

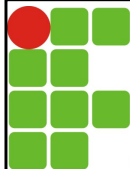
INSTITUTO FEDERAL DE  
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA  
RIO GRANDE DO NORTE



# Redes de Computadores

## Gerenciamento de Redes

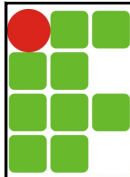
Prof. Thiago Dutra <thiago.dutra@ifm.edu.br>



## Agenda

- Introdução
- O que Gerenciar ?
- Definição
- Modelo de Gerenciamento
- Infraestrutura de Gerenciamento
- Padrão de Gerenciamento na Internet
  - SMI, MIB, SNMP, Segurança e Administração
- Ferramentas de Gerenciamento

2

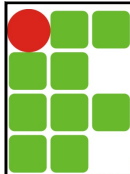


## Introdução

- Sistemas complexos, em todas as áreas de atuação, com diversos componentes interagindo necessitam ser monitorados e controlados
  - Avião de grande porte
  - Usina de geração de energia



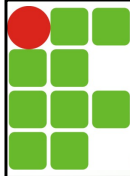
3



## Introdução

- Nesses sistemas, os operadores (pilotos, engenheiros, etc.) são responsáveis por visualizarem uma série de dados para garantir que os dispositivos (equipamentos, sensores, etc.) estejam funcionando e operando dentro dos limites especificados
- Papéis dos operadores
  - **Controlar reativamente** o sistema: realizar ajustes no sistema baseado em mudanças ocorridas no ambiente/sistema
  - **Gerenciar pró-ativamente** o sistema: por exemplo, detectar tendências ou comportamentos anômalos e realizando ações antes do surgimento de problemas sérios

4

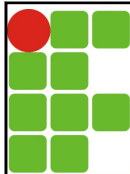


## Introdução

- Nesse mesmo sentido, o administrador de rede deve monitorar, gerenciar e controlar o "sistema" do qual esta encarregado
- NOC (Network Operations Center)
  - Centro de Operações de Rede

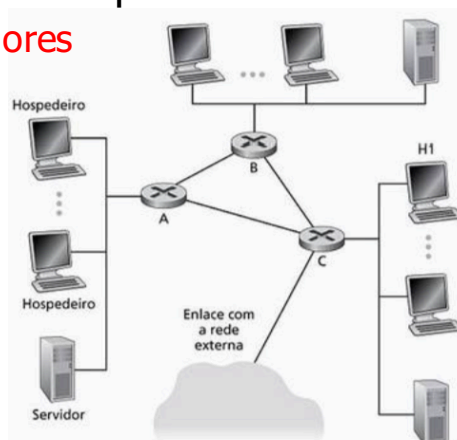


5

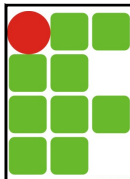


## O que Gerenciar ?

- Exemplo de uma rede simples
  - Três switches/roteadores
  - Estações clientes
  - Servidores

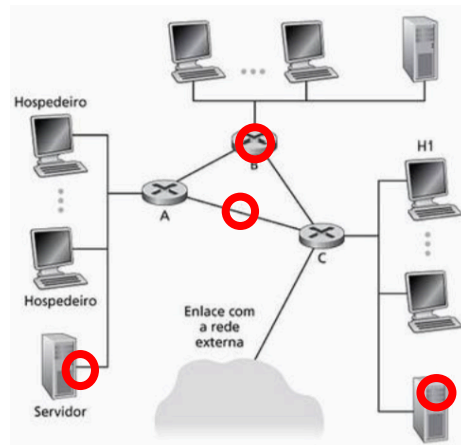


6

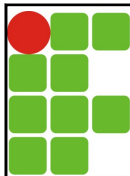


## O que Gerenciar ?

- O que gerenciar ?
  - Falhas em enlaces de rede
  - Falhas em interfaces de rede
  - Falhas em ativos de rede
  - Falhas no hardware ou software dos servidores
  - ...

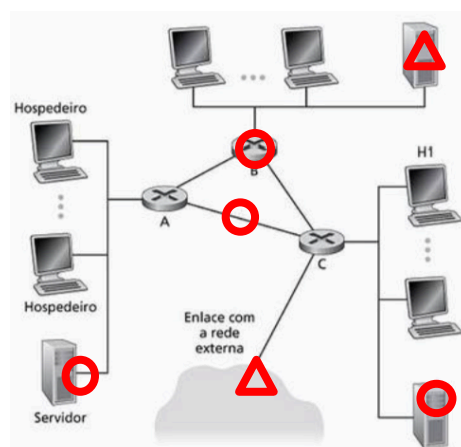


7

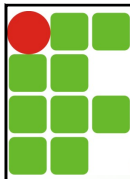


## O que Gerenciar ?

- O que gerenciar ?
  - Disponibilidade de serviços em servidores
  - Disponibilidade do acesso à Internet
  - ...

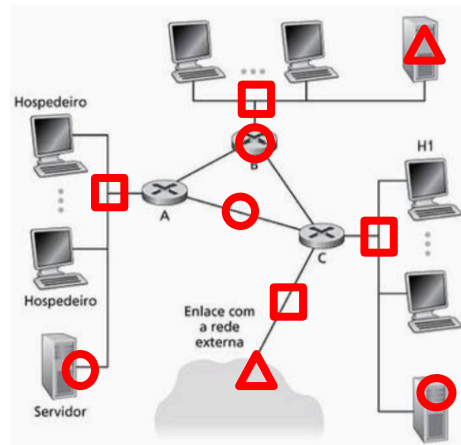


8

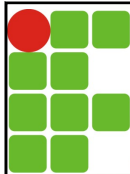


## O que Gerenciar ?

- O que gerenciar ?
  - Estatísticas de tráfego e uso de links na rede interna
  - Estatísticas de tráfego e uso de link na saída para Internet
  - ...

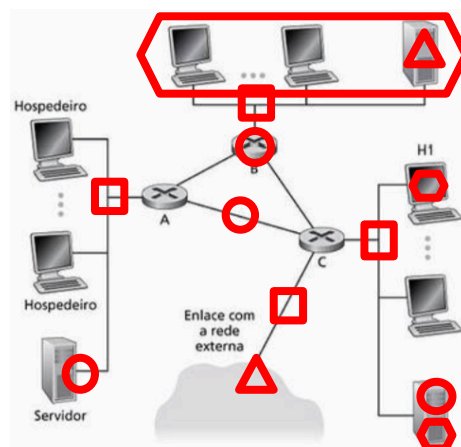


9

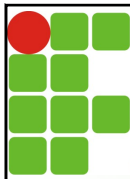


## O que Gerenciar ?

- O que gerenciar ?
  - Alterações no hardware de estações clientes e/ou servidores
  - Alterações significativas no "comportamento" da rede
  - ...

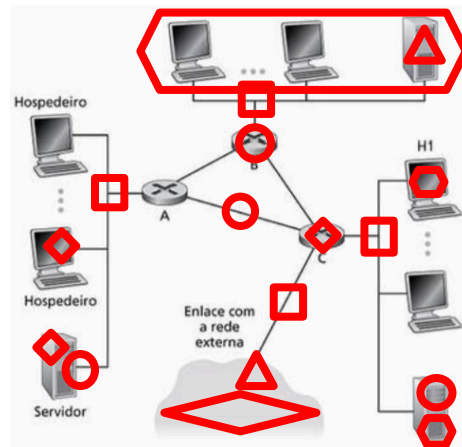


10

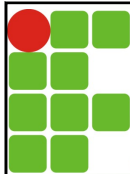


## O que Gerenciar ?

- O que gerenciar ?
  - Ocorrência de tráfegos vindos de fontes suspeitas
  - Ocorrência de eventos característicos de ataques
  - ...



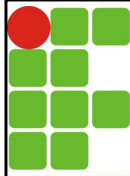
11



## Definição

- [Saydam, 1996]
  - "Gerenciamento de redes inclui o fornecimento, integração e coordenação de hardware, software e elementos humanos para monitorar, testar, configurar, consultar, analisar, avaliar e controlar a rede e recursos para atender aos requisitos de desempenho, qualidade de serviço e operação em tempo real dentro de um custo razoável."

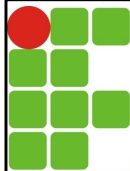
12



## Modelo de Gerenciamento

- No passado :
  - Não havia preocupação com questões de gerenciamento nas primeiras redes (ex.: ARPAnet)
  - As redes eram utilizadas por poucos usuários
  - Os usuários tinham conhecimento técnico sobre o funcionamento da rede
  - Quando ocorria um problema os próprios usuários realizavam testes e ajustes necessários para solucioná-lo
  - [RFC 789] – 1981 : primeira grande “queda” da ARPAnet

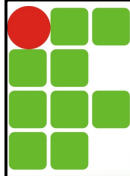
13



## Modelo de Gerenciamento

- No presente :
  - Intenso crescimento das Intranets privadas e da Internet pública
  - As redes são grandes infraestruturas, comumente com centenas ou milhares de elementos de hardware e software
  - O perfil do usuário torna-se cada vez mais “leigo”
- **Surge então a necessidade de uma forma sistêmica de gerenciamento de rede**

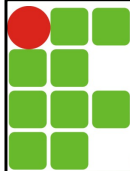
14



## Modelo de Gerenciamento

- A ISO criou um modelo de gerenciamento de redes que situa os exemplos anteriormente citados de uma maneira mais estruturada
- São definidas 5 áreas de gerenciamento de redes :
  - Gerenciamento de desempenho
  - Gerenciamento de falhas
  - Gerenciamento de contabilização
  - Gerenciamento de configuração
  - Gerenciamento de segurança

15

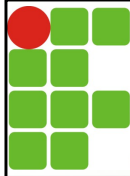


## Modelo de Gerenciamento

- Gerenciamento de desempenho : Quantificar, medir, informar, analisar e controlar o desempenho (ex.: utilização, vazão) de diferentes componentes de rede
- Gerenciamento de falhas : Registrar, detectar e reagir às condições de falha na rede
- Gerenciamento de configuração : Permitir ao administrador saber quais dispositivos fazem parte da rede e suas respectivas configurações de hardware e software
- Gerenciamento de contabilização : Especificar, registrar e controlar o acesso de usuários e dispositivos aos recursos da rede. Ex.: Quotas de utilização e cobrança por utilização
- Gerenciamento de segurança : Controlar o acesso aos recursos da rede de acordo com alguma política definida

16

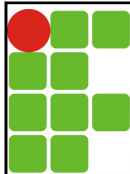




## Infraestrutura de Gerenciamento

- Possui 3 componentes principais :

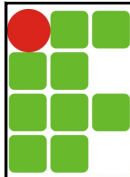
- Entidade gerenciadora
- Dispositivos gerenciados
- Protocolo de gerenciamento de rede



## Infraestrutura de Gerenciamento

- Entidade gerenciadora
  - Aplicação que em geral tem um ser humano no circuito e que é executada em uma estação central de gerência de rede no NOC
  - É o ponto de partida da atividade de gerenciamento de rede : ela controla a coleta, o processamento, a análise e/ou a apresentação das informações de gerenciamento de rede
  - É nela que são iniciadas ações para controlar o comportamento da rede, onde administrador humano interage com os dispositivos de rede

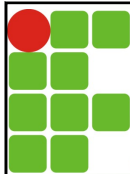
18



## Infraestrutura de Gerenciamento

- Dispositivo gerenciado
  - Equipamento de rede (incluindo seu software) dentro de uma rede gerenciada
    - Servidor, estação, roteador, switch, hub, bridge, impressora, ...
  - No dispositivo podem existir vários **objetos gerenciados**
    - Hardwares (ex.: placa de rede) e conjuntos de parâmetros de configuração para o hardware e software (ex.: RIP)
    - As informações associadas aos objetos são coletadas dentro de uma Base de Informações de Gerenciamento (MIB)
  - Em cada dispositivo reside um **agente de gerenciamento**
    - Processo que se comunica com a entidade gerenciadora e que executa ações no dispositivo sob comando e controle da entidade

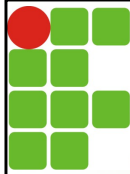
19



## Infraestrutura de Gerenciamento

- Protocolo de gerenciamento de rede
  - O protocolo é executado entre a entidade gerenciadora e o agente de gerenciamento
  - **Permite que a entidade gerenciadora investigue o estado dos dispositivos gerenciados e, através do agente, execute ações sobre eles**
    - Os agentes também podem usar o protocolo de gerenciamento para **informar a entidade gerenciadora sobre a ocorrência de eventos excepcionais**
  - Obs.: o protocolo em si não gerencia a rede, ele **fornece uma ferramenta pela qual o administrador pode gerenciar**

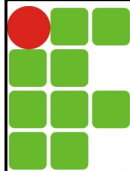
20



## Padrão de Gerenciamento na Internet

- Padrões de gerenciamento de rede começam a amadurecer no final da década de 1980
- Surgem 2 padrões principais que são independentes de produtos ou de redes proprietárias :
  - OSI CMISE/CMIP
    - Padrão de gerenciamento por excelência, porém sua padronização foi lenta demais
  - **SNMP (Simple Network Management Protocol)**
    - Originado na Internet (aprimoramento do SGMP)
    - Começou simples, foi projetado e oferecido rapidamente numa época que o gerenciamento começava a despontar, encontrando assim uma ampla aceitação
    - **É hoje o padrão de fato, evoluiu em tamanho e complexidade (SNMPv3)**

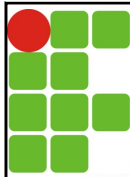
21



## Padrão de Gerenciamento na Internet

- A estrutura do padrão de gerenciamento na Internet é constituída de 4 partes :
  - **Uma linguagem de definição de dados**
    - SMI (Structure of Management Information)
  - **Definições dos objetos de gerenciamento de rede**
    - Objetos SMI e módulos MIB
  - **Um protocolo**
    - SNMP
  - **Capacidades de segurança e administração**

22

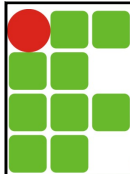


# Padrão de Gerenciamento na Internet SMI

- SMI (Structure of Management Information)
  - Linguagem usada para definir as informações de gerenciamento
  - **Assegura que a sintaxe e a semântica dos dados de gerenciamento sejam bem definidas e sem ambiguidade**
  - Tipos de dados básicos :

INTEGER	Número inteiro de 32 bits, como definido em ASN.1, com valor entre $-2^{31}$ e $2^{31} - 1$ , inclusive, ou um valor de uma lista de valores constantes possíveis, nomeados.
Integer32	Número inteiro de 32 bits, com valor entre $-2^{31}$ e $2^{31} - 1$ , inclusive.
Unsigned32	Número inteiro de 32 bits sem sinal na faixa de 0 a $2^{32} - 1$ , inclusive.
OCTET STRING	Cadeia de bytes de formato ASN.1 que representa dados binários arbitrários ou de texto de até 65.535 bytes de comprimento.
OBJECT IDENTIFIER	Formato ASN.1 atribuído administrativamente (nome estruturado); veja a Seção 9.3.2.
Endereço IP	Endereço Internet de 32 bits, na ordem de bytes de rede.
Counter32	Contador de 32 bits que cresce de 0 a $2^{32} - 1$ e volta a 0.
Counter64	Contador de 64 bits.
Gauge32	Número inteiro de 32 bits que não faz contagens além de $2^{32} - 1$ nem diminui para menos do que 0.
TimeTicks	Tempo, medido em centésimos de segundo, transcorrido a partir de algum evento.
Opaque	Cadeia ASN.1 não interpretada, necessária para compatibilidade com versões anteriores.

23



# Padrão de Gerenciamento na Internet SMI

- Principais construções SMI de mais alto nível
  - **OBJECT-TYPE** : especifica o tipo de dado, o status e a semântica de um objeto gerenciado
  - **MODULE-IDENTITY** : agrupar objetos relacionados entre si, formando um "módulo"

```

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}

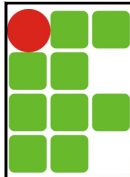
```

```

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}

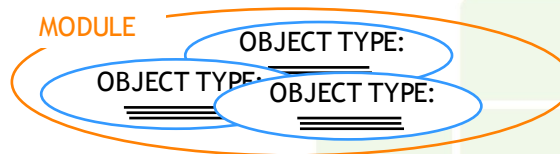
```

24

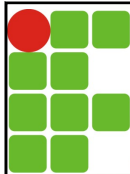


## Padrão de Gerenciamento na Internet MIB

- MIB (Management Information Base)
  - Base de Informações de Gerenciamento
  - Banco virtual de informações que guarda objetos gerenciados cujos valores, coletivamente, refletem o "estado" atual da rede
  - Esses valores podem ser consultados e/ou definidos por uma entidade gerenciadora por meio de mensagens SNMP enviadas aos agentes

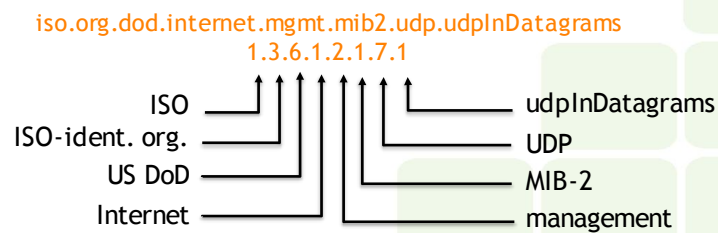


25

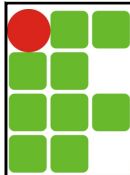


## Padrão de Gerenciamento na Internet MIB

- Nomenclatura dos objetos
  - Utiliza o padrão ISO object identifier tree
    - Nomeação hierárquica (árvore) de todos os objetos
    - Cada ramificação tem um nome e um número
    - Os objetos (folhas) possuem um identificador único (OID)

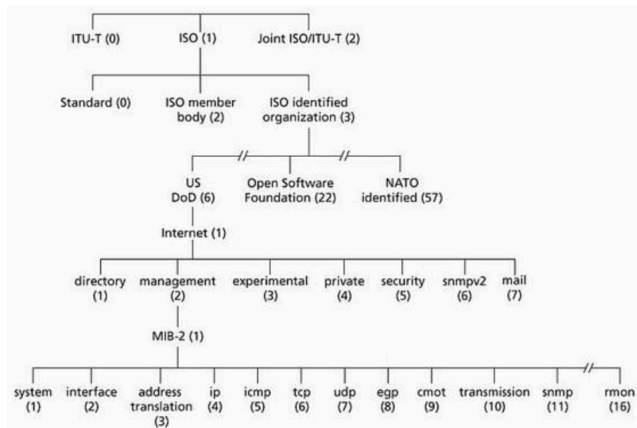


26

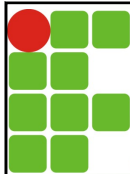


# Padrão de Gerenciamento na Internet MIB

## Árvore de identificadores



27

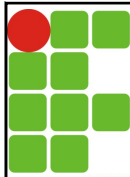


# Padrão de Gerenciamento na Internet MIB

## Exemplos de objetos gerenciados no grupo system da MIB-2

Identificador de objeto	Nome	Tipo	Descrição (segundo o RFC 1213)
1.3.6.1.2.1.1.1	sysDescr	OCTET STRING	"Nome completo e identificação da versão do tipo de hardware do sistema, do sistema operacional do software e do software de rede."
1.3.6.1.2.1.1.2	sysObjectID	OBJECT IDENTIFIER	ID atribuído pelo fabricante do objeto que "fornece um meio fácil e não ambíguo para determinar 'que tipo de caixa' está sendo gerenciado."
1.3.6.1.2.1.1.3	sysUpTime	TimeTicks	"O tempo (em centésimos de segundo) desde que a porção de gerenciamento de rede do sistema foi reinicializado pela última vez."
1.3.6.1.2.1.1.4	sysContact	OCTET STRING	"A pessoa de contato para esse nó gerenciado, juntamente com o informação sobre como contatá-la."
1.3.6.1.2.1.1.5	sysName	OCTET STRING	"Um nome atribuído administrativamente para esse nó gerenciado. Por convenção, esse é o nome de domínio totalmente qualificado do nó."
1.3.6.1.2.1.1.6	sysLocation	OCTET STRING	"A localização física do nó."
1.3.6.1.2.1.1.7	sysServices	Integer32	Um valor codificado que indica o conjunto de serviços disponível no nó: aplicações físicas (por exemplo, um repetidor), de enlace/sub-rede (por exemplo, ponte), de Internet (por exemplo, gateway IP), fim a fim (por exemplo, hospedeiro).

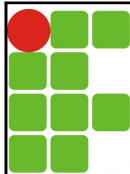
28



## Padrão de Gerenciamento na Internet SNMP

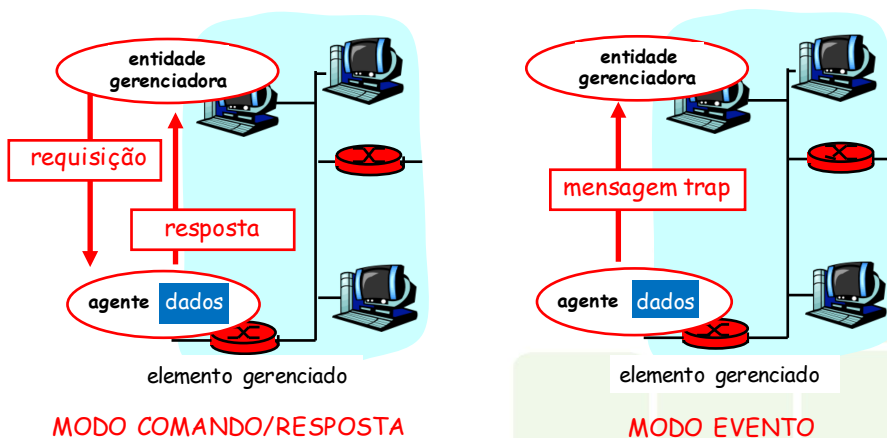
- SNMP (Simple Network Management Protocol)
  - Protocolo Simples de Gerenciamento de Rede
  - Usado para transportar informações da MIB entre entidades gerenciadoras e agentes
  - Possui 2 modos de transportar informações :
    - **Modo comando-resposta** : entidade gerenciadora envia requisição ao agente, que a recebe, realiza alguma ação (consultar ou modificar valores de objetos MIB) e envia uma resposta
    - **Modo evento** : o agente envia uma mensagem não solicitada (trap) à entidade gerenciadora; as mensagens são usadas para notificar um situação excepcional que resultou em mudança nos valores de objetos MIB

29

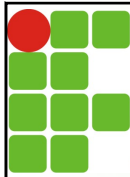


## Padrão de Gerenciamento na Internet SNMP

- Modos de transportar informações



30

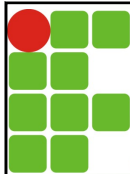


## Padrão de Gerenciamento na Internet SNMP

### ■ Tipos de mensagens SNMP

GetRequest	gerente a agente	pega o valor de uma ou mais instâncias de objetos MIB
GetNextRequest	gerente a agente	pega o valor da próxima instância de objeto MIB na lista ou tabela
GetBulkRequest	gerente a agente	pega valores em grandes blocos de dados, por exemplo, valores em uma grande tabela
InformRequest	gerente a gerente	informa à entidade gerenciadora remota valores da MIB que são remotos para seu acesso
SetRequest	gerente a agente	define valores de uma ou mais instâncias de objetos MIB
Response	agente a gerente ou gerente a gerente	gerada em resposta a  GetRequest.  GetNextRequest.  GetBulkRequest.  SetRequest PDU ou InformRequest
SNMPv2-Trap	agente a gerente	informa ao gerente um evento excepcional

31



## Padrão de Gerenciamento na Internet SNMP

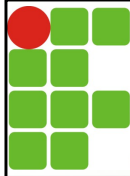
### ■ Exemplo de consultas SNMP

```
c:\usr\bin>snmpget -c public -v 1 -o f 10.0.0.127 1.3.6.1.2.1.1.3.0
.iso.org.dod.internet.mgmt.mib-2.system.sysUptime.sysUptimeInstance = Timeticks:
<128413495> 14 days, 20:42:14.95

c:\usr\bin>snmpwalk -c public -v 1 -o f 10.0.0.127 1.3.6.1.2.1.1
.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0 = STRING: 48-Port 10/100/1000
Gigabit Switch with WebUIw
.iso.org.dod.internet.mgmt.mib-2.system.sysObjectID.0 = OID: .iso.org.dod.intern
et.private.enterprises.3955.6.1.2048.1
.iso.org.dod.internet.mgmt.mib-2.system.sysUptime.sysUptimeInstance = Timeticks:
<128425087> 14 days, 20:44:10.87
.iso.org.dod.internet.mgmt.mib-2.system.sysContact.0 = STRING:
.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = STRING: Core Switch 1
.iso.org.dod.internet.mgmt.mib-2.system.sysLocation.0 = STRING: BSW Serverraum
.iso.org.dod.internet.mgmt.mib-2.system.sysServices.0 = INTEGER: 2
.iso.org.dod.internet.mgmt.mib-2.system.sysORLastChange.0 = Timeticks: <0> 0:00:
00.00
.iso.org.dod.internet.mgmt.mib-2.system.sysORTable.sysOREntry.sysORID.1 = OID: .
iso.org.dod.internet.private.enterprises.89.73
.iso.org.dod.internet.mgmt.mib-2.system.sysORTable.sysOREntry.sysORDescr.1 = STR
ING: RS capabilities
.iso.org.dod.internet.mgmt.mib-2.system.sysORTable.sysOREntry.sysORUptime.1 = Ti
meticks: <0> 0:00:00.00
```

32

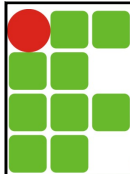




## Padrão de Gerenciamento na Internet Segurança e Administração

- O SNMPv3 pode ser imaginado como um SNMPv2 com capacidades adicionais de administração e segurança
- **Segurança baseada no usuário**
  - Utiliza o conceito de usuário, identificado por um nome, ao qual as informações de segurança (uma senha, um valor de chave ou acessos privilegiados) são associados
- O SNMPv3 fornece :
  - Criptografia
  - Autenticação
  - Proteção contra ataques de reprodução
  - Controle de acesso

33

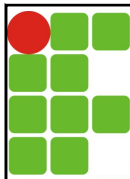


## Ferramentas de Gerenciamento

- Diversas opções open-source :

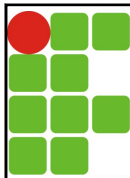


34



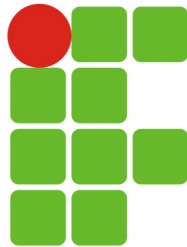
# Ferramentas de Gerenciamento

35



# Referências

- KUROSE, J. F. e ROSS, K. - Redes de Computadores e a Internet - 5a Ed., Pearson, 2010.
- Ferramentas de Gerenciamento
  - CACTI, <http://www.cacti.net> .
  - NAGIOS, <https://www.nagios.org> .
  - NAGVIS, <http://www.nagvis.org> .
  - ZABBIX, <http://www.zabbix.com> .
  - CENTREON, <https://www.centreon.com/en/> .
  - MRTG, <https://www.mrtg.com> .



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



# Redes de Computadores

## Gerenciamento de Redes

Prof. Thiago Dutra <[thiago.dutra@ifm.edu.br](mailto:thiago.dutra@ifm.edu.br)>