FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Wesley Roberto Soares

Monitoramento de infraestrutura de redes backbone através do Zabbix

Americana, SP

2018

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Wesley Roberto Soares

Monitoramento de infraestrutura de redes backbone através do Zabbix

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do professor Alberto Martins Júnior

Área de concentração: Infraestrutura de redes.

Americana, SP

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

S657m SOARES, Wesley Roberto

Monitoramento de infraestrutura de redes backbone através do zabbix. / Wesley Roberto Soares. – Americana, 2018.

37f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. MARTINS JÚNIOR, Alberto

1 Software livre 2. Transmissão de dados 3. Cabeamento de redes I. MARTINS JÚNIOR, Alberto. II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.3.05
681.519

Wesley Roberto Soares

Monitoramento de infraestrutura de redes backbone através do Zabbix

Trabalho de conclusão de curso apresentado à Faculdade de Tecnologia de Americana como parte dos requisitos para obtenção do título de Tecnólogo em Segurança da Informação
Área de concentração: Infraestrutura de redes.

Americana, 03 de Dezembro de 2018.

Banca Examinadora:

Alberto Martins Júnior (Presidente)
Mestre
Faculdade de Tecnologia de Americana

Wladimir da Costa (Membro)
Mestre
Faculdade de Tecnologia de Americana

Clerivaldo Jose Roccia (Membro)
Mestre
Faculdade de Tecnologia de Americana

DEDICATÓRIA

Dedico este trabalho, primeiramente a Deus, e aos meus pais e esposa que sempre me mostraram a importância e o valor do conhecimento. Agradeço também a todos os professores por todo apoio e pelos ensinamentos passados ao longo destes anos.

RESUMO

O presente trabalho aborda uma questão fundamental para o bom funcionamento de uma rede *backbone*, o monitoramento. Uma rede *backbone* também conhecida como espinha dorsal é o canal ou meio físico onde os dados de diferentes localidades trafegam, a rede *backbone* pode ser intercontinental, internacional, interestadual e até mesmo regional, o presente trabalho apresentará as características principais bem como o as ativos e equipamentos necessários para um *troubleshooting* dentro do SLA (Acordo de Nível de Serviço) mínimo estabelecido em acordo contratual, nesse ínterim é possível garantir segurança da informação em uma de suas bases a disponibilidade ao observar de que maneira a rede *backbone* está tratando o tráfego e as garantias quando necessárias ao contratar a última milha. Ter a rede *backbone* mapeada e monitorada é fundamental para o processo de crescimento de uma prestadora de serviços, provedor de TI ou operadora de telecomunicações. Para desenvolver esse trabalho foi utilizado a ferramenta Zabbix, ela possui código aberto (*Open Source*) que torna sua utilização mundialmente conhecida, pois reúne todos os recursos de outras ferramentas de monitoramento como as já conhecidas Nagios e Cacti. É uma ferramenta confiável de fácil instalação e utilização. Essa ferramenta faz monitoramento em tempo real do desempenho, disponibilidade e inventário dos ativos de uma rede, utilizando coletas de informações de servidores, roteadores, *switches*, computadores, *notebooks* e todos os equipamentos que estiverem conectados na rede. A partir dessa coleta é possível fazer o gerenciamento da rede afim de identificar, prevenir e solucionar vários problemas, desde a troca de ativos até a infraestrutura física e lógica da rede, evitando a ineficiência da rede ou a mesma deixar de funcionar, gerando prejuízos para a empresa, clientes e consumidores finais.

Palavras-chave: Gerenciamento de rede; Zabbix; Rede backbone.

ABSTRACT

The present work addresses a fundamental issue for the proper functioning of a backbone network, the monitoring. A backbone network also known as backbone is the channel or physical medium where data from different locations travel, the backbone network can be intercontinental, international, interstate and even regional, the present work will present the main characteristics as well as the active and equipment required for a troubleshooting within the SLA (Minimum Service Level Agreement) established in a contractual agreement, in the meantime it is possible to guarantee information security on one of its bases availability by observing how the backbone network is handling the traffic and the guarantees when needed when hiring the last mile. Having the mapped and monitored backbone network is critical to the growth process of a service provider, IT provider or telecom operator. To develop this work was used the tool Zabbix, it has open source (Open Source) that makes its use worldwide known, because it brings together all the resources of other monitoring tools such as the well-known Nagios and Cacti. It is a reliable tool that is easy to install and use. This tool makes real-time monitoring of the performance, availability, and inventory of network assets by collecting information from servers, routers, switches, computers, notebooks, and any equipment that is connected to the network. From this collection it is possible to manage the network in order to identify, prevent and solve various problems, from the exchange of assets to the physical and logical infrastructure of the network, avoiding the inefficiency of the network or it ceases to function, generating losses to the company, customers and final consumers.

Keywords: *Network management; Zabbix; Backbone network.*

SUMÁRIO

1 INTRODUÇÃO

O objetivo deste estudo é mostrar a importância do monitoramento da infraestrutura de rede *backbone*, ou seja, observar, em um determinado período tempo ou tempo real, se as condições dos ativos e enlaces estão dentro dos padrões estabelecidos, aliado a um *software* capaz de simplificar a leitura do comportamento do *hardware* de forma rápida, clara e eficiente e uma central de operações de rede que avalia os dados e toma ação sobre os riscos detectados.

Foi apresentado a função de uma equipe NOC, e quais as melhores práticas no monitoramento de ativos em um enlace *backbone* em tem real, essa equipe toma ações baseados no monitoramento de ativos e passivos que compõe a rede, o NOC utiliza ferramentas de monitoramento que coletam dados através do agente SNMP dos equipamentos, o tempo de análise deve ser rápido e as decisões acertadas pois a demora na normalização de um link pode causar desde saturação até perda total de uma abordagem.

Utilizou-se a ferramenta Zabbix afim de monitorar alguns ativos e passivos e avaliar como o comportamento detectado pode influenciar nas decisões a serem tomadas. Essas por sua vez devem estar associadas à análise de risco e plano de resposta a incidentes. A dupla abordagem, ou seja, enlaces redundantes ajudam a criar um ambiente mais seguro e evitar que os usuários finais sejam afetados de forma direta, porém o custo é dobrado e os ativos devem suportar os protocolos.

Este trabalho apoiou-se no mapeamento de processos presentes no ITIL (*Information Technology Infrastructure Library*)

Por fim, as ferramentas de *troubleshooting* e suas definições ajudam a cumprir os SLAs propostos e acordados na entrega do serviço, a ferramenta adequada traz soluções rápidas e exatas sobre a tratativa de qualquer incidente na rede.

Na pesquisa foram utilizados dados reais de um CRM (*Customer Relationship Management*), sistema que armazena todas as informações dos clientes e controla os atendimentos do NOC e também foram coletados dados do *software* de monitoramento Zabbix, pertencente a um Provedor de Tecnologia da Informação e Comunicação da RMC (Região Metropolitana de Campinas).

As considerações finais apresentam conclusões relevantes dos resultados das simulações e testes, de forma que seja possível avaliar critérios para alcance de resultados, onde software, hardware, análise e processos entregam valor a negócios.

2 GERENCIAMENTO DE REDES

Segundo Kurose (2006), gerenciamento de rede inclui o oferecimento, a integração e a coordenação de elementos de *hardware*, *software* e humanos, pra monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer as exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável.

Russo (2013) afirma que o monitoramento é o ato de observar, em um determinado período tempo, se as condições de um equipamento estão dentro dos padrões estabelecidos. Russo também afirma que além da detecção de interrupções de serviços, o monitoramento é responsável por coletar informações de determinados equipamentos/serviços e armazenar estas informações de modo que seja possível prevenir e ou dimensionar o futuro, com as informações coletadas no passado, de forma mais assertiva.

Foi apresentado a importância de três componentes essenciais para o bom funcionamento de uma rede *backbone*, um *software*, uma equipe especializada e uma infraestrutura adequada, respectivamente o Zabbix, NOC (*Network Operation Center*) e uma rede com capacidade acima de 10 *Gigabits*.

2.1 Gerenciamento de incidentes

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de redes de computadores (CERT.BR, [s.d]).

Russo (2013) conclui que a identificação de incidentes e o tratamento adequado, ou seja, restabelecer o serviço de forma eficiente e eficaz minimizando o impacto negativo sobre o serviço é algo esperado e fundamental dentro de uma organização. E todo este trabalho, somente pode ser realizado com sistemas capazes de identificar os incidentes, atuando de forma pró ativa. Para todo este processo, é concedido o nome de Gerenciamento de Incidentes.

A grande vantagem do monitoramento de equipamentos/serviços é a capacidade de medir a qualidade do serviço que o Item de Configuração fornece. Com base nesta medição é possível analisar, identificar possíveis “pontos fora da curva”,

planejar de forma mais assertiva o futuro tendo como base os fatos ocorridos no passado.

Cabe a equipe da central de operações de rede mais conhecido como o NOC (*Network Operation Center*) a análise do incidente ou evento.

2.2 ZABBIX

Zabbix é uma solução em software livre para monitoramento de infraestrutura de rede de uma empresa, provedor ou qualquer rede seja ela local ou não. É um *software* que monitora vários parâmetros de diversos ativos em uma rede de computadores.

O Zabbix é uma ferramenta moderna, *open source* e multiplataforma, com sistema de monitoramento distribuído, capaz de monitorar a disponibilidade e o desempenho da infraestrutura de uma rede, além de aplicações (LIMA, 2014, p.192). Sua principal vantagem é a facilidade de manipulação dos objetos, o que agiliza muito o trabalho do dia-a-dia, por exemplo, ao se obter 50 *switches* iguais com a finalidade de monitorar o tráfego de rede de cada porta, será necessário configurar os itens de cada porta uma única vez e salvá-los como *template*, depois basta usar este *template* para os 50 *switches*. Cria-se os gráficos apenas do primeiro switch e depois é necessário copiar para os outros 49, tudo isso selecionando itens e clicando em botões como *copy* e/ou clone (LIMA, 2014, p.193).

A solução Zabbix é composta por cinco elementos: Servidor é responsável pela coleta dados para o monitoramento sem agentes e de agentes. Quando detecta alguma anormalidade, alertas são emitidos visualmente e através de uso de sistemas de comunicação como *e-mail*, mensagens de texto, *google talk* e etc. Banco de dados faz o armazenamento de dados. Componente de Banco de Dados Relacional que armazena e relaciona os dados em tabelas. Interface *Web* provida para dar acesso ao Servidor Zabbix, a partir de qualquer lugar e a qualquer dispositivo que interprete HTML (LIMA, 2014, p.193).

Lima afirma que *Proxy* é um componente opcional para monitoramento distribuído. O *Proxy* pode coletar dados de disponibilidade e *performance* a favor de um Servidor Zabbix. Pode ser benéfico ao servidor Zabbix, distribuir a carga de monitoramento entre vários *Proxys.* Além disso, com o *Proxy* é possível monitorar

ambientes onde a segurança é mais restrita ao ponto de não ser permitido acesso as configurações do *firewall*.

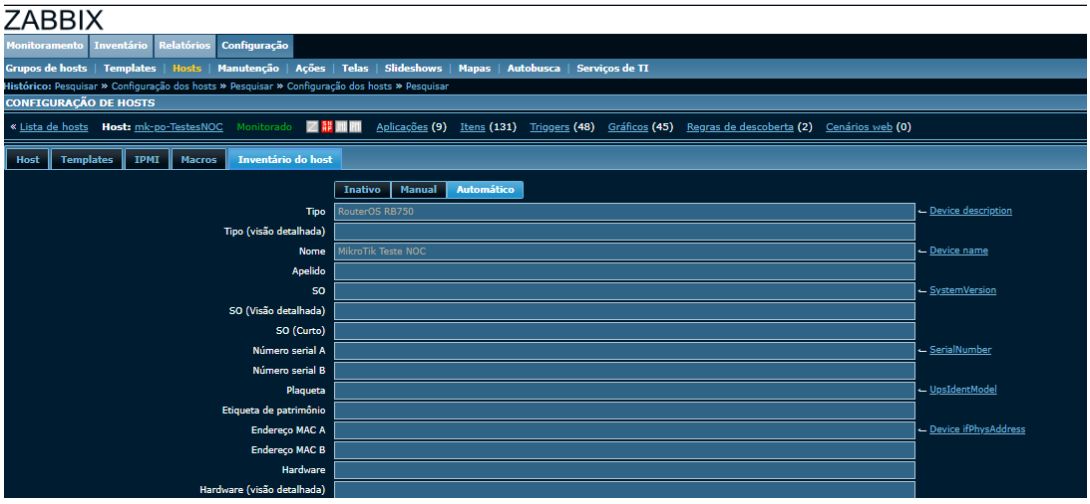
E para finalizar o agente Zabbix que é instalado nos *hosts*, permite coletar métricas comuns específicas de um sistema operacional, como processador e memória. Além disso, o agente Zabbix permite a coleta de métricas personalizadas com uso de *scripts* ou programas externos permitindo a coleta de métricas complexas e até tomada de ações diretamente no próprio agente Zabbix; (LIMA, 2014, p.193).

2.3 Gerenciamento de Hosts através do Zabbix

A partir desse estudo de Jansen Lima, concluiu-se que se pode fazer um gerenciamento eficiente, pois no seu controle de grupos é feita a utilização de *templates* que controlam os *hosts* e padronizam o processo. O grupo de *hosts* tem a finalidade de separar os *hosts* por grupos ou departamentos de uma empresa enquanto o inventário é onde ficam guardadas as informações relacionadas aquele *host*.

A aba Inventário do *host* é utilizada para cadastramos as informações de *hardware* e software do *host* monitorado. Por padrão essa opção vem desabilitada podendo ser utilizada manualmente ou de forma automática pelo sistema.

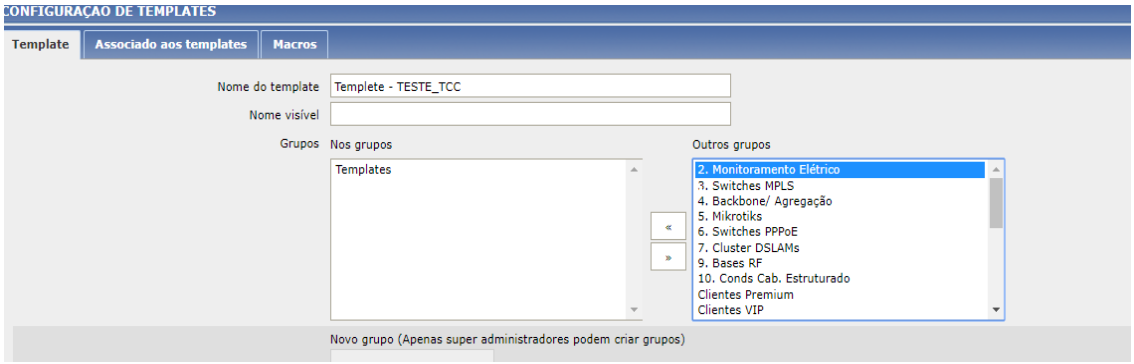
Figura: Inventário



Fonte: Próprio autor

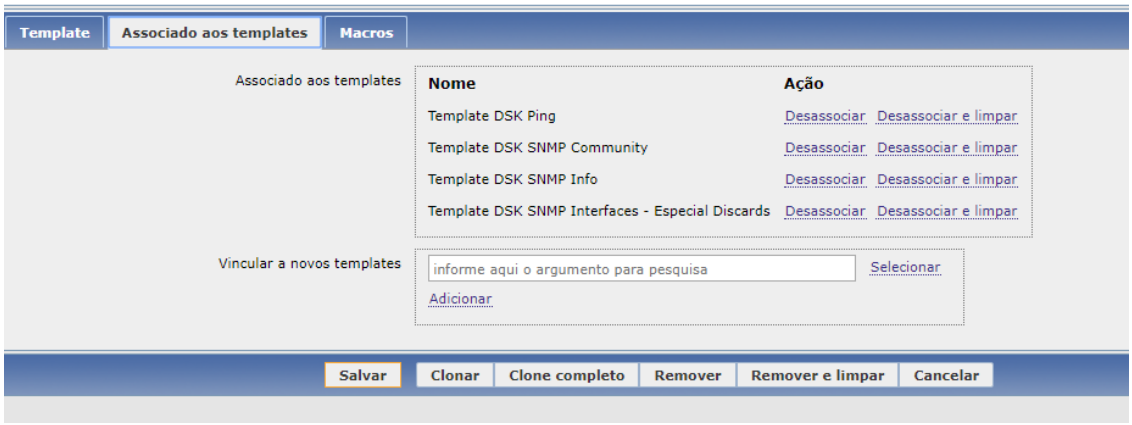
Segundo Lima (2014), *Template* define um conjunto de configurações a serem aplicadas em um determinado grupo de *host* afim de associar a uma *trigger* que é um aviso ou mensagem relacionado ao comportamento do *host*, assim identificamos se há alguma anormalidade para que possamos tomar ação.

Figura: *Template*



Fonte: Próprio autor

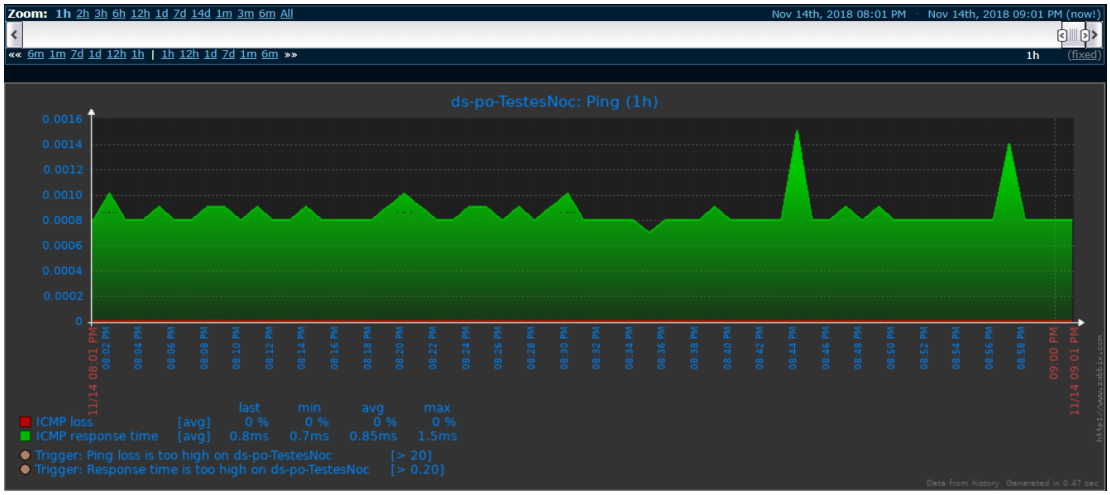
Figura: Associado aos *templates*



Fonte: Próprio autor

Usa-se gráficos para visualizar períodos específicos, navegar através da linha de tempo ou selecionar apenas uma parte do gráfico para visualizar além de mostrar tendência, os mapas tornam a visão mais ampla possibilitando uma análise mais global da rede como um todo.

Figura: Gráficos

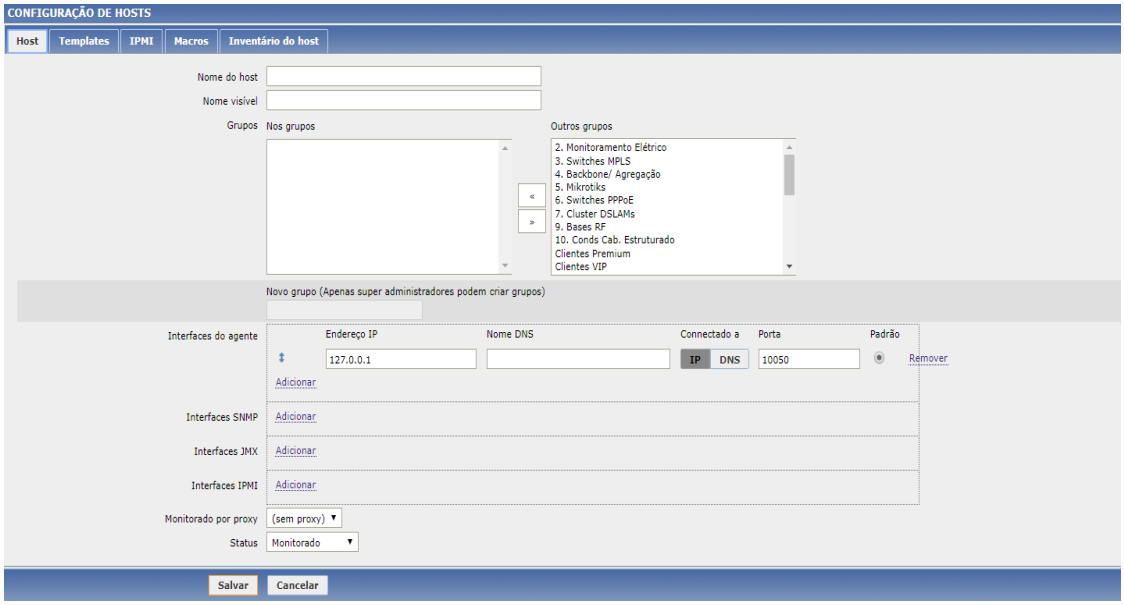


Fonte: Próprio Autor

Para finalizar a tela de cadastro de *host*, temos disponível na aba *host* a opção de selecionarmos por qual interface será realizado o monitoramento do *host* (LIMA, 2014, p.73).

Vejamos a figura a seguir:

Figura: *Host*



Fonte: Próprio autor

2.4 NOC

O NOC (*Network Operation Center*) é a central de operações de rede, é equipe de análise e *troubleshooting* sobre incidentes, requisições e eventos na rede, essa equipe monitora em tempo real o estado dos *hosts* e baseado na coleta de SNMPs analisa se há alguma anomalia ou algo que possa interromper os serviços.

Dentro deste contexto, conforme CROCA; DOMINGOS; SILVA (2001, apud Oliveira 2008), centro de operações de redes, comumente chamado de NOC (*Network Operation Center*) desempenha um papel essencial em determinadas empresas de Telecom e TI. O NOC é responsável pela verificação de falhas na infraestrutura, pela monitoração de problemas apontados pelos clientes (ou não) e, também, pelo suporte dado a solução destes obstáculos. Para OMARI; AL-ZUBAIDY (2005 apud Oliveira 2008), o NOC de um Datacenter se caracteriza como uma central de monitoramento de multiserviços, tanto de TI como de Telecomunicações, este não se identifica a um *Call Center*, pois difere nas atividades técnicas diversificadas e de alta tecnologia.

Os mapas de processos relacionados ao NOC são de extrema importância para a criação de valor agregado aos clientes e a garantia da qualidade nas prestações de serviços.

Os atendimentos do NOC são diretamente relacionados à quantidade de produtos oferecidos e as tecnologias empregadas na infraestrutura que corroboram no envolvimento de diferentes serviços e tecnologias no processo da gestão da qualidade. (ISO:9000, 2001).

2.4.1 Acordos de Níveis de Serviço

A importância dos Acordos de Níveis de Serviços passa pela garantia contratual na entrega de serviços confiáveis, atendimentos dentro de prazos previamente estabelecidos, qualidade de serviços e a manutenção dos negócios. De acordo com Lewis (1999, apud Oliveira 2008), os Acordos de Níveis de Serviços (SLA - *Service Level Agreement*) são baseados na qualidade dos atendimentos e nas descrições dos itens contratados, os seus critérios são redigidos e legitimados por meio de contratos empresariais entre duas empresas. Estes procuram entregar os serviços/produtos vendidos aos seus clientes, assim como estabelece as

responsabilidades de ambas as partes, criando os critérios de qualidade e de cobrança e/ou descontos. Isto requer uma gestão eficaz de ambas às partes, por este motivo são utilizados os métodos de Gestão de Níveis de Serviço conhecido como SLM – *Service Level Management.*

Como o NOC é a o setor que realizada os serviços e a reparação dos ativos monitorados, a responsabilidade por eventuais quebras de contrato por não cumprimento de SLA pode ser computado ao mesmo, nesse ínterim documentar qualquer justificava íntegra e verdadeira vem a ajudar em uma reversão de cancelamento.

2.4.2 ITIL - *Information Technology Infrastructure Library*

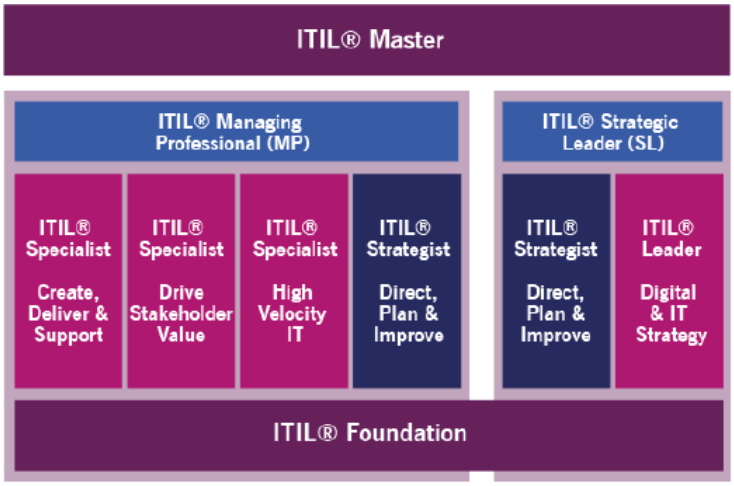
O ITIL (*The IT Infrastructure Library*) foi criado pela Agência de Telecomunicações e Computação do governo do Reino Unido – CCTA *(UK government's Central Computer and Telecommunications Agency)*, tendo como seu principal objetivo, a criação de um guia com as melhores práticas na gestão de serviços voltados à Tecnologia da Informação. Atualmente, o ITIL possui diversos processos para gerenciamento de serviços que são divididos entre duas subáreas: serviços de suporte e serviços de entrega.

Os processos e funções relacionadas ao NOC são descritos na seguinte ordem: Service Desk (função); Serviços de Suporte com a Gerência de Incidentes, Gerência de Problemas e Gerência de Mudanças; Serviços de Entrega com a Gerência de Nível de Serviço e Gerência de Capacidade

Segundo anunciado pela TI Exames Em 1 de outubro de 2018, AXELOS anunciou o novo esquema de qualificação ITIL 4 na Conferência Fusion2018 sobre gerenciamento de serviços.

Abaixo está o novo esquema.

Figura: ITIL Master



Fonte: Axelos(2018) [1]

O novo esquema compreende os seguintes módulos:

- ITIL *Foundation*
- ITIL *Specialist* (existem 3 módulos distintos)
- ITIL *Strategist*
- ITIL *Leader*
- ITIL *Master*

A certificação ITL 4 Foundation será obrigatória para avançar para os módulos seguintes. Para prestar este exame do nível *Foundation* não será necessário passar por treinamento credenciado, ou seja, ainda será permitido o auto estudo.

Os títulos dos módulos avançados ficaram bem mais atrativos. Apenas com um curso/exame o profissional pode se tornar ITIL "*Specialist*", "*Strategist*" ou "*Leader*". Essa mudança a AXELOS implementou porque houve muitas queixas com a venda dos cursos do nível intermediário no esquema da v3, pois muitos profissionais não enxergavam valor em obter um título "*Intermediate*".

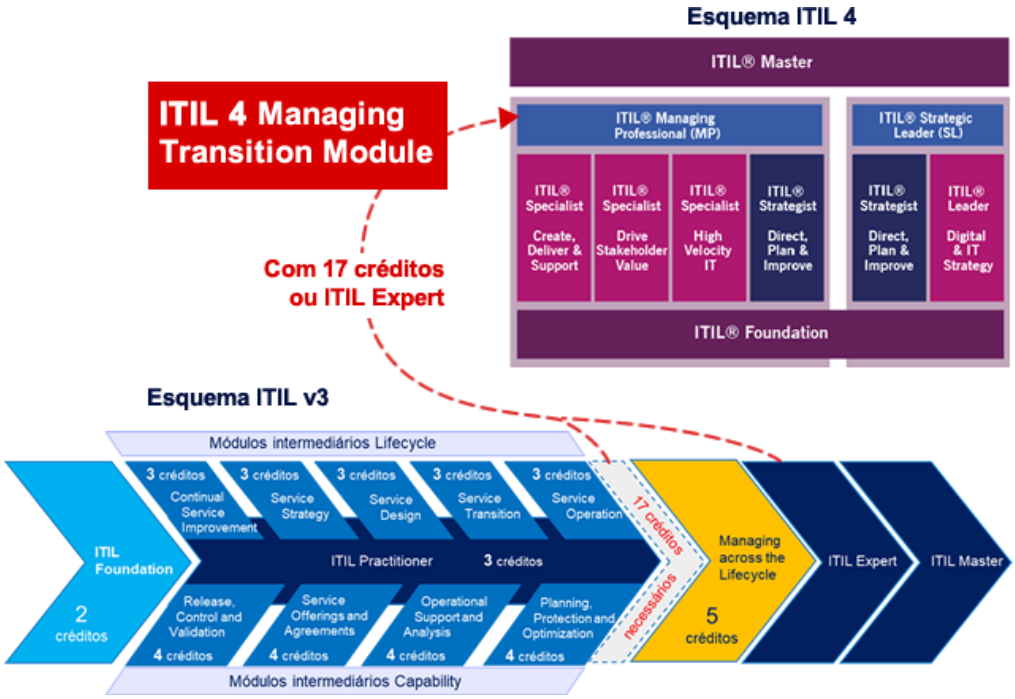
O novo esquema não é baseado em créditos como no esquema da v3. Para obter a credencial ITIL *Managing Professional* (ITIL MP) ou ITIL *Strategic Leader* (ITIL SL), o profissional precisa completar todos os módulos da trilha correspondente, sendo que o módulo ITIL *Strategist* é universal nas duas trilhas. Por exemplo, para obter o título ITIL MP, após ser certificado ITIL 4 *Foundation*, o profissional precisará

[1] Disponível em:< https://www.axelos.com/itil-update>. Acesso em 15 de nov de 2018.

completar 3 módulos *Specialist (Create, Deliver & Support, Drive Stakeholder Value e High Velocity IT)* e o módulo ITIL *Strategist Direct, Plan & Improve.*

Segue modelo de transição entre as versões:

Figura:Transição



Fonte: Axelos(2018)[2]

A AXELOS também informa que os exames da ITIL v3 poderão ser oferecidos até meados de 2020. E será confirmado com pelo menos 6 meses de antecedência da data oficial de descontinuidade desses exames. Então haverá tempo suficiente para que todos os profissionais que já iniciaram os estudos pelo esquema da ITIL v3 possam completar os créditos necessários para o módulo de transição para ITIL 4.

2.4.3 – Gerência de Evento

Segundo Palma (2013), um evento pode ser definido como qualquer mudança de estado que tem importância para a gestão de um item de configuração (IC) ou serviço de TI. Em outras palavras, qualquer ocorrência dentro do escopo de TI que tenha relevância para a gestão dos serviços entregues ao(s) cliente(s).

[2] Disponível em:< https://www.axelos.com/itil-update>. Acesso em 14 de nov de 2018.

Um evento tem diversas naturezas, portanto devem ser categorizados por nomenclaturas como: normal; não usual, exceção, alerta, ou quaisquer outras classificações relevantes.

Os eventos são normalmente reconhecidos através de notificações criadas por ferramenta de monitoramento.

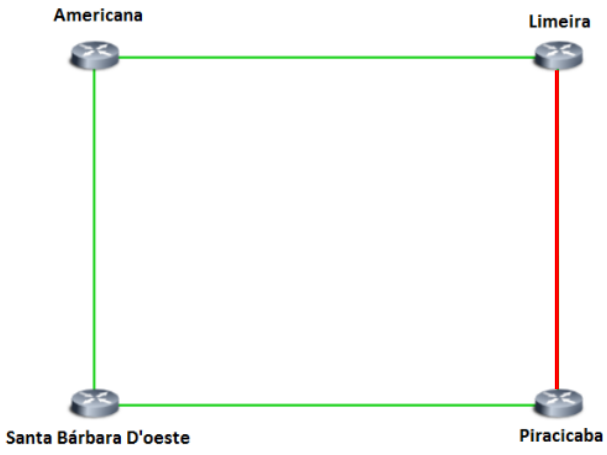
2.4.4 Gerência de Incidentes

Para Palma (2013), um incidente é definido pela ITIL como uma interrupção não planejada de um serviço de TI ou redução da qualidade de um serviço de TI. Um incidente é qualquer evento que causa interrupção no serviço.

Gerenciamento de incidentes é o processo responsável por gerenciar o ciclo de vida de todos os incidentes. Incidentes podem ser identificados equipe técnica, detectado e relatado por ferramentas de monitoramento de eventos, comunicações de usuários, ou relatadas por terceiros fornecedores e parceiros.

Para exemplificar foram construídos cenários que mostram desde o alarme até a recuperação total do enlace. O cenário a seguir mostra um exemplo de incidente em um enlace *backbone* composto por quatro POPs (Pontos de Presença), os quatro formam um anel com capacidade de 40Gbs de tráfego e a causa da indisponibilidade foi um rompimento de cabo *óptico* causado por caminhão com carga.

Figura: Anel

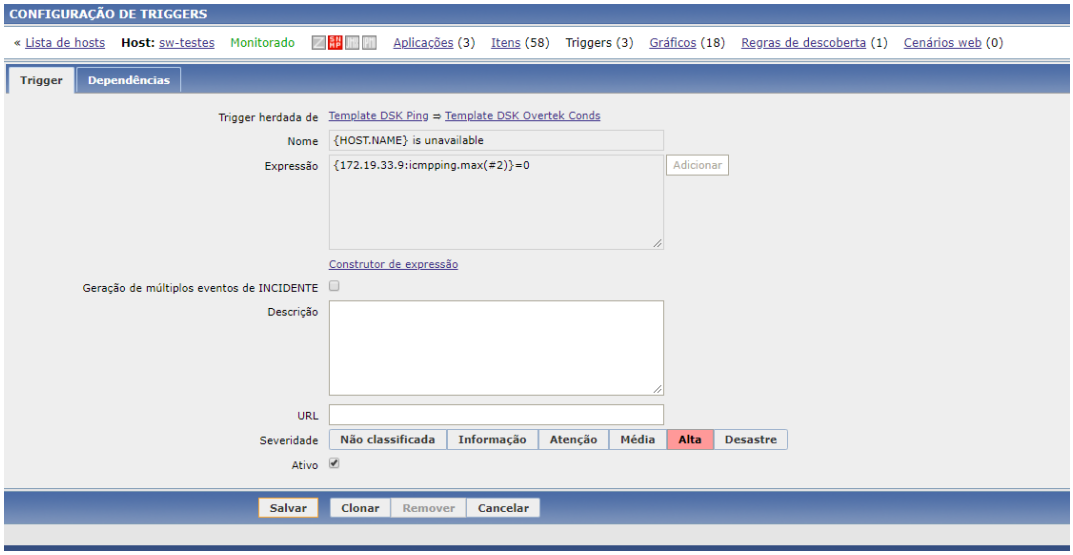


Fonte: Próprio autor

Assim que o rompimento é causado, o Zabbix através do protocolo SNMP coleta os dados e através de *triggers* associadas à *templates* os analistas de incidentes do NOC conseguem dimensionar o problema e quais as tratativas que devem ser tomadas para recuperação.

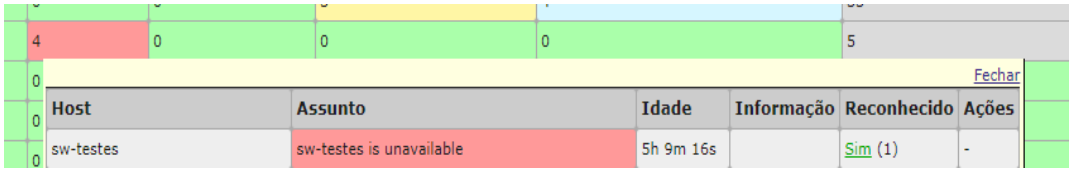
Segue exemplo de uma trigger e um alarme.

Figura: Trigger



Fonte: Próprio autor

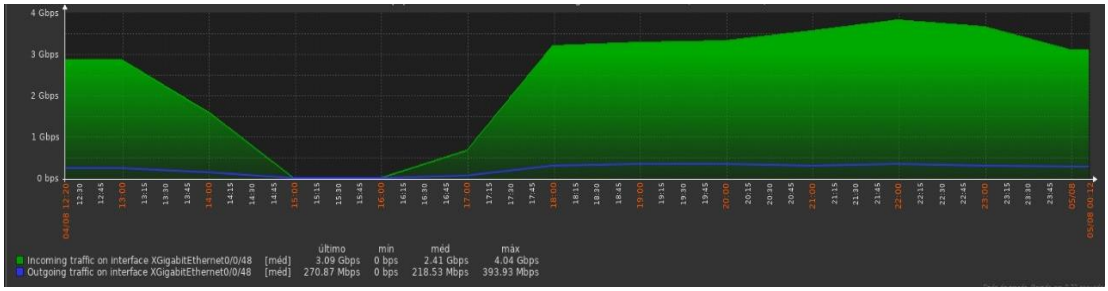
Figura: Alarme



Fonte: Próprio autor

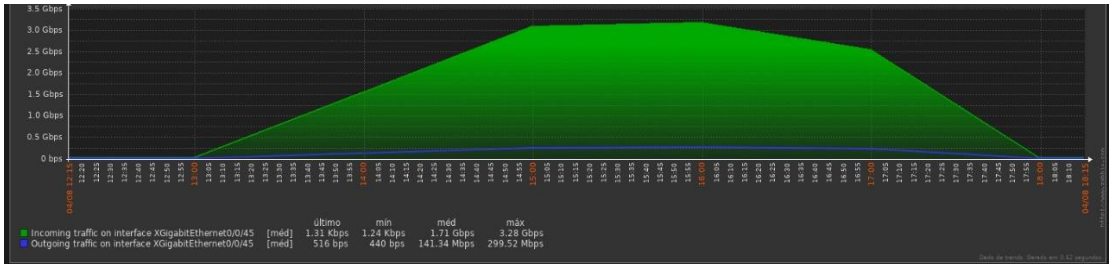
Após a detecção do incidente é necessário verificar se a redundância assumiu o tráfego pelo enlace que ficou ativo. Essa troca ocorre automaticamente usando protocolos como o OSPF por exemplo.

Figura: Enlace Principal



Fonte: Próprio autor

Figura: Enlace redundante



Fonte: Próprio autor

É importante ressaltar que o tráfego será dobrado do lado do anel na qual está assumindo o tráfego, por isso é necessário se ter o dobro de disponibilidade de tráfego afim de que o enlace não venha “chapar” causando lentidão e erros de CRC. Uma vez que a rede não está sendo afetada, então o SLA (Acordo de Nível de Serviço) de recuperação precisa ser atendido pois um novo incidente no enlace ativo causará o desligamento total da rede nesse cenário.

O próximo passo foi a abertura do chamado no CRM, esse chamado contém os dados necessários para identificação rápida do enlace e os possíveis usuários afetados, além de conter os endereços dos POPs, trajeto em que a fibra percorre, a importância dessa abertura de chamado é alta pois em um futuro incidente esse protocolo pode ser consultado sinalizando uma medida que não venha deixar o enlace vulnerável ao mesmo problema.

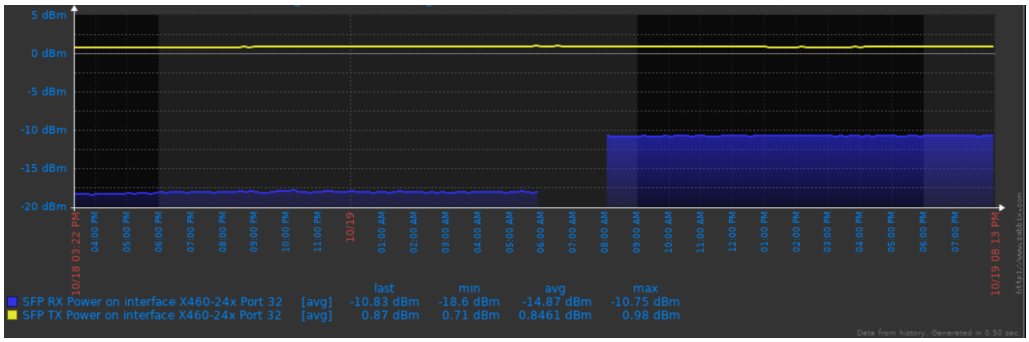
Afim de restabelecer o enlace utilizamos as ferramentas de *troubleshooting*, o OTDR (*Optical time-domain reflectometer*) será mostrado no próximo capítulo, o mesmo é capaz de enviar um pulso de luz e retornar a medida em metros do local onde não há mais continuidade da mesma, ou seja, o ponto para reparo.

Figura: Medição

Fonte: Próprio autor

Com o ponto para reparo em mãos então foi acionada a equipe de reparo, nesse momento utilizou-se a máquina de fusão para restaurar o enlace. Nesse ponto a equipe do NOC confere se as *triggers* no Zabbix e passa-se a monitorar o nível de sinal das fibras, deve-se alcançar um valor de recepção muito aproximado do valor constado antes, só será acrescido perda de Dbm (potência) em caso da necessidade de adicionar uma CEO (Caixa de emenda óptica), assim a nova medida de sinal pode variar de 0,3dbm a 0,6dbm por CEO inserida, uma fusão mal executada pode afetar a potência de uma maneira que a luz não alcance os níveis aceitáveis pelos *transceivers ópticos* e consequentemente a indisponibilidade do serviço.

Figura: Nível de Sinal



Fonte: Próprio autor

Por fim, não havendo nenhuma anormalidade pós incidente o chamado é encerrado e a documentação atualizada.

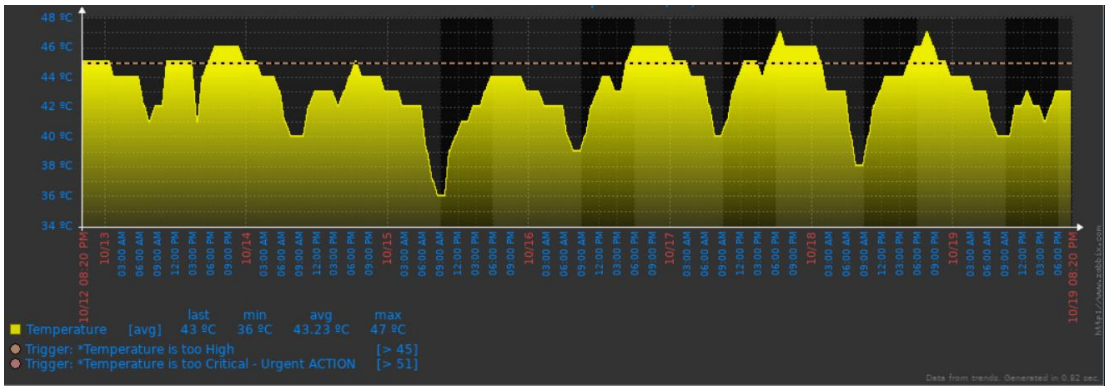
2.4.5 – Gerencia de Problemas

Conforme Oliveira (2008), a gerência de problemas resolve os chamados encaminhados pela gerência de Incidentes, quando sua causa não é identificada e/ou esta é desconhecida. Portanto, o NOC prioriza este tipo de chamado, analisando o seu conteúdo e resolvendo o problema. As resoluções são por meio de ferramentas analíticas, acompanhadas em uma base de conhecimento e o uso de uma força tarefa procura disponibilizar a volta do serviço. Depois de encontrada a causa raiz, o NOC cria procedimentos e informações para o armazenamento no bando de dados CMDB (*Configuration Management Data Base*). Caso exista à necessidade de um novo projeto, os especialistas indicam a nova demanda às áreas responsáveis, ou propõem melhorias na infraestrutura via uma nova Requisição de Mudanças.

As mudanças corretivas são encaminhadas à Gerência de Mudanças para a sua respectiva aprovação e emprego na rede.

Um exemplo comum para esse tipo de chamado está relacionado a temperatura, o Zabbix deve coletar esses dados e mostrar uma *trigger* ao encontrar anormalidade. Segue exemplo:

Figura: Temperatura



Fonte: Próprio autor

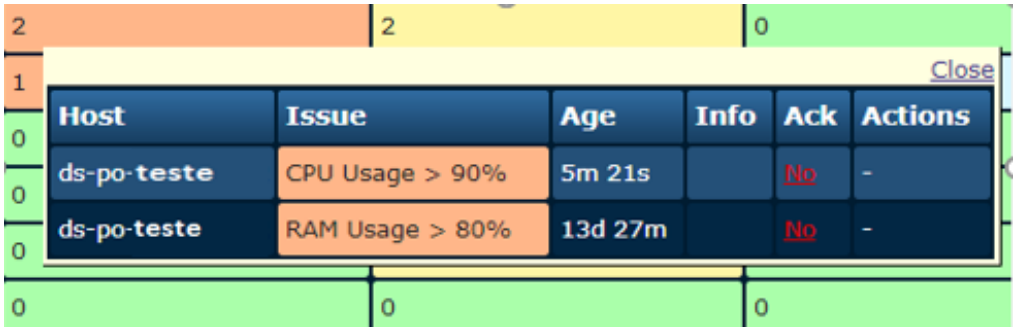
Foi necessário acionar uma equipe contratada especializada em temperatura de ambiente pra encontrar uma solução, a gerência de problemas está atenta a tudo aquilo que pode vir a se tornar um incidente, nesse caso a temperatura pode aumentar ou diminuir ao ponto de causar o desligamento do equipamento.

2.4.6 – Gerência de Mudanças

Oliveira (2008) relata que o processo da Gerência da Mudança é responsável pelo planejamento e execução de alterações nos serviços e na infraestrutura. Todas as mudanças devem demonstrar a necessidade, para melhoria no negócio, a resolução de um problema, a melhoria do serviço ou uma redução de custo. O NOC pode ser envolvido neste processo de duas maneiras, a primeira é descrita como uma correção de um problema na infraestrutura em um ou mais clientes. A segunda refere-se à execução programada relacionada nas tarefas gerenciadas pela equipe de mudanças. Portanto, nas duas condições o NOC é sempre envolvido por meio de chamados, esses controlados pelo CRM (*Customer Relationship Management*) e inseridos no CMDB.

Segue exemplo de uma trigger relacionada a gerência de mudança, essa trigger após analise do NOC, concluiu-se que será necessário a troca do *switch* devido a não suportar mais os serviços contratados. As figuras mostram a *trigger* e o gráfico de uso da CPU.

Figura: Trigger-CPU



Fonte: Próprio Autor

Figura: Processamento

Fonte: Próprio autor

A equipe de mudanças acompanhou todo processo desde o planejamento até a execução da troca, monitorou se os resultados foram satisfatórios, documentou todas as atividades, atualizou as nomenclaturas e *backups* e informou a todos os interessados sobre a mudança ocorrida.

3 INFRAESTRURA DE REDES BACKBONE

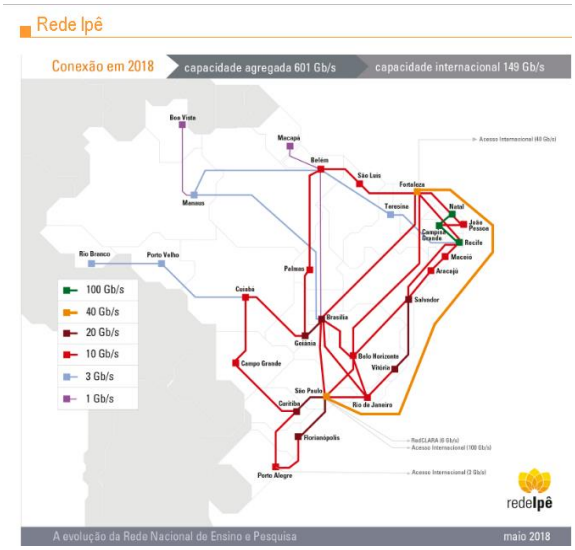
Segundo o Canaltech (2016), Backbone ("espinha dorsal" ou "rede de transporte", em português) é uma rede principal por onde os dados dos clientes da internet trafegam. Ele controla o esquema de ligações centrais de um sistema mais abrangente com elevado desempenho.

O *backbone* é o responsável pelo envio e recebimento dos dados entre diferentes localidades, dentro ou fora de um país. Essa grande espinha dorsal é dividida em partes menores com a finalidade de impedir que o tráfego e a transmissão de dados sejam lentos. No entanto, por continuar a ser a rede principal, o *backbone* faz a conexão de todas as redes menores, sendo possível, então, acessar qualquer rede por meio dele.

A rede nacional de Ensino e Pesquisa (RPN) possui um *backbone* chamada rede Ipê dedicada à comunidade brasileira de ensino superior e pesquisa, que interconecta universidades e seus hospitais, institutos de pesquisa e instituições culturais.

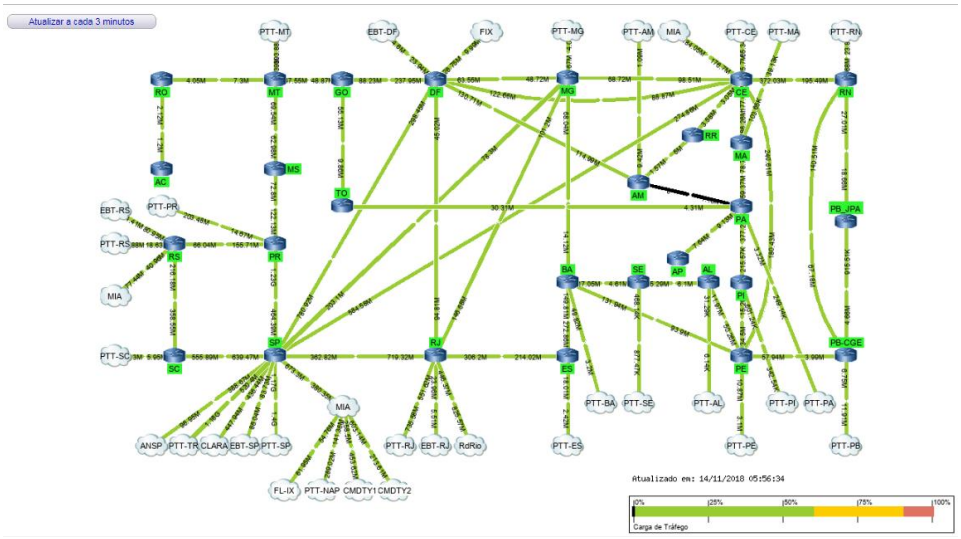
Segundo a Rede Nacional de Ensino e Pesquisa o *backbone* é projetado para garantir não só a velocidade necessária ao tráfego de internet de aplicações básicas (navegação *web*, correio eletrônico e transferência de arquivos), mas também ao tráfego de serviços, aplicações avançadas e projetos científicos, e à experimentação de novas tecnologias, serviços e aplicações. A infraestrutura da rede Ipê engloba 27 POPs pontos de presença um em cada unidade da federação, além de ramificações para atender 1522 campi e unidades de instituições de ensino, pesquisa e saúde em todo o país, beneficiando mais de 3,5 milhões de usuários. Segue mapa do *backbone* e capacidade de tráfego.

Figura: Backbone



Fonte: RNP(2018)[3]

Figura: Enlaces



Fonte: RNP(2018)[4]

3.1 Ativos

Os ativos em uma rede *backbone* estão na camada de enlace do modelo OSI, através deles é possível definir a capacidade de tráfego, processamento, protocolos e outros a serem utilizados. apresentado os ativos mais utilizados, suas principais características e definições.

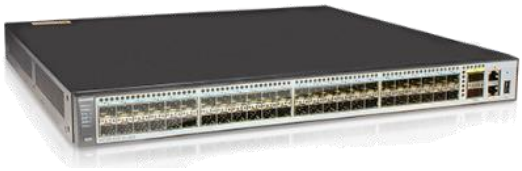
[3] Disponível em: <https://www.rnp.br/servicos/conectividade/rede-ipe>. Acesso 14 nov 2018.

[4] Disponível em: <http://memoria.rnp.br/ceo/trafego/panorama.php>. Acesso 14 nov 2018.

3.1.1 Switches

Switch é um comutador de redes, em uma rede *backbone* é essencial que o mesmo possua interfaces que suportem o tráfego e processamento suficiente para garantir o transporte da tabela de MACs.

Figura: Switch



Fonte: Huawei (2018)[5]

3.1.2 Transceivers

Os *transceivers ópticos* plugáveis são módulos de entrada e saída *hot-swap* que suportam aplicações *Gigabit Ethernet*. Eles são compatíveis entre uma ampla variedade de roteadores, *switches* e equipamentos de transporte *óptico.*

Na figura abaixo se tem uma *transceiver* com capacidade de 10Gb.

Figura: Transceiver

Fonte: Precision (2018)[6]

[5] Disponível em: <https://e.huawei.com/br/products/enterprise-networking/switches/campus-switches/s5700-hi-model>. Acesso 14 nov 2018.

[6] Disponível em: <https://www.precisionot.com/pre-xfp-mfct-80-1/>. Acesso 14 nov 2018.

Segue figura de uma *transceiver* com capacidade de 40Gb. Esse *transceiver* tem a capacidade de transmitir e receber em quatro canais simultaneamente.

Figura: QSFP

Fonte: Precision (2018)[7]

3.1.3 Conversor de mídia

O conversor de mídia no contexto de uma rede *backbone* é utilizado quando não há mais portas SFP disponíveis no *switch*, nesse casos deve-se atentar a negociação da porta pra que não haja uma demanda maior do que o conversor possa suportar, em caso da necessidade de muitos conversores então é necessário a utilização e um chassis de mídia que é unificação de vários conversores em um chassis.

Figura: Conversor de mídia

Fonte: Intelbrás(2018)[8]

[7] Disponível em: <https://www.precisionot.com/pre-qsfp28-lr4-1/>. Acesso 14 nov 2018.

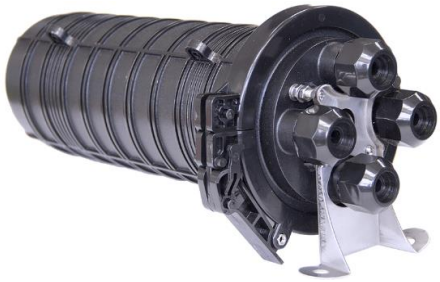
[8] Disponível em: <http://www.intelbras.com.br/empresarial/redes-opticas-e-cabeadas/conversores-de-midia/kfsd-1120-b>. Acesso 14 nov 2018.

3.2 Passivos

Os passivos de rede são elementos da camada física e são responsáveis por transportar os dados no meio físico, são compostos por cabos, acessórios, acopladores, terminações e caixas de acomodação. Segue abaixo os passivos mais utilizados em um enlace *backbone.*

A caixa de emenda *óptica* (CEO) possui fechamento mecânico através de rosca e pode ser utilizada tanto na vertical quanto na horizontal, é indicada para ambientes externos podendo armazenar até 96 fusões.

Figura: CEO



Fonte: CIANET(2018)[9]

Segundo a CIANET os cordões *ópticos* são cabos de fibra óptica do modelo *Tight*, dielétricos e pré-conectorizados em ambas extremidades, fornecido com uma ou duas fibras (simplex/duplex) monomodo ou multimodo. Estes cordões se destinam ao uso exclusivamente interno e sua aplicação mais comum é a interligação de equipamentos *ópticos*, acessórios de terminação dos cabos, tais como os DIO's e terminações *ópticas*.

Segue abaixo figura com as conectorizações mais utilizadas:

[9] Disponível em: <https://www.cianet.com.br/produto/caixa-de-emenda-optica-8001/>. Acesso

Figura: Cordões Ópticos

Fonte: CIANET(2018)[10]

O distribuidor interno é utilizado em sistemas de cabeamento estruturado para instalações em *rack*. A sua função é organizar e armazenar o cabeamento *óptico* com módulos de encaixe rápidos e gaveta deslizante.

Figura: DIO

Fonte: CIANET(2018)[11]

Existem diversos tipos de cabos ópticos usados em redes *backbone*, os cabos costumam possuir 2,4,12, 24, 36, 48 e 72 fibras, quanto mais fibras possui um cabo, maior a possibilidades de enlaces podem ser utilizados no mesmo, também em caso de degradação parcial, pode se utilizar outras fibras de outro tubete para reparo imediato.

---

[10] Disponível em: <https://www.cianet.com.br/site/wp-content/uploads/2015/11/Folder-Cordoes-%C3%93pticos-v.3.pdf>. Acesso 14 nov 2018.

[11] Disponível em: <https://www.cianet.com.br/produto/distribuidor-interno-optico/>. Acesso 14 nov 2018.

A figura abaixo apresenta um cabo de fibras *ópticas*:

Figura: Cabo óptico

Fonte: Furukawa(2018)[12]

[12] Disponível em: <https://www.efurukawa.com/storefront/p/cabo-optico-cfot-sm-mf-02f-cog/17070002>. Acesso 14 nov 2018.

4 FERRAMENTAS DE TROUBLESHOOTING

As ferramentas de *troubleshooting* são essenciais para manter uma rede *backbone* com níveis de sinais dentro do padrão, são essas ferramentas que irão tratar os passivos de rede, mostrando em quais pontos a rede está degradada definindo se a mesma necessita de uma ação imediata ou uma janela programada.

4.1 Power Meter

O Power Meter *óptico* mede o sinal de uma fibra *óptica* na lamda que está em uso, essa medição é importante pois existe um *range* aceitável para comunicação entre os *transceivers*, uma atenuação na fibra pode causar a falha na comunicação entre as mesmas.

Figura: Power Meter

Fonte:Viavi(2018)[13]

4.2 OTDR

O OTDR (*Optical time-domain reflectometer*) é um instrumento optoeletrônico usado para inspeção de fibra óptica, seja na pré ativação atuando como certificador nos padrões internacionais IEC 61300-3-25: 2016 como no *troubleshooting* sendo utilizado para detecção de eventos, degradação, rompimentos e outras falhas decorrentes do dia a dia.

[13]Disponível em: <https://www.viavisolutions.com/pt-br/node/2967>. Acesso 14 nov 2018.

Figura:OTDR

Fonte:Viavi(2018)[14]

4.3 Caneta para limpeza de conectores ópticos

A caneta para limpeza de conectores *ópticos* elimina as impurezas presentes em conectores e/ou adaptadores *ópticos*.

Figura: Caneta de limpeza

Fonte:e2cloud(2018)[15]

4.4 PDA

O PDA (*Personal digital assistant*) é um computador de mão ou com dimensões reduzidas sem perda de funcionalidades, essa definição resume bem o uso de um PDA para redes, o mesmo possui inúmeras funcionalidades além de ser discreto para ser usado no dia a dia, seu sistema Android faz com que o aparelhos possua diversos aplicativos que facilitam a vida de um profissional de redes.

[14] Disponível em: <https://www.viavisolutions.com/pt-br/produtos/smartotdr-testador-portatil-de-fibra>. Acesso 14 nov 2018.

[15]Disponível em: <http://www.e2cloud.com.br/rede-optica/caneta-para-limpeza-de-conectores-opticos-fibra-optica-2-5mm>. Acesso 18 out 2018.

Figura: PDA

Fonte:Senter(2018)[16]

4.5 Máquina de Fusão

A Máquina de fusão é responsável por fazer emenda de fibras *ópticas*,é ideal para construção e manutenção de redes *backbone*. Com seu sistema de fechamento automático, tanto do forno de aquecimento quanto do protetor de fusão, garante operação manual mínima.

Figura: Máquina de fusão

Fonte:Terzian(2018)[17]

[16]Disponível em: <http://en.senter.com.cn/products_detail/productId=211.html>.Acesso 18 out 2018.

[17] Disponível em: <http://www.terzian.com.br/areas-de-atuacao/o-tech-solucoes opticas/maquinas-de-fusao>. Acesso 18 out 2018.

CONSIDERAÇÕES FINAIS

Mostrou-se a complexidade e a importância do monitoramento de uma rede *backbone* seja ela de pequena ou de grande complexidade. Detalhou-se como é importante ter a informação certa no momento certo e que é de primordial importância à captação de informações sobre o *status* dos dispositivos ativos na rede. Os resultados colhidos através da ferramenta Zabbix foram fiéis ao que acontece dentro de uma rede. O monitoramento em tempo real de um *host*, servidores, *switches* e outros ativos na infraestrutura se tornou muito eficiente. Quando encontrados os *bugs* e falhas, que provocaram o alerta pela ferramenta, percebe-se a importância da ferramenta para resolução do problema de forma proativa muitas vezes antes mesmo da percepção pelo usuário final. Verificou-se que esses alertas devem denunciar não só quando ocorre um problema (ou um limite crítico que está sendo atingido), mas também sempre que um novo aplicativo ou peça de equipamento é ativado. Eles devem conter informações sobre o dispositivo, o problema e o evento que desencadeou a notificação. Detalhou-se a estrutura de um NOC, bem como suas principais funções, as divisões do departamento de acordo com a ITIL, gerência de incidentes, gerência de problemas e gerência de mudanças, as melhores práticas com o objetivo de entregar o SLA (acordo de nível de serviço) proposto. Foi visto a estrutura de uma rede *backbone* bem como seus principais ativos e passivos necessários para mantê-la em funcionamento. As ferramentas necessárias para *troubleshooting* foram de grande relevância para a finalização do trabalho pois uma rede *backbone* em bom estado depende de ferramentas capazes de encontrar os problemas de forma rápida e precisa, desta maneira o NOC conseguirá ter efetividade e sucesso no troubleshooting de um enlace importante no âmbito geral da rede e também garantir redundância funcional para todos os casos, não permitindo que um serviço fique fora do ar e prejudique de alguma maneira o cliente final seja ele um usuário ou um intermediário. Esse trabalho trouxe a oportunidade de conhecer a importância da profissão de administrador de rede e o detalhamento do que deve ser feito para se ter uma rede saudável e sempre ativa. Encontrar o problema antes que ele aconteça e trata-lo é sem dúvida a melhor maneira de ter uma rede funcional e confiável.

REFERÊNCIAS BIBLIOGRÁFICAS

KUROSE, James F. **Redes de computadores e a Internet**: uma abordagem top-down. São Paulo: Pearson, 2006. 634p.

LIMA, Janssen dos Reis. **Monitoramento de redes com Zabbix**: monitore a saúde dos servidores e equipamentos de rede. Rio de Janeiro: Brasport, 2014. 300p.

RUSSO, Bruno. **A importância do monitoramento da Infraestrutura**, 2013. Disponível em: <https://www.brunorusso.com.br/monitoramento>. Acesso em 18 set 2018.

PALMA, Fernando. **Gerenciamento de eventos x gerenciamento de incidentes da itil**, 2013. Disponível em: <https://www.portalgsti.com.br/2013/01/gerenciamento-de-eventos-x-gerenciamento-de-incidentes-da-itil.html>. Acesso em 18 nov 2018.

OLIVEIRA, Andrey Guedes. **Indicadores de desempenho e dimensionamento de recursos humanos no Centros de Operações de Redes**. 2008. 100f. Dissertação (Programa de Pós-Graduação Stricto-Sensu), Faculdade de Ciências Exatas Ambientais e Tecnologia, Pontifícia Universidade Católica, Campinas, 2008.