

Análise de Tráfego da Coordenadoria de Informática do IFS - Campus Lagarto

Dívia França de Oliveira ¹, Rogério Silva Santos² , Rubens de Souza Matos Júnior³

¹Curso Integrado de Redes – Instituto Federal de Sergipe (IFS) – Campus Lagarto
Lagarto – SE– Brasil

²Curso Integrado de Redes – Instituto Federal de Sergipe (IFS) – Campus Lagarto
Lagarto – SE– Brasil

³Professor Orientador – Instituto Federal de Sergipe (IFS) – Campus Lagarto
Lagarto – SE– Brasil

¹divia.rds@gmail.com , ²rogersil.RrS@gmail.com, ³rubens.matos@gmail.com

Abstract

In this article we will present the monitoring of network traffic from the Instituto Federal de Sergipe - Campus Lagarto showing the any results obtained after a period of rhythm analysis . We begin with a brief explanation about monitoring networks, after show which tool was used, results, comparisons and finally the conclusions taken from the collected data.

Resumo

Neste artigo iremos apresentar o monitoramento do tráfego da rede do Instituto Federal de Sergipe - Campus Lagarto mostrando os eventuais resultados obtidos após um período de tempo de análises. Iniciaremos com uma breve explicação sobre monitoramento de redes, logo após mostraremos qual ferramenta foi utilizada, resultados, comparações e por fim as conclusões tomadas a partir dos dados coletados.

1. Introdução

As redes de computadores são essenciais para as atividades de qualquer empresa ou organização atual. Elas permitem o compartilhamento de dados e execução de tarefas administrativas usando sistemas e serviços hospedados na própria instituição, tais como consultas on-line à biblioteca e registro eletrônico de aulas e notas além de permitir o acesso a todos os recursos disponíveis globalmente na Internet (MACHADO, 2009). O monitoramento do desempenho e disponibilidade dos equipamentos e enlaces de rede é uma tarefa essencial para detectar possíveis problemas, permitindo que sejam propostas soluções, assim como melhorias para a infraestrutura existente.

A qualidade de serviço (QoS - Quality of Service) das aplicações em rede pode ser medida através de atributos como vazão, latência, e taxa de perda de pacotes (TANENBAUM, 2013). A vazão requerida por uma aplicação, comumente representada em bits por segundo, somente será alcançada se houver largura de banda suficiente para tal. Isto vai depender das características do meio físico, tecnologias de enlace, da quantidade de usuários e de aplicações concorrendo pelos mesmos recursos da rede local ou do enlace de longa distância com o provedor de Internet. O monitoramento de tráfego é uma das tarefas essenciais do gerenciamento de rede. Através do monitoramento é possível identificar o nível de utilização dos enlaces e relacionar problemas de desempenho com determinados hosts ou sub-redes que podem estar gerando uma sobrecarga na infraestrutura existente (LOPES; SAUVÉ; NICOLETTI, 2003).

Este projeto visa analisar o tráfego da rede do campus Lagarto do Instituto Federal de Sergipe, utilizando ferramentas de monitoração baseadas no protocolo de gerenciamento SNMP. Inicialmente serão coletados dados do switch de distribuição localizado no prédio das coordenações dos cursos de redes de computadores e de sistemas de informação (COINF/CBSI), que agrega os dados recebidos da camada de acesso referente aos laboratórios e salas dessas coordenações. Pretende-se monitorar a rede durante um período de 14 dias, e analisar questões como: percentual médio de utilização da largura de banda; horários e dias de pico de utilização da rede; laboratórios que mais geram tráfego; principais sites acessados; principais protocolos presentes no tráfego de rede. É importante ressaltar que a coleta de dados será realizada de maneira a preservar a privacidade dos usuários da rede. Não serão capturados pacotes, nem armazenados quaisquer outras informações que permitam associar, de forma individual, os usuários com os sites e demais serviços acessados através da rede.

2. Materiais e Métodos

Para o monitoramento da rede, utilizou-se o Cacti (Cacti, 2016), uma ferramenta open source que monitora e analisa informações sobre o funcionamento de uma rede de computadores exibindo-as em forma de gráficos. É uma ferramenta robusta e de fácil usabilidade, feita para se adaptar a diversas necessidades.

Dentre suas vantagens estão: um rápido coletor de dados; personalização avançada de gráficos; métodos de aquisição de dados múltiplos; e monitoramento do estado de elementos de rede, programas, largura de banda utilizada e uso de CPU. Estas características tornam o Cacti adequado para o monitoramento desde redes pequenas até redes complexas com centenas de dispositivos.

O Cacti é preparado para funcionar na estrutura do RRDTOol (Round Robin Database), que é responsável pelo armazenamento dos dados numéricos em série sobre o estado de redes de computadores ou no armazenamento de qualquer outra série de dados (temperatura, uso de CPU e outros), que são obtidos em um período de tempo pré-determinado. O Cacti é utilizado pelo RRDTOol como front-end para poder gerar toda a ilustração visual dos resultados obtidos. A comunicação entre eles é feita através de scripts que transferem os dados entre os programas.

Para o monitoramento de equipamentos de rede com o Cacti, utilizamos o protocolo SNMP (*Simple Network Management Protocol*), que é um protocolo de gerenciamento de rede. O SNMP permite monitorar remotamente switches, roteadores e servidores que possuam suporte a este protocolo.

A primeira versão do SNMP não gerenciava, ele apenas monitorava dispositivos de forma simples com arquitetura TCP/IP. A segunda versão possibilitou o gerenciamento dos agentes (sistema do equipamento gerenciado), gerenciamento de serviços, e implementação de segurança e confidencialidade.

Já na terceira e atual versão, utilizada neste projeto, houve o aprimoramento da segurança, implementação de autenticação e controle de acesso entre gerente (aplicação que propicia a troca de mensagens com o agente) e agentes, tornando-a melhor e mais segura que as anteriores.

O monitoramento feito na rede da COINF teve duração de 14 dias e ocorreu de 01 à 07 e 15 à 21 de Maio onde foi analisado, através de gráficos, o tráfego de 159 (cento e cinquenta e nove) computadores distribuídos entre 09 (nove) laboratórios e a sala da Coordenação.

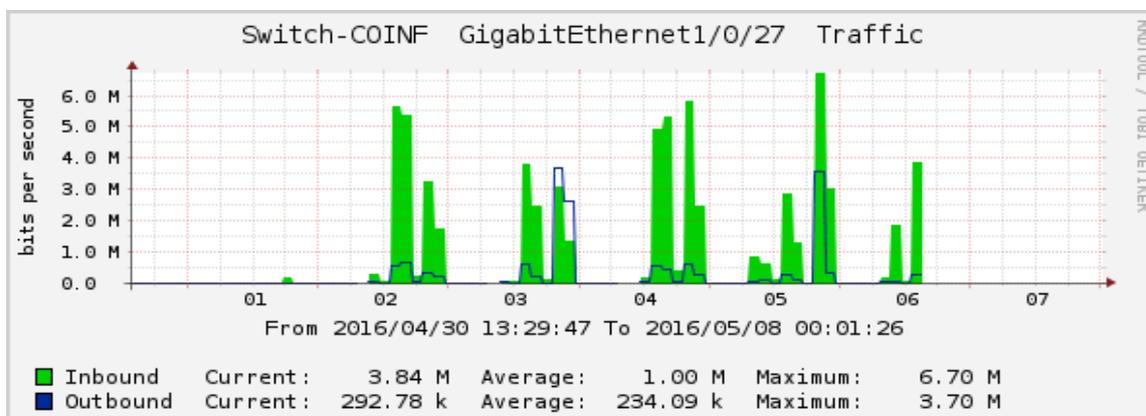
3. Resultados e Discursões

Antes de analisar os dados graficos coletados a partir do monitoramento do switchi da Coinf fizemos uma tabela (tabela 1) com os horarios em que há aula nos laboratorios da mesma. Utilizamos esta tabela para poder fazer comparações entre os dias monitorados.

	Segunda	Terça	Quarta	Quinta	Sexta
Manhã			X*	X	
Tarde	X	X	X	X	X
Noite	X	X	X	X	X

*Tabela 1

A imagem 1 refere-se as dias de 01 à 07 de Maio, primeira semana que foi monitorada.



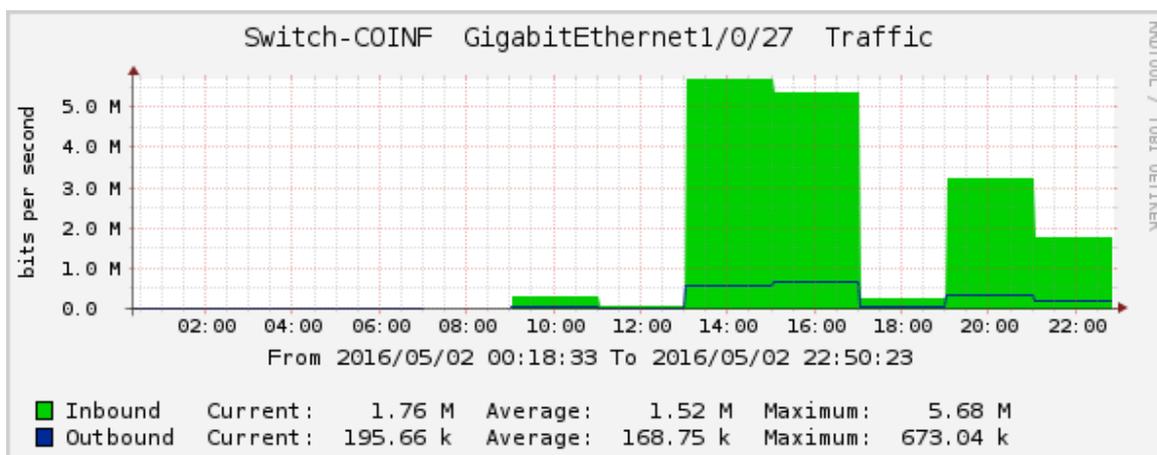
*Imagem 1

A tabela 2 mostra, de forma mais detalhada, as infoirmações de trafego que foram obtidos a partir do gráfico da imagem 1. Essas formações mostram os dias que foram analisados, seu horario e tráfego de pico e média, se tinha aula ou não na referente dia. Nesta tabela será possível perceber que no sábado e domingo não há usuários na rede, mas há comunicação entre o switch da COINF e os demais switchs do Instituto. Essa troca de mensagens entre os equipamento deve-se aos protocolos de roteamento e gerenciamento de redes, por exemplo o STP (Spanning Tree Protocol) e outros similares, explicando o tráfego tão baixo verificado. O percentual da semana, em relação a largura de banda do IFS, que é de 20Mbps, foi de 33,5% e o percentual da média da semana foi de 5%.

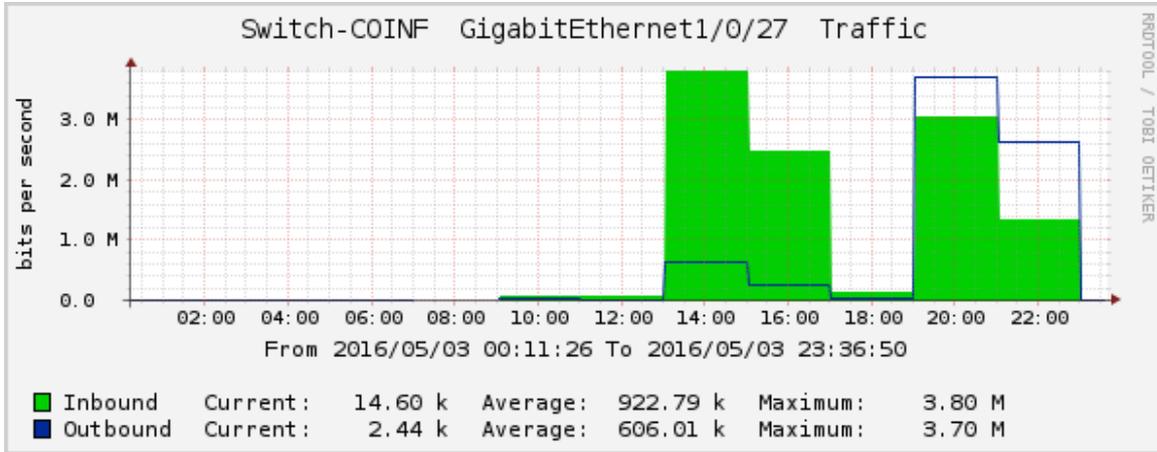
Dia	Pico	Horário do Pico	Vazão média	Horário de Aula
Dom, 01/05	185.75Kbps	entre 17 - 19h	74.52Kbps	Sem aula**
Seg, 02/05	5.68Mbps	entre 13 - 17h	1.39Mbps	Sim
Ter, 03/05	3.80Mbps	entre 13 - 15h	922.79Kbps	Sim
Qua, 04/05	5.84Mbps	entre 19 - 21h	1.75Mbps	Sim
Qui, 05/05	6.70Mbps	entre 19 - 21h	1.20Mbps	Sim
Sex, 06/05	3.84Mbps	entre 13 - 15h	1.0Mbps	Sim
Sáb, 07/05	-	-	-	Sem aula**

*Tabela 2

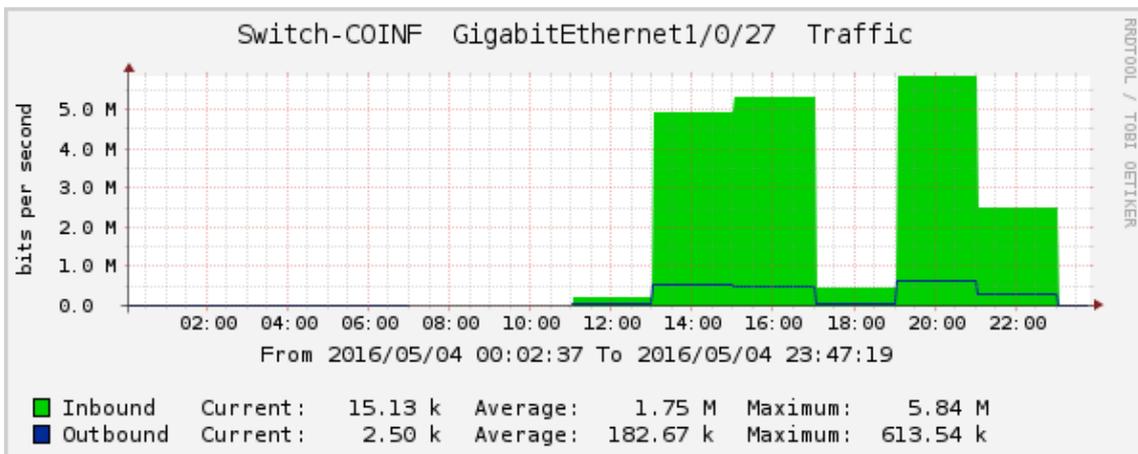
- Segunda (02/05/16)



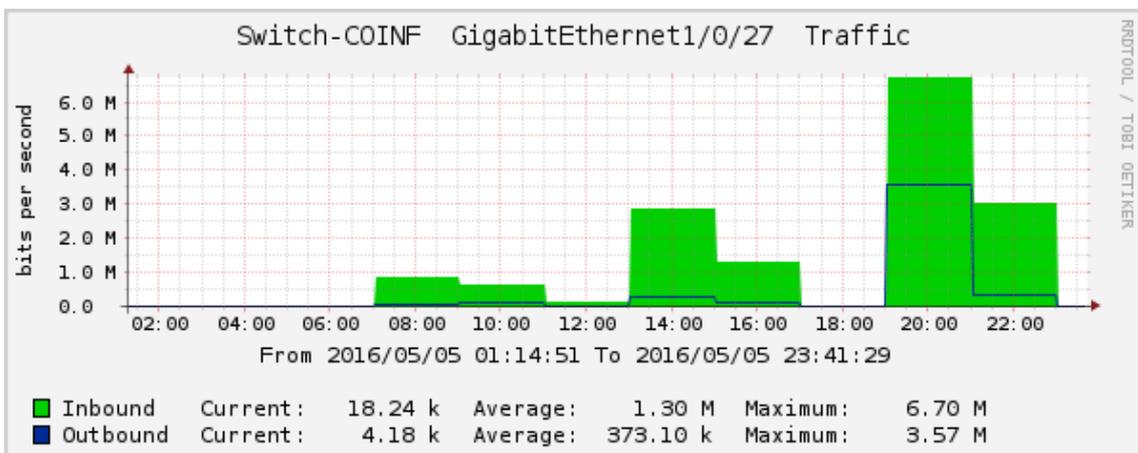
- Terça (03/05/16)



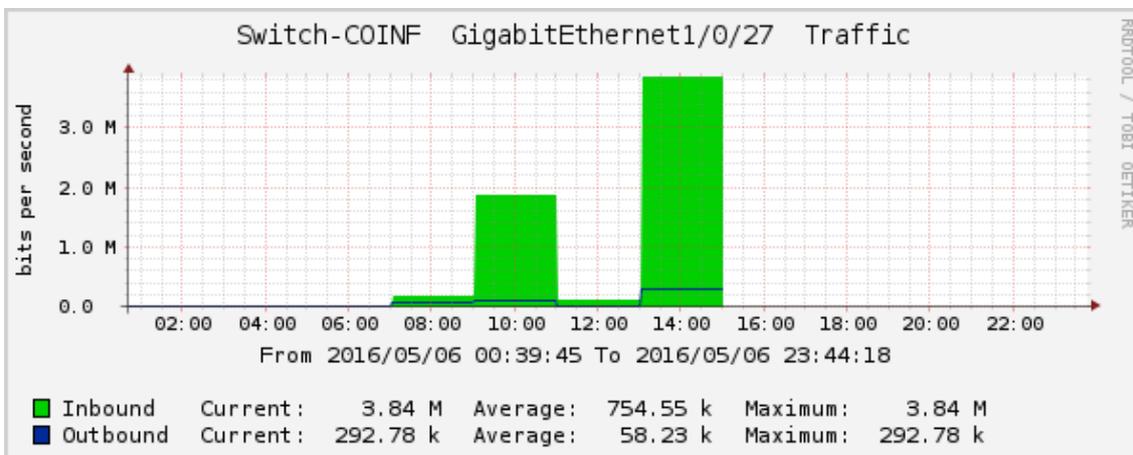
- Quarta (04/05/16)



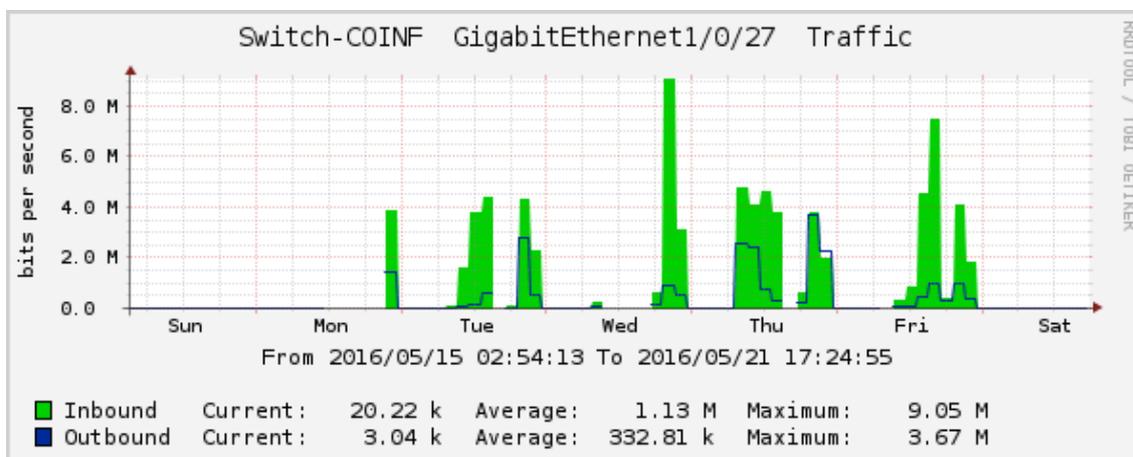
- Quinta (05/05/16)



- Sexta (06/05/16)



A imagem 2 refere-se aos dias de 15 à 21 de Maio, segunda semana que foi monitorada.



*Figura 2.

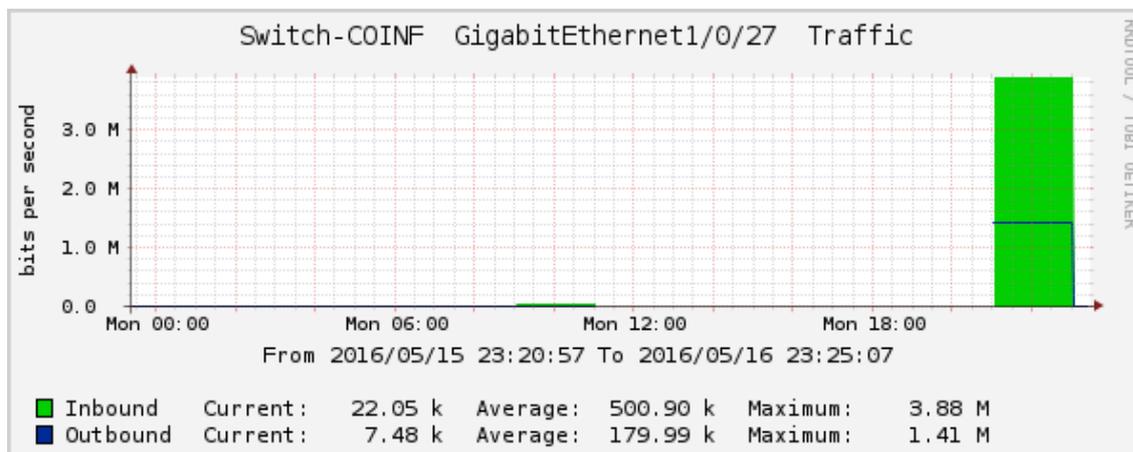
A tabela 3 mostra, assim como a tabela 2, de forma mais detalhada as informações de tráfego que foram obtidos a partir do gráfico da imagem 2. Na tabela há informações dos dias que foram analisados, seu horário e tráfego de pico e média, se tinha aula ou não na referente dia. Nela tbm é possível perceber que no sábado e domingo não há usuários na rede, por conta da comunicação entre o switch da COINF e os demais switches do Instituto. Essa troca de mensagens entre os equipamento deve-se aos protocolos de roteamento e gerenciamento de redes, por exemplo o STP (Spanning Tree Protocol) e outros similares, explicando o tráfego tão baixo verificado. O

percentual da semana, em relação a largura de banda do IFS, que é de 20Mbps, foi de 45.25% e o percentual da média da semana foi de 5,65%.

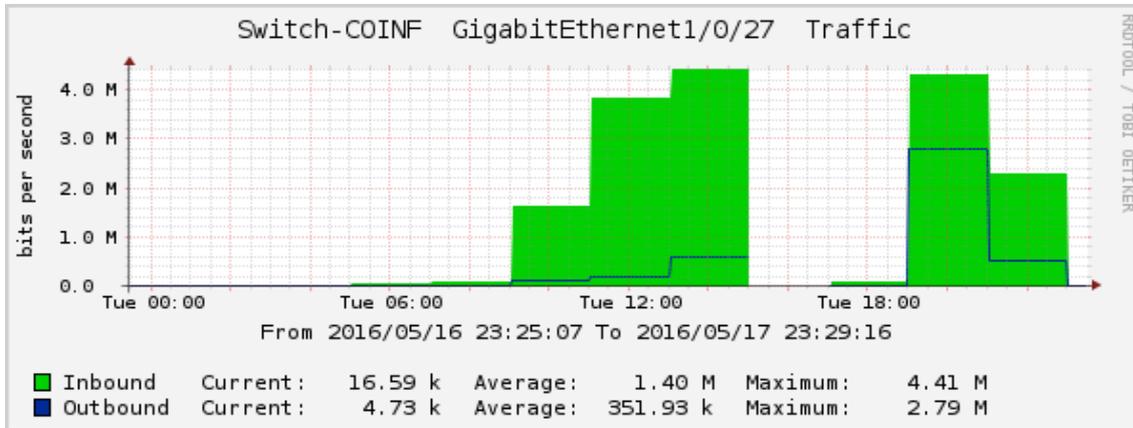
Dia	Pico	Horário do Pico	Média de Consumo	Horário de Aula
Domingo, 15/05	55.61Kbps	entre 11 - 13h	20.3Kbps	Sem aula**
Segunda, 16/05	3.88Mbps	entre 21 - 23h	500.9Kbps	Sim
Terça, 17/05	4.41Mbps	entre 13 - 15h	1.4Mbps	Sim
Quarta, 18/05	9.05Mbps	entre 19 - 21h	1.46Mbps	Sim
Quinta, 19/05	4.77Mbps	entre 07 - 09h	2.08Mbps	Sim
Sexta, 20/05	7.51Mbps	entre 15 - 17h	1.5Mbps	Sim
Sábado, 21/05	39.33Kbps	entre 09 - 11h	23.49Kbps	Sem aula**

*Tabela 2.

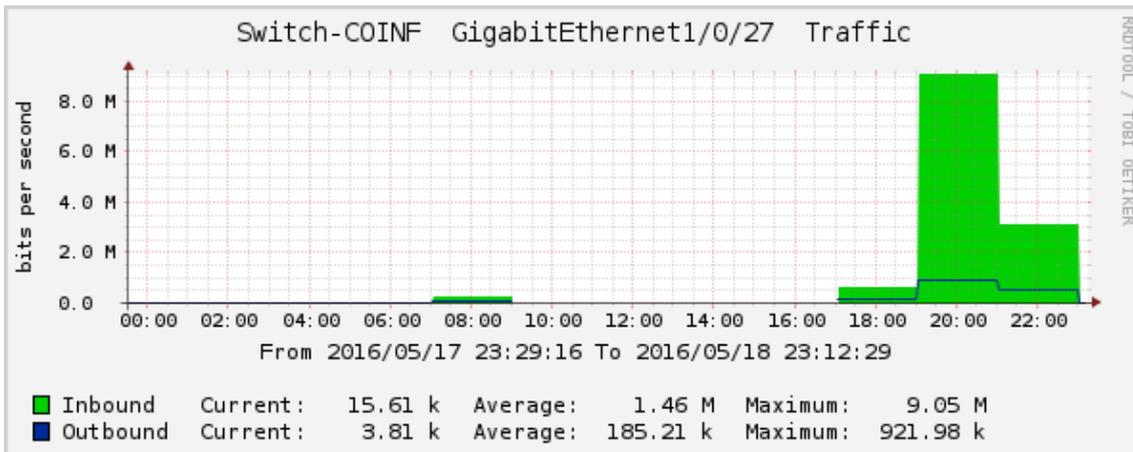
- Segunda (16/05/16)



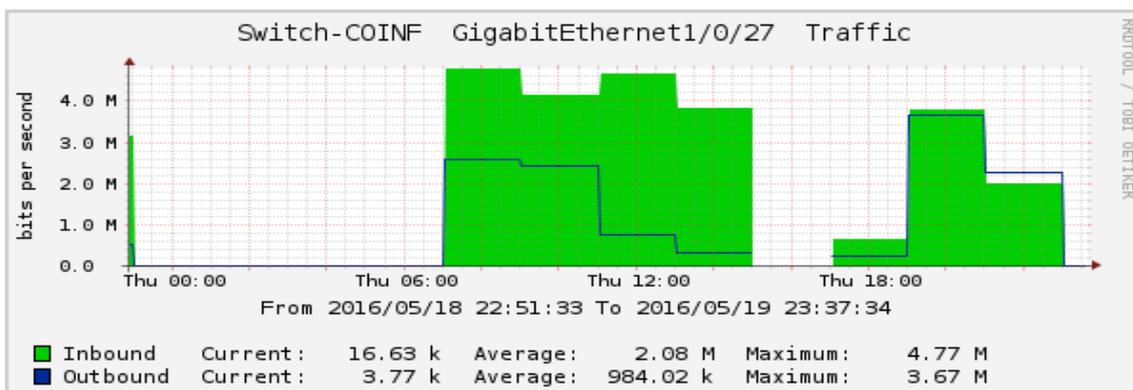
- Terça (17/05/16)



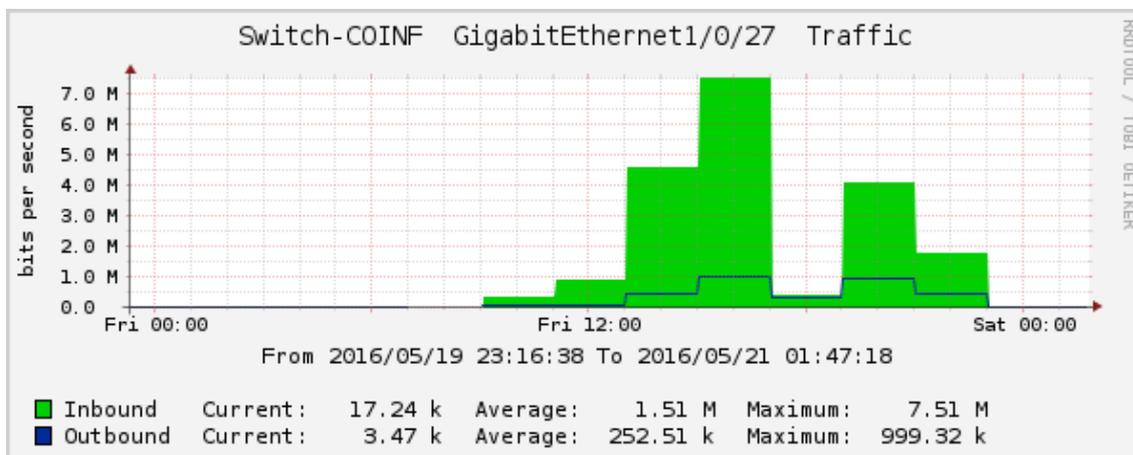
- Quarta (18/05/16)



- Quinta (19/05/16)



- Sexta (20/05/16)



4. Conclusão

Este projeto teve como objetivo analisar, através de gráficos, o fluxo de dados da rede da Coordenadoria de Informática (Coinf) do IFS - Lagarto. Com os gráficos obtidos foi possível fazer um comparatório entre os dias analisados e os horários de aula nos laboratórios da Coinf, onde nota-se que os a maior de demanda de tráfego é em horário de aula. A média das duas semanas analisadas, em relação a largura de banda do IFS, que é de 20Mbps, foi de 37,87%, e o maior pico registrado foi de 9.05%, ocorreu em uma quarta-feira entre às 19 - 21h, em horário de aula.

5. Referências

LOPES, R. V.; SAUVÉ, J. P.; NICOLETTI, P. S. “Melhores Práticas para a Gerência de Redes de Computadores”. Campus, ed, 2003.

MACHADO, R. “Sistema de Informação Baseado numa Intranet para a Gestão Pedagógica de uma Escola do Ensino Secundário.” Porto: Universidade do Porto. 1999.

MRTG, “Multi Router Traffic Grapher”. Disponível: <<http://oss.oetiker.ch/mrtg/>>. Acesso: Fevereiro/2016.

NAGIOS, “The Industry Standard In IT Infrastructure Monitoring”. Disponível: <<https://www.nagios.org/>>. Acesso: Fevereiro/2016.

TANENBAUM, A. S. “Computer Networks.” Campus, 4.ed, 2013.

ZABBIX, “The Enterprise-class Monitoring Solution for Everyone”. Disponível: <<http://www.zabbix.com/>>. Acesso: Fevereiro/2016.

TECHTUDO. “Cacti: Descrição”. 2010. Disponível: <<http://www.techtudo.com.br/tudo-sobre/cacti.html#carousel-galeria>>. Acesso: Fevereiro/2016

CACTI, the complete RRDTool-based graphing solution. . “About Cacti”. Disponível em: <<http://www.cacti.net/>>. Acesso: Fevereiro/2016.

DAGHETTI, Rafael. “Cacti: Gerenciamento de redes com os plugins Weathermap e Monitor no Debian Etch Linux”. 2008. Disponível: <<https://www.vivaolinux.com.br/artigo/Cacti-Gerenciamento-de-redes-com-os-plugins-Weathermap-e-Monitor-no-Debian-Etch-Linux>>. Acesso: Fevereiro/2016

FASSI. “Comparativo entre as versões do SNMP”. Disponível: <<http://www.fassi.eti.br/artigos/gerencia-de-redes/comparativo-entre-as-versoes-do-snm>>. Acesso: Maio/2016

4LINUX. “O que é SNMP?”. Disponível: <<https://www.4linux.com.br/o-que-e-snm>>. Acesso: Maio/2016