

**INSTITUTO DE ENSINO SUPERIOR DO ESPÍRITO SANTO
FACULDADE DO ESPÍRITO SANTO – UNES
CURSO DE SISTEMAS DE INFORMAÇÃO**

**JEFFERSON BUGIM DA SILVA
MÁRCIO RODRIGUES PIRES VARELA**

PRTG – GERÊNCIA DE REDES

**CACHOEIRO DE ITAPEMIRIM
2013**

**JEFFERSON BUGIM DA SILVA
MÁRCIO RODRIGUES PIRES VARELA**

PRTG – GERÊNCIA DE REDES

Trabalho de Conclusão de Curso apresentado ao curso de Sistemas de Informação na Faculdade do Espírito Santo, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Marcelo A Schuster

**CACHOEIRO DE ITAPEMIRIM
2013**

**JEFFERSON BUGIM DA SILVA
MÁRCIO RODRIGUES PIRES VARELA**

PRTG – GERÊNCIA DE REDES

Trabalho de Conclusão de Curso apresentado ao curso de Sistemas de Informação na Faculdade do Espírito Santo, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Aprovado em.....

COMISSÃO EXAMINADORA

Orientador: Marcelo A Schuster

Jefferson Bugim da Silva

Dedico a minha família, principalmente meus pais, Francisco Carlos e Neuzeli Bugin, meus maiores exemplos. por cada incentivo e orientação, pelas orações em meu favor, pela preocupação para que estivesse sempre andando pelo caminho correto. A minha esposa, Jessica, por todo amor, carinho, paciência e compreensão que tem me dedicado.

Ao professor Marcelo A Schuster que, com muita paciência e atenção, dedicou do seu valioso tempo para me orientar em cada passo deste trabalho. Aos professores de sistemas de informação da instituição UNES pela contribuição na minha vida acadêmica e por tanta influência na minha futura vida profissional.

Aos meus colegas de classe, a quem aprendi a amar e construir laços eternos. Obrigado por todos os momentos em que fomos estudiosos, brincalhões, atletas, músicos e cúmplices. Porque em vocês encontrei verdadeiros irmãos. Obrigado pela paciência, pelo sorriso, pelo abraço, pela mão que sempre se estendia quando eu precisava. Esta caminhada não seria a mesma sem vocês.

Quero agradecer em especial ao meu parceiro de conclusão de curso, acima de tudo meu amigo e irmão Marcio Rodrigues, que sempre esteve presente desde o início de minha formação escolar e desde então seguimos juntos fortalecendo nossa amizade e ultrapassando juntos os obstáculos que a vida ate este presente momento nos proporcionou.

Márcio Rodrigues Pires Varela

Dedico a Deus, primeiramente, por ter me dado força, coragem durante esses quatro anos de Curso, a meio de dificuldades. Por ter me iluminado nas decisões mais difíceis e por ter me guiado ao longo do curso para trilhar o caminho mais correto possível.

Dedico a minha família, especialmente meus pais, Anivaldo Pires Varela, Inete Rodrigues Pova e minha noiva Mônica Aparecida Noenta Oliveira que sempre me deram força, coragem e constante apoio para seguir em busca de meus objetivos.

AGRADECIMENTOS

Agradecemos a Deus por iluminar nossos caminhos percorridos e nos permitir realizar este sonho em nossas vidas. Estendemos nossos agradecimentos a nossa família que sempre acreditou em nossos potenciais e nos incentivou mesmo quando passávamos por momentos turbulentos, nos confortou com conselhos que nos fez crescer não somente na vida acadêmica, mas como ser humano, diante disso agradeço toda dedicação exercida para o nosso crescimento acadêmico, profissional e pessoal.

“Sem sonhos, a vida não tem brilho. Sem metas, os sonhos não têm alicerces. Sem prioridade, os sonhos não se tornam reais. Sonhe, trace metas, estabeleça prioridade e corra riscos para executar seus sonhos. Melhor é errar por tentar do que errar por se omitir! Não tenhas medo dos tropeços da jornada. Não podemos esquecer que nós, ainda que incompleto, fomos o maior aventureiro da história”.

Augusto Cury

SILVA, Jefferson Bugim Da; VARELA, Márcio Rodrigues Pires. **Gerenciamento de rede com auxílio do PRTG**. 2013. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) – Faculdade do Espírito Santo, Cachoeiro de Itapemirim, 2013.

RESUMO

Muitos dos profissionais técnicos e gerentes da área de redes de computadores possuem a percepção de que o gerente desta área necessita de ferramentas para o gerenciamento dos seus ativos e passivos. O objetivo do presente trabalho é verificar o comportamento de equipamentos em um ambiente de rede virtualizado utilizando-se para isto de duas máquinas como hospedeiras para a criação de máquinas virtuais. Na simulação mostra-se os dois ambientes e serviços diferentes em execução, em busca de alterações significativas no comportamento usando o protocolo SNMP. O ambiente de rede em questão foi analisado pelo software PRTG, software que faz uso de sondas para pesquisar e monitorar os serviços da rede, e o hardware dos hosts e servidores. No hardware, o ponto de preocupação era a utilização da memória e do processador. Na parte lógica da estrutura proposta, optou-se por monitorar o tráfego de rede, possibilitando a captura de informações do tráfego de HTTP, upload, download. De forma geral, percebeu-se que o software PRTG correspondeu às expectativas sobre a captura de informações. As informações são disponibilizadas em tempo real e seus dados coletados são exibidos em gráficos para melhor tomada de decisão por parte do gestor, indicando o momento de modificar a estrutura, o que pode se traduzir em investimentos por parte da empresa. O software analisado supriu todas as expectativas esperadas em relação ao gerenciamento dos ambientes imposto, de modo que podemos afirmar que o PRTG atende a necessidade dos gestores para o gerenciamento completo dos seus ambientes de rede.

Palavras-Chave: PRTG. SNMP. Gerente. Rede.

SILVA, Jefferson Bugim Da; VARELA, Márcio Rodrigues Pires. **Gerenciamento de rede com auxílio do PRTG**. 2013. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) – Faculdade do Espírito Santo, Cachoeiro de Itapemirim, 2013.

RESUMEN

Muchos de los profesionales técnicos y gerentes del area de redes de ordenadores poseen la percepción de que la gerencia de esta area necesita de herramientas para la gestión de sus activos y pasivos. El objetivo de este trabajo es apuntar el comportamiento de materiales en un ambiente de red virtualizado, utilizándose para esto dos máquinas como huéspedes para la creación de máquinas virtuales. En el simulacro se muestra los dos ambientes y servicios distintos en la ejecución, con una búsqueda de alteraciones significativas en el comportamiento usando el protocolo SNMP. El ambiente de red en cuestión fue analizado por el software PRTG, éste que hace uso de sondas para pesquisar y monitorar los servicios de la red, y el hardware de los hosts y servidores. En el hardware, el punto de preocupación era la utilización de la memoria y el procesador. En la parte lógica de la estructura propuesta, se eligió por monitorar el tránsito de red, haciendo posible la captura de informaciones del tránsito de HTTP, upload y download. De forma general, se pudo percibir que el software PRTG correspondió a las expectativas sobre la captura de informaciones. Las informaciones son disponibilizadas en tiempo real y sus datos colectados son exhibidos en gráficos para una mejor tomada de decisión de parte del gestor, indicando el momento de cambiar la estructura. Esto que puede traducirse en incrementos de parte de la empresa. El software analizado suplió todas las expectativas esperadas en relación al gerenciamento de los ambientes puestos, de modo que podemos afirmar que el PRTG atiende la necesidad de los gestores para el total gerenciamento de sus ambientes de red.

Palavras-Chave: PRTG. SNMP. Gerente. Red.

LISTA DE ILUSTRAÇÕES

Figura 1 – Modelo SNMP	17
Figura 2 – Modelo FCAPS	19
Figura 3 – gerenciamento de segurança	20
Figura 4 – arquitetura de gerencia SNMP	27
Figura 5 – software CACTI	29
Figura 6 – software openNMS	30
Figura 7 – software MRTG	31
Figura 8 – software Whats up gold	32
Figura 9 – software PRTG	33
Figura 10 – licença do PRTG	37
Figura 11 – Manutenção do PRTG	37
Figura 12 – Rede em Packet tracer	42
Figura 13 – Analise de processamento do hospedeiro 1 - rede 1	44
Figura 14 – Analise de processamento do hospedeiro 2- rede 2	45
Figura 15 – Analise de processamento do Cliente 1- rede 1	46
Figura 16 – Analise de processamento do Cliente 1- rede 2	46
Figura 17 – Analise de processamento do Cliente 2- rede 1	47
Figura 18 – Analise de processamento do Cliente 2- rede 2	47
Figura 19 – Analise de processamento do Cliente 3- rede 1	48
Figura 20 – Analise de processamento do Cliente 3- rede 2	49
Figura 21 – Analise de processamento do Cliente 4- rede 1	49
Figura 22 – Analise de processamento do Cliente 4- rede 2	50

Figura 23 – Analise de utilização de Memória do hospedeiro 1- rede 1	50
Figura 24 – Analise de utilização de Memória do hospedeiro 2- rede 2	51
Figura 25 – Analise de utilização de Memória do Cliente 1- rede 1	52
Figura 26 – Analise de utilização de Memória do Cliente 1- rede 2	52
Figura 27 – Analise de utilização de Memória do Cliente 2- rede 1	53
Figura 28 – Analise de utilização de Memória do Cliente 2- rede 2.....	53
Figura 29 – Analise de utilização de Memória do Cliente 3- rede 1	54
Figura 30 – Analise de utilização de Memória do Cliente 3- rede 2	54
Figura 31 – Analise de utilização de Memória do Cliente 4- rede 1	55
Figura 32 – Analise de utilização de Memória do Cliente 4- rede 2.....	55
Figura 33 – Analise de utilização da banda da internet hospedeiro 1- rede 1	56
Figura 34 – Analise de utilização da banda da internet hospedeiro 2- rede 2	56
Figura 35 – Analise de utilização da banda da internet cliente 1- rede 1	57
Figura 36 – Analise de utilização da banda da internet cliente 1- rede 2	58
Figura 37 – Analise de utilização da banda da internet cliente 2- rede 1	58
Figura 38 – analise de utilização da banda da internet cliente 2- rede 2	59
Figura 39 – Analise de utilização da banda da internet cliente 3- rede 1	59
Figura 40 – Analise de utilização da banda da internet cliente 3- rede 2	60
Figura 41 – Analise de utilização da banda da internet cliente 4- rede 1	60
Figura 42 – Analise de utilização da banda da internet cliente 4- rede 2	61

Lista de Tabelas

Tabela 1 - Elementos de rede 1	41
Tabela 2 - Elementos de rede 2.....	42

LISTA DE SIGLAS

- CMIP** - Common Management Information Protocol
- DMZ** - Zona desmilitarizada
- FCAPS** - Fault, Configuration, Accounting, Performance and Security
- HTML** – Hyper Text Markup Language
- IETF** - Internet Engineering Task Force
- MIB** - Management Information Base
- MRTG** - The Multi Router Traffic Grapher.
- RMON** - Remote Monitoring
- RFC** - Request for Comments
- SMI** - estrutura de informações de gerenciamento
- SNMP** - Simple Network Management Protocol
- TCP** - Transmission Control Protocol

SUMÁRIO

1 INTRODUÇÃO	11
2 PROTOCOLOS DE COMUNICAÇÃO PARA GESTÃO DE REDES	14
2.1 Protocolos de Gestão: atividades e conceitos	14
2.1.1 SNMP (protocolo específico)	15
3 FUNÇÕES DE GERENCIAMENTO	19
3.1 Gerenciamento de Segurança	19
3.2 Gerenciamento de Desempenho	20
3.3 Gerenciamento de Configuração	21
3.4 Gerenciamento de Contabilização	22
3.5 Gerenciamento de Falhas	23
4 GERÊNCIA DE REDES DE COMPUTADORES	25
4.1 Gerência de Redes e suas Ferramentas	25
4.1.1 Estruturas a serem gerenciadas (periféricos diversos de rede)	27
4.1.2 Ferramentas de Gestão (Ferramentas no geral PRTG)	28
5 SOFTWARE PARA GESTÃO DE REDES	34
5.1 Histórico e Mercado	34
5.1.1 PRTG	35
5.1.2 Dados técnicos do software	35
5.1.3 Estrutura do PRTG	38
6 AMBIENTE ESTUDADO	40
6.1 Máquina Virtual	40
6.1.1 Software (virtual box)	40
6.1.2 Configuração (hospedeiro e cliente padrão / hardware)	41
6.1.3 Estrutura em rede (Packet tracer)	42
6.1.4 Justificativa para o uso de máquina virtual	43
7 ANÁLISE DA SIMULAÇÃO	44

7.1 Análise de processamento dos hospedeiros	44
7.2 Análise de processamento dos clientes	46
7.3 Análise de utilização de memória dos hospedeiros.....	50
7.4 Análise de utilização de memória dos clientes	51
7.5 Análise de utilização da banda da interface de rede dos hospedeiros	55
7.6 Análise de utilização da banda da interface de rede dos clientes	57
8 CONSIDERAÇÕES FINAIS	62
9 REFERÊNCIAS.....	64

1 INTRODUÇÃO

Com o advento da internet os tipos de serviços à disposição tornaram-se mais numerosos, e com este crescimento o tráfego de dados cresceu paralelamente com o desenvolvimento de novas tecnologias. Com esta grande quantidade de dados trafegando e a limitação dos equipamentos e links, surgem a necessidade de monitorar o tráfego de informações a fim de verificar os gargalos existentes em uma determinada rede.

É a partir do monitoramento que se pode solucionar problemas atuais e evitar futuras deficiências nos sistemas. Uma rede local pode ter problemas que a impeçam de se manter operacional por muito tempo, pois as tarefas gerenciais de uma rede devem ser monitoradas no sentido de prevenir e detectar possíveis problemas.

Segundo Comer (2001), a utilização de software de gerência de rede é um artifício para que o gerente encontre problemas e possa sanar sua causa. Esses tipos de softwares tem como base o protocolo SNMP, que são capazes de monitorar o estado de serviços e equipamentos da rede.

O gerenciamento de rede com software PRTG tem como objetivo minimizar os problemas com segurança, eficiência e transparência da rede. Estes problemas advêm do crescimento dos usuários conectados a rede e dos mecanismos que são usados para interligar os usuários e suas informações. Este tráfego de dados, dependendo de seu porte, pode influenciar na disponibilidade da internet para um determinado usuário ou trazer para máquina softwares que tem como intuito roubar informações e danificar os computadores onde estão alojados.

Com o crescimento e dependência da rede de computadores nas empresas um dos principais problemas nas organizações vem sendo a falta de controle de tráfego na rede. Os gerentes de redes têm como tarefas monitorar o tráfego de dados com a utilização de software específico. Para isto, o PRTG é utilizado para descobrir hosts que utilizam muita banda da internet, confirmando se o host esta realmente

utilizando toda banda da internet ou está com algum vírus que faz a utilização da internet sem permissão.

Portanto, o objetivo deste trabalho de conclusão de curso é verificar o comportamento de equipamentos em um ambiente de rede virtualizado utilizando-se para isto de duas máquinas como hospedeiras para a criação de máquinas virtuais tendo como objetivos específicos:

- Criar um ambiente de teste para o software;
- Demonstrar graficamente a utilização de acesso internet de determinados hosts;
- Instalar o software PRTG em uma rede empresarial;
- Analisar os resultados do PRTG;
- Analisar o protocolo SNMP;
- Buscar problemas ou eventuais anomalias no comportamento da rede;
- Fundamentar a utilização do SNMP pelo programa.

Neste trabalho de conclusão de curso é proposta uma solução em software para análise de rede, tendo como referência o PRTG, a fim de gerenciar a estrutura de rede e utilizar suas ferramentas para detectar possíveis falhas existentes. Com o uso das ferramentas do sistema PRTG é possível gerenciar a segurança, o desempenho, as configurações da rede, contabilizar os acessos de rede e corrigir as falhas que surgirem nestes processos.

O sistema PRTG é considerado um dos mais robustos e utilizados por profissionais da área de gerenciamento de rede. Porém, sua utilização necessita de um conhecimento básico sobre o protocolo SNMP que tem como função serviços de

gerenciamento utilizando arquitetura distribuída. Através de testes e simulação pode-se comprovar, se for o caso, a viabilidade do sistema de gestão.

2 PROTOCOLOS DE COMUNICAÇÃO PARA GESTÃO DE REDES

2.1 Protocolos de Gestão - atividades e conceitos

Para que ocorra a troca de informações entre gerente/agente é necessário que haja um protocolo de gerência que tem como finalidade o monitoramento dessa transação e controles. Existem alguns tipos de protocolos de gerenciamento de rede que possuem esta finalidade.

Um destes protocolos de gerenciamento existente é o CMIP (Common Management Information Protocol), que foi criado pela ISO. Segundo Menezes e Silva (1998) foi projetado para fornecer soluções simples para gerenciar a rede como um todo. Apesar da proposta de prover soluções de prover soluções simples, o protocolo CMIP é considerado sofisticado, por suas ferramentas. É utilizado em redes mais simples e também em redes mais complexas, possuindo mais alternativas que o protocolo SNMP.

O protocolo CMIP utiliza muito mais os recursos de sistema do que SNMP. Deste modo existem poucos sistemas que possuem a capacidade de manipular uma implementação completa do CMIP e também é muito difícil para programar neste protocolo, sendo complexo, aumenta a dificuldade para o desenvolvedor do sistema, além de apresentar características que são desnecessárias em alguns casos.

De acordo com Lessa (1999) o RMON (Remote Monitoring) é um protocolo de gerenciamento de monitoramento remoto, desenvolvido pela mesma entidade que criou o TCP/IP sendo um padrão IETF. Dessa forma, este protocolo não é uma solução proprietária. Este protocolo tem o intuito de analisar o tráfego, identificar resoluções de problemas, demonstrações de tendência em gerenciamento proativo de rede.

O protocolo de gerenciamento RMON é um dos primeiros a ter a funcionalidade de detectar problemas, tendo a possibilidade de notificação para que possam ser feitos os ajustes necessários. Fazendo que os custos de manutenção de uma rede tenham

um declínio, este protocolo está embutido no SNMP e seu padrão é uma MIB que tem o intuito de gravar os esquemas proativos. Espera-se uma implementação no protocolo RMON que venha dar suporte a arquitetura cliente/servidor e a topologia avançada.

Não devemos deixar de citar o protocolo TCP (Transmission Control Protocol), Gerchman e Weber (2006) define o protocolo como uma ponte serviço de transferência confiável de dados entre aplicações parceiras, O TCP também garante que os dados são entregues livres de erro, em sequência e sem perdas ou duplicação.

2.1.1 SNMP (protocolo específico)

O protocolo de enfoque deste trabalho científico foi criado pelo departamento de defesa dos EUA, com o intuito de distribuir de forma fácil e prática para o gerenciamento de equipamentos de rede, através de um protocolo com base na monitoração de gateways IP um monitoramento simples e claro em tempo real da rede, sendo empregado no gerenciamento de diversas formas de sistema (ESTEVEZ, Jr, 2013).

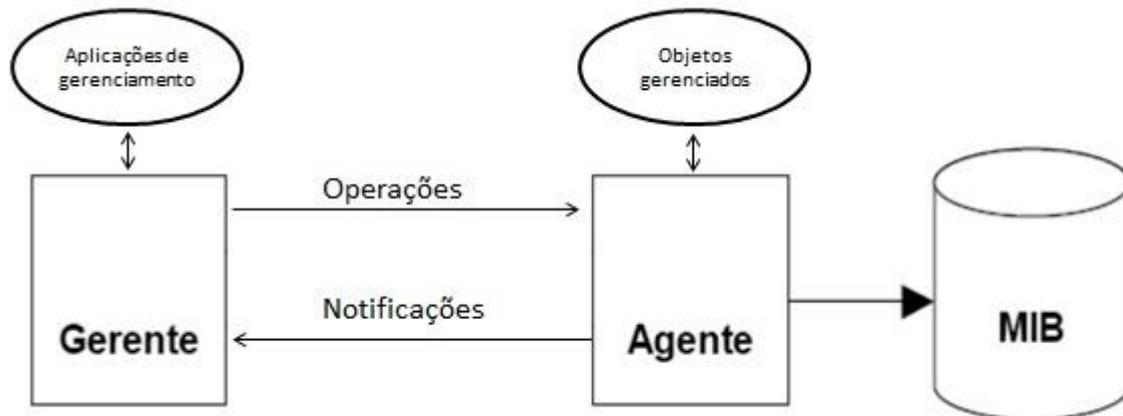
O protocolo SNMP (Simple Network Management Protocol), que de acordo com Oliveira (2002) usufrui do serviço do protocolo de transporte UDP e foi padronizado nos anos 80 pelo grupo chamado IETF (Internet Engineering Task Force) que é responsável pelas especificações de padrões para a internet. Este modelo vem sendo utilizado nos últimos 12 anos como padrão de gerenciamento de equipamentos de rede pela simplicidade de implementação e sua eficiência, devido ao pouco consumo de recurso de rede e processamento, podendo ser incluso em equipamentos simples. O SNMP é baseado no gerenciamento do modelo OSI (International Organization for Standardization) e requer a presença de três componentes básicos que Azambuja (2000) cita e define suas características como:

- Agentes: pode ser definido por duas formas distintas: pela maneira que são implementadas as suas funcionalidades no protocolo SNMP e pela forma que ocorre a interação com os dispositivos gerenciados;

- Agente extensível: apresenta implementação das funcionalidades do protocolo SNMP. Para uma comunicação com os dispositivos gerenciados é essencial a criação de agentes estendidos. Também não possuem nenhum suporte ao MIB, para haver interação com o mesmo deve existir uma biblioteca para que haja este suporte.
 - Agente Estendido: este agente busca informações por meio de funções básicas de comunicação. As respostas das requisições do protocolo SNMP são concluídas apenas pelo agente extensível. Desta forma, o agente estendido faz a comunicação com o dispositivo gerenciado e disponibiliza ao agente extensível informações da monitoração.
- Gerente: É um software executado junto ao servidor que possibilita o recebimento e envio de informações de gerenciamento. Através dessa aplicação é possível o monitoramento dos agentes em requisições de dados na base de informação;
 - MIB (Management Information Base): Ela é à base de informações de gerenciamento e utiliza diversas variáveis para simbolizar informações dinâmicas ou estáticas junto com um tipo de dispositivo gerenciado. Tem como objetivo encaminhar a troca de dados existentes na base de informações de gerenciamento com softwares gerente/agente. O agente tem a capacidade de comunicar-se com o gerente através de consultas SNMP sobre o conjunto de informações contido na MIB, criando-se um arquivo de MIB onde são armazenadas informações que auxiliam ao gerente as informações de alerta do agente para o gerente e solicitações de informações do gerente para o agente.

[...] “O SNMP ajuda o administrador a localizar e corrigir erros ou problemas de uma rede. Através de agentes SNMP, o administrador da rede consegue visualizar estatísticas de tráfego da rede e após analisar estes dados o administrador pode atuar na rede, alterando a sua configuração” (OLIVEIRA, 2002, p.3).

Figura 1 – Modelo SNMP



Fonte: Pesquisa do autor

Na imagem 1 pode-se observar todo o processo de comunicação entre gerente, agente e a mib. Entre o tráfego de gerente e agente, analisaremos o tráfego de informações entre eles, onde o gerente é o responsável por enviar os dados com as informações das operações a serem feitas pelo agente. Ao receber estes comandos o agente irá capturar as informações solicitadas e enviá-las através de notificações para o gerente. Ao término deste processo o responsável pelo armazenamento dos dados obtidos é a MIB que irá posteriormente disponibilizá-los para os softwares capturarem estes dados de acordo com a necessidade do gestor.

O SNMP possui três versões que Moqadi (2011) descreve-o como:

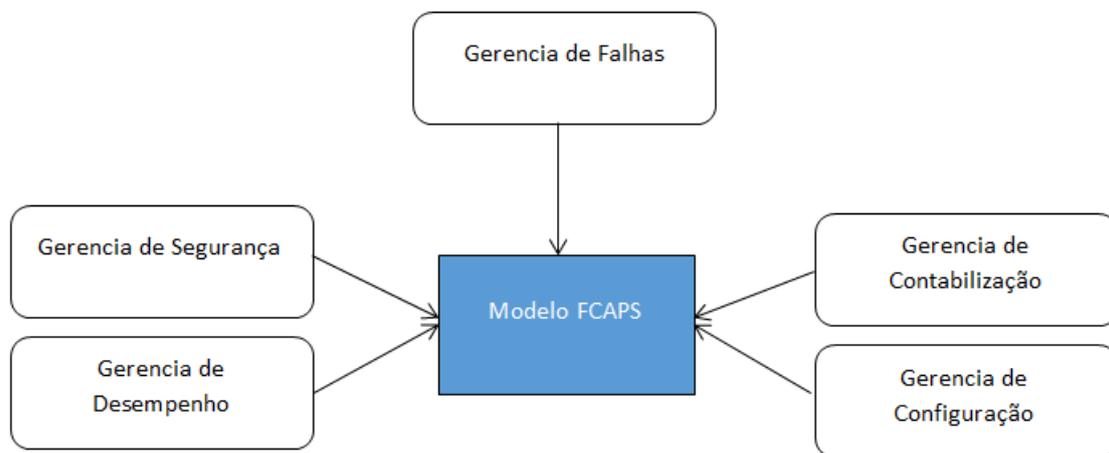
- **SNMPv1:** Nesta versão existem três tipos de documentos o RFC 1155, que tem como função a definição de mecanismos de captura dos objetos a serem gerenciados e os descrevem e renomeiam. O segundo documento, RFC 1155, define o SNMP e, por fim, o documento RCF 1212 possui uma descrição mais concisa do que a RFC 1155. A sua segurança é simples, pois qualquer aplicativo baseado em SNMP tem acesso as informações de gerenciamento de dispositivo;

- SNMPv2: Sua definição esta presente nas RFCs 1902 a 1907 e se baseia em strings de comunidade. A diferença sobre a primeira versão é a melhoria na eficiência e desempenho como operador get-bulk que notifica eventos confirmados como operador inform e maior detalhamento de erros;
- SNMPv3: A versão três é definida nas RFCs 1905 a 1907 e 2570 a 2786. A diferença entre estas versões é definida por Mauro e Schmidt (2001) em que a versão SNMPv3 supre a falta de segurança existentes nas duas versões anteriores e possui suporte para as operações existentes nas versões 1 e 2. Logo, a terceira versão só opera os problemas com segurança.

3 FUNÇÕES DE GERENCIAMENTO

Cardoso (2010) cita a International Organization for Standardization como a criadora de um modelo de gerenciamento, o FCAPS – (Fault, Configuration, Accounting, Performance and Security), que surgiu com o intuito de situar os cenários apresentados em um quadro mais estruturado. Em sua criação houve a definição de cinco áreas para o gerenciamento de redes, que são gerenciamento de segurança, desempenho, configuração, contabilização e falhas, também ilustradas na figura 2.

Figura 2 - Modelo FCAPS



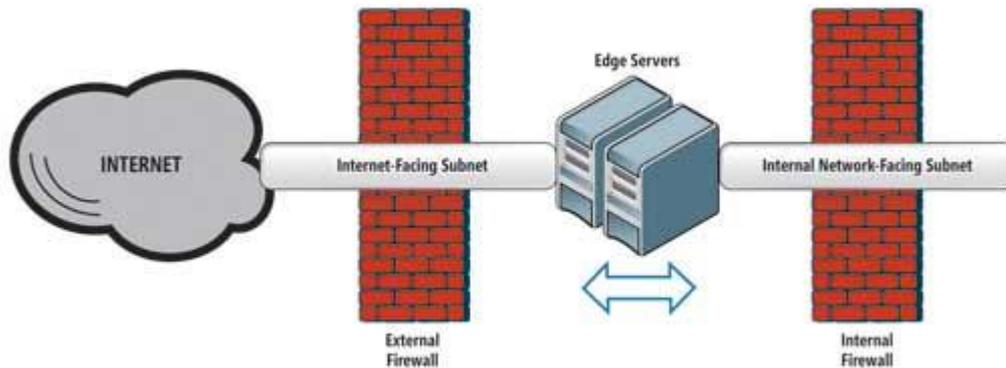
Fonte: Pesquisa do autor

Na imagem 2 pode-se ver claramente que o modelo FCAPS é composto pela união de cinco modelos de gerenciamento na qual são responsável pelo gerenciamento da rede por completo.

3.1 Gerenciamento de Segurança

Este tipo de gerenciamento é definido por Kurose e Rose (2010) como um serviço cuja finalidade é a monitoração de acessos aos recursos presentes na rede. Este monitoramento é efetuado de acordo com definições de normas impostas pelo gestor. Nesta gestão é necessária a utilização de componentes como as centrais de distribuições de chave e autoridades certificadoras. Outro ponto importante é aplicar o uso do firewall para gerenciar os pontos externos de acesso à rede.

Figura 3 – Gerenciamento de segurança



Fonte: Autoria própria

Mostra-se na figura 3, uma rede com proteção de dois firewalls, caracterizando uma DMZ – Zona desmilitarizada, objeto do monitoramento feito por este tipo de gerenciamento. Observa-se que há uma clara tendência em centralização das ferramentas de segurança, porém o gerenciamento deve ser feito em todos os elementos responsáveis pelo enlace e link de dados.

3.2 Gerenciamento de Desempenho

Segundo Kurose e Rose (2010) o gerenciamento de desempenho é utilizado com a finalidade de medir, analisar, qualificar, informar e controlar o desempenho de diversos componentes da rede. Dentre os componentes existentes estão presentes os periféricos individuais como roteadores, hospedeiros e enlaces bem como os trajetos do tráfego de informações na rede. Deve-se lembrar que o protocolo SNMP tem o papel decisivo para o gerenciamento de desempenho da internet, analisando os equipamentos da rede local para este gerenciamento.

- Ribeiro e Gerk (2005) fala que o desempenho corrente em uma rede deve-se basear em indicadores, throughput, disponibilidade, utilização, taxa de erros, recuperabilidade, tempo médio entre falhas, entre outros. É possível através da monitoração de indicadores estabelecer um comportamento normal da

rede. Com esta definição é possível gerar eventos ou alarmes e registros históricos, que permitem aos gestores fazerem uma análise de desempenho e um planejamento de capacidade, indicando a necessidade de mudança na rede.

- Nos tópicos seguintes Ribeiro e Gerk (2005), cita algumas estatísticas de desempenho de acordo com o elemento monitorado
- Interfaces: utilização dos enlaces por unidade de tempo, utilização por protocolo, qualidade dos enlaces por unidade de tempo (fração de erros na entrada e na saída, número total de erros, disponibilidade, piores interfaces diariamente, etc);
- Roteadores: utilização de CPU e memória, disponibilidade, taxa de descarte, taxa total de pacotes comutados por segundo;
- LANs Ethernet: percentagem de colisões;
- Hosts: taxa de retransmissão TCP.

3.3 Gerenciamento de Configuração

O método de gerenciamento de configuração é citado por Magalhães (2010) como um processo que tem a responsabilidade de fornecer as informações precisas sobre a infraestrutura de TI, verificar todos os itens de configuração que estão sendo utilizados, assim como gerenciar o banco de dados da gestão de configuração onde é encontrada a base de dados contendo detalhes da configuração do ambiente. Este tipo de gerenciamento não possui um modelo a ser seguido, sendo possível localizar modelos diferentes do padrão.

Ribeiro e Gerk (2005) cita suas funções básicas como:

- Coleta de dados de configuração através do descobrimento dos elementos e da interconectividade entre os elementos encontrados;

- Geração de eventos a partir da adição ou remoção de recursos, permitindo a manutenção de um inventário atualizado;
- Atribuição de valores iniciais aos parâmetros dos elementos gerenciados;
- Registro de informações de configuração que possibilite emissão de relatórios a partir dos dados coletados nas funções anteriores;
- Alterar as configurações dos elementos gerenciados para corrigir alguma falha ou problema de segurança existente, ou mesmo redimensionar a alocação de recursos com o intuito de melhorar o desempenho, onde existe uma relação com a área de Gerenciamento de Desempenho;
- Início e Encerramento das operações dos elementos gerenciados.

Magalhães (2010), ainda ressalta as vantagens obtidas através do gerenciamento de configuração traz ao gestor um extenso controle para incidentes e problemas, além prover planos táticos para poder gerenciar os itens de configurações que abrange os hardwares, softwares e documentações, conseqüentemente auxilia o plano orçamentário e possibilita a redução da utilização de softwares sem licenciamento.

3.4 Gerenciamento de Contabilização

Neste tipo de gerenciamento Kurose e Rose (2010) os cita como cruciais para o gerente poder administrar, registrar e controlar o acesso de usuários e dispositivos que estejam utilizando os recursos presentes na rede. Com este poder de gerenciamento abre-se a possibilidade do gestor controlar cobrança por utilização e alocação de acesso privilegiado a recursos.

Ribeiro e Gerk (2005) completa citando as suas principais funções como:

- A coleta de informações: nela é monitorado quais e quando os recursos são utilizados e por quem estão sendo usados;
- Estabelecer cotas de utilização dos dados, estabelecendo limites aos usuários os recursos que poderão ser acessados;
- Aplicação de tarifas e faturamento;
- Estabelecer escala de tarifação: estas escalas vão servir como estatísticas para os gestores.

3.5 Gerenciamento de Falhas

O método de gerenciamento de falhas tem como finalidade fazer uma prevenção e resolução definitiva de falhas desconhecidas ou provocadas por incidentes. Existem ações que auxiliam na gestão de problemas como controle de problemas, controle de erros conhecidos, prevenção proativa, apoio ao Tratamento dos Incidentes, revisão dos principais problemas e informações gerenciais (MAGALHÃES, 2010).

Ribeiro e Gerk (2005) simplifica o gerenciamento de falhas em tarefas básicas como:

- Diagnóstico de problemas ou Isolação de falhas;
- Soluções emergenciais para evitar a paralisação da rede;
- Resolução de problemas;
- Notificação e registro ou Supervisão de alarmes.

Os problemas que vão ocorrendo no decorrer dos dias afetam diretamente o funcionamento da TI, comprometendo diretamente seu desempenho, entretanto é necessária uma administração pró ativa que minimize os impactos causados pelos problemas atuais e futuros.

Levando em consideração casos que podem danificar a movimentação de dados e serviços do cotidiano do usuário é necessária a utilização de prevenções a fim de tratar situações antes mesmo que aconteçam, minimizando os problemas do usuário com o setor de TI. Após o estudo de caso dos possíveis problemas, é necessário que ocorra a construção de uma documentação dos processos, adicionando neste documento procedimentos e históricos de mudanças (MAGALHÃES, 2010).

A comunicação com o usuário é crucial para obter sucesso com gerenciamento de falhas. A nível de gerencia é interessante a divulgação dos passos da criação do projeto e sua resolução para outros gerentes a fim de padronizar boas práticas de elaboração de projetos para o gerenciamento de falhas.

Segundo as boas práticas de gerenciamento é possível obter bons resultados. Segundo Magalhães (2010), os resultados mais evidentes são:

- Otimização da disponibilidade dos serviços;
- Redução no volume de incidentes;
- Soluções permanentes;
- Melhor uso dos recursos de TI;
- Melhoria na monitoração do ambiente;
- Disseminação do conhecimento;
- Redução do impacto negativo para o negócio.

4 GERÊNCIA DE REDES DE COMPUTADORES

4.1 Gerência de Redes e Suas Ferramentas

O crescimento da variedade de equipamentos de rede aumentou por consequência a probabilidade de possíveis problemas e a dificuldade para solucioná-los, exigindo dos gerentes um melhor entendimento das redes e ferramentas que ele utiliza. Assim, o gerenciamento de rede ajuda os gerentes a trabalhar com a dificuldade dos dados envolvidos, garantindo segurança, eficiência e transparência da rede para os usuários de acordo com Melchior (2003).

Segundo Albuquerque (2011), no gerenciamento de uma rede existe a integração e a coordenação de elementos de hardware e software, com o intuito de monitorar, testar, consultar, configurar, analisar, avaliar e controlar recursos da rede, e possuem elementos que além de cumprir condições operacionais de desempenho e de qualidade de serviço em um custo baixo e em tempo real.

De acordo com Sztajnberg (2012) gerência de redes é um controle de atividades e de recursos da rede, sendo que para haver este controle é necessário que se obedecem etapas básicas a serem seguidas, como a obtenção de informações da rede, e utilizar esta informação para identificação de um problema e visar soluções dos problemas apresentados.

Convenciona-se através do que diz Sztajnberg (2012) que para o gerente ter êxito no gerenciamento é importante que ele tenha um conhecimento profundo em procedimentos, desempenho e descobertas de falhas que virão acontecer.

Para o auxílio do gerente existem sistemas que tem como objetivo reduzir a sobrecarga de informações sobre o gerente. Tanenbaum (1999) cita elementos que consiste em um sistema de gerenciamento:

- **Dispositivos gerenciados:** São os hardwares que estão conectados na rede, computadores, roteadores e serviços de terminais;

- **Agentes:** São softwares que estão interligados na rede e coletam e armazenam informações de gerenciamento;
- **Base de informação de gerenciamento:** As informações recolhidas pelos agentes são depositadas nesta base;
- **Gerente:** (CONTESSA E POLINA, 2006) é uma aplicação que fica instalada e executando no host do gerenciamento, sendo possível a execução de um ou vários gerentes no mesmo host unindo-se com intuito de coletar as informações para o gerenciamento. Algo em comum entre estes gerentes é que ambos utilizam do mesmo protocolo de gerencia em que é disponibilizado pelo host ao qual estão associados.

A responsabilidade do gerente SNMP é implementar políticas que serão utilizadas pelos gestores para otimizar o gerenciamento da rede. Entre as funções disponibilizadas pelo gerente SNMP está o alerta de falha da rede. Este alerta é disponibilizado através de chamadas ou mensagens telefônicas, envio de e-mails, ou algum outro meio de comunicação viável para contato de forma rápida e eficiente com o gestor responsável.

Outra funcionalidade interessante disponibilizada é a visualização através de gráficos dos estados dos equipamentos, que possibilita ao gerente visualizar a evolução dos valores ou condições do equipamento ao longo do tempo, disponibilizando as informações sobre o comportamento e as tendências dos equipamentos.

O presente trabalho tem um capítulo específico sobre o tema, portanto será abordado novamente.

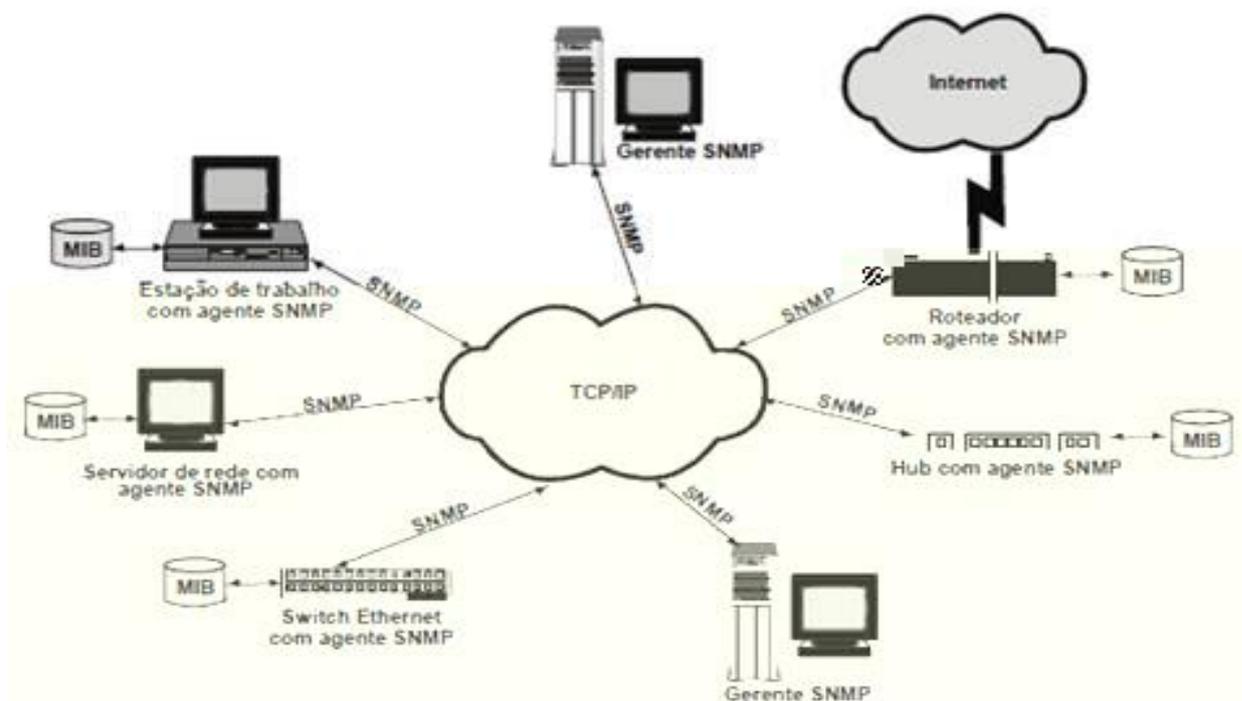
O gerenciamento da rede segue algumas etapas de acordo com Cardoso (2012), são elas:

- **Coleta de dados:** é um método geralmente automático, que consiste de monitoração sobre os recursos gerenciados;
- **Diagnóstico:** Este processo tem como objetivo tratar e analisar as informações realizadas de acordo com os dados coletados. São executados vários procedimentos que necessariamente não precisam ser feitos através de um operador no computador de gerenciamento. Esses procedimentos tem o intuito de identificar a causa do problema;
- **Ação:** após a identificação de um problema, caso seja um problema persistente é feita uma ação, ou controle sobre o local.

4.1.1 Estruturas a serem gerenciadas (periféricos diversos de rede)

Oliveira (2002) considera o protocolo SNMP como o protocolo que possibilita o gerenciamento em quase todos os equipamentos de forma simples e fácil de implementação tanto para o agente quanto para o gerente. A imagem ilustrativa 3 exemplifica alguns dos principais periféricos gerenciáveis.

Figura 3 - Arquitetura de gerencia SNMP



Fonte: http://www.teleco.com.br/tutoriais/tutorialgmredes2/pagina_2.asp, acesso em: 2013

Ao analisar-se a imagem 3, vê-se um dispositivo que possui um agente SNMP instalado, possibilitando seu monitoramento através de qualquer máquina que possua ferramenta de gerente e se utilize do protocolo SNMP.

4.1.2 Ferramentas de gestão

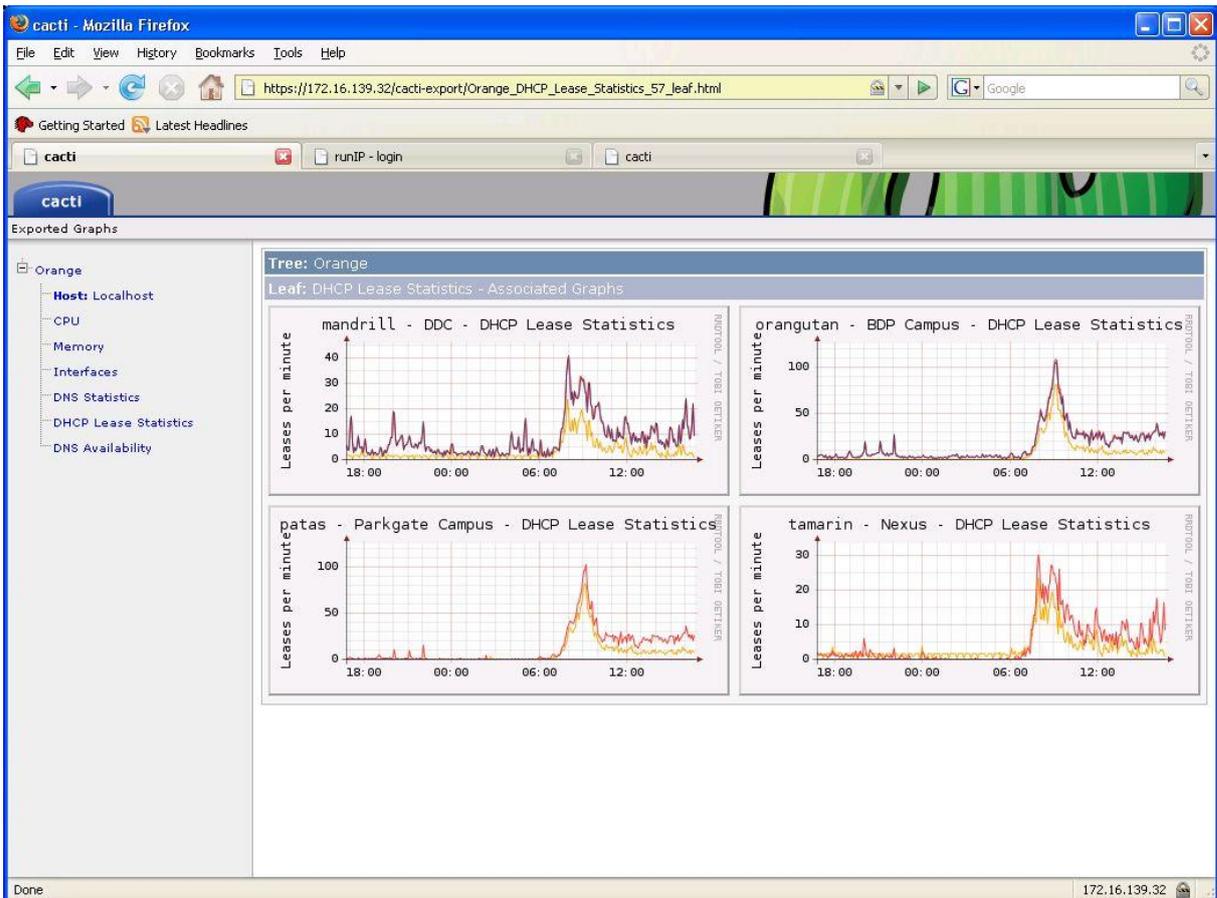
Existem diversos softwares proprietários e não proprietário para o gerenciamento de rede, que tem o objetivo de analisar e monitorar possíveis erros que possam vir a comprometer a eficácia da rede. Segundo Cardoso (2012), os softwares seguem o modelo Cliente-servidor, que convencionalmente tem uma aplicação “Servidora” na máquina gerente e uma aplicação “Cliente” no dispositivo monitorado, sendo que para evitar conflitos é utilizado “Gerente” para a aplicação servidora e “Agente” para os dispositivos clientes.

No ano de 2013 o mercado possibilita a utilização de diversas ferramentas para o gerenciamento da rede como NAGIOS, CACTI e OpenNMS. Citaremos abaixo estes softwares não proprietários e suas principais características:

Cardoso (2012) NAGIOS é um dos softwares mais conhecido para o gerenciamento de rede, que por sua vez tem o diferencial de notificar o administrador da rede através de sms de acordo com o que o usuário configurar por meio de plugin quando serviços ou equipamentos estiverem inoperantes, mostra-se neste ponto, ser abrangente nas suas funcionalidades, mostrando vantagens sobre alguns concorrentes. Porém, assim como os outros softwares, possui peculiaridades e pontos negativos, tais como relatórios insuficientes e grau de dificuldade maior para inserir novos dispositivos da rede.

Tem-se no software CACTI que tem o seu foco em apresentar graficamente informações como: tráfego na rede, uso de memória, espaço em disco, switches e roteadores, entre outros. As informações coletadas por ele são armazenadas em um banco de dados MySQL, podendo ser consultadas via web (YANO, 2010).

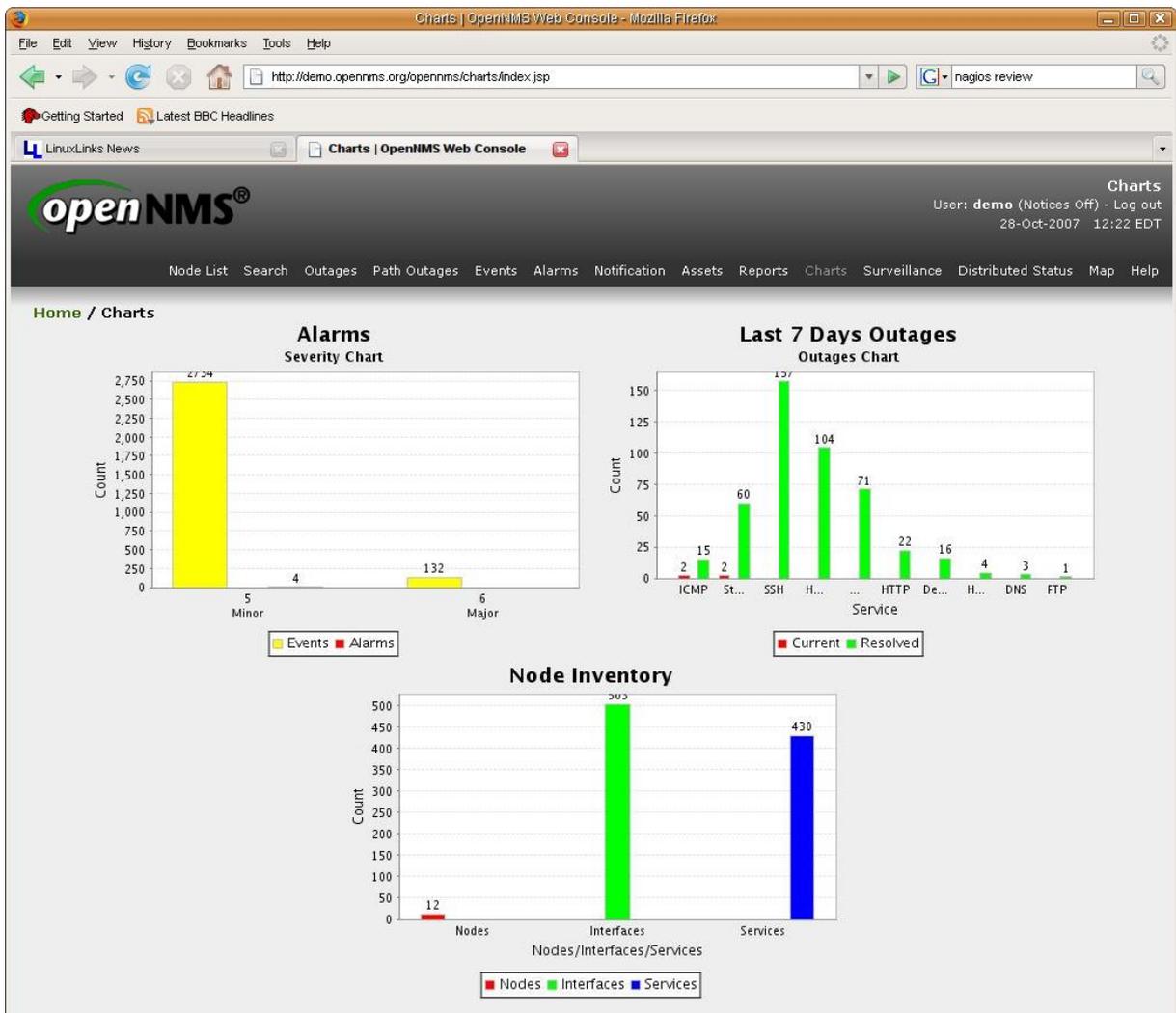
Figura 5 – Software CACTI



Fonte: CACTI, acesso em 2013

O OpenNMS é um projeto não proprietário que foi criado voltado para camada de aplicação. Tem as funcionalidades de fornecer para o gerente a qualidade/tempo de disponibilidade de serviço. Também contém opções de vários relatórios com tudo que foi analisado, sendo possível configurar alertas de falhas via e-mail (CARDOSO, 2012).

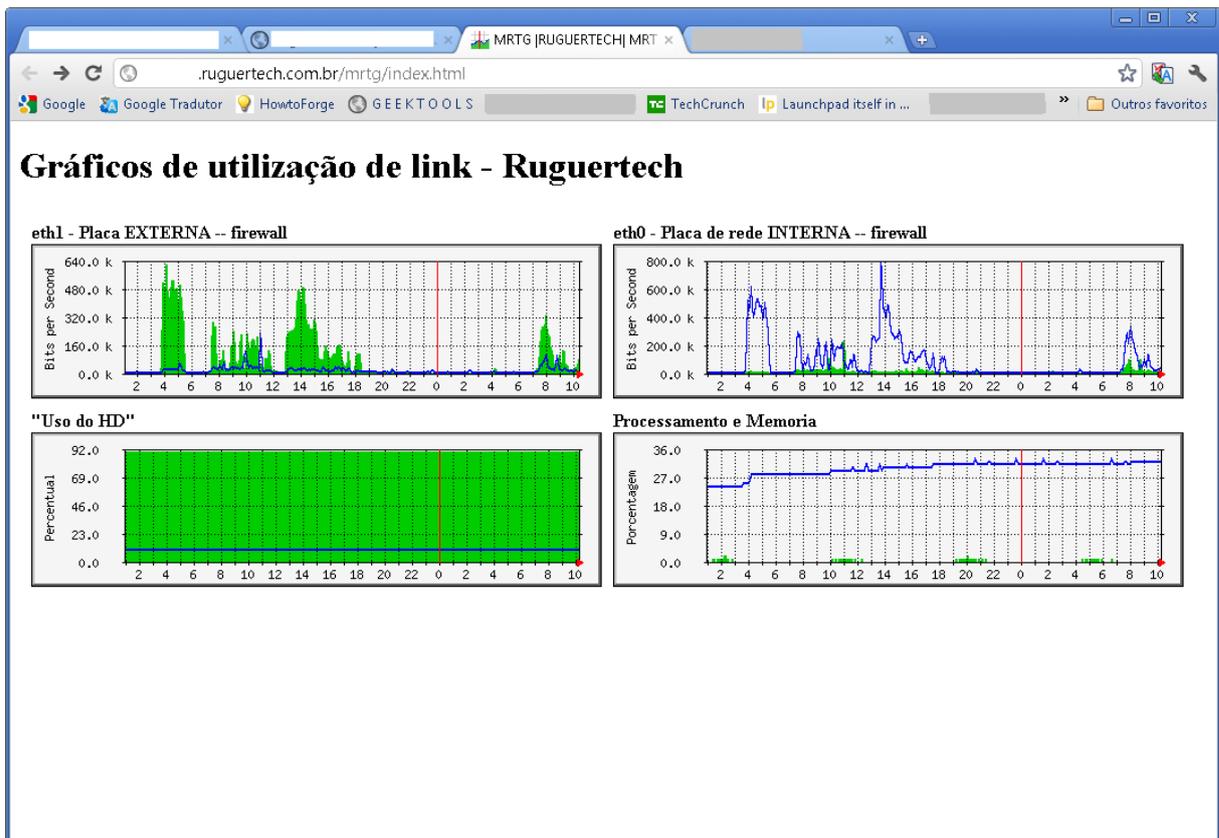
Figura 6 – Software openNMS



Fonte: OpenNMS, acesso em 2013

O MRTG é um software que utiliza o protocolo SNMP, oferecendo quaisquer informações que seja obtido através deste protocolo. Tem a possibilidade de gerar gráficos que pode ser visualizados em formato HTML e é basicamente usado para a análise de tráfego na rede sendo o mais utilizado atualmente. (BAZZI et al. 2007)

Figura 7 – Software MRTG

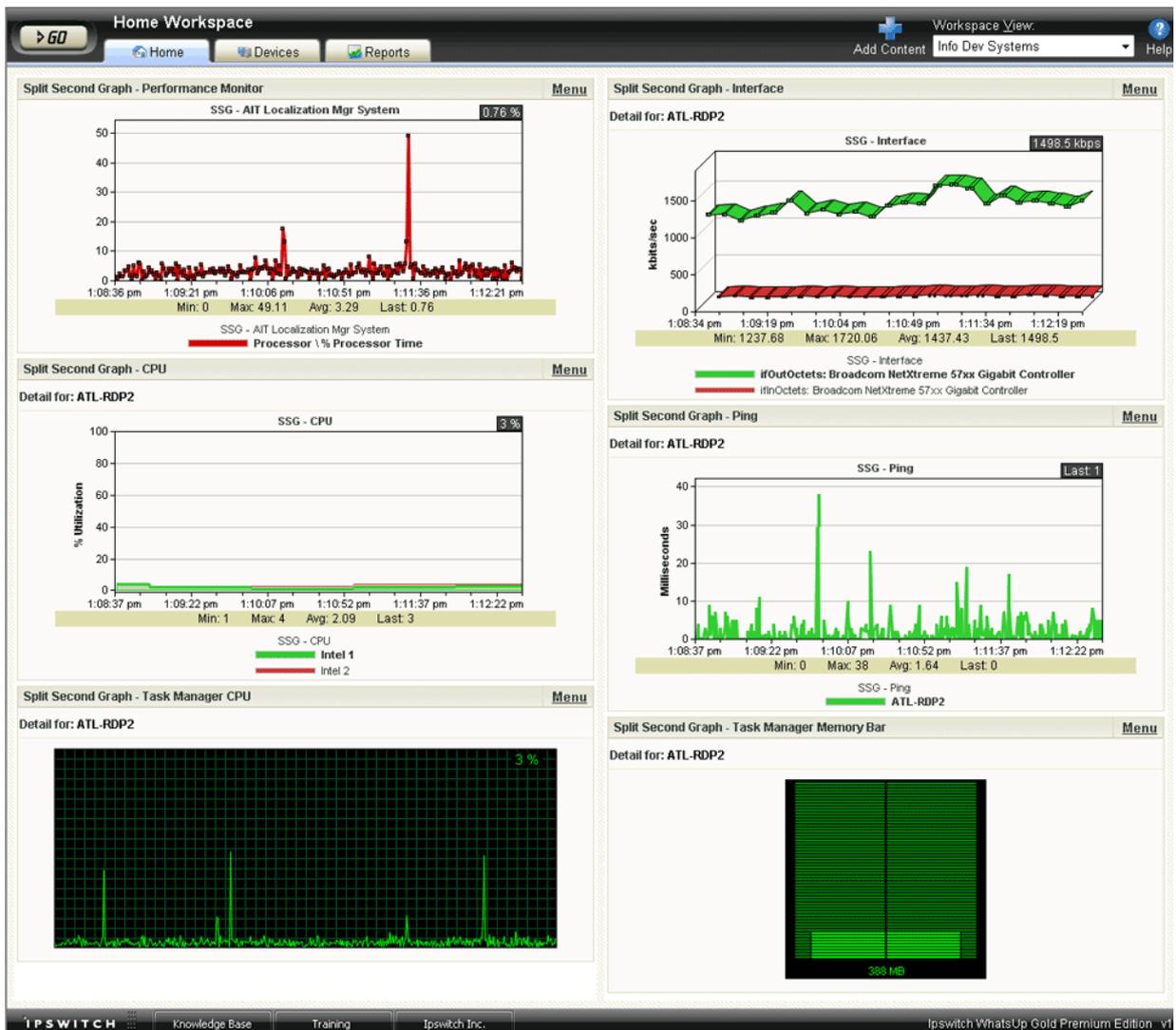


Fonte: MRTG, acesso em 2013

Diante dos softwares livres citados, mostraremos ao término deste parágrafo outros softwares de gerenciamento, porém de uso proprietário. Serão abordadas suas principais características, custo e benefício.

O software Whats Up Gold é desenvolvido pela empresa IPSWITCH, sendo que suas versões variam de acordo com a quantidade de máquinas na empresa, podendo variar de 25 máquinas a um valor de US\$2,195.00 até o pacote máximo de 500 máquinas no valor de US\$8,495.00. Segundo Albuquerque (2011), o Whats Up Gold é um sistema de fácil manuseio que permite ao usuário detectar, mapear e gerenciar toda a estrutura de TI da empresa, desde servidor, dispositivos de rede, recursos virtuais, aplicativos, tráfego e configurações da rede. O software visa proporcionar a seus usuários um aplicativo rico em recursos, porém mais fácil e intuitivo de se usar para proporcionar ao gestor de TI uma forma mais simples de gerenciamento sem pecar no desempenho e recursos.

Figura 8 – Software whats up gold



Fonte: Ipswitch, acesso em 2013

Segundo Guillermo (2008) o PRTG Traffic Grapher é um software baseado na plataforma Windows, entretanto pode-se monitorar sistemas linux. O software possibilita ao gestor monitorar não só a rede, mas também toda a estrutura da CPU e disponibiliza em tempo real gráficos dos dados da rede e dos hardwares.

Com os dados coletados é possível verificar onde estão os problemas, se estão na banda da internet ou na especificação técnica da máquina. Com esses dados em mãos, o gestor tem a possibilidade de ter uma visão ampla da rede e otimizar a sua eficiência, assim como fazer uma prevenção de futuros problemas que podem vir a ocorrer.

Figura 9 – Software PRTG



Fonte: Passler, acesso em 2013

O PRTG é executado 24h todos os dias e constantemente registra as informações do tráfego assim como o desempenho das máquinas conectadas á rede. Para sua aquisição no ano de 2013 a (PAESSLER, 2013) disponibiliza pacotes que variam de 100 sensores por US\$ 400,00 a um pacote corporativo com sensores ilimitados com o valor de US\$ 32,400.00.

5 SOFTWARE PARA GESTÃO DE REDES

A complexidade dos sistemas de rede e o grande número de protocolos e serviços a serem gerenciados iniciou uma busca por ferramentas que possibilitassem dinamicidade às análises com consequente retorno rápido dos serviços vitais para a continuidade dos trabalhos

Segundo Reynolds e Stair (2011) um ambiente empresarial normalmente contempla ferramentas Web e também consultas que são necessárias para o fluxo contínuo das tarefas prestadas pelo grande número de usuários dos Sistemas de Processamento de transações, por exemplo, que fazem parte da inserção e edição dos dados que possivelmente serão usados pela gerência na tomada de decisão.

Considera-se através desta análise acadêmico-empresarial que a necessidade destas análises está ligada diretamente à qualidade dos serviços de rede prestados para o cliente interno.

5.1 Histórico e Mercado

O Software PRTG surgiu de uma necessidade de seu desenvolvedor, Dirk Paessler, que em 1997 criou a empresa Paessler AG, no intuito de formalizar a estrutura empresarial que dá sustentabilidade à ferramenta. No desenvolvimento do software, priorizou as ferramentas que possibilitam ao administrador visualizar a disponibilidade e o desempenho da rede em uma única tela, com a vantagem de não necessitar de grande espaço em disco para a instalação da ferramenta completa.

A solução desenvolvida em módulos possibilita que empresas de diversos tamanhos, considerando sua rentabilidade, possam adquiri-lo. De acordo com Paessler (2013), o seu produto é considerado de ponta devido às suas funcionalidades, podendo ser usado por empresas como as listadas no Fortune 100, que classifica as 100 melhores do mundo, reiterando que 70% destas se utilizam do software.

5.1.1 PRTG

Silva (2012), considera que o PRTG é um software bem consolidado no mercado de gerenciamento de rede, capaz de monitorar na LANs, WANs, WLANs e VPNs seus tráfegos de banda de rede e sua disponibilidade, assim como outros segmentos dispersos a rede como uso de CPU, carga de memória, sistemas Windows e Linux, roteadores, servidor de e-mail e arquivo, switches entre outras funcionalidades. O PRTG facilita o cotidiano dos administradores, pois gera em tempo real relatórios e gráficos de dados gerados no host. Com estes relatórios os gestores podem verificar e prevenir problemas, além de otimizar a eficiência do sistema e da rede.

Para executar as verificações dos dados gerenciados o PRTG necessita de protocolos os quais irão auxiliar as coletas dos dados e a monitoração. Os protocolos mais utilizados são o Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), packet sniffer e Cisco NetFlow. Os dados coletados por estes protocolos são armazenados na MIB, proporcionando ao gestor utilizar estes dados para uma visão de longo prazo. (GUILHERMO, 2008)

5.1.2 Dados técnicos do software

Para a utilização do software PRTG são necessárias especificações técnicas mínimas para sua execução. Silva,(2012) detalha os requisitos para a execução de 1000 sensores. Para esta monitoração a máquina deve possuir:

- Um CPU para monitorar com facilidade os 1000 sensores é necessário possuir um processador de capacidade mediana construído a partir de 2007;
- A memória RAM deve possuir no mínimo 1024MB, será utilizado por sensor cerca de 150 kilobyte de RAM;
- Para o armazenamento o disco rígido deve possuir 200 kilobyte de espaço por dia para cada sensor.

De acordo com o fabricante Paessler (2013), é necessário que haja para sua execução compatibilidade com o sistema operacional. Existem sistemas que ocasionam perda de desempenho no processo, é o caso do Windows server 2008 R1 e Windows vista que não são recomendados para este tipo de monitoração, porem podem ser utilizados. Segue abaixo os tópicos de sistemas compatíveis com o PRTG.

- Microsoft Windows XP SP2 ou superior;
- Microsoft Windows Vista;
- Microsoft Windows Server 2003 SP1 ou superior;
- Microsoft Windows Server 2008;
- Microsoft Windows Server 2008 R2;
- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows Server 2012;

De acordo com o manual, fabricante Paessler (2013), o PRTG permite ao usuário utilizar o software para teste, é disponibilizada durante 30 dias a licença Trial Edition. Esta versão vem com todos os sensores disponíveis e sem limite de máquinas. Ao término deste período são disponibilizadas licenças de aquisição Caso o usuário não se interesse em adquiri-la o software permite que o usuário utilize a licença Freeware Edition. Esta versão é gratuito com apenas 10 sensores sem limite de tempo. (PAESSLER, 2013)

Nas imagens abaixo são exibidas as licenças, manutenções e seus respectivos valores.

Figura 10 – Licença do PRTG

Select Your PRTG License Type		
License 	Sensors 	Price including 12 months maintenance
<input type="radio"/> PRTG 100	100	US\$ 400.00
<input type="radio"/> PRTG 500	500	US\$ 1,350.00
<input checked="" type="radio"/> PRTG 1000	1,000	US\$ 2,230.00
<input type="radio"/> PRTG 2500	2,500	US\$ 4,700.00
<input type="radio"/> PRTG Unlimited	unlimited	US\$ 10,800.00
<input type="radio"/> PRTG Corporate	unlimited	US\$ 32,400.00

Fonte: Paessler, acesso em 2013

Nesta figura a PAESSLER disponibiliza os pacotes de licenças com o limite de sensores disponíveis que variam de acordo com cada pacote e seus respectivos valores de aquisição.

Figura 11 – Manutenção do PRTG

Choose Maintenance Plan		
Maintenance 	Until	Total Price
<input checked="" type="radio"/> 12 months	2014-10-13	US\$ 2,230.00
<input type="radio"/> 24 months	2015-10-13	US\$ 2,734.00
<input type="radio"/> 36 months	2016-10-13	US\$ 3,182.00

Fonte: Paessler, acesso em 2013

- Nota: Os dados da Figura 10 e Figura 11 foram coletados em 14/10/2013 da seguinte fonte: <https://shop.paessler.com/en/prtg#maint>

A imagem exibe os pacotes de manutenção que variam de 12 meses a 36 meses. Ela calcula o término deste contrato partindo do dia que o usuário visualizou a página para aquisição, após o cálculo também é exibido o valor de cada pacote.

5.1.3 Estrutura do PRTG

O PRTG pode ser dividido em três partes distintas Silva (2012) as classifica como: partes do sistema, interfaces de controle e interfaces de administração básicas. Em sua instalação o principal item a ser observado é o core server que faz parte do sistema. Sua responsabilidade é a execução dos principais passos do PRTG. Estes procedimentos são citados como:

- Gestão do Cluster;
- Gestão e eliminação de dados com mais de 365 dias;
- Banco de dados para observar os dados;
- Gerador de relatórios;
- Gerador de conta de usuários;
- Gestão de notificação, com servidor de correio para entrada de e-mails;
- Servidor Web e APIs, o servidor web já vem embutido na instalação e suporta HTTP e HTTPS, sem a necessidade da instalação do IIS ou apache, para a sua execução;
- Gestão e configuração das estações conectadas.

A Interface de Controle é definida por Silva (2012) em três partes.

- Ajax web Interface: responsável pela configuração de sensores, dispositivos e análise dos resultados da monitoração. Outra função importante é administração do sistema de modo geral;
- Enterprise Console: É nativo do sistema Windows. Sua utilização possibilita uma alternativa para interface web, onde é possível, através deste aplicativo, conectar em diferentes instalações do PRTG, e ao realizar a conexão é possível gerencia-lo em uma visualização. Para empresas que possuem um grande número de sensores, o PRTG é o ideal pois mostra as informações agregadas para todos os servidores;
- Mobile Web GUI: É uma interface em jQuery mobile. Esta interface é somente de leitura, compatível com quase todos os dispositivos móveis disponibilizados pelo mercado.

6 AMBIENTE ESTUDADO

6.1 Máquina virtual

Uma máquina virtual é definida por Laureano (2008) como “uma duplicata eficiente e isolada de uma máquina real”, ou seja, é a utilização dos recursos existentes em uma máquina física e distribuídos para a criação das máquinas virtuais. Ao optar pela virtualização das máquinas o usuário não precisa ter varias máquinas físicas com seus respectivos sistemas operacionais. Em apenas um computador pode-se abrigar várias máquinas virtuais com seus sistemas operacionais, serviços e aplicações.

Em 1960 criou-se o termo máquina virtual com base na máquina criada pela IBM chamada M44/44X. Esta máquina foi o ponto de partida para o desenvolvimento de sistemas com suporte a virtualização. Entre os sistemas criados o que ganhou destaque foi o modelo OS/370. As máquinas a partir da versão M44/44X davam suporte a virtualização e possibilitava aos usuários a criação de apenas uma máquina com seu próprio sistema operacional, aplicações e independente dos demais usuários.

6.1.1 Software (virtual box)

Optou-se pela utilização do VirtualBox para a criação das máquinas virtuais. Segundo Costa (2009) o VirtualBox é um sistema criado pela empresa Sun com o intuito de emular máquinas virtuais usando técnicas de virtualização total. Um dos motivos para a escolha deste emulador é que, além de ser uma ferramenta livre, sua utilização pode ser multi plataforma, possibilitando sua utilização em sistemas como Windows, Linux, Solaris, BSD e IBM, inclusive virtualizando todos ao qual ele suporta e permite ao gestor alocar a quantidade de preferencia de memória RAM e disco rígido podendo este ser expandido automaticamente quando atingido seu limite configurado.

Outra característica importante do virtualbox é a emulação de CD/DVD, drivers USB, 4 adaptadores de rede com 4 placas diferentes (2 PCnet, uma PCI II e outra FAST

III, 1 Intel PRO/1000 MT desktop e 1 Intel pro/1000 T Server) com a 4 tipos de conexão e até 2 portas seriais e possui também uma característica única de dar suporte 3D de até 128MB.

6.1.2 Configuração (hospedeiro e cliente padrão / hardware)

Na criação das máquinas virtuais optou-se pela criação de oito máquinas virtuais clientes com configuração de hardware da seguinte maneira: 512 mb de memória, 20 gb de disco rígido, com processador Core I5, o mesmo padrão do hospedeiro. Para manter padrão de análise, optou-se pela instalação do Sistema Operacional Windows 7 em oito equipamentos virtualizados. Já nas máquinas hospedeiras contou-se com computadores que utilizavam-se de processador core i5, 4 Gb de memória e 500Gb de Hd.

Tabela 1 – Elementos de rede 1

Nome	IP	Serviços	Sistema Operacional
Marcio	192.168.1.100	Hospedeiro Vídeo conferência	Windows 7
Host1	192.168.1.101	Acesso remoto	Windows 7
Host2	192.168.1.102	Download Upload	Windows 7
Host3	192.168.1.103	streaming de áudio web Acesso remoto	Windows 7
Host4	192.168.1.104	Vídeo online	Windows 7

Fonte: Autoria própria

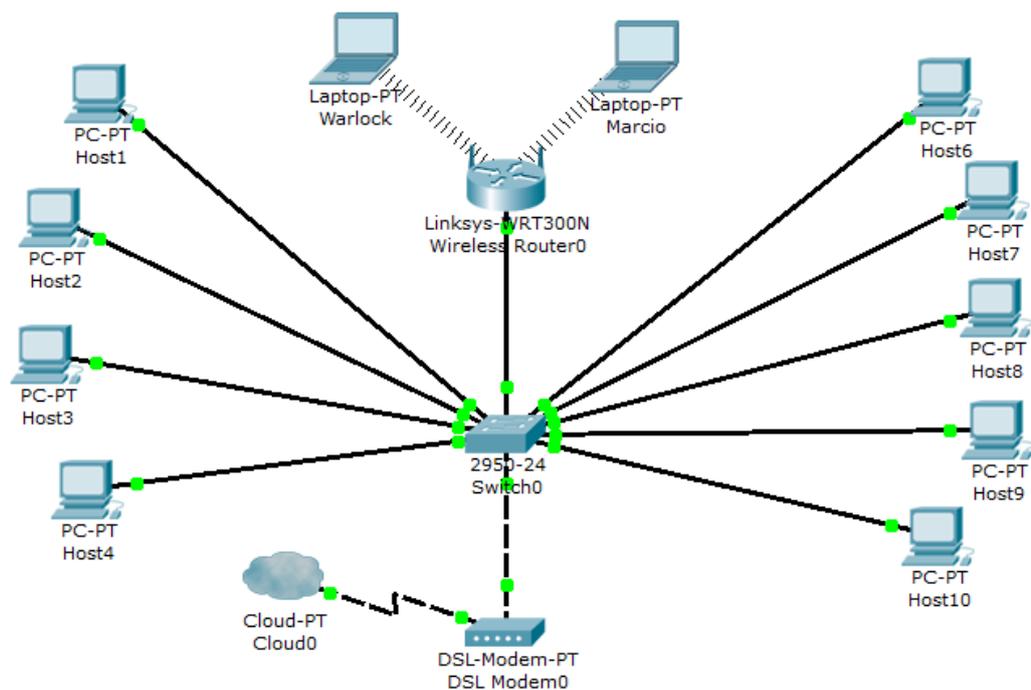
Tabela 1 – Elementos de rede 1

Nome	IP	Serviços	Sistema Operacional
Warlock	192.168.0.100	Hospedeiro vídeo conferencia	Windows 7
Host6	192.168.0.101	Acesso remoto	Windows 7
Host7	192.168.0.102	Download	Windows 7
Host8	192.168.0.103	streaming de áudio web Acesso remoto	Windows 7
Host9	192.168.0.104	Vídeo online	Windows 7

Fonte: Autoria própria

6.1.3 Estrutura em rede (Packet tracer)

Figura 12 – Rede em Packet tracer



Fonte: Pesquisa do autor, acesso em 2013

Para criação de um modelo de fácil visualização, criou-se a estrutura de rede no Software Packet Tracer, da Cisco, permitindo um panorama lógico da rede proposta para os testes. Na imagem 12 podemos analisar dois notebooks conectados no mesmo roteador wireless, que por sua vez também está conectado em um switch, bem como a estrutura dos hosts e o enlace com a Internet sendo feito por um modem, sugerindo uma conexão ADSL.

6.1.4 Justificativa para o uso de máquina virtual

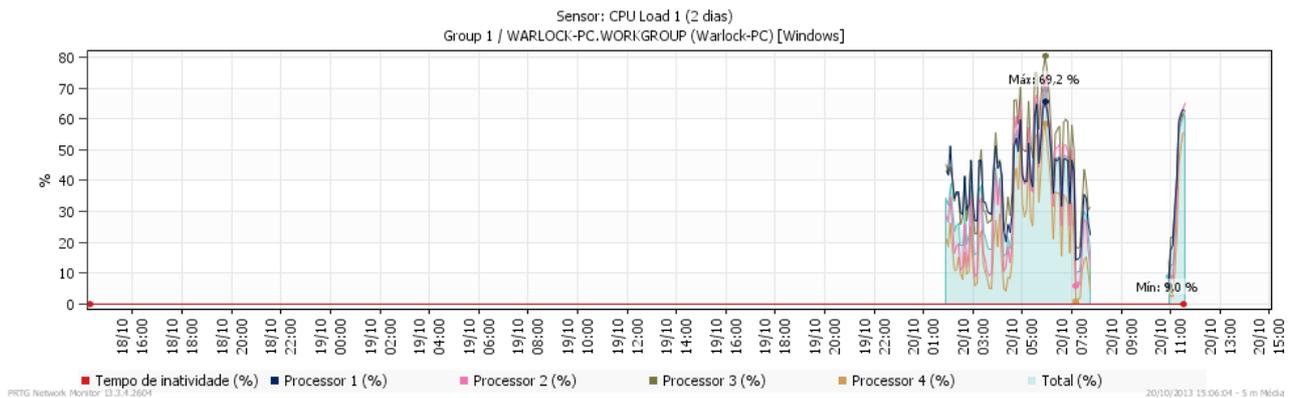
Dentro de uma organização é importante o gerenciamento da rede, pois é através dele que o gestor poderá verificar se a banda da rede está sendo utilizada corretamente. Caso aja alguma irregularidade, o gestor com os dados obtidos em mãos poderá tratá-la da melhor forma possível. Nas análises feitas no trabalho, fez-se o monitoramento de uma rede montada com base em ferramentas de virtualização, com o objetivo de obter informações a respeito de utilização do link por parte dos usuários. O monitoramento foi direcionado aos serviços de rede e aos equipamentos presentes no contexto da rede proposta.

Optou-se pela criação de máquinas virtual para a execução dos testes, pois sua utilização nos possibilitou uma melhor portabilidade para a execução dos testes além de reduzir o número necessário de máquinas físicas presentes em um mesmo ambiente de teste e nos permitiu ter uma grande praticidade ao utilizar simultaneamente as máquinas necessárias para os testes.

7 ANÁLISE DA SIMULAÇÃO

7.1 Análise de Processamento dos Hospedeiros

Figura 13 - Análise de processamento do hospedeiro 1 - rede 1



Fonte: PRTG, acesso em 2013

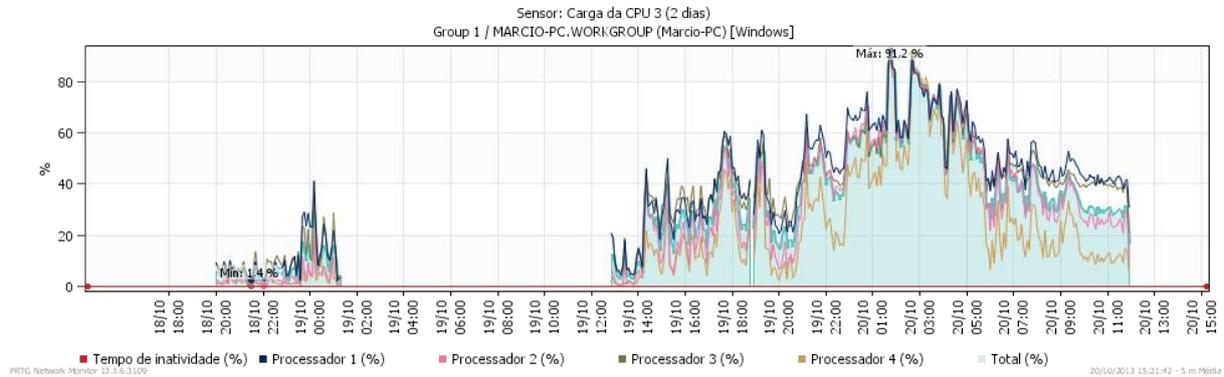
A figura 13 corresponde à análise feita em um dos dois computadores hospedeiros, onde se tinha toda a base computacional de suporte às máquinas virtuais clientes, cujos gráficos também fazem parte da análise e serão mostrados posteriormente.

Nesta figura pode-se ver o uso efetivo do processador por parte do equipamento hospedeiro, lembrando que no hospedeiro também tem-se a presença do software PRTG fazendo as respectivas análises de rede e geração de gráficos.

Na Imagem 13 vemos um período de análise de seis horas (no primeiro ciclo), indicando um uso constante e excessivo do processador. Uma experiência a relatar é a de que o equipamento superaqueceu quando exposto à esta análise quando feita em conjunto com as máquinas virtuais. Em pleno funcionamento, o processador chegou próximo ao limite de utilização viável.

Na preparação das máquinas virtuais, observou-se que a utilização do hardware teve de ser cuidadosamente feita, pois nos testes constatou-se que os limites do equipamento não permitiam sequer a criação das máquinas virtuais com quantidades maiores de memória do que o estabelecido.

Figura 14 - Análise de processamento do hospedeiro 2 – rede 2



Fonte: PRTG, acesso em 2013

A análise feita pelo PRTG, mostrada no equipamento hospedeiro 2 (correspondente à simulação de rede 2), mostrou-se contínua durante os testes do PRTG, aumentando visivelmente após as sete horas, momento em que ainda estavam sendo preparados os cliente, com a instalação do seu respectivo sistema Operacional. Nota-se uma evolução quantitativa no gráfico, exatamente no momento em que os equipamentos passaram a ser iniciados e inseridos no contexto da análise feita pelo PRTG, o que indica forte utilização de recursos neste momento. A partir das 07:00 horas, vê-se que o sistema se estabiliza, indicando que as atividades dos hospedeiros também se estabilizaram.

No momento em que há indícios de normalização do gráfico, é exatamente o ponto em que as atividades foram se findando – atividades que foram iniciadas para verificação da evolução do gráfico. Significando portanto que as máquinas virtuais estavam paradas.

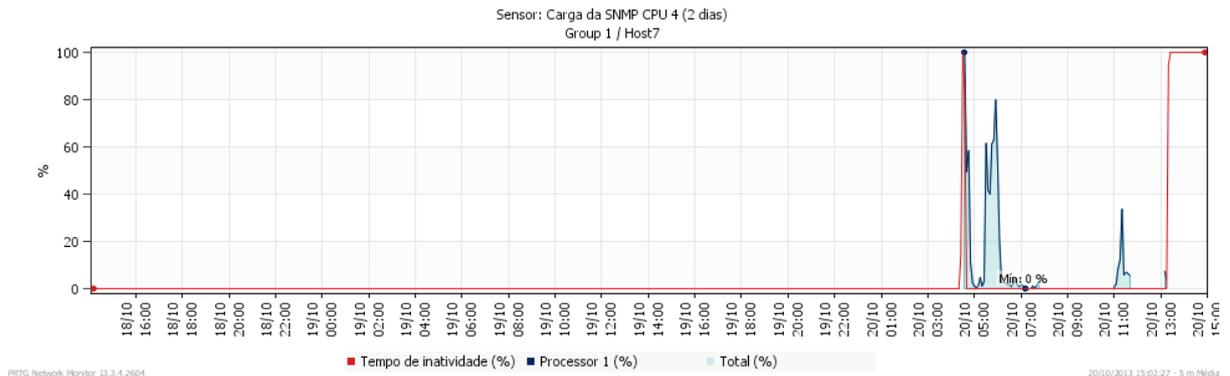
O intervalo de análise foi de aproximadamente 11 horas, o que possibilitou mostrar a efetiva utilização do hardware em 3 momentos chave: Sistema Hospedeiro parado e sem clientes, Sistema Hospedeiro com clientes em instalação e utilização efetiva de serviços de rede, e Sistema Hospedeiro com Clientes estáveis.

Os equipamentos hospedeiros foram também utilizados para utilização como computadores de trabalho durante o teste. Verificou-se que mesmo assim, com

tantos processos ao mesmo tempo, os pesquisadores puderam utilizar-se de vídeo conferência enquanto trabalhavam remotamente.

7.2 Análise de Processamento dos Clientes

Figura 15 - Análise de processamento do cliente 1– rede 1

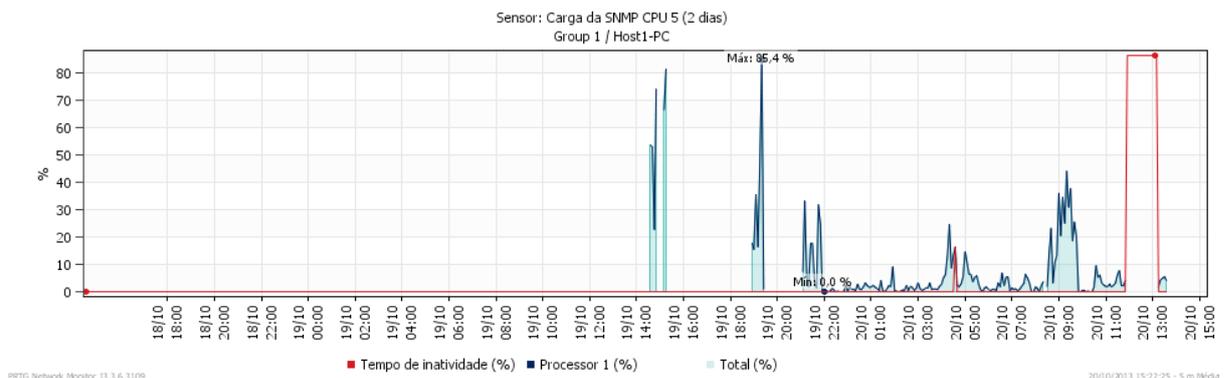


Fonte: PRTG, acesso em 2013

Na figura 15, mostra-se o gráfico do processamento de um dos clientes, neste momento fazendo testes de acesso remoto via software de VPN – Rede Virtual privada no cliente 3 presente na mesma rede. Realizou-se o teste na rede 2 também, o que mostra-se na imagem 16 (próxima).

O comportamento do sistema mostra-se perto do seu limite, conforme esperado para um equipamento no qual se tem compartilhamento de hardware – caso de um cliente de virtualização em um hospedeiro que contém mais clientes em funcionamento, ou seja, utilização considerável de processamento.

Figura 16 - Análise de processamento do cliente 1– rede 2

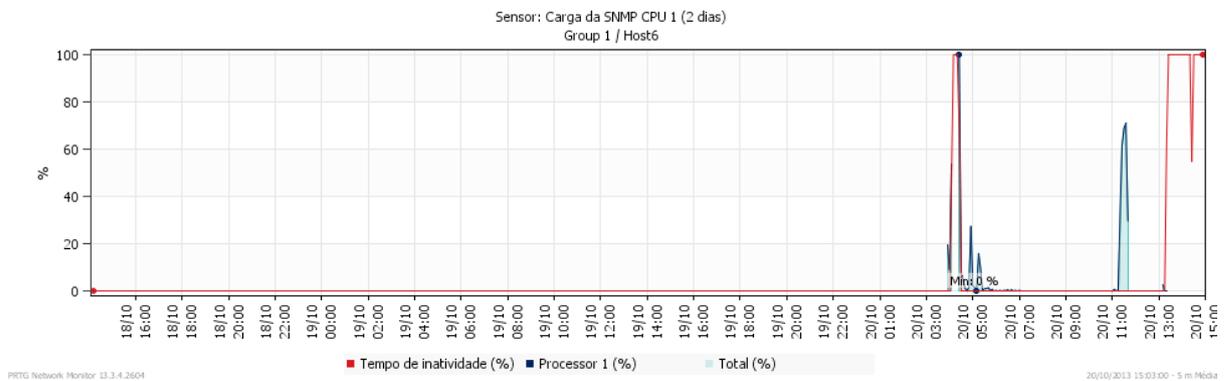


Fonte: PRTG, acesso em 2013

No cliente 2, representado pela imagem 16 mostra-se também a utilização de processamento, entrando em conformidade o Cliente 1, porém com mais tempo de utilização. Novamente no momento em que se fez uso de acesso remoto, o equipamento virtualizado mostrou utilização excessiva do processador.

Observa-se então uma boa capacidade de análise deste tipo de hardware por parte do PRTG, que mostra em tempo real os reflexos dos acontecimentos sob forma de gráfico de utilização. Esta análise indica que o Gerente de rede pode ter segurança na análise feita pelo PRTG no que diz respeito à utilização de CPU.

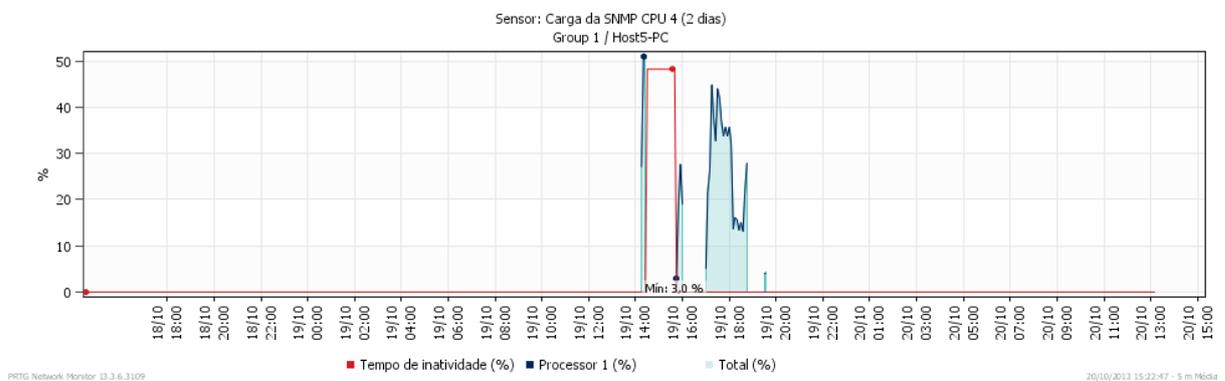
Figura 17 - Análise de processamento do cliente 2 – rede 1



Fonte: PRTG, acesso em 2013

Buscando parâmetros para análise, fez-se também a busca de informações a respeito do processamento nos clientes 2 da rede 1 e da rede 2, durante o download de um arquivo, no Cliente 2 da rede 1, e upload no cliente 2 da rede 2.

Figura 18 - Análise de processamento do cliente 2 – rede 2

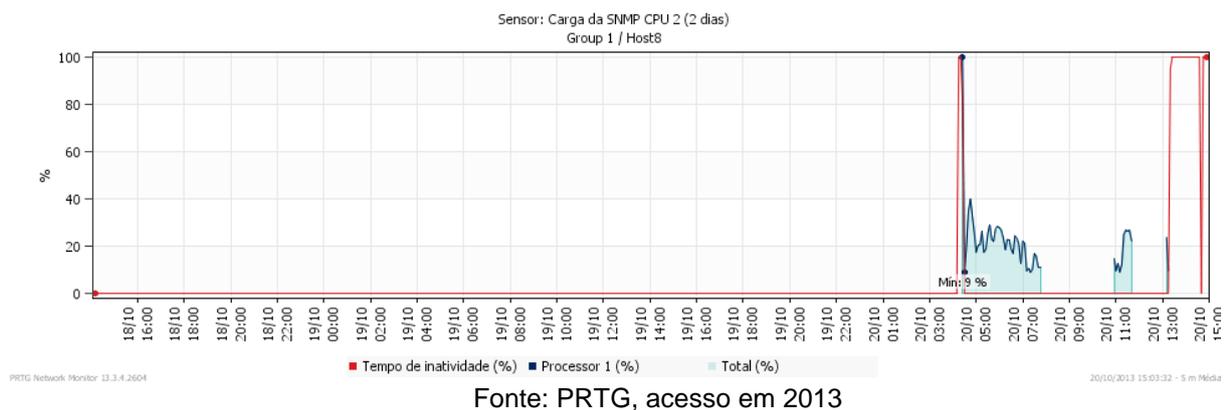


Fonte: PRTG, acesso em 2013

Observa-se então uma característica de manter-se no ápice do processamento, por parte dos cliente 2 da rede 1, no momento inicial do download, sendo a mesma característica observada no upload feito no Cliente 2 da rede 2.

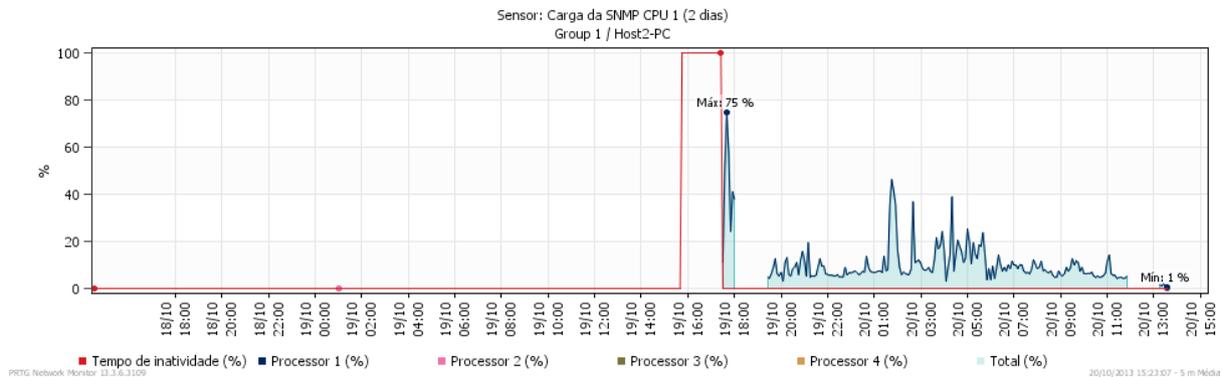
Conclui-se através destes resultados que novamente o comportamento inicial é diferenciado por parte dos equipamentos, estabilizando-se no decorrer do tempo. Mostra-se também na imagem que o monitoramento realizou-se de forma efetiva. Reitera-se que para o gerente da rede, estas medições são muito interessantes, pois problemas de limitação no processamento podem ser o indicador de troca dos equipamentos, que se estiverem sendo utilizados para downloads não autorizados, pode influenciar nos resultados de uma análise que pode culminar em um investimento desnecessário por parte da empresa.

Figura 19 - Análise de processamento do cliente 3 – rede 1



A figura 19 mostra análise de processamento no Cliente 3, no qual utilizou-se como parâmetro o uso de software para músicas no formato mp3, apontando também utilização constante do processador nesta função.

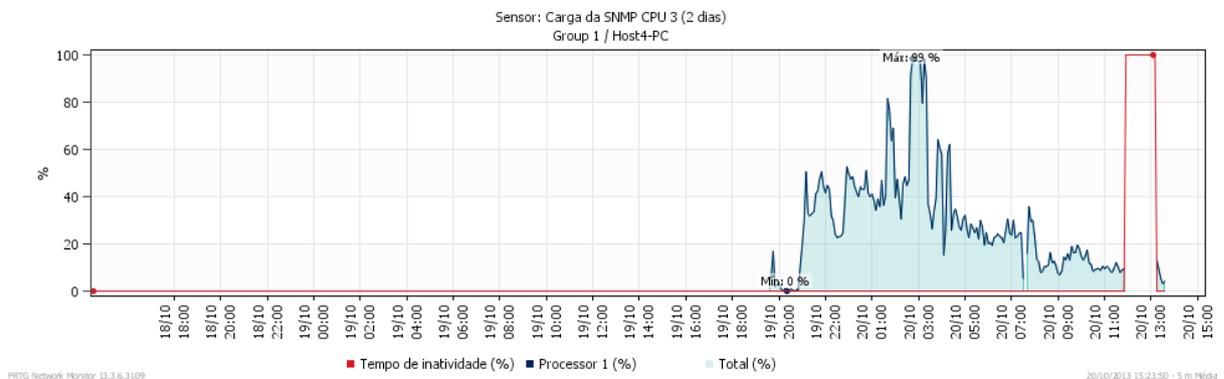
Figura 20 - Análise de processamento do cliente 3 – rede 2



Fonte: PRTG, acesso em 2013

A imagem 20 mostra o Cliente 3 da rede 2 na mesma situação do Cliente 3 da rede 2, ou seja, executando uma música no formato mp3, sendo verificada a mesma característica de utilização do processador, e uma demonstração fiel de gerenciamento por parte do PRTG.

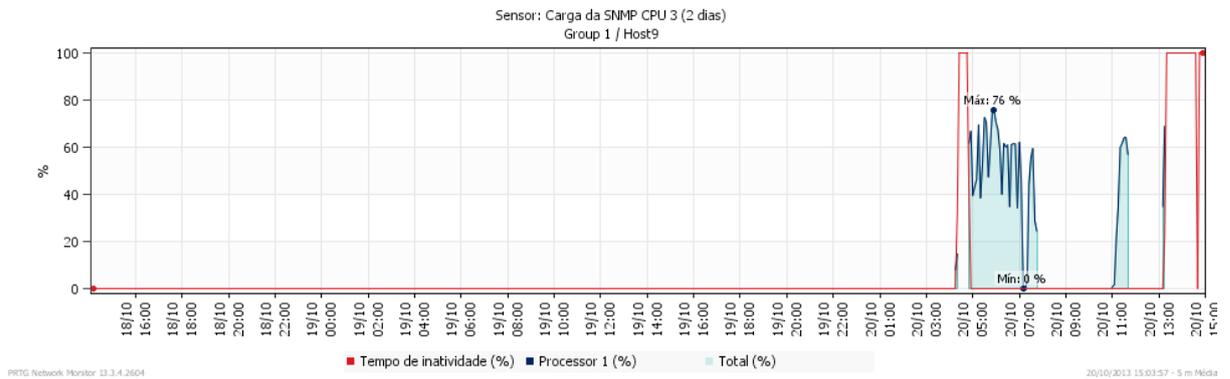
Figura 21 - Análise de processamento do cliente 4 – rede 1



Fonte: PRTG, acesso em 2013

O cliente 4 da rede 1, mostra uma utilização menor do processador, tendência que se mostra em todos os gráficos comparativos das duas redes pela diferença do hardware do hospedeiro, que no caso da rede 2 tem poder de processamento menor.

Figura 22 - Análise de processamento do cliente 4 – rede 2



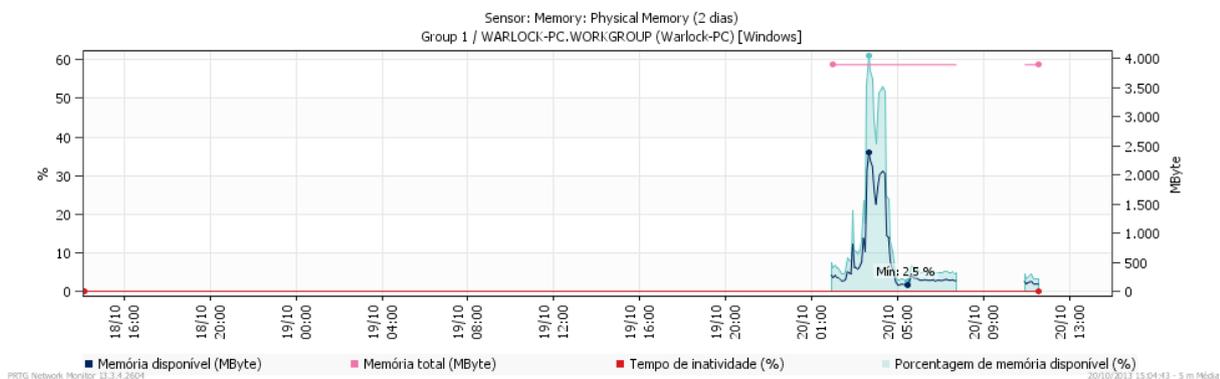
Fonte: PRTG, acesso em 2013

A imagem 22, correspondente ao cliente 4, vê-se o comportamento de um cliente que está utilizando-se de um serviço de vídeo para Web – Youtube. O uso do processador mostra uma também prejudicial utilização do hardware, caso não seja este o propósito do equipamento por parte do usuário.

O comportamento registrado pelo PRTG foi próximo à realidade, mostrando que a sua proposta quanto ao gerenciamento é confiável, e o seu efetivo papel de suporte ao Gerente da rede.

7.3 Análise de Utilização de Memória dos Hospedeiros

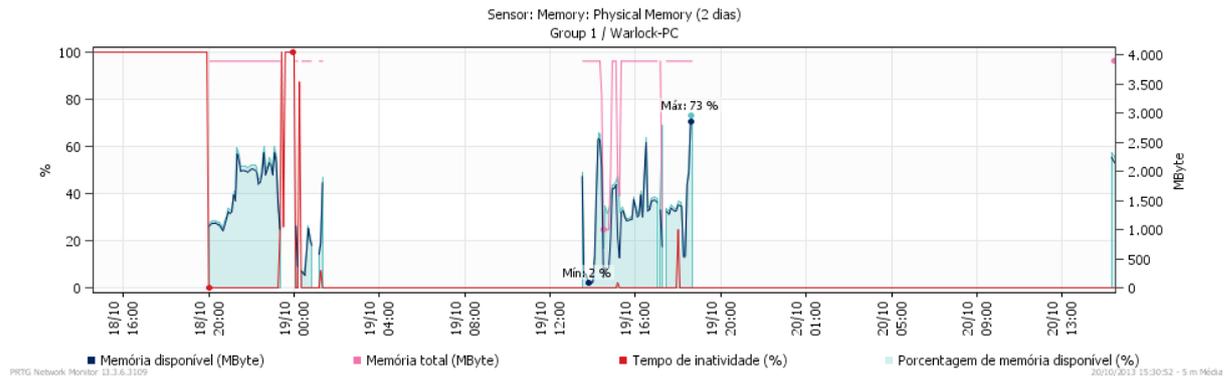
Figura 23 - Análise de utilização de memória hospedeiro 1 – rede 1



Fonte: PRTG, acesso em 2013

A figura 23 mostra análise de utilização de memória do Hospedeiro 1, com análise feita em um intervalo de 7 horas de trabalhos com vídeo conferência, já citados na análise do processamento feito no mesmo equipamento.

Figura 24 - Análise de utilização de memória hospedeiro 2 – rede 2

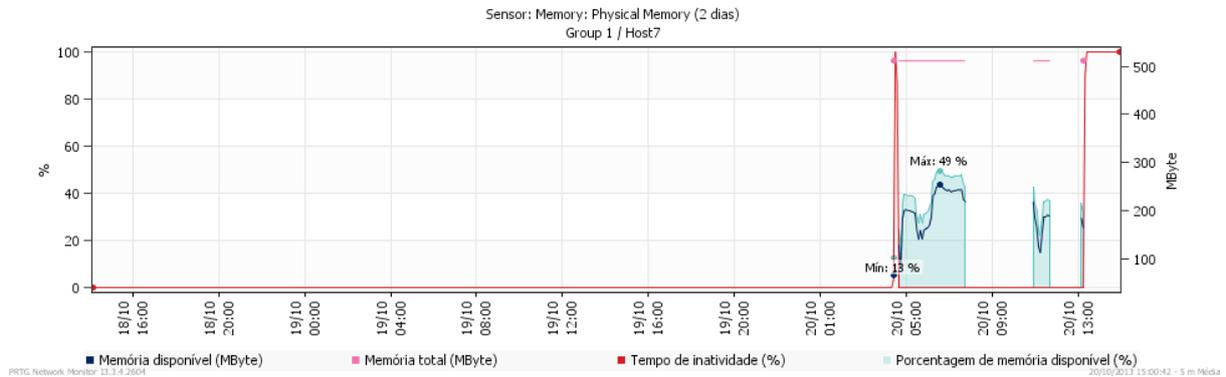


Mostra-se no gráfico apresentado na figura 24 a análise de utilização de memória do hospedeiro 2, corroborando a situação que foi visualizada no processamento, a estabilidade depois de um certo momento, sofrendo influências quando do início de software que concorrem pela memória – no caso dos clientes que estavam sendo configurados para testes neste momento.

7.4 Análise de Utilização de Memória dos Clientes

A análise de utilização de memória por parte dos componentes de uma rede pode indicar, assim como no caso do processador, o momento de upgrade ou troca do hardware. Esta vida útil do equipamento pode ser maximizada no caso de boa utilização do hardware por parte do usuário, resumindo a utilização somente aos processos que sejam inerentes ao seu serviço, o que no caso de uma empresa, corroborando o que foi constatado no caso do processador, pode indicar uma vida útil do hardware maior, evitando investimentos desnecessários por parte do administrador.

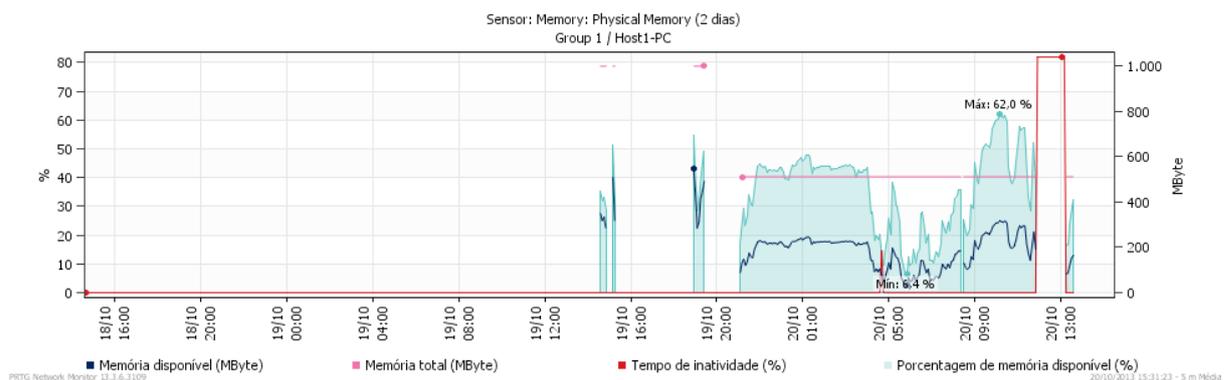
Figura 25 - Análise de utilização de memória cliente 1 – rede 1



Fonte: PRTG, acesso em 2013

A figura 25 mostra a utilização de memória no cliente 1 da rede 1, durante teste de acesso remoto.

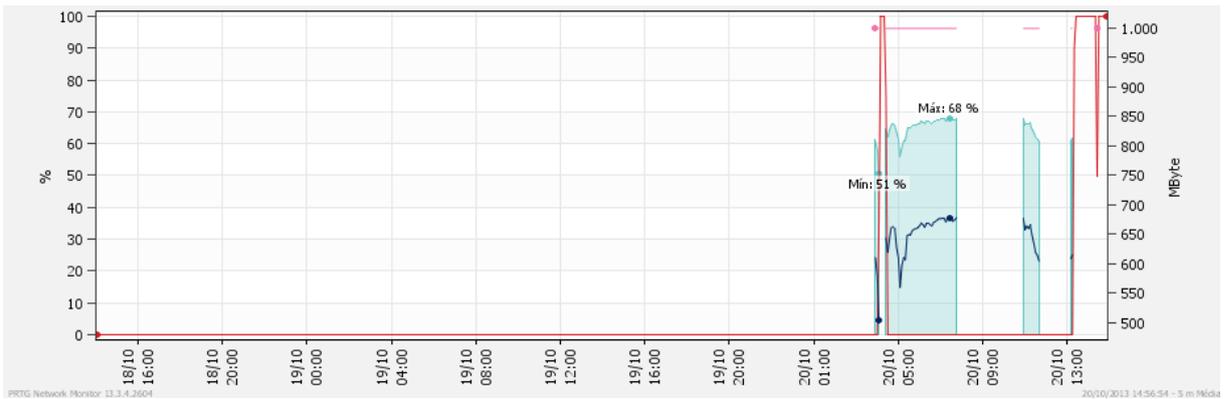
Figura 26 - Análise de utilização de memória cliente 1 – rede 2



Fonte: PRTG, acesso em 2013

Assim como se fez no caso do cliente 1 da rede 1 e da rede 2, testou-se a utilização de memória do host 1 da rede 2 durante o acesso remoto. Verificou-se que o software PRTG respondeu de forma positiva, apontando no gráfico todas as tendências de utilização do hardware em questão.

Figura 27 - Análise de utilização de memória cliente 2 – rede 1

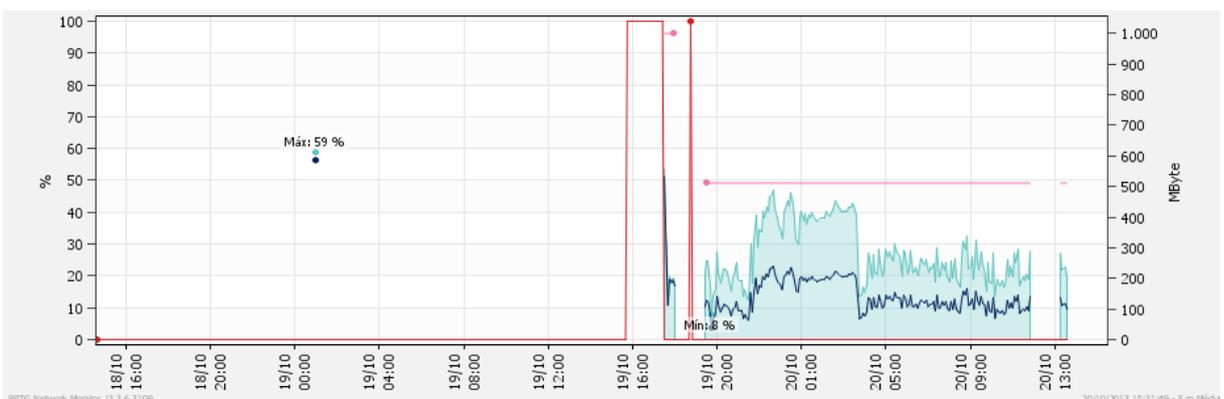


Fonte: PRTG, acesso em 2013

Na figura 27, mostra-se a análise feita no cliente 2 da rede 1 pode-se visualizar o mesmo comportamento das memórias, mesmo que em tempo diferente, assumindo o ápice apenas, com a diferença do hardware do hospedeiro. Ressalta-se que esta diferença tem reflexos nos resultados de um e outro, porém mostra tendências de utilização parecidas.

No caso destes dois gráficos, reitera-se que se tem na situação, análise feita durante o download (cliente 2 da rede 1), e upload no caso do cliente 2 da rede 2 na imagem 28 (abaixo).

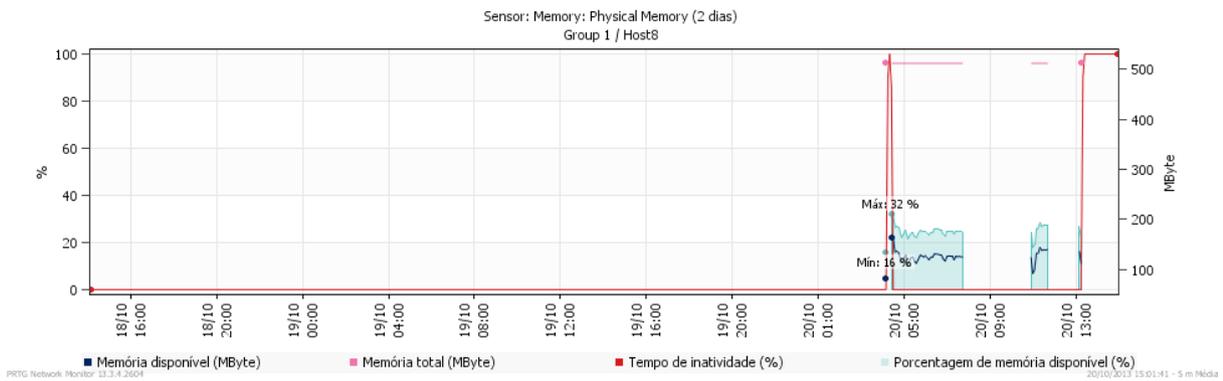
Figura 28 - Análise de utilização de memória cliente 2 – rede 2



Fonte: PRTG, acesso em 2013

Análise de utilização de memória do cliente 2 da rede 2, com o comportamento do upload representado no gráfico do PRTG.

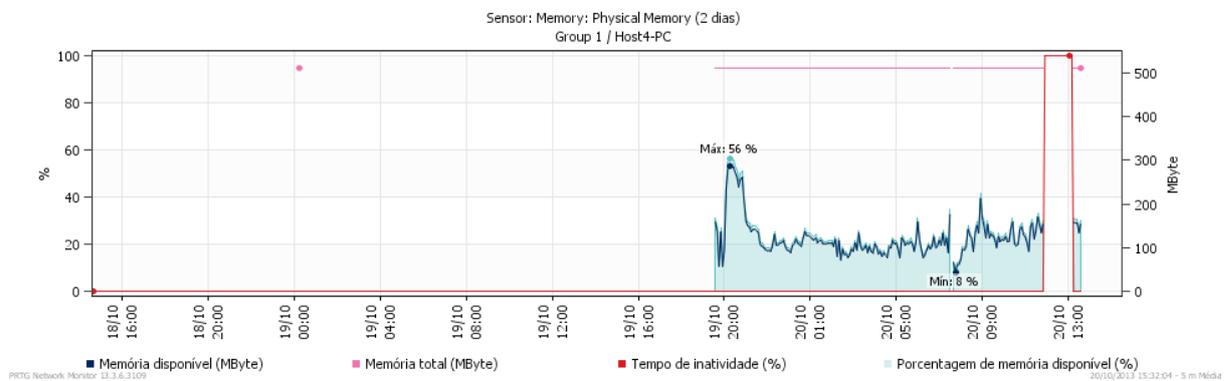
Figura 29 - Análise de utilização de memória cliente 3 – rede 1



Fonte: PRTG, acesso em 2013

Na figura 29 (acima), o gráfico mostra a utilização da memória durante a utilização com um software de execução de músicas em formato mp3, conforme medido no processamento. O equipamento se mostra constante durante esta requisição junto ao hardware.

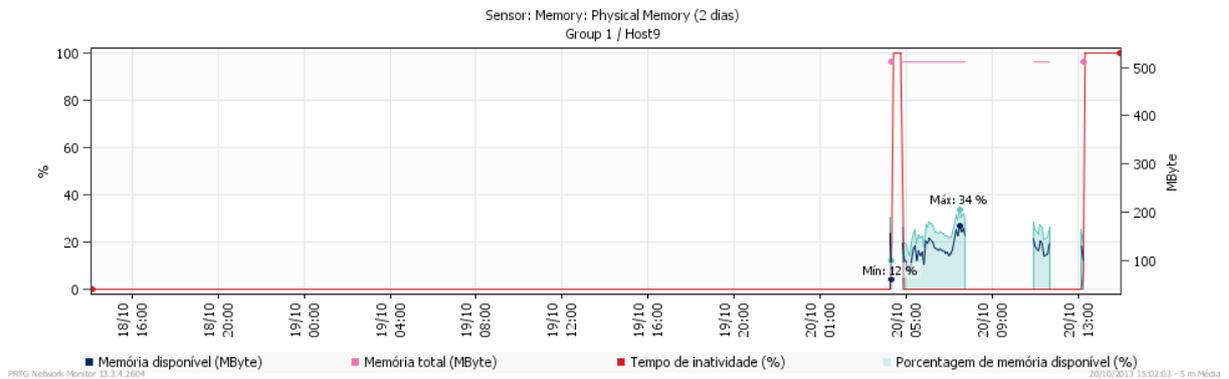
Figura 30 - Análise de utilização de memória cliente 3 – rede 2



Fonte: PRTG, acesso em 2013

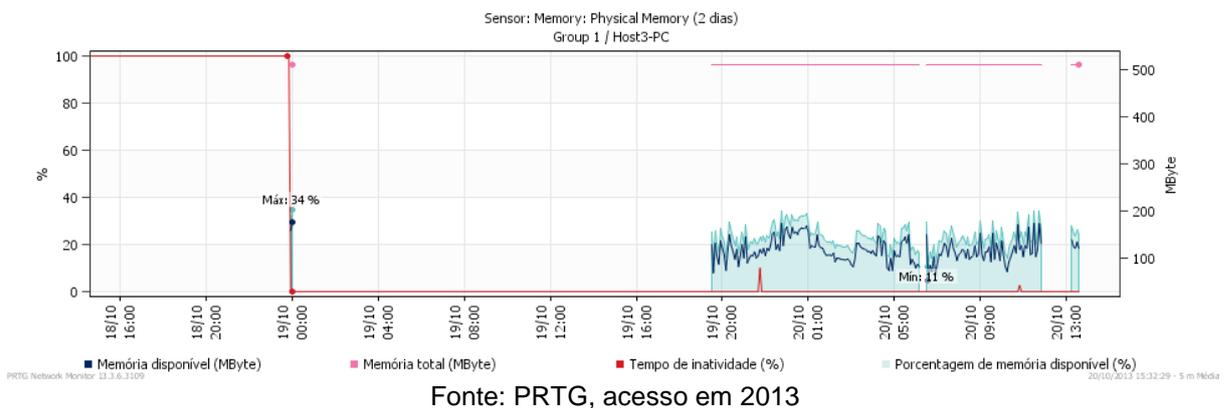
Durante a análise no mesmo contexto, feita na imagem 30 (acima), vê-se a mesma característica de utilização de memória, levando à conclusão que neste teste o PRTG mostrou com eficácia a tendência de utilização da memória no momento de upload, com característica de utilização parecida com o download mostrado na imagem 29.

Figura 31 - Análise de utilização de memória cliente 4 – rede 1



Na figura 31 (acima), que mostra o PRTG permitindo ao administrador ter a noção clara da utilização de memória durante a execução de um vídeo no Youtube.

Figura 32 - Análise de utilização de memória cliente 4 – rede 2



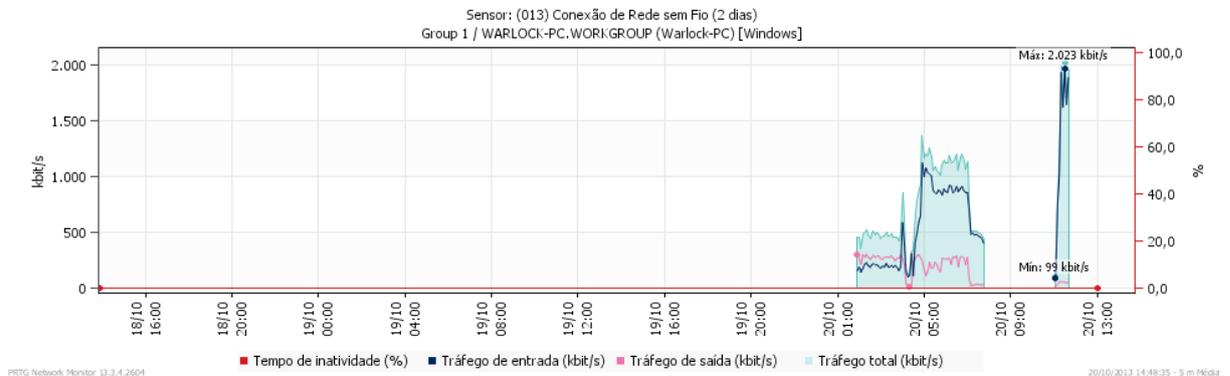
A figura 32 (acima), do cliente 4, da rede 2, mostra-se o padrão de memória durante a execução do vídeo do youtube novamente, apenas mudando o contexto em que o hospedeiro é diferente. Comportamento igual, porém índices apontando diferenças no hardware, assim como no processamento.

7.5 Análise de Utilização da Banda da Interface de Rede dos Hospedeiros

A busca por otimização da utilização de banda por parte dos usuários, é ponto importante na administração de um recurso limitado e necessário para serviços bancários, de vídeo conferência, VPN, e até compartilhamento de base de dados.

Levando em consideração esta importância, tem-se nesta análise, ponto chave para administração deste recurso.

Figura 33 - Análise de utilização da banda da internet Hospedeiro 1 – rede 1

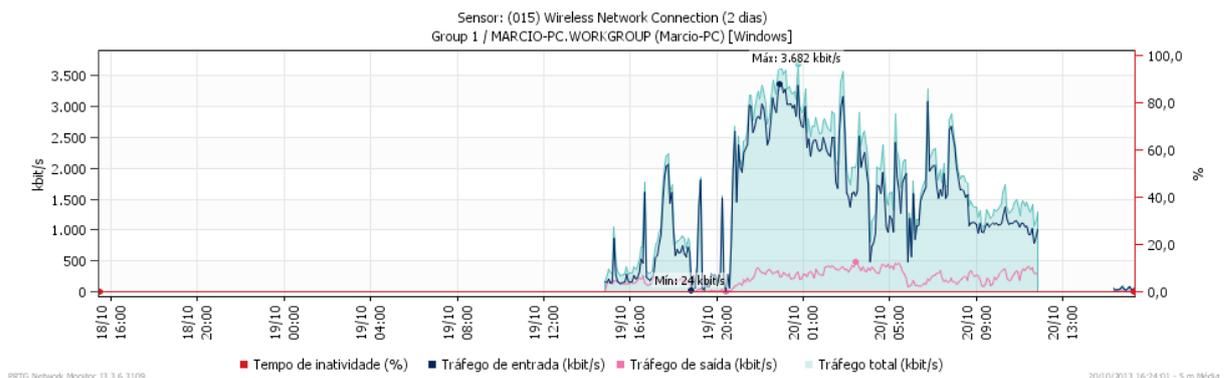


Fonte: PRTG, acesso em 2013

Na figura 33 (acima), o administrador tem por parte do PRTG, um gráfico que mostra a utilização da banda de redes por parte do equipamento, fragmentando-a em tempo de inatividade, tráfego de entrada, tráfego de saída e tráfego total.

Na imagem mostra-se o hospedeiro em situações que corroboram a realidade. Pode-se ver que o Hospedeiro 1 está com tráfego de saída e bom tráfego de entrada. O gráfico mostra exatamente o uso da banda de Internet para uma vídeo-conferência – gerando tráfego de entrada e saída. Como o Hospedeiro 1 foi utilizado para monitoramento dos Clientes na simulação de redes proposta pelo trabalho, existe também um tráfego de entrada expressivo, que mostra exatamente a alimentação por parte do sistema, com os dados vindos dos clientes.

Figura 34 - Análise de utilização da banda da internet Hospedeiro 2 – rede 2



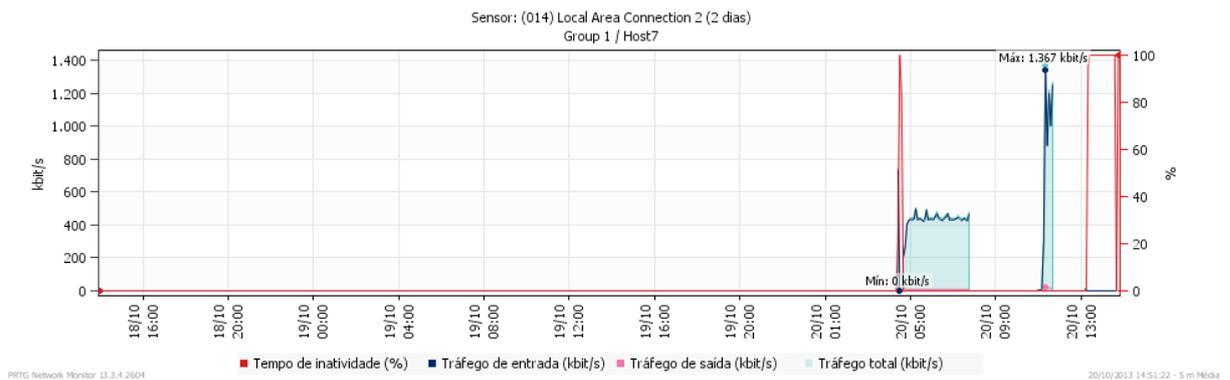
Fonte: PRTG, acesso em 2013

Na imagem 34 acima, o gráfico permite observar a tendência de maior tráfego de entrada por parte do equipamento, gerenciando os clientes. Nota: O gerenciamento de banda feito é de redes, sendo assim, tem-se resultados externos e internos.

7.6 – Análise de Utilização da Banda da Internet dos Clientes

A utilização de banda de rede por parte dos clientes foi aferida por ferramentas do PRTG, mostrando a utilização em diversos momentos, sendo monitorados de forma separada para melhor análise das situações que envolvem os serviços de rede do modelo proposto.

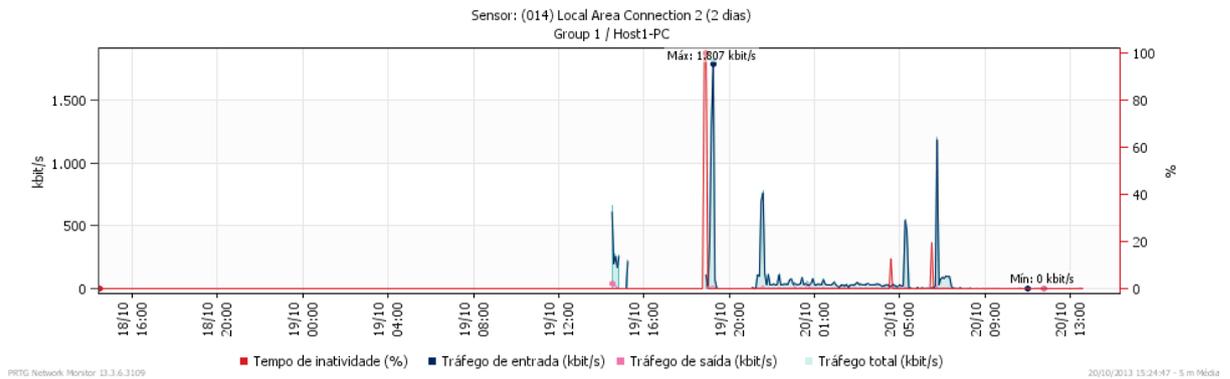
Figura 35 - Análise de utilização da banda da rede cliente 1– rede 1



Fonte: PRTG, acesso em 2013

Nas imagens que correspondem às figuras 35 e 36, do cliente 1 das redes 1 e 2, mostra-se o resultado da utilização de banda de rede por parte dos equipamentos clientes, durante uma vídeo conferência. Os dois equipamentos tem situações e serviços parecidos, porém ressalta-se que têm hardware diferente, o que mostra no caso do link menor, uma tendência de utilização perto do limite máximo.

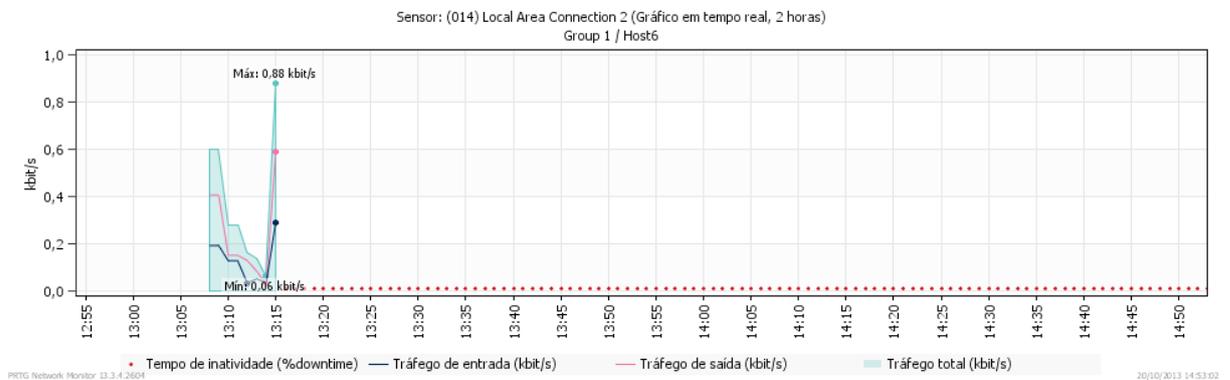
Figura 36 - Análise de utilização da banda da rede cliente 1– rede 2



Fonte: PRTG, acesso em 2013

Na análise do gráfico da rede 2, em alguns momentos o tráfego de entrada mostra-se superior ao tráfego de saída, entrecortado por momentos em que há inatividade ou pouco transporte, característica do serviço que está sendo utilizado (com a utilização de buffer, em alguns momentos a comunicação para, porém a continuidade é garantida pelo recurso usado também em vídeos na Internet.

Figura 37 - Análise de utilização da banda de rede cliente 2– rede 1

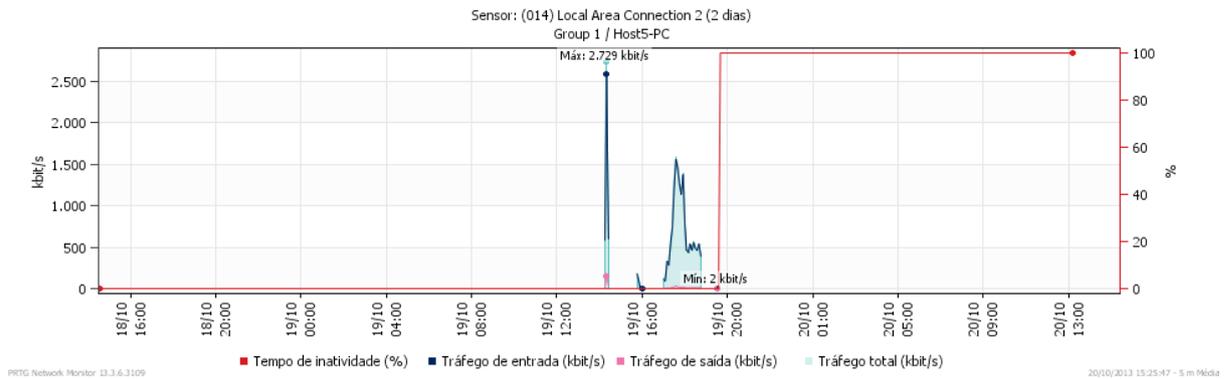


Fonte: PRTG, acesso em 2013

Na Figura 37 (acima), o processo de download de arquivos, mostra tráfego de entrada e saída. Neste momento, o PRTG permite visualizar uma característica do tipo de download feito – Torrent.

No caso do Torrent, temos tráfego de entrada, e por ser propício ao compartilhamento, o tráfego de saída torna-se uma constante também. Neste caso, pode-se fazer também o comparativo com o Host 2 da Rede 2, que também mostra download.

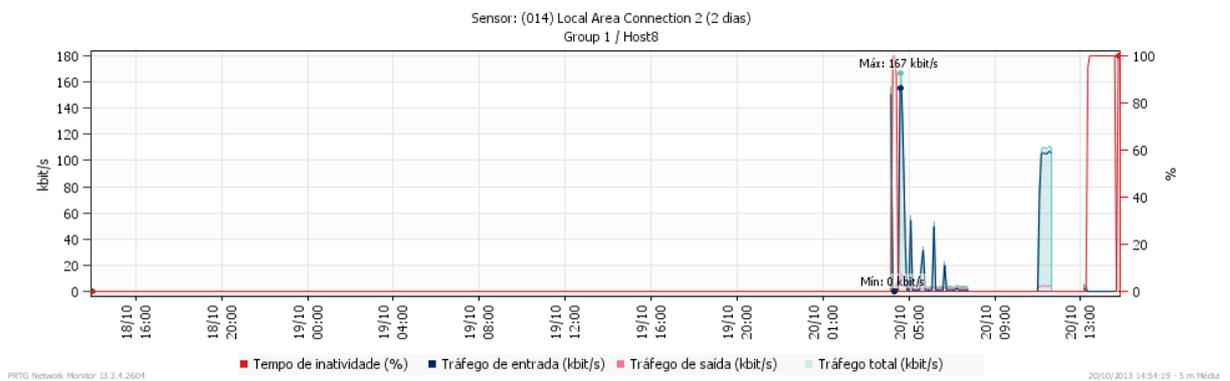
Figura 38 - Análise de utilização da banda de rede cliente 2– rede 2



Fonte: PRTG, acesso em 2013

A imagem 38, mostra no cliente 2 da rede 2, um download direto, que diferentemente do cliente 2 da rede 1 mostra apenas tráfego de entrada, confirmando nas diferenças das imagens o auxílio efetivo que o PRTG, nas também diferentes características dos downloads correlatos.

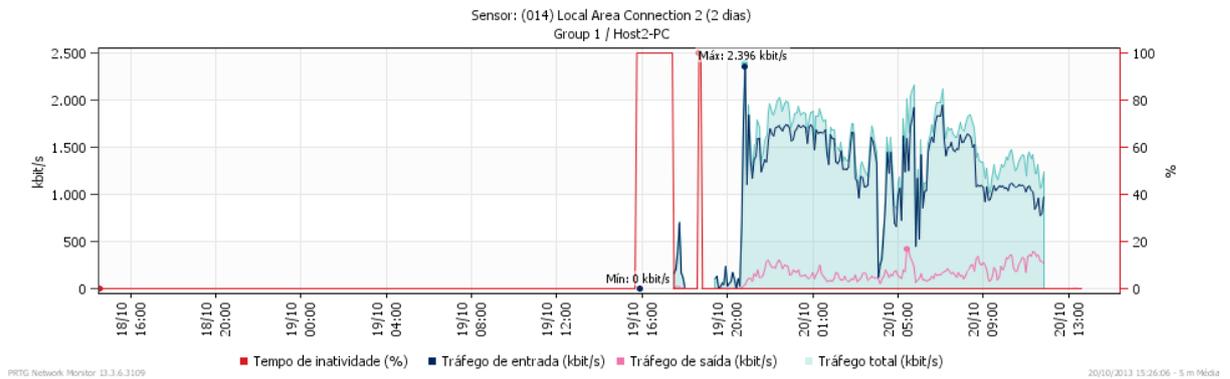
Figura 39 - Análise de utilização da banda de rede cliente 3 – rede 1



Fonte: PRTG, acesso em 2013

Durante os testes com a execução do áudio via web (radio online), o PRTG mostra na geração do gráfico, o tráfego de entrada constante, com um ápice inicial. Na imagem, mostra-se também um momento de parada na transmissão de dados, o que se dá por um problema de reinicialização do equipamento hospedeiro.

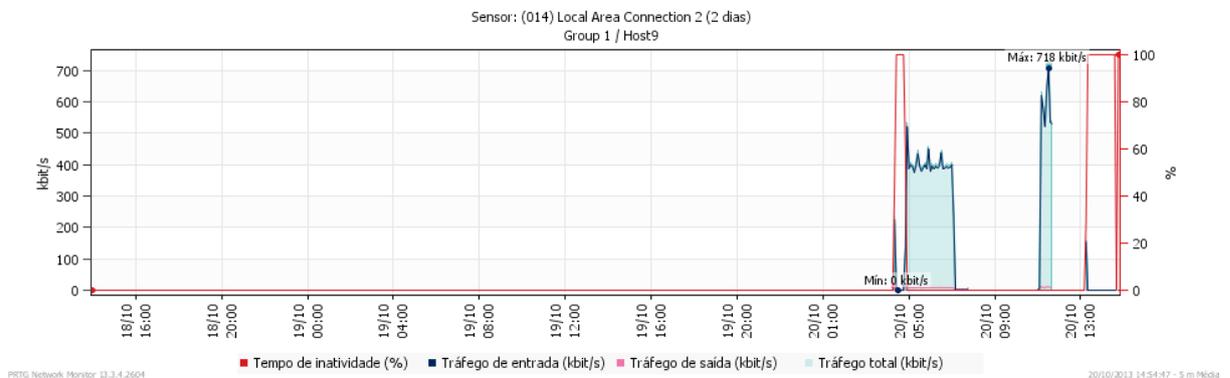
Figura 40 - Análise de utilização da banda de rede cliente 3 – rede 2



Fonte: PRTG, acesso em 2013

Na Figura 40 (acima), o gráfico gerado pelo PRTG mostra a execução do áudio, assim como feito na imagem do Host 3 da rede 1, da utilização da banda de rede. Ao contrário do Host da rede 1, esta simulação seguiu com transferência de dados constante, sem problemas na continuidade da transferência de dados mostrada no gráfico.

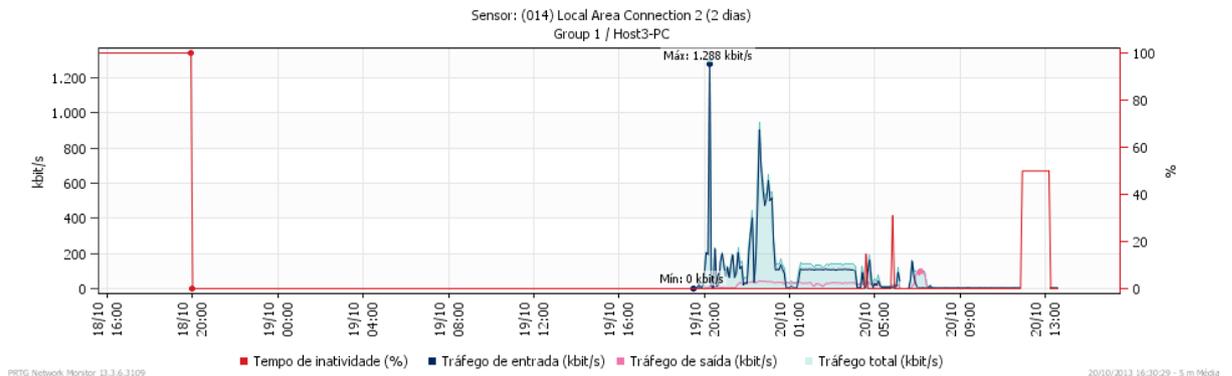
Figura 41 - Análise de utilização da banda de rede Host 4– rede 1



Fonte: PRTG, acesso em 2013

Na imagem 41, correspondente à análise feita durante a visualização do vídeo no Youtube mostra algo parecido com as imagens dos computadores 3 das duas redes. No caso, observa-se um comportamento parecido no vídeo e também na execução do áudio.

Figura 42 - Análise de utilização da banda de rede Host 4 – rede 2



Fonte: PRTG, acesso em 2013

Com a utilização do PRTG na análise do cliente 4 da rede 2, há um pico de utilização, e uma maior utilização do tráfego de entrada. Nos pontos em que há parada, mostra pontos em que a conexão com a Internet ficou mais lenta, e que em contrapartida o vídeo parou de carregar.

8 CONSIDERAÇÕES FINAIS

A utilização de ferramentas de rede se torna interessante devido à complexidade dos serviços disponíveis no ambiente. O software torna uma simples percepção do gerente de rede em informações estatísticas que podem ser usadas como base para tomada de decisão.

O PRTG é uma ferramenta de instalação relativamente rápida, com grau de complexidade de configuração médio, que proporciona gráficos, alarmes, listas e registros em tempo real da rede de computadores. O protocolo de redes SNMP permite ao software a análise de cada elemento de rede tratando-os como agentes em um contexto em que o servidor é o gerente.

O software utilizado na análise utiliza-se dos parâmetros obtidos através das sondas para formação dos gráficos e posterior formação de um banco de dados com as informações da rede. Na rede proposta, os agentes são representados por funcionalidades do SNMP nos clientes, para coleta de dados. Os gerentes são os hospedeiros citados no decorrer da análise dos gráficos.

Na análise da rede proposta obtiveram-se resultados que mostram uma tendência parecida no comportamento da rede 1 e da rede 2. Ao explorar os mesmos serviços em ambientes virtualizados diferentes conseguiu-se observar o padrão de comportamento em cada serviço de rede e ainda assim entender o comportamento de redes com hardwares distintos.

A influência do hardware diferente dos dois contextos mostra que ao simular um ambiente com o apoio de máquinas virtuais, toda estrutura deve ser bem planejada de forma que os serviços estejam sempre em pleno funcionamento. Comportamento da rede em questão mostra através dos gráficos o fluxo de entrada e saída de dados nas interfaces de rede e a consequente utilização do processador e das memórias.

Considera-se após a análise que o software PRTG traduziu de maneira satisfatória as situações propostas na estrutura simulada. Os gráficos apontaram o comportamento da interface de rede dos elementos que em alguns casos mostravam diretamente o reflexo da banda de internet e da variação dos serviços, e da limitação das máquinas virtuais ao administrador.

Os gráficos de download, por exemplo mostram uma situação característica dos serviços utilizados na demonstração. Em um equipamento mostra-se um download via torrent com sua consequente utilização da banda para entrada e saída. No caso do download simples via web mostra-se um tráfego maior na entrada. Leva-se em consideração então que o PRTG cumpre seu papel na análise do tráfego mostrando ao administrador a realidade da rede.

Foi possível então através desse trabalho entender a dinâmica por trás da análise baseada em protocolo de gerência, facilmente visualizada nas ações do software. O trabalho em questão leva em consideração testes realizados em um pequeno espaço de tempo corroborando o objetivo do trabalho que era especificamente fazer o teste em ambiente virtualizado e especificamente com o PRTG.

Em trabalhos futuros pretende-se colocar como objetivo o tempo como fator analítico.

8 REFERÊNCIAS

ALBUQUERQUE Evandro, **Gerencia de Redes**, Brasilia. Disponível em: <<http://www.slideshare.net/Evandromadeira/artigo-gerencia-deredes>>. Acesso em: 25 Ago. 2013

AZAMBUJA Macelo Cunha. **WebMan: uma ferramenta www de gerenciamento snmp**, Porto Alegre – RS. Disponível em: <<https://www.rnp.br/wrnp2/2000/posters/webman.pdf>> Acesso em: 10 Set. 2013

CARDOSO Cinthia, **Gerenciamento de redes com a utilização de software livre**, Belém-PA. Disponível em: <<http://www3.iesam-pa.edu.br/ojs/index.php/sistemas/article/viewFile/442/374>>. Acesso em: 04 Abr. 2013

Comer, D. **Redes de Computadores e Internet**. Person, Porto Alegre, 2ªed., 2001.

CONTESSA Diego Fraga, POLINA Everton Rafael **Gerenciamento de equipamentos usando o protocolo SNMP**, Porto Alegre – RS. Disponível em: <http://www.cp.com.br/upl/artigo_3.pdf> Acesso em: 03 Set. 2013

ESTEVES Antonio. JR Nilton, **O protocolo SNMP**, Rio de Janeiro – RJ. Disponível em: <<http://revistas.cbpf.br/index.php/nt/article/view/24/31>>Acesso em: 21 Set. 2013

GERCHMAN Júlio, **WEBER Taisy, Emulando o Comportamento de TCP/IP em um Ambiente com Falhas para Teste de Aplicações de Rede**, Porto Alegre – RS. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/wtf/2006/st2_3.pdf> Acesso em: 10 out. 2013

GUILLERMO Oscar Eduardo Patrón, **Uso de agentes SNMP para monitoramento de Servidores e equipamentos de rede com mobilidade**, Rio Grande do Sul – RS. Disponível em: <<http://www.lume.ufrgs.br/bitstream/handle/10183/15981/000695294.pdf?...1>> Acesso em: 05 Set. 2013

KUROSE J. ROSS W. K. **Redes de Computadores e a Internet – uma abordagem Top down**. 3ª ed. Pearson. 2005.

LAUREANO Marcos Aurelio Pchek, MAZIERO Carlos Alberto, **Virtualização: Conceitos e Aplicações em Segurança**, Curitiba – PR. Disponível em: <<http://www.dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/research:2008-sbseg-mc.pdf>> Acesso em: 30 Ago. 2013

LESSA Demian, **O protocolo de gerenciamento RMON**, Rio de Janeiro – RJ. Disponível em: <<http://www.rnp.br/newsgen/9901/rmon.html>> Acesso em: 30 Ago. 2013

MAGALHAES Ivan, **Gerenciamento de serviços de TI na prática**. 1.ed. São Paulo: Novatec, 2011. 296 p.

MAURO Douglas R. SCHMIDT, Kevin J. **SNMP Essencial**. Rio de Janeiro: Campus 2001.

MENEZES Elionildo da Silva, SILVA Pedro Luciano Leite, **Gerenciamento de Redes: Estudos de Protocolos**, Pernambuco – PE. Disponível em: <<http://www.di.ufpe.br/~flash/ais98/gerrede/gerrede.html>> Acesso em: 30 Set. 2013.

MELCHIORS, C. **Raciocínio baseado em casos aplicado ao gerenciamento de falhas**. 151f. Tese de Mestrado em Ciência da Computação. Universidade Federal do Rio Grande do Sul. UFRGS. Porto Alegre. 2003.

MOQADI Kanan Ali Abdulla, **Uso de ferramentas de gerência de rede para análise de desempenho de uma rede local**, Canoas – RS. Disponível em: <http://www.ulbra.inf.br/joomla/images/documentos/TCCs/2011_02/PROJETO_RC_KANAN_ALI_ABDULLA_MOQADI.pdf> Acesso em: 30 Ago. 2013.

OLIVEIRA Lécia, **O protocolo SNMP**, Salvador- BH. Disponível em: <http://www.logicengenharia.com.br/mcamara/ALUNOS/SNMP_Lecia.PDF> acesso em: 02 Ago. 2013

PASSLER, Disponível em:< <http://www.br.paessler.com>> acesso em: 01 Ago. 2013

Reynolds, George W. II. Silva, Flávio Soares Corrêa da. III. **Sistemas de informação gerencial**, 9ª ed. CENGAGE Learning. 2011.

RIBEIRO Cesar. GERK Livia, **Integração de gerências SNMP em um ambiente distribuído**, Niterói-RJ. Disponível em: <<http://www.midiacom.uff.br/~schara/alunos/livia-ig.pdf>> Acesso em: 01 Out. 2013

SZTAJNBERG Alexandre, **Gerência de redes de computadores**. Disponível em: <<http://www.gta.ufrj.br/~alexszt/ger/gerencia.html>>. Acesso em: 04 Out. 2013

TANENBAUM Andrew S. **Redes de computadores**. 6.ed. Rio de Janeiro: Campus, 1999. 923 p. ISBN 85-352-0157-2.

YANO Inacio Henrique, **Gerenciamento de redes de computadores utilizando CACTI**, Campinas-SP. Disponível em: <<http://www.infoteca.cnptia.embrapa.br/bitstream/doc/883562/1/doc10510.pdf>> Acessado em: 06 Set. 2013.