Ciências da Computação

CAP 7. GERENCIAMENTO DE REDES

AULA 1: Introdução e Componentes Principais

INE5422 Redes de Computadores II

Prof. Roberto Willrich (INE/UFSC)

roberto.willrich@ufsc.br

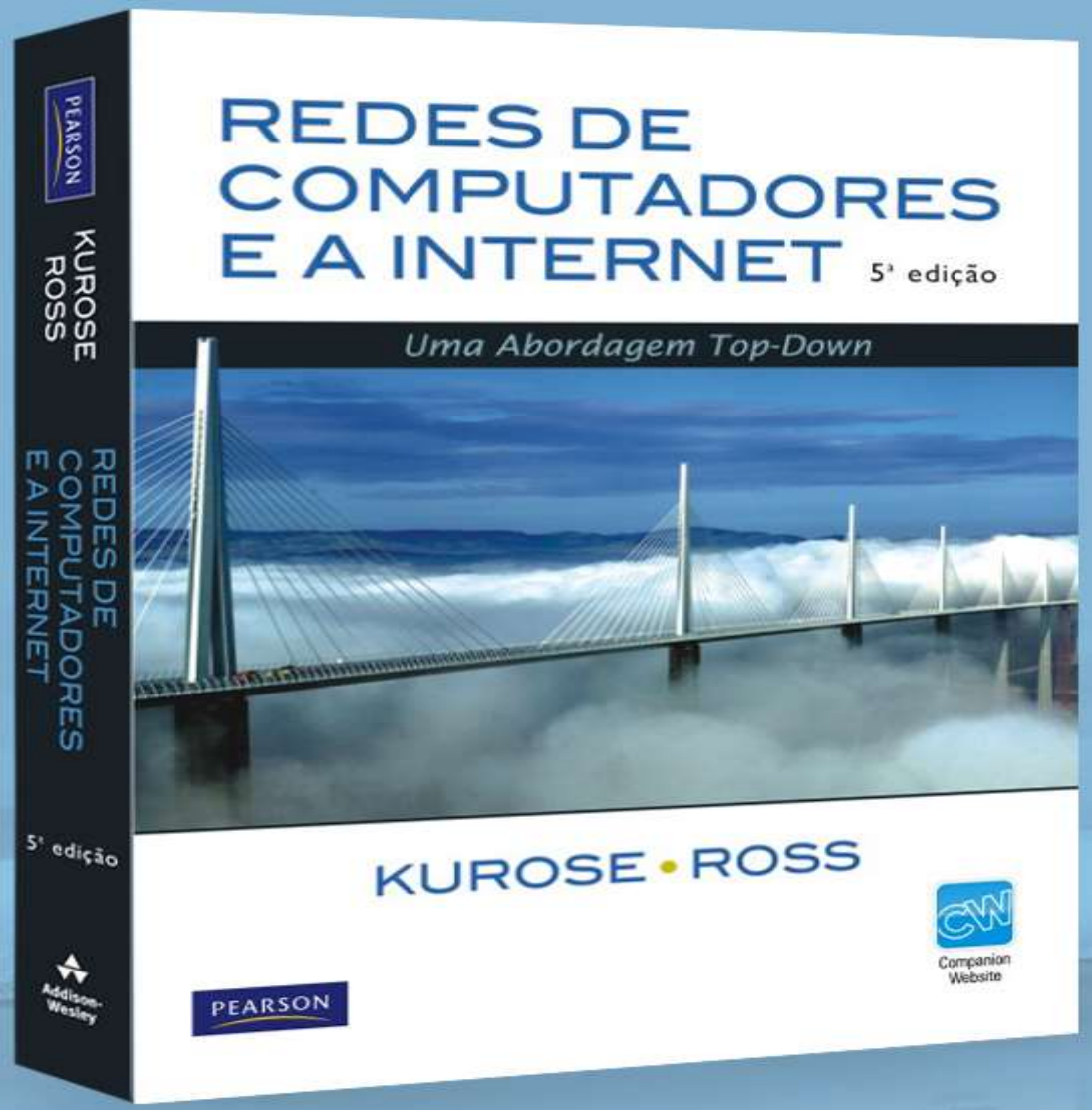
https://moodle.ufsc.br

Nota sobre o uso destes slides ppt:

Estamos disponibilizando estes slides gratuitamente a todos (professores, alunos, leitores). Eles estão em formato do PowerPoint para que você possa incluir, modificar e excluir slides (incluindo este) e o conteúdo do slide, de acordo com suas necessidades. Eles obviamente representam *muito* trabalho da nossa parte. Em retorno pelo uso, pedimos apenas o seguinte:

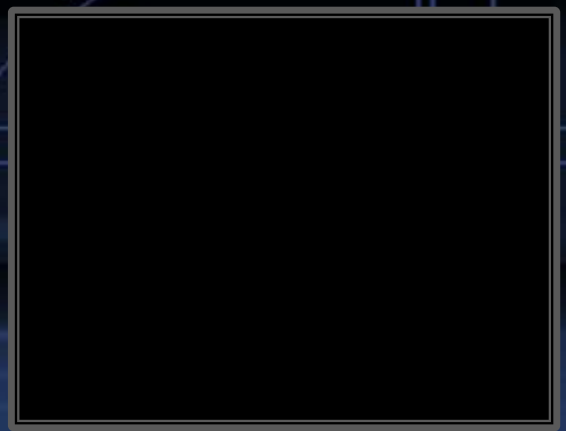
- Se você usar estes slides (por exemplo, em sala de aula) sem muita alteração, que mencione sua fonte (afinal, gostamos que as pessoas usem nosso livro!).
- Se você postar quaisquer slides sem muita alteração em um site Web, que informe que eles foram adaptados dos (ou talvez idênticos aos) nossos slides, e inclua nossa nota de direito autoral desse material.

Obrigado e divirta-se! JFK/KWR



Gerenciamento de rede

- **Objetivos do capítulo:**
  - Introdução ao gerenciamento de redes: motivação e principais principais
  - Serviços de apresentação: ASN.1
  - Ambiente de gerenciamento de redes da Internet
    - MIB: base de informações de gerenciamento
    - SMI: linguagem de definição de dados
    - SNMP: protocolo para gerenciamento de redes

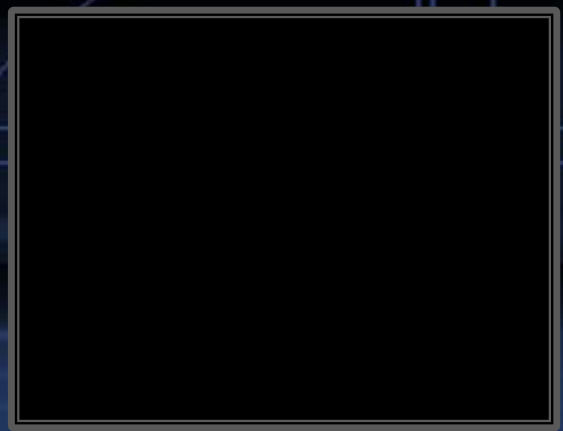


O que é gerenciamento de redes?

"Gerenciamento de redes inclui o fornecimento, a integração e a coordenação de hardware, software e elementos humanos para monitorar, testar, configurar, consultar, analisar, avaliar e controlar a rede e os recursos para atender aos requisitos de desempenho, qualidade de serviço e operação em tempo real dentro de um custo razoável."

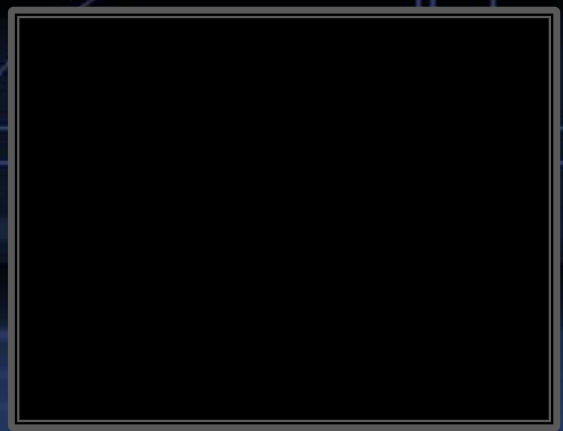
O que é gerenciamento de redes?

- **Áreas de gerenciamento de redes**
  - Gerenciamento de desempenho: meta é qualificar, medir, informar, analisar e controlar o desempenho (utilização, vazão) dos componentes da rede (enlaces, roteadores, hospedeiros) e tráfegos fim-a-fim
    - Abordagem de longo prazo
  - Gerenciamento de falhas: meta é registrar, detectar e reagir às condições de falhas da rede
    - Tratamento imediato a falhas transitórias de rede
  - Gerenciamento de configuração: permite que o administrador de rede saiba quais dispositivos fazem parte da rede administrativa e quais são suas configurações de hardware e software



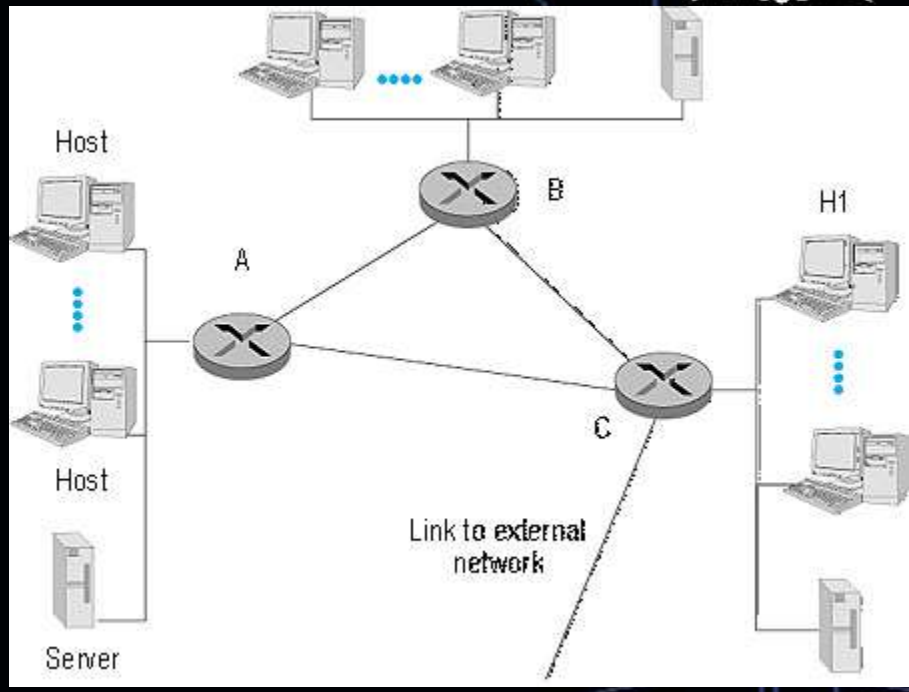
O que é gerenciamento de redes?

- **Áreas de gerenciamento de redes**
  - Gerenciamento de contabilidade: permite ao administrador especificar, registrar e controlar o acesso de usuários e dispositivos aos recursos de rede
    - Quotas de uso, cobranças por uso e alocação de acesso privilegiadas a recursos
  - Gerenciamento de segurança: meta é controlar o acesso aos recursos de acordo com alguma política definida
    - Centrais de distribuição de chaves e as autoridades certificadoras



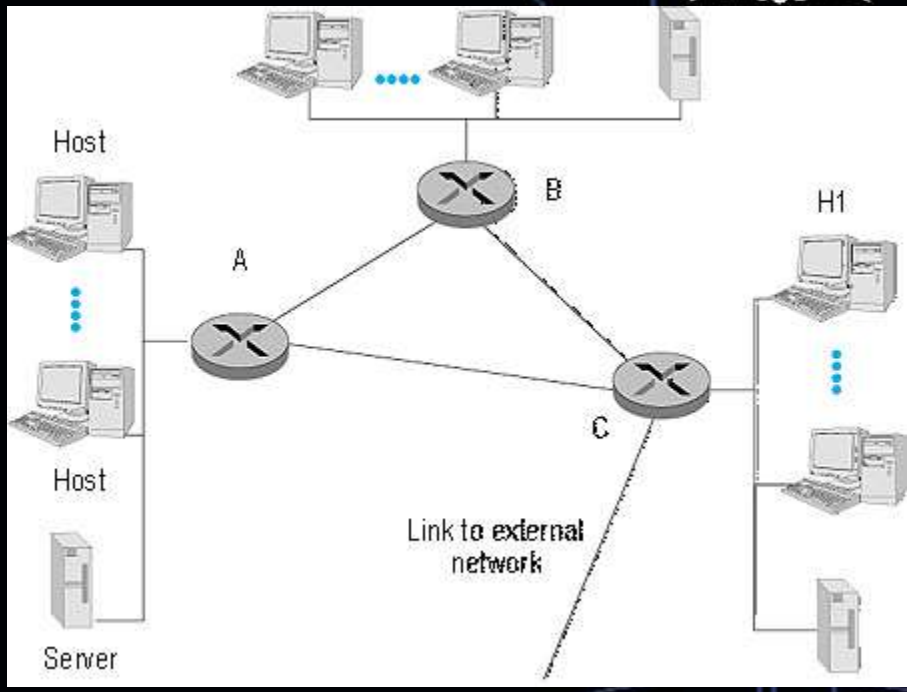
O que é gerenciamento de redes?

- **Começando com um exemplo simples**
  - Objetivo: Mostrar benefícios do uso de uma ferramenta de gerenciamento
- **Cenários:**
  - Detecção de falha em uma placa de rede em um hospedeiro ou roteador
    - Ex.: roteador sinaliza a falha, detecção de falhas eminentes (aumento de erros de checksums)
  - Monitoramento de um hospedeiro
    - Verificando se estão ativos e operacionais



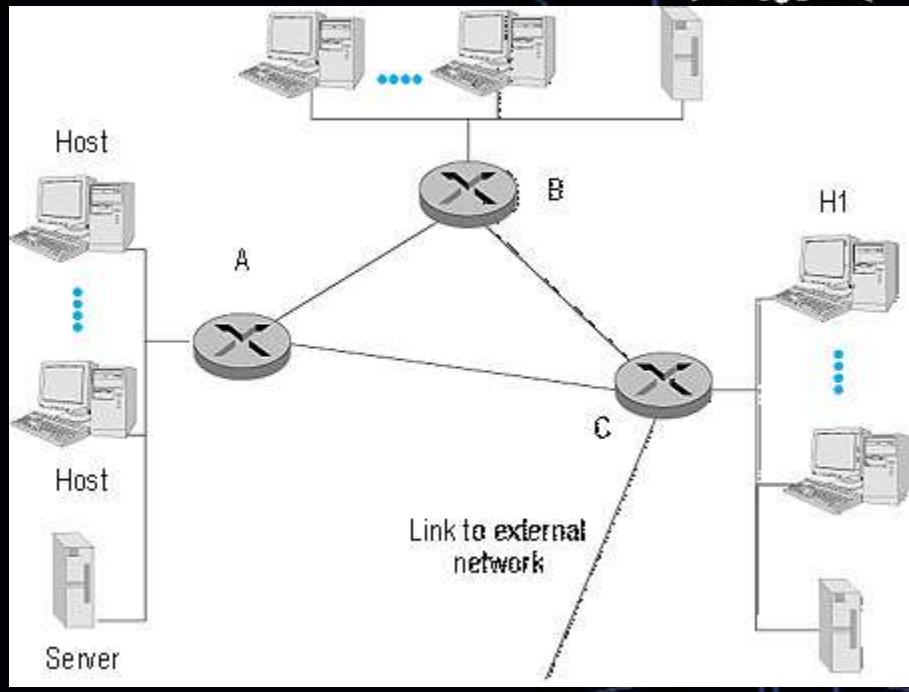
O que é gerenciamento de redes?

- **Cenários:**
  - Monitoramento de tráfego para auxiliar o oferecimento de recursos
    - Monitorando tráfego entre fontes e destinos é possível detectar mudança de servidores para outras LANs para evitar que o tráfego passe por várias LANs
    - Verificar se o enlace para a Internet está sobrecarregado (ou sobrecarga interna, exigindo aumento da largura de banda)



O que é gerenciamento de redes?

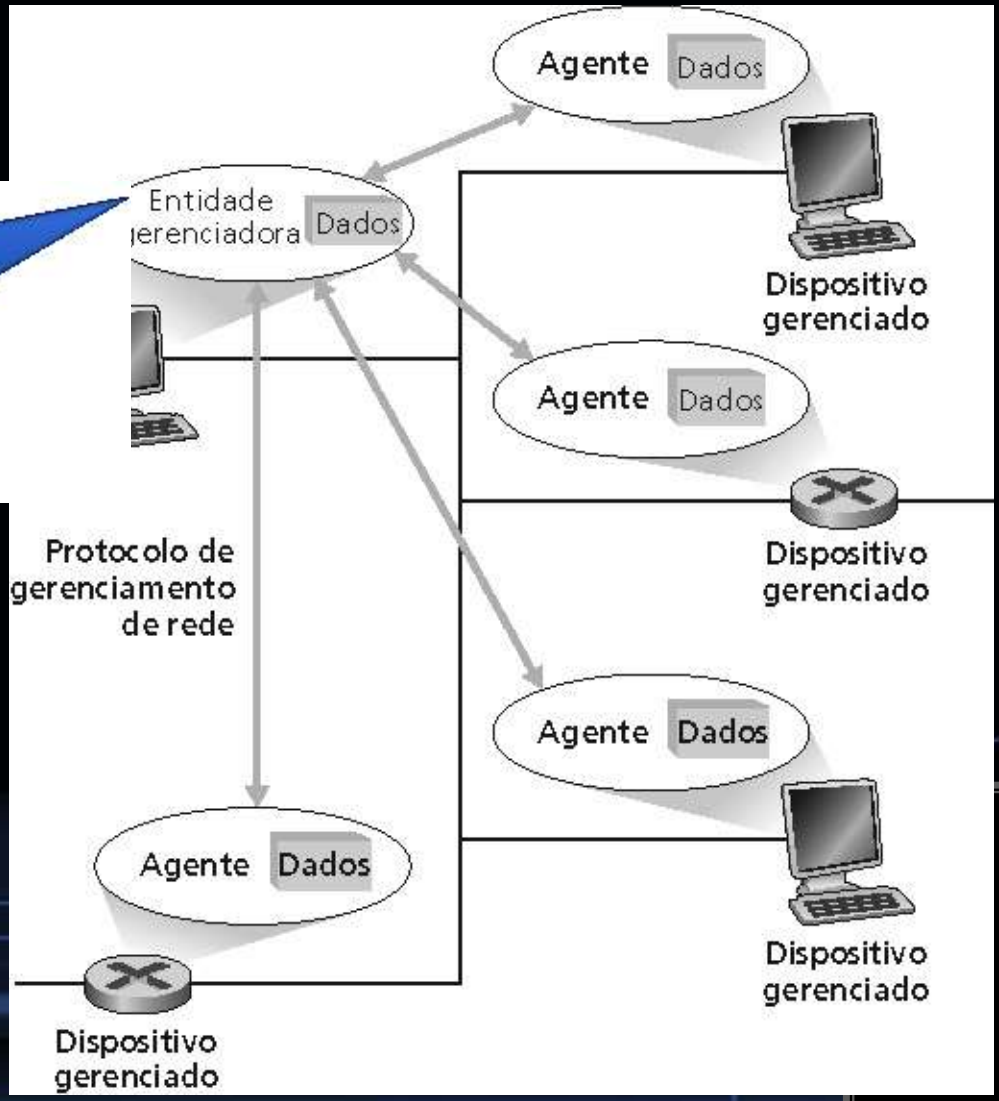
- **Cenários:**
  - Detecção de mudanças rápidas em tabelas de roteamento
    - Pode ser sinal de instabilidade nos roteadores ou problemas de configuração
  - Monitoramento de Acordo de Níveis de Serviço (SLA)
    - Contratos que definem parâmetros específicos de medida e níveis aceitáveis de desempenho do provedor
    - Define disponibilidade do serviço, latência, vazão, ...
  - Detecção de intrusos
    - Tráfego de uma fonte suspeita ou quando se destinar a ela (p.e. hospedeiro, porta)
    - Ataques do tipo DoS (envio excessivo de pacotes SYN para um destino)



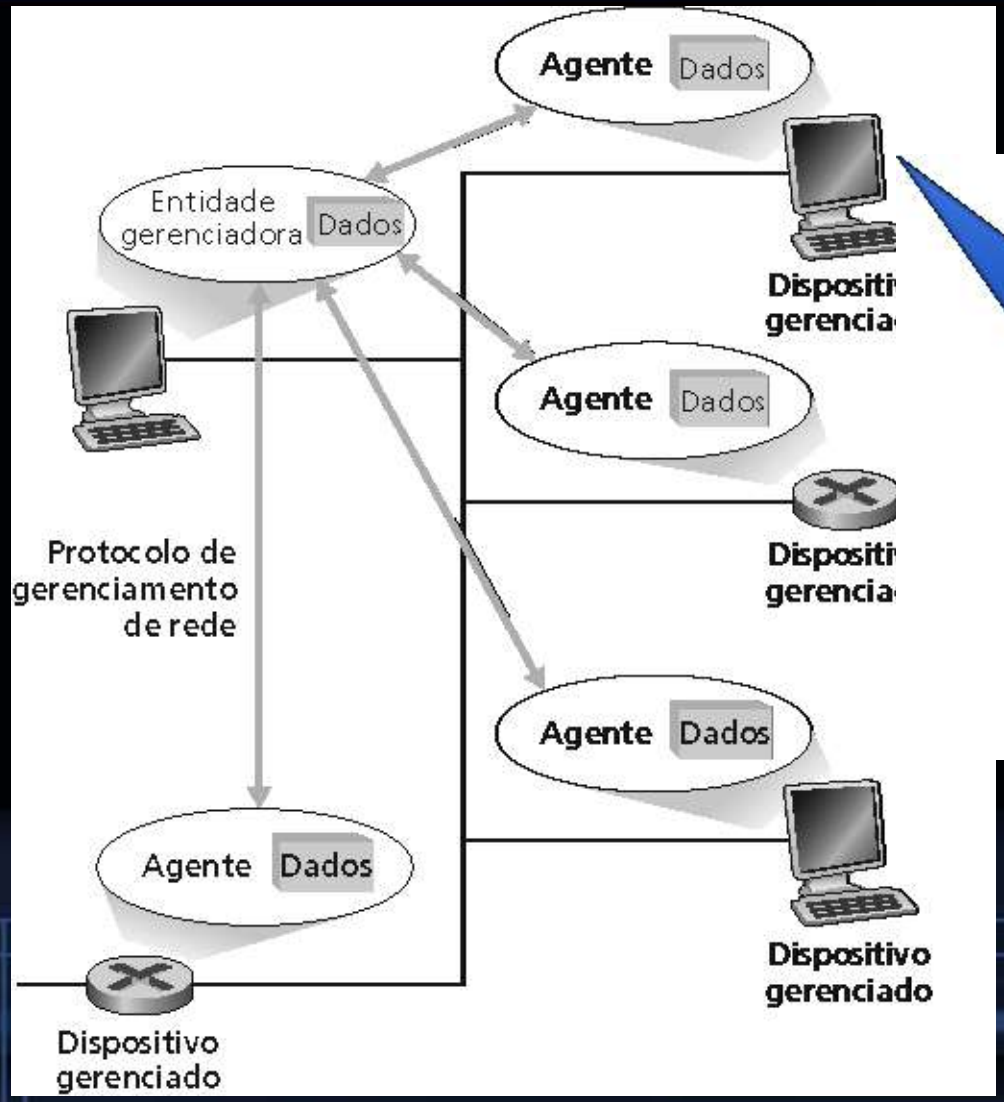
Infraestrutura de gerenciamento de redes

Definições:

Aplicação usada pelo administrador: controla a coleta, o processamento, a análise e/ou a apresentação de informações de gerencia de rede.

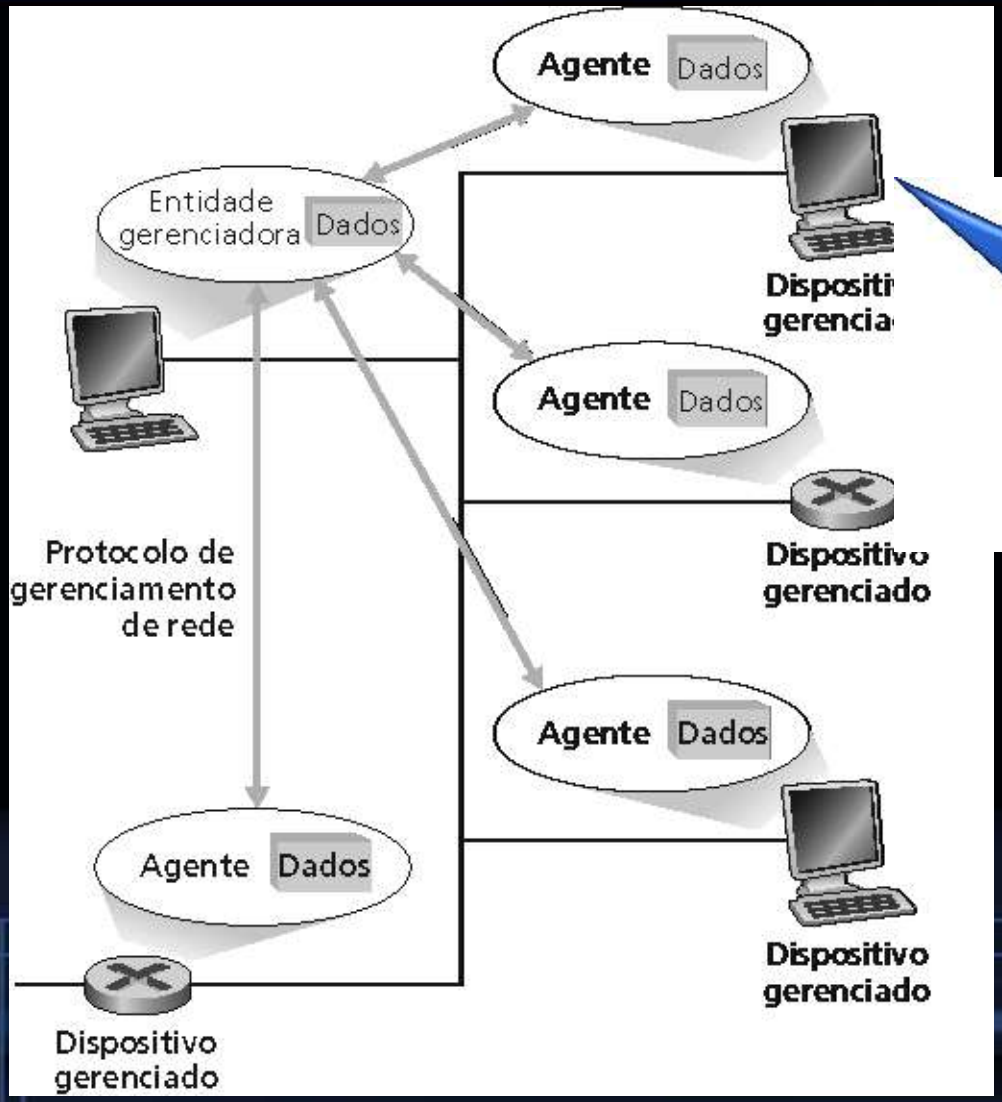


Infra-estrutura de gerenciamento de redes



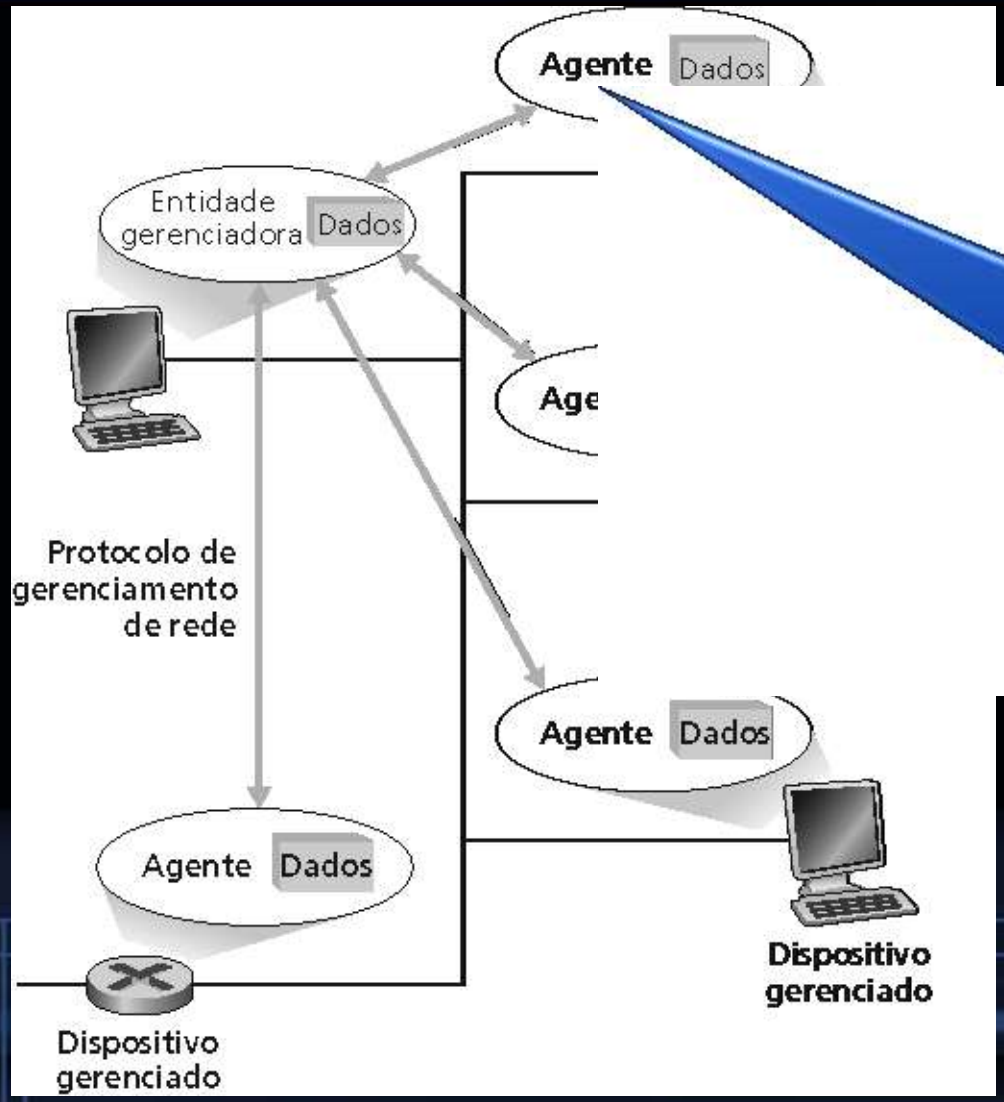
Equipamento de rede (incl. Software) : hospedeiro, roteador, switch, impressora, modem..
Contém diversos objetos gerenciados: partes do dispositivo (placa de rede...) e os parâmetros de configuração

Infra-estrutura de gerenciamento de redes



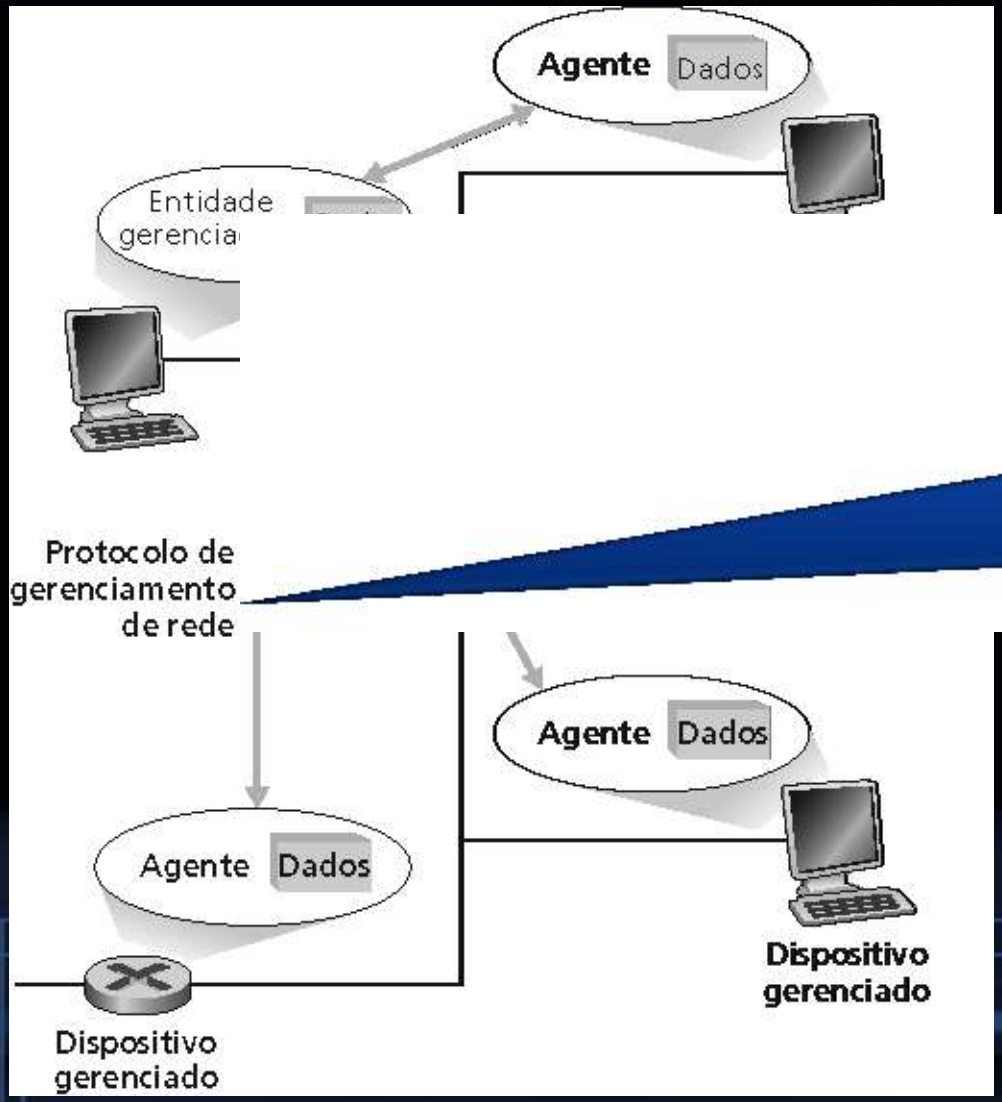
Informações dos objetos gerenciados são mantidas em uma Base de Informações de Gerenciamento (MIB): disponível para a entidade gerenciadora

Infra-estrutura de gerenciamento de redes



Agente de Gerenciamento: processo executando no dispositivo gerenciado que se comunica com a entidade gerenciadora.
Executa ações locais sob o comando e controle da entidade gerenciadora

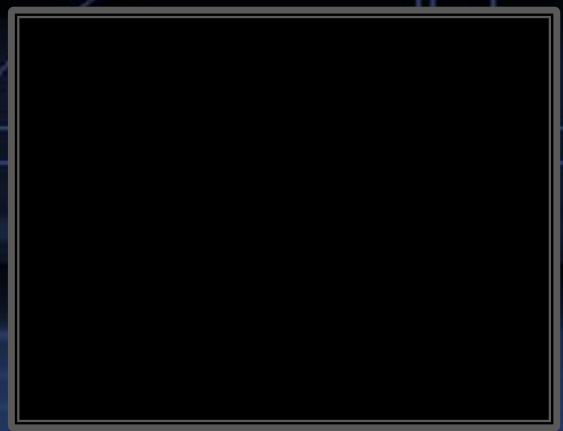
Infra-estrutura de gerenciamento de redes



Executado entre a entidade gerenciadora e os agente de gerenciamento: para investigar o estado dos dispositivos e executar ações sobre estes agentes.

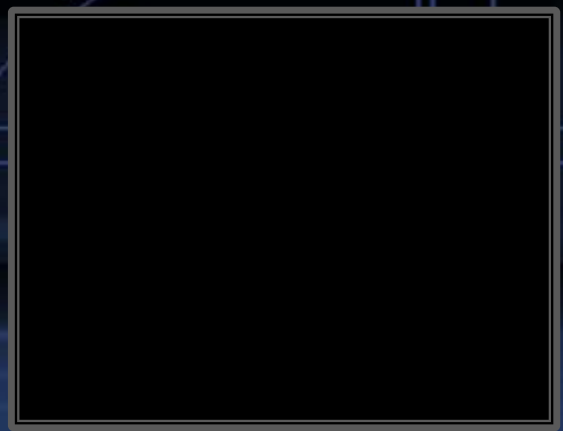
SNMP visão geral

- **SNMP: Simple network management protocol**
  - Origem na Internet (SGMP)
  - Começou simples
  - Desenvolvido e adotado rapidamente
  - Crescimento: tamanho e complexidade
  - Atualmente três: SNMP, SNMPv2 e SNMPv3
  - Padrão de fato para gerenciamento de redes



SNMP visão geral: 3 partes-chave

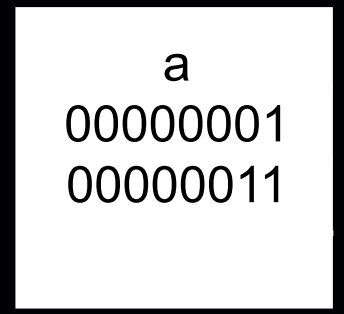
- **• Management Information Base (MIB):**
  - Base de dados distribuída com dados de gerenciamento de rede
  - Objetos MIB: objetos de gerenciamento de rede
    - Ex.: contador de pacotes IP descartados em um roteador; versão do software DNS; etc.
    - Objetos MIB relacionados são reunidos em Módulos MIB
- **• Structure of Management Information (SMI):**
  - Linguagem de definição de objetos da MIB
  - Define tipos de dados, modelo de objeto e regras para escrever e revisar informações de gerência
- **• Protocolo SNMP**
  - • Transporta informações e comandos sobre objetos entre o gerenciador e o elemento gerenciado



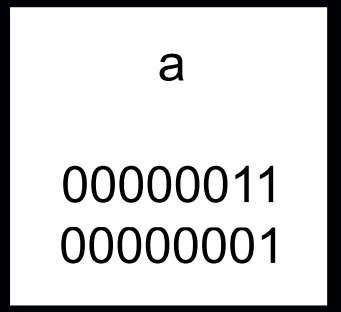
O problema de apresentação

- **P.: Uma cópia perfeita dos dados de memória, a memória, resolve o problema de comunicação entre computadores distintos?**
  - R: Nem sempre!

```
struct {
   char code;
    int x;
    } test;
test.x = 259;
test.code='a'
```



Formato do hospedeiro 1



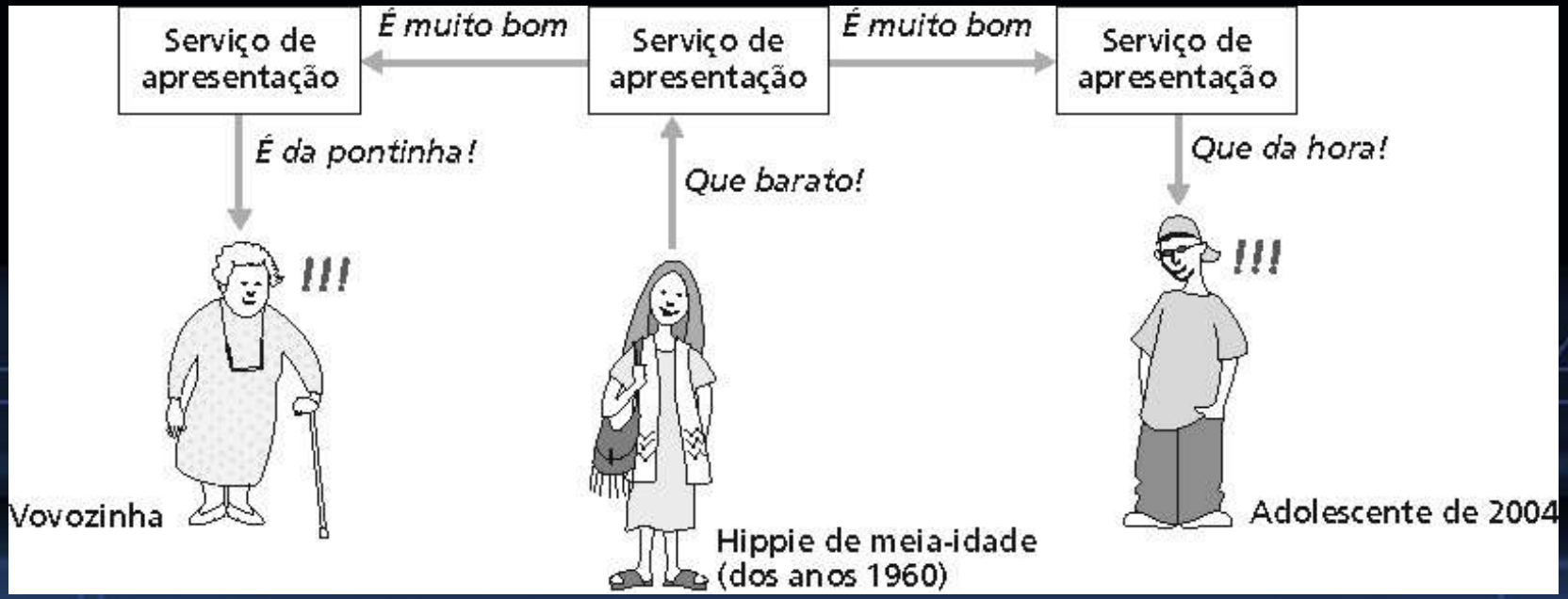
Formato do hospedeiro 2

Problema: diferentes formatos de dados e convenções de armazenamento

Um problema de apresentação da vida real:

Resolvendo o problema de apresentação

- 1. Transladar o formato do hospedeiro local para um formato independente de hospedeiro
- 2. Transmitir os dados num formato independente de hospedeiro
- 3. Transladar o formato independente para o formato do hospedeiro remoto



ASN.1: Abstract syntax notation 1

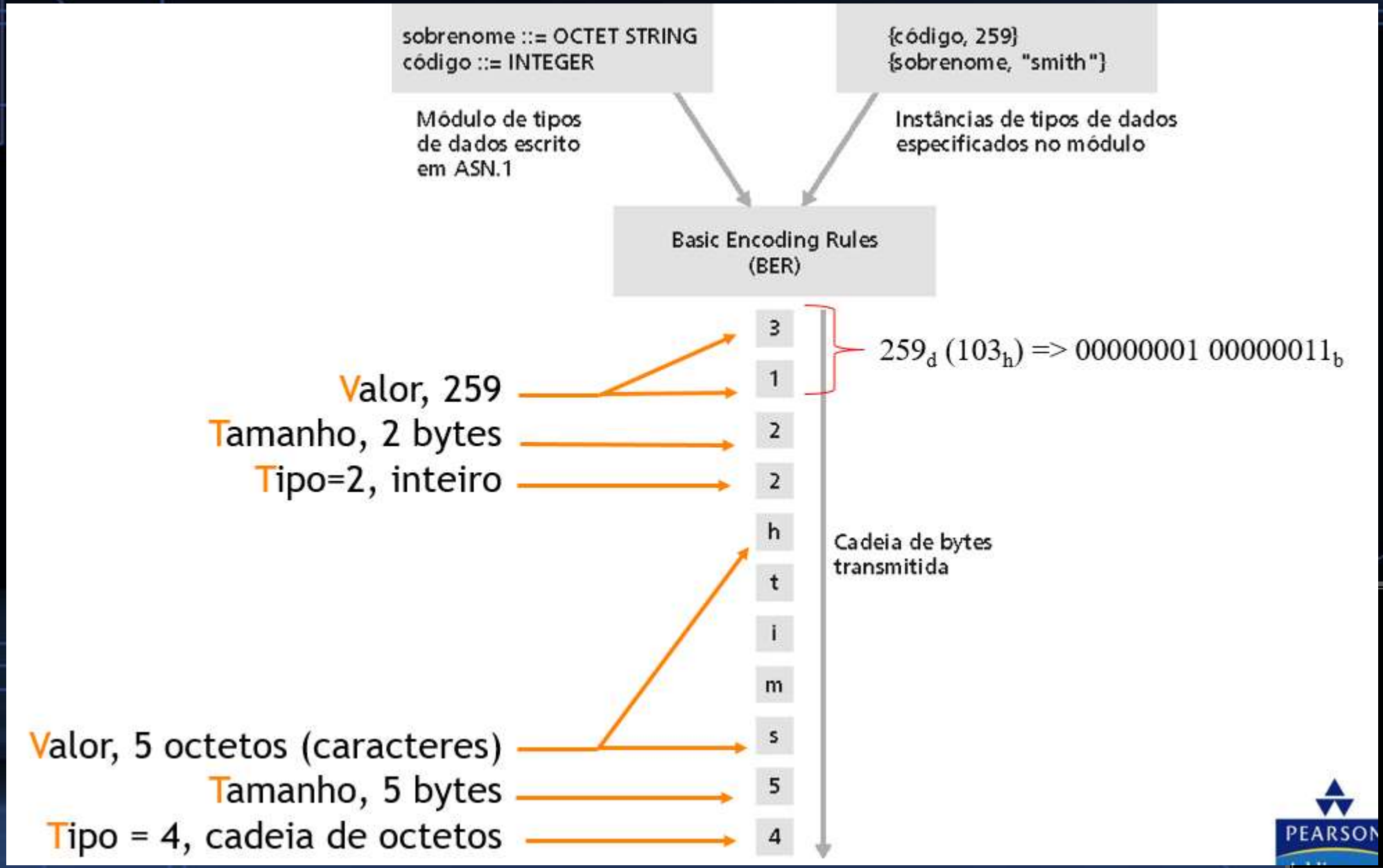
- **Padrão ISO X.208**
  - Usado extensivamente na Internet
  - BER: Basic encoding rules
    - Especificam como os dados definidos em ASN.1 devem ser transmitidos
  - Cada objeto transmitido tem codificação type, length, value (TLV) — Tipo, tamanho, valor

ASN.1 adota a abordagem TLV

- **Ideia: os dados transmitidos são auto-identificáveis**
  - T: tipo de dados, um dos tipos definidos em ASN.1
  - L: tamanho dos dados em bytes
  - V: valor dos dados, codificado de acordo com as regras do ASN.1

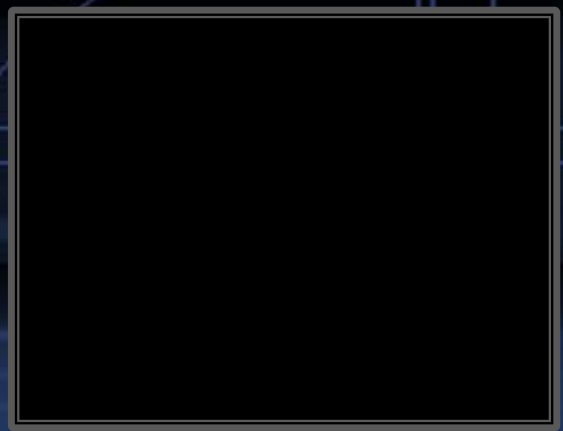
Valor do tag	Tipo
1	Booleano
2	Inteiro
3	Cadeia de bits
4	Cadeia de octeto
5	Nulo
6	Identificador de objeto
9	Real

Codificação TLV: exemplo



SMI: Structure of Management Information

- **Linguagem de Definição de Dados**
  - Propósito: criação de uma sintaxe e semântica para definição de dados de gerenciamento de forma não ambígua
    - Conjunto de regras que define como uma MIB é especificada
  - Definido na RFC 1155 (melhorias nas RFCs 1212 e 1215)
  - Um arquivo de MIB usa a notação ASN.1 e as regras SMI para definir objetos da MIB
- **SMI define o que cada objeto da MIB deve possuir**
  - Um nome (OID) que identifica o objeto unicamente
  - Uma sintaxe que identifica o tipo do objeto
  - Uma codificação que descreve como as informações serão transmitidas

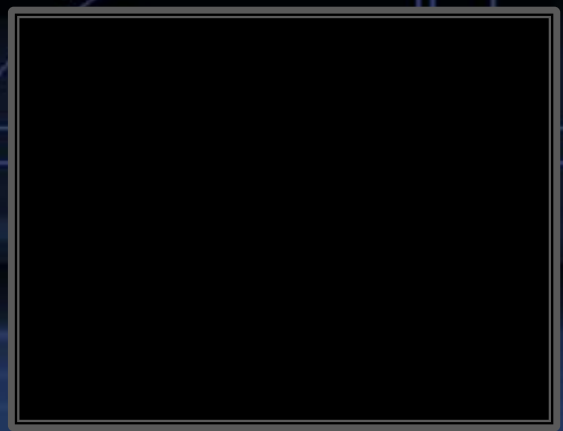


SMI: linguagem de definição de dados

- **Macros:**
- **• OBJECT-TYPE**
  - • Usada para especificar o tipo de dado, status, semântica do objeto gerenciado
- **• MODULE-IDENTITY**
  - • Permite que objetos relacionados sejam agrupados num módulo MIB

Tipos de dados básicos

INTEGER
Integer32
Unsigned32
OCTET STRING
OBJECT IDENTIFIER
IPaddress
Counter32
Counter64
Gauge32
Time Ticks
Opaque



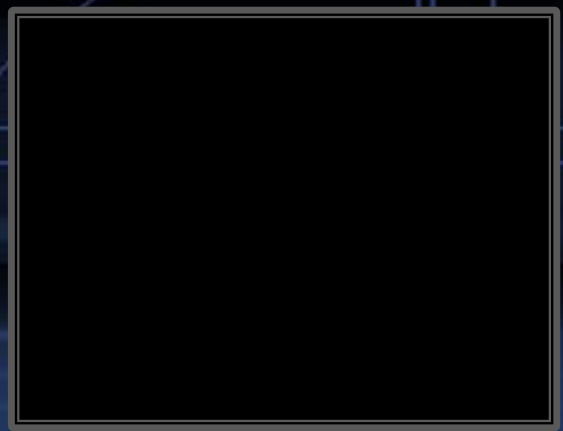
SMI: exemplo de objeto e módulo

OBJECT-TYPE: ipInDelivers

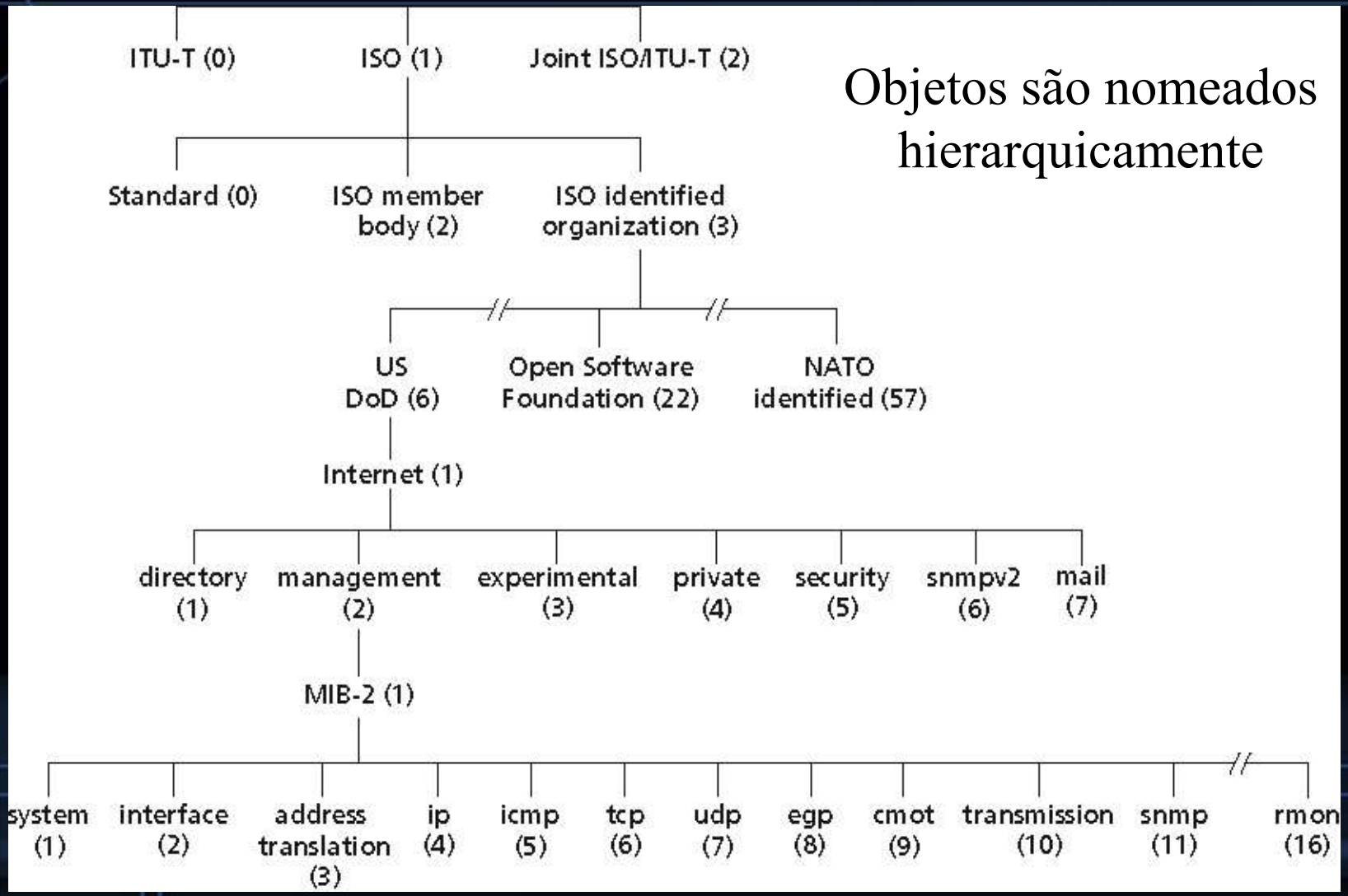
```
ipInDelivers OBJECT TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
     "The total number of input
      datagrams successfully
      delivered to IP user-
      protocols (including ICMP)"
::= { ip    9}
```

MODULE-IDENTITY: ipMIB

```
ipMIB MODULE-IDENTITY
  LAST-UPDATED "941101000Z"
  ORGANIZATION "IETF SNMPv2
              Working Group"
  CONTACT-INFO
     " Keith McCloghrie
     ....."
  DESCRIPTION
     "The MIB module for managing IP
     and ICMP implementations, but
     excluding the management of
     IP routes."
  REVISION "019331000Z"
 .........
::= {mib-2 48}
```



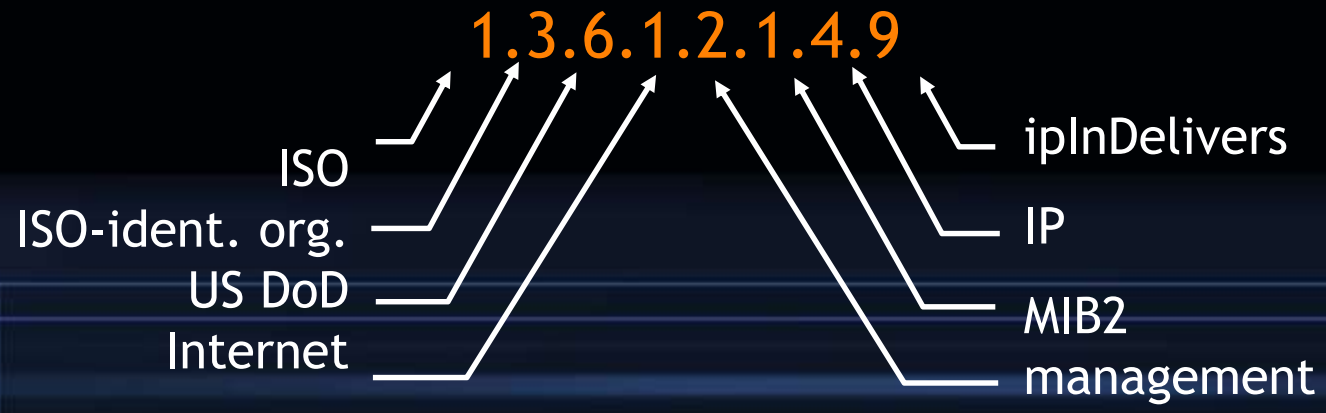
Árvore de identificação de objetos ISO



Objetos são nomeados hierarquicamente

Nomeação de objetos

- **P.: Como nomear cada possível objeto-padrão (protocolos, dados, outros...) em cada possível padrão de rede??**
  - R.: ISO object identifier tree:
    - Nomeação hierárquica de todos os objetos
    - Cada ramificação tem um nome e um número



Pontos Importantes

Gerenciamento de Redes

- Entender o que é
- As vantagens de uso
- Os 3 pontos-chaves: SNMP, MIB, SMI

Ciências da Computação

CAP 7. GERENCIAMENTO DE REDES

AULA 2: Protocolo SNMP e Sistemas de Gerenciamento

INE5422 Redes de Computadores II

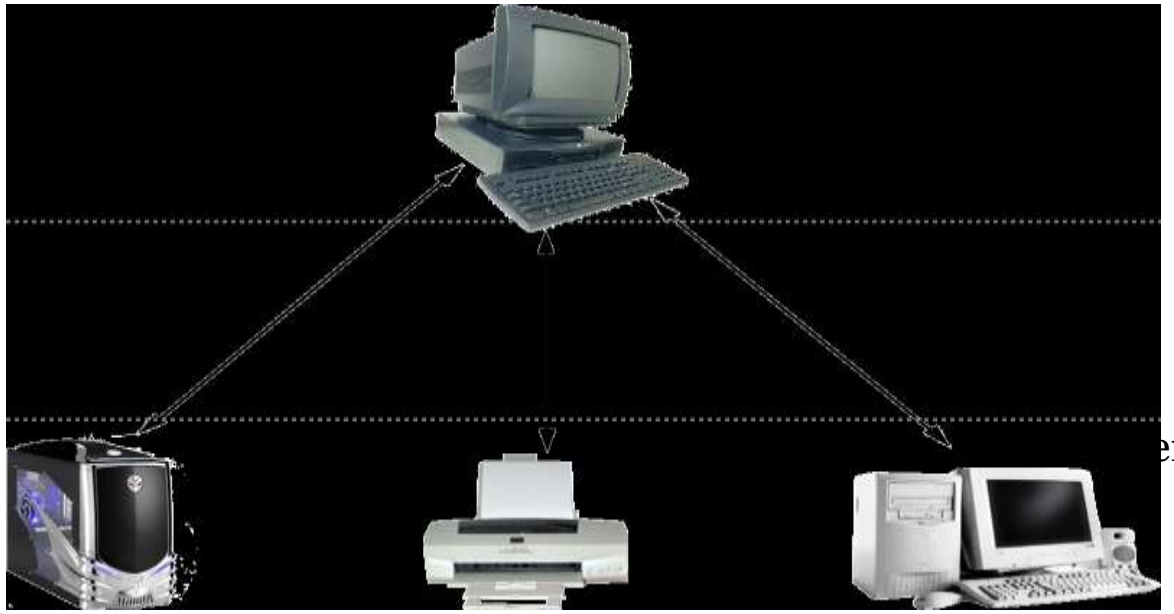
Prof. Roberto Willrich (INE/UFSC)

roberto.willrich@ufsc.br

https://moodle.ufsc.br

Protocolo SNMP

- **Protocolo SNMP (Simple Network Management Protocol)**
  - Padrão de fato para gerenciamento de redes
  - Extensível, permitindo aos fabricantes adicionar funções de gerenciamento aos seus produtos
  - Independente do hardware



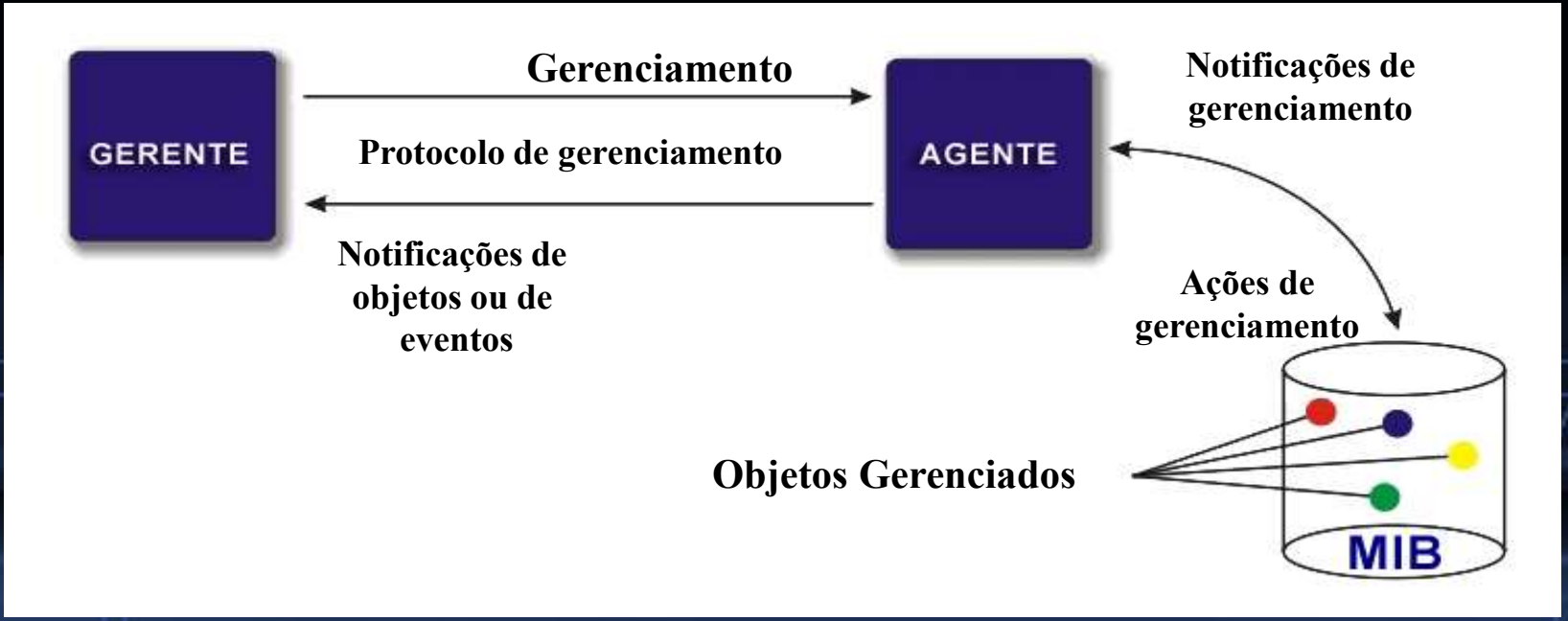
entes

Protocolo SNMP

- **Objeto gerenciado**
  - Representa um recurso, que pode ser um sistema hospedeiro (host, servidor, etc.), um gateway ou equipamento de transmissão (modems, pontes, concentradores, etc.)
  - Cada objeto gerenciado é visto como uma coleção de variáveis cujo valor pode ser lido ou alterado

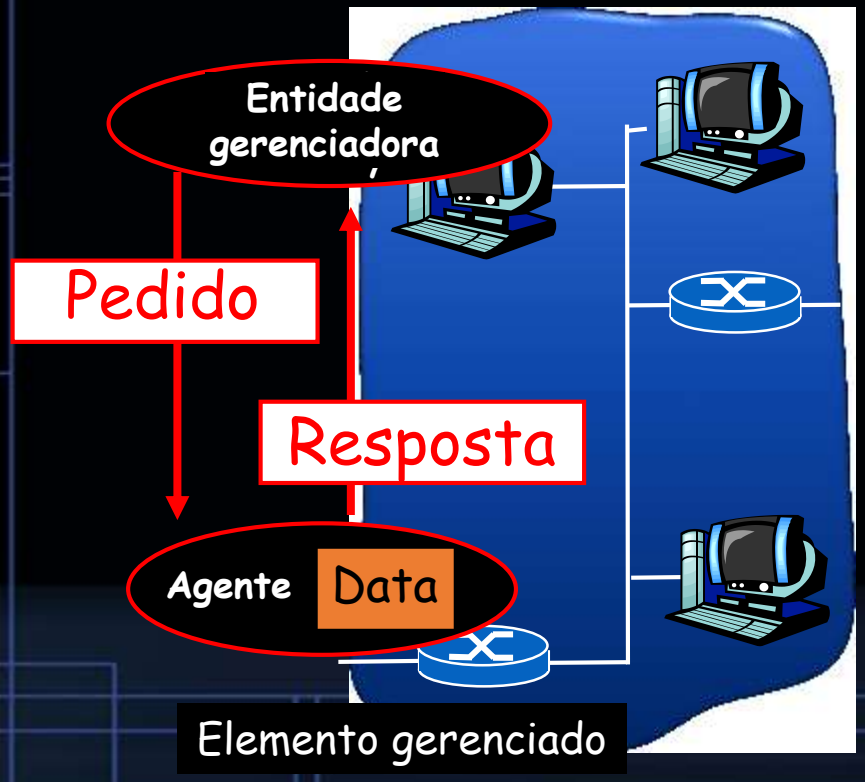
Protocolo SNMP

- **MIB (Management Information Base)**
  - Mantém informações sobre os objetos gerenciados
    - Informações sobre o funcionamento dos hosts, dos gateways, e dos processos que executam os protocolos de comunicação (IP, TCP, ARP, etc.)

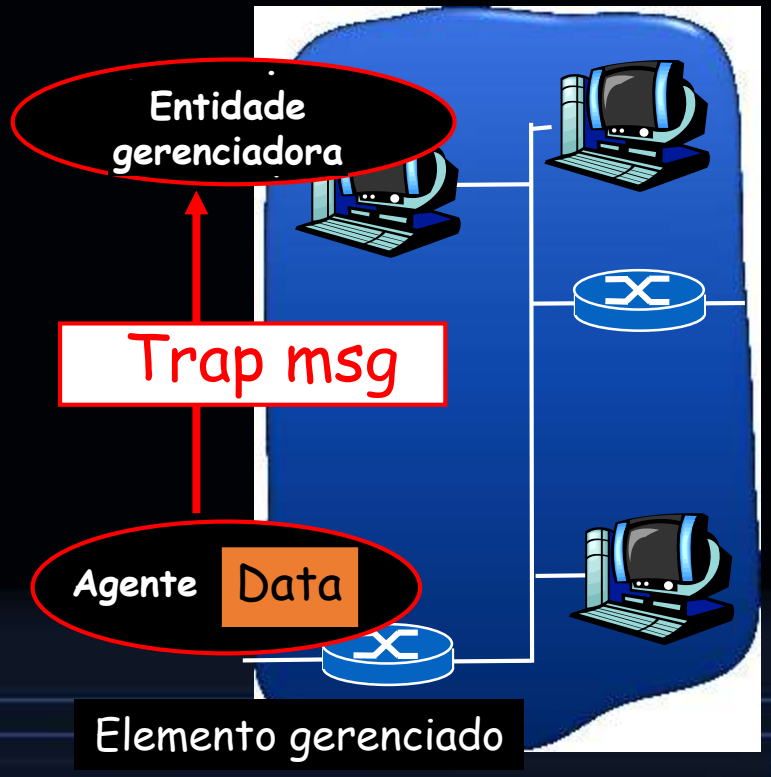


Protocolo SNMP

- **Duas formas de transportar informações da MIB: comandos e eventos**



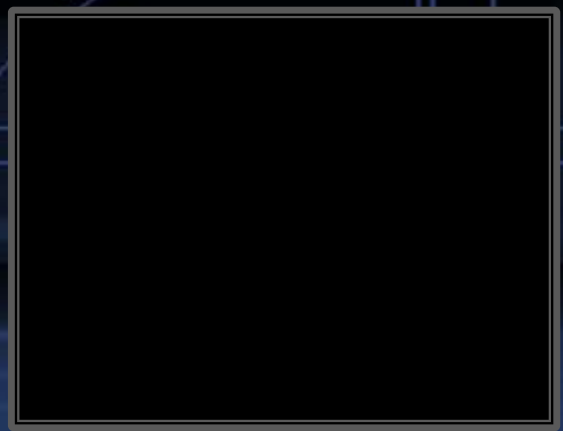
Modo comando/resposta



Modo evento

Protocolo SNMP

- **Três versões são disponíveis hoje:**
  - SNMPv1 (1990)
  - SNMPv2c (1996)
    - Adiciona a função“GetBulk” e novos tipos
    - Adiciona capacidade de monitoramento remoto RMON
  - SNMPv3 (2002)
    - Resolveu problemas de segurança
- **Todas as versão são mantidas hoje**
  - Muitos agentes e gerenciadores SNMP suportam as três versões.

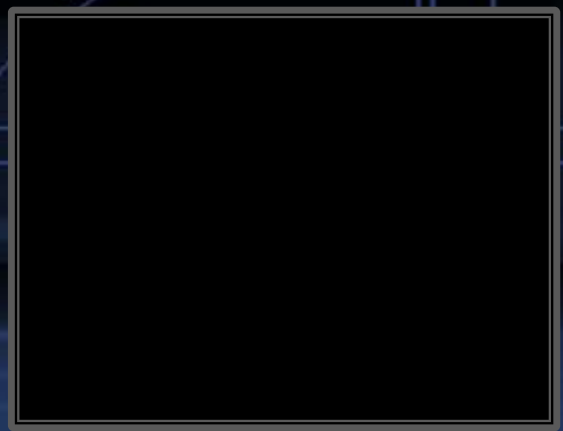


SNMP - Campos das Mensagens

- **Campos**

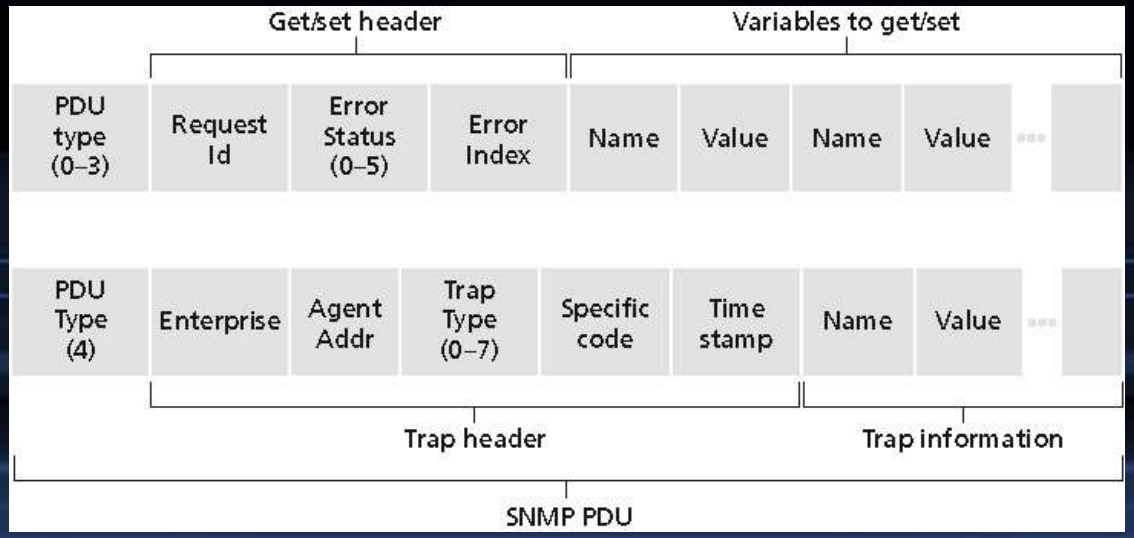
Versão	Comu-nidade	PDU GetRequest, GetNextRequest, GetResponse ou SetRequest

  - Versão. Para garantir que gerente e agente estão executando a mesma versão do protocolo.
    - Mensagens com versões diferentes são descartadas.
  - Comunidade. Garante o acesso a um conjunto limitado de objetos da MIB
    - o agente acessa apenas um conjunto de entidades de aplicação SNMP
  - Caso exista diferenças na comunidade é emitido pelo agente uma trap que indica falha de autenticação
    - Funciona como uma password
  - Caso a versão e comunidade estejam consistentes então é processada a PDU logo a seguir



SNMP - Campos das Mensagens

- **Tipo de PDU. Inteiro que identifica a operação a ser processada**
  - 0 - GetRequest; 1 - GetNextRequest; 2 - GetResponse; 3 - SetRequest;
  - 4 - Trap
- **Request ID. Inteiro que identifica pares de mensagens SNMP entre agente e gerente.**
  - Permite associar a pergunta e a resposta

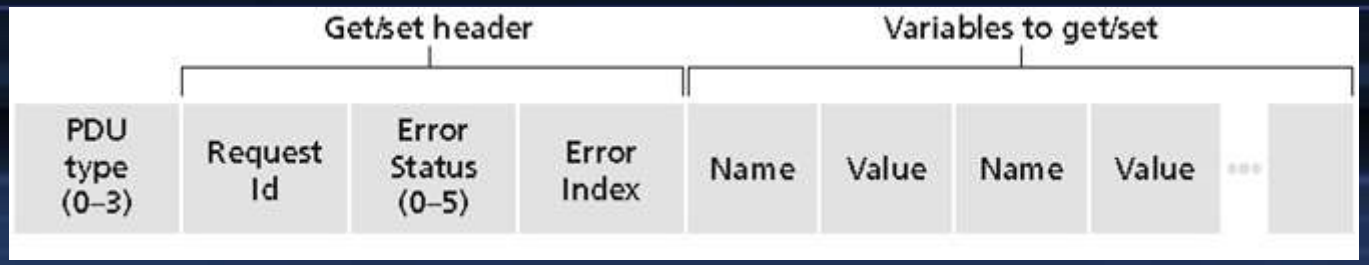


Protocolo SNMP: tipos de mensagens

Tipo de mensagem snmpv2	Função
GetRequest GetNextRequest GetBulkRequest	manager-to-agent: “envie-me dados” (instância, próximo na lista, bloco)
InformRequest	manager-to-manager: eis o valor da MIB
SetRequest	manager-to-agent: define o valor da MIB
Response	agent-to-manager: valor, resposta ao pedido
Trap	agent-to-manager: informa gerenciador de evento excepcional

SNMP - Campos das Mensagens

- **Status de Erro. Identifica operações executadas com sucesso ou um dos cinco erros previstos**
  - 0 (noError) - Operação sem erros
  - 1 (tooBig) - O tamanho da PDU GetResponse excede um limite local
  - 2 (noSuchName) - Não existe objeto com o nome requisitado
  - 3 (badValue) - Uma PDU SetRequest contém uma variável de tipo, tamanho ou valor inconsistente
  - 4 (readOnly) - Uma PDU SetRequest foi enviada para alterar o valor de um objeto read-only
  - 5 (genErr) - Erro genérico



SNMP - Portas e protocolo de transporte

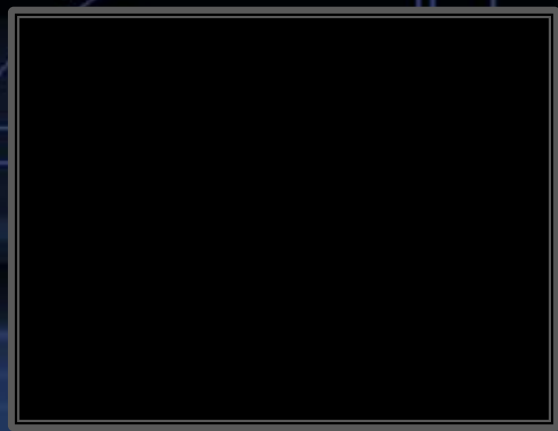
- **SNMP usa protocolo UDP como mecanismo de transporte para mensagens SNMP**
  - Porta 161 - Mensagens SNMP
  - Porta 162 - Mensagens SNMP Trap

Arquitetura de Gerenciamento Baseada na Web

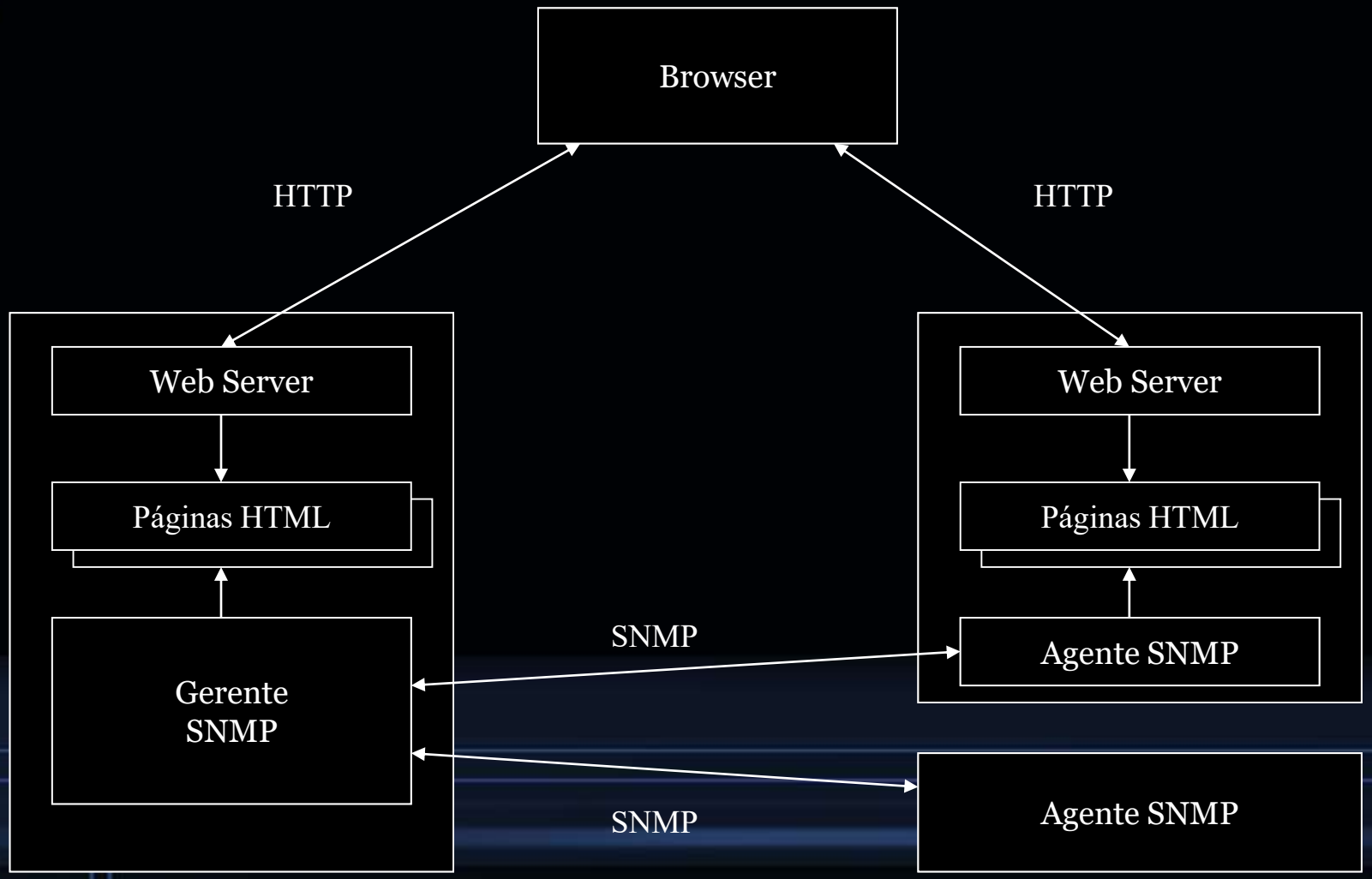
- **Interface de gerenciamento: browser**
  - Vantagem: Independência de plataforma
    - Existem navegadores para todas as plataformas mais usadas
- **As informação de gerenciamento são armazenadas em um WebServer**
  - O browser acessa o WebServer para obter tais informações

Arquitetura de Gerenciamento Baseada na Web

- **Existem duas formas de gerenciamento**
  - Gerentes SNMP usando WebServers
    - O sistema web acessa um gerente que acessa as informações via SNMP
    - As informações são disponibilizadas em páginas Web dinâmicas pelo gerente SNMP
  - Agentes SNMP com HTTP
    - O browser acessa diretamente os recursos através do http
    - O WebServer acessa os dados através de SNMP
    - Os dados são disponibilizados através de páginas HTML geradas pelo agente SNMP
    - O recurso gerenciado deve possuir capacidade de processamento para suportar ao mesmo tempo um WebServer e um agente SNMP

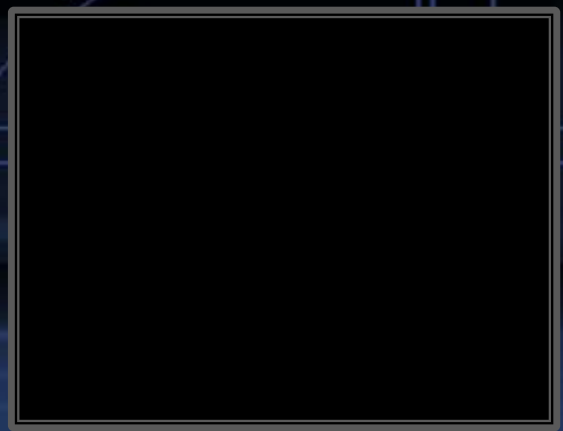


Arquitetura de Gerenciamento Baseada na Web



Ferramentas

- **Cacti (http://www.cacti.net)**
  - Uma interface gráfica web feita em PHP para a ferramenta RRDTool, que coleta dados via SNMP, armazena informações em uma base de dados MySQL
  - Apresenta os gráficos de estatísticas, contas de usuários e demais configurações.



cacti - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://web/cacti/cacti-0.8.6/graph_view.php?action=tree&tree_id=1&leaf_id=10

console graphs settings

Graphs -> Tree Mode

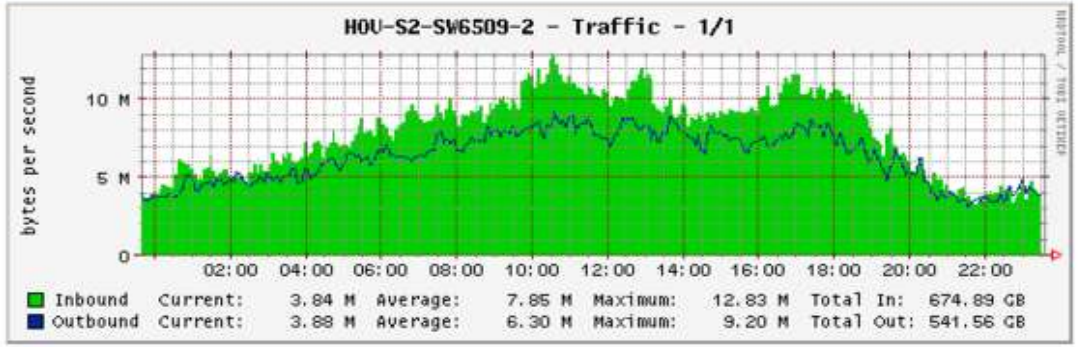
Logged in as **admin** (Logout)

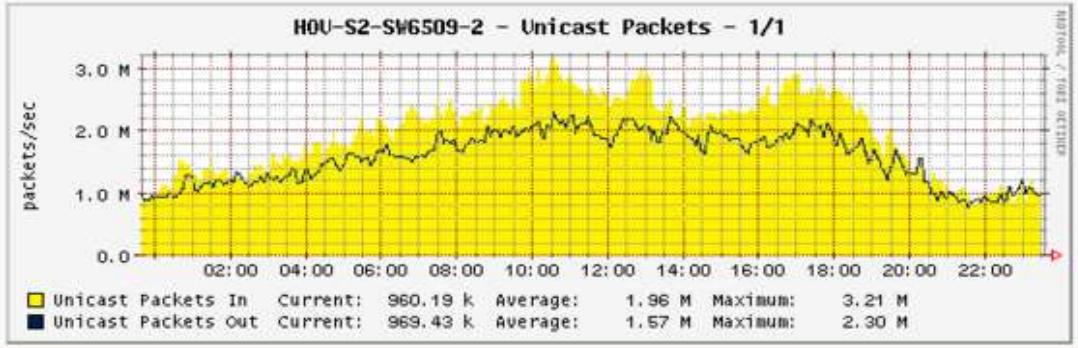
- Arlington, MA
- Charlotte, NC
- Charlottesville, VA
- Columbus, GA
- Dallas, TX
  - Switches
    - **Host:** HOU-S2-SW3548-1
    - **Host:** HOU-S2-SW6509-2
  - Data Center Core
    - **Host:** HOU-A4-ATM-1
    - **Host:** HOU-A4-ATM-2
    - **Host:** HOU-A4-ATM-3
    - **Host:** HOU-A4-ATM-4
- Dayton, OH
- Detroit, MI
- Harrisburg, PA
  - Web Hosting Farm
    - **Host:** HAR-CUST-WWW0
    - **Host:** HAR-CUST-WWW1
    - **Host:** HAR-CUST-WWW2
    - **Host:** HAR-CUST-WWW3
    - **Host:** HAR-CUST-WWW4
    - **Host:** HAR-CUST-WWW5
- Houston, TX
- Miami, FL
  - Public Peering
    - **Host:** MIA-R8-C7200-3
- Phoenix, AZ
- Salt Lake City, UT
- San Diego, CA

Tree: Dallas, TX-> **Host:** HOU-S2-SW6509-2

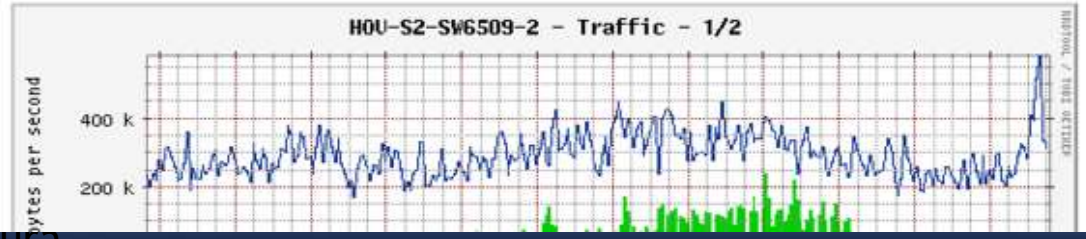
Data Query: SNMP - Interface Statistics

Port 1/1



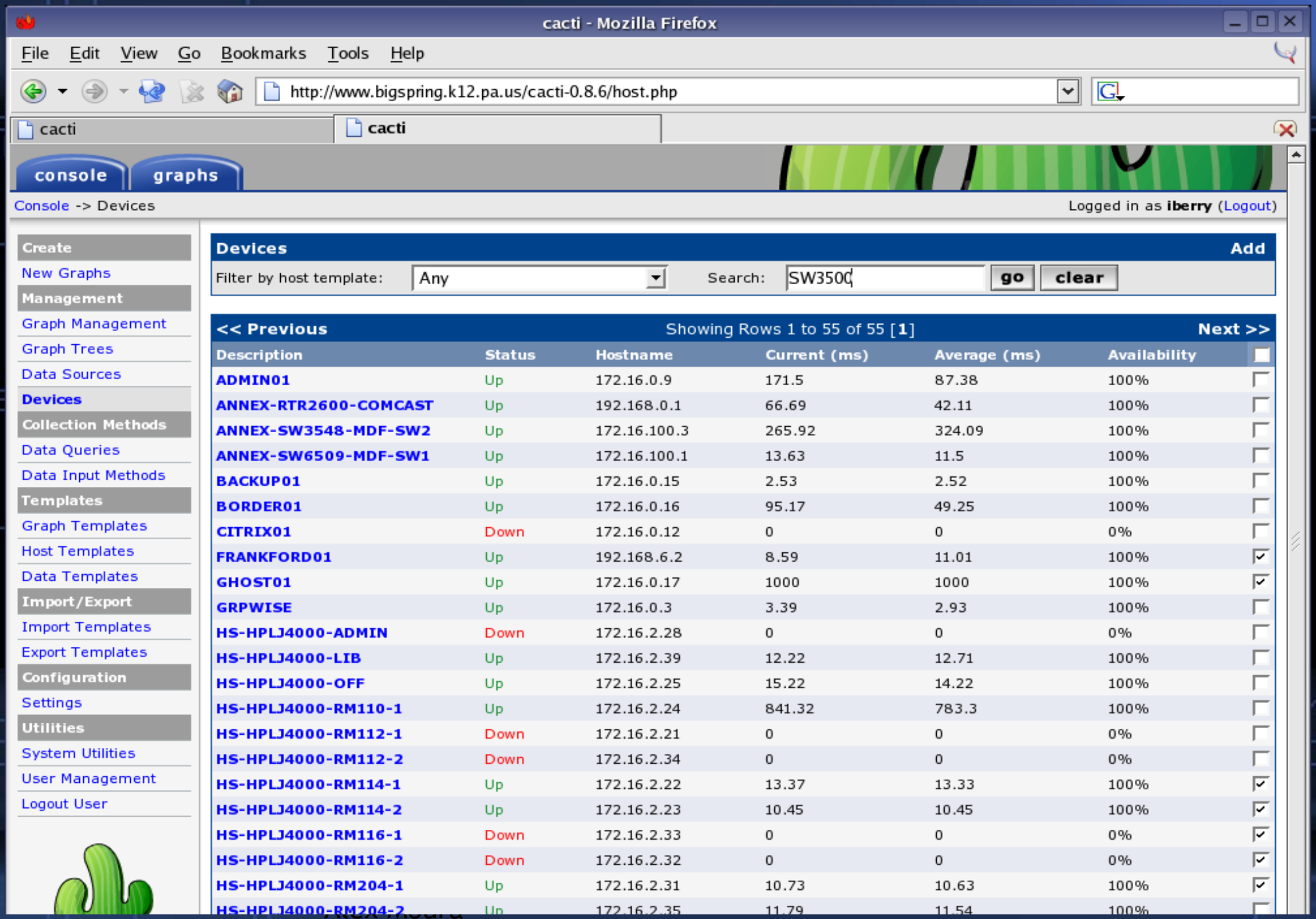


Port 1/2



Alex Moura

UFSC


cacti - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.bigspring.k12.pa.us/cacti-0.8.6/host.php
cacti
cacti
console
graphs
Console -> Devices
Logged in as iberry (Logout)
Create
New Graphs
Management
Graph Management
Graph Trees
Data Sources
Devices
Collection Methods
Data Queries
Data Input Methods
Templates
Graph Templates
Host Templates
Data Templates
Import/Export
Import Templates
Export Templates
Configuration
Settings
Utilities
System Utilities
User Management
Logout User
Devices
Add
Filter by host template:
Any
Search:
SW350
go
clear
<< Previous
Showing Rows 1 to 55 of 55 [1]
Next >>
Description
Status
Hostname
Current (ms)
Average (ms)
Availability
ADMIN01 Up 172.16.0.9 171.5 87.38 100%
ANNEX-RTR2600-COMCAST Up 192.168.0.1 66.69 42.11 100%
ANNEX-SW3548-MDF-SW2 Up 172.16.100.3 265.92 324.09 100%
ANNEX-SW6509-MDF-SW1 Up 172.16.100.1 13.63 11.5 100%
BACKUP01 Up 172.16.0.15 2.53 2.52 100%
BORDER01 Up 172.16.0.16 95.17 49.25 100%
CITRIX01 Down 172.16.0.12 0 0 0%
FRANKFORD01 Up 192.168.6.2 8.59 11.01 100%
GHOST01 Up 172.16.0.17 1000 1000 100%
GRPWISE Up 172.16.0.3 3.39 2.93 100%
HS-HPLJ4000-ADMIN Down 172.16.2.28 0 0 0%
HS-HPLJ4000-LIB Up 172.16.2.39 12.22 12.71 100%
HS-HPLJ4000-OFF Up 172.16.2.25 15.22 14.22 100%
HS-HPLJ4000-RM110-1 Up 172.16.2.24 841.32 783.3 100%
HS-HPLJ4000-RM112-1 Down 172.16.2.21 0 0 0%
HS-HPLJ4000-RM112-2 Down 172.16.2.34 0 0 0%
HS-HPLJ4000-RM114-1 Up 172.16.2.22 13.37 13.33 100%
HS-HPLJ4000-RM114-2 Up 172.16.2.23 10.45 10.45 100%
HS-HPLJ4000-RM116-1 Down 172.16.2.33 0 0 0%
HS-HPLJ4000-RM116-2 Down 172.16.2.32 0 0 0%
HS-HPLJ4000-RM204-1 Up 172.16.2.31 10.73 10.63 100%
HS-HPLJ4000-RM204-2 Up 172.16.2.35 11.79 11.54 100%

cacti - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.bigspring.k12.pa.us/cacti-0.8.6/graph_view.php?action=tree&tree_id=31&leaf_id=408

graphs settings

Graphs -> Tree Mode

- Backbone - Annex
  - Host: ANNEX-SW6509-MDF-SW1
  - Host: ANNEX-SW3548-MDF-SW2
  - Host: ANNEX-RTR2600-COMCAST
- Backbone - High School
- Backbone - Middle School
  - Host: MS-SW3548-MDF-SW1
- Backbone - Old High School
- Backbone - WAN
- Elementary Servers
- Printers
- Servers
  - Host: ADMIN01
  - Host: BACKUP01
  - Host: BORDER01
  - Host: CITRIX01
  - Host: GHOST01
  - Host: GRPWISE
  - Host: SPEC-ED
  - Host: WWW
- Weather
- Wireless Statistics

Presets: Last Day From: 2004-08-27 22:47 To: 2004-08-28 22:47 refresh clear

August, 2004

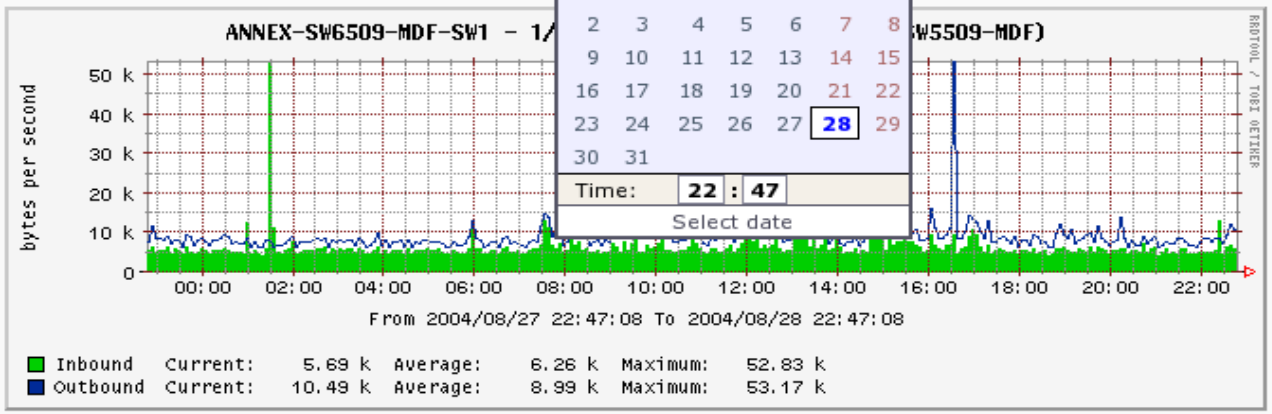
Mon	Tue	Wed	Thu	Fri	Sat	Sun
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

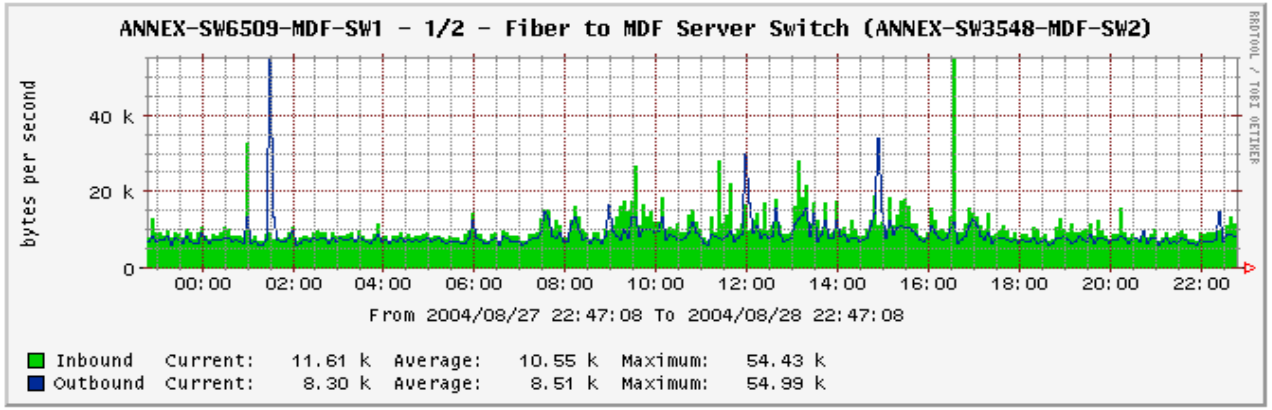
Time: 22 : 47

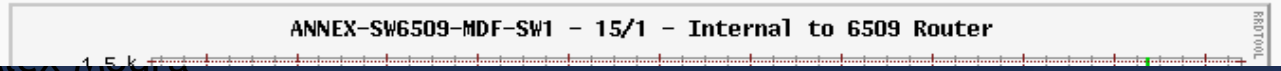
Select date

Tree: Backbone - Annex-> Host: ANNEX-SW6509-MD

Graph Template: Interface - Backbone Traffic

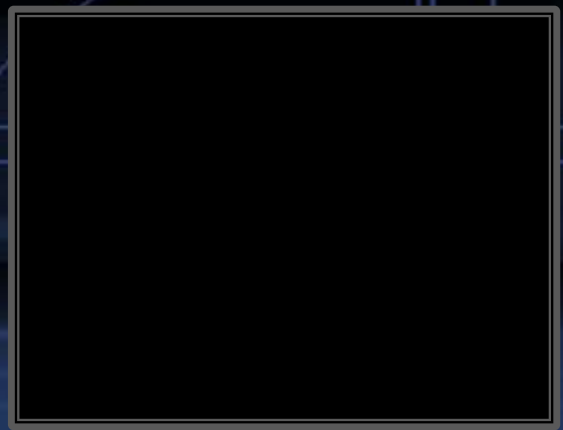




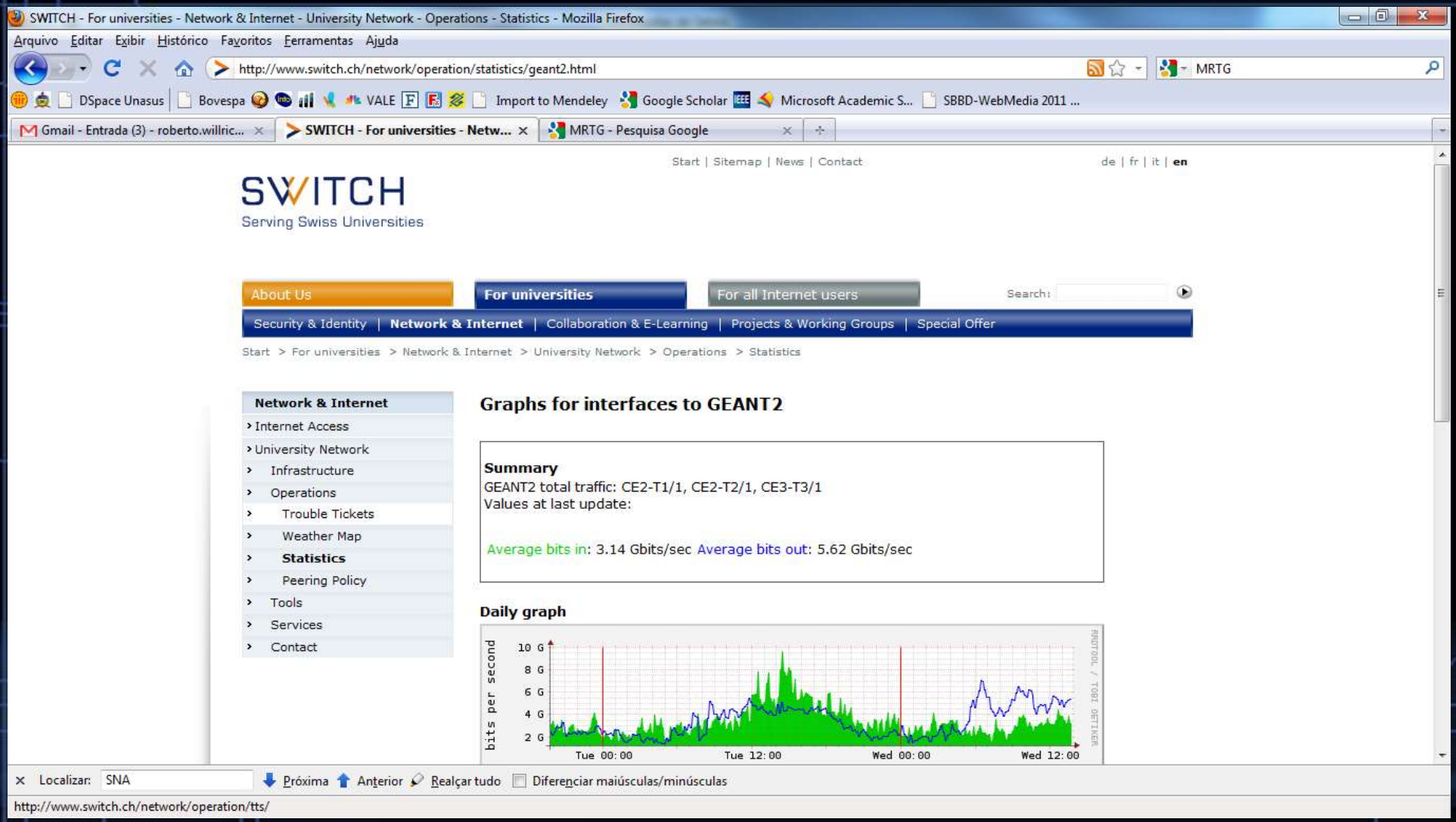


Ferramentas

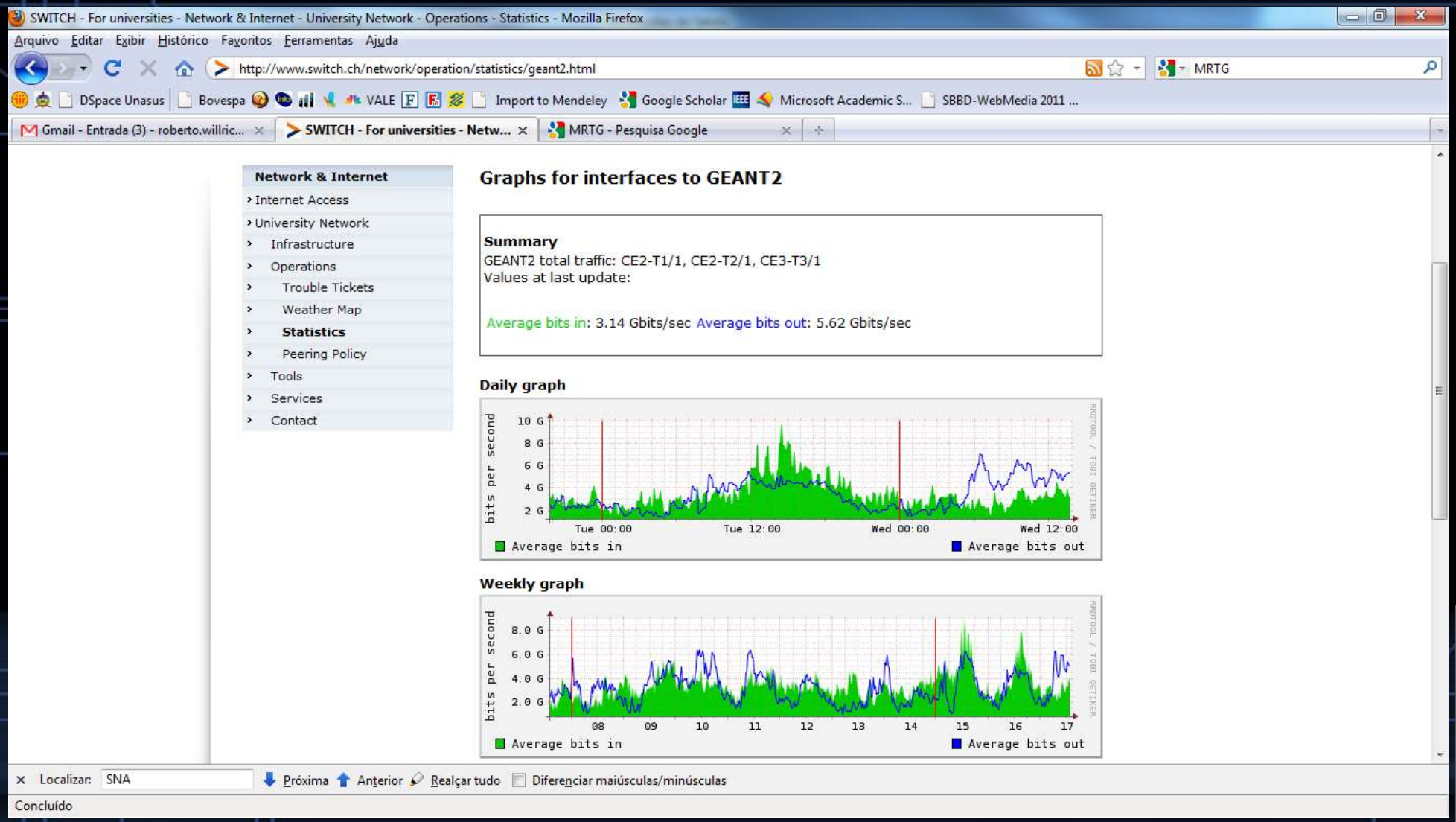
- **MRTG - Ferramenta para coletar informações e gerar estatísticas**
  - http://www.mrtg.org/
  - Usada para registrar tráfego de rede
  - Gera páginas HTML com imagens PNG
  - Fornece uma representação visual do tráfego
  - Permite monitorar e analisar diversas funções (roteadores, servidores, latência, utilização, temperatura etc.)
  - Diversas formas de visualização de dados
  - Licença: GPL
  - Autor: Tobias Oetiker



Ferramentas

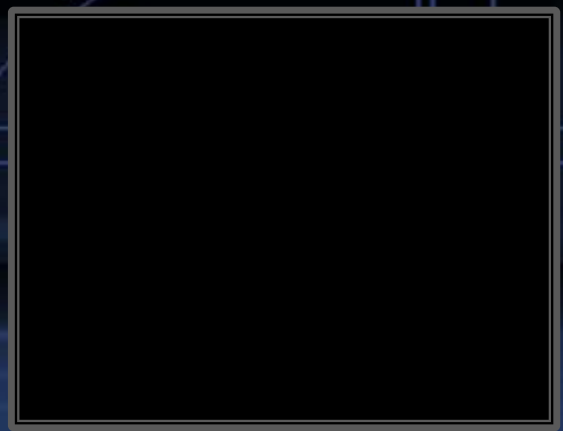


Ferramentas

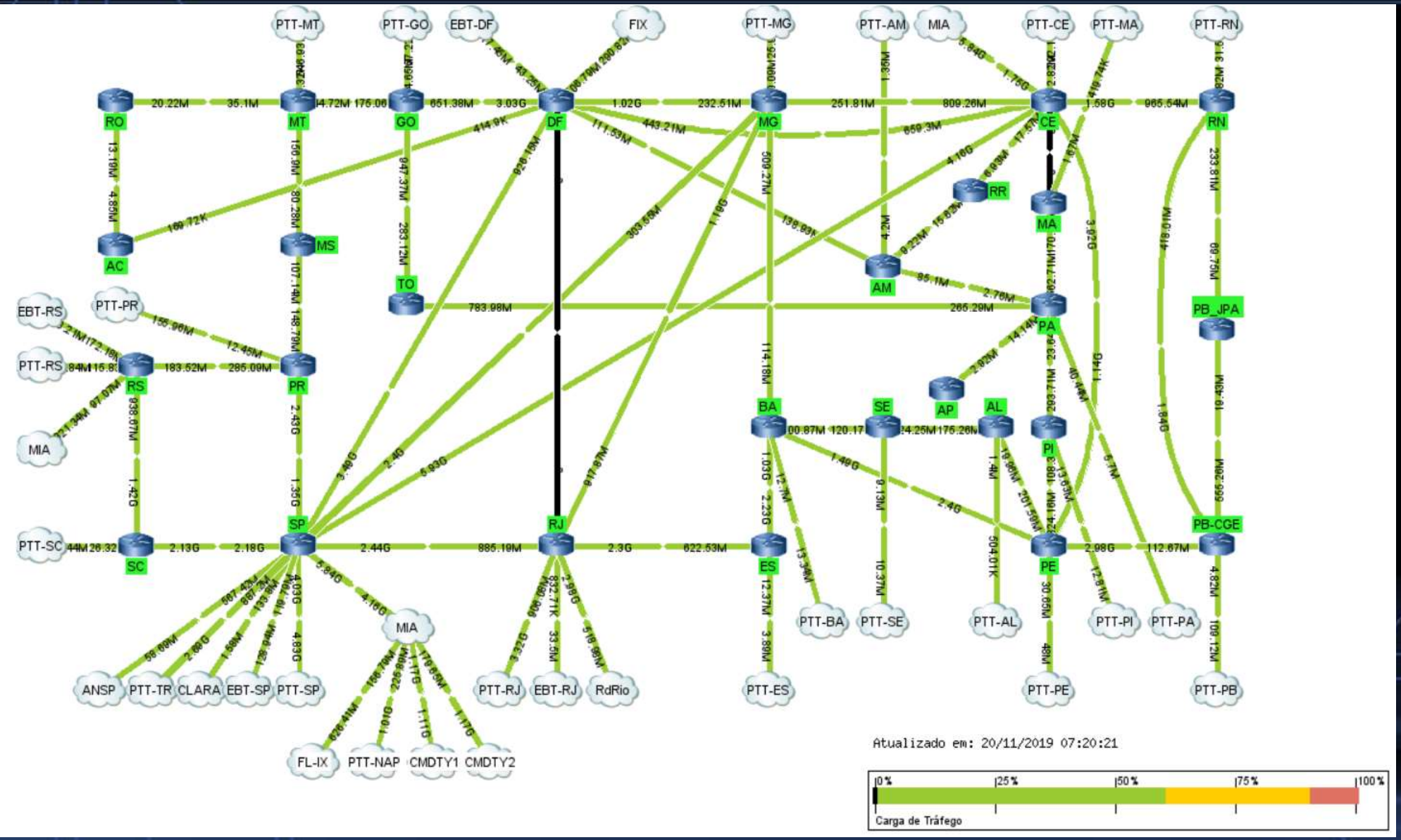


Network Weathermap

- **Network Weathermap –Software livre e gratuito, feito em script perl**
  - http://netmon.grnet.gr/weathermap
  - Licença: GPL (General Public License)
  - Linguagem: Perl



Network Weathermap da RNP



Pontos Importantes

Protocolo SNMP

- Entender as principais características e funções do SNMP