

## SIMULAÇÃO DE QoS EM AMBIENTE CORPORATIVO

*Democlydes Divino Pereira de Carvalho, Fausto Andrade dos Santos Junior*

**Resumo:** Este trabalho apresenta uma comparação entre técnicas de configuração de redes de computadores para permitir a alta disponibilidade em ambientes corporativos. Foram identificadas técnicas com notórios resultados de desempenho e resiliência, elementos fundamentais para este tipo de sistema. O resultado esperado desta pesquisa é identificar características que justificam o uso de uma ou outra técnica e quais impactos ocorrerão no ambiente a partir da escolha. A metodologia adotada foi de pesquisa bibliográfica para delimitar as técnicas e protocolos necessários e em seguida da elaboração de protótipos. A partir de uma topologia padrão, foram realizados testes de carga para comparar os resultados entre as abordagens visualizadas.

**Palavras-chaves:** Simulação; Ambiente corporativo; QoS; Rede.

### Introdução

O presente trabalho se aplica ao Exército Brasileiro (EB), Força Armada subordinada ao Ministério da Defesa (MD), que opera formalmente em função da defesa territorial brasileira, pela garantia da lei, da ordem e do poderes constitucionais. Seu Comandante Supremo é o Presidente da República.

O Exército Brasileiro mantém sistemas críticos para sua atividade m. Fatores como alta disponibilidade e recuperação de desastres são imprescindíveis dado o cenário de atuação das Forças Armadas. A infraestrutura desses sistemas caminha no mesmo ritmo, fundamenta-se no caos e instabilidade e precisa continuar funcionando apesar disso.

O cenário escolhido foi o Departamento-Geral do Pessoal do Exército Brasileiro (DGP), um Órgão de Direção Setorial de grande importância para a Força Terrestre. Suas atribuições estratégicas e operacionais orientam-se em sistemas críticos e em alguns casos de tempo real – a indisponibilidade dos serviços ali prestados compromete milhares de cidadãos brasileiros e, em casos extremos, a soberania nacional.

Para implementar os experimentos de avaliação, o cenário do DGP foi conjugado ao do Centro Integrado de Telemática do Exército (CITEx), Órgão responsável pela interconexão da Rede Corporativa do Exército (EBNet). Dessa forma foi possível elaborar um contexto realista e mais próximo do que se obterá ao implementar cada abordagem na prática.

### Quality of service

Tanenbaum *et al.* definem QoS (do inglês *Quality of Service*) como um conjunto de parâmetros exigido por cada fluxo. Estes parâmetros são: confiabilidade – podemos traduzir como taxa de perda de pacotes e pacotes com erro, retardo ou delay – tempo em que um pacote leva do emissor até o receptor, flutuação ou jitter – variação (desvio) nos tempos de chegada entre pacotes e largura de banda – recurso do canal consumido normalmente em bits por segundo. A mensuração destes parâmetros é influenciada pelos fatores humanos, neste

caso a experiência do usuário, e pelos atributos das aplicações.

Muita pesquisa e desenvolvimento foram feitas pelo IETF (do inglês *Internet Engineering Task Force*), por exemplo, IETF RFC 1633, IETF RFC 2430, IETF RFC 2475, entre outros. A Associação Cooperativa de Análise de Dados da Internet (do inglês *Cooperative Association for Internet Data Analysis - CAIDA*) criou ambiente para a medição de tráfego de rede, que é utilizado para a coleta de dados e análise de QoS.

A QoS pode ser definida de diferentes formas e pode incluir uma vasta variedade de requisitos de serviço, tais como desempenho, disponibilidade, confiabilidade, segurança, etc.

A medida de garantia de QoS pode ser fornecida de formas determinísticas e aleatórias. A forma determinista, por exemplo, pode ser expressa em uma rede que possui uma largura de banda constante. A forma aleatória, por exemplo, poderia ser expresso em uma rede em que algum percentual (por exemplo, 95%) de pacotes pode ser permitido um certo atraso médio, etc. A influência da gestão da rede deve ser mínima e o algoritmo de gestão deverá responder rapidamente à deterioração da QoS da rede. Isto pode ser conseguido através de controle e análise do tráfego de rede.

### Modelos de Monitoramento de QoS de Redes de Computadores

O monitoramento dos parâmetros de QoS podem ser divididos em monitoramento de ponta a ponta e monitoramento distribuído. No monitoramento de ponta a ponta, o tráfego de QoS entre dois pontos, isto é, entre o remetente e o destinatário, é observado. Uma abordagem distribuída para a monitorização de QoS, juntamente com o método de monitorização de ponta-a-ponta, monitoriza vários segmentos da rede.

A modelagem tradicional de QoS da rede inclui os seguintes componentes funcionais descritos na pilha de protocolo QoS, como pode ser visto na figura 1.

Conforme o trabalho de Shikhaliyev (2012), o modelo de monitorização de QoS é semelhante ao tradicional modelo de monitoramento de rede, mas existem algumas diferenças.

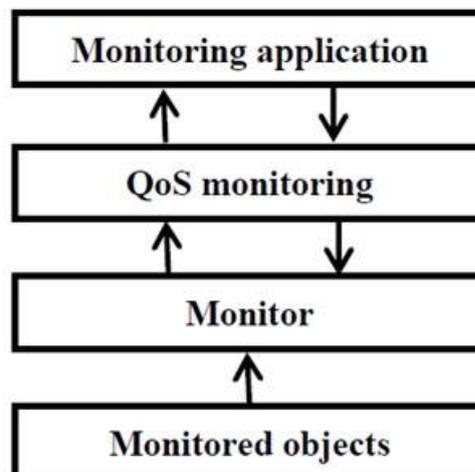


Figura 1. Pilha de Protocolo QoS.

Em primeiro lugar, o modelo de monitoramento de QoS usa um componente multi-monitor que coleta e armazena informações sobre os vários objetos utilizados para monitoramento.

Segundo, o modelo de monitoramento QoS utiliza locais de monitoramento na parte principal do fluxo, enquanto que o modelo tradicional de monitoramento de rede monitora objetos na parte principal do tráfego total.

A terceira diferença é que em um modelo para QoS de monitoramento, o acompanhamento é realizado no nível da aplicação.

A quarta diferença é que o modelo de monitorização QoS inclui um novo componente, o componente que permite a monitorização dos componentes de aplicação para as informações adequadas sobre os parâmetros de QoS de tráfego de rede.

O modelo de monitoramento de QoS pode realizar a análise para identificar problemas em QoS e configurar o sistema para monitoramento e reconfiguração de sistemas de rede.

### **Métricas e Métodos de Monitoramento de Redes de Computadores**

Apesar do alto nível atual de tecnologias de rede, ainda não existe um parâmetro objetivo comum para avaliar a QoS de redes de computadores. Hoje, a QoS é definido por três parâmetros não relacionados um com o outro de vários modos: o nível de Ethernet, no nível de IP e de redes ATM. ITU (International Telecommunications Union), criou SLA (Service Level Agreements - Acordos de Nível de Serviço) para uso entre ISPs (do inglês *Internet Service Providers*) e os seus assinantes para determinar os parâmetros de QoS de serviços de rede. No entanto, SLA não está baseado em padrões objetivos e pode variar dependendo do cliente, o ISP, e os serviços oferecidos. Por conseguinte, a falta de um padrão uniforme de QoS torna a determinação correta do QoS da rede de serviços em uma tarefa árdua.

Parâmetros genéricos de QoS que são necessários para os serviços de rede são: disponibilidade, entrega, atraso, largura de banda, MTBF (do inglês *Mean Time Between Failure*) eo MTRS (do inglês *Medium Time to Restore Service*).

Métricas de desempenho de redes de computadores são o principal meios de avaliação da eficácia do nível de rede gestão. Métricas de desempenho típicos de computador redes utilizadas na definição de QoS são largura de banda, latência e perda de pacotes.

IETF IPPM também desenvolveu vários padrões para medir o desempenho de redes de computadores :

- Métrica para medir Conectividade (RFC2678), que define uma série de procedimentos para medir conectividade entre um par de hosts da Internet;
- *One-way Delay Metric* (RFC2679), que define um métrica para medir o atraso de um caminho de pacotes através Caminhos da Internet;
- *One-way Packet Loss Metric* (RFC2680), que define os meios de encontrar uma forma de perda de pacotes através de Caminhos da Internet;
- *Round-trip Delay Metric* (RFC2681), que define uma métrica para encontrar atraso

de ida e volta de pacotes através de caminhos da Internet ;

- *One-way Loss Pattern Sample Metric* (RFC3357), que define duas métricas derivadas “loss distance“ and “loss period“, e as estatísticas associadas que, juntas, capturam padrões de perda experimentadas por fluxos de pacotes na Internet; e
- *IP Packet Delay Variation Metric* (RFC3393), que define uma métrica para a variação no atraso dos pacotes que fluem a partir de um hospedeiro para outro por meio de um caminho de IP.

Também segundo Shikhaliyev (2012), mecanismos de QoS podem ser realizados em modos off-line ou on-line, isto é, com base no pré-processamento de dados recolhidos ou análise de dados em tempo real. Sistemas de monitoramento de QoS podem ter arquiteturas centralizadas ou distribuídas. A abordagem centralizada fornece um método fácil para a obtenção de uma visão abrangente do desempenho da rede, mas pode ter problemas com escalabilidade. Ou seja, com um aumento significativo no número de nós, o monitoramento de dados na infraestrutura pode se tornar difícil. Em uma abordagem distribuída, os dados de monitoramento são coletados e processados em cada ponto de medição.

### **Acompanhamento e Gestão de QoS em Arquiteturas de Redes de Computadores**

Em redes de computadores atuais, Shikhaliyev (2012) define que QoS de serviços de rede é proporcionado através da diferenciação de tráfego e nível de serviço. Por exemplo, a comparação de aplicações e-mail com VoIP, sabendo o volume de vazão e atraso de pacotes é crucial. No entanto, para se assegurar o necessária nível de QoS, não são suficientes para fornecer os recursos necessários para QoS. Portanto, mecanismos apropriados para a monitorização e gestão de QoS são necessários.

Nas últimas duas décadas, várias arquiteturas foram propostas para auxiliar no monitoramento e gerenciamento de QoS em redes de computadores.

1) *OSI QoS architecture*: A arquitetura OSI foi uma das primeiras arquiteturas de monitorização e gestão de QoS e concentra-se principalmente sobre a gestão das comunicações OSI Define os termos e conceitos de redes de computadores como um modelo para a QoS , que então é utilizado para definir sistemas abertos , ou objetos de QoS . Consiste em dois níveis de governança (níveis especiais e sistêmicos), que fornece meios de acompanhamento e várias exigências apoios de QoS.

2) *XRM architecture*:

- A arquitetura XRM é usada para acompanhamento e gestão de QoS de redes ATM e sistemas multimídia e é constituída pelos seguintes componentes:
  - gestão e sistemas de rede;
  - Gestão de Comunicação;
  - Processos de planeamento;
  - Gestão de fluxo; e

- Abstração e gerenciamento de dados.

3) *QoS-A architecture*:: A arquitetura QoS –A é uma arquitetura de serviços multi-camadas e de mecanismos de gestão e controle de QoS para mídia contínua fluir em redes multi-serviços. Inclui os seguintes conceitos básicos:

- Fluxos , caracterizando o processamento, transmissão e consumo de multimídia contínua com a QoS apropriada;
- Os requisitos de manutenção que são acordos vinculativos entre usuários e prestadores de serviços que determinam os níveis de QoS; e
- Fluxo de controle, que fornece controle e suporte para o nível apropriado de QoS.

## Ambiente de avaliação

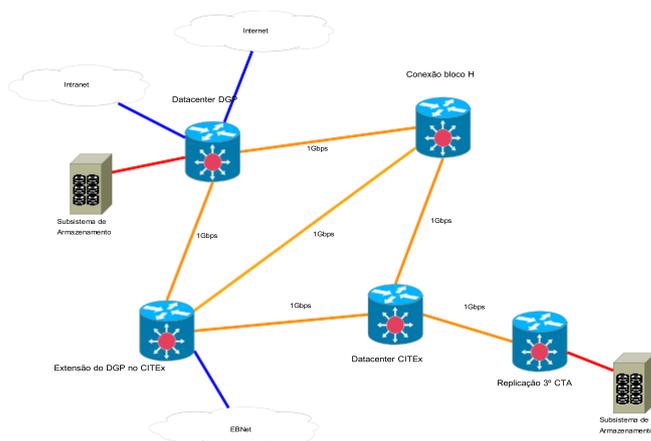


Figura 2. Topologia de aplicação de QoS.

O ambiente avaliado apresenta 3 sub-redes distintas, com o total de 1100 aproximadamente usuários na Intranet, outros 80 mil usuários na rede corporativa do Exército (EBNet) e ainda mais de 250 mil usuários na grande rede (Internet). Apesar de ilustrados, os usuários de sistemas externos estão considerados como tráfego de fundo para o modelo pois o QoS será aplicado a serviços entre sistemas de armazenamento.

### Descrição dos Equipamentos:

Foram pesquisados aplicativos de simulação de rede, com intuito de identificar o que se adequaria ao objetivo proposto. Os trabalhos de Akbaş and Gümüşkaya (2011), Zhang *et al.* (2012) e Salah *et al.* (2008) sugerem opções adequadas para esta pesquisa. Abaixo

estão descritas peculiaridades dos softwares pesquisados.

- NS3: Network Simulator 3 é um simulador de rede de eventos discretos para sistemas de Internet, destina-se principalmente para pesquisa e uso educacional;
- GNS3: Inicialmente baseou-se no NS3, atualmente fomenta uma interface gráfica e permite a emulação de roteadores CISCO utilizando-se de IOS reais além de integrar-se ao Virtual BOX e com a rede local;
- OPNET IT Guru Academic Edition: É a versão gratuita do simulador de rede OPNETIT, mostra-se maduro e possui diversas características de rede já embarcadas;
- TC: Traffic Control é software em LINUX usado para configurar controle de tráfego no Kernel do Linux, permite tornar-se um roteador com controle de tráfego.
- O GNS3 foi escolhido em função da familiaridade e da proximidade da com a aplicação da solução, faz emulação de roteadores utilizando-se IOS (Internetwork Operating System). Contudo após montar o ambiente e iniciar as simulações houveram descarte de pacotes superiores a 70% e baixo desempenho.

Para o ambiente foi utilizado o sistema GNS3 (do inglês *Graphical Network Simulator*) que consegue integrar a simulação de máquinas virtuais e ativos de rede. O ambiente também contou com o sistema de virtualização VirtualBox, que implementa virtualização total e com isso permite executar tarefas complexas e fidedignas a um ambiente de produção implementado em computadores reais.

Os roteadores foram implementados usando o sistema operacional IOS da Cisco modelo 3640, que oferece suporte a conectividade Ethernet, que é o objetivo deste trabalho. Cada roteador utiliza memória principal (RAM) de 128 Megabytes, e foram montados com 4 interfaces Fast Ethernet 100Mbps. Isso permitiu a simulação proporcional da rede objeto de estudo, já que a rede real está toda implementada com conexões Gigabit Ethernet, mantendo proporcionalidade em todos os ativos de rede.

Os computadores virtuais, representando aqui hospedeiros de sistemas corporativos, apresentam tráfego de dados equivalente ao ambiente de produção. Todos foram implementados através do ambiente VirtualBox e integrados à rede de simulação do GNS3, utilizando as configurações dos dois ambientes como pode ser visto nas figuras 3 e 4.

Dois computadores virtuais, denominados na simulação de BG1 e BG2, foram responsáveis por manter um tráfego de fundo simulando as operações quotidianas do ambiente de produção. Isso inclui acessos externos, conexões de clientes internos, operações de sistemas e bancos de dados locais.

Outros dois computadores, denominados nesta simulação de SERV1 e SERV2, foram designados como ambientes de hospedagem de sistemas dinâmicos, onde a gravação de arquivos é frequente. Este perfil de aplicação é típico do cenário estudado, onde diversos sub-sistemas de informação trabalham com armazenamento de dados em arquivos, não só bancos de dados. Como essas atividades são críticas e de alto volume de requisições de clientes, foram designados dois servidores para hospedar os sub-sistemas. Por esse motivo os arquivos

de dados devem transitar entre os sistemas e permanecerem sincronizados.

A simulação de roteamento contou com a infraestrutura como disposta na figura 13. Para configurar os roteadores foi utilizado o mapa de parâmetros disponíveis na figura 10.

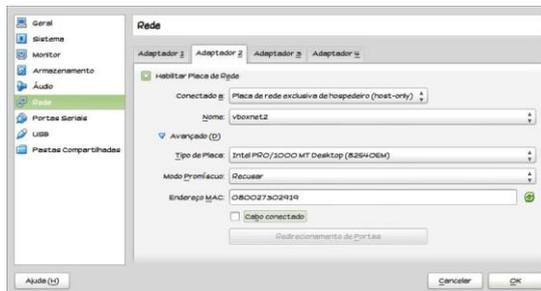


Figura 3. Configuração do VirtualBox para adaptar as máquinas virtuais ao NS3

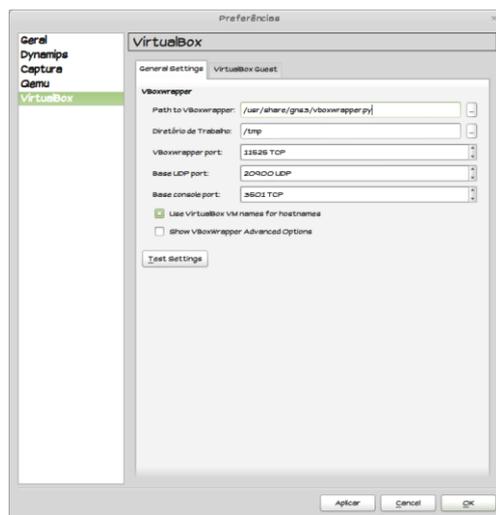


Figura 4. Configuração do GNS3 para integrar-se ao VirtualBox

Para o tráfego de fundo foi utilizado o protocolo HTTP simulando requisições de clientes das diversas aplicações ali hospedadas, pois este é o tráfego predominante nessa rede. Já para o ambiente de sincronização de arquivos foi utilizado o protocolo SSH, que utiliza criptografia presente no ambiente de produção atual.

Para a simulação foram implementados os seguintes cenários:

**Ambiente de sincronia atual sem QoS:** neste ambiente foi possível identificar os principais problemas que a rede corporativa está sujeita.

Roteador	Rede	IP	Porta
R1	1.1.1.0/24	1.1.1.10	g1
R1	3.3.3.0/24	3.3.3.10	g2
R1	5.5.5.0/24	5.5.5.10	g3
R1	6.6.6.0/24	6.6.6.10	g4
R2	5.5.5.0/24	5.5.5.20	g1
R2	7.7.7.0/24	7.7.7.20	g2
R2	10.10.10.0/24	10.10.10.20	g3
R3	6.6.6.0/24	6.6.6.30	g1
R3	8.8.8.0/24	8.8.8.30	g2
R3	10.10.10.0/24	10.10.10.30	g3
R4	7.7.7.0/24	7.7.7.40	g1
R4	8.8.8.0/24	8.8.8.40	g2
R4	9.9.9.0/24	9.9.9.40	g3
R5	2.2.2.0/24	2.2.2.50	g1
R5	4.4.4.0/24	4.4.4.50	g2
R5	9.9.9.0/24	9.9.9.50	g3

Figura 5. Mapa da configuração dos roteadores no sistema GNS3.

```

R1
telnet localhost 2101

enable
configure terminal
interface gigabitEthernet 1/0
ip address 1.0.0.10 255.255.255.0
no shutdown
exit

interface gigabitEthernet 2/0
ip address 3.0.0.10 255.255.255.0
no shutdown
exit

interface gigabitEthernet 3/0
ip address 5.0.0.10 255.255.255.0
no shutdown
exit

interface gigabitEthernet 4/0
ip address 6.0.0.10 255.255.255.0
no shutdown
exit

router ospf 1
network 1.0.0.0 0.0.0.255 area 0
network 3.0.0.0 0.0.0.255 area 0
network 5.0.0.0 0.0.0.255 area 0
network 6.0.0.0 0.0.0.255 area 0
exit

exit
copy running-config startup-config

```

Figura 6. Configuração do roteador R1.

- **Ambiente de sincronia com QoS:** utilizando a topologia descrita na figura 2 foram implementadas as políticas de controle de filas WFQ (do inglês *Weighted Fair Queuing*) e política de descarte de pacotes *Drop Tail* - descarte da cauda ou pacotes mais recentes. Para a política de controle de tráfego foi aplicado a implementação *Leak Bucket*.

```
R2
telnet localhost 2102

enable
configure terminal
interface gigabitEthernet 1/0
ip address 5.0.0.20 255.255.255.0
no shutdown
exit

interface gigabitEthernet 2/0
ip address 7.0.0.20 255.255.255.0
no shutdown
exit

interface gigabitEthernet 3/0
ip address 10.0.0.20 255.255.255.0
no shutdown
exit

router ospf 1
network 5.0.0.0 0.0.0.255 area 0
network 7.0.0.0 0.0.0.255 area 0
network 10.0.0.0 0.0.0.255 area 0
exit

exit
copy running-config startup-config
```

Figura 7. Configuração do roteador R2.

```
R4
telnet localhost 2104

enable
configure terminal
interface gigabitEthernet 1/0
ip address 7.0.0.40 255.255.255.0
no shutdown
exit

interface gigabitEthernet 2/0
ip address 8.0.0.40 255.255.255.0
no shutdown
exit

interface gigabitEthernet 3/0
ip address 9.0.0.40 255.255.255.0
no shutdown
exit

router ospf 1
network 7.0.0.0 0.0.0.255 area 0
network 8.0.0.0 0.0.0.255 area 0
network 9.0.0.0 0.0.0.255 area 0
exit

exit
copy running-config startup-config
```

Figura 8. Configuração do roteador R3.

```
R3
telnet localhost 2103

enable
configure terminal
interface gigabitEthernet 1/0
ip address 6.0.0.30 255.255.255.0
no shutdown
exit

interface gigabitEthernet 2/0
ip address 8.0.0.30 255.255.255.0
no shutdown
exit

interface gigabitEthernet 3/0
ip address 10.0.0.30 255.255.255.0
no shutdown
exit

router ospf 1
network 6.0.0.0 0.0.0.255 area 0
network 8.0.0.0 0.0.0.255 area 0
network 10.0.0.0 0.0.0.255 area 0
exit

exit
copy running-config startup-config
```

Figura 9. Configuração do roteador R4.

- **Ambiente de videoconferência sem QoS:** utilizando o mesmo cenário, os computadores virtuais SERV1 e SERV2 simularam a presença de um ambiente de videoconferência através da entrega de rajadas de pacotes UDP, mas no cenário atual onde não há QoS.
- **Ambiente de videoconferência com QoS:** no mesmo cenário acima, foi implementado o serviço de QoS as políticas de controle de filas WFQ (do inglês *Weighted Fair Queuing*) e política de descarte de pacotes *Drop Tail* - descarte da cauda ou pacotes mais recentes. Para a política de controle de tráfego foi aplicado a implementação *Leak Bucket*.

```
R5
telnet localhost 2105

enable
configure terminal
interface gigabitEthernet 1/0
ip address 2.0.0.50 255.255.255.0
no shutdown
exit

interface gigabitEthernet 2/0
ip address 4.0.0.50 255.255.255.0
no shutdown
exit

interface gigabitEthernet 3/0
ip address 9.0.0.50 255.255.255.0
no shutdown
exit

router ospf 1
network 4.0.0.0 0.0.0.255 area 0
network 5.0.0.0 0.0.0.255 area 0
network 9.0.0.0 0.0.0.255 area 0
exit

exit
copy running-config startup-config
```

Figura 10. Configuração do roteador R5.

Para implementar a simulação de sincronia de servidores, foram utilizados scripts que executam comandos consecutivos de transferência de dados e geram tráfego proporcional ao ambiente de produção, observado o dimensionamento da simulação e o ambiente real. A geração de tráfego também é bidirecional, portanto os comandos devem ser realizados concomitantemente, como é o ambiente de produção. As figuras 11 e 12 exibem as rotinas de automação deste cenário.

Todo tráfego de dados foi direcionado para gravar somente em memória principal, evitando assim que o acesso a gravação em disco pudesse prejudicar os resultados de comutação de pacotes.

```
#!/bin/bash

while [ 1 ]
do
  wget http://2.0.0.2/debian.iso -O /dev/null
done
```

Figura 11. Script utilizado para sincronizar os ambientes em SERV1 e SERV2.

```
#!/bin/bash

while [ 1 ]
do
  wget http://2.0.0.2/debian.iso -O /dev/null
done
```

Figura 12. Script utilizado para simular tráfego HTTP de fundo.

## Resultados e análise

Através da simulação do ambiente sem aplicação de QoS, foi possível observar que a flutuação de desempenho culminou sempre em retransmissão de pacotes. A transmissão dos dados objetivos desta pesquisa, conforme visualizado na figura 14, tem ocasiões de retransmissão sempre que a quantidade de pacotes aumenta acima da média. A simulação durou 5 minutos (300 segundos) e durante este período foram transferidos 244183 pacotes de dados. Destes, ] 10010 pacotes foram retransmissões de pacotes perdidos, ou seja, a rede apresentou ineficiência de 4,1%. Em média, foram transmitidos 597 pacotes por segundo, enquanto que a perda ficou em 24 pacotes por segundo. Também a maior taxa de transmissão foi de 1384 pacotes em um único segundo, e a maior perda acumulada em um segundo foi de 295 pacotes de dados.

As simulações trouxeram informações importantes também sobre o sistema de simulação. O aplicativo GNS3 possui peculiaridades interessantes para a pesquisa em redes, mas seu funcionamento apresenta diversas falhas sérias, e com isso tornou as simulações inviáveis em alguns cenários. A comunidade de desenvolvimento do aplicativo apresenta muito material de apoio, contudo as falhas encontradas durante a simulação estão fracamente documentadas.

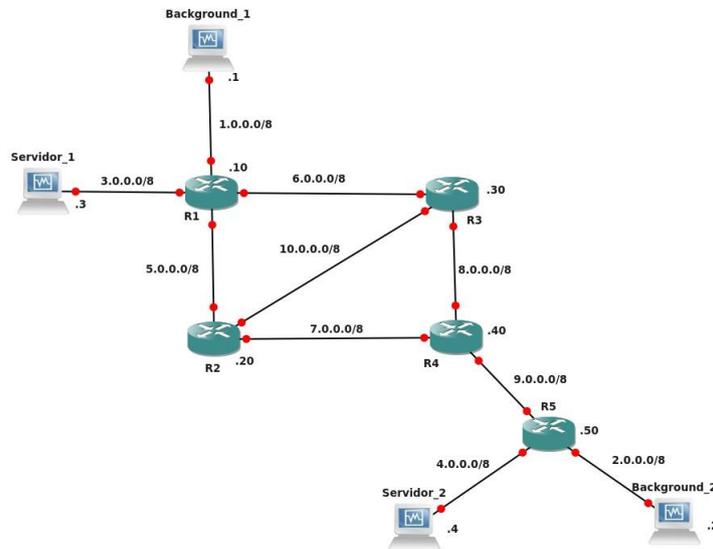


Figura 13. Topologia do ambiente de simulação no aplicativo GNS3.

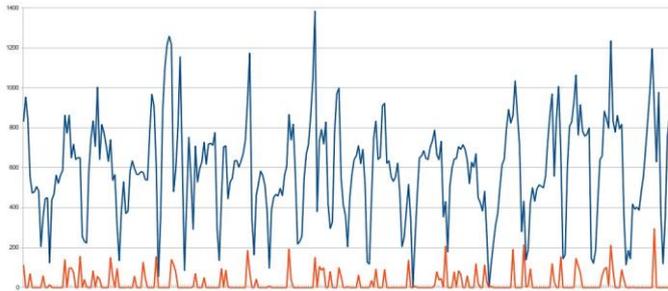


Figura 14. Transmissão de pacotes durante simulação do ambiente sem QoS.

O ambiente demonstrou instabilidade durante a configuração dos roteadores de forma incompatível com os equipamentos reais. A perda de configurações de forma espontânea tornou os experimentos inconclusivos, pois a perda de pacotes poderia ser não só por congestão na rede mas também por falha do simulador. A própria captura de pacotes apresenta falhas pois ao transmitir dados, os cabeçalhos TCP/IP gerados apresentam falhas aleatórias que impedem as ferramentas de captura de operar. Somente foi possível capturar pacotes no servidor virtual, o que mascara seriamente a atuação de configurações de QoS na rede. A marcação de pacotes na rede tornou-se impossível de monitorar justamente porque o simulador falha ao entregar pacotes capturados durante a escuta dos enlaces centrais de roteamento. Durante consultas aos fóruns da comunidade de manutenção do aplicativo GNS3 ficou claro que o software de simulação de roteadores possui falhas em seu funcionamento e que comprometeu diretamente os experimentos aqui apresentados.

## Conclusão

Apesar das falhas do ambiente de simulação, o trabalho apresentou resultados úteis à comunidade. O simulador apresenta falhas e os experimentos realizados nesse trabalho demonstram a possibilidade de contornar tais problemas. Ficou claro que é possível testar redes sem aplicação de QoS e que, com aplicação de QoS, somente foi possível captar a percepção do usuário, pois há entaves na captura de pacotes dentro dos enlaces de roteamento.

Vale observar que os aplicativos utilizados para simulação - GNS3 e VirtualBox - possuem opções muito interessantes para essa finalidade e que ainda há espaço para sua utilização em larga escala. Vale também como trabalhos futuros continuar a pesquisa e descobrir alternativas para a captura de pacotes não obtida neste trabalho, seja por configuração alternativa do ambiente ou por inserção de novos elementos como elementos intermediários no roteamento.

## Referências

- AKBAŞ, D.; GÜMÜŞKAYA, H. Real and {OPNET} modeling and analysis of an enterprise network and its security structures. *Procedia Computer Science*, v.3, p.1038 – 1042. World Conference on Information Technology, 2011.
- SALAH, K.; CALYAM, P.; BUHARI, M. I. Assessing readiness of ip networks to support desktop videoconferencing using opnet. *J. Netw. Comput. Appl.*, v.31, n.4, p.921–943, 2008.
- SHIKHALIYEV, R. Methods for monitoring and managing computer networks qos. In *Problems of Cybernetics and Informatics (PCI), 2012 IV International Conference*, p.1–5, 2012.
- TANENBAUM, A., WETHERALL, D.. *Redes de Computadores*. Prentice Hall Brasil.
- ZHANG, Y.; LIANG, R.; MA, H. Teaching innovation in computer network course for undergraduate students with packet tracer. *{IERI} Procedia*, 2(0):504 – 510. International Conference on Future Computer Supported Education, August 22- 23, 2012, Fraser Place Central – Seoul, 2012.