

Capítulo 6 – Gerência de Redes de Computadores



Um dia, um homem resolveu
dar asas a sua imaginação,
superar desafios e provou que
o Conhecimento não tem limite.



Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Introdução
- Equipe de Gerência
- Áreas Funcionais
- SNMP
- Monitoração e Controle
- Metodologia de Detecção
- Softwares de Gerência



Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Gerência de Redes de Computadores
- SNMP x CMIP
- Recursos Humanos
- Arquitetura de Gerência
- Mercado
- Recursos Gerenciados
- Necessidade de Gerenciamento



PUC Minas

Gerência de Redes

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

“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 serviços em tempo real a um custo razoável.”

T. Saydam & T. Magedanz. “From Networks and Network Management into Service and Service Management”. Journal of networks and system management, 1996.





PUC Minas

Gerência de Redes

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

A gerência de redes nasceu da necessidade de monitoração e controle dos dispositivos da rede.

- Atualmente, as redes e seus serviços são fundamentais, de tal forma, que eles **“não podem falhar”**.
- O nível de falhas e de **degradação de desempenho aceitáveis está diminuindo, chegando a zero**, dependendo da importância da rede para uma instituição.



SNMP (Simple Network Manag. Protocol):

- Protocolo
- Especificação de estrutura de dados;
- Um conjunto de objetos de dados.

Sistemas de gerenciamento OSI:

- Conhecido como CMIP (ISO 1991)
- Conjunto de padrões de grande complexidade,
- Devido a lentidão de padronização, não é muito popular.



PUC Minas

Recursos Humanos

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- A implementação de um sistema de gerenciamento pode significar um aumento da equipe
- Aumento da carga de manutenção e operação do ambiente
- Pode haver necessidade de plantões
- O tamanho da equipe vai variar de acordo com o porte e a complexidade da rede gerenciada



Human Resources



PUC Minas

Arquitetura

Sumário

Introdução

Equipe

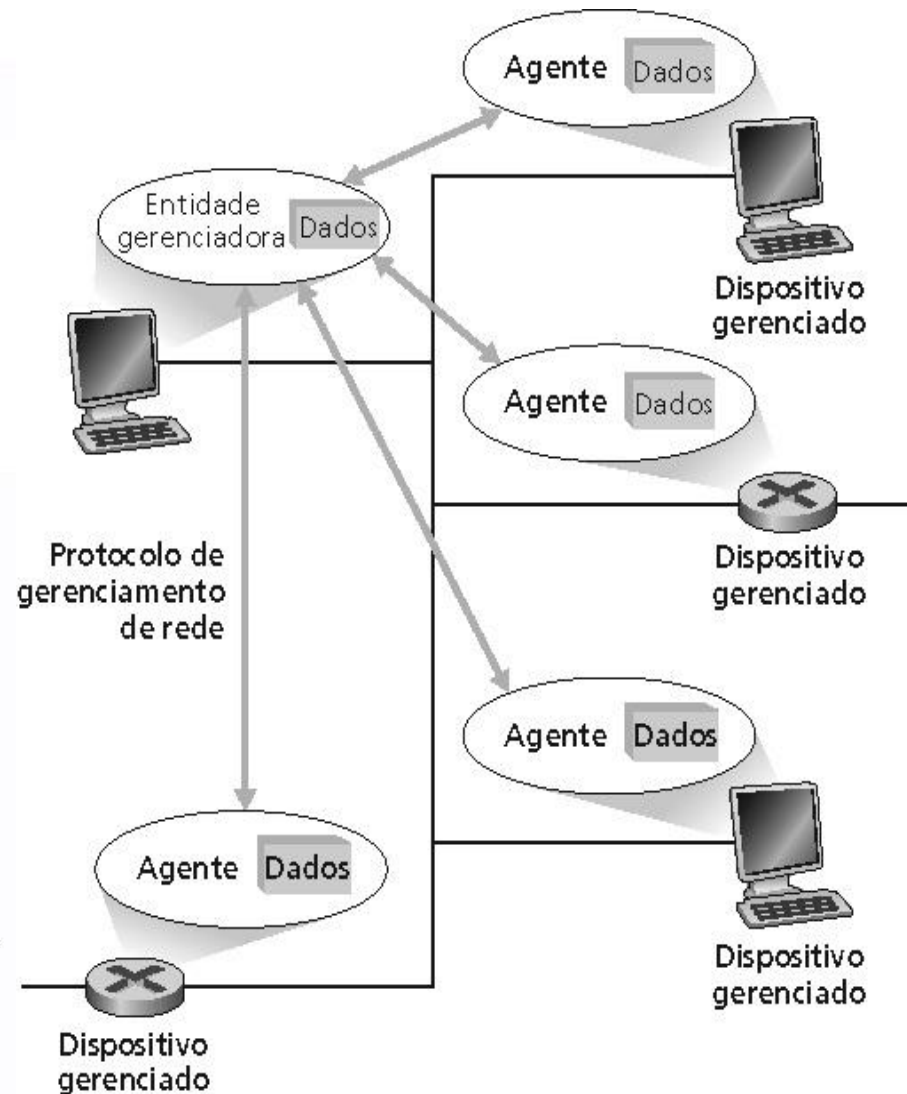
Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência





A solução de gerência de redes mais usada:

- Internet-standard Network Management Framework.
- **Esta solução é mais conhecida como gerência SNMP, este padrão descreve:**
 - O protocolo de gerência
 - Um conjunto de regras para definir as informações de gerência e um conjunto inicial de informações de gerência a ser utilizada.



Recursos Gerenciados (1)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

A estação de gerência obtém informações como:

- taxa erros
- estado operacional de enlaces e equipamentos
- utilização de enlace, etc.

“ Tão importante quanto obter estas informações é saber interpretá-las. Por exemplo, a taxa de erros de um certo enlace é 1%. Esta é uma taxa de erros aceitável?”



Recursos Gerenciados (2)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

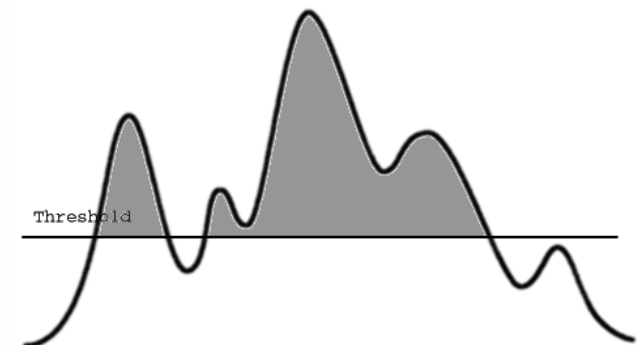
Softwares de
Gerência

Para muitas informações de gerência, são estabelecidos limites.

Se o valor que coletamos é maior/menor que o limite estabelecido, inferimos que algo anormal está acontecendo.

Chamamos estes limites de thresholds.

“Limiares excedidos podem gerar alarmes na estação de gerência”





Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- **Toda rede deve ser gerenciada;**
- Garantir disponibilidade de serviços com desempenho aceitável;
- Redes grandes requerem automatização de monitoração e controle.



Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- A equipe de GRC
- Helpdesk
- Operador
- Suporte Técnico
- Gerente de Equipe



PUC Minas

A equipe de gerência de redes

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

Objetivo:

- Prevenir e solucionar problemas na rede.
- Vários níveis de profissionais.
- Quatro tarefas distintas:
 - Helpdesk*,
 - Operadores (de rede),
 - Suporte técnico,
 - Gerência da equipe,

*Não faz parte efetivamente da equipe de gerência de redes.



Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Atende chamadas telefônicas;
- Tem certo grau de conhecimento;
- Lidam com problemas já reportados;
- Composto por pessoas pouco especializadas;
- Auxiliadas por aplicações para gerenciar problemas reportados;
- Incluir novo problema
- Ver estado de problemas
- **Criticidade**





Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Acompanhar os alarmes gerados pela estação de gerência.
- Quando, por exemplo, um equipamento passa para o estado não operacional, o operador perceberá um alarme na estação de gerência.

Alarmes podem ser informados de diversas formas:

- mudança de cores no mapa da rede;
 - e-mail;
 - celular, etc.
- Ao perceber um problema, tenta resolvê-lo ou o encaminha à equipe de suporte técnico.



PUC Minas

Suporte Técnico

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- É quem põe a mão na massa.
- Deve solucionar os problemas que não foram solucionados pela equipe de helpdesk nem pelo operador (do sistema de gerência).
- Responsável pela configuração, operação e manutenção dos equipamentos da rede.
- Este time deve possuir alto nível de conhecimento





Gerente da Equipe (1)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- O gerente da equipe de gerência de rede não é, necessariamente, um expert técnico em redes.
- Deve ter conhecimento em redes, mas não necessariamente no nível do suporte técnico.
- Deve avaliar o desempenho da sua equipe, para tanto usa as métricas, tais como:
 - Tempo médio entre falhas;
 - Tempos médio para correção de falhas;
 - Percentual de problemas resolvidos em menos de 1h;
 - Entre outros.



PUC Minas

Gerente de Equipe (2)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Solicita compra de equipamentos, aplicações ou outros recursos, quando necessário;
- Providencia treinamento;
- Encaminha os problemas para outros membros da equipe, quando a solução demora, etc.





PUC Minas

Áreas Funcionais

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Gerência de Configuração;
- Gerência de Falhas;
- Gerência de Desempenho;
- Gerência de Segurança;
- Gerência de Contabilidade;



PUC Minas

Áreas funcionais de gerência

Sumário

Introdução

Equipe

Áreas Funcionais

Monitoração e Controle

SNMP

Metodologia de Detecção

Softwares de Gerência

O modelo OSI define 5 áreas de gerenciamento (modelo funcional denominado FCAPS).

- Gerenciamento de falhas (Fault)
- Gerenciamento de configuração (Configuration)
- Gerenciamento de contabilização (Accounting)
- Gerenciamento de desempenho (Performance)
- Gerenciamento de segurança (Security)

A gerência de redes abrange estas cinco áreas funcionais.

Em ordem decrescente de importância estas áreas são (ISO/IEC 7498, 2007)...





Gerência de Configuração (1)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- É responsável pela configuração inicial da rede, descobrimento de topologia, manutenção e monitoração de mudanças a sua estrutura física e lógica.
- Do ponto de vista do usuário, é a área mais importante da gerência, uma vez que se a rede não estiver configurada apropriadamente ela não irá funcionar ou poderá funcionar apresentando muitas falhas.



Gerência de Configuração (2)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Inicialização da rede
- Adição e atualização de componentes e do status dos componentes.
- Alguns recursos podem ser configurados para executar diferentes serviços como, por exemplo, um equipamento pode atuar como roteador, como estação de trabalho ou ambos.
- Decidido como o equipamento deve ser usado, o gerente de configuração escolhe o sw e um conjunto de valores coletados.



Gerência de Configuração (3)

Sumário

Introdução

Equipe

Áreas Funcionais

Monitoração e Controle

SNMP

Metodologia de Detecção

Softwares de Gerência

- Identificar os componentes da rede e definir a conectividade entre eles.
- Também deve ser capaz de modificar a configuração em resposta às avaliações de desempenho, recuperação de falhas, problemas de segurança, atualização da rede ou a fim de atender à necessidades dos usuários.
- Relatórios de configuração podem ser gerados periodicamente ou em resposta às requisições de usuários.



Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

Funções básicas:

- Coletar informações da topologia de rede;
- Controlar inventário;
- Iniciar e encerrar as operações dos elementos gerenciados;
- Alterar a configuração dos elementos gerenciados;
- Gerar relatórios de configuração;



Gerência de Falhas (1)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Refere-se à detecção, diagnóstico e correção de falhas na rede.
- Esta é a segunda área de gerência mais importante e quando bem planejada, além de solucionar problemas atuais, pode evitar a ocorrência de falhas futuras;



Gerência de Falhas (2)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Falha não é o mesmo que erro
- Uma falha é uma condição anormal cuja recuperação exige ação de gerenciamento.
- Uma falha normalmente é causada por operações incorretas ou um número excessivo de erros.



Gerência de Falhas (3)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Para controlar o sistema como um todo, **cada componente essencial deve ser monitorado individualmente** para garantir o seu perfeito funcionamento.
- O impacto e a duração do estado de falha pode se minimizado pelo uso de componentes redundantes e rotas de comunicação alternativas, para dar à rede um grau de **"tolerância a falhas"**.



Gerência de Falhas (4)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

Quando ocorre uma falha, é importante que seja possível, rapidamente:

- Determinar com precisão onde a falha ocorreu;
- Isolar o resto da rede da falha, de tal forma que ela continue a funcionar sem interferências;
- Reconfigurar ou modificar a rede para minimizar o impacto da operação sem o componente que falhou;
- Reparar ou trocar o componente com problemas para restaurar a rede ao seu estado anterior.



Gerência de Desempenho (1)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Monitora o desempenho da rede, analisa-o para identificar problemas e permite planejamento de capacidade.
- Juntamente com a gerência de segurança é considerada a terceira mais importante área da gerência de redes

Ela basicamente monitora a rede e calcula índices de desempenho tais como utilização de tempo e de resposta em vários pontos de rede.



Gerência de Desempenho (2)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- O gerenciamento do desempenho de uma rede consiste na monitoração das atividades da rede e no controle dos recursos através de ajustes e trocas. Algumas das questões relativas ao gerenciamento do desempenho, são:
 - Qual é o nível de capacidade de utilização?
 - O tráfego é excessivo?
 - Existem gargalos?
 - O tempo de resposta está aumentando?



Gerência de Desempenho (3)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Para tratar estas questões, o gerente deve focalizar um conjunto inicial de recursos a serem monitorados, a fim de estabelecer níveis de desempenho. Isto inclui associar métricas e valores apropriados aos recursos de rede que possam fornecer indicadores de diferentes níveis de desempenho.
- **Muitos recursos devem ser monitorados para se obter informações sobre o nível de operações da rede.**



Gerência de Desempenho (4)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Coleccionando e analisando estas informações, o gerente da rede pode ficar mais e mais capacitado no reconhecimento de situações indicativas de degradação de desempenho.
- Estatísticas de desempenho podem ajudar no planejamento, administração e manutenção de grandes redes. Estas informações podem ser utilizadas para reconhecer situações de gargalo antes que elas causem problemas para o usuário final.
- Ações corretivas podem ser executadas, tais como, trocar tabelas de roteamento para balancear ou redistribuir a carga de tráfego durante horários de pico, ou ainda, a longo prazo, indicar a necessidade de expansão de linhas para uma determinada área.



Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Ações corretivas podem ser executadas, tais como, trocar tabelas de roteamento para balancear ou redistribuir a carga de tráfego durante horários de pico, ou ainda, a longo prazo, indicar a necessidade de expansão de linhas para uma determinada área.



PUC Minas

Gerência de Segurança (1)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

Protege os elementos da rede, monitorando e detectando violações da política de segurança estabelecida, isto é, trata de manter os dados de uma organização nas mãos das pessoas certas, ou ainda não os deixa chegar nas mãos das pessoas erradas;





Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Provê facilidades para proteger os recursos da rede e informações dos usuários.
- Estas facilidades devem estar disponíveis apenas para usuário autorizados.
- É necessário que a política de segurança seja robusta e efetiva e que o sistema de gerenciamento da segurança seja, ele próprio, seguro.



Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

Trata questões como:

- Geração, distribuição e armazenamento de chaves de criptografia;
- Manutenção e distribuição de senhas e informações de controle de acesso;
- Monitoração e controle de acesso à rede ou parte da rede e às informações obtidas dos nodos da rede;
- Coleta, armazenamento e exame de registros de auditoria e logs de segurança, bem como ativação e desativação destas atividades.



Abrangência:

- Controle de serviços
- Garantir que a política de segurança seja seguida em conformidade;
- Controlar acesso à rede ou parte da rede e às informações obtidas dos nodos da rede;
- Coletar, armazenar e examinar os registros de auditoria e logs de segurança, bem como ativação e desativação destas atividades.



PUC Minas

Gerência de Contabilização (1)

Sumário

Introdução

Equipe

Áreas Funcionais

Monitoração e Controle

SNMP

Metodologia de Detecção

Softwares de Gerência

- É responsável por contabilizar e verificar a utilização dos recursos da rede por seus usuários, levando em consideração a divisão de contas feita por usuários ou grupos de usuários



Accounting



PUC Minas

Gerência de Contabilização (2)

Sumário

Introdução

Equipe

**Áreas
Funcionais**

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

O administrador de rede deve estar habilitado a controlar o uso dos recursos por usuário ou grupo de usuários, com o objetivo de:

- Evitar que um usuário **abuse de seus privilégios de acesso e monopolize a rede**, em detrimento de outros usuários;
- Evitar que usuários façam uso ineficiente da rede, assistindo-os na troca de procedimentos e **garantindo o desempenho da rede**.
- **Conhecer as atividades dos usuários** com detalhes suficientes para planejar o crescimento da rede.
- Deve ser capaz de especificar os tipos de informações de contabilização que devem ser registrados em cada nodo, o intervalo de entrega de relatórios para nodos de gerenciamento de mais alto nível e os algoritmos usados no cálculo da utilização.



Sumário

Introdução

Equipe

Áreas
Funcionais

**Monitoração
e Controle**

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Funções de Gerenciamento
- Monitoração
- Controle
- Resumo



PUC Minas

Funções de Gerenciamento

Sumário

Introdução

Equipe

Áreas
Funcionais

**Monitoração
e Controle**

SNMP

Metodologia
de Detecção

Softwares de
Gerência

As funções de gerenciamento de rede podem ser agrupadas em duas categorias:

Monitoração de rede e controle de rede.

- A monitoração da rede está relacionada com a tarefa de observação de seus componentes; é uma função de “leitura”.
- O controle da rede é uma função de “escrita” e está relacionada com a tarefa de alteração de valores de parâmetros e execução de determinadas ações.



Monitoração (1)

Sumário

Introdução

Equipe

Áreas
Funcionais

**Monitoração
e Controle**

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Consiste na observação de informações relevantes ao gerenciamento, classificadas em três categorias:
 - **Estática:** Caracteriza a configuração atual e os elementos na atual configuração, tais como o número e identificação de portas em um roteador.
 - **Dinâmica:** Relacionada com os eventos na rede, tais como a transmissão de um pacote na rede.
 - **Estatística:** Pode ser derivada de informações dinâmicas; ex. Média de pacotes por unidade de tempos em um determinado sistema.



Sumário

Introdução

Equipe

Áreas
Funcionais

**Monitoração
e Controle**

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- A informação de gerenciamento é coletada e armazenada por agentes e repassada para um ou mais gerentes.
- Duas técnicas podem ser utilizadas na comunicação entre agentes e gerentes: **polling e event-reporting**.
- A técnica de **polling** consiste em uma interação do tipo **request/response**.
 - O gerente pode solicitar a um agente o envio de valores de diversos elementos de informação.
 - O agente responde com os valores constantes em sua MIB



- Na técnica de **event-reporting**, a iniciativa é do agente.
 - O gerente fica na escuta, esperando pela chegada de informações.
 - Um agente pode gerar um relatório periodicamente para fornecer ao gerente o seu estado atual.
 - A periodicidade do relatório pode ser configurada previamente pelo gerente.
 - Um agente também pode enviar um relatório quando ocorre um evento significativo ou não usual.



Sumário

Introdução

Equipe

Áreas
Funcionais

**Monitoração
e Controle**

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Tanto o **polling** quanto o **event-reporting** são usados nos sistemas de gerenciamento, porém a ênfase dada a cada um dos métodos difere muito entre sistemas.
- Em sistemas de gerenciamento de redes de telecomunicações, a ênfase maior é dada para o método de **event-reporting**.
- Em contraste, o modelo **SNMP** dá **pouca importância ao event-reporting**. O modelo OSI fica entre estes dois extremos.



A escolha da ênfase depende dos seguintes fatores:

- A quantidade de tráfego gerada por cada método;
- Robustez em situações críticas;
- O tempo entre ocorrência do evento e a notificação ao gerente;
- A quantidade de processamento nos equipamentos gerenciados;
- A problemática referente à transferência confiável versus transferência não confiável;
- As aplicações de monitoração de rede suportadas;
- As considerações referentes ao caso em que um equipamento falhe antes de enviar um relatório.



Sumário

Introdução

Equipe

Áreas
Funcionais

**Monitoração
e Controle**

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Refere-se à modificação de parâmetros e à execução de ações em um sistema remoto. Todas as cinco áreas funcionais de gerenciamento (falhas, desempenho, contabilização, configuração e segurança), envolvem monitoração e controle.
- A ênfase nas três primeiras destas áreas, tem sido na monitoração, enquanto que nas duas últimas, o controle tem sido mais enfatizado.



Sumário

Introdução

Equipe

Áreas
Funcionais

**Monitoração
e Controle**

SNMP

Metodologia
de Detecção

Softwares de
Gerência

O controle de configuração inclui as seguintes funções:

- Definição da informação de configuração – recursos e atributos dos recursos sujeitos ao gerenciamento
- Atribuições e modificação de valores de atributos;
- Definição e modificação de relacionamentos entre recursos ou componentes da rede;
- Inicialização e terminação de operações de rede;
- Distribuição de software;
- Exame de valores e relacionamentos;
- Relatórios de status de configuração;



Sumário

Introdução

Equipe

Áreas
Funcionais

**Monitoração
e Controle**

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- O controle de segurança é relativo à segurança dos recursos sob gerenciamento, incluindo o próprio sistema de gerenciamento.
- Os principais objetivos em termos de segurança, são relativos à confidencialidade, integridade e disponibilidade.
- **As principais ameaças à segurança referem-se à interrupção, interceptação, modificação e mascaramento.**



Sumário

Introdução

Equipe

Áreas
Funcionais

**Monitoração
e Controle**

SNMP

Metodologia
de Detecção

Softwares de
Gerência

As funções de gerenciamento de segurança podem ser agrupadas em três categorias:

- manutenção da informação de segurança
- controle de acesso aos recursos
- controle do processo de criptografia



Sumário

Introdução

Equipe

Áreas
Funcionais

**Monitoração
e Controle**

SNMP

Metodologia
de Detecção

Softwares de
Gerência

Classificação da informação

- Estática (ex. A localização e o responsável por um determinado equipamento)
- Dinâmica (ex. Estado de uma interface de rede)
- Estatística (ex. Quantidade média de pacotes transmitidos por hora)

Técnicas para coleta de informações

- Polling e Event Reporting

Controle de redes

- Controle de configuração (ex. Distribuição de sw)
- Controle de segurança
- Tipos de ameaças



Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- O que é? Para que serve?
- SMI e MIB
- RFC e Outras Mibs
- Gerentes e Agentes
- Host resource MIB
- UDP
- Comunidades
- OID
- Operações
- SNMPv3
- RMON



Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- **Simple Network Management Protocol (SNMP)** é um protocolo de gerenciamento de dispositivos que atua na camada de aplicação da pilha TCP/IP.
- O SNMP foi lançado em 1988 para atender a necessidade crescente de padronização do gerenciamento de dispositivos IP.
- Sucedeu o Simple Gateway Management Protocol (SGMP) anteriormente definido na RFC 1028 de 1987 que tinha sido desenvolvido para gerenciar roteadores da Internet.



Para que serve?

- **Apesar de ter sido desenvolvido, inicialmente, para gerenciar dispositivos de rede, pode gerenciar sistemas (Unix, Windows, Linux,...), impressoras, modem, fontes de energia e muito mais.**
- É possível gerenciar qualquer dispositivo que execute um software (agente) que permita a recuperação de informações de acordo com o protocolo SNMP. Isso inclui não só dispositivos de hardware, mas softwares como SGBDs, servidores web e de aplicações.



Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

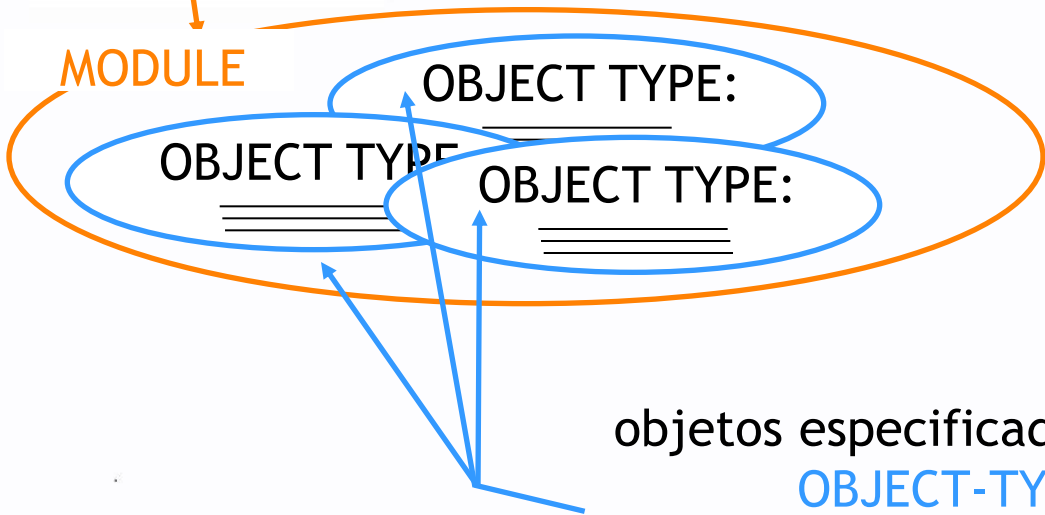
Softwares de
Gerência

- Um agente tem uma lista dos objetos por ele suportados (exemplos: status da interface do roteador, taxa de utilização do processador, memória disponível)
- Management Information Base (MIB) é **uma base de dados de objetos gerenciados que o agente tem acesso**
- A MIB é uma base de dados, cuja estrutura é especificada pelo padrão SMI



- Sumário
- Introdução
- Equipe
- Áreas Funcionais
- Monitoração e Controle
- SNMP**
- Metodologia de Detecção
- Softwares de Gerência

Um módulo MIB é especificado pela SMI como:
MODULE-IDENTITY
(100 MIBs padronizadas, mais proprietárias)





PUC Minas

Structure of Management Information (SMI)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- São as regras para se definir objetos gerenciados e respectivos comportamentos
- **Todo tipo de informação solicitado pela NMS, como status e/ou estatísticas, são definidos em uma MIB**
- Um agente pode implementar algumas ou **várias MIBs**, mas todos implementam uma específica chamada MIB-II (RFC 1213)



- Internet Engineering Task Force (IETF) é responsável pela definição de protocolos padrão que controlam o tráfego na Internet, o que inclui o SNMP.
 - SNMPv1 RFC 1157
 - SNMPv2 RFC 1905, RFC 1906, RFC 1907
 - SNMPv3 RFC 2571, 3410, 3414
 - <http://www.ietf.org/rfc.html>



Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Um fornecedor pode definir uma MIB exclusiva como um diferencial para o seu produto
- Essas MIBs podem oferecer informações mais consistentes para o gerenciamento do dispositivo do fabricante que não estão cobertas na MIB padrão
- O carregamento de uma nova MIB na NMS não garante que as informações serão fornecidas pelo agente.
- O agente só fornece as informações para as quais ele foi programado, portanto procure as MIBs fornecidas pelo fabricante do dispositivo



Gerentes e Agentes

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Network Management Station (NMS) solicita informações continuamente dos agentes (polling)
- O agente responde à solicitação da NMS
- A NMS recebe traps enviados por agentes a qualquer momento
- Traps assíncronos informam se algo aconteceu no dispositivo
- O agente pode ser implementado como um serviço (daemon) ou como parte do sistema operacional



PUC Minas

Host Resource MIB (1)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- A host resource MIB fornece um conjunto de objetos para auxiliar o gerenciamento de recursos dos diversos sistemas operacionais
- Informações como capacidade de disco, processos em execução, números de usuários concorrentes, podem ser definidas nessa MIB
- Host resource MIB está definida na RFC 2790



Host Resource MIB (2)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- A Host Resource MIB é importante para o gerenciamento da rede, mas nem todo agente implementa essa MIB
 - hrSystem: Objetos pertencentes ao sistema
 - hrStorage e hrDevice: armazenamento e sistemas de arquivos
 - hrSWRun: Softwares em execução
 - hrSWRunPerf: Aspectos de desempenho de softwares
 - hrSWInstalled: Softwares instalados



O SNMP usa o UDP como protocolo de transporte:

- Utiliza a porta 161 para envio e recebimento de informações
- Utiliza a porta 162 para recebimento de traps de dispositivos gerenciados

O recebimento de traps não é confirmado, na versão 2 no v3 existe o INFORM.



Comunidades (1)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- O SNMPv1 e SNMPv2 usa o conceito de comunidades para definir uma certa confiabilidade entre estação de gerência (NMS) e o agente.
- Um agente é configurado com três nomes de comunidade associadas a: read-only, read-write e trap.
- Se a NMS informa a comunidade read-only, terá acesso somente de leitura podendo, portanto, solicitar informações do agente, mas não enviar informações a ele.



Comunidades (2)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Informando a **string (comunidade)** read-write é possível enviar uma solicitação de alteração ao agente
- A string associada à permissão de trap possibilita que a NMS receba as notificações enviadas pelo agente
- Como as strings de comunidade trafegam como texto livre, isso facilita a interceptação dessas strings
- **SNMPv3 trata disso**



- SMIV1 (RFC 1155) define exatamente como os objetos gerenciados são nomeados e especifica os respectivos tipos de dados.
- A definição dos objetos gerenciados pode ser dividida em três partes:
 - Nome ou identificadores do Objeto (OID – Objeto Identifier): Define exclusivamente um objeto gerenciado.
 - Tipo e sintaxe: Definida em Abstract Syntax Notation One (ASN.1)
 - Codificação: Codificada em Basic Encoding Rules (BER)



Sumário

Introdução

Equipe

Áreas

Funcionais

Monitoração e
Controle

SNMP

Metodologia de
Detecção

Softwares de
Gerência

1.3.6.1.2.1.7.5
porta em

Object ID

Nome

Tipo

Comentários

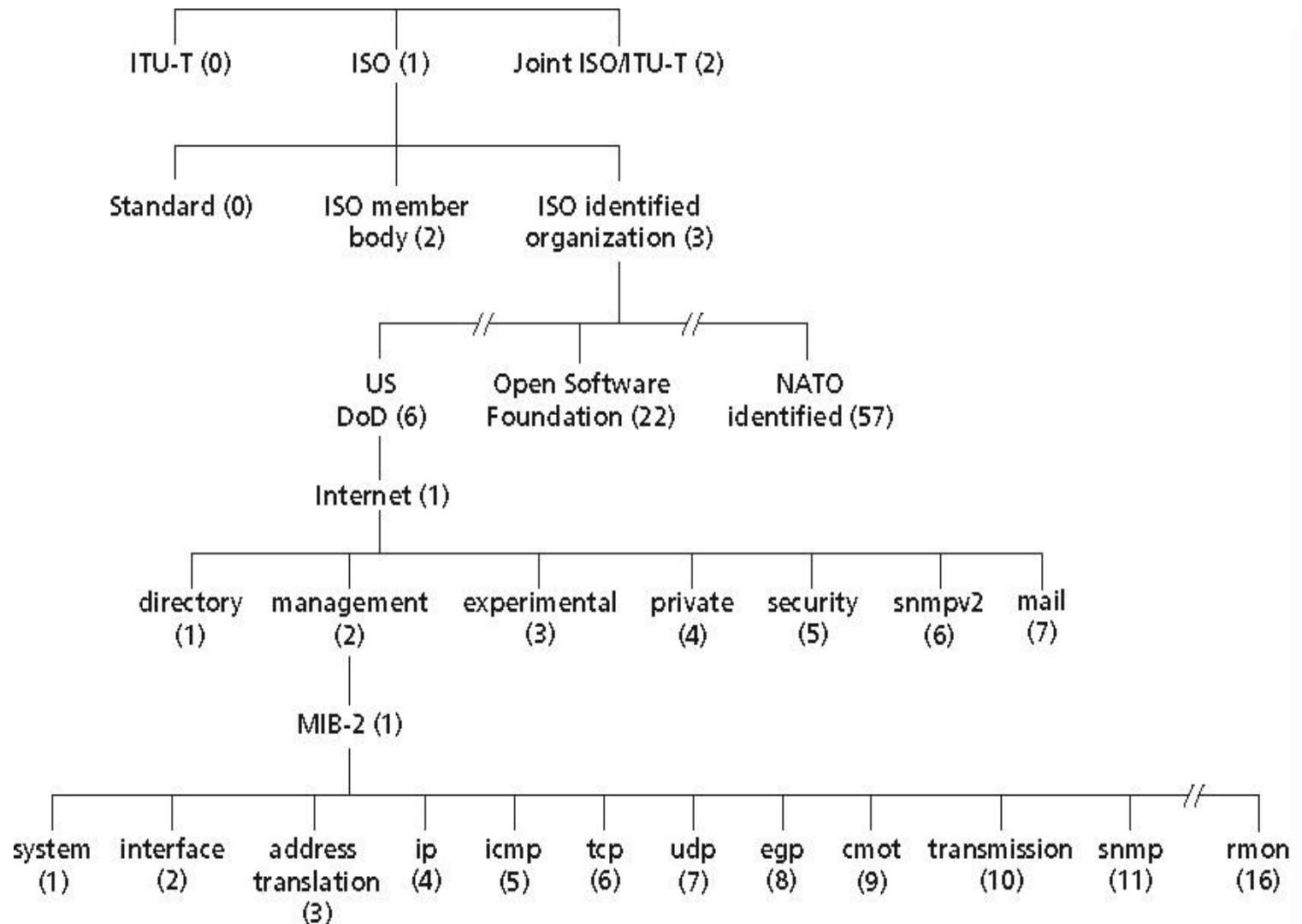
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	número total de datagramas entregues neste nó
-----------------	----------------	-----------	---

1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	número de datagramas com app destino inexistente
-----------------	------------	-----------	--

1.3.6.1.2.1.7.3	UDPInErrors	Counter32	número de datagramas não entregues por outras razões
-----------------	-------------	-----------	--

1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	número de datagramas enviados
-----------------	-----------------	-----------	-------------------------------

1.3.6.1.2.1.7.5	udpTable	SEQUENCE	uma linha para cada uso por uma aplicação fornece o número da porta e o endereço IP
-----------------	----------	----------	---





- Existe um formato (PDU) padrão para cada operação:
 - get
 - get-next
 - get-bulk (SNMPv2 e SNMPv3)
 - set
 - get-response
 - trap
 - notification (SNMPv2 e SNMPv3)
 - inform (SNMPv2 e SNMPv3)
 - report (SNMPv2 e SNMPv3)



Operações - Trap (2)

Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

- Um meio do agente informar a NMS que aconteceu algo errado.
- Existem 6 tipos genéricos de trap:
 - coldStart(0)
 - warmStart(1)
 - linkDown (2)
 - linkUP (3)
 - authenticationFailure(4)
 - egpNeighborLoss(5)
 - enterpriseSpecific(6)



- **Criptografia:** mensagem SNMP criptografada com DES
- **Autenticação:** calcular, enviar $\text{MIC}(m,k)$: calcula hash (MIC) sobre a mensagem (m), com chave secreta compartilhada (k)
- **Proteção contra playback:** usar nonce
- **Controle de acesso baseado em visões**
 - A entidade SNMP mantém uma base de dados de direitos de acesso e regras para vários usuários
 - A própria base de dados é acessível como um objeto gerenciado!



RMON é uma extensão do SNMP.

Monitora a rede como um todo, e não apenas seus elementos individuais. (limitado a camada de Enlace)

Padronizado para operar apenas em segmentos Ethernet.

RMON Probes (Sondas)

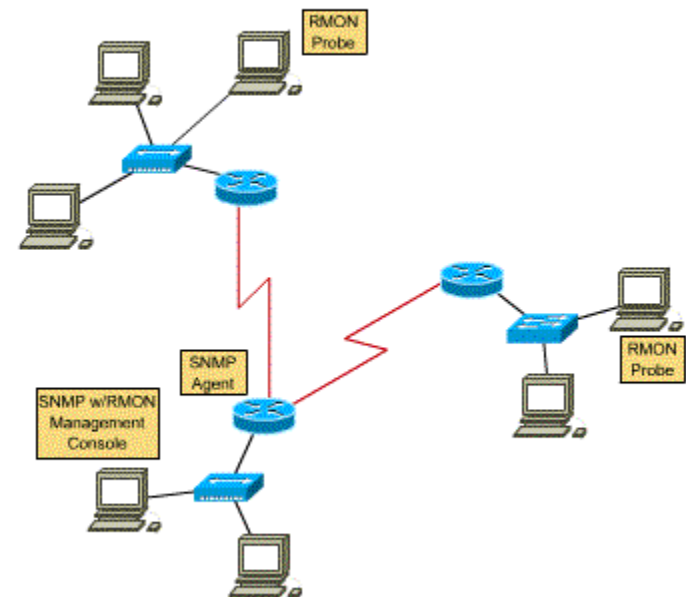
Mesma função do agente SNMP.

Possui capacidade de monitoramento remoto que os agentes não possuem.

Deve estar localizada em cada segmento da rede

Pode estar em hosts dedicados, residente em um servidor, ou incluída em um equipamento de rede (roteador ou switch).

Network With RMON Probes





Sumário

Introdução

Equipe

Áreas
Funcionais

Monitoração e
Controle

SNMP

Metodologia
de Detecção

Softwares de
Gerência

Objetivos do Monitoramento Remoto

Coleta de dados de valor agregado

Detectar e relatar problemas

Utilização de múltiplos gerentes

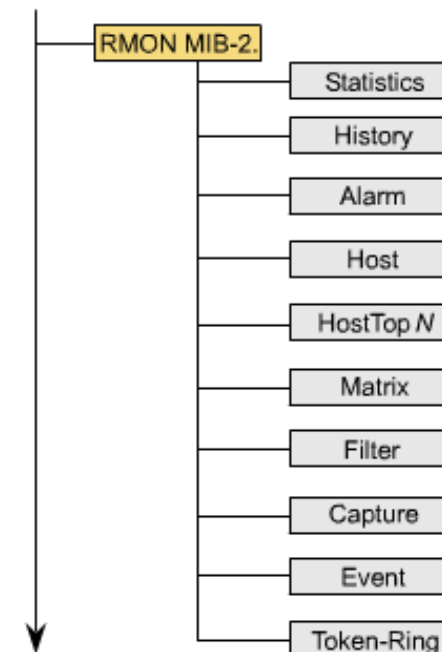
Propiciar operação off-line

Monitoramento preemptivo

RMON 2

Atua a partir da
camada de rede

MIB Tree With RMON Extension





PUC Minas

Metodologia de Detecção

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



PUC Minas

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.



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.



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



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.



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.



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?



PUC Minas

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)



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.



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



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



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 ser paliativa.
- A solução definitiva e correta deve ser elaborada.
- Na gerência de redes, todos os problemas tem solução.



Teste a solução implantada

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



PUC Minas

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



Necessidade de Gerenciamento

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.



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)

Configuração

SWPR34-05		UP	2012-04-19 15:34:08	1d 0h 48m 25s	PING OK - Packet loss = 0%, RTA = 1.66 ms
SWPR34-06		UP	2012-04-19 15:33:57	32d 20h 55m 23s	PING OK - Packet loss = 0%, RTA = 4.20 ms
SWPR34-07		UP	2012-04-19 15:33:57	32d 20h 45m 23s	PING OK - Packet loss = 0%, RTA = 17.19 ms
SWPR34LAB02-01		UP	2012-04-19 15:33:57	32d 20h 30m 22s	PING OK - Packet loss = 0%, RTA = 4.23 ms
SWPR34LAB02-02		UP	2012-04-19 15:33:57	32d 20h 30m 22s	PING OK - Packet loss = 0%, RTA = 17.50 ms
SWPR34LAB04-01		UP	2012-04-19 15:33:57	32d 20h 30m 27s	PING OK - Packet loss = 0%, RTA = 16.90 ms
SWPR34LAB06-01		UP	2012-04-19 15:33:57	32d 20h 25m 27s	PING OK - Packet loss = 0%, RTA = 4.14 ms
SWPR34LAB06-02		UP	2012-04-19 15:33:57	32d 20h 24m 56s	PING OK - Packet loss = 0%, RTA = 15.95 ms
SWPR38-01		UP	2012-04-19 15:33:59	7d 0h 9m 27s	PING OK - Packet loss = 0%, RTA = 8.15 ms
SWPR40-01		UP	2012-04-19 15:33:58	7d 0h 9m 37s	PING OK - Packet loss = 0%, RTA = 1.46 ms
SWPR41-01		UP	2012-04-19 15:33:58	7d 0h 9m 27s	PING OK - Packet loss = 0%, RTA = 4.23 ms
SWPR42-01		UP	2012-04-19 15:33:58	7d 0h 9m 7s	PING OK - Packet loss = 0%, RTA = 7.93 ms
SWPR43-01		UP	2012-04-19 15:34:08	1d 0h 48m 45s	PING OK - Packet loss = 0%, RTA = 77.88 ms
SWPR46-01		UP	2012-04-19 15:33:58	7d 0h 9m 7s	PING OK - Packet loss = 0%, RTA = 21.64 ms
SWPR46-02		UP	2012-04-19 15:33:57	7d 0h 9m 7s	PING OK - Packet loss = 0%, RTA = 17.25 ms
SWPR47-01		UP	2012-04-19 15:33:58	7d 0h 9m 7s	PING OK - Packet loss = 0%, RTA = 11.28 ms
SWPR47-02		UP	2012-04-19 15:33:58	10d 3h 3m 37s	PING OK - Packet loss = 0%, RTA = 12.34 ms
SWPR49-01		UP	2012-04-19 15:33:58	2d 23h 7m 20s	PING OK - Packet loss = 0%, RTA = 13.91 ms
SWPR54-01		UP	2012-04-19 15:33:58	2d 23h 57m 30s	PING OK - Packet loss = 0%, RTA = 3.07 ms
SWPR54-02		UP	2012-04-19 15:34:00	7d 0h 8m 57s	PING OK - Packet loss = 0%, RTA = 6.04 ms
SWPR54-03		UP	2012-04-19 15:33:57	9d 7h 6m 4s	PING OK - Packet loss = 0%, RTA = 15.21 ms
SWPR61-01		UP	2012-04-19 15:33:58	7d 0h 8m 57s	PING OK - Packet loss = 0%, RTA = 7.82 ms
SWPR65-01		UP	2012-04-19 15:34:00	7d 0h 9m 37s	PING OK - Packet loss = 0%, RTA = 16.15 ms
SWPR80-01		UP	2012-04-19 15:33:59	9d 6h 7m 44s	PING OK - Packet loss = 0%, RTA = 12.95 ms



PUC Minas

Nagios (2)

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**

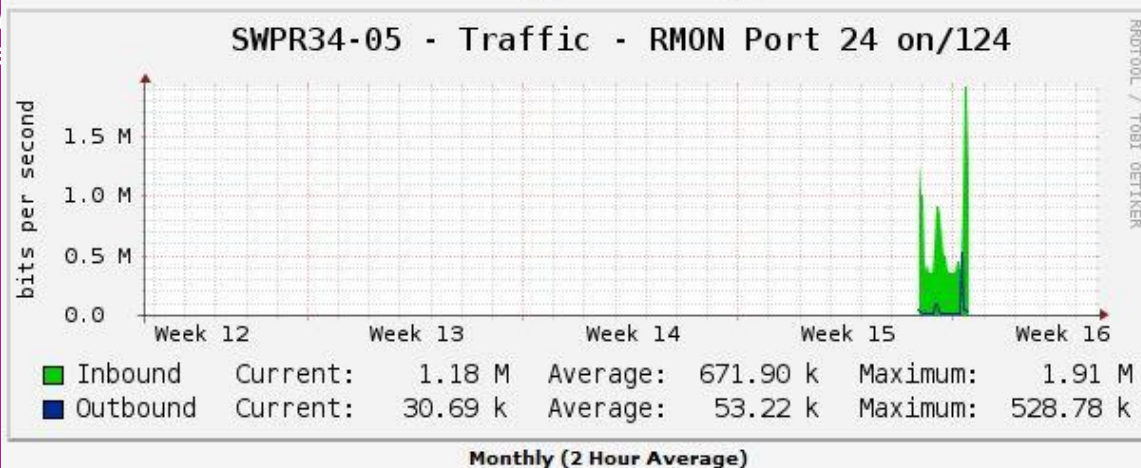
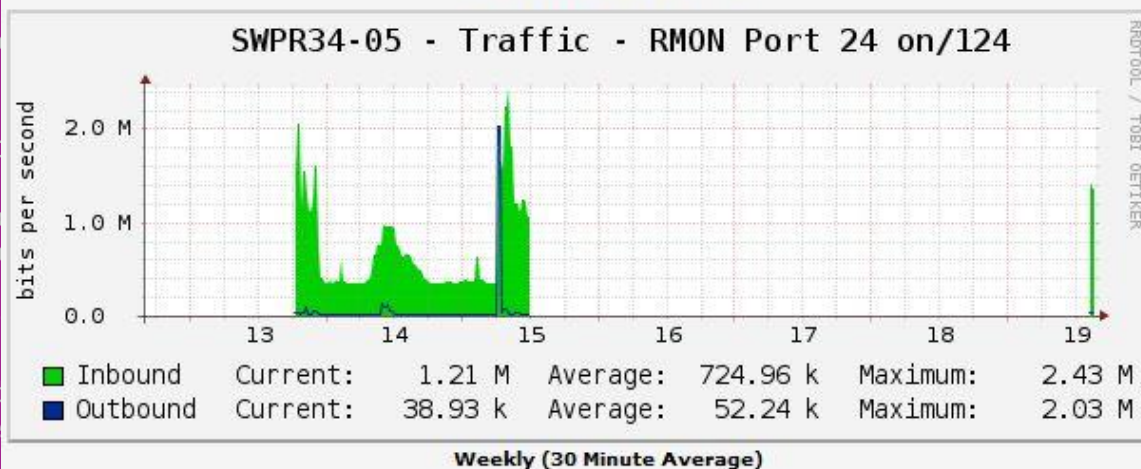
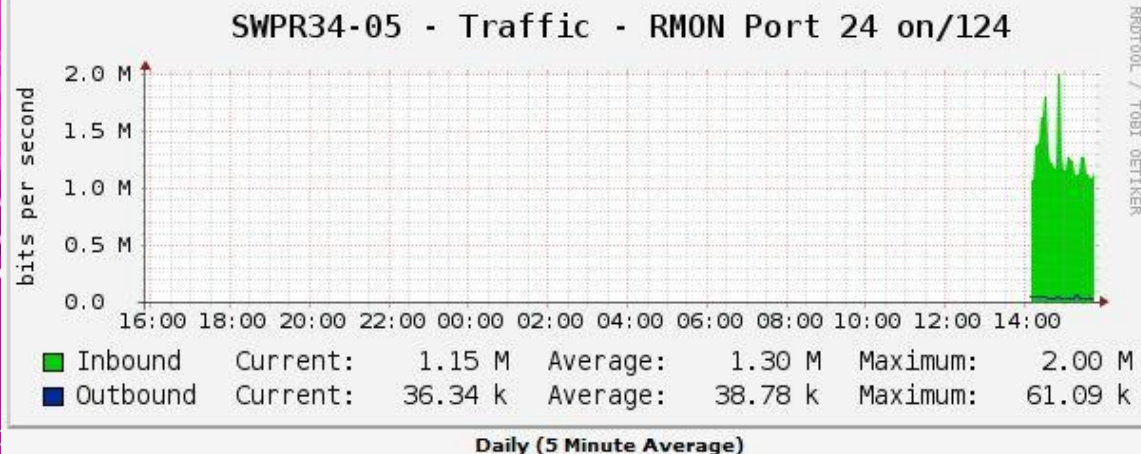
Obsessing: **ENABLED**

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)





PUC Minas

Cacti (2)

console

graphs

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: Status: Search: Rows per Page:

<< 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		0.04	0.05	100	<input type="checkbox"/>
SWPR06-01	3	28	28	Up	0		28.63	22.17	99.04	<input type="checkbox"/>
SWPR13-02	4	28	28	Up	0		7.07	9.36	98.65	<input type="checkbox"/>
SWPR34-02	6	28	28	Up	0		14.3	11.86	100	<input type="checkbox"/>
SWPR34-05	2	24	24	Up	0		3.35	3.68	99.62	<input type="checkbox"/>
SWPR41-01	5	28	28	Up	0		6.87	7.56	100	<input type="checkbox"/>

<< Previous

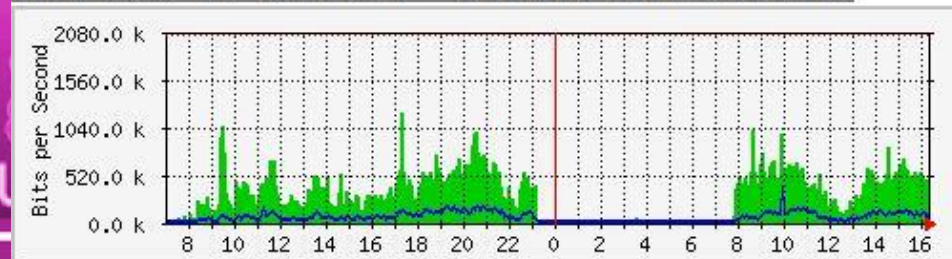
Showing Rows 1 to 6 of 6 [1]

Next >>

Choose an action:

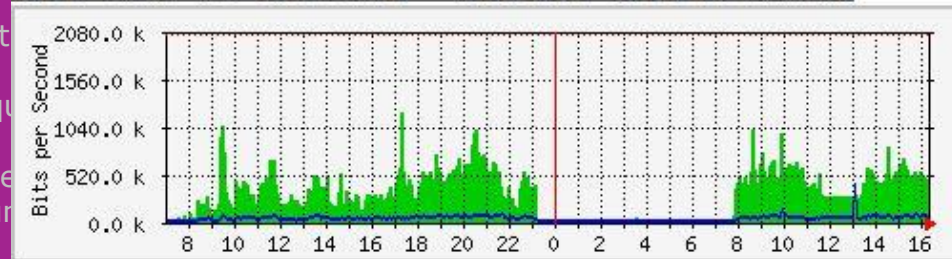


Link PUC <> Barreiro - Circuito BHE 5374843

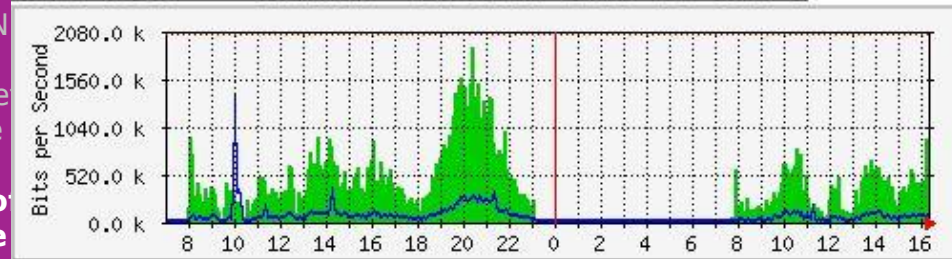


MRTG (1)

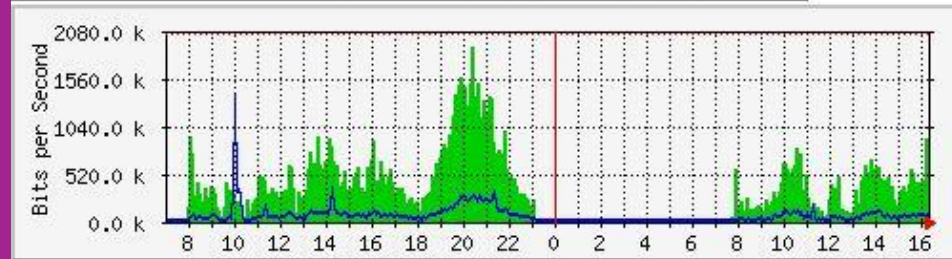
Link PUC <> Barreiro - Circuito BHE 5756438



Link PUC <> Betim - Circuito BET 5022370



Link PUC <> Betim - Circuito BET 5756443





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 [all](#) Host [SWPR34-01](#) Graph [Traffic Port 28](#)

[Filter](#)

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

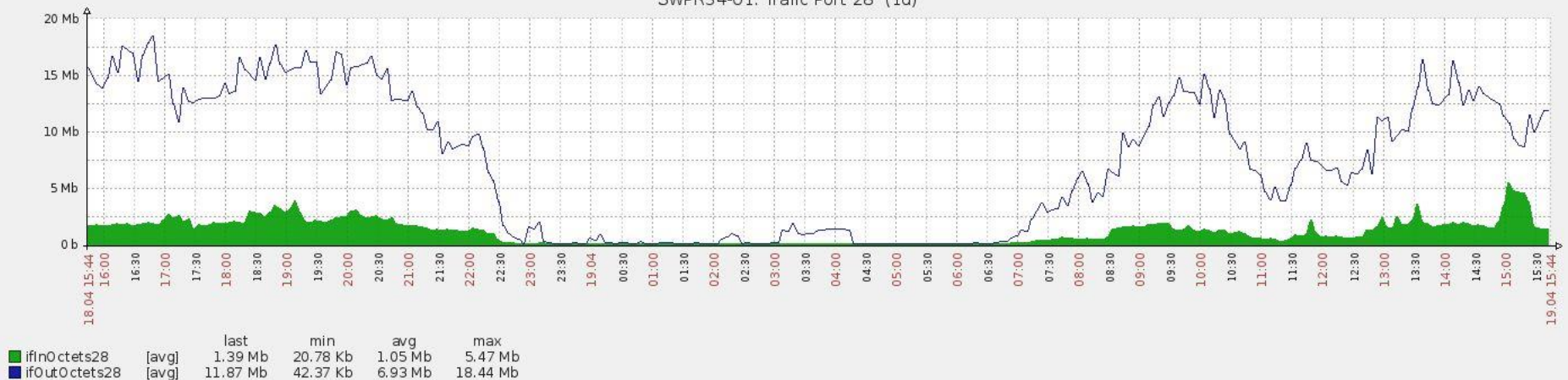
18.04.2012 15:40 - 19.04.2012 15:40 (now)



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

01d 00h 00m (fixed)

SWPR34-01: Traffic Port 28 (1d)



Data from history. Generated in 0.28 sec



PUC Minas

Zabbix (2)

Sumário

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

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



EVENTS

Group Host Source

Displaying 1 to 5 of 5 found

Filter

Time	Description	Status	Severity	Duration	Ack	Actions
18 Apr 2012 14:58:24	icmping	OK	High	1d 46m	No	-
18 Apr 2012 14:48:24	icmping	PROBLEM	High	10m	No	Failed
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	-

Softwares
de Gerência



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	46 / 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