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

Gerência de Redes de Computadores
SNMP

Prof. Alex Furtunato

alex.furtunato@ifrn.edu.br

SNMP

- Simple Network Management Protocol
  - Provê uma ferramenta padrão, adotada por todos os fornecedores
  - Disponível em praticamente todos os tipos de produtos conectados a uma rede
  - Baseado em TCP/IP
  - Composto por:
    - Um protocolo de comunicação
    - Uma especificação de estrutura de base de dados (MIB)
    - Um conjunto de objetos

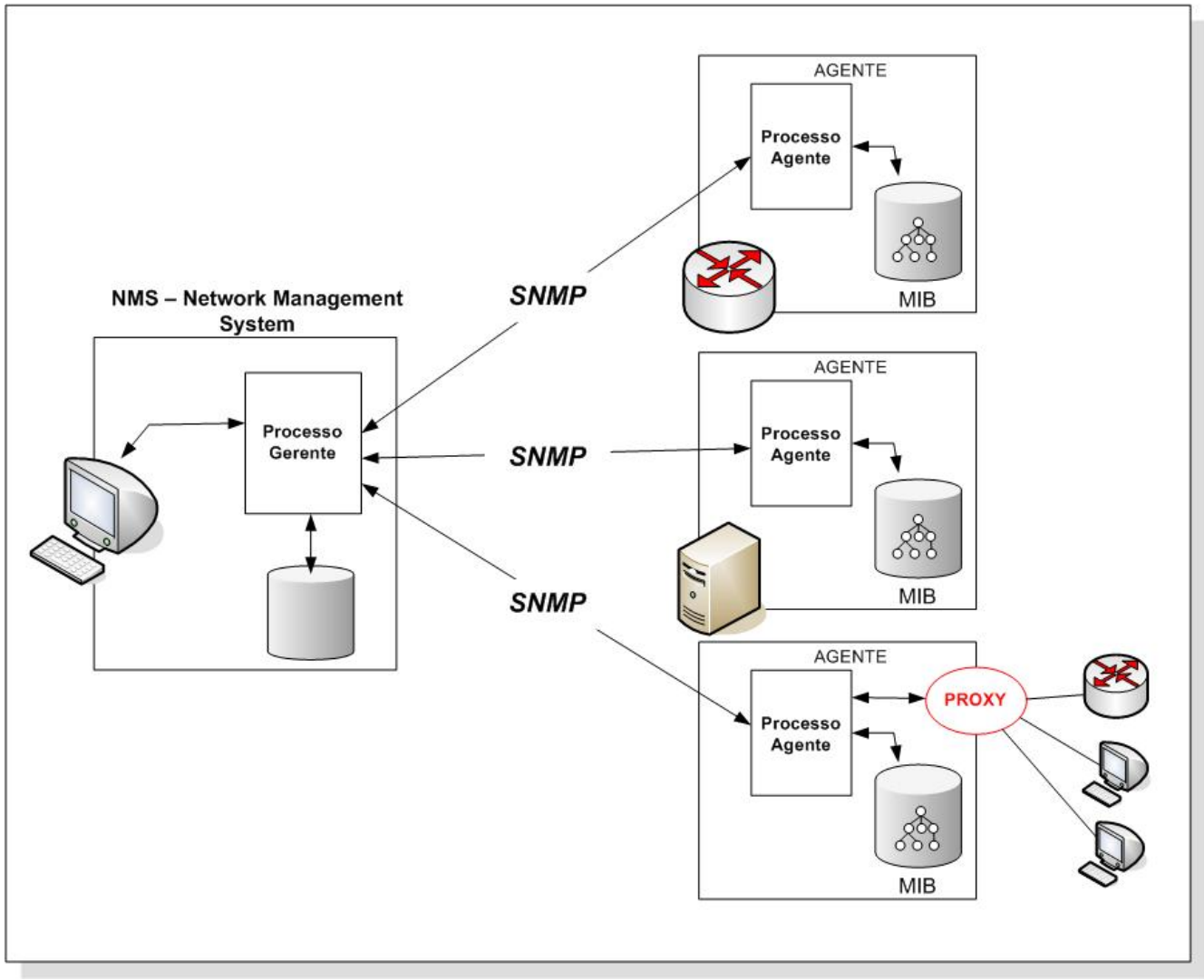
Histórico

- SMI (Structure of Management Information) especificada na RFC 1155
- MIB I (Management Information Base I) especificada na RFC 1156
- SNMPv1 (Simple Network Management Protocol version 1) especificada na RFC 1157
- MIB II especificada na RFC 1213
- SNMPv2 especificada na RFC 1902
- SNMPv3 especificada na RFC 3410

Componentes da Arquitetura SNMP

- Estação de Gerenciamento
- Agente de Gerenciamento
- Base de Informações Gerenciadas (MIB)
- Protocolo de Gerenciamento

Arquitetura SNMP



Classificação das informações

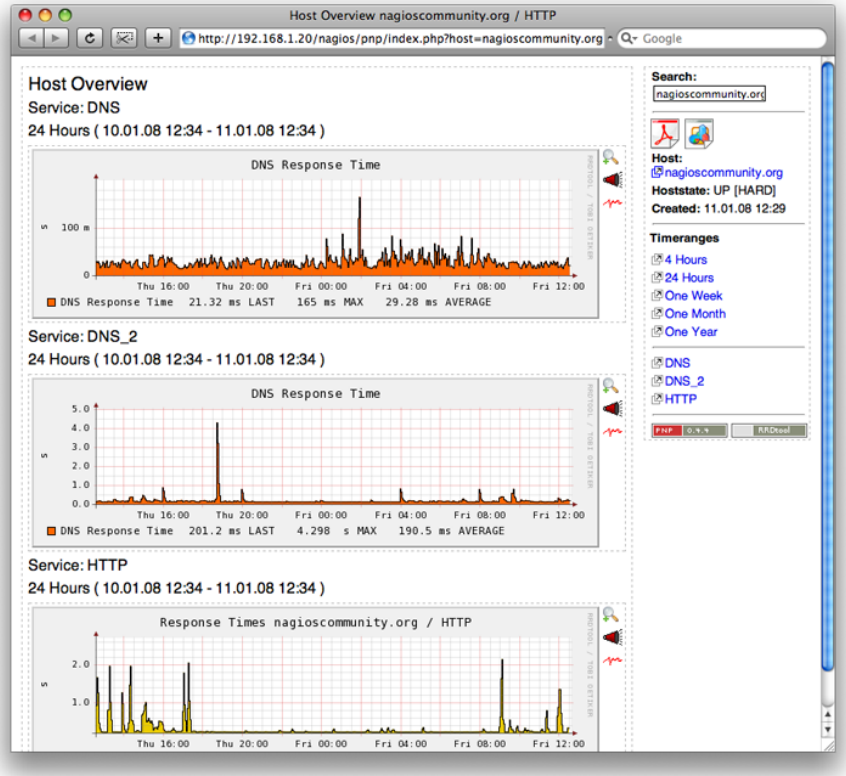
- Estática
  - Informações de configuração que sofrem pouca ou nenhuma alteração. Ex: Nome do dispositivo.
- Dinâmica
  - Relacionadas a eventos da rede q que sofrem alteração constante. Ex: Pacotes transferidos, Total de erros, etc.
- Estatística
  - Derivadas das informações dinâmicas após operações estatísticas. Ex: Taxa de utilização de CPU, vazão em bps, etc.

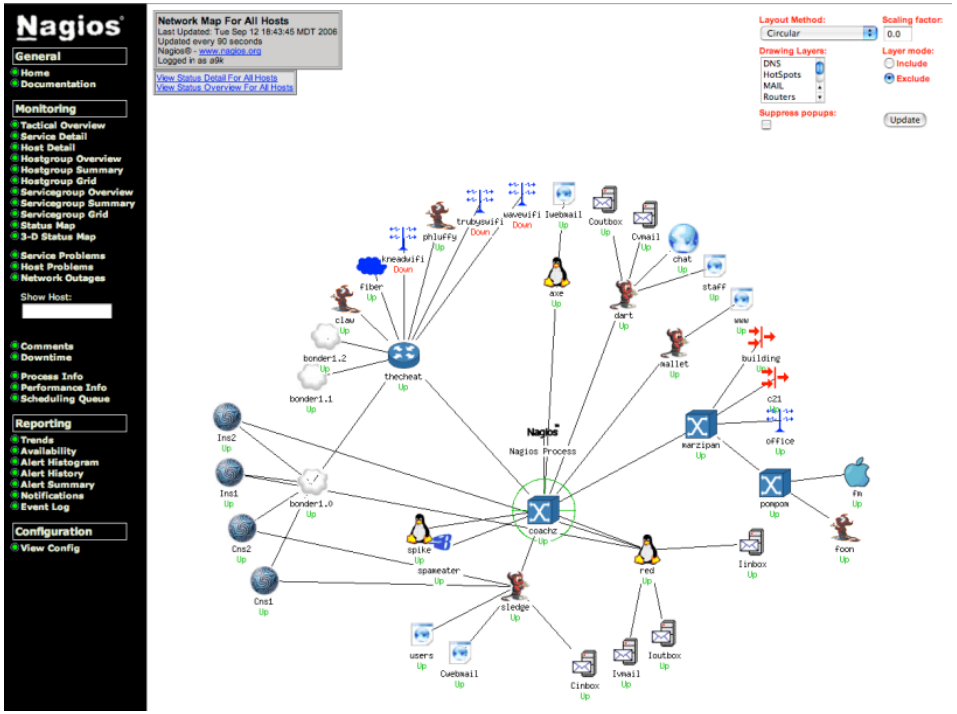
Arquiteturas de gerência

- Centralizada
  - Existe apenas um gerente com um banco de dados centralizado
- Hierárquica
  - Existe um gerente Central e vários gerentes que atuam como clientes do gerente central. Os dados são centralizados em um único banco de dados
- Distribuída
  - Existem vários gerentes independentes com bancos de dados próprios com esquema de replicação da base de dados
- Proxies
  - Tradução de protocolos entre gerente e agente que não falam mesmo protocolo de gerência

Estação de Gerenciamento

- Interface entre o Gerente de Rede e o sistema de gerenciamento
- Executa aplicações ou plataformas de gerenciamento





Agente de Gerenciamento

- Recebem mensagens SNMP dos gerentes para enviar ou modificar dados e também enviam alertas aos gerentes
- Não existe especificações para interação com o recurso gerenciado
- Localizado perto do dispositivo gerenciado

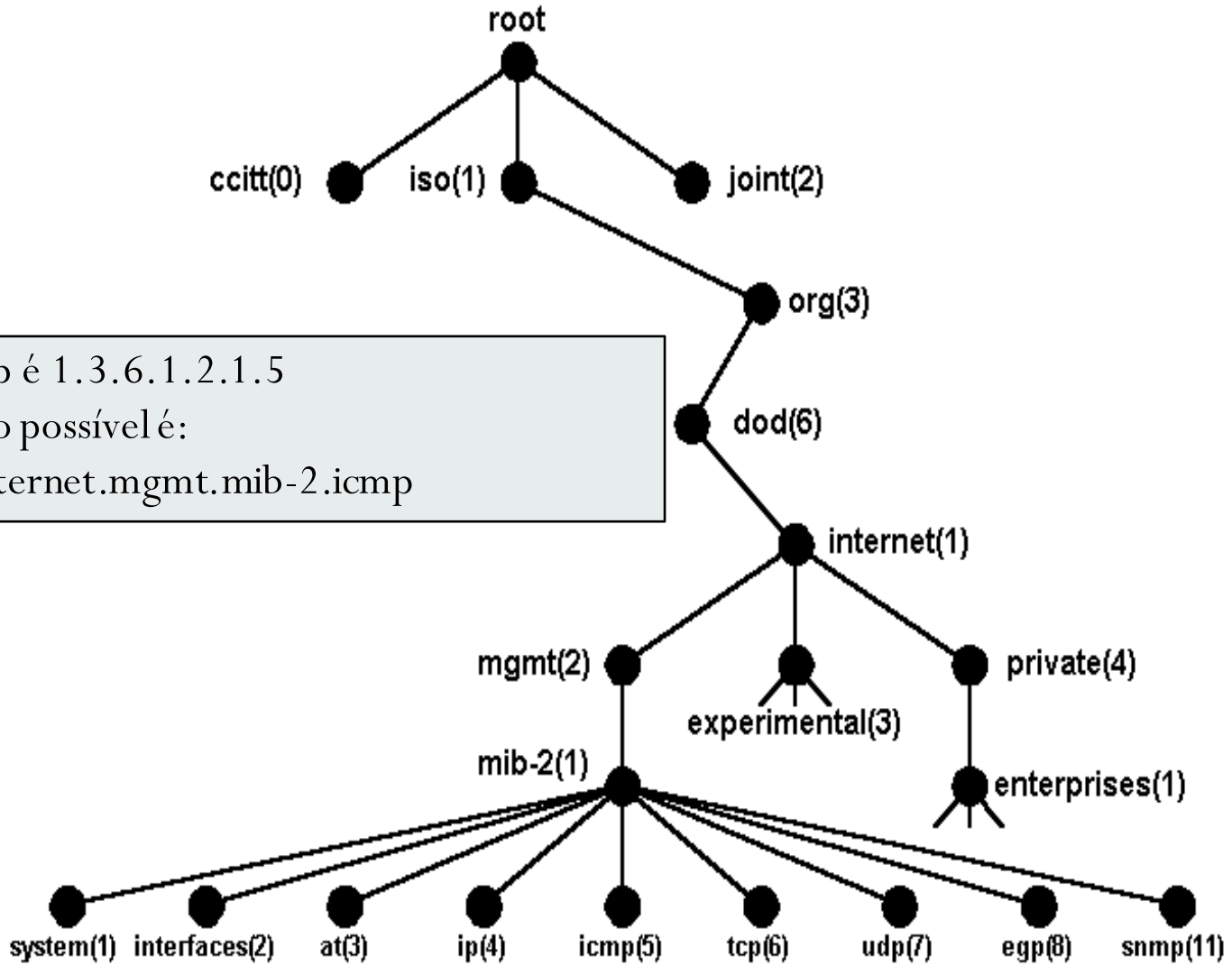
Base de Informações Gerenciadas

- Base de dados composta de objetos gerenciados organizada na forma de árvore
- Cada objeto representa uma variável que pode ter seu valor lido ou alterado
- As variáveis representam ítens de informação sobre o dispositivo gerenciado
- Cada dispositivo gerenciado mantém uma MIB que armazena informações
- MIBs
  - MIB I (RFC 1156) e MB II (RFC 1213)
  - MIB RMON I (RFC 1757) e MIB RMON II (RFC 2021)
- Pública (IETF) ou Privada (Empresas)

MIB

- Representação em uma estrutura em árvore
  - Nós intermediários possuem sub-nós
  - As folhas são os objetos e possuem valores associados
  - Cada nó (exceto o raiz) possui um OID (Object Identifier)
    - OID é usado como um identificador único para nominar objetos em uma estrutura hierárquica. Bastante utilizado em esquemas LDAP, Certificados X.509;
  - O OID de um nó é construído concatenando o seu identificador ao OID do seu nó pai
  - As variáveis de uma MIB são organizadas em grupos. Ex: system, icmp, interfaces, tcp.

Árvore MIB



- OID do Objeto icmp é 1.3.6.1.2.1.5
- Outra representação possível é:
  - iso.org.dod.internet.mgmt.mib-2.icmp

SMI
Structure of Management Information

- Define como os objetos gerenciados são nomeados e especifica os tipos de dados associados, ou seja, é um conjunto de regras que define como uma MIB deve ser especificada
- A MIB representa o Banco de Dados de objetos e a SMI representa a documentação para definição dos tipos de dados em cada objeto que compõe a MIB
- SMIv1 - RCF 1155 e SMIv2 RFC 2578
- A definição pode ser dividida em
  - Nome
  - Tipo e Sintaxe
  - Codificação

SMI - Nomenclatura

- Um OID é composto por uma sequência de inteiros separados por ponto(.)
- Existe uma forma alternativa de representação mais legível por humanos.
  - Ex: 1.3.6.1 pode ser representado por iso.org.dod.internet
- O grupo Private é para empresas que podem reservar OIDs. A instituição responsável por pelo gerenciamento dos OIDs é a IANA (Internet Assigned Numbers Authority)
  - Designação dos nós abaixo do grupo enterprise:
    - https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers
  - Qual a diferença entre utilizar objetos no nó mgmt ou utilizar objetos dentro da ramificação de uma empresa (enterprises)?

SMI – Sintaxe

- Descrição textual da MIB para efeito de padronização
- Definida por um subconjunto de facilidades de uma linguagem de descrição de dados denominada ASN.1 (Abstract Syntax Notation One)
- Cada objeto na MIB possui um nome, um tipo, um valor, uma forma de acesso, um status e uma descrição, e a sua própria definição segundo a SMI

SMI - Sintaxe

- SYNTAX – Tipo do objeto
- ACCESS – Modo de acesso: read-only, read-write, write-only e not-accessible
- STATUS – mandatory, optional, obsolete e depracated
- DESCRIPTION – Nome textual para descrever o objeto de maneira mais legível

ASN.1

- Os tipos de dados utilizados na SMI são definidos pela ASN.1
  - ASN.1 é uma linguagem formal para descrever padrões de informação sendo transmitidas por protocolos de telecomunicações, sem detalhes de sua implementação
  - Utilizada nos mais diversos campos de pesquisa. Praticamente tudo que utilizamos relacionados a protocolos de comunicação hoje foi definido usando ASN.1. Ex: Celulares, Caixas Eletrônicos, NetMeeting, Compras Onlines, etc.
  - A ASN.1 pode utilizar várias regras de codificação para transferência das informações:
    - Basic Encoding Rule (BER) **Codificação utilizada no SNMP**
    - Canonical Encoding Rule (CER)
    - Distinguished Encoding Rule (DER)
    - XML Encoding Rule (XER)
    - Entre outros
  - A ASN.1 é como uma linguagem de programação para descrever padrões e o BER é como se fosse a compilação deste padrão para a transmissão em um meio de comunicação

ASN.1

- Exemplo de definição de informacão utilizando ASN.1:

```
Cliente ::= SEQUENCE {
  nome       PrintableString(SIZE (1..20)),
  endereco   PrintableString(SIZE (1..50)) OPTIONAL,
  cep        NumericString(SIZE (8)),
  cidade     PrintableString(SIZE (1..30))
  sexo       Sexo
}

Sexo ::= ENUMERATED {
  masculino(1), feminino(2)
}
```

Codificação BER

- Definida na recomendação ITU-T-X-690 ou ISO 8825
- Conjunto de regras para codificação de dados ASN.1 para transmissão por um link de comunicação através de um fluxo de octetos
- Traduzem cada item de dados em triplas denominadas TLV (Tag, Length, Value): Etiqueta, Tamanho e Valor

- Tag
  - Identificação do tipo do dado, 8 bits:
    - bit 1 e 2 – classe do tipo (Universal, Application, context-specific, Private
    - bit 3 – primitivo ou composto
    - 4-8 – indica o tipo dentro da classe (Boolean, Integer, Sequence…)
- Length
  - Identificação de quantos bytes serão utilizados para os dados a seguir
- Value
  - Valor do Dado ou uma seqüência de TLVs aninhados

Codificação BER

- Exemplo:
  - 04 06 70 75 62 6c 69 63 (string 6 bytes "public")

- Exemplo:

```
Questao ::= SEQUENCE  {
        numeroQuestao  INTEGER,
        questao        IA5String
    }

minhaQuestao  Questao ::= {
    numeroQuestao     5,
    questao           "Anybody there?"
}
```

30 13 02 01 05 16 0e 41 6e 79 62 6f 64 79 20 74 68 65 72 65 3f

SMI - Sintaxe

- Tipo
  - INTEGER – Inteiro 32bits (Pode ser usado também em tipos enumerados)
  - OCTET STRING – String de zero ou mais octetos
  - Counter – Inteiro de 0 a 2^{32} (Um inteiro que só incrementa de 1)
  - OBJECT IDENTIFIER – String de decimais que representa um OID
  - NULL – Atualmente sem uso em SNMP
  - SEQUENCE – Sequência que contem 0 ou mais tipos diferentes ASN.1
  - SEQUENCE OF – Objeto formado por uma SEQUENCE de tipos ASN.1
  - IpAddress – Representa um endereço IPv4 (IPv6 só definido em SMING)
  - NetwordAddress – Pode representa tipos diferentes de endereços de rede
  - Timeticks – Inteiro que mede tempo em centésimos de segundos
  - Gauge – Inteiro de 32 bits que pode ser incrementado ou decrementado
  - Opaque – Pode armazenar qualquer tipo ASN.1

Exemplo

```
sysUpTime OBJECT-TYPE
  SYNTAX        TimeTicks
  ACCESS        read-only
  STATUS        mandatory
  DESCRIPTION
  "The time (in hundreths of a second)
  since the network management portion
  of the system was last re-
  initialized."
:: = { system 3 }
```

Exemplo MIB2-Módulos

```
system OBJECT IDENTIFIER ::= { mib-2 1 }
interfaces OBJECT IDENTIFIER ::= { mib-2
  2 }
at OBJECT IDENTIFIER ::= { mib-2 3 }
ip OBJECT IDENTIFIER ::= { mib-2 4 }
icmp OBJECT IDENTIFIER ::= { mib-2 5 }
tcp OBJECT IDENTIFIER ::= { mib-2 6 }
udp OBJECT IDENTIFIER ::= { mib-2 7 }
egp OBJECT IDENTIFIER ::= { mib-2 8
transmission OBJECT IDENTIFIER ::= { mib-
  2 10 }
snmp OBJECT IDENTIFIER ::= { mib-2 11 }
```

Exemplo MIB2-Tabela

```
ifTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IfEntry
  ACCESS not-accessible
  STATUS mandatory
  DESCRIPTION
  "A list of interface entries. The
  number of entries is given by the
  value of ifNumber."
::= { interfaces 2 }
```

Exemplo MIB2-Linha

```
ifEntry OBJECT-TYPE
  SYNTAX IfEntry
  ACCESS not-accessible
  STATUS mandatory
  DESCRIPTION
  "An interface entry containing
  objects at the subnetwork layer and
  below for a particular interface."
  INDEX { ifIndex }
::= { ifTable 1 }
```

Exemplo MIB2-Linha

```
IfEntry ::= SEQUENCE {
  ifIndex INTEGER
  ifDescr DisplayString,
  ifType INTEGER,
  ifMtu INTEGER,
  ifSpeed Gauge,
  ifPhysAddress PhysAddress,
  ifAdminStatus INTEGER,
  ifOperStatus INTEGER,
  ifLastChange TimeTicks,
```

Exemplo MIB2-Linha

```
ifInOctets Counter,
ifInUcastPkts Counter,
ifInNUcastPkts Counter,
ifInDiscards Counter,
ifInErrors Counter,
ifInUnknownProtos Counter,
ifOutOctets Counter,
ifOutUcastPkts Counter,
ifOutNUcastPkts Counter,
ifOutDiscards Counter,
ifOutErrors Counter,
ifOutQLen Gauge,
ifSpecific OBJECT IDENTIFIER }
```

Exemplo MIB2 - Escalar

```
ifIndex OBJECT-TYPE
  SYNTAX INTEGER
  ACCESS readonly
  STATUS mandatory
  DESCRIPTION
  "A unique value, greater than zero, for
  each interface. It is recommended that
  values are assigned contiguously starting
  from 1. The value for each interface sub-
  layer must remain constant at least from
  one re-initialization of the entity's
  network management system to the next re-
  initialization."
  ::= { ifEntry 1 }
```

SMIv2

- Estende a árvore da SMI adicionando um novo ramo *snmpV2* ao nó *internet*
- Acrescentou alguns tipos novos
  - Ex: Integer32, Counter32, …
- Acrescentou alguns campos adicionais as definições
  - Ex: UnitParts, MAX-ACCESS

Grupos da MIB2

- system (1) informações básicas do sistema (Status)
- interfaces (2) interfaces de rede (Status das interfaces)
- at (3) tradução de endereços (somente para manter compatibilidade e será removido na MIB3)
- ip (4) protocolo ip (Aspectos de roteamentos IP)
- icmp (5) protocolo icmp (erros ICMP, exclusões de pacotes, etc)
- tcp (6) protocolo tcp (conexões fechadas, syn, etc)
- udp (7) protocolo udp (Datagramas, etc)
- egp (8) protocolo egp
- transmission (10) meios de transmissão (Não existe atualmente objetos nesse grupo)
- snmp (11) protocolo snmp (Números de pacotes SNMP recebidos, etc)

Exercício

- Trabalho em grupo de dois

- Desenvolver uma MIB para o gerenciamento dos objetos gerenciáveis de uma máquina de café. Esses objetos devem fazer parte de um mesmo grupo e retornarem, no mínimo, as seguintes informações: descrição do modelo da máquina, número de cafés tirados na máquina, nível do reservatório de água, temperatura do dispositivo de extração do café, presença de capsula na máquina. Utilize a sintaxe para criar o arquivo da MIB.