UniAcademia – Centro Universitário
Curso de Bacharelado em Sistemas de Informação
Trabalho de Conclusão de Curso – Artigo

ANÁLISE DO MPLS PARA A CONSTRUÇÃO DE VPNS ATRAVÉS DO GNS3

José Flávio de Assis Júnior[1]
UniAcademia, Juiz de Fora, MG
Romualdo Monteiro de Resende Costa[2]
UniAcademia, Juiz de Fora, MG

Linha de Pesquisa: Redes de Computadores e Sistemas Distribuídos

RESUMO

O MPLS (*Multiprotocol Label Switching*) é um protocolo comumente utilizado em circuitos de telecomunicação, pois realiza o transporte dos pacotes no *backbone* pela técnica de comutação por rótulos, cria circuitos virtuais e define múltiplos caminhos para um mesmo destino, permitindo uma melhor distribuição do tráfego pelas rotas alternativas que uma rede *WAN* (*Wide Área Network*) normalmente oferece. A VPN (*Virtual Private Network)* é uma rede sobreposta às redes públicas, mas com a maioria das propriedades de redes privadas. A utilização da VPN permite às corporações interligarem localidades ou redes com segurança, alta disponibilidade e transparência de protocolos. Considerada a importância e a popularidade da utilização da VPN, a ferramenta *Graphical Network Simulator*-3 (GNS3) pode ser empregada para simular a construção dessas redes e monitorar o seu tráfego e roteamento. Nesse contexto, esse trabalho tem por objetivo analisar o processo de gerenciamento da rede MPLS pelo GNS3 e avaliar a possibilidade de novas soluções.

Palavras-chaves: Fibras ópticas. *MPLS. VPN. GNS3.*

1 INTRODUÇÃO

Embora diversos serviços distintos de comunicação possam ser empregados, a *Web* tornou-se a maior fonte de tráfego na Internet e permanece assim (COMER, 2015). Ela é amplamente utilizada, particularmente em várias empresas ao redor do mundo.

[1]Discente do Curso de Bacharelado em Sistemas de Informação da Universidade Academia - UniAcademia. Endereço: Rua Silva Jardim, 331. Ap. 302. Centro. Juiz de Fora – MG. Celular: (32)98422-5436. E-mail: joseflavioajr@gmail.com.
[2]Docente do Curso de Bacharelado em Sistemas de Informação do da Universidade Academia - UniAcademia. Orientador.

A utilização da *Web*, independente da tecnologia de comunicação particular escolhida, oferece diversas facilidades, como a possibilidade de emprego de ferramentas, *softwares* e aplicativos usualmente conhecidos que, no caso particular das empresas, podem prover vantagens econômicas e, consequentemente, o alcance de metas financeiras.

Em relação a solução tecnológica de comunicação, são parâmetros importantes, particularmente no ambiente empresarial, requisitos de fluxo de tráfego suficiente para a transmissão e recepção de dados, além de suporte e infraestrutura adequada. Conforme relatado por (PINHEIRO, 2017), a utilização da fibra óptica na instalação de uma rede de computadores, em lugar de soluções de cabeamento de par metálico convencional, apresenta vantagens significativas devido a capacidade da fibra de permitir o tráfego das informações com taxas elevadas. Adicionalmente, a impossibilidade de interferência magnética no meio óptico tem favorecida a instalação em ambientes inóspitos e permitida a aplicação em grandes distâncias, favorecendo, principalmente, sua aplicação em redes geograficamente distribuídas, como é o caso da Internet.

De acordo com OLIVEIRA et. al. (2012), a tecnologia MPLS (*MultiProtocol Label Switching*) é indicada para prover evolução, otimização e flexibilidade ao núcleo da rede que une vários enlaces de alta velocidade, mostrando-se como uma tecnologia emergente a ser empregada nos provedores de acesso à Internet.

Para uma eficiente utilização do MPLS, torna-se necessário uma ferramenta de monitoramento que permita analisar, classificar, coletar e registrar estatísticas de equipamentos diversos como *backbones*, roteadores de acesso e concentradores, identificando condições do sistema, uso de largura de banda, tempo de atividade, temperatura, dentre outros. O emulador *Graphical Network Simulator-3*[3] além de poupar espaço físico e tempo, contribuiu para um ambiente versátil que não obriga o uso de equipamentos físicos, assemelhando-se muito de um modelo real (MENDES, 2013) e que serão analisados ao longo deste trabalho.

Sendo assim, este trabalho tem como objetivo principal analisar a aplicação do emulador *GNS3*, detalhando procedimentos de instalação e melhores práticas de utilização com o objetivo principal de análise de redes *MPLS*. Para atingir esse objetivo, a primeira seção deste trabalho versa sobre as características e aplicação do protocolo *MPLS* e os demais a que ele se aplica. A próxima seção entra em

[3] https://gns3.com/

detalhes sobre a criação de *VPNs MPLS,* pois *e*ste protocolo permite a criação de *VPN*s garantindo um isolamento completo do tráfego com a criação de tabelas de rótulos, que são usadas para roteamento, exclusivas de cada *VPN,* permitindo acesso entre corporações, conforme será exemplificado na simulação prática.

A seguir, o capítulo 4 apresenta uma simulação prática de criação de *VPNs* pelo *GNS3* e por último, a seção 5 apresenta as conclusões e possíveis trabalhos futuros.

2 O MPLS

Nesta seção são descritas as definições do MPLS necessárias a realização deste trabalho.

2.1. Especificações e características

Na segunda metade da década de 1990, a tecnologia *Asynchronous Transfer Mode* (ATM), embora ainda com preço elevado e protocolo complexo em planos e camadas já era a tecnologia dominante para a construção de *backbones* (TANENBAUM, 2003). OLIVEIRA et. al. (2012) ressaltam que já se sabia que a pilha de protocolos TCP/IP (*Transmission Control Protocol / Internet Protocol*) era um padrão mundial e que todas as tecnologias que fossem desenvolvidas a partir de então deveriam ser compatíveis com esses protocolos. No entanto, a natureza da tecnologia ATM, com células de tamanho fixo e qualidade de serviço intrínseca, difere totalmente da natureza do protocolo IP.

Os mesmos autores relatam que na mesma década surgiram pesquisas inicialmente chamadas de “comutação IP”, pois alguns fabricantes entendiam que pacotes IPs não precisavam ser roteados nos núcleos da rede e que era possível adquirir a qualidade de serviço de redes ATM por meio da comutação de pacotes IPs, a qual seria realizada por rótulos adicionados a cada pacote. Então, algumas empresas começaram a desenvolver tecnologias baseadas na utilização de rótulos, mas devido à incapacidade de interação entre essas tecnologias desenvolvidas foi criado em dezembro de 1996 um grupo de trabalho visando à padronização dessas tecnologias.

Lucek e Minei (2005) descrevem que o MPLS é uma tecnologia desenvolvida no âmbito do *IETF* (*Internet Engineering Task Force*)[4] inicialmente como uma tentativa de padronizar a comutação de pacotes baseada na troca de rótulos e, com isso, melhorar a eficiência de fluxos de tráfegos através da rede, modificando um paradigma fundamental até então existente nas redes *IPs* com a inserção de um rótulo ao datagrama, propiciando assim a comutação *IP*.

Tanenbaum (2003) ressalva a utilização do *MPLS* como meio de permitir o roteamento rápido e oferecer qualidade de serviço, diferenciando o modo como a Internet trata a construção de rotas e o modo como a construção de rotas é tratada nas redes orientadas a conexões, o que torna a técnica de comutação de circuitos tradicional inadequada.

O autor detalha as distinções entre roteamento, que é o processo que consiste em procurar um endereço de destino em uma tabela, a fim de descobrir para onde enviar um pacote; e a comutação, que utiliza um rótulo tirado do pacote como um índice para uma tabela de encaminhamento. Porém não há campo disponível para números de circuitos virtuais dentro do cabeçalho *IP*.

Por essa razão, surgiu a necessidade de adicionar um novo cabeçalho *MPLS* antes do cabeçalho IP. Em uma linha de roteador para roteador e usando-se o *PPP (Point-to-Point Protocol)* como protocolo de enquadramento, o formato do quadro, incluindo os cabeçalhos *PPP, MPLS*, *IP* e *TCP*, é semelhante ao da figura 1. De certo modo, pode-se considerar que o *MPLS* é a camada 2,5.

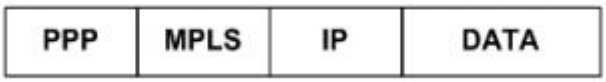


Figura 1: Cabeçalho MPLS. (OLIVEIRA et. al., 2012)

2.2. O roteamento baseado em rótulos

A tecnologia IP deverá continuar sendo a principal ferramenta adotada por provedores de serviços. Tal tecnologia, aliada ao *MPLS* e à possibilidade de unificar as comunicações de voz, vídeo e dados, proporciona benefícios econômicos e tecnológicos para as operadoras (OLIVEIRA et. al., 2012).

Os autores citam que para suportar o crescimento mundial da internet, os provedores de serviços precisam de roteadores de alto desempenho, pois, além da

[4] https://www.ietf.org/

crescente demanda por banda, eles precisam lidar com o crescente número de nós na rede e, consequentemente, com um aumento nas tabelas de roteamento.

De acordo com Pepelnjak e Guichard (2000), os *switches* oferecem um desempenho muito superior na comutação de células ou segmentos que os roteadores para encaminhamento de pacotes. Isso se deve ao fato de que o tipo das informações a serem analisadas pelos *switches* é basicamente mais simples, tornando o processo de encaminhamento dos segmentos muito mais rápido, fato esse que levou a maior parte dos *backbones* IPs a serem implementados utilizando uma rede ATM em seu núcleo, de acordo com a figura 2.

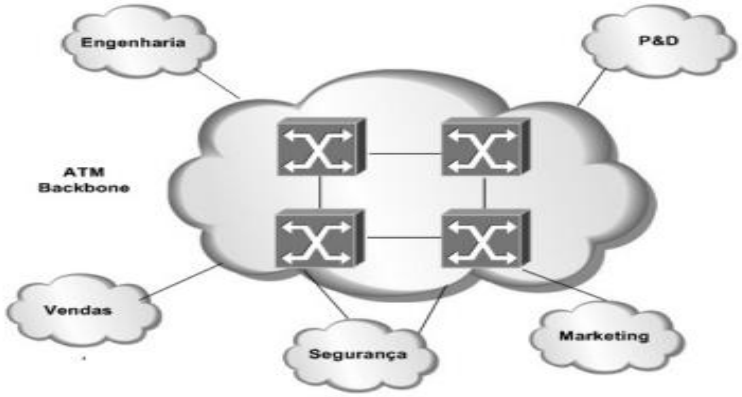


Figura 2: Backbone de uma rede ATM. (Pepelnjak e Guichard, 2000)

O *MPLS* é uma tecnologia aberta que foi apresentada inicialmente como uma solução que possibilitava melhorar o desempenho das redes *IPs* na função de encaminhamento de pacotes *IPs*, combinando o processo de roteamento de nível 3 com a comutação de nível 2 para realizar o encaminhamento de datagramas através de pequenos rótulos de tamanho fixo. Tais rótulos são números utilizados no protocolo *MPLS* e, através destes, a decisão de qual interface encaminhar o datagrama é tomada (ROSEN et. al., 2001).

De acordo com os mesmos autores, a comutação de rótulos multiprotocolos combina a funcionalidade dos protocolos de roteamento da camada de rede e a comutação por rótulos, além de fornecer benefícios significativos às redes com *IP* e *ATM*, ou uma combinação de outras tecnologias no nível da camada de rede. Portanto, em uma arquitetura IP sobre *MPLS*, as informações necessárias para o encaminhamento são obtidas do cabeçalho *MPLS* (32 bits), que é bem menor e menos complexo que o cabeçalho IP (20 bytes), com isso contribuindo para que os

equipamentos de menor poder de processamento e armazenamento tenham desempenho melhor nesse tipo de arquitetura em relação a outras arquiteturas.

OLIVEIRA et. al. (2012) destacam que outra vantagem significativa da arquitetura *IP* sobre *MPLS* diz respeito ao encaminhamento de datagramas ao longo de um caminho. Em redes *IPs* convencionais, todos os roteadores da topologia precisam saber a melhor rota em sua tabela de roteamento para encaminhar o pacote ao seu destino pelo melhor caminho possível. Já o protocolo *MPLS* trabalha com encaminhamento dos pacotes baseado em rótulos, pois os roteadores de núcleo, conhecidos como P (*Provider*), não têm acesso ao endereço *IP* de destino do pacote; assim, não há inteligência de roteamento nesses roteadores de núcleo, e sim o encaminhamento local, de uma interface para outra, tomando como base os valores dos rótulos dos pacotes, ou seja, fazendo um processo apenas de comutação de rótulos.

2.3. O cabeçalho *MPLS*

Oliveira et. al. (2012) relata que o rótulo é um identificador curto, de 4 bytes, e com significado local no roteador que é usado para identificar uma FEC (*Forwarding Equivalent Class*), isto é, um grupo de pacotes *IPs* que são enviados na mesma maneira, sobre o mesmo trajeto e com o mesmo tratamento de transmissão.

Tanenbaum (2003) ressalta que como os cabeçalhos *MPLS* não fazem parte do pacote da camada de rede ou do quadro da camada de enlace de dados, considera-se o *MPLS* em grande parte independente de ambas as camadas. Entre outras coisas, essa propriedade significa que é possível construir switches *MPLS* que podem encaminhar tanto pacotes *IP* quanto células *ATM*, dependendo do tipo de objeto que surgir. Essa característica explica a palavra "multiprotocolo" no nome *MPLS*.

Segundo Oliveira et. al. (2012), o rótulo associa pacotes às respectivas conexões. Seu formato é apresentado na figura 3, seguida da função de cada campo.

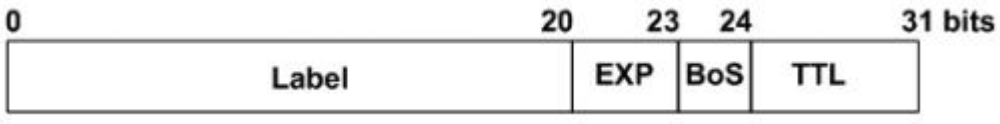


Figura 3: Cabeçalho MPLS. (Oliveira et, al., 2012)

• *Label* (Rótulo): contém o valor do rótulo MPLS. Como o tamanho é de 20 bits, esse valor pode variar de 0 a (220 -1), ou 1.048.575. Existem alguns valores que são reservados ao protocolo e têm significados especiais;

• EXP (*Experimental Bits*): este campo é composto por três bits e são utilizados para alterar os algoritmos de enfileiramento e descarte; dessa forma é possível dar prioridade a determinados pacotes. Usado atualmente por classes de serviços (CoS);

• BoS (*Bottom of Stack*): formado por apenas um bit, este campo permite a criação de uma pilha hierárquica de rótulos. Indica se o cabeçalho ao qual o pacote pertence é o último da pilha MPLS. Todos os cabeçalhos MPLS devem ter esse bit em 0, e através desse campo um roteador de saída tem condições de decidir se o próximo encaminhamento será baseado em MPLS ou IP;

• TTL (*Time To Live*): Campo formado por 8 *bits*. Especifica um limite de quantos saltos o pacote pode atravessar. Quando um datagrama entra em um roteador de borda MPLS, o valor inicial do TTL no cabeçalho MPLS deve ser igual ao valor do TTL do cabeçalho IP e decrementado de 1 em cada roteador. Na saída do caminho, o roteador deve copiar o valor do TTL do cabeçalho MPLS para o TTL do cabeçalho IP.

2.4. Funcionamento

Nas redes *MPLS* os pacotes são rotulados assim que entram na rede e são encaminhados apenas com base no conteúdo desses rótulos ao longo do caminho. Os roteadores tomam decisão de encaminhamento com base em tais rótulos, evitando assim o esquema de intenso processo de pesquisa de dados utilizado no roteamento convencional. É possível também que, em vez de um único rótulo, o *MPLS* permita que os pacotes de dados carreguem uma pilha de rótulos, segundo a ordem de que o último rótulo a ser colocado no pacote deverá ser o primeiro a ser retirado (Lobo, 2008).

Oliveira et. al. (2012) definem o funcionamento do MPLS em 4 etapas:

• Etapa 1 – Construção das tabelas de roteamento: através dos protocolos de roteamento, como *OSPF (Open Shortest Path First)*, são construídas as tabelas de roteamento que irão determinar os melhores caminhos para atingir as redes de destino por toda a rede do provedor. Nesta etapa também há a atuação do protocolo LDP (*Label Distribution Protocol*), que irá fazer o mapeamento entre rótulos e IPs de destino.

• Etapa 2 – Ingresso dos pacotes na rede. O roteador de borda (*Edge LSR*) de ingresso recebe os pacotes que irão entrar na rede, executando serviços de nível 3 e valor agregado, tais como *QoS* (*Quality of Service*), e em seguida acrescenta o rótulo aos pacotes.

• Etapa 3 – Encaminhamento dos pacotes na rede. O *LSR* (*Label Switching Routers*) encaminha pacotes usando o mecanismo de troca de rótulos (*Label Swapping*). Ao receber o pacote com rótulo, o *LSR* lê o rótulo, o substitui de acordo com a tabela *LFIB (Label Forwarding Information Bases)* e o encaminha, sendo essa ação repetida por todos os roteadores no núcleo do *backbone*.

• Etapa 4 – Saída do pacote na rede. O roteador de borda (*Edge LSR*) de saída remove o rótulo e entrega pacotes *IPs*.

O funcionamento pode ser observado na figura 4 de acordo com sua respectiva etapa:

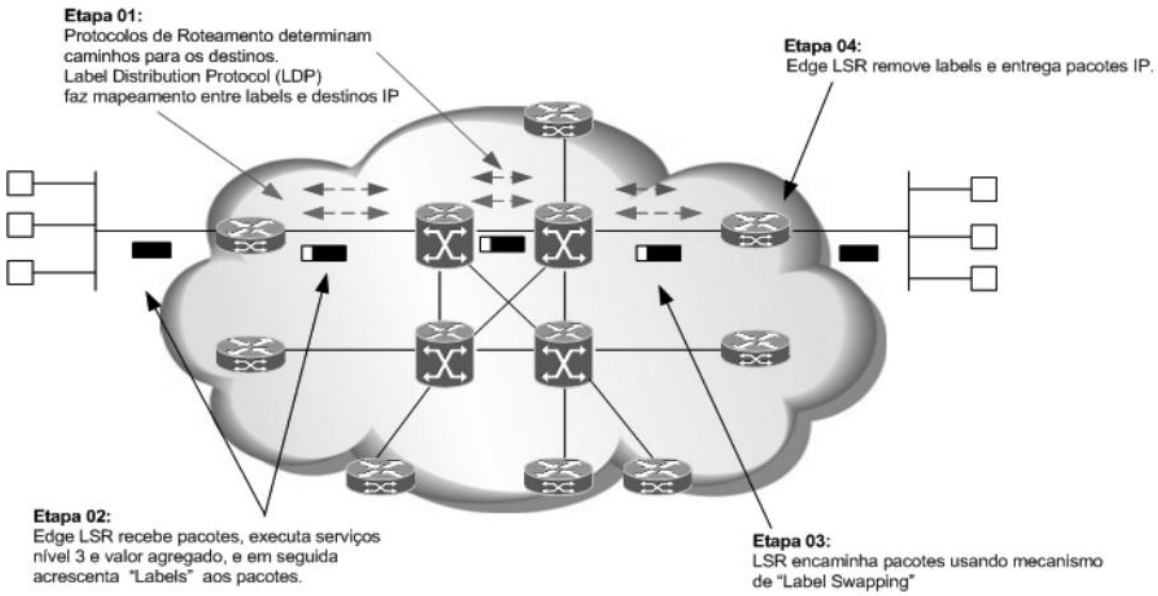


Figura 4: Operação do MPLS. (Oliveira et. al., 2012)

2.5. Vantagens e desvantagens do *MPLS*

Oliveira et. al. (2012) citam as principais vantagens do *MPLS*, tais como a possibilidade da melhoria do desempenho no encaminhamento dos pacotes, já que existe uma separação do plano de controle do plano de dados. Ganho na diminuição da latência, já que não há roteamento e sim a comutação dos rótulos. Possibilidade de criação de túneis, mecanismo útil para permitir que muitos *LSPs* sejam tratados

da mesma forma no núcleo da rede sem perder sua individualidade nas bordas, resultando em ganho na escalabilidade dos *LSRs* do núcleo da rede. Facilita a engenharia de tráfego nas redes *IPs* de provedores de serviços de telecomunicações. A principal capacidade que o *MPLS* traz às redes com engenharia de tráfego é a possibilidade de configurar um circuito virtual overlay comutado para o modelo de roteamento da Internet. Redução de custo com a utilização de *VPN* baseada no protocolo IP. Priorização de tráfego, assegurando transmissão de dados de modo mais eficiente. Utilização de serviços, tais como *QoS*, *VPN* e engenharia de tráfego.

Dentre as desvantagens, foram citadas o aumento das informações de controle ocasionado pela adição de rótulos, com a consequente redução de carga útil das informações e o fato da conexão do cliente ao provedor de serviços passar a ser uma conexão de nível 3, herdando com isto suas vulnerabilidades. Por exemplo, a tabela de rotas do cliente pode ser vista no *backbone MPLS*.

3. VPNs MPLS

Neste capítulo será detalhado as funções e utilizações das *VPNs MPLS*.

3.1. Conceito de VPN

Conforme relatado por Ricci (2007), pode-se dizer que uma *VPN* (*Virtual Private Network*) é um conjunto de políticas que controlam a conectividade e a qualidade de serviço de uma rede privada. São redes que compartilham um meio físico comum, porém possuem privacidade dos dados através de criptografia. São redes virtuais, pois não possuem enlaces ou linhas dedicadas entre as suas extremidades. No entanto, para os usuários e clientes, são “transparentes” e possuem as mesmas funcionalidades de segurança de enlaces dedicados. As *VPNs* consistem em soluções simples e flexíveis, tratando-se de uma poderosa ferramenta de tunelamento oferecida pelos provedores de serviço de Internet (*ISPs*). As *VPNs* foram originalmente introduzidas para permitir aos provedores de serviços o uso de uma mesma infraestrutura comum na emulação de enlaces ponto-a-ponto entre os sites dos clientes, e foram desenvolvidas nos moldes de uma rede geograficamente distribuída ou *WAN* (*Wide Area Network*), podendo abranger uma ampla área geográfica, frequentemente um país ou continente, com todos os atributos de segurança, gerenciamento e processamento.

Guimarães et. al. (2006) relata que ao usar protocolos padronizados, as empresas são capazes de conectar suas redes privadas com segurança usando os recursos econômicos e altamente disponíveis da Internet. O objetivo da Internet é proporcionar comunicação entre os nós das redes de modo irrestrito. A maneira de baixo custo e eficiente de obter tal resultado é a utilização de *VPNs*.

3.2. Utilização do MPLS para estabelecer VPN

Todos os tipos de *VPNs* se baseiam na tecnologia de tunelamento, que pode ser definida como o processo de encapsular um protocolo dentro de outro; porém, antes de encapsular, este deverá ser criptografado, de forma que, caso seja interceptado durante o transporte, não possa ser lido. O pacote que é criptografado e encapsulado é enviado pela Internet até ao destino, onde é desencapsulado e decriptografado, para entrega ao destinatário. Portanto, o túnel é a denominação do caminho lógico que é percorrido pelos pacotes ao longo da rede. Após alcançar o destino, o pacote é desencapsulado e encaminhado ao seu destino final, conforme ilustrado na Figura 5. (OLIVEIRA et. al., 2007)

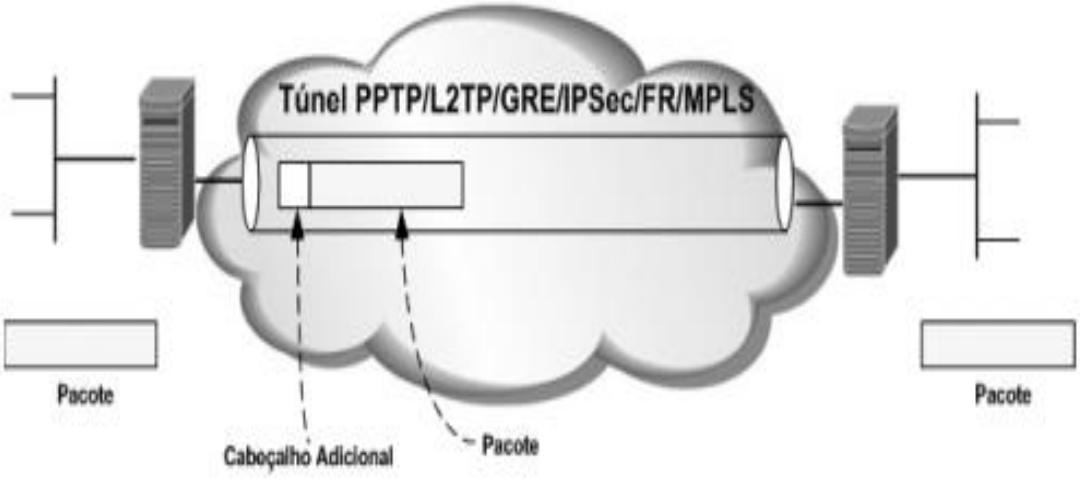


Figura 5: Tunelamento VPN. (Oliveira et. al., 2007)

4 O SIMULADOR GNS3

Conforme relatado por Oliveira et. al. (2012), o *GNS3* é um simulador de domínio público que permite simular redes complexas através de diversas simulações de ambientes com a tecnologia MPLS e seus serviços, objetivando facilitar o

aprendizado e servindo de base para o leitor desenvolver seus próprios cenários, suas configurações e aplicações..

Os mesmos autores citam que uma das grandes vantagens em adotar um software de emulação como o *GNS3* é permitir a interconexão do ambiente virtual com um ambiente real, além da possibilidade de interação com um ambiente idêntico ao proporcionado por elementos de rede reais.

4.1. Simulação prática

Oliveira et. al. (2012) relatam que com o uso da tecnologia *MPLS*, as *VPNs* oferecem grandes benefícios, fazendo com que a rede seja mais segura e tenha maior agilidade no tráfego, permitindo também a integração de qualquer tipo de rede, planos de endereçamentos e roteamento. Por fazer uso do conceito de Roteador Virtual, reduz significativamente a necessidade de equipamento para cada enlace do usuário na operadora.

Os rótulos do *MPLS* podem ser usados para isolar o tráfego entre as *VPNs*. Todas as *VPNs* dos clientes compartilham o mesmo meio físico que compõe o núcleo da rede. Os dados de cada *VPN* são isolados entre si e, também, todo o núcleo é oculto/isolado para as *VPNs*. Isto significa que usuários de uma *VPN* não têm acesso e desconhecem as outras *VPNs* e o núcleo da rede.

Para validar estes conceitos, este trabalho simulou uma *VPN Site-to-Site,* que é um tipo de conexão remota, porém que ocorre entre redes inteiras (Datarain, 2020). Para isso, serão utilizados dois rotadores (R1 e R2) para simular um acesso entre empresas, interligando as unidades em que estão funcionando os negócios, como matriz e filial, com outros usuários que estão em localidades diferentes, conforme Figura 6:

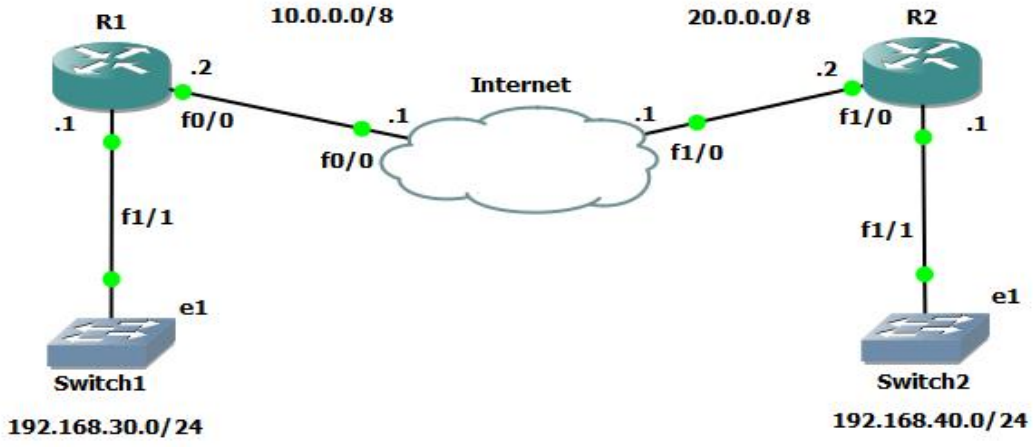


Figura 6. Fonte: do autor.

Primeiramente, para que os roteadores sejam alcançáveis, as interfaces de ambos devem ser configuradas. Portanto, para permitir uma interface específica, é preciso entrar no modo de configuração de interface usando o comando do modo de instalação “interface *type-and-number”,* no caso do roteador R1: interface f0/0. A seguir é preciso definir o endereço *IPv4* (10.0.0.2) e a máscara de sub-rede (255.0.0.0) usando o comando de configuração da interface “ip address *address subnet-mask”* (ip address 10.0.0.2 255.0.0.0). Por padrão, as interfaces LAN e WAN não são ativadas. A interface deve ser ativada usando o comando *no shutdown* (no sh) e seguido de *exit* (ex), encerrando a configuração da interface f0/0 do roteador R1, e então iniciar o mesmo procedimento para a f1/1, conforme a Figura 7, interface de configuração do R1 pelo GNS3 com os comandos utilizados:

Figura 7. Fonte: do autor.

A seguir, o mesmo processo para a criação das interfaces da rede de Internet (f0/0 e f1/0), conforme a Figura 8:

Figura 8. Fonte: do autor.

E então, as interfaces do Roteador R2 (f1/0 e f1/1), também efetuadas de forma semelhante ao mesmo procedimento feito para o R1, conforme Figura 9:

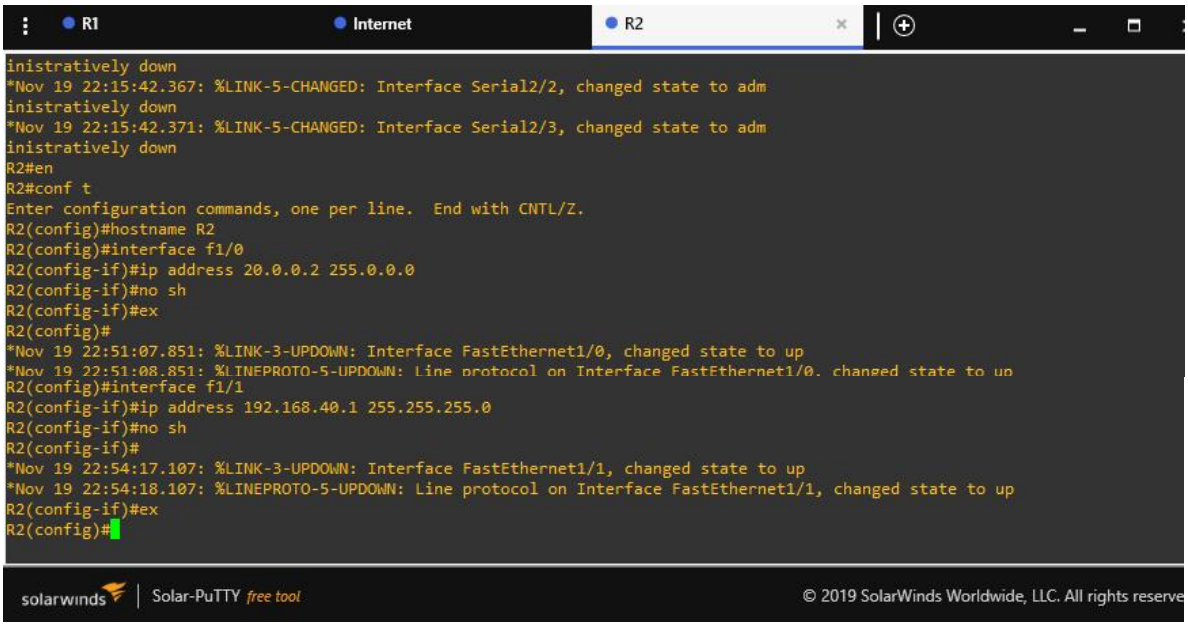


Figura 9. Fonte: do autor.

O próximo passo é configurar o protocolo de roteamento *OSPF* para o roteador R2. Essa configuração é necessária para o envio de avisos sobre o estado de conexão entres os roteadores de mesma área, no caso o R1 e o R2 na área 0, conforme Figura 10:

Figura 10. Fonte: do autor.

A mesma configuração de protocolo *OSPF* deve ser feito para o Internet, conforme Figura 11:

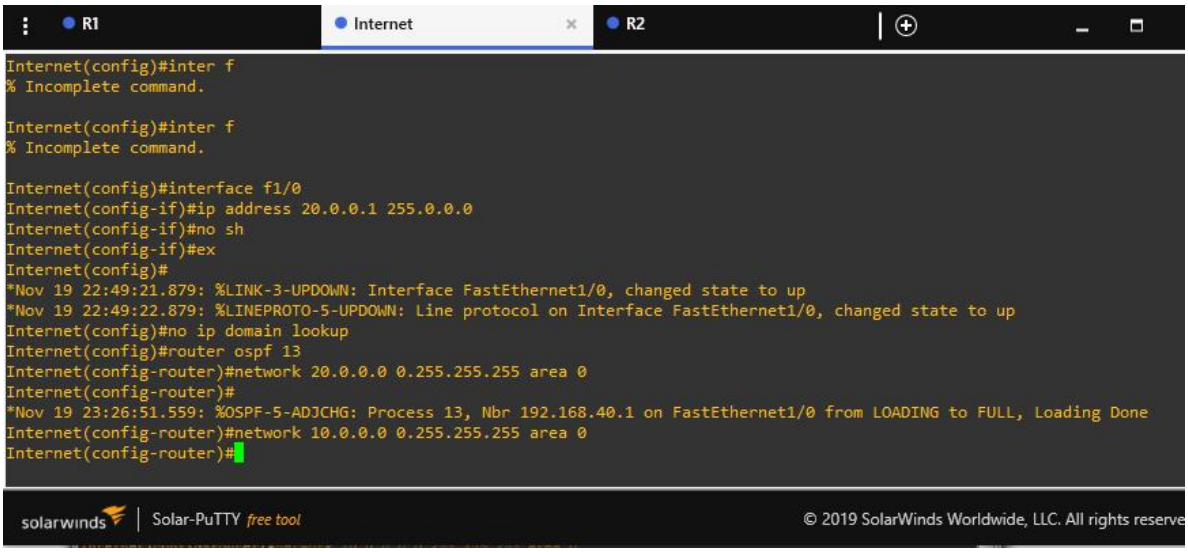


Figura 11. Fonte: do autor.

E então a configuração do *OSPF* para o R1 de forma semelhante ao procedimento efetuado para o R2, conforme Figura 12:

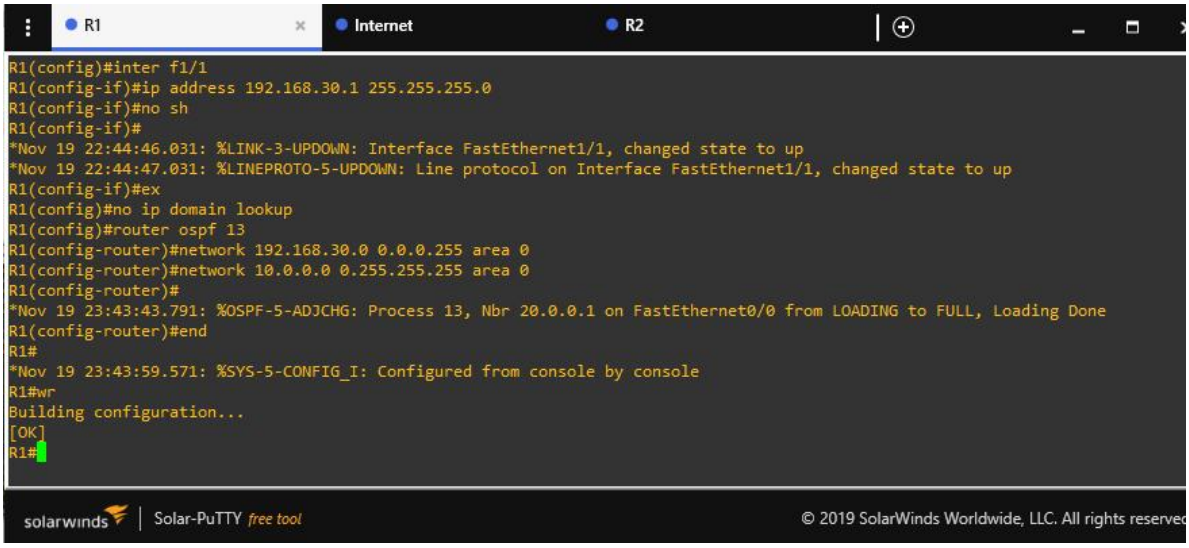


Figura 12. Fonte: do autor.

Efetuada as configurações de roteamento *OSPF*, é possível visualizar as rotas dos *IPs* que estão conectados ao R1 com o comando “*show ip route*”, conforme Figura 13:

Figura 13. Fonte: do autor.

A Figura 14 ilustra a visualização das rotas dos *IPs* que estão conectados ao R2:

Figura 14. Fonte: do autor.

A Figura 15 ilustra a visualização das rotas dos IPs que estão conectados ao Internet:

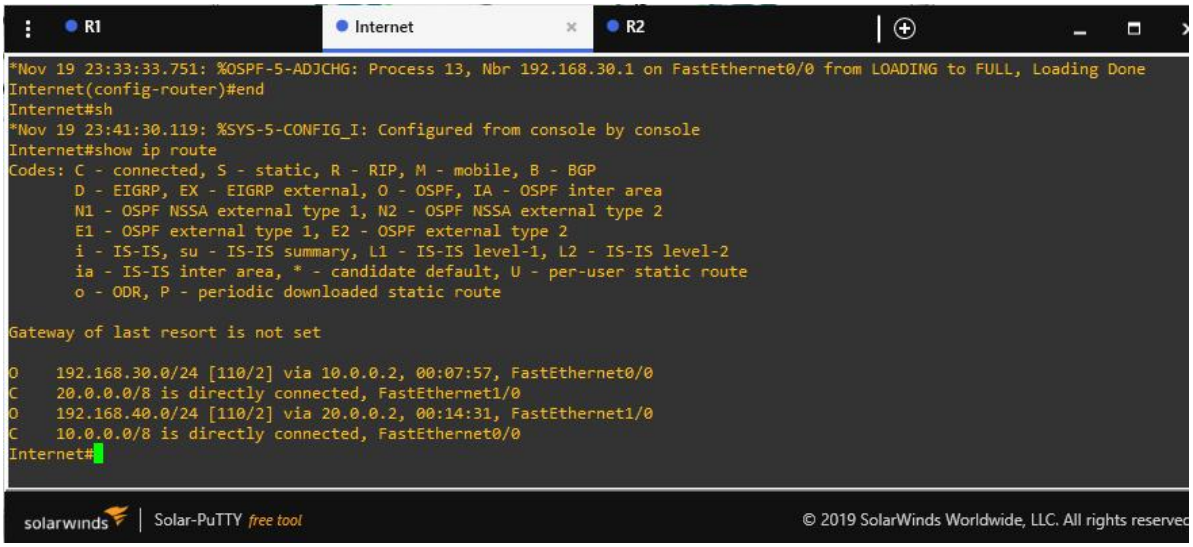


Figura 15. Fonte: do autor.

A seguir será configurado o túnel *VPN* do roteador R1, que são responsáveis por permitir que a *VPN* estabeleça conexão antes do usuário fazer *logon.* Neste passo também é necessário configurar a política de criptografia *ISAKMP,* a qual é necessária para permitir a alteração de chaves de segurança entre os roteadores, conforme Figura 16:

Figura 16. Fonte: do autor.

A mesma configuração do túnel *VPN* deve ser aplicada ao roteador R2, conforme Figura 17:

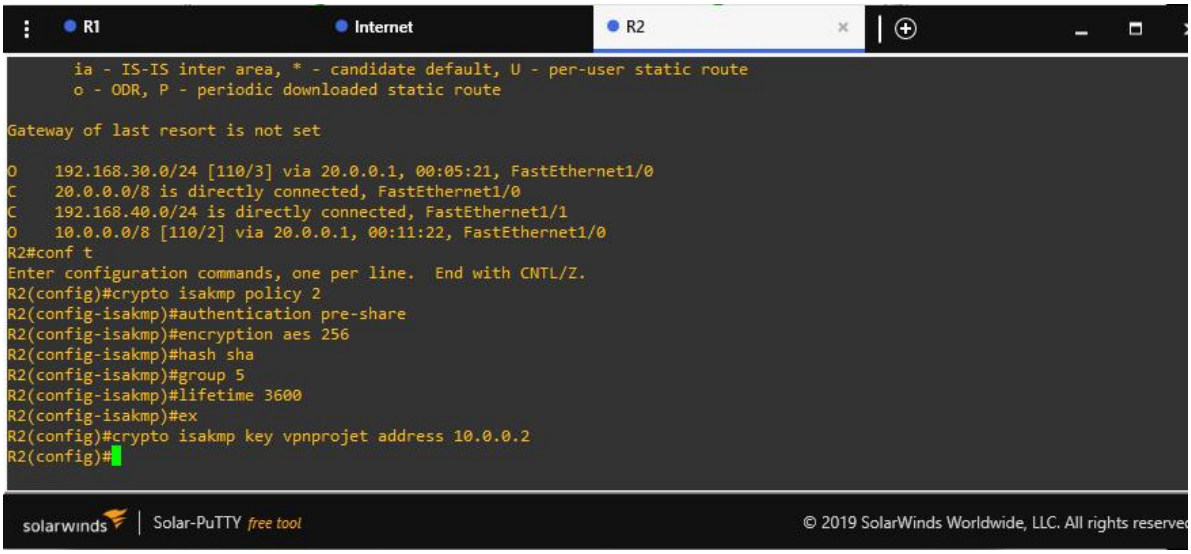


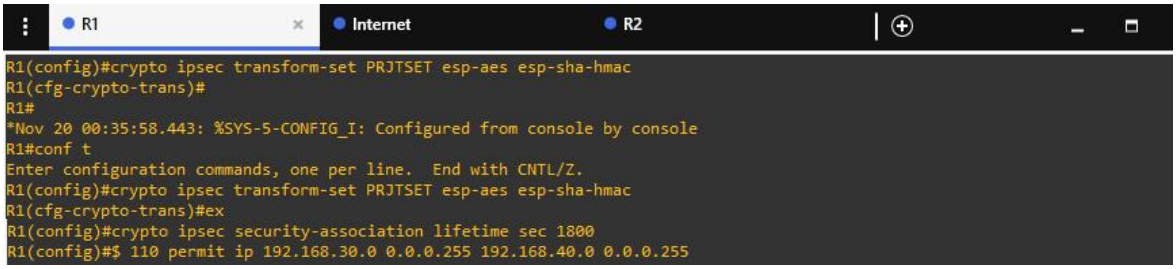
Figura 17. Fonte: do autor.

Efetuada as configurações dos túneis *VPN*, é necessário criar o mapa de criptografia (que nesta simulação foi nomeado como PRJMAP), o qual interligará os parâmetros da primeira fase do *ISAKMP* através do comando *crypto map*, que é responsável por mapear os parâmetros de troca de chaves para que as informações criadas na origem sejam compatíveis com as informações de troca de chaves no destino.

A seguir é definido o par de destino, ou seja, em que outra parte será estabelecido o túnel para troca de chaves e estabelecimento da VPN; nesse caso, o comando *peer* define o destino 20.0.0.2.

O comando *set transform-set* define o parâmetro PRJSET como um conjunto de atributos que serão compartilhadas entre a origem e destino para estabelecer a VPN. É por meio desse processo que é dito que tanto a origem, quanto o destino, utilizaram as mesmas diretrizes de segurança para estabelecimento do tráfego.

O *match address* 110 mapeia o processo VPN com a lista de acesso, permitindo que o tráfego a ser gerado pela VPN seja autorizado tanto na origem quanto no destino, conforme Figura 18:



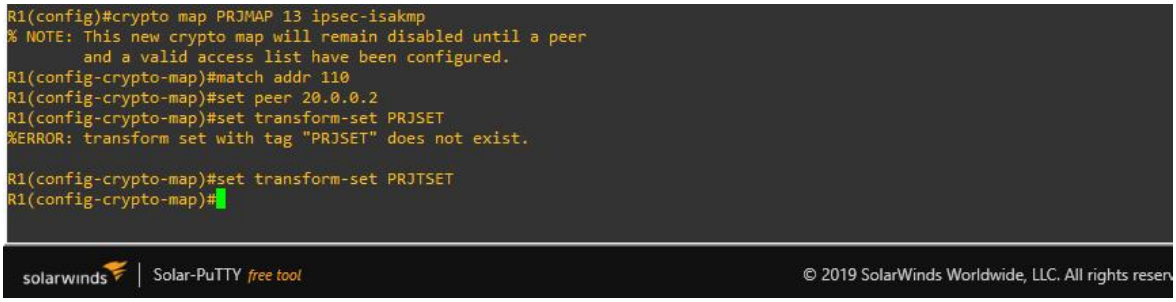


Figura 18. Fonte: do autor.

O mesmo procedimento anterior deve ser efetuado de forma semelhante para o R2, conforme Figura 19:

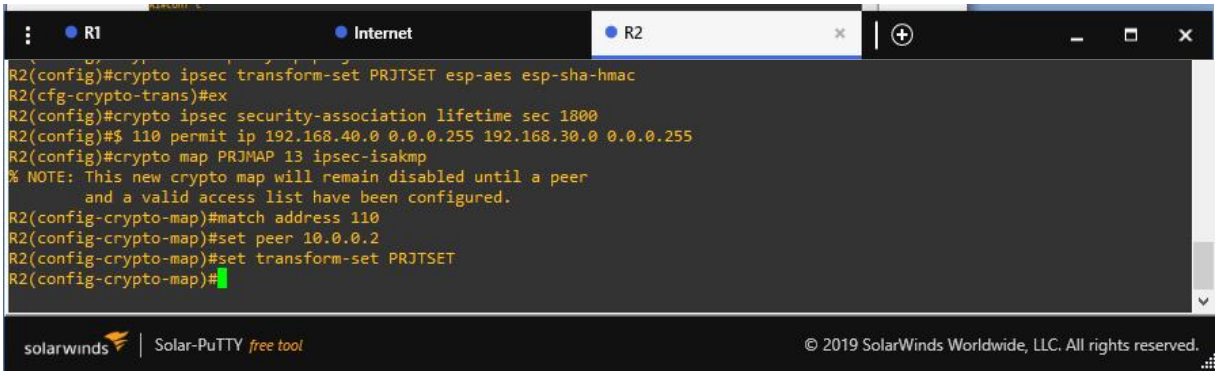


Figura 19. Fonte: do autor.

Logo, é preciso mapear a interface serial do R1 para habilitar a comunicação entre os roteadores para a VPN e especificar que o mapeamento dos parâmetros para o estabelecimento do *IPsec* está contido no mapa de criptografia PRJMAP, conforme Figura 20:

Figura 20. Fonte: do autor.

O mesmo procedimento deve ser efetuado de forma semelhante para a interface do R2, conforme Figura 21:

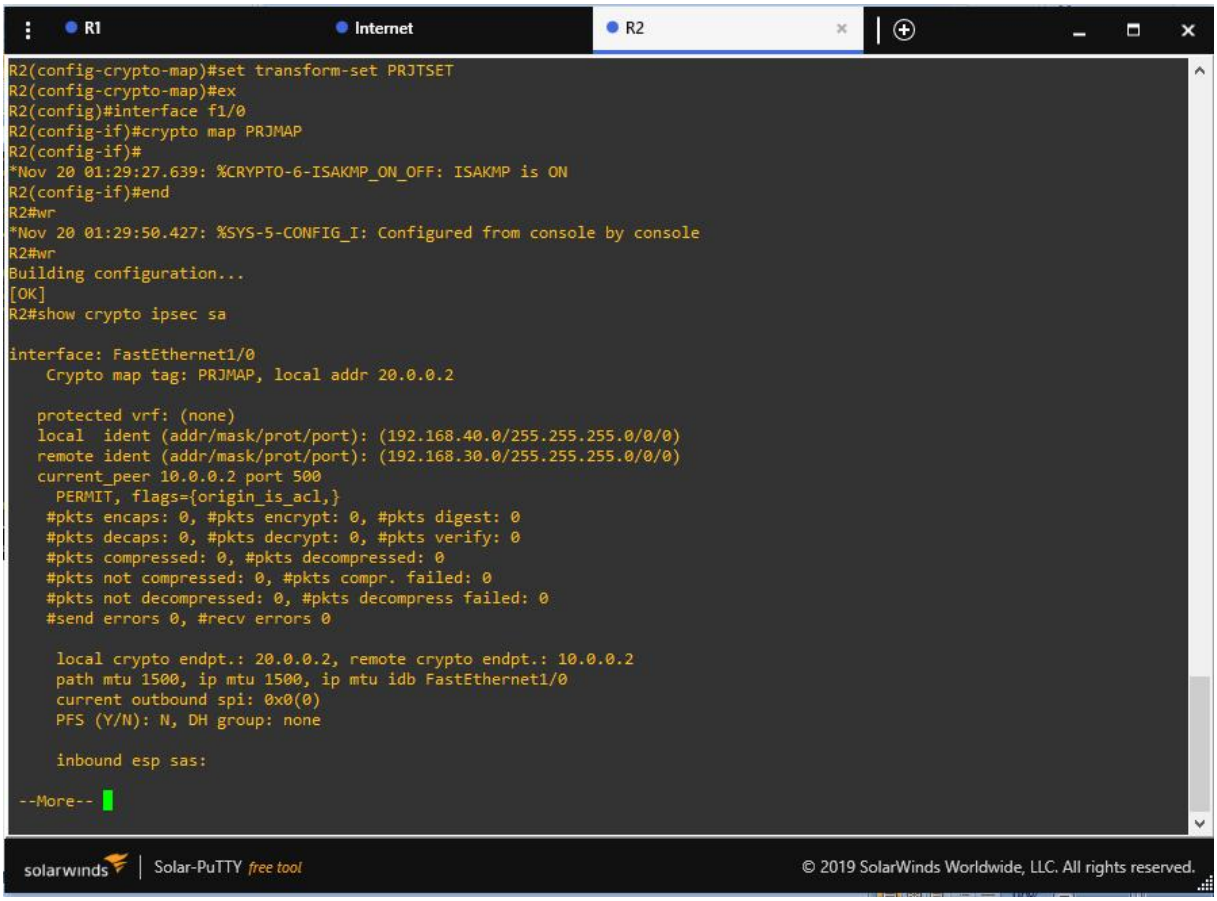


Figura 21. Fonte: do autor.

A partir de então, é possível visualizar os dados de encriptação para o R1 através do comando "*show crypto isakmp policy*", conforme Figura 22:

Figura 22. Fonte: do autor.

O mesmo comando pode ser executado para visualização da encriptação para o R2, conforme Figura 23:

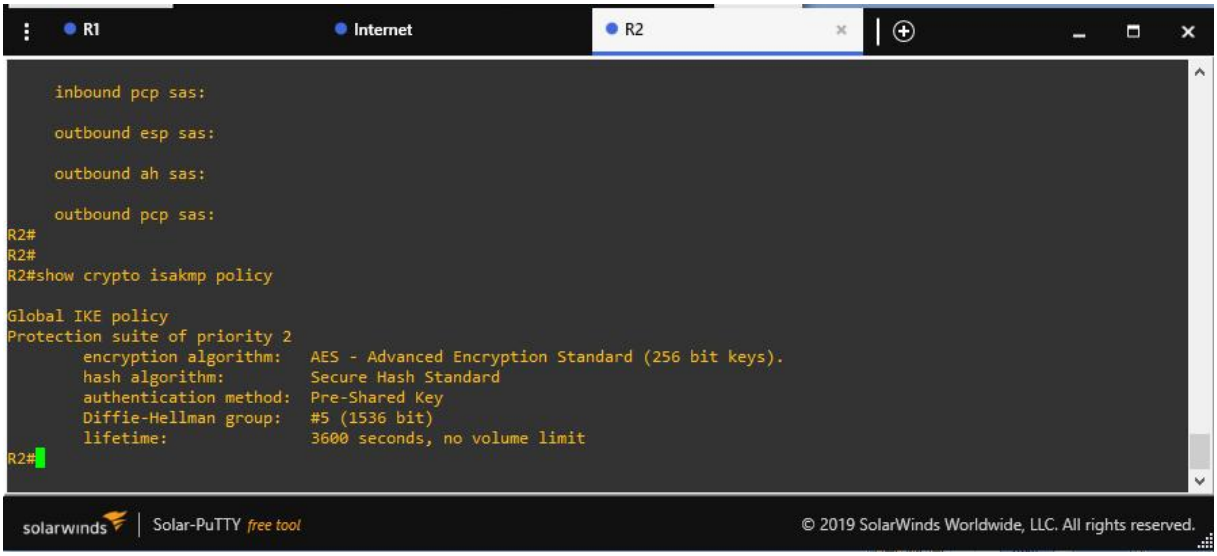


Figura 23. Fonte: do autor.

E para testar o funcionamento da *VPN*, pode-se verificar se o túnel foi estabelecido e se a conexão foi criptografada pelo teste de *ping* do R1, conforme Figura 24. Esse teste simula uma troca de pacotes entre os roteadores no cenário e depois analisa se os pacotes enviados foram recebidos e criptografados. Na imagem da Figura 25 é possível observar que todos os pacotes foram enviados de forma correta até o destino.

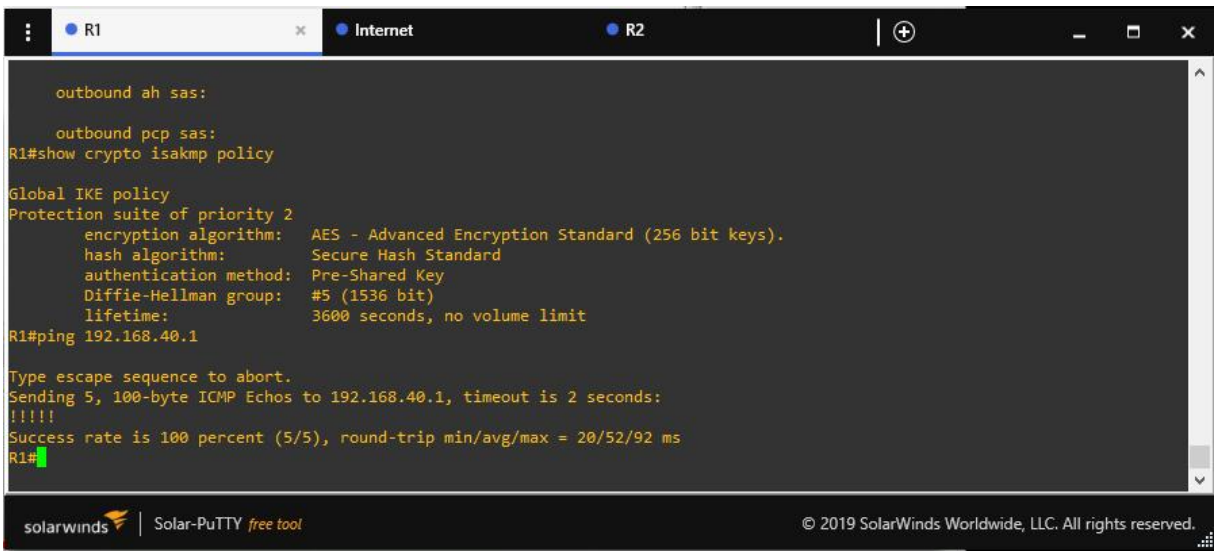


Figura 24. Fonte: do autor.

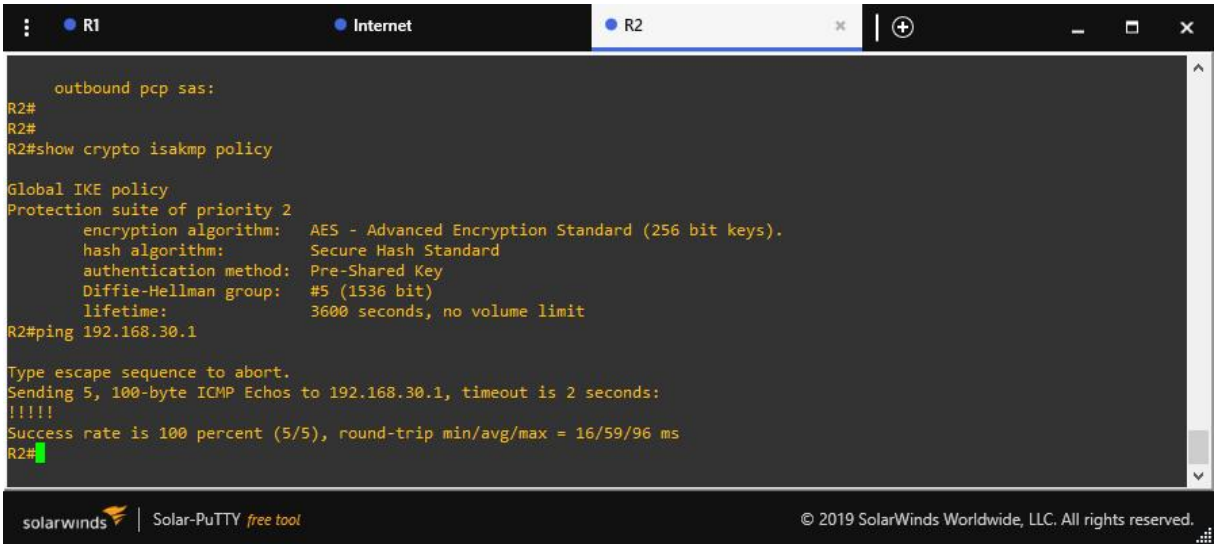


Figura 25. Fonte: do autor.

Com o retorno de sucesso no teste de *ping,* a simulação realizada permitiu concluir como o uso das *VPNs* facilita a comunicação por meio de acesso remoto interligando clientes e empresas de modo que ambos possam de comunicar com segurança e praticidade.

5 CONSIDERAÇÕES FINAIS

A tecnologia *MPLS* trouxe um novo conceito de padronização da comutação de pacotes baseando-se na troca de rótulos, visando melhorar o fluxo de tráfego de redes mantendo a relevante qualidade de serviço da tecnologia *ATM*, porém com importantes aprimoramentos.

Já as redes virtuais privadas (*VPNs*) são voltadas para conectar usuários de forma residencial ou empresarial mesmo que estejam fisicamente distantes. As *VPNs MPLS* utilizam uma ferramenta de encapsulamento que faz uma melhor utilização dos protocolos necessários para o tráfego da rede desde o início até o destino por meio de tunelamentos.

O GNS3 permite simular de forma mais clara e objetiva como funciona o tráfego de uma rede *MPLS* em redes virtuais privadas, executando de forma todo o processo de criação e configuração da *VPN*.

Como trabalho futuro, há o interesse de aprimorar o conhecimento em redes *MPLS* e a criação de *VPNs* mediante estudo de monitoramento e gerenciamento em casos reais.

REFERÊNCIAS

COMER, Douglas E. **Interligação de redes com TCP/IP.** 6ª ed. Rio de Janeiro: Elsevier, 2015.

DATARAIN **Qual a diferença entre VPN Site-to-Site e VPN Client-to-Site?**. 2020. Disponível em: <https://www.datarain.com.br/blog/tecnologia-e-inovacao/diferenca-vpn-site-vpnclient/>. Acesso em: 16 nov. 2020.

GUIMARÃES, Alexandre; LINS, Rafael Dueire; OLIVEIRA, Raimundo. **Segurança em Redes Privadas Virtuais - VPNs.** Rio de Janeiro: Brasport, 2006.

LOBO, Lancy. **MPLS Configuration on Cisco IOS Software.** Indianapolis: Cisco Press, 2008.

LUCEK, Julian; MINEI, Ina. **MPLS – Enabled Applications: emerging developments and new technologies.** Indianapolis: Wiley, 2005.

MENDES, Roberto G. Redes **MPLS I: Modelo Conceitual – 1.** Disponível em: < https://blog.ccna.com.br/2008/08/25/qos-qualidade-de-servico-parte-ii/>. Acesso em: 24 nov. 2020.

OLIVEIRA, José Mário; LINS, Rafael Dueire; MENDONÇA, Roberto. **Redes MPLS: Fundamentos e Aplicações.** 1 ed. Rio de Janeiro: Brasport, 2012.

PEPELNJAK, Ivan; GUICHARD, Jim. **MPLS and VPN Architectures.** Indianapolis: Cisco Press, 2000.

PINHEIRO, Jose Mauricio Santos. **Guia completo de cabeamento de redes.** Rio de Janeiro: Elsevier, 2003.

RICCI, Bruno. **Rede Segura: VPN Linux.** 1 ed. Rio de Janeiro: Ciência Moderna, 2007.

ROSEN, E.; TAPPAN, D.; FEDORKOW, G.; REKHTER, Y.; LI, T.; CONTA, A. **RFC 3032. MPLS Label Stack Encoding.** The Internet Society, 2001.

TANENBAUM, Andrew S. **Redes de Computadores.** 4ª ed. Rio de Janeiro. Elsevier. 2003.