



# Administração e Gerência de Redes de Computadores Disciplina – Projeto de Redes de Computadores

## Sumário

1	Introdução .....	2
2	Equipe de Gerência de Redes de Computadores .....	3
2.1	Helpdesk .....	4
2.2	Operador.....	4
2.3	Suporte Técnico ou Administrador da Rede .....	4
2.4	Gerente de Equipe .....	5
3	Áreas de Gerenciamento ISO/IEC .....	5
3.1	Gerencia de Configuração.....	6
3.2	Gerencia de Desempenho.....	7
3.3	Gerencia de Segurança .....	8
3.4	Gerencia de Contabilização .....	8
4	Monitoração e Controle .....	9
4.1	Monitoração .....	9
4.2	Controle .....	10
5	SNMP .....	10
6	RMON (Remote Monitoring) .....	12
7	Metodologia de Detecção .....	14
8	Softwares de Gerência.....	15

# 1 INTRODUÇÃO

O “Gerenciamento<sup>1</sup> de uma 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 rela a um custo razoável.”

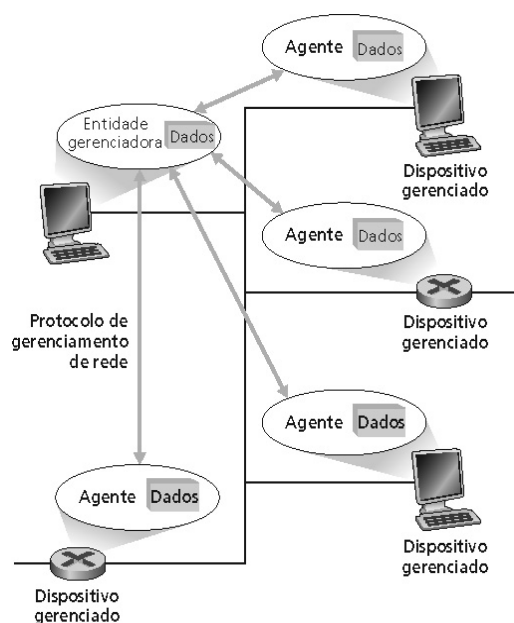
A gerência de redes nasceu da necessidade de monitoração e controle dos dispositivos da rede. Atualmente, as redes e seus serviços são fundamentais, de tal forma, que eles “não podem falhar”.

O nível de falhas e de degradação de desempenho aceitáveis está diminuindo, chegando a zero, dependendo da importância da rede para uma instituição.

A quantidade de dispositivos em uma rede tem crescido de forma espantosa nos últimos anos e sem ferramentas de suporte a gerência e protocolos para automatizar a tarefa, a equipe responsável pela manutenção da operação pode ficar informada pelos usuários sobre quedas dos serviços, o que pode ser descrito como o pior cenário.

Para tanto foram desenvolvidos 2 protocolos de comunicação entre estação gerente e dispositivos gerenciados que basicamente respeitam a arquitetura proposta na figura 1. Estes protocolos são o SNMP (Simple Network Management Protocol – Protocolo Simples de Gerência de Redes) e o CMIP (Common Management Information Protocol). O SNMP definido pela IETF e o CMIP pela ISO. Nesta arquitetura temos o gerente consultando os agentes que mantem uma base de dados com objetos relativos as características e tráfegos daquele dispositivo.

Figura 1. Arquitetura de Equipamentos Gerenciados



Fonte 1. Kurose e Ross

<sup>1</sup> T. Saydam & T. Magedanz. “From Networks and Network Management into Service and Service Management”. Jornal of networks and system management, 1996.

A solução de gerência de redes mais usada é a Internet-standard Network Management Framework, mais conhecida como gerência SNMP<sup>2</sup>. 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.

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?”

Assim, 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.

Podemos dizer que toda rede deve ser gerenciada para que seja garantida a disponibilidade de serviços com desempenho aceitável. As ferramentas disponíveis permitem as equipes de gerência perceber queda ou mesmo redução de desempenho antes dos usuários reclamarem da indisponibilidade. A automatização de grandes redes é feita com operações de monitoração e controle que veremos mais adiante nesta unidade.

## 2 EQUIPE DE GERÊNCIA DE REDES DE COMPUTADORES

A equipe de Gerência de Redes de Computadores<sup>3</sup> que cuida da administração da rede tem como objetivo prevenir e solucionar problemas na rede. Essa equipe possui vários níveis de profissionais e que atuam em áreas distintas como:

- Helpdesk,
- Operadores (de rede),
- Suporte técnico,
- Gerência da equipe

Esta classificação é encontrada em empresas de médio a grande porte e é comum encontrarmos um mesmo profissional acumulando várias atribuições de áreas diferentes em empresas menores que não comportam todos estes grupos que serão descritos nas próximas seções.

Alguns softwares para gestão das solicitações abertas são recomendados para coordenar as atividades do dia a dia dessas equipes. Podemos citar: OCOMON, Jira, GLPI, entre outras.

---

<sup>2</sup> Leia também o texto **Texto Protocolo de Gerenciamento SNMP**, de Dias e Alves Jr. Disponível em: <http://www.rederio.br/downloads/pdf/nt00601.pdf>

<sup>3</sup> Veja o vídeo do CGR da Telemar: <http://www.youtube.com/watch?v=qOi7JJEcZ-A>

## 2.1 HELPDESK

É o responsável pelo atendimento de primeiro nível que por padrão atende as chamadas telefônicas dos usuários e consultando uma base de conhecimento prévio procura solucionar problemas mais rotineiros. O grau de conhecimento normalmente é menor e exige uma formação menos especializada. Tendem a lidar com problemas já reportados e quando não conseguem resolver o problema escalam para equipes de 2º ou terceiro nível (operadores ou suporte técnico).

Tradicionalmente essa equipe é auxiliada por aplicações para gerenciar problemas reportados, em empresas maiores é comum ter o suporte de Centrais de PABX que gravam as chamadas dos usuários.

Ferramentas do tipo Wiki podem ser usadas para criar a base de conhecimento. E alguma aplicação para gerenciamento da fila de chamados é importante para promover um fluxo adequado de atendimento e permitir a mensuração de eficiência da equipe. As solicitações abertas no sistema normalmente permitem a mudança de estado (Em execução, em análise, fechada, etc.) e ao término o usuário pode emitir seu parecer sobre a qualidade de atendimento.

## 2.2 OPERADOR

Normalmente atua atendendo chamados de segundo nível que o helpdesk não conseguiu resolver consultado a base de conhecimento. Os problemas também podem ser detectados acompanhando os alarmes gerados pela estação de gerência.

Na prática quando, por exemplo, um equipamento passa para o estado não operacional, o operador perceberá um alarme na estação de gerência e deve atuar seguindo procedimentos criados pela empresa ou simplesmente atuando seguindo experiência acumulada em ocorrências anteriores.

Os alarmes podem ser informados de diversas formas:

- mudança de cores no mapa da rede;
- e-mail;
- celular, etc.

Ao perceber um problema o operador deve tentar resolvê-lo ou o encaminhar à equipe de suporte técnico, que seria a equipe de terceiro nível em algumas empresas conhecido também como administrador da rede.

## 2.3 SUPORTE TÉCNICO OU ADMINISTRADOR DA REDE

É quem definitivamente deve ter a maior competência técnica da equipe, pois acima dele não há ninguém que poderá resolver o problema. Ou seja, ele é a última alternativa para solucionar os problemas que não foram solucionados pela equipe de helpdesk nem pelo operador (do sistema de gerência). A não ser que a empresa tenha interesse em contratar serviço externo.

Este suporte técnico ou administrador da rede é responsável em tomar as decisões sobre os recursos computacionais a serem utilizados e pela configuração, operação e manutenção dos equipamentos da rede, para que se alcance o melhor desempenho dos recursos disponíveis.

Não há dúvida que nesta equipe devemos ter pessoas de preferência graduadas, com especializações e certificações quando for o caso da amplitude da rede da empresa.

## 2.4 GERENTE DE EQUIPE

Não se deve confundir o gerente da equipe com o gerente de rede, normalmente este último nome também é usado para o administrador da rede.

O gerente da equipe de gerência de rede não é, necessariamente, um expert técnico em redes. Ele deve ter conhecimento em redes, mas não necessariamente no nível do suporte técnico.

É função desse gerente avaliar o desempenho da sua equipe. Para tanto são necessários especificar algumas métricas, tais como:

- Tempo médio entre falhas;
- Tempos médio para correção de falhas;
- Percentual de problemas resolvidos em menos de 1h;
- Entre outros.

O gerente da equipe solicita compra de equipamentos, aplicações ou outros recursos, quando necessário, normalmente acompanhando a recomendação feita pela sua equipe de suporte técnico.

Este gerente deve ficar atento a necessidade de reciclagem da equipe com treinamentos, aperfeiçoamentos, promoções entre grupos, ou seja, alguém que se destaque no helpdesk deve ser promovido a operador, um bom operador deve ser promovido ao suporte técnico.

É também o gerente quem tem a interface com os outros núcleos da instituição para negociar investimentos e verificar demanda dos demais departamentos para conduzir as tarefas à sua equipe.

## 3 ÁREAS DE GERENCIAMENTO ISO/IEC

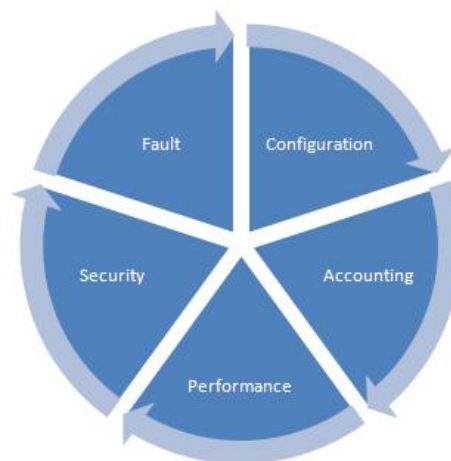
A ISO/IEC define 5 áreas de gerenciamento (modelo funcional denominado FCAPS). Este modelo auxilia as equipes a se organizarem para atuação e definição de políticas no sentido de aumentar a disponibilidade dos recursos de rede das empresas e alcançar individualmente o que uma das áreas preconiza.

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

A figura 2 apresenta o ciclo de interação destas cinco áreas funcionais definidas na ISO/IEC 7498 de 2007. Cada uma dessas áreas terá uma descrição sucinta nas próximas seções onde teremos a

oportunidade de perceber certa interseção de objetivos e consequentes aproveitamentos de ferramentas em duas ou mais áreas, por exemplo, o Visualizador de Eventos que pode ser utilizado na gerência de falhas para contabilizar quedas de serviços, ou na gerência de contabilização para manter contabilidade de tempo de login dos usuários.

Figura 2. Áreas de Gerência de Rede



Fonte 2: ISO/IEC 7498.

### 3.1 GERENCIA DE CONFIGURAÇÃO

Em linhas gerais é a área funcional que responde pelo patrimônio de hardware e software da empresa e sua configuração inicial, mantendo também arquivos de configurações dos equipamentos para facilitar e diminuir o tempo de recuperação de desastre quando um equipamento precisar ser trocado. Mais detalhadamente podemos enumerar as seguintes características dessa área:

- 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.
- Responsável pela inicialização da rede
- Responsável pela 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. Uma vez decidido como o equipamento deve ser usado, o gerente de configuração escolhe o sw e um conjunto de valores coletados.
- Responsável por 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.

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

É fundamental utilizar recursos de controle de inventário como OCS, Cacic, Acronus, Microsoft Inventory analyzer, etc. Para facilitar a coleta de informações das estações de trabalho e dos servidores.

### 3.2 GERENCIA DE DESEMPENHO

Em linhas gerais afere se os parâmetros definidos durante o projeto da rede estão sendo alcançados, como tempo de resposta, latência, largura de banda, etc. Mais precisamente podemos enumerar as seguintes características para esta área de gerência funcional:

- 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.
- 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?
- 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.
- Coletando 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.

Podemos usar uma ou várias ferramentas de análise de desempenho para nos auxiliar nesta área funcional, podemos citar o Cacti, NAgios, Zabbix, MRTG, NetFlow, Ntop, entre outros que procuram

gerar gráficos de consumo de recursos de rede para apontar à equipe de gerência onde possíveis gargalos podem acontecer.

### 3.3 GERENCIA DE SEGURANÇA

Esta área funcional tem como principal objetivo garantir que a política de segurança definida pela instituição alcance sua meta. É claro que para isto vários aspectos precisam ser dimensionados, a seguir uma lista de itens que a equipe atribuída a esta área terá que se envolver:

- Proteger 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 deixar chegar a mãos das pessoas erradas;
- Prover facilidades para proteger os recursos da rede e informações dos usuários e garantir que estas facilidades só estejam disponíveis para os usuários autorizados.
- Procurar redigir uma política de segurança seja robusta e efetiva e que o sistema de gerenciamento da segurança seja, ele próprio, seguro.

O dia a dia desta equipe 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.

Até que ponto devem ser relacionados às atribuições da equipe da área funcional de segurança? Esta abrangência pode ser posta nos seguintes itens:

- 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.

### 3.4 GERENCIA DE CONTABILIZAÇÃO

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. 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.

## 4 MONITORAÇÃO E CONTROLE

A monitoração e controle trata a questão de como a gerência da rede será feita pela a equipe descrita na seção 2. Em particular as funções de gerenciamento de rede podem ser agrupadas em duas categorias:

- 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.

### 4.1 MONITORAÇÃO

Aprofundando um pouco mais estes dois aspectos, vamos inicialmente falar sobre o monitoramento que em outras palavras vai consistir na observação de informações relevantes ao gerenciamento, estas informações costumam ser 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.

Estas informações de gerenciamento são coletadas e armazenadas por agentes e repassadas a um ou mais gerentes por dois métodos de consultas (leituras) diferentes: *Polling* ou *event-reporting*.

No método de *polling* a interação é do tipo request-response disparada pelo gerente em direção do agente que responde àquela consulta. O gerente neste caso pode solicitar a um gerente o envio de valores de diversos elementos de informação e o agente responde com os valores constante em sua MIB. (Descreveremos melhor estes termos quando estudarmos SNMP na próxima seção neste texto).

Por outro lado a técnica de *event-reporting* a iniciativa da comunicação é feita pelo agente, a partir de eventos que acontecem na estação gerenciada. O gerente neste caso fica em escuta, esperando a chegada de informações. O agente pode gerar um relatório periodicamente, ou seja, depois de um tempo fornecido por um gerente indicando seu estado atual, ou este relatório pode ser gerado por um evento significativo como, por exemplo, um reboot inesperado.

A escolha por um método ou outro, ou seja, pelo polling ou event-reporting depende de uma série de questões, entre elas:

- 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.

## 4.2 CONTROLE

Como dito anteriormente a abordagem de controle tem a perspectiva de alteração de parâmetros da rede e à execução de ações em um sistema remoto, ou ainda, atua na escrita nos dispositivos. Todas as cinco áreas funcionais de gerência envolvem monitoração e controle, mas podemos apontar um enfoque maior de monitoração nas áreas de falha, desempenho e contabilização e nas áreas de configuração e segurança a atuação é mais de controle.

O controle na área funcional 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;

Já na área funcional de segurança o controle é relativo à segurança dos recursos sob gerenciamento da equipe, incluindo o próprio sistema de gerenciamento. Os principais objetivos em termos de segurança estão atrelados à confidencialidade, autenticação, integridade, disponibilidade e não repúdio.

As principais ameaças à área funcional de segurança estão associadas à interrupção dos serviços e da rede em si, interceptação do tráfego, modificação de informações e mascaramento de identidade. 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

## 5 SNMP

O SNMP (Simple Network Management Protocol – Protocolo Simples de Gerência de Redes) é o principal protocolo de gerência de redes atualmente utilizado na pilha TCP/IP, ou seja, na Internet e também em outros tipos de rede como redes telefônicas. Começou a ser desenvolvido em 1987 a partir do SGMP e hoje já se encontra em sua terceira versão.

A leitura do texto disponível em <http://www.rederio.br/downloads/pdf/nt00601.pdf> é **obrigatório**, neste texto vocês encontrarão toda descrição desse protocolo como sua arquitetura, comandos e objetos padrões gerenciados. No restante dessa seção vou trazer apenas alguns detalhes que considero importante ressaltar.

O primeiro aspecto que considero importante indicar é que este protocolo vem sofrendo várias atualizações desde sua criação e a IETF (Internet Engineering Task Force) que controla os padrões de protocolos na Internet lançou as seguintes RFCs (Reques For Comments) para definir as variações sobre o SNMP:

- SNMPv1 RFC 1157
- SNMPv2 RFC 1905, RFC 1906, RFC 1907
- SNMPv3 RFC 2571, 3410, 3414

Você terá dificuldades em entender o texto a partir deste ponto se não ler o pdf recomendado anteriormente.

O SNMP é basicamente um modelo cliente servidor, onde os gerentes podem mandar requisições aos agentes e receber as respostas dos mesmos. As consultas são feitas aos objetos mantidos nas MIBs dos agentes. Estes agentes também podem reportar eventos que ocorrem na estação gerenciada.

O mais comum é vermos o SNMP rodando na camada de aplicação sobre o protocolo UDP usando as portas 161 para transmissão e recebimento dos comandos do tipo request/response e a porta 162 para recebimento das notificações. Que a partir da V2 do SNMP podiam também ser com confirmação de recebimento, ou seja, na versão 1 do SNMP o agente notificava algum evento ao gerente, mas não tinha resposta (nem certeza se a notificação havia chegado) esta notificação é feita com o comando Trap, a partir da versão 2 o agente podia optar pelo comando Inform que exigia o retorno do gerente confirmando o recebimento da notificação.

Alguns avanços na versão 2 do SNMP como vimos no parágrafo anterior foi para criar um novos comando o Inform, mas tivemos também o GetBulk que permitia a recuperação de vários objetos de um agente ao mesmo tempo, ou com um único pacote. Foram criados também o Report e o Notification. Com isto o desempenho para se obter a árvore completa da MIB de um Agente melhorou consideravelmente.

Aproveitando esta nova versão novos códigos de erro foram também acrescentados, assim quando um comando era enviado para um agente e o mesmo não conseguia executá-lo a mensagem de erro devolvida era mais representativa em relação as que existiam na versão 1. Porém o principal motivo foi a tentativa de melhorar a segurança na comunicação entre gerente e agente que era autorizada apenas verificando uma *string* denominada Community.

Neste sentido a versão 2 desenvolveu o SNMPv2C e a SNMPv2U, a v2C ou versão 2 Community era equivalente a versão 1, ou seja, quando um gerente encaminhava uma mensagem para o agente, o agente para autorizar a operação de apenas leitura (read-only) ou leitura e escrita (read-write) conferia o campo community do pacote enviado pelo gerente que estava em texto aberto. Na versão v2U ou versão 2 User, o objetivo era autorizar os comandos baseado em usuário, mas assim que foi lançado foram descobertos falhas no padrão que inviabilizaram sua utilização, sendo assim esta versão (SNMPv2U) não chegou a ser implementada em larga escala.

Este fato gerou a necessidade da criação da versão 3. Que tinha como meta proporcionar uma comunicação segura entre gerente e agente. Pois em uma realidade atual não podemos confiar em troca de informações sigilosas na rede com texto abertos. Considere o risco de se trocar o ip de um servidor com um comando SNMP, isto é possível!

Podemos enumerar as seguintes evoluções na versão 3 do SNMP:

- Criptografia: mensagem SNMP criptografada entre gerente e agente
- Autenticação: calcular, enviar  $MIC(m,k)$ : calcula hash (MIC) sobre a mensagem (m), com chave secreta compartilhada (k). Com este processo o agente tem certeza de qual gerente está recebendo a ordem e vice-versa.
- Proteção contra playback: usar nonce. Evita-se o ataque de repetição, ou seja, ninguém consegue retransmitir uma ordem já encaminhada no passado.
- Controle de acesso baseado em visões, cada usuário recebe autorização específica em blocos da MIB, antes o acesso era sobre a MIB inteiro do tipo read-only ou read-write.
- 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!

## 6 RMON (REMOTE MONITORING)

O SNMP apesar de bastante conhecido, difundindo e usado tem um problema, pode se tornar muito trabalhoso administrar em caso de instalação em todas as estações e dispositivos da rede. O volume de informações e o tráfego gerado para administrar a rede pode se tornar proibitivo em função da quantidade de estações e dispositivos do ambiente.

Nestes casos, a solução pode ser instalar um protocolo que funciona como uma extensão do SNMP que monitora a rede como um todo e não os elementos da rede individualmente. Neste caso, não saberemos, por exemplo, à quanto tempo um computador em particular está ligado, mas podemos saber qual o tráfego que uma determinada máquina gerou, ou quem são os top 10 de download na rede. Desde que instalemos a sonda no lugar correto, como, por exemplo, no switch da camada de agregação da rede ou no firewall por onde todos deverão passar para sair para Internet.

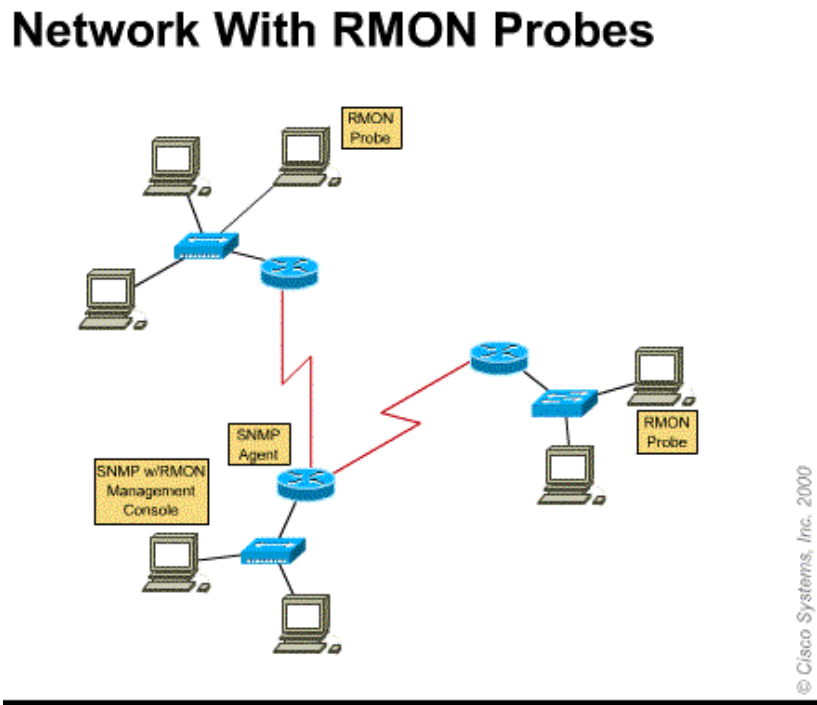
Logo a ideia é que um equipamento fique responsável em coletar todos os dados que trafegam naquele segmento de rede, podendo até entregar dados consolidados do que ele descobriu como: quem conversa com quem; quais são os destinos mais acessados; etc. Mas como já disse, perderemos informações individuais dos equipamentos que nós só teríamos se tivéssemos o SNMP instalado em cada máquina.

Na figura 3 você pode perceber como a arquitetura do RMON funciona, neste exemplo, temos 3 segmentos de rede, no segmento de cima são três computadores, um switch e um roteador, neste segmento uma das máquinas fica com a sonda coletando informações de todo o tráfego que passa naquele barramento. No modelo do SNMP eu teria que ter instalado o agente nos 5 elementos de rede (os 3 computadores, no switch e no roteador). Nos outros dois segmentos a lógica é a mesma, ao invés de eu instalar 4 agentes SNMP eu instalei uma sonda RMON.

O objetivo com o RMON é coletar dados até a camada de enlace de um segmento de rede com valor agregado, ou seja, quem falou mais com quem, quem transmitiu mais naquele grupo de máquinas, para onde mais as pessoas acessaram, etc. Além disso, fica mais fácil detectar e relatar problemas, utilizar múltiplos gerentes, propiciar coleta off-line e descarregar os dados coletados quando o gerente voltar a ficar ativo e o monitoramento pode ser agendado para acontecer só em determinados momentos do dia, o chamado monitoramento preemptivo.

O RMONv2 coleta dados a partir da camada de rede aumentando a capacidade da sonda em verificar características do tráfego gerado em um segmento de rede. A figura 4 mostra a MIB2 do RMON.

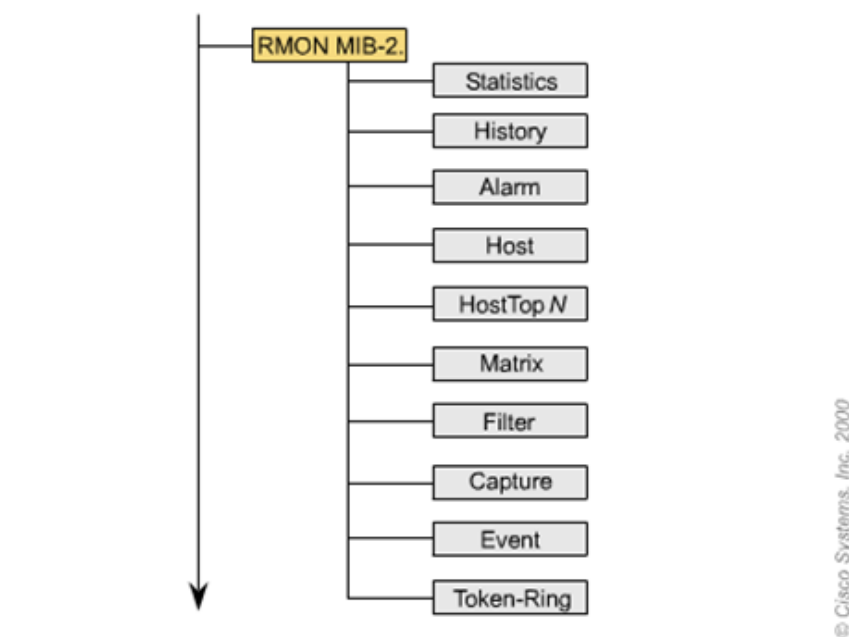
Figura 3. Arquitetura RMON



Fonte 3. Cisco Systems

Figura 4. Árvore da MIB-2 com Extensão do RMON

## MIB Tree With RMON Extension



Fonte 4. Cisco Systems

## 7 METODOLOGIA DE DETECÇÃO

As seções anteriores deste documento nos levam a criar condições de entender melhor com uma equipe de gerência é composta, que áreas eu devo atuar, como eu devo proceder (monitorando ou controlando), qual protocolo tenho à disposição para me comunicar com os dispositivos. Agora podemos discutir como devemos abordar um problema quando ele acontece, ou seja, que etapas devemos seguir para manter nossa rede funcionando ou retornar a operação normal da rede quando algum desastre acontece.

Neste sentido, algumas literaturas comparam este processo com o dia a dia da equipe de gerência de redes com a de um médico que em linhas gerais identifica problemas, enumera possíveis causas e procura a partir de então isolar cada causa até solucionar o problema. A tabela 1 a seguir aponta esta metodologia.

MEDICINA	GERENCIA DE REDES
SINAIS/SINTOMAS	
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.

Mais precisamente uma Metodologia de Detecção de Gerência de Redes poderia ter as seguintes etapas:

1. Detecção: feita pelo usuário ou pelo operador. O ideal é não deixar o usuário detectar a falha, para tanto softwares de monitoramento podem auxiliar na detecção, manter especial atenção aos pontos críticos. O problema deve ser bem caracterizado, para tanto 4 elementos são essenciais:
  - a. Descrição: circunstância do ocorrido
  - b. Sintomas: informam o que um usuário de rede pode perceber como consequência de um problema (efeito negativo do problema para o usuário)
  - c. Sinais: características mais internas, normalmente usuário não percebe (taxas de erro, taxas de colisão)
  - d. Testes confirmatórios: recomendado apenas quando não houver sinais evidentes

2. Coleta de Informações: passa pela resposta de perguntas do tipo:
  - a. Quem está sendo afetado pelo problema? Apenas um usuário? Todos os usuários? Alguns usuários que fazem parte da mesma sub-rede?
  - b. Quando o problema começou a ser percebido?
  - c. Desde então, o problema ocorre sempre, ou apenas em certos horários? Neste caso, em que horários?
  - d. O problema se manifesta sempre ou apenas quando alguma aplicação e/ou serviço específicos são usados? Neste caso, que aplicações e/ou serviços?
  - e. Alguma mensagem de erro está sendo gerada? Qual?
3. Recorrência de problema ou mudança na rede? Consultas a Base de Dados pode agilizar a solução, então é interessante se questionar:
  - a. Esse problema já ocorreu recentemente?
  - b. Houve alguma mudança recente na rede que possa causar os sintomas detectados?
  - c. Se sim, vá direto ao ponto...
  - d. Desenvolva hipóteses específicas considerando apenas o alvo
  - e. Se, ao testar as hipóteses, detectar que é outro problema, desenvolva hipóteses genéricas (volte na etapa)
4. Desenvolva Hipóteses: O que pode estar causando o problema? Necessário conhecimento técnico e boa experiência para conduzir esta etapa.
5. Organizar as hipóteses: para que se teste primeiro as com maior probabilidade de resolução do problema. Um plano de ação para os testes é importante para não cometer erro durante os testes.
6. Teste as Hipóteses: implementar os planos de teste criados na fase anterior para confirmar ou negar a hipótese. Caso nenhuma hipótese se confirme volte ao passo 4.
7. Solucione o problema: mesmo que mais rapidamente com alternativa paliativa e depois com solução definitiva
8. Teste a solução: confirme a solução implementada antes de se dar por satisfeito, use os recursos de software para tal.
9. Documente a ocorrência e solução: o problema pode voltar a acontecer e talvez seja necessário consulta a base de dados, ou talvez o atendimento de primeiro nível pode atender a solicitação.

## 8 SOFTWARES DE GERÊNCIA

Por fim para alcançar nosso objetivo principal de administração e gerência de redes de computadores precisamos lançar mão de softwares de gerenciamento, considerando que os mesmos não resolvem todos os problemas sozinhos e que estes existem para nos alimentar de informações para que tomemos ações. Os motivos que nos permitem afirmar que os softwares de gerência não resolvem tudo sozinho são:

- Softwares normalmente são subutilizados;
- Inúmeras características inexploradas;
- Utilizados de modo pouco eficiente;
- Usuários despreparados.

Não há dúvidas que é humanamente impossível controlar dezenas, centenas e alguns casos milhares de dispositivos sem o auxílio de softwares e como vimos os protocolos que nos dão suporte



para tal já foram desenvolvidos. Logo 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.

À medida que um determinado recurso vai sendo mais importante na rede sua demanda por disponibilidade também aumenta e nosso software de gerenciamento deve prezar por esta disponibilidade. Podemos enumerar vários softwares que tem o objetivo de auxiliar na gerência de uma rede de computadores e outros podem ser facilmente desenvolvidos por você considerando que praticamente todas as linguagens de programação possuem bibliotecas de suporte ao SNMP.

A figura 5 apresenta uma ferramenta de monitoramento de recursos de rede que pode disparar pings a uma determinada frequência para equipamentos de rede e servidores ou conferir portas de serviços hospedados em servidores para verificar sua disponibilidade. Nesta figura 5 em particular conseguimos verificar que vários switches da rede acadêmica estão com status UP, sem perda de ping e a quanto tempo estão ligados o que indica uma consulta de SNMP para requisitar o parâmetro SysUpTime de cada switch. A Figura 6, mostra em detalhes mais parâmetros da MIB do switch 02 do prédio 47.

**Figura 5. Print de tela do Nagios monitorando operação de Switchs da Rede acadêmica da PUC**

























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
SWPR34LA602-01		UP	2012-04-19 15:33:57	32d 20h 30m 22s	PING OK - Packet loss = 0%, RTA = 4.23 ms
SWPR34LA602-02		UP	2012-04-19 15:33:57	32d 20h 30m 22s	PING OK - Packet loss = 0%, RTA = 17.50 ms
SWPR34LA604-01		UP	2012-04-19 15:33:57	32d 20h 30m 27s	PING OK - Packet loss = 0%, RTA = 16.90 ms
SWPR34LA606-01		UP	2012-04-19 15:33:57	32d 20h 25m 27s	PING OK - Packet loss = 0%, RTA = 4.14 ms
SWPR34LA606-02		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



Figura 6. Informações detalhadas do Switch 02 do Prédio 47 capturadas pelo Software Nagios.

**Host Information**  
 Last Updated: Thu Apr 19 15:38:43 BRT 2012  
 Updated every 90 seconds  
 Nagios® Core™ 3.2.3 - [www.nagios.org](http://www.nagios.org)  
 Logged in as nagiosadmin

**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

Ao perceber alguma indisponibilidade o software pode ser configurado para emitir um alerta na forma de mensagem para uma conta de email, indicando o problema. O software Cacti também pode assumir a função do Nagios no monitoramento de equipamentos e serviços como podemos ver na figura 07, onde seis equipamentos estão sendo monitorados em relação a resposta de ping.

Figura 7. Software Cacti monitorando status de equipamentos de rede da PUC-Minas

**Devices**

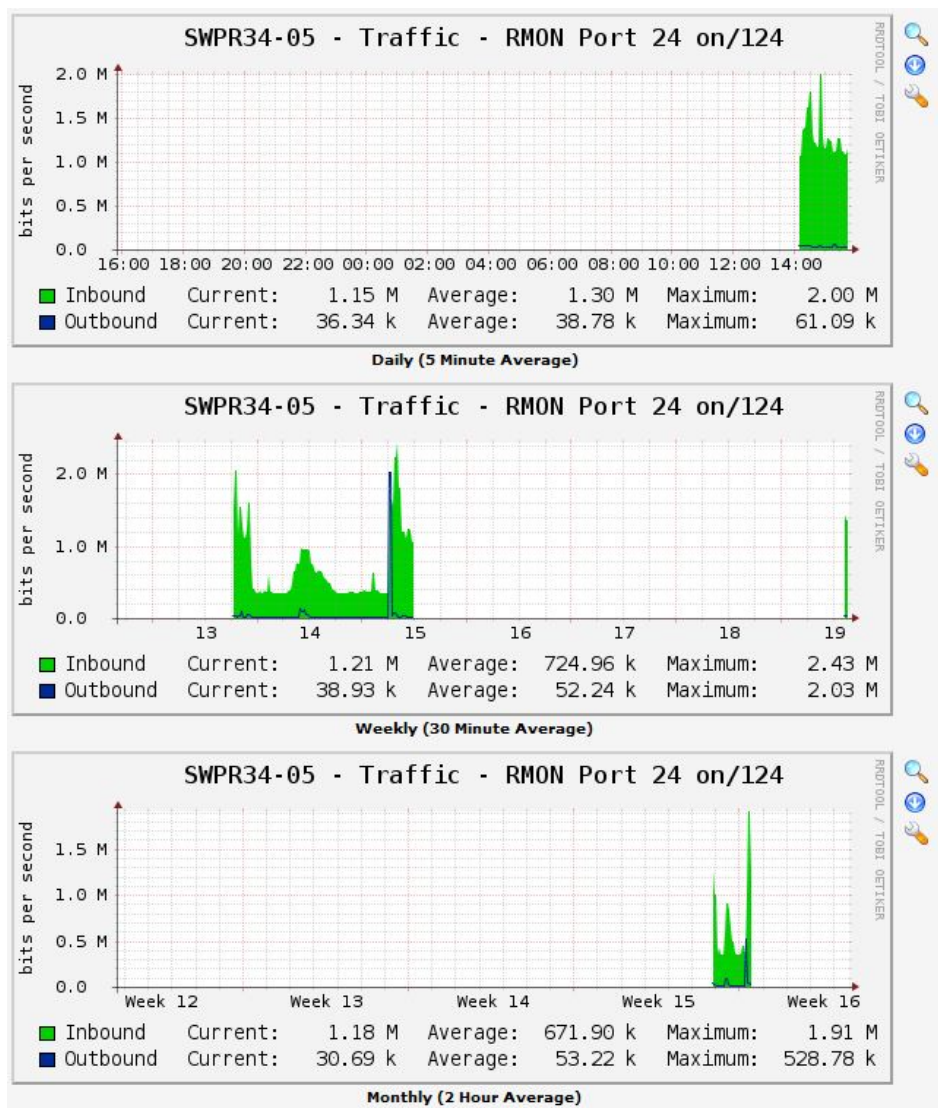
Type: Any Status: Any Search: Rows per Page: 30 Go Clear

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
SWPR06-01	3	28	28	Up	0		28.63	22.17	99.04
SWPR13-02	4	28	28	Up	0		7.07	9.36	98.63
SWPR34-02	6	28	28	Up	0		14.3	11.86	100
SWPR34-05	2	24	24	Up	0		3.35	3.68	99.62
SWPR41-01	5	28	28	Up	0		6.87	7.56	100

Choose an action: Delete Go

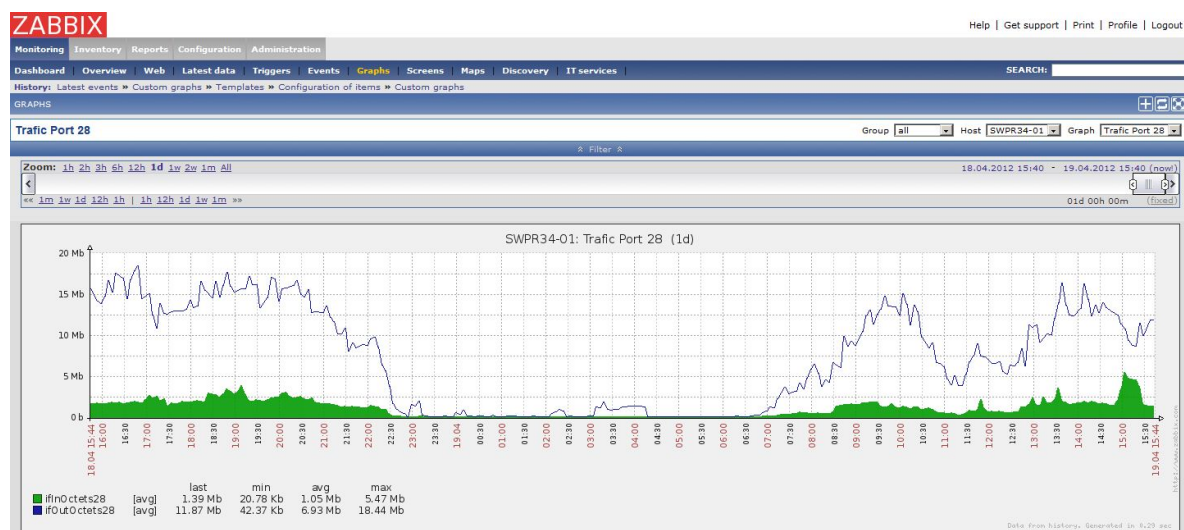
Na figura 08 apresentamos a interface de outra funcionalidade do Cacti que é de verificação de consumo de trafego de portas de switchs e roteadores, semelhante também ao MRTG e Zabbix. Em particular esta figura mostra o consumo da porta 24 do switch 05 do prédio 34 da PUC Coração Eucarístico.

Figura 8. Consumod e Tráfego da porta 24 do Switch 05 do Prédio 34 da PUC-Minas



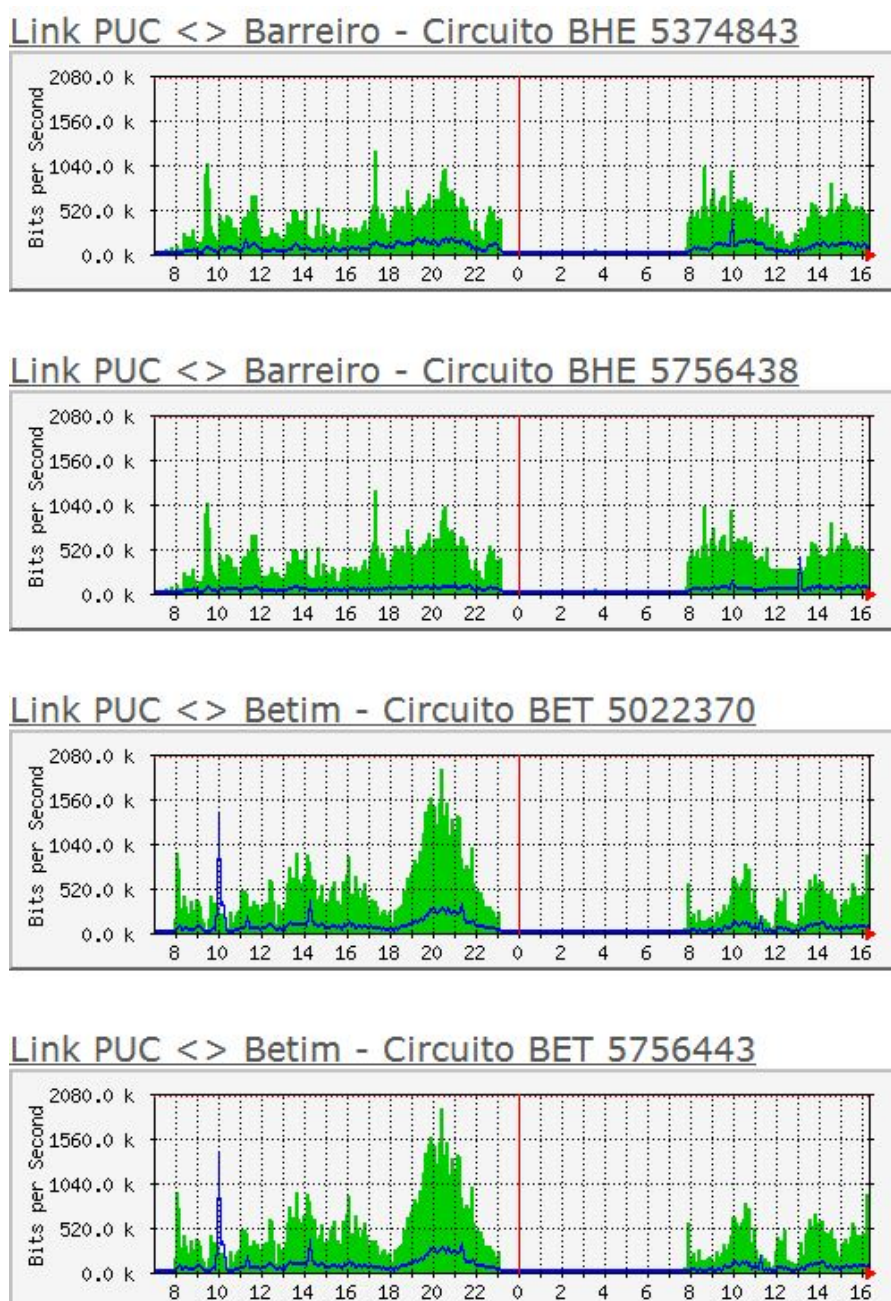
O equivalente a figura 8 sendo feito na figura 09 pelo software Zabbix.

Figura 9. Análise de Consumo de uma porta de Switch da rede PUC-Minas



Normalmente temos uma linha que representa o tráfego de entrada e outro de saída daquela interface (lembre que a rede ethernet na maioria dos casos é full duplex) e como você já deve ter percebido, temos softwares diferentes fazendo a mesma coisa. Veja a figura 10 onde tenho o MRTG monitorando o consumo de links de Internet de algumas unidades da PUC-Minas.

Figura 10. Monitoramento do Consumo de Link Internet das UNidades da PUC-Minas.



Todas estas apresentadas até então são ferramentas gratuitas e concorrentes entre si, diferenciando em alguns aspectos de o que pode ser configurado para ser monitorado e como os alertas serão emitidos. Não apresentei com maiores detalhes nenhuma delas, mas olhando a figura 11 é possível ter a dimensão de equipamentos que podemos ter gerenciados por uma ferramenta dessas. É claro que existem ferramentas pagas e com outros atrativos e diferenciais e cada característica deve ser avaliada ao escolher uma que melhor se adequa ao ambiente que será gerenciado.



Figura 11. Tela de Status geral do Zabbix

Monitoring

Inventory

Reports

Configuration

Administration

Dashboard

Overview

Web

Latest data

Triggers

Events

Graphs

Screens

Maps

Discovery

IT servi

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
<a href="#">SW-PMG</a>	0	0	0	0	0	0
<a href="#">Windows servers</a>	0	0	0	0	0	0

Updated: 15:45:37

Host status

Host group	Without problems	With problems	Total
<a href="#">SW-PMG</a>	45	0	45
<a href="#">Windows servers</a>	1	0	1

Updated: 15:45:37