

Análise Do Desempenho de VPNs nas Camadas de Rede e Enlace

Daniel R. Stasiak ¹, Walter Priesnitz Filho ²

¹ Tecnólogo em Redes de Computadores
Universidade Federal de Santa Maria (UFSM) – Santa Maria, RS – Brazil

daniel.ramos, walter@redes.ufsm.br

Abstract. *The interconnection of remote places is vital to the operation of enterprises. Therefore the use of VPN technologies is essential to the application of the enterprise strategies. To ordinary enterprises be employing resources and personal on the implementation of these services is not always a viable solution, so Internet providers are hired to execute the interconnection e implementation of the VPNs. A critical factor associated with all TI service is in delivering performance, providing adequate throughput levels to the clients is necessary to avoid financial loss to the TI operator. With vast possibilities of choices in the implementation of VPN services, the performance factor can be the key in this process of choosing the right technology. Therefore this paper presents the analysis of the performance of three types of technologies that support the VPN functionality on a level of the data link and network layers, MPLS, Frame Relay, and IPSec.*

Resumo. *A interconexão de lugares remotos é vital para a operabilidade de certas empresas, dessa forma a utilização de tecnologias de VPN é essencial na aplicação das suas estratégias. Pois para as empresas gastarem recursos e pessoal para implementar esse serviço nem sempre é uma solução viável, portanto são contratadas provedores de Internet para realizar a interconexão e implementação das VPNs. Um fator muito importante associado a todo serviço de TI está na entrega de desempenho, entregar uma taxa de transmissão adequada aos clientes é necessário para evitar prejuízos financeiros para provedora de TI. Com as amplas possibilidades para a escolha da implementação do serviço de VPN, o fator de desempenho pode ser desequilibrante nessa balança. Portanto este artigo apresenta a análise do desempenho de três tecnologias de VPN nas camadas de enlace e camada de rede, são elas: MPLS, Frame Relay e IPSec.*

1. Introdução

Empresas que possuem filiais espalhadas por diferentes cidades precisam que essas filiais possam se comunicar. Esta comunicação deve ocorrer preferencialmente através de um meio seguro, já que nesse tráfego podem estar sendo transmitidos dados estratégicos da corporação [Stallings and Brown 2008]. Um recurso que pode ser utilizado é uma conexão física entre as filiais, como por exemplo, através de fibra óptica entre os roteadores das filiais. Entretanto, essa abordagem pode não ser a ideal, pois o preço e o caminho do cabeamento podem ser empecilhos na implementação. Outro método está na utilização de

uma *Virtual Private Network* (VPN), que é uma rede privada feita sobre uma rede pública (*Internet*) [Borges et al. 2014].

Os Provedores de serviço de *Virtual Private Network* (VPN) possuem obrigações estabelecidas em contratos no que diz respeito ao desempenho do serviço entregue ao cliente. Descumprir as métricas de desempenho firmadas em contrato pode ocasionar multas para o provedor. Portanto é importante analisar os protocolos de VPN sob esse escopo.

Este trabalho apresenta uma comparação, com o foco no desempenho, entre três protocolos que fornecem serviços de VPN nas camadas de rede e de enlace, são eles: o *IP Security Protocol* (IPSec), o *Multi Protocol Label Switching* (MPLS), e *Frame Relay*. A escolha de protocolos que atuam nessas camadas permite que estes protocolos sejam comparados no mesmo nível de equipamentos, podendo todos serem implementados em roteadores. Esses protocolos foram configurados em ambiente simulado e real. Assim, foram comparados não só a performance dos protocolos em si, mas também a fidedignidade dos resultados de testes de desempenho nos dois cenários.

O artigo foi está estruturado da seguinte forma: A Seção 2 apresenta o referencial teórico. A Seção 3 traz os trabalhos relacionados, na Seção 4 são descritos os cenários de teste utilizados. A Seção 5 apresenta e discute os resultados obtidos e, por fim, a Seção 6 apresenta as conclusões.

2. Referencial Teórico

Nesta seção serão abordados os conceitos dos protocolos que forma utilizados para a realização dos testes de desempenho no desenvolvimento deste trabalho.

2.1. VPN (Virtual Private Network)

Virtual Private Network (VPN) é um dos principais métodos de se fazer a interconexão entre lugares geograficamente distantes [Borges et al. 2014]. Além disso, as VPNs fornecem funções que integram a segurança dos dados, como a garantia da confidencialidade destes dados [Borges et al. 2014].

As VPNs realizam o tunelamento da transmissão dos dados, permitindo que os dados trafeguem de forma segura na rede, de um ponto até o outro [Borges et al. 2014]. Existem vários níveis de atuação com protocolos distintos, por exemplo na camada de transporte o *Security Sockets Layer* (SSL), na camada de rede o IPSec [Kurose and Ross 2012] e na de enlace, os exemplos são o MPLS e o *Frame Relay* [Ghein 2007].

2.2. IPSec (IP Security)

O IPSec é um conjunto de serviços que provê serviços de segurança para a camada de rede, e subsequentemente, para as camadas superiores no modelo TCP/IP [Kozierok 2005]. Algumas das características providas são a encriptação dos dados do cliente, autenticação das mensagens, um método seguro para a troca de chaves, e dois modos de uso (túnel e transporte) [Kozierok 2005].

O modo túnel realiza a encriptação dos dados na camada de rede, dessa forma é criado um novo cabeçalho IP, com um novo endereço [Borges et al. 2014]. Sendo assim,

é criado um túnel entre os dois roteadores, sendo aplicado em nível de *hardware*. O modo de transporte faz encriptação na camada de transporte, esse modo é aplicado em nível de *software* [Borges et al. 2014].

2.3. Frame Relay

O *Frame Relay* é uma tecnologia de camada de enlace que realiza o repasse de quadros em uma rede *Wide Area Network* (WAN) [Ghein 2007]. É baseado em circuitos virtuais, que é o caminho bi-direcional em que os dados serão transmitidos na rede *Frame Relay* entre os clientes, portanto os clientes acabam por dividir recursos da rede, como largura de banda [Castelli 2002].

Uma rede *Frame Relay* fornece alguns serviços como, *Quality of Service* (QoS) e controle de congestionamento [Castelli 2002]. Um *host* é denominado *Data Terminal Equipment* (DTE), e um dispositivo da rede é chamado de *Data Communication Equipment* (DCE) [Cisco 2003]. O *Frame Relay* faz a identificação de um quadro com o número *Data-Link Connection Identifier* (DLCI) [Castelli 2002].

2.4. MPLS (Multi Protocol Label Switching)

O MPLS é um protocolo da camada de enlace que faz o repasse de pacotes baseado em *labels* [Jamhour 2011]. O roteamento dos pacotes dentro da rede MPLS é feito através dessas *labels*, portanto não são utilizados protocolos da camada de rede.

O MPLS fornece serviços de VPN, QoS, e *Traffic Engineering* (TE), e pode ser usado em uma rede interna [Ghein 2007]. Um roteador que faz o repasse dos quadros dentro da rede é o *Label Switching Router* (LSR), o roteador que insere uma *label* em um pacote é o *Ingress LSR*, e o roteador que retira a *label* e encaminha para o FEC adequado é o *Egress LSR* [Ghein 2007].

2.5. Desempenho

Existem alguns fatores que influenciam no desempenho de uma rede, Entre eles está a vazão, que é a taxa da transmissão de dados em um canal por um período de tempo determinado [Kurose and Ross 2012]. Outro conceito importante é a largura de banda, pois ela possui relação com a largura da frequência, determinando o quão rápido a transferência de dados pode ocorrer em um canal de dados [Kurose and Ross 2012].

3. Trabalhos Relacionados

Nesta Seção serão apresentados os trabalhos sobre tecnologias de VPN que abordam configuração e desempenho, e que foram usados como base para o desenvolvimento da proposta deste trabalho.

No trabalho de [GIACOMELLI ZANON 2016] é apresentada uma comparação entre duas tecnologias de VPN: MPLS e *Frame Relay*. Foi feita uma comparação sob o enfoque teórico entre *Frame Relay* e MPLS, utilizando operadoras de Internet como parâmetro. Para a execução da proposta, foi implementada uma rede com VPN MPLS, fazendo a comunicação entre clientes passando por uma rede MPLS de uma provedora, e testado se a comunicação ocorreu. Um comparativo das características do *Frame Relay* e do MPLS foi feito envolvendo duas operadoras, abordando as características dos protocolos aplicados por elas. Contudo, não foram feitas avaliações sobre os serviços de VPN dessas operadoras, apenas uma descrição das características.

O trabalho de [ROMEO 2016] aborda o desempenho do MPLS em redes WAN. Foram implementados três cenários, com a configuração básica do MPLS, com uma VPN MPLS, e com políticas de controle de tráfego. Nesses cenários foram feitas avaliações variando a taxa de transmissão, e utilizando como parâmetros de comparação os pacotes transmitidos na rede e a perda desses pacotes, variação da taxa de transmissão, e variação do *jitter* (atraso na transmissão). Não foram feitos comparativos com outras tecnologias de VPN, dessa forma o estudo ficou restrito somente ao MPLS.

No artigo [N Kate and A. Waichol 2014] é feita uma comparação entre desempenho do protocolo MPLS e o protocolo de roteamento OSPF, baseado em IP. Foram feitos testes de vazão, e usados como parâmetros dados fornecidos pelo *Wireshark*, como pacotes recebidos, *bytes*, latência, perda de pacotes entre outros. Os dados foram obtidos por meio do uso de filtros no *Wireshark*, que permitem que a análise adequada seja feita.

O artigo de [Stangarlin and Filho 2012] apresentou um análise sobre o desempenho de protocolos de segurança para redes sem fio. Foram utilizados tempos distintos para análise do pacote, 1, 2, 4, e 8 minutos. Foi constatado que conforme a alteração do tempo do teste, o melhor desempenho variava, ou seja, o desempenho não era linear durante o tempo. Os parâmetros analisados foram o *jitter*, a vazão, o atraso, e a média de pacotes perdidos. Não foram implementados protocolos de roteamento e VPN, apenas os protocolos de segurança.

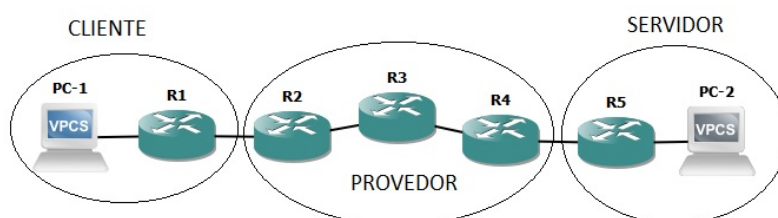
4. Cenários de Teste

Para a execução dos testes foi necessário estabelecer uma topologia em que os três protocolos pudessem ser aplicados. A topologia mínima especificada no modelo de VPN do MPLS seriam com 3 roteadores no provedor, e dois roteadores de cliente. Sendo assim, foi necessário fazer uma modificação no IPSec, realizando uma autenticação em dois níveis, uma no cliente e outra no provedor. O *Frame Relay* era adaptável aos dois formatos.

A alteração da topologia foi necessária para que os protocolos fossem comparáveis. Portanto foi criado um ambiente em que o resultado dos testes entre os protocolos fosse fidedigna. O PC-1 ficou estabelecido como cliente e o PC-2 como servidor, como pode ser visto na Figura 1.

Foram utilizados 3 tempos de execução: 1, 3 e 5 minutos. Isso foi feito porque no início da comunicação entre os *hosts* apresentava uma lentidão variando de acordo com o protocolo. Assim, com mais tempos estipulados, foi possível realizar a análise em situações distintas e verificar o comportamento da variação do fluxo de dados ao longo do tempo, assim como em [Stangarlin and Filho 2012]. Os cenários definidos foram configurados nos dois ambientes.

Figura 1. Topologia dos Testes



4.1. Materiais e Parâmetros

Os testes foram executados utilizando no ambiente virtual o *Graphical Network Simulator-3* (GNS-3) 2.1.21, Cisco 3720, Máquina Virtual *Windows 7* (512 MB RAM). No ambiente real o roteador Cisco 1941, Ubuntu 18.04, e ambos os ambientes foram utilizados o *Wireshark* 3.0.3 e o *Jperf* 2.0.2.

Os parâmetros estabelecidos para realizar a análise foram os Pacotes Capturados, Média de Pacotes Capturados *Bytes* Capturado Média *Bytes/s* Capturados, Média Largura de Banda, Variação da Largura de Banda, e Erros na Transmissão. Os resultados obtidos através do *JPerf* foram os relacionados a largura de banda, e os demais pelo *Wireshark*. Todos os dados apresentados foram capturados no lado do servidor.

Os mesmos parâmetros foram utilizados nos dois ambientes. Entretanto, não foi possível utilizar os mesmos roteadores nos dois ambientes, pois o GNS3 não possuía suporte para os roteadores que se apresentavam a disposição para os testes no ambiente físico: Cisco 1941 e 2901. O modelo de roteador Cisco 3720 foi escolhido devido ao suporte dado aos três protocolos, assim como os roteadores utilizados no ambiente real. Dessa forma, foi estabelecido um padrão entre os teste no mesmo ambiente. As mesmas aplicações para a captura de dados, *Wireshark* e *JPerf*, foram utilizadas em ambos os ambientes.

5. Resultados

Os resultados consideram os dados obtidos dos pacotes que entraram e saíram da interface do servidor, portanto também foram contabilizados pacotes de confirmação do TCP. Entretanto foram desconsiderados os dados referente aos erros, que são mostrados em um parâmetro específico.

5.1. Ambiente Simulado

Os resultados dos testes apresentados nesta seção foram obtidos através da utilização do simulador de rede GNS-3.

Conforme pode ser visto na Tabela 1, no teste que foi executado durante um minuto, o *Frame Relay* obteve os melhores resultados em todos os parâmetros estipulados., como em Média de Largura de Banda com 1.071 Kbps.

Tabela 1. Resultados Ambiente Simulado - Todos os Protocolos 1 Minuto

Parâmetro	Frame Relay	IPSec	MPLS
Pacotes Capturados	8.857	8.715	8.816
Média de Pacotes Capturados	147,63	145,25	146,93
<i>Bytes</i> Capturados	8.523.437	7.255.127	8.480.305
Média <i>Bytes/s</i> Capturados	142,06 <i>kbytes</i>	120,92 <i>kbytes</i>	141,34 <i>kbytes</i>
Média Largura de Banda	1.071 Kbps	904 Kbps	1.066 Kbps
Var. Largura de Banda	1049 - 1.114 Kbps	674 - 983 Kbps	786 - 1.114 Kbps
Erros na Transmissão	0 (0,0)	6 (0,1%)	6 (0,1%)

A Tabela 2 apresenta os resultados dos testes com 3 minutos de execução. Ela indica uma pequena superioridade do *Frame Relay* com relação aos *Bytes* Capturados em comparação ao MPLS, com 25.458.494 *bytes*.

Tabela 2. Resultados Ambiente Simulado - Todos os Protocolos 3 Minutos

Parâmetro	Frame Relay	IPSec	MPLS
Pacotes Capturados	26.457	26.460	26.460
Média de Pacotes Capturados	146,98	147	147
Bytes Capturados	25.458.494	22.041.648	25.435.134
Média Bytes/s Capturados	141,44 <i>kbytes</i>	122,45 <i>kbytes</i>	141,31 <i>kbytes</i>
Média Largura de Banda	1.067 Kbps	916 Kbps	1.067 Kbps
Var. Largura de Banda	590 - 1.114 Kbps	721 - 983 Kbps	721 - 1.114 Kbps
Erros na Transmissão	0 (0,0)	0 (0,0%)	6 (0,0%)

Nos testes em ambiente simulado com 5 minutos o MPLS foi superior em *bytes* capturados e largura de banda, 42.298.765 e 1064 Kbps, como pode ser visto na Tabela 3.

Tabela 3. Resultados Ambiente Simulado - Todos os Protocolos 5 Minutos

Parâmetro	Frame Relay	IPSec	MPLS
Pacotes Capturados	43.862	43.991	43.964
Média de Pacotes Capturados	146,21	146,64	146,55
Bytes Capturados	42.226.482	36.639.636	42.298.765
Média Bytes/s Capturados	140,75 <i>kbytes</i>	122,13 <i>kbytes</i>	140,99 <i>kbytes</i>
Média Largura de Banda	1.063 Kbps	913 Kbps	1.064 Kbps
Var. Largura de Banda	786 - 1.114 Kbps	674 - 983 Kbps	786 - 1.114 Kbps
Erros na Transmissão	0 (0,0)	7 (0,0%)	7 (0,0%)

5.1.1. Considerações

Com relação aos resultados dos testes em ambiente simulado, o *Frame Relay* apresentou o melhor desempenho nos testes de 1 e 3 minutos. O MPLS teve o melhor desempenho no teste com a execução em 5 minutos. E o IPSec obteve o pior desempenho em todos os testes. Com exceção do parâmetro de pacotes recebidos, em que o IPSec obteve resultados superiores em alguns testes.

Durante a análise dos pacotes, foi constatado que os pacotes dos protocolos que chegavam ao servidor possuíam tamanhos distintos, o IPSec com 1368 *bytes*, o MPLS com 1506 *bytes*, e o *Frame Relay* com 1514 *bytes*.

Também foi possível notar que conforme eram aumentados os tempos de execução dos testes, o MPLS diminuía a diferença para o *Frame Relay*, até que o ultrapassou no teste dos 5 minutos. Contudo, os dois protocolos apresentaram resultados muito semelhantes nos 3 testes feitos. Os protocolos praticamente não apresentaram erros durante a transmissão, sendo apresentados no máximo 0,1% de erros.

5.2. Ambiente Real

Os testes realizados no ambiente real foram feitos com o roteador Cisco 1941. Observa-se que não foi possível obter os resultados para os testes do *Frame Relay* em tempo hábil.

Como pode ser visto na Tabela 4, o IPSec apresentou valores superiores ao MPLS em alguns dos testes no parâmetros de Pacotes Capturados e Erros de Transmissão. No teste com 5 minutos, por exemplo, ficaram com respectivamente, 68.384 e 13,2%.

Tabela 4. Resultados Ambiente Real - IPSec

Parâmetro	1 Min.	3 Min.	5 Min.
Pacotes Capturados	13.425	41.100	68.384
Média de Pacotes Capturados	223,75	228,33	227,95
Bytes Capturados	13.586.798	41.136.789	68.805.331
Média Bytes/s Capturados	226,45 <i>kbytes</i>	228,54 <i>kbytes</i>	229,35 <i>kbytes</i>
Média Largura de Banda	1.785 Kbps	1.771 Kbps	1.772 Kbps
Var. Largura de Banda	0 - 3.019 Kbps	0 - 4.399	0 - 5.512 Kbps
Erros na Transmissão	2.739 (14,4%)	3.069 (13,4%)	10.854 (13,2%)

Na Tabela 5 o MPLS foi superior na maioria dos parâmetros, como Bytes Capturados, e Média de Largura de Banda. Isso pode ser visto nos testes de 3 minutos, em que os resultados desses parâmetros foram, 43.983.106 *bytes* e 1.995 kbps.

Tabela 5. Resultados Ambiente Real - MPLS

Parâmetro	1 Min.	3 Min.	5 Min.
Pacotes Capturados	14.097	40.405	66.807
Média de Pacotes Capturados	234,95	224,47	222,69
Bytes Capturados	14.829.124	43.983.106	73.730.075
Média Bytes/s Capturados	247,15 <i>kbytes</i>	247,15 <i>kbytes</i>	245,76 <i>kbytes</i>
Média Largura de Banda	1.971 Kbps	1.995 Kbps	2.060 Kbps
Var. Largura de Banda	0 - 4.976 Kbps	0 - 5.553 Kbps	0 - 6.175 Kbps
Erros na Transmissão	2.282 (13,4%)	9.273 (18,4%)	16.684 (20%)

5.2.1. Considerações

Em relação aos resultados do ambiente real, o MPLS apresentou o melhor desempenho na maioria dos parâmetros de todos os testes. Os parâmetros em que o IPSec foi superior foram novamente com relação aos pacotes recebidos, e também nos erros de transmissão. Entretanto os pacotes mostraram o mesmo tamanho nos dois ambientes, portanto não é possível analisar o desempenho sobre esse aspecto. Os erros de transmissão do MPLS foram maiores nos teste de 3 e 5 minutos, chegando até 20% de erros. Isso ocorreu no momento em que o MPLS obteve também o maior desempenho na largura de banda.

No ambiente real o MPLS apresentou uma grande instabilidade, atingindo em alguns momentos uma largura de banda alta, e em outros não foi transmitido nenhum pacote. Isso ocorre devido a velocidade que os dados eram enviados, alguns pacotes que demoravam mais acabavam não chegando no tempo estipulado pelo *time out* do TCP. O *time out* do TCP é recalculado durante a transmissão para se adequar a velocidade da transmissão. Portanto, os pacotes perdidos ocasionavam erros, principalmente *ACKs* duplicados, entre outros.

6. Conclusão

Podem ser tiradas algumas conclusões a despeito dos dois ambientes, foi possível atestar que ambos os ambientes apresentaram os mesmos resultados quanto a superioridade dos protocolos, ou seja, o MPLS foi melhor que o IPSec nos dois ambientes.

Os resultados dos testes apresentaram diferenças na geração dos pacotes, porém isso já era esperado. O parâmetro de erros de transmissão não pode ser considerado no ambiente simulado, já que no ambiente real foi demonstrado uma diferença muito grande entre eles. O ambiente simulado apresentou no máximo 0,1% de erros de transmissão, e no ambiente real o máximo foi de 20%, mas sempre apresentado na casa dos 10%. Os dois ambientes apresentaram o mesmo tamanho de pacotes, isso demonstra uma integridade nos resultados dos testes simulados. Em relação aos pacotes capturados, eles não podem ser utilizados como parâmetro na comparação entre protocolos, já que eles apresentam tamanhos distintos, isso pode gerar erros na análise do desempenho.

Considerando os dois ambientes, o MPLS obteve o melhor desempenho. Sendo assim, é o protocolo mais indicado a ser utilizado na implementação de um provedor, visando o escopo de desempenho. Entretanto, é importante ressaltar que os testes simulados do *Frame Relay* apresentaram uma proximidade com o MPLS, mas isso só poderia ser confirmado caso os testes no ambiente real fossem realizados. Mas como os dois ambientes mostraram essa semelhança, o *Frame Relay* é um protocolo a ser considerado. Desta forma, este trabalho apresentou um comparativo entre diferentes protocolos para a implementação de VPNs considerando as camadas 2 e 3 do MR OSI. Ainda apresentou um comparativo de desempenho considerando de uma topologia em um ambiente simulado e em um ambiente físico/real.

Referências

- Borges, F., Fagundes, B. A., and da Cunha, G. N. (2014). Vpn: Protocolos e segurança. Acessado em 24 jul. 2019.
- Castelli, M. J. (2002). *Network Consultants Handbook*. Cisco Press, USA.
- Cisco, S. I. (2003). *Internetworking Technologies Handbook*. Cisco Press, USA.
- Ghein, L. D. (2007). *MPLS Fundamentals*. Cisco Press, Indianapolis.
- GIACOMELLI ZANON, A. (2016). Comparativo entre as tÉcnologias frame relay e mpls vpn em camada 3.
- Jamhour, E. (2011). Mpls. Acessado em 24 jul. 2019.
- Kozierok, C. M. (2005). *THE TCP/IP GUIDE A Comprehensive, Illustrated Internet Protocols Reference*. No Starch Press, USA.
- Kurose, J. and Ross, K. (2012). *Computer Networking a Top-Down Approach*. Pearson, USA.
- N Kate, N. and A. Waichol, S. (2014). Performance analysis of mpls network with traditional ip network in service provider environment. *International Journal of Advanced Research in Computer Engineering Technology*, 3(4):1311–1316.
- ROMEO, R. (2016). Testes de desempenho de uma rede wan utilizando o protocolo mpls: Uma anÁlise prÁtica.
- Stallings, W. and Brown, L. (2008). *Computer Security, Pinciples and Practice*. Pearson, USA.
- Stangarlin, D. P. and Filho, W. P. (2012). AnÁlise de desempenho de redes sem fio com diferentes protocolos de criptografia. *Escola Regional de Redes de Computadores*, 7:4.