

# Monitoramento da Rede Acadêmica do Unifafibe e suas Soluções.

Jhonij Carvalho Gomes, Renan Pereira Pizolato

Orientador: Diego Fiori de Carvalho

{sisunifafibe}@unifafibe.com.br

Curso de Sistemas de Informação – Centro Universitário UNIFAFIBE  
Bebedouro –SP – Brazil

**Resumo.** Atualmente as redes de computadores são fundamentais, tanto para empresas quanto para residências, pois se tornou essencial que a navegação e o compartilhamento de arquivos sejam seguros, sem lentidão no acesso aos dados ou serviços. Visando essas necessidades este artigo tem como intuito implementar o sistema de monitoramento Zabbix, sendo uma ferramenta criada para monitorar o desempenho e a disponibilidade dos ativos de uma rede, ele foi projetado para trabalhar através da coleta das informações de servidores, switches, roteadores e os demais diferenciados equipamentos encontrados na rede. O Zabbix será implementado na rede acadêmica do Centro Universitário UNIFAFIBE por um determinado período, para que possamos identificar os problemas da rede com o auxílio do software e outras ferramentas que possam ajudar no monitoramento, a fim de gerar relatórios e gráficos buscando encontrar falhas e desta forma elaborar uma estratégia para que o problema seja solucionado. O monitoramento será diário e estaremos sempre analisando os dados coletados para que possamos melhorar o desempenho da rede, todas as ferramentas que serão utilizadas não irão gerar custos para instituição.

**Palavras Chaves:** Redes, Zabbix, triggers, monitoramento.

## 1. INTRODUÇÃO

Com os grandes benefícios que as redes de computadores podem oferecer, seu crescimento vem se tornando cada vez maior, já que seus recursos e aplicações se tornam ainda mais indispensáveis para as organizações que as utilizam. Com a grande expansão, começam a surgir problemas que também aumentam, podendo deixar a rede inoperante ou a níveis inadequados de uso e desempenho.

A utilização de tecnologias *Web* é uma tendência no ramo de monitoramento de redes, já que seu custo de implementação é baixo. O acesso às informações geradas por estas tecnologias pode ser feito a partir de qualquer local e é totalmente independente da plataforma, por este motivo, este artigo tem por finalidade realizar a implementação de uma ferramenta de monitoramento *OpenSource* conhecida como Zabbix na rede acadêmica do centro universitário UNIFAFIBE localizado em Bebedouro – São Paulo, coletando assim informações dos equipamentos que na rede estão hospedados e com estas informações conseguir através de gráficos e relatórios utilizar técnicas para corrigir os erros e prevenir futuros problemas que a rede possa ter.

O monitoramento será realizado em determinados períodos para análise e comparação de dados com o interesse de checar se os problemas encontrados foram solucionados ou se outra técnica ou ferramenta serão necessárias para a correção do problema. Visando sempre tomar decisões estratégicas junto com o departamento responsável de T.I para não comprometer o funcionamento da rede e sim o melhor funcionamento da mesma, por isso este artigo é um estudo de caso real e com metas a serem alcançadas para o setor de tecnologia da empresa.

## **2. REFERENCIAL BIBLIOGRÁFICO**

### **2.1 Redes**

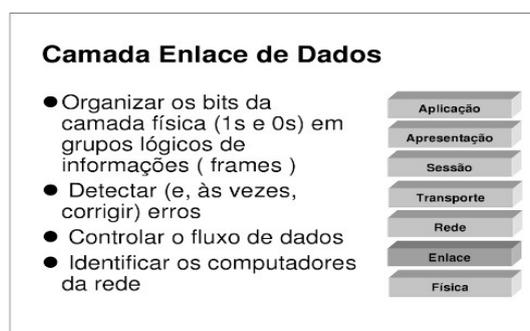
#### **2.1.1 Camadas TCP/IP**

Segundo Tanenbaum (2003), com a expansão das redes de radio e satélite, iniciaram-se problemas com protocolos existentes, onde teve a necessidade da criação de uma estrutura melhor e mais eficiente. Resumindo, o propósito do projeto foi focado em unir redes de diversas partes. Deste modo a estrutura obteve o nome de Modelo de Referencia TCP/IP.

#### **2.1.2. Camada 2 enlace**

Conforme Uchôa (2009) diz, a camada de enlace também conhecida pelo nome Acesso ao Meio (*Media Access Control - MAC*) é responsável pela comunicação dos dados identificando e optando a corrigir problemas ocorridos

na camada física ou camada de transporte (TCP/IP). Contudo, ela possui a capacidade de especificar como se devem organizar os dados selecionando seus formatos de transmissão adequados (em *frames* ou *bits*). A Figura 1, ilustra mais especificamente a estrutura da camada 2 com seus objetivos em si.



**Figura 1: Componente da Camada de Enlace (ROSS, 2008).**

Conforme a camada *Link* de Dados (conhecida também pelo nome de Conexão de Dados ou especificamente Enlace) tem uma série de funções para serem realizadas coletando os dados recebidos da camada superior (camada de Redes), inserindo placas de origem e destino, complementando informações de endereçamento, controle de dados e também a possibilidade de controlarem erros. Porém, esta camada possui a possibilidade de detectar e opcionalmente corrigir erros encontrados, organizando os *bits* da camada física em *frames* que são conhecidos como conjuntos de *bits*, deste controle, podem identificar computadores da rede (ROSS, 2008).

### 2.1.2.1 Problemas

Dentre os problemas que ocorrem, Forouzan (2009) fala a respeito das redes de computadores, devem possuir a capacidade de transferir os *frames* de uma máquina para outra com clareza. Para todas as aplicações, a rede deve administrar os dados recebidos que devem ser idênticos dos que foram enviados. Durante o caminho da movimentação destes dados de nó a nó, podem ser corrompidos. Vários motivos podem alterar vários *bits* de uma mensagem. Existem erros capazes de sofrerem alterações inesperáveis causadas por interferências na rede (FOROUZAN, 2009).

### 2.1.2.2 Soluções

Forouzan (2009) explica que tais erros podem ser corrigidos aplicando repetições, diferentes tentativas encaminhando *bits* extras junto com os dados, permitindo que o receptor dos dados possa identificar ou corrigir com clareza onde e quais são os erros. Para poder corrigir os erros encontrados, primeiro é necessário saber a quantidade exata dos *bits* alterados e o tamanho que a mensagem possui em que algumas ocasiões passam despercebidas.

### **2.1.3 Redes – Inter Redes**

A principal função da camada de rede é permitir que a notificação encaminhada pelo transmissor, chegue a outro dispositivo. Esse reencaminhamento da mensagem tem o nome de comutação. Enquanto a camada de enlace esta focada com a comunicação em si, entre dispositivos diretamente conectados, preocupando-se com erros ocorrendo no fluxo e alterando informações, a camada de rede em si está preocupada em fazer acontecer à comunicação entre dispositivos que não estão próximos (MAIA, 2013).

#### **2.1.3.1 Roteamento**

Quando falamos sobre processos entrega de pacotes na rede, necessita de endereçamento e roteamento para controlá-los. Para que haja o roteamento em uma rede é necessária à atuação de um *host* ou roteador possua uma tabela de roteamento. Quando um *host* possui um pacote para poder ser encaminhado, ou quando um pacote chega externamente para o roteador, sempre é verificado pelo *host* o destino final na tabela de roteamento. No entanto, hoje em dia, este método se torna muito difícil na *internetwork*, devido ao fluxo que ocorre (FOROUZAN, 2006).

#### **2.1.3.2 Broadcast**

O termo basicamente transmite informações do dispositivo para um grande público, por exemplo, um dispositivo necessita achar uma impressora na rede. Ele formula um meio de especificar uma impressora (coletando como notificação o nome dela, por exemplo) e então, envia essa notificação utilizando a técnica do *broadcast* para todos os dispositivos da rede. Entretanto, como todos os dispositivos iram receber o *broadcast*, somente a

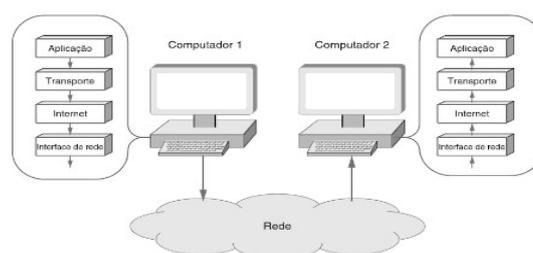
impressora com o nome especificado pelo dispositivo irá responder (COMER, 2007).

### 2.1.3.3 Multicast

Como um computador em uma rede tem a possibilidade de ser configurado para descartar quadros desnecessários, o processamento e o descarte de um quadro exigem muitos recursos de um computador, desperdiçando tempo da CPU para apagar informações irrelevantes. Entretanto, existe outra forma de *broadcasting* mais restrito com o nome de grupos. Diferente do modo que é tratado o *broadcast*, sendo recebidos por todos os dispositivos da rede, os *hardwares* de interface são configurados com informações específicas de quais quadros *multicast* devem aceitar ou rejeitar. Tendo em vista que os quadros serão encaminhados especificamente para um grupo de dispositivos, onde os demais que receberam irão descartar os quadros fúteis (COMER, 2007).

### 2.1.4 Camada 4 Transportes

As funções das camadas inferiores estão concentradas em acompanhar a transmissão de notificações entre os dispositivos, já o nível de transporte está focado mais na comunicação entre os processos que estão sendo executados destes dispositivos. A camada de transporte realiza procedimentos de segurança, notificando que será realizado, caso ocorrendo algum erro serão detectados solicitando uma retransmissão ou informando para protocolos superiores realizarem medidas necessárias de correção. Devido à própria rede não garantir que pacotes cheguem sem nenhum erro, à camada de transporte é a mais confiável por fornecer uma comunicação fim a fim. A Figura 2 exibe como ocorre o fluxo dos dados por meio da rede, passando por cada camada (ROSS, 2008).



**Figura 2. Fluxo dos dados através das camadas (COMER, 2016).**

Podemos observar como ocorre a movimentação dos dados por meio de uma rede física, supondo que o Computador 1, envie dados para o Computador 2, no momento que os dados saírem, são transformados em pacotes e cada pacote irá passar por meio de cada camada dos protocolos, quando este pacote passar sem nenhum tipo de erro por todas as camadas dos protocolos do Computador 1 ao qual está encaminhando o pacote, irão cair na rede física para poderem chegar ao seu destinatário que é o Computador 2, assim que chegar, iram passar novamente pelas camadas de protocolos da máquina destinatária emitindo uma resposta para a máquina receptora, repetindo o processo até chegar a receptor do pacote (COMER, 2016).

## **2.2 Problemas de rede e Solução**

### **2.2.1 *Troubleshooting***

*Troubleshooting* consiste em resolver problemas ou processos que não estão funcionando corretamente em busca de analisar e identificar a melhor maneira de resolvê-lo seguindo uma ordem ou fluxograma para solução, sendo possível a utilização de ferramenta ou *software* para o auxílio da resolução do problema (De FRANCESCHI, MORALES, BARRETO, ROISENBERG, 2000).

## **2.3. Possíveis soluções**

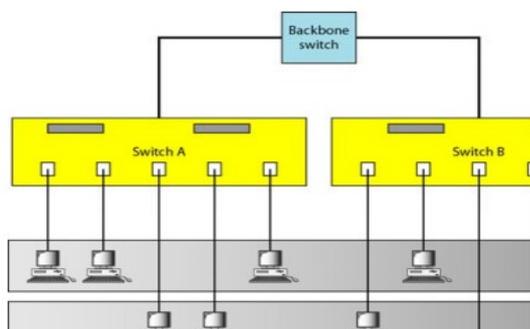
### **2.3.1 Qos**

A QoS (*Quality of Service*) em tradução significa qualidade de serviços é fundamental para o desempenho nas redes de IP sendo importante entender os seus princípios, parâmetros, mecanismos, algoritmos e protocolos utilizados para se ter uma QoS. Ele é um requisito de aplicação para qual deve-se determinar parâmetros como atrasos, *delays* e *throughput* para que seus limites estejam bem definidos, garantindo a qualidade prevista para seus usuários que se comunicam por meio da rede de IP (SANTANA, 2006).

### **2.3.2 VLAN**

Com aumento das redes de computadores e com suas dificuldades, grandes empresas decidiram utilizar as VLANs (redes locais virtuais) como

meio para estruturação deste crescimento de maneira lógica. Uma VLAN é composta por uma coleção de nós que ficam agrupados em um domínio *broadcast*, entre suas vantagens temos como separar sistemas que contém dados sigilosos do resto da rede, melhora do desempenho de largura de banda e reduzir o tráfego de *broadcasts*. As VLANs podem se expandir por vários *switches* onde é possível configurar diversos VLAN para cada *switch*, para que múltiplas VLANs possam se comunicar através de um *link* deve-se utilizar um processo chamado *Trunking*, que é a tecnologia que permite o tráfego de dados através de um único *link* segundo a CISCO (BEZERRA, 2008).



**Figura 3: Representação de 3 VLANs com *Trunking* (BEZERRA, 2008)**

### 2.3.2.1 *Throughput*

Segundo Stangarlin (2007), o *throughput* em uma rede de computadores pode ser definido como vazão da rede, significando assim que é a capacidade máxima que um canal de transmissão consegue processar e transmitir em determinado tempo; tendo como medidas básicas o KBps, o MBps e o Gbps que são a quantidade de dados que consegue ser transferidos de um lugar para outro.

### 2.3.3 SNMP

O SNMP foi lançado em 1988 com a finalidade de definir um padrão de gerenciar os dispositivos IP (*internet Protocol*). Oferecendo aos seus usuários uma forma mais simples de orações que permitem o gerenciamento remoto dos dispositivos. SNMP abreviação de *Simple Network Management Protocol* tem a função de definir como um gerente (servidor) se comunica com o agente (equipamento) enviando uma informação ou solicitando alguma informação também podendo escolher o formato que seu agente deve retornar a resposta,

ele também define o exato significado de cada solicitação de resposta possível, essas respostas são codificadas utilizando o padrão (ASN.1) *Abstract Syntax Notation*.1. (COMER, 2007).

#### **2.3.4 MIBS**

Todo objeto ao qual o SNMP possui acesso deve-se definir um nome único, onde os *softwares* que é o gerente e o cliente devem concordar com os nomes e significados das operações de carga de armazenamento. A junção de todos os objetos que o SNMP acessa é chamada de *Management Information Base* (MIB), os MIBS são definidos por meio do esquema ASN.1, que designa para cada objeto um nome que deve ser único na rede em que estiver hospedado (COMER, 2007).

### **2.4 Ferramentas de monitoramento**

#### **2.4.1 Zabbix**

Segundo Fachini (2010) Zabbix é uma ferramenta de monitoramento com capacidade para grande quantidade de parâmetros, ele foi desenvolvido para monitorar e controlar o funcionamento dos equipamentos em rede e seus serviços, ele oferece excelentes características de relatórios e visualização de dados armazenados, ideal para planejamento de capacidade o Zabbix possui suporte para mecanismos *polling* (forma de capturar dados de tempo em tempo) e *trapping* (notificação de alarmes) oferecendo recursos de alto desempenho.

Várias empresas com a dificuldade de criar uma infraestrutura sofisticada hoje em dia, se beneficiou com a ferramenta devido aos seus métodos e ferramentas de monitoramento disponíveis sem custo (*Open Source*). O Zabbix auxiliou no desempenho do setor de informática no máximo fornecendo suas soluções. Um ponto importante a se discutir é o limite em que o Zabbix consegue apresentar seus resultados, conseguindo relacionar diferentes dados de aplicativos e dispositivos por forma de gráficos.

#### **2.4.2 Cacti**

O Cacti é o *software* de monitoramento de redes, que possui sua escrita em *Hypertext Preprocessor* (PHP), para o *RRDTool*, que guarda dados que são necessários para a disponibilização de gráficos em uma base de dados *MySQL*, sendo possível monitorar diversos itens desde memória utilizada, quantidade de processos rodando, quantidade de usuário conectados à rede, tráfego de entrada e saída entre outros, todos estes itens podem ser exibidos em gráficos possibilitando a análise do administrador em horários de pico e dimensionamento de carga, seu uso é bastante acessível pois se trata de uma ferramenta *Open Source* (YANO, 2010).

### 3. DESENVOLVIMENTO

#### 3.1 Zabbix

O sistema que utilizaremos para realizar o monitoramento da rede é o Zabbix ferramenta que é disponibilizada de forma gratuita.

Foi disponibilizado um computador físico para que possa se tornar nosso servidor de monitoramento com as seguintes configurações:

1 Intel (R) core (TM) 2 CPU E7500 de 2.93 GHz;

2 GB de memória RAM;

HD de armazenamento com 160 GB

Sistema Operacional utilizado é um Linux Debian 8.9 instalado sem a interface gráfica para que o melhor desempenho do servidor.

#### 3.2 Cenário

A rede que será monitorada trabalha com uma máscara /24 (255.255.255.0), ou seja, temos disponível 1 grades de IP (192.168.4.0 até 192.168.4.255).

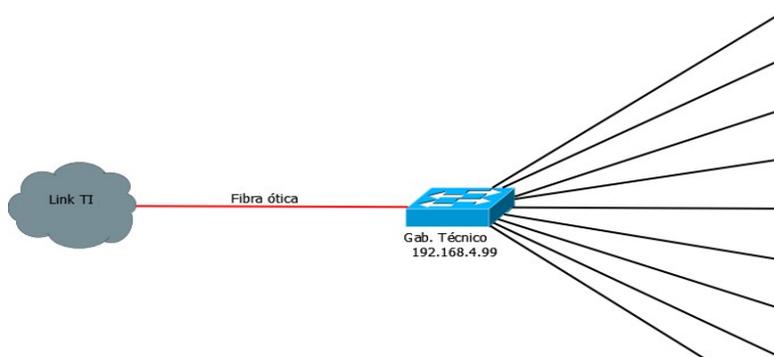
Na rede também encontramos 9 *Mikrotiks* que depois que recebem o *link* de *internet*, criam sua própria rede distribuindo uma grade diferente para cada laboratório, a máscara de cada *Mikrotik* também trabalha com a /24.

O ambiente mencionado não possui VLANs, sendo assim, todos os equipamentos estão em uma única e grande rede.

A rede acadêmica do UNIFAFIBE possui 1 *switch* localizado no gabinete técnico que recebe um *link* de fibra óptica, e distribui o *link* para 9 *Mikrotiks* localizados no laboratório de informática. A tabela abaixo apresenta os IPs e a subdivisão dos laboratórios de informática:

IP	Mascára	Local	Porta Switch
192.168.4.1 19	255.255.255 .0	Laboratório 1	3
192.168.4.1 18	255.255.255 .0	Laboratório 2	4
192.168.4.1 17	255.255.255 .0	Laboratório 3	5
192.168.4.1 16	255.255.255 .0	Laboratório 4	6
192.168.4.1 24	255.255.255 .0	Laboratório 5	8
192.168.4.1 21	255.255.255 .0	Laboratório 6	7
192.168.4.1 23	255.255.255 .0	Laboratório 7	9
192.168.4.1 25	255.255.255 .0	Laboratório 8	12
192.168.4.1 26	255.255.255 .0	Laboratório 9	10

A Figura 4, mostra como a estrutura está montada no gabinete técnico antes do monitoramento. Logo vemos que todos os equipamentos se encontram em uma única rede interligados a um único *switch*.



**Figura 4: Estrutura da rede**

### 3.3 Monitoramento

Depois de configurado toda parte do ZABBIX e também configurado os SNMP nos dispositivos, foi necessário adicionar os *hosts* no ZABBIX. A Figura 5 mostra os *hosts* monitorados, entre eles o *switch* responsável por distribuir o *link*.

Nome	Aplicações	Itens	Triggers	Gráficos	Descoberta	Web	Interface	Templates	Status
Mikrotik Laboratorio 01	Aplicações 4	Itens 75	Triggers 9	Gráficos 9	Descoberta 3	Web	192.168.4.119: 161	Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors	Ativo 26
Mikrotik Laboratorio 02	Aplicações 4	Itens 75	Triggers 9	Gráficos 9	Descoberta 3	Web	192.168.4.118: 161	Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors	Ativo 26
Mikrotik Laboratorio 03	Aplicações 4	Itens 75	Triggers 9	Gráficos 9	Descoberta 3	Web	192.168.4.117: 161	Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors	Ativo 26
Mikrotik Laboratorio 04	Aplicações 4	Itens 75	Triggers 9	Gráficos 9	Descoberta 3	Web	192.168.4.116: 161	Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors	Ativo 26
Mikrotik Laboratorio 05	Aplicações 4	Itens 75	Triggers 9	Gráficos 9	Descoberta 3	Web	192.168.4.124: 161	Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors	Ativo 26
Mikrotik Laboratorio 06	Aplicações 4	Itens 75	Triggers 9	Gráficos 9	Descoberta 3	Web	192.168.4.121: 161	Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors	Ativo 26
Mikrotik Laboratorio 07	Aplicações 4	Itens 75	Triggers 9	Gráficos 9	Descoberta 3	Web	192.168.4.123: 161	Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors	Ativo 26
Mikrotik Laboratorio 08	Aplicações 4	Itens 75	Triggers 9	Gráficos 9	Descoberta 3	Web	192.168.4.124: 161	Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors	Ativo 26
Mikrotik Laboratorio 09	Aplicações 4	Itens 75	Triggers 9	Gráficos 9	Descoberta 3	Web	192.168.4.124: 161	Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors	Ativo 26

**Figura 5: Hosts cadastrados no ZABBIX.**

A Figura 6 mostra os dados recentes dos nove *Mikrotiks* dos laboratórios de informática capturados pelo ZABBIX, de acordo com o *template* feito manualmente através do SNMP. Os dados recentes mostram a locação em disco, memória utilizada, o espaço de disco.

Host	Nome	Última checagem	Último valor
Mikrotik Laboratorio 05	Disk partitions (12 Itens)		
	Allocation units for storage disk: system	08-09-2017 10:00:02	1 KB
	Allocation units for storage main memory	08-09-2017 10:00:02	1 KB
	Description of storage disk: system	08-09-2017 10:00:02	disk: system
	Description of storage main memory	08-09-2017 10:00:02	main memory
	Total disk space on disk: system	08-09-2017 10:03:40	124 MB
	Total disk space on disk: system in units	08-09-2017 10:00:02	126.98 Kunits
	Total disk space on main memory	08-09-2017 10:03:39	32 MB

**Figura 6: Dados dos mikrotiks**

A Figura 7 exibe os dados recentes do *switch* acadêmico HP V1920 capturados pelo ZABBIX. Os *templates* usados capturam vários dados, como: *Uptime*, nome, status das interfaces, tráfego das interfaces, entre outros dados.

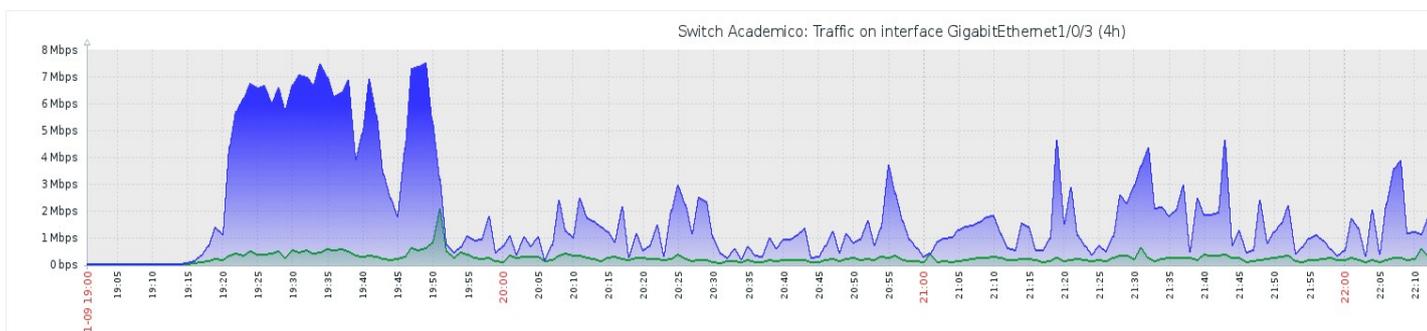
Nome	Última checagem	Último valor
<b>General (5 Itens)</b>		
Device contact details	08-09-2017 10:00:12	Hewlett Packard Enterprise Cor
Device description	08-09-2017 10:00:12	1920-240 Switch Software Vers
Device location	08-09-2017 10:00:12	
Device name	08-09-2017 10:00:12	HPE
Device uptime	08-09-2017 10:26:11	3 dias, 13:08:25
<b>Interfaces (241 Itens)</b>		
Admin status of interface GigabitEthernet1/0/1	08-09-2017 10:26:11	up (1)
Admin status of interface GigabitEthernet1/0/2	08-09-2017 10:26:11	up (1)
Admin status of interface GigabitEthernet1/0/3	08-09-2017 10:26:11	up (1)
Admin status of interface GigabitEthernet1/0/4	08-09-2017 10:26:11	up (1)
Admin status of interface GigabitEthernet1/0/5	08-09-2017 10:26:11	up (1)
Admin status of interface GigabitEthernet1/0/6	08-09-2017 10:26:11	up (1)

**Figura 7: Dados recentes do switch**

### 3.3.1 Taxa de *Download* e *Upload*

Foram gerados gráficos de *throughput* das portas do *switch* que mandam o *link* cada equipamento para a verificação do tráfego nos horários de aula onde um grande fluxo devido ao uso de todo o laboratório de informática.

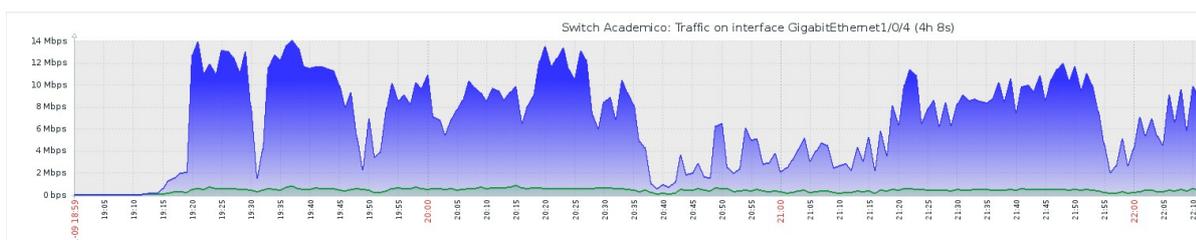
Logo abaixo na figura 8 vemos o gráfico de *throughput* da porta 3 no dia 01/08, que é responsável por enviar o *link* para o laboratório 1. Podemos ver que o uso é maior no início da aula, por volta das 19h e 50min a taxa de *Download* representada na cor azul no gráfico atinge 7.45 Mbps, que pode ser devido ao uso de internet para coleta de arquivos para aula, a taxa de *upload* representada pela cor verde se mantém baixa tendo apenas um pico de 2.03 Mbps por volta das 19 h e 50min.



**Figura 8: Gráfico de *Throughput* porta 3**

Logo abaixo na figura 9 vemos o gráfico de *throughput* da porta 4 no dia 01/08, que é responsável por enviar o *link* para o laboratório 2. Vemos que a

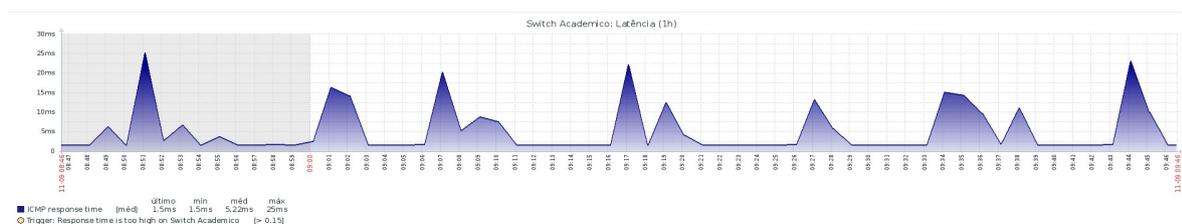
taxa de *download* se mantém acima dos 8 Mbps a maior parte do tempo a taxa de *download* só abaixou no horário do intervalo as 20 h e 40 min., a taxa de *upload* representada pela cor verde se manteve baixa atingindo um pico de 1.57 Mbps por volta das 22 h e 15 min., onde os alunos deveriam estar subindo o conteúdo da aula para algum *drive*.



**Figura 9: Gráfico de *Throughput* porta 4**

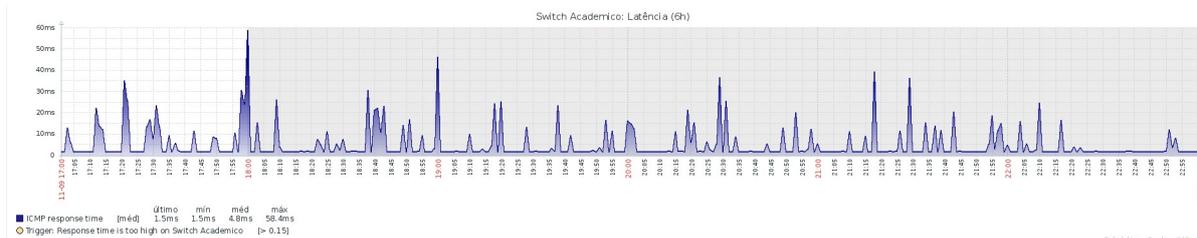
### 3.3.2 Taxa de latência

A figura 10 logo abaixo, mostra o gráfico de latência do *switch* responsável pelo gerenciamento dos laboratórios em um período onde não estava tendo aulas, ele atinge pico de 25ms, o correto é que ele se mantivesse abaixo dos 10ms visando que neste período não havia nenhum laboratório em uso.



**Figura 10: Gráfico de latência sem aulas.**

Na figura 11 podemos fazer a comparação com o gráfico anterior onde agora foi analisado o gráfico de latência no período de aula, todos os laboratórios estavam em uso e podemos verificar que o *switch* atinge um pico de 60ms considerado alto, pois a perda de pacotes influenciam na lentidão da *internet*, seguindo este raciocínio é possível notar que o *switch* pode estar sobrecarregado, pois ele é o único responsável por gerenciar os nove laboratórios.



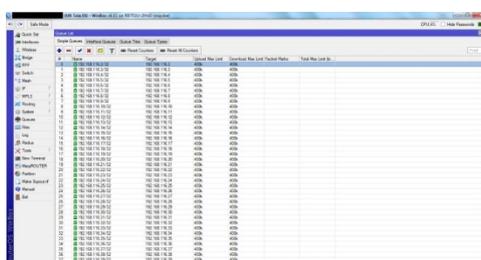
**Figura 11: Gráfico de latência no período de aula.**

### 3.3.3 Limitando Taxa de *download* e *upload* por IP

Todos laboratórios estão com as redes segmentadas, portanto cada *Mikrotik* recebe um IP da rede acadêmica e posteriormente faz o roteamento liberando o *link* para a rede dentro do laboratório.

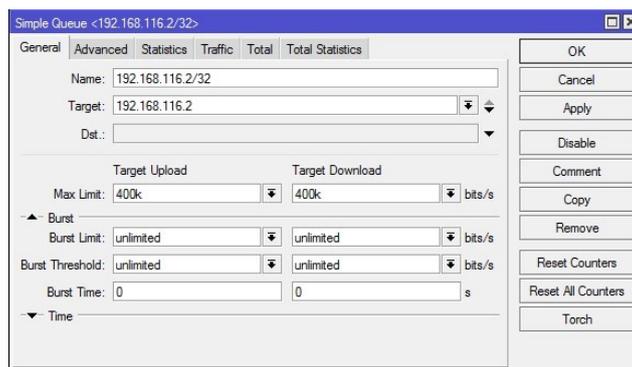
Para que os laboratórios não consumam toda banda da faculdade foram criados limitadores para cada *Mikrotik*, estes limitadores eram baseados no range de IP's de cada laboratório, por exemplo o 192.168.116.0/24, o único problema de usar esse tipo de configuração é em relação ao próprio laboratório, pois se alguma máquina começar a consumir banda demasiadamente, automaticamente as outras máquinas serão prejudicadas pois compartilham do mesmo limite.

Para resolver este problema o limitador foi refeito, agora o limite é fixado em todos IP's do range, dessa forma se uma máquina consumir muita banda a única máquina prejudicada será ela mesma. Essa configuração nós podemos ver na Figura 12.



**Figura 12: Limitando banda por IP's.**

Os limitadores por IP foram fixados em 400k, portanto cada dispositivo dentro do laboratório possui 400k para download e 400k para upload, como podemos ver na Figura 13.



**Figura 13: Limitando banda.**

## 4. RESULTADOS

Logo de início identificamos que as partes de cabeamentos dos laboratórios são bem antigas, elas permanecem as mesmas desde a abertura de cada laboratório, os cabos utilizados são cabos CAT.5 e que trafegam na taxa de 100mbps considerado muito pouco, pois cada laboratório tem no mínimo 150 conexões divididas entre computadores *desktop* e aparelhos celulares, nossa sugestão para o departamento de informática responsável foi à manutenção nesta rede e que fossem utilizados cabos categoria CAT.6 para que a rede possa trafegar em *Gigabit*, essa alteração aumenta a qualidade de distribuição de pacotes pela rede com uma velocidade muito superior a utilizada hoje.

Outro problema identificado foi o *switch* que gerencia todos os laboratórios de informática, ele se sobrecarrega todas as vezes que os laboratórios são utilizados gerando perda de pacotes, onde para chegar ao equipamento destino demora em alguns casos 60ms o que é considerado alto, todos estes dados foram possíveis a serem notados nos gráficos que foram gerados e foi sugerida ao departamento responsável a compra de um *switch* que tenha um melhor processamento ou a utilização de dois *switches* para que possa ser dividido o gerenciamento, com isso diminuindo a perda de pacotes.

Identificamos também que independentemente da quantidade de banda liberada para cada laboratório a lentidão da rede se mantinha onde os alunos burlavam o *proxy*, resolvemos realizar testes de limitação de *Download* e *Upload* por equipamentos seja *desktop* ou *wireless* através do *Mikrotik*, logo de

início foi notado uma melhora significativa pois os sites passaram a abrir rapidamente o que antes que era difícil até mesmo abrir um site de notícias.

## 5. CONSIDERAÇÕES FINAIS

Podemos concluir que a implementação do Zabbix na rede acadêmica consegue trazer grandes benefícios, pois ele traz um melhor controle dos ativos na rede e consegue monitorar com precisão o ambiente em geral, podendo ajudar muito na prevenção de problemas que possam ocorrer. A implementação e o monitoramento da rede descritos neste artigo a fim de procurar gargalos foi um caso de sucesso. Como trabalhos futuros citamos a expansão do projeto para toda a rede da UNIFAFIBE contando administrativo e também demais prédios.

## REFERÊNCIAS

BEZERRA, Romildo Martins. **Interconexão de Redes**. Disponível em: <<http://www2.ufba.br/~romildo/downloads/ifba/interconexao.pdf>>. Acesso em: 08 mai. 2017

COMER, Douglas E. **Redes de Computadores E Internet**. São Paulo: Bookman, 4ª edição, p.137-138. 2007.

COMER, Douglas E. **Redes de Computadores e Internet**. São Paulo: Bookman, 6ª edição, p.13. 2016.

COMER, Douglas E. **Redes de Computadores E Internet**. São Paulo: Bookman, 4ª edição, p.541,542. 2007.

DE FRANCESCHI, ANALÚCIA SCHIAFFINO MORALES.; BARRETO, J. M.; ROISENBERG, M. **Desenvolvimento de Agentes Autônomos em gerência de Redes de Computadores**. Disponível em: <[https://www.researchgate.net/profile/Analucia\\_Morales/publication/266037786\\_DESENVOLVIMENTO\\_DE\\_AGENTES\\_AUTONOMOS\\_PARA\\_GERENCIA\\_D\\_E\\_REDES\\_DE\\_COMPUTADORES/links/549011480cf225bf66a8115f.pdf](https://www.researchgate.net/profile/Analucia_Morales/publication/266037786_DESENVOLVIMENTO_DE_AGENTES_AUTONOMOS_PARA_GERENCIA_D_E_REDES_DE_COMPUTADORES/links/549011480cf225bf66a8115f.pdf)>. Acesso em: 09 mai. 2017

FACHINI, Thiago. **Implementação da ferramenta Zabbix para monitoramento reativo**. Disponível em: <[http://www.ulbra.inf.br/joomla/images/documentos/TCCs/2010\\_2/redes-thiago%20fachini.pdf](http://www.ulbra.inf.br/joomla/images/documentos/TCCs/2010_2/redes-thiago%20fachini.pdf)>. Acessado em: 09 mai. 2017

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. São Paulo: Bookman, p.446. 2006.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. São Paulo: AMGH, 4ª edição, p.267-269. 2009.

MAIA, Luis Paulo. **Arquitetura de Redes de Computadores**. LTC, 2ª edição, p.29-152. 2013.

ROSS, Julio. **Redes de computadores**. Julio Ross, p.65-67. 2008.

SANTANA, Hugo. **Qualidade de serviço (QoS) em redes ip princípios básicos parâmetros e mecanismos**. Disponível em: <[http://professores.unisanta.br/santana/downloads%5CTelecom%5CCom\\_Digitais%5CAulas%20o.%20Bimestre%5CTexto%20QoS\\_IP\\_Istelcon.pdf](http://professores.unisanta.br/santana/downloads%5CTelecom%5CCom_Digitais%5CAulas%20o.%20Bimestre%5CTexto%20QoS_IP_Istelcon.pdf)>. Acesso em: 08 mai. 2017

STANGARLIN, Douglas P. ; PRIESNTZ FILHO, Walter. **Análise de desempenho de redes sem fio com diferentes protocolos de criptografia**. Disponível em: <[http://www.redes.ufsm.br/docs/tccs/Douglas\\_Pegoraro\\_Stangarlin.pdf](http://www.redes.ufsm.br/docs/tccs/Douglas_Pegoraro_Stangarlin.pdf)>. Acesso em: 08 mai. 2017

TANENBAUM, Andrew S. **Redes de Computadores**. Rio de Janeiro: Elsevier, 4ª edição, p.44. 2003.

O que é Zabbix? Disponível em: <<https://www.4linux.com.br/o-que-e-zabbix>>. Acesso em: 18 sete. 2017.

UCHOA, Joaquim Quinteiro. **Algoritmos Imunoinspirados aplicados em segurança computacional: utilização de algoritmos inspirados no sistema imune para detecção de intrusos em redes de computadores**. 2009. 279 f. Tese de Doutorado (Doutor em Bioinformática). Universidade Federal de Minas Gerais. Belo Horizonte. 2009.

YANO, I. H. **Gerenciamento de redes de computadores utilizando CACTI**. Disponível em: <<http://agris.fao.org/agris-search/search.do?recordID=BR20101883562>>. Acesso em: 09 mai. 2017

ZABBIX DOCUMENTATION. Disponível em: <<https://www.zabbix.com/documentation/3.4/pt/manual>>. Acesso em: 13 sete. 2017.