UNIVERSIDADE DE CAXIAS DO SUL

GEORDANO MARCEL AREND

MONITORAMENTO VIA SNMP PARA REDES DE FIBRA ÓPTICA DO TIPO FTTH

CAXIAS DO SUL
2014

GEORDANO MARCEL AREND

MONITORAMENTO VIA SNMP PARA REDES DE FIBRA ÓPTICA DO TIPO FTTH

Trabalho de Conclusão de Curso para obtenção do grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.

Orientadora: Profª. Drª. Maria de Fátima Webber do Prado Lima

CAXIAS DO SUL
2014

GEORDANO MARCEL AREND

MONITORAMENTO VIA SNMP PARA REDES DE FIBRA ÓPTICA DO TIPO FTTH

Trabalho de Conclusão de Curso para obtenção do grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.

Aprovado(a) em 03/12/2014.

Banca Examinadora

_____
Prof. Drª. Maria de Fátima Webber do Padro Lima
Universidade de Caxias do Sul – UCS

_____
Prof. Dr. Andre Luis Martinotto
Universidade de Caxias do Sul – UCS

_____
Prof. Dr. Ricardo Vargas Dorneles
Universidade de Caxias do Sul – UCS

Dedico este trabalho à minha família por ter me apoiado sempre e por entender os momentos em que precisei ficar sozinho e tive que me fazer ausente para dedicar-me à sua realização.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus por ter dado condições para que esse trabalho pudesse ser realizado.

Agradeço também à minha orientadora Profª. Maria de Fátima, pela sua dedicação e atenção nas orientações prestadas, incentivando-me e colaborando com o desenvolvimento de minhas idéias.

De forma muito especial, agradeço à minha mãe Lourdes, meu irmão Luciano e meu tio Ari por entenderem os momentos nos quais tive que me fazer ausente para poder me dedicar à realização deste trabalho. Agradeço também pelo apoio dado e por terem se esforçado junto comigo para que sua realização fosse possível.

À minha namorada Susane, pelos momentos de ausência e de comprometimento com o trabalho, deixando o tempo que era nosso para depois.

Agradeço também à empresa Bom Tempo Telecom por ter permitido que seu nome fosse utilizado nessa publicação e também por permitir a implementação desta solução dentro do seu ambiente de trabalho e produção.

RESUMO

Este trabalho tem como objetivo analisar e avaliar *softwares* que possibilitam monitorar redes de fibra óptica. As redes a serem monitoradas são fundamentadas no conceito de que um cabo óptico chega até a residência do assinante, fazendo com que o meio físico entre a central da operadora e o assinante seja totalmente constituído por fibra óptica. Para embasar esta avaliação, foram utilizados diversos conceitos, como a definição de fibra óptica, topologias de redes ópticas, a arquitetura de gerenciamento TCP/IP e métricas para avaliação de desempenho de redes. Entre os diversos *softwares* estudados e analisados, os escolhidos para serem testados foram o *Cacti*, o *Nagios* e o *Zabbix*. Para realizar o comparativo entre os *softwares* será utilizado o Método Analítico Hierárquico, que é uma importante ferramenta no auxílio de tomada de decisões. O comparativo entre os *softwares* será realizado baseado na definição de critérios, que servirão para definir qual deles atende da melhor forma aos requisitos de funcionalidades solicitadas.

Palavras-chave: Monitoramento de Fibra Óptica, Gerenciamento GPON, FTTH, Monitoramento com SNMP, Método Analítico Hierárquico.

ABSTRACT

This study aims to analyze and evaluate software that enables monitoring fiber optic networks. The networks to be monitored are based on the concept that an optical cable reaches the home of the subscriber, causing the physical medium between the plant operator and the subscriber to be entirely constituted by optical fiber. To support this assessment, several concepts such as the definition of optical fiber, optical network topologies, the TCP/IP Management Architecture and metrics for evaluating the performance of networks were used. Among the various software studied and analyzed, the ones to be tested were Cacti, Nagios and Zabbix. To perform the comparison between them Analytic Hierarchy software, which is an important tool to support decision making is used. The comparison between the software will be made based on the definition of criteria, which serve to define which one suits the best to the requirements of requested features.

Keywords: Fiber Optic Monitoring, Management GPON, FTTH, Monitoring with SNMP, Analytic Hierarchy Process.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ADSL	*Asymmetric Digital Subscriber Line*
AES	*Advanced Encryption Standard*
AON	*Active Optical Network*
APON	*Asynchronous Transfer Mode Passive Optical Network*
ARP	*Address Resolution Protocol*
ASN.1	*Abstract Syntax Notation One*
ATM	*Asynchronous Transfer Mode*
BPON	*Broadband Passive Optical Network*
CDM	*Code Division Multiplexing*
CGI	*Common Gateway Interface*
DBA	*Dynamic Bandwidth Allocation*
DHCP	*Dynamic Host Configuration Protocol*
EGP	*Exterior Gateway Protocol*
EPON	*Ethernet Passive Optical Network*
EUA	Estados Unidos da América
FAN	*Fully Automated Nagios*
FTTA	*Fiber-to-the-Apartment*
FTTB	*Fiber-to-the-Building*
FTTC	*Fiber-to-the-Curb*
FTTH	*Fiber-to-the-Home*
FXS	*Foreign Exchange Office*
Gbps	*Gigabits* por Segundo
GPL	*Gnu General Public License*
GPON	*Gigabit Passive Optical Network*
GSM	*Global System for Mobile Communications*
HTML	*HyperText Markup Language*
IAB	*International Activities Board*
IAM	Inconsistência Aleatória Média
IC	Índice de Consistência
ICMP	*Internet Control Message Protocol*
IEEE	*Institute of Electrical and Electronic Engineers*
IETF	*Internet Engineering Task Force*

IPv4	*Internet Protocol Version* 4
IPv6	*Internet Protocol Version* 6
ISO	Imagem de Sistema Operacional
MAC	*Medium Access Control*
MAH	Método Analítico Hierárquico
Mbps	*Megabits* por segundo
MIB	*Management Information Base*
MPCP	*Multi-Point Control Protocol*
NAT	*Network Address Translation*
OCDM	*Optical Code Division Multiplexing*
OID	*Object Identifier*
OLT	*Optical Line Terminal*
ONU	*Optical Network Unit*
OSI	*Open Systems Interconnection*
OTDM	*Optical Time Domain Multiplexing*
PHP	*Hypertext Preprocessor*
PON	*Passive Optical Network*
PPPoE	*Point-to-Point Protocol over Ethernet*
RC	Razão de Consistência
RF	*Radio Frequency*
RRDTOOL	*Round Robin Database*
SGBD	Sistema Gerenciador de Banco de Dados
SGMP	*Simple Gateway Management Protocol*
SLA	*Service Level Agreement*
SMI	*Structure of Management Information*
SMING	*Structure of Management Information Next Generation*
SMS	*Short Message Service*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol/Internetworking Protocol*
TDMA	*Time Division Multiple Access*
UDP	*User Datagram Protocol*
UTP	*Unshielded Twisted Pair*

VOIP	*Voice Over Internet Protocol*
VPN	*Virtual Private Network*
XML	*eXtensible Markup Language*
WDM	*Wavelength Division Multiplexing*
WDM-PON	*Wavelength Division Multiplexing – Passive Optical Network*

SUMÁRIO

1 INTRODUÇÃO

Com o surgimento da informática e do conceito de globalização, que pregam a comunicação em redes, surgiu a necessidade de interconectá-las. Inicialmente essa interconexão apresentava pouca velocidade. De fato, segundo Assis e Waldman (2004), desde a invenção do computador até os anos 80, a capacidade de processamento eletrônico aumentava mais rapidamente do que as velocidades de transmissão. Era necessário que a velocidade de transmissão acompanhasse o poder computacional existente.

Assim nos anos 80 e 90, grandes operadoras de telefonia passaram a utilizar a tecnologia ADSL (*Asymmetric Digital Subscriber Line*) para fazer a conexão entre redes de computadores, disponibilizando acesso à internet através de um cabo metálico que entrava na residência do assinante. Mesmo operando sobre um meio de transporte de informações cabeado, o ADSL possuía limitações de largura de banda, o que não permitia entregar para o assinante diversos serviços, como a TV por assinatura, por exemplo. De acordo com Tanenbaum (2003), a tecnologia ADSL não era capaz de suportar a demanda por essa largura de banda, fazendo com que fosse necessária a procura por outras tecnologias capazes de oferecerem maior capacidade de transmissão de dados e informações.

Para suprir essa demanda, foi desenvolvida a fibra óptica, resultado da aplicação de estudos, pesquisas e desenvolvimento sobre o assunto. Ela começou a ser estudada no século XIX. O matemático Willebrord Snell, em 1621, fez uma importante descoberta, onde percebeu que quando a luz atravessava dois meios, sua direção mudava. Com isso o matemático descreveu o princípio de refração da luz, fenômeno que ele foi capaz de demonstrar através de uma vara em um copo de água (OLIVEIRA, 2010).

Empregando o conceito de refração descoberto anteriormente, em 1960, com a invenção do laser, a capacidade de banda de comunicação aumentou em relação aos meios de comunicação existentes até a época. Através desse avanço tecnológico, a tecnologia de redes de comunicação óptica começava a tomar forma (OLIVEIRA, 2010).

A partir das descobertas e estudos feitos, foi então desenvolvido um cabo que continha diversas ramificações internas conhecidas como fibras ópticas, que passou então a ser utilizada para fazer a transmissão de dados e informações. Segundo Assis e Waldman (2004), a partir dessa visão, com o amadurecimento da tecnologia óptica, as velocidades de transmissão tiveram um aumento de várias ordens de magnitude, fazendo com que o gargalo passasse a ficar por conta dos nós eletrônicos de processamento, e não mais nos meios de

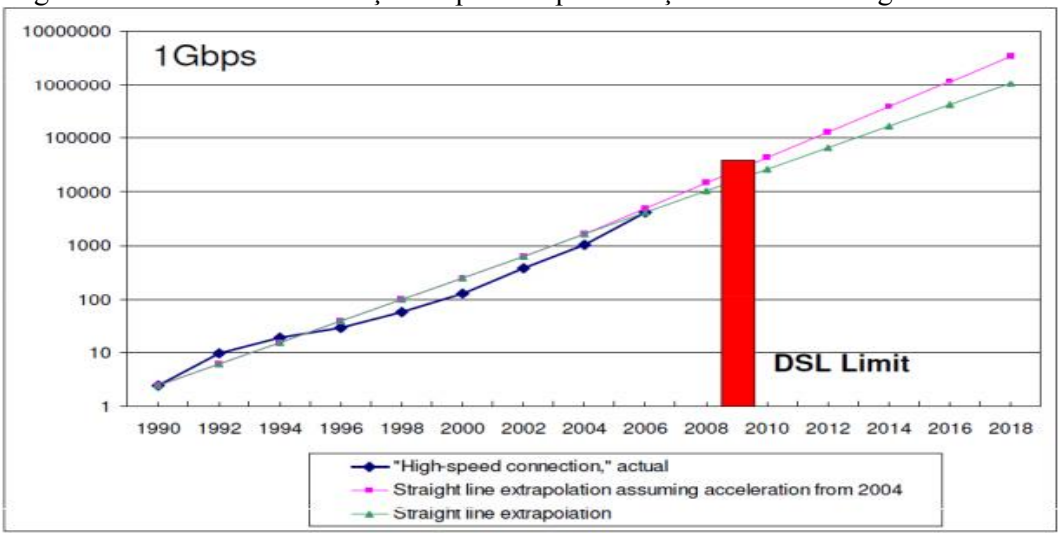
transmissão. Ela passou a ser utilizada também para fazer comunicações ópticas intercontinentais, tamanha a sua eficiência e capacidade.

Apesar do grande desempenho na transmissão de dados, todo sinal transmitido em um meio de comunicação sofre atenuação de sinal. Quando feita uma transmissão em grandes distâncias, geralmente superiores a 100 quilômetros, as redes ópticas requerem a utilização de retransmissores ou amplificadores de sinal óptico que fazem o papel de amplificar o sinal transmitido na fibra. Isso faz com que o sinal chegue com qualidade e com a intensidade adequada até o seu ponto final.

Através do aproveitamento das características de baixa atenuação da fibra óptica em curtas distâncias aliadas ao desenvolvimento de tecnologias que possibilitavam o compartilhamento de fibra óptica para a rede de acesso de assinantes, começou a formar-se uma ótica diferente em relação à tecnologia de acesso por fibra óptica. Consistia em utilizar uma mesma fibra para atender mais de um assinante. Dessa forma, diversos assinantes seriam atendidos através de uma única fibra, diferentemente da arquitetura tradicional, que era capaz de atender a apenas um único assinante.

Através da arquitetura de atendimento compartilhada, a rede óptica ficou mais rentável, devido ao número de assinantes atendidos ser exponencialmente maior do que em uma rede convencional. Ramos (2009) afirma que existe um aumento exponencial na procura por serviços que possibilitem a entrega de maior largura de banda, resultante de inovação dos equipamentos e da tecnologia aplicada na entrega dos serviços aos usuários finais. A Figura 1 mostra esse aumento e faz uma projeção de demanda até o ano de 2018.

Figura 1 - Tendência da evolução da procura por serviços com maior largura de banda

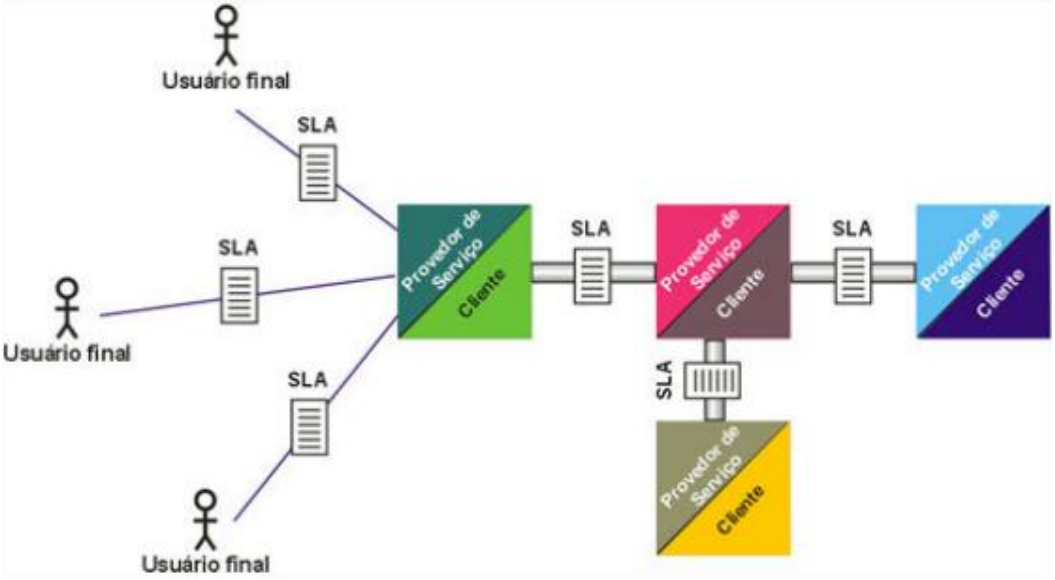


Fonte: RAMOS (2009)

Apesar da nova arquitetura de atendimento compartilhada por diversos assinantes ser interessante e possuir bastante procura conforme indicado na figura anterior, existem algumas dificuldades nesse tipo de rede que não eram encontradas na arquitetura de rede tradicional, como por exemplo, o gerenciamento. Na nova arquitetura, a identificação de falhas no trajeto percorrido pelo cabo fica mais difícil de ser constatada devido ao fato das conexões passarem por compartilhamento e por não serem mais conexões fim-a-fim. Arquiteturas tradicionais com dois equipamentos em cada enlace são mais fáceis de serem gerenciadas do que redes com 64 equipamentos em um mesmo barramento, como acontece em alguns casos de arquiteturas ópticas compartilhadas.

O gerenciamento de rede é capaz de determinar o seu estado e é considerado um fator vital. Para aquelas que oferecem garantias de qualidade de serviço, o monitoramento se torna ainda mais vital, uma vez que possui o objetivo de assegurar que os objetivos de QoS (*Quality of Service*) estabelecidos em contrato estão sendo atingidos. Contratos de Acordo de Nível de Serviço (SLA – *Service Level Agreement*) são firmados e asseguram o fornecimento de um determinado serviço com disponibilidade e qualidade especificados. Conforme Guimarães (2007), o não cumprimento do SLA implica em penalidades aplicadas ao prestador de serviços, estabelecidas em contrato. A Figura 2 apresenta os diferentes atores que compõem os diversos relacionamentos de um contrato de SLA.

Figura 2 – Envolvimento entre clientes e provedores de serviço



Fonte: GUIMARÃES (2007)

Através do monitoramento da rede é possível verificar o cumprimento de acordos de interconexão até mesmo entre provedores de serviços, medindo e monitorando, por exemplo, o fluxo de tráfego que atravessa os enlaces de interconexão e os roteadores de borda.

Com o avanço das tecnologias que possibilitam atender vários assinantes com uma única fibra óptica e também das técnicas de monitoramento, começou a chegar-se a uma arquitetura de rede com uma boa relação custo-benefício. Segundo Silva (2012), algumas tecnologias têm uma boa aceitação por parte dos usuários devido ao custo acessível, mas possuem limitação de largura de banda que não permite a oferta de alguns serviços. Outras tecnologias permitem o tráfego de altas taxas de velocidade, mas possuem elevados custos de implantação.

A necessidade de equilíbrio entre custo e largura de banda, motivou o desenvolvimento das Redes Ópticas Passivas (PON – *Passive Optical Networks*). Um dos tipos de arquitetura PON é chamado de FTTH (*Fiber-to-the-Home*), a qual será tema deste trabalho.

1.1 PROBLEMA DE PESQUISA

Em redes de acesso por fibra óptica, na mesma proporção em que a capacidade de transmissão de dados e informações é elevada, também é elevada a probabilidade de ocorrerem problemas com o meio físico de transporte, no caso o cabo de fibra óptica. O cabo de fibra óptica pode sofrer rupturas, onde o serviço fica totalmente indisponível e pode sofrer atenuações, que a médio ou longo prazo poderá causar rupturas e, conseqüentemente, a indisponibilidade do serviço. Para possibilitar a confiabilidade desses serviços, atitudes preventivas poderiam ser tomadas através do auxílio de um *software* que faça a identificação automática de degradações nos níveis de sinal dos *links* de acesso dos clientes.

O *software* deverá possibilitar o envio de alertas para as áreas responsáveis por reparos e manutenções a fim de corrigir o problema no menor prazo possível. Atitudes pró-ativas como essa fazem com que os níveis de SLA estabelecidos em contrato firmado entre a empresa prestadora do serviço e o cliente sejam mantidos dentro do estabelecido. Devido à escassez de recursos para a elaboração e implantação deste projeto, o *software* deve ser de licença de utilização livre. Além disso, deve trabalhar com o protocolo SNMP (*Simple Network Management Protocol*) em cima da rede TCP/IP (*Transmission Control Protocol/Internetworking Protocol*) para realizar o monitoramento do sinal dos equipamentos instalados nos clientes. A *interface* do *software* deve ser *web* e de fácil utilização, a fim de

permitir um monitoramento pró-ativo à todas as áreas da empresa, principalmente no nível de suporte.

1.2 OBJETIVOS

O objetivo geral deste trabalho é selecionar, adaptar e implantar uma solução baseada em *software* livre para monitorar e emitir alarmes quando houver variação e degradação em *links* de fibra óptica. Esta solução deverá permitir a tomada de decisões pró-ativas a fim de restabelecer os serviços prestados o mais breve possível.

Para atingir o objetivo deste trabalho, ele será orientado por dois objetivos específicos:

- Definir as características importantes que devem ser monitoradas através do *software*;

- Selecionar um *software* livre que melhor realize o monitoramento do sinal em *links* de acesso por fibra óptica.

1.3 ESTRUTURA DO TRABALHO

No Capítulo 2 deste trabalho, é feita uma explanação sobre os conceitos referentes à fibra óptica, bem como as suas principais características e aplicações. O Capítulo 3 explica o tipo de arquitetura de rede de acesso FTTH que é utilizada para fazer a transmissão de dados entre o provedor de serviços e o assinante. O Capítulo 4 descreve as principais métricas possíveis de serem utilizadas em redes de acesso óptico, a fim de manter uma disponibilidade sempre alta e o serviço sempre dentro da qualidade esperada pelo assinante. O Capítulo 5 apresenta o funcionamento da arquitetura para gerenciamento TCP/IP, que foi adotado como padrão para gerência de redes e monitoramento de dispositivos. O Capítulo 6 detalha o Método Analítico Hierárquico, que será o método utilizado para comparar os *softwares* para gerenciamento de redes TCP/IP. O Capítulo 7 trata da elaboração e redação da proposta de solução para o problema explanado, bem como a seleção dos *softwares* que serão testados e os critérios para realizar o comparativo entre os *softwares* selecionados. No Capítulo 8 são relatados os testes efetuados com os softwares, bem como os problemas encontrados. O Capítulo 9 trata da avaliação dos critérios através do Método Analítico Hierárquico para cada

um dos softwares testados. Por fim, no Capítulo 10, são apresentadas as conclusões obtidas através da realização deste trabalho.

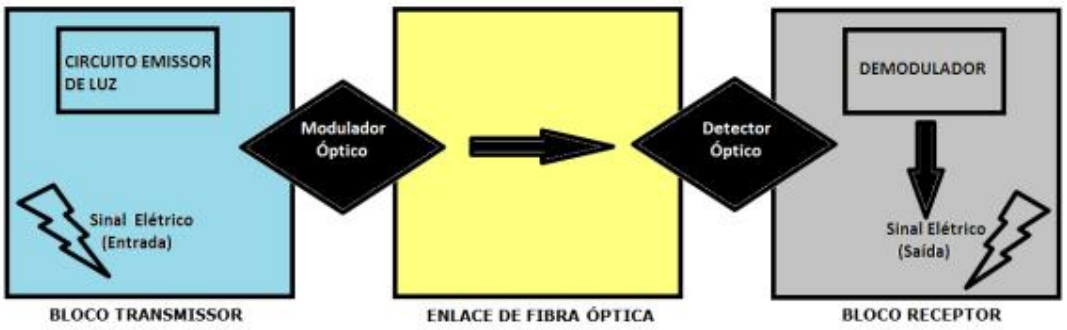
2 REDES ÓPTICAS

Um sistema óptico de comunicação é composto basicamente por três elementos: sistema transmissor, meio de propagação e detector óptico. O sistema transmissor é responsável por inserir o sinal óptico no meio de propagação. O meio de propagação é a fibra óptica que é formada por fibras de vidro ultrafinas. O detector óptico é uma espécie de receptor. Sua função é detectar o recebimento de um sinal óptico e converter esse sinal novamente em elétrico. Esse processo de conversão feito pelo detector óptico possibilita a comunicação através de um meio óptico, visto que a maior parte dos equipamentos envia sinais elétricos (PAIVA, 2010).

2.1 TRANSMISSÃO

Em um sistema de comunicação óptica digital, representado na Figura 3, o sinal de entrada é apresentado em pulsos elétricos. Um modulador óptico recebe o sinal elétrico já convertido em sinal óptico pelo circuito emissor de luz, e propaga o sinal através do enlace de fibra óptica. No final do enlace óptico encontra-se um detector óptico, que faz a detecção do recebimento do sinal óptico e o envia para o demodulador. Este por sua vez, faz a interpretação dos sinais ópticos recebidos e também a sua conversão para sinal elétrico. Dessa forma, um sistema de comunicação óptica digital é capaz de trafegar informações de um lado do enlace, que seria o transmissor, para o outro lado, o receptor.

Figura 3 - Sistema de comunicação óptica digital



Fonte: http://www.cin.ufpe.br/~pasg/gpublications/pgfp10-monografia-esp.pdf acesso em 04/05/2014

De acordo com Paiva (2010), o funcionamento de um sistema de comunicação óptica necessita de diversos elementos, chamados componentes ópticos. São eles:

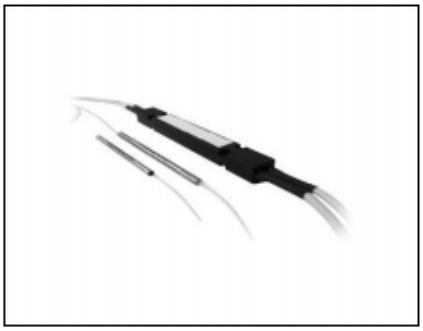
- Detectores ópticos: são componentes responsáveis por fazer a detecção do sinal óptico em um enlace óptico.
- Amplificadores ópticos ou repetidores (Figura 4): são equipamentos que aumentam a intensidade do sinal óptico propagado em um enlace. Geralmente são utilizados em enlaces muito distantes, onde o sinal não tem intensidade suficiente para chegar ao outro lado do enlace para estabelecer a conexão.

Figura 4 – Amplificador óptico

Fonte: http://www.cin.ufpe.br/~pasg/gpublications/pgfp10-monografia-esp.pdf acesso em 04/05/2014

- Acoplador de fibra (Figura 5): componente responsável por fazer a distribuição do sinal a partir de uma fibra principal para outras fibras secundárias.

Figura 5 - Acoplador de fibra



Fonte: http://www.cin.ufpe.br/~pasg/gpublications/pgfp10-monografia-esp.pdf acesso em 04/05/2014

- Conectores de fibra (Figura 6): a comunicação óptica em um enlace necessita de emendas no cabo para completar o seu percurso, visto que os enlaces geralmente são distantes o que impossibilita a instalação de um cabo inteiro. Assim sendo, são instalados diversos cabos menores que posteriormente devem ser unidos. A

emenda desses cabos pode ser do tipo permanente ou desmontável. Para o tipo de emenda desmontável são utilizados conectores.

Figura 6 - Conectores ópticos

Fonte: http://www.classeacabos.com.br/fibraoptica.html acesso em 04/05/2014

- Emendas ópticas por fusão: as conexões feitas de forma permanente são feitas através de fusões ópticas. A fusão é feita através da utilização de uma máquina de fusão (Figura 7) e consiste na junção perfeita dos núcleos de duas pontas de fibra óptica a fim de permitir a transmissão de luz com o mínimo de perda possível através do seu meio.

Figura 7 – Máquina de fusão

Fonte: http://www.dicomp.com.br/produto/9245/maquina-de-fusao-para-fibra-optica-nazda-nz-02h acesso em 04/05/2014

2.2 TÉCNICAS DE MULTIPLEXAÇÃO EM REDES ÓPTICAS

A possibilidade de compartilhamento de banda em uma única fibra óptica se tornou possível após o desenvolvimento de técnicas de multiplexação de redes ópticas e consiste em transmitir diversos comprimentos de onda em uma única fibra óptica. O objetivo do desenvolvimento da multiplexação é transmitir o maior número de sinais ópticos em uma mesma fibra óptica, possibilitando assim o aumento da largura de banda transmitida no meio físico. Segundo Paiva (2010), as técnicas de multiplexação desenvolvidas foram a Multiplexação por Divisão de Comprimento de Onda ou WDM (*Wavelenght Division Multiplexing*), a Multiplexação Óptica por Divisão de Tempo ou OTDM (*Optical Time Domain Multiplexing*), a Multiplexação por Divisão de Códigos Ópticos ou OCDM (*Optical Code Division Multiplexing*), além das técnicas híbridas WDM/OTDM e WDM/OCDM.

2.2.1 Multiplexação óptica por comprimento de onda - WDM

A técnica de multiplexação WDM consiste em enviar diversos sinais ópticos através de uma única fibra óptica, sendo eles de comprimentos de onda diferentes. Cada sinal trafega no meio físico com o seu próprio comprimento de onda, sem ser interferido por outro comprimento, mesmo que esse seja transmitido na mesma fibra óptica. Essa técnica de multiplexação permite a transmissão de qualquer combinação de comprimentos de onda diferentes (CHAGAS, 2010).

Essa técnica de multiplexação foi desenvolvida inicialmente para ser utilizada em enlaces ponto-a-ponto, possibilitando assim uma maior largura de banda de transmissão em grandes distâncias. Têm-se conhecimento de transmissões com a técnica de multiplexação WDM com alcance de 10.000 quilômetros transmitindo uma largura de banda de 100Gbps (*Gigabits* por Segundo).

2.2.2 Multiplexação óptica por divisão de tempo – OTDM

A técnica de multiplexação óptica por divisão de tempo (TDM – *Time Division Multiplexing*) consiste em enviar diversos sinais ópticos em um mesmo canal óptico. Esses sinais são armazenados numa espécie de buffer, que é uma fila no equipamento transmissor do sinal óptico, e recebem um número de sequência determinado pelo multiplexador. Paiva (2010) cita como uma vantagem da utilização dessa técnica de multiplexação, a variação

rápida do número de sinais ao longo da fibra, fazendo melhor aproveitamento do meio físico onde por conseqüência a largura de banda é maior.

2.2.3 Multiplexação por divisão de códigos ópticos – OCDM

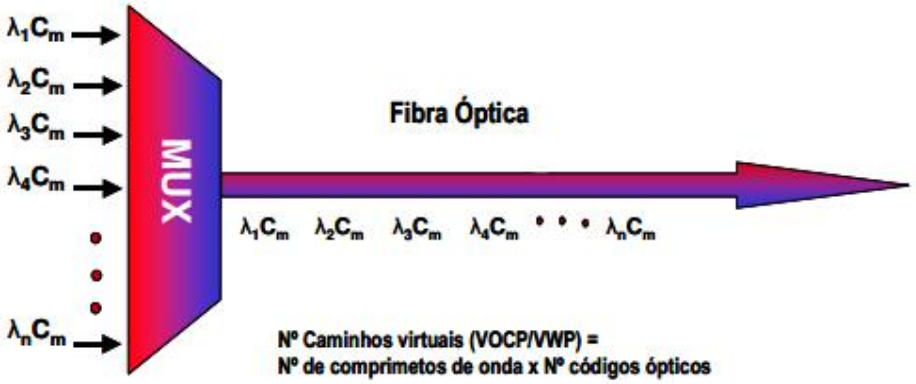
Essa técnica de multiplexação é derivada da técnica de Multiplexação por Divisão de Códigos – CDM (*Code Division Multiplexing*) que havia sido desenvolvida para a comunicação em redes sem fio. A técnica OCDM foi desenvolvida para funcionar em redes ópticas. Os componentes necessários para o funcionamento dessa técnica de multiplexação são um codificador, localizado no transmissor, e um decodificador, localizado no receptor. Para o funcionamento dessa técnica, o transmissor envia um sinal óptico contendo um código único através da fibra óptica. No lado receptor do enlace, o decodificador recebe o sinal óptico e faz a leitura dos códigos recebidos para poder entregar os sinais recebidos na sua ordem correta (Galdino, 2008).

Quando utilizada a técnica OTDM, existe o risco de ocorrer algum atraso no envio de informações, fazendo com que dados possam ser perdidos. A técnica OCDM por sua vez, não é afetada pelo atraso no envio de informações, devido a ser baseada em códigos. Assim sendo, é possível observar que a técnica OCDM tem vantagem sobre a técnica OTDM, tornando-se assim mais estável. Quando comparada à técnica WDM, a técnica OCDM leva vantagem porque a WDM precisa reservar banda para prevenir interferências na fibra óptica, que é uma necessidade não encontrada quando se utiliza a técnica OCDM.

2.2.4 Técnicas híbridas de multiplexação

Apesar de ter sido desenvolvida originalmente para ser utilizada em enlaces ponto-a-ponto, a técnica de multiplexação WDM pode ser combinada com outras técnicas, como por exemplo, a OTDM e a OCDM. Essa combinação é utilizada para aumentar a capacidade de número de usuários ou assinantes num mesmo canal de comunicação. Em uma rede WDM combinada com OCDM (Figura 8), por exemplo, vários canais são criados através da técnica de multiplexação WDM, e dentro de cada canal, a técnica OCDM se encarrega de distribuir os códigos para cada sinal gerado. Dessa forma obtêm-se uma rede com maior largura de banda e que, consequentemente, suporta um maior número de recursos (GALDINO, 2008).

Figura 8 – Técnica de multiplexação WDM/OCDM



Fonte: GALDINO (2008)

2.3 CONSIDERAÇÕES DO CAPÍTULO

Em um sistema de comunicação óptica, as técnicas de multiplexação são largamente utilizadas para aumentar a largura de banda disponível e para otimizar os recursos do meio físico, que são limitados, como por exemplo, o número de fibras de um cabo óptico. Através da utilização da multiplexação em sistemas de comunicação óptica, é possível entregar diversos serviços diferentes para o assinante, sendo cada um deles logicamente separado através de comprimentos de onda diferentes dentro do mesmo cabo óptico. Para entregar esse tipo de serviços, o conceito de tecnologia FTTH surge forte no mercado e vem possibilitando entregar serviços heterogêneos de qualidade para o assinante, conforme será descrito no capítulo seguinte.

3 FTTH

Um dos conceitos de tecnologia desenvolvida em redes ópticas passivas foi a FTTH, que segundo Mohandas, Jayasree e Varghese (2013), surgiu como a melhor solução para conectividade de última milha em comparação com todas as outras tecnologias com fio. A tecnologia FTTH funciona em uma arquitetura onde uma única fibra óptica possibilita o atendimento a diversos assinantes.

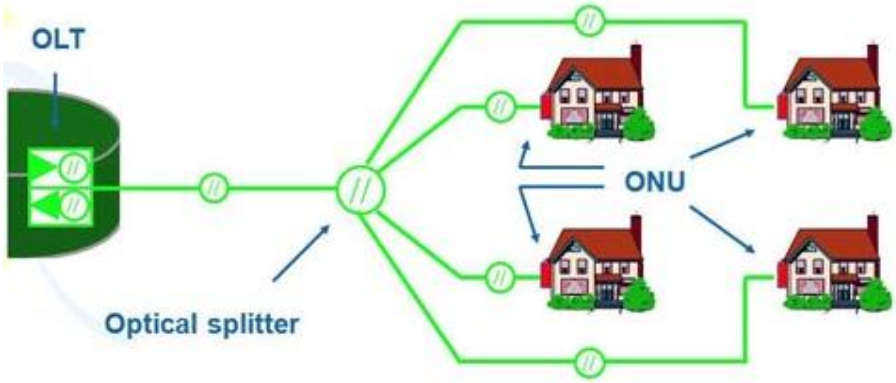
Para possibilitar a montagem de uma arquitetura que permita compartilhar uma única fibra óptica para acesso, existe a possibilidade de utilização de duas arquiteturas de redes ópticas: a PON e a AON (*Active Optical Network*). Neste trabalho serão tratadas apenas as redes ópticas do tipo PON, devido ao fato de se mostrarem mais estáveis para a montagem de uma estrutura de atendimento óptico para usuários finais. A seção seguinte tratará desse tipo de rede óptica de acesso.

3.1 REDES ÓPTICAS PASSIVAS (PON)

Redes ópticas passivas são redes de acesso óptico que possibilitam o compartilhamento de fibras ópticas para o atendimento de assinantes. Esse tipo de rede é caracterizada pela utilização apenas de componentes ópticos passivos no decorrer da rede e pela limitação de distância para atender assinantes a no máximo 50 quilômetros. A estabilidade superior de uma rede PON, quando comparada à rede AON, caracteriza-se pelo fato de não necessitar de energia elétrica em todo o trajeto do cabo óptico entre a central da operadora até a residência do assinante.

Segundo Takeuti (2005), redes ópticas passivas são redes de acesso que utilizam fibra óptica em uma estrutura ponto-multiponto, sendo constituídas apenas por componentes ópticos passivos entre o Terminal de Linha Óptica (*Optical Line Terminal* - OLT) e a Unidade de Rede Óptica (*Optical Network Unit* – ONU). A Figura 9 ilustra de uma maneira simples o funcionamento de uma rede óptica passiva.

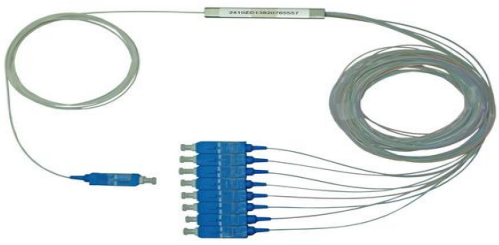
Figura 9 – Estrutura de uma rede óptica passiva



Fonte: http://www.instaladoresdetelecomhoy.com/analizador-y-emulador-para-redes-gpon/ acesso em 04/05/2014

Em uma estrutura ponto-multiponto, a OLT é o equipamento gerador do sinal óptico e que gerencia as conexões para todos os usuários de uma rede de acesso óptico. A ONU, vulgarmente conhecida como modem óptico, é o equipamento que é instalado na residência do assinante e é responsável por fazer a conversão do sinal de fibra óptica em sinal de dados. Para possibilitar o compartilhamento de uma mesma fibra óptica, é utilizado um divisor óptico chamado *splitter* (Figura 10). O *splitter* geralmente contém uma entrada e pode ter 2, 4, 8, 16, 32 ou 64 saídas. Ele recebe o sinal óptico na entrada e divide a potência do sinal recebido para as saídas, fazendo com que o sinal chegue até todas as suas saídas, porém com menor intensidade. A ONU possui uma porta óptica de entrada para a conexão da fibra e saídas elétricas RJ45, variando geralmente de 1 a 4 saídas. Entre os diversos modelos existentes de ONU, existem as que possuem *wireless* integrado, *interface* VOIP (*Voice Over Internet Protocol*) para a conexão de um aparelho telefônico e também as com saída RF (*Radio Frequency*), utilizada para transmitir a imagem da ONU para a conexão de vídeo da TV.

Figura 10 – *Splitter* PON 1x8



Fonte: http://www.ispshop.com.br acesso em 22/04/2014

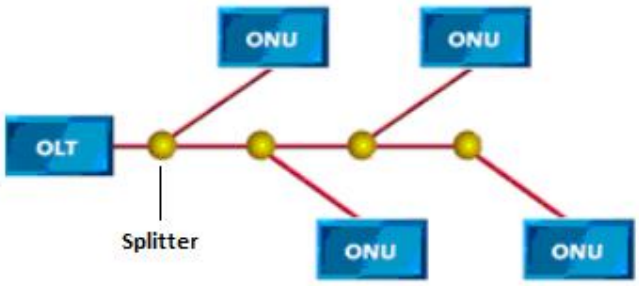
Apesar do conceito de topologia PON ser simples, existem diferentes topologias de rede que podem ser construídas dependendo do projeto de montagem da rede por parte da operadora. A seção seguinte tratará das topologias de rede PON disponíveis e explicará as suas características.

3.2 TOPOLOGIAS DE REDES PON

Lage e Oliveira (2006) citam três tipos de topologias que podem ser aplicadas a redes ópticas de acesso: topologia em barra, anel e árvore.

Na topologia em barra (Figura 11), segundo Lage e Oliveira (2006), as ONUs são conectadas a uma OLT através de um segmento de fibra óptica, que faz uso de um *splitter* de derivação de 1:2 (lê-se 1 para 2). Um *splitter* 1:2 possui uma entrada e duas saídas. Nesse caso, a entrada do splitter é alimentada pela fibra óptica vinda da OLT e uma das saídas é utilizada para atender os clientes geograficamente próximos. A outra saída do *splitter* é utilizada para levar a rede até o ponto do próximo *splitter*.

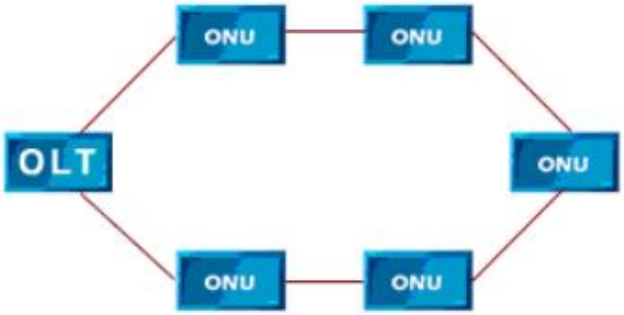
Figura 11 – Representação da topologia em barra



Fonte: LAGE E OLIVEIRA (2006)

A topologia em anel (Figura 12) é aquela onde duas ONU's são conectadas a uma OLT formando então dois segmentos de rede (LAGE E OLIVEIRA, 2006). A próxima ONU de cada segmento deverá então ser conectada à última ONU do segmento e não diretamente à OLT. Dessa forma, a conexão deverá ser feita de ONU para ONU, de modo que os dois segmentos de rede possam se encontrar fazendo com que se forme um anel óptico. Um fator atrativo dessa topologia de rede PON é a capacidade de prover redundância na rede de acesso para os clientes.

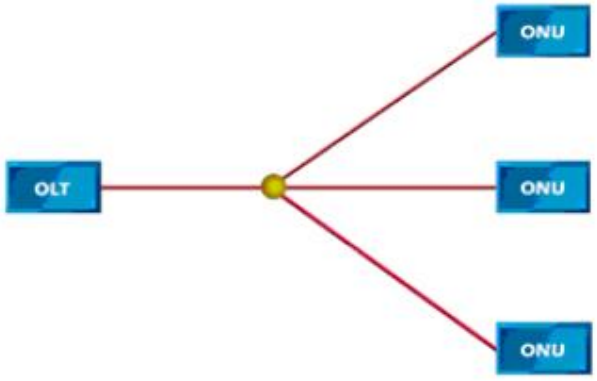
Figura 12 – Representação da topologia em anel



Fonte: LAGE E OLIVEIRA (2006)

Na representação da topologia em árvore (Figura 13), Lage e Oliveira (2006) cita que as ONU's são conectadas a uma OLT através de um único segmento de fibra. Esse segmento de fibra deve ter, no mínimo, um fator de derivação de 1:2, pois dessa forma um *splitter* dividirá a rede em dois sub-segmentos. Dessa forma é possível que, se não houverem ONUs perto para serem atendidas, sejam lançados alguns quilômetros de cabo óptico para a partir de certo ponto passar a fazer a derivação desse sub-segmento criado anteriormente pelo *splitter*.

Figura 13 – Representação da topologia em árvore



Fonte: LAGE E OLIVEIRA (2006)

Independente da topologia de rede PON a ser utilizada, existem diversas tecnologias que podem ser empregadas quando se trabalha com esse tipo de rede. Cada uma possui o seu tipo de aplicação e pode ser utilizada para finalidades específicas nas quais poderá oferecer uma resposta melhor do que as outras tecnologias disponíveis. Na seção seguinte serão citadas as principais tecnologias, bem como suas características e situações de aplicação.

3.3 TECNOLOGIAS UTILIZADAS EM REDES PON

Segundo Coelho (2009), os tipos de tecnologias PON disponíveis são: APON (*Asynchronous Transfer Mode Passive Optical Network*), BPON (*Broadband Passive Optical Network*), EPON (*Ethernet Passive Optical Network*), WDM-PON (*Wavelength Division Multiplexing – Passive Optical Network*) e GPON (*Gigabit Passive Optical Network*).

APON é a tecnologia utilizada em aplicações residenciais utilizando fibra óptica com distância entre a OLT e a ONU limitada a 20 quilômetros. A taxa de transmissão é proveniente da especificação do ATM (*Asynchronous Transfer Mode*), sendo 622 *Mbps (Megabits por segundo)* no sentido *downstream*, e 155 *Mbps* no sentido *upstream*. Como os tráfegos de *downstream* e *upstream* são transportados na mesma fibra óptica, são utilizados dois comprimentos de onda diferentes. O APON tipicamente utiliza os comprimentos de onda de 1490 *nm* para o *downstream* e 1310 *nm* para o *upstream*. Para uma melhor performance, a transmissão é associada ao acesso multiplexado por divisão no tempo (*Time Division Multiple Access* – TDMA), que faz o papel de impedir a colisão de pacotes . Na tecnologia APON os dados são transmitidos em pacotes de até 53 *bytes*, sendo 5 *bytes* de cabeçalho e 48 *bytes* úteis para transportar informação, de acordo com a especificação do protocolo ATM.

BPON é a evolução do APON, permitindo WDM (*Wavelength Division Multiplexing*) e alocação dinâmica de largura de banda para *upstream* (DBA – *Dynamic Bandwidth Allocation*). A tecnologia BPON foi criada indicando que essa tecnologia é capaz de fornecer aos usuários finais mais do que apenas serviços ATM. Através do BPON é possível entregar serviços como, por exemplo, banda larga incluindo acesso *Ethernet* e distribuição de vídeo.

Na tecnologia EPON os dados são transmitidos em pacotes de até 1518 *bytes*, seguindo o protocolo para Ethernet IEEE (*Institute of Electrical and Electronic Engineers*) 802.3. A taxa de transmissão é de 1 *Gbps* em uma distância de até 20 quilômetros. De acordo com Takeuti (2005), o EPON utiliza um mecanismo baseado em TDMA (*Time Division Multiple Access*), chamado MPCP (*Multi-Point Control Protocol*), definido como uma função presente na subcamada de controle MAC (*Medium Access Control*). Por intermédio do protocolo MPCP, a OLT se comunica com as ONUs, numa tecnologia ponto-multiponto. Devido à rede *Ethernet* possuir características do tipo difusão dos sinais (*broadcasting*), os pacotes são enviados pela OLT e extraídos na respectiva ONU, com base no endereçamento do controle do acesso ao meio MAC. Coelho (2009) cita ainda que o EPON foi a primeira tecnologia FTTH a fornecer largura de banda simétrica de 1 *Gbps*. Essa tecnologia tem menor

custo de implementação, pois o processamento de pacotes Ethernet é mais simples e barato do que o processamento de pacotes ATM.

Diferentemente das tecnologias APON, BPON e EPON, a tecnologia WDM-PON utiliza múltiplos comprimentos de onda para aumentar a largura de banda disponível para os usuários finais. O WDM-PON pode oferecer maior largura de banda através de distâncias maiores, pois faz utilização da tecnologia WDM para melhorar o seu alcance. Para enviar sinais da OLT para as ONU's, são utilizados *lasers* com freqüências fixas ou um *laser* com várias frequências.

GPON é a tecnologia estabelecida pela norma ITU-T G.984. O GPON foi uma evolução do BPON e possibilitou o aumento da largura de banda disponível para os assinantes, através do uso de pacotes maiores e de tamanho variável. Essa tecnologia fornece taxas mais elevadas de banda (2,5 *Gbps* no sentido *downstream* e 1,25 *Gbps* no sentido *upstream*), além de permitir a escolha do protocolo entre o ATM e o *Ethernet*.

Apesar da tecnologia GPON disponibilizar uma largura de banda superior às outras tecnologias, Coelho (2009) afirma que as tecnologias BPON, EPON, e GPON tem as mesmas características falando-se em comprimento de onda. Todas essas tecnologias utilizam comprimento de onda de 1490 *nm* no sentido de *downstream* e 1310 *nm* no sentido *upstream*. O comprimento de onda de 1550 *nm* é reservado para serviços opcionais, como por exemplo, a transmissão de sinal analógico através de RF.

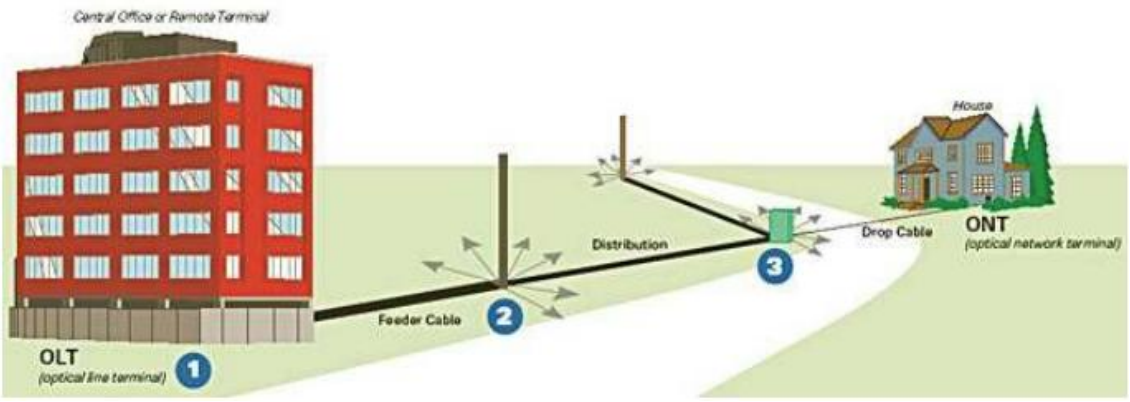
Para Bang et al. (2010), as redes PON de serviços e de atendimento a clientes em redes de acesso proporcionam um custo eficiente e uma infraestrutura flexível. Ele também afirma que as melhores alternativas se falando em tecnologia para montagem de redes de acesso óptico para atendimentos de assinantes hoje, são a Rede Óptica Passiva *Gigabit* (GPON) e a Rede Óptica Passiva *Ethernet* (EPON), pois apresentam várias vantagens em relação às outras tecnologias PON existentes, principalmente se falando em largura de banda que pode ser disponibilizada para acesso. Como a rede PON do tipo *Gigabit* fornece maior largura de banda e é uma tecnologia que está surgindo forte entre os provedores de serviço de acesso à internet, essa tecnologia será tema da próxima seção.

3.4 GPON

Recentemente as operadoras e provedores de acesso à internet vêm investindo fortemente na instalação de redes FTTH onde a tecnologia mais utilizada é a GPON (*Gigabit Passive Optical Network*). Nesse tipo de rede, não existem elementos ativos na rede, exceto o

equipamento que transmite o sinal na fibra óptica, denominado OLT e o equipamento que fica na residência/empresa do assinante, denominado ONU (Figura 14).

Figura 14 - Estrutura de atendimento FTTH com a utilização da tecnologia GPON



Fonte: RAMOS (2009)

A rede GPON é uma rede óptica ponto-multiponto capaz de em uma única fibra compartilhada atender a demanda de diversos assinantes. O sinal óptico é transmitido pela OLT em uma única fibra e através de várias derivações feitas mediante a utilização de *splitters*, possibilita conectar diversas ONU's a uma mesma porta de atendimento da OLT. As topologias utilizadas para construir redes GPON são do tipo em barra e em árvore. Cada ONU recebe um canal óptico independente e possui fluxo de tráfego independente das outras ONU's. A topologia em anel não é comum de ser utilizada em redes de acesso para assinantes, mas apenas em redes *backbone*.

Como o tráfego de *downstream* da tecnologia GPON é transmitido em modo *broadcast*, ou seja, chega a todos os nós da rede, é necessário pensar na segurança das informações transmitidas no meio físico. Para evitar que os usuários tenham acesso à informação dirigida para outros usuários, segundo Coelho (2009), os sinais de *downstream* são criptografados. Os sinais *upstream* são combinados usando protocolos de múltiplos acessos, geralmente TDMA (*Time Division Multiple Access*).

Oliveira (2010) demonstra através da Tabela 1 as características gerais do GPON, descritas no padrão ITU-T G984.1:

Tabela 1 – Características gerais do GPON

Parâmetro	Especificação GPON
Taxa de Dados	*Downstream*=1.244 e 2.488 Gbit/s; *Upstream*= 155 Mbit/s, 622 Mbit/s, 1.244 Mbit/s, 2.488 Gbit/s
Distância	Máximo de 20 quilômetros
Número de Divisões	Máximo 64 divisões
Comprimentos de onda	*Downstream* voz/dados= 1480 a 1550*nm*; *Upstream* voz/dados= 1260 a 1360*nm*; *Downstream* de vídeo= 1550 a 1560*nm*
Segurança	Utilização do AES (*Advanced Encryption Standard*)

Fonte: OLIVEIRA (2010)

Baseado nas características de uma rede GPON, de acordo com Silva (2012), as arquiteturas de rede mais utilizadas são:

- *Fiber to the Curb* (FTTC): o cabo óptico é levado até um armário na calçada ou na rua – *outdoor* – e a partir desse ponto a rede segue com cabos metálicos até chegar ao assinante.
- *Fiber to the Building* (FTTB): a fibra óptica chega até a sala de telecomunicações de um edifício, onde é instalada uma ONU. Um cabo de rede é ligado da ONU para um *switch* que faz a distribuição da rede no prédio. A conexão da rede até os apartamentos ou escritórios do edifício é feita através da utilização de cabeamento estruturado metálico.
- *Fiber to the Apartment* (FTTA): o ponto de terminação da fibra óptica é a ONU dentro do apartamento do assinante.
- *Fiber to the Home* (FTTH): o ponto de terminação da fibra óptica é uma ONU no interior da casa do assinante.

Independente da arquitetura de rede utiliza para construir a rede de acesso para os assinantes, Jay, Neumann e Plückebaum (2013), afirmam que a limitação de velocidade da tecnologia GPON é de 2,5 *Gbps* (*Gigabits* por segundo) de *downstream* e 1,25 *Gbps* de *upstream*, compartilhados por todos os usuários de uma mesma porta da OLT. Padrões futuros irão melhorar a largura de banda máxima do GPON chegando a até quatro vezes mais velocidade se comparado ao padrão atual, tanto nas direções de *downstream*, quanto *upstream*. Também é esperado que se possa dobrar o número de ONU's por porta da OLT, para fazer um aproveitamento adequado de toda a velocidade disponível em cada porta da OLT.

Como no caso da tecnologia GPON a comunicação com cada ONU não é feita através de um caminho único, e sim compartilhado por diversos assinantes, é necessário que ele seja monitorado para a identificação de falhas. Em uma estrutura ponto-a-ponto

tradicional, quando um dos equipamentos ativos da conexão óptica ficar inacessível, é sinal de que o meio físico, no caso a fibra óptica, ou algum dos equipamentos ativos (OLT ou ONU) está com problema. Em uma estrutura ponto-multiponto que trabalha em uma topologia PON do tipo barra, por exemplo, pode acontecer o rompimento de um cabo óptico secundário que é nada mais que uma derivação do cabo principal feita através de um *splitter*. Identificar e até mesmo prevenir esse tipo de problema é mais complexo em uma estrutura ponto-multiponto do que em uma estrutura ponto-a-ponto. Devido a esses motivos, a próxima seção tratará dos problemas e dificuldades encontradas para fazer esse tipo de monitoramento.

3.5 CONSIDERAÇÕES DO CAPÍTULO

A utilização da fibra óptica para entregar serviços como banda larga, telefonia e TV através da internet está se tornando mais frequente no dia-a-dia das pessoas e já é uma realidade. Para possibilitar a entrega desses serviços, as topologias possíveis de serem utilizadas na rede de atendimento de acesso são a topologia em barra, em anel e em árvore.

Existem dois tipos de redes ópticas, sendo elas as redes ópticas ativas e as passivas, sendo estudada neste trabalho apenas a rede passiva. As redes ópticas passivas possibilitam o emprego de diversas tecnologias, como a GPON, APON, BPON, WDM-PON e EPON. Dentre todas essas tecnologias, a GPON se destaca por possibilitar entregar mais velocidade ao assinante utilizando o mesmo meio físico que as outras tecnologias.

Como a tecnologia GPON funciona em uma arquitetura do tipo ponto-multiponto e envolve o tráfego de grande quantidade de dados e informações, é essencial que haja um monitoramento eficiente dos equipamentos ativos da rede, no caso a OLT e as ONUs instaladas na casa ou na empresa dos assinantes. Para fazer o monitoramento, é fundamental que sejam definidos os parâmetros que serão monitorados. O capítulo seguinte explicará quais são os principais parâmetros possíveis de serem monitorados em redes TCP/IP.

4 MEDIÇÕES EM REDES ÓPTICAS

Conhecer as características e qualidade de uma rede é possível e essencial para que se possa estabelecer parâmetros a serem monitorados. Após o estabelecimento dos parâmetros, dados são coletados, armazenados, comparados e analisados para determinar o desempenho de uma rede e a qualidade dos serviços prestados, tornando possível a identificação de situações anormais, como por exemplo, congestionamento, diminuição de desempenho ou falhas (FERREIRA, 2005). A medição fim a fim de parâmetros pré-estabelecidos é a única forma possível de determinar e assegurar a qualidade de uma rede contendo fluxo de tráfego de dados.

Os dados coletados são indispensáveis para atividades de pesquisa e planejamento, assim como para a administração e manutenção da infra-estrutura operacional existente. É de suma importância que a coleta de dados não interfira no desempenho da rede, não gerando tráfegos desnecessários e não interferindo assim na estabilidade da rede. Também é preciso assegurar que a coleta de dados não viole os direitos de privacidade e segurança do assinante (FERREIRA, 2005).

As atividades de coleta de dados devem ser planejadas com o fim de atingir as metas operacionais com o menor impacto possível na rede de fluxo de tráfego de dados. Ou seja, as informações medidas e as metodologias utilizadas devem ser avaliadas cuidadosamente, evitando degradação na rede através da utilização de recursos desnecessários.

4.1 OBTENÇÃO DE INDICADORES DE DESEMPENHO

A obtenção de dados de desempenho pode ser feita através da consulta individual dos elementos de rede para aquisição de informações ou através da consulta a um nó central que armazena as informações dos elementos da rede. Quando as consultas de informações são muito constantes, os sistemas de gerenciamento calculam médias a partir dos dados coletados em um intervalo de tempo, geralmente de minuto em minuto ou de cinco em cinco minutos.

Existem dois métodos de medição que são usualmente utilizados: a medição passiva e a medição ativa.

4.1.1 Medição passiva

Essa técnica de medição parte do princípio de que não é necessário gerar tráfego na rede para realizar a coleta de dados da rede utilizados para fazer a sua medição. Desta forma, é medido o tráfego real de uma rede, através apenas da observação do tráfego normal da mesma.

Para possibilitar a utilização da técnica de medição passiva, é necessária a montagem de uma infra-estrutura de *hardware* e *software* específica para desempenhar essa função. No escopo deste tipo de medição, o número de pontos de medição deve ser considerado, pois é determinante para definir quais informações devem ser extraídas da rede, bem como para dimensionar o *hardware* e definir um *software* que possua o poder computacional adequado.

Neste tipo de medição os equipamentos são periodicamente acessados através de um *polling*. *Polling* é uma rotina de captura de dados feita através da estação de gerenciamento de dados. Os dados coletados pelo *polling* são transferidos para uma base de dados centralizada após cada coleta de informações realizada. Esses dados são então utilizados para avaliar o desempenho e o estado da rede (BASTOS, 2008).

4.1.2 Medição ativa

Ao contrário da técnica de medição passiva, a medição ativa, regulamentada pela RFC1262 (*http://tools.ietf.org/html/rfc1262*), possui o propósito de enviar pacotes de teste através da rede para monitorar, por exemplo, o tempo de resposta necessário para enviar um pacote a um nó da rede e o tempo necessário para recebê-lo de volta. Com a utilização dos dados obtidos através dessa técnica de medição, é possível mensurar gargalos na rede, atraso em uma via, atraso em vias de ida e volta, perda de pacotes e variação no atraso (*jitter*). Essa técnica de medição precisa obrigatoriamente injetar tráfego na rede para poder fazer as suas medições, não sendo apropriada, por exemplo, para medir o tráfego real da rede.

A necessidade de utilização da capacidade de processamento dos equipamentos de rede e a concorrência com o tráfego real da rede podem ser vistos como características desfavoráveis dessa técnica de medição (GUIMARÃES, 2007). Outro problema relacionado à utilização dessa técnica é a necessidade de sincronização precisa de tempo nos pontos envolvidos no processo de medição, para evitar cálculos errados de tempo de resposta, por exemplo. Para sanar esse problema torna-se necessário o investimento em fontes confiáveis de tempo.

Como exemplos de técnicas de medições ativas empregadas em sistemas operacionais pode-se citar o emprego dos utilitários *Ping* e *Traceroute*, os quais utilizam pacotes ICMP (*Internet Control Message Protocol*), para determinar atraso de ida e volta e topologia de rota da rede (GUIMARÃES, 2007).

4.2 PRINCIPAIS MÉTRICAS DE DESEMPENHO

Uma métrica é uma unidade de medida relacionada com a quantidade medida de alguma propriedade de um componente em questão. Para medir o desempenho de uma rede, podem ser utilizadas diversas métricas, independente da técnica de medição utilizada. A métrica a ser utilizada depende do recurso a ser monitorado e medido. Assim sendo, essa seção descreve as principais métricas utilizadas para medir e monitorar o desempenho de redes.

4.2.1 Latência

A medição de latência retorna a informação do tempo necessário que um pacote leva para ir de um lado do enlace até o outro lado. Bastos (2008) cita os principais componentes que devem ser considerados para fazer a medição da latência de uma rede:

- Tempo de transporte: é o tempo que o pacote leva para ser transmitido através de todos os nós de processamento que compõem o caminho da rede;

- Tempo de enfileiramento: dependendo das políticas de QoS adotadas pelos roteadores do caminho, alguns tipos de pacotes mais importantes como VOIP, por exemplo, tem prioridade sobre pacotes menos importantes como o ICMP, por exemplo;

- Tempo de envio/transferência: é o tempo de processamento necessário empregado pelo roteador para fazer o roteamento dos pacotes recebidos na sua *interface* de entrada;

- Tempo de resposta do servidor: é o tempo necessário para o lado remoto receber a mensagem e enviar uma mensagem de resposta.

As medições de rede através da latência são afetadas por todos os indicadores mencionados. A medição da latência pode ser prejudicada quando roteadores estiverem com carga alta de processamento, se o caminho estiver congestionado devido a gargalos de largura de banda e também dependendo do tipo de pacotes que estão passando pelos roteadores que priorizam determinados tipos de tráfego.

Para acompanhar as variações na latência é uma prática comum armazenar as informações em gráficos a fim de possibilitar consultas futuras. Em redes de acesso doméstico que fazem compartilhamento de banda para acesso, os gráficos normalmente apresentam um aumento na latência em períodos noturnos, que é quando o fluxo de tráfego da rede aumenta, a largura de banda ociosa é menor e os roteadores demoram mais tempo para processar os pacotes. Já em *backbones* de universidades ou em redes de acesso dedicado, a variação na latência não ocorre de forma acentuada de acordo com horários do dia. O que pode acontecer nesse tipo de *backbone* causando variação e aumento na latência é a ocorrência de problemas técnicos ou problemas em equipamentos que fazem parte da rede óptica.

4.2.2 Perda de pacotes

A perda de pacotes é o percentual ou número de pacotes perdidos em relação ao número de pacotes enviados durante um intervalo de tempo. A taxa de perdas de pacotes pode variar da mesma forma que a latência, ou seja, quando a largura de banda ociosa diminuir e consequentemente os roteadores aumentam o tempo de processamento de pacotes. Dependendo da taxa de perdas de pacotes, uma rede pode tornar-se praticamente inviável de ser utilizada (BASTOS, 2008).

Mesmo em redes com taxas de perda de pacotes acima do normal, pode ser possível utilizar aplicações que toleram a perda de pacotes sem causar prejuízos ao seu desempenho. Quando utilizado o protocolo TCP (*Transmission Control Protocol*), o próprio protocolo consegue tratar a perda de pacotes através da identificação da perda e reenvio de um novo pacote para compensar o pacote perdido.

4.2.3 Vazão

A medida da vazão de uma rede é obtida considerando a taxa de informação que chega e que é entregue por um nodo da rede por unidade de tempo. Geralmente essa métrica se refere à taxa de transferência total de *bits* que entra ou sai da rede dividida por uma unidade de tempo. Segundo Motoyama (2006), a vazão máxima de uma rede é calculada considerando-se apenas os pacotes sem erro de transmissão. Vazão máxima é o mesmo que a capacidade máxima do canal de comunicação, conforme a fórmula a seguir:

$$\text{Vazão} = \frac{\text{Número médio de pacotes bem sucedidos (sem erro)}}{\text{Tempo médio de transmissão de um pacote}}$$

Fonte: MOTOYAMA (2006)

A escolha do intervalo de tempo para fazer o cálculo de vazão de um canal deve ser feita com cautela porque intervalos de tempo grandes tendem a incorporar a captura de rajadas de tráfego que não relatam a vazão real do canal. Intervalos de tempo curtos também podem medir rajadas fazendo com que o cálculo de vazão fique muito acima do real (BASTOS, 2008).

4.2.4 Capacidade

A capacidade de um enlace é a medição da vazão máxima que ele pode prover para uma aplicação. A medição da capacidade de um enlace é o mesmo que medir a largura de banda. De acordo com Battisti (2007), a capacidade, ou largura de banda, pode ser avaliada de diferentes formas, como:

- Largura de banda de contenção: é a taxa máxima de transmissão capaz de ser alcançada em um meio sem tráfego de dados;

- Largura de banda utilizada: é a soma de todos os tráfegos presentes no enlace e corresponde ao tráfego real num dado momento;

- Largura de banda disponível: é calculada considerando-se a vazão máxima do enlace menos a largura de banda utilizada, ou seja, a capacidade total de um canal de comunicação descontando o tráfego que já está sendo utilizado num dado momento;

- Largura de banda alcançável: é a taxa de transmissão entre dois pontos considerando variáveis inseridas no meio físico como o protocolo TCP, velocidade de processamento dos pacotes pelo *hardware* e pelo *software* de roteadores, sistema operacional e mecanismos de QoS implementados para aplicações ou serviços específicos.

4.2.5 Intensidade do sinal

A medição da intensidade do sinal é largamente empregada em monitoramentos de redes. Em casos de certificações de redes com cabeamento estruturado, é utilizado um aparelho que faz a medição de intensidade e qualidade do sinal de uma extremidade a outra do

cabo de rede. Em enlaces que utilizam a tecnologia *wireless*, que assim como a rede com cabeamento estruturado, é suscetível a interferências, a intensidade do nível de sinal pode variar durante determinados períodos de tempo. A variação climática, por exemplo, pode causar mudanças na intensidade do sinal de um enlace. Em enlaces ópticos a variação da intensidade do sinal caracteriza um problema físico de rede, visto que a intensidade do sinal óptico não sofre do problema de atenuação por interferência externa.

A métrica de intensidade de sinal deve ser parametrizada considerando o nível de sinal mínimo necessário para o funcionamento de um enlace. O nível de sinal recebido por um dispositivo deve ser superior ao nível mínimo necessário. A diferença entre o sinal mínimo e o sinal recebido resulta na margem para atenuação. Uma vez ultrapassada a margem de atenuação do sinal, a perda constatada ocasionará quedas de performance no canal de comunicação entre os dois dispositivos inseridos no mesmo e dependendo do caso até mesmo a interrupção da comunicação entre os dispositivos.

4.3 CONSIDERAÇÕES DO CAPÍTULO

Através de ambas as técnicas de medição, tanto na ativa quanto na passiva, é possível realizar o monitoramento de recursos de uma rede. Dependendo de qual característica da rede deve ser monitorada, uma técnica pode desempenhar a função específica de uma maneira mais satisfatória do que a outra. A análise do tipo de dado a ser obtido é fundamental para a definição da técnica de medição a ser empregada.

Através da utilização das técnicas de monitoramento de rede, é possível definir métricas a serem monitoradas para que se chegue a indicadores que possibilitem avaliar o estado e desempenho de uma rede.

O intuito deste trabalho é identificar atenuações e perdas de sinal em *links* de fibra óptica em estruturas do tipo FTTH. As métricas utilizadas para fazer as medições serão a latência, perda de pacotes, vazão, capacidade do canal de comunicação e a intensidade do sinal. Será necessário que seja monitorado essencialmente o nível de sinal recebido pela ONU instalada na casa do assinante. Para identificar atenuações no sinal óptico, será empregada a técnica de medição passiva. Mesmo havendo uma atenuação de sinal em uma rede do tipo FTTH, caso essa não ultrapasse o limite mínimo de sinal estabelecido, isso não quer dizer que a rede esteja com desempenho reduzido. Para monitorar as medições de latência, perda de pacotes, vazão e capacidade será utilizada a técnica de medição ativa, devido à necessidade de monitorar recursos e também o estado da rede em diferentes períodos do dia. Para fazer esse

monitoramento serão enviados pacotes de teste através da rede até o equipamento para o qual se deseja fazer a medição. Os resultados obtidos em períodos diferentes podem também ser diferentes, caracterizando problemas como congestionamentos de rede, por exemplo.

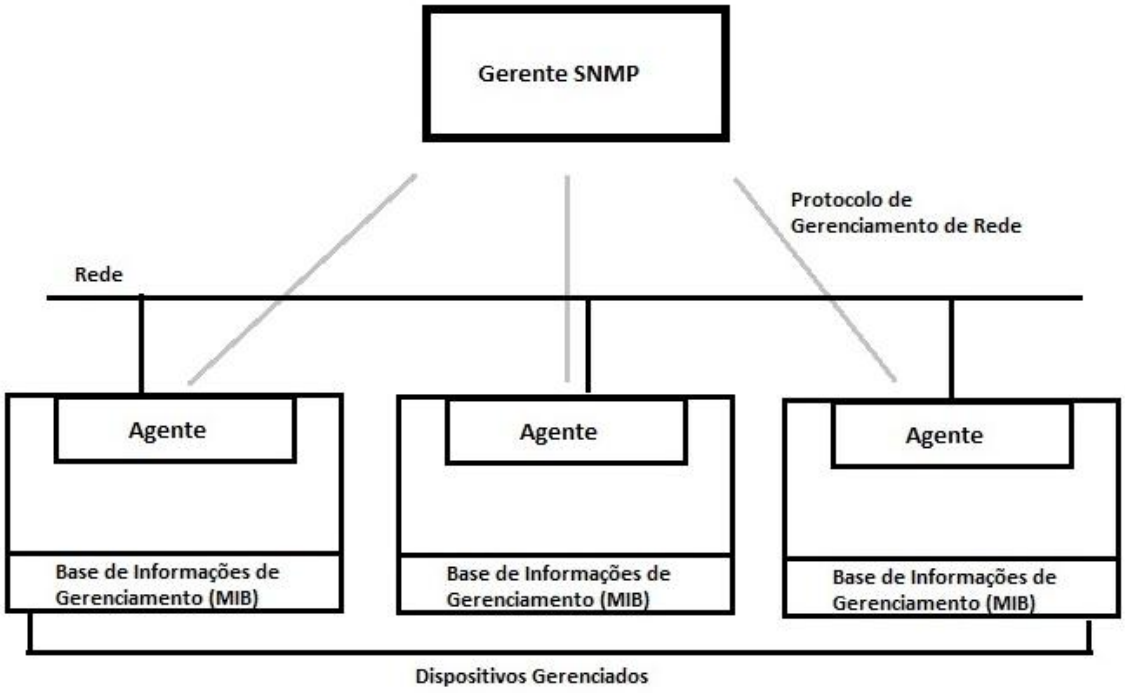
Para a aplicação das técnicas de medição a fim de monitorar características e desempenho de dispositivos de rede, torna-se necessária a utilização de um *software* capaz de interpretar um protocolo e de prover a comunicação entre dispositivos de rede. O próximo capítulo trará o estudo sobre arquiteturas de gerenciamento TCP/IP e os seus componentes.

5 ARQUITETURA DE GERENCIAMENTO TCP/IP

Com a evolução das redes, número de equipamentos utilizados, amplitude geográfica de distribuição e o elevado número de usuários conectados, o gerenciamento de redes se tornou algo indispensável para garantir o bom funcionamento da rede. O gerenciamento de redes através da arquitetura de gerenciamento TCP/IP, também conhecida como Arquitetura de Gerenciamento Internet, é feito através do protocolo SNMP, que foi adotado como o protocolo padrão para a gerência de redes TCP/IP.

A arquitetura de gerenciamento TCP/IP possui quatro componentes básicos: gerentes, agentes, SNMP e MIB (*Management Information Base*). A Figura 15 ilustra o funcionamento dessa arquitetura de gerenciamento.

Figura 15 – Funcionamento da Arquitetura de Gerenciamento TCP/IP



Fonte: Elaborado pelo autor.

Além do gerente, agente, SNMP e da MIB, existe também a SMI (*Structure of Management Information*). Segundo Esteves (2013), a SMI é um conjunto de documentos que definem uma série de regras para a construção de estruturas de gerenciamento, como por exemplo, as sintaxes permitidas para uso e a lista de objetos que integra cada equipamento gerenciado. As seções a seguir explicarão todos os componentes envolvidos em uma arquitetura de gerenciamento de rede TCP/IP.

5.1 AGENTE

O agente é um processo executado em um elemento de rede, como por exemplo, um modem, máquina, servidor ou qualquer dispositivo que possa ser gerenciado.

Segundo Paiva (2010), o agente é responsável por coletar e armazenar as informações de um dispositivo a ser monitorado na sua MIB local, bem como fornecê-las para o gerente SNMP quando solicitado. Também é papel do agente manter as informações armazenadas na MIB sempre atualizadas, a fim de evitar inconsistências na coleta de dados. Outra função do agente é enviar informações para o gerente SNMP através de *traps*. *Traps* são notificações pré-configuradas que são enviadas pelo agente para o gerente informando alguma anormalidade.

5.2 GERENTE

O gerente é um processo servidor que executa um programa responsável por se conectar aos dispositivos a serem monitorados para obter as informações desejadas.

Dias e Junior (2002) afirmam que o gerente SNMP é o responsável pelo monitoramento, pela geração de relatórios e gráficos, e pela tomada de decisões em caso de ocorrência de falhas.

O gerente SNMP deve ter a capacidade de interpretar as informações coletadas nos agentes. Como o protocolo conta com mais de uma versão, os agentes podem executar versões do protocolo que diferem de dispositivo para dispositivo. Cabe ao gerente de redes da organização padronizar a versão do protocolo utilizada nos dispositivos gerenciados ou então utilizar um *software* que seja capaz de interpretar todas as versões.

5.3 SMI

De acordo com Kurose e Ross (2006), a SMI é a linguagem utilizada para definir as informações de gerenciamento presentes em uma unidade gerenciada de rede. Essa linguagem é necessária para garantir que a sintaxe e o modo de organização dos dados de gerenciamento sejam padronizados e bem definidos. A SMI tem a função de especificar regras para definir e identificar os tipos e a codificação dos objetos. Ela não é responsável por nomear e nem determinar a associação entre um objeto e os seus valores.

A SMI define três atributos para manipular um objeto: nome, tipo de dados e método de codificação.

O nome definido pela SMI deve ser único para cada objeto gerenciado. A nomenclatura é baseada em uma estrutura de árvore e utiliza um identificador de objeto hierárquico.

Para definir suas variáveis, a SMI utiliza a ASN.1 (*Abstract Syntax Notation One*). A Tabela 2 demonstra os 11 tipos de dados básicos utilizados pela SMI e definidos na RFC2578 (*http://tools.ietf.org/html/rfc2578*).

Tabela 2 – Tipos de dados utilizados pela SMI

Tipo	Tamanho	Descrição
Integer	4 *bytes*	Valor entre -2^{31} e 2^{31} -1
Integer32	4 *bytes*	Mesmo que integer
Unsigned32	4 *bytes*	Valor sem sinal entre 0 e 2^{32} -1
Octet String	Variável	String até 65.535 *bytes*
Object Identifier	Variável	Identificador de objeto
IP Address	4 *bytes*	Endereço ip, formado por 4 valores inteiros
Counter32	4 *bytes*	Valor inteiro que pode ser incrementado de 0 a 2^{32}; quando chega ao valor máximo é zerado
Counter64	8 *bytes*	Contador de 64 *bits*
Gauge32	4 *bytes*	Mesmo que Counter32, mas não é zerado automaticamente
TimeTicks	4 *bytes*	Tempo, medido em centésimos de segundo, transcorrido a partir de algum evento
Bits		String de bits
Opaque	Variável	String não interpretada

Fonte: KUROSE e ROSS (2006)

5.4 MIB

Kurose e Ross (2006) definem a MIB como sendo um banco virtual de informações armazenadas a respeito de um objeto gerenciado, informações estas, que coletivamente refletem o estado atual do objeto gerenciado.

Para Paiva (2010), a MIB é definida como a base de dados acessada pelo protocolo SNMP para obter todas as estatísticas e informações possíveis dos equipamentos monitorados.

Esteves (2013) afirma que a MIB é formada por uma coleção de objetos, que são a abstração dos recursos de um sistema. Os objetos disponíveis para acesso podem ser configurados com permissão de leitura e escrita ou então somente leitura, dependendo do nível de permissão concedido ao gerente. A permissão de leitura permite ao agente apenas ler dados da MIB que demonstram o estado atual de um equipamento. A permissão de leitura e escrita por sua vez, permite além de ler os dados da MIB, também enviar comandos para que o agente realize alterações no objeto gerenciado em tempo real, possibilitando assim uma nova leitura do estado já atualizado.

Com o aumento do número de objetos e de equipamentos que possibilitam serem gerenciados, foi criado mais do que um tipo de MIB. Esteves (2013) cita três tipos de MIB: a MIB II, MIB experimental e MIB privada. A MIB II foi especificada na RFC1213 (*http://tools.ietf.org/html/rfc1213*), como sendo evolução da MIB I. A MIB II fornece informações de gerenciamento sobre um determinado equipamento, possibilitando dessa forma obter estatísticas como, por exemplo, número de pacotes, *bytes* transmitidos por cada uma das suas *interfaces*, total de pacotes enviados e recebidos, número de pacotes com falha, estado das *interfaces*, etc.

Dias e Junior (2002) afirmam que objetos que estão em fase de desenvolvimento ou teste integram a MIB experimental, que possui geralmente características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos utilizados.

A MIB privada é o tipo de MIB onde objetos fornecem estatísticas e informações específicas sobre os equipamentos gerenciados, como por exemplo, características de configuração, colisões de pacotes, etc. Contessa e Polina (2010) afirmam que a MIB privada pode ser baseada na MIB padrão ou totalmente customizada pelo fabricante do equipamento para o qual foi desenvolvida a MIB. Através desse tipo de MIB é possível até mesmo desabilitar ou reinicializar *interfaces* do equipamento gerenciado. Com a utilização de MIB privada, obtêm-se um gerenciamento mais específico, onde a qualidade das informações é superior à qualidade das informações da MIB padrão.

5.4.1 Estrutura da MIB

As regras de construção da MIB são descritas na SMI (*Structure of Management Information*). Esta descrição deve considerar a estrutura e as restrições do equipamento no qual a MIB é implementada. Para cada objeto são definidas as seguintes instâncias:

- *Object Name*: nome do objeto composto por uma *string* de texto curto;

- *Object Identifier* (OID): identificador único do objeto. É formado por números separados por pontos. Exemplo: 1.4.5.6.14988.1.34.4;

- *Syntax*: sintaxe do objeto. Descreve o formato ou o valor da informação. Pode ser de um tipo simples como inteiro, OID, *string*; ou pode ser uma sintaxe de aplicação como, por exemplo, um contador, uma medida específica ou um intervalo de tempo;

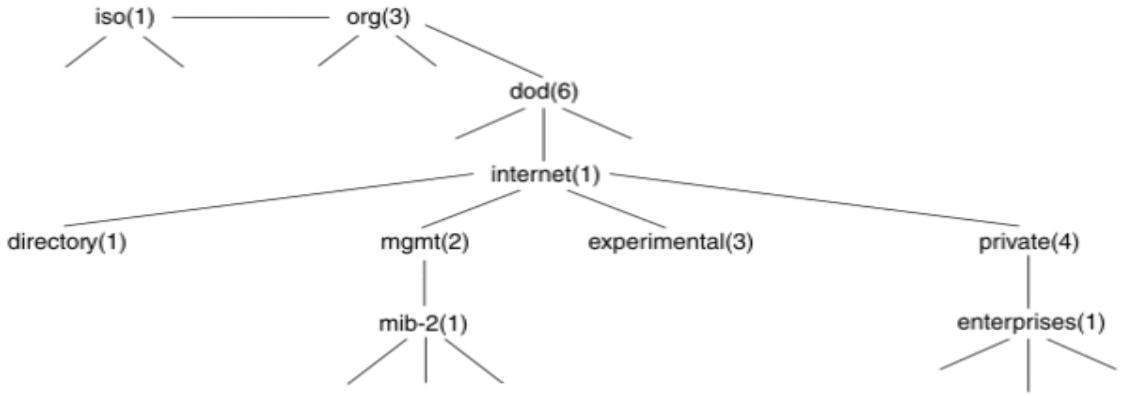
- Definição: descrição textual do que é o objeto em questão;

- Acesso: tipo de permissão de acesso concedida. Pode ser somente leitura, leitura e escrita ou sem acesso algum.

A Figura 16 representa a estrutura lógica da MIB. Sob o nó .1 fica o nó .1.3, chamado *org*, que pode ser utilizado por outras instituições. Abaixo de *org* fica o *dod* (.1.3.6), pertencente ao departamento de defesa dos EUA (Estados Unidos da América). O departamento de defesa dos EUA, por sua vez, alocou um nó para a comunidade internet (.1.3.6.1), que é administrado pela organização IAB (*International Activities Board*). Abaixo deste estão os nós *directory* (.1.3.6.1.1), *management* (.1.3.6.1.2), *experimental* (.1.3.6.1.3) e *private* (.1.3.6.1.4).

Sob o *directory* estão as informações sobre o serviço de diretórios OSI (*Open Systems Interconnection*). Sob a estrutura *management* estão as informações de gerenciamento, e sob esta está o nó responsável pela MIB II (.1.3.6.1.2.1). Sob o nó *experimental* estão os nós das MIB's experimentais. Sob o *private* fica o nó *enterprises* (.1.3.6.1.4.1) e sob este ficam os nós das indústrias de equipamentos gerenciados na sua própria MIB privada. Por exemplo, o nó da IBM está na estrutura (.1.3.6.1.4.1.2) e o da Cisco na estrutura (.1.3.6.1.4.1.9).

Figura 16 – Estrutura lógica da MIB



Fonte: http://wiki.sj.ifsc.edu.br/wiki/index.php/GER-2010-1 acesso em 06/05/2014

5.4.2 MIB II

Abaixo da sub-árvore MIB II estão os objetos utilizados para obter informações específicas dos equipamentos da rede. A Figura 17, demonstra os dez principais grupos de informações presentes na MIB II.

Figura 17 – Grupos de informações da MIB II

Grupo	Informação
system (1)	informações básicas do sistema
interfaces (2)	interfaces de rede
at (3)	tradução de endereços
ip (4)	protocolo IP
icmp (5)	protocolo ICMP
tcp (6)	protocolo TCP
udp (7)	protocolo UDP
egp (8)	protocolo EGP
transmission (10)	meios de transmissão
snmp (11)	protocolo SNMP

Fonte: Esteves (2013)

Esteves (2013) define os grupos de objetos da seguinte forma:

a) Sys: informações gerais sobre o sistema como nome e localização;
b) If: informações sobre as *interfaces* do dispositivo, incluindo o nome ou número da *interface*, endereço físico e IP;
c) At: informações sobre a tabela ARP (*Address Resolution Protocol*);
d) IP: informações relacionadas ao protocolo internet, como a tabela de roteamento do dispositivo;
e) ICMP: informações relacionadas ao ICMP, como o número de pacotes enviados e recebidos;
f) TCP: informações relacionadas ao TCP, como a tabela de conexões;
g) UDP (*User Datagram Protocol*): informações relacionadas ao UDP, como o número de pacotes enviados e recebidos;
h) EGP (*Exterior Gateway Protocol*): rastreia diversos dados estatísticos sobre o EGP;
i) *Transmission*: reservado para MIBs específicas de mídia;
j) SNMP: informações relacionadas ao SNMP.

Dentro de cada um dos dez grupos definidos pela MIB II, existem variáveis que apresentam informações diferentes referentes ao seu grupo específico. Por exemplo, Kurose e Ross (2006), citam a subdivisão do grupo Sys:

a) *sysDescr*: completa descrição do sistema (versão, *hardware*, sistema operacional);

b) *sysObjectID*: objeto para identificação do vendedor;
c) *sysUpTime*: tempo desde a última reinicialização;
d) *sysContact*: nome da pessoa de contato;
e) *sysName*: nome do equipamento gerenciado;
f) *sysLocation*: localização física do equipamento;
g) *sysServices*: serviços oferecidos pelo dispositivo.

Na sub-árvore MIB II, cada objeto contém um determinado tipo de dado. De acordo com a RFC2578**,** os tipos de dados considerados pelo SMI são:

a) *Integer*: normalmente um número inteiro de 32*bits*. O valor "0" não pode ser utilizado para este tipo de dado, senão o objeto não será listado na MIB;
b) *String*: utilizada para especificar textos e deve conter zero ou mais *bytes*;
c) *Counter*: é um número de 32 *bits*, geralmente utilizado para contabilizar quaisquer totais de tráfego de um equipamento, como por exemplo, o total de pacotes recebidos e enviados. Esse tipo de dado é crescente, nunca sofrendo decréscimo;
d) *Object Identifier* (OID): *string* formada por números separados por pontos. Exemplo: 1.2.3.6.14988.2.3.6.6.3;
e) *Null*: representa um objeto que não está sendo utilizado pelo protocolo SNMP;
f) *Sequence*: utilizado para definir listas de dados. Pode conter zero ou mais tipos;
g) *Sequence Of*: utilizado para especificar objetos gerenciados formados por dados do tipo *Sequence*;
h) *IpAddress*: representa endereços de rede do padrão IPv4 (*Internet Protocol Version 4*). O documento SMI não processa endereços IP segundo o padrão IPv6 (*Internet Protocol Version 6*), que conta com 128 *bits*. Na próxima versão do SMI, o SMING (*Structure of Management Information Next Generation*) deverá estar previsto o tratamento de endereçamento IPv6;
i) *Network Address*: possui a mesma função do *IpAddress*, podendo representar tipos de endereços de rede diferentes do IPv4;
j) *Gauge*: mesmo tipo de dado que o *Counter*, porém com a diferença de poder aumentar e diminuir seu valor, enquanto o C*ounter* pode apenas aumentar seu valor;
k) *TimeTicks*: dado numérico de tamanho igual aos dados *Counter* e *Gauge*, geralmente utilizado para medir algum intervalo ou período de tempo, como por exemplo, o tempo que o equipamento está ligado desde a última reinicialização;
l) *Opaque*: habilita o armazenamento de codificações do documento ASN.1 em objetos do tipo *String*;

m) *Unsigned32*: exclusivo da versão SMIv2. É utilizado para representar valores numéricos de 0 até 2^{32} -1;
n) *Counter64*: exclusivo da versão SMIv2. Apresenta o mesmo princípio de funcionamento que o *Counter32*, porém com 64 *bits* de tamanho, variando de 0 até 2^{64} – 1. Geralmente é utilizado quando números de 32 *bits* não possibilitam representar valores muito expressivos, que ultrapassem os 32 *bits* de tamanho limite. Nesses casos é utilizado o *Counter64*, que possibilita representar valores com até 64 *bits*;
o) *Bits*: exclusivo da versão SMIv2. Listagem de *bits* não negativos de um objeto que está sendo gerenciado.

5.5 SNMP

No início da década de 80, foi dado início ao desenvolvimento de um protocolo de gerenciamento de redes através de uma organização chamada IETF (*Internet Engineering Task Force*). Este protocolo foi então chamado de SNMP, e tinha propósito de gerenciar os dispositivos de uma rede de computadores de forma simples. Segundo Esteves (2013), antes da utilização do SNMP, o protocolo utilizado era o SGMP (*Simple Gateway Management Protocol*). A principal limitação do SGMP era o fato de que ele havia sido desenvolvido para gerenciar apenas roteadores, o que fazia com que a sua utilização ficasse limitada. O protocolo SNMP, diferentemente do SGMP, tem a capacidade de gerenciar sistemas operacionais, periféricos e demais dispositivos capazes de interpretar o novo protocolo. O SNMP começou a ser utilizado efetivamente na década de 90, através do surgimento da RFC1157 (*http://tools.ietf.org/html/rfc1157*).

Juntamente com o aumento da complexidade da gerência de redes, o número de equipamentos que possibilitam o gerenciamento por SNMP também tende a aumentar cada vez mais, possibilitando assim o monitoramento de grande parte dos recursos dos equipamentos de uma rede (CONTESSA E POLINA, 2010).

Com a evolução do protocolo, foram adicionadas novas funcionalidades que possibilitaram monitorar cada vez mais recursos dos equipamentos e com maior e mais segurança. De acordo com Esteves (2013), atualmente existem três versões do protocolo SNMP disponíveis para utilização: SNMPv1, SNMPv2c e SNMPv3. Na seqüência serão explicadas as características de cada uma delas.

5.5.1 SNMP versão 1

A primeira versão do protocolo SNMP foi a SNMPv1. Essa é a versão que passou a ser utilizada na década de 90, após a publicação da RFC1157. Santos (2006) afirma que a segurança dessa versão do protocolo baseia-se no conceito de comunidades (*communitys*), que são capazes de estabelecer uma confiabilidade na conexão entre gerentes e agentes. Dependendo da situação, através da *community* é possível ler e/ou alterar informações da MIB no agente.

A vulnerabilidade da utilização de *communitys* está no fato delas serem enviadas sem criptografia. Para reduzir o risco de captura da informação da *community* por indivíduos não autorizados, é indicada a utilização de *firewalls* para restringir a comunicação SNMP entre dispositivos, VPNs (*Virtual Private Networks*) para garantir a criptografia do tráfego ou então alterar as *communitys* regularmente. Através da c*ommunity* é concedida permissão de leitura para acessar as estatísticas desejadas, ou então permissão de leitura e escrita, na qual é possível enviar comandos para o equipamento que está sendo monitorado.

O SNMPv1 era limitado nas questões que diziam respeito a segurança e quantidade de comandos possíveis de serem recebidos e enviados pelo protocolo.

5.5.2 SNMP versão 2

A segunda versão do protocolo, a SNMPv2, também conhecida como SNMPv2c, assim como a versão SNMPv1, também foi desenvolvida pelo IETF. De acordo com Esteves (2013), como principais melhorias que essa versão do protocolo trouxe em relação à versão SNMPv1 pode-se citar melhorias de segurança na autenticação das *communitys*, mais especificamente quando ocorre uma conexão entre gerente e agente. Na autenticação por *communitys* existiam diversas falhas de segurança que faziam com que fosse possível extrair informações de um dado equipamento apenas sabendo o nome da *community*. A partir dessa mudança surgiu a letra “c” no final do nome desta versão, justificando assim a nomenclatura SNMPv2c. Outra melhoria que pode ser citada é a criação das mensagens *InformRequest* e *GetBulkRequest*, que possibilitam a comunicação entre gerentes para prover a gerência descentralizada da rede e também a otimização da recuperação de informações de equipamentos que estão sendo monitorados, quando necessário.

5.5.3 SNMP versão 3

A versão SNMPv3 é fortemente focada em segurança, quando comparada às versões anteriores do protocolo. Uma melhoria adicionada a essa versão foi a possibilidade de autenticação individual para cada equipamento monitorado, mediante utilização de usuário e senha. Outra melhoria da terceira versão do SNMP é o estabelecimento de uma comunicação privativa entre os agentes e o gerente do monitoramento.

De acordo com Esteves (2013), o principal objetivo de pesquisas e desenvolvimento de plataformas ou sistemas de gerenciamento tem se concentrado na necessidade do máximo desempenho no funcionamento da rede, melhorando o uso dos elementos de gerência e monitoramento da rede. Como se tornou o protocolo padrão para o gerenciamento de redes, o SNMP tem sido constantemente melhorado e otimizado para obter mais desempenho gerando o mínimo de processamento nos equipamentos e também baixo tráfego na rede.

5.5.4 Operações do protocolo SNMP

Dias e Junior (2002) citam como operações básicas do SNMP, os comandos *GET* e *SET*, e suas derivações que são o *GET-NEXT* e *TRAP*.

A operação *SET* é utilizada para fazer uma alteração de valor em uma variável. Para fazer essa alteração o gerente solicita ao agente que ele faça a mudança do valor de uma variável.

A operação *GET* é utilizada para fazer a leitura de uma variável da MIB, sendo que o gerente solicita ao agente que ele leia e retorne o valor da variável solicitada.

A operação *GET-NEXT* é utilizada para fazer a leitura da próxima variável, ou seja, a variável que vem depois da variável especificada. Dias e Junior (2002) afirmam que essa operação também é utilizada para buscar valores em tabelas de tamanho desconhecido.

A operação *TRAP* é utilizada para comunicar ao gerente a ocorrência de um evento. O envio de *TRAP* SNMP deve ser previamente configurado. Dias e Junior (2002), citam os tipos básicos de *TRAP* existentes, sendo eles sete:

a) *coldStart*: o dispositivo gerenciado foi reinicializado, indicando que a configuração do agente pode ter sido alterada;
b) *warmStart*: o dispositivo gerenciado foi reinicializado, porém a configuração do agente não foi alterada;
c) *linkDown*: o enlace de comunicação está inativo ou foi interrompido;

d) *linkUp*: o enlace de comunicação foi estabelecido;

e) *authenticationFailure*: o agente recebeu uma mensagem vinda do gerente SNMP que não foi autenticada;

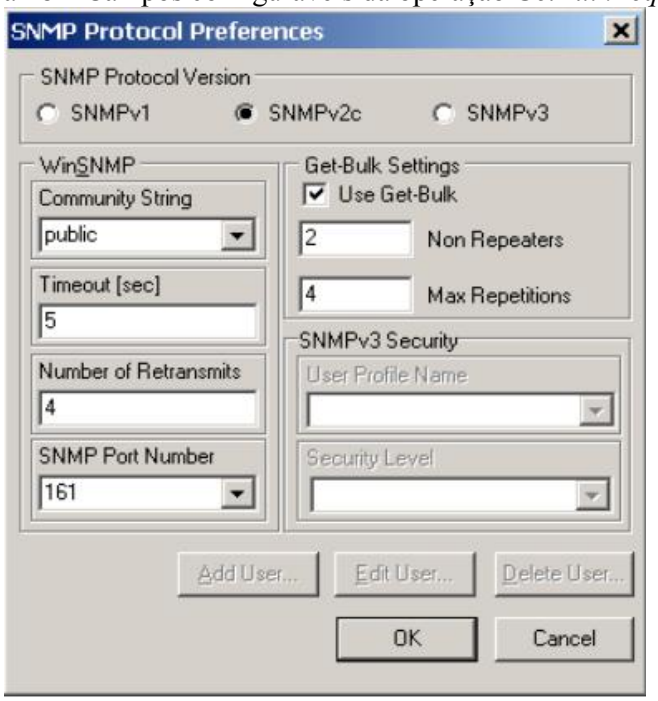
f) *egpNeighborLoss*: um par EGP parou. O EGP é o protocolo responsável por detectar equipamentos ou redes que estejam conectados ao equipamento monitorado;

g) *enterpriseSpecific*: indica a ocorrência de uma operação *TRAP* mais complexa.

As operações *GetBulkRequest* e *InformRequest* também são utilizados pelo SNMP. As duas operações foram implantadas na segunda versão do protocolo, a SNMPv2. Abaixo a descrição das funções de cada uma delas:

- *GetBulkRequest*: seu principal objetivo é recuperar grandes quantidades de informação com o menor número possível de troca de mensagens do protocolo. Seu princípio de funcionamento é igual ao *Get-Next*, porém com a capacidade de especificar o número de variáveis sucessoras que serão lidas (KOCH, 2008).
- Koch (2008), explica que essa operação possui os campos *non-repeaters* e *max-repititions*, que são utilizados para especificar o número de objetos para os quais deve ser retornado apenas um sucessor e para especificar o número de sucessores que devem ser recuperados. A Figura 18 ilustra como esses campos podem ser configurados:

Figura 18 – Campos configuráveis da operação *GetBulkRequest*



Fonte: KOCH (2008)

InformRequest: Koch (2008) afirma que essa operação possibilita a interação entre dois gerentes. Através do início da utilização da operação *InformRequest*, possibilitou-se a presença de mais de um gerente para monitoramento SNMP, visto que eles passaram a poder comunicar-se. Quando um agente envia uma solicitação *InformRequest* a outro gerente, recebe como retorno a informação *Response*.

5.6 CONSIDERAÇÕES DO CAPÍTULO

Com o desenvolvimento e utilização do protocolo SNMP para a gerência de redes, a tarefa de monitorar equipamentos e dispositivos de rede ficou mais simples. Através da consulta à MIB, é possível obter dados de diversos recursos do equipamento, que por vezes possibilitam a identificação de falhas.

Para efetuar a coleta e armazenamento dos dados, é utilizado um *software* executado em um servidor, denominado gerente SNMP. O gerente SNMP, além de coletar e armazenar informações, constrói gráficos baseado nas informações obtidas junto aos agentes SNMP. Ele também deve ter a capacidade de interpretar as informações coletadas dos agentes SNMP e tomar decisões pré-estabelecidas para cada caso, como por exemplo, enviar alertas para a área responsável pelo monitoramento toda vez que os valores obtidos junto ao agente ultrapassam os limites pré-estabelecidos na configuração. O capítulo seguinte irá explicar um método de avaliação utilizado para tomada de decisões que será utilizado posteriormente para definir qual o *software* que obteve melhor desempenho para fazer o papel de gerente SNMP.

6 MÉTODO ANALÍTICO HIERÁRQUICO

O Método Analítico Hierárquico (*Analytic Hierarchy Process*) é um método de avaliação desenvolvido na década de 70 por Tomas L. Saaty, sendo fundamentado em conceitos de Álgebra Relacional, Pesquisa Operacional e Psicologia. Segundo Guglielmetti, Marins e Salomon (2003), esse método é um importante instrumento para a tomada de decisões baseadas em muitos critérios, e será utilizado para avaliação dos *softwares* de gerenciamento de redes pesquisados.

O Método Analítico Hierárquico (MAH) permite através de sua metodologia, fazer comparações eficientes de critérios estabelecidos. Metodologias como esta são largamente utilizadas para padronizar avaliações e garantir a transparência nos resultados, para que as conclusões fiquem o mais próximo possível dos aspectos observados (SILVEIRA, 2011). O MAH possibilita transformar impressões subjetivas em notas lineares para a classificação de alternativas, além de aceitar variáveis quantitativas e qualitativas (MORAES e SANTALIESTRA, 2008). O MAH é simples e confiável, que facilita a tomada de decisões dado um número finito de possibilidades baseado num conjunto de critérios, para os quais são definidos pesos ou importâncias diferentes (JORDÃO e PEREIRA, 2006).

A utilização do MAH pode ser feita de diferentes formas, onde uma delas é proposta por Jordão e Pereira (2006), que se destaca pela facilidade de aplicação e possibilidade de comparação através de matrizes simplificadas baseadas em cálculos. O trabalho será orientado pela forma de trabalho proposta por Jordão e Pereira (2006). Nesta proposta a aplicação do MAH é composta por seis etapas: (1) Definição do Problema; (2) Estruturação Hierárquica; (3) Construção de Matrizes de Avaliação; (4) Normalização das Matrizes; (5) Construção das Matrizes de Prioridade e (6) Obtenção dos Resultados.

A primeira etapa consiste basicamente em definir o problema. O problema pode ser considerado como o objetivo a ser atingido através da execução do cruzamento e comparação de todos os critérios entre as alternativas analisadas (JORDÃO e PEREIRA, 2006).

A segunda etapa é a estruturação hierárquica do problema, sendo representada através de um diagrama composto por diferentes níveis. Segundo Moraes e *Santaliestra* (2008), nos níveis intermediários são listados os critérios de avaliação, denominados Objetivos e Subobjetivos. No nível mais externo da estrutura está a meta final. Ao final toda a estrutura é interligada a cada uma das alternativas em análise de modo a garantir que todas as alternativas serão avaliadas de acordo com os critérios estabelecidos.

A terceira etapa é a construção de matrizes de avaliação, que tem por objetivo cruzar os critérios de avaliação definidos com todas as alternativas em análise, nesse caso, os *softwares* de gerenciamento que estão sendo analisados. São elaborados dois conjuntos de matrizes onde são estabelecidos os pesos dos critérios e o impacto das alternativas sobre os critérios. Para atingir a meta final, será feito o cruzamento das matrizes que possibilitarão fazer comparações binárias (MORAES e SANTALIESTRA, 2008).

Na matriz de avaliação cada célula receberá um valor que representa o peso da alternativa ou critério em comparação com os demais. Se o item definido na linha tiver prioridade sobre o item definido na coluna, o resultado será elevado para a célula equivalente. Caso ocorra o contrário, tendo o item definido na coluna prioridade sobre o item definido na linha, a célula receberá um valor proporcionalmente inferior. Se ambos os itens tiverem a mesma prioridade, é atribuído o valor 1. Em um cruzamento entre linha e coluna do mesmo item, o resultado é sempre 1 (SALOMON, 2002).

A Escala Fundamental de Comparações é base para atribuição de pesos. Na Tabela 3 é possível identificar que quanto maior o peso de uma alternativa, maior é o valor atribuído à célula correspondente.

Tabela 3 – Escala Fundamental de Comparações

(continua)

Intensidade da Importância	Definição	Explicação
1	Igual importância	As duas atividades contribuem igualmente para o objetivo.
3	Fraca importância	A experiência e o julgamento favorecem levemente uma atividade em relação à outra.
5	Forte importância	A experiência e o julgamento favorecem fortemente uma atividade em relação à outra.
7	Importância muito forte	Uma atividade é fortemente favorecida em relação à outra; sua importância é demonstrada na prática.

(conclusão)

Intensidade da Importância	Definição	Explicação
9	Importância absoluta	A evidência favorece uma atividade em relação à outra com o mais alto grau de certeza.
2, 4, 6 e 8	Valores intermediários	Quando se procura uma condição e compromisso entre duas definições.
Recíproco dos valores	Se a atividade i recebe uma das designações diferente de zero, quando comparada com a atividade j, então j tem o valor recíproco quando comparada com i.	Uma designação razoável.

Fonte: SAATY, 1995 apud JORDÃO; PEREIRA, 2006

6.1 APLICAÇÃO DO MÉTODO

A Tabela 4 ilustra o comparativo entre o "Critério 1" que possui peso 1 e o "Critério 2" que possui peso 6. Os pesos atribuídos para os critérios poderiam ser de qualquer valor. Os pesos 1 e 6 foram atribuídos apenas para fins de exemplificação do método. Quando os critérios da linha e da coluna forem iguais, é atribuído o valor 1 à célula. Se o critério da linha for superior ao da coluna, é atribuído o valor 6 à célula. Mas se o critério da coluna for superior ao da linha, é atribuído o peso 1/6.

Tabela 4 – Comparação Binária de Critérios

	Critério 1	Critério 2
Critério 1	1	1/6
Critério 2	6	1

Fonte: JORDÃO e PEREIRA (2006)

Para fazer a comparação de alternativas, é elaborada uma matriz de Comparação Binária de Alternativas. Essa matriz possui o mesmo formato da Tabela 4, sendo que a forma

de comparação é exatamente a mesma. A Tabela 5 exemplifica como se faz a Comparação Binária de Alternativas.

Tabela 5 – Comparação Binária de Alternativas

	Alternativa 1	Alternativa 2
Alternativa 1	1	1/6
Alternativa 2	6	1

Fonte: JORDÃO e PEREIRA (2006)

Após a elaboração das matrizes, é realizada a normalização das matrizes. A normalização é calculada através da soma dos valores de uma coluna dividida pela soma dos valores atribuídos a cada elemento da coluna, de forma que a soma de todos os seus elementos seja igual a 1. Para finalizar a normalização, as frações são divididas e convertidas em números decimais para que seja possível encontrar a média aritmética de cada linha da matriz normalizada.

A Tabela 6 representa a soma das colunas da matriz. Na Tabela 7, cada elemento da matriz é dividido pela soma encontrada anteriormente. Por fim, a média é calculada dividindo o valor de cada célula pela soma de sua coluna. Os valores resultantes são somados e divididos pelo número de elementos.

Tabela 6 – Normalização da Matriz

	Alternativa 1	Alternativa 2
Alternativa 1	1	1/6
Alternativa 2	6	1
Soma	(1 + 6) = 7	(1/6 + 1) = 7/6

Fonte: JORDÃO e PEREIRA (2006)

Tabela 7 – Normalização da Matriz e Cálculo da Média

	Alternativa 1	Alternativa 2	Média
Alternativa 1	(1/7) = 1/7	[(1/6) / (7/6)]= 1/7	0,143
Alternativa 2	(6/7) = 6/7	[1 / (7/6)= 6/7	0,857
Soma	(1/7 + 6/7) = 1	(1/7 + 6/7) = 1	

Fonte: JORDÃO e PEREIRA (2006)

A Matriz de Prioridades (Tabela 8) é a matriz que lista todas as alternativas e a média obtida para cada um dos seus respectivos critérios. As linhas representam todas as alternativas

que estão em análise e as colunas são os critérios de avaliação. Em cada uma das células da Matriz de Prioridades é atribuído o valor obtido anteriormente no Cálculo da Média.

Tabela 8 – Matriz de Prioridades

	Critério 1
Alternativa 1	0,143
Alternativa 2	0,857

Fonte: JORDÃO e PEREIRA (2006)

De acordo com Freitas, Marins e Souza (2006), após calculada a matriz de prioridades, é necessário verificar a consistência das informações da matriz. Por exemplo, em uma matriz com as possibilidades A, B e C. Se A é maior que B e B é maior que C, então C não pode ser maior que A. Através de uma série de cálculos é possível encontrar uma relação de consistência para cada matriz de comparação. Para cada linha da matriz de comparação é necessário determinar a soma ponderada. Para determinar a soma ponderada, cada valor da linha deve ser multiplicado pela média obtida pela alternativa correspondente. Após realizadas as multiplicações, realizar a soma dos valores obtidos em cada linha. Os resultados obtidos pelas somas das linhas devem ser divididos pelo valor da média obtida pela alternativa correspondente. Os valores resultantes desta operação devem então ser somados e divididos pelo número de alternativas existentes na matriz de comparações, gerando então a média dos resultados de cada linha. A média dos resultados de cada linha é representada pela simbologia λmax.

Obtido o valor de λmax, é possível calcular o Índice de Consistência (IC), através da fórmula abaixo:

$$IC = (\lambda max - n) / (n - 1)$$

Após calculado o valor de IC, é necessário calcular o valor da Razão de Consistência (RC). Para isso é necessário dividir o valor de IC pelo valor da Inconsistência Aleatória Média (IAM), que é uma constante que depende do tamanho da matriz em análise (FREITAS, MARINS e SOUZA, 2006). Através da Tabela 9 pode ser visualizada a tabela de IAM.

Tabela 9 – Tabela de Inconsistência Aleatória Média

Dimensão da Matriz	1	2	3	4	5	6	7	8	9	10
Inconsistência Aleatória Média	0,00	0,00	0,52	0,89	1,11	1,25	1,35	1,40	14,5	1,49

Fonte: FREITAS, MARINS e SOUZA (2006)

Assim sendo, para realizar o cálculo de RC, utiliza-se a seguinte fórmula:

RC = IC / IAM

No MAH, é desejável que o valor de RC seja menor ou igual a 0,10 ou 10%(FREITAS, MARINS E SOUZA, 2006). Para casos de grande superioridade de um *software* em relação a outro, não é necessário realizar o cálculo de RC, pois fica evidenciada a superioridade de um dos avaliados. O cálculo de RC é utilizado com eficiência quando a avaliação de dois ou mais softwares ficam com valores finais muito próximos em um determinado critério de avaliação.

Para melhor entendimento do funcionamento e da aplicabilidade do MAH, a seguir será apresentado um exemplo de aplicação construído por Calloni (2012), para avaliar os *softwares* de gestão de riscos *VS Risk*, *STREAM*, *SOBF* e *SecureAware*.

6.2 EXEMPLO DE APLICAÇÃO DO MÉTODO

Calloni (2012) aplicou o MAH utilizando 13 critérios para avaliar os *softwares*, conforme a Tabela 10.

Tabela 10 – Critérios de avaliação dos *softwares*

Legenda	Critério	Peso
C1	Identificação e definição dos valores dos ativos	7
C2	Identificação de ameaças	7
C3	Identificação de vulnerabilidades	7
C4	Identificação de controles	6
C5	Biblioteca do *software*	7
C6	Definição do impacto e do risco	7
C7	Histórico de incidentes	6
C8	Capacidade de adaptação às mudanças	9
C9	Dependência dos ativos	9
C10	Tratamento do risco	9
C11	Usabilidade do *software*	6
C12	Relatórios gerados	7
C13	Documentação do *software*	6

Fonte: CALLONI (2012)

Na comparação realizada por Calloni (2012) através do Método Analítico Hierárquico, quando um *software* de uma linha é comparado com ele mesmo, é atribuído o

valor 1. Se o *software* de uma linha possuir avaliação igual ao de uma coluna, também é atribuído o valor 1. Se o *software* localizado na linha possuir uma avaliação melhor que o *software* encontrado na coluna, será atribuído um valor maior do que 1, definido de acordo com a escala fundamental de comparações (Tabela 3). Por fim, se o *software* da coluna for avaliado com superioridade em relação ao *software* encontrado na linha, seu valor será 1/9, por exemplo, de acordo com o grau de superioridade. Para casos onde existe grande superioridade de um *software* em relação a outro será utilizado o valor 9, e o valor 6 será utilizado para casos onde existe superioridade de um *software* em relação a outro, mas não de forma tão acentuada. Através da utilização dos valores padrão 6 e 9, a realização das comparações se tornará mais simplificada.

A soma das colunas fica representada na última linha de cada tabela. O valor da soma será utilizado para o cálculo da média, que é a coluna localizada mais a direita da tabela. O cálculo da média para cada linha é realizado da seguinte forma, sendo N de 1 até o número de elementos:

$$\frac{\frac{\text{(valor da linha 1)}}{\text{soma coluna 1}} + \frac{\text{(valor da linha N)}}{\text{soma coluna N}}}{N}$$

Critério 1: Identificação e definição dos valores dos ativos

De acordo com as características encontradas nos *softwares*, foi construída uma matriz de comparação para avaliá-los utilizando o MAH. Os *softwares* que obtiveram melhor média neste critério foram o SOBF e o *SecureAware*.

O *software VS Risk* ficou em uma faixa de avaliação intermediária, onde atendeu alguns requisitos propostos de forma satisfatória, porém deixou a desejar em outros.

O *software STREAM* foi o pior colocado entre os quatro *softwares* comparados em relação ao primeiro critério, conforme demonstrado na Tabela 11.

Tabela 11 – Matriz de avaliação para o critério C1

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	6	1/9	1/9	0,09
STREAM	1/6	1	1/9	1/9	0,03
SOBF	6	9	1	1	0,42
SecureAware	6	9	1	1	0,42
Soma	13,16	25	2,22	2,22	

Fonte: CALLONI (2012)

Após obtida a matriz de avaliação dos *softwares* para o critério C1, deve ser calculada a consistência das avaliações. Abaixo os cálculos de consistência para C1.

(1x0,9) + (6x0,03) + (1/9x0,42) + (1/9x0,42) = 0,362

(1/6x0,09) + (1x0,03) + (1/9x0,42) + (1/9x0,42) = 0,137

(6x0,09) + (9x0,03) + (1x0,42) + (1x0,42) = 1,65

(6x0,09) + (9x0,03) + (1x0,42) + (1x0,42) = 1,65

A soma ponderada para cada linha deve ser dividida pela média da alternativa correspondente. Nesse caso:

0,362/0,09 = 4,022

0,137/0,03 = 4,566

1,65/0,42 = 3,928

1,65/0,42 = 3,928

$\lambda max = (4,022 + 4,566 + 3,928 + 3,928) / 4 = 4,111$

Após obter o valor de λmax deverá ser aplicada a fórmula abaixo:

$IC = (\lambda max - n) / (n - 1)$

$IC = (4,111 - 4) / (4 - 1) = 0,111 / 3$

IC = 0,037

Após calculado o IC, deve ser calculado o RC:

RC = IC / IAM

RC = 0,037 / 0,89

RC = 0,04

Critério 2: Identificação de ameaças

Para este critério, os *softwares VS Risk*, *STREAM* e SOBF foram avaliados de forma igual. O *SecureAware* foi o *software* melhor avaliado, conforme ilustrado pela Tabela 12.

Tabela 12 – Matriz de avaliação para o critério C2

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	1	1	1/6	0,10
STREAM	1	1	1	1/6	0,10
SOBF	1	1	1	1/6	0,10
SecureAware	6	6	6	1	0,66
Soma	9	9	9	1,48	

Fonte: CALLONI (2012)

Após obtida a matriz de avaliação dos *softwares* para o critério C2, deve ser calculada a consistência das avaliações. Abaixo os cálculos de consistência para C2.

(1x0,10) + (1x0,10) + (1x0,10) + (1/6x0,66) = 0,41

(1x0,10) + (1x0,10) + (1x0,10) + (1/6x0,66) = 0,41

(1x0,10) + (1x0,10) + (1x0,10) + (1/6x0,66) = 0,41

(6x0,10) + (9x0,10) + (6x0,10) + (1x0,66) = 2,76

A soma ponderada para cada linha deve ser dividida pela média da alternativa correspondente. Nesse caso:

0,41/0,10 = 4,1

0,41/0,10 = 4,1

0,41/0,10 = 4,1

2,76/0,66 = 4,18

λmax = (4,1 + 4,1 + 4,1 + 4,18) / 4 = 4,12

Após ober o valor de λmax deve ser aplicada a fórmula abaixo:

IC = (λmax – n) / (n – 1)

IC = (4,12 – 4) / (4 – 1) = 0,12 / 3

IC = 0,04

Após calculado o IC, deve ser calculado o RC:

RC = IC / IAM

RC = 0,04 / 0,89

RC = 0,045

Critério 3: Identificação de vulnerabilidades

Para esse critério, os *softwares* melhor avaliados foram o *VS Risk* e o SOBF. O *SecureAware* ficou com uma avaliação estabelecida como intermediária e o pior dos *softwares* nesse critério foi o *STREAM*, conforme a Tabela 13 demonstra.

Tabela 13 – Matriz de avaliação para o critério C3

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	9	1	6	0,42
STREAM	1/9	1	1/9	1/6	0,03
SOBF	1	9	1	6	0,42
SecureAware	1/6	6	1/6	1	0,11
Soma	2,27	25	2,27	13,16	

Fonte: CALLONI (2012)

Após obtida a matriz de avaliação dos *softwares* para o critério C3, deve ser calculada a consistência das avaliações. Abaixo os cálculos de consistência para C3.

(1x0,42) + (9x0,03) + (1x0,42) + (6x0,11) = 1,77

(1/9x0,42) + (1x0,03) + (1/9x0,42) + (1/6x0,11) = 0,14

(1x0,42) + (9x0,03) + (1x0,42) + (6x0,11) = 1,77

(1/6x0,42) + (6x0,03) + (1/6x0,42) + (1x0,11) = 0,43

A soma ponderada para cada linha deve ser dividida pela média da alternativa correspondente. Nesse caso:

1,77/0,42 = 4,21

0,14/0,03 = 4,66

1,77/0,42 = 4,21

0,43/0,11 = 3,91

$\lambda max = (4,21 + 4,66 + 4,21 + 3,91) / 4 = 4,247$

Após obter o valor de λmax deve ser aplicada a fórmula abaixo:

$IC = (\lambda max - n) / (n - 1)$

$IC = (4,247 - 4) / (4 - 1) = 0,247 / 3$

IC = 0,082

Após calculado o IC, deve ser calculado o RC:

RC = IC / IAM

RC = 0,082 / 0,89

RC = 0,092

Com as médias calculadas para todos os critérios analisados, é necessário fazer o cálculo final que determina o valor total de cada *software*. Para fazer esse cálculo, a média de cada critério é multiplicada pelo peso do mesmo critério. Esse cálculo é feito para todos os critérios analisados e após feito isso, o resultado das multiplicações é somado a fim de obter o valor total de cada *software*. A Tabela 14 demonstra a matriz de médias dos critérios, onde são apresentadas as médias que cada *software* obteve para cada critério, o peso de cada critério e ao final, o total de pontuação obtida por cada um deles.

Tabela 14 – Matriz de médias dos critérios

Critérios	VS Risk	STREAM	SOBF	SecureAware	Peso Critério
C1 – Ident. e definição dos valores dos ativos	0,09	0,03	**0,42**	**0,42**	7
C2 – Ident. de ameaças	0,10	0,10	0,10	**0,66**	7
C3 – Ident. de vulnerabilidades	**0,42**	0,03	**0,42**	0,11	7
Total	**0,61**	**0,16**	**0,94**	**1,19**	

Fonte: CALLONI (2012)

Através dos testes efetuados por Calloni (2012), foi possível observar que de acordo com os três critérios comparados e pesos estabelecidos para avaliação, o *software* que

apresentou melhor desempenho foi o *SecureAware*. Em segundo lugar ficou SOBF. Em terceiro o *VS Risk* e com a pior avaliação e no último lugar, o *STREAM*.

6.3 CONSIDERAÇÕES DO CAPÍTULO

Como pode ser visto, o MAH é uma ferramenta de apoio para gestores e auxilia na tomada de decisões importantes dentro de uma organização. Neste trabalho o MAH será utilizado para definir qual dos *softwares* de gerenciamento de redes é o mais adequado para ser utilizado no cenário da empresa Bom Tempo Telecom.

Um método de análise de requisitos, onde é possível estabelecer importâncias através de pesos para cada funcionalidade, é muito importante, pois reforça e justifica uma tomada de decisão. Tomadas de decisão devem possuir embasamento e não podem ser algo impensado. O MAH é o auxiliar do gestor ao demonstrar para onde estão sendo direcionados os rumos da empresa.

7 PROPOSTA DE SOLUÇÃO

A empresa Bom Tempo Telecom identificou em seu cenário de atuação diversas falhas em serviços fornecidos a assinantes através de fibra óptica. Ao longo de vinte meses de experiência com a tecnologia FTTH, foi possível identificar uma das causas mais comuns que ocasiona interrupções nos serviços prestados ao assinante: a atenuação. A atenuação possui como característica a apresentação de perdas de sinal óptico, que inicialmente faz com que a métrica de vazão até a ONU do assinante e, consequentemente, também a métrica de capacidade do enlace fiquem com desempenho reduzido. Com a vazão e a capacidade prejudicadas, operações antes executadas normalmente podem ter seu desempenho comprometido. A perda de desempenho pode ser identificada através de características específicas como a perda de pacotes e aumento da latência.

7.1 CENÁRIO ATUAL

A Bom Tempo Telecom conta com uma estrutura de cerca de 400 quilômetros de fibra óptica utilizada para a interligação da estrutura de *backbone* e também para o atendimento de assinantes através da estrutura do tipo FTTH.

Em pontos estratégicos do *backbone*, geralmente situados em grandes centros, ficam as OLT's. Do ponto da OLT até a ONU que fica dentro da residência do assinante, o meio físico de transporte dos dados é composto totalmente por fibra óptica.

Atualmente, para os assinantes de serviços entregues por fibra óptica, a Bom Tempo Telecom comercializa planos de acesso à internet de até 15 *Megabits* por segundo e também telefonia VOIP, que realiza chamadas de voz através da internet.

Para atender a essa demanda, a Bom Tempo Telecom investiu em equipamentos GPON da marca Parks. A Parks é uma empresa gaúcha e que está no mercado de telecomunicações desde 1966, fabricando equipamentos para transmissão eletrônica de informações.

A Parks fornece 28 tipos de modelos diferentes de ONUs, iniciando pelo modelo mais simples, que possui apenas uma porta *Fast Ethernet*, e chegando até o modelo mais completo, com duas portas *Gigabit Ethernet*, duas portas FXS, *interface* coaxial para televisão e *wireless* integrado. A Bom Tempo Telecom utiliza três modelos de equipamentos Parks: a OLT *Fiberlink* 10000S e as ONUs *Fiberlink* 1000 e *Fiberlink* 1000B. A Figura 19

ilustra a estrutura de atendimento montada pela Bom Tempo Telecom em diversas cidades do Vale do Caí.

Figura 19 – Estrutura de atendimento FTTH da empresa Bom Tempo Telecom

Fonte: Elaborado pelo autor.

Através da Figura 19 é possível identificar duas OLT's, que seriam de cidades diferentes, atendendo cada uma delas a sua região. A OLT *Fiberlink* 10000S (Figura 20) é o modelo de equipamento utilizado pela Bom Tempo Telecom na central de atendimento. A estrutura sempre é montada com a utilização de OLT's de 8 portas GPON, onde em cada uma delas é possível conectar de 64 a 128 assinantes. O número de assinantes por porta varia de acordo com a distância dos assinantes até a OLT. Se a distância máxima for inferior a dois quilômetros, é possível atender até 128 assinantes. Se a distância máxima estiver situada entre dois e cinco quilômetros, o número de assinantes por porta GPON é reduzido para 96. Por fim, se a distância máxima for acima de cinco quilômetros, o número de assinantes possíveis de serem atendidos cai para 64.

Figura 20 – OLT Parks *Fiberlink* 10000S

Fonte: http://www.parks.com.br/site/pt/produto.php?idcat=282&id=309 acesso em 11/06/2014

A OLT *Fiberlink* 10000S possui diversas *interfaces*: fonte redundante, 8 portas GPON, 2 portas XFP (10 *Gigabit Small Form Factor Pluggable*) utilizadas para *uplink*, 2 portas SFP (*Small Form Factor Pluggable*) *para uplink*, 4 portas *Gigabit Ethernet* também utilizadas para *uplink* e 2 portas *Fast Ethernet*, sendo uma delas para gerenciamento via console e outra porta dedicada para gerenciamento WEB e SNMP.

Em assinantes residenciais é instalada uma ONU do modelo *Fiberlink* 1000 (Figura 21), que possui as funcionalidades de VLAN, portas FXS (*Foreign Exchange Office*) que são utilizadas para conectar um telefone analógico possibilitando realizar chamadas através de VOIP, *firewall*, NAT (*Network Address Translation*), PPPoE (*Point-to-Point Protocol over Ethernet*), DHCP (*Dynamic Host Configuration Protocol*), endereçamento IP estático, entre outras funcionalidades. Para que o assinante tenha acesso à internet ele deve autenticar-se junto ao provedor de serviços Bom Tempo Telecom. Para que a autenticação ocorra, cada assinante possui um usuário e senha que é configurado dentro da sua ONU no momento da instalação, sendo esses dados validados mediante uma autenticação.

Figura 21 – ONU Parks modelo *Fiberlink* 1000

Fonte: http://www.parks.com.br/site/pt/produto.php?idcat=282&id=463 acesso em 11/06/2014

Em assinantes que fazem parte de um condomínio ou contratam planos empresariais, é instalada uma ONU do modelo *Fiberlink* 1000B. A única diferença existente entre a ONU *Fiberlink* 1000 e a *Fiberlink* 1000B, do ponto de vista estético, é que o modelo *Fiberlink* 1000B não possui portas FXS. Tecnicamente falando, essa diferenciação se faz devido ao fato de não ser necessário colocar uma ONU dentro da residência de cada assinante de um condomínio, pois é lançada uma fibra óptica até um ponto central do condomínio onde ficará

a ONU. A partir desse ponto é montada uma estrutura com cabeamento estruturado UTP (*Unshielded Twisted Pair*) até todos os apartamentos ou casas onde houver assinantes. A ONU utilizada nesse caso não possui nenhuma característica que permita realizar a autenticação do assinante com o provedor, servindo então apenas para fazer a conversão do sinal óptico em sinal elétrico. Para entregar os serviços de internet e telefonia IP para um assinante de um condomínio são necessários equipamentos adicionais, visto que na casa do assinante estará chegando apenas um cabo de rede. Nesse caso, os dados de autenticação do assinante são configurados em um ponto de acesso *wireless* (Figura 22), ao invés de serem configurados dentro da ONU, como acontece em assinantes residenciais. Para disponibilizar um telefone capaz de realizar e receber chamadas VOIP, um cabo de rede deve partir do ponto de acesso *wireless* do assinante e deve ser conectado a um ATA (Adaptador para Telefone Analógico) (Figura 23). Esse ATA conterá a configuração da conta VOIP do assinante e terá diretamente conectado a ele um telefone analógico que será utilizado para efetuar ligações.

Figura 22 – Ponto de Acesso *Wireless*

Fonte: http://www.tp-link.com.br/products/?categoryid=1680 acesso em 11/06/2014

Figura 23 – ATA VOIP

Fonte: http://www.wdvoip.com.br/spa3102-na-linksys-cisco-c-roteador/ acesso em 11/06/2014

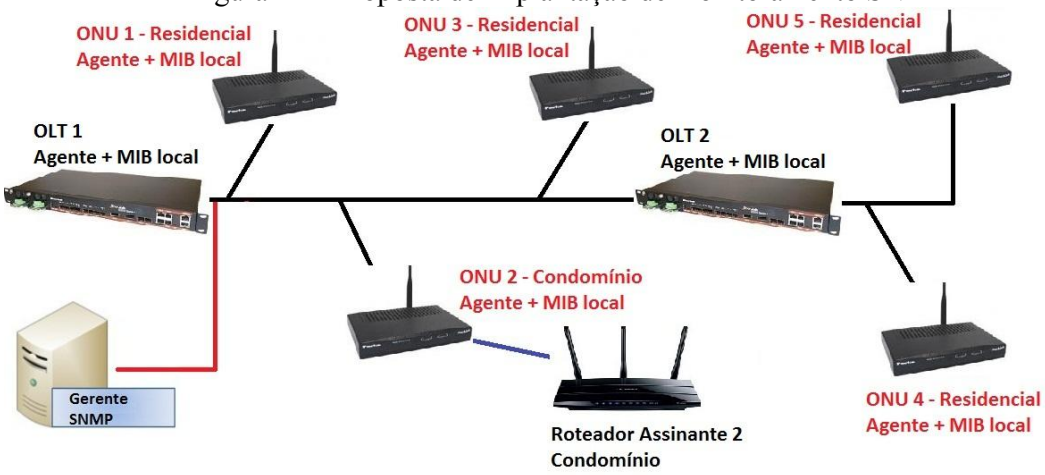
A estrutura montada pela Bom Tempo Telecom para atender aos seus assinantes é homogênea e de arquitetura proprietária, sendo toda a estrutura construída em parceria com a empresa Parks. Baseado no princípio de homogeneidade da rede fica mais simples de monitorá-la, visto que é necessário parametrizar as configurações para os equipamentos de apenas um fabricante.

7.2 ARQUITETURA DE GERENCIAMENTO TCP/IP PROPOSTA

Para fazer um monitoramento da estrutura FTTH da Bom Tempo Telecom, visando prevenir e antecipar-se aos problemas, será necessário efetuar um monitoramento com o auxílio de um *software*.

De acordo com Santos (2009), *softwares* para gerência e monitoramento de redes funcionam em uma arquitetura cliente-servidor, ou seja, gerente-agente. O gerente é a máquina onde executa o processo servidor e o agente é o dispositivo de rede gerenciado que executa o processo cliente. O *software* implantado deverá funcionar baseado no protocolo SNMP em uma estrutura gerente-agente. A Figura 24 ilustra a proposta de implantação do monitoramento na rede da Bom Tempo Telecom.

Figura 24 – Proposta de implantação de monitoramento SNMP



Fonte: Elaborado pelo autor.

Na proposta apresentada, serão testados três *softwares* de monitoramento que utilizam o protocolo SNMP. Os *softwares* farão o papel de coletar informações da MIB

proprietária contida no equipamento de cada assinante. Os dados obtidos da MIB deverão ser armazenados em um banco de dados.

As MIBs proprietárias fornecidas pela empresa Parks, já são nativas em todos os modelos de ONU. O agente que executa em cada ONU e OLT faz a função de armazenar as informações atualizadas dentro da MIB local do equipamento, garantindo assim que os dados coletados pelo gerente SNMP estarão sempre atualizados.

Através do monitoramento proposto, a MIB II possibilitará identificar e monitorar valores padrão, como o estado e velocidade das *interfaces* da ONU, por exemplo. As métricas de desempenho de latência e perdas de pacotes serão monitoradas através da utilização do protocolo TCP/IP. A MIB proprietária por sua vez, permitirá o monitoramento da vazão, capacidade do enlace da OLT até a ONU do assinante e também o nível de sinal recebido pela ONU. Para testar a comunicação SNMP com uma ONU a fim de verificar se as informações eram retornadas conforme o esperado, foi utilizado um *software* genérico de testes de SNMP, chamado *GetIf* . As informações foram retornadas conforme o esperado e através desse teste foi possível concluir que a realização do monitoramento poderá ser concretizada sem maiores empecilhos.

Os *softwares* serão instalados em servidores virtuais para aproveitar recursos já alocados que encontram-se ociosos. Mesmo sendo virtuais, os três servidores serão visíveis para a rede como sendo máquinas físicas, garantindo assim que o resultado dos testes não seja prejudicado.

7.3 *SOFTWARES* DE GERENCIAMENTO

Mecanismos automatizados de monitoramento vêm se tornando cada vez mais necessários para garantir a estabilidade e SLA de redes de fibra óptica do tipo FTTH. Ju-Guang, Jun e Dong-Ming (2011) afirmam que na gestão de rede moderna, o protocolo SNMP vem desempenhando papel muito importante devido à sua simplicidade.

Ferramentas de monitoramento de rede são responsáveis por monitorar, analisar e alertar problemas em redes de computadores. O uso desse tipo de ferramenta de monitoramento possibilita ao administrador da rede isolar os problemas em segmentos de rede específicos. Através do isolamento de segmentos de rede, a identificação de problemas torna-se mais simples, pois não é considerado mais o todo, e sim apenas o segmento especificado.

No mercado existem diversas soluções de *software* que possibilitam o monitoramento de rede. A seguir serão explicados os principais *softwares* disponíveis realizando um comparativo entre as características de cada um deles.

De acordo com matéria publicada pelo site Cisco Console[1] em janeiro de 2012, os seis principais *softwares* utilizados para monitoramento de redes são, *Cacti*, PRTG *Network Monitor*, Nagios, *Orion Network Performance Monitor* (ONPM), *Colasoft Packet Graphing* (CPG) e Munin.

Outra pesquisa, realizada pelo conceituado blog americano *Tech Source*[2], coloca o *Zabbix* como sendo uma das cinco melhores ferramentas livres para monitoramento de redes.

Os *softwares* que serão selecionados para o teste devem atender as seguintes premissas:

a) Ser distribuído sob licença livre;
b) Executar em plataforma Linux;
c) A *interface* deve ser Web;
d) Trabalhar com o protocolo SNMP;
e) Permitir a importação de MIB proprietária bem como interpretá-la;
f) Armazenar as informações em um banco de dados;
g) Gerar gráficos a partir dos dados obtidos;
h) Suportar as três versões do protocolo SNMP;
i) Possibilitar o envio de alertas em casos de ocorrência de alterações no funcionamento normal da rede.

Analisando a documentação dos *softwares* a fim de verificar o atendimento dos requisitos especificados, foi construída a Tabela 15.

Tabela 15 – Comparativo entre ferramentas de monitoramento

(continua)

Caracterís-ticas	*Softwares*						
	Cacti	ONPM	*Nagios*	CPG	PRTG	*Munin*	*Zabbix*
Sistema Operacional	*Linux*	*Windows Server* 2003/2008	*Linux Unix*	*Windows*	*Windows*	*Windows* e *Linux*	*Linux*

[1] *http://www.ciscoconsole.com/network-tools/monitoring-tools/top-10-best-network-monitoring-software-tools.html/* acesso em 07/06/2014
[2] *http://www.junauza.com/2010/12/free-server-monitoring-software.html* acesso em 13/06/2014

(conclusão)

Característi-cas	*Softwares*						
	Cacti	ONPM	*Nagios*	CPG	PRTG	*Munin*	*Zabbix*
Licença	Livre	Pago	Livre	Pago	Pago	Livre	Livre
MIB Proprietária	Sim	Sim	Sim	Não	Sim	Não	Sim
Interface	*Web*	*Web*	*Web*	*Desktop*	*Web*	*Web*	*Web*
Banco de dados	*MySQL*	*SQL Server* 2005 ou 2008	*MySQL*	Não	Sim, versão não publicada	*Postgre-SQL*	*MySQL Postgre SQL* ou *Oracle*
Geração de Gráficos	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Protocolo SNMP	Sim	Sim	Sim	Não	Sim	Sim	Sim
Versão SNMP	1, 2 e 3	1, 2 e 3	1, 2 e 3	-	1, 2 e 3	1, 2 e 3	1, 2 e 3
Alertas	Alerta visual, sonoro e *email*	*Email* e alerta sonoro	*Email*, SMS (*Short Message Service*), ligação e alerta visual	*Popup*	*Email* e SMS	*Email*	*Email*, SMS e ligação

Fonte: Elaborado pelo autor.

De acordo com a Tabela 15, é possível observar que os *softwares* mais completos são o *Cacti*, o *Nagios* e o *Zabbix*. Esses *softwares* são livres, utilizam banco de dados para guardar as informações do SNMP, interpretam e se comunicam através das três versões do protocolo, possibilitam o envio de alertas, entre outras características citadas que fizeram com que eles se sobressaíssem sobre os demais *softwares*. Como fatores contra cada um dos quatro *softwares* rejeitados, as principais características negativas são:

a) O PRTG é pago e é executável apenas em plataforma Windows, sendo que uma das premissas é que o *software* deve ser executável em plataforma Linux.
b) O ONPM também é pago e executável apenas em plataforma Windows.

c) O CPG é pago, executável apenas em plataforma Windows, não guarda as informações em banco de dados, não trabalha com o protocolo SNMP, possui *interface desktop* e possibilita apenas enviar alertas através de *popup*.
d) O Munin não é capaz de interpretar MIBs proprietárias e a única forma de enviar alertas é por email.

7.4 CRITÉRIOS PARA ANÁLISE DOS *SOFTWARES*

Para realizar a avaliação dos *softwares*, foram definidos doze critérios. Para cada critério foi definido um peso, que será utilizado para fazer o cálculo de comparação. Baseado nos conceitos de tecnologias PON, métricas de desempenho e SLA estudados anteriormente, alguns critérios são de fundamental importância para definir qual o melhor *software*, tais como:

a) Medição de latência: o *software* deve possibilitar a realização de testes contínuos de latência entre o gerente SNMP e os agentes.
b) Medição de perda de pacotes: o *software* deve possibilitar o monitoramento constante do índice de perda de pacotes entre o gerente SNMP e os agentes.
c) Medição de vazão: o *software* também deve possibilitar medir e monitorar a vazão do canal de comunicação com cada agente SNMP.
d) Medição de capacidade: o *software* deve permitir medir e monitorar a capacidade do canal de comunicação com cada agente SNMP.
e) Medição de intensidade de sinal: o *software* deve permitir medir e monitorar a intensidade do sinal de fibra óptica recebido por cada agente SNMP.
f) Envio e configuração de tipos de alertas: ao perceber alterações no estado normal da rede, o *software* deve possibilitar a configuração de envio de alertas aos setores responsáveis.
g) Facilidade de configuração: tem o objetivo de avaliar qual dos *softwares* apresenta maior facilidade de configuração dos serviços de monitoramento.
h) Histórico de SLA: o *software* deve armazenar, de preferência em gráfico, um resumo do SLA separado por dispositivo em um determinado período de tempo selecionado pelo usuário.
i) Usabilidade: o *software* deve ser de simples utilização e com *interface* amigável e intuitiva.

j) Documentação do *software*: para que o *software* seja entendido de forma adequada é importante que ele possua documentação detalhada que auxilie o usuário caso o mesmo tenha dúvidas.
k) Registro de incidentes: o *software* deve armazenar os incidentes ocorridos com cada dispositivo em determinado período de tempo selecionado pelo usuário, bem como permitir a consulta a esses dados.
l) Integração de MIBs proprietárias: o *software* deve permitir adicionar MIBs proprietárias bem como interpretá-las a fim de identificar e compreender as informações coletadas dos equipamentos através de SNMP.

O peso para cada critério foi definido de acordo com a sua relevância para o processo de monitoramento por SNMP para redes ópticas do tipo FTTH, conforme pode ser visto na Tabela 16:

Tabela 16 - Critérios de avaliação dos *softwares*

Legenda	Critério	Peso
C1	Medição de latência	3
C2	Medição de perda de pacotes	3
C3	Medição de vazão	3
C4	Medição de capacidade	6
C5	Medição de intensidade de sinal	9
C6	Envio e configuração de tipos de alertas	9
C7	Facilidade de configuração	9
C8	Histórico de SLA	6
C9	Usabilidade	9
C10	Documentação do *software*	6
C11	Registro de incidentes	6
C12	Integração de MIBs proprietárias	9

Fonte: Elaborado pelo autor.

Os pesos para cada critério foram definidos de acordo com a sua importância para o ambiente de monitoramento da Bom Tempo Telecom e em conjunto com a direção da empresa, sendo o valor 3 considerado pouco importante, o valor 6 como sendo de média importância e o valor 9 para critérios muito importantes.

8 TESTES DOS *SOFTWARES*

Os três *softwares* testados, que são o *Nagios*, *Cacti* e *Zabbix*, já estão a bastante tempo no mercado e são largamente utilizados para monitoramento de redes. Os mesmos foram instalados em uma plataforma de virtualização baseada em *Xen Server,* da Bom Tempo Telecom, onde foram alocados recursos disponíveis para possibilitar o teste dos *softwares*.

A estrutura de virtualização conta com poder computacional que proporciona desempenho igual a um servidor físico instalado especialmente para prover a funcionalidade do gerenciamento. Isso faz com que os *softwares* a serem testados não tenham seu desempenho prejudicado.

8.1 OBJETOS A SEREM LIDOS DA MIB PROPRIETÁRIA

Para coletar as informações das métricas de monitoramento desejadas, foi necessário realizar a leitura das MIBs proprietárias disponibilizadas pela empresa Parks. As seis MIBs disponibilizadas são extensas e juntas apresentam cerca de 815 objetos. Apesar de disponibilizar muitos objetos para consulta, grande parte deles apresentam informações relativas ao protocolo GPON e são informações estáticas que não sofrem atualização, como por exemplo, o objeto *gponSysCfgKeyExchangeInterval* que retorna o tempo de troca de chaves entre a OLT e as ONUs para manterem a conexão ativa. Esse tempo possui o valor padrão de 3600 segundos e permanece inalterado.

Os objetos das MIBs que são relevantes para este trabalho possibilitam extrair a informação da potência do sinal óptico recebido pelas ONUs instaladas nos assinantes e também a configuração de capacidade do canal de comunicação entre a OLT e cada ONU. A Tabela 17 apresenta os objetos a serem consultadas para a realização do trabalho, bem como a informação e o tipo de informação que eles retornam.

Tabela 17 – Objetos relevantes a serem consultados

(continua)

MIB	Tabela / Objeto	Valor retornado	Tipo do valor
GPON-OLT-EQPT	*OnuCfgTable* / *onuCfgSlotNo*	Valor do índice correspondente ao *slot* ao qual pertence a porta PON da OLT	Inteiro (variável entre 1 e 2)
GPON-OLT-EQPT	*OnuCfgTable* / *onuCfgPortNo*	Valor do índice correspondente à porta PON da OLT	Inteiro (variável de 1 a 8)

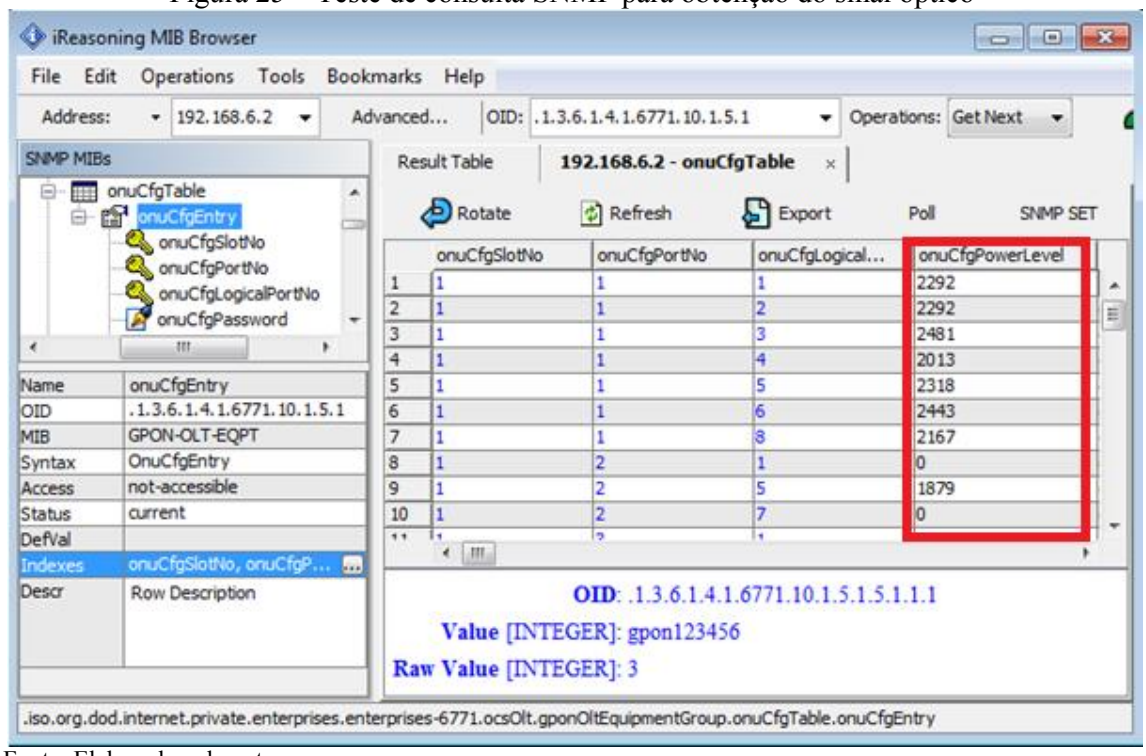
(conclusão)

MIB	Tabela / Objeto	Valor retornado	Tipo do valor
GPON-OLT-EQPT	*OnuCfgTable* / *onuCfgLogicalPortNo*	Valor do índice correspondente à posição da ONU na porta PON da OLT	Inteiro (variável de 1 a 128)
GPON-OLT-EQPT	*OnuCfgTable* / *onuCfgTcontVirtualPortBindingProfileIndex*	Valor do índice correspondente ao fluxo de tráfego da ONU a ser monitorada	Inteiro (variável de 1 a 4096)
GPON-OLT-SVC	*onuTcontVPortBindProfTable* / *tcontVirtualPortBindingProfileIndex*	Valor do índice que faz a associação entre o perfil de tráfego e o perfil de serviço	Inteiro (variável de 1 a 4096)
GPON-OLT-SVC	*onuTcontVPortBindProfTable* / *tcontServiceProfileIndex*	Valor do índice do perfil de serviço da *vlan* utilizada pela ONU	Inteiro (variável de 1 a 4096)
GPON-OLT-SVC	*onuTcontSvcProfTable* / *onuTcontServiceProfileIndex*	Valor do índice que faz a associação entre o perfil de serviço e o perfil de banda	Inteiro (variável de 1 a 4096)
GPON-OLT-SVC	*onuTcontSvcProfTable* / *upstreamBandwidthProfileIndex*	Valor do índice de perfil de banda ao qual pertence o perfil de serviço utilizado pela ONU	Inteiro (variável de 1 a 4096)
GPON-OLT-SVC	*onuBwProfTable* / *bandwidthProfileIndex*	Valor do índice do perfil de banda	Inteiro (variável de 1 a 4096)
GPON-OLT-SVC	*onuBwProfTable* / *maximumBandwidth*	Velocidade do canal de comunicação do perfil de banda ao qual a ONU pertence	Inteiro (variável de 1 a 2500000)

Fonte: Elaborado pelo autor.

Para a obtenção dos valores de sinal óptico e de capacidade do canal de comunicação entre a OLT e uma ONU utilizada para efetuar os testes, foi possível identificar através do *software Ireasoning*[3] que é necessário realizar uma combinação de MIBs e objetos para chegar ao valor correto a ser consultado. Com esse *software* é possível importar uma MIB com vários objetos para realizar as simulações de consulta SNMP. A Figura 25 demonstra um teste de consulta na MIB GPON-OLT-EQPT utilizando os objetos *onuCfgSlotNo*, *onuCfgPortNo*, *onuCfgLogicalPortNo* e *onuCfgPowerLevel* para obtenção da potência óptica recebida pela ONU do assinante. Para obter esses valores, a consulta SNMP foi direcionada diretamente à OLT, pois é ela quem armazena a posição e distribuição das ONUs dentre as portas PON, bem como a leitura dos sinais das ONUs. O retorno da consulta SNMP para a obtenção do nível de sinal das ONUs sempre é dado em um formato numérico e inteiro contendo quatro números. Porém, tecnicamente o sinal óptico recebido por uma ONU pode ser variável de 0 a 28, podendo conter até duas casas decimais. Por exemplo, o sinal 24,81 é apresentado pelo objeto *onuCfgPowerLevel* com o valor 2481.

Figura 25 – Teste de consulta SNMP para obtenção do sinal óptico



Fonte: Elaborado pelo autor.

Outra métrica a ser monitorada é a capacidade do canal de comunicação entre a OLT e cada ONU. Para obter o valor de capacidade através de SNMP, assim como para obter a

[3] *http://www.ireasoning.com/*

potência óptica de cada ONU, é necessário realizar uma combinação de resultados de consultas para chegar ao OID correto a ser consultado. A configuração da OLT Parks é baseada em perfis de alocação de banda, onde podem ser realizadas diferentes alocações de banda para cada ONU, dependendo do plano de acesso contratado pelo assinante.

O funcionamento da OLT da empresa Parks segue algumas premissas:

a) cada ONU possui um fluxo de tráfego associado à ela;
b) o fluxo de tráfego faz a comunicação com a ONU através de um perfil de serviço.
c) o perfil de serviço está associado a um perfil de banda, que possui uma configuração de limitação de capacidade do canal de comunicação.

As consultas SNMP direcionadas aos objetos utilizados neste trabalho não retornam os valores reais utilizados para realizar o monitoramento, exceto para os objetos *onuCfgPowerLevel* e *maximumBandwidth.* Os demais objetos retornam valores de índices atribuídos internamente pela OLT, que são utilizados para realizar a combinação de consultas.

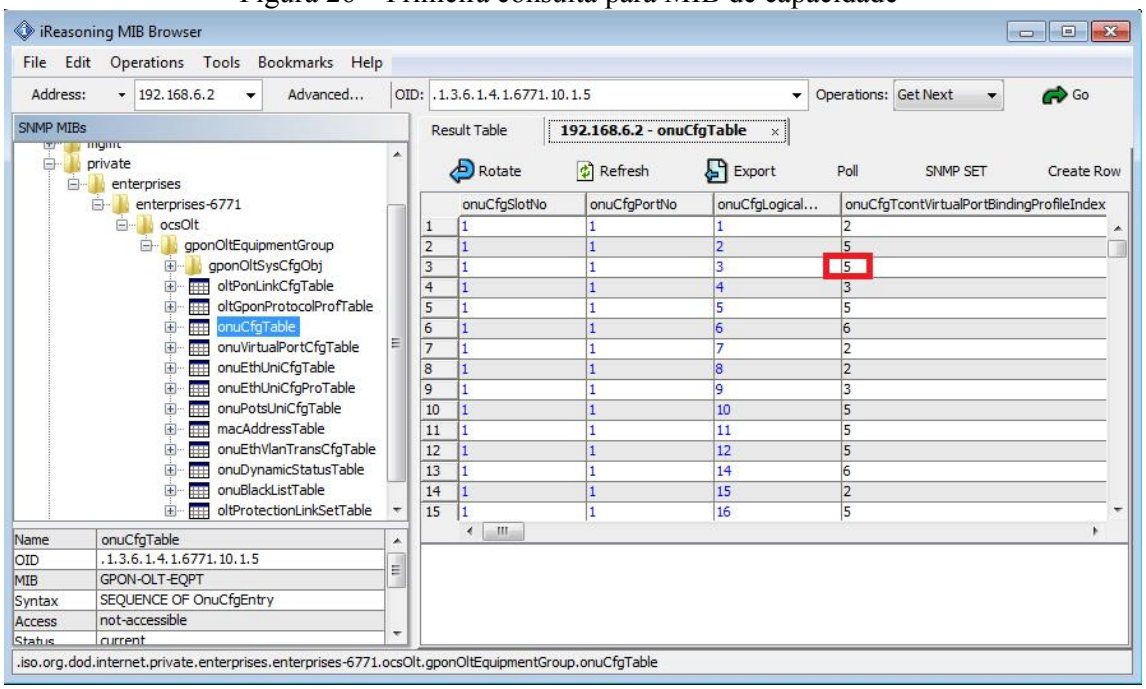
Para exemplificar a realização de uma consulta a fim de medir a capacidade de um canal de comunicação entre a OLT e uma ONU, foi realizada uma simulação para a ONU da PON 1 e posição 3 da OLT. As consultas que devem ser realizadas são, nesta ordem:

a) Consultar o valor do objeto *onuCfgTcontVirtualPortBindingProfileIndex*. Nesse caso, o valor do índice para o fluxo de tráfego ao qual pertence a ONU possui o valor 5 (Figura 26).
b) Com o valor obtido na primeira consulta, consultar o objeto *tcontVirtualPortBindingProfileIndex* contido na tabela *onuTcontVPortBindProfTable* e procurar pelo valor anotado na primeira consulta, nesse caso o valor 5. O objeto *tcontVirtualPortBindingProfileIndex* apresenta o valor 5, duplicado e isso acontece para todas as ONUs, cada uma com o seu índice. Após contato, a empresa Parks não soube informar o porquê do valor ser retornado duas vezes. Assim sendo, é necessário consultar o objeto *tcontServiceProfileIndex* correspondente ao primeiro valor 5 obtido na consulta. Nesse caso o valor retornado foi 5 (Figura 27). Esse valor é o índice armazenado internamente pela OLT para indicar o perfil de serviço ao qual pertence a ONU.
c) Com o valor anotado no passo anterior, consultar o objeto *onuTcontServiceProfileIndex* pertencente à tabela *onuTcontSvcProfTable* e localizar o valor obtido na consulta anterior. Após localizado o valor correto, consultar o objeto *upstreamBandwidthProfileIndex* correspondente. Nesse caso o valor retornado

foi 5 (Figura 28) e é referente ao índice atribuído internamente pela OLT para identificar o fluxo de tráfego ao qual a ONU pertence .

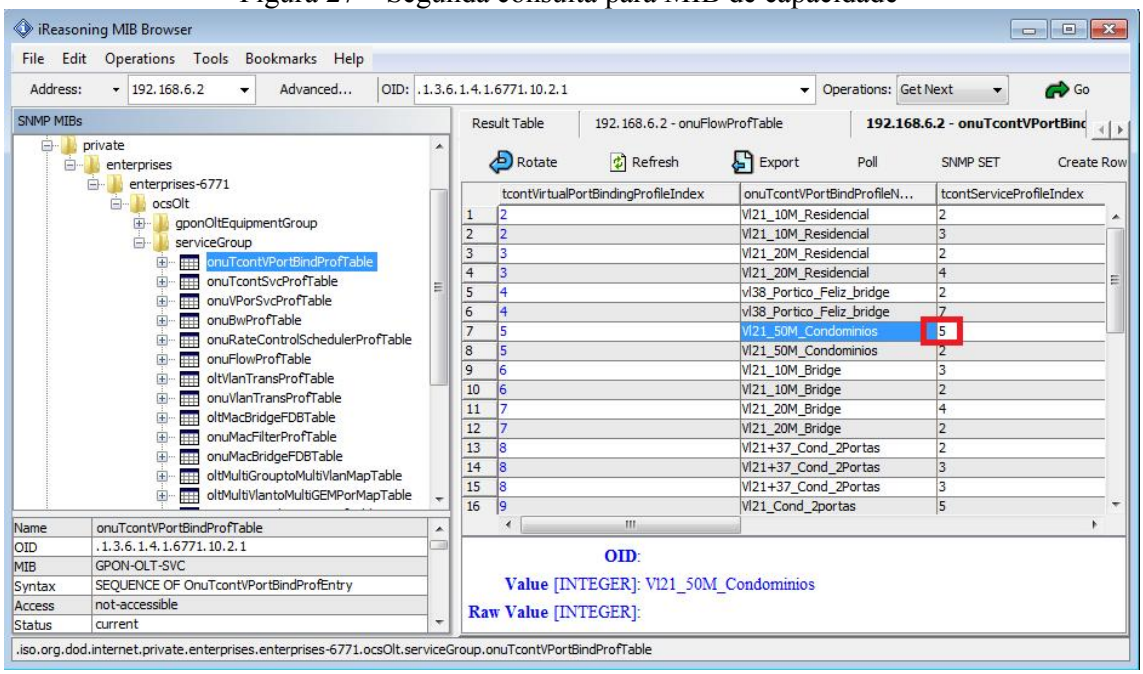
d) Por fim, consultar a tabela *onuBwProfTable*, e dentro dela identificar o valor do objeto *bandwidthProfileIndex* corresponde ao valor obtido na consulta anterior, no caso, o valor 5. Por fim, é necessário consultar o objeto *maximumBandwidth* correspondente ao valor retornado pela consulta anterior. Nesse caso o valor retornado pela consulta foi 51200 (Figura 29), que corresponde à configuração da capacidade do canal de comunicação entre a OLT e a ONU do exemplo.

Figura 26 – Primeira consulta para MIB de capacidade



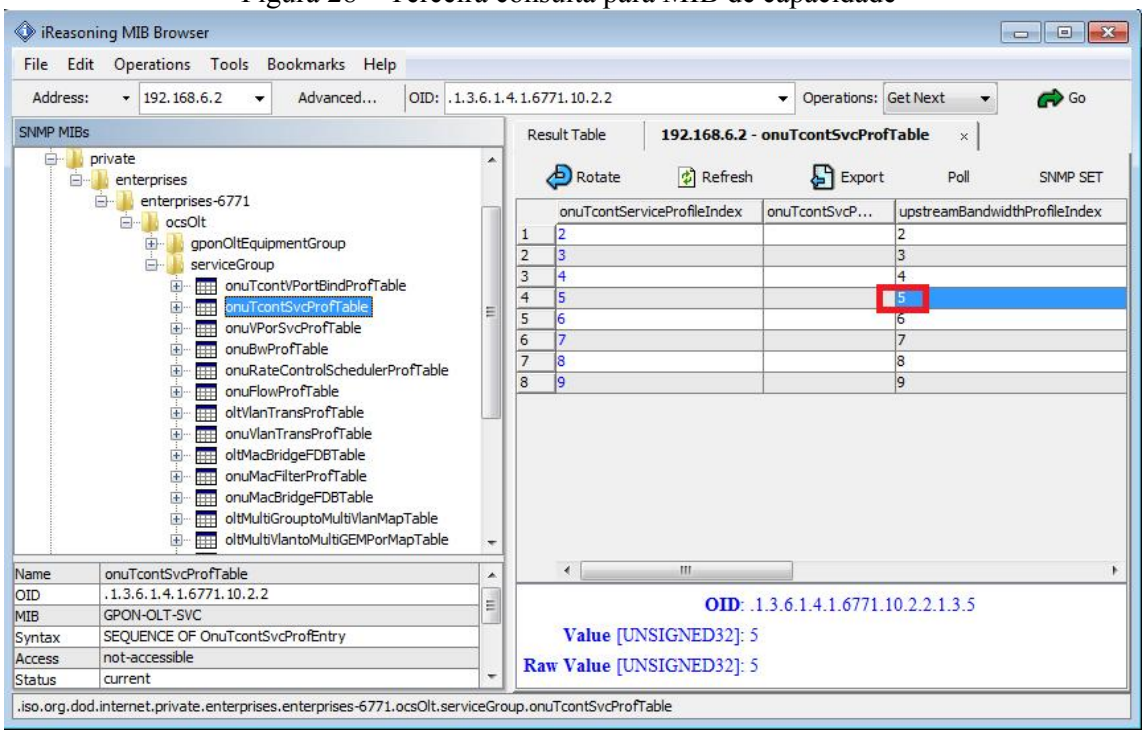
Fonte: Elaborado pelo autor.

Figura 27 – Segunda consulta para MIB de capacidade



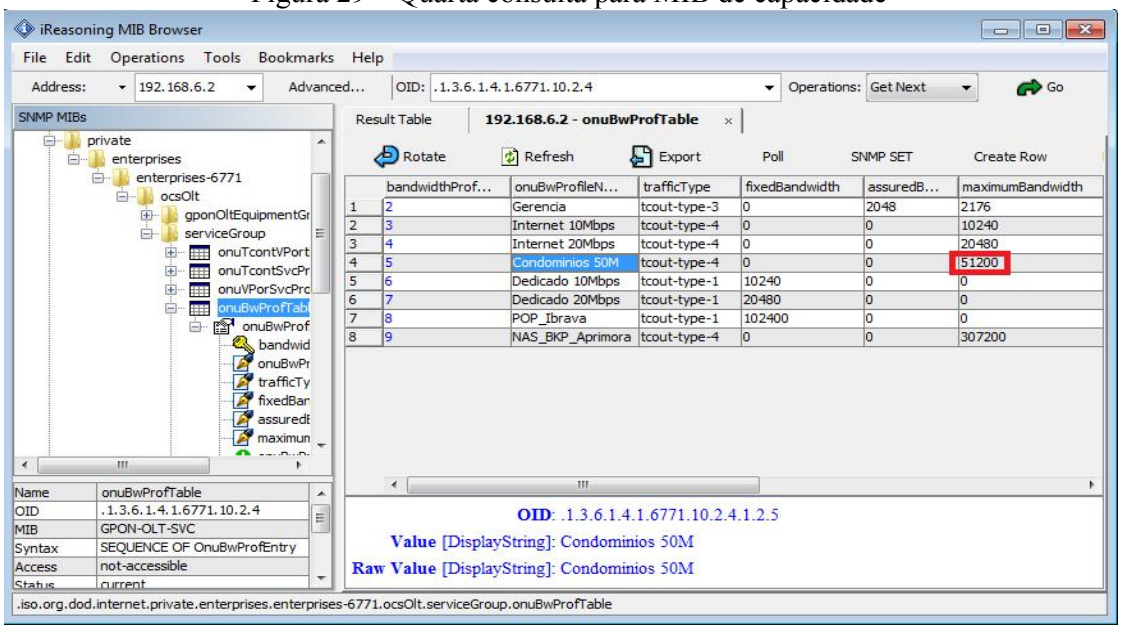
Fonte: Elaborado pelo autor.

Figura 28 – Terceira consulta para MIB de capacidade



Fonte: Elaborado pelo autor.

Figura 29 – Quarta consulta para MIB de capacidade



Fonte: Elaborado pelo autor.

O valor de capacidade de uma ONU é fixo e não deve sofrer alterações. O gráfico está sendo armazenado para emitir alertas caso a configuração de capacidade do canal de comunicação entre a OLT e uma ONU seja alterada. Esse monitoramento é realizado com o objetivo de evitar problemas de baixa largura de banda de comunicação causados por falhas de configuração.

Outra métrica desejável de ser monitorada é a vazão. Porém, de acordo com a empresa Parks, a MIB não disponibiliza essa informação até o momento. Também foi informado que a disponibilização dessa informação através de MIB não faz parte do plano de desenvolvimento da empresa. Assim sendo, não é possível monitorar essa métrica através de um gerente SNMP.

Após identificadas e testadas as MIBs e os objetos a serem monitorados, elas foram inseridas nos *softwares* de gerência SNMP para serem monitoradas. As seções seguintes explicam os *softwares* e os testes realizados.

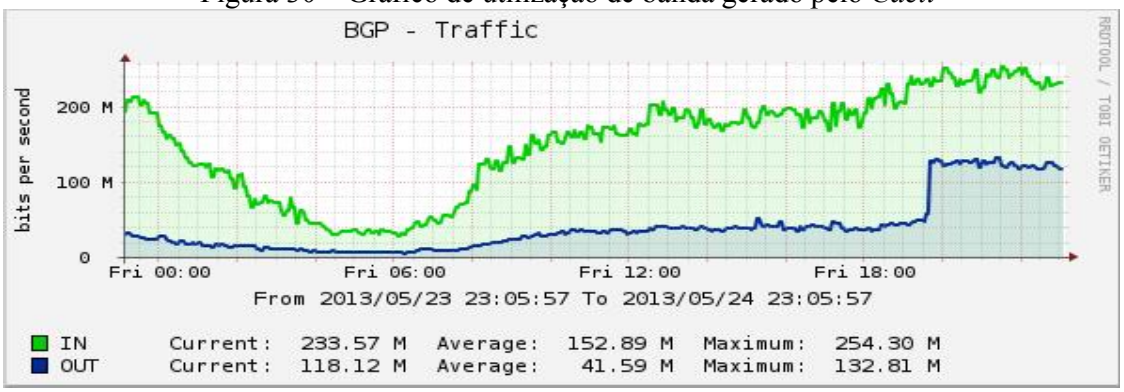
8.2 CACTI

O *Cacti* é uma *interface web* desenvolvida em PHP (*Hypertext Preprocessor*) para o RRDTOOL (*Round Robin Database*), com a capacidade de armazenar os dados em um banco *MySQL*. Através da utilização do *Cacti* é possível gerar gráficos e criar políticas de acesso às informações coletadas pelo *software* para diferentes usuários ou grupos (SANTOS, 2006).

Black (2008) explica que o RRDTOOL foi criado por *Tobias Oetiker* com a função de monitorar e armazenar dados obtidos em períodos de tempo pré-determinados. Mesmo tendo a capacidade de armazenar dados, o RRDTOOL não possibilita a geração de páginas HTML (*HyperText Markup Language*) ou gráficos, o que torna obrigatória a sua utilização associada a uma *interface web*, como o *Cacti*, por exemplo. A Figura 30 demonstra um gráfico de utilização de banda montado pelo *Cacti* baseado nas informações coletadas pelo RRDTOOL.

O *Cacti* e o RRDTOOL são distribuídos gratuitamente, sob a licença de uso GPL (*Gnu General Public License*) e estão disponíveis para *download* de forma gratuita.

Figura 30 – Gráfico de utilização de banda gerado pelo *Cacti*



Fonte: http://www.openx.com.br/2013/05/melhorando-o-visual-dos-graficos-de-trafego-no-cacti/ acesso em 03/06/14

Através da coleta de informações por SNMP, o *Cacti* possibilita gerar gráficos referentes aos mais variados parâmetros de cada equipamento, tais como memória, quantidade de processos em execução, tráfego de rede e espaço em disco, por exemplo. Atualmente o *software* suporta as três versões do protocolo SNMP, o que o torna compatível com a maioria dos equipamentos que executam o mesmo protocolo (BLACK, 2008).

A arquitetura do *software* permite a expansão através da adição de *plugins* a fim de complementar as funções desempenhadas pelo mesmo. Um exemplo de *plugin* é o PHP *Network Weathermap*, que possibilita a criação de um mapa da rede demonstrando o estado de cada elemento.

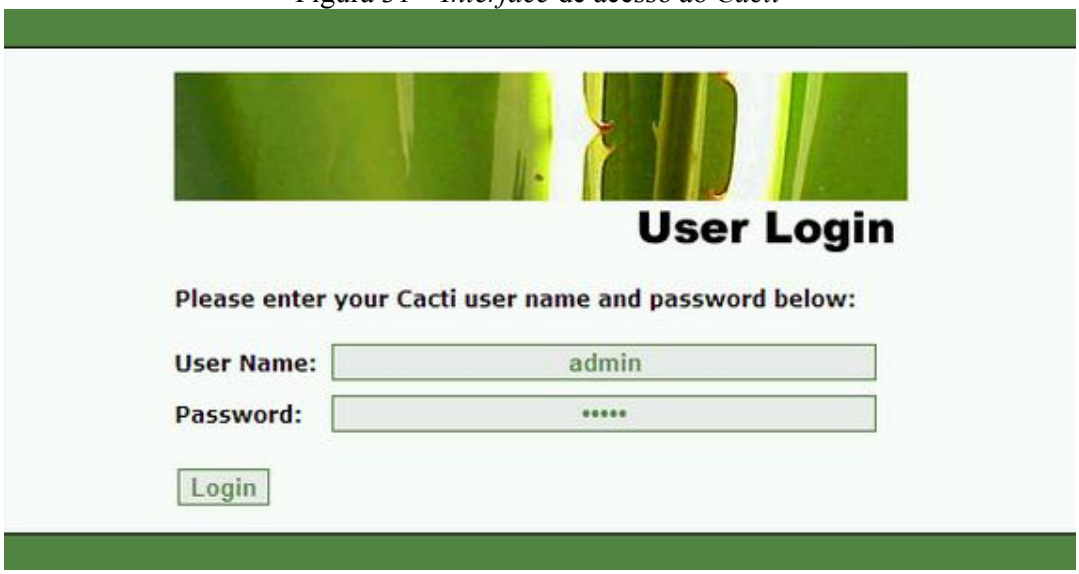
Devido ao fato de ter sido escrito em PHP e ser executado em plataforma *web*, os recursos computacionais para executar o *Cacti* não são muitos, já que a ferramenta é rápida por natureza. O desenvolvimento do *Cacti* é constante e o compartilhamento de informações sobre a ferramenta em fóruns na internet é de suma importância, visto que isso auxilia no esclarecimento de dúvidas e em situações onde ocorre um problema.

8.2.1 Instalação e Configuração do *Cacti*

A instalação do *software Cacti* foi baseada em um manual encontrado no site *Openmaniak*[4]. A instalação do *Cacti* foi feita com base no sistema operacional *Ubuntu*, versão 12.04 LTS.

A instalação do *software* consiste basicamente na instalação do pacote *Cacti*, configuração da senha do banco de dados *MySQL* e na definição do tipo de servidor *Web* utilizado pelo sistema, nesse caso o *Apache*. A Figura 31 ilustra a *interface* de acesso ao *Cacti*.

Figura 31 – *Interface* de acesso ao *Cacti*



Fonte: Elaborado pelo autor.

8.2.2 Testes Realizados

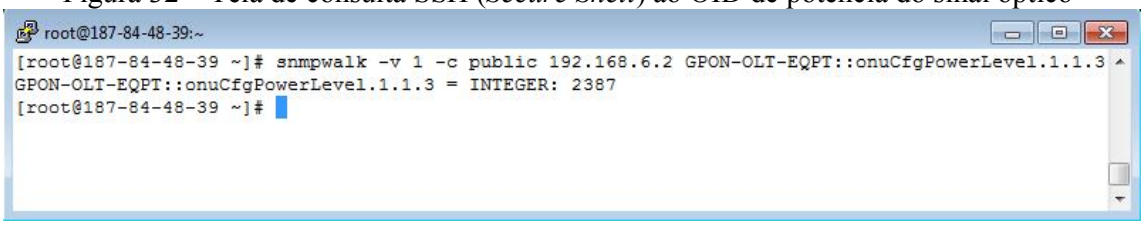
Para iniciar os testes de consulta SNMP, o primeiro passo foi adicionar os dispositivos no *Cacti*. Na tela de cadastro de *devices* foi adicionada uma OLT que será utilizada para realizar os testes. Após adicionada a OLT, o próximo passo foi importar as MIBs proprietárias fornecidas pela Parks para dentro do *software*.

Para importar as MIBs foi necessário copiar os arquivos para o diretório */usr/share/snmp/mibs/*. Após a cópia dos arquivos foi necessário reiniciar o módulo *snmpd* do *Cacti* para ativar as novas MIBs através do comando "*/etc/init.d/snmpd restart*". Após esses

[4] *http://openmaniak.com/pt/cacti_tutorial.php*

procedimentos, os testes de consulta SNMP para obtenção da leitura do sinal óptico foram efetuados com sucesso, conforme demonstra a Figura 32.

Figura 32 – Tela de consulta SSH (*Secure Shell*) ao OID de potência do sinal óptico



Fonte: Elaborado pelo autor.

Conforme explicado anteriormente, para chegar ao valor da potência óptica recebida pela ONU do assinante, é necessário combinar as consultas dos objetos *onuCfgSlotNo*, *onuCfgPortNo*, *onuCfgLogicalPortNo* e *onuCfgPowerLevel*. Para realizar a combinação desses objetos no *Cacti* é necessário criar um arquivo XML (*eXtensible Markup Language*). No *Cacti* os arquivos XML devem ser adicionados no diretório */var/www/html/resource/snmp_queries/*. Após adicionado, o arquivo necessita de permissão de execução para o usuário do *apache*, que é o usuário que executa o servidor *web* do gerente SNMP. O arquivo XML criado para a consulta do nível de potência óptica pode ser visto na Figura 33.

Figura 33 – Arquivo XML para consulta do nível de potência óptica

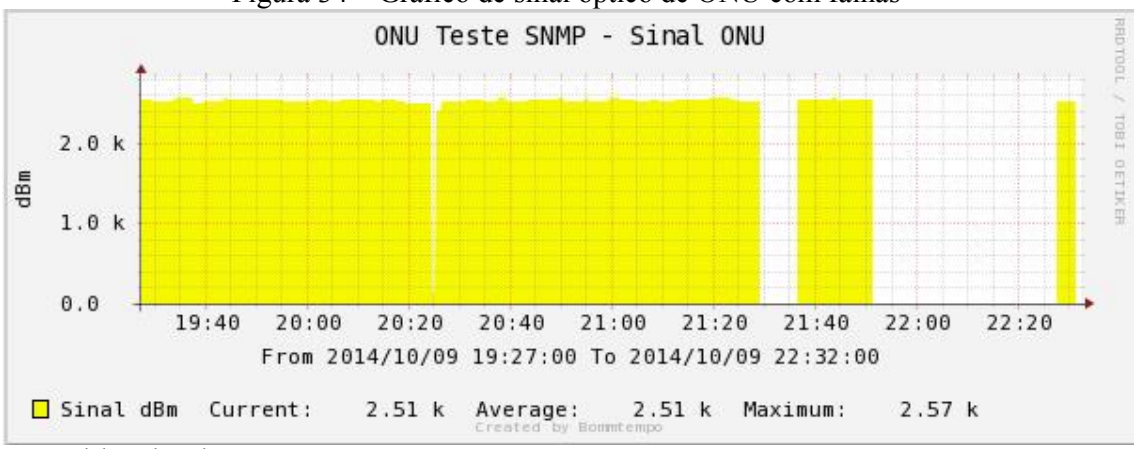
```
<interface>
        <name>Busca Potencia Optica de ONUs</name>
        <description>Atraves de SNMP realiza coleta de dados de potencia optica de ONUs</description>
        <oid_index>.1.3.6.1.4.1.6771.10.1.5.1</oid_index>
        <index_order>onuCfgPowerLevel:onuCfgSlotNo:onuCfgPortNo:onuCfgLogicalPortNo</index_order>
        <index_order_type>numeric</index_order_type>
        <fields>
                <onuCfgSlotNo>
                        <name>Device da porta PON da OLT</name>
                        <method>walk</method>
                        <source>value</source>
                        <direction>input</direction>
                        <oid>.1.3.6.1.4.1.6771.10.1.5.1.1</oid>
                </onuCfgSlotNo>
                <onuCfgPortNo>
                        <name>Numero da porta PON da OLT</name>
                        <method>walk</method>
                        <source>value</source>
                        <direction>input</direction>
                        <oid>.1.3.6.1.4.1.6771.10.1.5.1.2</oid>
                </onuCfgPortNo>
                <onuCfgLogicalPortNo>
                        <name>Device da porta PON da OLT</name>
                        <method>walk</method>
                        <source>value</source>
                        <direction>input</direction>
                        <oid>.1.3.6.1.4.1.6771.10.1.5.1.3</oid>
                </onuCfgLogicalPortNo>
                <onuCfgPowerLevel>
                        <name>Potencia do Sinal Optico</name>
                        <method>walk</method>
                        <source>value</source>
                        <direction>output</direction>
                        <oid>.1.3.6.1.4.1.6771.10.1.5.1.15</oid>
                </onuCfgPowerLevel>
        </fields>
```

Fonte: Elaborado pelo autor.

A configuração para que os valores retornados pelos gráficos fossem armazenados em gráficos foi realizada de acordo com as instruções encontradas no site de referência e suporte para o *Cacti* [5].

Ao executar os testes de coleta de dados, apesar do sucesso no retorno da consulta, o *Cacti* estava apresentando problemas no armazenamento de gráficos, onde por vezes os gráficos paravam de ser gerados sem motivo aparente. Realizando a consulta através de SSH os valores eram retornados corretamente pelo dispositivo, porém os gráficos eram armazenados com diversos cortes, como se estivessem com falhas. As falhas nos gráficos podem ser vistas na Figura 34.

Figura 34 – Gráfico de sinal óptico de ONU com falhas



Fonte: Elaborado pelo autor.

Para tentar resolver o problema encontrado foram realizadas consultas em diversos *sites* e fóruns do próprio *Cacti*. Alguns usuários dos fóruns recomendaram realizar alguns procedimentos como por exemplo, aumentar o tempo de execução do *poller*, que é um script em PHP que roda na *Cron*[6] do *Linux* e é responsável por solicitar aos agentes SNMP dos dispositivos configurados no *Cacti* as informações necessárias para realizar o monitoramento. Esse e outros diversos procedimentos foram executados, porém os gráficos não pararam de apresentar o problema identificado.

A solução encontrada foi reinstalar o *Cacti*, porém dessa vez através de uma ISO (Imagem de Sistema Operacional) pré-compilada, chamada *CactiEZ*. A versão instalada foi o *CactiEZ* 0.7[7], que possui como sistema base o *CentOS* 6.2.

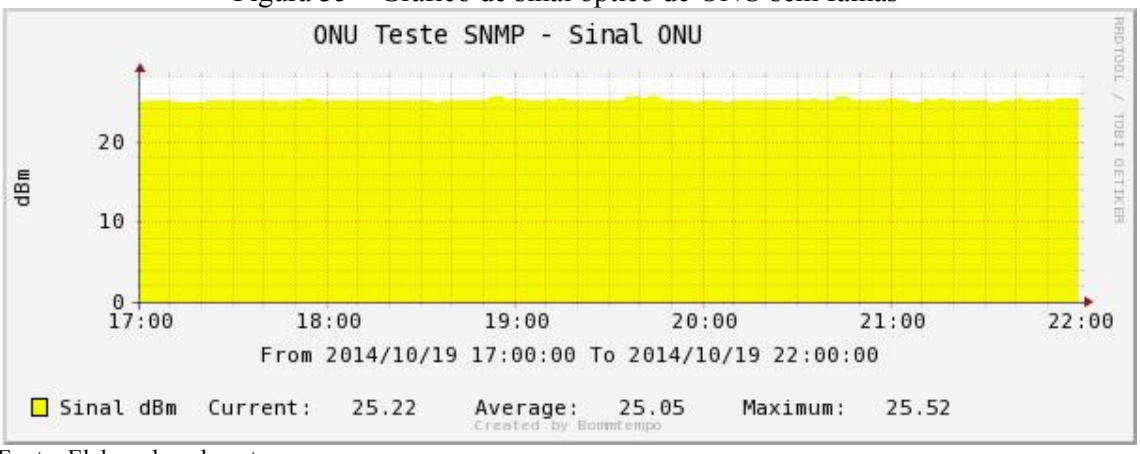
Após a instalação foram realizadas as configurações básicas do sistema e foi realizada uma nova consulta SNMP para o OID que retorna o valor da potência óptica. Os

[5] *http://docs.cacti.net/manual:087:3a_advanced_topics.3b_snmp_data_query_walkthrough*
[6] *Cron*: agendador de tarefas para o *Linux*
[7] *http://cactiez.cactiusers.org/download/*

gráficos passaram a ser apresentados da maneira correta e sem falhas, como pode ser visto na Figura 31. Conforme citado anteriormente, o retorno da consulta para o nível de potência do sinal óptico é apresentado em um número inteiro contendo quatro dígitos. Na Figura 35 a geração do gráfico foi customizada para apresentar no gráfico os valores reais, ou seja, com quatro dígitos porém com duas casas decimais. Essa configuração é realizada dentro dos *templates* de gráficos do *Cacti*, que são os modelos utilizados para a geração dos gráficos, conforme apresentado na Figura 36.

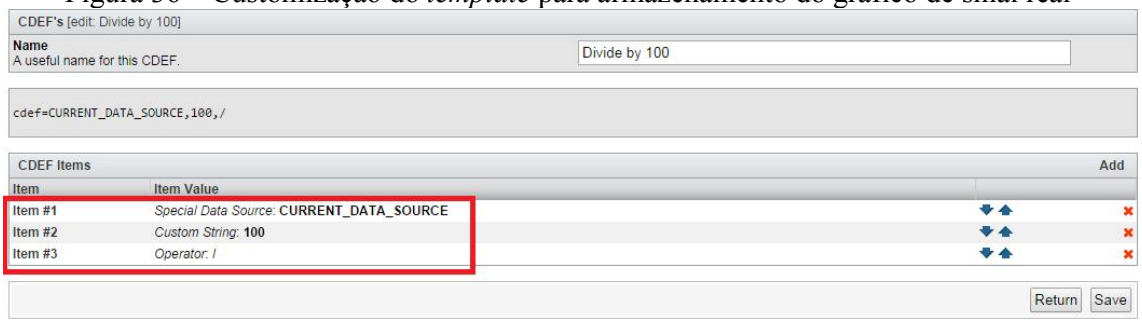
Outra vantagem observada no *CactiEZ* foi o acompanhamento de diversos *plugins*, que são componentes adicionais do sistema para realizar funções específicas, como o *Thold*, que é utilizado para enviar alertas pré-configurados para determinados serviços e o *Monitor*, que monitora a disponibilidade dos dispositivos cadastrados no sistema e emite alertas em casos de indisponibilidades.

Figura 35 – Gráfico de sinal óptico de ONU sem falhas



Fonte: Elaborado pelo autor.

Figura 36 – Customização do *template* para armazenamento do gráfico de sinal real



Fonte: Elaborado pelo autor.

Com o sistema armazenando os gráficos de forma correta, foi dada continuidade na configuração do mesmo. Para coletar os dados de capacidade do canal de comunicação entre a OLT e cada ONU, também foi necessário criar um arquivo XML para combinar as consultas

dos objetos *onuCfgTcontVirtualPortBindingProfileIndex*, *tcontServiceProfileIndex*, *upstreamBandwidthProfileIndex* e *maximumBandwidth* conforme pode ser visto na Figura 37.

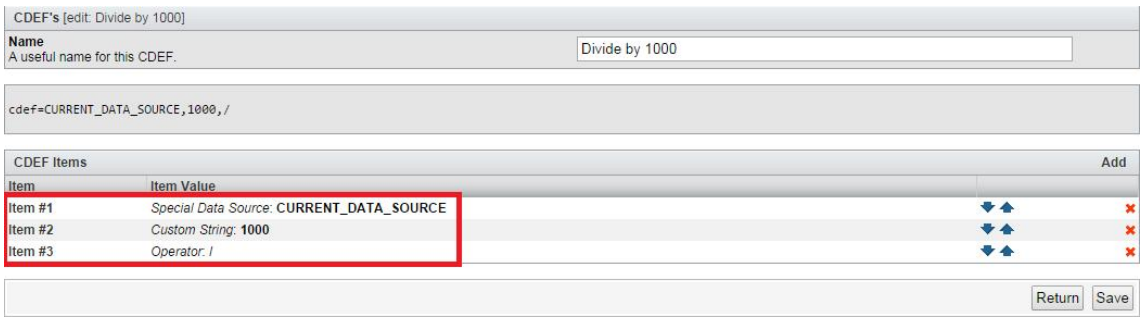
Figura 37 – Arquivo XML para consulta de capacidade

```
<interface>
        <name>Capacidade do Canal de Comunicacao entre a OLT e as ONUs</name>
        <description>Atraves de SNMP busca a capacidade do canal de comunicacao ate as ONUs</description>
        <oid_index>.1.3.6.1.4.1.6771.10</oid_index>
        <index_order>maximumBandwidth:onuCfgTcontVirtualPortBindingProfileIndex:tcontServiceProfileIndex:up
streamBandwidthProfileIndex</index_order>
        <index_order_type>numeric</index_order_type>
        <fields>
                <onuCfgTcontVirtualPortBindingProfileIndex>
                        <name>Fluxo de trafego</name>
                        <method>walk</method>
                        <source>value</source>
                        <direction>input</direction>
                        <oid>.1.3.6.1.4.1.6771.10.1.5.1.11</oid>
                <tcontVirtualPortBindingProfileIndex>
                        <name>ID do Fluxo de trafego</name>
                        <method>walk</method>
                        <source>value</source>
                        <direction>input</direction>
                        <oid>.1.3.6.1.4.1.6771.10.2.1.1.1</oid>
                </tcontVirtualPortBindingProfileIndex>
                <tcontServiceProfileIndex>
                        <name>Perfil de servico</name>
                        <method>walk</method>
                        <source>value</source>
                        <direction>input</direction>
                        <oid>.1.3.6.1.4.1.6771.10.2.1.1.6</oid>
                </tcontServiceProfileIndex>
                <onuTcontServiceProfileIndex>
                        <name>ID do Perfil de servico</name>
                        <method>walk</method>
                        <source>value</source>
                        <direction>input</direction>
                        <oid>.1.3.6.1.4.1.6771.10.2.2.1.1</oid>
                </onuTcontServiceProfileIndex>
```

Fonte: Elaborado pelo autor.

Após a criação do arquivo XML, foi realizado um teste de consulta pelo sistema para obter os gráficos de capacidade. Na consulta para a obtenção da capacidade, o valor retornado contém sempre 5 dígitos. Nesse caso o retorno para o objeto consultado foi 51200. Para o armazenamento desse gráfico foi criado um *template* que faz a divisão do valor obtido por 1000, a fim de armazenar no gráfico o valor com três casas decimais, conforme demonstrado na Figura 38.

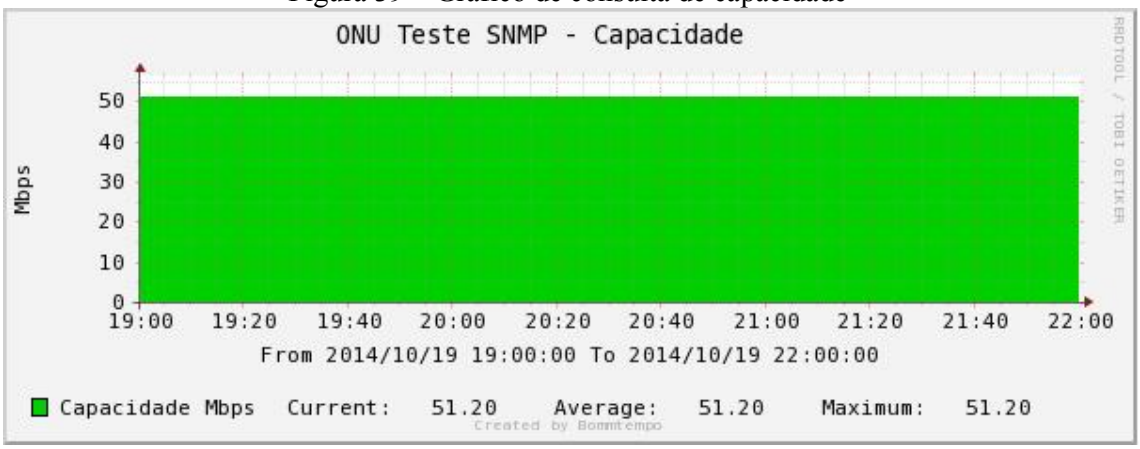
Figura 38 - Customização do *template* para armazenamento do gráfico de capacidade real



Fonte: Elaborado pelo autor.

Com o *template* configurado de forma correta, o armazenamento do gráfico de capacidade do canal de comunicação entre a OLT e uma ONU de teste pode ser visualizado através da Figura 39.

Figura 39 – Gráfico de consulta de capacidade



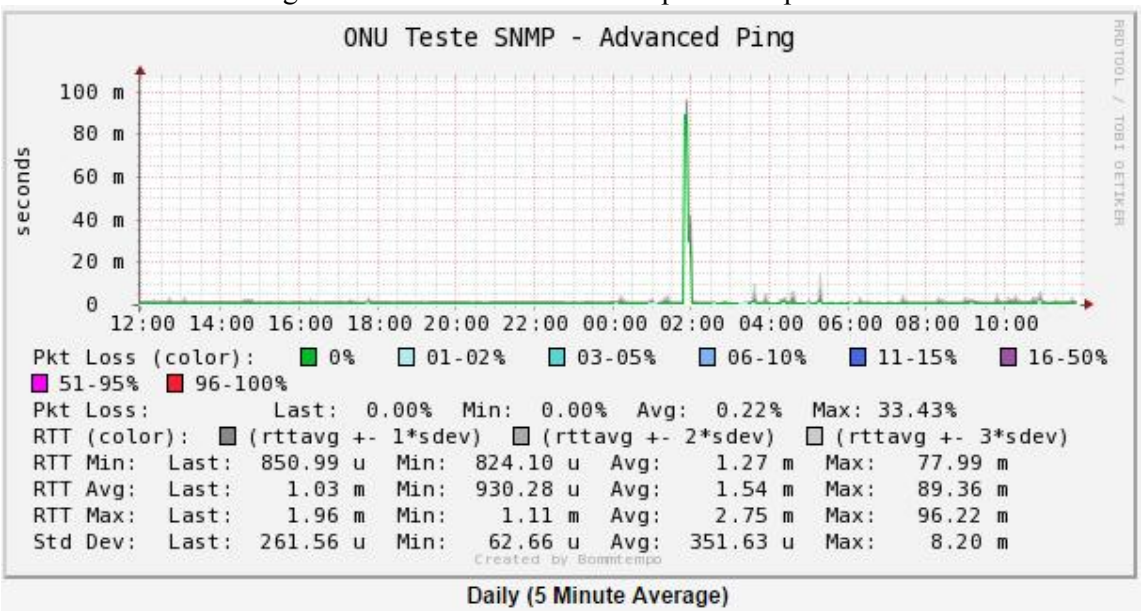
Fonte: Elaborado pelo autor.

Outras métricas de desempenho monitoradas são a latência e a perda de pacotes. Para monitorar esses valores foi instalado um *template* no *Cacti* chamado de *Advanced Ping*. O *download* do *template* foi feito do site oficial do *Cacti*[8], onde também são dadas as instruções para instalação do mesmo. Para a realização da medição de latência e perda de pacotes não foi necessário utilizar MIBs e nem SNMP pois o *software* faz essa checagem através do protocolo ICMP.

Após a instalação e configuração do *template*, foi ativado o monitoramento para uma ONU de teste, porém o gráfico não armazenava valor algum, ou seja, as consultas não retornavam nenhuma informação. Após pesquisas sobre o problema apresentado, a solução foi encontrada em um Fórum do *Cacti*[9]. O tópico apresentado orientava o usuário a instalar o pacote *php-process* para o Linux, para possibilitar então a realização da consulta. O pacote foi instalado através do comando *yum install php-process*. Após feito isso, os dados passaram a ser apresentados no gráfico, conforme pode ser visto na Figura 40.

[8] *http://docs.cacti.net/usertemplate:graph:advanced_ping_alt*
[9] *http://forums.cacti.net/viewtopic.php?f=12&t=10049&start=480*

Figura 40 – Gráfico de latência e perdas de pacotes



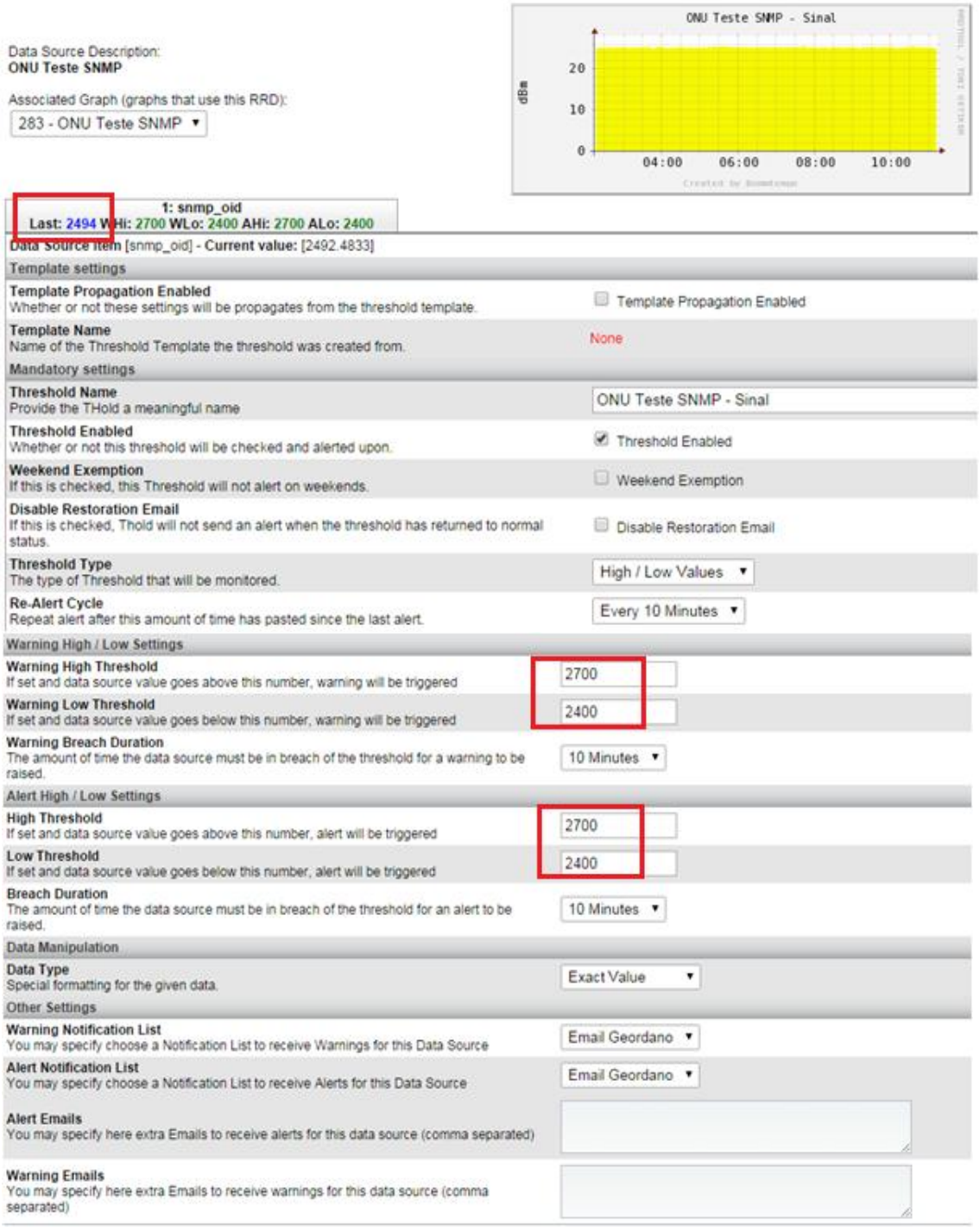
Fonte: Elaborado pelo autor.

Com a coleta de informações das métricas de desempenho configuradas, é possível ativar o monitoramento e envio de alertas dessas métricas, baseando-se sempre em valores pré-configurados.

Para ativar o monitoramento das informações coletadas pelo *Cacti*, é necessária a utilização do *plugin Thold,* que vem pré-compilado com a versão do *CactiEZ* instalada. Através desse *plugin* é possível definir qual gráfico deve ser monitorado e também os parâmetros que devem ser respeitados para o envio de alerta.

Por exemplo, para o gráfico de potência do sinal óptico, o valor lido para a ONU de teste é 2494. No exemplo da Figura 41, o parâmetro para envio de alertas está configurado para enviar *email* quando o valor lido estiver fora do intervalo entre 2400 e 2700.

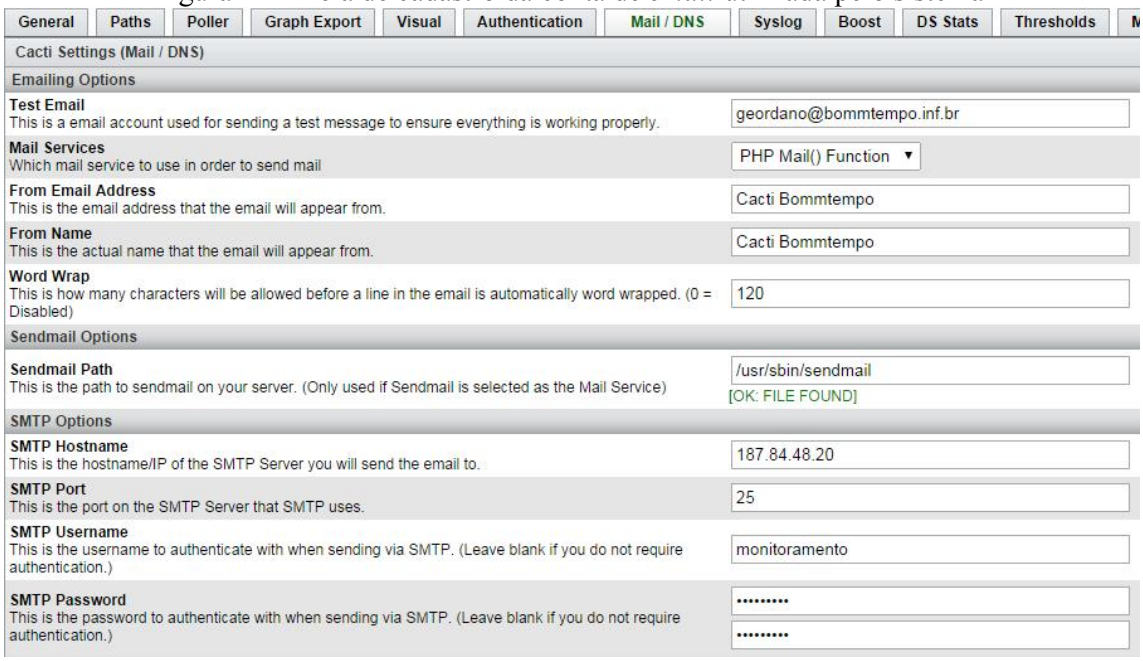
Figura 41 – Configuração da tela de monitoramento e envio de alertas



Fonte: Elaborado pelo autor.

Para enviar os *emails* de alerta, o *Cacti* necessita de um usuário e senha válidos de uma conta de *email* que esteja ativa. Neste caso foi utilizada a conta monitoramento@bommtempo.inf.br. A tela de cadastro da conta de *email* utilizada para enviar os alertas é nativa do *Cacti* e pode ser vista na Figura 42.

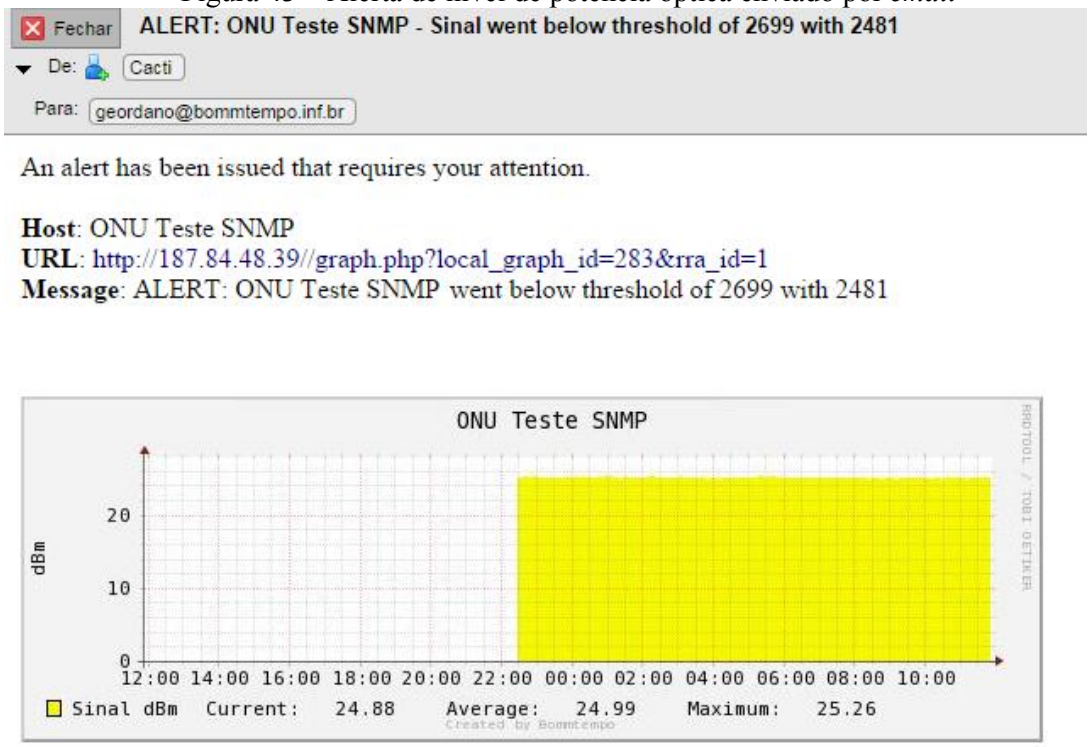
Figura 42 – Tela de cadastro da conta de *email* utilizada pelo sistema



Fonte: Elaborado pelo autor.

Na Figura 43 pode ser visto um alerta enviado por *email* devido ao nível de potência óptica estar fora do limite pré-configurado no alerta do *plugin Thold*.

Figura 43 – Alerta de nível de potência óptica enviado por *email*

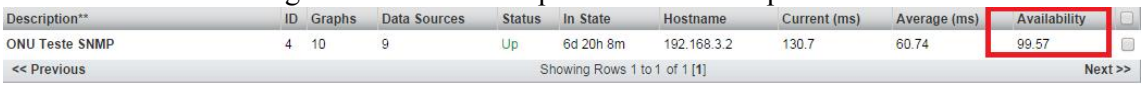


Fonte: Elaborado pelo autor.

O único tipo de alerta enviado pelo *Cacti* é o alerta por *email*. Foi realizada pesquisa sobre a implementação de envio de alerta via SMS, porém é necessário conectar um modem GSM (*Global System for Mobile Communications*) com um *chip* diretamente ao servidor onde é executado o gerente SNMP. Como o servidor é virtual, essa conexão não é possível, o que impossibilita o envio de alertas por SMS.

O *Cacti* apresenta a disponibilidade dos dispositivos na tela de *devices*, conforme demonstrado na Figura 44.

Figura 44 – Tela de disponibilidade de dispositivos



Fonte: Elaborado pelo autor.

Existem *plugins* como o *availreport*[10] e o *cereusreporting*[11] que possibilitam reportar informações de disponibilidade. O *availrepor*t exporta os valores de disponibilidade de um determinado dispositivo selecionado, mas não disponibiliza nenhuma informação referente à SLA. O *cereusreporting* na versão *Corporate* consegue reportar informações de SLA para os dispositivos da rede, porém nessa versão a ferramenta é paga. Na versão *Express*, que é gratuita, o *cereusreporting* e o *availreport* possuem as mesmas funcionalidades.

8.3 NAGIOS

O *Nagios* é um sistema de monitoramento baseado na licença GPL e possibilita monitorar servidores, aplicativos, processos, equipamentos e serviços de rede garantindo o bom funcionamento da rede em geral.

Nativamente o *Nagios* possui poucos *plugins* para gerenciamento, porém ele é uma ferramenta dinâmica e possui suporte à implementação de diversos tipos de *plugins*. Como exemplos de *plugins* podem ser citados o *Centreon*, que é uma *interface web* para o *Nagios* e o *NagVis*, que possibilita a elaboração de mapas gráficos da rede.

Segundo Becker e Moura (2012), os *plugins* são aplicativos intermediários entre o *Nagios* e os dispositivos a serem monitorados, sempre sendo utilizados para agregar funções de monitoramento ao *software* gerente.

[10] *http://docs.cacti.net/userplugin:availreport*
[11] *http://docs.cacti.net/userplugin:cereusreporting*

Os alertas gerados pelo *Nagios* em resposta a uma variação além dos parâmetros pré-definidos podem ser o envio de *email*, mensagem de texto ou uma ligação telefônica para a área responsável dizendo o nome do dispositivo que está apresentando problemas.

Apesar de possuir diversas funções, a infraestrutura de *hardware* necessária para executar o *Nagios* é pequena. Black (2008) afirma que é necessário apenas possuir um computador executando o sistema operacional *Linux* (ou variações do *Unix*) e um compilador C.

8.3.1 Instalação e Configuração do *Nagios*

A configuração do *Nagios* é baseada em arquivos. De acordo com Becker e Moura (2012), os principais arquivos de configuração do *Nagios* são:

a) *nagios.cfg*: é o arquivo principal da configuração. É nesse arquivo que são feitas as referências para os outros arquivos de configuração;
b) *cgi.cfg*: arquivo onde são configuradas as CGIs (*Common Gateway Interface*), utilizadas para dar suporte a funcionalidades extras do *Nagios*;
c) *commands.cfg*: arquivo onde são configurados os comandos possíveis de serem executados pelo *Nagios*;
d) *contacts.cfg*: arquivo onde são configurados os contatos que receberão notificações quando ocorrerem eventos que emitirem alertas. Nesse arquivo também é possível criar grupos de contatos;
e) *timeperiods.cfg*: arquivo onde se configura os períodos de monitoramento. Por exemplo, um serviço não crítico que precisa estar ativo somente em horário comercial pode ter o monitoramento desativado no final de semana, para não gerar alertas sem necessidade, já que o seu funcionamento não é vital nesse período.

Para realizar a instalação do Nagios foi utilizada uma ISO do FAN (*Fully Automated Nagios*) obtida diretamente do *site* oficial do FAN [12]. No próprio *site* de onde foi feito o *download* da ISO para instalação foi consultada também a documentação para realização da instalação.

Através da utilização da *interface web Centreon*, a utilização do *Nagios* se torna mais atrativa e agradável, substituindo inclusive a edição dos arquivos de configuração em interface de linha de comando pela edição em *interface web*. O *Centreon* é responsável por trocar informações com o *Nagios* e possibilita ao usuário configurar e visualizar tudo o que

[12] *http://www.fullyautomatednagios.org/wordpress/download/*

acontece com os dispositivos da rede através de uma *interface web*. A Figura 45 ilustra a *interface* de acesso ao *Nagios*.

Figura 45 – *Interface* de acesso ao *Nagios*

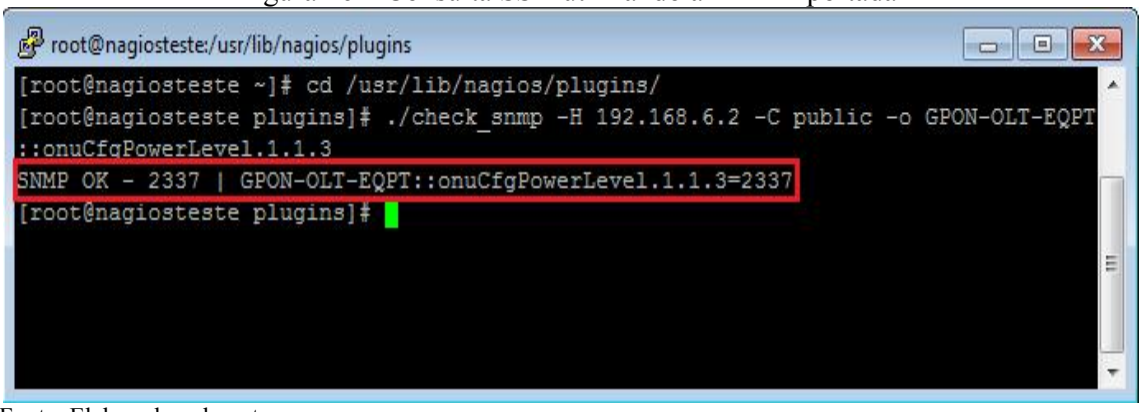
Fonte: Elaborado pelo autor.

Após a instalação do sistema operacional, foram realizados testes de monitoramento do sistema dentro da rede da Bom Tempo Telecom.

8.3.2 Testes realizados

A primeira etapa após a instalação do *software* foi adicionar os *hosts*, através do *menu* "*Configuration* > *Hosts*". Após adicionados os *hosts* de testes, foi necessário importar as MIBs proprietárias. O processo de importação das MIBs se deu através da cópia das MIBs da Parks para o diretório */usr/share/snmp/mibs*. Para testar se as MIBs estavam funcionando da maneira adequada, foi utilizado o *plugin check_snmp*, que é nativo do *Nagios*. Para executar o *plugin* primeiramente foi necessário entrar no diretório do *Nagios* onde estão contidos os *plugins* para depois executar o comando, conforme pode ser visto na Figura 46. Os parâmetros necessários para a execução do comando são o –H (endereço de ip do *host* para o qual será enviada a consulta), -C (*community* SNMP) e –o (OID que deve ser consultado).

Figura 46 – Consulta SSH utilizando a MIB importada

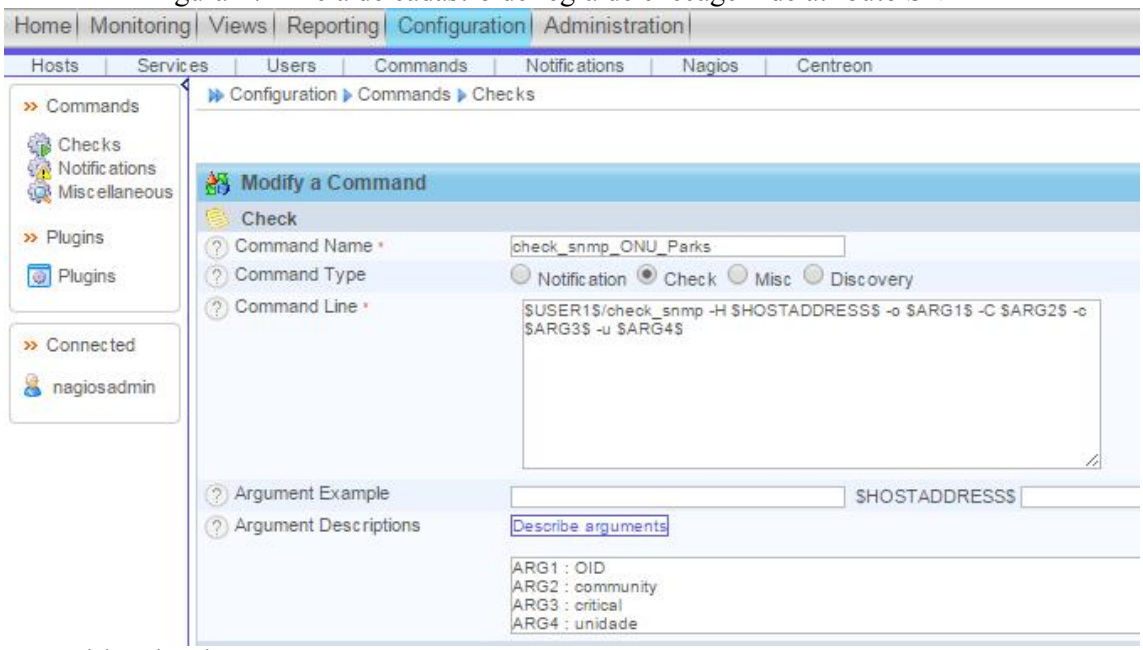


Fonte: Elaborado pelo autor.

Depois de identificado o sucesso com o teste de consulta SNMP realizado através de SSH utilizando a MIB proprietária, foi necessário realizar a configuração dos testes de monitoramento através da *interface web* do *Centreon*. Após pesquisas em fóruns e *sites* da internet, foi constatado que o *Nagios* não possui nenhum aplicativo ou *plugin* que permita a criação de gráficos de forma dinâmica e que façam a combinação de objetos em uma consulta. O usuário do *Nagios*/*Centreon* deve criar os gráficos de forma manual com o auxílio de uma ferramenta como o *Ireasoning* para navegar pelas MIBs proprietárias a fim de conseguir as informações dos OIDs dos objetos a serem consultados.

A configuração para a coleta de dados SNMP para os dispositivos cadastrados é realizada no *Centreon* através do *menu* "*Configuration* > *Services*". Ao criar um serviço, é possível selecionar um dos serviços de checagem disponibilizados de forma nativa pelo *Nagios*. Porém, antes de criar um serviço, é necessário criar uma regra de checagem, através do *menu* "*Configuration* > *Commands*", conforme pode ser visto na Figura 47. Na configuração da regra de checagem, são especificados os parâmetros –H (endereço ip do *host* a ser checado), -o (OID a ser consultado), -C (*community* SNMP) e –u (unidade que a consulta retorna).

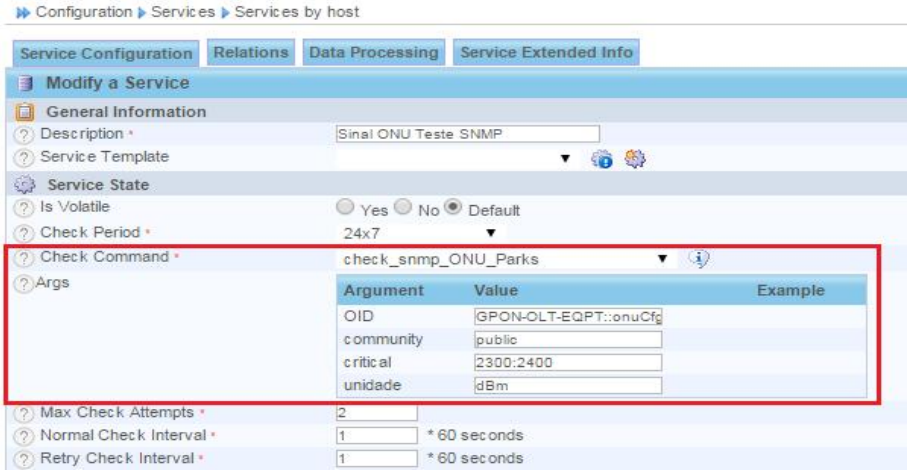
Figura 47 – Tela de cadastro de regra de checagem de atributo SNMP



Fonte: Elaborado pelo autor.

Após configurar a regra de checagem, foi configurado o serviço para o *host* a ser monitorado. Através da Figura 48 é possível visualizar a configuração realizada para monitorar o nível de sinal da ONU utilizada para testes. É possível perceber que no campo "*critical*" foi preenchido o valor "2300:2400", que é o intervalo de sinal aceito como normal para o monitoramento realizado para a ONU em teste, pois a ONU em condições normais de funcionamento retornou para a consulta SNMP o valor 2337, visualizado anteriormente na Figura 46. A unidade foi configurada com o valor "*dBm*" para especificar o tipo de informação retornada pela consulta SNMP.

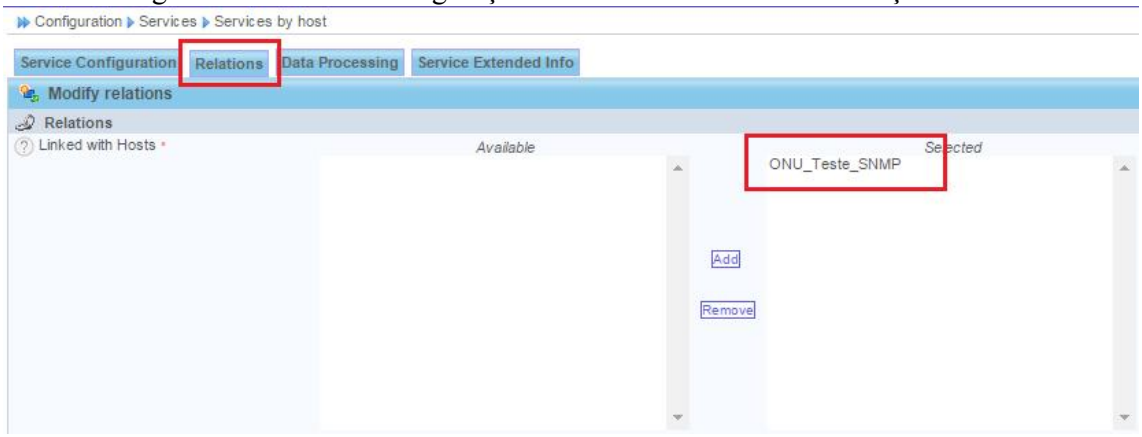
Figura 48 – Tela de cadastro de serviço para monitoramento da potência do sinal óptico



Fonte: Elaborado pelo autor.

Dentro da tela de configuração do serviço, foi necessário definir quais *hosts* são monitorados por ele através da aba "*Relations*", conforme apresentado na Figura 49. Uma vantagem da configuração baseada em relações é o fato de poder criar algum tipo de serviço uma única vez e relacionar com diversos *hosts*, sem ser necessário criar serviços iguais várias vezes.

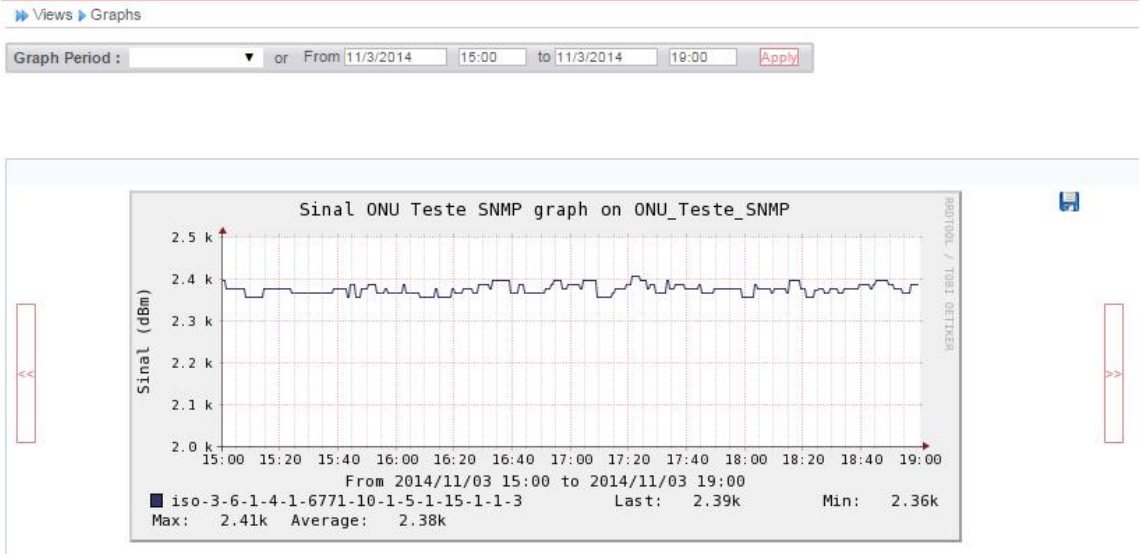
Figura 49 – Tela de configuração de relacionamento entre serviço e *hosts*



Fonte: Elaborado pelo autor.

Após configurado o serviço para a coleta dos dados de sinal óptico é possível visualizar o gráfico gerado através do *menu* "*Views* > *Graphs*" (Figura 50).

Figura 50 – Gráfico de nível de potência óptica



Fonte: Elaborado pelo autor.

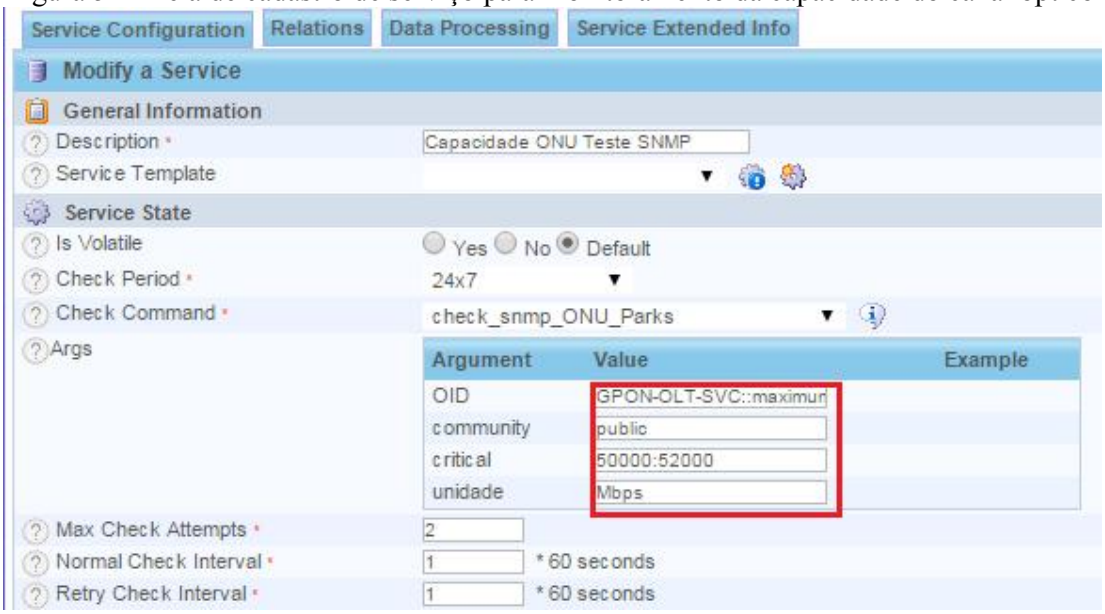
É possível observar através da Figura 50 que o último valor retornado pela consulta SNMP foi "2.39k", ou seja, 2390*dBm*. Na configuração da regra de checagem criada

anteriormente, foi utilizado o *plugin* "*check_snmp*", que não permite especificar um divisor ou multiplicador para o retorno do resultado. Por exemplo, multiplicando o valor 2390 por 0,01 o valor final seria 23,9*dBm*, que é o valor real recebido pela ONU de teste. Um *plugin* que permite a configuração de um multiplicador customizado é o "*check_centreon_snmp_value*" que também é nativo do *Nagios*, porém ele não permite configurar os alertas de forma confiável. Por exemplo, para a consulta em questão, que retornou o valor 2390, com o *check_snmp* é possível configurar que o intervalo de sinal aceitável é entre 2200 e 2600, por exemplo. Esse parâmetro é configurado no campo *critical* do serviço, na notação "sinal mais baixo permitido : sinal mais alto permitido". No exemplo citado, o campo *critical* ficaria configurado como "2200:2600". Já o *check_centreon_snmp_value* não permite configurar um intervalo de valores pois aceita apenas valores numéricos. O *caracter* que representa um intervalo entre valores é o ":" (dois pontos). Como não é aceito um intervalo de valores, é possível apenas configurar um valor como "*warning*" e um como "*critical*". Porém o valor retornado pela consulta gerará um alarme apenas se for maior do que *warning* ou *critical*. É importante que sejam gerados alertas também em caso de potência óptica inferior ao valor especificado pois evidenciam mudanças de topologia de rede que podem ter sido causadas por manutenções.

Assim sendo, através do uso do *check_snmp* os gráficos obtidos ficam com os valores inteiros e sem customização, porém os alertas ficam funcionais. O *check_centreon_snmp_value* possibilita gerar gráficos com valores customizados, porém os alertas ficam inconsistentes, sendo possível emitir alertas quando o sinal estiver menor que o especificado na regra de checagem. Assim sendo, optou-se por criar os gráficos através do *check_snmp* para obter uma maior confiabilidade nos alertas enviados.

Após configurado o gráfico que armazena o nível de potência óptica recebido pela ONU em teste, foi configurado o serviço que monitora o valor de capacidade do canal de comunicação configurado entre a OLT e a ONU. Com o auxílio do *Ireasoning* foi obtido o OID necessário e foi configurado o serviço, conforme pode ser visto na Figura 51.

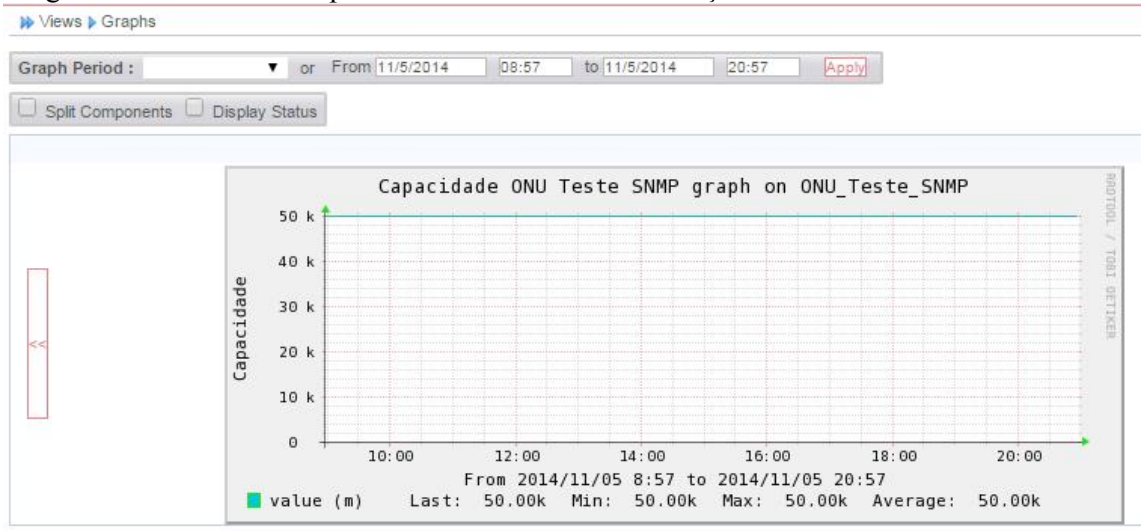
Figura 51 - Tela de cadastro de serviço para monitoramento da capacidade do canal óptico



Fonte: Elaborado pelo autor.

Após a configuração do serviço que coleta as informações de capacidade do canal de comunicação entre a OLT e a ONU de teste, foi possível verificar que o gráfico passou a ser gerado, conforme apresentado na Figura 52.

Figura 52 – Gráfico de capacidade do canal de comunicação entre a OLT e a ONU de teste

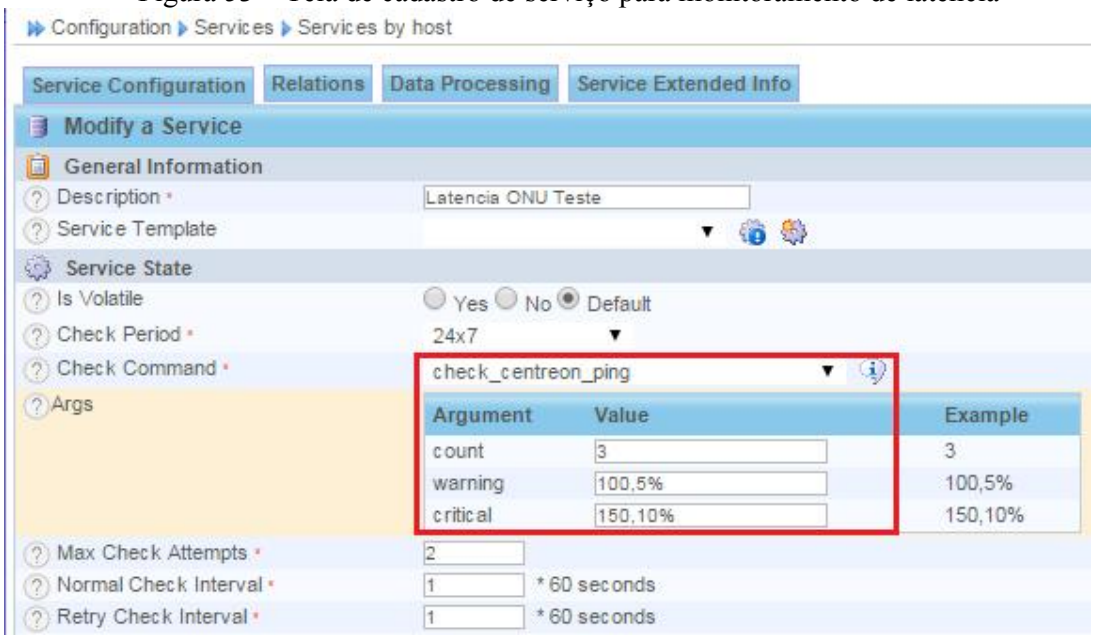


Fonte: Elaborado pelo autor.

Após configurados os serviços para o monitoramento e geração de gráficos para o nível de potência óptica e a capacidade do canal de comunicação, foi necessário configurar também os serviços para monitorar e gerar os gráficos de latência e perda de pacotes. Para

realizar a configuração do monitoramento de latência foi utilizado o *plugin* *check_centreon_ping*, que é nativo do *Centreon*. Como parâmetros para a utilização do *plugin* são configurados os campos "*count*" (especifica o número de vezes que o teste deve ser executado com falha para caracterizar uma falha no dispositivo monitorado), "*warning*" (especifica os limites aceitáveis para tempo de resposta em milisegundos e também o percentual de perda – nesse caso, 100 milisegundos e 5% de perda – antes de enviar um alarme de alerta básico) e "*critical*" (especifica os limites aceitáveis para tempo de resposta em milisegundos e também o percentual de perda – nesse caso, 150 milisegundos e 10% de perda – antes de enviar um alarme de alerta crítico). Através da Figura 53 é possível visualizar a configuração destes parâmetros.

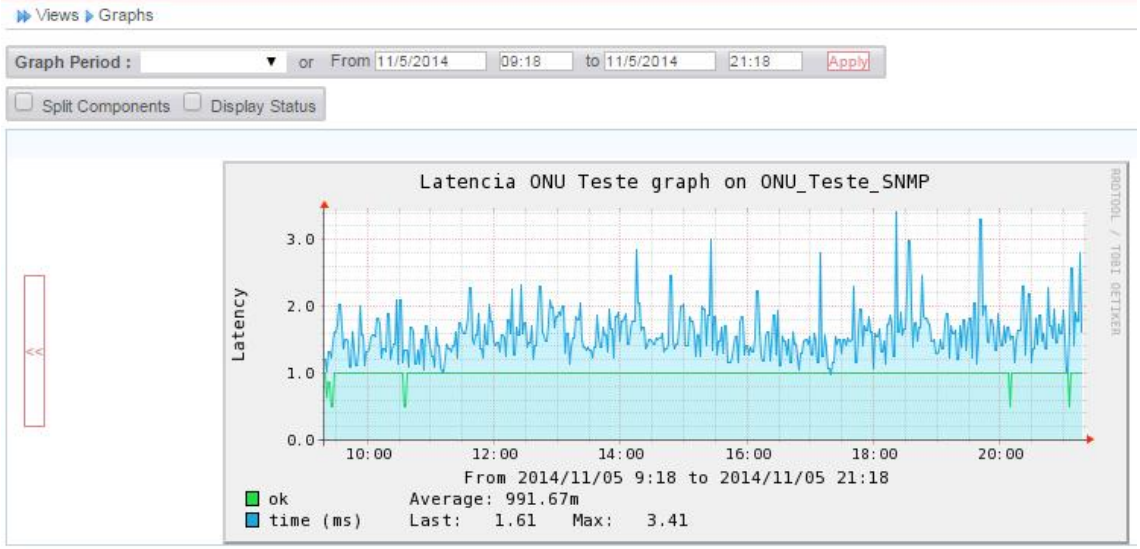
Figura 53 – Tela de cadastro de serviço para monitoramento de latência



Fonte: Elaborado pelo autor.

Após configurado o serviço para a obtenção dos dados de latência, foi possível verificar os dados sendo armazenados em gráfico, conforme pode ser visto na Figura 54.

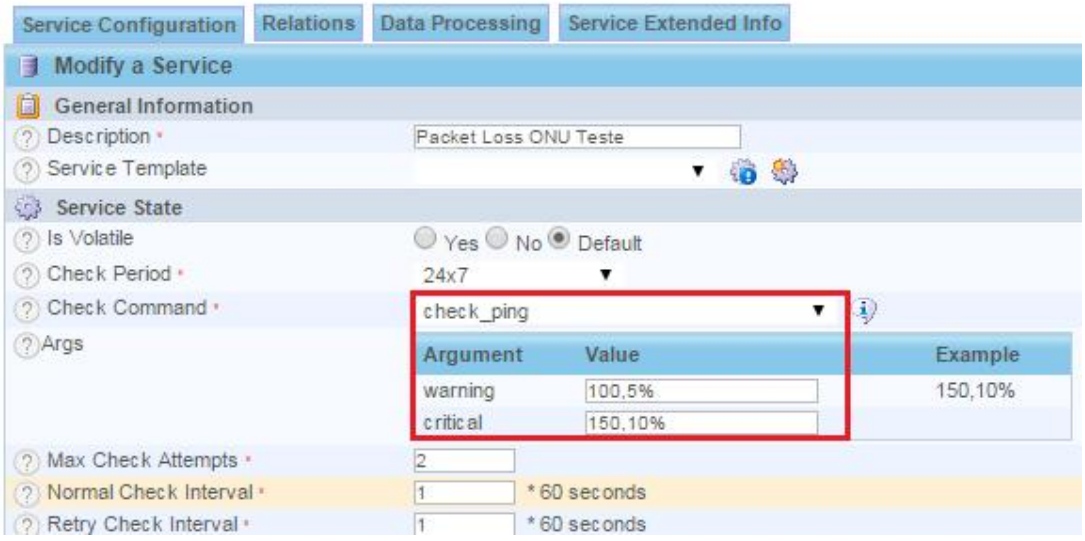
Figura 54 – Gráfico de latência



Fonte: Elaborado pelo autor.

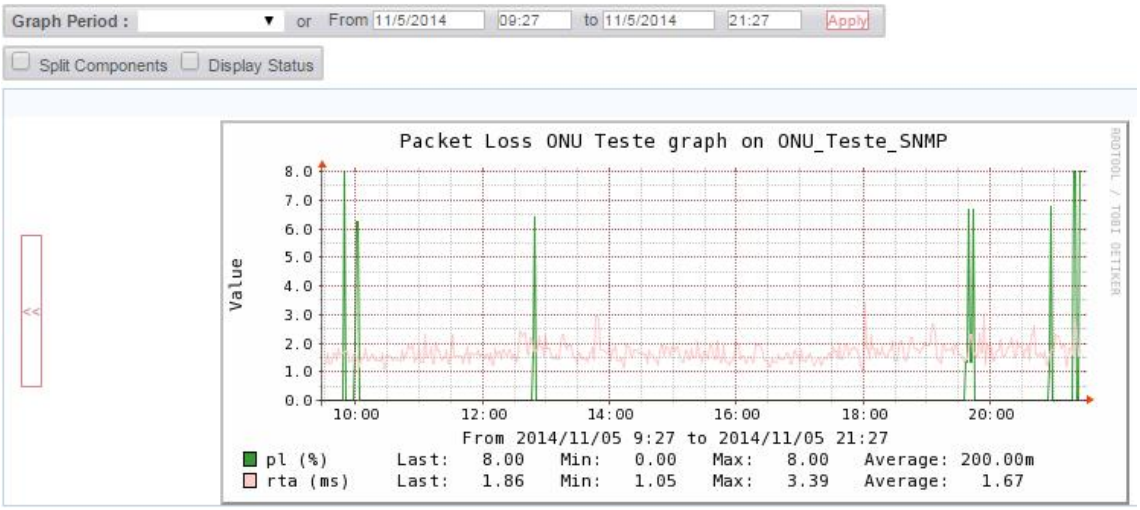
Finalizada a configuração do monitoramento de latência, foi configurado o serviço que monitora a perda de pacotes. Para configurar o serviço (Figura 55) que monitora esse indicador foi utilizado outro *plugin* nativo do *Centreon*, o *check_ping*. Não foi possível utilizar o *plugin check_centreon_ping* porque ele não insere no gráfico os dados de perdas de pacotes, mas somente a latência. Com o *check_ping* foi possível inserir os dados de perdas de pacotes no gráfico bem como registrar também a latência, conforme pode ser visto na Figura 56.

Figura 55 – Tela de cadastro de serviço para monitoramento de perda de pacotes



Fonte: Elaborado pelo autor.

Figura 56 – Gráfico de perda de pacotes



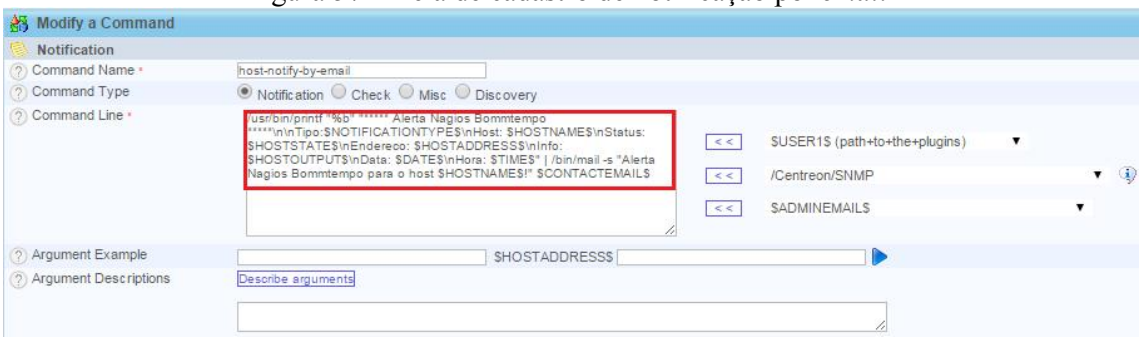
Fonte: Elaborado pelo autor.

Na Figura 56, a legenda "*pl*" significa "*packet loss*" e pode-se notar que em determinados momentos o sistema apresenta perdas de pacotes, perdas estas que o *Cacti* e o *Zabbix* não apresentaram durante o período de monitoramento. Para averiguar a confiabilidade das informações apresentadas pelo *Nagios*, foi realizado um teste de monitoramento ICMP através do *Prompt* de Comando do *Windows*, durante o mesmo período de monitoramento do gráfico gerado. O teste de monitoramento realizado manualmente não apresentou perdas de pacotes, assim como o *Cacti* e o *Zabbix*. Assim sendo, foi identificado que o teste de latência realizado e apresentado pelo *Nagios* não é consistente.

Para realizar o envio de alertas através do *Nagios*, é necessário primeiramente configurar o sistema para que ele possa enviar *emails*. O FAN vem com o servidor de *emails* *Postfix* instalado nativamente. A configuração do *Postfix* foi realizada baseado em um guia[13] encontrado no *site* do próprio FAN. Após configurado o servidor, usuário e senha utilizados para enviar os *emails*, foi necessário cadastrar um alerta por *email* dentro do servidor. Esse alerta foi configurado dentro de "*Configuration* > *Commands* > *Notifications*", e pode ser visualizado através da Figura 57.

[13] *http://www.fullyautomatednagios.org/wordpress/faq/#ii*

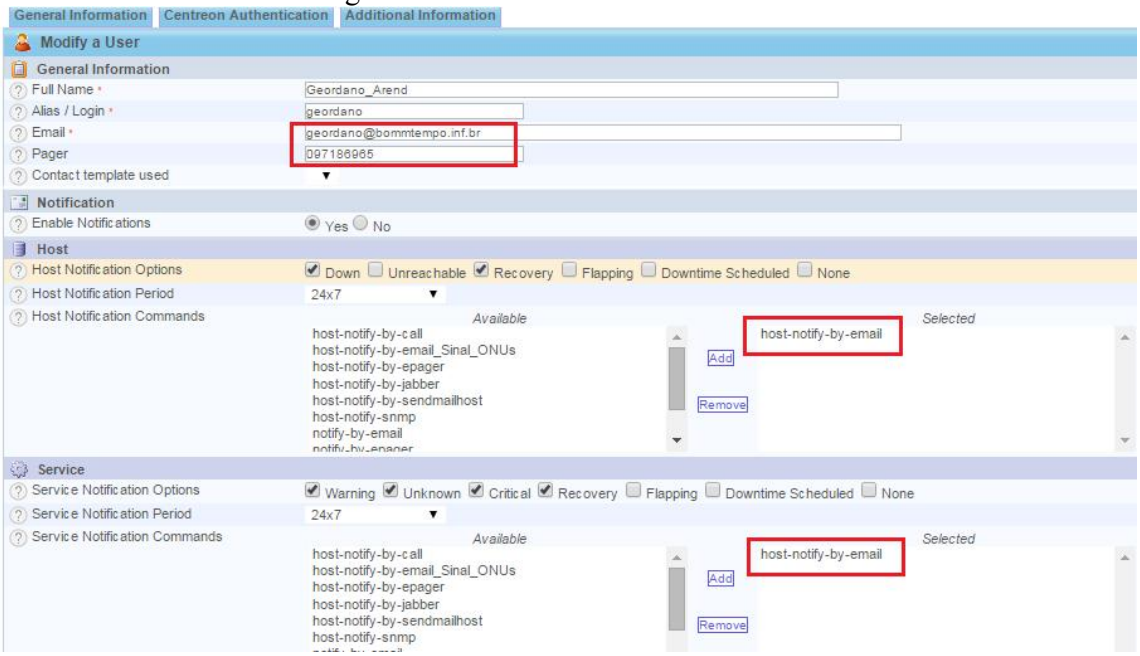
Figura 57 – Tela de cadastro de notificação por *email*



Fonte: Elaborado pelo autor.

Após configurada a notificação, foi necessário cadastrar um usuário dentro do sistema. Através da Figura 58 é possível visualizar a tela de cadastro de usuários do *Centreon*, onde pode ser definido um *email* e também um telefone.

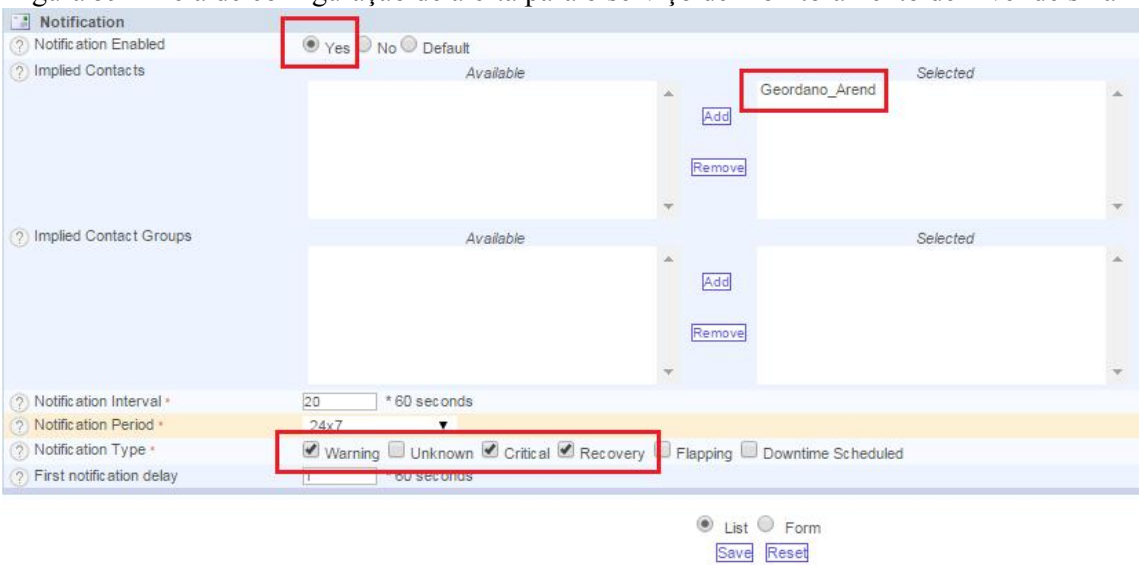
Figura 58 – Tela de cadastro de usuários



Fonte: Elaborado pelo autor.

Após cadastrado o usuário, o envio de alertas foi configurado para cada serviço monitorado. Por exemplo, a configuração de alerta para o serviço que monitora o nível de sinal recebido pela ONU em teste pode ser visualizada através da Figura 59. Para o alerta é possível configurar em quais estados de alerta o contato deve ser notificado. Nesse caso o contato será notificado quando o serviço estiver no estado "*Warning*" e "*Critical*" e também quando tiver voltado ao estado normal, caracterizado pelo estado "*Recovery*".

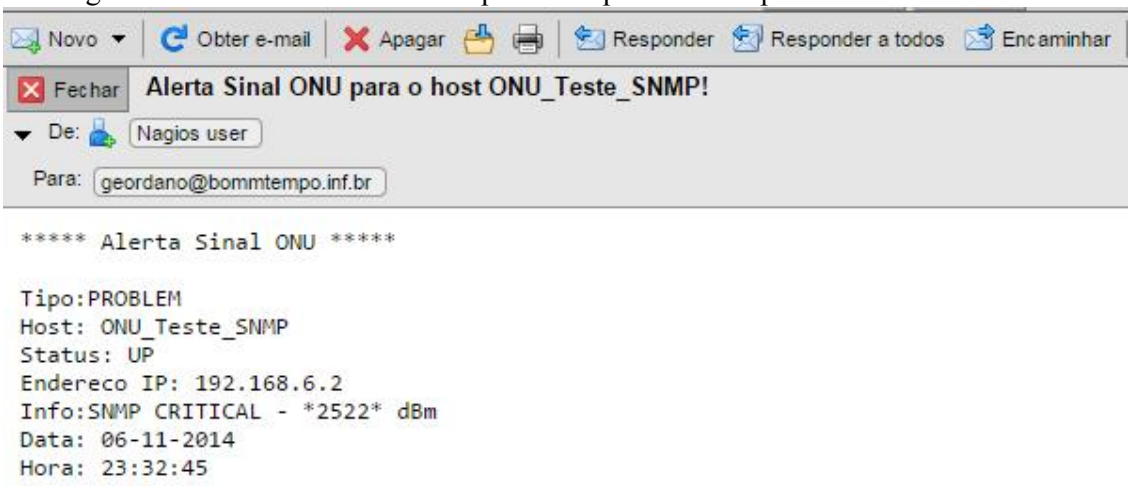
Figura 59 – Tela de configuração de alerta para o serviço de monitoramento de nível de sinal



Fonte: Elaborado pelo autor.

Após configurado o contato para receber o alerta dentro do serviço, sempre que o valor lido por SNMP no serviço que monitora o nível de sinal óptico estiver fora do limite estabelecido na configuração, neste caso fora do intervalo entre 2300 e 2400, será enviado um alerta por *email*. Através da Figura 60 é possível visualizar um alerta enviado pelo *Centreon* por *email* para o contato cadastrado.

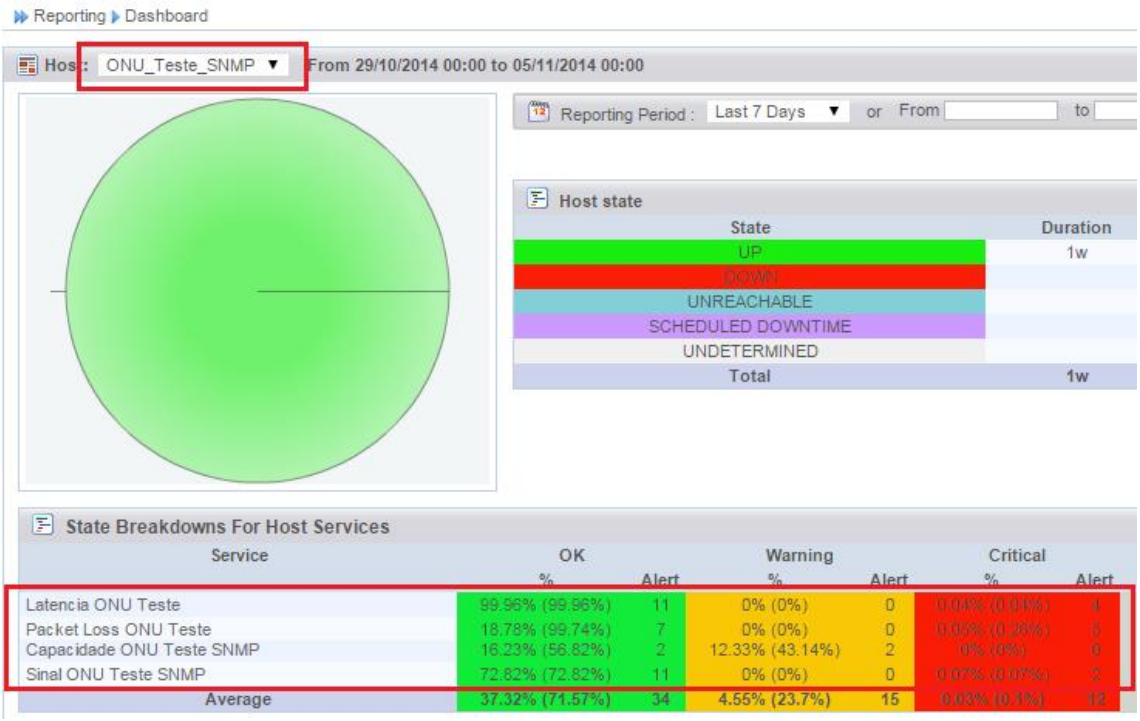
Figura 60 – Tela de alerta enviado por *email* pelo sistema para o contato cadastrado



Fonte: Elaborado pelo autor.

Para visualizar a disponibilidade de um dispositivo, o *Centreon* disponibiliza uma interface através do *menu* "*Reporting* > *Dashboard*", conforme pode ser visto na Figura 61.

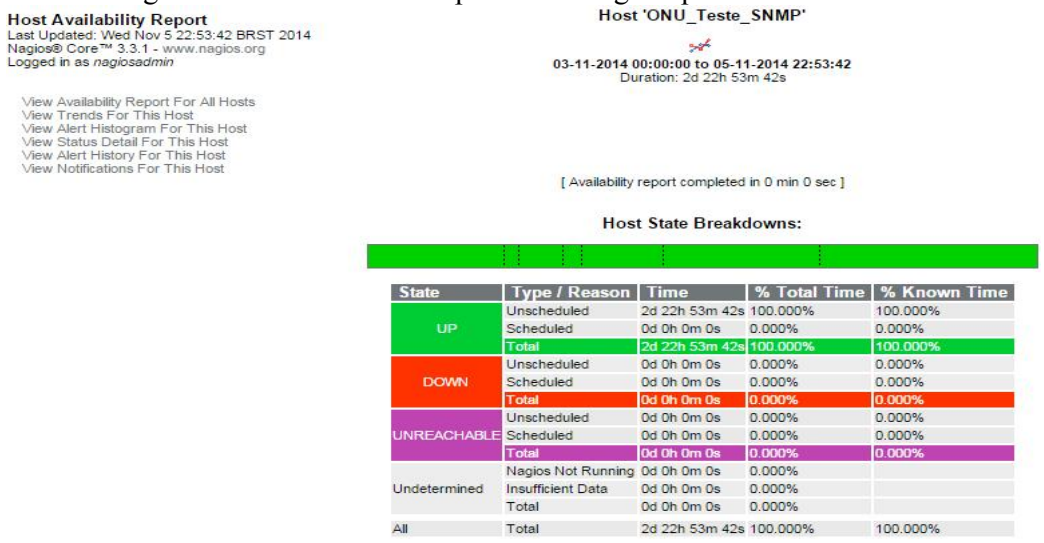
Figura 61 – Tela de disponibilidade do *Centreon*



Fonte: Elaborado pelo autor.

Além da disponibilidade apresentada através do *Centreon*, o *Nagios* também possui uma *interface web* própria, onde é possível visualizar um relatório de disponibilidade mais detalhado. Através da Figura 62 é possível visualizar o relatório de disponibilidade geral apresentado pelo *Nagios*. Além desse relatório é possível gerar relatórios separados por serviço e por *host*.

Figura 62 – Relatório de disponibilidade geral para a ONU de teste



Fonte: Elaborado pelo autor.

8.4 ZABBIX

Assim como o *Nagios* e o *Cacti*, o *Zabbix* é um *software* livre distribuído gratuitamente sob a licença de uso GPL. O *Zabbix* monitora diversos parâmetros de uma rede de computadores, bem como a integridade e operacionalidade de serviços e ativos. Os alertas enviados pelo *Zabbix* quando os limites pré-estabelecidos para um parâmetro forem ultrapassados, podem ser feitos através de envio de *emails* ou então através de envio de mensagens de texto destinadas diretamente ao setor responsável (BECKER e MOURA, 2012).

O modelo de gerenciamento utilizado pelo *Zabbix* baseado no protocolo SNMP, possibilita ter mais de um servidor executando, caracterizando redundância. Uma vez que mais de um servidor poderá coletar os dados gerados pelos agentes nos dispositivos a serem gerenciados. Os dados coletados pelo *Zabbix* são armazenados em bancos de dados, podendo ele ser *MySQL*, *PostgreSQL* ou *Oracle* (BLACK, 2008).

O *Zabbix* é um *software* que pode ser utilizado desde pequenas até médias ou grandes empresas. Os requisitos de *hardware* necessários para executarem o sistema variam proporcionalmente com o número de dispositivos monitorados. A Tabela 18 mostra os requisitos de *hardware* necessários para o *Zabbix*.

Tabela 18 – Requisitos de *hardware* aproximados para o *Zabbix*

Tipo de Rede	Plataforma	CPU/Memória	Banco de Dados	Dispositivos Monitorados
Pequena	*Ubuntu Linux 32-bit*	*Intel Pentium 350Mhz/256Mb*	*MySQL MyISAM*	20
Média	*Ubuntu Linux 64-bit*	*AMD Athlon64 3200+ / 2Gb*	*MySQL InnoDB*	500
Grande	*Ubuntu Linux 64-bit*	*Intel Dual Core 6400 / 4Gb*	*MySQL InnoDB, Oracle* ou *PostgreSQL*	>1000
Muito Grande	*Red Hat Enterprise*	*2x Intel Xeon 2Ghz / 8Gb*	*MySQL InnoDB, Oracle* ou *PostgreSQL*	>10000

Fonte: BLACK (2008)

Santos (2009), afirma que através da *interface web* centralizada do *Zabbix* é possível realizar o monitoramento em tempo real e visualizar o estado de todos os dispositivos monitorados. Os dados armazenados pelo *Zabbix* possibilitam a geração de gráficos visualmente atrativos e atualizados em tempo real.

O *Zabbix* possibilita também gerar mapas visuais da rede e dos dispositivos monitorados. Essa funcionalidade auxilia da identificação visual de falhas e dá uma idéia mais ampla da topologia de rede gerenciada.

Quando identificada uma falha, é possível enviar alertas por *email*, mensagem de texto e até mesmo através de uma ligação telefônica para notificar a área responsável sobre a indisponibilidade de um dispositivo monitorado.

De acordo com Black (2008), o *Zabbix* caracteriza-se por ser um *software* livre que conta com a possibilidade de contratação de suporte especializado. Esse suporte especializado encarrega-se de fazer atualizações no sistema, otimizações de desempenho, resolução de problemas remotamente e principalmente garantir o funcionamento do *software* em tempo integral.

8.4.1 Instalação e Configuração do *Zabbix*

A versão 2.4.1 do *Zabbix* foi instalada com base no sistema operacional *CentOS*, versão 6.5 64-*bit*. O processo de instalação foi orientado por um guia[14] encontrado no site oficial da *Zabbix* e os passos utilizados durante a instalação podem ser conferidos no Anexo 1.

Após realizar a configuração de todos os módulos e serviços necessários foi possível acessar a *interface web* do *software*. A Figura 63 demonstra a tela de acesso à *interface* do *Zabbix*.

Figura 63 – *Interface* de acesso ao *Zabbix*

Fonte: Elaborado pelo autor.

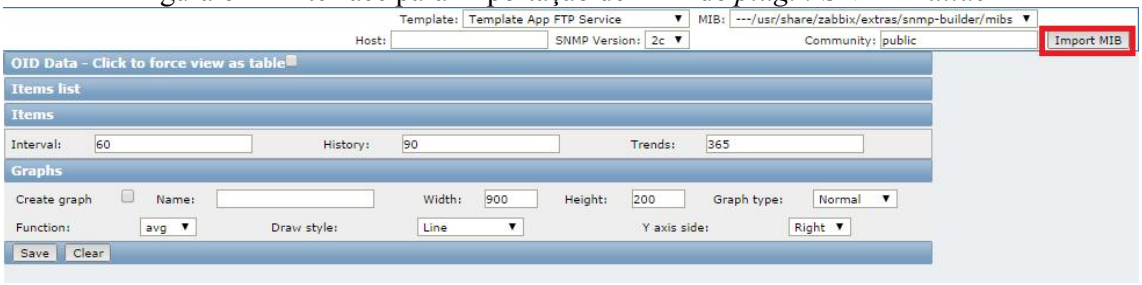
[14] *https://www.zabbix.com/documentation/2.4/manual/installation/install_from_packages*

8.4.2 Testes Realizados

Para a realização de testes com o *Zabbix* foi necessário primeiramente cadastrar os dispositivos utilizados para a realização dos testes através do *menu* "*Configuration* > *Hosts*". Após adicionados os dispositivos, foi necessário fazer a importação das MIBs. Para realizar a importação das MIBs e também a combinação de consultas para a obtenção dos valores necessários para o monitoramento desejado, foi utilizado o *plugin* "SNMP Builder". Esse *plugin* apresenta uma espécie de árvore da MIB na tela do sistema e tem o intuito de possibilitar a criação de gráficos clicando em cima dos objetos.

A instalação do *plugin* SNMP *Builder* foi realizada através da utilização de um guia[15]. Após instalado, o primeiro passo foi executar a importação das MIBs da Parks. A importação foi realizada através de um botão "*Import* MIB", que faz parte do *plugin* SNMP *Builder*, conforme pode ser visto na Figura 64. Ao clicar no botão, é possível selecionar a MIB a ser importada do computador pessoal do usuário. As MIBs importadas são armazenadas no diretório */usr/share/zabbix/extras/snmp-builder/mibs*, juntamente com outras MIBs que já vem armazenadas por padrão no sistema.

Figura 64 – Interface para importação de MIB do *plugin* SNMP *Builder*

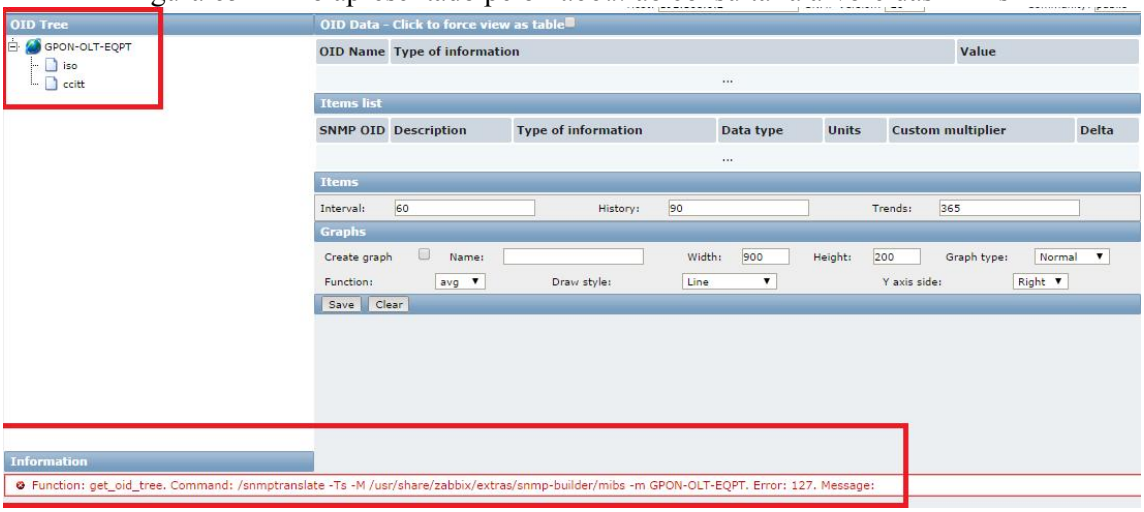


Fonte: Elaborado pelo autor.

Após instalado, o pacote SMP *Builder* apresentava um erro, conforme pode ser visto na Figura 65, fazendo com que a árvore da MIB não fosse apresentada.

[15] *http://spinola.net.br/blog/?p=544*

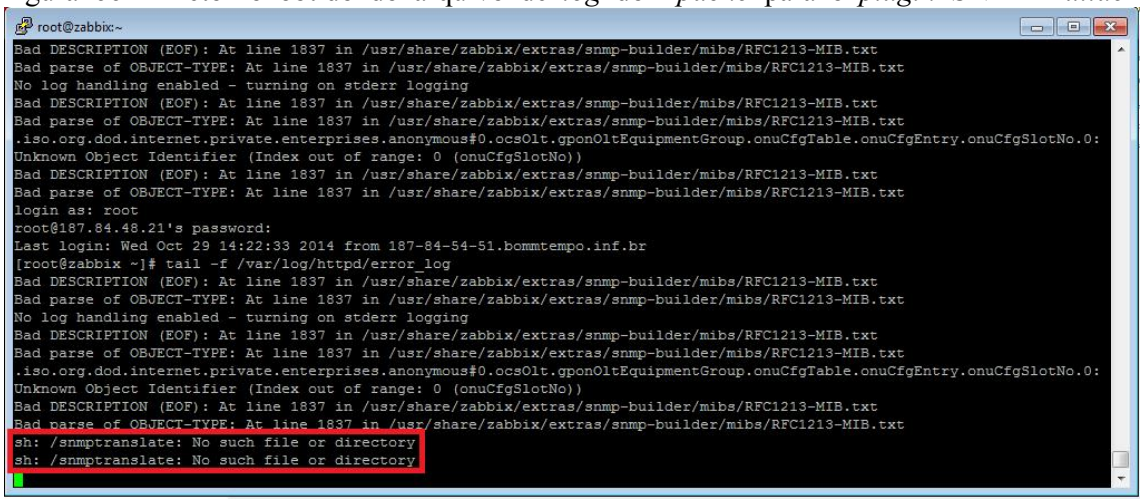
Figura 65 – Erro apresentado pelo *Zabbix* ao consultar a árvore das MIBs



Fonte: Elaborado pelo autor.

Para solucionar esse problema, o servidor do *Zabbix* foi acessado via SSH e foi executada a linha de comando "*tail -f /var/log/httpd/error_log*" que faz com que o sistema apresente os *logs* do *Apache* em tempo real na tela. O retorno obtido na tela apresentava erro de sintaxe no comando "*snmptranslate*", conforme Figura 66.

Figura 66 – Retorno obtido do arquivo de *log* do *Apache* para o *plugin* SNMP *Builder*

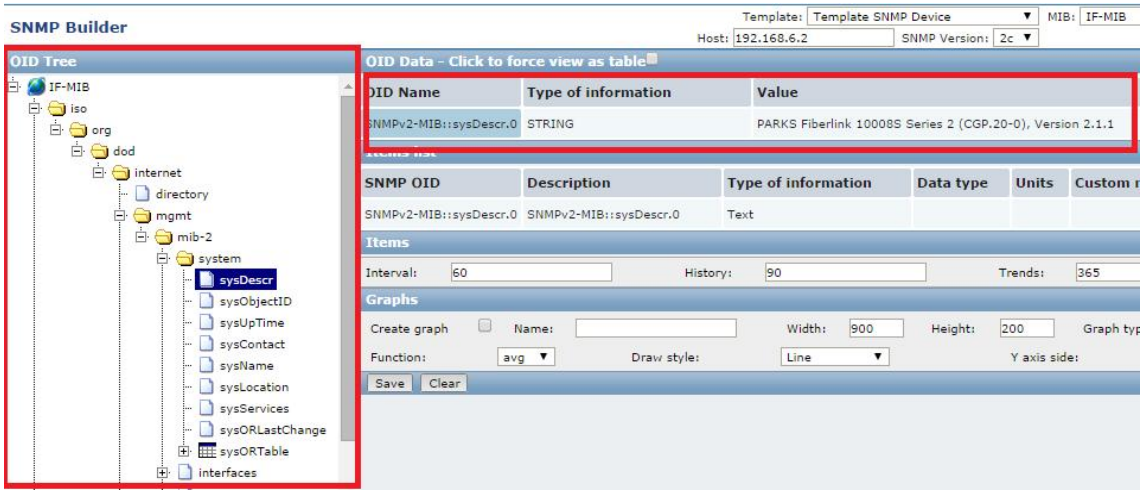


Fonte: Elaborado pelo autor.

A solução para o problema não foi encontrada através das pesquisas realizadas em *sites* e fóruns. Ao revisar o arquivo "*zbxe-snmp-builder.php*", encontrado dentro do diretório */usr/share/zabbix* foi constatado que as chamadas para o comando *snmptranslate* dentro do arquivo estavam com um *caracter* "/" antes do comando, o que fazia com que o sistema não conseguisse identificar o comando. Após removido o *caracter* à frente do comando, o *plugin*

SNMP *Builder* passou a conseguir acessar as árvores das MIBs, conforme pode ser visto na Figura 67.

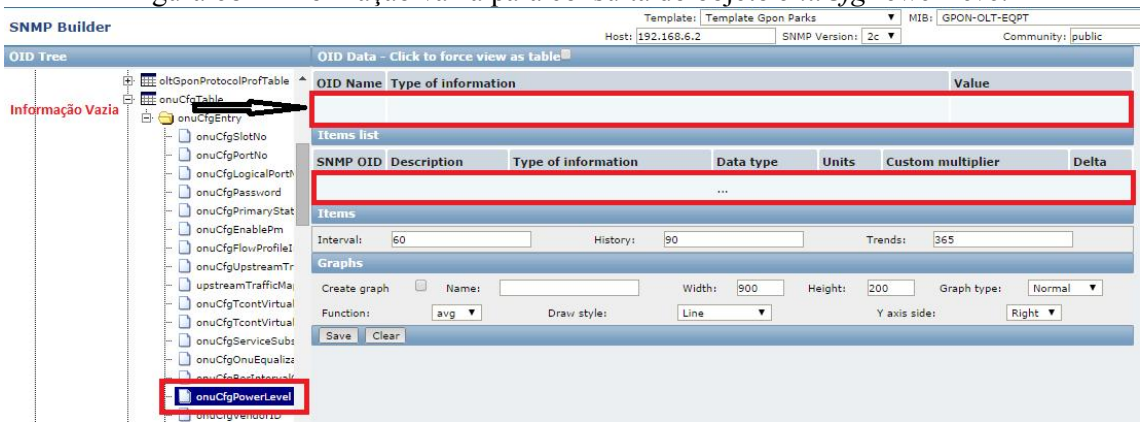
Figura 67 – Acesso à arvore de MIBs através do *plugin* SNMP *Builder*



Fonte: Elaborado pelo autor.

Com o *plugin* conseguindo acessar as árvores de MIBs, foi realizado um teste de consulta para o objeto *onuCfgPowerLevel* da tabela *onuCfgTable*, pertencente à MIB GPON-OLT-EQPT. O retorno da consulta SNMP para o objeto ficou em branco, ou seja, sem nenhuma informação, conforme pode ser visto na Figura 68.

Figura 68 – Informação vazia para consulta do objeto *onuCfgPowerLevel*

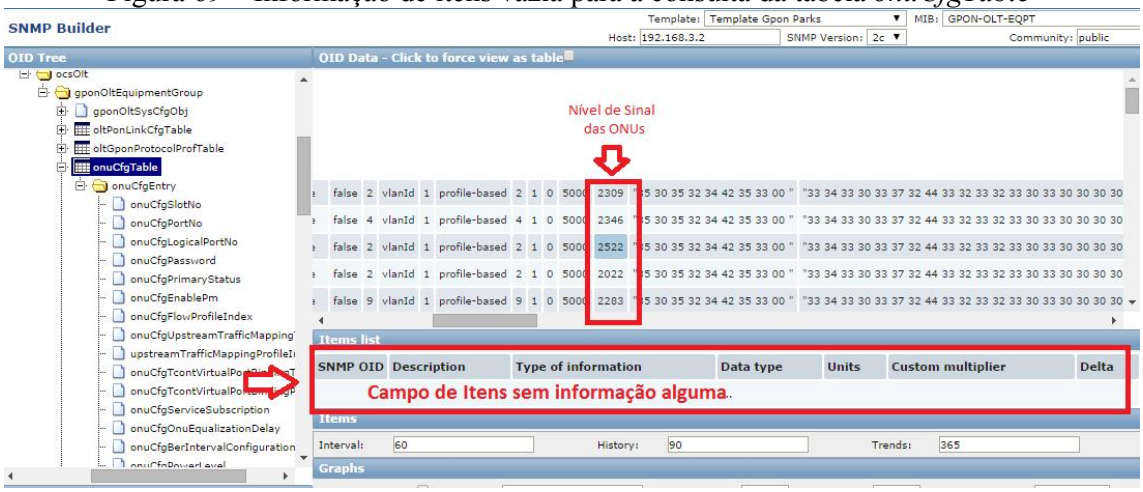


Fonte: Elaborado pelo autor.

Ao realizar a consulta para a tabela *onuCfgTable*, as informações são apresentadas no SNMP *Builder*, conforme pode ser visto na Figura 69. Porém não é possível criar gráficos a partir delas pois o campo de itens ficou sem nenhuma informação, diferentemente da consulta

utilizando a MIB padrão *IF-MIB*, da Figura 67, onde é possível visualizar o preenchimento do campo de itens, o que possibilita a criação de gráficos a partir dessa consulta.

Figura 69 – Informação de itens vazia para a consulta da tabela *onuCfgTable*

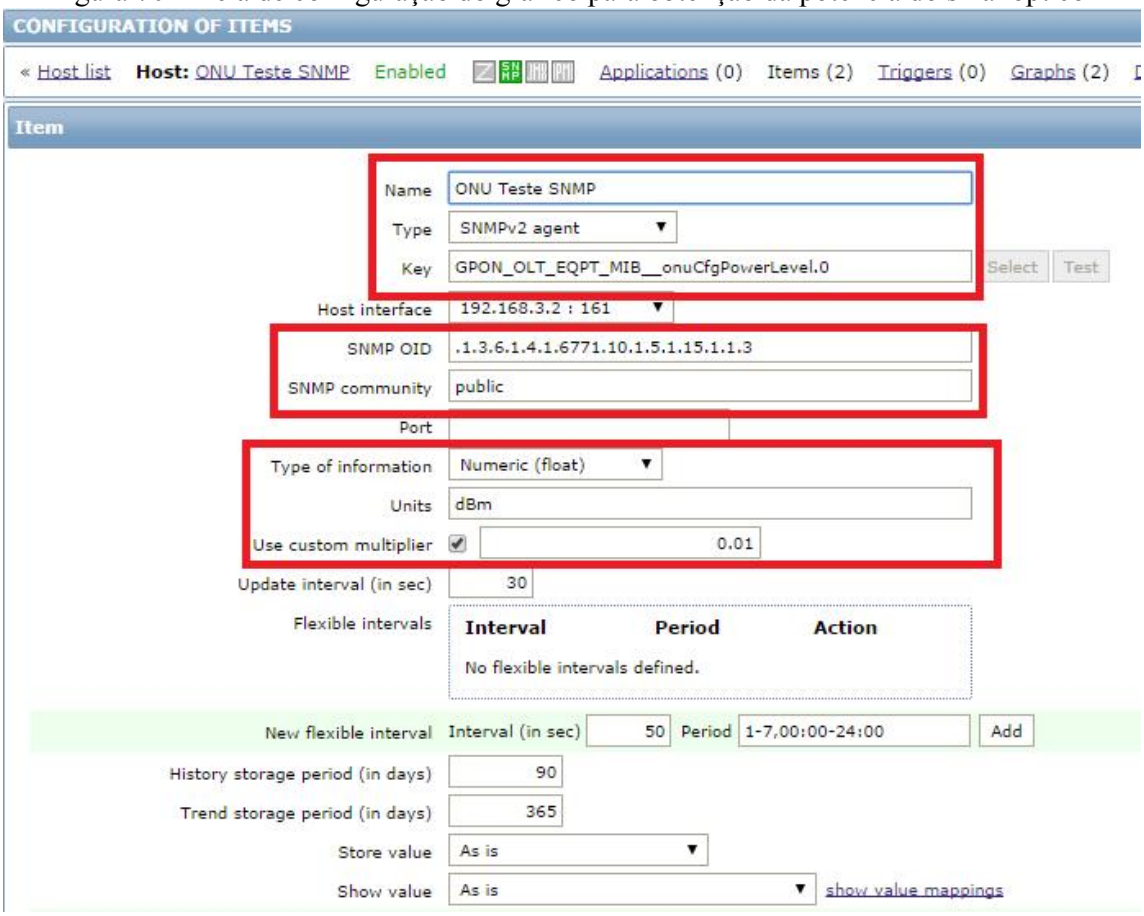


Fonte: Elaborado pelo autor.

Baseado nos testes realizados, foi possível concluir que não é possível realizar os testes de consultas SNMP com combinação de objetos no *Zabbix*. Para realizar o armazenamento dos gráficos para diferentes ONUs, é necessária a utilização de uma ferramenta de apoio para realizar as consultas da MIB da Parks, como o *Ireasoning* por exemplo.

Utilizando o *Ireasoning* foram configurados os objetos para a obtenção do nível de potência do sinal óptico da ONU utilizada para testes. A Figura 70 demonstra a configuração dos parâmetros *Name* (nome da ONU), *Type* (tipo de consulta), *Key* (identificador do objeto a ser consultado), SNMP OID (OID numérico correspondente ao objeto a ser consultado), SNMP *community* (comunidade SNMP utilizada para realizar a consulta), *Type of information* (tipo de unidade de medida retornada pela consulta), *Units* (nome de unidade que aparece no gráfico) e *Use custom multiplier* (número pelo qual o retorno da consulta deve ser multiplicado antes de ser armazenado no gráfico). Os demais campos configuráveis ficaram configurados com os valores padrão do *Zabbix*.

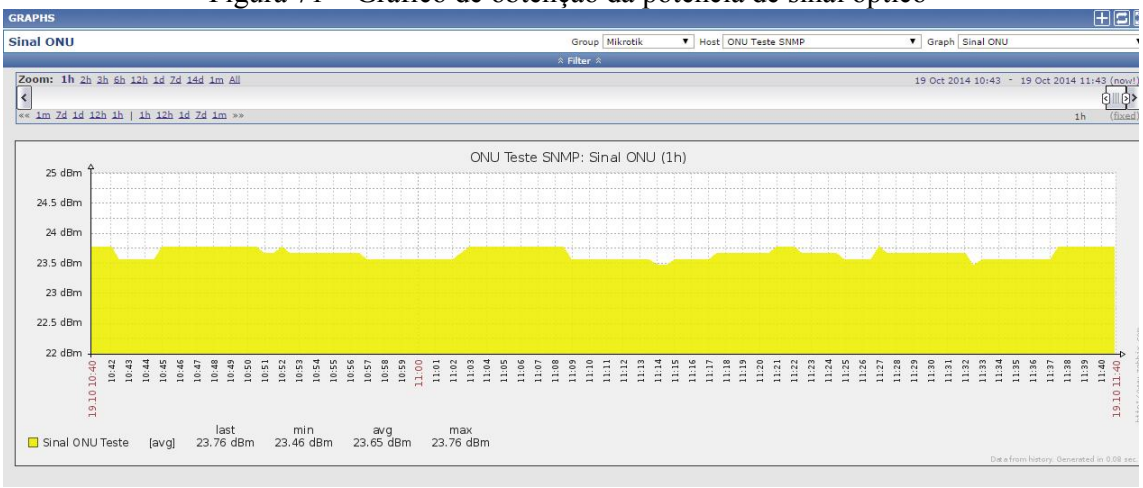
Figura 70 – Tela de configuração do gráfico para obtenção da potência do sinal óptico



Fonte: Elaborado pelo autor.

Baseado nessa configuração, através da Figura 71 é possível visualizar o gráfico da potência do sinal óptico recebido pela ONU utilizada para realizar os testes.

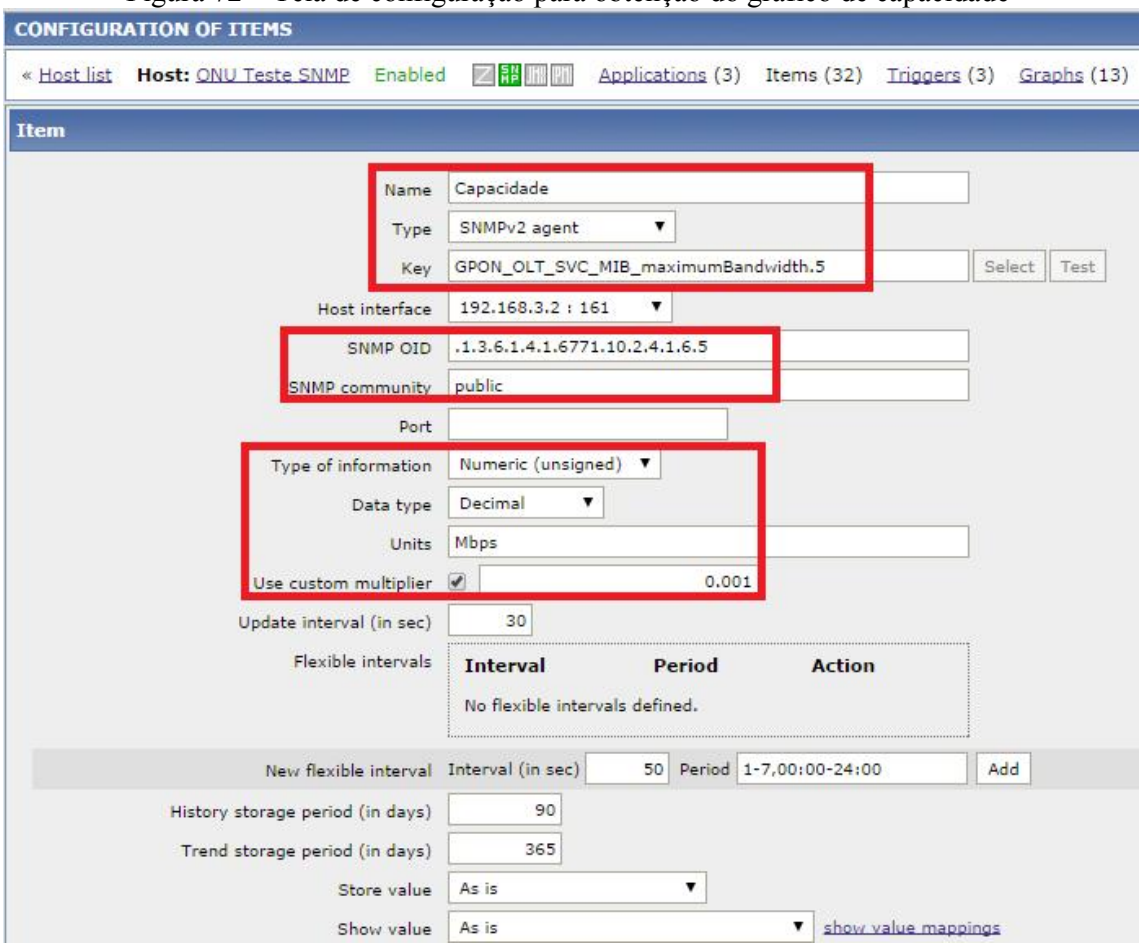
Figura 71 – Gráfico de obtenção da potência de sinal óptico



Fonte: Elaborado pelo autor.

Após a configuração da consulta para obtenção da potência do sinal óptico, foi configurada a consulta para obtenção da capacidade do canal de comunicação entre a OLT e a ONU. Através da consulta com o Ireasoning, foi identificado o objeto correto que possui a informação da configuração de capacidade do canal de comunicação entre a OLT e a ONU utilizada no teste. Através da Figura 72 é possível observar os parâmetros configurados para a obtenção do valor configurado para a capacidade.

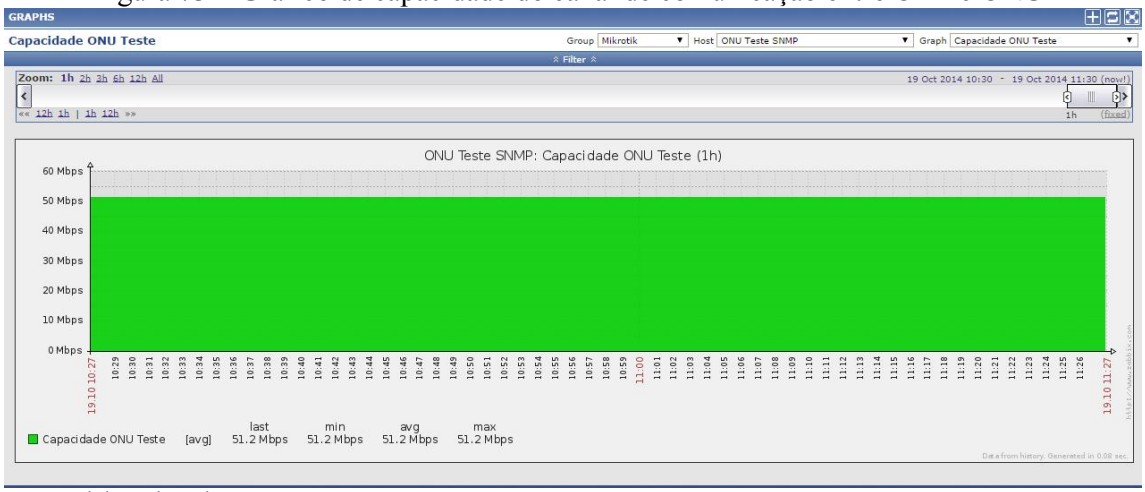
Figura 72 – Tela de configuração para obtenção do gráfico de capacidade



Fonte: Elaborado pelo autor.

Após realizada a configuração para a obtenção do gráfico, foi possível visualizá-lo, conforme demonstra a Figura 73.

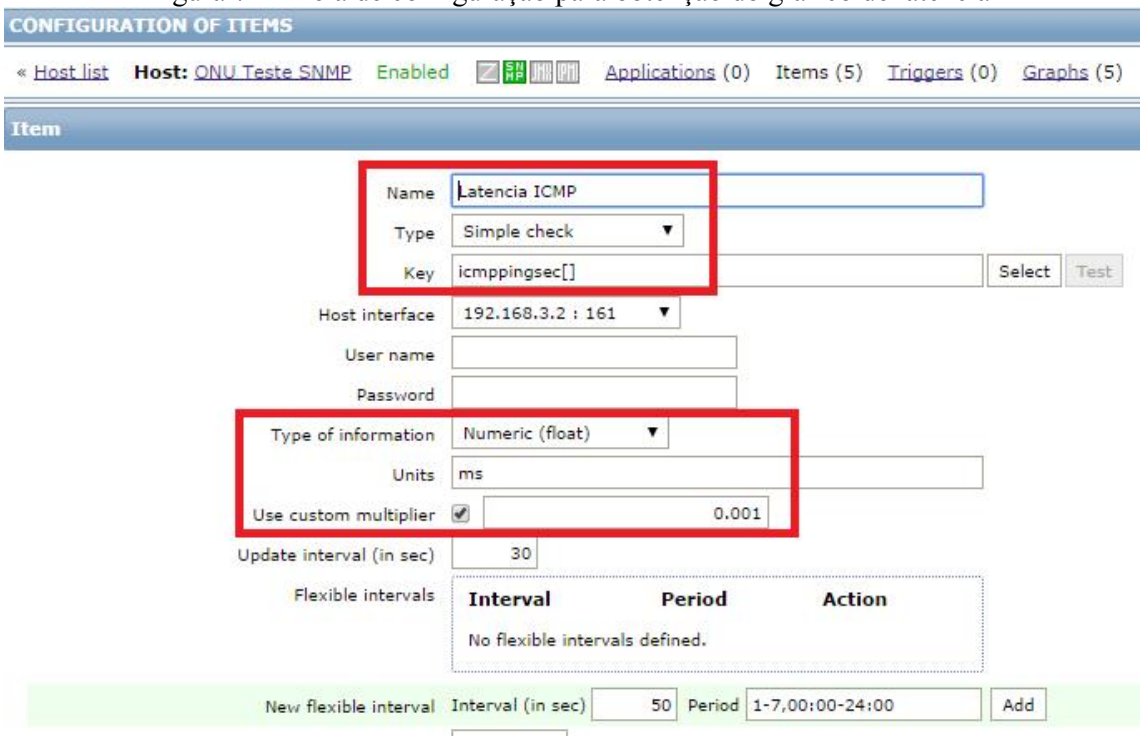
Figura 73 – Gráfico de capacidade do canal de comunicação entre OLT e ONU



Fonte: Elaborado pelo autor.

O próximo passo foi coletar os dados de latência. Para realizar os testes de latência foi utilizada a função *icmppingsec*, que é nativa do *Zabbix*. Através da Figura 74 é possível visualizar a configuração dos parâmetros utilizados para obter o gráfico de latência.

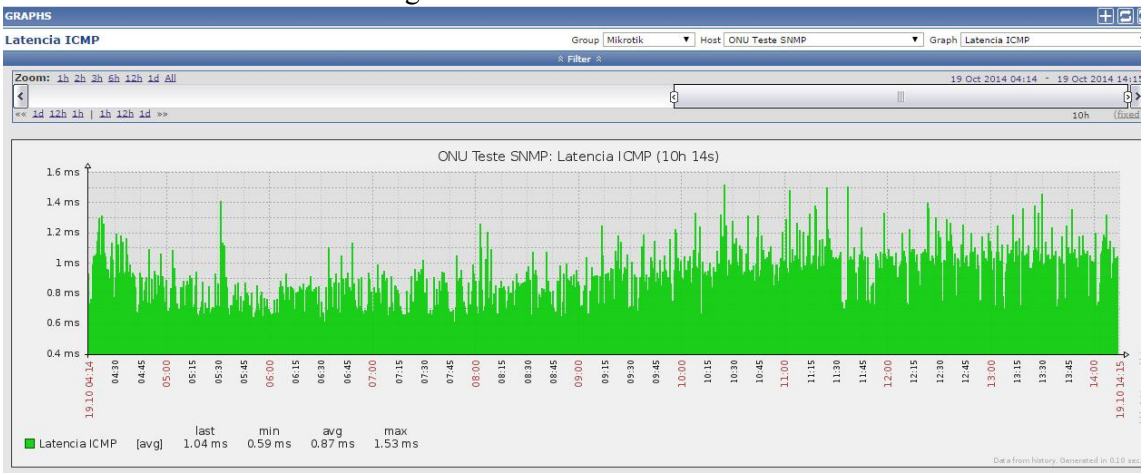
Figura 74 – Tela de configuração para obtenção do gráfico de latência



Fonte: Elaborado pelo autor.

A Figura 75 demonstra como ficou o gráfico de latência armazenado pelo *Zabbix*.

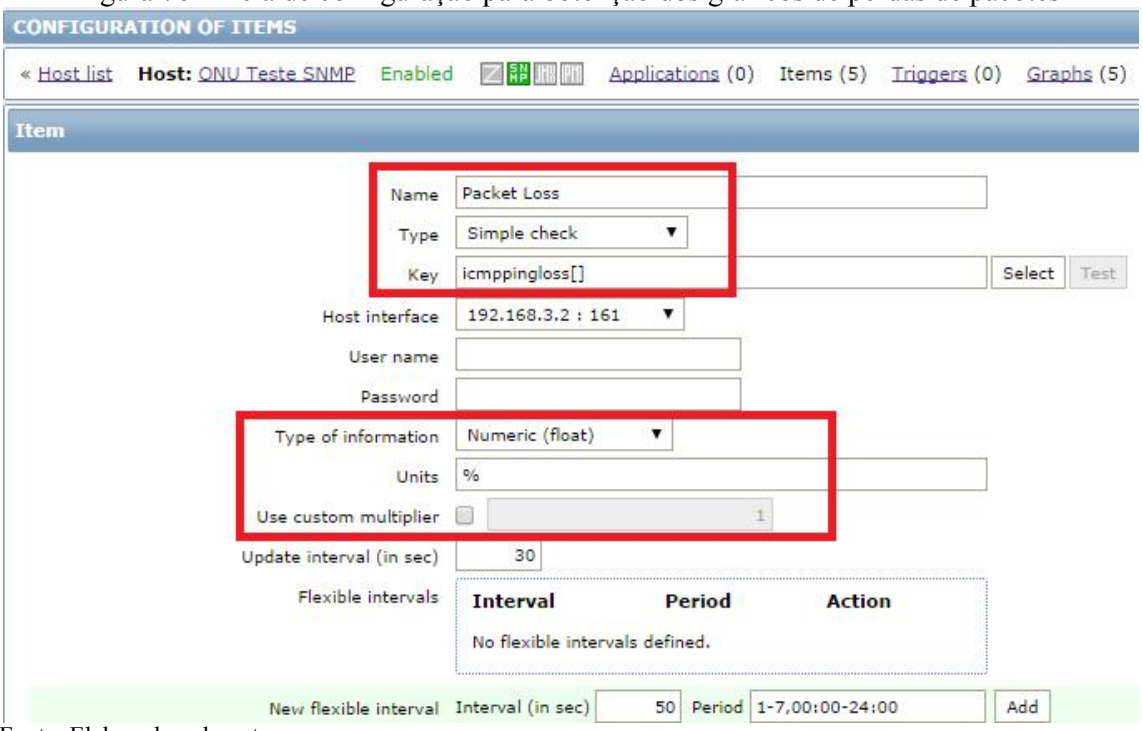
Figura 75 – Gráfico de latência



Fonte: Elaborado pelo autor.

Após efetuada a configuração dos testes de latência, foi configurada a coleta dos dados de perdas de pacotes. Para realizar os testes foi utilizada a função *icmppingloss*, que assim como a função *icmppingsec* utilizada para obter o gráfico de latência, também é nativa do *Zabbix*. A tela de configuração para a obtenção dos dados de perdas de pacotes pode ser visualizada através da Figura 76.

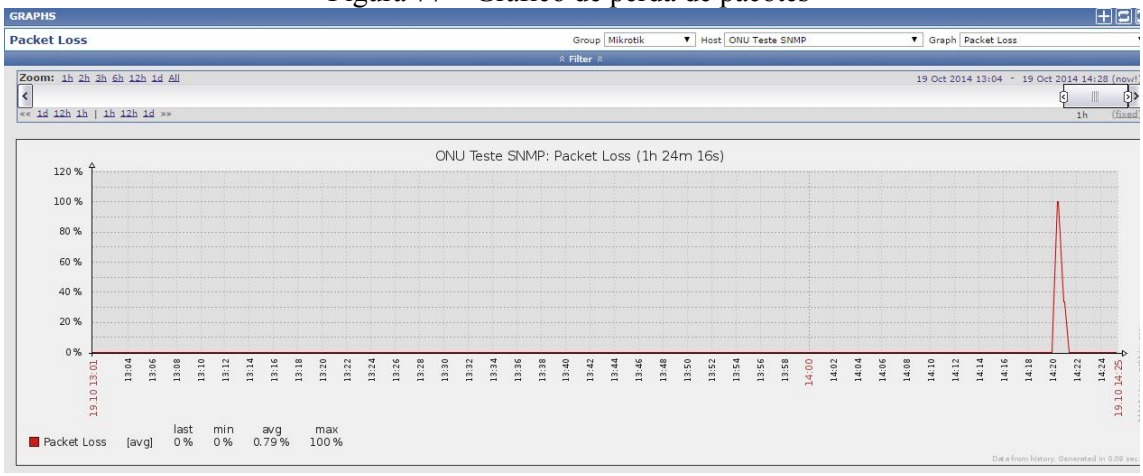
Figura 76 – Tela de configuração para obtenção dos gráficos de perdas de pacotes



Fonte: Elaborado pelo autor.

Na Figura 77 é possível observar a geração do gráfico de perda de pacotes. Para que o gráfico apresentasse uma variação, foi criada uma regra de *firewall* com a função de impedir a comunicação entre o gerente SNMP do *Zabbix* e a ONU. Após adicionar a regra foi possível visualizar uma variação no gráfico que demonstra que ele está funcionando da maneira correta. Após a verificação da variação causada pela regra de *firewall*, a regra foi novamente removida para que o gráfico voltasse a apresentar os valores reais de perda de pacotes.

Figura 77 – Gráfico de perda de pacotes



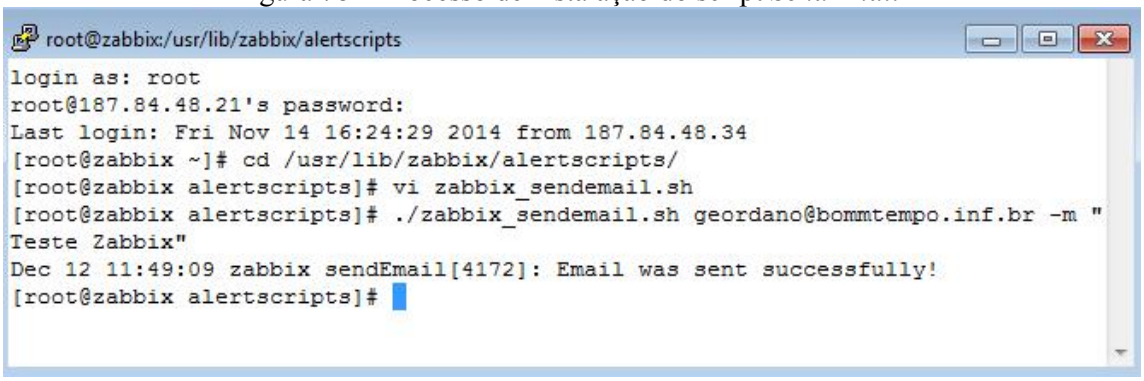
Fonte: Elaborado pelo autor.

Para cada gráfico armazenado, o *Zabbix* permite criar alertas customizados. Para o envio de alerta via SMS, assim como o *Cacti*, o *Zabbix* necessita de um modem GSM com um chip conectado fisicamente ao servidor para realizar o envio das mensagens de alerta. Como o servidor onde o *Zabbix* é executado não é físico e sim virtual, não foi possível enviar alertas via SMS. Outra forma de envio de alertas disponibilizado pelo *Zabbix* é o alerta por *email*. O *Zabbix* possui uma forma nativa de enviar alertas por *email*, porém sem autenticação. Como na Bom Tempo Telecom o servidor de *emails* não permite o envio de *emails* sem realizar autenticação, foi necessário procurar uma forma alternativa de enviar os alertas.

O método encontrado para enviar os alertas foi através de um *script*[16] encontrado no *site* da *Zabbix* Brasil chamado *SendEmail*. Os procedimentos recomendados pelo site para efetuar a instalação foram seguidos e um *email* de teste foi enviado com sucesso, conforme demonstrado na Figura 78.

[16] *http://zabbixbrasil.org/wiki/tiki-index.php?page=Envio+de+alertas+por+e-mail+utilizando+SMTP+autenticado*

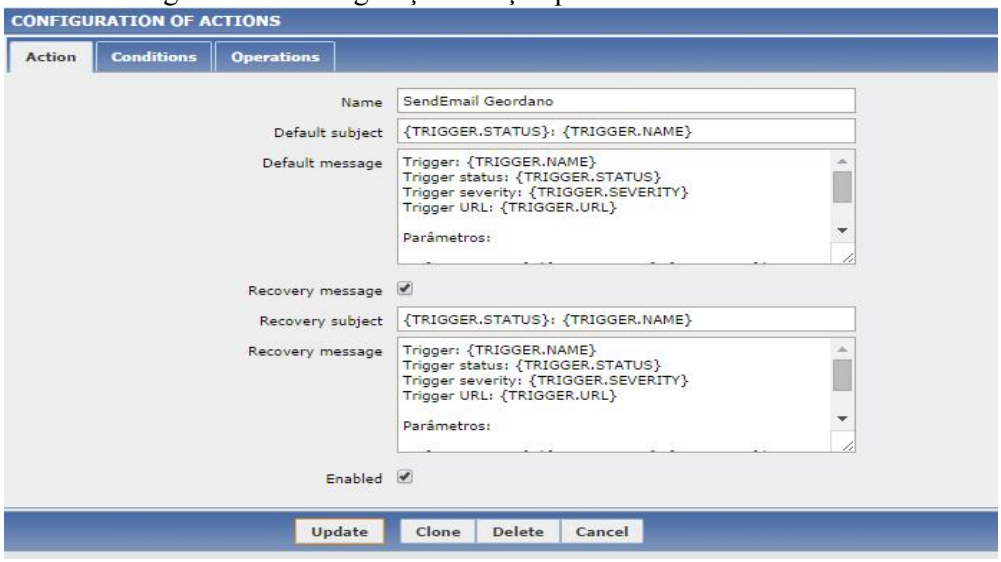
Figura 78 – Processo de instalação do script *SendEmail*



Fonte: Elaborado pelo autor.

A configuração de alertas no *Zabbix* é realizada em três etapas. Primeiramente é necessário configurar uma ação, no *menu* "*Configuration* > *Actions*". A ação é composta de uma ação propriamente dita, condições e operações. Na ação são configurados basicamente um nome para a ação, o assunto e o corpo do *email* que será enviado, conforme pode ser observado na Figura 79.

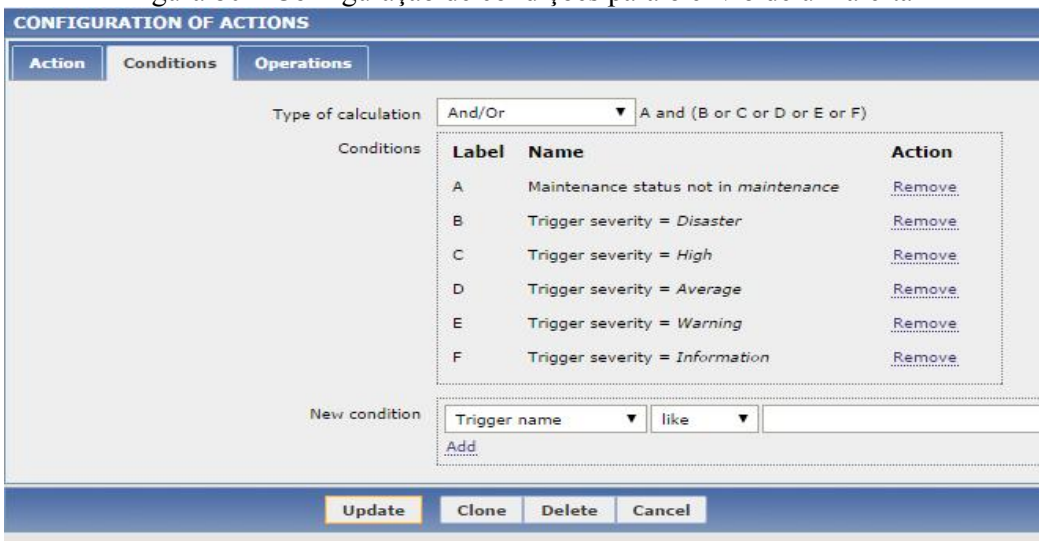
Figura 79 – Configuração de ação para o envio de um alerta



Fonte: Elaborado pelo autor.

No campo de configuração das condições podem ser configurados diversos tipos de condições, como por exemplo, permitir a ativação da ação apenas se o *host* monitorado não estiver em manutenção. Nesse caso, se o *Zabbix* tiver sido informado que o *host* monitorado está em manutenção, não será tomada nenhuma ação. Através da Figura 80 é possível visualizar a tela de configuração de condições.

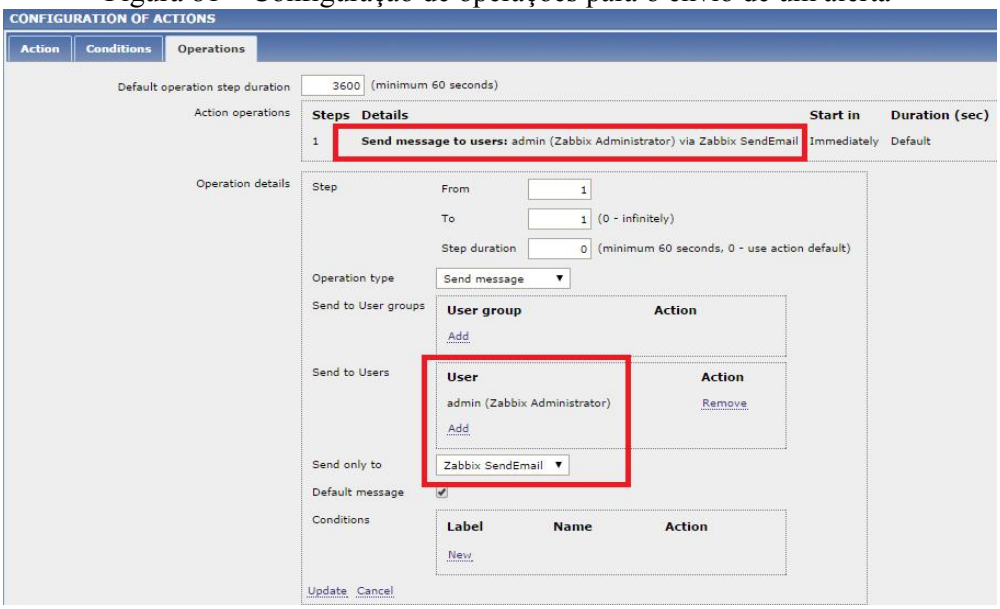
Figura 80 – Configuração de condições para o envio de um alerta



Fonte: Elaborado pelo autor.

No campo de configuração das operações é possível cadastrar para quais usuários algum tipo de alerta deve ser enviado. No exemplo da Figura 81 um alerta será enviado através do *script SendEmail* para o usuário admin.

Figura 81 – Configuração de operações para o envio de um alerta

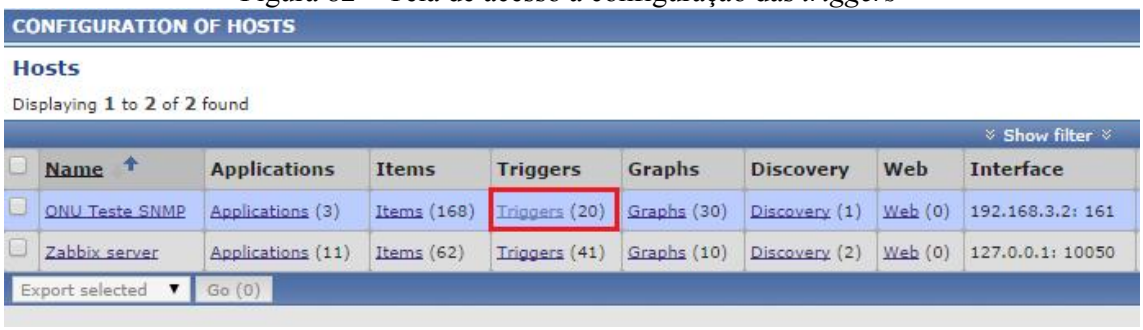


Fonte: Elaborado pelo autor.

Após configurada a ação, foi necessário configurar o que o *Zabbix* chama de *triggers*. As *triggers* possuem a função de monitorar parâmetros de consultas SNMP já configuradas no *Zabbix* e ativar o envio de alertas caso o parâmetro lido esteja fora do valor pré-configurado na *trigger*. Para exemplificar, foi criada uma *trigger* para envio de alertas em caso de variação no sinal óptico de uma ONU utilizada para testes. As *triggers* são

configuradas dentro de cada *host* e são acessadas através do *menu* "*Configuration* > *Hosts*". Ao entrar na tela de *hosts*, é possível clicar em cima da *string Triggers*, conforme pode ser visto na Figura 82.

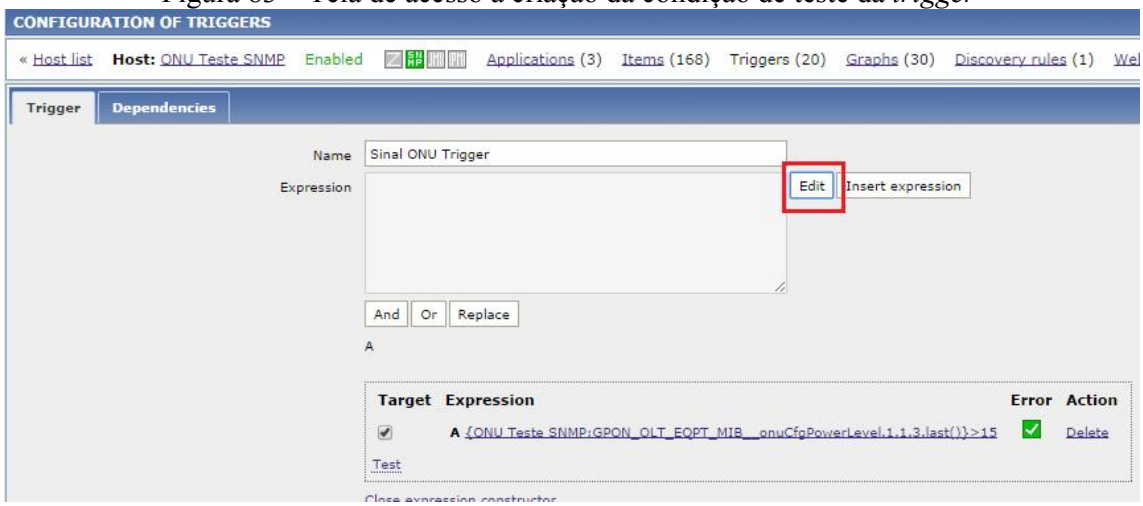
Figura 82 – Tela de acesso à configuração das *triggers*



Fonte: Elaborado pelo autor.

Após entrar na tela de configuração das *triggers*, foi necessário criar uma nova *trigger*. Ao criar uma nova *trigger*, a primeira coisa a ser realizada foi criar uma condição de teste para um item monitorado. Conforme pode ser visto na Figura 83, clicar no botão "*Edit*".

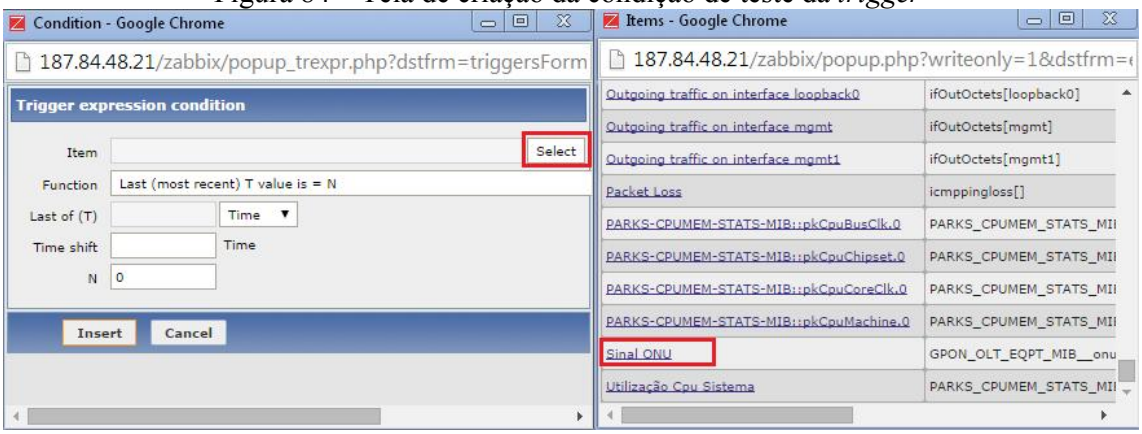
Figura 83 – Tela de acesso à criação da condição de teste da *trigger*



Fonte: Elaborado pelo autor.

Na janela aberta após clicar no botão "*Edit*", foi clicado no botão "*Select*" para selecionar um item a ser monitorado. Para o exemplo foi utilizado o item que armazena os dados da potência do sinal óptico da ONU utilizada para os testes, chamado de "Sinal ONU", conforme pode ser observado na Figura 84.

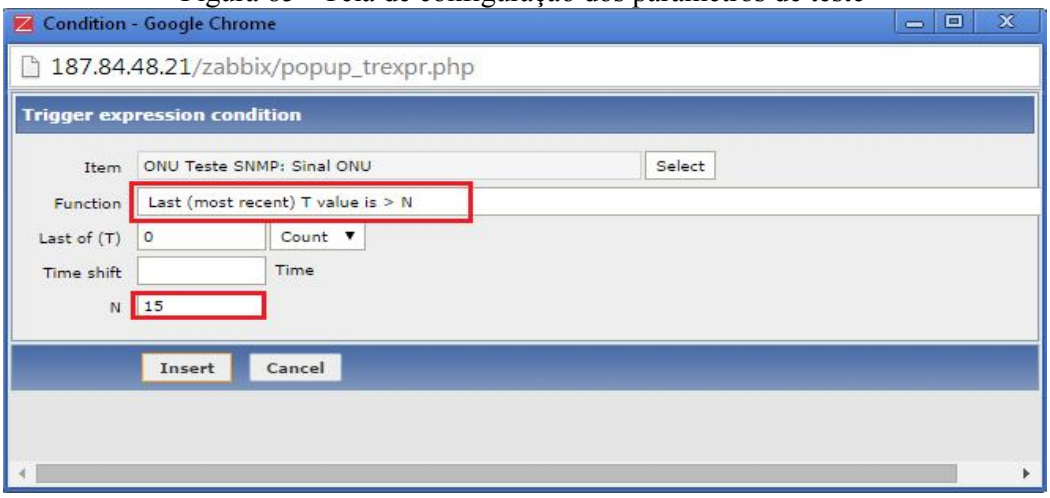
Figura 84 – Tela de criação da condição de teste da *trigger*



Fonte: Elaborado pelo autor.

Após selecionado o item a ser monitorado pela *trigger*, foi selecionada a função de comparação para realizar o monitoramento e o valor configurado como padrão para o monitoramento. Conforme pode ser visto na Figura 85, para o teste foi selecionada a função "*Last (most recent) T value is > N*" e foi definido o valor 15 para a variável N. O valor 15 foi escolhido devido ao fato do nível de potência óptica recebido pela ONU de teste ser de 25dBm. Como o valor 25 é maior do que o valor 15 configurado para N, a *trigger* será ativada e o sistema enviará um *email* de alerta.

Figura 85 - Tela de configuração dos parâmetros de teste

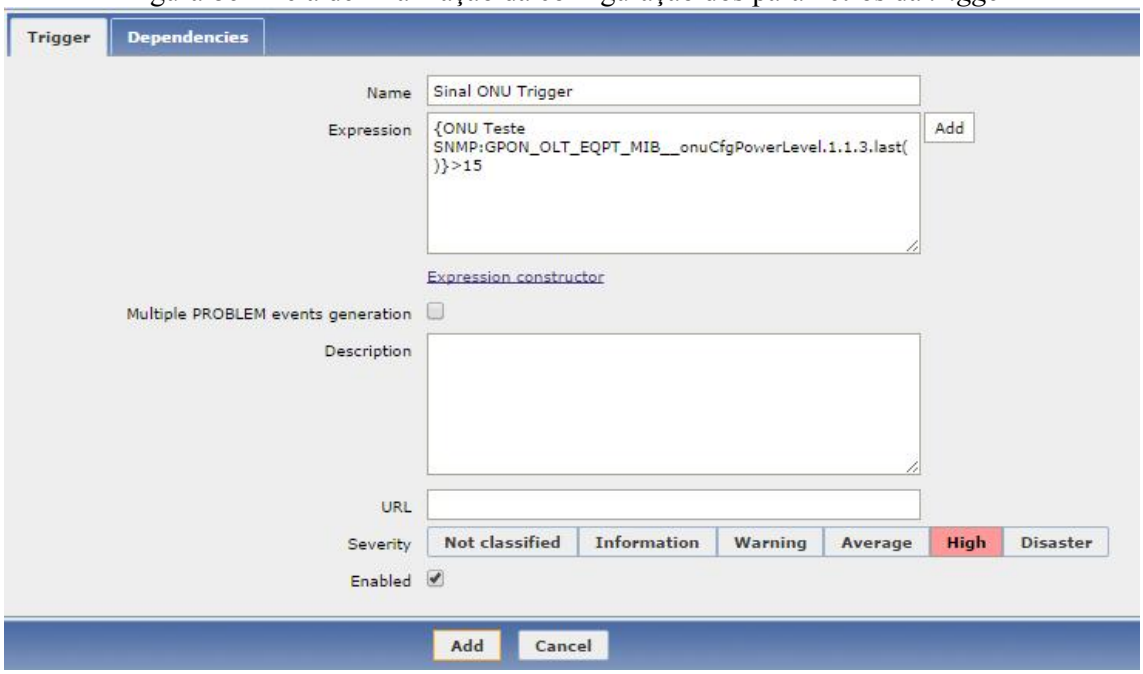


Fonte: Elaborado pelo autor.

Após clicar no botão "*Insert*", a *trigger* está configurada para monitorar o serviço selecionado na janela anterior seguindo os parâmetros configurados. Para finalizar a criação da *trigger*, foi selecionado o nível de importância do serviço monitorado nas opções ao lado

da *string* "*Severity*" e por fim, foi utilizado o botão "*Add*" para adicionar a *trigger* ao *Zabbix* conforme demonstrado na Figura 86.

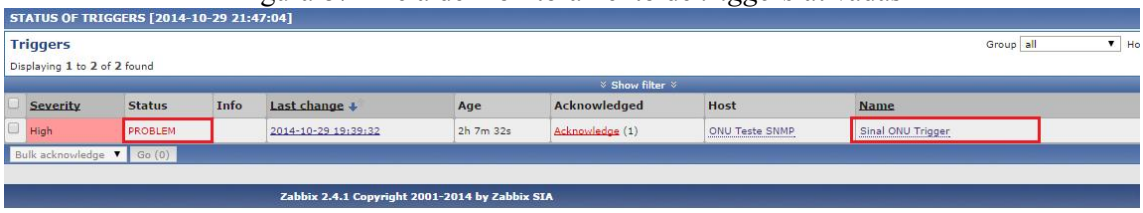
Figura 86 - Tela de finalização da configuração dos parâmetros da *trigger*



Fonte: Elaborado pelo autor.

Após configurada a *trigger*, para verificar se ela foi ativada, foi utilizado o *menu* "*Monitoring* > *Triggers*". A *trigger* de teste foi configurada propositalmente com um parâmetro para que ela fosse ativada. Através da Figura 87 é possível observar a tela de monitoramento de *triggers*.

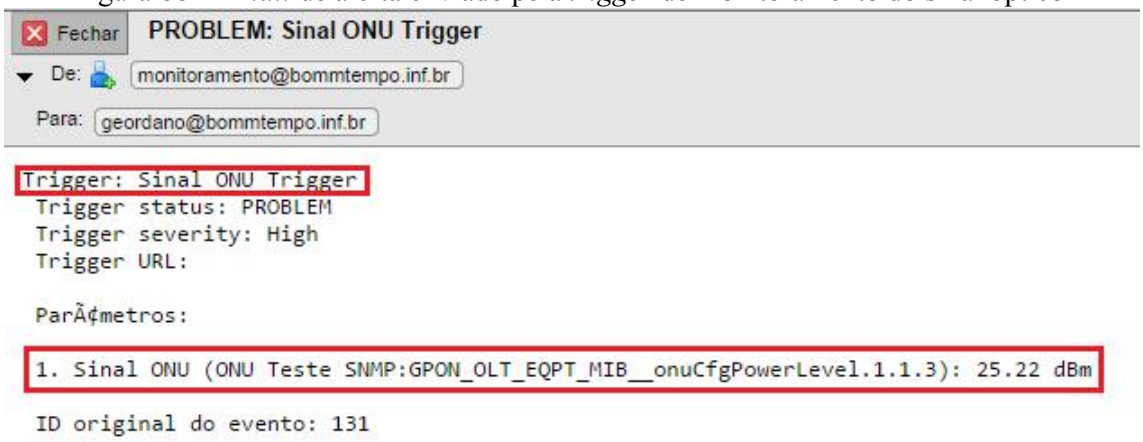
Figura 87 - Tela de monitoramento de *triggers* ativadas



Fonte: Elaborado pelo autor.

Na Figura 88 pode ser visto um alerta enviado por *email* devido ao nível de potência óptica estar fora do limite pré-configurado na *trigger*.

Figura 88 – *Email* de alerta enviado pela *trigger* de monitoramento do sinal óptico



Fonte: Elaborado pelo autor.

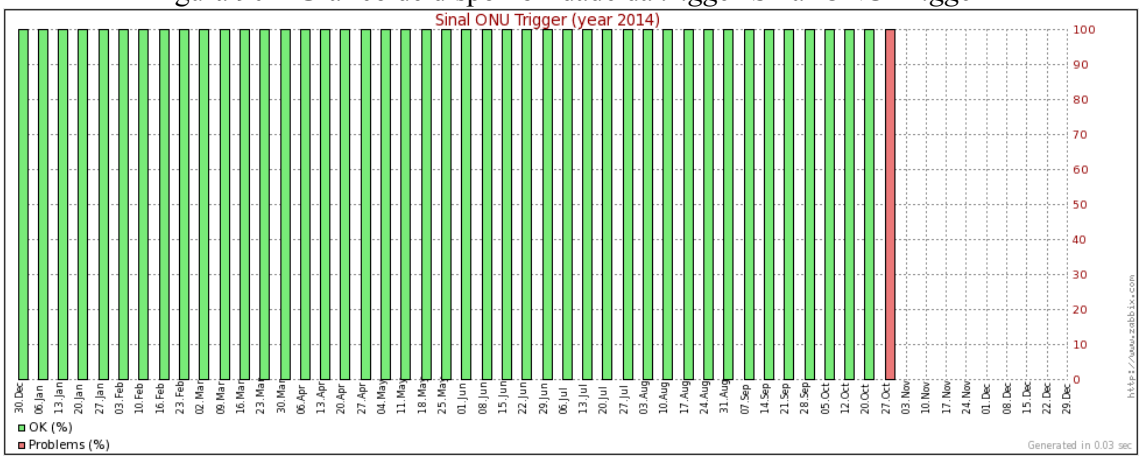
A disponibilidade dos serviços dos *hosts* para os quais existe uma *trigger* configurada, pode ser verificada através do *menu* "*Reports* > *Availability report*", conforme pode ser visualizado na Figura 89. Não é possível visualizar a disponibilidade de um serviço que não possui uma *trigger* configurada. Para visualizar o gráfico de disponibilidade é necessário clicar na string "*Show*".

Figura 89 – Tela de disponibilidade das *triggers* dos serviços configurados

Fonte: Elaborado pelo autor.

Após clicar na string "*Show*" é possível visualizar o gráfico de disponibilidade de um determinado serviço, conforme pode ser visto na Figura 90. No gráfico é possível observar que no período em que o sistema nem estava instalado ainda, o *Zabbix* preencheu o gráfico com linhas em verde, que de acordo com a escala significam que o serviço da *trigger* estava funcionando corretamente no período. No *Zabbix* não é possível visualizar a disponibilidade por *host*, mas apenas por serviços.

Figura 90 – Gráfico de disponibilidade da *trigger* Sinal ONU *Trigger*



Fonte: Elaborado pelo autor.

8.5 CONSIDERAÇÕES DO CAPÍTULO

Após a realização dos testes de monitoramento com os *softwares*, foi possível identificar que cada um possui as suas particularidades e a sua própria maneira de organizar e interpretar as informações.

A etapa de instalação dos *softwares* não foi muito complexa, exceto no caso do *Cacti*, onde foi necessário reinstalá-lo devido aos problemas encontrados com a geração dos gráficos. A liberdade de escolha da distribuição *Linux* utilizada como sistema base para a execução dos *softwares,* apesar de parecer uma grande vantagem, possui também o seu lado negativo, pois impacta diretamente no funcionamento dos *softwares*. Como para cada distribuição *Linux* o funcionamento dos pacotes é diferente, isso pode causar instabilidades nas ferramentas executadas.

No capítulo seguinte será realizada uma análise dos critérios a serem avaliados de acordo com cada *software* através da aplicação do Método Analítico Hierárquico.

9 AVALIAÇÕES DOS CRITÉRIOS DOS *SOFTWARES*

Após a realização dos testes, foram montadas as matrizes de avaliação para cada critério, a fim de definir qual *software* atende melhor aos requisitos impostos separadamente. Por final, será realizada a média de todos os critérios para chegar à média geral. Os testes realizados com os *softwares* são explicados no Capítulo 8. Os critérios avaliados são os especificados anteriormente na Tabela 16.

Para realizar a comparação entre os *softwares* para cada critério, foi atribuído o valor 9 quando o *software* atendeu completamente o critério, 6 quando o critério foi parcialmente atendido e 1 quando não foi atendido. Quando o *software* da linha recebeu uma avaliação inferior ao *software* da coluna, a célula recebe o valor proporcionalmente inferior ao avaliado para o *software* da coluna. Além dos comentários dos testes realizados, esse capítulo possui as matrizes de avaliação juntamente com cálculos de consistência do MAH para cada critério avaliado.

9.1 CRITÉRIO 1 – MEDIÇÃO DE LATÊNCIA

Os três *softwares* permitem realizar os testes de monitoramento de latência. No *Zabbix* foi utilizada a função nativa do *software* chamada *icmppingsec*. No *Nagios* foi utilizado um *plugin* nativo do *Centreon* chamado *check_centreon_ping*. Ambos foram de configuração simples. No *Cacti*, ao cadastrar um dispositivo, o sistema já passa a efetuar testes de ICMP para o mesmo a fim de testar a sua disponibilidade. Porém, os resultados não são armazenados em gráfico. Para armazenar os testes de latência realizados para cada dispositivo monitorado, foi necessário importar o *template Advanced Ping*, pois o *Cacti* não possui uma forma nativa de armazenar gráficos para os testes realizados. A Tabela 19 demonstra a matriz de avaliação calculada para este critério.

Tabela 19 – Matriz de avaliação para o critério 1

Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	1	1	0,333
Nagios	1	1	1	0,333
Zabbix	1	1	1	0,333
SOMA	3	3	3	RC = 0

Fonte: Elaborado pelo autor.

Após obtida a matriz de avaliação dos *softwares* para o critério 1, foi calculada a consistência das avaliações. Abaixo os cálculos de consistência para o critério em questão.

(1x0,333) + (1x0,333) + (1x0,333) = 0,999

(1x0,333) + (1x0,333) + (1x0,333) = 0,999

(1x0,333) + (1x0,333) + (1x0,333) = 0,999

A soma ponderada para cada linha foi dividida pela média da alternativa correspondente. Nesse caso:

0,999/0,333 = 3

0,999/0,333 = 3

0,999/0,333 = 3

$\lambda max = (3 + 3 + 3) / 3 = 3$

Após obtido o valor de λmax, foi aplicada a fórmula abaixo:

$IC = (\lambda max - n) / (n - 1)$

$IC = (3 - 3) / (3 - 1) = 0 / 2$

$IC = 0$

Após calculado o IC, foi calculado o RC:

RC = IC / IAM

RC = 0 / 0,52

RC = 0

Devido ao fato dos três *softwares* permitirem o monitoramento de latência para os dispositivos armazenando os resultados em gráfico, para este critério os *softwares* ficaram empatados.

9.2 CRITÉRIO 2 – MEDIÇÃO DE PERDA DE PACOTES

Os três *softwares* permitem realizar o monitoramento de perda de pacotes. O *Nagios* utiliza o *plugin* nativo *check_icmp*, que é capaz de monitorar a perda de pacotes e armazenar esse valor em gráfico. O *Zabbix* faz utilização do *plugin* nativo *icmppingloss* para realizar o monitoramento das perdas de pacotes e armazenar o valor retornado pelo teste em gráficos. O *Cacti*, assim como para o critério de latência, faz utilização do *template Advanced Ping*. A Tabela 20 apresenta os resultados obtidos na matriz de comparação para o critério de medição de perda de pacotes.

Tabela 20 – Matriz de avaliação para o critério 2

Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	1	1	0,333
Nagios	1	1	1	0,333
Zabbix	1	1	1	0,333
SOMA	3	3	3	RC = 0

Fonte: Elaborado pelo autor.

Para este critério a média dos *softwares* ficou empatada devido a todos eles atenderem plenamente ao critério avaliado.

9.3 CRITÉRIO 3 – MEDIÇÃO DE VAZÃO

Diferentemente dos critérios 1 e 2, este critério necessita de informações disponibilizadas pela MIB para coletar informações. Conforme explicado anteriormente, a MIB da Parks não fornece a informação de vazão para as ONUs. De acordo com a empresa, o plano de desenvolvimento e atualização das MIBs por enquanto não contempla a disponibilização dessa informação. Assim sendo, não foi possível coletar essa informação e por este motivo não foi construída uma matriz de avaliação. A informação não pôde ser armazenada devido a uma falta de disponibilização da informação, e não devido a uma limitação dos *softwares*.

9.4 CRITÉRIO 4 – MEDIÇÃO DE CAPACIDADE

Os três *softwares* atenderam sem problemas a medição deste parâmetro de configuração. O *Cacti* permitiu a criação de combinação de valores para as consultas através da criação e customização de arquivos XML. O *Nagios* e o *Zabbix* necessitam de ferramentas de apoio para conseguir coletar a informação correta. A Tabela 21 demonstra a matriz de avaliação para este critério.

Tabela 21 – Matriz de avaliação para o critério 4

Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	1	1	0,333
Nagios	1	1	1	0,333
Zabbix	1	1	1	0,333
SOMA	3	3	3	RC = 0

Fonte: Elaborado pelo autor.

Os três *softwares* obtiveram um resultado de empate, pois todos atenderam ao critério de forma satisfatória, gerando gráficos para manter um histórico dos dados.

9.5 CRITÉRIO 5 – MEDIÇÃO DE INTENSIDADE DE SINAL

Os três *softwares* permitem realizar a medição de intensidade de sinal óptico recebido pelas ONUs dos assinantes. O *Cacti* facilita a criação dos gráficos através de um arquivo XML que fornece ao usuário a relação das ONUs que estão conectadas à OLT e permite criar gráficos de intensidade de sinal para as mesmas. No *Nagios* e no *Zabbix* é necessária a utilização de uma ferramenta de apoio para identificar o objeto correto do qual a informação foi coletada para cada ONU. Na Tabela 22 é demonstrada a matriz de avaliação para este critério.

Tabela 22 – Matriz de avaliação para o critério 5

Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	1	1	0,333
Nagios	1	1	1	0,333
Zabbix	1	1	1	0,333
SOMA	3	3	3	RC = 0

Fonte: Elaborado pelo autor.

Como os três *softwares* atenderam ao critério especificado, novamente persistiu o empate entre os mesmos na matriz de avaliação.

9.6 CRITÉRIO 6 – ENVIO E CONFIGURAÇÃO DE TIPOS DE ALERTAS

Os três *softwares* permitem enviar alertas por *email* e por SMS, porém o envio por SMS não foi testado pois era necessário conectar um modem fisicamente ao servidor para

enviar as mensagens. Os três *softwares* enviam emails de alerta de forma nativa. O *Zabbix* é capaz de enviar apenas *emails* sem autenticação no servidor de *emails*, ou seja, sem enviar a senha da conta que ele está utilizando para enviar o *email*. Para possibilitar o envio de *emails* de alerta fazendo uso de autenticação, foi instalado o *plugin SendEmail*. O *Nagios* e o *Cacti* enviaram os *emails* de alerta sem a necessidade de instalação de *plugins* adicionais. A Tabela 23 apresenta a matriz de avaliação para o critério 6.

Tabela 23 – Matriz de avaliação para o critério 6

Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	1	1	0,333
Nagios	1	1	1	0,333
Zabbix	1	1	1	0,333
SOMA	3	3	3	RC = 0

Fonte: Elaborado pelo autor.

Conforme apresentado na Tabela 23, devido ao fato dos três *softwares* atenderem o critério, novamente ocorreu empate na matriz de avaliação.

9.7 CRITÉRIO 7 – FACILIDADE DE CONFIGURAÇÃO

Entre os três *softwares* avaliados, o que possui maior facilidade de configuração é o *Cacti*. Através dos arquivos XML criados, é possível criar os gráficos de monitoramento com facilidade. Os alertas também são configurados de forma simples.

No *Nagios*, a necessidade da utilização de uma ferramenta de apoio para consultar os objetos corretos da MIB torna a tarefa de configurar um serviço mais complexa do que no *Cacti*. Após criado o serviço, o alerta é configurado facilmente na mesma janela de configuração do serviço.

No *Zabbix*, configurar um serviço também se torna uma tarefa complexa assim como no *Nagios* devido ao fato da necessidade da mesma ferramenta de apoio. A configuração dos alertas é complexa, pois depende da definição de *triggers*. A definição e configuração das *triggers* demanda tempo e customização um tanto complexa de se fazer. Através da Tabela 24 é apresentada a matriz de avaliação dos *softwares*.

Tabela 24 – Matriz de avaliação para o critério 7

Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	9	9	0,766
Nagios	1/9	1	5	0,173
Zabbix	1/9	1/5	1	0,058
SOMA	1,222	10,2	15	RC = 0,29

Fonte: Elaborado pelo autor.

Como para casos de grande superioridade de um *software* em relação a outros, não é necessário realizar o cálculo de RC, pois fica evidenciada a superioridade de um dos avaliados. Mesmo assim, o cálculo de RC foi realizado.

Com as médias obtidas é possível observar que o *Cacti* teve desempenho muito superior ao *Nagios* e ao *Zabbix* devido à facilidade apresentada para configurar os monitoramentos. A diferença na média superior do *Cacti* também se dá pelo fato de não necessitar de um *software* de apoio para realizar as consultas aos objetos da MIB.

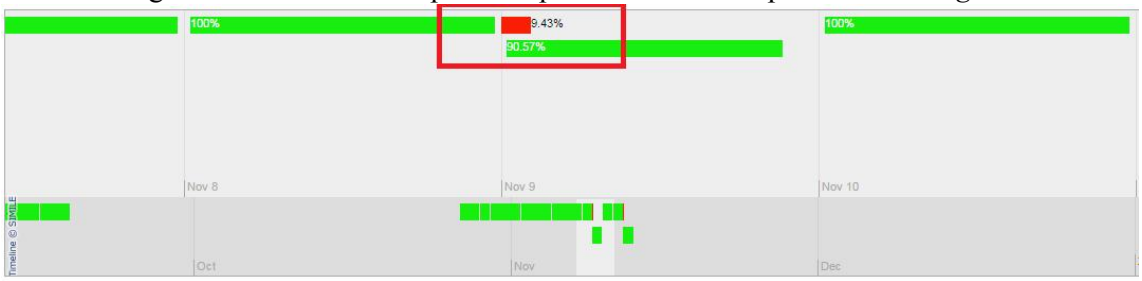
9.8 CRITÉRIO 8 – HISTÓRICO DE SLA

O histórico de SLA ou de disponibilidade da rede apresentado pelo *Zabbix* deixa a desejar na quantidade e na qualidade das informações. O gráfico é apresentado em barras, e sempre é demonstrado até o dia anterior. Nunca é apresentado gráfico do mesmo dia, pois o sistema não sabe se todos os dispositivos permanecerão operacionais até o término do dia. O gráfico demonstra uma barra na cor verde quando todos os dispositivos monitorados pelo *software* estavam operacionais no dia anterior e uma barra na cor vermelha quando um ou mais dispositivos estavam em estado não-operacional.

No *Cacti* não é apresentado nenhum tipo de gráfico. Apenas é apresentado um valor do percentual do tempo de disponibilidade do dispositivo desde que o mesmo passou a ser monitorado. Não é possível fazer nenhuma busca por período de tempo e nem tirar relatórios mais detalhados.

No *Nagios*, é possível gerar relatórios detalhados de várias formas. Os relatórios podem ser gerados retratando todos os eventos ocorridos em um determinado período de tempo, percentual de disponibilidade por equipamento e por período. Também é possível navegar através de uma linha do tempo para identificar por quanto tempo e em que horário o dispositivo ficou indisponível, conforme pode ser visto na Figura 91.

Figura 91 – Linha do tempo de disponibilidade de dispositivos no *Nagios*



Fonte: Elaborado pelo autor.

Através da Tabela 25 é possível visualizar a matriz de avaliação para o critério de histórico de SLA.

Tabela 25 – Matriz de avaliação para o critério 8

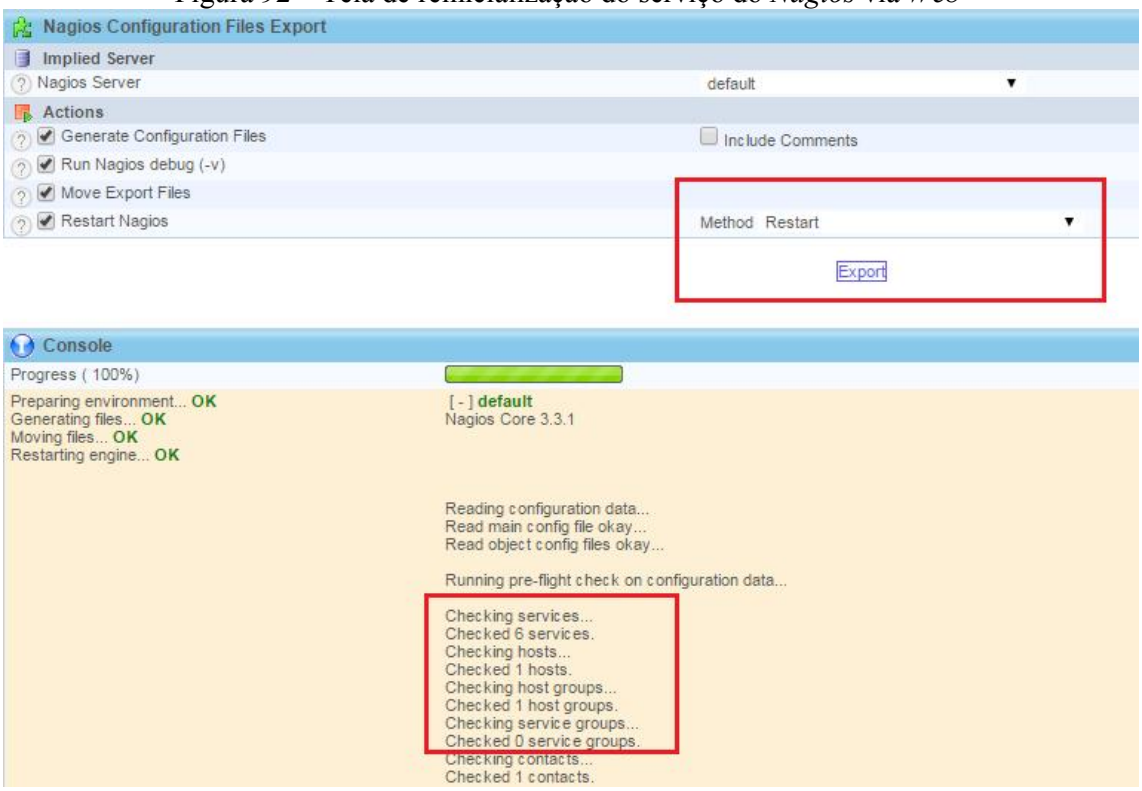
Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	1/9	1/5	0,058
Nagios	9	1	9	0,766
Zabbix	5	1/9	1	0,174
SOMA	15	1,222	10,2	RC = 0,29

Fonte: Elaborado pelo autor.

9.9 CRITÉRIO 9 – USABILIDADE

As *interfaces* dos *softwares* e a forma que cada um tem de organizar os itens são bastante diferentes. O *Nagios* possui uma interface limpa e fácil de usar, onde as informações podem ser alcançadas facilmente. O acesso e a navegação por dentro dos *menus* do *software* acontecem de forma rápida. A possibilidade de customização dos gráficos é pequena, já que os dados inseridos no gráfico são provenientes dos *plugins* nativos do *software* que fazem as coletas por SNMP. Uma característica que marcou negativamente o *software* foi a necessidade de a cada conjunto de configurações alteradas, ser necessário reiniciar o serviço do *Nagios* através da *interface Web*. Isso faz com que o *Nagios* recarregue todos os módulos novamente e faça uma checagem nos arquivos de configuração à procura de erros, conforme pode ser visto na Figura 92.

Figura 92 – Tela de reinicialização do serviço do *Nagios* via *Web*



Fonte: Elaborado pelo autor.

No *Cacti*, após configurados os *templates* para os gráficos e para a coleta de informações por SNMP, pode-se caracterizar a usabilidade do *software* como simples. A configuração do *software* foi um tanto complicada e necessita de pesquisa em *sites* e fóruns, a fim de buscar apoio de outros usuários do *software*. Um ponto negativo para o *software* é a utilização de um *menu* muito extenso do lado esquerdo, que segue seqüência de cima para baixo e não cabe em uma tela de 17 polegadas, por exemplo.

O *Zabbix* possui usabilidade razoável. Os *menus* primários ficam acessíveis, mas por diversas vezes é necessário acessar até quatro *submenus* para realizar uma configuração, como a de uma *trigger* para gerar um alerta, por exemplo. A apresentação dos gráficos é interessante e possibilita boas condições de customização. Uma característica importante do *software* é a possibilidade de montar telas de monitoramento customizadas inserindo diversos gráficos até mesmo de dispositivos diferentes.

Através da Tabela 26 é possível visualizar a matriz de avaliação para o critério de usabilidade.

Tabela 26 – Matriz de avaliação para o critério 9

Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	1	1	0,333
Nagios	1	1	1	0,333
Zabbix	1	1	1	0,333
SOMA	3	3	3	RC = 0

Fonte: Elaborado pelo autor.

Como todos os *softwares* atenderam ao critério de forma bastante similar e nenhum deles se sobressaiu em relação aos demais, os três *softwares* ficaram empatados na avaliação realizada para este critério.

9.10 CRITÉRIO 10 – DOCUMENTAÇÃO DO *SOFTWARE*

A documentação encontrada para o *Cacti* foi bastante extensa e a comunidade de usuários do *Cacti* possui o hábito de compartilhar informações a fim de deixá-las registradas. Essas informações podem ser consultadas por outros usuários que possam passar pela mesma dificuldade, podendo então resolver o problema com uma maior facilidade. O *Cacti* também possui uma variedade considerável de *plugins*[17] que podem ser adicionados ao *software* de acordo com a necessidade do usuário.

O *Nagios* também possui documentação extensa, porém a quantidade de fóruns e grupos de ajuda a usuários é menor do que no *Cacti*. O sistema possui menos *plugins*[18] do que o *Cacti*, porém a distribuição FAN já vem acompanhada de grande parte dos recursos necessários para se realizar o monitoramento SNMP dos dispositivos de uma rede.

Entre os três *softwares* avaliados, o *Zabbix* é o que possui menor quantidade de documentação e fóruns para colaboração de usuários. Quanto ao número de *plugins*[19] o software fica atrás apenas do *Cacti*. Apesar de possuir mais *plugins* que o *Nagios*, ao apresentar algum problema durante o processo de instalação ou de utilização de um *plugin*, a documentação se mostrou insuficiente. Assim sendo, é possível concluir que de nada adianta possuir muitos *plugins* se os usuários podem não conseguir utilizá-los conforme o esperado. A Tabela 27 demonstra a matriz de avaliação para o critério de documentação dos *softwares*.

[17] *http://docs.cacti.net/plugins*
[18] *http://www.nagios.org/download/addons*
[19] *http://www.zabbix.com/third_party_tools.php*

Tabela 27 – Matriz de avaliação para o critério 10

Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	9	9	0,766
Nagios	1/9	1	5	0,174
Zabbix	1/9	1/5	1	0,058
SOMA	1,222	10,2	15	RC = 0,29

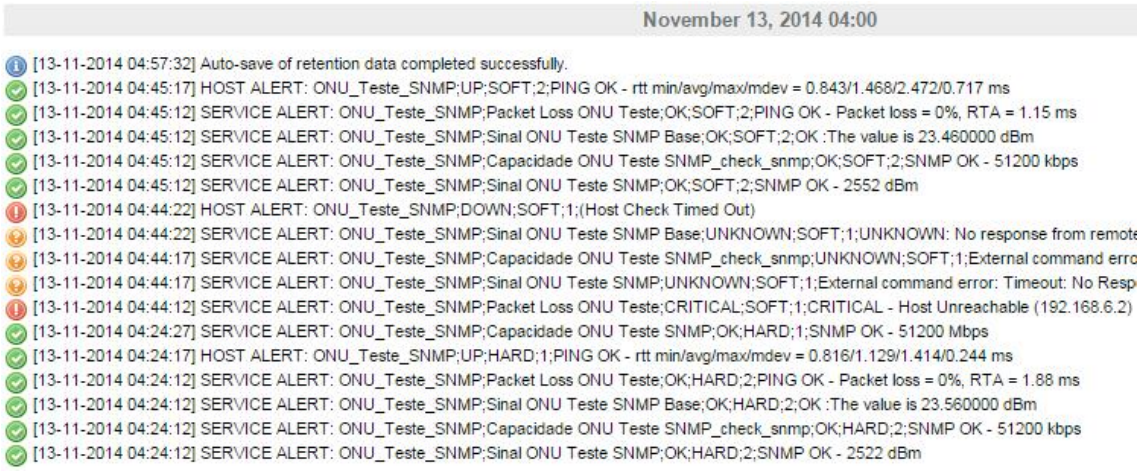
Fonte: Elaborado pelo autor.

Analisando os resultados obtidos na Tabela 27 foi possível observar que o *Cacti* teve grande vantagem no comparativo entre os *softwares* e o *Zabbix* foi o *software* com pior avaliação por possuir documentação insuficiente para possibilitar a correção de eventuais problemas que possam vir a ocorrer com o *software*.

9.11 CRITÉRIO 11 – REGISTRO DE INCIDENTES

No *Nagios* é possível gerar relatórios para cada dispositivo onde são detalhados todos os incidentes ocorridos em um intervalo de tempo (Figura 93). Todos os eventos ocorridos em um dispositivo ficam armazenados no *software* possibilitando consultas futuras.

Figura 93 – Relatório de incidentes por dispositivo gerado pelo *Nagios*



Fonte: Elaborado pelo autor.

O *Cacti* e o *Zabbix* não possuem a funcionalidade de visualização de incidentes ocorridos para os dispositivos, mas apenas os relatórios para SLA, explicados anteriormente. A Tabela 28 apresenta a matriz de avaliação para o critério de registro de incidentes.

Tabela 28 – Matriz de avaliação para o critério 11

Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	1/9	1	0,091
Nagios	9	1	9	0,818
Zabbix	1	1/9	1	0,091
SOMA	11	1,222	11	RC = 0

Fonte: Elaborado pelo autor.

Como o *Nagios* foi o único que atendeu ao requisito, a média obtida foi muito superior à dos *softwares* que não atenderam ao critério.

9.12 CRITÉRIO 12 – INTEGRAÇÃO DE MIBS PROPRIETÁRIAS

Os três *softwares* permitiram a integração de MIBs proprietárias, seja pela *interface Web* do *software* ou pela adição das MIBs diretamente dentro do diretório padrão utilizado pelo SNMP. No *Cacti* e no *Nagios* a importação foi realizada através da cópia das MIBs diretamente para o diretório padrão utilizado pelo SNMP. No *Zabbix* a importação foi realizada através da *interface Web* do *plugin* SNMP *Builder*, que havia sido instalado anteriormente. A Tabela 29 demonstra a matriz de avaliação para o critério de importação de MIBs proprietárias.

Tabela 29 – Matriz de avaliação para o critério 12

Software	*Cacti*	*Nagios*	*Zabbix*	Média
Cacti	1	1	1	0,333
Nagios	1	1	1	0,333
Zabbix	1	1	1	0,333
SOMA	3	3	3	RC = 0

Fonte: Elaborado pelo autor.

Como todos os *softwares* atenderam ao critério de forma bastante similar e nenhum deles se sobressaiu em relação aos demais, os três *softwares* ficaram empatados na avaliação realizada para este critério.

9.13 CONSIDERAÇÕES DO CAPÍTULO

Após a construção das matrizes de avaliação e dos cálculos de consistência para cada critério, foi possível montar a Tabela 30, que apresenta a pontuação total dos critérios para cada *software*.

Tabela 30 – Matriz de pontuação total dos critérios

Critérios	*Cacti*	*Nagios*	*Zabbix*
C1 – Medição de latência	0,333	0,333	0,333
C2 – Medição de perda de pacotes	0,333	0,333	0,333
C3 – Medição de vazão	-	-	-
C4 – Medição de capacidade	0,333	0,333	0,333
C5 – Medição de intensidade de sinal	0,333	0,333	0,333
C6 – Envio e configuração de tipos de alertas	0,333	0,333	0,333
C7 – Facilidade de configuração	0,766	0,173	0,058
C8 – Histórico de SLA	0,058	0,766	0,174
C9 – Usabilidade	0,333	0,333	0,333
C10 – Documentação do *software*	0,766	0,174	0,058
C11 – Registro de incidentes	0,091	0,818	0,091
C12 – Integração de MIBs proprietárias	0,333	0,333	0,333

Fonte: Elaborado pelo autor.

Como os critérios possuem pesos diferentes, na avaliação foi necessário construir uma tabela com as médias dos *softwares* multiplicadas pelo peso de cada critério, para chegar a uma definição de qual o melhor *software* a ser adotado para realizar o monitoramento por SNMP na Bom Tempo Telecom. A Tabela 31 apresenta a matriz de pontuação total dos critérios multiplicados pelo peso de cada um deles.

Tabela 31 – Matriz de pontuação total dos critérios multiplicados pelo peso

(continua)

Critérios	*Cacti*	*Nagios*	*Zabbix*	Peso
C1 – Medição de latência	0,333	0,333	0,333	3
C2 – Medição de perda de pacotes	0,333	0,333	0,333	3
C3 – Medição de vazão	-	-	-	3
C4 – Medição de capacidade	0,333	0,333	0,333	6
C5 – Medição de intensidade de sinal	0,333	0,333	0,333	9

(conclusão)

Critérios	*Cacti*	*Nagios*	*Zabbix*	Peso
C6 – Envio e configuração de tipos de alertas	0,333	0,333	0,333	9
C7 – Facilidade de configuração	0,766	0,173	0,058	9
C8 – Histórico de SLA	0,058	0,766	0,174	6
C9 – Usabilidade	0,333	0,333	0,333	9
C10 – Documentação do *software*	0,766	0,174	0,058	6
C11 – Registro de incidentes	0,091	0,818	0,091	6
C12 – Integração de MIBs proprietárias	0,333	0,333	0,333	9
Total	**28,368**	28,089	18,444	

Fonte: Elaborado pelo autor.

De acordo com a Tabela 31, o *software* mais indicado para realizar o monitoramento por SNMP da estrutura de fibra óptica na Bom Tempo Telecom é o *Cacti*. O *Cacti* obteve leve vantagem sobre o *Nagios*, que foi o segundo colocado, principalmente no critério de facilidade de configuração, ao qual foi atribuído peso 9. O peso 9 foi atribuído para esse critério devido ao fato da utilização e configuração do *software* estar presente diariamente após a implantação. Sendo o sistema simples de configurar, isso representa ganho de tempo e agilidade nas tarefas, sem prejudicar o resultado final.

Outro critério bastante favorável ao *Cacti* foi a grande disponibilidade de informação sobre o *software* e sobre seus *plugins*. A tarefa de adicionar um *plugin* ao sistema torna-se uma tarefa menos complexa quando existe documentação de apoio para realizar a instalação e configuração do mesmo.

Os alertas também são mais fáceis de serem configurados no *Cacti* do que nos outros *softwares*. O *plugin Thold* facilitou muito a configuração, visto que é necessário apenas selecionar um serviço de um dispositivo que está sendo monitorado e configurar o padrão aceitado como normal. Ao identificar que o valor lido está fora do padrão configurado, o sistema envia emails de alerta para notificar os contatos selecionados

O *Nagios* se destacou nos critérios de registro de incidentes e histórico de SLA. Mas como esses critérios não estão presentes no dia-a-dia da operação da Bom Tempo Telecom, receberam um peso intermediário, no caso, peso 6. O *software* necessita de interações manuais para realizar o monitoramento SNMP, o que o torna um pouco trabalhoso de ser configurado. Os alertas teriam sido mais fáceis de ser configurados se não tivesse sido

necessário configurar o *PostFix* do *Linux* para enviar os *emails*. Para essa tarefa foi importante a utilização da documentação encontrada em fóruns do *Nagios*.

Entre os três *softwares* testados, o *Zabbix* é o mais difícil de ser configurado e utilizado. Para criar um monitoramento também é necessário realizar interações manuais. A configuração dos alertas exige um conhecimento básico de programação e não é intuitivo. Demanda a instalação de um *plugin* para o envio de alertas por *email*, o que deveria ser algo básico para um sistema de monitoramento. É necessário percorrer várias telas para realizar configurações simples no *software*. A documentação é escassa e existem poucos *plugins* disponíveis se comparado com o *Cacti*. Por esses motivos ele foi o *software* avaliado com a menor média.

Com o *Cacti* as tarefas ficam mais automatizadas e com menor probabilidade de erros, visto que não são necessárias consultas manuais a cada criação de uma tarefa de monitoramento.

10 CONCLUSÃO

Este trabalho teve por objetivo avaliar *softwares* para realizar o monitoramento SNMP de equipamentos utilizados na estrutura de fibra óptica da Bom Tempo Telecom. Os *softwares* de gerenciamento avaliados foram *Cacti*, *Nagios* e *Zabbix*. Para isso realizou-se um estudo sobre o funcionamento do protocolo SNMP, levantamento dos principais *softwares* utilizados no mercado, funcionamento de redes ópticas do tipo FTTH e estudo dos principais tipos de medições possíveis de serem realizadas através da utilização de SNMP.

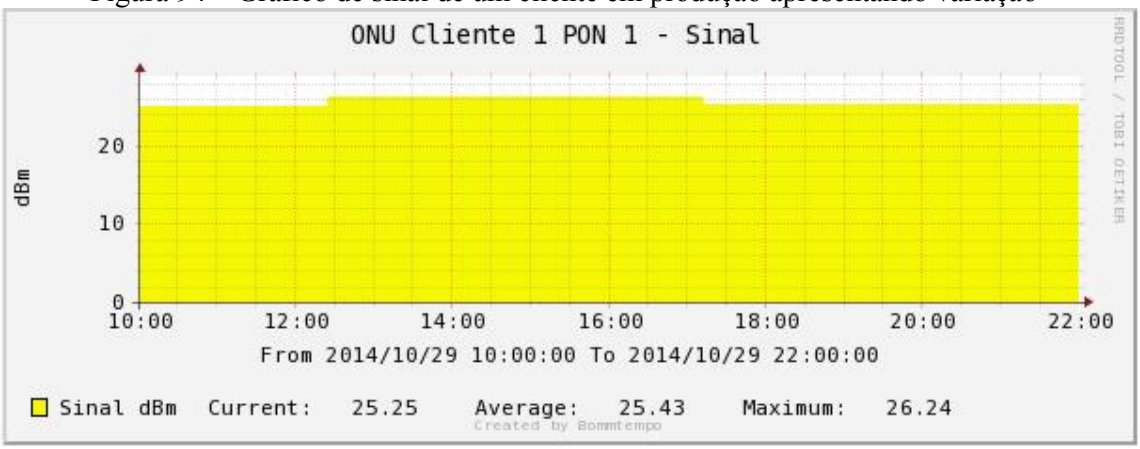
Para realizar as avaliações, foi selecionado o Método Analítico Hierárquico. Baseado neste método foi definido um modelo de avaliação fundamentado em doze critérios, contendo cada um deles um peso definido de acordo com a sua importância para a realização do monitoramento. Os critérios definidos para realizar a avaliação foram: medição de latência, medição de perda de pacotes, medição de vazão, medição de capacidade, medição de intensidade de sinal, envio e configuração de tipos de alertas, facilidade de configuração, histórico de SLA, usabilidade, documentação do *software*, registro de incidentes e integração de MIBs proprietárias. Para a realização dos testes e avaliação dos requisitos, foi utilizada uma ONU de teste disponibilizada pela Bom Tempo Telecom.

Após a realização dos testes e avaliação dos critérios, o *software* que obteve maior pontuação foi o *Cacti*. O *Cacti* demonstrou ser a ferramenta mais simples de ser gerenciada e também de ser mantida devido à simplicidade das suas configurações. Com o *Cacti* foi possível atender dez critérios dos doze critérios avaliados. Os dois critérios que não foram atendidos foram o histórico de SLA e o registro de incidentes. Esses critérios foram muito bem atendidos pelo *Nagios*, que ficou com a média final bastante próxima do *Cacti*, mas deixou a desejar em critérios como a facilidade de configuração, por exemplo. Baseado nessa avaliação, foi possível constatar que para montar um ambiente de monitoramento completo, é necessário utilizar o *Cacti* em conjunto com o *Nagios*. Ao utilizar os dois *softwares* simultaneamente, o *Cacti* fica responsável por coletar os dados de SNMP e armazenar em gráficos, e por fazer o envio de alertas em caso de oscilações nos valores coletados. O *Nagios* por sua vez, monitora os dispositivos através de ICMP e fica encarregado de gerar relatórios de SLA e de disponibilidade da rede.

Os ganhos obtidos com a implantação do *software* puderam ser observados nas primeiras semanas de testes. Através dele, foi possível identificar oscilações de potência óptica nos assinantes. Um caso de uso do monitoramento para a identificação e prevenção de falhas foi após uma manutenção realizada. Após uma manutenção programada em um armário

óptico, o *software* enviou diversos alertas informando que o nível de sinal óptico dos assinantes da porta GPON número 1 do *device* 1 da OLT estava inferior ao valor anterior à manutenção. Através da Figura 94 foi possível identificar uma variação do sinal no horário compreendido entre 12:00 e 12:15h. Ao verificar que o sinal estava fora da faixa configurada como o valor padrão para a leitura SNMP, o *Cacti* passou a emitir alertas informando os responsáveis sobre o problema. Uma equipe técnica da Bom Tempo Telecom foi deslocada até o local do armário onde havia sido realizada a manutenção. Após a realização de uma verificação foi constatado que um cabo óptico estava parcialmente dobrado, o que fez com que o sinal transmitido para os assinantes sofresse atenuação. Na Figura 94 é possível identificar que o nível de sinal foi normalizado no horário entre 17:00 e 17:15h.

Figura 94 – Gráfico de sinal de um cliente em produção apresentando variação



Fonte: Elaborado pelo autor.

Foi constatado que a utilização de um *software* de gerenciamento por SNMP auxilia muito a tarefa de monitorar uma rede de fibra óptica FTTH. E também foi possível concluir que um único *software* pode não ser capaz de realizar um monitoramento eficiente sozinho, podendo necessitar do auxílio de ferramentas ou *softwares* de apoio para monitorar uma rede óptica de maneira eficiente.

Em tempos de grande evolução da prestação de serviços na área de conectividade de rede, o monitoramento pró-ativo de dispositivos e assinantes é algo que se torna indispensável para se ter um diferencial no mercado. Este estudo pode contribuir para a implementação do monitoramento de uma rede óptica FTTH através da utilização do protocolo SNMP utilizando *softwares* gratuitos, bem como o estudo e avaliação das principais características de cada um deles.

Este trabalho teve a exclusão da avaliação do critério de medição de vazão, devido à MIB proprietária da empresa Parks não disponibilizar essa informação para ser coletada através de SNMP. Os demais critérios foram avaliados com êxito.

Tendo em vista a importância de monitorar o tráfego de dados de uma ONU em tempo real, como sugestão para a complementação deste trabalho pode ser citada a interação com o desenvolvedor da MIB proprietária a fim de possibilitar o monitoramento da informação de vazão através de SNMP. Outra sugestão é a criação de um *plugin* para o *Cacti* que faça o armazenamento dos eventos ocorridos com os dispositivos monitorados e também gere relatórios customizados conforme a necessidade do usuário do sistema. Através da criação desse *plugin* seria possível utilizar apenas um *software* de monitoramento, o que simplificaria a tarefa de monitorar uma rede com eficiência.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSIS, Karcius D.R.; WALDMAN, Helio. **Topologia Virtual e Topologia Física de Redes Ópticas: Uma Proposta de Projeto Integrado. 2004**. Disponível em: <http://twa.googlecode.com/svn/dissertacao/bibfile/Karcius%20-%202004%20-%20sbrt%20-%20Projeto%20Integrado.pdf>. Acesso em: 10 abr. 2014.

BANG, Hakjeon; KIM, Sungchang; LEE, Dong-Soo; PARK, Chang-Soo. **Dynamic Bandwidth Allocation Method for High Link Utilization to Support NSR ONUs in GPON**. 2010. Disponível em: <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5440137>. Acesso em: 24 abr. 2014.

BASTOS, Michele P. C. Hemerly. **SCGT – Um conceito de geração de tráfego distribuído**. Disponível em: <http://www.ppgeet.uff.br/index.php/historico/category/3-2008?download=13:dissertao-michele-perpetuo-chequetto-h-bastos-scgt-2008>. Acesso em: 29 mai. 2014.

BATTISTI, Gerson. **Modelo de Gerenciamento para Infra-Estruturas de Medições de Desempenho em Redes de Computadores**. 2007. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/12671/000632788.pdf?sequence=1>. Acesso em: 03 abr. 2014.

BECKER, Pedro Cristiano; MOURA, Marcos Daniel de. **Utilização da Ferramenta Nagios para Monitoramento de Sinal de Antenas de Rede Wireless**. 2012. Disponível em: <http://sites.setrem.com.br/stin/2012/anais/Pedro.pdf>. Acesso em: 28 set. 2014.

BLACK, Tomas Lovis. **Comparação de Ferramentas de Gerenciamento de Redes**. 2008. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/15986/000695315.pdf?sequence=1>. Acesso em: 20 set. 2014.

CALLONI, Allan. **Avaliação de softwares de gestão de riscos**. 2012. 132 f. Monografia (Bacharelado em Sistemas de Informação) – Universidade de Caxias do Sul, Programa de Graduação em Sistemas de Informação, Caxias do Sul, 2012.

CHAGAS, Simone Cintra. **Uma Abrodagem Distribuída para o Problema de Roteamento e Alocação de Comprimentos de Onda em Redes WDM**. 2010. Disponível em: <http://repositorio.unb.br/bitstream/10482/8274/1/2010_SimoneCintraChagas.pdf>. Acesso em: 08 mai. 2014.

COELHO, Sara Catarina Rasteiro. **Fibra Óptica na Rede de Acesso:** Tecnologias e Soluções. 2009. Disponível em: <https://ria.ua.pt/bitstream/10773/7435/1/245167.pdf>. Acesso em: 21 abr. 2014.

CONTESSA, Diego Fraga; POLINA, Everton Rafael. **Gerenciamento de Equipamentos Usando o Protocolo SNMP**. 2010. Disponível em: <http://petry.pro.br/arquivos/Artigo_Gerenciamento_SNMP_MRTG.pdf>. Acesso em: 07 jun. 2014.

DIAS, Beethovem Zanella; JUNIOR, Nilton Alves. **Protocolo de Gerenciamento SNMP**. 2002. Disponível em: <http://www.rederio.br/downloads/pdf/nt00601.pdf>. Acesso em: 07 jun. 2014.

ESTEVES, Antonio Matheus Benaion. **Sistema de Monitoramento de Redes baseado nos protocolos SNMP e Spanning Tree**. 2013. Disponível em: <http://cbpfindex.cbpf.br/publication_pdfs/Dissertacao_AntonioBenaion.2014_01_09_11_55_36.pdf>. Acesso em: 05 jun. 2014.

FERREIRA, Ana Elisa Leitão Alonso. **Engenharia de tráfego em redes IP:** estudo e aplicação de ferramentas de medição. 2005. Disponível em: <http://www2.ic.uff.br/PosGraduacao/Dissertacoes/259.pdf>. Acesso em: 27 mai. 2014.

FREITAS, André Luís Policani; MARINS, Cristiano Souza; SOUZA, Daniela de Oliveira. **A metodologia de multicritério como ferramenta para a tomada de decisões gerenciais: um estudo de caso**. 2006. Disponível em: <http://revista.feb.unesp.br/index.php/gepros/article/viewFile/116/66>. Acesso em: 29 out. 2014.

GALDINO, Lídia. **Análise de Desempenho de Redes Ópticas Híbridas WDM/OCDM**. 2008. Disponível em: <http://www.bibliotecadigital.unicamp.br/document/?down=000435988>. Acesso em: 10 mai. 2014.

GUGLIELMETTI, Fernando Ribeiro; MARINS, Fernando Augusto Silva; SALOMON, Valério Antonio Pamplona. **Comparação teórica entre métodos de auxílio à tomada de decisão por múltiplos critérios**. In: XXIII Encontro Nac. de Eng. de Produção - Ouro Preto, MG, Brasil, 21 a 24 de out de 2003.

GUIMARÃES, Vinícius Tavares. **Amostragem Aleatória Estratificada Adaptativa para Identificação de Fluxos "Elefantes" em Redes Convergentes**. 2007. Disponível em: <http://repositorio.pucrs.br/dspace/handle/10923/3158>. Acesso em: 16 abr. 2014.

JAY, Stephan; NEUMANN, Karl-Heinz; PLÜCKEBAUM, Thomas. **Comparing FTTH access networks based on P2P and PMP fibre topologies**. 2013. Disponível em: <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5897963>. Acesso em: 25 mai. 2014.

JORDÃO, Bruno Miguel da Cruz. PEREIRA, Susete Rodrigues. **A Análise Multicritério na Tomada de Decisão - O Método Analítico Hierárquico de T. L. Saaty:** Desenvolvimento do método com recurso à análise de um caso prático explicado ponto a ponto. 2006. Disponível em: <http://pt.scribd.com/doc/94888515/Met-Analitico-Hierarquico-Caso-Pratico-DOC>. Acesso em: 14 jun. 2014.

JU-GUANG, L.; JUN, Q.; DONG-MING, T.. **HFC equipment management based on SNMP protocol**, 2011, p. 115-119. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6008211/>. Acesso em: 26 abr. 2014.

KOCH, Moisés. **Uma Proposta de Solução de Gerenciamento de Contabilização utilizando Nagios e Cacti**. 2008. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/15980/000695290.pdf?sequence=1>. Acesso em: 08 jun. 2014.

KUROSE, James F.; ROSS, Keith W.. **Redes de computadores e a Internet**: uma abordagem top-down. 3ª edição. São Paulo: Pearson Education do Brasil.

LAGE, Luíza Basílio; OLIVEIRA, Maria Clara Alcântara. **Estudo de uma Rede de Acesso via Fibra Óptica**. 2006. Disponível em: <http://bdm.bce.unb.br/bitstream/10483/849/1/2006_LuizaLage_MariaClaraOliveira.pdf>. Acesso em: 20 abr. 2014.

MOHANDAS, Karthika; JAYASREE, V. K.; VARGHESE, Samuel. **A simple in-service monitoring system for passive optical networks**. 2013. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6686351>. Acesso em: 14 abr. 2014.

MORAES, Edmilson Alves; SANTALIESTRA, Rodrigo. **Modelo de decisão com múltiplos critérios para escolha de software de código aberto e software de código fechado**. Organizações em contexto, Ano 4, n. 7, junho 2008. Disponível em: < http://www.spell.org.br/documentos/download/5923>. Acesso em: 10 jun. 2014.

MOTOYAMA, S.. **Redes de Telecomunicações:** Análise de Desempenho. 2006. Disponível em: <http://www.dt.fee.unicamp.br/~motoyama/ie670/aulas/06-2aula-15.pdf>. Acesso em: 02 abr. 2014.

OLIVEIRA, Patrícia Beneti de. **Soluções de Atendimento em Fibra Óptica I**. 2010. Disponível em: < http://www.teleco.com.br/tutoriais/pdf2011/tutorialsolfo1.pdf>. Acesso em: 12 abr. 2014.

PAIVA, Pedro Gustavo de Farias. **Ambiente Integrado para Gerenciamento da Rede Interna da Secretaria da Receita da Paraíba (SER-PB)**. 2010. Disponível em: <http://www.cin.ufpe.br/~pasg/gpublications/pgfp10-monografia-esp.pdf>. Acesso em: 04 mai. 2014.

RAMOS, Sérgio Filipe Carvalho. **Redes "Fiber To The Home – FTTH": O Despertar de Novos Serviços de Telecomunicações**. 2009. Disponível em: <http://recipp.ipp.pt/bitstream/10400.22/3652/1/ART_SergioRamos_2009_NAT.pdf>. Acesso em: 12 abr. 2014.

RFC1157. A Simple Network Management Protocol (SNMP). Disponível em: <http://tools.ietf.org/html/rfc1157> Acesso em: 07 jun. 2014.

RFC1213. Management Information Base for Network Management of TCP/IP-based internets: MIB-II. Disponível em: <http://tools.ietf.org/html/rfc1213> Acesso em: 07 jun. 2014.

RFC1262. Guidelines for Internet Measurement Activities. Disponível em: <http://tools.ietf.org/html/rfc1262> Acesso em: 16 abr. 2014.

RFC2578. Structure of Management Information Version 2 (SMIv2). Disponível em: <http://tools.ietf.org/html/rfc2578> Acesso em: 17 jun. 2014.

SALOMON, Valério A. P. **Auxílio à Decisão para a Adoção de Políticas de Compras. Produto & Produção,** vol. 6, n. 1, p. 01-08, fev 2002.

SANTOS, Madson da Silva. **Estudo de gerenciamento da rede de distribuição com o protocolo SNMP e tutorial para implantação de ferramentas de gerência**. 2006. Disponível em: <http://www.pop-pi.rnp.br/system/uploads/article/archive/6/Madson_ProjetoGerenciamento_2006.pdf>. Acesso em: 10 jun. 2014.

SANTOS, Cinthia Cardoso dos. **Gerenciamento de Redes com a Utilização de Software Livre**. 2009. Disponível em: <http://www3.iesam-pa.edu.br/ojs/index.php/sistemas/article/viewFile/442/374>. Acesso em: 13 jun. 2014.

SILVA, Eron da. **Implantação de uma Rede de Acesso GPON**. 2012. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/1829/1/CT_GESER_II_2012_06.pdf>. Acesso em: 14 abr. 2014.

SILVEIRA, Tiago Zattera. **A Tecnologia da Informação como ferramenta de suporte à gestão da inovação**. 2011. Disponível em: <http://tede.ucs.br/tede_simplificado/tde_busca/arquivo.php?codArquivo=359>. Acesso em: 10 jun. 2014.

TAKEUTI, Paulo. **Projeto e Dimensionamento de Redes Ópticas Passivas (PONs)**. 2005. Disponível em: < http://www.livrosgratis.com.br/arquivos_livros/cp028641.pdf>. Acesso em: 18 abr. 2014.

TANENBAUM, Andrew S.. **Computer Networks**. 2003. Disponível em: <http://www.ebah.com.br/content/ABAAAfuQkAA/tanenbaum>. Acesso em: 10 abr. 2014.

ANEXO 1

O processo de instalação do Zabbix consistiu basicamente em fazer o *download* dos pacotes de instalação através do comando "*yum install*" do *CentOS*, ajustar a configuração de fuso horário do PHP de Europa/Riga para America/São_Paulo e criar o banco de dados. O guia utilizado para realizar a instalação não previa a instalação do pacote "*mysql-server*", o que fazia com que não fosse possível criar um banco de dados sem possuir um Sistema Gerenciador de Banco de Dados (SGBD) instalado. A instalação foi realizada através do comando "*yum install mysql-server*". Após realizada a instalação do SGBD, o sistema foi reiniciado para sincronizar todos os processos. Ao inicializar novamente, foi verificado que os serviços do SGBD e do servidor *Web* não haviam sido inicializados automaticamente. Para corrigir esse problema foi executado o utilitário "*ntsysv*" e os serviços que não haviam sido inicializados foram habilitados para iniciar automaticamente.