MUStaChe - Monitor de Uso, Status e Checagem de Informações em Elementos de Rede

Cristian Cleder Machado
E-mail: <cristian@cristian.com.br>.
URI - Universidade Regional Integrada - Câmpus de Frederico Westphalen
Departamento de Engenharias e Ciência da Computação

Daniel Dotto
E-mail: <danieldottho@gmail.com>.
Universidade Regional Integrada (URI) - Câmpus de Frederico Westphalen.
Departamento de Engenharias e Ciência da Computação

Resumo

Sistemas de monitoramento de redes foram criados para que administradores de rede pudes- sem identificar possíveis problemas na rede, tais como, gargalos, desconexões, entre outros. Apesar de apresentar diversos benefícios, um dos problemas ainda presente no contexto de monitoramento é a necessidade de utilização de um conjunto de ferramentas para monito- ramento de objetivos/contextos distintos, por exemplo, CPU, largura de banda, usuários conectados. Neste contexto, este trabalho apresenta uma ferramenta de monitoramento chamada MUStaChe, que agrupa e apresenta um conjunto de informações não encontradas tradicionalmente em sistemas de monitoramento. Os resultados dos testes mostraram que a ferramenta é equivalente as ferramentas existentes, e que oferece um conjunto maior de informações e recursos para identificar possíveis problemas.
Palavras-chave: Monitoramento, CPU, Largura de banda, Usuários Conectados, Problemas de rede

Introdução

A Internet, com sua diversidade de informações, vem cada vez mais conquistando usuários. Desde as suas primeiras experiências, onde foi utilizada somente para comunicação entre universidades, até os dias de hoje, a grande rede de computadores deixou de ser de uso exclusivo comercial e institucional, e passou a ser utilizada nas mais diversas áreas.

Com a crescente quantidade de dispositivos conectados à rede, a tendência é gerar uma alta carga de tráfego, podendo assim sobrecarregar dispositivos transmissores e fazendo com que esses dispositivos tornem-se lentos ou até mesmo, parem de funcionar. Em uma rede com vários transmissores, um trabalho manual de identificação e checagem destes dis- positivos pode levar muito tempo. Diante disso, estudos e implementações de novas técnicas e ferramentas para tornar essa checagem de dispositivos o mais simples possível são reali- zadas até hoje. Esses estudos tendem a levar para o melhoramento da forma como hoje é monitorada a rede, deixando de forma mais robusta e agradável possível a visualização das informações coletadas dos dispositivos.

Muitas ferramentas para monitoramento tem sido propostas, e apresentaram/apresentam resultados satisfatório, tais como, Nagios (Nagios, 2015), Zabbix (Zabbix, 2015) e Cacti (Cacti, 2015). Porém, a grande maioria delas é limitada ou voltada somente para monitoramento de tráfego, por exemplo, tráfego de entrada e saída, ou somente para monitoramento do equi- pamento, por exemplo, CPU ou memória. Além disso, tais ferramentas não são integradas ou colaborativas, fazendo com que o administrador tenha que observar diferentes dados em diferentes ferramentas, tornando o monitoramento de rede uma tarefa difícil.

DOI: 10.18256/2359-3539/reit-imed.v2n2p24-32

Diante deste cenário e destes problemas, este artigo apresenta a criação de uma ferramenta de monitoramento chamada MUStaChe. Os objetivos principais desta ferramenta são efetuar o monitoramento de forma interativa com o usuário, informando-lhe diversas infor- mações, tais como, status e problemas em equipamentos, além de mostrar através de gráficos particularidades, tais como, o consumo de largura de banda, a utilização de memória e CPU dos dispositivos, entre diversos outros. Para validação da ferramenta, a mesma foi instalada numa rede em produção de um provedor, onde problemas estão sujeitos a ocorrer repentina- mente, além da identificação de tráfego em horários de picos para os clientes. Os resultados dos experimentos e comparativos com outras ferramentas mostraram que a ferramenta apresenta informações de monitoramento equivalentes as ferramentas já conhecidas, e apresenta um agrupamento melhor de informações, do que o uso de ferramentas não integradas.

O artigo está organizado da seguinte forma: a Seção apresenta uma breve visão de algumas ferramentas existentes para monitoramento. A Seção apresenta brevemente a ferra- menta e suas funcionalidades. Na Seção são apresentados e discutidos alguns dos resultados iniciais. Por fim, a Seção conclui o trabalho, mostrando suas principais contribuições e apontando direções para trabalhos futuros.

Visão Geral de Outras Ferramentas

Além dos protocolos que determinam as regras de comunicação em uma rede, também são necessárias ferramentas que possam utilizar esses protocolos para efetuar o monitora- mento. Para que haja o monitoramento dos dispositivos que compõem uma rede, ferramentas são utilizadas fazendo com que, os resultados coletados possam ser visualizados de uma ma- neira mais clara ao administrador de rede, que pode identificar dispositivos que estejam operando de forma incorreta. A seguir serão descritas algumas ferramentas de monitora- mento já existentes no mercado.

Nagios

O Nagios é uma ferramenta utilizada para o monitoramento de dispositivos em uma rede. Além disso, ele pode monitorar serviços operantes, enviando alertas na ocorrência de mudanças no status dos mesmos (Barth, 2008; Josephsen, 2007; Ali, 2015). Segundo Joseph (Josephsen, 2007), o Nagios foi inicialmente desenvolvido para funcionar em máquinas Linux. Porém, em novas versões, foi adicionado também o suporte para outros sistemas operacionais, como Unix e Windows. Suas principais características são:

- Monitorar serviços de rede.
- Monitorar recursos de equipamentos, como carga de processamento, memória, espaço em disco entre outros.
- Alerta quando em equipamentos ou serviços ocorram problemas.
- Geração de arquivo de log, para posterior análise do operador de rede.
- Interface web para visualização do estado da rede.

Cacti

O Cacti, assim como o Nagios, é uma ferramenta de monitoramento de rede. Além de monitoramento da rede, o Cacti pode efetuar o monitoramento de unidades de discos, CPU, entre outras informações. O Cacti possui uma interface amigável de visualização, com menus intuitivos de navegação e organização dos dados (Haiyan, 2008; Weiqiang, Canhua, & Shujuan, 2011; Ali, 2015).

Zabbix

O Zabbix é uma ferramenta que possui características semelhantes ao Nagios e ao Cacti. Uma das vantagens ao instalar o software Zabbix, é que ele possui um sistema de descoberta automática de *hosts* em uma rede, formando assim, a topologia de monitoramento conforme a estrutura utilizada na rede. Isso faz com que no momento da configuração de novos dispositivos, não haja problemas de configurações incorretas, que acarretam em perda de tempo na configuração (Olups, 2010; Mescheryakov & Shchemelinin, 2014; Vacche & Lee, 2015).

MUStaChe: Um Monitor de Uso, Status e Checagem de Informações

Esta seção apresenta a criação da ferramenta denominada MUStaChe. Inicialmente, para o desenvolvimento do *front-end*, foram utilizadas as linguagens *HyperText Markup Lan- guage* (HTML) juntamente com *Cascading Style Sheets* (CSS), *Javascript* e Python. Além disso, foram utilizados os frameworks Django (Django, 2015) e Bootstrap (BootStrap, 2015 para a estrutura da página web. Posteriormente, foram criados alguns scripts para o back-end do sistema com funções, tais como, capturar dados de todos os equipamentos cadastrados no sistema, gerar logs, monitorar alertas, entre outras. As linguagens utilizadas nestes scripts foram Shel l Script e Python. Para a coleta de informações da rede e dos equipamentos foram utilizados os protocolos Simple Network Management Protocol (SNMP) e Internet Control Message Protocol (ICMP). Por fim, o banco de dados utilizado foi o MySQL (MySQL, 2015).

Módulo de configurações

O módulo de configurações é responsável pelo cadastrado de diversas informações necessárias para o sistema. A Figura 1 ilustra a interface de administração do sistema, onde é efetuado o cadastro de usuários, grupos de usuários, *check-points*, e-mails, equipamentos e serviços. A esquerda desta figura, é apresentando um sistema de *log* com ações que o usuário efetuou. Por questões de segurança, informações de pessoas, dispositivos, entre outras, serão ocultadas das figuras, uma vez que o sistema foi testado em uma rede em produção.

A Figura 2 apresenta uma tela de cadastro de equipamentos. Nesta opção, o usuário cadastra novos equipamentos para o sistema de monitoramento, utilizando informações, tais como, nome do equipamento, endereço IP, tipo de equipamento (roteador, switch, access point, etc.), equipamento que ele encontra-se conectado (parent), e uma descrição do equipamento.

A Figura 3 apresenta a tela de configuração do que o sistema irá monitorar em cada equipamento. O usuário define qual equipamento, informa qual *check-point* (CPU, memória RAM, tráfego, entre outros) ele irá monitorar, e argumentos para o equipamento, isto é, valores em porcentagem que indicam se o equipamento está em estado de alerta ou crítico, por exemplo, entre 75% e 90%, o equipamento está em estado de alerta, pois consumiu mais de 75% de sua capacidade. Em resumo, os argumentos são definidos para estipular os limites de nível de alerta e crítico para o sistema.

Módulo de Monitoramento

A Figura 4 ilustra a página inicial do sistema. Nela é apresentado um mapa da rede monitorada, bem como as ligações entre cada um dos pontos. No menu à esquerda são apresentadas as opções que o usuário pode realizar para visualizar informações adicionais do sistema. Além disso, podem ser identificados equipamentos que apresentam algum problema na rede. Por fim, a opção Gráficos, apresenta um conjunto detalhado de informações dos equipamentos, tais como, utilização de memória, CPU, entre outras.

Dentre as informações disponíveis na ferramenta, encontram-se a listagem de todos os dispositivos cadastrados e a listagem de equipamentos em estado de alerta. A Figura 5 apresenta a tela de visualização de equipamentos do tipo roteador. A Figura 6 apresenta a tela de visualização de equipamentos em estado de alerta.

A ferramenta também apresenta gráficos de consumo e de informações gerais de cada equipamento. A Figura 7 apresenta gráficos com informações de utilização de CPU e memória de um determinado equipamento.

A Figura 8 apresenta os gráficos de consumo de largura de banda de um determinado cliente. No mesmo sentido, a Figura 9 apresenta os gráficos de consumo de largura de banda em uma determinada porta de um determinado equipamento. Esses gráficos possuem opções de consumo nos últimos 5 minutos, 1 hora, 12 horas, 24 horas, 7 dias, 15 dias, 1 mês, 6 meses e 1 ano.

Experimentos, Resultados e Comparações

Para a realização dos testes, foram utilizados dois pontos de acesso em uma empresa real. Cada ponto de acesso possui em média 35 clien-

tes conectados na sua interface WiFi, e cerca de 200 clientes que autenticam via PPPoE. Esses dois pontos possuíam os equipamentos necessários para que pudesse ser efetuado o monitoramento dos mesmos. Por questões de segurança da informação, durante o texto, a empresa será chamada de empresa TESTE.

Os pontos de acesso à Internet que foram concedidos para os testes no sistema possuem aparelhos classificados como roteadores e como transmissores. Cada ponto possui um equipamento do tipo roteador. Os equipamentos classificados como transmissores possuem somente suporte à conexão de cliente na interface *wireless*. Por outro lado, os roteadores, possuem suporte também para autenticação de usuários e controle de Internet dos clientes. Com isso, foi possível obter uma grande quantidade de dados para a criação dos testes no sistema.

As Figuras 10 e 11 apresentam os gráficos do tráfego de Internet da interface brd- ptm do equipamento cadastrado como Y para a ferramenta MUStaChe e para o Zabbix. Os mesmos apresentam algumas diferenças em relação ao tráfego. Isso deve-se ao fato do sistema Zabbix efetuar mais verificações no equipamento num determinado intervalo de tempo. É importante ressaltar que a ferramenta MUStaChe é configurável, e pode realizar as consultas no mesmo intervalo de tempo que o Zabbix. Essa configuração não pode ser realizada devido à localização da ferramenta MUStaChe na rede, o que iria influenciar na degradação e aumento no tráfego de pacotes em determinados pontos de rede. Dessa maneira, um fator que influencia na consulta é a localização do servidor na rede, já que o servidor do sistema Zabbix, encontra-se mais centralizado do que o servidor da ferramenta MUStaChe, melhorando o tempo das consultas nos equipamentos. Mesmo assim, pode-se perceber que o tráfego apresentado pelo gráfico do sistema MUStaChe se mantem na mesma linha que o gráfico apresentado pelo sistema Zabbix. Com isso, o sistema MUStaChe apresenta igualdade em relação ao sistema Zabbix.

Outro teste realizado para validação dos gráficos, foi efetuado com clientes que au- tenticam via PPPoE. Na Figura 12, é apresentado o gráfico de um cliente monitorado pelo sistema MUStaChe. A Figura 13 apresenta o mesmo monitoramento, agora realizado com o Zabbix. Quando observadas as Figuras 12 e 13 é possível percebe que o consumo do cliente é apresentado de forma idêntica nos dois gráficos.

Considerações Finais

Este trabalho apresentou como ideia principal a criação de um sistema de monitora- mento de rede capaz de auxiliar o operador de rede em suas tarefas chamado MUStaChe. Além disso, o sistema desenvolvido foi comparado com outras ferramentas já consolidadas no mercado, a fim de desenvolver um sistema diferente em aspectos de interação e nível de usabilidade. Uma inovação apresentada na ferramenta é um mapa interativo, onde os dis- positivos que fazem parte da rede, juntamente com os usuários neles conectados podem ser observados afim de identificar claramente locais de possíveis problemas. Por fim, os resulta- dos dos testes apresentam que a ferramenta foi equivalente a outras ferramentas de mesmo propósito, além de provar que ela pode apresentar um conjunto maior de informações sobre o comportamento da rede e seus dispositivos, quando comparada individualmente com cada ferramenta.

Como trabalhos futuros, pretende-se realizar melhorias em cada função, afim de aperfeiçoar os seus resultados. Além disso, pretende-se analisar como as informações podem ser agrupadas de forma a indicar da melhor forma possíveis problemas na rede.

Referências

Ali, S. (2015). Monitoring with nagios and trend analysis with cacti. Em *Practical linux infrastructure* (pp. 167-195). Springer.

Barth, W. (2008). *Nagios: system and network monitoring*. No Starch Press.

BootStrap. (2015). Página oficial do BootStrap Framework. Available at: <http://getbootstrap.com/>. Accessed: Dezembro 2015.

Cacti. (2015). Página oficial do Cacti. Available at: <http://www.cacti.net/>. Accessed: Dezembro 2015.

Django. (2015). Página oficial do Django Framework. Available at: <https://www.djangoproject.com/>. Accessed: Dezembro 2015.

Haiyan, L. Y. L. J. Z. (2008). The application of cacti in the campus network traffic moni- toring [j]. *Computer & Telecommunication*, *4*, 004.

Josephsen, D. (2007). *Building a monitoring infrastructure with nagios*. Prentice Hall PTR.

Mescheryakov, S. V. & Shchemelinin, D. A. (2014). Analytical overview of zabbix internati- onal confe-

rence 2013. *St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunications and Control System*, 91-98.

MySQL. (2015). Página oficial do MySQL Database. Available at: <https://www.mysql.com/>. Accessed: Dezembro 2015.

Nagios. (2015). Página oficial do Nagios. Available at: <https://www.nagios.org/>. Acces- sed: Dezembro 2015.

Olups, R. (2010). *Zabbix 1.8 network monitoring.* PACKT Publishing Ltd. Vacche, A. D. & Lee, S. K. (2015). Zabbix network monitoring essentials.

Weiqiang, Z., Canhua, C. & Shujuan, L. (2011). Monitoring system for the campus card based on cacti and nagios [j]. *Experimental Technology and Management*, *4*, 079.

Zabbix. (2015). Página oficial do Zabbix. Available at: <http://www.zabbix.com/>. Acces- sed: Dezembro 2015.

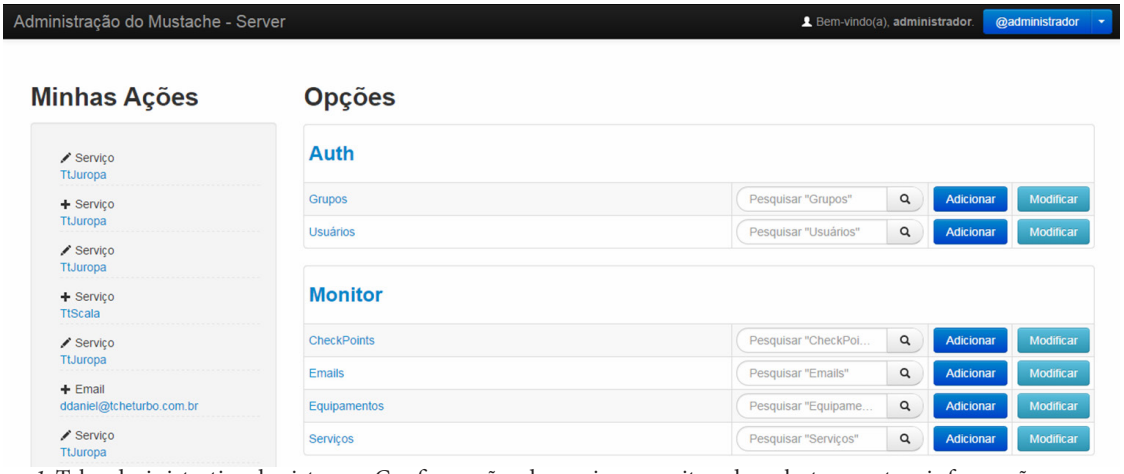

Figura 1. Tela administrativa do sistema - Configurações de serviços monitorados, alertas e outras informações.

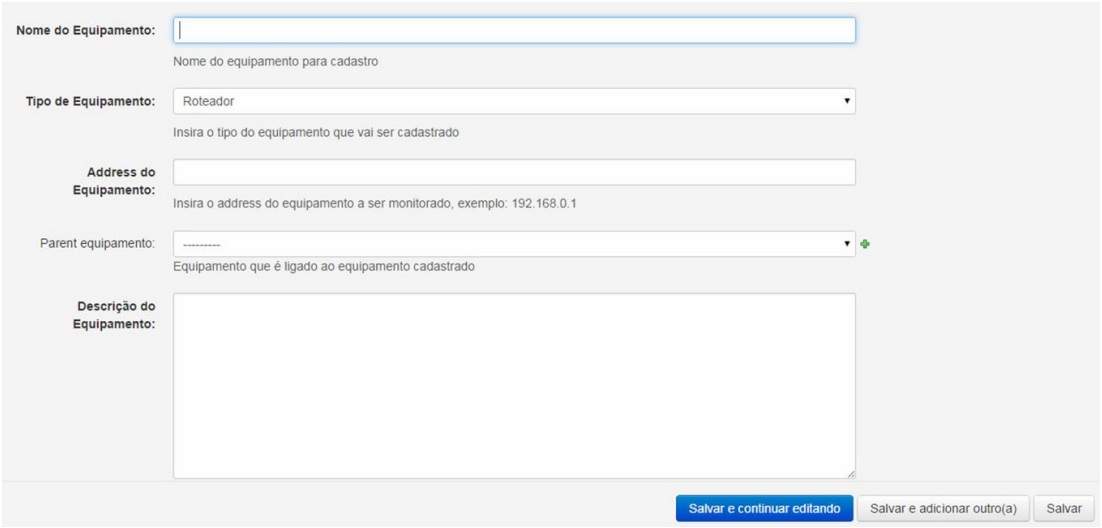

Figura 2. Tela administrativa do sistema - Cadastro de equipamentos.

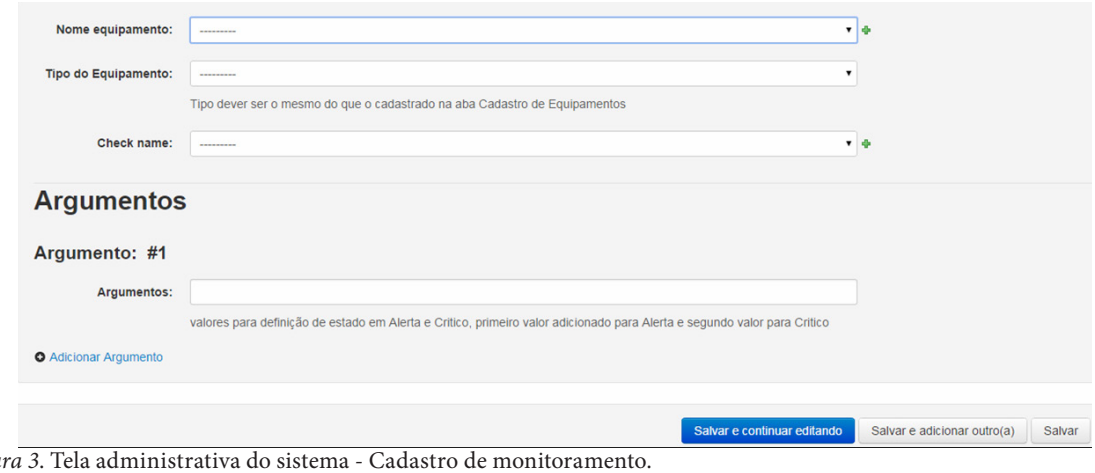

Figura 3. Tela administrativa do sistema - Cadastro de monitoramento.

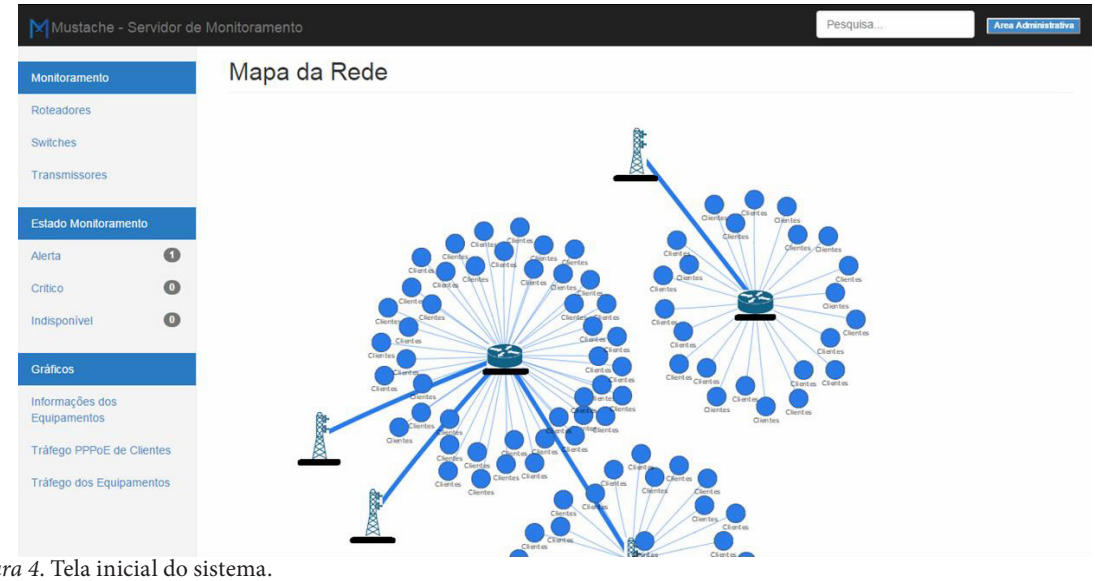

Figura 4. Tela inicial do sistema.

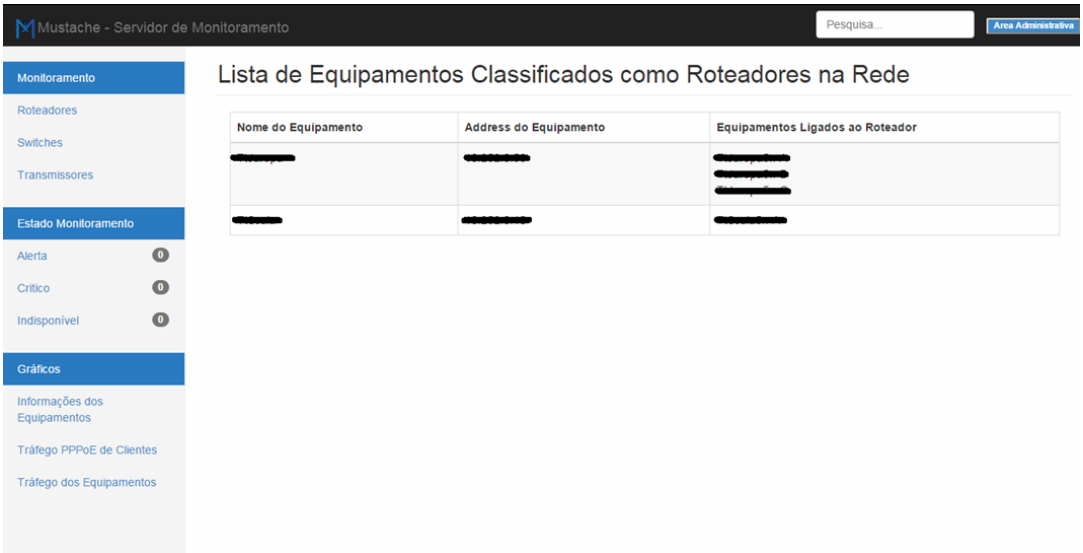

Figura 5. Listagem dos equipamentos cadastrados no sistema, filtrados por tipo roteador.

Figura 6. Listagem de todos os equipamentos que apresentam estado de alerta na rede.

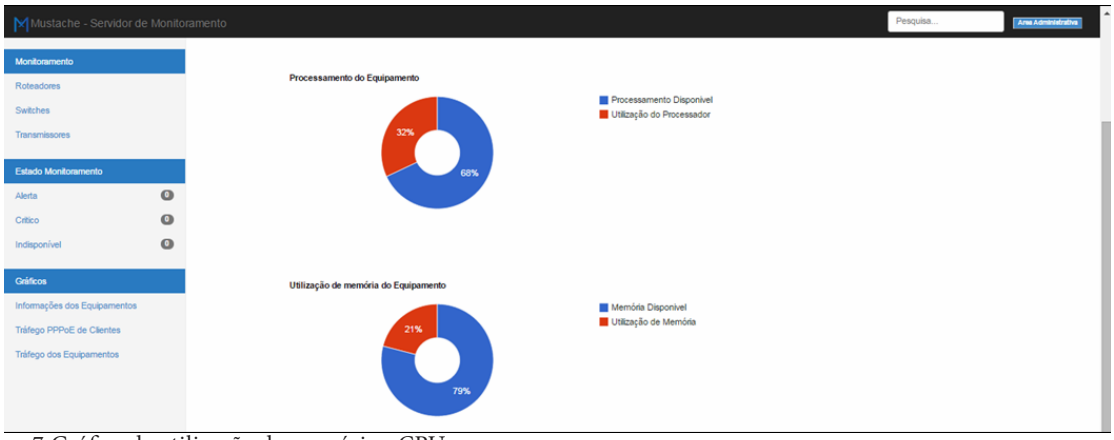

Figura 7. Gráfico de utilização de memória e CPU.

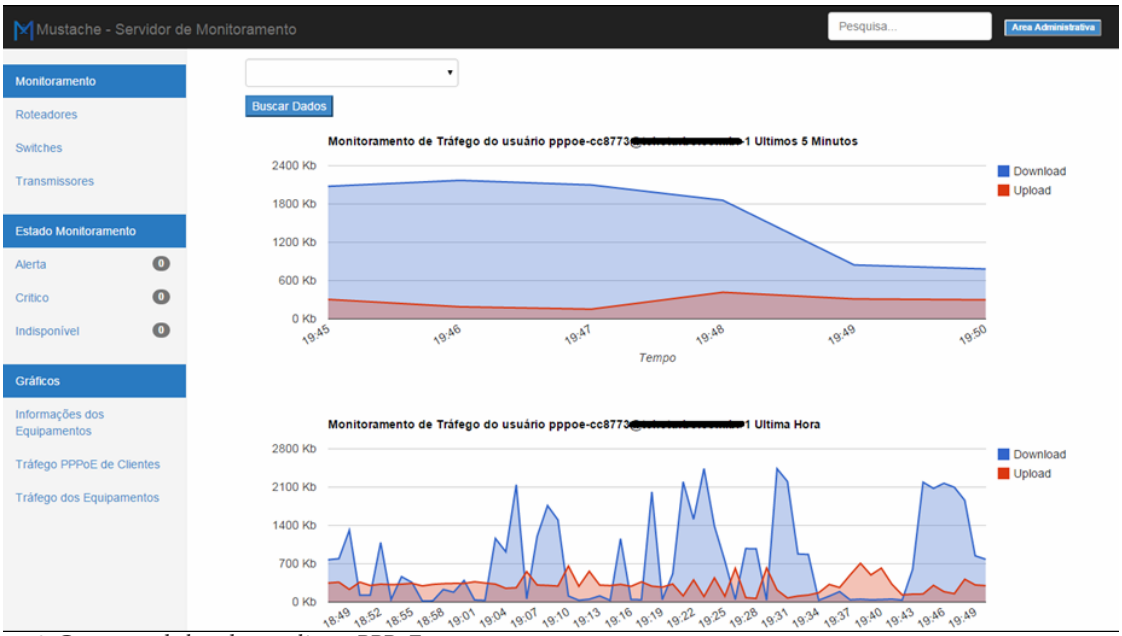

Figura 8. Consumo de banda em cliente PPPoE.

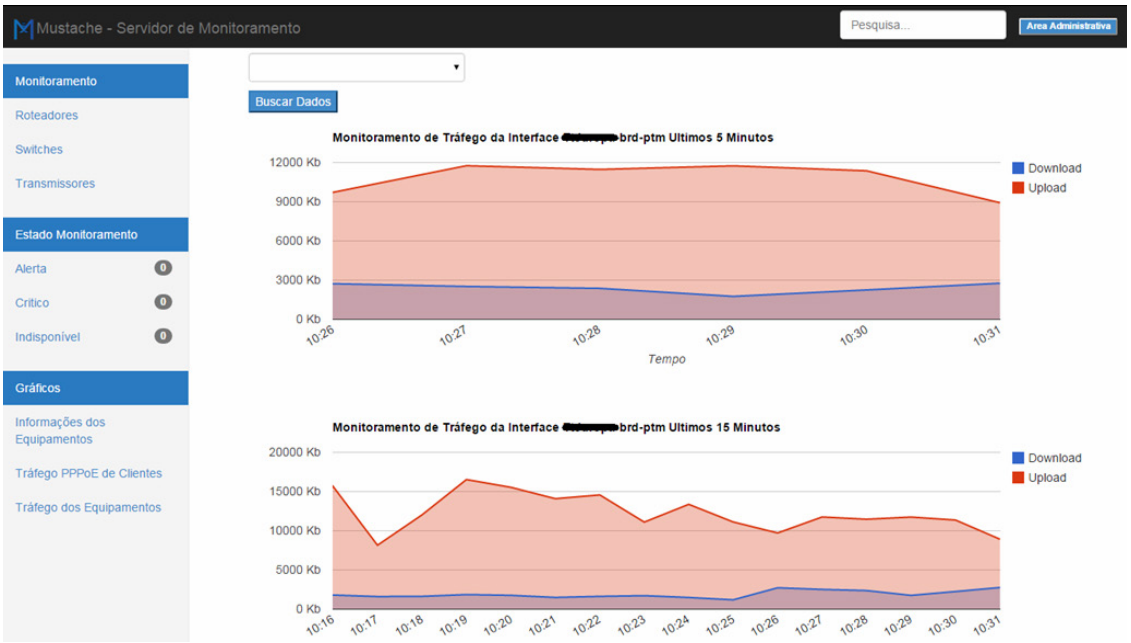

Figura 9. Consumo de banda em uma interface do equipamento.

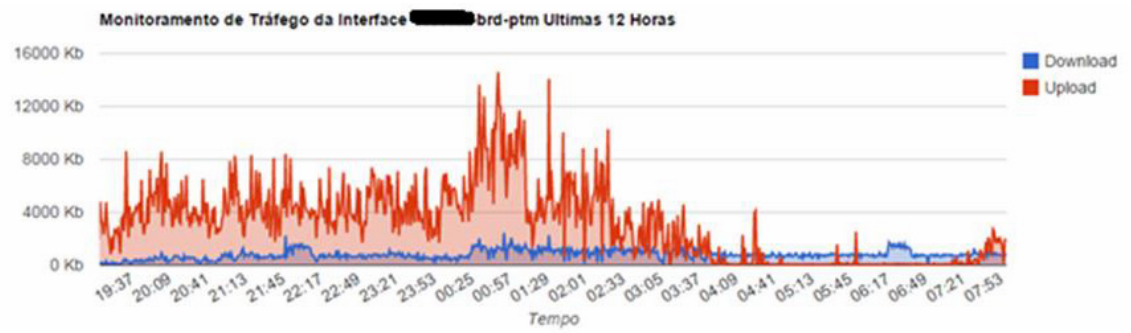

Figura 10. Gráfico da Interface Brd-Ptm do equipamento apresentado pela ferramenta MUStaChe.

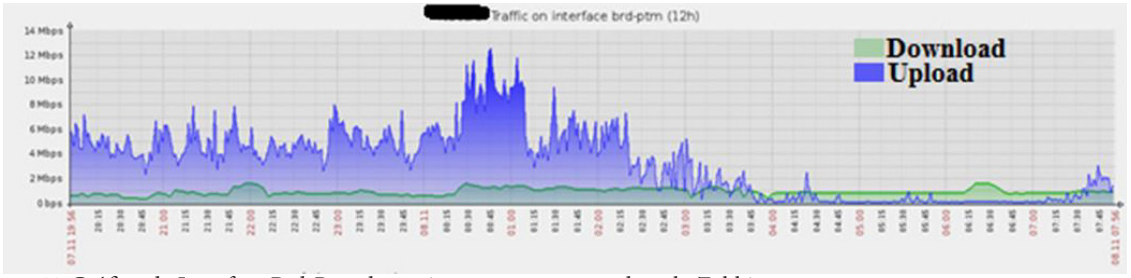

Figura 11. Gráfico da Interface Brd-Ptm do equipamento apresentado pelo Zabbix.

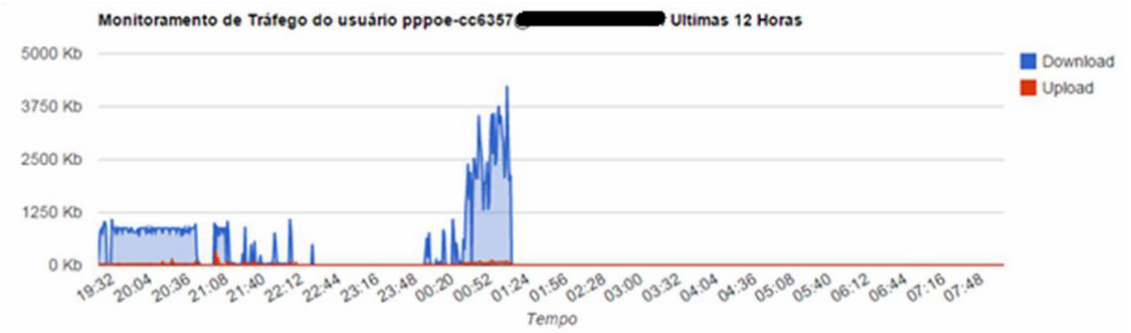

Figura 12. Gráfico da Interface Brd-Ptm do equipamento apresentado pela ferramenta MUStaChe.

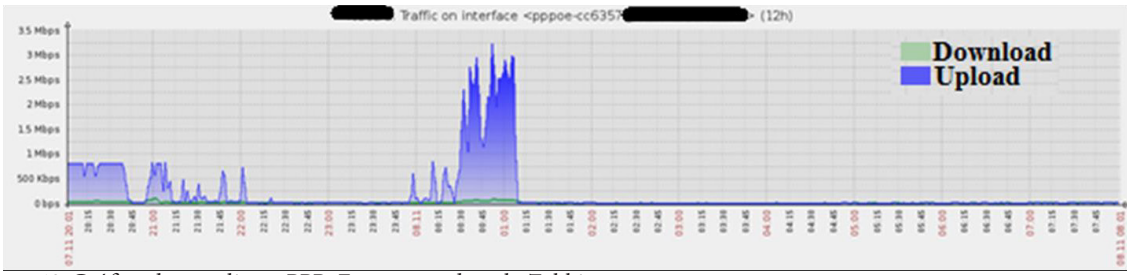

Figura 13. Gráfico de um cliente PPPoE apresentado pelo Zabbix.

Abstract

Network monitoring systems have been created in order to network administrators could identify potential network problems, such as bottlenecks, disruptions, among others. Despite presenting many benefits, one of the problems still present in the monitoring context is the necessity of use a set of tools for monitoring of goals or distinct contexts, for example, CPU, bandwidth, online users. In this context, we present a tool for network monitoring called MUStaChe, which brings together and presents a set of information not tradicionally found in network monitoring systems.The experiment results show that the MUStaChe is equivalent to existing tools, and offering a wider range of information and resources to identify potencial problems.

Keywords: Monitoring, CPU, Bandwidth, Online Users, Network Problems