

Apresentação SNMP

- Introdução
- SNMP
- Fundamentos do protocolo SNMP
- MIBs e objetos
- Exemplos com comandos SNMP
- Laboratório
- Atividade extra

Intro

- Área de atuação agnóstica ao modelo/arquitetura
- Áreas de gestão de redes:
 - Desempenho
 - Falhas
 - Configuração
 - Contabilização
 - Segurança



Diversos protocolos: Common Management Information Protocol (CMIP) foi o protocolo a seguir a especificação OSI, contudo o Simple Network Management Protocol (SNMP) tornou-se o padrão de fato na Internet.

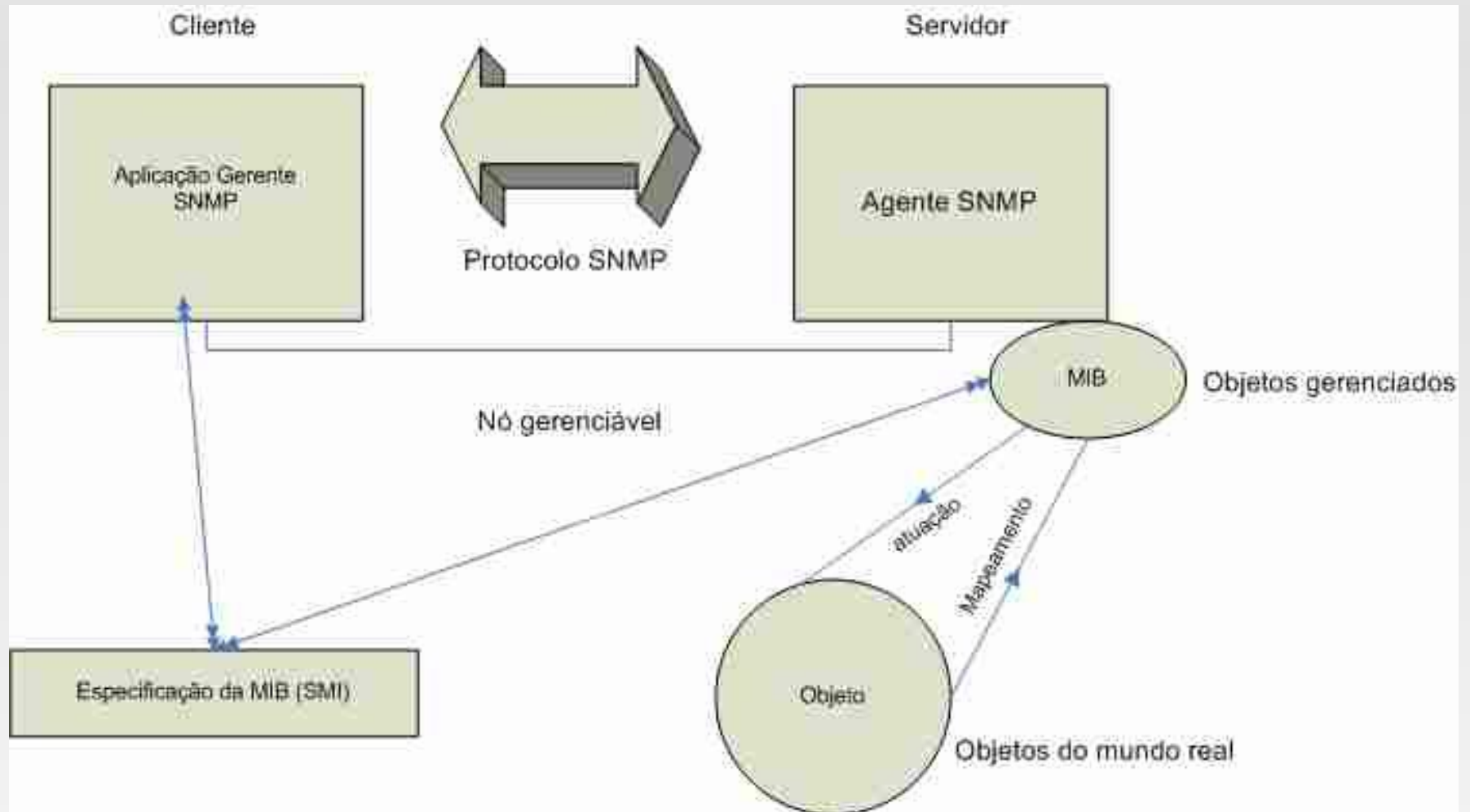
História

- Abstract Syntax Notation 1 (ASN.1) é usada para elaborar a linguagem Structure of Management Information (SMI) do SNMP.

Versões:

- SNMPv1 – RFC 1157 em 1990.
- SNMPv2 – RFC 1441-1452 em 1993.
- SNMPv2c – RFC 1901-1908 em 1996.
- SNMPv3 – RFC 1909-1910 em 1998.

Fundamentos SNMP



Fundamentos SNMP



- Protocolo roda sob UDP, portas 161, 162, 1061 e 1062.
- Versões SNMP definem diferentes *Protocol Data Units* (PDU). Dentre eles: GetRequest, SetRequest, Response, Trap, InformRequest, GetNextRequest, etc.
- Management Information Base (MIB) fica no agente e pode seguir as definições de RFC, ou serem personalizadas.
- Os tipos de objetos da MIB são escalares ou tabulares. Dados da SMI podem ser: Counter, Gauge, Timeticks, Integer, IPAddress, Integer, etc.

Data Type	v1 (RFC1155) STD16	v2 (RFC1442) Historic	v2 (RFC1902) (RFC2578) STD58	Access Restrictions	ASN.1 BER Tag	Note
INTEGER	yes (3.2.1.1)	yes	yes (7.1.1)		0x02	signed 32-bit integer. allows enumerations
Integer32	no	yes	yes (7.1.1)			signed 32-bit integer
OCTET STRING	yes (3.2.1.1)	yes	yes (7.1.2)		0x04	
BITS	no	no	yes (7.1.4)			
NULL	yes (3.2.1.1)	yes	yes		0x05	never has an associated value
OBJECT IDENTIFIER	yes (3.2.1.1)	yes	yes (7.1.3)		0x06	
IpAddress	yes (3.2.3.2)	yes	yes (7.1.5)		0x40	
Counter	yes (3.2.3.3)	no	allowed		0x41	non-negative, non- decreasing 32-bit values
Counter32	no	yes	yes (7.1.6)	not writeable		
Gauge	yes (3.2.3.4)	no	allowed		0x42	non-negative 32-bit values
Gauge32	no	yes	yes (7.1.7)			
Unsigned32	no	no	yes (7.1.11)			
TimeTicks	yes (3.2.3.5)	yes	yes (7.1.8)		0x43	non-negative, non- decreasing 32-bit values
Opaque	yes (3.2.3.6)	yes	deprecated, allowed (7.1.9)		0x44	only SMIv1 MIBS
NsapAddress	no	yes	no		0x45	Deprecated
Counter64	no	yes	yes (7.1.10)	not writeable	0x46	non-negative, non- decreasing 64-bit values
UInteger32	no	yes	no		0x47	Deprecated
BIT STRING	no	yes	no		?	Deprecated

Fundamentos

Versão	Segurança	Autenticação	Criptografia	PDU
1	community string	ausente	ausente	Get, Response GetNext, Set, Trap
2c	community string	ausente	ausente	Anteriores + GetBulk, Inform
3	USM/VACM	SHA/MD5	DES/AES	Todas anteriores

Objetos e MIBs

Objetos a serem monitorizados devem ter tipos especificados na SMI. Suas definições, em geral, seguem as MIBs de uso comum.

- MIB-I (RFC 1066 – 1988). Usado no SNMPv1. standardized
- MIB-II (RFC 1213 – 1991). MIB mais usada no SNMPv2.
- RMON MIB (RFC 1271 – 1993).
- Host Resources MIB (RFC 1514 – 1995). Padrão ISO
- MIB TCP e UDP (RFC 4022 e 4113).

MIBs e Objetos

Exemplos de um objeto escalar definido na MIB II

sysDescr OBJECT-TYPE

SYNTAX DisplayString (SIZE (0..255))

ACCESS read-only

STATUS mandatory

DESCRIPTION

"A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters."

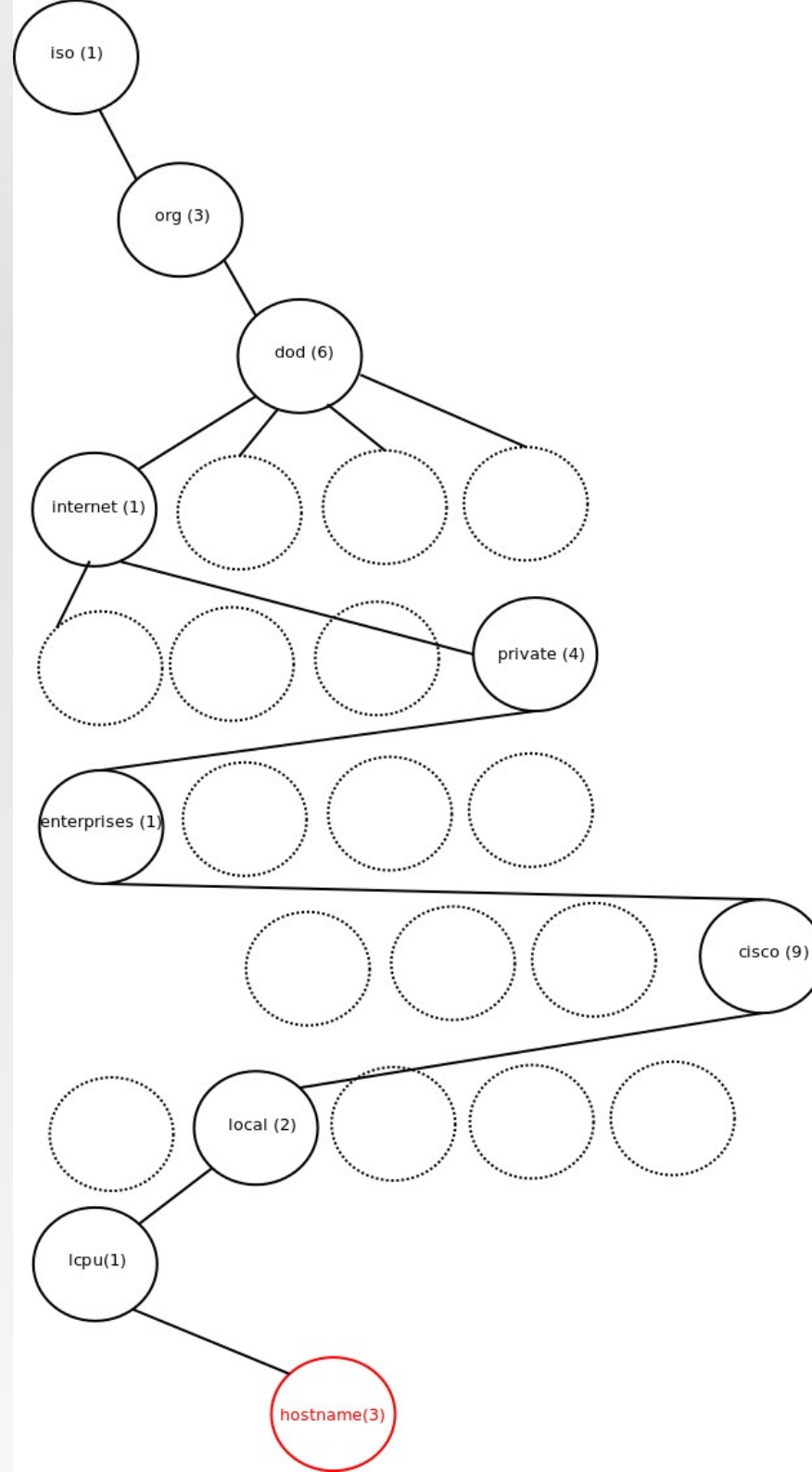
::= { system 1 }

Objetos e MIBs

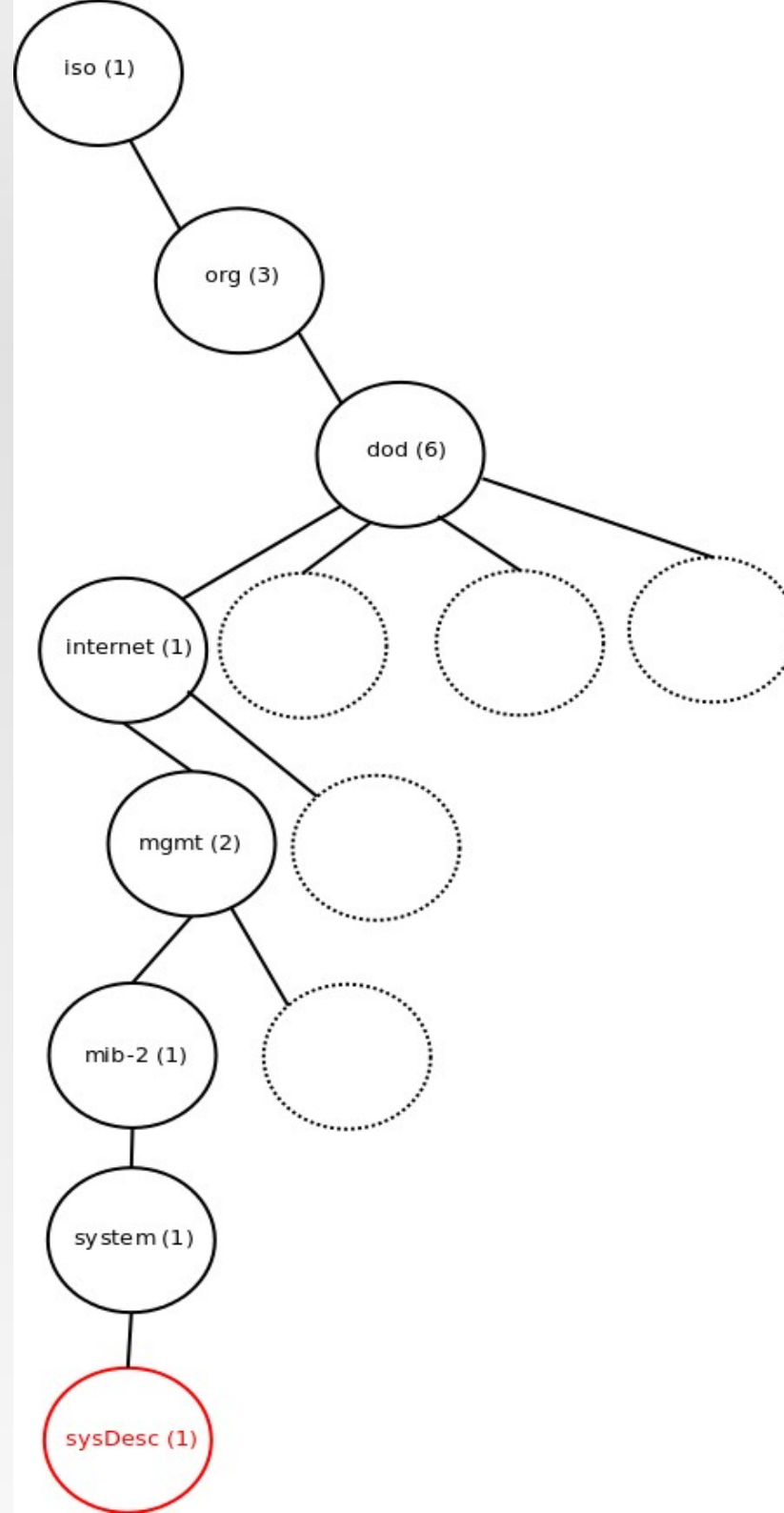
- Estrutura e identificação de objeto através de *Object Identifier* (OID).
- Conceito herdado da ASN.1, onde objetos são representados através de uma árvore hierárquica.



. iso (1) .
org (3) .
dod (6) .
internet (1) .
private (4) .
enterprises (1) .
cisco (9) .
local (2).
lcpu (1).
hostname (3)



.iso (1) .
org (3) .
dod (6) .
internet (1) .
mgmt (2).
mib-2 (1).
system (1).
sysDescr (1)



Objetos e MIBs

https://mibbrowser.online/mibdb_search.php



Exemplos com comandos SNMP

```
root@maki:~# snmpget -v1 -c bluves2013 172.20.10.5 iso.3.6.1.2.1.1.1.0
```

PDU	versão	string	ip do agente	objeto
-----	--------	--------	--------------	--------

iso.3.6.1.2.1.1.1.0 = STRING: "HP V1910-24G Switch Software Version 5.20 Release 1111P02 Copyright (c) 2004-2012 Hewlett-Packard Development Company, L.P."

Resposta SNMP

```
root@maki:~# snmpwalk -v1 -c bluves2013 172.20.10.5 1.3.6.1.2.1.1
```

PDU	versão	string	ip do agente	objeto
-----	--------	--------	--------------	--------

iso.3.6.1.2.1.1.1.0 = STRING: "HP V1910-24G Switch Software Version 5.20 Release 1111P02 Copyright (c) 2004-2012 Hewlett-Packard Development Company, L.P."

iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.25506.11.1.82

iso.3.6.1.2.1.1.3.0 = Timeticks: (992506283) 114 days, 20:57:42.83

iso.3.6.1.2.1.1.4.0 = STRING: "TI Senado Fedral"

iso.3.6.1.2.1.1.5.0 = STRING: "V1910-DILI-TR"

iso.3.6.1.2.1.1.6.0 = STRING: "Data Center Superior"

iso.3.6.1.2.1.1.7.0 = INTEGER: 78

Resposta SNMP

Exemplos com comandos SNMP

```
root@maki:~# snmpwalk -v1 -c bluves2013 172.20.10.5 1
```

PDU	versão	string	ip do agente	objeto
-----	--------	--------	--------------	--------

iso.2.840.10006.300.43.1.2.1.1.2.1 = INTEGER: 32768

iso.2.840.10006.300.43.1.2.1.1.2.2 = INTEGER: 32768

iso.2.840.10006.300.43.1.2.1.1.2.3 = INTEGER: 32768

iso.2.840.10006.300.43.1.2.1.1.2.4 = INTEGER: 32768

iso.2.840.10006.300.43.1.2.1.1.2.5 = INTEGER: 32768

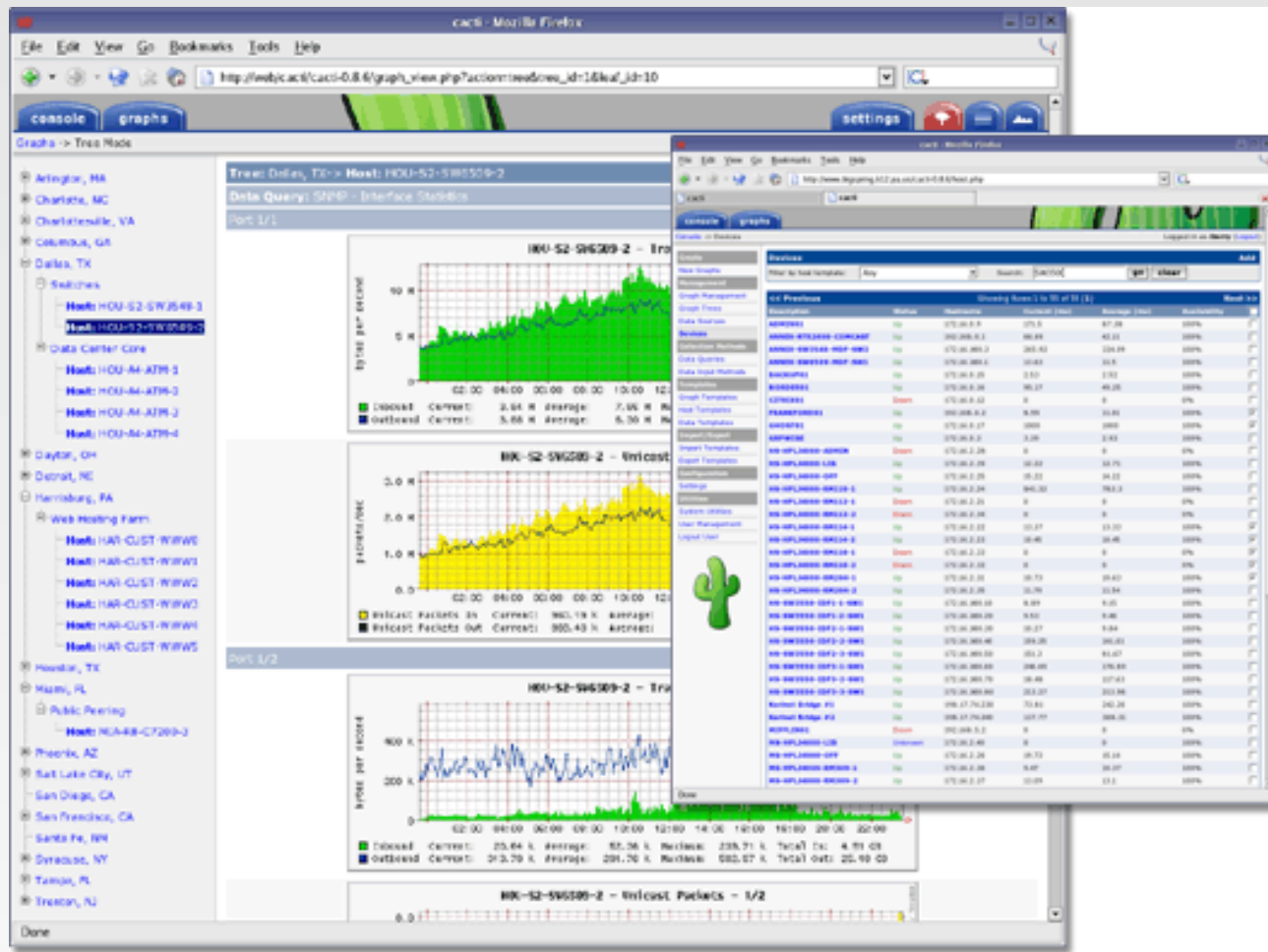
iso.2.840.10006.300.43.1.2.1.1.2.6 = INTEGER: 32768

iso.2.840.10006.300.43.1.2.1.1.2.7 = INTEGER: 32768

*Here's a clue that a network technician is in really bad physical shape...
He needs to rest after doing an SNMPwalk.*

Caso prático

- Sistemas de monitorização como Zabbix, Nagios, Cacti, MRTG, PRTG, etc.



Conclusões



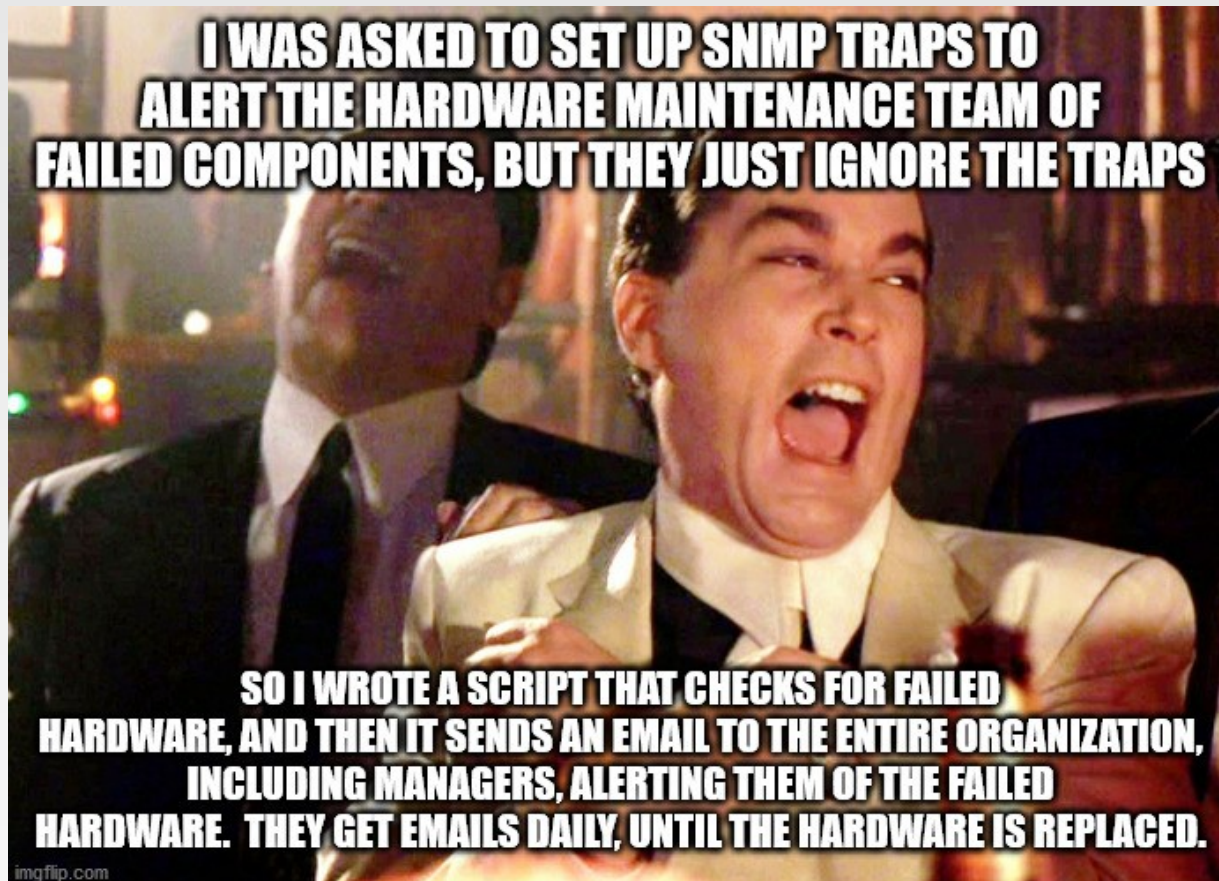
- SNMPv2c ainda é o mais usado, porém v3 deve substituí-lo.
- Outras soluções como NetConf-Yang começam a despontar como prováveis padrões para substituir SNMP.
- Restrito ao universo de redes, infraestrutura e telecomunicações, dado que outros modelos são mais adequados para monitorização de serviços e observability: OpenTelemetry, Prometheus, Datadog, etc.

Laboratório

- Instalar um agente SNMP no “server” do laboratório e configurar as community strings adequadamente.
- Instalar as MIBs no agente SNMP local.
- Realizar comandos para obter valores e escrever valores nos objetos.
- Instalar e utilizar o MRTG de tal sorte que consiga visualizar e monitorizar o tráfego da interface de rede.

Atividade extra

- Faça o exercício extra em <http://rzuolo.com/2025/grs/atividade-extra-10-SNMP.pdf>



The End

