

Gerência de Redes de Computadores

Graduação, Pós-Graduação Lato e Stricto Sensu
2021 / 2023

Mario Lemes Proença Jr.
DC/UEL

1

Referência do Autor

- **Mario Lemes Proença Jr.**
 - Universidade Estadual de Londrina
 - Departamento de Computação
 - E-mail : proenca@uel.br
 - Home page : <http://proenca.uel.br>
 - Telefone : 043-3371-4534 (UEL)

2

Objetivos do Curso

Aprender sobre Gerência de Redes de Computadores

- I) **Introdução a Gerência de Redes**
 - **Tendências**
- II) **Áreas funcionais**
- III) **Padrões de Gerência**
 - **Gerência do TCP/IP**
 - **SNMP**
 - **RMON**
 - **Gerenciamento de Fluxo**
- IV) **Ferramentas de Gerência**
- V) **Problemas no dia a dia de uma Rede**
- VI) **Network Operation Center (NOC)**
- VII) **Segurança em Redes**

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

3

3

I - INTRODUÇÃO

4

Introdução – Redes de Computadores

- As redes atualmente adquiriram uma importância tão grande para as empresas quanto os serviços de água, luz e telefonia.
- As redes se tornaram imprescindíveis para o funcionamento das empresas, elas devem ficar 24 horas em funcionamento.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

5

5

Introdução – Tendências de TIC

- Serviços integrados
 - voz e dados integrados na mesma rede
 - A divisão tradicional entre rede de dados (Internet) e rede de voz (PSTN) não existe mais !!!
 - Convergência !
 - Telefonia, celular (3G, 4G, 5G)
 - Tudo em uma única Rede !
 - Rede de Comunicação de Dados
 - ✓ TCP/IP
 - ✓ Ethernet
 - ✓ LTE2, WiMAX2, IEEE 802.11 ac, ax (wi-fi 4ª, 5ª, 6ª geração)
 - ✓ **Redes Híbridas ! Compartilhamento e otimização dos recursos.**

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

6

6

Introdução – Tendências de TIC

➤ Serviços integrados

- As companhias telefônicas são os principais provedores de Internet
- O mercado mundial de telecomunicações convergiu para integração total das duas áreas

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

7

7

Introdução – Tendências de TIC

➤ Serviços integrados

- As novas gerações de redes de telecomunicações que começam a serem instaladas possibilitam:
 - Novos serviços surgirem em um ritmo muito mais rápido do que estamos acostumados
 - VoIP
 - Stream Video
 - Video on Demand (VoD)
 - Telemedicina
 - HDTV, UHDTV (2012 ITU)
 - (3840x2160 4k) (7680x4320 8k)
 - IPTV
 - Jogos em Rede pela Internet
 - Muitos equipamentos estão surgindo em um curto espaço de tempo

Serviço	Banda requerida
Áudio MP3	32 – 320 Kbit/s
Videoconferência	128 a 384 kbit/s
DVD - MPEG2	5 Mbit/s
SD TV	5 Mbit/s
Full HD	10 Mbit/s
4k Ultra HD	15-30 Mbit/s
8K Ultra HD	60-100 Mbit/s

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

8

8

Introdução – Tendências de TIC

➤ Serviços integrados (triple play ou quad)

- Novos serviços surgirem em um ritmo muito mais rápido do que estamos acostumados
 - Chat agora não é só teclado é voz + vídeo + teclado
 - Acesso de casa + rápido (10, 15, 50, 100 Mbit/s ADSL, GPON) ADSL padrão antes era 320/160 640/320 Kbit/s)
 - Biometria sendo mais e mais utilizada
 - Face, mão, assinatura, dedo, iris, fala, odor, (**fingerprint**)
 - LTE2 e WiMAX2 (IEEE 802.16) 100 – 1 Gbit/s até 40 Km
 - Celular com bluetooth, Wi-Fi e WiMax utilizando agora o fixo para fazer ligações
 - E-mail para tudo = problema – muitas msg ... A pessoal manda e-mail para o colega que senta ao lado ou na frente.
 - Problemas mais comuns hoje e-mail: Phishing!
 - Internet das Coisas ! (Tudo conectado) 25-50 bilhões de dispositivos/2025.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

9

9

Introdução – Tendências de TIC

• Quais os investimentos

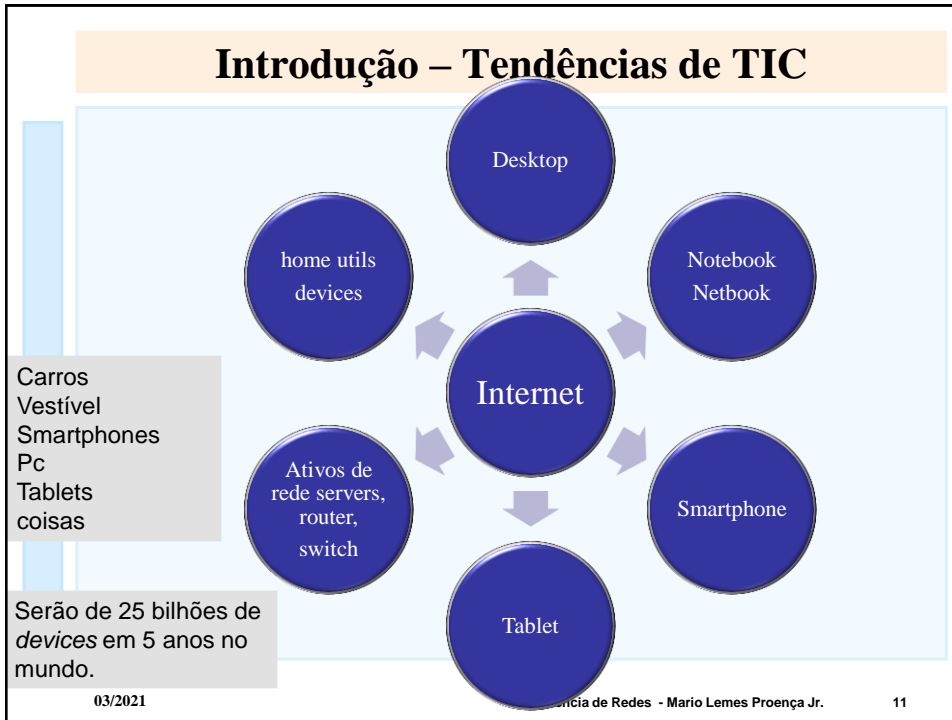
- CRM, ERP, Supply Chain,
- Software livre x proprietário,
- Business Intelligence,
- *Software as service*,
- Outsourcing / consultoria,
- Datacenter próprio ou terceirizado ?
- Web, e-mail,
- Segurança,
- Infraestrutura (PC, impressão, servidores, storage, backup)
- Soluções de comunicação, LAN, links, telefonia fixa e móvel,
- Help Desk / Service Desk,
- ? ? ?

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

10

10



11

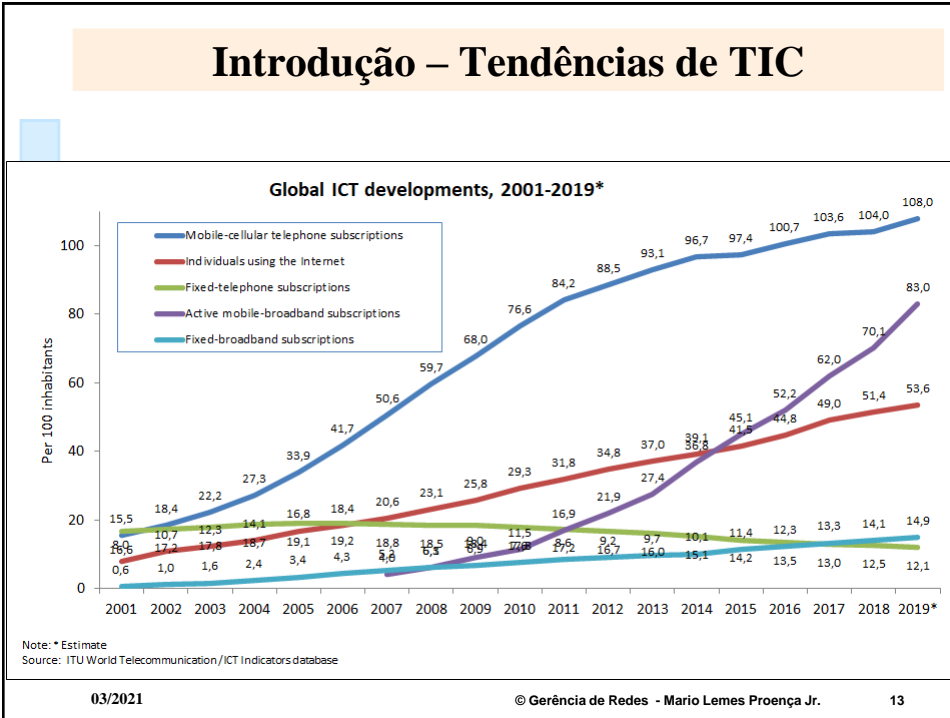
Introdução – Tendências de TIC

TOP 20 COUNTRIES WITH HIGHEST NUMBER OF Internet Users fonte <http://www.internetworldstats.com/top20.htm> 03/03/2021

#	Country or Region	Population, Internet Users		Population, Internet Users		
		2020 Est.	2020 Q1	2000 Est.	2000 Q4	
1	China	1.439.062.022	854.000.000	59%	1.283.198.970	22.500.000
2	India	1.368.737.513	560.000.000	41%	1.053.050.912	5.000.000
3	United States	331.002.651	313.322.868	95%	281.982.778	95.354.000
4	Indonesia	273.523.615	171.260.000	63%	211.540.429	2.000.000
5	Brazil	212.392.717	149.057.635	70%	175.287.587	5.000.000
6	Nigeria	206.139.589	126.078.999	61%	123.486.615	200.000
7	Japan	126.854.745	118.626.672	94%	127.533.934	47.080.000
8	Russia	145.934.462	116.353.942	80%	146.396.514	3.100.000
9	Bangladesh	164.689.383	94.199.000	57%	131.581.243	100.000
10	Mexico	132.328.035	88.000.000	67%	2.712.400	2.712.400
11	Germany	83.783.942	79.127.551	94%	81.487.757	24.000.000
12	Philippines	109.581.078	79.000.000	72%	77.991.569	2.000.000
13	Turkey	84.339.067	69.107.183	82%	63.240.121	2.000.000
14	Vietnam	98.168.833	71.540.000	73%	200.000	200.000
15	United Kingdom	67.886.011	63.544.106	94%	58.950.848	15.400.000
16	Iran	83.992.949	67.602.731	80%	66.131.854	250.000
17	France	65.273.511	60.421.689	93%	59.608.201	8.500.000
18	Thailand	69.799.978	57.000.000	82%	62.958.021	2.300.000
19	Italy	60.461.826	54.798.299	91%	57.293.721	13.200.000
20	Egypt	102.334.404	49.231.493	48%	69.905.988	450.000
TOP 20 Countries		5.233.377.837	3.241.273.512	62%	4.312.497.691	251.346.400
Rest of the World		2.563.237.873	1.332.876.622	52%	1.832.509.298	109.639.092
Total World		7.796.615.710	4.574.150.134	59%	6.145.006.989	360.985.492

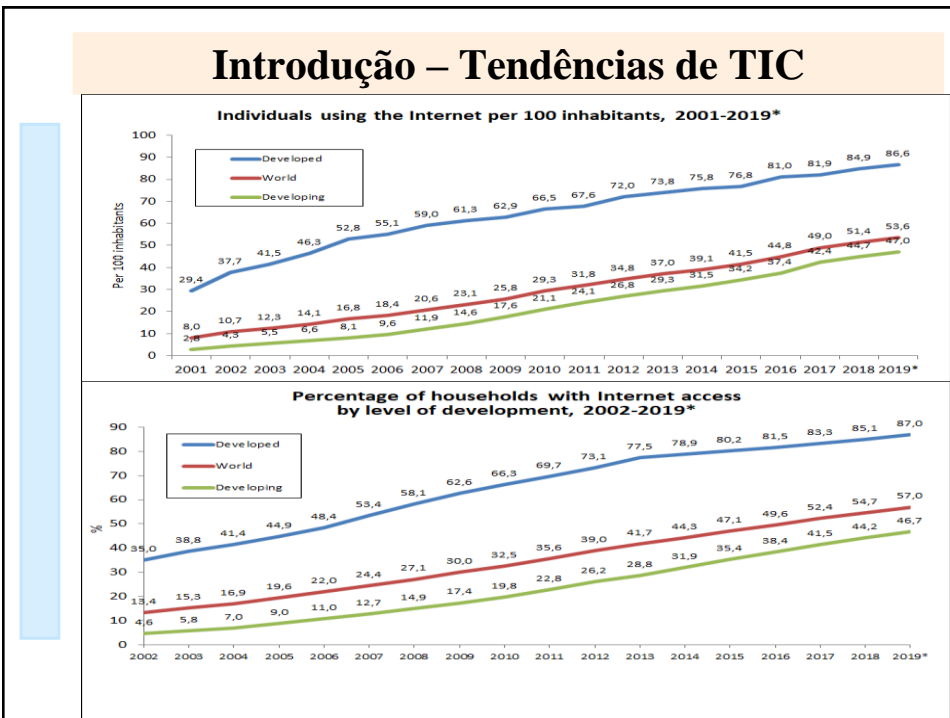
12

Introdução – Tendências de TIC



13

Introdução – Tendências de TIC



14

Introdução – Tendências de TIC

U.S. and Worldwide PC Market Growth <small>http://www.eforecasts.com (8/3/2015)</small>										
	1975	1980	1985	1990	1995	2000	2005	2010	2015	2020
U.S. PC Sales (#M)	0.04	0.76	6.6	9.5	21.4	46.0	62.0	83.8	122	140-150
U.S. PC Revenues (\$B)	0.05	1.5	17.2	24.5	56.8	86.9	90.5	84.0	93	95-100
U.S. PC Installed Base (#M)	0.04	1.4	19	51	86	177	234	296	392	450-470
Worldwide PC Sales (#M)	0.05	1.1	11	24.2	70.1	132	207	325	517	600-630
Worldwide PC Revenues (\$B)	0.06	3.6	29.5	71.3	155	251	301	321	383	400-420
Worldwide Installed Base (#M)	0.05	2.1	33	100	225	529	910	1,415	2,165	2,4 – 2,5

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

15

15

Introdução – Tendências de TIC

Internet Access Device Scenario: 2010 - <http://www.eforecasts.com>

USA	Worldwide
<ol style="list-style-type: none"> Over 250M Internet users Over 290M PCs in use Over 75% of office workers will use PCs at work Over 80% of households will have PCs There will be over 400M web devices in use Over 60% of workers will use web cell phones and web devices at home and at work 	<ol style="list-style-type: none"> Over 2B Internet users Over 1.4B PCs in use Over 45% of office workers will use PCs at work Nearly 25% of households will have PCs There will be over 2.5B web devices in use Over 20% of office workers will use web cell phones and web devices at home and at work

Internet Access Device Scenario: 2015 - <http://www.eforecasts.com>

USA	Worldwide
<ol style="list-style-type: none"> In 2015 there will be over 2858 Internet users In 2015 there will be over 336M PCs in use Over 80% of office workers use PCs Over 95% of households will have PCs There will be over 330M cell phones in use There will be 196M wireless Internet users 	<ol style="list-style-type: none"> In 2015 there will be over 2.8B Internet users In 2015 there will be over 1.95B PCs in use Over 65% of office workers use PCs Over 50% of households will have PCs There will be over 5.5B cell phones in use There will be 1.85B wireless Internet users

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

16

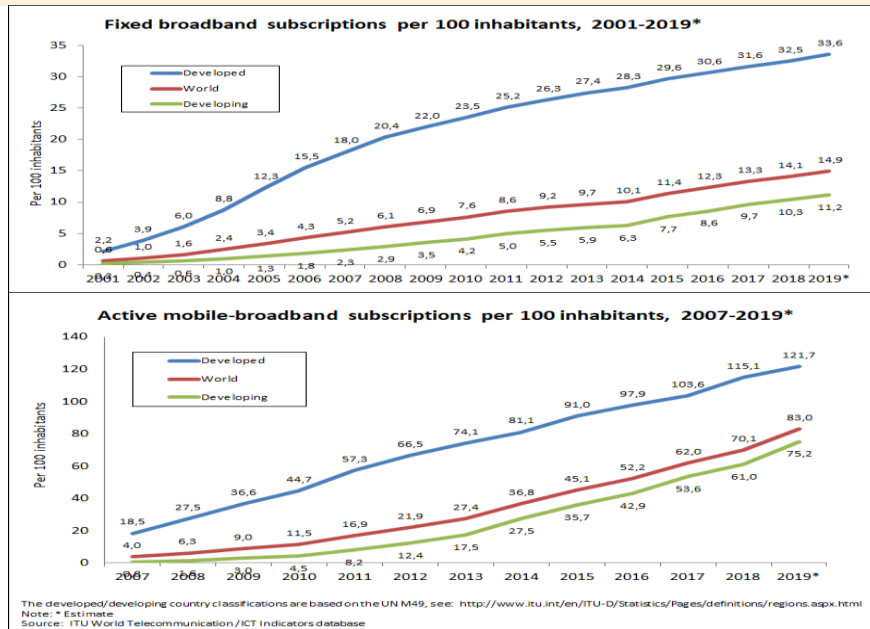
16

Introdução – Tendências de TIC

List of countries by number of broadband Internet subscriptions								
fonte wikipedia 03/03/2021								
Country or area	Fixed wired internet subscriptions				Mobile cellular subscriptions			
	Number[4]	Rank	%[5]	Rank	Number[6]	Rank	%[7]	Rank
China	378,540,000	1	26.86	43	1,474,097,000	1	104.58	105
United States	109,838,000	2	33.85	24	395,881,000	4	122.01	65
Japan	40,390,640	3	31.68	28	170,128,499	7	133.45	36
Germany	33,217,000	4	40.45	10	106,000,000	15	129.09	45
Russian Federation	30,872,788	5	21.44	54	227,341,873	6	157.89	12
Brazil	28,670,016	6	13.70	74	236,488,548	5	113.00	90
France	28,429,000	7	43.75	5	69,017,000	22	106.21	99
United Kingdom	26,015,818	8	39.31	13	79,173,658	20	119.63	74
South Korea	21,195,918	9	41.58	9	63,658,688	23	124.86	55
India	17,856,024	10	1.33	126	1,186,902,277	2	87.28	128
Mexico	17,131,820	11	13.26	75	114,326,842	14	88.51	126
Italy	16,586,376	12	27.94	39	83,871,543	19	141.29	26
Spain	14,473,888	13	31.22	30	52,484,655	28	113.22	89
Canada	13,922,504	14	38.01	15	31,458,600	43	85.90	131
Turkey	11,924,905	15	14.77	70	77,800,170	21	96.35	116
Viet Nam	11,269,936	16	11.80	81	120,016,181	12	125.62	53
Iran	10,057,769	17	12.39	79	87,106,508	18	107.32	96
Thailand	8,208,000	18	11.89	80	121,530,000	11	176.03	6
Australia	7,923,000	19	32.40	27	27,553,000	47	112.69	91
Argentina	7,870,222	20	17.78	64	61,897,379	26	139.81	28
Bangladesh	7,296,000	21	4.43	106	145,113,669	8	88.12	127
Netherlands	7,210,800	22	42.33	7	20,532,000	55	120.52	72
Poland	7,053,333	23	18.48	61	49,828,596	30	130.54	43
Colombia	6,318,936	24	12.88	76	62,222,011	25	126.81	49
Indonesia	6,044,712	25	2.29	121	458,923,202	3	173.84	7
Taiwan	5,713,568	26	24.18	49	28,777,408	44	121.80	67
Ukraine	5,239,743	27	12.55	78	55,714,733	27	133.49	35
Egypt	5,223,311	28	5.35	105	102,958,194	16	105.54	102
Romania	4,780,000	29	24.29	48	22,550,000	54	114.59	85
Belgium	4,378,973	30	38.31	14	11,961,089	74	104.65	104
Switzerland	3,850,000	31	45.42	3	11,292,000	78	133.22	37
Greece	3,778,263	32	33.86	23	12,937,106	70	115.93	84
Sweden	3,735,884	33	37.70	16	12,435,709	72	125.48	54

17

Introdução – Tendências de TIC



18

Introdução – Tendências de TIC

countries by number of mobile phones in use					
Rank	Country or regions	Number of mobile phones	Population	Connections/100 citizens	Date of evaluation
-	World	6,800,000,000+	7,012,000,000[1]	97	2013
1	China	1,276,660,000[4]	1,369,811,000[5]	93.2	October 2014[4]
2	India	970,955,980[6]	1,267,402,000[7]	77.58	31 December 2014
3	United States	327,577,529	317,874,628[9]	103.1	April 2014[10]
4	Brazil	278,480,000	201,032,714[11]	137.14	September 2014
5	Russia	256,116,000	142,905,200[11]	155.5	July 2013[13]
6	Indonesia	236,800,000	237,556,363	99.68	September 2013
7	Nigeria	167,371,945	177,155,754	94.5	Feb 2014[14]
8	Pakistan	140,000,000[15]	180,854,781[16]	77 ⁽¹⁷⁾ [18]	July 2014[19]
9	Japan	121,246,700	127,628,095	95.1	June 2013[20]
10	Bangladesh	121,860,000	157,497,000[21]	77.37	December 2014
11	Germany	107,000,000	81,882,342	130.1	2013[23]
12	Philippines	106,987,098	94,013,200	113.8	October 2013[24]
13	Iran	96,165,000	73,973,650	130	February 2013[25]
14	Mexico	101,339,000	112,322,757	90.2	Jul. 2013[26]
15	Italy	88,580,000	60,090,400	147.4	Dec. 2013[27]
16	United Kingdom	83,100,000	64,100,000	129.6	Q4 2013[28]
17	Vietnam	72,300,000	90,549,390	79	October 2013[29]
18	France	72,180,000	63,573,842	114.2	Dec. 2013[30]
19	Egypt	92,640,000	82,120,000	112.81	2013[31]
20	Thailand	69,000,000	65,001,021	105	2013[32]
21	Turkey	68,000,000	75,627,384	89.9	2013[33]
22	Ukraine	57,505,555	45,579,904	126.0	Dec. 2013[34]
23	South Korea	56,004,887	50,219,669	111.5	2014[35]
24	Spain	55,740,000	47,265,321	118.0	Feb. 2013[36]
25	Argentina	56,725,200	40,134,425	141.34	2013[37]

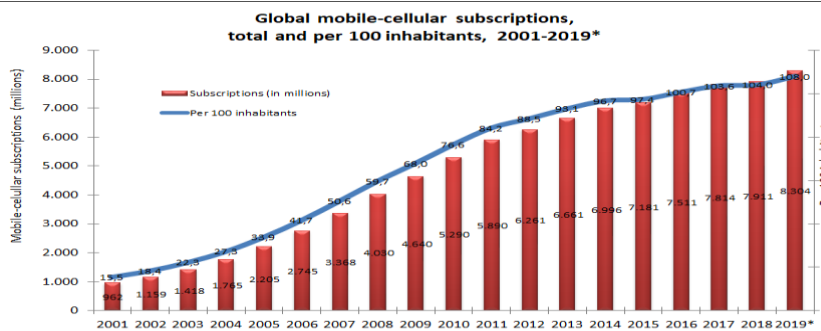
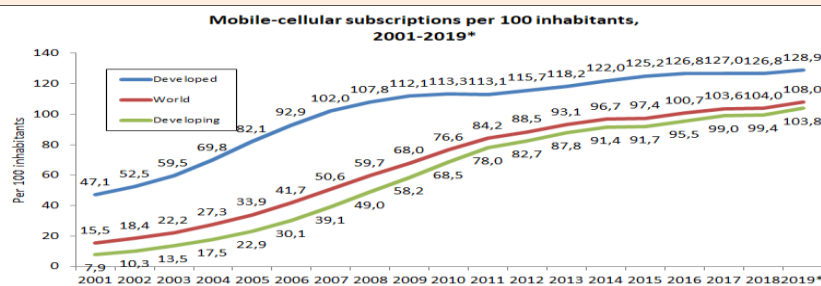
03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

19

19

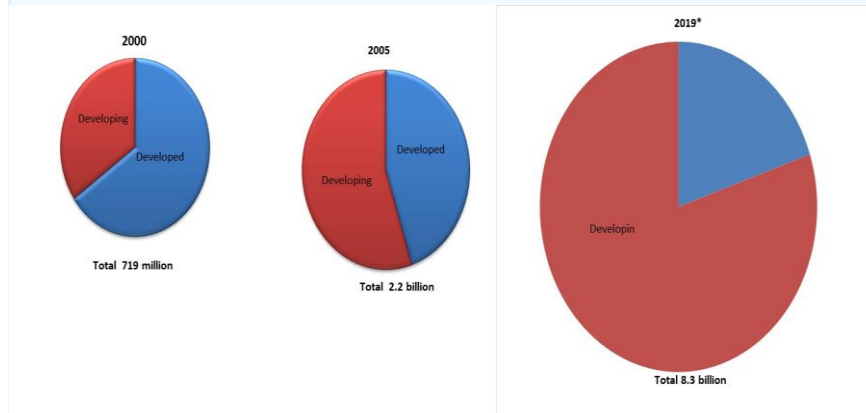
Introdução – Tendências de TIC



20

Introdução – Tendências de TIC

- **Celular Share world, by ITU Statistics** (<http://www.itu.int/ict/statistics>)
Mobile-cellular subscriptions, by level of development



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

21

21

Introdução – Tendências de TIC

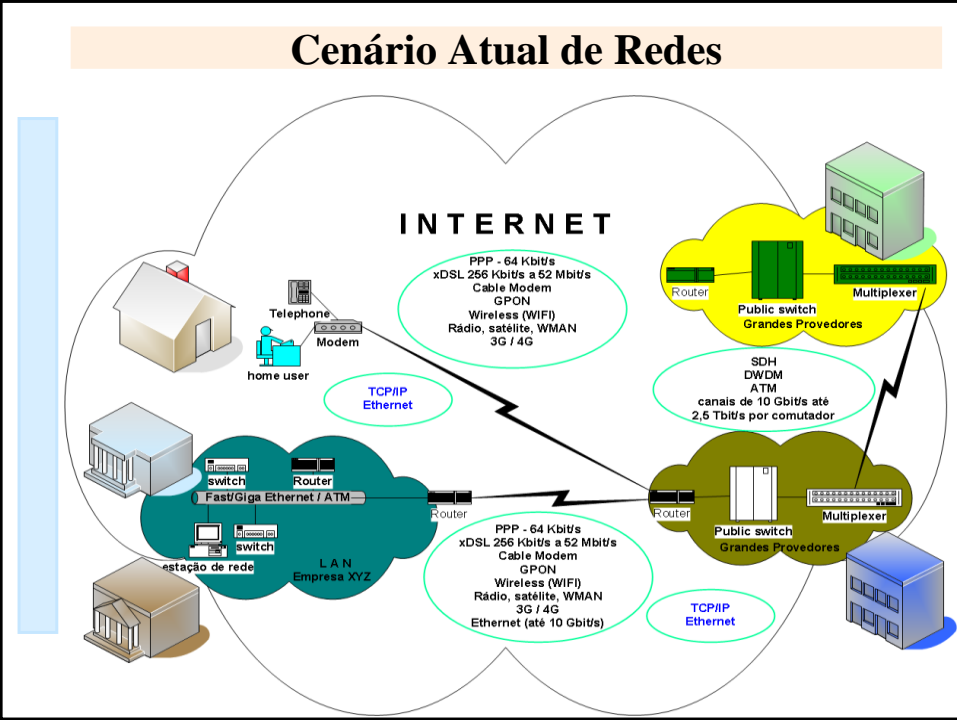
Gastos com E-Commerce		
Ano	Mundo	Brasil
1999	US\$ 55 Bilhões	
2004	US\$ 140 Bilhões	R\$ 1,75 Bilhão
2005	US\$ 169 Bilhões	R\$ 2,5 Bilhões
2006	US\$ 211 Bilhões	R\$ 4,4 Bilhões
2010	US\$ 680 Bilhões	R\$ 14,0 Bilhões
2011	US\$ 893 Bilhões	R\$ 20,0 Bilhões
2012	US\$ 1,0 Trilhões	R\$ 22,5 Bilhões
2013	US\$ 1,2 Trilhões	R\$ 31,0 Bilhões
2014	US\$ 1,5 Trilhões	R\$ 35,8 Bilhões
2015	US\$ 1,7 Trilhões	R\$ 41,3 Bilhões
2016	US\$ 1,85 Trilhões	R\$ 44 Bilhões
2017	US\$ 2,29 Trilhões	R\$ 47 Bilhões
2018	US\$ 2,8 Trilhões	R\$ 53,2 Bilhões
2019	US\$ 3,5 Trilhões	R\$ 75 Bilhões
2020	US\$ 4,2 Trilhões	R\$ 80 Bilhões

03/2021

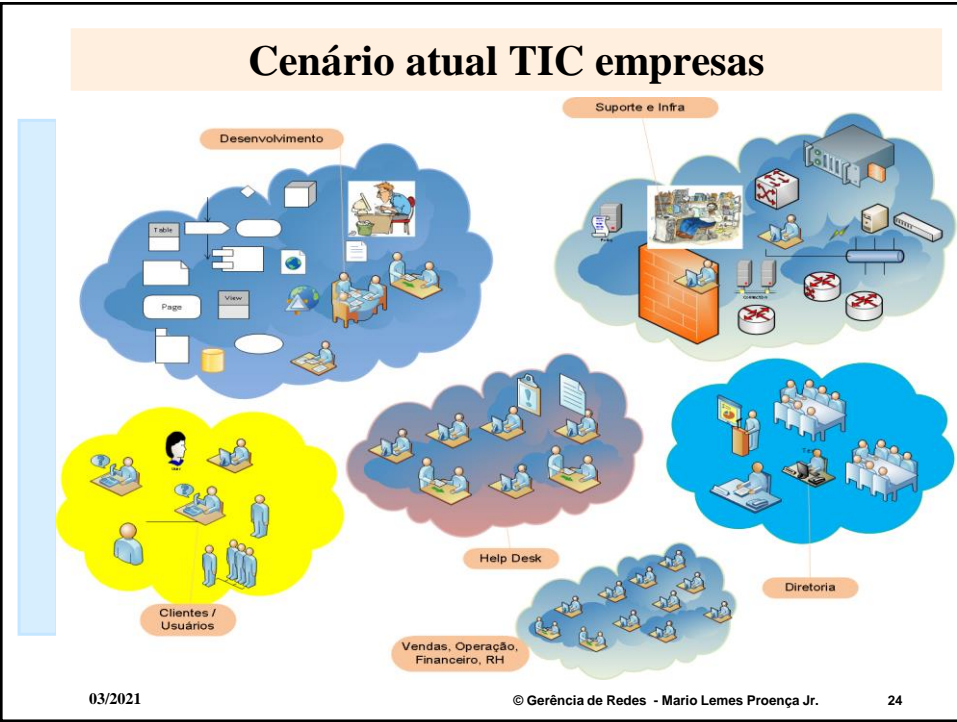
© Gerência de Redes - Mario Lemes Proença Jr.

22

22



23



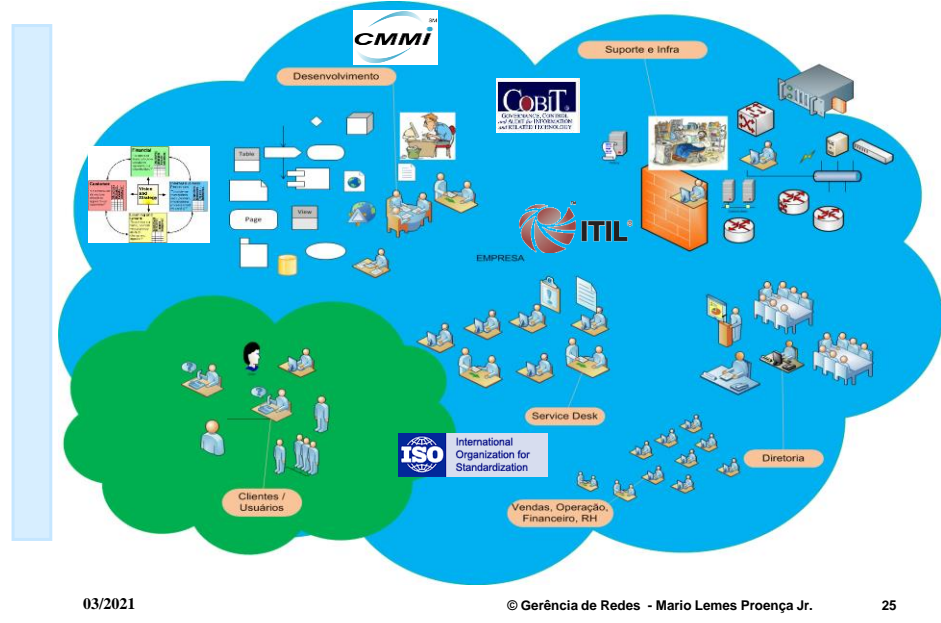
03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

24

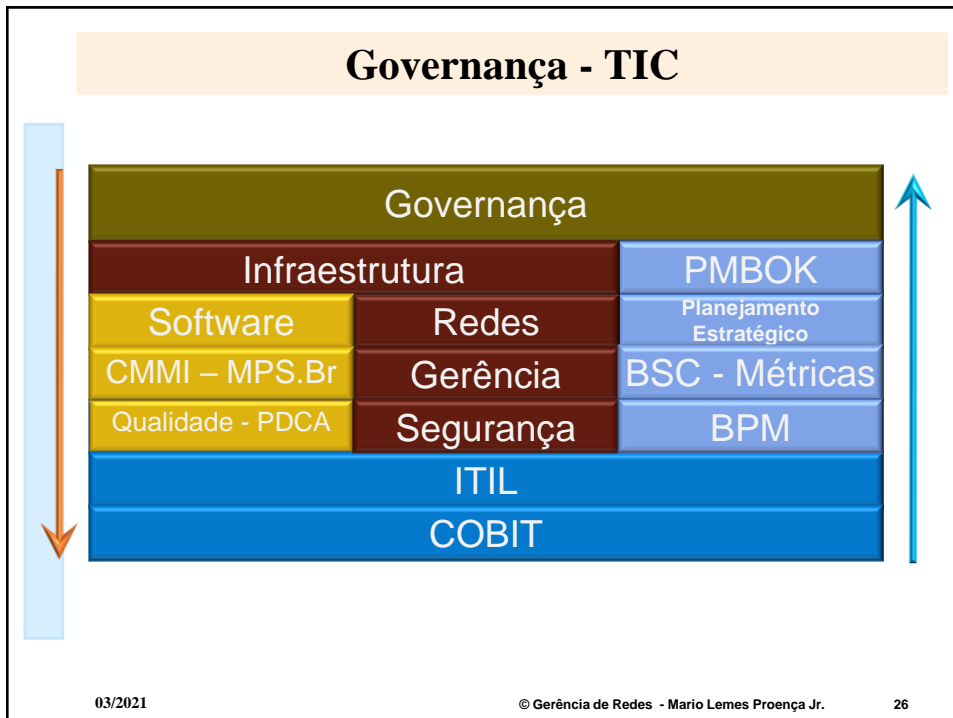
24

Cenário esperado para TIC empresas



25

Governança - TIC



26

Cenário Atual de Redes

	LANs	Teles
Aplicação		
Transporte	TCP / UDP	
Rede	IP	IP
Enlace	rádio (IEEE 802.11a,b,g,n) WinMAX / 802.16 x Ethernet (10/100/1G/10G) ATM (155/622) PPP (dial up) xDSL Frame Relay HDLC	rádio (IEEE 802.11a,b,g,n) WinMAX / 802.16 x / LTE Ethernet (10/100/1G/10G/ 40G) DWDM ATM SDH / PDH Frame Relay HDLC
Físico	Ethernet (10/100/1G/10G) ATM (155/622) PPP (dial up) xDSL radio (IEEE 802.11) Frame Relay HDLC	DWDM ATM SDH PDH

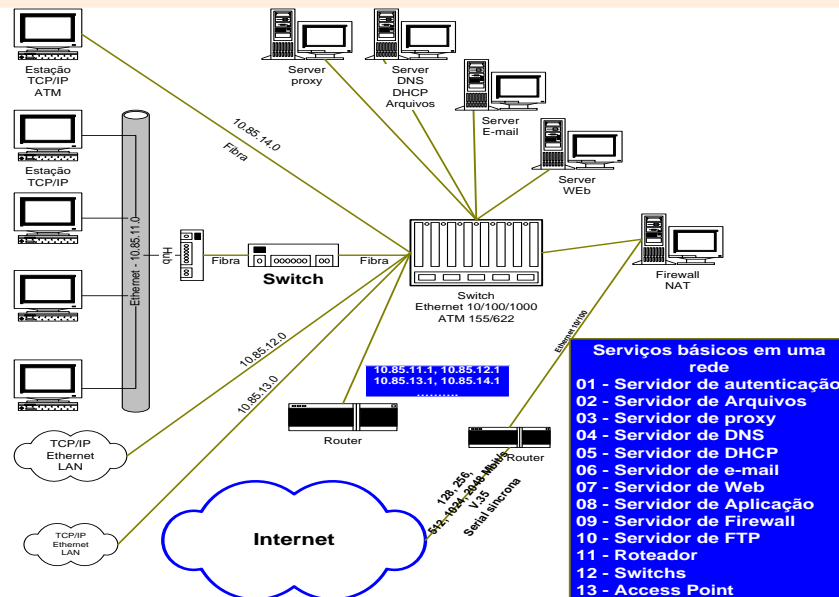
03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

27

27

Infraestrutura de Redes



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

28

28

Infraestrutura de Redes - Datacenter

✓ Datacenter

✓ É o local onde se concentra o principal da infraestrutura convergente ou hiperconvergente de TIC da empresa.

- ✓ Servidores
- ✓ Storages
- ✓ Switches de core, de borda
- ✓ Roteadores
- ✓ Firewall
- ✓ Aplicações
- ✓ Dados / Informação

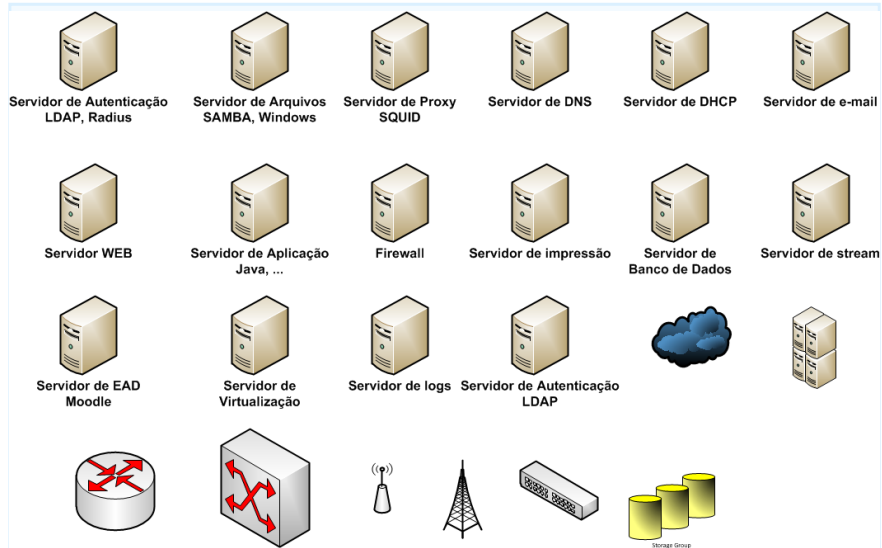
03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

29

29

Infraestrutura de Redes



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

30

30

Gerência de Redes

➤ GERENCIAMENTO DE REDES SERÁ UM DOS PONTOS PRINCIPAIS NESTE NOVO CONTEXTO

➤ A integração de dados, voz, redes de pacotes e redes de circuito não poderá ter sucesso sem que um efetivo gerenciamento seja realizado, visando:

- Garantir a qualidade
- Cobrança integrada
- Segurança

Gerência de Redes

➤ O que é Gerenciamento de Redes ?

➤ “Gerenciamento de rede inclui a disponibilização, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável”

T.Saydam & T. Magedanz, “*From Networks and Network Management into Service and Service Management*” 1996, *journal of Networks and system Management*

Gerência de Redes

➤ Gerenciamento de Redes

- ✓ Definir conjunto de objetos que devem ser gerenciados ?
 - ✓ *Quais seriam ?*
- ✓ Escolher modelo/framework/protocolo para gerenciamento?
 - ✓ *Qual utilizar ?*
- ✓ Para gerenciar a rede é necessário ter medições ?
 - ✓ *Quais ?*
- ✓ Escolher/criar ferramentas ?
 - ✓ *Quais ?*
- ✓ Estabelecer *baseline* ?
 - ✓ *O que seria ?*

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

33

33

Por que Gerenciar a Rede ?

- 1º Controlar o uso dos recursos
 - Quem esta fazendo o que e com o que e para que ?
- 2º Melhorar o uso dos recursos
 - Otimizar
- 3º Reduzir custos
 - Recursos são muito caros
- 4º Serviço essencial deve estar sempre disponível
 - Rede tão essencial quanto água, luz, telefone

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

34

34

Por que Gerenciar a Rede ?

- ✓ **Agregar Valor, Controlar e Gerenciar Risco são a essência da Governança de Tecnologia de Informação e Comunicação (TIC).**
- ✓ **Atualmente é fundamental medir, controlar, otimizar e demonstrar o resultado dos investimentos.**

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

35

35

Por que Gerenciar a Rede ?

- ✓ **Controlar significa verificar se as atividades desenvolvidas estão de acordo com o planejado.**
- ✓ **Incorporar e institucionalizar boas práticas para que a área de TIC da empresa possa suportar os objetivos de negócios.**
- ✓ **Proporciona para as empresas a obtenção de vantagens de suas informações com o objetivo de criar oportunidades e aumentando seu poder de competição.**

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

36

36

Por que Gerenciar a Rede ?

- A área de TI deve trabalhar de forma pró-ativa, seguir as políticas da organização e adotar procedimentos e práticas de forma rigorosa em seu funcionamento.
- Para isso é fundamental o comprometimento da organização e de todos envolvidos visando agregar valor ao seu negócio.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

37

37

Service Level Agreement (SLA)

- *Service Level Agreement (SLA)*
 - Acordo de nível de serviço estabelece os parâmetros mínimos aceitáveis de qualidade do serviço prestado entre duas partes;
 - Por exemplo entregas ou performance mínima aceitável;
 - Tempo mínimo para recuperação de falhas;
 - Tempo médio entre falhas;
 - Disponibilidade
 - Integridade
 - Resiliência
 - O acordo deve prever todos os parâmetros requeridos pelo serviço para ambas as partes cumprirem.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

38

38

Service Level Agreement (SLA)

- **Service Level Agreement (SLA)**
 - Acordo de nível de serviço deve estabelecer principalmente parâmetros mínimos referente ao funcionamento do serviço:
 - Qual o % de tempo funcionando é aceitável para você ?
 - 90 % é bom ?
 - 99 % é ótimo ?

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

39

39

Service Level Agreement (SLA)

- Quanto tempo pode ficar fora do ar o seu serviço de TIC ?
- Qual é a disponibilidade mínima aceitável para você do serviço funcionando?

✓ 90	%
✓ 95	%
✓ 99	%
✓ 99,9	%

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

40

40

Service Level Agreement (SLA)

- Quanto tempo o serviço pode ficar fora do ar ?

% disponibilidade x não disponibilidade		
horas em um ano	8.760	
minutos em um ano	525.600	% disponível
minutos disponível no ano	0	0
minutos fora do ar / ano	525.600,00	
em horas	8.760	60
em dias	365	

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

41

41

Service Level Agreement (SLA)

- Quanto tempo o serviço pode ficar fora do ar ?

% disponibilidade x não disponibilidade		
horas em um ano	8.760	
minutos em um ano	525.600	% disponível
minutos disponível no ano	473.040	90
minutos fora do ar / ano	52.560,00	
em horas	876	60
em dias	36,5	

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

42

42

Service Level Agreement (SLA)

- Quanto tempo o serviço pode ficar fora do ar ?

% disponibilidade x não disponibilidade		
horas em um ano	8.760	
minutos em um ano	525.600	% disponível
minutos disponível no ano	499.320	95
minutos for a do ar / ano	26.280,00	
em horas	438	60
em dias	18,25	

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

43

43

Service Level Agreement (SLA)

- Quanto tempo o serviço pode ficar fora do ar ?

% disponibilidade x não disponibilidade		
horas em um ano	8.760	
minutos em um ano	525.600	% disponível
minutos disponível no ano	520.344	99
minutos for a do ar / ano	5.256,00	
em horas	87,6	60
em dias	3,65	

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

44

44

Service Level Agreement (SLA)

- Quanto tempo o serviço pode ficar fora do ar ?

% disponibilidade x não disponibilidade		
horas em um ano	8.760	
minutos em um ano	525.600	% disponível
minutos disponível no ano	525.074,4	99,9
minutos for a do ar / ano	525,60	
em horas	8,76	60
em dias	0,365	

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

45

45

Service Level Agreement (SLA)

- Quanto tempo pode ficar fora do ar o seu serviço de TIC ?
- Qual Seria a disponibilidade mínima aceitável para você do serviço funcionando?

✓90 %
✓95 %
✓99 %
✓99,9 %
✓99,999 %
✓99,9999 %

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

46

46

Service Level Agreement (SLA)

- Quanto tempo o serviço pode ficar fora do ar ?

% disponibilidade x não disponibilidade		
horas em um ano	8.760	
minutos em um ano	525.600	% disponível
minutos disponível no ano	525.547,44	99,99
minutos for a do ar / ano	52,56	
em horas	0,876	60
em dias	0,0365	

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

47

47

Service Level Agreement (SLA)

- Quanto tempo o serviço pode ficar fora do ar ?

% disponibilidade x não disponibilidade		
horas em um ano	8.760	
minutos em um ano	525.600	% disponível
minutos disponível no ano	525.594,74	99,999
minutos for a do ar / ano	5,26	
em horas	0,0876	60
em dias	0,00365	

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

48

48

II – ÁREAS FUNCIONAIS

49

ÁREAS FUNCIONAIS

➤ A Sigla FCAPS sintetiza bem as cinco áreas que a Gerência de redes abrange:

- 1.Fault (falhas),***
- 2.Configuration (Configuração),***
- 3.Accounting (Contabilização),***
- 4.Performance (Performance),***
- 5.Security (Segurança).***

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

50

50

ÁREAS FUNCIONAIS

➤ Visão atual da Gerência de Redes. TIC x Negócio:

✓ **A ATI deve ser parceira e não fornecedora**

ÁREAS FUNCIONAIS – Falhas

- Pode ser representado pelo **conjunto de operações responsáveis para localizar, isolar e corrigir se possível problemas ou falhas na rede.**
- Através do Gerenciamento de falhas o gerente de rede pode de forma **pró-ativa** e/ou **reativa** identificar rapidamente uma falha e iniciar imediatamente o processo de solução.
- Para o Gerenciamento de falhas é necessário manter e examinar continuamente os *logs* da rede, usando se possível ferramentas adequadas, que podem ir de um simples *sniffer* a sofisticados sistemas de Gerenciamento.
- Para o Gerenciamento de falhas tem-se as seguintes opções básicas:
 - 1ª coleta de dados sobre o problema
 - 2ª identificar segmento onde esta o problema

ÁREAS FUNCIONAIS – Falhas

- Funções importantes que devem ser observadas pelo gerente no tocante a falhas:
 - Ter pronto um *checklist* sobre o que deve ser verificado
 - Ter pronto **plano de contingência** para
 - Servidores
 - *Switches*
 - Roteadores
 - Backup
 - Documentação da rede

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

53

53

ÁREAS FUNCIONAIS – Falhas

- **Falhas comuns – Hardware**
 - Placa de rede
 - Cabos
 - Conectores
 - *Hubs*
 - *Switches*
 - *Tranceivers*
 - Conversor de mídia
 - Servidores
 - Roteadores
 - ??? O que mais ???

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

54

54

ÁREAS FUNCIONAIS – Falhas

- **Falhas comuns – Software**
 - Configurações erradas de rede
 - Vírus
 - DNS out
 - DHCP out
 - Firewall
 - Servidor Web
 - Servidor de e-mail
 - Servidor de contas
 - Servidor de arquivos
 - Servidor de impressão
 - ??? O que mais ???

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

55

55

ÁREAS FUNCIONAIS – Configuração

- Se caracteriza pelo **conjunto de operações necessárias para a inicialização, término, alteração e armazenamento da configuração dos equipamentos da rede.**
- Como benefício do gerenciamento de configuração tem-se: fácil alteração na configuração dos equipamentos, fácil acesso a documentação sobre a configuração dos equipamentos, manutenção de um inventário atualizado.
- Para o gerenciamento de configuração tem-se as seguintes opções básicas:
 - 1ª coleta de dados da rede
 - 2ª inicializar e alterar a configuração de equipamentos
 - 3ª manter banco de dados sobre configuração de equipamentos da rede

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

56

56

ÁREAS FUNCIONAIS – Configuração

- **Funções importantes que devem ser observadas pelo gerente:**
 - Documentação das configurações realizadas
 - Ter sempre duas pessoas que realizem o mesmo trabalho
 - **REFÉM de um profissional**
 - Documentação da rede é fundamental

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

57

57

ÁREAS FUNCIONAIS – Configuração

- **Problemas comuns relacionados a configuração**
 - Configurações erradas acarretam em falhas
 - Padronização nas configurações
 - Se possível equipamentos iguais e do mesmo fabricante
 - *Upgrades*
 - As pessoas insistem em não fazer, [exemplo \(26/04/2012\)](#)
 - Casa de ferreiro espeto é de pau!
 - ???

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

58

58

ÁREAS FUNCIONAIS – Contabilização

- **Gerenciamento de Contabilização (Accounting)** : Esta área é responsável por fazer **medições na rede visando estabelecer parâmetros quanto a utilização da rede**, para se necessário determinar cotas grupos e usuários procurando uma melhor distribuição dos recursos da rede.
- Dentre os muitos recursos que podem ser Gerenciados tem-se: espaço em disco, tempo de conexão, quantidade de conexões, tempo de processamento, utilização da banda.
- Para o gerenciamento de contabilização deve-se fazer 3 operações básicas:
 - 1ª coletar dados da rede;
 - 2ª Analisar os dados coletados;
 - 3ª contabilizar por usuários.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

59

59

ÁREAS FUNCIONAIS – Contabilização

- **Funções importantes que devem ser observadas pelo gerente:**
 - Manter ativos os *logs* das principais aplicações
 - Servidor de contas
 - **Lightweight Directory Access Protocol (LDAP) RFC 4510**
 - Servidor de e-mail
 - Servidor proxy
 - squid
 - Firewall
 - iptables
 - Backup

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

60

60

ÁREAS FUNCIONAIS – Contabilização

➤ Problemas comuns relacionados a contabilização

- Falta de informação auxiliar no gerenciamento da rede
 - espaço em disco,
 - tempo de conexão,
 - quantidade de conexões,
 - tempo de processamento,
 - utilização da banda
 - uso indevido dos recursos
 - Navegação
 - E-mail

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

61

61

ÁREAS FUNCIONAIS – Performance

- **Gerenciamento de Desempenho (*Performance*)** : É o conjunto de funções necessárias para o gerente de rede monitorar e analisar as atividades na rede, fazendo os devidos ajustes necessários.
- A prevenção de congestionamentos na redes e a necessidade de prever o crescimento da rede são benefícios oferecidos por esta atividade do gerenciamento.
- Para esta tarefa é necessário a coleta de dados na rede, de forma aleatória, respeitando regras estatísticas que possibilitarão avaliar a situação da rede.
 - *Baseline*
 - Gargalos
 - Padrão do trafego
 - Monitoramento constante
 - Imprescindível software

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

62

62

ÁREAS FUNCIONAIS – Performance

- Funções importantes que devem ser observadas pelo gerente:
 - Manter em funcionamento aplicativos de monitoramento dos segmentos da rede
 - Construir um *baseline* da rede
 - Perfil sobre comportamento da rede
 - Limiares mínimos e máximos sobre utilização

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

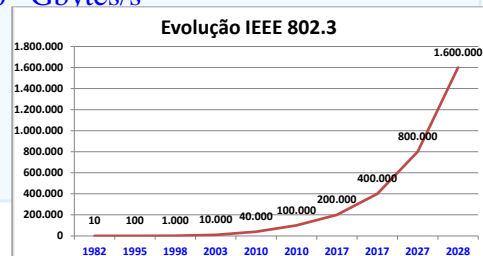
63

63

ÁREAS FUNCIONAIS – Performance

- Funções importantes que devem ser observadas pelo gerente
 - 10 Mbit/s = 1,25 MByte/s
 - 100 Mbit/s = 12,5 MByte/s
 - 1 Gbit/s = 125,0 MByte/s
 - 10 Gbit/s = 1,25 Gbyte/s
 - 40 Gbit/s !!! = 5 Gbytes/s
 - 100 Gbit/s !!! = 12,5 Gbytes/s
 - 400 Gbit/s !!! = 50,0 Gbytes/s
 - 800 Gbit/s
 - 1,6 Terabit/s

03/2021



64

ÁREAS FUNCIONAIS – Performance

- Funções importantes que devem ser observadas pelo gerente:
 - Manter servidores atualizados ao seu contexto
 - Processadores (Xeon, Risc)
 - Memória

	velocidade	Frequência	Ano
DDR	400 Mbit/s	100, 200 MHz	1998
DDR 2	667 Mbit/s	533, 667 MHz	2005
DDR 3	17 Gbit/s	800, 1.066, 1.333, 1600 1.866, 2.133 MHz	2007
DDR 4	25,6 Gbit/s	2.133, 2.400, 2.666, 3200 MHz	2014
DDR 5	??	??	??

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

65

65

ÁREAS FUNCIONAIS – Performance

- Funções importantes que devem ser observadas pelo gerente:
 - Discos
 - SCSI-3 (15 K) Ultra 160 Ultra 320 (320 Mbytes/s)
 - SAS-1 – Serial Attached SCSI (3Gbit/s)
 - SAS-2 (6 Gbit/s),
 - SAS-3 (12 Gbit/s 2013)
 - SAS-4 (22,5 Gbit/s, 2017)
 - SAS-5 (45 Gbit/s ...)
 - (servidores de disco – alta performance - Storage)
 - ✓ Storage Area Network (SAN)
 - ✓ Network Attached Storage (NAS)

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

66

66

ÁREAS FUNCIONAIS – Performance

- Funções importantes que devem ser observadas pelo gerente:

- Barramento

- PCI – 32 bits e 64 bits

Versões	1 lane	16 lanes	Ano
PCIe 1.0	250 Mbit/s	4 Gbit/s	2003
PCIe 2.0	500 Mbit/s	8 Gbit/s	2007
PCIe 3.0	1 Gbit/s	16 Gbit/s	2010
PCIe 4.0	2 Gbit/s	32 Gbit/s	2017
PCIe 5.0	4 Gbit/s	64 Gbit/s	2019
<i>PCIe 6.0</i>	<i>8 Gbit/s</i>	<i>128 Gbit/s</i>	<i>2021/2022</i>

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

67

67

ÁREAS FUNCIONAIS – Performance

- Interfaces: **USB**

tipo	velocidade	conector	power	ano
USB 1.1	12 Mbit/s		2,5V, 500mA	1996
USB 2.0	480 Mbit/s		2.5V, 1,8A	2001
USB 3.0	5 Gbit/s		5V, 1,8A	2011
USB 3.1	10 Gbit/s		20V, 5A	2014
USB 3.2	20 Gbit/s	Type C	20V, 5A	2017
USB 4.0	40 Bbit/s	Type C	20V, 5A	2019

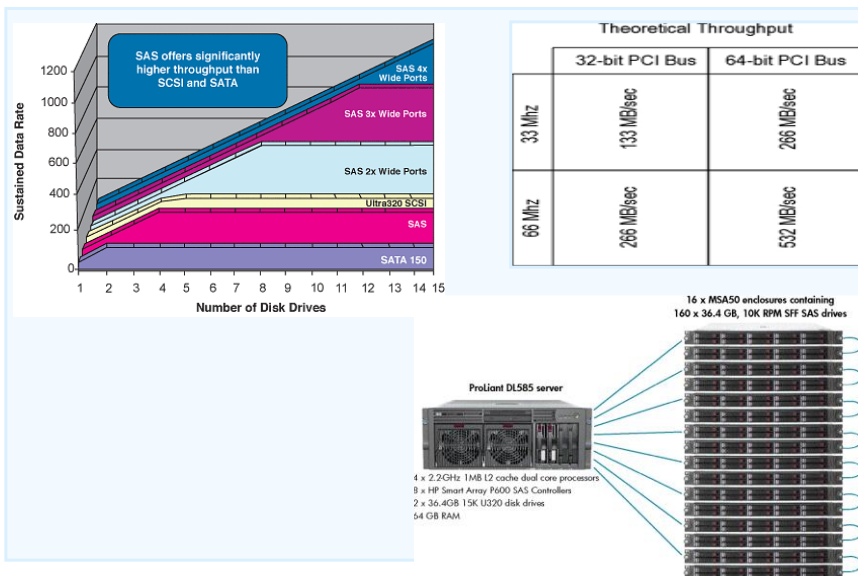
03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

68

68

ÁREAS FUNCIONAIS – Performance



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

69

69

ÁREAS FUNCIONAIS – Performance

- Solid-State Drive (SSD)
 - Baixo consumo, peso, dimensão.
 - Alta velocidade:
 - ✓ 400 – 700 Mbytes/s



✓ 2013 foram obtidas velocidade de 7 Gbytes/s com PCIe 3.0



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

70

70

ÁREAS FUNCIONAIS – Performance

➤ Problemas Comuns

- Tempo de resposta das aplicações muito longo
- Sistemas que demandam muito processamento
- Demora na realização dos serviços:
 - Acesso a Web
 - Recebimento ou envio de um e-mail

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

71

71

ÁREAS FUNCIONAIS – Segurança

- **Gerenciamento de Segurança (*Security*)** : É o conjunto de funções que o gerente de rede deve executar, para identificar e proteger equipamentos e dados da rede, de ataques e violações oriundas de pessoas não autorizadas (*hackers, crackers*).
- Para isto deve-se limitar o acesso a *hosts*, contas de usuários e base de dados com ferramentas adequadas como *firewall, proxy* e outros softwares de segurança.
- Os principais procedimentos que devem ser executados para o gerenciamento de segurança são:
 - 1º identificar informações e equipamentos que devem ser protegidos.
 - 2º encontrar possíveis pontos de acesso a rede e protegê-los.
 - 3º manter a rede protegida.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

72

72

ÁREAS FUNCIONAIS – Segurança

- **Funções importantes que devem ser observadas pelo gerente:**
 - Implementar / instalar ferramentas para auxílio no monitoramento da rede
 - Análise diária dos logs dos servidores
 - Firewall
 - Contas
 - **Ter um sistema de backup implementado e funcionando!**
 - Quando o backup é realmente um backup ?
 - Software
 - Hardware
 - Fitas DAT / DLT / LTO (até 18 TBytes aproximadamente 1,4 Tbyte/hora (400*60*60) ou 400 Mbytes/s)
 - LTO-8 drive, R\$ 40.000,00 e R\$ 1.100,00 a fita, LTO-8
 - Cópia em disco
 - DVD-RW (4,7 GByte +- 25 m)

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

73

73

ÁREAS FUNCIONAIS – Segurança

- **Fitas para backup**
 - padrão Linear Tape-Open (LTO) chamadas de Ultrium

Atributo	LTO-1	LTO-2	LTO-3	LTO-4	LTO-5	LTO-6	LTO-7	LTO-8	LTO-9	LTO-10	LTO-11	LTO-12
Release Date	2000	2003	2005	2007	2010	2012	2015	2017	2020	?	?	?
Native Data Capacity	100 GB	200 GB	400 GB	800 GB	1.5 TB	2.5 TB	6.0 TB	12 TB	18 TB	36 TB	72 TB	144
Max Speed (MB/s)	15	40	80	120	140	160	300	360	400	1.100	?	?

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

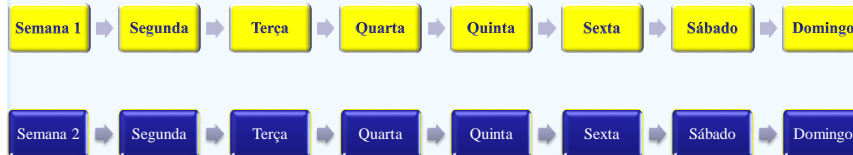
74

74

ÁREAS FUNCIONAIS – Segurança

➤ Backup

- Estabelecer uma política de backup para os serviços de rede.
- Frequência e o que deve ser copiado
 - Diários 7x4 (7 dias da semana / 4 semanas no mês) totalizando 28 fitas no mês
 - Retenção de uma fita a cada início de mês, totalizando 12 fitas por ano
 - Necessidade de no mínimo 40 fitas.



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

75

75

ÁREAS FUNCIONAIS – Segurança

➤ Problemas comuns

- Ataques
- Vírus
- Perdas de dados
- Perda de Servidores ou estações
- Indisponibilidade de algum serviço

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

76

76

ÁREAS FUNCIONAIS – Documentação

- **É fundamental para o gerenciamento de redes**
 - Assim como para o desenvolvimento de software !
- **A ausência de documentação gera inúmeros problemas**
 - Perda de tempo (precioso) na resolução de problemas, geralmente simples com ajuda de uma documentação adequada
 - Perde-se a visão do todo, a medida que a rede cresce

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

77

77

ÁREAS FUNCIONAIS – Documentação

- Deve-se produzir uma documentação sobre
 - Cabeamento de pares metálicos
 - Cabeamento de fibras
 - Mapas dos pontos
 - Verificar arquivo [mapas-rede.pdf](#)
 - Verificar arquivo [DC Switches](#)

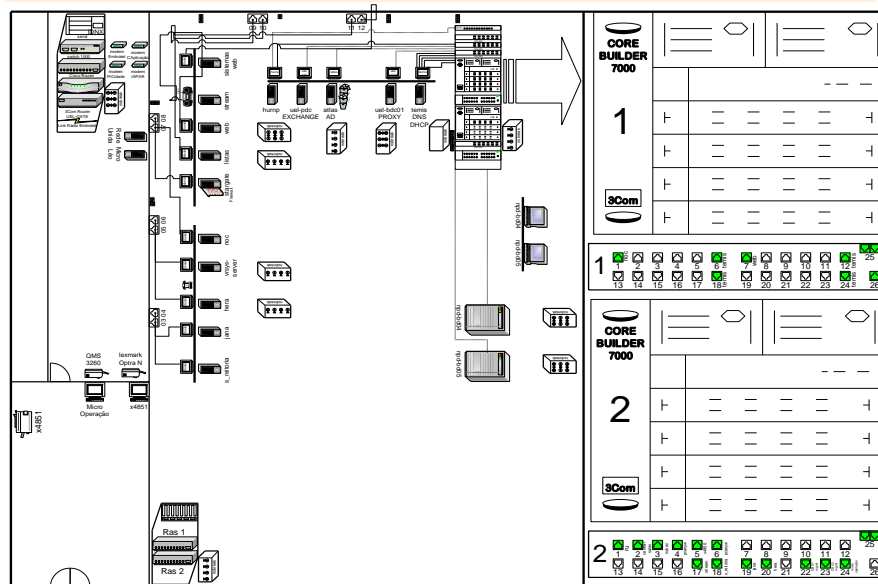
03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

78

78

ÁREAS FUNCIONAIS – Documentação



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

79

79

ÁREAS FUNCIONAIS – Documentação

• Se aplica no gerenciamento de configuração

- Servidores
 - Arquivos
 - Tipos de partição
 - Parâmetros de instalação
 - Firewall
 - Regras instaladas
 - E-mail
 - Configurações básicas
 - Listas
 - forward
 - Web
 - Local dos diretórios dos sites
 - Tipos de segurança

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

80

80

ÁREAS FUNCIONAIS – Documentação

- Se aplica no gerenciamento de configuração
 - Equipamentos de rede
 - Switchs
 - Vlans
 - Elans
 - Detalhes de configuração
 - Roteadores
 - Tabela de roteamento dinâmicas ou estáticas
 - Detalhes de configuração

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

81

81

III – Padrões para Gerência

82

Padronizações - Gerência

- **ISO**
 - **Grupo ISO-IEC/JTC 1/WG 4**
 - RM-OSI adotou modelo agente e gerente
 - Gerenciamento deveria ser poderoso
 - **CMIP-CMIS**
- **Gerência na Internet ou no TCP/IP - IETF**
 - **Grupo OPERATIONS AND MANAGEMENT AREA**
 - Modelo agente e gerente mais simplificado
 - **SNMP**

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

83

83

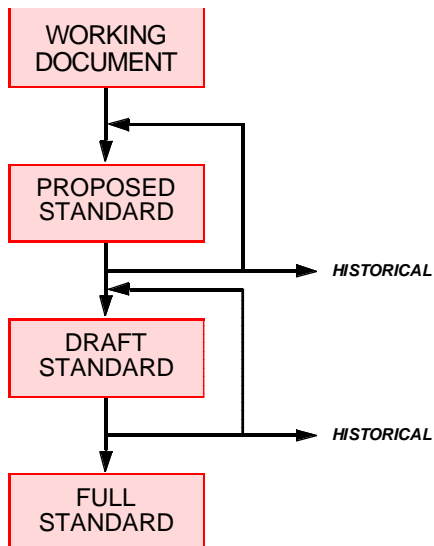
Padronizações - IETF

*implementation
experience
must be obtained*

after a maximum
of 2 years

*several independent
implementations
must interwork*

after a maximum
of 4 years



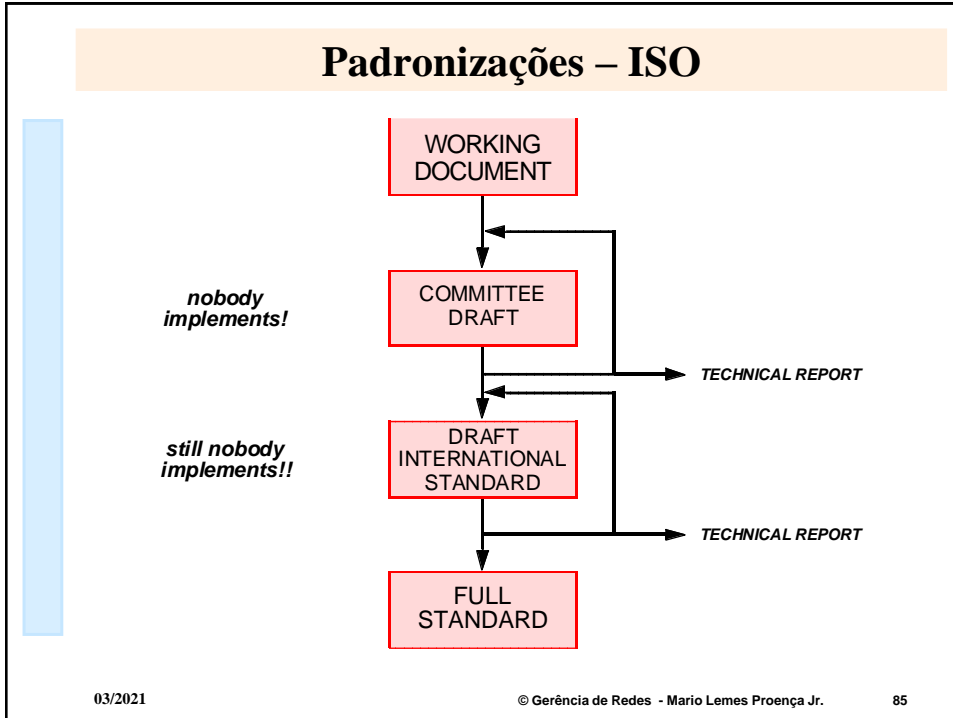
03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

84

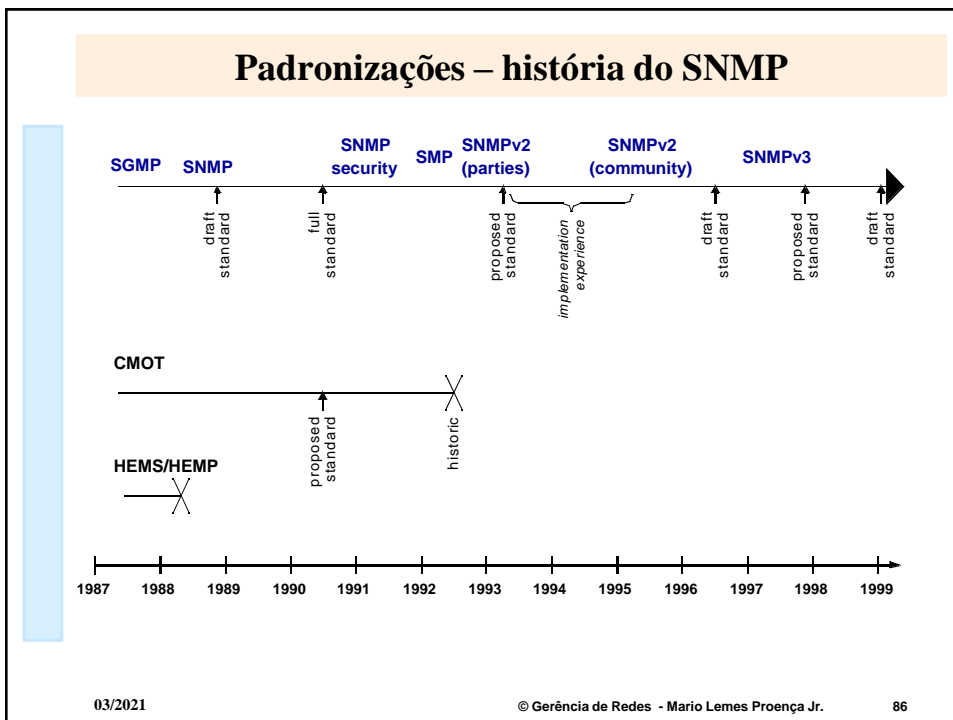
84

Padronizações – ISO

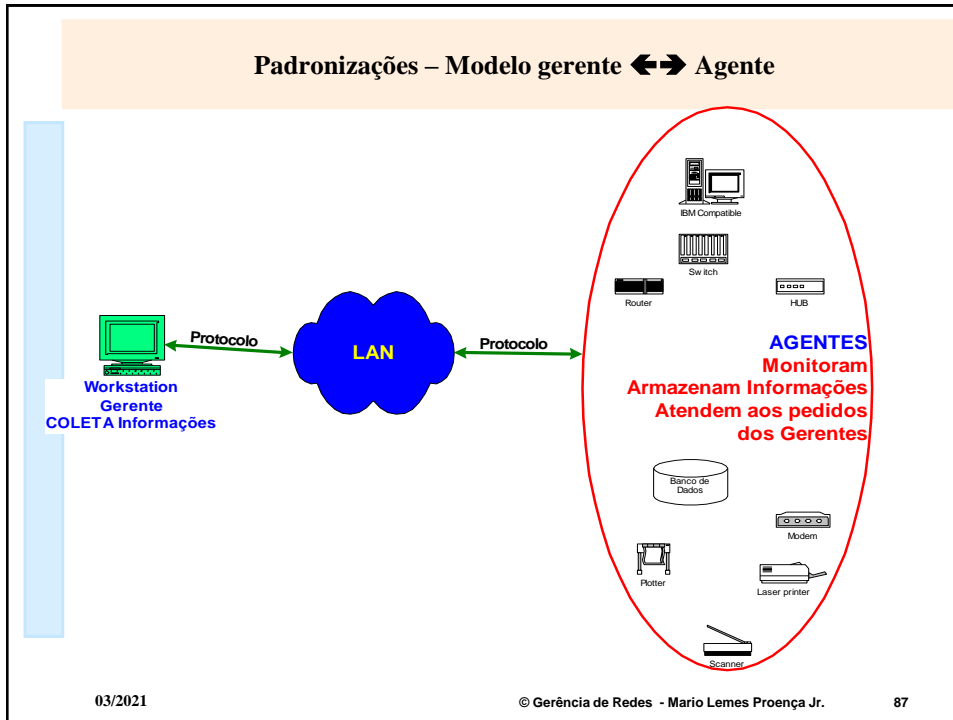


85

Padronizações – história do SNMP



86



87

ÁREAS FUNCIONAIS – Exercícios

➤ **Exercícios – Questão 00 - (30 minutos)**

- ✓ Apresente uma lista de informações que são necessárias para você gerenciar:
 - ✓ Uma impressora?
 - ✓ Um switch?
 - ✓ Um servidor de rede ?

03/2021 © Gerência de Redes - Mario Lemes Proença Jr. 88

88

3.2 - Gerência no TCP/IP – SNMP

Simple Network Management Protocol

89

Gerência no TCP/IP - SNMP

- *Simple Network Management Protocol (SNMP)*
 - Aprovado em 1988 pelo *Internet Activities Board (IAB)*
 - *Internet Engineering Task Force (IETF)* produziu os padrões

Publicações do IETF para 1ª versão do SNMP	RFC	Ano
<i>Simple Network Management Protocol (SNMP)</i>	1157	1990
<i>Structure of Management Information (SMI)</i>	1155	1990
<i>Management Information Base versão 1 (MIB-I)</i>	1156	1990
<i>Management Information Base versão 2 (MIB-II)</i>	1213	1991

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

90

90

Gerência no TCP/IP - SNMP

- Componentes
 - Gerente
 - Estação de trabalho com software apropriado
 - Agente
 - Hardware e software instalado em um equipamento (hub, switch, roteador, servidor, modem, porta, cafeteira, etc..)
 - Protocolo
 - SNMP

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

91

91

Gerência no TCP/IP - SNMP

- SNMP
 - Utiliza o UDP para transporte
 - Qual porta ?
 - Protocolo sem conexão
 - Agente deveria ser simples
 - **Razão do sucesso !!!**
 - Disponível em quase todos os elementos da rede
 - Hub, switch, roteador, servidor, modem,
 - Gerente faz *pooling* no agente
 - Gera tráfego na rede para as consultas e respostas
 - Gerente deve avaliar o impacto na rede

03/2021

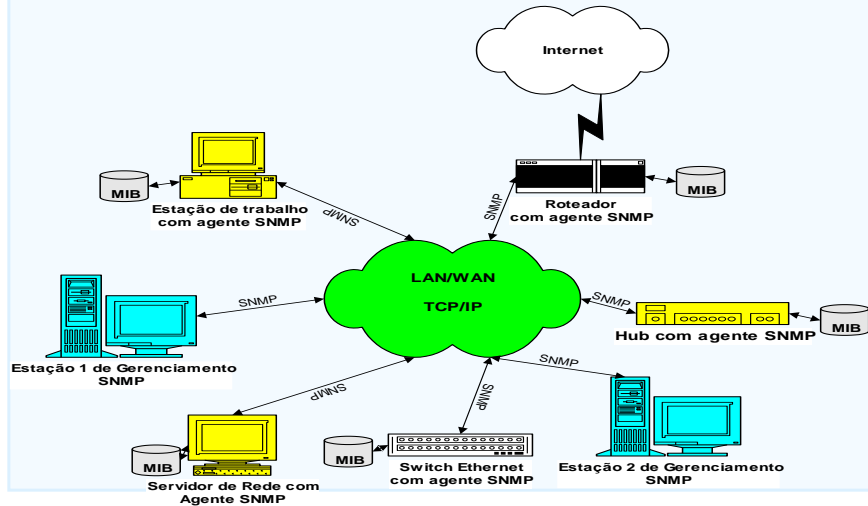
© Gerência de Redes - Mario Lemes Proença Jr.

92

92

Gerência no TCP/IP - SNMP

➤ Modelo de Gerência adotado no SNMP



03/2021

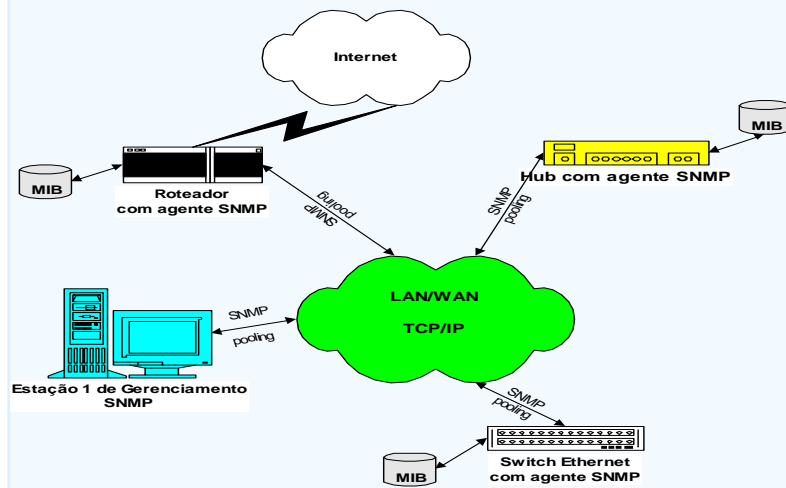
© Gerência de Redes - Mario Lemes Proença Jr.

93

93

Gerência no TCP/IP - SNMP

➤ Modelo de Gerência adotado no SNMP



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

94

94

Gerência no TCP/IP - SNMP

- Modelo de Gerência adotado no SNMP
 - Estação de gerenciamento
 - Aplicação de gerenciamento
 - Saber a topologia da rede
 - Manter logs sobre operações realizadas
 - Agente de gerenciamento SNMP
 - Proxy agent
 - *Management Information Base* (MIB)
 - Protocolo de Comunicação SNMP

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

95

95

Gerência no TCP/IP - SNMP

- Operações no SNMP
 1. Mudar o valor de um objeto residente na *Management Information Base* (MIB) (Set)
 2. Obter o valor de um objeto na MIB (Get)
 3. Trap
 - É uma mensagem enviada pelo agente não solicitada pelo gerente. Ela é enviada a um gerente previamente informado no agente, pode informar:
 - Coldstart
 - Warmstart
 - Link up
 - Link down

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

96

96

Gerência no TCP/IP – Protocolo SNMP

➤ Protocolo SNMP

- Para a troca de informação entre o agente SNMP e a estação de gerenciamento é utilizado o protocolo SNMP que teve sua 1ª versão publicada na RFC 1157.
- A maioria das implementações SNMP utilizam o protocolo *User Datagram Protocol* (UDP) para nível de transporte. O UDP é um protocolo não orientado a conexão. Como não existe mecanismo para garantir que a mensagem SNMP seja transportada com sucesso, o controle deve ser feito pela aplicação de gerenciamento.

03/2021

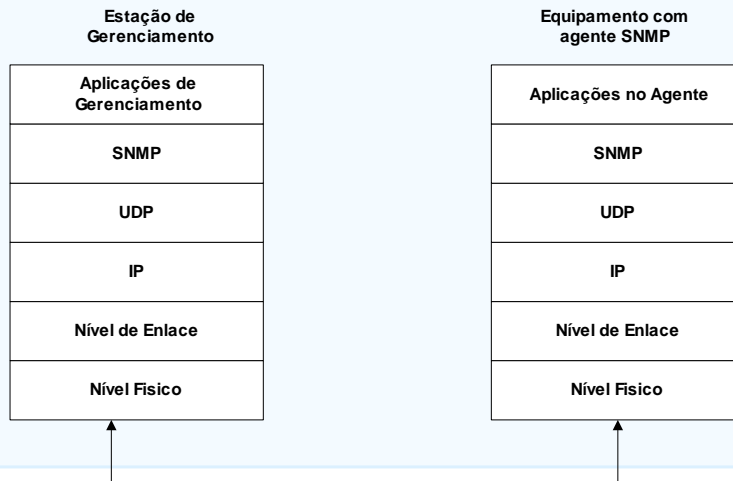
© Gerência de Redes - Mario Lemes Proença Jr.

97

97

Gerência no TCP/IP – Protocolo SNMP

➤ Modelo de referencia SNMP



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

98

98

Gerência no TCP/IP – Protocolo SNMP

- Comandos básicos do SNMP
 - **GET** : Permite que a estação de gerenciamento recupere informação do agente SNMP,
 - **SET** : Permite que a estação de gerenciamento altere valores de objetos na MIB do agente SNMP.
 - **TRAP** : Permite que o agente notifique a estação de gerenciamento sobre a ocorrência de algum evento.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

99

99

Gerência no TCP/IP – Protocolo SNMP

- A troca de informações entre o agente e o gerente é feita usando mensagens SNMP.
- A mensagem SNMP é composta por:
 - nome da comunidade
 - *Protocol Data Units* (PDU).
- Existem cinco tipos de PDUs que podem ser usados para troca de informação entre o gerente e o agente.

Versão do SNMP	Nome da Comunidade	PDU SNMP
----------------	--------------------	----------

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

100

100

Gerência no TCP/IP – Protocolo SNMP

➤ PDUs SNMP

- *get-request* : Usado pela estação de gerenciamento para recuperar um objeto informação da MIB do agente SNMP.
- *get-response* : Usado pelo agente para responder o pedido *get-request* da estação de gerenciamento.
- *get-next-request* : Usado em conjunto com o *get-request* para obter o próximo objeto da MIB, próximo a partir do ultimo recuperado com *get-request*.

Gerência no TCP/IP – Protocolo SNMP

➤ PDUs SNMP

- *set-request* : Permite a estação de gerenciamento alterar o valor de objetos na MIB.
- *Trap* : Permite ao agente informar a estação de gerenciamento sobre a ocorrência de um evento específico. Existem sete tipos de *traps* possíveis segundo especificado

Gerência no TCP/IP – Protocolo SNMP

➤ *Trap*

1. Inicialização ou reinicialização do equipamento a frio (*Coldstart*);
2. reinicialização do equipamento a quente(*Warmstart*);
3. link desativado;
4. link ativo;
5. falha de autenticação entre agente e gerente;
6. perda na conexão *Exterior Gateway Protocol* (EGP) com equipamento vizinho;
7. *trap* específico para evento definido pelo fabricante do equipamento.

03/2021

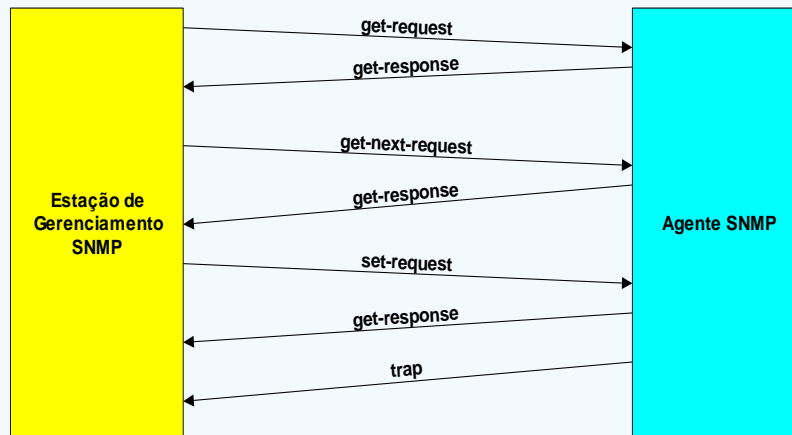
© Gerência de Redes - Mario Lemes Proença Jr.

103

103

Gerência no TCP/IP – Protocolo SNMP

➤ Protocolo SNMP



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

104

104

Gerência no TCP/IP – Protocolo SNMP

- Problemas da 1ª versão do SNMP
 - No SNMPv1 a segurança é fraca e baseada somente no nome da comunidade que existe em cada mensagem SNMP. As mensagens SNMP são transmitidas no modo texto sem nenhuma proteção de seu conteúdo

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

105

105

Gerência no TCP/IP – Protocolo SNMP

- Características
 - O nome da comunidade fica definido no agente, onde é feita a autenticação e o policiamento no acesso a MIB.
 - A autenticação é baseada no fato de que o gerente deve saber o nome da comunidade para acessar a MIB, caso contrario o agente retorna uma mensagem com erro de autenticação

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

106

106

Gerência no TCP/IP – Protocolo SNMP

➤ Características

- O policiamento é um outro mecanismo de segurança do SNMP baseado no nome da comunidade.
- Podem existir mais de uma comunidade no agente e cada qual com tipo de acesso diferente as informações da MIB, como por exemplo uma comunidade nome *public* com direitos à operações só de *read* (*comando get*), e uma comunidade com nome *suporte* com direitos *read/write* (*comandos get / set*).

03/2021

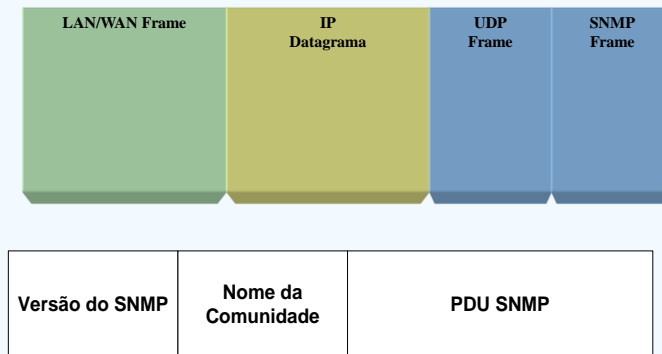
© Gerência de Redes - Mario Lemes Proença Jr.

107

107

Gerência no TCP/IP - SNMP

➤ Formato do Frame SNMP



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

108

108

➤ *Management Information Base (MIB)*

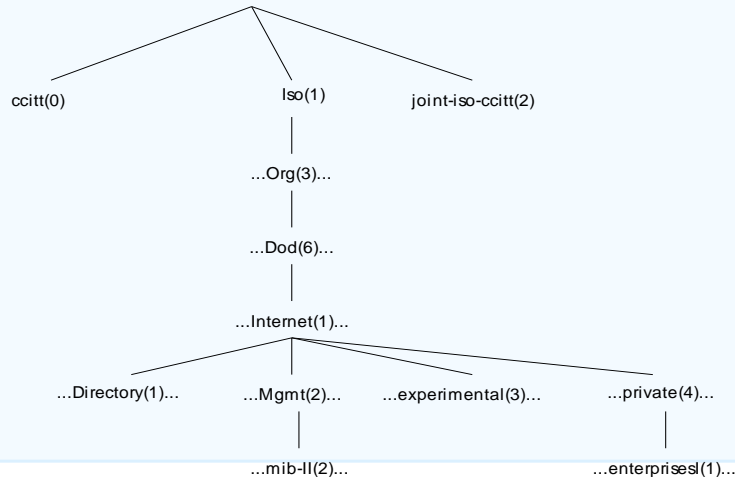
- É um conjunto de objetos gerenciados definidos segundo um padrão estruturados em grupos hierárquicos
- **Os objetos gerenciados contem um valor que representa o estado de um objeto real em um determinado instante**
- É o local onde estão definidas e armazenadas as informações que podem ser acessadas através de um protocolo de gerenciamento
- Repositório de objetos gerenciados

➤ *Management Information Base (MIB)*

- Para o armazenamento de informações na MIB é definida uma estrutura em árvore, compostas por nós, onde cada nó tem um *Object Identifier (OID)* e um nome associado.
- O OID é uma série de inteiros separados por pontos. Cada nó da árvore pode ter uma nova subárvore associada. Para a raiz da árvore foram definidos três nós iniciais contendo (ccitt(0), iso(1), joint-iso-ccitt(2)),

Gerência no TCP/IP – SNMP - MIB

• *Management Information Base (MIB)*



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

111

111

Gerência no TCP/IP – SNMP - MIB

➤ *Management Information Base (MIB)*

- Para definição da sintaxe, tipos de informações e regras para criação de objetos que estarão contidos na MIB o IAB utiliza a **Structure of Management Information (SMI)**, que é definida por um subconjunto do *ISO Abstract Syntax Notation One (ISO ASN.1)*.
 - Versão atual da *Structure of Management Information Version 2 (SMIv2)* RFC 2578 de 04/1999
- Cada objeto na MIB tem identificação única evitando duplicidade ao acessar os dados da MIB.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

112

112

Gerência no TCP/IP – SNMP - MIB

➤ Tipos de dados existentes na MIB.

Tipos de dados	obs
Integer32 e INTEGER	números inteiros
OCTET STRING	representa dados textuais
OBJECT IDENTIFIER	representa nomes de designação administrativa
BITS	uma enumeração de bits pré-designados
IPADDRESS	um endereço de Internet de 32 bits
Counter32	um inteiro não negativo que se incrementa desde zero até ao máximo de $2^{32}-1$, altura em que dá a volta e recomeça do zero;
Gauge32	um inteiro não-negativo que pode ser incrementado ou decrementado , podendo assumir valores entre zero e $2^{32}-1$; (indicador ou medida)
TimeTicks	inteiro não-negativo que representa o tempo, no módulo 2^{32} , em centésimos de segundo entre dois instantes
Opaque	tipo é usado somente para compatibilidade com tipos antigos
Counter64	Idem ao Counter32, mas com um máximo de $2^{64}-1$
Unsigned32	número inteiro entre 0 e $2^{32}-1$;
Tabelas Conceptuais	tabelas que permitem usar uma estrutura tabular e uma coleção de objetos dentro da MIB.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

113

113

Gerência no TCP/IP – SNMP - MIB

➤ *Management Information Base (MIB)*

- Estes objetos são definidos com base nos campos:
 - SYNTAX tipo do objeto
 - ACCESS leitura/gravação
 - STATUS se é ou não obrigatório
 - DESCRIPTION descrição do objeto

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

114

114

Gerência no TCP/IP – SNMP - MIB

➤ *Management Information Base (MIB)*

- Definida por um subconjunto do *ISO Abstract Syntax Notation One* (ISO ASN.1)
- A 1ª MIB oficial para o protocolo SNMP da Internet, também conhecida como MIB-I foi definida na RFC 1156 (120 elementos)
- A segunda versão da MIB para a Internet, foi publicada na RFC 1213 em 1991, e recebeu o nome de MIB-II (220 elementos).
- Os grupos da MIB-II são: *System, Interfaces, Address Translation, IP, ICMP, TCP, UDP, EGP, Transmission, SNMP*
- Extensível

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

115

115

Gerência no TCP/IP – SNMP - MIB

➤ *Management Information Base (MIB)*

- Atualmente existem inúmeras MIBs implementadas que foram propostas em RFCs, e também muitas MIBs proprietárias implementadas por fabricantes para melhor gerenciar seus equipamentos.
- **Com isto temos uma quantidade muito grande de variáveis o que torna a escolha um trabalho difícil para o gerente, no sentido de especificar o que é mais importante para ser gerenciado, dentre as milhares de possibilidades disponíveis.**

03/2021

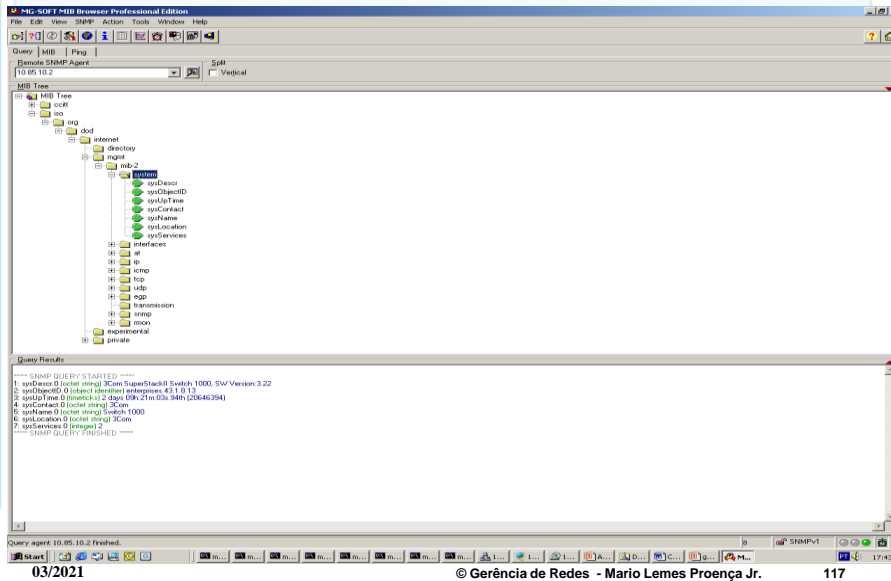
© Gerência de Redes - Mario Lemes Proença Jr.

116

116

Gerência no TCP/IP – SNMP - MIB

➤ Management Information Base (MIB)



The screenshot shows the MIB Browser Professional Edition interface. The MIB Tree on the left displays a hierarchy starting with 'internet' and 'mib-2'. Under 'mib-2', several objects are listed, including 'sysDescr', 'sysObjectID', 'sysUpTime', 'sysContact', 'sysName', 'sysLocation', 'sysServices', 'interfaces', 'if', 'icmp', 'tcp', 'udp', 'egp', 'transmission', 'snmp', 'snmpMibs', 'experimental', and 'private'. The 'Query Results' window at the bottom shows the following output:

```
--- SNMP QUERY STARTED ---  
1. sysDescr.0 (object string) SCOM SuperStackII Switch 1000, SW Version 3.22  
2. sysObjectID.0 (object identifier) enterprise 43.1.0.13  
3. sysContact.0 (textual string) Edm Edm 21m 03s 94m 125646294  
4. sysName.0 (object string) SCOM  
5. sysLocation.0 (text string) Switch 1000  
6. sysServices.0 (object identifier) 1  
7. sysServices.0 (integer) 1  
--- SNMP QUERY FINISHED ---
```

At the bottom of the window, the date '03/2021' and the text '© Gerência de Redes - Mario Lemes Proença Jr. 117' are visible.

117

Gerência no TCP/IP – SNMP – MIB-2

- Grupos da MIB-2
 - 01) System
 - 02) Interfaces
 - 03) At
 - 04) IP
 - 05) ICMP
 - 06) TCP
 - 07) UDP
 - 08) EGP
 - 09) Transmission
 - 10) SNMP

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

118

118

Gerência no TCP/IP – SNMP – MIB-2

- 01) Grupo System
 - sysDescr
 - Descrição do equipamento
 - sysObjectID
 - Código para identificar fabricante
 - sysUpTime
 - Quanto tempo o equipamento está ligado

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

119

119

Gerência no TCP/IP – SNMP – MIB-2

- 01) Grupo System
 - sysContact
 - Contato com o gerente do equipamento / Rede
 - sysName
 - Nome do administrativo do equipamento
 - sysLocation
 - localização
 - sysServices
 - Serviços que estão funcionando neste equipamento

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

120

120

Gerência no TCP/IP – System Group

- **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."

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

121

121

Gerência no TCP/IP – System Group

- **sysObjectID** OBJECT-TYPE
 - SYNTAX OBJECT IDENTIFIER
 - ACCESS read-only
 - STATUS mandatory
 - DESCRIPTION "The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router'."

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

122

122

Gerência no TCP/IP – System Group

- **sysUpTime** OBJECT-TYPE
 - SYNTAX TimeTicks
 - ACCESS read-only
 - STATUS mandatory
 - DESCRIPTION "The time (in hundredths of a second) since the network management portion of the system was last re-initialized."

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

123

123

Gerência no TCP/IP – System Group

- **sysContact** OBJECT-TYPE
 - SYNTAX DisplayString (SIZE (0..255))
 - ACCESS read-write
 - STATUS mandatory
 - DESCRIPTION "The textual identification of the contact person for this managed node, together with information on how to contact this person."

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

124

124

Gerência no TCP/IP – System Group

- **sysName** OBJECT-TYPE
 - SYNTAX DisplayString (SIZE (0..255))
 - ACCESS read-write
 - STATUS mandatory
 - DESCRIPTION "An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name."

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

125

125

Gerência no TCP/IP – System Group

- **sysLocation** OBJECT-TYPE
 - SYNTAX DisplayString (SIZE (0..255))
 - ACCESS read-write
 - STATUS mandatory
 - DESCRIPTION "The physical location of this node (e.g., 'telephone closet, 3rd floor')."

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

126

126

Gerência no TCP/IP – System Group

- **sysServices** OBJECT-TYPE
 - SYNTAX INTEGER (0..127)
 - ACCESS read-only STATUS mandatory
 - DESCRIPTION "A value which indicates the set of services that this entity primarily offers. The value is a sum. This sum initially takes the value zero, Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which performs primarily routing functions would have a value of 4 ($2^{(3-1)}$). In contrast, a node which is a host offering application services would have a value of 72 ($2^{(4-1)} + 2^{(7-1)}$). Note that in the context of the Internet suite of protocols, values should be calculated accordingly: layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways) 4 end-to-end (e.g., IP hosts) 7 applications (e.g., mail relays) For systems including OSI protocols, layers 5 and 6 may also be counted."

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

127

127

Gerência no TCP/IP – System Group

- System Group – exemplo de consulta
 - ***** SNMP QUERY STARTED *****
 - 1: sysDescr.0 (octet string) 3Com SuperStackII Switch 1000, SW Version:3.22
 - 2: sysObjectID.0 (object identifier) enterprises.43.1.8.13
 - 3: sysUpTime.0 (timeticks) 1 days 13h:51m:25s.93th (13628593)
 - 4: sysContact.0 (octet string) 3Com
 - 5: sysName.0 (octet string) Switch 1000
 - 6: sysLocation.0 (octet string) 3Com
 - 7: sysServices.0 (integer) 2
 - ***** SNMP QUERY FINISHED *****

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

128

128

IV- Problemas no Dia a Dia de uma Rede

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

129

129

Problemas no Dia a Dia de uma Rede

- São inúmeros
- São diferentes
- Requerem resposta rápida
 - Inventário dos ativos gerenciados.
 - Identificar onde o problema esta.
 - Efetuar a correção.
- ✓ O melhor seria uma abordagem Proativa !!!

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

130

130

Problemas no Dia a Dia de uma Rede

- Distância
- Número muito grande de equipamentos
- Diferentes fabricantes
- Mão de obra qualificada
 - Analista tem que conhecer diversas tecnologias e configurações
- Envolve pessoal de diversas áreas
 - Analista de suporte
 - *Help desk*
 - Operador
 - Analistas de sistemas (software aplicativo)
 - Usuários comuns
- Atividade complexa que exige alto grau de especialização do administrador

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

131

131

Problemas no Dia a Dia de uma Rede

- **Performance**
 - **Lentidão nos acessos**
 - **Colisões**
 - **Algum *tarado* fazendo ftp, download mp3 ou vídeo**
 - **Problema intermitente em um cabo ou placa**
 - **DNS**
 - **Link lotado !**
 - **Uso indevido**
 - **Acesso a Web**
 - **E-mail gigantesco**
 - **Verificar arquivo Word e ver log Cacti**

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

132

132

Problemas no Dia a Dia de uma Rede

➤ VÍRUS

- Estações
- Servidores
- E-mail
- Administradores !!!!!!!
 - (W32/Bugbear@MM, klez) Impressora

➤ HOAXES

- <http://home.mcafee.com/virusinfo/virus-hoaxes>
- <http://www.symantec.com/avcenter/hoax.html>

➤ Exercícios – Questão 03 - (10 minutos)

- Leitura dos dois sites e escrever pelo menos dois parágrafos explicando sobre o assunto, incluindo exemplos.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

133

133

Problemas no Dia a Dia de uma Rede

➤ Servidor trava

- Erro de hardware
 - O que fazer ? Ter um clone ?
- Erro de software
 - **Ataque !**
 - Reinstalar ? Ter um clone ?
 - Qual o plano de contingência ?
- Link externo fora do ar
 - O que acontece ?

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

134

134

Problemas no Dia a Dia de uma Rede

- **DNS**
 - Para tudo ! Por que ?
 - exemplo
- **Estações trocando de lugar físico**
 - Qual o problema ?
- **Alteração de senhas de usuários**
 - Política
- **Criar contas de usuários**
 - Política para criar e remover
 - Automação

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

135

135

Problemas no Dia a Dia de uma Rede

- **Controle dos home Dirs dos usuários**
 - Cotas
 - Armazenamento de arquivos indevidos
- **Novos projetos de rede (expansões)**
 - Inventário atualizado
- **Problemas de roteamento**
 - Novas sub-redes
- **Problemas de hardware**
- **Problemas de cabeamento**

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

136

136

Problemas no Dia a Dia de uma Rede

- **Problemas no firewall**
 - Liberar um serviço novo !!!
 - FTP
 - Estabelecer limites para o serviço
 - Cortes de serviços (portas)
 - NAT
 - Bloqueio de sacanas ! ☹
 - Exemplos

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

137

137

Problemas no Dia a Dia de uma Rede

- **Segurança**
 - Ataques a servidores
 - Ataques a estações de usuários
 - Ataques a usuários mamões
- **Configuração e manutenção do proxy server**
 - Roteamento, desempenho,
- **Servidor de e-mail**
 - SPAM, Phishing
 - Vírus

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

138

138

Problemas no Dia a Dia de uma Rede

- **Servidor Web**
 - Performance
 - Ataques
 - Política para log
- **Documentação inexistente**
 - Quem já não ficou procurando qual porta/ponto pertence a uma determinada estação, e se esta ligada ou não ?
- **Capacity Planning**
 - Realidade atual e crescimento ! ?
- **Alguma coisa a mais ???**

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

139

139

Problemas no Dia a Dia de uma Rede

- **Alguma coisa a mais ???**
 - Whenu savenow software instalado junto com o Kazaa
 - Whenu savenow !!! Acessos ao proxy !!!!!
 - 19/11/2002 1.332.262 ou 15/seg de 2.791.061 ou 32/seg
 - 20/11/2002 1.021.323 ou 11/seg de 2.705.108 ou 31/seg
 - 01/04/2003 1.126.887 ou 13/seg de 2.738.056 ou 31/seg
 - Arquivo com 384.280.517 bytes
 - Aproximadamente 15 requisições por seg. !!!
 - 10.85.160.151 - - [01/Apr/2003:00:00:40 -03001 "GET http://www.whenu.com/versions.html HTTP/1.0" 407 1358 TCP_DENIED:NONE



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

140

140

Problemas no Dia a Dia de uma Rede

- **Alguma coisa a mais ???**
 - **MSN Toolbar**
 - Problemas da mesma magnitude do whenu



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

141

141

Problemas no Dia a Dia de uma Rede

- **Um estudo científico sério demonstrou que 90 % dos problemas se encontra entre teclado e a cadeira, havendo fortes indícios de que não é o estofamento da cadeira !**



03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

142

142

Problemas no Dia a Dia de uma Rede

➤ **Melhor Remédio para os problemas ?**

➤ **ONOFRE !**

➤ **ON e OFF**

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

143

143

V - Ferramentas de Gerência

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

144

144

Ferramentas para Áreas de Gerenciamento (FCAPS)

- **Imprescindível ter um Inventário dos ativos de Rede**
 - Servidores
 - Switches
 - APs
 - Roteadores
 - Estações/desktop/notebook/smartphone
 - Pontos de rede
 - Plantas e mapas da rede
 - Informação sobre portas/switch que ligam 1º, 2º e 3º nível da rede
<http://noc.uel.br/networkmap/>
 - Softwares / licenças / validades / atualizações
 - Usuários / contas / diretórios / arquivos / e-mails /

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

145

145

Ferramentas para Áreas de Gerenciamento (FCAPS)

- **Imprescindível ter um Inventário dos ativos de Rede**
 - Software para inventário e asset management
 - OCS open source <http://www.ocsinventory-ng.org/en/>
 - Microsoft
 - Software Asset Management
 - openDCIM
 - ISO/IEC 19770-1:2012 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56000
 - Establishes a baseline for an integrated set of processes for Software Asset Management (SAM), divided into tiers to allow for incremental implementation, assessment and recognition
 - Documento Pago !!

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

146

146

Ferramentas para Áreas de Gerenciamento (FCAPS)

- **Imprescindível ter software para registro de chamados**
 - Software para registro de chamado
 - OTRS open source <http://www.otrs.com/>
 - GLPI
 - Mantis
 - Chamado
 - Data, hora, descrição do problema
 - Problema é identificar o problema
 - Fazer a triagem correta e direcionar o problema

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

147

147

Ferramentas para Áreas de Gerenciamento (FCAPS)

- **Falhas (FCAPS)**
 - Conhecimento empírico do administrador (MUITO VALIOSO)
 - Analisador de rede
 - Hardware
 - Testador de cabos
 - Fluke (<http://www.fluke.com>)
 - Software
 - Sniffer
 - *Network Management System* (NMS)

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

148

148

Ferramentas para Áreas de Gerenciamento (FCAPS)

➤ Configuração (FCAPS)

- Normalmente software proprietário
- Telnet (hubs, switches, roteadores)
 - Exemplo
- Putty
- Web
 - Impressoras
 - Roteadores
 - Proxy, etc.
- Terminal Server

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

149

149

Ferramentas para Áreas de Gerenciamento (FCAPS)

➤ Contabilização (FCAPS)

- Logs do sistema operacional
- Logs do software que está sendo utilizado
 - Sistema administrativo
 - Servidor de contas
 - Proxy
 - Firewall
 - RAS
 - Servidor de e-mail
- Ferramentas para análise de logs
 - Grande volume de dados
 - Sistema especialista

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

150

150

Ferramentas para Áreas de Gerenciamento (FCAPS)

➤ Performance (FCAPS)

- Sniffer
 - Análise de desempenho
- Ferramentas do sistema operacional
 1. Ping
 2. Traceroute ou tracert
 3. Netstat
 4. Arp
 5. Nslookup
- **EXERCÍCIO – Questão 01**
 - Testar estas 5 ferramentas e produzir um relatório sobre a utilidade de cada uma correlacionando com as respectivas áreas funcionais que elas podem atender ? 15 minutos

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

151

151

Ferramentas para Áreas de Gerenciamento (FCAPS)

➤ Performance (FCAPS)

- Ferramentas que utilizam SNMP, RMON
 - Network Management Systems
 - HP Openview da HP (<http://www.openview.com>)
 - 3com Network Supervisor (<http://www.3com.com>)
 - IBM Tivoli Netview (<http://www-3.ibm.com/software/tivoli/>)
 - CiscoWorks da Cisco
 - Optivity Network Management System (NMS) da Nortel
 - SolarWinds Network Management (<http://www.solarwinds.net>)
 - SNMPc <http://www.castlerock.com/>
 - Whatsup <http://www.ipswitch.com/>
 - Cacti <http://cacti.net/>
 - Epicenter <http://www.extremenetworks.com/products/epicenter.aspx>
 - Nagios <http://www.nagios.org/>

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

152

152

Ferramentas para Áreas de Gerenciamento (FCAPS)

➤ Performance (FCAPS)

- Ferramentas que utilizam SNMP, RMON
 - MRTG
 - Clássico para área de gerenciamento
 - <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>
 - <http://www.mrtg.org>
 - Cacti <http://www.cacti.net>
 - Exemplos:
 - <https://www.rnp.br/servicos/conectividade/trafego>
 - <http://noc.uel.br>

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

153

153

Ferramentas para Áreas de Gerenciamento (FCAPS)

➤ Segurança (FCAPS)

- Firewall
 - Análise de todos os pacotes que entram e saem da rede
 - Filtro de serviços não desejados
 - Bloqueio de redes ou IPs suspeitos ou indesejados
 - Iptables nativo no linux
 - Checkpoint <https://www.checkpoint.com/>
 - Palo Alto Networks <https://www.paloaltonetworks.com/>
 - Fortinet <https://www.fortinet.com/>
 - Cisco <http://www.cisco.com>
 - Watchguard
 - Dell SonicWall
 - Barracuda
 - Intel McAfee
 - Sophos
 - Pfsense Open Source <http://www.pfsense.org>

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

154

154

Ferramentas para Áreas de Gerenciamento (FCAPS)

➤ Segurança (FCAPS)

➤ **Unified Threat Management (UTM)**

- ✓ Detecção de Intrusão
- ✓ Detecção de Vírus
- ✓ Trojan
- ✓ Spam
- ✓ Worms
- ✓ Spyware
- ✓ IPS
- ✓ Filtro URL

- ✓ Todos os serviços integrados em uma solução
- ✓ Facilita o gerenciamento (instalação, manutenção, atualização...)
- ✓ Exemplos de fabricantes: Palo Alto Networks, Cisco, Fortinet, Check Point, SonicWall, Barracuda, Sophos, HPE,

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

155

155

Ferramentas para Áreas de Gerenciamento (FCAPS)

➤ Segurança (FCAPS)

➤ Sniffer

- Monitoramento do trafego em um segmento
- Captura de todos os pacotes em um segmento
- Análise de situações suspeitas
- Wireshark <https://www.wireshark.org/>

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

156

156

Ferramentas para Áreas de Gerenciamento (FCAPS)

➤ Segurança (FCAPS)

- Proxy
 - Squid
 - Microsoft
 - Analise do log
 - Descoberta de uso indevido do recurso, através do rastreamento
 - Webtrends <http://www.webtrends.com/>
- DHCP
 - Amarra IP ao *MAC address* da estação
 - Facilita a configuração e administração
 - Log indica data e hora da utilização do equipamento

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

157

157

Ferramentas para Áreas de Gerenciamento (FCAPS)

➤ Segurança (FCAPS)

- Backup
 - Cópia diária dos dados armazenados nos servidores
 - Arcserve <http://www.arcserve.com>
 - Veritas Backup <http://www.veritas.com/>
 - HP Data Protector <http://www.hp.com>
 - Bacula open source <http://blog.bacula.org/>
 - CommVault <https://www.commvault.com/solutions/by-function/data-protection-backup-and-recovery>
 - EMC Avamar <http://www.emc.com/data-protection/avamar.htm>

➤ Exercícios - Questão 02 - (15 minutos)


- Encontrar pelo menos 2 ferramentas de gerência que possam ser utilizadas no NOC. Explicar sua função de acordo com as áreas funcionais.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

158

158




VI - Network Operations Center (NOC)

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

159

159



Network Operations Center (NOC)

- Centro de operações da rede
- Responsável pelo gerenciamento e controle da rede
- Solucionar os problemas que possam acontecer nas áreas de gerenciamento
- NOCTools, <http://www.ietf.org/rfc/rfc1470.txt>
 - **Exercícios – Questão 04 - (10 minutos)**
 - **Analisar documento e escrever até dois parágrafos explicando sua finalidade**

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

160

160

Network Operations Center (NOC)

- Deve instituir normas para utilização da rede
- Plano de ação / contingência em caso de problema. O que fazer ?
 - Checklist
 - Plano de contingência
- Deve estar coletando o máximo possível de informações da rede. Problema ?
 - Onde armazenar e como recuperar ?
 - Banco de Dados
 - Sistemas Especialista

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

161

161

Network Operations Center (NOC)

- Com base nas informações coletadas da rede os gerentes que trabalham no NOC devem:
 - Produzir um *baseline*
 - Manter o monitoramento para as cinco áreas funcionais
 - Detectar intrusão (segurança)
 - Sanar problemas de forma
 - Pró-ativa sempre que possível e
 - Reativa quando necessário

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

162

162

Network Operations Center (NOC)

- Sistema de *trouble ticket*
 - Registrar todas as ocorrências
 - Melhora e ajuda na solução de problemas
 - **Muitos dos problemas que acontecem no dia a dia já aconteceram anteriormente**
 - Grandes redes este sistema é fundamental
 - Ajuda a registrar chamadas
 - Gerar relatórios analíticos sobre problemas e desempenho das equipes
 - Bonito na teoria mas na prática o usuário prefere ligar e perguntar diretamente a um técnico

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

163

163

Network Operations Center (NOC)

- Sistema de *troubleshooting*
 - **Internetwork Troubleshooting Guide (CISCO)**
 - http://www.cisco.com/en/US/docs/net_mgmt/element_manager_system/3.1/user/guide/trouble.html#wp1036537
 - Analisar 10 m.
 - **Centro de operações da RNP**
 - <http://www.rnp.br/operacao/>
 - Analisar 10 m.

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

164

164

Network Operations Center (NOC)

- Gerência centralizada
 - Vantagens
 - Estabelecimento de padrões
 - Redução de pessoal especializado
 - Documentação única
 - Visão única do todo
 - Servidores centralizados ?
 - Desvantagens
 - Distâncias ☹ ☹

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

165

165

Bibliografia



- **Snmp, Snmpv2, Snmpv3 and Rmon 1 and 2** [William Stallings](#)
Addison-Wesley, Hardcover, 3rd edition, Published December 1998, 620 pages, snmp_rmon3, ISBN 0201485346



- **REDES DE COMPUTADORES E INTERNET**, ABRANGE TRANSMISSAO DE DADOS, LIGAÇÃO INTER-REDES
Autor: [COMER, DOUGLAS E.](#), Editora: [BOOKMAN COMPANHIA ED](#)



- **Telecommunications Network Management**, Haogen Wang, editora Mcgraw-Hill Telecommunications, 1999 ISBN 0070681708

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

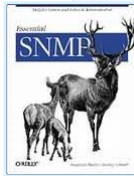
166

166

Bibliografia



- **Network Management A Pratical Perspective**, Leinwand, Allan, Addison Wesley, 1996, 2a edição, ISBN 0201609991



- **ESSENTIAL SNMP**, MAURO, DOUGLAS R. SCHMIDT, KEVIN J., OREILLY & ASSOC , 2001, 1a edição, ISBN 0596000200

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

167

167

Bibliografia - Web

- <http://proenca.uel.br/gerencia>
- Network Management, <http://netman.cit.buffalo.edu/>
- **Network Management What it is and what it isn't.** <http://netman.cit.buffalo.edu/Doc/DStevenson/>
- **The SimpleWeb**, <http://www.simpleweb.org/> (official)
- The Internet Engineering Task Force, <http://www.ietf.org/>
- SNMP and IT Management <http://www.snmpworld.com/>
- NOCTools, <http://www.ietf.org/rfc/rfc1470.txt>
- www.consoc.org
- www.ietf.org
- www.itu.org
- www.ieee.org
- www.ifip.org
- www.acm.org
- <http://www.noms.org/> - (Network Operations and Management Symposium)
- <http://penta.ufrgs.br/>
- www.linuxsecurity.org – (segurança)
- www.cert.org – (segurança)
- www.infosyssec.com – (segurança)

03/2021

© Gerência de Redes - Mario Lemes Proença Jr.

168

168