FACULDADE DE TECNOLOGIA SENAC GOIÁS
Segurança da Informação

Aldo Brito
Jordan Gladys
Liniker Lettierre
Rony Carneiro

FERRAMENTAS DE GERÊNCIA EM REDES

Fernando Pirkel Tsukahara

GOIÂNIA,
2016

Aldo Brito
Jordan Gladys
Liniker Lettierre
Rony Carneiro

FERRAMENTAS DE GERÊNCIA EM REDES

Relatório apresentado como requisito parcial para obtenção de aprovação na disciplina Gerência de Redes de Computadores, no Curso de Segurança da Informação, na Faculdade de Tecnologia Senac Goiás.

Fernando Pirkel Tsukahara

GOIÂNIA,
2016

SUMÁRIO

1 INTRODUÇÃO

O gerenciamento de rede pode ser definido como a coordenação de recursos lógicos, fisicamente distribuídos na rede, assegurando, na medida do possível, confiabilidade, tempos de resposta aceitáveis e segurança das informações.

2 DESENVOLVIMENTO

Conforme os objetivos específicos da PSI a alta disponibilidade e a garantia da proteção das informações em redes constituem um dos critérios de grande importância para a gerência de redes.

Como o gerenciamento de rede implica na utilização de várias ferramentas inseridas em uma estrutura, de certa forma complexa, com os limites de atuação definidos, se possível padronizado, entre os componentes envolvidos, é importante definir aspectos como a estratégia que será usada no atendimento dos usuários, atuação do pessoal envolvido nas tarefas de gerenciamento, supridores de serviços, etc.

Os tipos mais básicos de tarefas de gerenciamento de uma rede são: monitoração e controle. A monitoração consiste na observação periódica dos objetos gerenciados, importantes para a política de gerenciamento. A partir da monitoração, o gerente tem conhecimento do estado da rede e, desta forma, pode efetuar operações de controle sobre a mesma.

A distribuição das funções de monitoramento é mais premente em relação às funções de controle, pois a monitoração consome mais recursos da rede, bem como a atenção do gerente, pois através dela é que se obtém o estado da rede em relação ao tempo, enquanto que as funções de controle são invocadas em menor número, geralmente com objetivos de alteração de configuração e erradicação de problemas.

O limite de atuação desta gerência, ou seja, o controle deve levar em conta a amplitude desejada pelo modelo implantado na instalação que, além de operar a rede, deve envolver tarefas como:

- Controle de acesso à rede;
- Disponibilidade e desempenho;
- Documentação de configuração;
- Gerência de mudanças;
- Planejamento de capacidade
- Auxílio ao usuário;
- Gerência de falhas;
- Controle de inventário.

Dentre as inúmeras ferramentas para o monitoramento da rede foi escolhida o nagios e o cacti. Nagios para estar monitoramento os serviços, como o banco de dados da empresa, e o Cacti para estar monitorado a rede da empresa.

3 USO DAS FERRAMENTAS

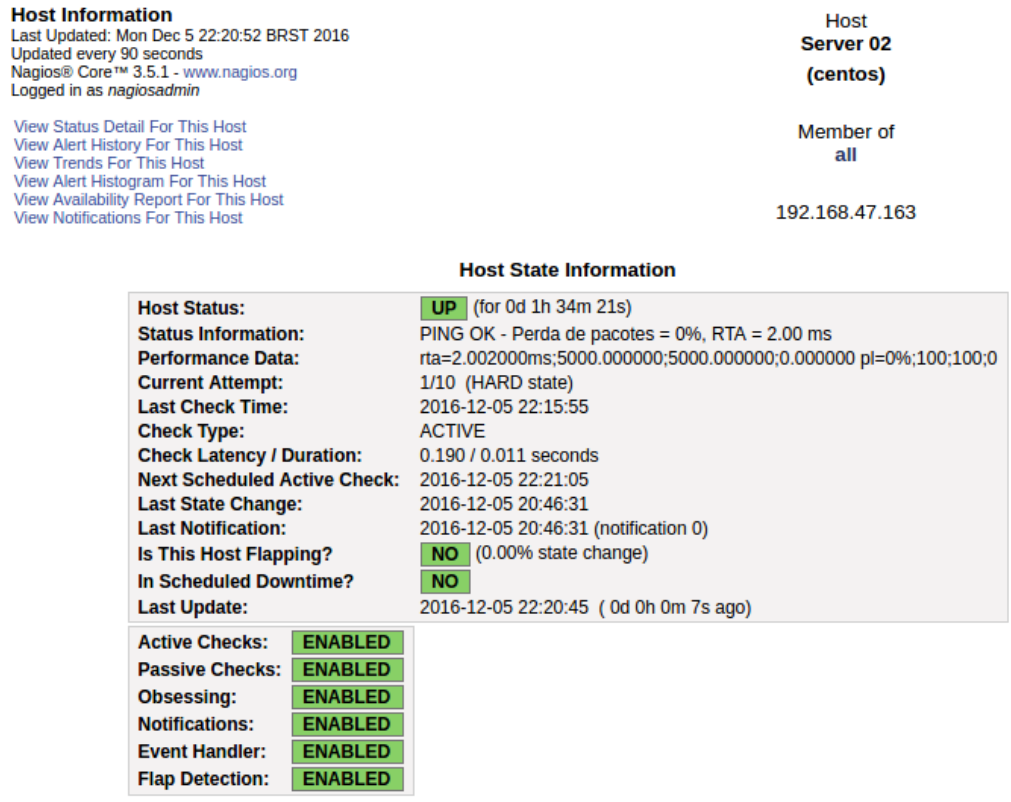
3.1 Nagios

Após ter o Nagios instalado e funcionando normalmente deverá ser adicionado uma definição de hosts e serviços para o Nagios comunicar com o banco de dados PostgreSQL.

Como solução de alta eficiência em ambientes controlados, será adotado o conceito de alta disponibilidade em um banco de dados.

Será utilizado a ferramenta Nagios (software livre), que é uma ferramenta de gestão de rede funcional e versátil comparado com outras ferramentas comerciais.

- Com a ferramenta nagios verificado o status do computador com o servidor de banco de dados.



Host Information
Last Updated: Mon Dec 5 22:20:52 BRST 2016
Updated every 90 seconds
Nagios® Core™ 3.5.1 - www.nagios.org
Logged in as *nagiosadmin*

View Status Detail For This Host
View Alert History For This Host
View Trends For This Host
View Alert Histogram For This Host
View Availability Report For This Host
View Notifications For This Host

Host
Server 02
(centos)

Member of
all

192.168.47.163

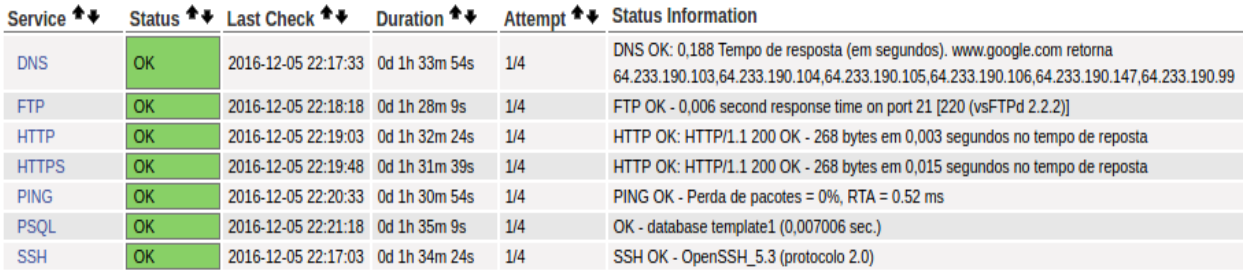
Host State Information

Host Status:	UP (for 0d 1h 34m 21s)
Status Information:	PING OK - Perda de pacotes = 0%, RTA = 2.00 ms
Performance Data:	rta=2.002000ms;5000.000000;5000.000000;0.000000 pl=0%;100;100;0
Current Attempt:	1/10 (HARD state)
Last Check Time:	2016-12-05 22:15:55
Check Type:	ACTIVE
Check Latency / Duration:	0.190 / 0.011 seconds
Next Scheduled Active Check:	2016-12-05 22:21:05
Last State Change:	2016-12-05 20:46:31
Last Notification:	2016-12-05 20:46:31 (notification 0)
Is This Host Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	2016-12-05 22:20:45 (0d 0h 0m 7s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

Máquina com sistema operacional CentOs

- Com a ferramenta nagios verificado como estão os serviços na máquina com o servidor de banco de dados.



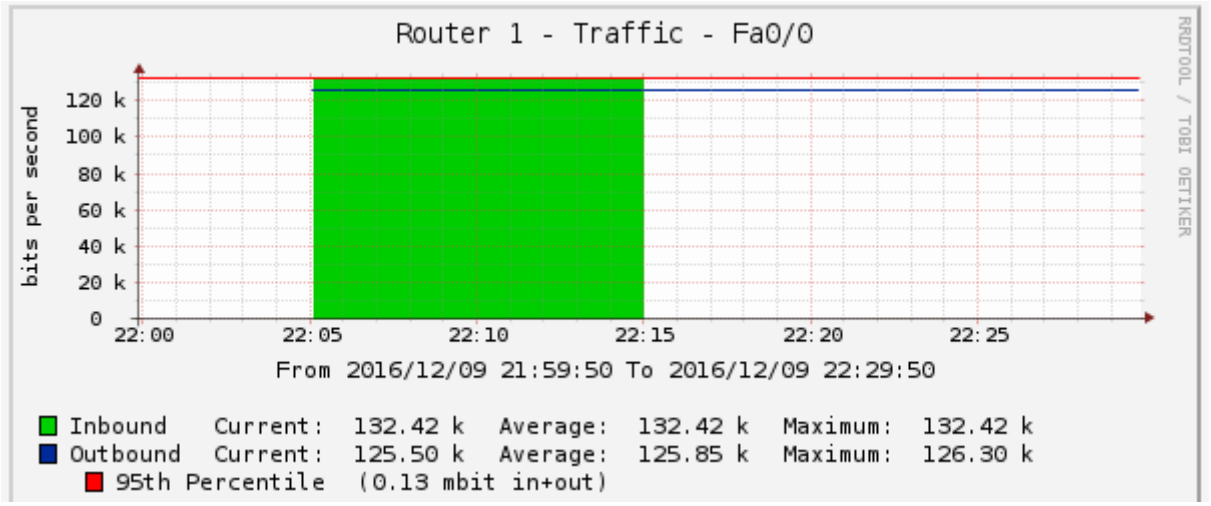
Service	Status	Last Check	Duration	Attempt	Status Information
DNS	OK	2016-12-05 22:17:33	0d 1h 33m 54s	1/4	DNS OK: 0,188 Tempo de resposta (em segundos). www.google.com retorna 64.233.190.103,64.233.190.104,64.233.190.105,64.233.190.106,64.233.190.147,64.233.190.99
FTP	OK	2016-12-05 22:18:18	0d 1h 28m 9s	1/4	FTP OK - 0,006 second response time on port 21 [220 (vsFTPd 2.2.2)]
HTTP	OK	2016-12-05 22:19:03	0d 1h 32m 24s	1/4	HTTP OK: HTTP/1.1 200 OK - 268 bytes em 0,003 segundos no tempo de reposta
HTTPS	OK	2016-12-05 22:19:48	0d 1h 31m 39s	1/4	HTTP OK: HTTP/1.1 200 OK - 268 bytes em 0,015 segundos no tempo de reposta
PING	OK	2016-12-05 22:20:33	0d 1h 30m 54s	1/4	PING OK - Perda de pacotes = 0%, RTA = 0.52 ms
PSQL	OK	2016-12-05 22:21:18	0d 1h 35m 9s	1/4	OK - database template1 (0,007006 sec.)
SSH	OK	2016-12-05 22:17:03	0d 1h 34m 24s	1/4	SSH OK - OpenSSH_5.3 (protocolo 2.0)

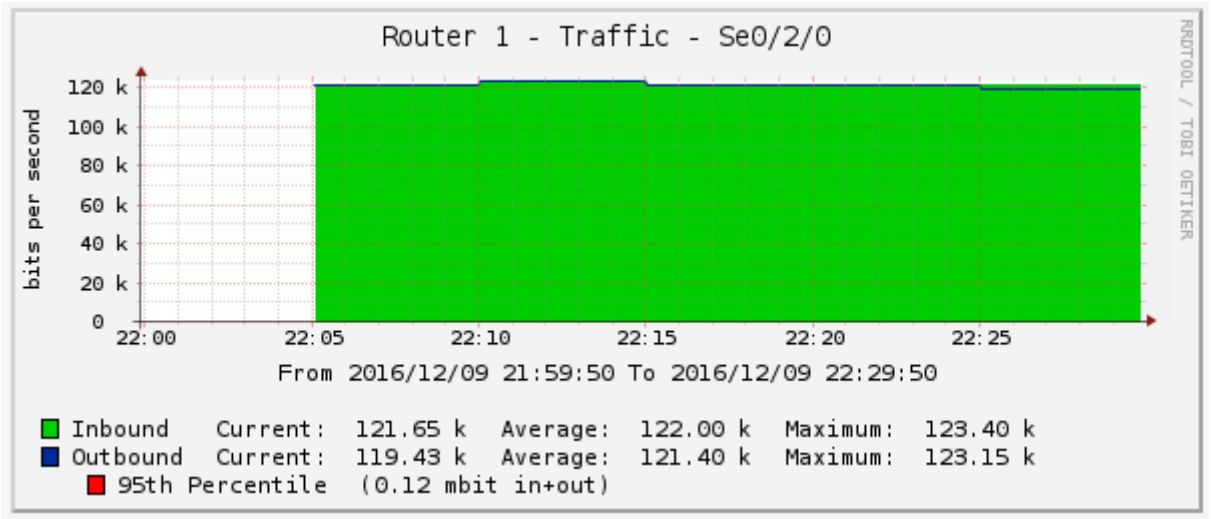
Máquina com sistema operacional CentOs

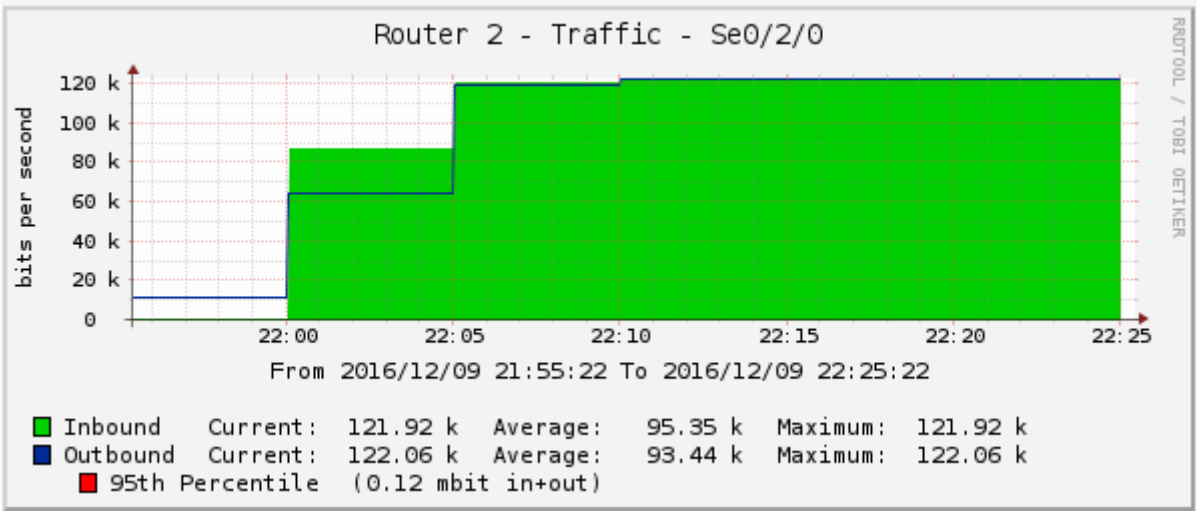
3.2 Cacti

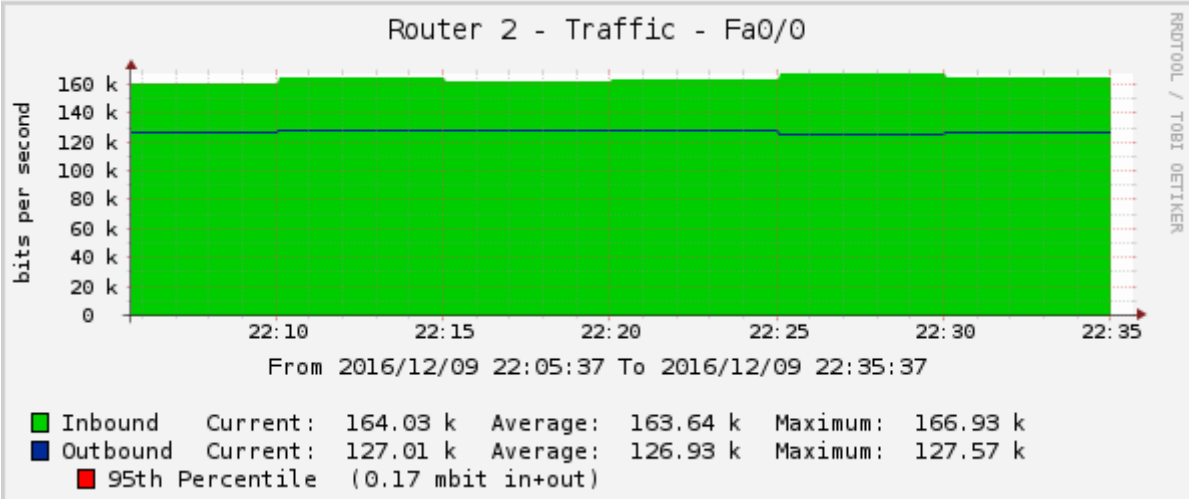
Para realizar o monitoramento da rede sobre o servidor VoIP (Asterisk) é utilizado a ferramenta Cacti.

Monitoramento da rede sem o uso de QOS no serviço de VoIP:



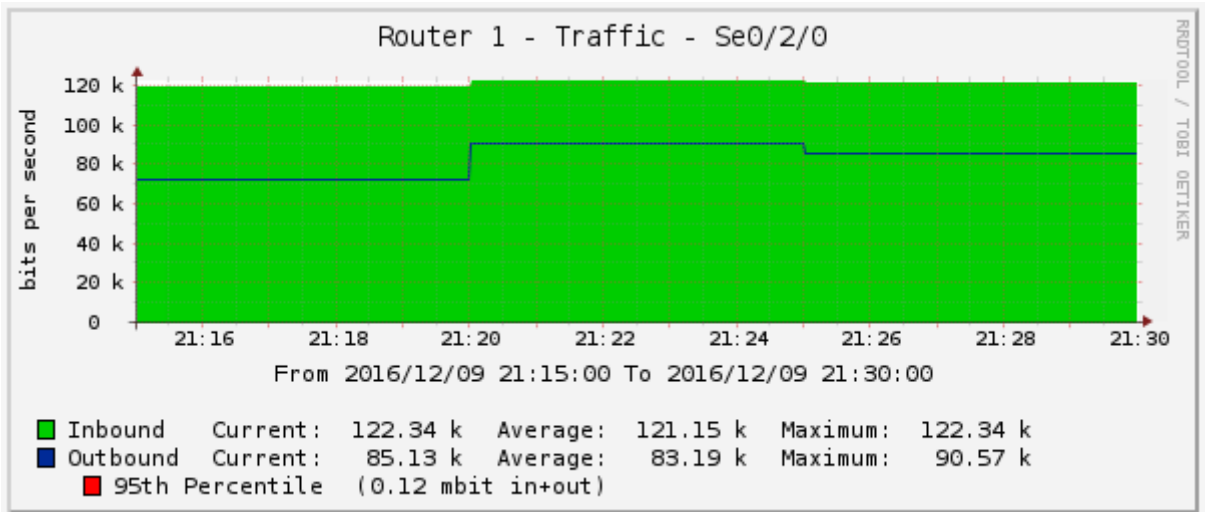


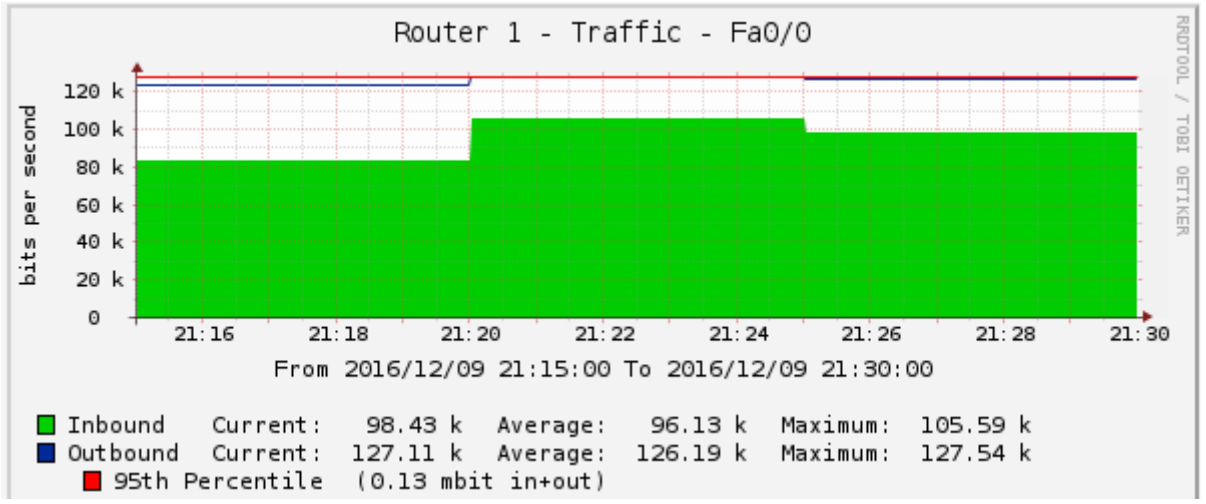


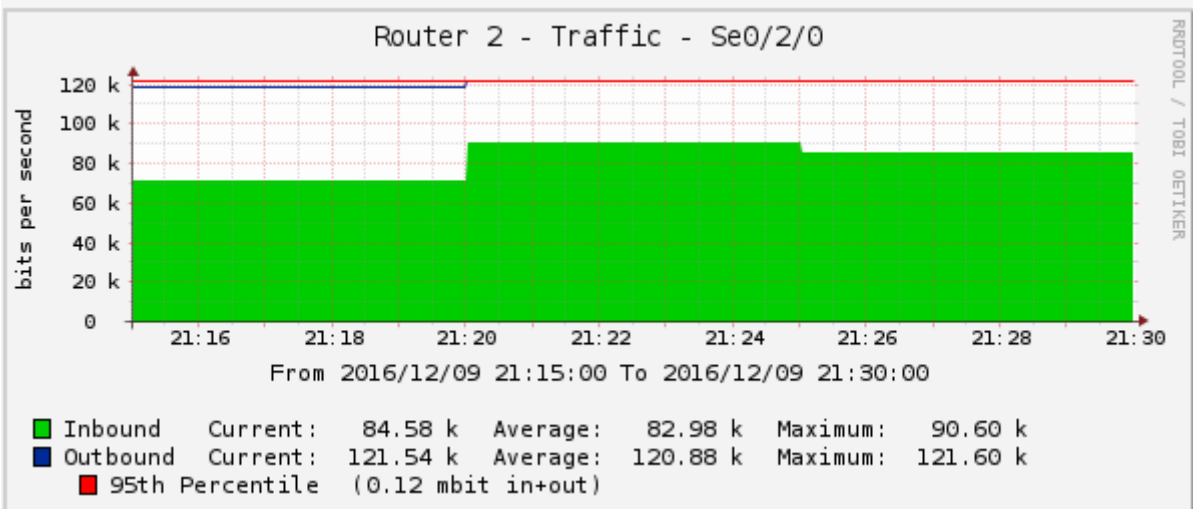


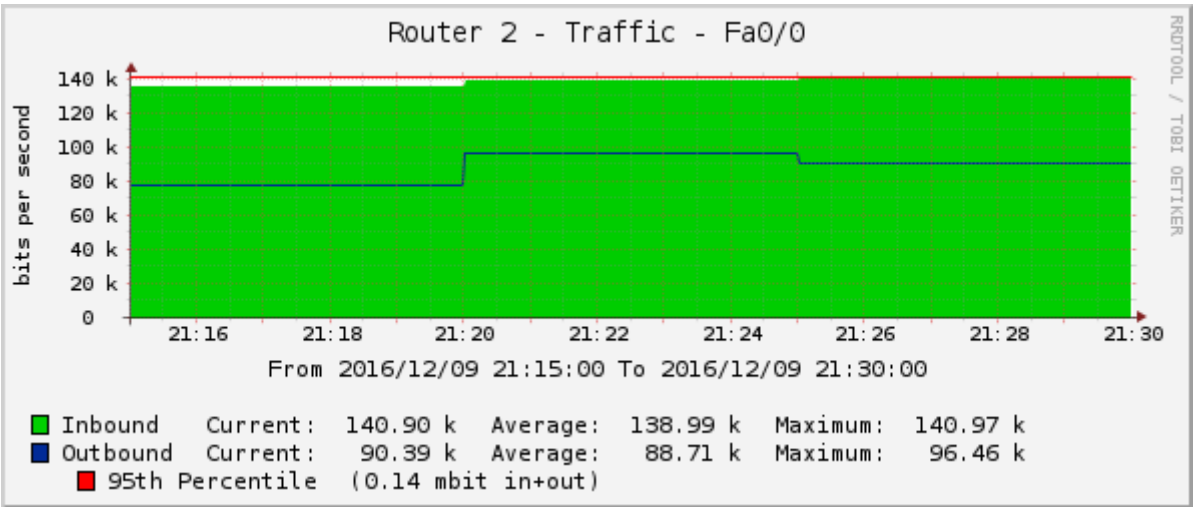
Conforme se pode analisar nos gráficos do trafego gerado pelo VOIP e Netcat, quando a transmissão estava sem o QOS não havia uma prioridade entre os pacotes e todos eram mandados sem exceções com algumas perdas.

Monitoramento da rede com o uso de QOS no serviço de VoIP:









Com a implementação do QOS os pacotes que estavam sendo enviados do VOIP obtiveram mais prioridade e não foi descartado, já os pacotes do Netcat foram descartados com maior frequência devido ao tipo de prioridade que lhe foi dado, conforme mostrado na imagem de output da interface.

```
Output queue (queue priority: size/max/drops):
    high: 0/20/0, medium: 0/40/0, normal: 0/60/42, low: 0/80/4329
```

A análise destes gráficos nos permitiu ter uma visão mais clara sobre o funcionamento geral do modelo TCP/IP em uma transmissão com uma largura de banda baixa para a atualidade devido a limitações do equipamento, fazendo assim, que utilizássemos técnicas para melhoria desta transmissão.

4 CONCLUSÃO

Conforme a PSI implantada o monitoramento das redes e dos recursos devem ser monitorados e analisados criticamente de forma regular é de extrema importância para que haja a prevenção de falhas e ativos de redes diminuindo perdas e prejuízos para a empresa.

5 REFERÊNCIAS BIBLIOGRÁFICAS

https://help.ubuntu.com/lts/serverguide/nagios.html

https://www.nagios.org/

http://www.cacti.net/