

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA
ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES
***CAMPUS* PATOS DE MINAS**

LEONARDO CAIXETA DIAS

Estudo Comparativo dos Protocolos de Roteamento RIP e OSPF

Patos de Minas

2017

LEONARDO CAIXETA DIAS

Estudo Comparativo dos Protocolos de Roteamento RIP e OSPF

Trabalho de conclusão de curso 2 apresentado à Universidade Federal de Uberlândia como requisito para graduação em Engenharia Eletrônica e de Telecomunicações.

Orientadora: Profa. Dra. Karine Barbosa Carbonaro.

Patos de Minas

2017

Sumário

CAPÍTULO 1	9
INTRODUÇÃO	9
CAPÍTULO 2	11
CARACTERIZAÇÃO DO PROCESSO DE ROTEAMENTO.....	11
2.1 Parte interna de um roteador	13
2.2 Roteamento Estático.....	15
2.3 Roteamento Dinâmico.....	15
2.4 RIP	15
2.5 OSPF	17
CAPÍTULO 3	20
SIMULAÇÃO DOS PROTOCOLOS RIP E OSPF	20
3.1 GNS3.....	20
3.2 OSTINATO	21
3.3 Wireshark	29
3.4 Cenários de simulação no GNS3.....	29
3.4.1 Configuração dos protocolos de roteamento	30
3.4.2 Resultados obtidos	32
3.5 Cenários de simulação no opnet.....	36
3.5.1 Resultados obtidos	44
CAPÍTULO 4.....	51
CONCLUSÕES GERAIS	51
REFERÊNCIAS BIBLIOGRÁFICAS.....	52

RESUMO

Neste trabalho objetiva-se um estudo comparativo do comportamento de redes de computadores submetidas aos protocolos de roteamento RIP e OSPF. As implementações destes protocolos foram feitas em softwares, o GNS3 e o OPNET. No GNS3 foram simulados dois cenários para cada protocolo de roteamento. No primeiro cenário transmitiram-se os dados sem qualquer perturbação na rede e no segundo cenário foi inserida uma limitação na largura de banda de um roteador que estava na rota de menor tamanho. No OPNET também foram simulados dois cenários em redes. No primeiro cenário tem-se uma rede idêntica à emulada no GNS3 e no segundo tem-se uma rede quatro vezes maior. Nestas simulações foram utilizados três tipos de aplicações vídeo, FTP e VoIP e inserido falhas entre os enlaces da rede de forma aleatória. Os resultados de todos estes testes podem ser encontrados neste documento.

Palavras-chaves: RIP, OSPF, GNS3, OPNET.

Abstract

This paper aims to study and analyze behavior computer network using RIP and OSPF routing protocols. This protocols were implemented on two different softwares, the GNS3 and OPNET. On GNS3, at the first scenario, the data transmission on network was free of fails or restrictions, and the second scenario we limited the bandwidth of a router who was at the shortest route. Using OPNET, we simulated two scenarios too, where the first scenario we use a identical network used on GNS3 and the second scenario we used a four times greater network. In this simulations we used three kinds of application Video, FTP and VoIP, inserted aleatory fail and recovery to test the protocols performance to work around the network disturbances. This simulations results will be showed in this paper.

Key words: RIP, OSPF, GNS3, OPNET.

LISTA DE FIGURAS

FIGURA 1 - USUÁRIOS DE INTERNET POR PORCENTAGEM DA POPULAÇÃO.	9
FIGURA 2 – (A)MODELO OSI E (B) MODELO TCP/IP.	11
FIGURA 3 - PARTE INTERNA DE UM ROTEADOR.	13
FIGURA 4 - TIPOS DE COMUTAÇÃO.	14
FIGURA 5 - REDE DE COMPUTADORES UTILIZANDO O PROTOCOLO DE ROTEAMENTO RIP.	16
FIGURA 6 - SIMULAÇÃO DE UM SISTEMA AUTÔNOMO.	17
FIGURA 7 - NOVA TOPOLOGIA DO SISTEMA AUTÔNOMO.	17
FIGURA 8 - ESQUEMA DE REDE COM OSPF.	18
FIGURA 9 - SOFTWARE DE SIMULAÇÃO GNS3.	20
FIGURA 10 - MENU DO GNS3 COM O ÍCONE OSTINATO.	22
FIGURA 11 - INTERFACE DE ESCOLHA DO OSTINATO.	22
FIGURA 12 - INTERFACE DE CONFIGURAÇÃO DO OSTINATO.	23
FIGURA 13 - (A) CRIAÇÃO DE UMA NOVA STREAM - (B) AÇÕES DAS STREAMS.	24
FIGURA 14 - SELEÇÃO DOS PROTOCOLOS DE CADA CAMADA.	25
FIGURA 15 - (A) ENDEREÇO MAC DE ORIGEM E DESTINO (B) ENDEREÇO IP DE ORIGEM E DESTINO.	26
FIGURA 16 - SELEÇÃO DE PORTAS DE PROTOCOLO DE CAMADA QUATRO.	26
FIGURA 17 - SELEÇÃO DO FORMATO DOS DADOS DA CARGA.	27
FIGURA 18 - CONTROLE DAS STREAMS.	27
FIGURA 19 - VISUALIZAÇÃO DOS DADOS QUE SERÃO TRANSMITIDOS.	28
FIGURA 20 - ESTATÍSTICAS DA TRANSMISSÃO DE DADOS.	28
FIGURA 21 - TOPOLOGIA DE REDE SIMULADA.	29
FIGURA 22 - CONFIGURAÇÃO DAS INTERFACES DOS ROTEADORES.	30
FIGURA 23- CONFIGURAÇÃO DO PROTOCOLO RIP.	31
FIGURA 24 - CONFIGURAÇÃO DO PROTOCOLO OSPF.	31
FIGURA 25 - TOPOLOGIA DE REDE UTILIZADA NA SIMULAÇÃO.	32
FIGURA 26 - TRÁFEGO DE DADOS ENTRE R5 E R6 UTILIZANDO O PROTOCOLO DE ROTEAMENTO RIP.	33
FIGURA 27 - TRÁFEGO DE DADOS ENTRE R5 E R6 UTILIZANDO O PROTOCOLO DE ROTEAMENTO OSPF.	33
FIGURA 28 - CONFIGURAÇÃO DE LIMITAÇÃO DE BANDA DO ROTEADOR R6.	34
FIGURA 29 - TRÁFEGO DE DADOS ENTRE OS ROTEADORES UTILIZANDO O RIP COM A VELOCIDADE LIMITADA EM 100KBPS.	34
FIGURA 30 - UTILIZAÇÃO DO OSPF (A) TRÁFEGO DE DADOS ENTRE OS ROTEADORES R5 E R6 (B) TRÁFEGO DE DADOS ENTRE OS ROTEADORES R4 E R5.	35
FIGURA 31 - OBJETOS UTILIZADOS PARA CRIAÇÃO DE UMA REDE NO OPNET.	37

FIGURA 32 - TOPOLOGIA DE REDE SIMULADA.	38
FIGURA 33 - SELEÇÃO DO NÚMERO DE APLICAÇÕES ADICIONADAS À REDE.	38
FIGURA 34 - SELECIONANDO A COMPOSIÇÃO DE CADA APLICAÇÃO.	39
FIGURA 35 – NOMEANDO CADA UM DOS PROFILES PARA RECEBER A APLICAÇÃO.	39
FIGURA 36 - ATRIBUINDO APLICAÇÃO E TEMPO DE SIMULAÇÃO PARA CADA PROFILE.	40
FIGURA 37- INSERÇÃO DE FALHA E RECUPERAÇÃO NOS LINKS DA REDE.	41
FIGURA 38 - CONFIGURAÇÕES DOS COMPUTADORES DA REDE.	42
FIGURA 39 - CONFIGURAÇÃO DO FTP SERVER.	43
FIGURA 40 - ESCOLHA DO PROTOCOLO DE ROTEAMENTO.	43
FIGURA 41 - ATRASO MÉDIO DOS PACOTES NA REDE.	44
FIGURA 42 - TEMPO MÉDIO DE CONVERGÊNCIA DE PACOTES E PERDA MÉDIA DE PACOTES POR SEGUNDO.	45
FIGURA 43 - TOPOLOGIA DE REDE COM 21 ROTEADORES	46
FIGURA 44 - TEMPO MÉDIO DE ATRASO DOS PACOTES FTP.	47
FIGURA 45 - TEMPO MÉDIO DE ATRASO DOS PACOTES DE VÍDEO.	48
FIGURA 46 - TEMPO MÉDIO DE ATRASO DOS PACOTES DE VOZ.	48
FIGURA 47 - TEMPO MÉDIO DE CONVERGÊNCIA DE PACOTES.	49
FIGURA 48 - PERDA MÉDIA DE PACOTES POR SEGUNDO.	50

LISTA DE QUADROS

QUADRO 1 - TEMPO DE FALHA E RECUPERAÇÃO DOS LINKS DURANTE A SIMULAÇÃO.	40
QUADRO 2 - TEMPOS DE FALHA E RECUPERAÇÃO DOS LINKS.	46
QUADRO 3 - COMPARAÇÃO DOS RESULTADOS.	50

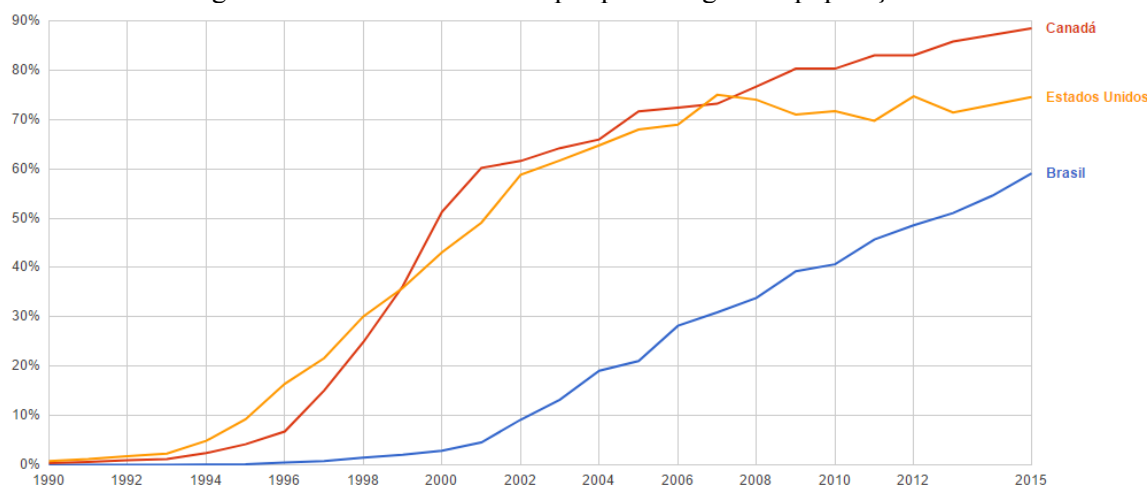
CAPÍTULO 1

INTRODUÇÃO

A necessidade humana por comunicação é algo percebido ao longo de toda história de acordo com as características e tecnologias disponíveis em cada época. Uma das primeiras formas de comunicação utilizadas foram as cartas, as quais eram utilizadas para enviar informações à alguém distante de forma segura e precisa, no entanto o prazo para a entrega das cartas era grande. Como o ser humano sempre desejava que as informações fossem transmitidas de forma mais rápida, criaram-se meios como rádios, TV e internet para que as informações pudessem ser enviadas e recebidas quase que instantaneamente.

Quando se analisa a internet, percebe-se que esta é a maior evolução para suprir a necessidade humana de obter informações, pois é a que possui maior velocidade e maior distância de transmissão de informação. Justamente por isso, a internet criada no final da década de 60 [1], teve crescimento de número de usuários de forma quase que exponencial ao longo dos anos como pode ser observado no gráfico ilustrado na Figura 1.

Figura 1 - Usuários de internet por porcentagem da população.



Fonte: baseado em [2].

Com o aumento excessivo do número de usuários, são necessárias evoluções em todas as partes de infraestrutura de rede, tanto para suportar mais usuários quanto para dar mais velocidade de acesso para cada um. Uma das formas de fazer isso, é aprimorando e desenvolvendo novos protocolos de roteamento que são basicamente a forma com que os roteadores comunicam entre si.

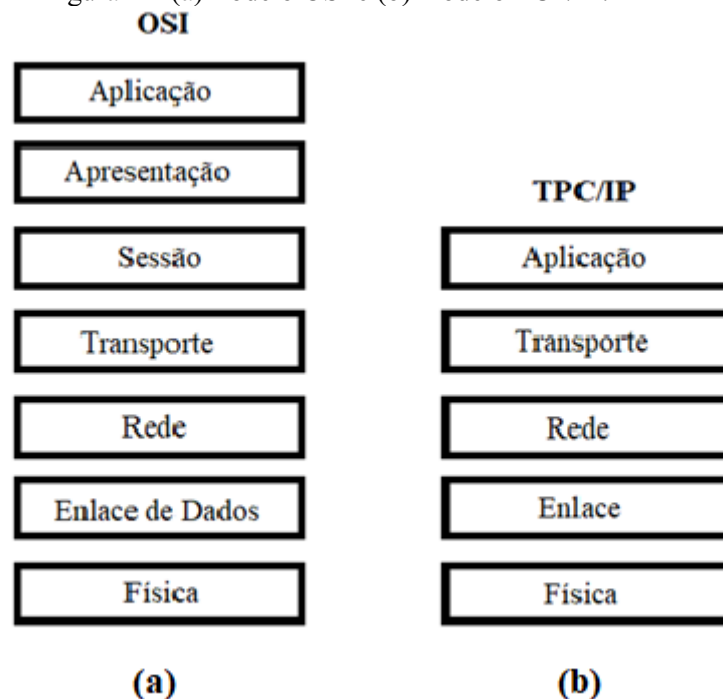
Com o desenvolvimento deste trabalho, visa-se um estudo comparativo entre os protocolos de roteamento RIP e OSPF. Será considerado suas características, suas versões, funcionamento dos algoritmos de roteamento de distância vetorial e roteamento hierárquico. Analisar-se-á diversos cenários de aplicação de cada protocolo para se obter o melhor desempenho da rede. Além disso, será feito um estudo das deficiências de cada um desses protocolos para se verificar quais são as possíveis melhorias que estão sendo desenvolvidas para versões futuras.

CAPÍTULO 2

CARACTERIZAÇÃO DO PROCESSO DE ROTEAMENTO

A internet não é considerada uma rede de computador, mas sim um conjunto de redes diferentes que utilizam alguns protocolos em comum que faz com que se obtenha a comunicação de ponta a ponta [1]. Por este motivo, é importante analisar profundamente como são estruturadas as redes de computadores e como elas funcionam. Existem dois modelos básicos de referência quando se trata de redes de computadores. São eles o modelo OSI (*Open Systems Interconnection*) e o modelo TCP/IP (*Transmission Control Protocol/Internet Protocol*). Ambos modelos trabalham com a ideia de subdividir a rede de computadores em camadas para que seja melhor compreendida. A principal diferença entre os modelos são a quantidade de camadas. O modelo OSI divide em 7 camadas enquanto o modelo TCP/IP divide em apenas 5 [3]. Essas camadas são ilustradas na Figura 2.

Figura 2 – (a) Modelo OSI e (b) modelo TCP/IP.



Fonte: O autor.

Existe uma grande correlação entre os modelos, onde se diz que o modelo TCP/IP é uma versão um pouco mais simplificada e otimizada em relação ao modelo OSI [1]. Por este

motivo, considera-se que existe uma correspondência aproximada entre as camadas do modelo OSI e TCP/IP conforme foi ilustrado na Figura 2.

Cada uma das camadas possui suas próprias funções e protocolos afim de que os dados sejam enviados de um usuário para outro de forma eficiente e segura. Uma das camadas mais importantes e estudadas é a camada de rede, a qual é responsável pelo endereço de origem e destino dos pacotes, o qual é conhecido como IP (*Internet Protocol*), e responsável também pelo roteamento dos pacotes da origem até o destino.

Roteamento é o nome dado aos serviços executados pelo roteador e consiste basicamente em determinar as melhores rotas de envio dos pacotes e o transporte desses até o destino final [1].

Analisando a comutação dos pacotes dentro de um roteador, da entrada à saída adequada sob uma visão de alto nível, divide-se um roteador genérico em 4 partes principais:

1. Porta de entrada: por onde o pacote enviado chega ao roteador;
2. Elemento de comutação: conecta as portas de entrada às portas de saída do roteador, utilizado para que o pacote seja enviado para o destino final, ou para um próximo roteador;
3. Porta de saída: recebe os pacotes do comutador e transmiti eles para o enlace de saída.
4. Processador de roteamento: onde são executados os protocolos de roteamento e se encontram as tabelas de roteamento, afim de fazer com que o pacote da entrada vá para a saída correta [3].

O método que o roteador utiliza para definir qual será a melhor rota para o envio do pacote, depende de qual algoritmo de roteamento está sendo executado. De maneira geral, esses algoritmos buscam simplicidade, robustez, estabilidade e eficiência e podem ser de dois tipos: adaptativos e não adaptativos:

- **Algoritmo não adaptativo:** roteamento estático, o qual suas rotas são estabelecidas com o roteador desligado e são carregadas no processo de inicialização da rede e permanecem sempre sem mudanças;
- **Algoritmo adaptativo:** roteamento dinâmico, ou seja, a tabela de roteamento vai se alterando com o passar do tempo, fazendo com que o roteador tome suas decisões de acordo com o tráfego e com as mudanças na topologia da rede[1].

Existem vários protocolos de roteamento tais como o RIP (*Routing Information Protocol*), IGRP (*Interior Gateway Routing Protocol*), OSPF (*Open Shortest Path First*) e IS-IS (*Intermediate System-to-Intermediate System*). Cada um desses protocolos possui suas

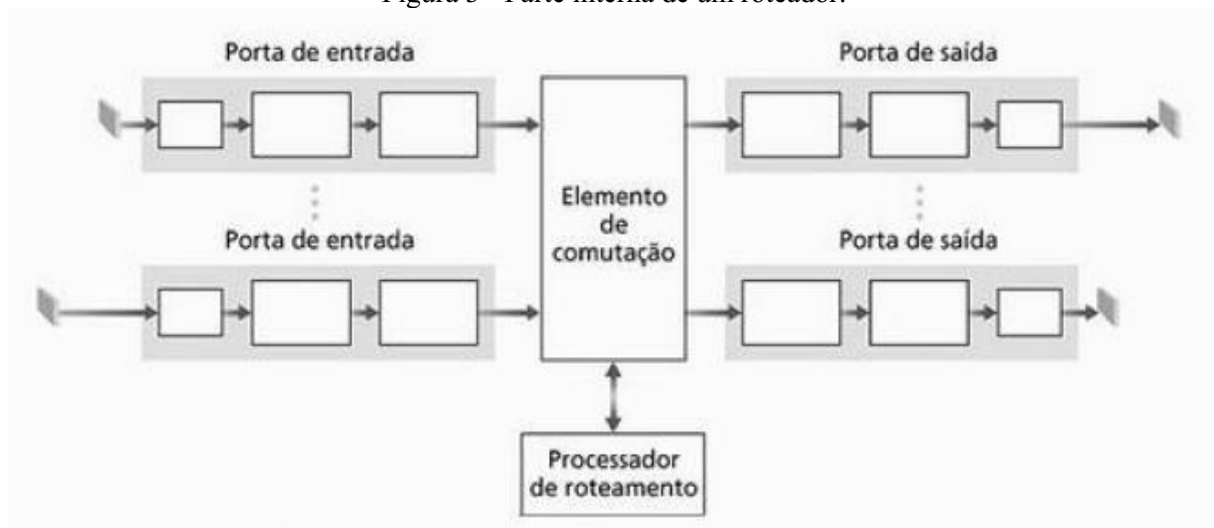
características específicas e que devem ser estudados separadamente para que se escolha qual será melhor para cada caso específico de rede.

Como já foi apresentado, o roteador possui basicamente duas funções que são: conduzir o pacote da porta de entrada até uma porta de saída adequada (repassse) e determinar o caminho pelo qual os pacotes serão trafegados entre os nós da rede até chegar ao destinatário final (roteamento) [3]. O repasse é uma ação interna do roteador, onde cada roteador possui uma tabela de repasse. Nessa tabela, existe uma indicação de qual interface de saída do roteador deve ser encaminhada o pacote que chegou. Quem determina os valores presentes dessa tabela de repasse é o algoritmo de roteamento.

2.1 Parte interna de um roteador

Analisando a parte interna de um roteador entende-se melhor como é feita toda a transferência de uma porta de entrada até uma porta de saída. A porta de entrada de um roteador possui funções de três camadas. Conforme ilustrado na Figura 3, a porta de entrada possui 3 blocos, onde cada um realiza uma função em uma camada.

Figura 3 - Parte interna de um roteador.



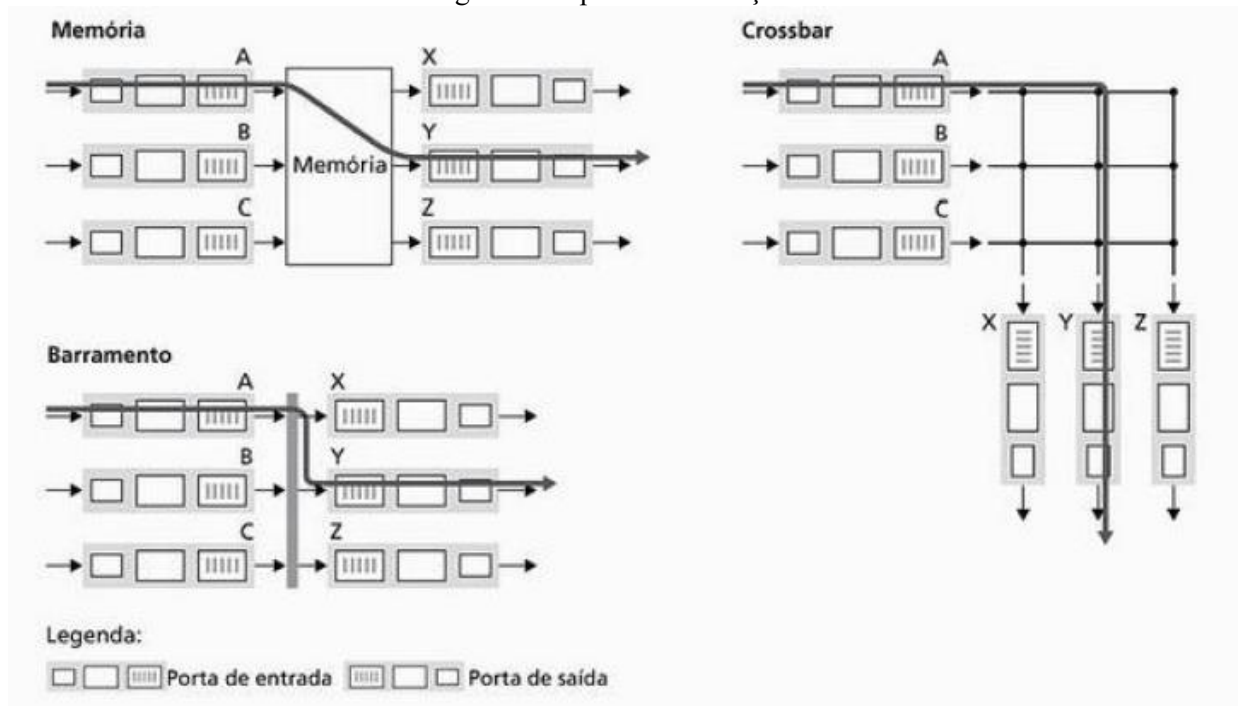
Fonte: KUROSE, J. F., 2010. p. 240.

No bloco mais à esquerda da porta de entrada e mais à direita da porta de saída a porta realiza função da camada física, fazendo um enlace físico a porta do roteador. Já no bloco central, tanto da porta de entrada quanto da porta de saída, tem-se as funções da camada de enlace que servem para interoperar com as funções da camada de enlace do outro lado do

enlace de entrada [3]. E por fim, no bloco mais à direita da porta de entrada e mais à esquerda da porta de saída temos a função de repasse[3].

O elemento de comutação conecta as portas de entrada às portas de saída. A comutação pode ser realizada de diversas maneiras como ilustrado na Figura 4.

Figura 4 - Tipos de comutação.



Fonte: KUROSE, J. F., 2010. p. 242.

- **Comutação por memória:** o pacote é copiado da porta de entrada para a memória do processador do roteador. O processador por sua vez, obtém o endereço de destino, consulta a tabela de repasse e encontra a porta de saída indicada por ela e copia o pacote para o *buffer* de saída daquela porta [3].
- **Comutação por barramento:** a porta de entrada envia o pacote para um barramento compartilhado sem a intervenção do processador de roteamento. Como o barramento é compartilhado, somente um pacote pode ser enviado ao barramento por vez. Mas como a velocidade de comutação por barramento é muito alta, isso faz com que não se tenha atraso e formação de fila nas portas de entrada do roteador [3].
- **Sistema crossbar:** tenta vencer a limitação de um único barramento compartilhado. Esse tipo de barramento permite que pacotes de entradas diferentes sejam repassados a saídas diferentes ao mesmo tempo. Entretanto se houver a tentativa de envio de dois pacotes para uma mesma porta de saída, o que chegar primeiro será repassado para a

saída e o outro será barrado e só será repassado à saída quando a mesma estiver livre[4].

2.2 Roteamento Estático

O roteamento estático é uma forma manual de se preencher a tabela de repasse do roteador. Ao contrário de roteamento dinâmico onde existe um protocolo de roteamento que faz com que se decida para qual saída o pacote deve ser encaminhado, neste modelo devemos informar ao roteador as rotas que devem ser tomadas. Uma vez que haja alguma alteração na rede, o sistema deverá ser atualizado, pois ele não consegue identificar a nova rede e se adaptar.

Esse roteamento é mais simples, indicado para redes menores e que não sofra alterações. Ele exige um menor custo computacional do roteador, entretanto se a rede for muito grande, haverá dificuldade para configurá-la [5].

2.3 Roteamento Dinâmico

O roteamento dinâmico, assim como o roteamento estático é um método de se preencher a tabela de rotas do roteador. Entretanto, no roteamento dinâmico, pode haver mais de uma única rota para um determinado ponto, além de conseguir fazer com que a tabela se atualize automaticamente em caso de alguma alteração na rede. Mas o “cérebro” por trás da escolha da rota dos pacotes é o protocolo de roteamento, o qual realiza um conjunto de operações matemáticas e indica qual a melhor opção de rota. Dentre os protocolos de roteamento dinâmico tem-se aqueles que são protocolos de roteamento interno (IGP - *Interior Gateway Protocols*) e os de roteamento externo (EGP - *Exterior Gateway Protocol*) [5].

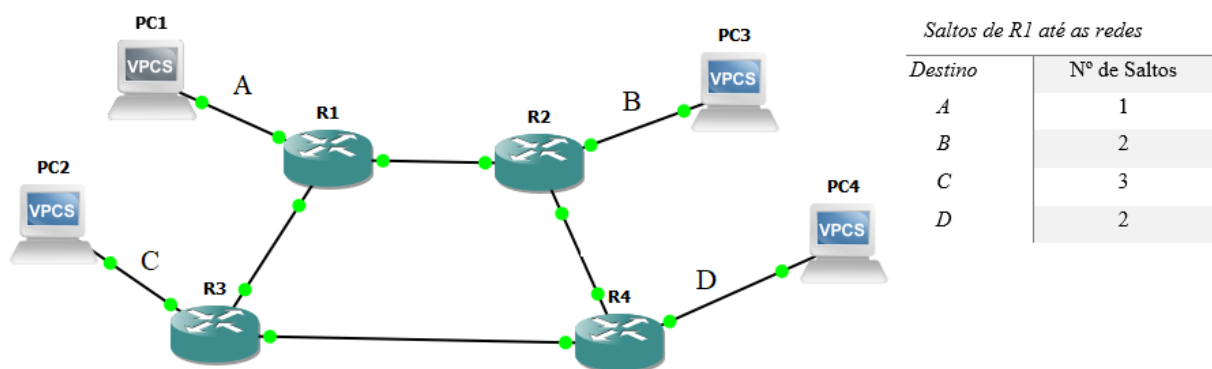
2.4 RIP

O RIP (*Routing Information Protocol*) é um protocolo de roteamento interno de um sistema autônomo baseado em um algoritmo de roteamento de vetor de distâncias. A sua primeira versão começou a ser amplamente difundida no início da década de 80 e posteriormente foi criada uma segunda versão um pouco mais eficiente [3].

O método usado conta em quantas sub-redes o pacote deverá passar para ser enviado para o endereço de destino contando com a rede de destino e depois escolhe o caminho com o menor número de saltos. O número máximo de saltos é 15.

Na Figura 5 tem-se uma rede configurada com quatro roteadores rodando protocolo RIP. À direita na imagem tem-se a tabela do roteador R1 com as possíveis subredes que podem receber pacotes e o número de saltos que são necessários para enviar um pacote até o destino final.

Figura 5 - Rede de computadores utilizando o protocolo de roteamento RIP.



Fonte: O autor (software GNS3).

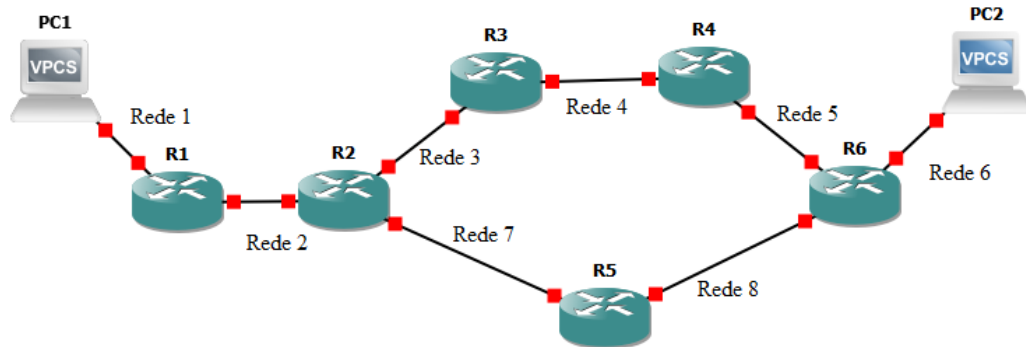
No RIP, os roteadores enviam suas tabelas de roteamento a cada 30 segundos para os roteadores vizinhos. Essa mensagem enviada pode conter uma lista de 25 sub-redes dentro do sistema autônomo. Cada roteador possui uma tabela RIP de roteamento que inclui as informações como: as sub-redes que o roteador alcança, o próximo roteador e o número de saltos que deve ser feito para que ele alcance cada sub-rede [3].

Caso um novo roteador seja adicionado à rede, quando se passar os 30 segundos e os roteadores trocarem suas tabelas de roteamento entre os vizinhos, o novo roteador poderá se tornar um caminho com menor custo e, por isso a rota pode ser alterada para passar por ele. Essa situação é ilustrada na Figura 6 onde se supõe que o PC1 deseja trocar informações com o PC2. Nesse cenário há duas possíveis rotas para o envio dos pacotes:

- Rota 1: passando pelas redes 2,3,4,5 e 6, contabilizando o total de 5 saltos;
- Rota 2: passando pelas redes 2,7,8 e 6 com um total de 4 saltos.

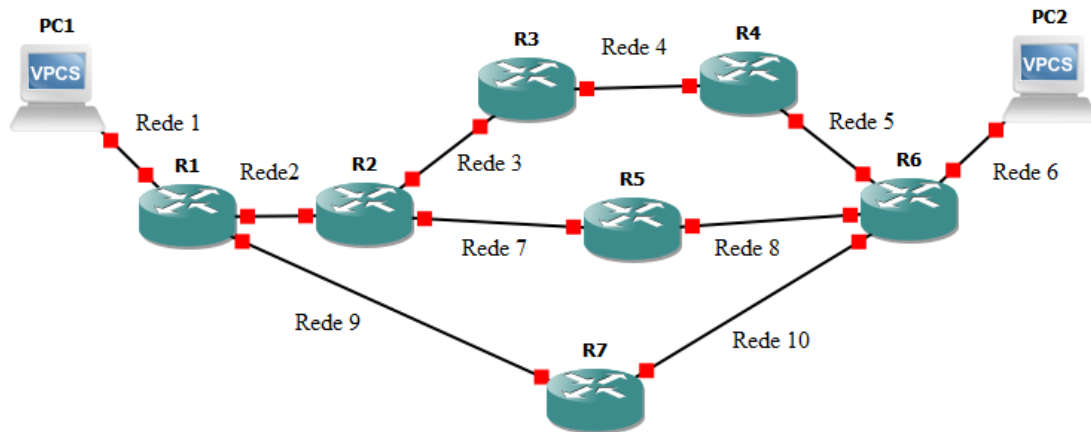
Portanto, o protocolo de roteamento enviará sempre os pacotes pela rota 2 uma vez que o seu custo é menor. Entretanto, caso haja alguma mudança na rede como a proposta ilustrada na Figura 7, o caminho de envio dos pacotes pode ser alterado.

Figura 6 - Simulação de um sistema autônomo.



Fonte: O autor (software GNS3).

Figura 7 - Nova topologia do sistema autônomo.



Fonte: O autor (software GNS3).

Outra característica do RIP é que como os roteadores trocam mensagens com os seus vizinhos a cada 30 segundos, quando se passa 180 segundos e um roteador não recebe nenhuma informação de um determinado vizinho, ele entende que esse vizinho está inalcançável e remove ele de sua tabela. Posteriormente, essa informação será repassada à seus vizinhos até a rede inteira saber que aquele roteador está inalcançável [7].

2.5 OSPF

Assim como o RIP, o OSPF (*Open Shortest Path First*) também é um protocolo utilizado dentro de um sistema autônomo. Ele veio para ser o sucessor do RIP porque possui aspectos mais avançados tais como:

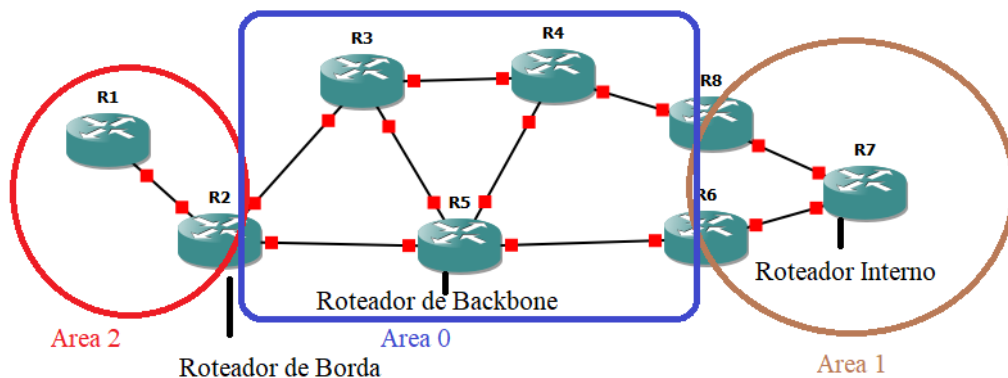
- Algoritmo de código aberto;
- Rotas com suporte a mais que 15 saltos;

- Segurança: trocas entre roteadores OSPF exigem autenticação na rede, evitando assim intrusos;
- Múltiplos caminhos de mesmo custo: quanto a tabela de roteamento OSPF percebe que existe dois ou mais caminhos com o mesmo custo, ela permite que todos os caminhos sejam usados, ou seja, não é escolhido um único caminho. Este recurso é conhecido como ECMP (*Equal Cost MultiPath*);
- Suporte para roteamento *unicast* e *multicast*: – possui suporte não só para entregas de pacote ponto a ponto (*unicast*), mas também para a entrega para todos os *hosts* conectados à rede (*multicast*);
- Estruturação hierárquica em áreas: necessário em redes de grande porte onde os roteadores não conseguiriam conhecer todas as rotas possíveis dentro da rede[6].

Esse protocolo começou a ser amplamente usado no final da década de 80 e em 1990 se tornou um padrão. Baseado no OSPF foi criado também o protocolo IS-IS, entretanto o OSPF é mais utilizado em redes empresariais enquanto o IS-IS é mais utilizado em ISP's (*Internet Service Providers*) [1].

A grande vantagem dele é a divisão de uma rede em áreas. Os roteadores que estão dentro de uma área são denominados de roteadores internos e cada sistema autônomo possui uma área de *backbone*, área 0, a qual todas as áreas estão conectadas. Os roteadores que conectam duas ou mais áreas são chamados de roteadores de borda de área. Essa configuração é ilustrada na Figura 8.

Figura 8 - Esquema de rede com OSPF.



Fonte: O autor (software GNS3).

Quando se envia um pacote de um roteador de uma determinada área para um roteador em uma outra área, o pacote vai até o roteador de borda, repassa o pacote ao *backbone* e

depois ele é encaminhado para a área de destino passando pelo roteador de borda daquela área até ser entregue ao roteador de destino. Lembre-se que o caminho utilizado é sempre o de menor custo [1].

Quando um roteador é adicionado em uma rede OSPF, ele envia uma mensagem de HELLO em todas as conexões ponto a ponto afim de conhecer todos os roteadores que estão na LAN (*Local Area Network*). Todos os roteadores na mesma LAN são considerados vizinhos. Entretanto, um roteador que é adjacente aos outros roteadores da LAN é nomeado como roteador designado. Este roteador serve para trocar informações com todos os roteadores da LAN, fazendo que os roteadores conversem apenas com o designado e não com os demais. Também um outro roteador é utilizado como roteador designado de backup, onde recebe todas as informações do roteador designado e em caso de falha ele assume o papel do roteador designado[1]. Este processo tem a finalidade de reduzir a quantidade de informação trocada entre os roteadores, reduzindo o tráfego de dados entre eles para liberar para a transmissão de pacotes.

CAPÍTULO 3

SIMULAÇÃO DOS PROTOCOLOS RIP E OSPF

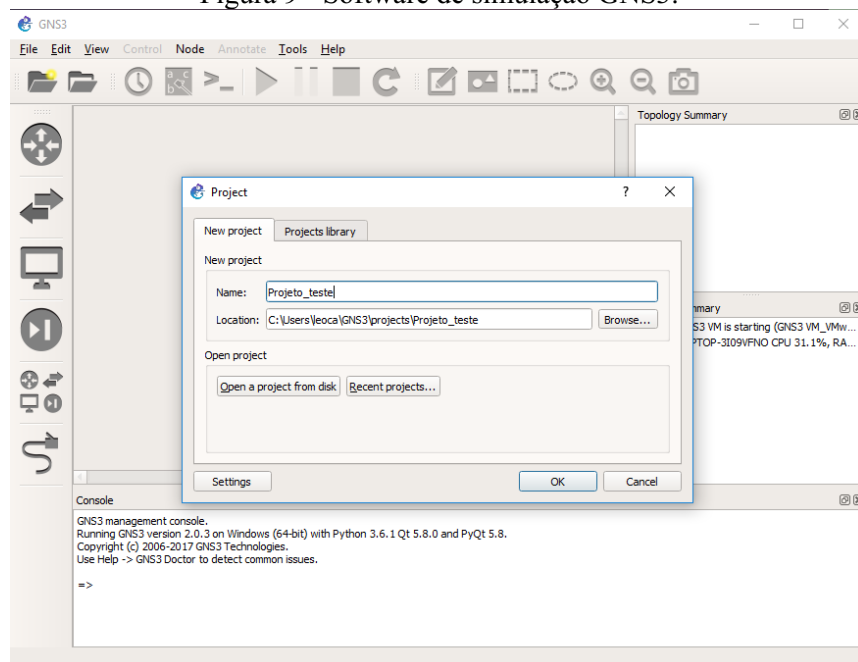
O cenário ideal seria criar uma rede com equipamentos e aplicar os protocolos de roteamento para estudá-los. Entretanto, isso não foi possível e uma alternativa foi utilizar os softwares de emulação e simulação de rede para obter resultados válidos.

3.1 GNS3

Inicialmente, utilizou-se o software GNS3 capaz de emular o ambiente de redes de computadores utilizando IOS (*Internetwork Operation System*) de roteadores do fabricante Cisco. Ele é gratuito e o seu download está disponível no site oficial www.gns3.com. Nesse site tem a documentação de referência para a instalação e para ajudar os usuários a trabalharem com software, desde os primeiros passos até configurações mais avançadas [8].

Após a instalação do GNS3 criou-se um novo projeto com a topologia de rede desejada conforme ilustrado na Figura 9.

Figura 9 - Software de simulação GNS3.



Fonte: *Print screen* do software GNS3.

Depois de criado um projeto o próximo passo é a criação da topologia. Para isso, basta clicar, arrastar e soltar os componentes na área de trabalho e a seguir adicionar um enlace

entre eles. Quando a topologia estiver montada, basta apertar o botão de play localizado na barra de ferramentas superior e todas as máquinas da sua rede serão ligadas. Já com as máquinas ligadas, clicando duas vezes sobre cada item, será aberto a janela de console, a qual é utilizada para enviar comandos de configuração para os dispositivos.

3.2 OSTINATO

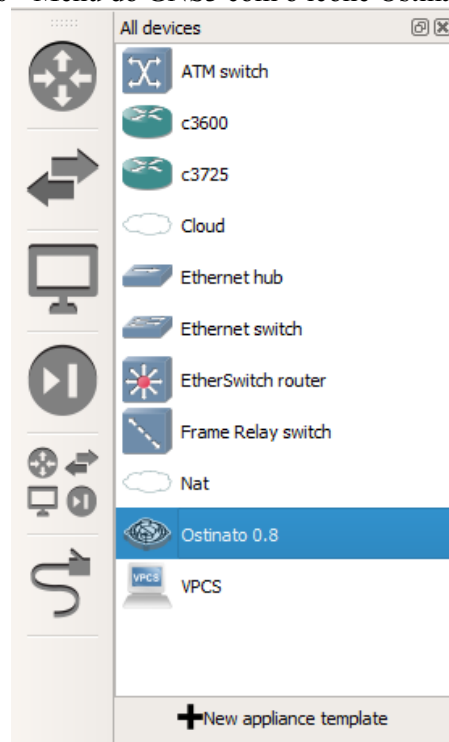
Ostinato é uma ferramenta desenvolvida para simular tráfego de dados dos mais diversos tipos e tem interface com o GNS3. O processo de instalação dele é complexo exigindo detalhes para que ele funcione adequadamente. Esse software é pago e está disponível no site oficial [9]. Entretanto, existe uma parceria entre o Ostinato e o GNS3 oferecendo um formato exclusivo chamado Ostinato Drone que funciona no GNS3 e é gratuita disponível em[10].

Antes de instalar o Ostinato no GNS3 criou-se uma máquina virtual GNS3 VM conforme definida em[11]. Ressalto que a máquina virtual baixada deve ser da mesma versão que o GNS3 instalado no computador. Após fazer o download do GNS3 VM, utilizou-se o software VMWare Pro para instalação do GNS3. O passo a passo está disponível em [12]. Após a instalação do GNS3 VM seguiu-se o passo a passo para a instalação do Ostinato.

- 1) Abra o GNS3;
- 2) Clique em *File – Import Appliance* e selecione o arquivo do Ostinato drone baixado do site do GNS3;
- 3) Clique em *Next* 3 vezes;
- 4) Selecione a versão mais atual do Ostinato e clique em *download*;
- 5) Depois terminado o *download*, clique em *next* por mais 2 vezes e o Ostinato estará instalado e pronto para o uso.

A Figura 10 ilustra o menu do GNS3 com o ícone Ostinato. Ele funciona como qualquer outro dispositivo presente no GNS3. Para utilizá-lo deve-se clicar, segurar e arrastá-lo para a área de trabalho e conectá-lo a algum dispositivo para o envio de pacotes de dados para ele. Depois de toda rede devidamente conectada, basta apertar no *play* para que todos os dispositivos sejam ligados.

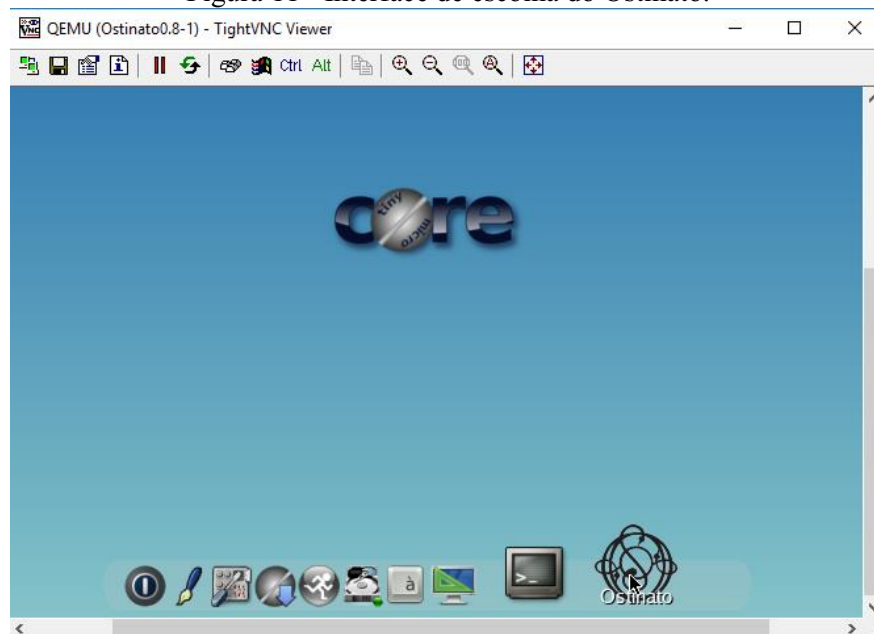
Figura 10 - Menu do GNS3 com o ícone Ostinato.



Fonte: *Print screen* da barra de ferramentas do GNS3.

O tráfego de dados para os dispositivos não conectados diretamente ao Ostinato só é possível após a ativação de um protocolo de roteamento. Para abrir a interface de configuração do Ostinato deve-se clicar duas vezes no ícone dele e será aberta uma janela conforme ilustrado na Figura 11.

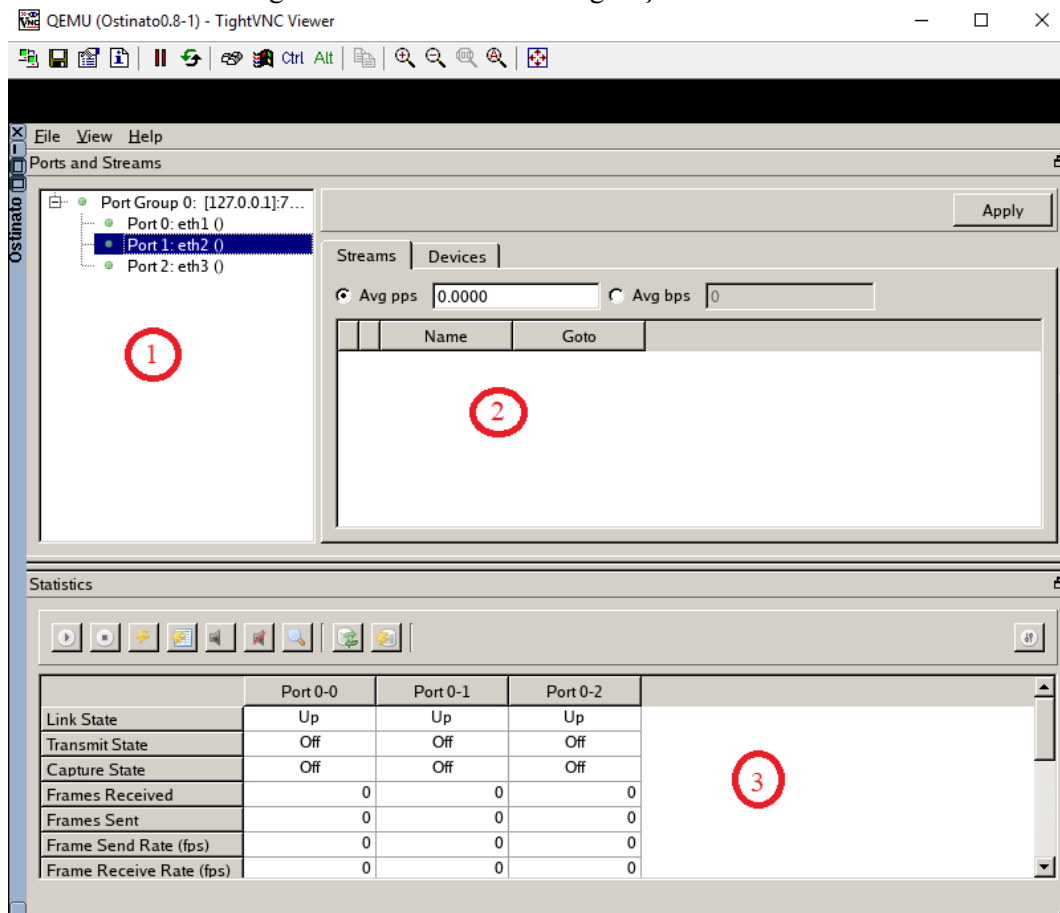
Figura 11 - Interface de escolha do Ostinato.



Fonte: *Print screen* da janela inicial do Ostinato.

Observem na Figura 11 algumas opções disponíveis na parte inferior, mas a opção de interesse é a última, a qual quando o mouse está em cima dela aparece a palavra *Ostinato*. Clicando neste ícone será aberta a janela para a configuração do tráfego de dados ilustrada na Figura 12.

Figura 12 - Interface de configuração do Ostinato.



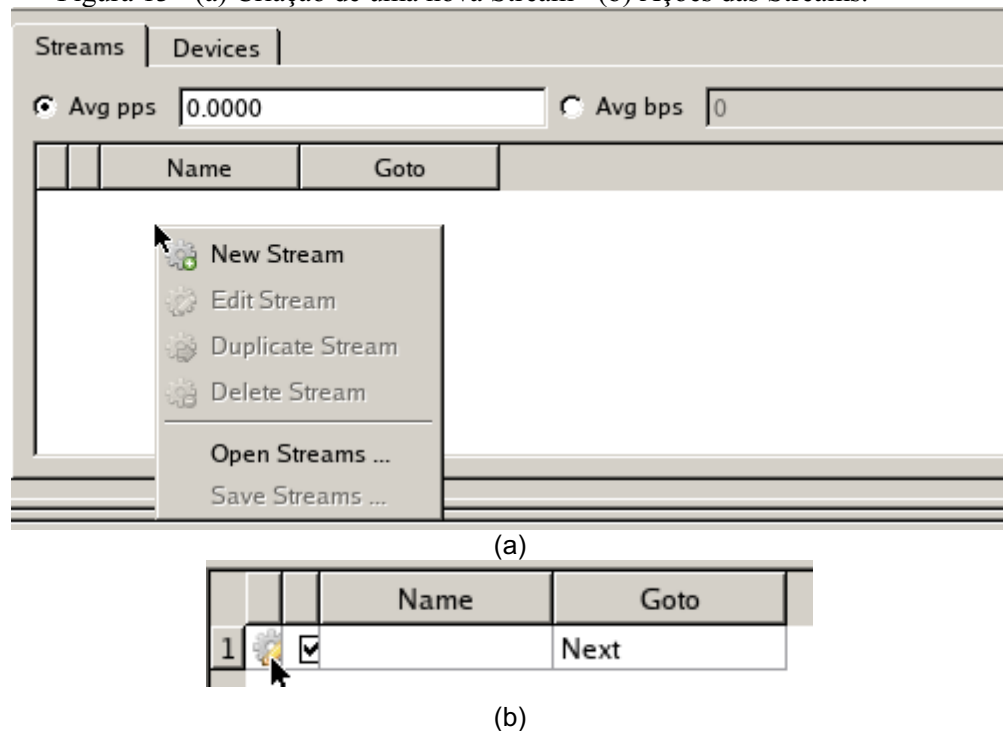
Fonte: *Print screen* da janela de configuração do Ostinato.

O software é composto de três regiões principais que são *Ports*, *Streams* e *Statistics* e, essas são descritas a seguir [13]:

A região 1 é *Ports* onde estão localizadas as portas de conexão do Ostinato. Essa versão tem três portas disponíveis para enviar *streaming* de dados, eth1, eth2 e eth3. Caso conecte-se na porta eth1 e queira transmitir dados através dela, deve-se clicar nesta porta para selecioná-la e então partir para a configuração de *streams* que se encontra na região 2.

A região 2 é *Streams* que após a seleção da porta deve-se ir até o campo em branco dessa região e clicar com o botão direito e selecionar “*New Stream*” como ilustrado na Figura 13 (a). Aparecerá uma linha contendo um ícone de engrenagem, um *checkbox*, um nome em branco e um campo Goto ilustrado na Figura 13 (b).

Figura 13 - (a) Criação de uma nova Stream - (b) Ações das Streams.



Fonte: *Print screen* da janela de criação de Streams do Ostinato.

- *Checkbox* - serve para decidir se a *stream* deve ser transmitida ou não. Supondo a criação de um conjunto de *streams*, mas não é desejado que todas elas sejam transmitidas em um determinado teste, então basta desmarcar o *checkbox* e a *stream* não será transmitida.
- *Name* – serve para nomear a *stream* para facilitar a identificação de quais protocolos estão sendo utilizados nela.
- *Goto* – representa a ação a ser tomada no final da transmissão da *stream*. As opções são ir para uma próxima, voltar para a primeira (loop) o encerrar a transmissão.

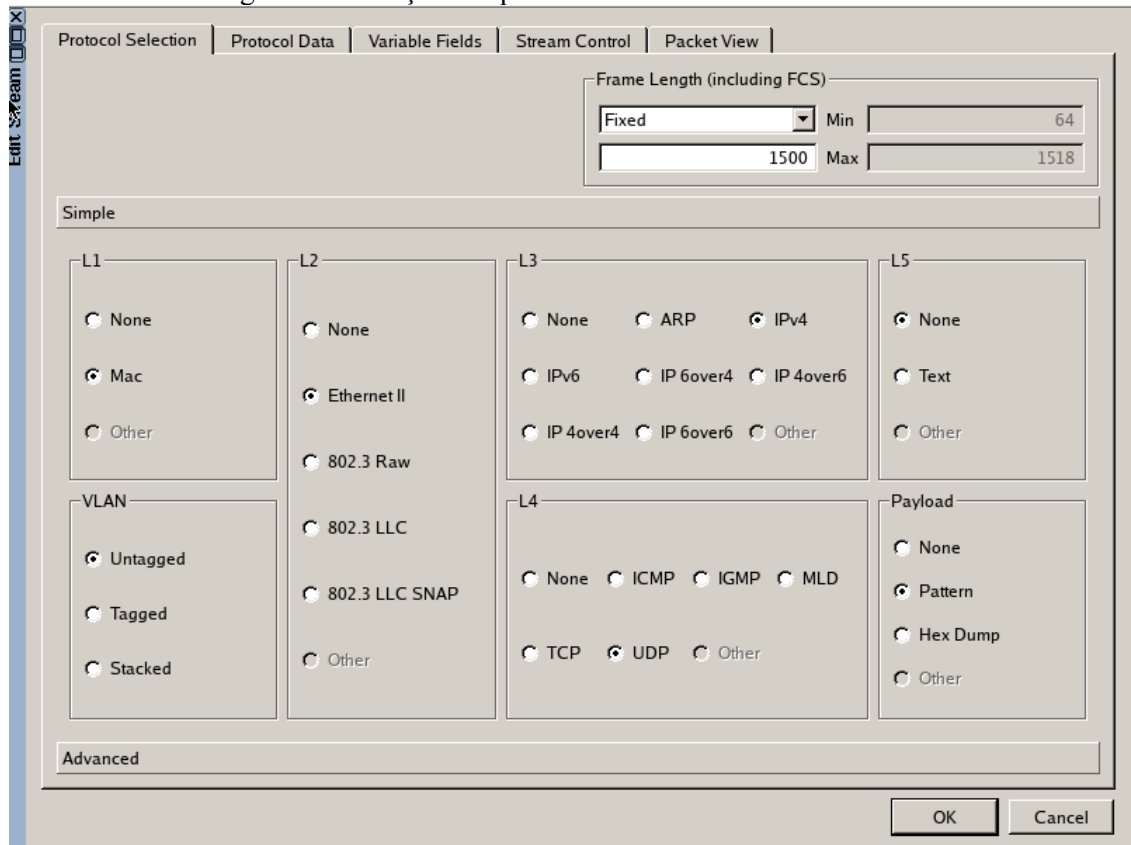
Um duplo clique no ícone da engrenagem abre o modo de configuração da *stream* ilustrado na Figura 14. Observe que há várias abas, cada uma com uma determinada função para que o tráfego de dados seja gerado.

A. “*Protocol Selection*” onde se escolhe quais os protocolos que fazem parte da *stream* que será transmitida. A seleção dos protocolos é de baixo para cima de acordo com os protocolos selecionados, o programa libera os protocolos de camada superiores compatíveis com o de camada inferior que foi selecionado.

- Mac para identificar fisicamente o equipamento que receberá os dados;

- Padrão Ethernet II para padronizar o formato dos frames, tamanho, taxa de transmissão, entre outros;
- IPV4 indica que a camada 3 utiliza o protocolo IP em sua versão 4, composto de uma sequência de 4 Bytes;
- UDP para orientar quais portas serão utilizadas para a transmissão dos dados;
- *Payload Pattern* indica que tem informação a ser transmitida.

Figura 14 - Seleção dos protocolos de cada camada.



Fonte: *Print screen* da janela configuração de protocolos do Ostinato.

- B. “*Protocol Data*” ilustrado na Figura 15 apresenta as configurações de cada protocolo que será utilizado para a transmissão de dados. A primeira parte é composta pelo “*Media Access Control*”, conhecido como MAC. Preenche-se com o endereço MAC do Ostinato o campo *Source* e com o endereço MAC do destino o campo *Destination*. O campo “Ethernet II” permanece inalterado e o terceiro campo “*Internet Protocol ver 4*” segue a configuração ilustrada na Figura 15 (b). Nessa aba configuram-se os endereços IP de origem e de destino da mensagem, a máscara de rede e outras características relacionadas ao cabeçalho dos pacotes.

Figura 15 - (a) Endereço Mac de origem e destino (b) Endereço IP de origem e destino.

Protocol Selection | Protocol Data | Variable Fields | Stream Control | Packet View

Media Access Protocol

	Address	Mode	Count	Step
Destination	00 00 00 00 00 00	Fixed	16	1
Source	00 00 00 00 00 00	Fixed	16	1

Ethernet II

Internet Protocol ver 4

Internet Control Message Protocol

Payload Data

OK Cancel

(a)

Internet Protocol ver 4

☐ Override Version 4

☐ Override Header Length (x4) 5

TOS/DSCP 00

☐ Override Length 46

Identification 04 D2

Fragment Offset (x8) 0

☐ Don't Fragment ☐ More Fragments

Time To Live (TTL) 127

☐ Override Protocol 01

☐ Override Checksum 36 FE

	Mode	Count	Mask
Source 0 .0 .0 .0	Fixed	16	255.255.255.0
Destination 0 .0 .0 .0	Fixed	16	255.255.255.0

Options TODO

(b)

Fonte: *Print screen* da janela configuração de protocolos do Ostinato.

C. “User Datagram Protocol”, ilustrado Figura 16, as portas UDP’s que serão utilizadas.

User Datagram Protocol

☐ Override Source Port 0

☐ Override Destination Port 0

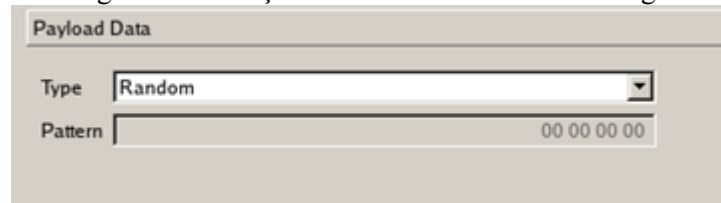
☐ Override Length 26

☐ Override Checksum FF BA

Fonte: *Print screen* da janela configuração de protocolos do Ostinato.

D. “*Payload Data*”, ilustrado na Figura 17, é a opção para a escolha de palavras aleatórias, palavras fixas, incremento ou decremento de bytes. Essa é a última configuração e é a escolha do tipo dos dados que serão utilizados no *Payload*.

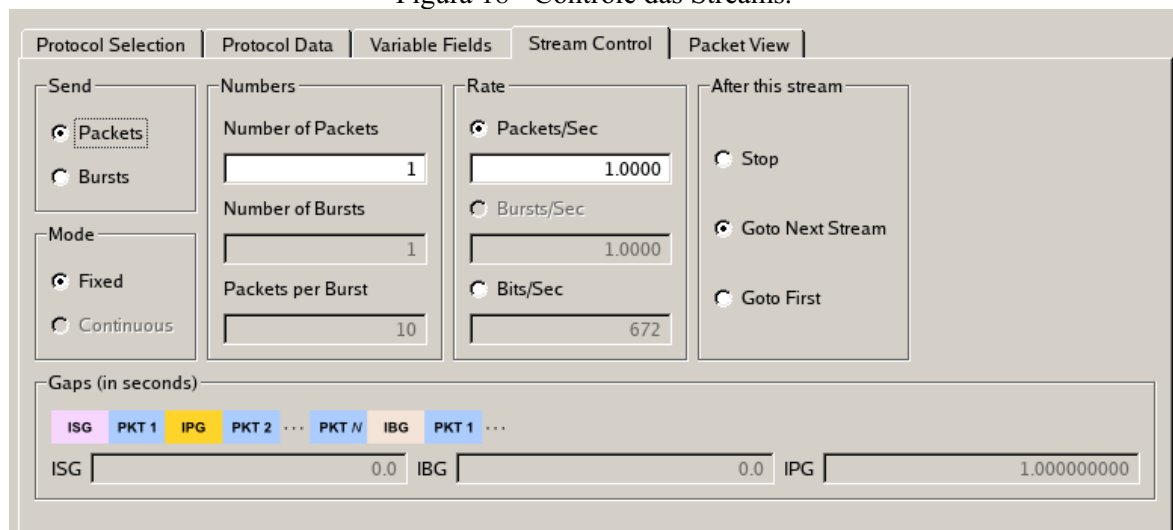
Figura 17 - Seleção do formato dos dados da carga.



Fonte: *Print screen* da janela configuração de protocolos do Ostinato.

Finalizado as configurações escolhe-se a taxa de transmissão dos dados em bits/segundo na aba “Stream Control” ilustrada na Figura 18. Nesta aba, é possível escolher o modo em rajadas ou em envio contínuo de pacotes. Também é possível escolher a quantidade de pacotes e quantos pacotes por segundo. Por fim, tem-se as opções de encerrar a transmissão de pacotes ao término, ir para a próxima stream ou voltar para a primeira stream.

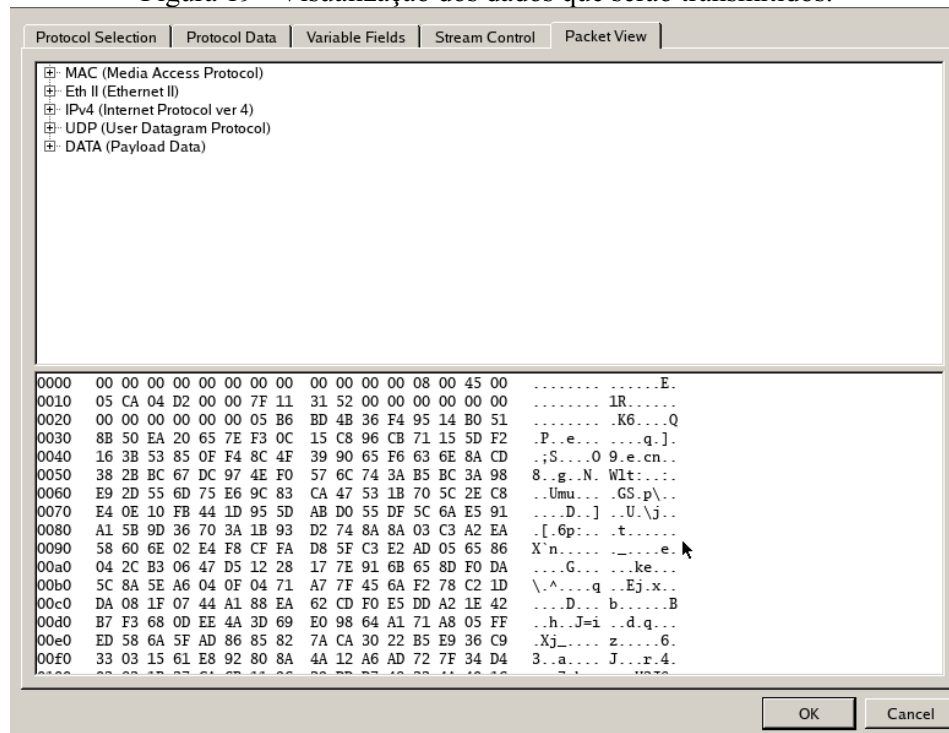
Figura 18 - Controle das Streams.



Fonte: *Print screen* da janela configuração de protocolos do Ostinato.

A Figura 19 ilustra a tela para visualizar a configuração dos pacotes a serem enviados. Depois de finalizar todo este processo de configuração descrito, clica-se em ok e a janela de configuração será fechada. Para criar novos tipos de *streams* repete-se o processo supracitado. Quando estiver pronto para transmitir, clica-se no botão “*Apply*” localizado na parte superior à direita da região de *streams* para que as configurações sejam aplicadas e transmitidas.

Figura 19 - Visualização dos dados que serão transmitidos.



Fonte: *Print screen* da janela configuração de protocolos do Ostinato.

A região 3 apresentada na figura 14 é a *Statistics*. Destinada para iniciar e pausar a transmissão de pacotes em uma determinada porta escolhida. Além disso, apresenta alguns parâmetros estatísticos como quantidade de *frames* transmitidos, *frames* recebidos e outras informações ilustradas na Figura 20.

Figura 20 - Estatísticas da transmissão de dados.

Statistics				
	Port 0-0	Port 0-1	Port 0-2	
Link State	Up	Up	Up	
Transmit State	Off	Off	Off	
Capture State	Off	Off	Off	
Frames Received	0	0	0	
Frames Sent	0	0	0	
Frame Send Rate (fps)	0	0	0	
Frame Receive Rate (fps)	0	0	0	

Fonte: *Print screen* da janela Statistics do Ostinato.

Para iniciar a transmissão, clique na coluna correspondente à porta que se deseja transmitir os dados e, em seguida no botão *play*.

Apesar das ferramentas estatísticas presente no Ostinato optou-se pela utilização do Wireshark. Ele captura os dados transmitidos entre os enlaces e assim, permite precisão na coleta dos resultados obtidos.

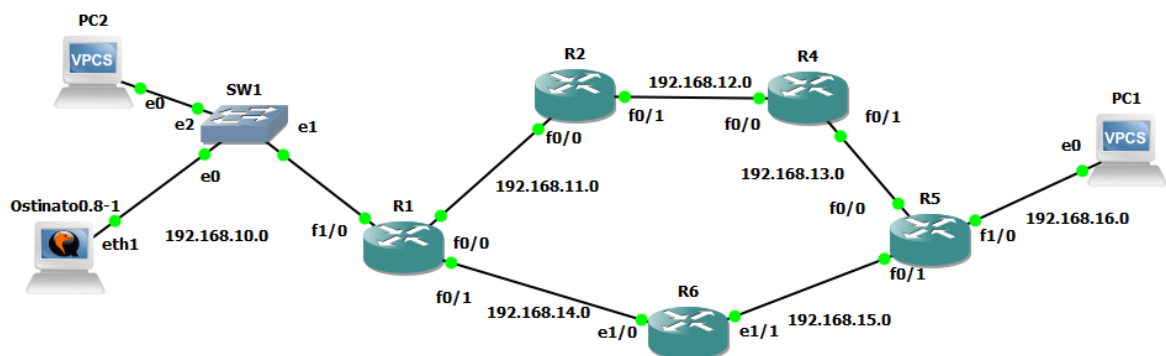
3.3 Wireshark

Wireshark é uma ferramenta utilizada para a análise de tráfego de dados em rede. É um software gratuito e pode ser baixado no seu site oficial [14]. A sua principal função é capturar os dados transmitidos pelo usuário e mostrar todas as informações presentes neles, protocolos utilizados, endereços de destino, informações contidas nos pacotes, etc [15]. Ele funciona integrado ao GNS3 e, para iniciá-lo deve-se clicar com o botão direito no enlace a ser analisado e selecionar a opção “*Start Capture*”. O Wireshark iniciará e todos os pacotes que trafegarem no enlace serão capturados e apresentados na tela do *software*. Deste modo, é possível saber se os dados transmitidos pelo Ostinato alcançaram o destino, por qual caminho passaram e se houve perda de informação.

3.4 Cenários de simulação no GNS3

A proposta inicial deste projeto era a análise do desempenho dos protocolos RIP e OSPF em três tamanhos de topologias diferentes. Entretanto, a utilização de três programas Ostinato GNS3 e Wireshark exigiu um custo computacional altíssimo tornando os testes em redes com 4 ou 5 roteadores pesados. As tentativas de expansão da rede para topologias com 10 roteadores foram frustradas, o computador não conseguiu processar. Por este motivo, os testes iniciais ficaram limitados à topologia ilustrada na Figura 21.

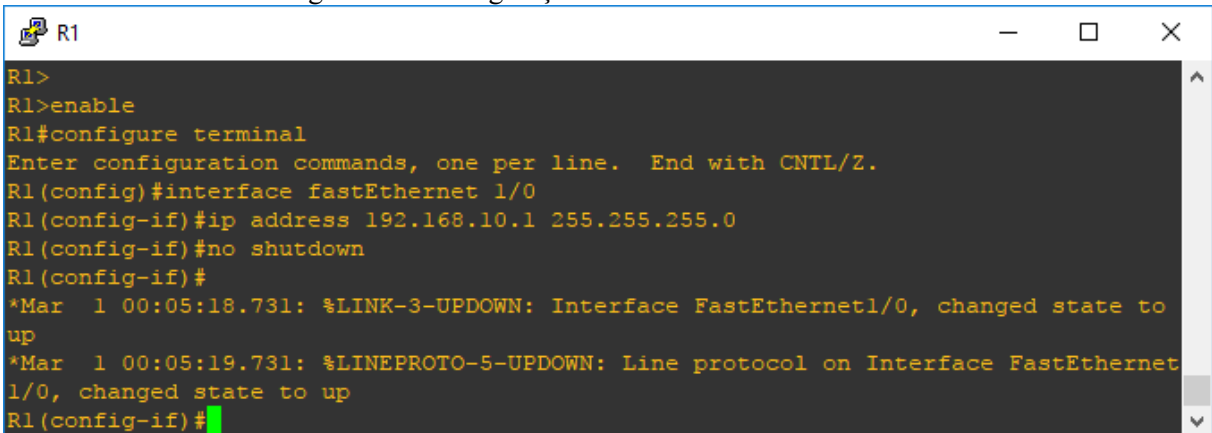
Figura 21 - Topologia de rede simulada.



Fonte: O autor (software GNS3).

A topologia proposta é composta por cinco roteadores e sete redes diferentes. A configuração das redes é feita individualmente em cada interface do roteador que será conectada. A figura 22 ilustra a sequência de comandos que se inicia com “enable”, o qual habilita o modo de privilégio do roteador, seguido pelo “configure terminal” para o modo de configuração. Na interface configurada fast-ethernet 1/0 habilitou-se o endereço ip e máscara por meio do comando “ip address 192.168.10.1 255.255.255.0”. Para finalizar ativa-se a interface com o comando “no shutdown”.

Figura 22 - Configuração das interfaces dos roteadores.

A screenshot of a terminal window titled 'R1'. The terminal shows the following commands and output: 'R1>' followed by 'R1>enable' to enter privileged mode. Then 'R1#configure terminal' to enter configuration mode. A prompt 'Enter configuration commands, one per line. End with CNTL/Z.' is shown. The user enters 'R1(config)#interface fastEthernet 1/0'. Then 'R1(config-if)#ip address 192.168.10.1 255.255.255.0'. Then 'R1(config-if)#no shutdown'. The prompt returns to 'R1(config-if)#'. Two status messages are displayed: '*Mar 1 00:05:18.731: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up' and '*Mar 1 00:05:19.731: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 1/0, changed state to up'. The prompt is now 'R1(config-if)#' with a green cursor.

Fonte: Print screen do terminal de configuração do roteador R1.

Esta sequência de comandos é repetida em todos os roteadores até que todas as interfaces estejam ativas e com um IP associado a elas. O próximo passo é a configuração dos protocolos de roteamento.

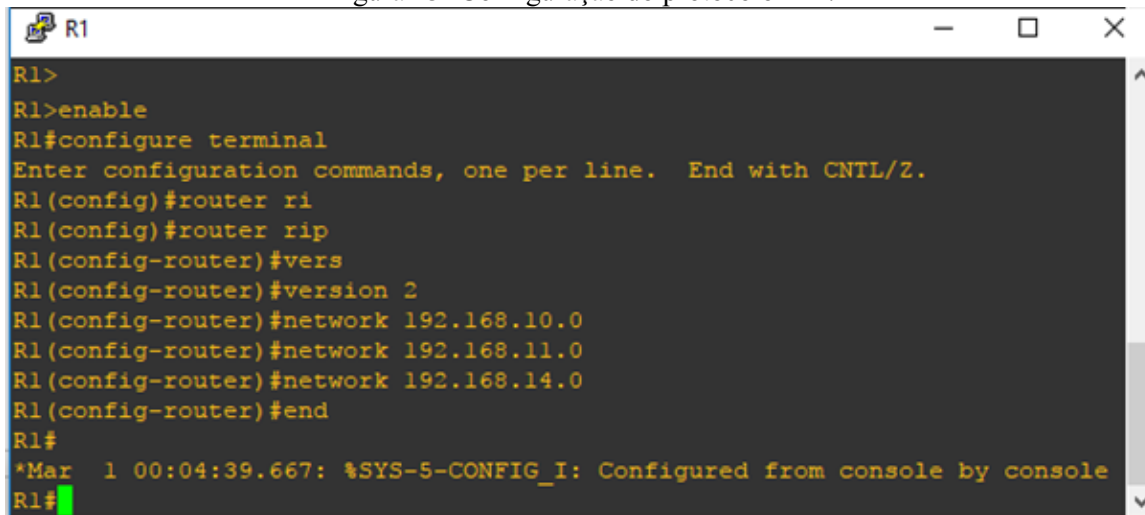
3.4.1 Configuração dos protocolos de roteamento

Para o PC2 comunicar-se com o PC1 é necessário que um protocolo de roteamento esteja ativo na rede. Os protocolos de roteamento implementados serão o RIP e o OSPF. Para isto, deve-se entrar no modo de privilégio do roteador e em seguida no modo de configuração onde se aplica os comandos específicos de ativação de cada um deles. Lembrando que este processo deve ser feito para todos os roteadores.

A Figura 23 ilustra os comandos utilizados na configuração do protocolo de roteamento RIP. A sequência de comandos é “enable”, “configure terminal” e o comando “router rip” e “version 2” para a definição do protocolo de roteamento RIP versão 2. Após estes comandos, apresenta-se todas as redes vizinhas ao roteador para que o mesmo as

reconheça e consiga enviar os dados de uma rede para outra por meio do comando “*network + rede*”.

Figura 23- Configuração do protocolo RIP.



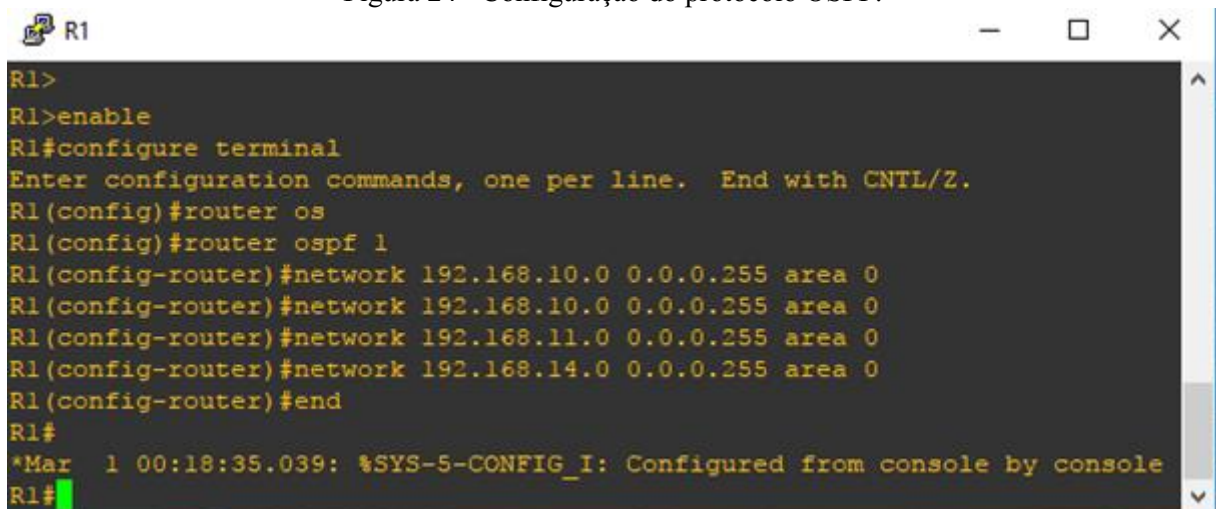
```

R1>
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ri
R1(config)#router rip
R1(config-router)#vers
R1(config-router)#version 2
R1(config-router)#network 192.168.10.0
R1(config-router)#network 192.168.11.0
R1(config-router)#network 192.168.14.0
R1(config-router)#end
R1#
*Mar  1 00:04:39.667: %SYS-5-CONFIG_I: Configured from console by console
R1#
  
```

Fonte: *Print screen* do terminal de configuração do roteador R1.

A Figura 24 ilustra a configuração do OSPF no roteador R1. A sequência de comandos é “*enable*”, “*configure terminal*” e o comando “*router ospf 1*” para habilitar o roteamento e depois anuncia-se as redes vizinhas com o comando “*network + rede + máscara de sub rede inversa + número da área*”.

Figura 24 - Configuração do protocolo OSPF.



```

R1>
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router os
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 192.168.11.0 0.0.0.255 area 0
R1(config-router)#network 192.168.14.0 0.0.0.255 area 0
R1(config-router)#end
R1#
*Mar  1 00:18:35.039: %SYS-5-CONFIG_I: Configured from console by console
R1#
  
```

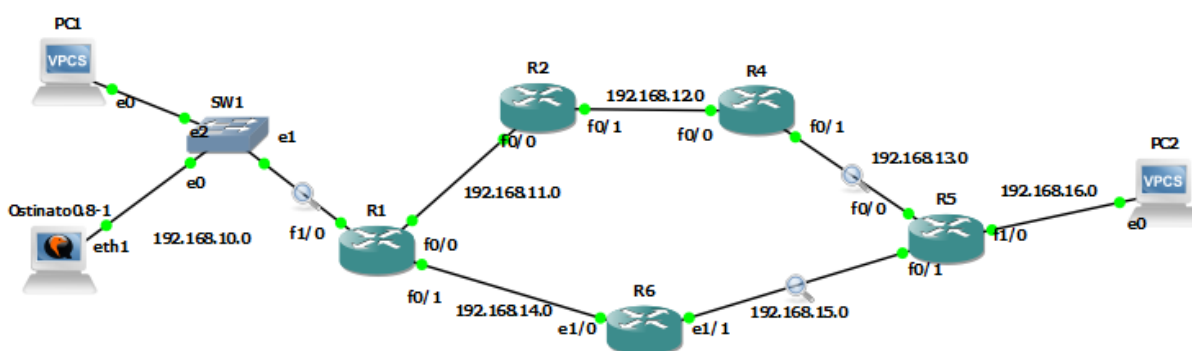
Fonte: *Print screen* do terminal de configuração do roteador R1.

Neste ponto da simulação têm-se os dois modelos de redes criados para a coleta dos resultados obtidos e uma análise comparativa.

3.4.2 Resultados obtidos

O parâmetro de análise é a perda de pacotes durante a transmissão. Para isso, gera-se um tráfego de controle (ICMP – *Internet Control Message Protocol*) transmitido do Ostinato conectado no R1 por meio do switch SW1 até o PC2 conectado no R5 conforme ilustrado na Figura 25. O tráfego gerado é de 600 pacotes com uma taxa de 10 pacotes por segundo. Esta é uma taxa de dados considerada baixa, entretanto quando se tenta transmitir a uma taxa de dados mais elevada o Ostinato não consegue, tanto por limitação do próprio software quanto do computador que neste caso possuía um processador core i5, 4GB de memória RAM e 2GB de placa gráfica dedicada, o que são configurações ideais para este tipo de trabalho. Também, não se conseguiu gerar múltiplos tráfegos na rede.

Figura 25 - Topologia de rede utilizada na simulação.



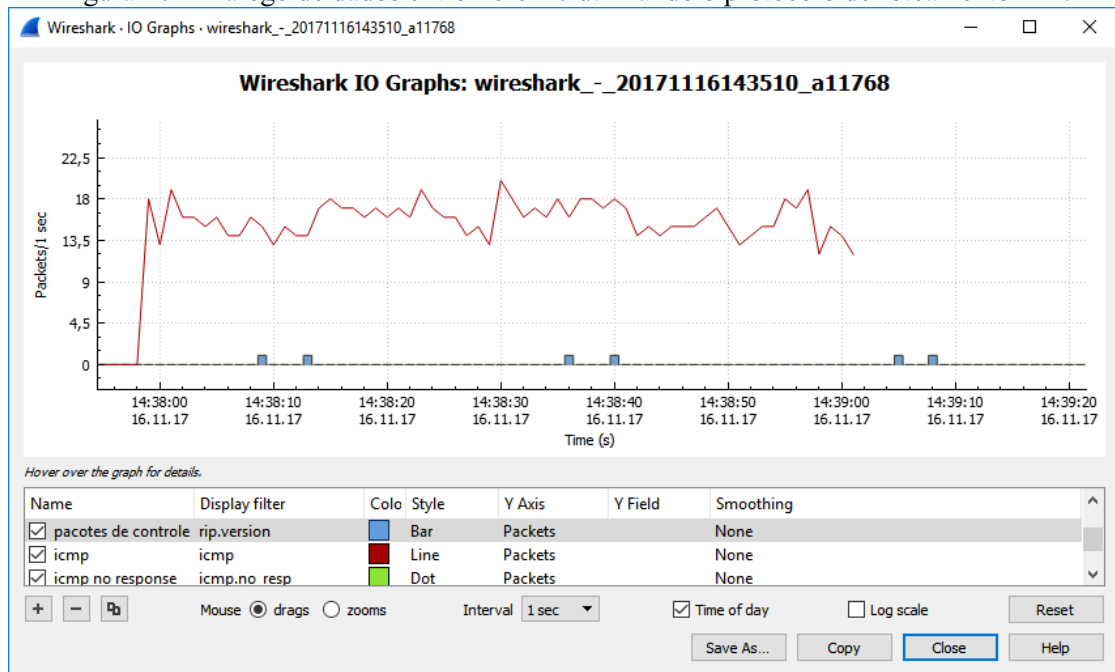
Fonte: O autor (software GNS3).

No cenário 1 tem-se uma limitação da largura de banda da interface do roteador R6 que compõe o menor caminho. O objetivo de se gerar um congestionamento de dados e, poder testar a perda de pacotes e a criação de novas rotas. O monitoramento com o Wireshark se deu nos pontos entre R4 – R5 e R6 – R5. Os gráficos dos resultados obtidos são ilustrados nas Figuras 26 e 27, respectivamente para o RIP e OSPF. Em ambos os protocolos, os dados trafegaram pelo caminho mais curto entre R5 e R6 e não houve tráfego de dados entre R4 e R5.

Já no cenário 2 tem-se uma limitação da velocidade de transmissão da interface do roteador R6 em no máximo 100kbps. As interfaces ethernet com velocidade de até 10 Mbps, porém a velocidade do enlace é limitada em 1% do seu valor, ou seja, 100 kbps. Qual será o comportamento da rede? Haverá perda de pacotes? Haverá atraso na entrega? A rota de envio dos pacotes será alterada? Os comandos para a criação do cenário 2 são ilustrados na Figura

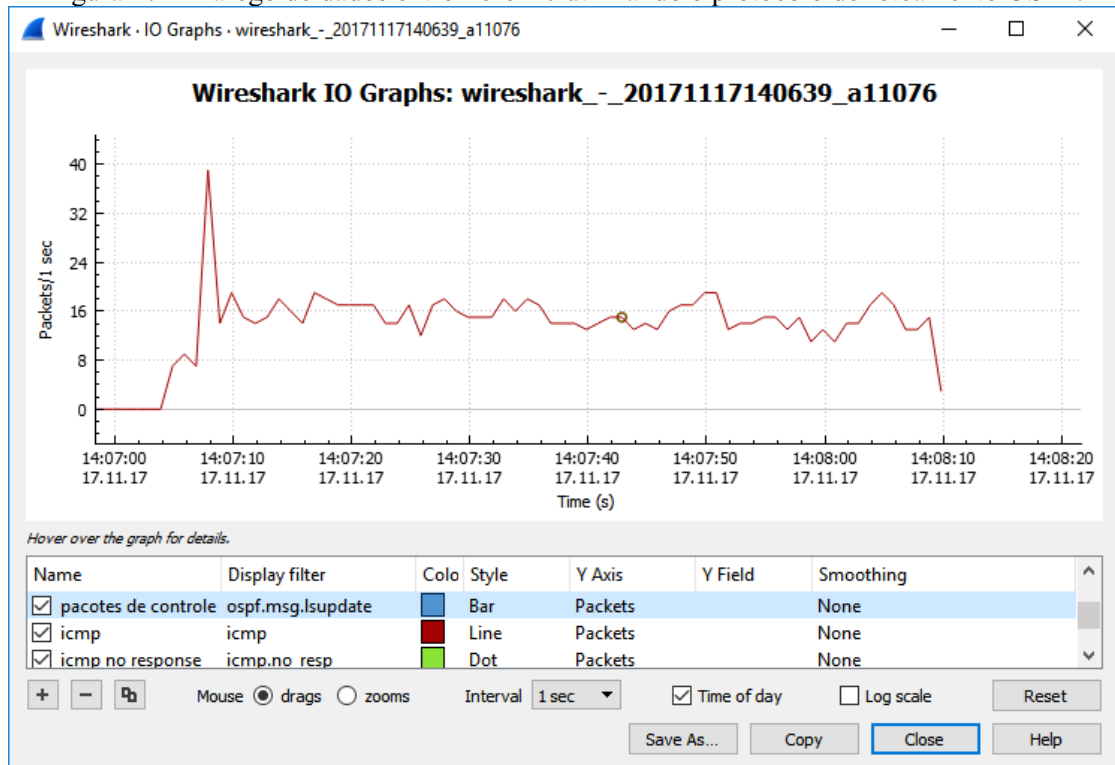
28. Após vinte segundos do início da transmissão de dados limitou-se a interface ethernet 1/0 do roteador R6 e a outra interface teve a sua velocidade alterada para 100kbps.

Figura 26 - Tráfego de dados entre R5 e R6 utilizando o protocolo de roteamento RIP.



Fonte: Print screen da janela I/O graph (software Wireshark).

Figura 27 - Tráfego de dados entre R5 e R6 utilizando o protocolo de roteamento OSPF.



Fonte: Print screen da janela I/O graph (software Wireshark).

Figura 28 - Configuração de limitação de banda do roteador R6.

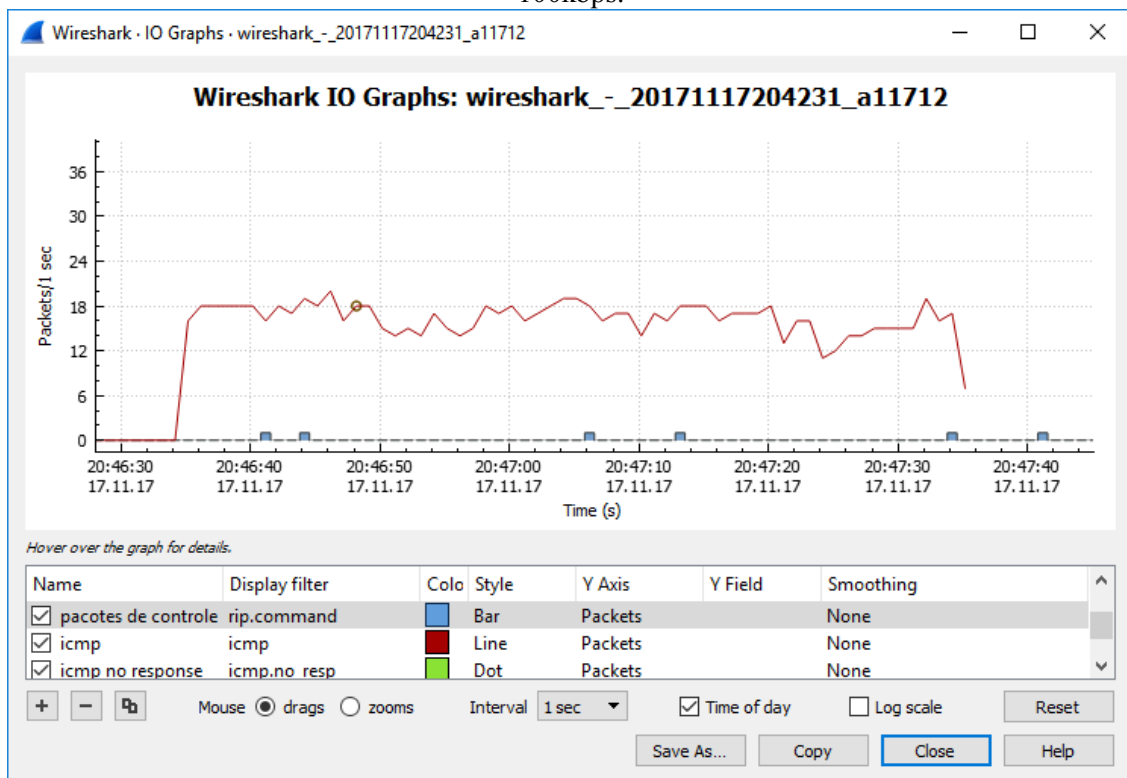
```

R6>
R6>
R6>enable
R6#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R6(config)#interface ethernet 1/0
R6(config-if)#bandwidth 100
R6(config-if)#end
R6#
*Mar  1 00:57:12.051: %SYS-5-CONFIG_I: Configured from console by console
R6#
  
```

Fonte: *Print screen* do terminal de configuração do roteador R6.

Os resultados obtidos no cenário 2 são ilustrados nas Figuras 29 e 30.

Figura 29 - Tráfego de dados entre os roteadores utilizando o RIP com a velocidade limitada em 100kbps.

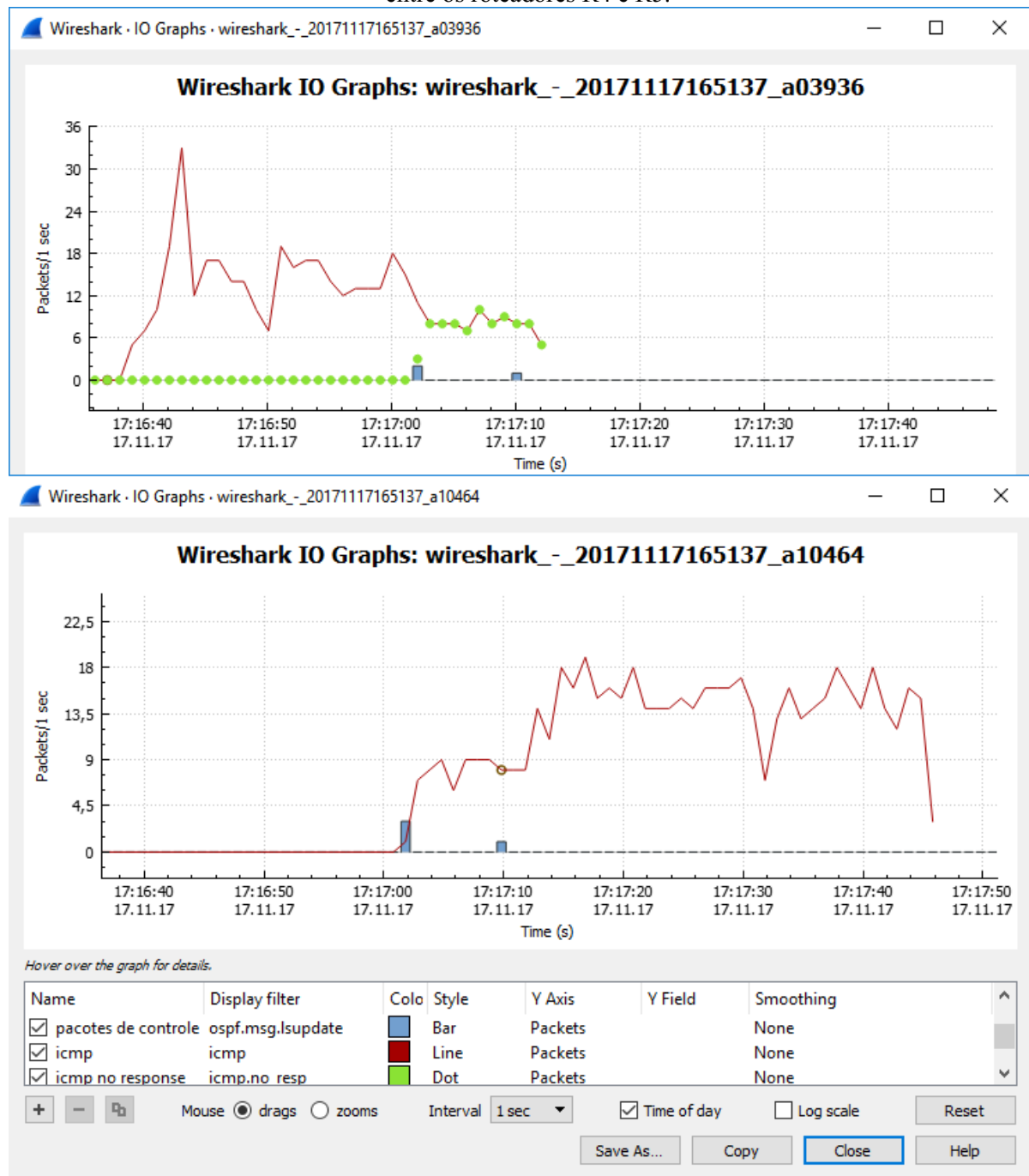


Fonte: *Print screen* da janela I/O graph (software Wireshark).

Considerando o enlace com velocidade de transmissão limitada, o RIP não altera a rota, ou seja, uma vez que a menor rota é estabelecida o protocolo enviará os dados apenas por ela. Os pacotes atrasaram cada vez mais à medida que a velocidade do enlace foi restringida. Não houve perda de pacotes porque os mesmos ficaram armazenados no buffer do roteador. Desde que o tempo de entrega do pacote não ultrapasse o tempo de vida dele, este

pacote não será perdido, sofrerá apenas atraso. O resultado obtido na simulação foi o esperado porque o parâmetro de avaliação do RIP considera apenas a menor quantidade de saltos para o envio dos pacotes de dados.

Figura 30 - Utilização do OSPF (a) Tráfego de dados entre os roteadores R5 e R6 (b) Tráfego de dados entre os roteadores R4 e R5.



Fonte: Print screen da janela I/O graph (software Wireshark).

No gráfico ilustrado na Figura 30 (a) tem-se o resultado obtido do tráfego no enlace de menor caminho R6 – R5, enquanto que na Figura 30 (b) tem-se o resultado obtido do tráfego no enlace de maior caminho R4 – R5. Em ambos os gráficos pode-se observar as mensagens de *link state update* do OSPF. A primeira mensagem foi gerada quando a interface do roteador R6 foi limitada e a segunda mensagem quando a outra interface do roteador R6 foi limitada em 100kbps. Entre as mensagens de *link state update* existem alguns pontos que são de pacotes ICMP sem resposta, ou seja, os pacotes foram enviados, mas não retornaram. Quando se restringiu o enlace, o OSPF apesar de encontrar a limitação entre R6 – R5 ainda enviou os pacotes do Ostinato para o PC2 neste caminho. Porém quando o PC2 retorna a resposta, o roteador R5 detecta que o caminho para R6 apresenta baixa velocidade e está congestionado. Então o protocolo indica o caminho para R4 como a melhor rota. Por este motivo, os pacotes capturados no enlace R6 – R5 não possuem retorno.

Observou-se ainda que entre as duas mensagens de *link state update* o tráfego caiu pela metade. Isso acontece porque metade do tráfego está indo por uma rota e a outra metade está voltando pela outra rota.

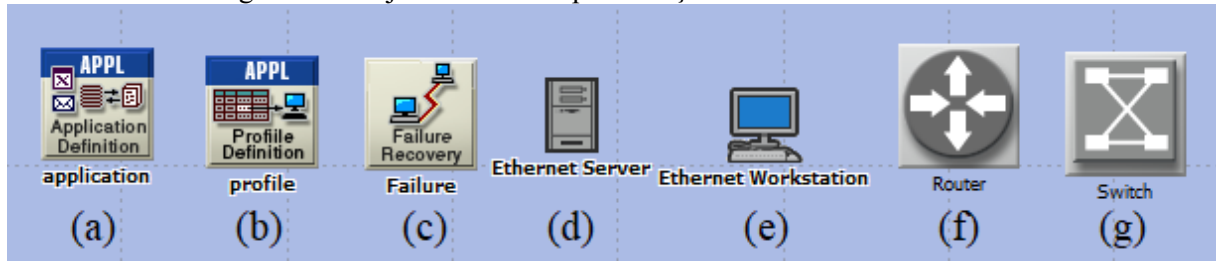
Observando os resultados obtidos conclui-se que quando há alteração na velocidade do enlace o protocolo OSPF indica uma nova rota diminuindo o atraso de resposta sem ocasionar perda de pacotes.

3.5 Cenários de simulação no opnet

O OPNET é um software desenvolvido pela OPNET Technologies utilizado para realizar modelagem de redes de computadores. Ele é utilizado em aulas básicas e avançado de redes de computadores e, em empresas para simular suas redes reais para identificar problemas que possam surgir caso seja feita alteração na rede [16]. Este software funciona de uma maneira muito diferente do GNS3, pois esse segundo é um emulador de rede que utiliza a IOS de cada roteador e, em cada equipamento devem ser configurados os parâmetros como um roteador real. Já o primeiro é um simulador que precisa apenas dos modelos dos equipamentos, tipo do enlace e o protocolo de roteamento. Não é necessário configurar IP's em interfaces, ativá-las ou configurar os protocolos. Esta simplicidade proporciona um custo computacional pequeno tornando viável a expansão do tamanho da rede e a realização de uma quantidade maior de testes. Outra diferença entre eles é que o OPNET não precisa de um *software* externo para capturar os pacotes porque ele exibe os resultados na forma gráfica [16].

Mantendo a mesma topologia feita no GNS3, mas fez-se a inserção de tráfego FTP (*File Transfer Protocol*), vídeo e VoIP (*Voz sobre IP*) utilizando algumas toolbox ilustradas na Figura 31 e descritas a seguir.

Figura 31 - Objetos utilizados para criação de uma rede no OPNET.



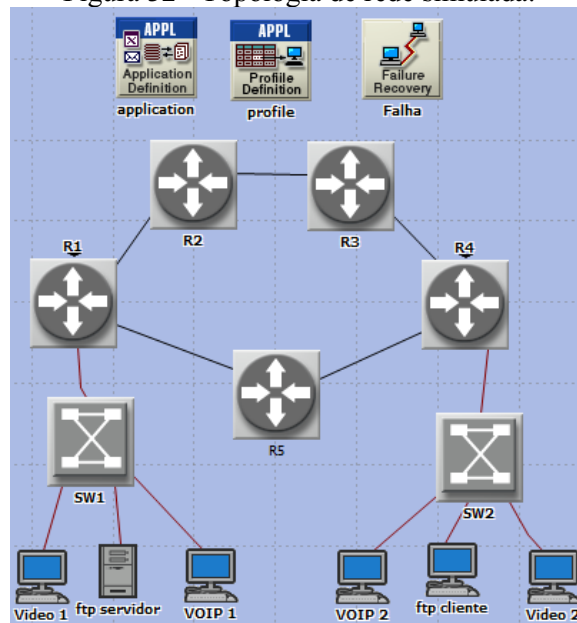
Fonte: *Print screen* da área de trabalho (software OPNET).

- (a) *Application* – neste bloco configura-se as aplicações de FTP, Vídeo e VoIP;
- (b) *Profile* – escolha do tempo para que a aplicação comece a ser executada, do tempo para interromper a aplicação e se deseja ou não repetir a aplicação durante uma mesma simulação. Na simulação proposta, todas as aplicações foram iniciadas no início simulação e permaneceram ativas até o final;
- (c) *Failure recovery* – responsável por inserir falha e recuperação entre os enlaces da rede;
- (d) *Ethernet server* – funciona como um servidor ethernet e será usado como um servidor FTP para enviar os dados para o cliente;
- (e) *Ethernet workstation* – comportamento de um computador na rede que envia e recebe dados. Na simulação proposta configurou-se duas *toolbox* para *streaming* de vídeo, duas para o tráfego VoIP e uma outra para um cliente FTP;
- (f) *Router* – roteadores da rede;
- (g) *Switch* – switches adicionados à rede com a finalidade de colocar todas as aplicações de tráfego diretamente em uma mesma interface de roteador.

Após o aprendizado da funcionalidade de cada uma das ferramentas montou-se a topologia da rede a ser simulada que é ilustrada na Figura 32.

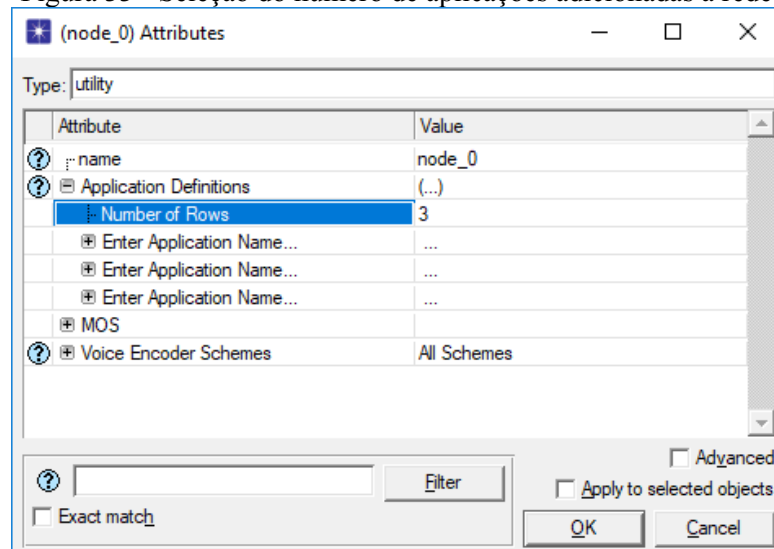
Foram escolhidas três aplicações FTP, vídeo e VoIP. Clicando com o botão direito na ferramenta “*Application*” selecione a opção “*Edit Attributes*”. Uma nova janela é aberta com a opção “*Application Definitions*” e o submenu “*Number of Rows*” selecionou-se o valor 3 como ilustrado na Figura 33.

Figura 32 - Topologia de rede simulada.



Fonte: *Print screen* da área de trabalho (software OPNET).

Figura 33 - Seleção do número de aplicações adicionadas à rede.

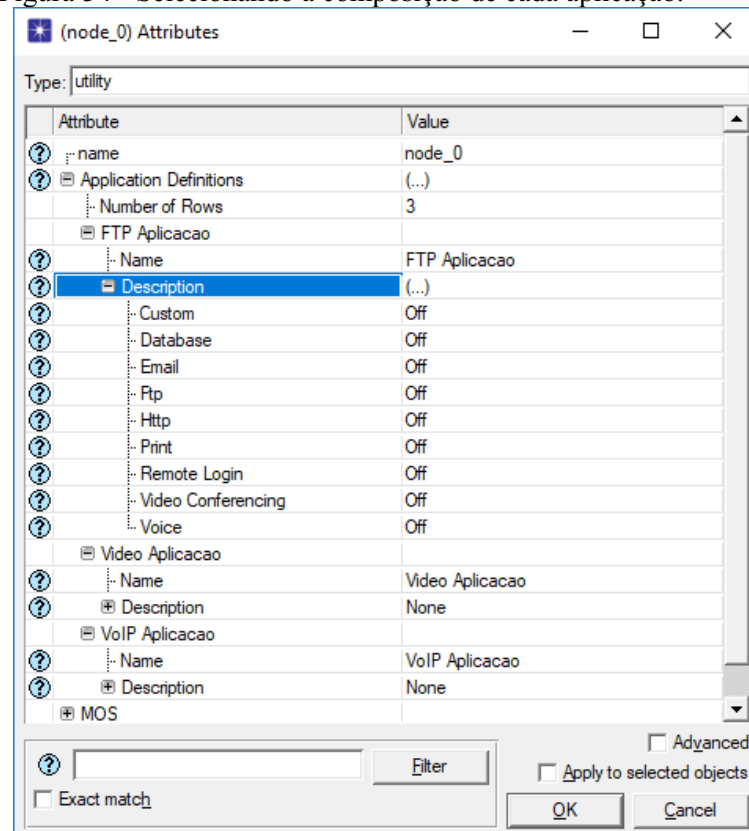


Fonte: *Print screen* da janela de configuração de aplicações (software OPNET).

Na opção “*Enter Application Name*” tem-se o campo “*Name*” para indicar o nome de cada aplicação ilustrado na Figura 34. Já no campo “*Description*” tem-se um menu formado por uma sequência de aplicações suportadas. As escolhas foram Ftp para a “*FTP Aplicacao*”, Video Conferencing para “*Video Aplicacao*” e Voice para “*VoIP Aplicacao*”.

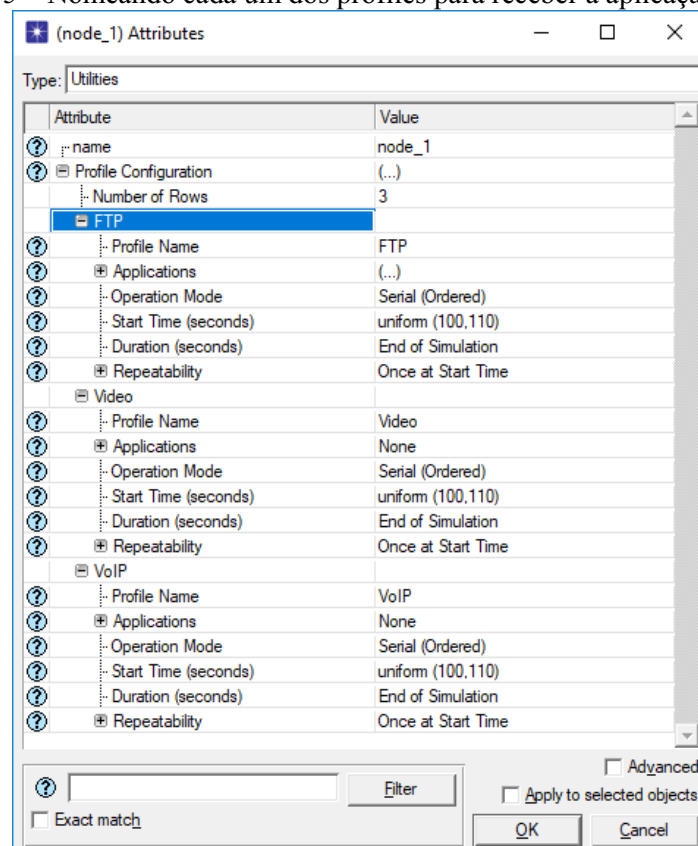
Para configurar o *Profile* clicou-se na opção “*Edit Attributes*” depois em “*Profile Configuration*” e alterou-se o “*Number of Rows*” para 3. Cada uma das guias do “*Enter Profile Name*” recebeu o nome de cada uma das aplicações novamente. Esse procedimento foi ilustrado na Figura 35.

Figura 34 - Selecionando a composição de cada aplicação.



Fonte: Print screen da janela de configuração de profile (software OPNET).

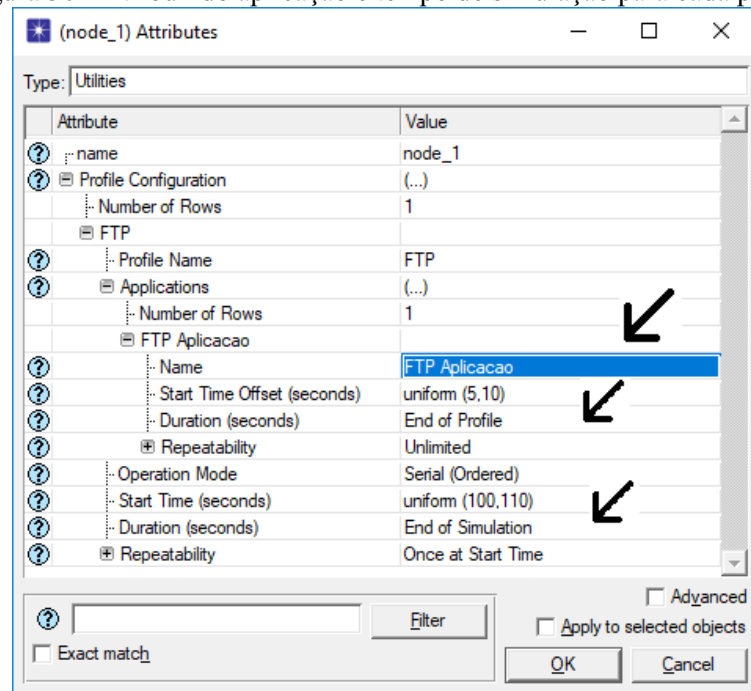
Figura 35 – Nomeando cada um dos profiles para receber a aplicação.



Fonte: Print screen da janela de configuração de profile (software OPNET).

Na aba “*Applications*” de cada um dos *profiles* estabeleceu-se “*Number of Rows*” igual a 1. Então uma nova aba é aberta para selecionar o nome da aplicação. Neste caso, escolhe-se a aplicação que foi criada e escolheu-se a opção “*End of Profile*” na primeira opção “*Duration (seconds)*” e na segunda opção “*End of Simulation*” conforme ilustrado na Figura 36.

Figura 36 - Atribuindo aplicação e tempo de simulação para cada profile.



Fonte: Print screen da janela de configuração de profile (software OPNET).

Quadro 1 - Tempo de falha e recuperação dos links durante a simulação.

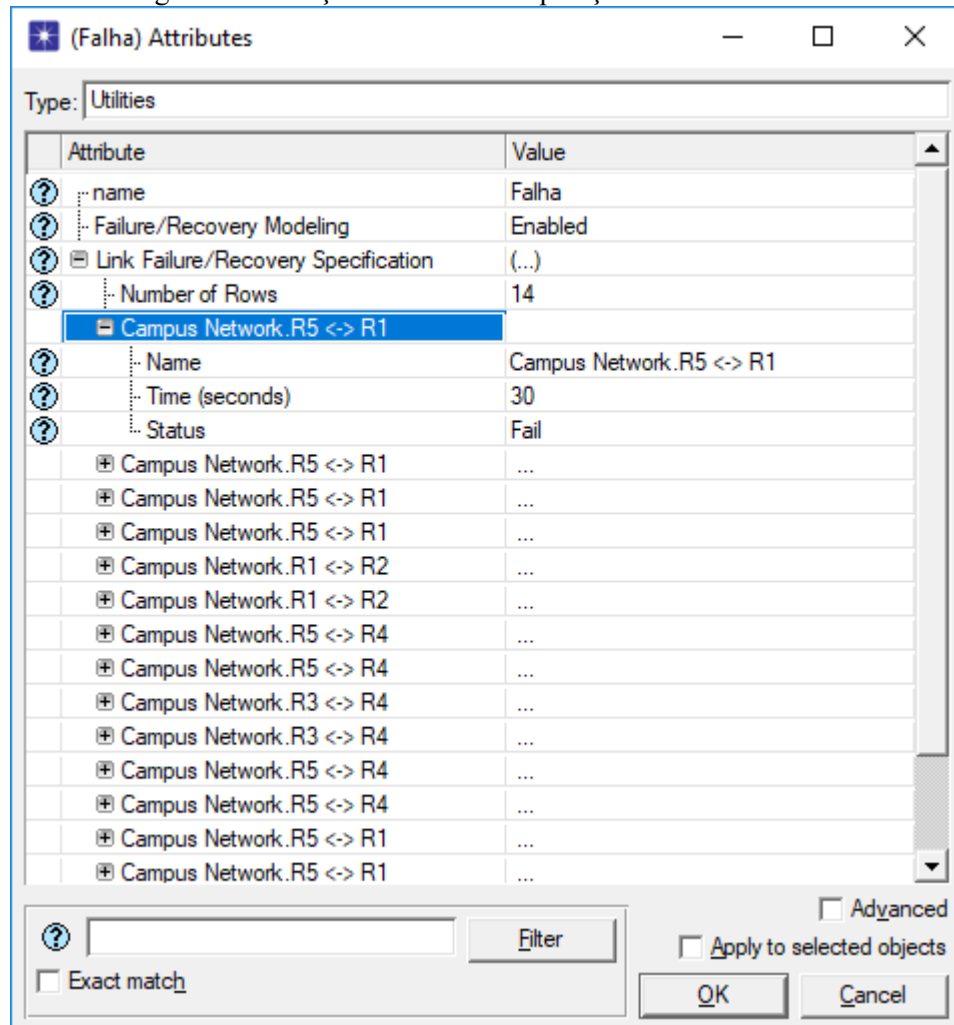
Link	Status	Time
R5 – R1	<i>Fail</i>	30
R5 – R1	<i>Recovery</i>	60
R5 – R1	<i>Fail</i>	90
R5 – R1	<i>Recovery</i>	120
R1 – R2	<i>Fail</i>	150
R1 – R2	<i>Recovery</i>	180
R5 – R4	<i>Fail</i>	190
R5 – R4	<i>Recovery</i>	200
R3 – R4	<i>Fail</i>	240
R3 – R4	<i>Recovery</i>	255
R5 – R4	<i>Fail</i>	260
R5 – R4	<i>Recovery</i>	280
R5 – R1	<i>Fail</i>	570
R5 – R1	<i>Recovery</i>	600

Fonte: O autor.

Para configurar a falha e a recuperação da rede ativou-se a ferramenta “*Failure Recovery*”. Clicando em “*Link Failure/Recovery Specification*” e “*Number of Rows*” igual a

14. A configuração de falhas e recuperações seguiu as especificações apresentadas no Quadro 01. Abriu-se cada um dos campos e escolheu-se o enlace, o tempo e o status como ilustrado na Figura 37.

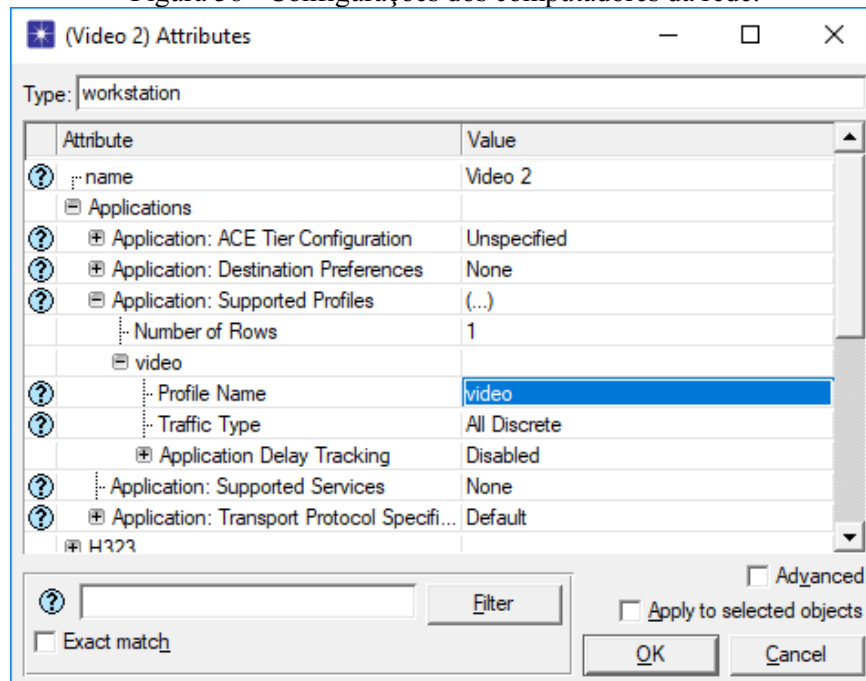
Figura 37- Inserção de falha e recuperação nos links da rede.



Fonte: Print screen da janela de configuração de falhas (software OPNET).

A configuração de todos os computadores da rede que são Video1, Video2, Voip1, Voip2 e FTP cliente são feitos da seguinte maneira: com o botão direito no item desejado “Edit Attributes” e a opção “Application: Suported Profiles” estabeleça *Number of Rows* igual a 1. No campo “Profile Name” coloque o nome do perfil desejado. A Figura 38 ilustra o exemplo da configuração do Video2.

Figura 38 - Configurações dos computadores da rede.



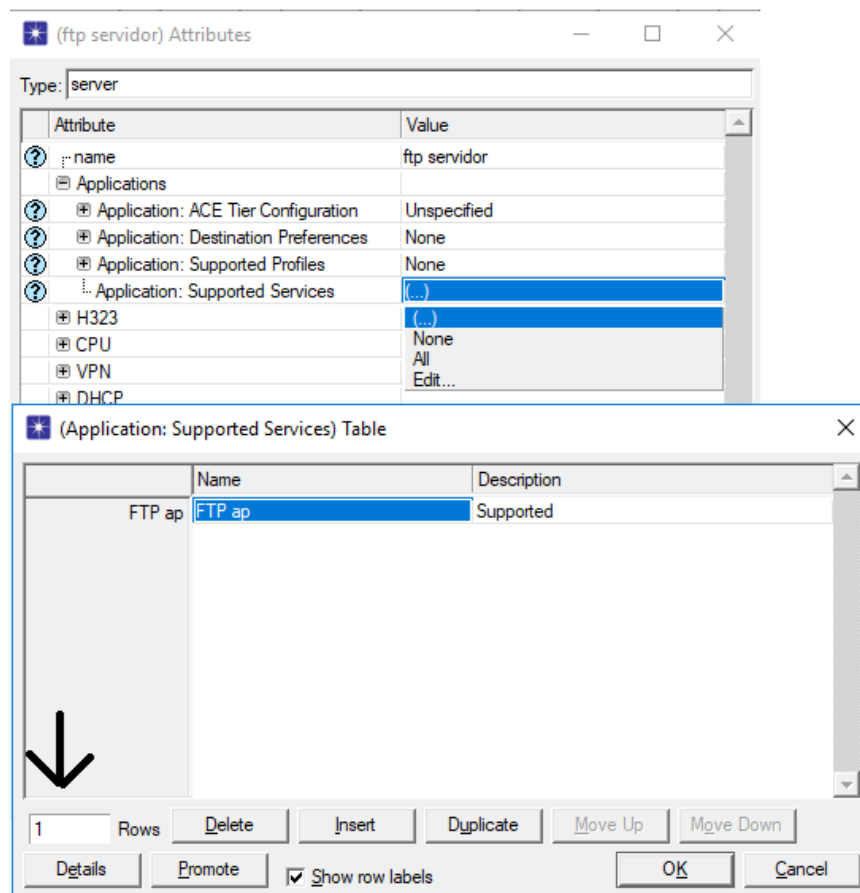
Fonte: Print screen da janela de configuração do Ethernet Workstation (software OPNET).

A configuração do *FTP server* opção “*Edit Attributes*” clique em “*Application: Supported Services*” opção *Edit*. Adicionou-se 1 no campo “*Rows*” conforme ilustrado na Figura 39.

Os switches não necessitam de configuração alguma, somente a inserção deles na rede e ligação dos enlaces. Já nos roteadores escolheu-se o protocolo de roteamento utilizado na rede conforme os passos ilustrados na Figura 40. Após clicar em *Configure Routing Protocols* abrirá uma nova janela contendo as opções de protocolo de roteamento disponíveis e deve-se escolher o RIP. Para fazer a rede com o protocolo OSPF, simplesmente duplica-se o cenário e altera o protocolo de roteamento para OSPF. Para duplicar o cenário vá em “*Scenarios*” e selecione a opção “*Duplicate Scenario*”.

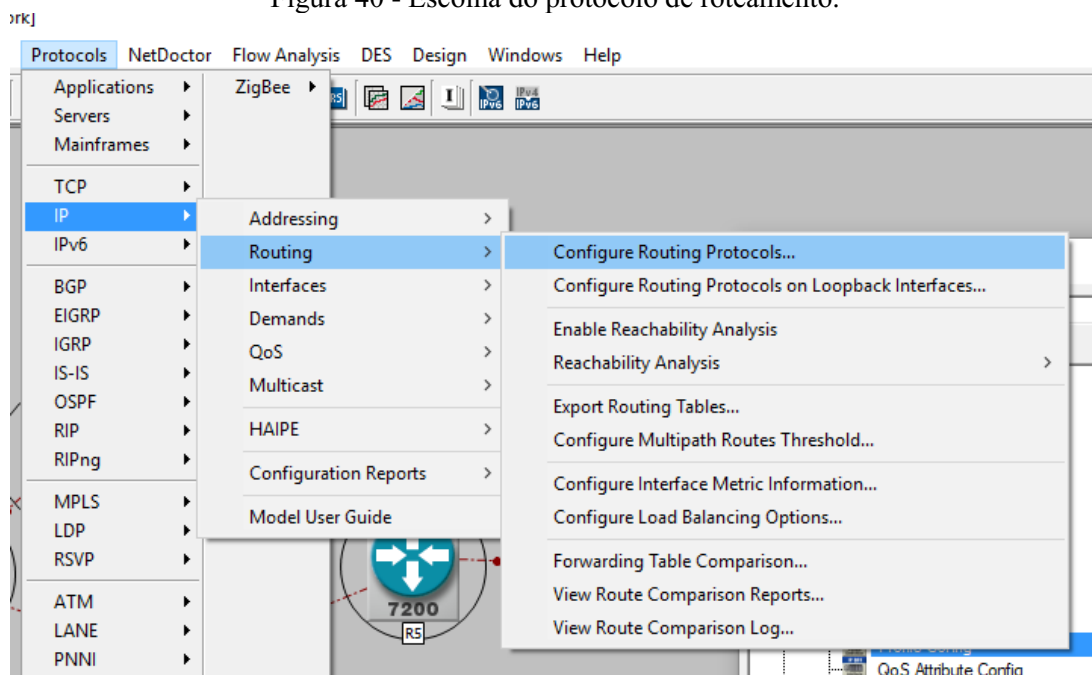
O tempo de simulação foi 15 minutos para a análise do comportamento da rede utilizando os protocolos RIP e OSPF. Ao final, serão gerados os gráficos indicando o tempo médio de resposta do FTP, o tempo médio de transmissão dos pacotes de vídeo fim a fim, o tempo médio de transmissão dos pacotes de voz fim a fim, a média de pacotes perdidos e o tempo de convergência.

Figura 39 - Configuração do FTP server.



Fonte: Print screen da janela de configuração do FTP Server (software OPNET).

Figura 40 - Escolha do protocolo de roteamento.

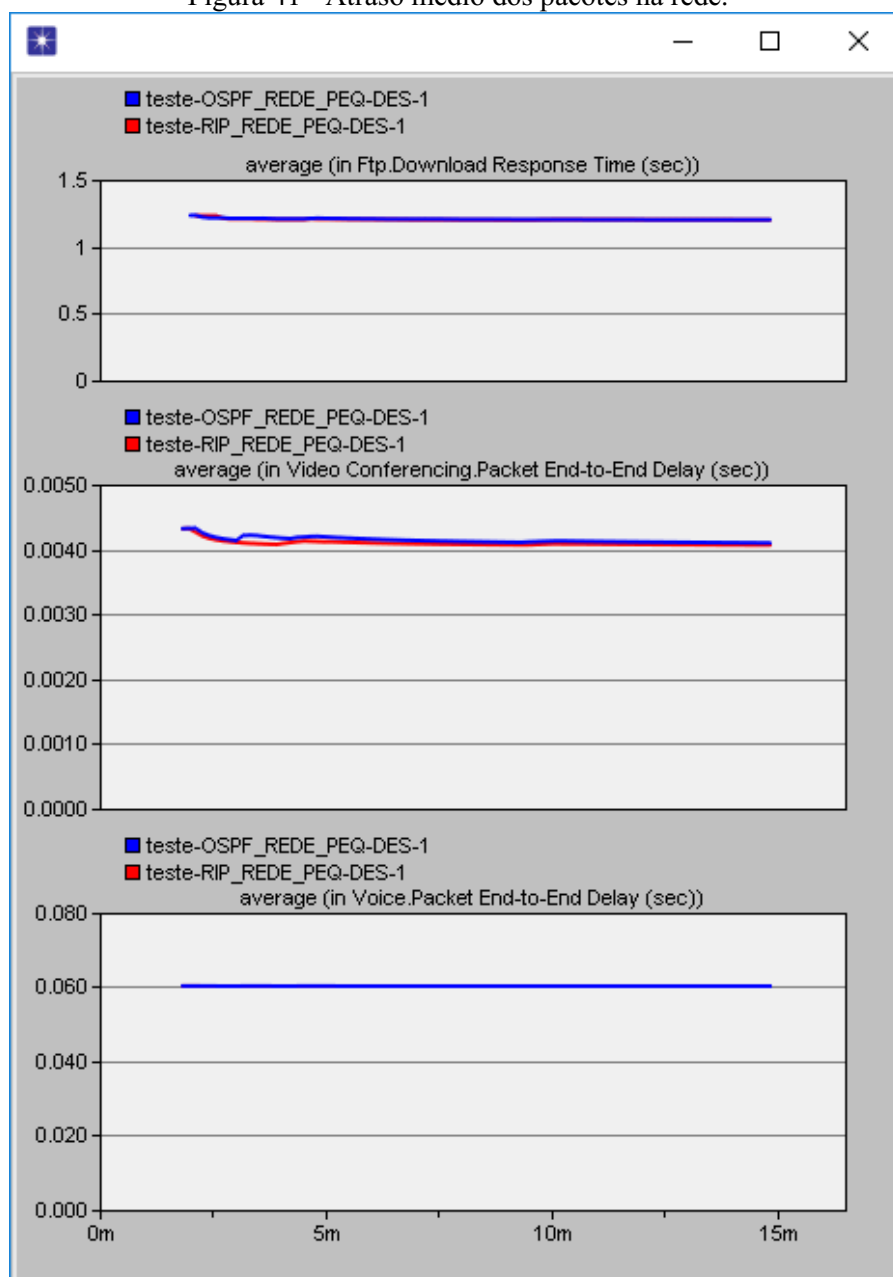


Fonte: Print screen da janela de configuração de roteamento (software OPNET).

3.5.1 Resultados obtidos

Utilizando o a topologia mostrada na figura 32 realizamos as configurações descritas acima e simulamos. A Figura 41 ilustra o gráfico do atraso da rede, tempo que os pacotes levam para ir da fonte até o destino passando por toda a rede. Observou-se que os protocolos possuem respostas muito idênticas, onde a média de atraso da rede independente se a aplicação era FTP, VoIP ou Vídeo se mantiveram praticamente idênticas entre os dois protocolos.

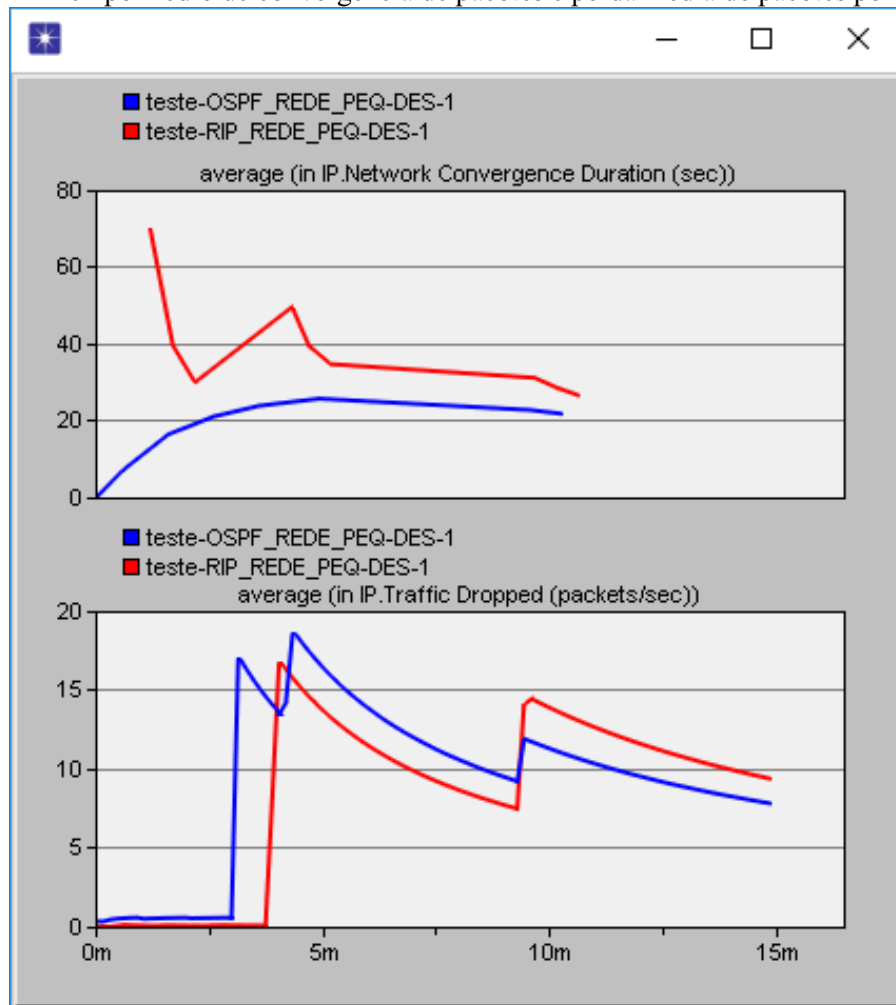
Figura 41 - Atraso médio dos pacotes na rede.



Fonte: *Print screen* da janela de gráficos de simulação (software OPNET).

Observando os gráficos ilustrados na Figura 42 avaliou-se o tempo de convergência médio de cada um dos protocolos. Notou-se que a diferença é grande para o OSPF em relação ao RIP. Note que o tempo convergência do OSPF é mais rápido e não varia tanto, já o tempo de convergência do RIP apesar de diminuir com o passar do tempo, sofre muitas variações quando ocorrem as falhas na rede. Em relação à média de pacotes perdidos, a quantidade de pacotes perdidos em ambos os protocolos também são bem parecidos, onde nenhum dos protocolos conseguiu apresentar uma maior eficiência para não perder pacotes.

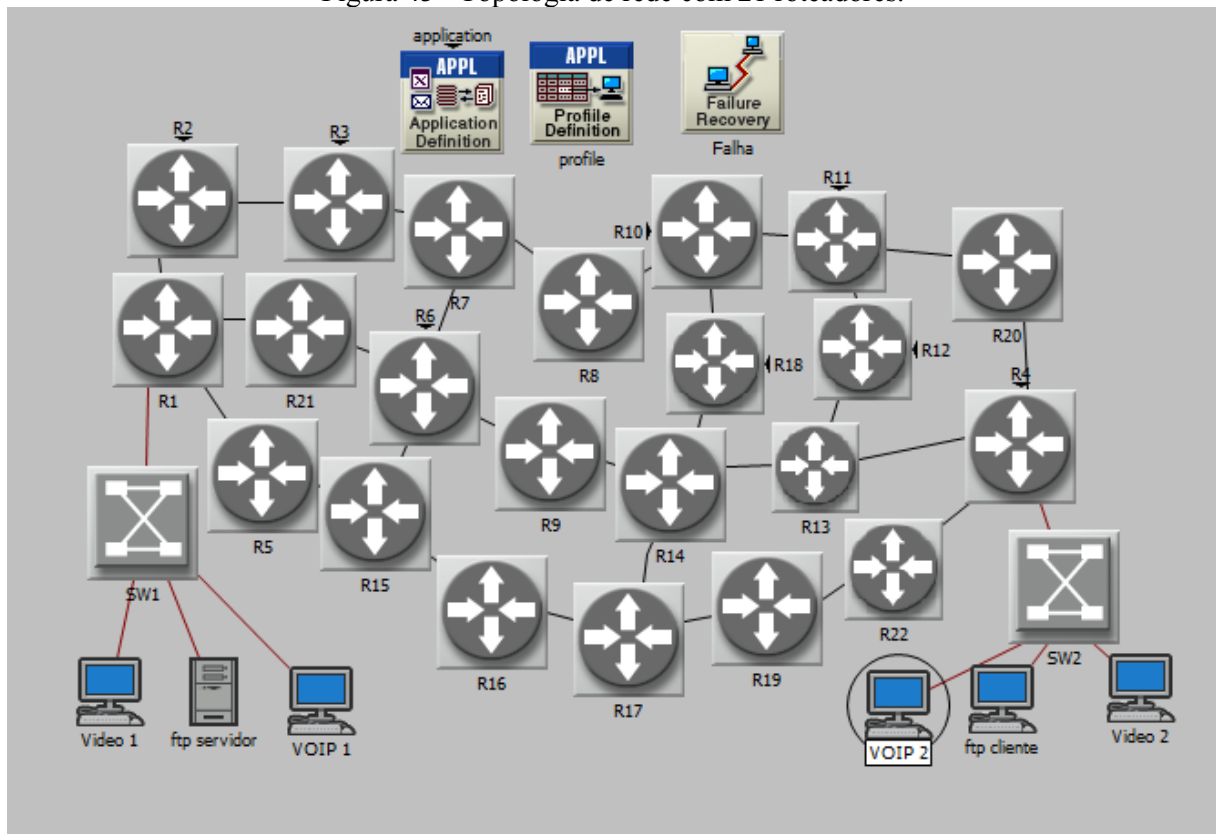
Figura 42 - Tempo médio de convergência de pacotes e perda média de pacotes por segundo.



Fonte: *Print screen* da janela de gráficos de simulação (software OPNET).

Baseado nos resultados apresentados, os protocolos RIP e OSPF possuem respostas muito parecidas quando se trata de uma rede pequena. Por isso, propõe-se um segundo cenário com 21 roteadores para o estudo da diferença entre os protocolos de roteamento conforme mostrado na figura xx abaixo.

Figura 43 - Topologia de rede com 21 roteadores.



Fonte: *Print screen* da topologia montada (software OPNET).

O tempo simulado será mantido em 15 minutos e também foram inseridas falhas e recuperações nos enlaces conforme apresentado no Quadro 2.

Quadro 2 - Tempos de falha e recuperação dos links.

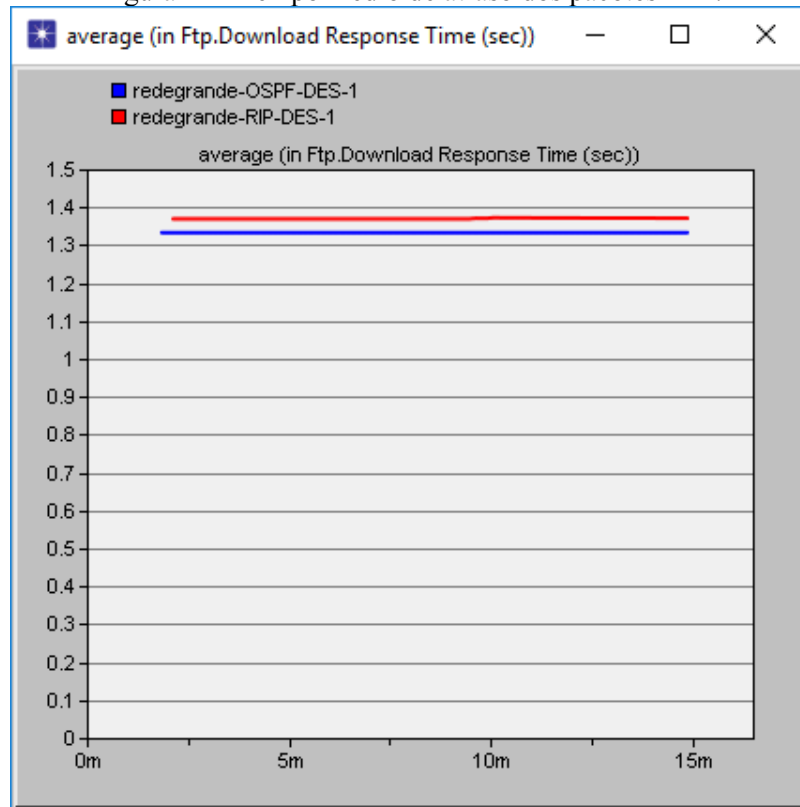
Link	Status	Time
R5 – R1	Fail	30
R5 – R1	Recovery	60
R5 – R1	Fail	90
R5 – R1	Recovery	120
R1 – R2	Fail	150
R1 – R2	Recovery	180
R1 – R2	Fail	190
R7 – R3	Fail	200
R7 – R3	Recovery	240
R1 – R2	Recovery	255
R2 – R3	Fail	400
R2 – R3	Recovery	430
R5 – R15	Fail	570
R5 – R15	Recovery	600

Fonte: O autor.

Comparando os gráficos obtidos para a nova rede notou-se que o atraso nas aplicações FTP e de vídeo é diferente, onde o RIP apresenta atraso maior para chegar ao destino do que o

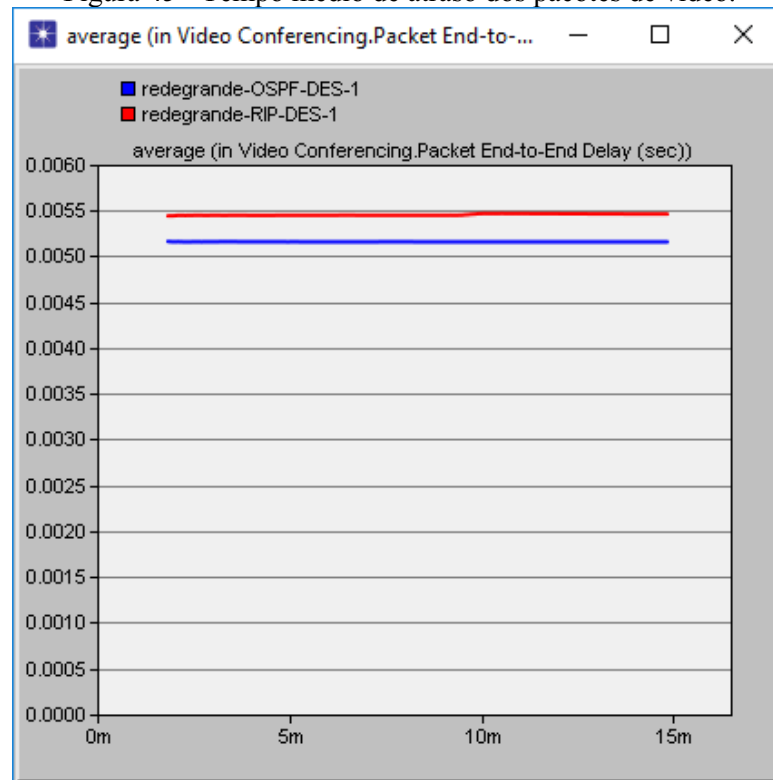
protocolo OSPF ilustrados nas Figuras 43 e 44. Para a aplicação de VoIP observou-se que os dois protocolos conseguem manter o mesmo atraso como ilustrado na Figura 45.

Figura 44 - Tempo médio de atraso dos pacotes FTP.



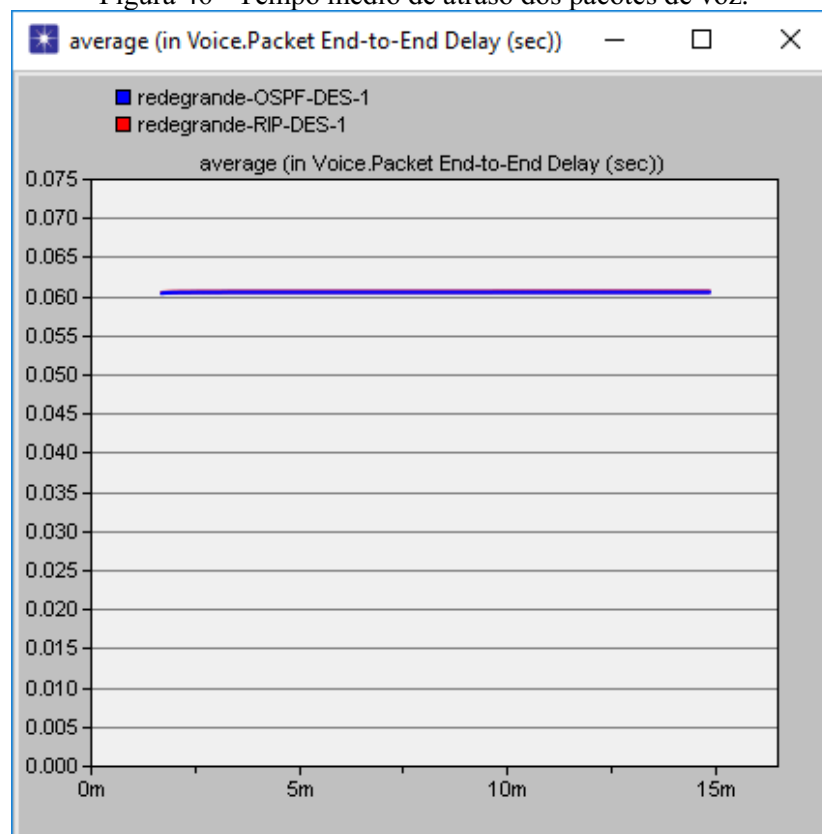
Fonte: *Print screen* da janela de gráficos de simulação (software OPNET).

Figura 45 - Tempo médio de atraso dos pacotes de vídeo.



Fonte: *Print screen* da janela de gráficos de simulação (software OPNET).

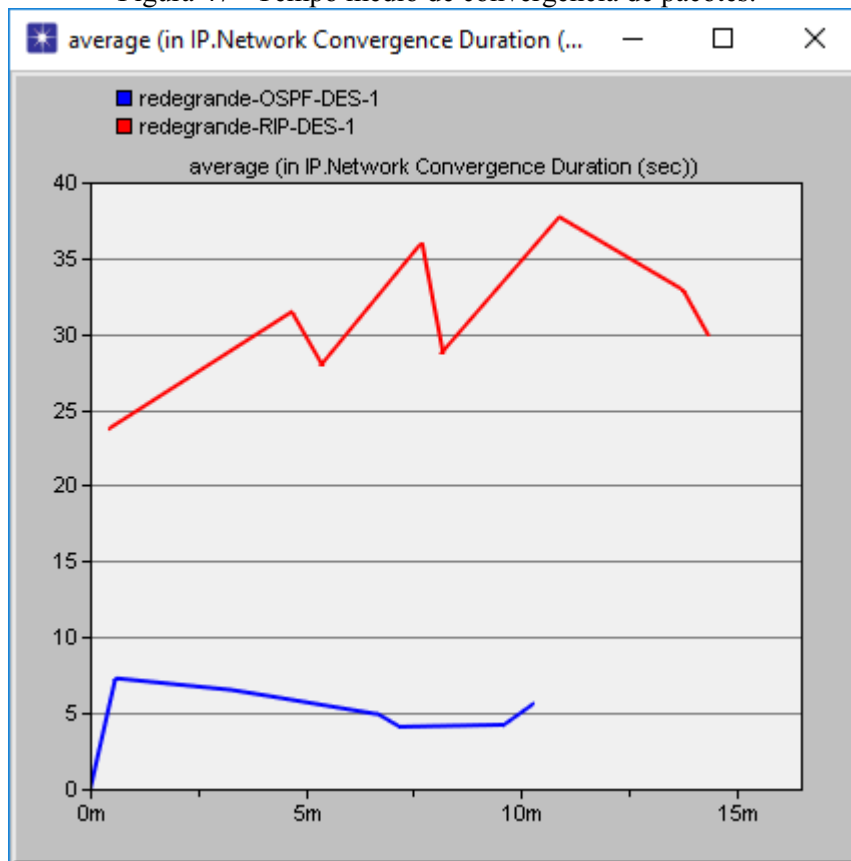
Figura 46 - Tempo médio de atraso dos pacotes de voz.



Fonte: *Print screen* da janela de gráficos de simulação (software OPNET).

O gráfico da duração de tempo de convergência é ilustrado na Figura 46. Em relação ao tempo médio de convergência, o aumento do tamanho da rede apresentou muita diferença. O protocolo RIP demorou um tempo maior para convergir enquanto que o protocolo OSPF diminuiu o tempo de convergência.

Figura 47 - Tempo médio de convergência de pacotes.

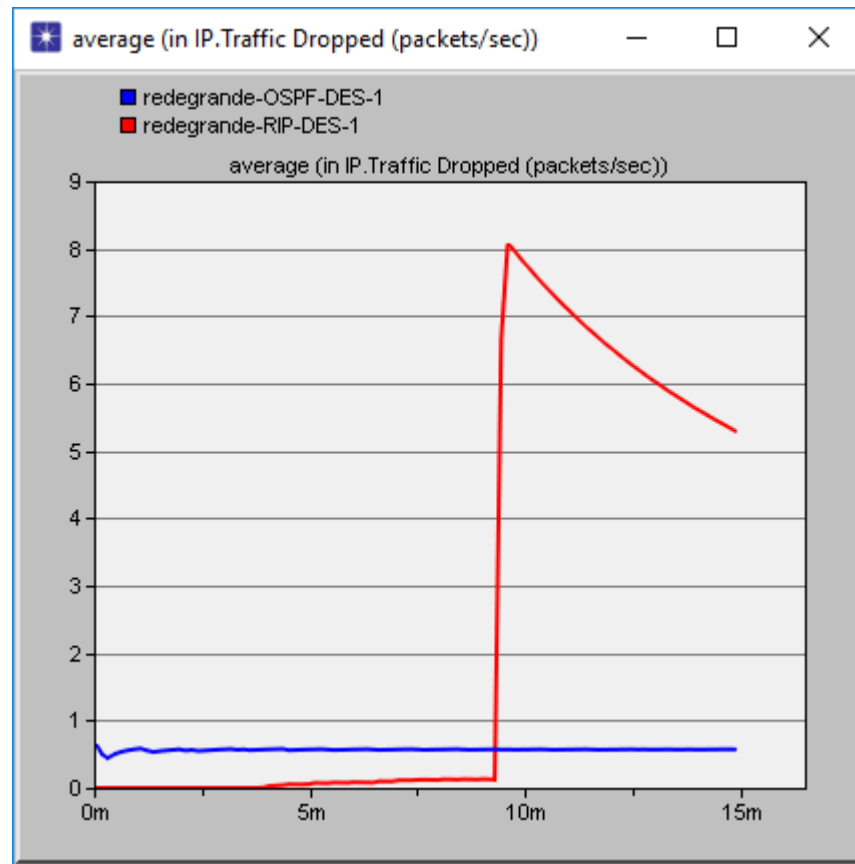


Fonte: *Print screen* da janela de gráficos de simulação (software OPNET).

A Figura 47 ilustra o gráfico resultante da perda de pacotes. O OSPF mantém uma média muito baixa de perdas enquanto que o RIP inicia sem perdas e com o passar do tempo devido às falhas da rede o protocolo passa a perder muitos pacotes.

O Quadro 3 apresenta um resumo comparativo dos protocolos avaliados no cenários de simulação proposto neste trabalho de conclusão de curso. Os resultados aqui apresentados não foram validados para outros cenários.

Figura 48 - Perda média de pacotes por segundo.



Fonte: *Print screen* da janela de gráficos de simulação (software OPNET).

Quadro 3 - Comparação dos resultados.

Parâmetro de desempenho	REDE PEQUENA	REDE GRANDE
Menor Tempo de Convergência	OSPF	OSPF
Maior Perda de Pacotes	Aproximadamente mesma perda em ambos	RIP
Maior Atraso FTP	Aproximadamente mesmo atraso	RIP
Maior Atraso Vídeo	Aproximadamente mesmo atraso	RIP
Maior Atraso VoIP	Aproximadamente mesmo atraso	Aproximadamente mesmo atraso

Fonte: O autor.

CAPÍTULO 4

CONCLUSÕES GERAIS

Por meio deste estudo, foi possível entender como funcionam os protocolos de roteamento RIP e OSPF. Utilizando o GNS3, foi possível configurar os roteadores e aplicar os protocolos na rede, de forma semelhante ao que seria feito em um roteador real. Além disso, a captura dos pacotes utilizando o Wireshark ajudou a entender qual a rota escolhida pelo roteador diante das adversidades ocasionadas na topologia da rede. Notou-se que para o protocolo RIP, não importa se o enlace está limitado ou não, ele sempre enviará os pacotes pelo caminho mais curto. Em relação ao OSPF observou-se que caso o enlace tenha uma limitação, o tráfego é transferido para uma rota alternativa para que se obtenha maior rendimento.

O OPNET ofereceu mais recursos para explorar o comportamento dos protocolos. Realizou-se testes utilizando três tipos de aplicações diferentes vídeo, VoIP e FTP. Além disso, inseriram-se falhas nos enlaces para avaliar qual protocolo iria apresentar desempenho melhor. Após a análise dos resultados obtidos concluiu-se que para redes de pequeno porte, a escolha do protocolo de roteamento RIP ou OSPF não trará impacto na perda de pacotes e no atraso das diversas aplicações. Entretanto quando se trata de uma rede maior, o OSPF apresenta desempenho superior em relação ao RIP e por este motivo a escolha do OSPF seria a mais adequada.

Se tratando de redes de computadores observa-se um cenário crescente de usuários acessando a rede com mais velocidade de navegação para assistir *streaming* de vídeos e descarregar arquivos da internet. Isto impacta na estrutura da rede, fazendo com que ela torne-se cada vez maior e com um tempo de resposta mais rápido. Por este motivo, a grande maioria das redes são configuradas utilizando o protocolo OSPF ao invés do RIP, pois pequenas diferenças quando elevadas a grandes escalas se tornam problemáticas para a empresa administradora da rede.

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] TANEMBAUM, A.S.; WETHERALL, D. **Redes de Computadores**. 5 ed. São Paulo: Pearson Prentice Hall, 2011.
- [2] GOOGLE, **Public Data**. Disponível em: <https://www.google.com.br/publicdata/explore?ds=d5bncppjof8f9_&met_y=it_net_user_p2&idim=country:BRA:USA:CAN&hl=pt&dl=pt#!ctype=1&strail=false&bcs=d&nselm=h&met_y=it_net_user_p2&scale_y=lin&ind_y=false&rdim=region&idim=country:BRA:USA:CAN&ifdim=region&hl=pt&dl=pt&ind=false> Acesso em: 04 de abril de 2017.
- [3] KUROSE, J. F. **Redes de Computadores e a Internet**. 5 ed. São Paulo: Addison Wesley, 2010.
- [4] PETERSON, L. L.; DAVIE, B. S. **Redes de computadores: Uma Abordagem de Sistemas**. 5ed Rio de Janeiro: Elsevier, 2013.
- [5] CISCOPRESS, **Cisco Networking Academy's Introduction to Routing Dynamically**. Disponível em: < <http://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=5>> Acesso em: 15 de junho de 2017.
- [6] TOOLS IETF, **RFC 2328 – OSPF Version 2**. Disponível em: < <https://tools.ietf.org/pdf/rfc2328.pdf> > Acesso em: 16 de junho de 2017.
- [7] TOOLS IETF, **RFC 2453 – RIP Version 2**. Disponível em: < <https://tools.ietf.org/pdf/rfc2453.pdf> > Acesso em: 16 de junho de 2017.
- [8] EXPLORE DOCUMENTATION, **The oficial guide and reference for GNS3**. Disponível em: < <https://docs.gns3.com/1FFbs5hOBbx8O855KxLetlCwlbyTN8L1zXXQzCqfmy4/index.html> > Acesso em: 20 de junho de 2017.
- [9] OSTINATO, **Network Traffic Generator and Analyzer**. Disponível em < www.ostinato.org/ > Acesso em 15 de julho 2017.
- [10] GNS3, **Appliances**. Disponível em < <https://www.gns3.com/marketplace/appliances> > Acesso em 03 de agosto de 2017.
- [11] GNS3, **Gns3-gui**. Disponível em < <https://github.com/GNS3/gns3-gui/releases> > Acesso em 08 de agosto de 2017.
- [12] GNS3, **GNS3 Setup Wizard with the GNS3 VM**. Disponível em < <http://docs.gns3.com/1wdfvS-OlFfOf7HWZoSXMbG58C4pMSy7vKJFiKKVResc/> > Acesso em 22 de agosto de 2017.
- [13] OSTINATO, **quickstart**. Disponível em < <https://userguide.ostinato.org/Quickstart.html> > Acesso em 05 de agosto de 2017.
- [14] WIRESHARK, **About Wireshark**. Disponível em < <https://www.wireshark.org/> > Acesso em 16 de agosto de 2017.
- [15] WIRESHARK, **Learn Wireshark**. Disponível em < <https://www.wireshark.org/#learnWS> > Acesso em 16 de agosto de 2017.
- [16] SETHI, A.S.; HNATYSHIN, V.Y. **OPNET User Guide for Computer Network Simulation**. Broken Sound Parkway NW, CRC Press, 2013.