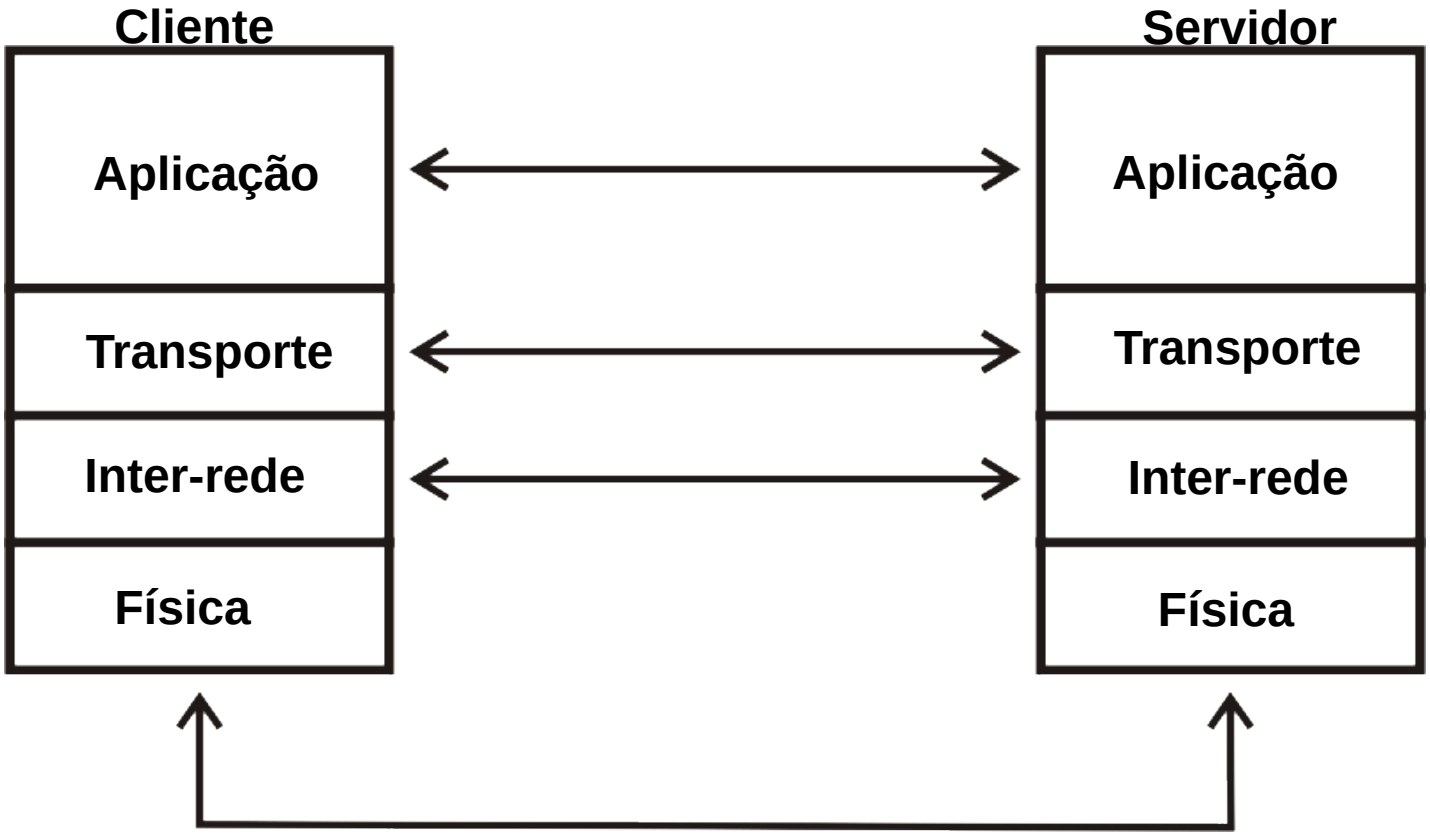
SNMP/TCP/IP

- O TCP/IP é o acrônimo para “Transmission Control Protocol / Internet Protocol”, e serve para caracterizar a família de protocolos utilizada nas comunicações de computadores.

SNMP/TCP/IP

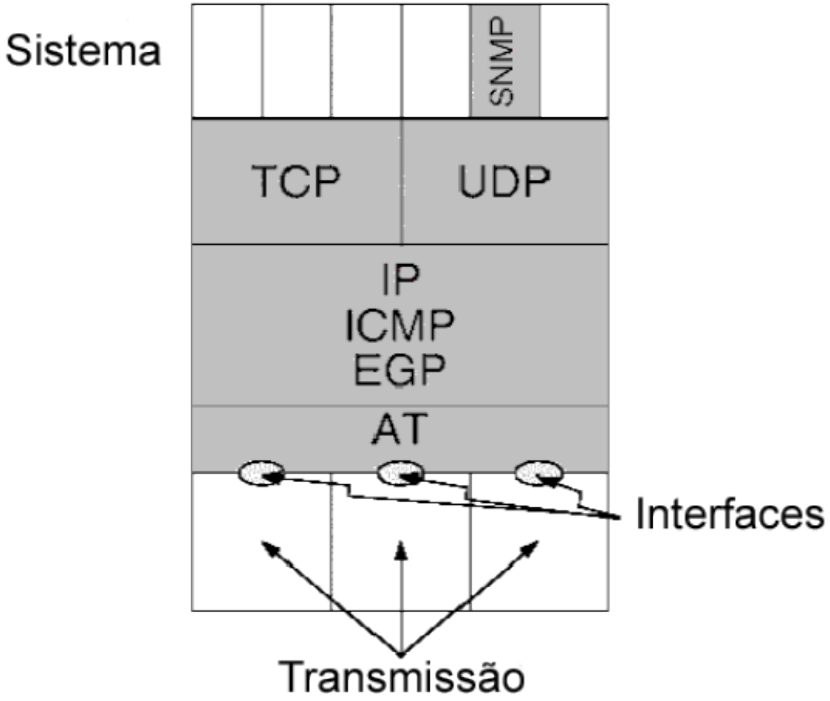
- É apresentado por meio de um modelo de 4 camadas que descreve o caminho que a informação percorre por uma rede:
  - *Camada de aplicativo;*
  - *Camada de transporte;*
  - *Camada de Inter-rede;*
  - *Camada Física;*

SNMP/TCP/IP


Cliente
Servidor
Aplicação
Transporte
Inter-rede
Física
Aplicação
Transporte
Inter-rede
Física

SNMP/TCP/IP

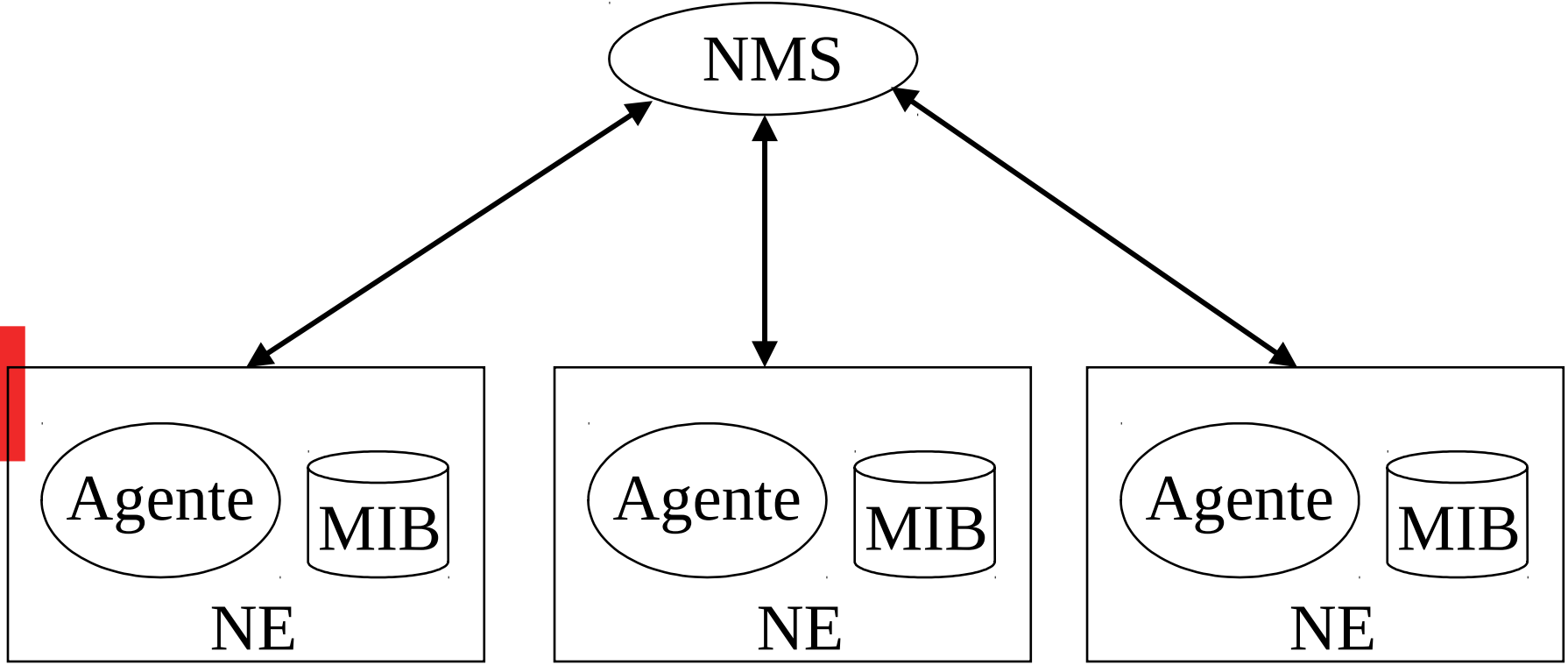
Localização do protocolo SNMP na pilha TCP/IP



Características do SNMP

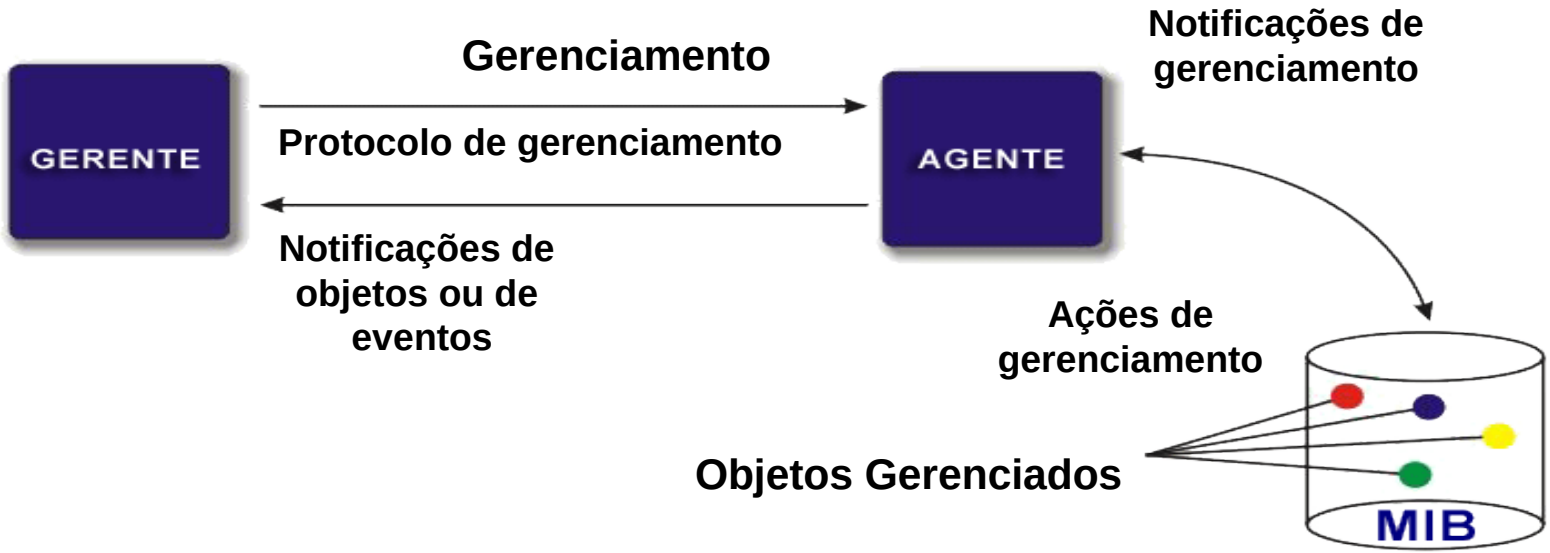
- O modelo de gerenciamento SNMP para redes TCP/IP, é composto pelos seguintes elementos:
  - *Estação de gerenciamento (NMS);*
  - *Agente de Gerenciamento;*
  - *Base de Informações (MIB);*
  - *SNMPv1, SNMPv2, SNMPv3;*

MIBs SNMP



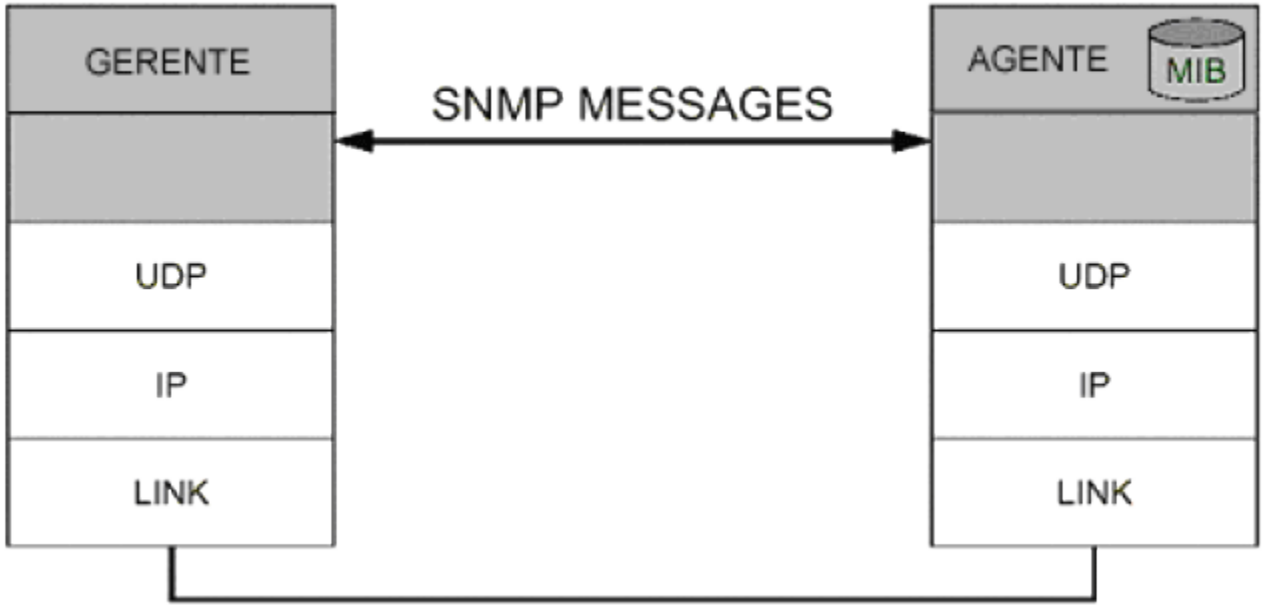
Fluxo do SNMP

Diagrama de fluxo do SNMP



Gerente e Agente SNMP

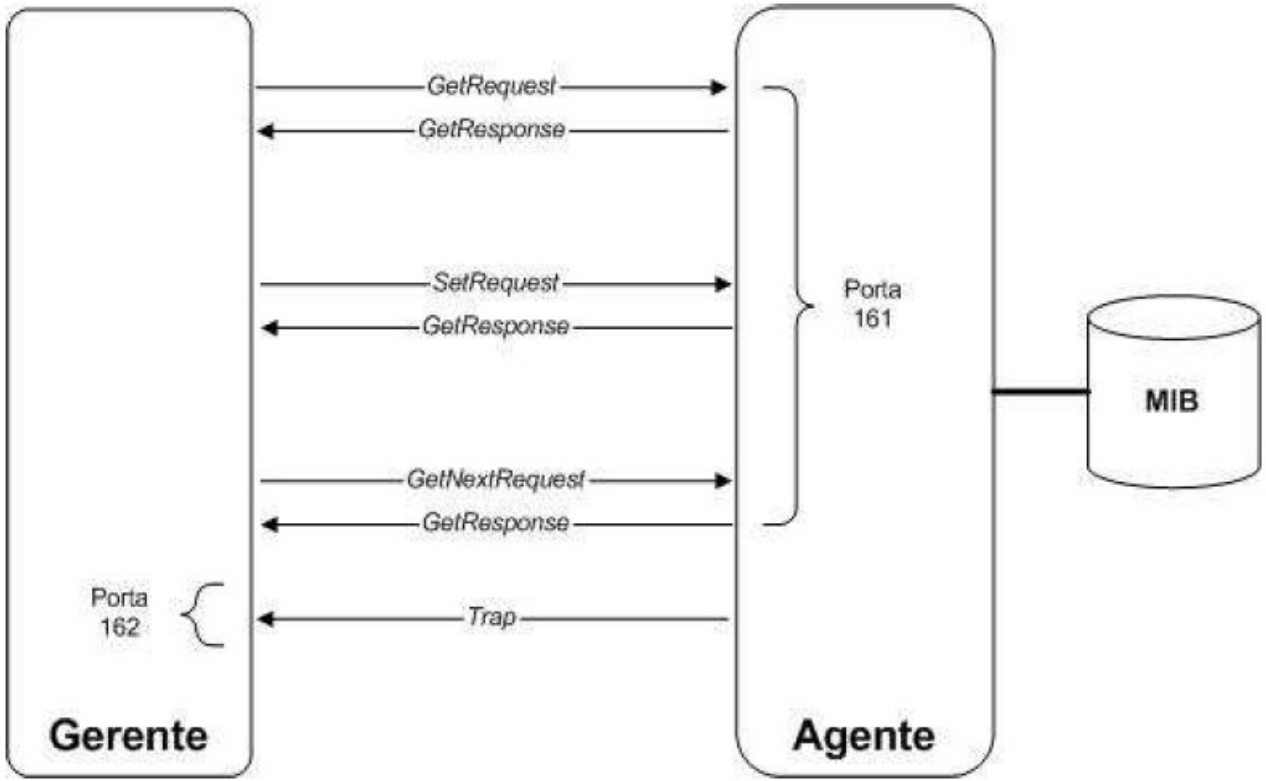
Relacionamento entre gerente e agente baseado no modelo TCP/IP



Operações do SNMP

- **GET**
  - Utilizada para ler o valor de uma variável; o gerente solicita que o agente obtenha o valor da variável
- **SET**
  - Utilizada para alterar o valor da variável; o gerente solicita que o agente faça uma alteração no valor de uma variável
- **TRAP**
  - Utilizada para comunicar um evento; o agente comunica ao gerente o acontecimento de um evento previamente determinado

Comunicação SNMP



MIB SNMP

MIB – *Management Information Base*

“Conjunto de objetos gerenciados, que abrange as informações necessárias para a gerencia da rede.”

Objetos Gerenciandos - SNMP

- *“Visão abstrata de um recurso real do sistema.”*
- **Objetos gerenciados:**
  - todos os recursos que devem ser gerenciados.
- Exemplo: Consumo de banda, Status de operação, colisões de pacotes

Tipos de MIB - SNMP

- Três tipos de MIBs:
  - MIB II: Estão os objetos usados para obter informações específicas dos dispositivos de rede.
  - MIB experimental: É aquela em que seus objetos ainda estão sendo pesquisados pela IAB (*Internet Architecture Board*)
  - MIB privada: É aquela que contém objetos definidos por outras organizações.

MIB - SNMP

- MIB-I
  - SNMP foi desenvolvido primariamente para gerenciar redes TCP/IP, assim a primeira MIB padronizada continha informações específicas a TCP/IP como:
    - número de interfaces de rede com seus endereços IP
    - contadores de datagramas UDP
    - tabela de conexões TCP ativas

MIB - SNMP

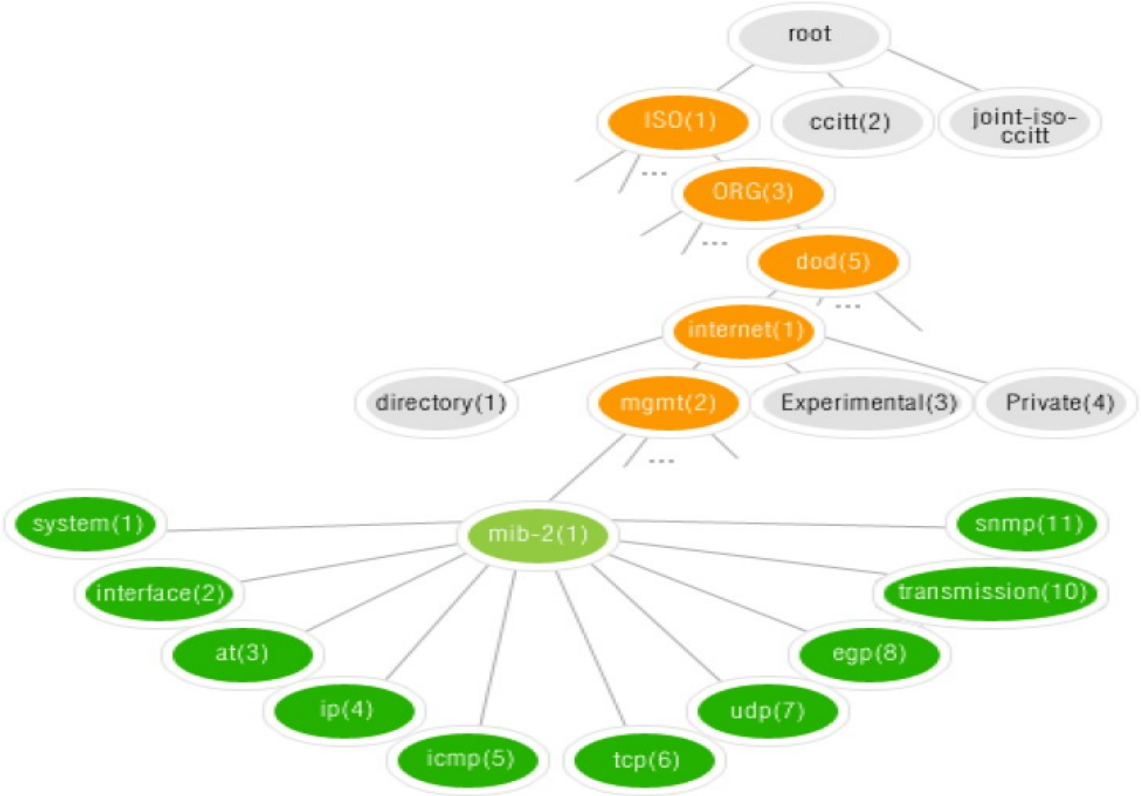
- MIB-II
  - Esta MIB, total ou parcialmente, é normalmente implementada em produtos comerciais. Contém objetos relacionados com características normalmente encontradas nos equipamentos ligados em redes
- A MIB-II é a MIB implementada por padrão em todos os agentes com suporte a SNMP.

SMI e ANS.1 - SNMP

- As regras de construção das estruturas da MIB são descritas através da SMI – *Structure of Management Information*.

- Cada objeto da MIB é especificado de acordo com a ASN.1 – *Abstract Syntax Notation One e contém: Nome, identificador, sintaxe, definição e acesso*

Estrutura Lógica da MIB



Estrutura Lógica da MIB

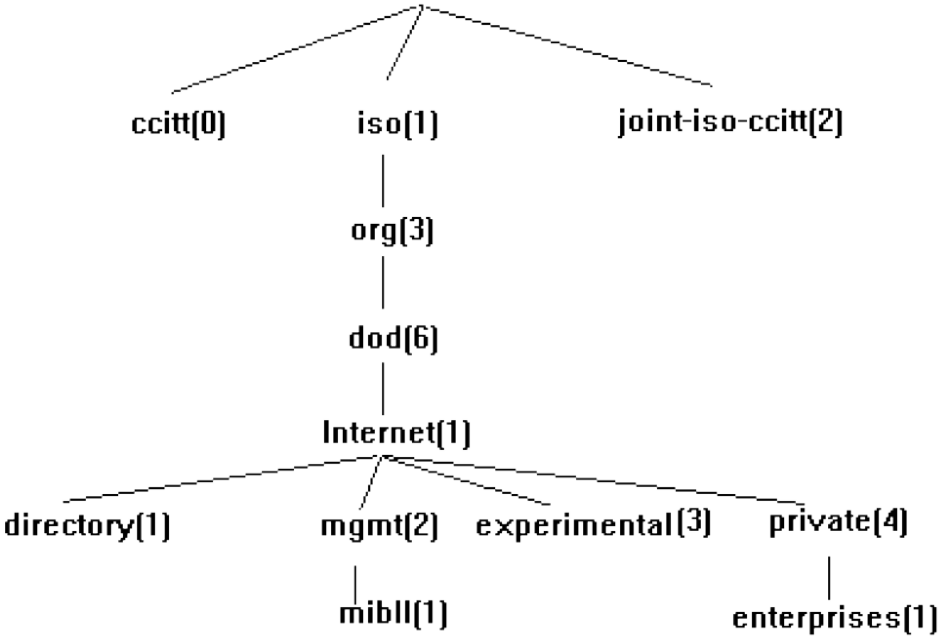
- A partir da raíz, temos 3 ramos:
  - ITU-T (CCITT) [0]
  - ISO [1]
  - Joint ITU-T e ISO [2]
- O ramo iso por sua vez se ramifica em:
  - Standard [0]
  - Registration Authority [1]
  - Member-body [2]
  - Identified-Organization [3]

Estrutura Lógica da MIB

- Dentro de [3], temos o Department of Defense (DoD) [6] e abaixo o IAB (Internet Architecture Board) [1], assim iso.identified-organization.DoD.IAB == 1.3.6.1
- Este normalmente é o prefixo para todos os objetos de interesse na área de gerenciamento.

Estrutura Lógica da MIB

Arvore hierárquica definida pela ISO



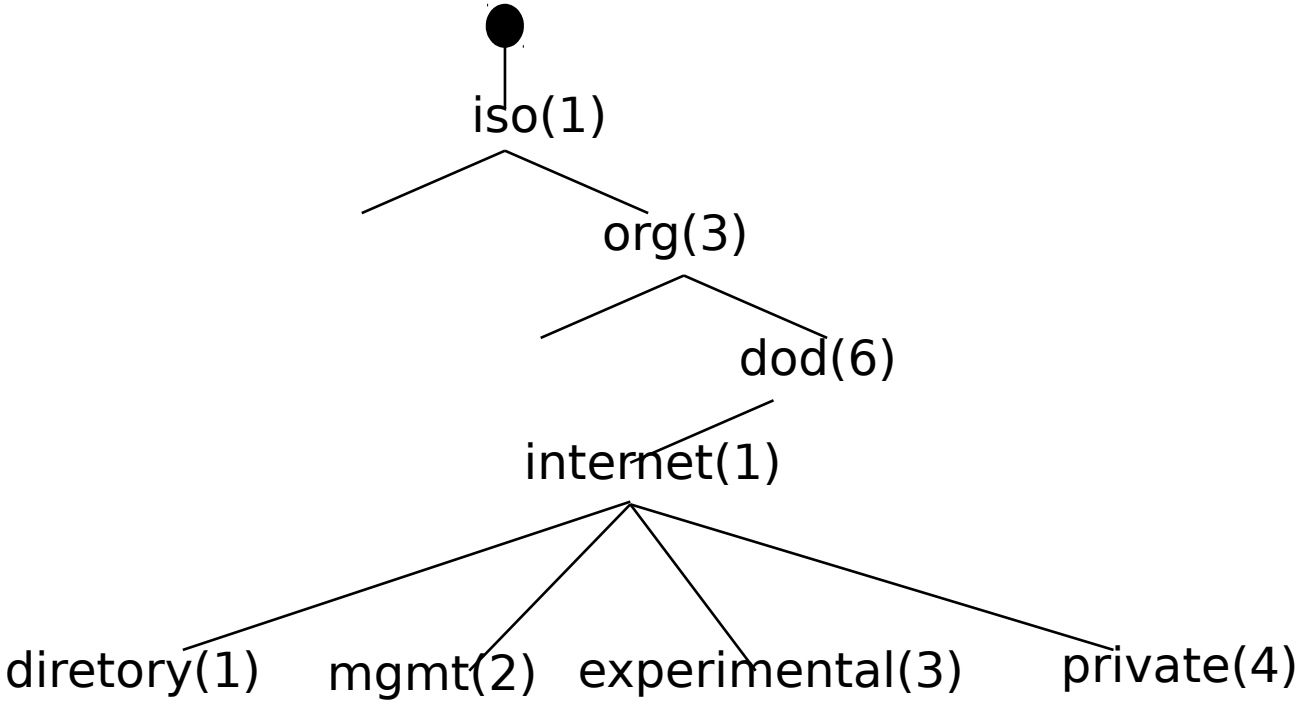
Estrutura Lógica da MIB

- Os inteiros indicam a seqüência de nodos ao longo de um caminho iniciando no topo da árvore.
- A árvore é estática, significando que os nodos são determinados quando a MIB é designada.
- Em acréscimo, para prover identificação única de tipos de objetos, a estrutura da árvore mostra grupos de objetos abaixo de uma única sub-árvore. Um nome próprio (correspondente ao identificador do objeto) é também associado ao tipo de objeto.

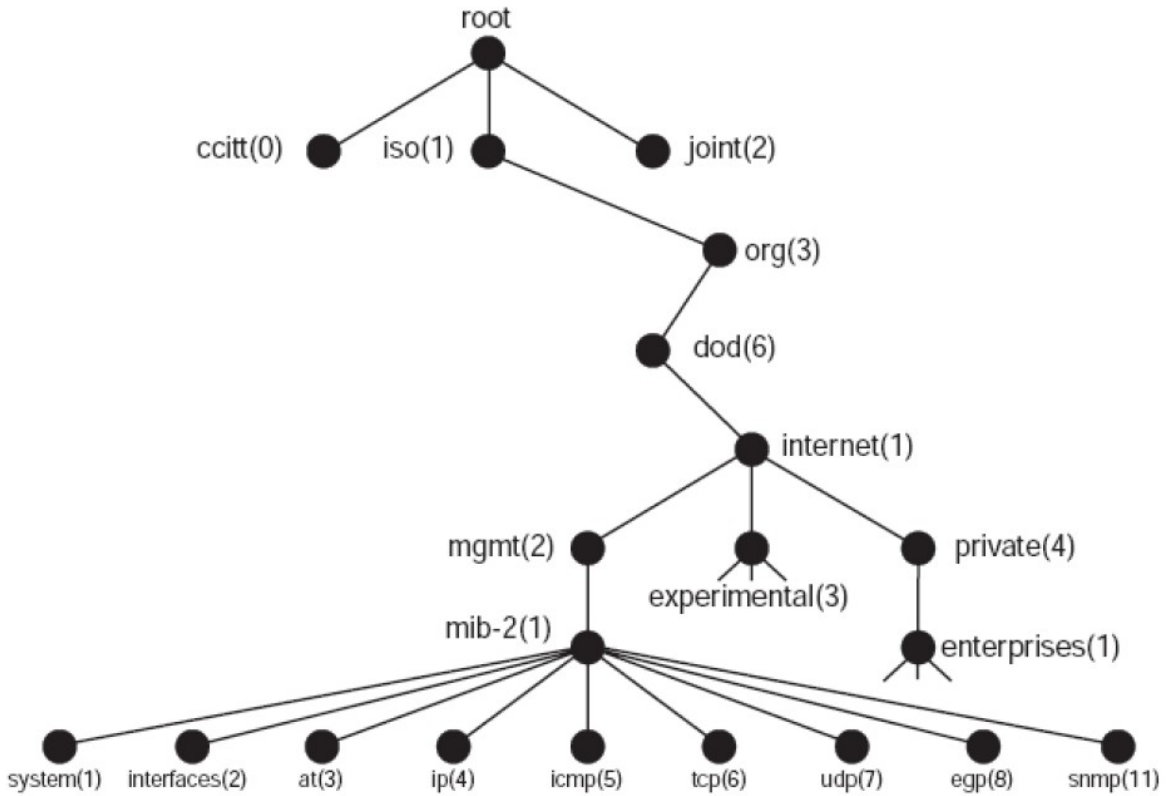
Estrutura Lógica da MIB

- A sintaxe define a estrutura de dados abstrata. Um subconjunto da ASN.1 é utilizada para definição de tipos de dados e suas propriedades.
- A codificação de objetos segue as regras básicas de codificações com ASN.1.
- Dados gerenciados são indexados pelas folhas, localizadas na base da árvore

Estrutura em Árvore da MIB SNMP



Estrutura em Árvore da MIB-II SNMP



Estrutura em Árvore da MIB-II SNMP

- Abaixo do ramo Internet, tem-se:
  - directory (1): uso futuro com serviços de diretórios OSI
  - mgmt (2): objetos definidos por documentos do IAB
  - experimental (3): objetos para testes e pesquisas
  - private (4): objetos definidos por grupos ou organizaçoes, como fabricantes por exemplo
- Logo abaixo do ramo mgmt (2) tem-se a

Grupos da MIB

Group	Objects for	#
System	Basic system information	7
Interfaces	Network attachments	23
AT	Address translation	3
IP	Internet protocol	42
ICMP	Internet control message protocol	26
TCP	Transmission control protocol	19
UDP	User datagram protocol	7
EGP	Exterior gateway protocol	18
SNMP	SNMP applications entities	39
Legend: # = Number of objects in the group		

Grupos da MIB

- **system**: informações gerais do agente/equipamento (descrição, up time, pessoa de contato)
- **interfaces**: descrição das interfaces do equipamento, endereços físicos e contadores
- **at** (address translation): mapeamento de endereços físicos/rede
- **ip**: tabelas de endereçamentos e contadores
- **icmp**: contadores ICMP
- **tcp**: tabela de conexões TCP e contadores
- **udp**: tabela UDP e contadores
- **egp**: tabela de vizinhos EGP e contadores
- **snmp**: registros estatísticos das mensagens SNMP

Grupos da MIB

- Houve extensões da MIB a partir do número 13
  - MIBs privadas – cada fabricante possuir seu próprio número
  - Novo grupo – transmission - onde ficam abaixo somente grupos de objetos relacionados com tecnologias de transmissão (tecnologias de rede).

Declarações das MIBs

- ✓ MODULE-IDENTITY
- ✓ OBJECT-IDENTITY
- ✓ OBJECT-TYPE
- ✓ NOTIFICATION-TYPE
- ✓ TEXTUAL-CONVENTION
- ✓ OBJECT-GROUP
- ✓ MODULE-COMPLIANCE
- ✓ AGENT-CAPABILITIES

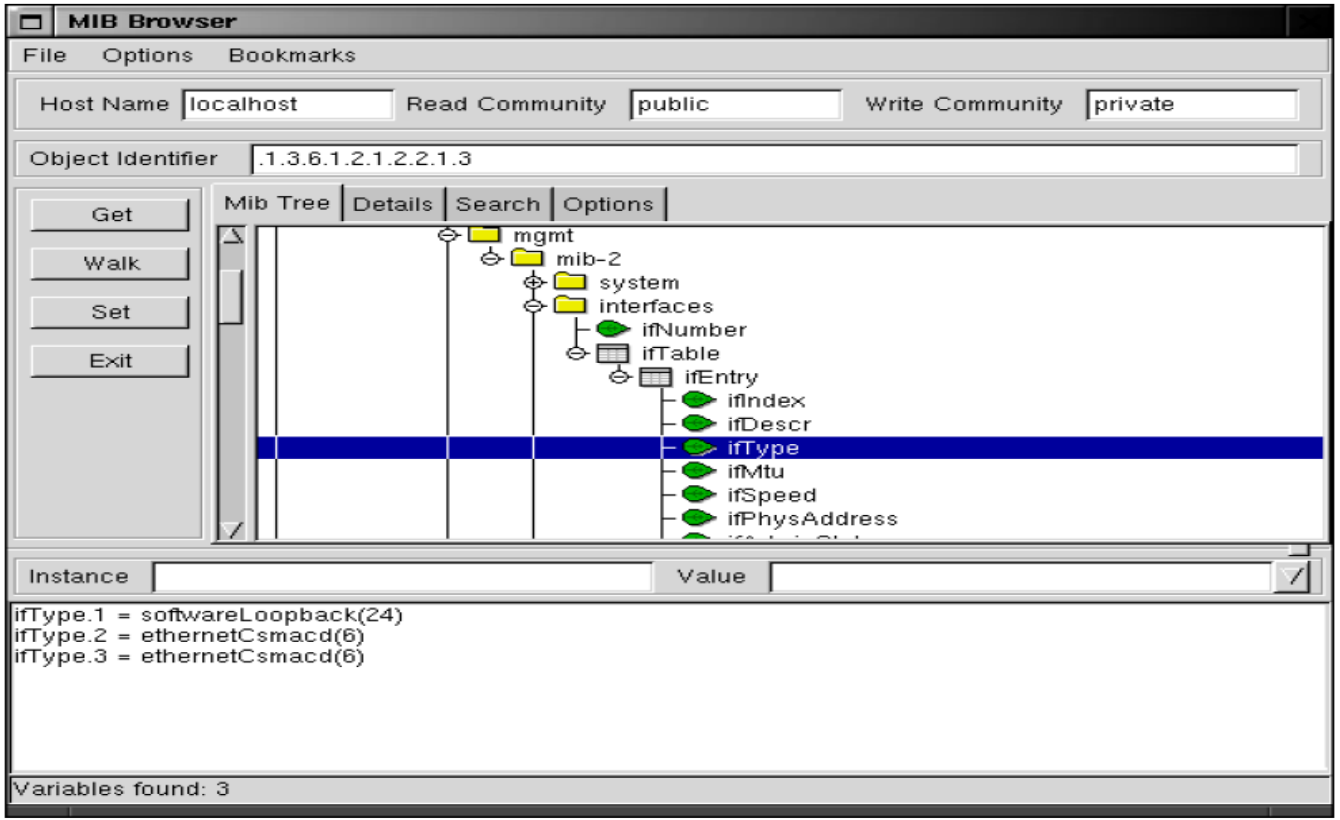
Declarações das MIBs

- A SMIv2 criou várias MACROS para melhorar as declarações de módulos de MIB.
- MODULE-IDENTITY . define, através de uma seção de identificação comum, um módulo de MIB
- OBJECT-TYPE . sintaxe e semântica de um objeto gerenciado
- OBJECT-IDENTITY . texto adicional sobre um objeto gerenciado

Declarações das MIBs

- NOTIFICATION-TYPE
  - sintaxe de um notificação SNMPv2 (trap). Substituiu a macro TRAP-TYPE, usada em SNMPv1
- TEXTUAL-CONVENTION
  - sintaxe refinada de um tipo de dado (melhora a compreensão de um tipo de dado específico).
- OBJECT-GROUP
  - define um conjunto de objetos relacionados
- MODULE-COMPLIANCE
  - lista os módulos de MIB obrigatórios ou opcionais
- AGENT-CAPABILITIES
  - detalha uma implementação particular
- Várias das MIB's criadas com a SMIv1, foram relançadas sob a SMIv2, inclusive vários dos grupos de objetos da MIB-II

MIB Browser


MIB Browser
File
Options
Bookmarks
Host Name
localhost
Read Community
public
Write Community
private
Object Identifier
.1.3.6.1.2.1.2.2.1.3
Get
Walk
Set
Exit
Mib Tree
Details
Search
Options
mgmt
mib-2
system
interfaces
ifNumber
ifTable
ifEntry
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
Instance
Value
ifType.1 = softwareLoopback(24)
ifType.2 = ethernetCsmacd(6)
ifType.3 = ethernetCsmacd(6)
Variables found: 3

MIB Browser

- Um MIB browser é uma aplicação que permite a obtenção (e alteração) de variáveis numa MIB de um agente SNMP. Este utilitário oferece uma interface adequada de visualização de objetos e seus valores e executa as operações SNMP necessárias para obter informações e alterá-las nos agentes.
- Opções livres:
  - Mib browser - http://www.ireasoning.com/mibbrowser.shtml
  - ServersCheck - https://serverscheck.com/mib_browser/
- Há várias opções comerciais que disponibilizam versões TRIAL.

Ferramentas de Gerência SNMP

- Comerciais
  - OpManager
    - https://www.manageengine.com/network-monitoring/
- Dominio público
  - MRTG
    - https://oss.oetiker.ch/mrtg/index.en.html
  - Cacti
    - https://www.cacti.net/

TCP e SNMP

- 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

TCP e SNMP

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

Vantagens do SNMP

- O agente SNMP é pequeno e simples
- Flexibilidade: Construção de MIB’s definida pelo usuário.
- Uso de um protocolo bem definido
- Disponibilidade de ferramentas da área de redes.

Desvantagens do SNMP

- Não é adequado para redes muito grandes;
- Traps SNMP não são reconhecidos;
- O padrão SNMP básico provê somente autenticação trivial;
- Não suporta comunicação manager-to-manager;

Conclusão

- Gerenciamento de rede:
  - Extremamente importante: representa 80% do “custo” da rede.
  - Padrão ASN.1 para descrição dos dados.
  - Protocolo SNMP como uma ferramenta para transportar a informação.
- Gerenciamento de rede: mais arte do que ciência:
  - O que medir/monitorar?
  - Como responder a falhas?
  - Correlação/filtragem de alarmes?

Referências

KUROSE, J.; ROSS,K. W. **Redes de Computadores e a Internet, 2016**

BRANCO, K. R. J. C; **Notas de Aula – Administração e Gerenciamento de Redes**.