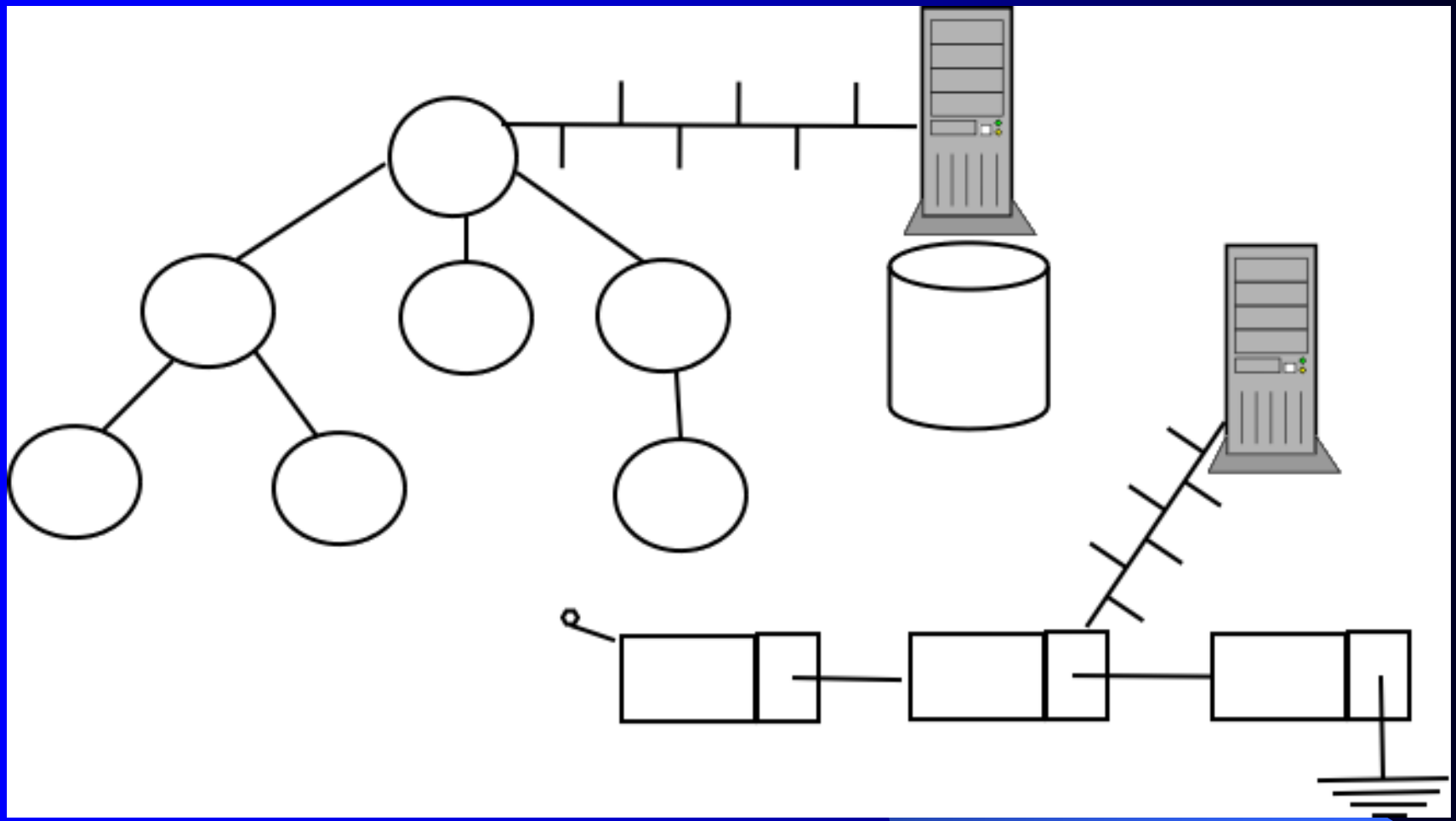
SNMP (Simple Network Management Protocol)



Anderson Alves de Albuquerque

1 – Introdução:

- **O que é SNMP (Basicamente):**
  - **Através de variáveis ou estruturas certos acontecimentos podem ser contabilizados (contados).**
  - **Exemplos (netif.h e net_in.c):**
    Contar frames que entram em uma interface.
  - **Exemplo no mundo físico:**
    Contador de consumo água, gás ou luz.

1 – Introdução:

- **Exemplo no linux: "/proc/net/snmp"**
  - **Olhem esse arquivo(/proc/net/snmp), faça testes com aplicações de rede (ICMP, TCP ou UDP) e tentem ver o que aconteceu depois dos testes.**
  - **Reparem as variáveis de "/proc/net/snmp" e seus significados, compare-os com: /usr/src/linux/include/net/snmp.h**

1 – Introdução:

- **Funções principais do SNMP (161/UDP):**
  - **Gerenciamento de redes;**
  - **Controlar equipamentos em rede;**
  - **Detectar problemas e ataques (Ex: flood);**
  - **Contabilizar ocorrências;**
  - **Usa paradigma Busca/Armazenamento (fetch-store);**
  - **Permite integrar equipamentos.**

1 – Introdução:

- **Características do SNMP v1:**
  - **Simples;**
  - **Estável;**
  - **Flexível;**
  - **Deve evitar muito tráfego.**

1 – Introdução:

- **Áreas de gerenciamento definidas pela ITU-T(*)**
  - Configurações;
  - Falhas;
  - Desempenho;
  - Segurança;
  - Contabilidade.

(*) ITU-T:**União Internacional de telecomunicações.**

2 – Versões do SNMP e CMIP:

- SNMPv1 (1989):
  - RFC 1157
- SNMPv2 (1993):
  - RFC 1448
- SNMPv3 (1997):
  - RFC 3414
- CMIP(Common management Information Protocol):
  - Usado em telecomunicações(Telefonia) e mais Complexo que o SNMP.
  - Segue o padrão OSI-ISO, trabalha na camada de transporte.

2 – Versões do SNMP:

- SNMPv1:
  - Vantagens:

  Simplicidade, popularidade, expansibilidade, aberto.

  - Desvantagens:

  Segurança. Password(*) "public" para "get"e "private" para "set". Podemos até desligar equipamentos.

*) campo communities do SNMP

2 – Versões do SNMP:

- SNMPv2:
  - Vantagens:

    Prevê integridade, autenticação e confiabilidade.

    Maior segurança na transmissão de senhas (melhor controle de acesso).

    Mensagens adicionais: “GetBulkRequest” e “InformRequest/Response”

  - Desvantagens:

    Complexidade e problemas entre os projetistas.

2 – Versões do SNMP:

- SNMPv3:
  - Vantagens:

    Avanço em segurança.

    Criptografia com algoritmo DES e autenticação com MD5 e SHA.

  - Desvantagens:

    Muitos equipamentos não tem suporte a versão 3.

3 – Gerenciamento & Camadas:

- Enlace:

  - Vantagens:

    Funciona com falha em outras camadas e possibilita mudança de rotas.

  - Desvantagens:

    Acesso apenas a intra-rede, em S.O. O gerenciamento fica com o fabricante.

3 – Gerenciamento & Camadas:

- Aplicação:

  - Vantagens:

    Uniformidade na rede e comunicação inter-redes.

  - Desvantagens:

    Se uma camada inferior cai ocorre perda de acesso.

4 – Vocabulário:

- Gerente.
- Agente.
- MIB (Management Information Base).
- ASN.1 (Abstract Syntax Natition da ISO) .
- SMI (Structure of Management Information).
- RMON (Remote MONitoring).
- Objetos.

5 – Solicitações enviadas:

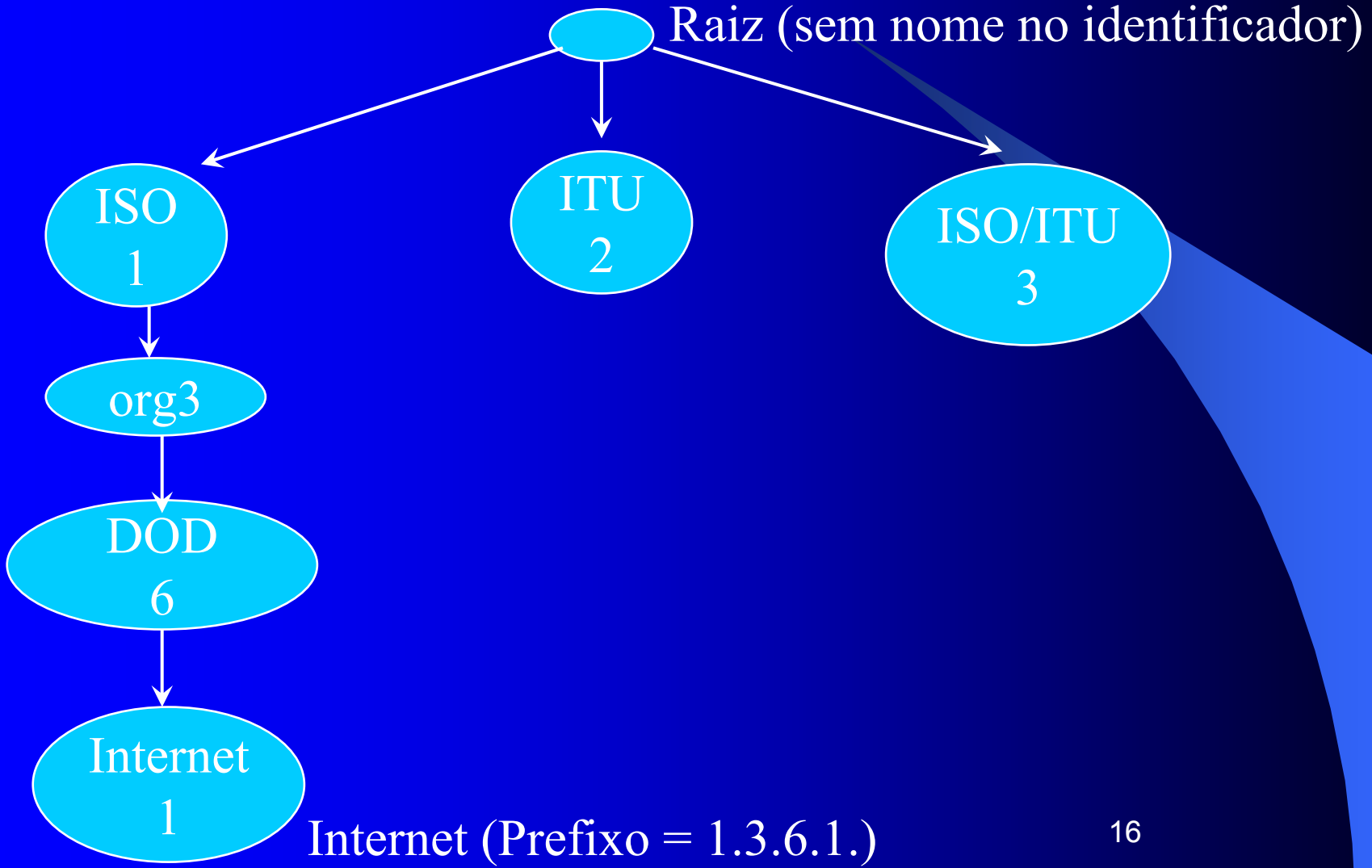
- Get e GetNext (GetResponse): Leitura de dados(Busca).
- Set: Alterar dados (Armazenamento).
- Trap: Alerta dado pelo agente sobre alguma anomalia.

Detalhes: Veja em asn1.h .

6 – MIB:

- MIB I: Primeira MIB. RFC 1066.
- MIB II: Evolução da MIB I. RFC 1213.
- MIB Experimental: Em desenvolvimento.
- MIB Privada: Desenvolvida pelo fabricante.

6 – MIB (Exemplo introdutório):



Internet (Prefixo = 1.3.6.1.)

6 – MIB (Estrutura de dados *mib.h* e *snmib.c*):

- Identificador de nome (*snmpvars.h*):
  - Nome no nó.
- Prefixo:
  - Nome no formato e entendimento humano.
- Identificador de objeto:
  - Segue o padrão ASN.1 da ISO. Codifica os nós em vez de nomes. Ex: 1.3.6.1.2.1.

6 – MIB (Estrutura de dados *mib.h* e *snmib.c*):

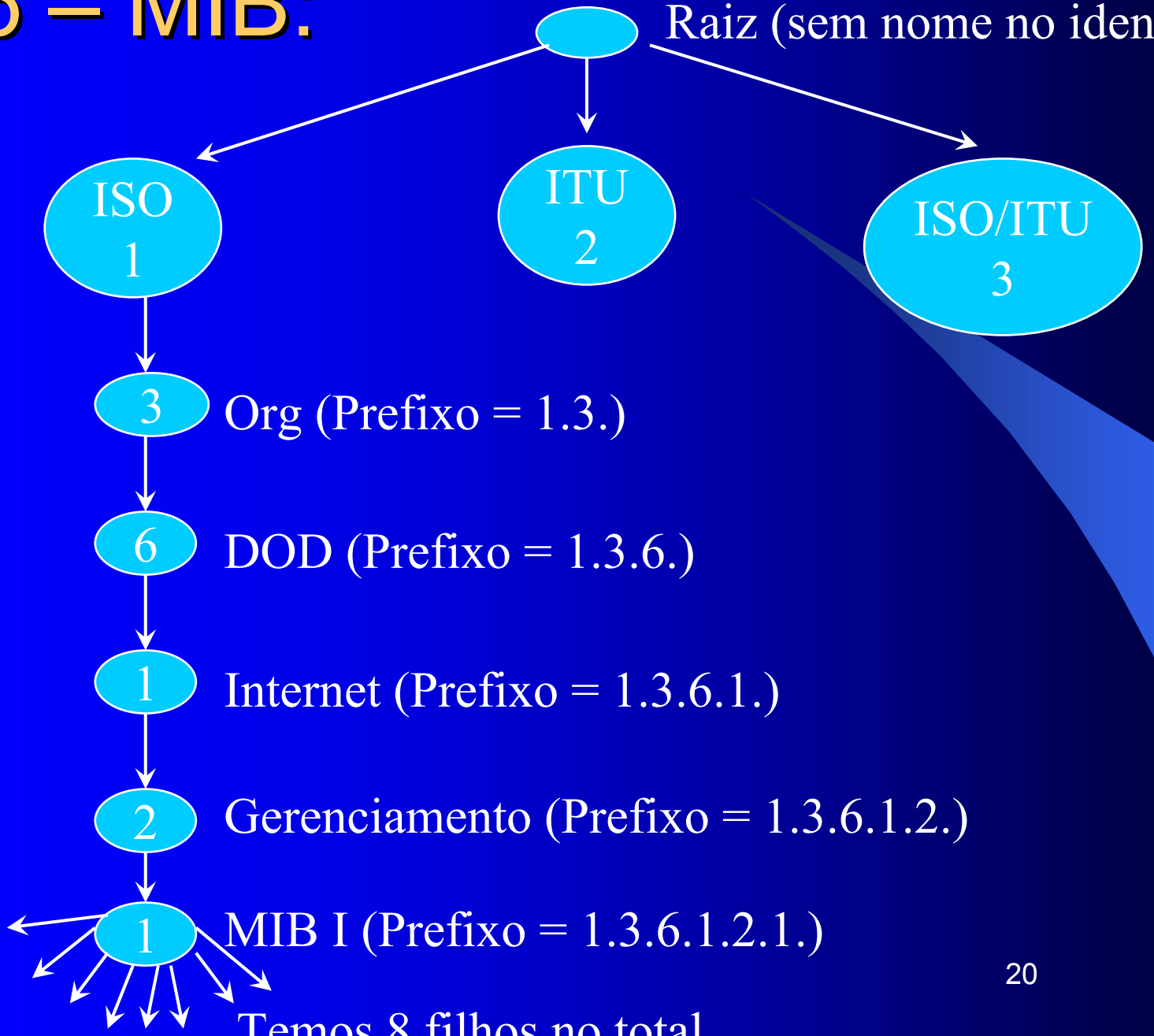
- Tipo da variável (*asn1.h*):
  - Padrão ASN.1 .
- Permissão de escrita (*mib.h*): Tipo Boolean.
- Folha (*mib.h*):
  - Tipo Boolean, definida como: NLEAF ou LEAF.

6 – MIB (Estrutura de dados *mib.h* e *snmib.c*):

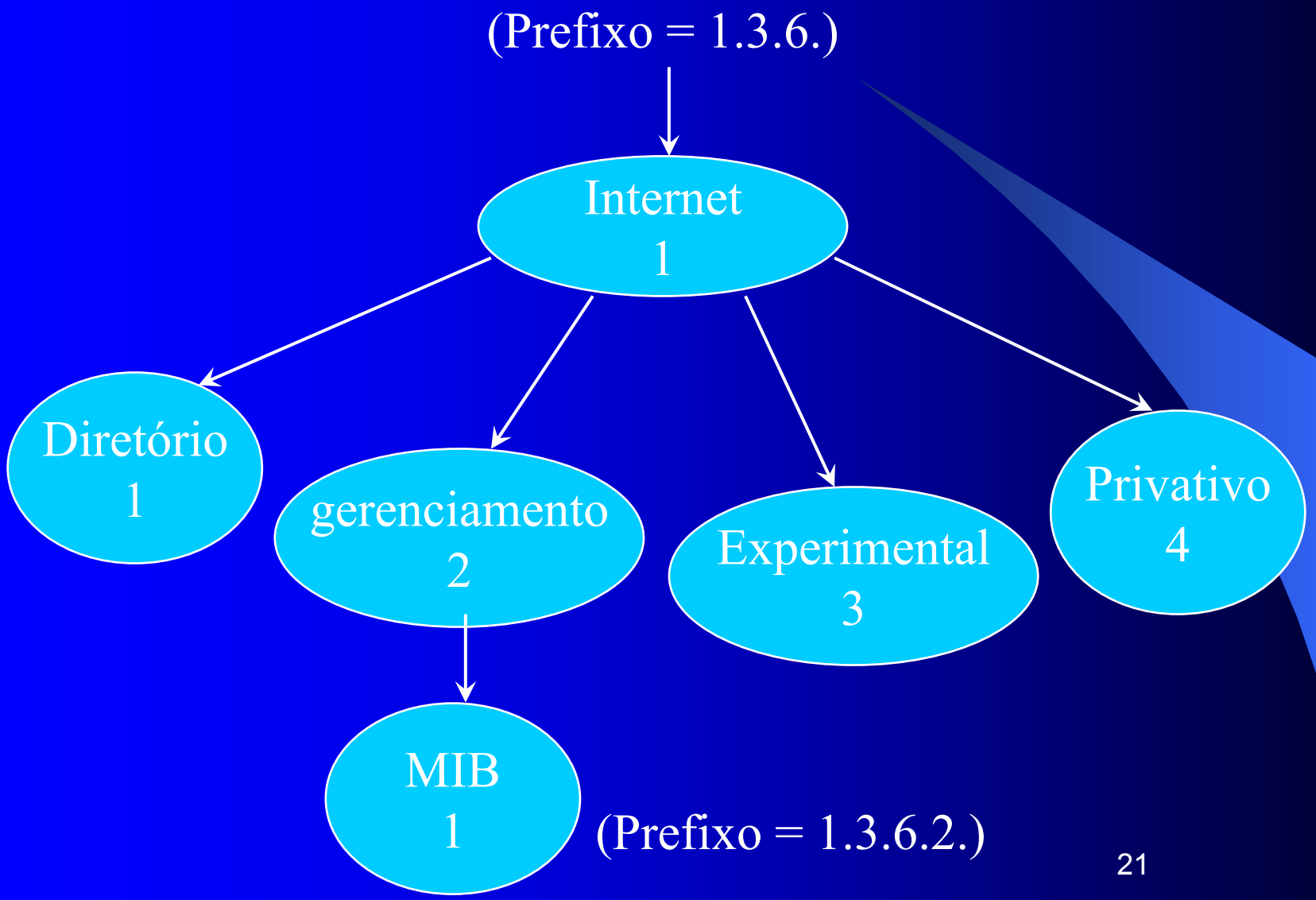
- Ponteiro para Função (*mib.h*):
  - Função que será chamada para o tratamento do nó e de seus objetos.

- Ponteiro *Next (*mib.h*):
  - Aponta para o próximo nó.
  - Usado pela instrução “GetNext”.

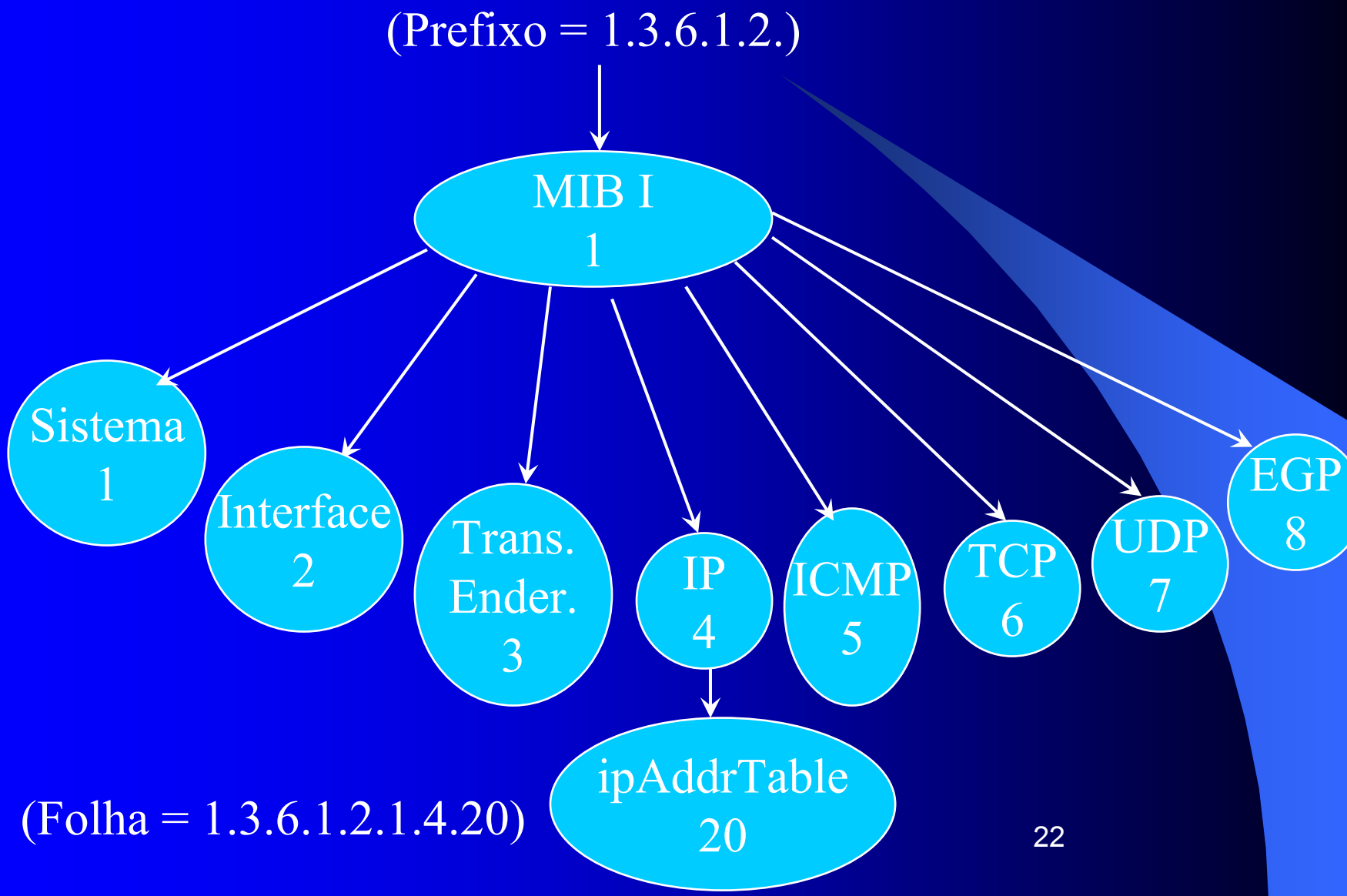
6 – MIB:


Raiz (sem nome no identificador
ISO
1
ITU
2
ISO/ITU
3
3
Org (Prefixo = 1.3.)
6
DOD (Prefixo = 1.3.6.)
1
Internet (Prefixo = 1.3.6.1.)
2
Gerenciamento (Prefixo = 1.3.6.1.2.)
1
MIB I (Prefixo = 1.3.6.1.2.1.)
Temos 8 filhos no total

6 – MIB (iniciado no nó DOD):



6 – MIB I (8 nós filhos - snmib.c):



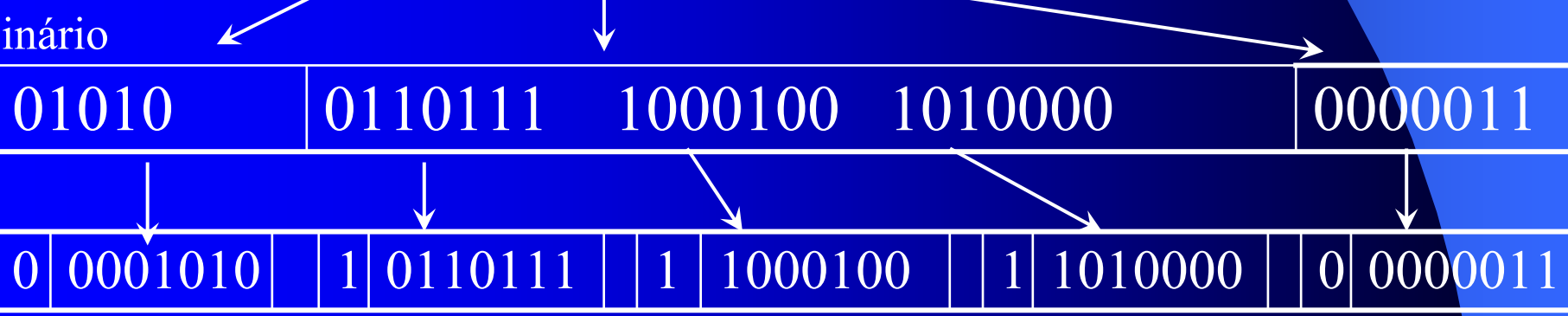
7 – SMI:

- Regras para atribuir nomes:
  - Forma de identificação e agrupamento das informações.
  - Sintaxe permitida.
- Regra para atribuir tipos:
  - Tipos de dados permitidos.

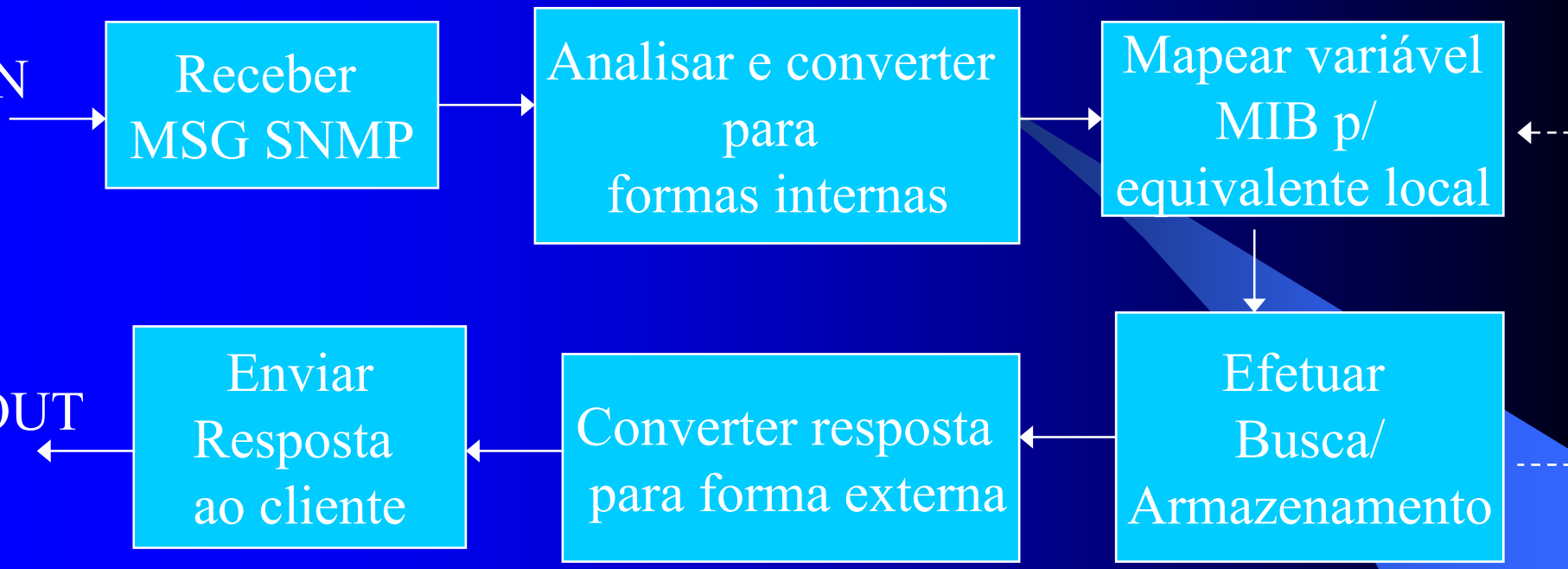
8 – ASN.1 (asn1.h):

- Representação de números no campo "identificação":
  - Bit mais significativo acionado (n>127).
  - Bit mais significativo desligado (n<=127).

- Exemplo: 10 . 909904 . 3 (Douglas E. Comer Vol.2, Cap 21)



9 – Mensagem SNMP



Fonte: Interligação em rede com TCP/IP
Douglas E. Comer Vol.2 (Cap.20)

9 – Mensagem:

- **Mensagem SNMP:**

Versão	Comminity	DADO(PDU)

- **PDU:**

PDU Type	Rquest ID	Erro Status	Erro Index	Variáveis

- **Variáveis:**

Nome “1”	Valor “1”	...	Nome”N”	Valor”N”

9 – Mensagem (Douglas E. Comer Vol.1, Cap 26):

- **Mensagem SNMP:**

30	29
Sequência	Len=41

- **Versão:**

02	01	00
Inteiro	Len=1	Versão=0

9 – Mensagem (Douglas E. Comer Vol.1, Cap 26):

- **Community:**

04	06
String	Len=6

70	75	62	6c	69	63
p	u	b	l	i	c

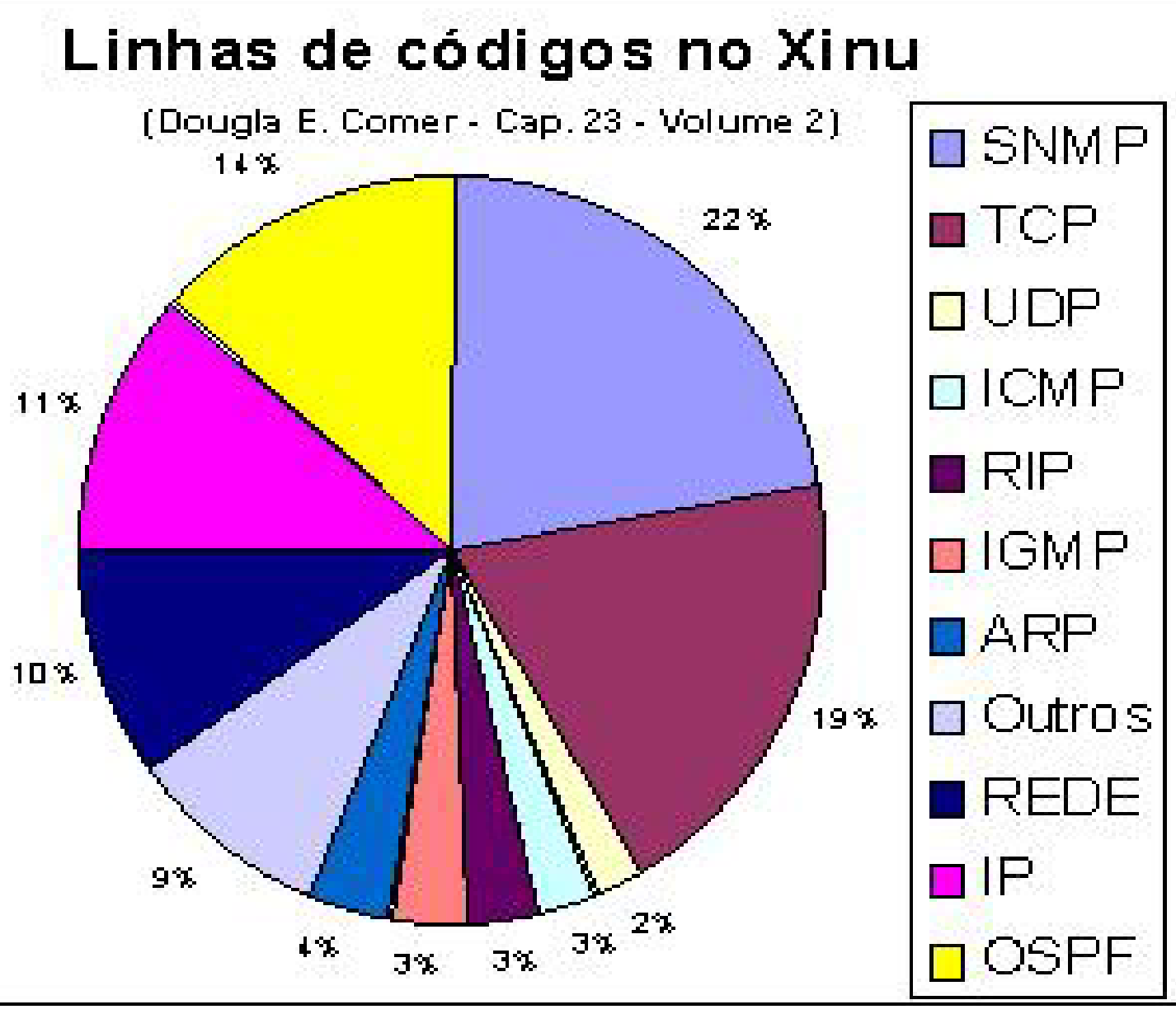
- **PDU Type e Request ID:**

A0	1C
GetReq	Len=28

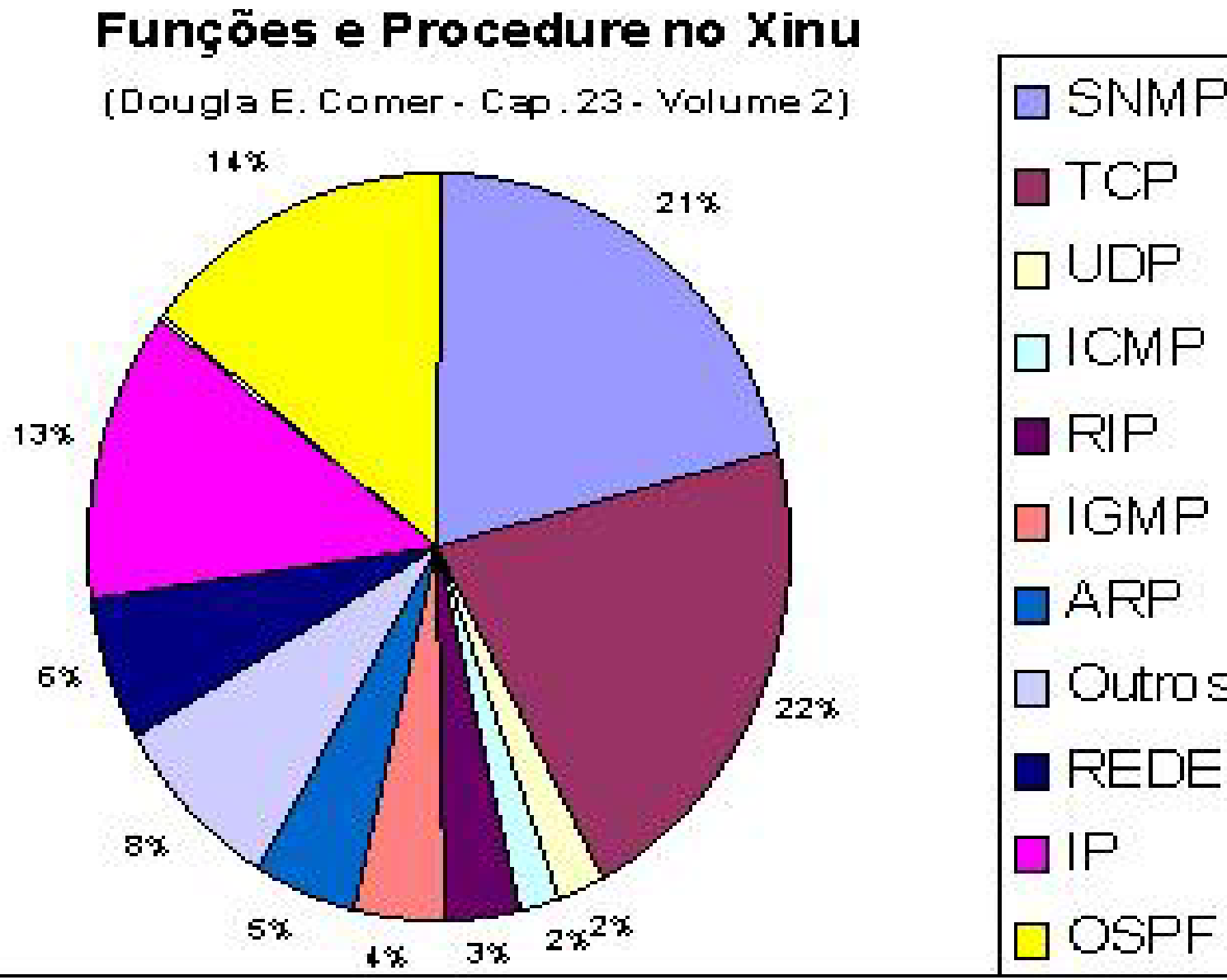
02	04	05 AE 56 02
Inteiro	Len=4	Pedido de ID

0201000201003 00E300C06082B06010201010 1000500

10 – Gráficos (Linhas de códigos no XINU):



10 – Gráficos (Funções e procedures no XINU):



11 – Softwares:

- Exploração:
  - ADMsnmp(Cracker SNMPv1): ADMsnmp.0.1.tgz

- Monitorar configuração:
  - Proprietário:

    OPenView, SunNet Manager, MibBowser.
  - GPL:

    Scotty, MRTG, CMU-snmp, SnmpPerl.

12 – Bibliografia:

- Sistema Operacional: XINU – Douglas E. Comer
  (Purdue - ftp://ftp.cs.purdue.edu/pub/comer/)

- Interligação em rede com TCP/IP, Vol.1 .
  "Princípios, protocolos e arquitetura"
  ISBN: 85-352-0270-6

- Interligação em rede com TCP/IP, Vol.2 .
  "Projeto, implementação e detalhes internos"
  ISBN: 85-352-0395-8

- Trabalhos GTA/UFRJ.