



PUC Minas

Metodologia de Detecção

Motivar/Justificar

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Analogia GRC x Medicina
- Caracterização de Problema
- Detecção
- Coleta de Informações
- Recorrência
- Desenvolvimento, organização e teste de hipóteses
- Solucionando o problema
- Teste da solução
- Documentando

SNMP
v1, v2, v3
Comunidade
OID
Comunidade
Agente

escrever
= escrever

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- Analogia GRC x Medicina
- Caracterização de Problema
- Detecção
- Coleta de Informações
- Recorrência
- Desenvolvimento, organização e teste de hipóteses
- Solucionando o problema
- Teste da solução
- Documentando

Analogia entre GRC e Medicina

Sumário

Introdução

Equipe

Áreas
Funcionais

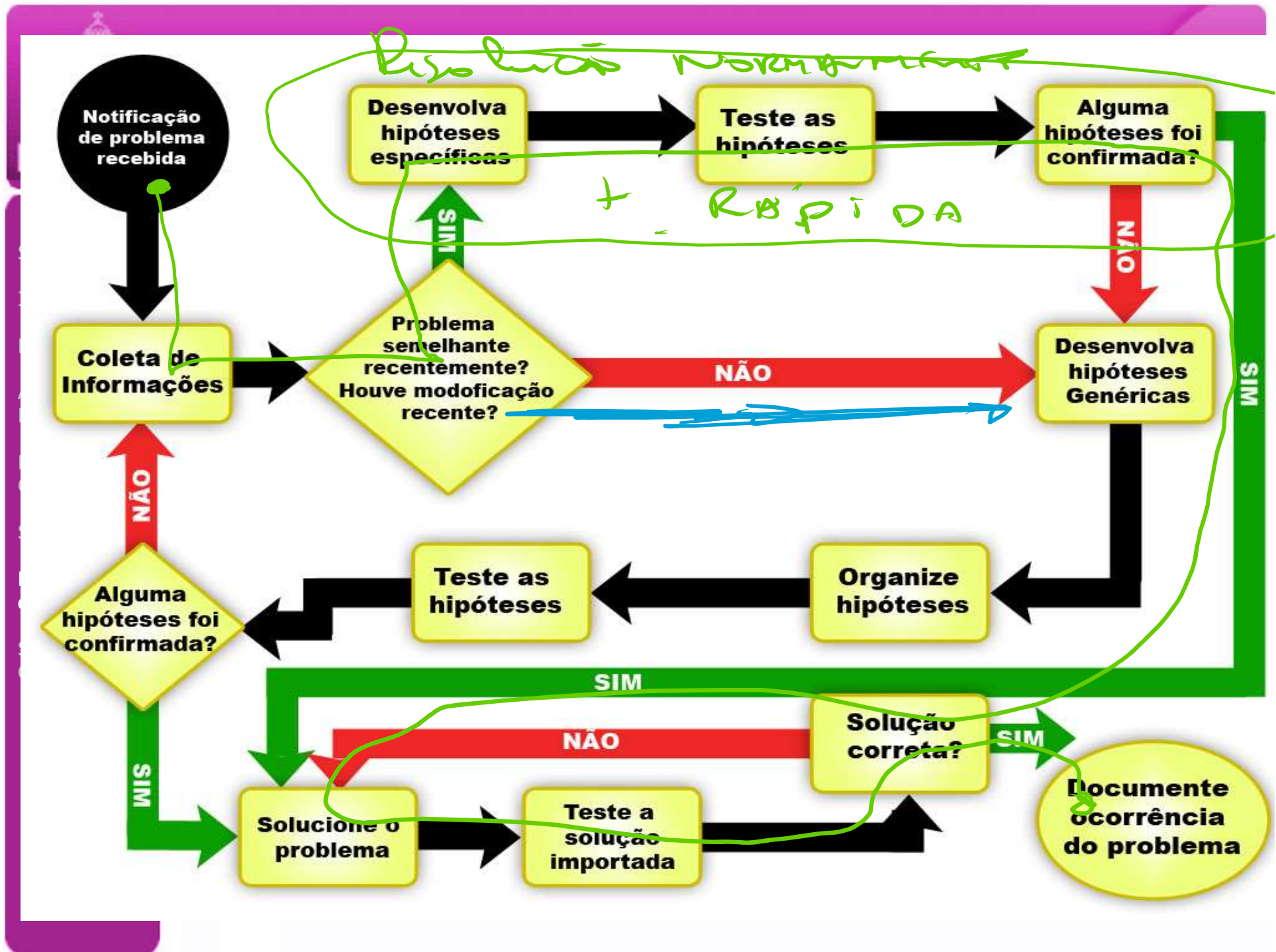
Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

MEDICINA	GERENCIA DE REDES
SINAIS	
Informações sobre o estado/comportamento do paciente obtidas pelo médico através de exames/ou observações	Informações sobre o estado/comportamento da rede obtidas pelo gerenciamento da rede obtidas pelo gerente da rede com o auxílio de instrumentação adequada
SINAIS PATOGNOMÔNICOS	SINAIS DIFERENCIAIS
Sinais cuja existência já confirmam a existência de uma certa doença.	Sinais cuja existência confirmam um certo problema.
TESTES CONFIRMATÓRIOS	
Testes que o médico precisa realizar para chegar ao diagnóstico diferencial quando estiver suspeitando de várias doenças.	Testes que o gerente de redes precisa realizar para confirmar ou negar um ou mais problemas.



Caracterização de um Problema

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

Um problema tem 5 elementos essenciais:

- Descrição
- Sintomas
- Sinais
- Testes confirmatórios
- Sugestões de tratamento

Descrição do Problema

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- Na descrição de um problema serão apresentadas as circunstâncias em que o problema surge.
- Algumas vezes poderão ser apresentadas causas mais comuns e subconjuntos mais específicos deste problema.

Se fosse uma doença, a descrição (resumida) de resfriado seria: processo inflamatório causado por vírus ou por vírus associados a outros microrganismos ou, ainda, de natureza alérgica.



PUC Minas

Sintomas do Problema

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

Os sintomas de um problema informam o que os usuários da rede podem perceber como consequência da existência do problema.

Em outras palavras, os sintomas descrevem o efeito negativo do problema para os usuários.



PUC Minas

Sinais

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- Os sinais são características mais internas da rede que têm seu estado normal alterado em consequência da existência do problema.
- Os sinais geralmente, **não são percebidos pelos usuários, pois geralmente, pois eles só podem ser obtidos com o auxílio de instrumentação adequada**, como estações de gerência, analisadores de protocolos ou outras ferramentas de gerência.
- **São manifestações adicionais, além das manifestações externas que se apresentam aos usuários.**
- Exemplos: taxa de erros elevada, taxa de colisões elevada, requisições ARP sem resposta e resolução de nomes externos não funciona



PUC Minas

Testes Confirmatórios

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- Os testes confirmatórios indicam os passos que devem ser seguidos para confirmar ou negar a existência do problema de rede que está sendo apresentado.
- Quando sinais diferenciais forem encontrados, não será necessário a realização de testes adicionais para confirmar o problema.

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- As sugestões de tratamento são soluções eficientes para o problema descrito.
- O problema que foi confirmado deve ser solucionado o mais rapidamente possível.
- A solução deve ser correta e não introduzir outros problemas na rede.



PUC Minas

Detecção

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

A detecção do problema pode se dar de duas formas:

- Usuário informa problema ao Helpdesk;
- O operador detecta problema.

Obs.: Não é interessante que problemas graves, que levem grande parte da rede a não funcionar, sejam descobertos através dos usuários, quando isso acontece uma das seguintes situações pode estar ocorrendo:

- Não existe ferramenta adequado para monitoramento;
- Os pontos críticos não estão sendo monitorados;
- A equipe não acompanha o gerenciamento.



PUC Minas

Coleta de informações

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

Responda:

- Quem está sendo afetado pelo problema? Apenas um usuário? Todos os usuários? Alguns usuários que fazem parte da mesma sub-rede?
- Quando o problema começou a ser percebido?
- Desde então, o problema ocorre sempre, ou apenas em certos horários? Neste caso, em que horários?
- O problema se manifesta sempre ou apenas quando alguma aplicação e/ou serviço específicos são usados? Neste caso, que aplicações e/ou serviços?
- Alguma mensagem de erro está sendo gerada? Qual?
- O problema é intermitente?

Recorrência de problema ou mudança na rede?

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- Esse problema já ocorreu recentemente?
- Houve alguma mudança recente na rede que possa causar os sintomas detectados?
- Se sim, vá direto ao ponto...
- Desenvolva hipóteses específicas considerando apenas o alvo
- Se, ao testar as hipóteses, detectar que é outro problema, desenvolva hipóteses genéricas (volte na etapa)



PUC Minas

Desenvolva hipóteses

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- Um problema foi detectado, conhecemos os sintomas e sinais reunidos e que partes da rede estão sendo afetadas.
- Com base nestas informações, podemos criar hipóteses sobre que problema pode estar correto.
- Que problemas podem causar os sintomas e sinais percebidos?
- A criação da lista de hipóteses é o primeiro passo para localizar especificamente o problema.
- Para isso é indispensável conhecimento técnico e do ambiente gerenciado.



PUC Minas

Organize Hipóteses

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- Organizar esta lista, já pensando na ordem em que os testes serão feitos.
- Crie um plano de ação, para não cometer erros na fase de testes.
- Classificar os problemas por camada OSI.
- Problemas de uma mesma camada podem também ser organizados por probabilidade de ocorrência ou facilidade de teste.
- A experiência ajudará a organizar esta lista



PUC Minas

Teste as hipóteses

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- Implementar o plano de ação de testes criado na fase anterior
- Para confirmar ou negar as hipóteses use os testes confirmatórios de cada problema
- Caso nenhuma das hipóteses tenha sido confirmada, volte para o passo de busca de informações
- Tente reunir mais informações sobre o problema e em seguida crie novas hipóteses, organize-as. Faça isto até localizar claramente o problema.
- Faça um teste de cada vez



PUC Minas

Solução o problema

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- O problema já foi confirmado, e você deve solucioná-lo no menor prazo de tempo e da melhor forma possível.
- Verifique sua documentação e procure por dicas de como corrigir o problema da forma correta e como evitar que ele ocorra novamente.
- A primeira solução (mais rápida) pode se paliativa.
- A solução definitiva e correta deve ser elaborada.
- Na gerência de redes, todos os problemas tem solução.

Teste a solução implantada

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- Teste a solução implantada, antes de se dar por satisfeito
- Para o teste, use a rede e analise as estatística da estação de gerência.

Documento ocorrência e solução

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

**Metodologia
de Detecção**

Softwares de
Gerência

- Documente as informações iniciais que obteve sobre o problema (o reflexo do problema na rede), as hipóteses levantadas, os testes e as soluções propostas.
- Se teve que voltar na metodologia em busca de novas informações para criar novas hipóteses, documente.
- Mesmo aquilo que não resolveu o problema deve ser documentado, pois ajudará outros (ou você próprio) a não repetir os mesmos erros.



PUC Minas

Softwares de Gerência

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

**Softwares
de Gerência**

- Necessidade
- Exemplos

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

**Softwares
de Gerência**

Um software de gerenciamento não resolve todos os problemas:

- Usuário pode ficar frustrado com os resultados;
- Softwares normalmente são subutilizados;
- Inúmeras características inexploradas;
- Utilizados de modo pouco eficiente;
- Usuários despreparados.

Para gerenciar um recurso, é necessário conhecê-lo bem e entender o que ele representa no contexto da rede.

Necessidade de Gerenciamento

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

**Softwares
de Gerência**

O investimento em um software de gerenciamento se justifica pelos seguintes fatores:

- As redes são vitais para a maioria das organizações.
- O crescimento das redes dificulta o gerenciamento.
- Os usuários esperam uma melhoria dos serviços oferecidos (ou no mínimo, a mesma qualidade).
- Novos recursos são adicionados ou são distribuídos.
- Os sistemas requerem diferentes níveis de suporte nas áreas de desempenho, disponibilidade e segurança.
- Atribuir e controlar recurso para atender de forma balanceada a estas várias necessidades.



PUC Minas

SW de GGRC que usamos na PUC

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

**Softwares
de Gerência**

- Zabbix
- OCS, SNOW
- Gestão X, SOL
- Solar Winds (NetFlox)
- Panorama (lê log do UTM)

Necessidade de Gerenciamento

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

**Softwares
de Gerência**

- Aumento da importância de um recurso, aumenta a sua demanda por **disponibilidade**.
- O sistema deve garantir esta **disponibilidade**.
- A utilização dos recursos deve ser monitorada e controlada para garantir que os usuários estejam satisfeitos a um custo razoável.



PUC Minas

Nagios (1)

Suma

Intro

Equip

Áreas

Funci

Moni

Cont

SNMP

Met

de D

Soft

de G

SWPR34-05		UP	2012-04-19 15:34:08	1d 0h 48m 25s	PING OK - Packet loss = 0%, F
SWPR34-06		UP	2012-04-19 15:33:57	32d 20h 55m 23s	PING OK - Packet loss = 0%, F
SWPR34-07		UP	2012-04-19 15:33:57	32d 20h 45m 23s	PING OK - Packet loss = 0%, F
SWPR34LAB02-01		UP	2012-04-19 15:33:57	32d 20h 30m 22s	PING OK - Packet loss = 0%, F
SWPR34LAB02-02		UP	2012-04-19 15:33:57	32d 20h 30m 22s	PING OK - Packet loss = 0%, F
SWPR34LAB04-01		UP	2012-04-19 15:33:57	32d 20h 30m 27s	PING OK - Packet loss = 0%, F
SWPR34LAB06-01		UP	2012-04-19 15:33:57	32d 20h 25m 27s	PING OK - Packet loss = 0%, F
SWPR34LAB06-02		UP	2012-04-19 15:33:57	32d 20h 24m 56s	PING OK - Packet loss = 0%, F
SWPR38-01		UP	2012-04-19 15:33:59	7d 0h 9m 27s	PING OK - Packet loss = 0%, F
SWPR40-01		UP	2012-04-19 15:33:58	7d 0h 9m 37s	PING OK - Packet loss = 0%, F
SWPR41-01		UP	2012-04-19 15:33:58	7d 0h 9m 27s	PING OK - Packet loss = 0%, F
SWPR42-01		UP	2012-04-19 15:33:58	7d 0h 9m 7s	PING OK - Packet loss = 0%, F
SWPR43-01		UP	2012-04-19 15:34:08	1d 0h 48m 45s	PING OK - Packet loss = 0%, F
SWPR46-01		UP	2012-04-19 15:33:58	7d 0h 9m 7s	PING OK - Packet loss = 0%, F
SWPR46-02		UP	2012-04-19 15:33:57	7d 0h 9m 7s	PING OK - Packet loss = 0%, F
SWPR47-01		UP	2012-04-19 15:33:58	7d 0h 9m 7s	PING OK - Packet loss = 0%, F
SWPR47-02		UP	2012-04-19 15:33:58	10d 3h 3m 37s	PING OK - Packet loss = 0%, F
SWPR49-01		UP	2012-04-19 15:33:58	2d 23h 7m 20s	PING OK - Packet loss = 0%, F
SWPR54-01		UP	2012-04-19 15:33:58	2d 23h 57m 30s	PING OK - Packet loss = 0%, F
SWPR54-02		UP	2012-04-19 15:34:00	7d 0h 8m 57s	PING OK - Packet loss = 0%, F
SWPR54-03		UP	2012-04-19 15:33:57	9d 7h 6m 4s	PING OK - Packet loss = 0%, F
SWPR61-01		UP	2012-04-19 15:33:58	7d 0h 8m 57s	PING OK - Packet loss = 0%, F
SWPR65-01		UP	2012-04-19 15:34:00	7d 0h 9m 37s	PING OK - Packet loss = 0%, F
SWPR80-01		UP	2012-04-19 15:33:59	9d 6h 7m 44s	PING OK - Packet loss = 0%, F



PUC Minas

Nagios (2)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares
de Gerência

Host Information

Last Updated: Thu Apr 19 15:38:43 BRT 2012
Updated every 90 seconds
Nagios® Core™ 3.2.3 - www.nagios.org
Logged in as *nagiosadmin*

[View Status Detail For This Host](#)

[View Alert History For This Host](#)

[View Trends For This Host](#)

[View Alert Histogram For This Host](#)

[View Availability Report For This Host](#)

[View Notifications For This Host](#)

Host
Switch 3Com 4210 - PR47
(SWPR47-02)

Member of
[SWITCHES, all](#)



(Switch 3Com)

Switch da Rede Academica

Host State Information

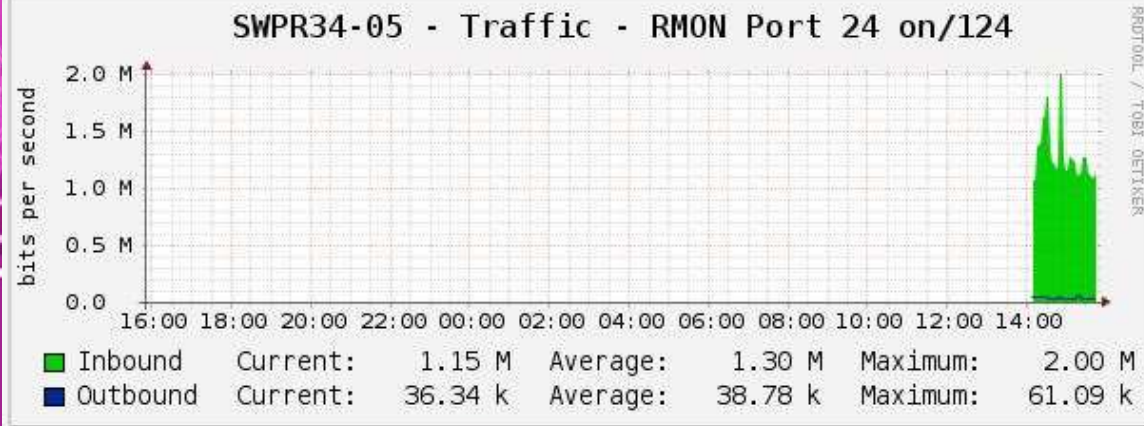
Host Status:	UP (for 10d 3h 7m 15s)
Status Information:	PING OK - Packet loss = 0%, RTA = 12.34 ms
Performance Data:	rta=12.344000ms;5000.000000;5000.000000;0.000000 pl=0%;100;100;0
Current Attempt:	1/10 (HARD state)
Last Check Time:	2012-04-19 15:33:58
Check Type:	ACTIVE
Check Latency / Duration:	1.294 / 0.046 seconds
Next Scheduled Active Check:	2012-04-19 15:39:07
Last State Change:	2012-04-09 12:31:28
Last Notification:	N/A (notification 0)
Is This Host Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	2012-04-19 15:38:37 (0d 0h 0m 6s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED

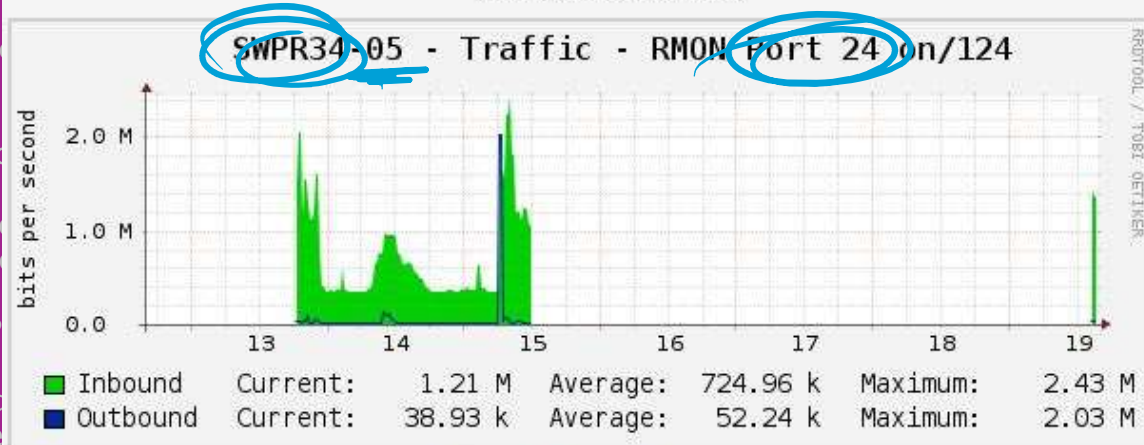
Host Commands

	Locate host on map
	Disable active checks of this host
	Re-schedule the next check of this host
	Submit passive check result for this host
	Stop accepting passive checks for this host
	Stop obsessing over this host
	Disable notifications for this host
	Send custom host notification
	Schedule downtime for this host
	Schedule downtime for all services on this host
	Disable notifications for all services on this host
	Enable notifications for all services on this host
	Schedule a check of all services on this host
	Disable checks of all services on this host
	Enable checks of all services on this host
	Disable event handler for this host
	Disable flap detection for this host

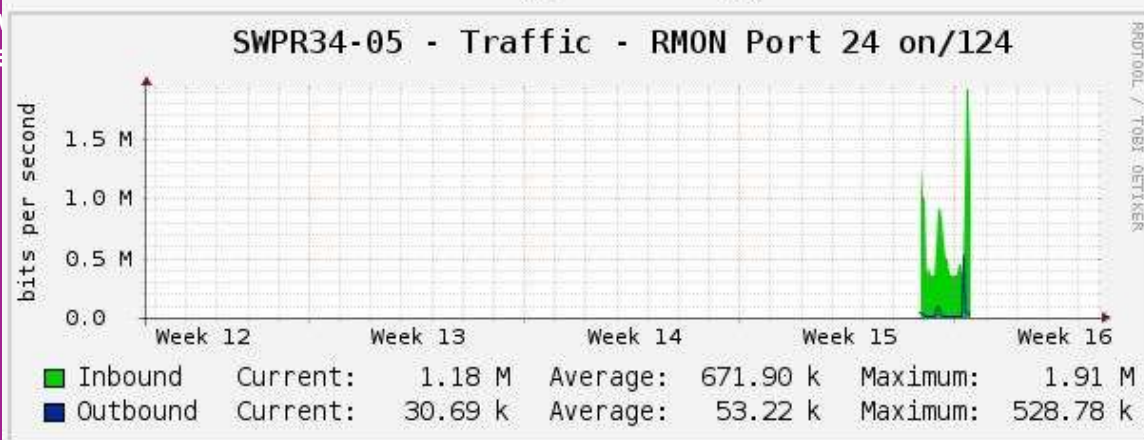
Cacti (1)



Daily (5 Minute Average)



Weekly (30 Minute Average)



Monthly (2 Hour Average)

2008



PUC Minas

Cacti (2)

consolegraphs

Console -> Devices

Logged in as admin (Logout)

Create

New Graphs

Management

Graph Management

Graph Trees

Data Sources

Devices

Collection Methods

Data Queries

Data Input Methods

Templates

Graph Templates

Host Templates

Data Templates

Import/Export

Import Templates

Export Templates

Configuration

Settings

Utilities

System Utilities

User Management

Logout User

Devices

Add

Type: AnyStatus: AnySearch: Rows per Page: 30GoClear

<< Previous

Showing Rows 1 to 6 of 6 [1]

Next >>

Description**	ID	Graphs	Data Sources	Status	Event Count	Hostname	Current (ms)	Average (ms)	Availability	
localhost	1	4	5	Up	0	10.0.1.1	0.04	0.05	100	
SWPR06-01	3	28	28	Up	0	10.0.1.1	28.63	22.17	99.04	
SWPR13-02	4	28	28	Up	0	10.0.1.1	7.07	9.36	98.65	
SWPR34-02	6	28	28	Up	0	10.0.1.1	14.3	11.86	100	
SWPR34-05	2	24	24	Up	0	10.0.1.1	3.35	3.68	99.62	
SWPR41-01	5	28	28	Up	0	10.0.1.1	6.87	7.56	100	

<< Previous

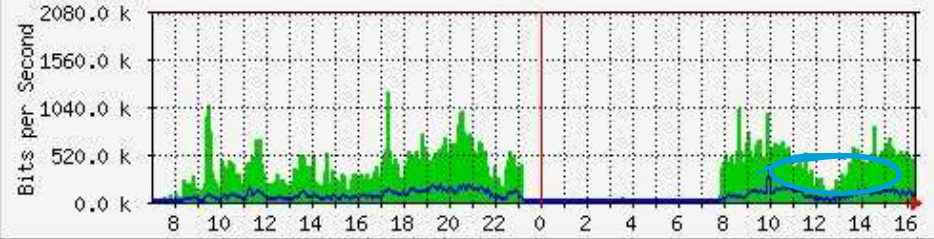
Showing Rows 1 to 6 of 6 [1]

Next >>

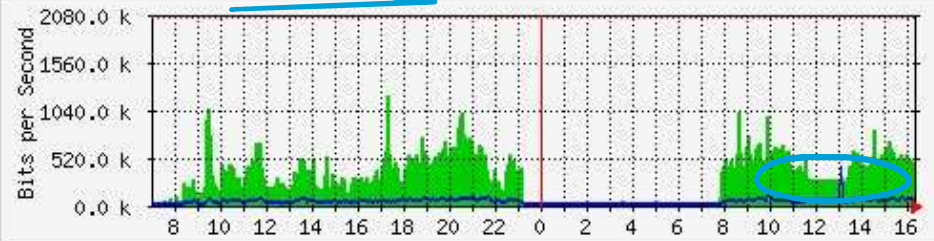
Choose an action: DeleteGo

MRTG (1)

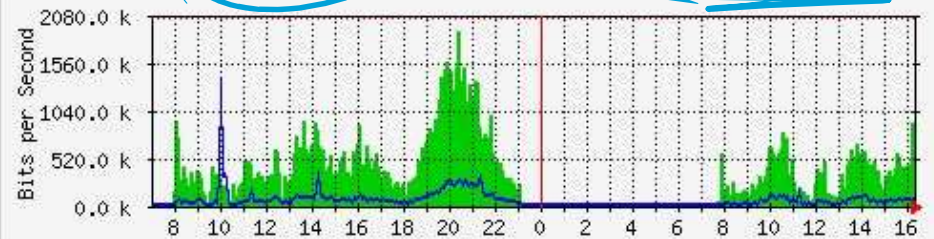
Link PUC <> Barreiro - Circuito BHE 5374843



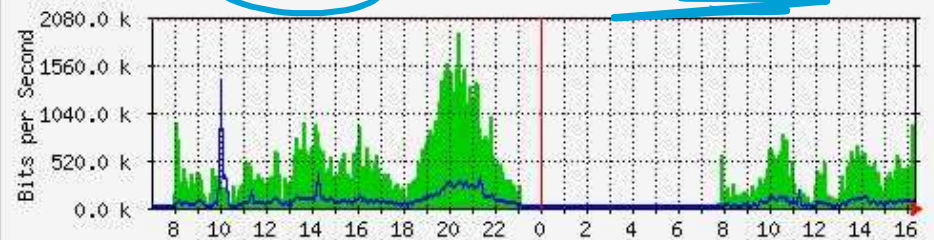
Link PUC <> Barreiro - Circuito BHE 5756438



Link PUC <> Betim - Circuito BET 5022370



Link PUC <> Betim - Circuito BET 5756443



Frame Relay

2 x 2Mbps

PUC Carro

↓
Betim



PUC Minas

Zabbix(1)

ZABBIX

[Help](#) | [Get support](#) | [Print](#) | [Profile](#) | [Logout](#)

[Monitoring](#) | [Inventory](#) | [Reports](#) | [Configuration](#) | [Administration](#)

[Dashboard](#) | [Overview](#) | [Web](#) | [Latest data](#) | [Triggers](#) | [Events](#) | [Graphs](#) | [Screens](#) | [Maps](#) | [Discovery](#) | [IT services](#)

SEARCH:

History: [Latest events](#) » [Custom graphs](#) » [Templates](#) » [Configuration of items](#) » [Custom graphs](#)

GRAPHS



Traffic Port 28

Group Host Graph

Filter

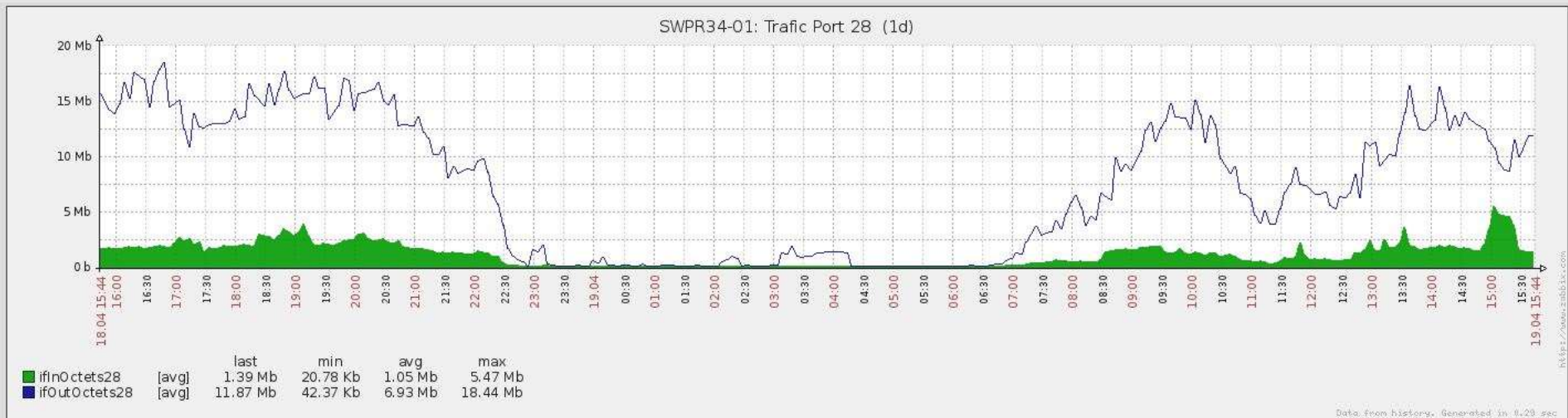
Zoom: [1h](#) [2h](#) [3h](#) [6h](#) [12h](#) [1d](#) [1w](#) [2w](#) [1m](#) [All](#)

18.04.2012 15:40 - 19.04.2012 15:40 (now)



« [1m](#) [1w](#) [1d](#) [12h](#) [1h](#) | [1h](#) [12h](#) [1d](#) [1w](#) [1m](#) »

01d 00h 00m (fixed)





PUC Minas

Zabbix (2)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares
de Gerência

ZABBIX Help

[Monitoring](#) [Inventory](#) [Reports](#) [Configuration](#) [Administration](#)

[Dashboard](#) [Overview](#) [Web](#) [Latest data](#) [Triggers](#) [Events](#) [Graphs](#) [Screens](#) [Maps](#) [Discovery](#) [IT services](#)

History: Custom graphs » Templates » Configuration of items » Custom graphs » Latest events

HISTORY OF EVENTS ON 19 Apr 2012, 15:45:06

EVENTS Group: Host:

Displaying 1 to 5 of 5 found Filter

Time	Description	Status	Severity	Duration	Ack
18 Apr 2012 14:58:24	icmping	OK	High	1d 46m	No
18 Apr 2012 14:48:24	icmping	PROBLEM	High	10m	No
17 Apr 2012 21:58:24	icmping	OK	High	16h 50m	No
16 Apr 2012 08:43:24	icmping	PROBLEM	High	1d 13h 15m	No
13 Apr 2012 17:23:24	icmping	OK	High	2d 15h 20m	No

7 10



PUC Minas

Zabbix (3)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

**Softwares
de Gerência**



ZABBIX

Monitoring | Inventory | Reports | Configuration | Administration

Dashboard | Overview | Web | Latest data | Triggers | Events | Graphs | Screens | Maps | Discovery | IT service



History: Custom graphs » Templates » Configuration of items » Custom graphs » Latest events

PERSONAL DASHBOARD

Favourite graphs  



...

Graphs »

Favourite screens  



...

Screens »

Favourite maps  



...

Maps »

Status of Zabbix  



Parameter	Value	Details
Zabbix server is running	Yes	127.0.0.1:10051
Number of hosts (monitored/not monitored/templates)	98	6 / 1 / 51
Number of items (monitored/disabled/not supported)	1048	424 / 410 / 214
Number of triggers (enabled/disabled)[problem/unknown/ok]	416	134 / 282 [0 / 98 / 36]
Number of users (online)	4	3
Required server performance, new values per second	3.67	-

Updated: 15:45:37

System status  

Host group	Disaster	High	Average	Warning	Information	Not classified
SW-PMG	0	0	0	0	0	0
Windows servers	0	0	0	0	0	0

Updated: 15:45:37

Host status  

Host group	Without problems	With problems	Total
SW-PMG	45	0	45
Windows servers	1	0	1

Updated: 15:45:37