

UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

MARCELO CECHINEL

SIMULAÇÃO E SEGMENTAÇÃO VIRTUAL DE REDES DE COMPUTADORES

CRICIÚMA

2016

MARCELO CECHINEL

SIMULAÇÃO E SEGMENTAÇÃO VIRTUAL DE REDES DE COMPUTADORES

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA

2016

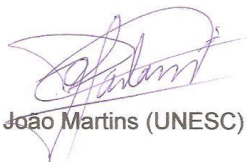
MARCELO CECHINEL

SIMULAÇÃO E SEGMENTAÇÃO VIRTUAL DE REDES DE COMPUTADORES

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Redes.

Criciúma, 21 de junho 2016.

BANCA EXAMINADORA



Prof. MSc. Paulo João Martins (UNESC) – Orientador



Prof. MSc. Rogério Antônio Casagrande (UNESC)



Prof. Esp. Sérgio Coral - (UNESC)

AGRADECIMENTOS

Agradeço primeiramente, a DEUS, por ter dado saúde para concluir este trabalho.

À minha família, em especial aos meus pais, Gilberto e Delourdes, que sempre me apoiaram e não mediram esforços para que eu chegasse até aqui, pela dedicação, pelo incentivo, pela confiança, pelo apoio em todos dos momentos.

Ao meu professo e orientador Paulo Martins, pela confiança, apoio, dedicação e comprometimento com este projeto. Pela paciência, pela excelente supervisão e as várias revisões até o término desta monografia.

Ao professor Kristian Madeira, por ter me recebido prontamente, e pela contribuição no projeto.

Aos professores e funcionários do Departamento da Computação.

A todos os amigos e colegas que de alguma maneira me ajudaram ao longo de todo o caminho.

RESUMO

Com o aumento significativo de nós nas redes, tem-se percebido que o desempenho tem se tornado um fator crítico, uma das formas de melhorar esse cenário é utilizando *Virtual Local Area Network* (VLAN). O objetivo desta pesquisa, foi em realizar experimentos por meio da técnica de simulação, que é uma ferramenta precisa que auxilia profissionais na tomada de decisão de forma preventiva, de forma a demonstrar por meio de alguns cenários, o momento de auxiliar na escolha de implementar ou uma rede virtual. Nas simulações o software empregado foi o OPNET, escolhido por ser de fácil instalação, não requisitar alto processamento, e por possuir uma versão acadêmica. E foi empregado a análise de tráfego em *switches* e servidores de aplicativos. O cenário comparado foi utilizando ou não a VLAN, com sete, quatorze e trinta máquinas. Com a realização das simulações realizadas em diferentes cenários, foi possível observar uma performance melhor com a rede com VLAN sobre a rede segmentada, e conforme o aumento de dispositivos no ambiente, a diferença de desempenho da rede segmentada tornasse considerável em relação a rede normal. Onde o tráfego em um segmento pode ser inibido de ser capturado por membro de outra rede virtual, mesmo que estejam no mesmo *switch*, descartando assim, o tráfego desnecessário pelo *switch* não ocasionando nenhum prejuízo ao desempenho da rede.

Palavras-chave: VLAN, segmentação, simulação, tráfego.

ABSTRACT

With the significant increase of us in the nets, we have observed that the performance has become a critical factor, one way to improve this scenario is using Virtual Local Area Network (VLAN). The objective of this research was to conduct experiments through simulation technique, which is a precise tool that assists professionals for making-decision preventively, in order to demonstrate through some scenarios, the time to assist in choosing to implement a virtual network. In the simulations, the software used was the OPNET, chosen because it is easy to install, do not request high throughput, and have an academic version. And it was used to traffic analysis in switches and application servers. The scenario compared was using or not the VLAN with seven, fourteen and thirty machines. With the completion of the simulations in different scenarios, we observed a better performance to network with VLAN regarding segmented network, and with the increase of devices in the environment, the performance difference of segmented network become considerable in relation to normal network. Where traffic on a segment can be inhibited from being captured by a member of another virtual network, even if they are on the same switch, discarding unnecessary traffic by the switch not causing any harm to the network performance.

Keyword: VLAN, segmentation, simulation, traffic.

LISTA DE ILUSTRAÇÕES

FIGURA 1. REDE LAN CORPORATIVA.....	23
FIGURA 2. REDE LAN COM DIVERSAS VLAN.	24
FIGURA 3. INSERÇÃO DO CAMPO DE IDENTIFICAÇÃO DE VLAN.	28
FIGURA 4. REDE <i>VIRTUAL</i>	28
FIGURA 5. QUADROS <i>ETHERNET</i> SEM E COM MARCAÇÃO DE VLAN.	29
FIGURA 6. ASSOCIAÇÃO DE PORTAS DE UM <i>SWITCH</i> A DIFERENTES VLAN.	32
FIGURA 7. ASSOCIAÇÃO DE PROTOCOLOS A DIFERENTES VLAN.....	32
FIGURA 8. ASSOCIAÇÃO DE ENDEREÇOS IP ÀS VLAN.	32
FIGURA 9. VLAN COM USO DE TRUNKING.	37
FIGURA 10. PROCESSO VTP E NÚMERO DE REVISÃO.	38
FIGURA 11. ETAPAS DO MÉTODO CIENTÍFICO PARA CENÁRIOS DE REDE.....	40
FIGURA 12. TELA INICIAL DO SOFTWARE OPNET IT RIVERBED MODELER ACADEMIC EDITION	43
FIGURA 13. FLUXO DE TRABALHO BÁSICO PARA CONSTRUÇÃO DE MODELOS NO OPNET.....	51
FIGURA 14. AMBIENTE DO OPNET PARA MODELAGEM DO CENÁRIO.	52
FIGURA 15. MOSTRA DE ALGUNS OBJETOS DO <i>OBJECT PALETTE</i>	53
FIGURA 16. OBJETO APLICAÇÃO E SEUS ATRIBUTOS	54
FIGURA 17. CONFIGURAÇÃO DE <i>PROFILE DEFINITION</i> E SEUS ATRIBUTOS.	55
FIGURA 18. CENÁRIO 1 NO OPNET COM 7 COMPUTADORES CLIENTES	56
FIGURA 19. CENÁRIO 1 DO OPNET COM 14 ESTAÇÕES DE TRABALHO	56
FIGURA 20. CENÁRIO 1 DO OPNET COM 21 ESTAÇÕES DE TRABALHO.	57
FIGURA 21. CENÁRIO 1 DO OPNET COM 30 ESTAÇÕES DE TRABALHO.	57
FIGURA 22. CENÁRIO 2 NO OPNET COM 7 ESTAÇÕES DE TRABALHO.	58
FIGURA 23. CENÁRIO 2 NO OPNET COM 14 ESTAÇÕES DE TRABALHO	58
FIGURA 24. CENÁRIO 2 NO OPNET COM 24 ESTAÇÕES DE TRABALHO.	59
FIGURA 26. TELA DE SELEÇÃO DAS ESTATÍSTICAS.	61
FIGURA 27. BOTÃO <i>CONFIGURE/RUN SIMULATION</i> NO AMBIENTE DO OPNET	61
FIGURA 28. JANELA DE CONFIGURAÇÃO DA SIMULAÇÃO NO OPNET.	62
FIGURA 30. JANELA DE VISUALIZAÇÃO DE RESULTADOS OBTIDOS.	63
FIGURA 33. GRÁFICO DE TRÁFICO ENCAMINHADO DO <i>SWITCH</i> BORDA01 NOS CENÁRIOS 1 E 2.....	67
FIGURA 34. GRÁFICO DE TRÁFICO RECEBIDO DO <i>SWITCH</i> BORDA01 NOS CENÁRIOS 1 E 2.	67
FIGURA 35. GRÁFICO DE TRÁFICO ENCAMINHADO DO <i>SWITCH</i> BORDA02 NOS CENÁRIOS 1 E 2.....	68
FIGURA 36. GRÁFICO DE TRÁFICO RECEBIDO DO <i>SWITCH</i> BORDA02 NOS CENÁRIOS 1 E 2.	69
FIGURA 37. GRÁFICO DE TRÁFICO ENCAMINHADO DO <i>SWITCH</i> BORDA03 NOS CENÁRIOS 1 E 2.....	69
FIGURA 38. GRÁFICO DE TRÁFICO RECEBIDO DO <i>SWITCH</i> BORDA03 NOS CENÁRIOS 1 E 2.	70
FIGURA 40. TRÁFEGO RECEBIDO <i>SWITCH CORE</i> EM AMBIENTE COM 14 COMPUTADORES.	72

FIGURA 41. TRÁFEGO ENCAMINHADO NO SWITCH BORDA01 EM AMBIENTE COM 14 COMPUTADORES.....	73
FIGURA 42. TRÁFEGO RECEBIDO NO SWITCH BORDA01 EM AMBIENTE COM 14 COMPUTADORES. .	75
FIGURA 43. TRÁFEGO ENCAMINHADO NO SWITCH BORDA02 EM AMBIENTE COM 14 COMPUTADORES.....	75
FIGURA 44. TRÁFEGO RECEBIDO NO SWITCH BORDA02 EM AMBIENTE COM 14 COMPUTADORES. .	76
FIGURA 46. TRÁFEGO RECEBIDO NO SWITCH BORDA03 EM AMBIENTE COM 14 COMPUTADORES. .	77
FIGURA 47. TRÁFEGO ENCAMINHADO NO SWITCH CORE EM AMBIENTE COM 30 COMPUTADORES..	79
FIGURA 48. TRÁFEGO RECEBIDO NO SWITCH CORE EM AMBIENTE COM 30 COMPUTADORES.	80
FIGURA 49. TRÁFEGO ENCAMINHADO NO SWITCH BORDA01 EM AMBIENTE COM 30 COMPUTADORES.....	80
FIGURA 50. TRÁFEGO RECEBIDO NO SWITCH BORDA01 EM AMBIENTE COM 30 COMPUTADORES. .	81
FIGURA 53. TRÁFEGO ENCAMINHADO NO SWITCH BORDA03 EM AMBIENTE COM 30 COMPUTADORES.....	83
FIGURA 54. TRÁFEGO RECEBIDO NO SWITCH BORDA03 EM AMBIENTE COM 30 COMPUTADORES. .	85
FIGURA 1. REDE LAN CORPORATIVA.	96
FIGURA 2. REDE LAN COM DIVERSAS VLAN.	97
FIGURA 10. PROCESSO VTP E NÚMERO DE REVISÃO.....	99

LISTA DE TABELAS

TABELA 1. COMPARAÇÃO ENTRE DOMÍNIOS DE COLISÃO E DE <i>BROADCAST</i> CRIADOS POR DISPOSITIVO DE REDE	25
TABELA 2. MODOS E CARACTERÍSTICAS DO VLAN TRUNKING PROTOCOL (VTP).	36
TABELA 3. TRÁFEGO RECEBIDO, ENCAMINHADOS E ENVIADOS DOS CENÁRIOS 1 E 2 COM 7 DISPOSITIVOS CLIENTES.	71
TABELA 4. TRÁFEGOS RECEBIDO, ENCAMINHADOS E ENVIADOS DOS CENÁRIOS 1 E 2 COM 14 DISPOSITIVOS CLIENTES.	78

LISTA DE ABREVIATURAS E SIGLAS

ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Eletronics Engineers
LAN	Local Area Network
MAN	Metropolitan Area Network
RTT	Round Trip Time
TCI	Tag Control Information
TCP	Transmission Control Protocol
TPDI	Tag Protocol Identifier
TTL	Time to Live
VLAN	Virtual Local Area Network
VTP	Virtual Trunk Protocol
WAN	Wide Area Network

SUMÁRIO

1 INTRODUÇÃO	11
1.1 OBJETIVO GERAL	12
1.2 OBJETIVOS ESPECÍFICOS	12
1.3 JUSTIFICATIVA	12
1.4 ESTRUTURA DO TRABALHO	14
2 REDES DE COMPUTADORES	15
2.1 PROBLEMAS E SOLUÇÕES EM REDES DE COMPUTADORES	16
2.2 DESEMPENHO EM REDES DE COMPUTADORES	18
2.2.1 caracterização do Problema	19
2.2.2 Métricas de desempenho em redes de computadores	19
2.2.3.1 Métricas de análise	20
2.2.3.2 Definição de protocolos utilizados	21
2.2.4 Modelagem de redes de computadores	22
3 SEGMENTAÇÃO DE REDES DE COMPUTADORES	23
3.1 VIRTUAL LOCAL AREA NETWORKS (VLAN)	26
3.1.1 O padrão IEEE 802.1Q	29
3.1.2 Vantagem na utilização de VLAN	30
3.1.3 Tipos de VLAN	31
3.2 TIPOS DE CONEXÃO DE DISPOSITIVOS EM VLAN	33
3.3 SOLUÇÃO VTP (VIRTUAL TRUNKING PROTOCOL)	33
3.3.1 O Processo VTP e Números de Revisão	37
4 SIMULAÇÃO	39
4.1 OBJETIVOS DA SIMULAÇÃO EM REDES DE COMPUTADORES	39
4.2 SOFTWARES DE SIMULAÇÃO PARA REDES	41
4.3 PROJETO E ANÁLISE DE EXPERIMENTOS DE SIMULAÇÃO	43
5 TRABALHOS CORRELATOS	45
5.1 PROJETO DE IMPLEMENTAÇÃO DE REDE LOCAL HIERÁRQUICA NO CAMPUS PONTA GROSSA DA UNIVERSIDADE TECNOLOGIA FEDERAL DO PARANÁ 45	
5.2 VLAN: ESTUDO, TESTE E ANÁLISE DESTA TECNOLOGIA	45
5.3 SEGURANÇA DE REDES LOCAIS COM A IMPLEMENTAÇÃO DE VLAN	46
6 SIMULAÇÃO E SEGMENTAÇÃO VIRTUAL DE REDES DE COMPUTADORES	48

6.1 METODOLOGIA.....	48
6.2 PROCESSO DE SIMULAÇÃO	48
6.3 MODELAGEM DE REDES DE COMPUTADORES	49
6.4 TOPOLOGIAS UTILIZADAS	50
6.5 MÉTRICAS E APLICAÇÕES.....	50
6.6 FLUXO DE TRABALHO	51
6.7 MODELAGEM DO PROJETO.....	51
6.8 CENÁRIOS E TOPOLOGIAS.....	55
6.9 ESCOLHAS DAS ESTATÍSTICAS	60
6.10 EXECUÇÃO DA SIMULAÇÃO	61
6.11 VISUALIZANDO E ANALISANDO RESULTADOS	63
6.12 RESULTADOS OBTIDOS	64
6.12.1 Cenários 1 e 2 com 7 máquinas	64
6.12.2 Cenários 1 e 2 com 14 máquinas	71
6.12.3 Cenários 1 e 2 com 30 máquinas	78
7 CONCLUSÃO	87
REFERÊNCIAS.....	89
APÊNDICE.....	94
1. Introdução.....	94
2. Descrição do Problema	95
2.1. Desempenho em Rede de Computadores	95
2.2. Modelagem de Redes de Computadores.....	95
3. LAN, Segmentação e VLAN.....	96
3.1. Tipos de VLAN	97
3.2. Tipo de Conexão de Dispositivos em VLAN	98
3.3. Solução VTP (Virtual Trunking Protocol)	98
3.4. O Processo VTP e Números de Revisão	99
3.5. Vantagem na utilização de VLAN.....	99
3.5.1. Redução de domínios de broadcast	99
3.5.2. Segurança	100
3.5.3. Gerenciamento	100
4. Simulação.....	100
4.1. Objetivos da Simulação em Redes de Computadores	100
5. Conclusão.....	101

6. Referências bibliográficas	101
--	------------

1 INTRODUÇÃO

Com o avanço da tecnologia e a expansão da Internet, vários serviços surgiram para facilitar a vida no dia a dia das pessoas e das organizações, como transações bancárias e comércio eletrônico (KUROSE; ROSS, 2011).

As redes de computadores têm demonstrado a sua importância para as empresas, principalmente no que tange o retorno que podem dar a organização, pois estando bem projetada e em funcionamento tornam os processos que dela dependem muito mais ágil, com isso os funcionários acabam se tornando mais produtivos, o que vai gerar retorno para a organização.

Mas, todo esse aumento na utilização das redes de computadores, e a dependência cada vez maior das pessoas, principalmente dentro das organizações, que hoje realizam praticamente tudo por meio da comunicação, como tarefas bancárias, notas para liberação de produtos, entre outras, com isso houve um aumento considerável dos dispositivos conectados há essas redes. Com este aumento, alguns problemas começaram a surgir, como por exemplo, a lentidão na transferência de pacotes e a segurança das informações.

A configuração dos equipamentos de redes e dos protocolos utilizados, devem ser ajustados de maneiras bem planejadas e estudadas, para que possa cumprir o objetivo para quais foram projetados, não ocasionando lentidão ou até mesmo indisponibilidade de serviços que dependem de uma rede estável e confiável (DOOLEY, 2002).

Algumas alternativas estão disponíveis no mercado para amenizar os problemas de redes, entre as opções, a segmentação da rede de computadores é uma das alternativas, com a construção de VLAN, que é uma forma de organizar a comunicação do ambiente, para melhorar o gerenciamento e a performance.

O projeto abordou o funcionamento deste modelo de rede, como uma forma de solucionar redes com elevado tráfego de pacotes encaminhados, recebidos e enviados, em relação ao custo benefício de se investir em equipamentos para a implementação.

Para avaliar o desempenho tem-se a implementação dessa tecnologia, de forma a trabalhar com *software* de simulação para os experimentos do modelo que rede não segmentado e segmento, procurando ser o mais fiel a realidade, gerando

informações de desempenho para análise a fim de demonstrar a performance entre um ambiente normal de um ambiente segmentado.

1.1 OBJETIVO GERAL

Simular um ambiente de segmentação virtual de redes, caracterizando o desempenho e reduzindo o domínio de colisão.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

- a) compreender e aplicar os conceitos de redes e seus protocolos para o ambiente a ser estudado;
- b) descrever e analisar o domínio de colisão, segmentação de rede, segmentação *virtual* por meio de VLAN;
- c) realizar testes de desempenho em um simulador de redes por meio de cenários, e algumas métricas de análise;
- d) analisar os resultados dos testes nos seus cenários.

1.3 JUSTIFICATIVA

Na atualidade, o homem e a tecnologia em diversos aspectos caminham juntos, sendo relevante para o seu desenvolvimento. E nos dias atuais a tecnologia cada vez mais faz parte do dia a dia das pessoas e das organizações. Com isso as redes de computadores estão se tornando cada vez mais importante para essa evolução (CAVALCANTE, 2009).

Redes de computadores é uma conexão entre dois ou mais computadores para permitir o compartilhamento de recursos e a troca de informações entre as máquinas.

Atualmente, com a importância cada vez maior de se dispor de acesso a informação e facilidades de comunicação, as redes de computadores estão projetadas para crescer indefinidamente (CANTÚ, 2003).

O crescimento acontece de forma gigantesca, principalmente com a grande popularidade que vem tendo as redes sociais e também os *e-commerce*¹ que estão representando um aumento constante dos números de usuários conectados (FELIPINI, 2006).

As redes locais são frequentemente configuradas para trabalhar hierarquicamente, com cada grupo de trabalho com seu próprio comutador de LAN conectado ao comutador de LAN de outros grupos via uma hierarquia de comutadores. Esses modelos podem trazer algumas desvantagens na sua utilização (KUROSE; ROSS, 2010).

A falta de isolamento de tráfego é uma das desvantagens, pois em uma rede não segmentada gera um tráfego de *broadcast* desnecessário, percorrendo todo o ambiente institucional. Outro problema encontrado é o uso ineficiente dos comutadores e também o gerenciamento de usuários, que podem causar problemas de segurança, como o acesso de usuários a informações não autorizadas dentro de uma organização, podendo ocasionar danos ainda maior para o administrador de rede (KUROSE; ROSS, 2010).

A segmentação de redes, surgiu para, entre outros motivos, limitar a disseminação de *broadcasts* em uma rede local e consiste em inserir dispositivos no ambiente que bloqueiam a passagem de pacotes de *broadcasts* quando atravessam suas interfaces. Os roteadores que são responsáveis por realizarem o gerenciamento, tem a função de interligar diferentes LAN (HAFFERMANN, 2009).

Para se obter o mesmo nível de segmentação e segurança de uma rede local pode se utilizar uma solução de baixo custo, utilizando o conceito de *Virtual Local Area Network* (VLAN) (HAFFERMANN, 2009).

Uma rede *virtual* é um agrupamento lógico de estações, serviços e dispositivos que não estão restritos a um segmento físico de uma rede local. A virtualização das redes locais pode facilitar a administração de grupos lógicos de estações e servidores de modo que possam se comunicar como se estivessem no mesmo segmento físico de uma LAN.

A comunicação de uma estação de trabalho em um grupo de rede virtualizado é restrita ao grupo de estações do mesmo grupo de uma rede *virtual*. E

¹ E-commerce é abreviação de *eletronic commerce*, que em português significa comércio eletrônico.

elas segmentam a rede logicamente em diferentes domínios de *broadcast* de modo que os pacotes sejam comutados somente entre portas designadas à mesma VLAN (CADORIN; SOMBRIO, 2012).

Para se obter uma boa estrutura de rede, sem que haja perda de produtividade com tráfego lento, domínio de colisão, *broadcast*, pode-se realizar uma simulação do ambiente, e com isso realizar um estudo mais detalhado, sobre qual tecnologia, e de que maneira poderá tratar a implantação dessa estrutura, analisando a viabilidade de implementação e a possibilidade de melhorar o desempenho da mesma.

Para a realização das simulações e análises de desempenho foi utilizado o *software* OPNET IT Guru Academic Edition, desenvolvido pela OPNET Technologies Inc. É um *software* utilizado por milhares de organizações, tais como governos e universidades do mundo todo, com o foco computacional, é uma ferramenta utilizada para modelar redes em um ambiente *virtual*, analisar e prever seu desempenho, incluindo aplicações, usuários, tecnologias e protocolos (OPNET IT, 2014).

1.4 ESTRUTURA DO TRABALHO

Será apresentado no projeto os conceitos básicos de rede, seu funcionamento, os principais problemas encontrados em uma rede de computadores e, algumas soluções que podem ser adotadas para solucioná-las. Há também, um foco sobre desempenho, apresentando sua caracterização, suas métricas utilizadas para a análise e resultados desses problemas. No capítulo 3, são apresentados os conceitos de VLAN, suas características e aplicações. Também são descritos seus benefícios, formas de implementação, os padrões utilizados, os tipos de VLAN que podem ser adotados.

2 REDES DE COMPUTADORES

Redes de computadores é um conjunto de dispositivos (locais ou remotos) que são interligados entre si por meio de roteadores, *switches* e entre outros, possibilitando a troca de informações entre os dispositivos, por meio de uma rede local, ou até mesmo remotamente, possibilitando a conexão de qualquer equipamento que esteja conectado em rede, como microcomputadores, notebooks, tablets, smartphones e outros. Para se caracterizar uma rede de computadores, precisa-se no mínimo de dois elementos interconectados, sendo que o número máximo não tem limite, pois teoricamente, todos os computadores do mundo poderiam estar interligados, a Internet é um exemplo (MIRANDA, 2008).

De forma geral o objetivo é possibilitar aos usuários acesso a todos os programas, dados e outros recursos independentemente de sua localização física, proporcionando uma maior disponibilidade com a opção de migração para outro equipamento quando a máquina sofrer alguma falha, confiabilidade, e nas organizações a economia pois com o compartilhamento dos sistemas, facilita o uso, com a vantagem de se evitar ao máximo a probabilidade de conter informações duplicadas ou desatualizadas. É isso que leva as organizações investirem no uso de redes, por reconhecerem o quanto elas podem economizar e ganhar em produtividade utilizando-as (MIRANDA, 2008).

O funcionamento de uma rede depende de três estruturas básicas, as sub-redes que são compostas pelos nós da rede, onde são interconectados aos equipamentos de comunicação. Os dispositivos de dados, que são conectados, e são responsáveis por gerar e consumir informações. E os protocolos, que são as regras de sintaxe e semântica que validam as trocas de informações entre os instrumentos da sub-redes de comunicação (MIRANDA, 2008).

As redes de computadores podem ter várias dimensões em seu uso, podendo abranger poucos ou milhares de clientes conectados que vai realizar requisições de serviços como e-mail, páginas de Internet entre outros serviços. Existem algumas classificações conforme seu uso. *Local Area Network* (LAN) que é a tecnologia de rede local que liga os dispositivos em uma área geográfica limitada,

como por exemplo, uma rede usada em um mesmo edifício, ou residência, e são utilizadas em conexão de computadores pessoais. *Metropolitan Area Network* (MAN) é a rede que abrange um espaço maior do que uma LAN, como por exemplo a comunicação de uma cidade. Essas redes são bastante utilizadas em redes de televisão a cabo. *Wide Area Network* (WAN) são as redes de distâncias maiores, quando envolve uma grande área geográfica, fazendo a conexão entre redes localizadas em países e continentes diferentes (TANENBAUM; WETHERALL, 2011).

Outra questão importante para um funcionamento correto de toda a forma de comunicação são a necessidade de algum mecanismo. E na área de comunicação de dados isso não foge à regra, para que possam se comunicar, são necessários equipamentos específicos que façam sua interligação. Esses equipamentos são conhecidos como comutadores de pacote, pois enviam dados em partes por meio da rede de origem até o destino. Os comutadores mais comuns são os roteadores e *switches*. Os *switches* são utilizados geralmente em redes LAN, enquanto os roteadores são utilizados no núcleo destas, fazendo com que redes diferentes possam comunicar-se (KUROSE; ROSS, 2010).

A utilização das redes deixou de ser apenas uma ferramenta de compartilhamento de dados entre dispositivos, e se tornou uma ferramenta muito poderosa, muito por conta da explosão das mídias sociais, e também muito pela grande expansão dos comércios virtuais, que vem crescendo ano a ano, como base só no ano de 2014 o e-commerce no Brasil teve um crescimento de 24%. Esses números só mostram o como as redes de computadores são fundamentais (E-COMMERCE, 2015).

2.1 PROBLEMAS E SOLUÇÕES EM REDES DE COMPUTADORES

Uma infraestrutura de rede construída sem um bom planejamento, acaba ocasionando alguns fatores que podem prejudicar sua performance. Um dos fatores que pode influenciar o desempenho em uma infraestrutura de rede, são as escolhas dos equipamentos de interconexão. Dispositivos como hubs por exemplo, são produtos de baixo valor que tem como objetivo apenas estender a distância de uma rede. Porém, são equipamentos não inteligentes, e que não possuem mecanismos para identificar o tráfego de dados que está passando por ele, e apenas retransmitem

os sinais de uma rede para todos os demais. Portanto se um quadro enviado possui erros, ou não cumpre o comprimento mínimo ou máximo padrão as informações são repassadas mesmo assim. Caso aconteça uma colisão em uma das portas, ela se estenderá para todas as outras portas do hub, pois toda as estações conectadas ao hub, sem exceção, recebem todo o tráfego, sendo útil ou não (CLARK; HAMILTON, 1999).

Também em uma rede de computadores mal elaborada, podem ocorrer pacotes em excesso em uma sub-rede, ou em parte dela, isso vai deixando o ambiente de comunicação degradada, deixando os nós da rede lentos, ocasionando um congestionamento. Uma rede com problema de congestionamento pode chegar a condição de impasse (*deadlock*) (COMER, 2006).

Quando há um aumento na quantidade de informações trafegando na rede, pode ocorrer problemas de perdas de pacotes, e quando isso ocorre pode se transformar em um grande problema na rede, pois as informações podem não chegar ao destino corretamente, e conseqüentemente tendo que reenviar os pacotes perdidos, resultando em mais congestionamento na rede (TANENBAUM, 2003).

Um problema muito grave que pode prejudicar a credibilidade de uma rede é falta de segurança da mesma, pois se não há uma política bem definida, e regras de acesso não tão rigorosas, pode deixar a rede muito vulnerável a qualquer ataque malicioso. Pois uma ameaça pode partir de uma possível violação da segurança do sistema, ocasionando alguns transtornos que podem ser irreversíveis, como a destruição de informação ou de recursos, modificação ou deturpação da informação, roubo, remoção ou perda de informações, revelação de informações confidenciais e interrupção de serviços (SOARES, 1995).

Podem ocorrer em uma rede de computadores ameaças que podem ser classificadas como acidentais, ou intencionais, podendo ser ativas ou passivas. As ameaças acidentais são aquelas que não estão vinculadas a intenção premeditada, como bugs de *software* e *hardware*. As ameaças intencionais se definem pela variação desde a observação de dados com ferramentas simples de monitoramento de redes, ataques sofisticados baseados no conhecimento de como funciona o sistema. Ameaças passivas que são as que, quando aplicadas, não resultam em alteração de nenhuma informação contida na rede. E as ameaças ativas onde as informações são modificadas em seu sistema ou em seu estado de operação (SOARES, 1995).

Definir e projetar uma rede de computadores, é o começo para solucionar problemas que já se encontram no ambiente e prevenir outros no futuro. Saber fazer a escolha de qual é o mais adequado para cada segmento, facilita muito no gerenciamento.

A segmentação da rede em muitas situações acaba se tornando uma boa solução para resolver os problemas citados anteriormente, e necessitam de equipamentos específicos para a sua implantação. Por exemplo, as interfaces de um *switch* de camada 2 podem ser configuradas em VLANs diferentes como os da camada 3. Mas caso há necessidade de que VLAN diferentes se comuniquem, será preciso um roteador ou *switch* que trabalhe na camada 3 (FILIPPETTI, 2008).

Avaliar o desempenho de um ambiente de comunicação é muito importante, principalmente quando tem um planejamento para se organizar a mesma de maneira eficiente, analisando seus gargalos e problemas pontuais, fazendo um inventario completo, para que assim possa se aplicar tecnologias para melhorar o desempenho e a segurança, e caso contrário, auxiliar no redimensionamento de uma nova topologia (TANEMBAUM, 2003).

2.2 DESEMPENHO EM REDES DE COMPUTADORES

A necessidade de, cada vez mais, buscar uma melhor forma de como os dados são transmitidos em redes convencionais e de telecomunicação, principalmente pela grande utilidade e popularidade que a mesma possui não é nova. Nesses ambientes muitas aplicações são extremamente utilizadas e posta ao seu limite por usuários que querem sempre obter, quando possível, o melhor de desempenho das aplicações buscando um maior nível de satisfação durante sua utilização (OLIVEIRA et al, 2008).

Para se obter um melhor desempenho das aplicações que é utilizado através da rede, é necessário conhecer seus requisitos, e também a situação atual dos canais de comunicação de testes e medições, a fim de inferir o melhor momento para utilização de determinada aplicação. Para determinar o estado momentâneo da rede, existem diversas ferramentas que realizam essa tarefa que trazem essas informações de várias maneiras. Porém, os dados apresentados, em geral, são muitas vezes, quase impossível de ser interpretado por usuários que não tenha tanta

experiência na área, e acaba se tornando inacessíveis para esses profissionais. Com isso, além dos requisitos das aplicações e dos resultados obtidos através dos testes, tem que se levar em conta o tipo de usuário que vai analisar o resultado e suas preferências, podendo esses dados ser apresentado de maneira distinta e específica para cada indivíduo, obtendo assim um diagnóstico e, conseqüentemente, uma recomendação mais precisa e confiável (OLIVEIRA et al, 2008).

2.2.1 Caracterização do Problema

O problema de roteamento de pacotes em ambientes de redes consiste em definir um caminho para que um pacote de dados possa navegar de um nodo de origem para um nodo destino na rede. Normalmente, se assume que a rede tem estabilidade de enlaces e nodos, admitindo prováveis falhas. Mas, no entanto, os estudos aplicados a redes de computadores dinâmicos revela que na maioria das vezes as técnicas tradicionais não são eficientes (ZHANG, 2006).

2.2.2 Métricas de desempenho em redes de computadores

Mesmo que possua um ambiente bem estruturado, uma das maiores dificuldades que pode ser encontrado na estrutura, é conseguir atender os requisitos de desempenho que se deseja. Uma vez que o projeto é homologado, pode ser necessário uma realização de testes para verificar a qualidade da rede. Às vezes, os engenheiros que planejaram o ambiente precisam analisar alguns cenários de operação, mais críticos, para assim analisar se os resultados obtidos cumprem as metas desejadas ou são compatíveis com os testes obtidos. Estas avaliações podem ser utilizadas tanto para avaliar cenários com grandes quantidades de dispositivos, quanto para realizar testes em dispositivos individualmente (CECHIN, 2005).

Seguindo um padrão de execução, as avaliações de desempenho são iniciadas com a inserção de um determinado tráfego na rede e, conseqüentemente, a realização da análise da rede a este tráfego disposto. O tipo de geração destes tráfegos, pode ser de forma simplificada ou aderir a padrões complexos (CECHIN, 2005).

Para poder avaliar se uma rede tem um desempenho adequado, é importante definir os principais parâmetros que serão utilizados para obter os resultados. Para que assim, se observe onde se encontram as eventuais deficiências de produtividade com precisão.

A medição de desempenho de um ambiente de dados, precisa ser executada várias vezes para evitar dúvida sobre o resultado obtido. E as medições devem ser efetuadas em dias e horas diferenciados para que o efeito de diferentes cargas do sistema sobre a quantidade medida possa ser verificada.

O conhecimento do desempenho de uma rede pode se justificar por alguns motivos, entre eles, contabilizar ou fiscalizar o uso dos recursos de rede, verificando se os recursos que as máquinas possuem são o suficiente ou não (HASSAN; JAIN, 2004).

2.2.3.1 Métricas de análise

A largura de banda que é a taxa de transmissão de informações que um enlace pode disseminar conteúdo, e possui três métricas que são relacionadas a largura de banda (SHRIRAM et al, 2005):

- a) **largura de banda de contenção:** é a taxa máxima de transmissão que uma rede pode obter ao transferir dados para um receptor, esta métrica não tem alteração com o aumento ou diminuição do tráfego;
- b) **largura de banda utilizada:** é a quantidade de dados sendo transferido por um enlace em tempo real;
- c) **largura de banda disponível:** é a taxa de transferência máxima que um dispositivo consegue chegar em determinado momento do caminho na transmissão de dados, esta medição considera o tráfego no momento da medição.

Outra métrica de análise é o atraso, que corresponde ao tempo de transmissão entre dois dispositivos da mesma rede ou diferente. O atraso de ida e volta é o tempo necessário que um pacote leva ao ser transmitido ao destino e retransmiti-lo a origem, chamado de *Round-Trip-Time* (RTT). Já o atraso em um sentido, é o tempo para que um pacote leva para sair do local de origem para um destino e vice-versa. O tempo gasto em uma transferência é a soma de vários fatores

para seu resultado, como o tempo para o dispositivo processar um pacote, processamento de CPU. O tempo de propagação é chamado de latência (SHRIRAM et al, 2005).

A métrica de variação do atraso é a diferença entre os atrasos na transferência de pacotes posteriores. Esta, é muito importante para aplicações multimídias em tempo real, porque a variação do atraso muito grande pode ter uma perda de desempenho muito significativo da aplicação (HASSAN; JAIN, 2004).

A perda de pacotes é quantidade de pacotes que chegam ao destino em relação a quantidade enviados. A situação que é mais favorável a esse cenário de perdas é a falta de espaço em *buffer* dos equipamentos utilizados e pacotes corrompidos causados por erros de transmissão (HASSAN; JAIN, 2004).

A disponibilidade é o passo primordial para conseguir medir o desempenho de um ambiente, pois determina se a rede está ativa, ou seja, se o tráfego está atravessando a rede (HASSAN; JAIN, 2004).

A partir das métricas mencionadas é possível fazer a escolha dos métodos de medição e quais ferramentas a serem utilizadas para descrever o desempenho de uma rede (SHRIRAM et al, 2005).

2.2.3.2 Definição de protocolos utilizados

Para a realização da medição, são utilizados alguns protocolos. A escolha destes varia de acordo com a metodologia que é adotado no projeto, ou mesmo, a ferramenta utilizada.

O protocolo IP (*Internet Protocol*) tem a função de roteamento, e as ferramentas se utilizam do campo *Time To Live* (TTL) para obter endereços dos equipamentos entre os dispositivos. É um protocolo não confiável. O protocolo Internet Control Message *Protocol* (ICMP) faz parte do protocolo IP e permite o envio de mensagens de erro ou de controle pela rede. O *Transmission Control Protocol* (TCP) é o protocolo mais usado para a transferência de informações entre dois dispositivos, sua grande vantagem é que esse protocolo implementa mecanismo de retransmissão, com isso garante que os pacotes de medição são totalmente transmitidos (HASSAN; JAIN, 2004).

2.2.4 Modelagem de redes de computadores

A modelagem é o modelo de projeto de uma situação real de sistemas que se quer analisar para um ambiente de simulação específico, de maneira que fique o mais próximo de um ambiente real, o comportamento desses sistemas diante das situações simuladas. Com isso, por exemplo, a segmentação lógica de um ambiente de comunicação através de VLAN, a modelagem é uma tarefa que exige muito mais do que conhecer o ambiente de simulação que será utilizado, mas também conhecimento teórico sobre VLAN, de detalhes dos componentes a serem modelados e dos objetivos que se quer alcançar com os testes. Um fator muito relevante é saber diferenciar emulação e simulação nos ambientes modelados. Pois a simulação é uma réplica da rede representando totalmente os detalhes envolvidos. Já a emulação tem o objetivo de extrair resultados da simulação, e transformar em estatísticas os dados obtidos. Com isso, na simulação não é necessário apresentar todas as funcionalidades, mas somente detalhes importantes de acordo com o que precisa saber (ALBERTI; SOUZA NETO; MENDES, 1999).

No próximo capítulo, será abordado sobre a segmentação de rede e suas funcionalidades.

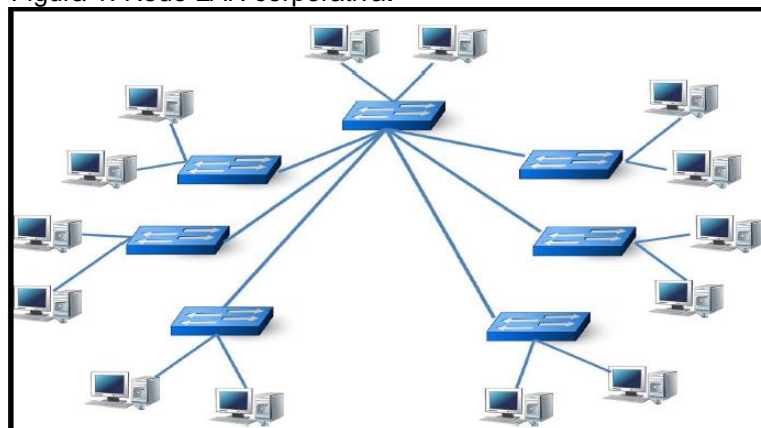
3 SEGMENTAÇÃO DE REDES DE COMPUTADORES

Para os profissionais que gerenciam e lidam com redes de computadores, o aumento do número de usuários, e a largura de banda disponível para suprir a demanda requisitada, fez que surgisse a necessidade de uma ampliação desses ambientes. Uma mudança na parte física da rede não envolve somente substituições das interfaces, mas também as alterações dos equipamentos pré-existentes. O principal problema desse tipo de atualização, mesmo que seja eficiente, não seria viável por ser de custo elevado (CLARK; HAMILTON, 1999).

Para obter uma rede com um bom funcionamento, um dos principais objetivos ao realizar um projeto bem elaborado, é conseguir reduzir todo tráfego desnecessário, e uma das maneiras de se fazer isso, é limitando o alcance do tráfego (*broadcast*) somente para os domínios para os quais ele é aplicável (KENYON, 2002).

O ambiente de uma organização de grande porte onde possuem mais de 300 dispositivos na rede por exemplo, ocorre uma exorbitante troca de informações em uma mesma rede física. Em uma empresa onde possuem muitos departamentos, certamente terá muitos setores em comuns mais também pouca comunicação entre diferentes departamentos. Com isso ocorre muito tráfego de dados congestionando a rede, conforme demonstra a figura 1. Além disso, o desempenho também é prejudicado devido ao grande número de domínios de *broadcast* (FEY; GAUER, 2015).

Figura 1. Rede LAN corporativa.



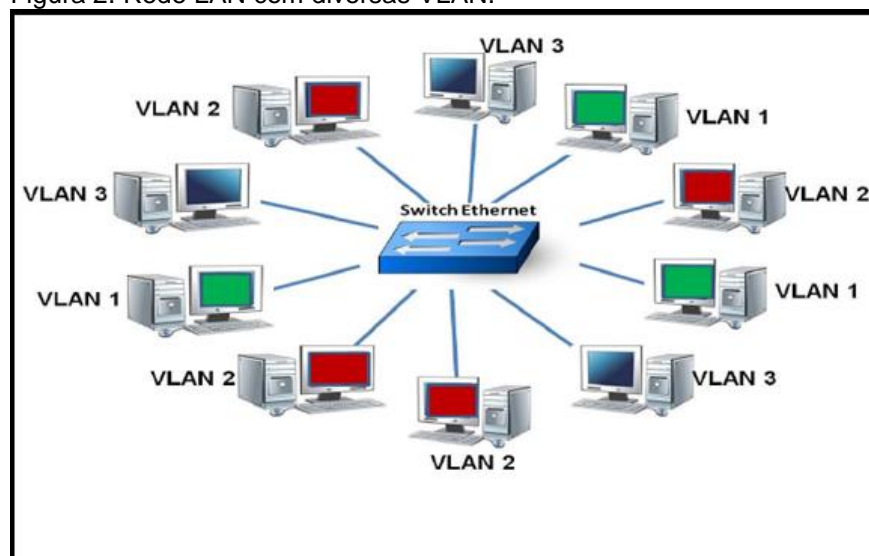
Fonte: Fey e Gauer (2015).

O domínio de *broadcast* é utilizado sempre que se necessita localizar o endereço *MAC address*² de um computador, e podem prejudicar a estrutura de comunicação de uma organização, com lentidão na transferência de dados, pelo fato destes através de conjuntos de equipamentos, ao enviar uma mensagem na rede, acabar enviando essa mensagem para todos os equipamentos (FEY; GAUER, 2015).

Uma boa opção para estruturação e funcionamento da rede sem que seja necessário a substituição de equipamentos é a segmentação da rede. Segmentar uma rede de computadores é fazer uma divisão lógica de segmentos simples de *Ethernet* em múltiplos segmentos, essa configuração é chamada de *Virtual Local Area Network* (VLAN). As redes lógicas funcionam de maneira parecida a uma LAN, a grande diferença em relação a esses ambientes, é que cada VLAN possui o seu próprio domínio de *broadcast*, o que significa que o tráfego diminui de maneira significativa. Quando não se utiliza uma rede *virtual*, o equipamento que gerencia a estrutura de comunicação como o *switch*, considera que todas as redes estão na mesma LAN, mas com a segmentação, pode ser criado vários domínios de *broadcast* e colocar cada dispositivo em domínios distintos (WENDELL, 2008).

Na figura 2, pode-se observar algumas VLAN, com dispositivos em cada uma delas, em apenas um *switch*.

Figura 2. Rede LAN com diversas VLAN.



Fonte: Fey e Gauer (2015).

²É um endereço físico associado à interface de comunicação, que conecta um dispositivo à rede.

Existem várias razões que tornam a segmentação de redes de computadores uma reorganização necessária (MUELLER; OGLETREE, 2004). As principais são:

- a) **limitações topológicas:** quando é necessário a inserção de mais pontos em uma rede, mas não sendo possível devido a limitação de distância ou o número de pontos por segmento que já esteja atingido;
- b) **limitações no protocolo de rede:** quando há a necessidade de agrupar dois ou mais segmentos de redes de endereços diferentes em apenas um segmento;
- c) **limitações na largura de banda de rede:** quando serviços de alto desempenho ou estações de trabalho consomem recursos altos de largura de banda do segmento;
- d) **segurança:** quando se tem o interesse de limitar acessos externos à rede local e acessos internos à rede externa, ou mesmo bloquear o acesso de determinados dispositivos a outras do mesmo segmento;
- e) **separação geográfica:** para impedir que o tráfego desnecessário não chegue a uma conexão remota.

Os principais equipamentos para realizar tal reestruturação, são *bridges*, roteadores e *switches*, conforme a tabela 1 (CLARK; HAMILTON, 1999).

Tabela 1. Comparação entre Domínios de Colisão e de *Broadcast* criados por dispositivo de rede

Dispositivos de Rede	Domínios de Colisão	Domínios de <i>Broadcast</i>
<i>Hub</i>	Um	Um
<i>Bridge</i>	Muitos	Um
Roteador	Muitos	Muitos
<i>Switch</i>	Muitos	Configurável

Fonte: Mueller e Ogletree (2004).

Para obter uma rede de alta qualidade, a redução do número de equipamentos por segmento acaba se tornando uma medida primordial para evitar problemas que reduzam o funcionamento do ambiente de comunicação, como colisões e *broadcasts*. Com a redução do número de dispositivos por segmento, diminui a possibilidade de ocorrer colisões, pois terá menos tráfego em um determinado momento. Para amenizar o *broadcast*, o ideal é criar uma barreira na

borda do segmento de rede para que assim o tráfego de *broadcast* não passe ou seja enviado (HUCABY, 2007).

Broadcast, é uma mensagem que é propagada para todos os dispositivos que pertence a um segmento de rede. O quadro *broadcast* é disseminado dentro de uma LAN, e repassado de um *switch* para outro, gerando um tráfego pesado na rede, e acaba afetando muito o desempenho da mesma (MORAES, 2010).

Existem algumas formas de segmentar e expandir uma rede de computadores utilizando alguns equipamentos, como *hubs*, *bridges*, roteadores e *switches* que podem ser tanto não gerenciáveis como gerenciáveis, que podem ajudar a minimizar os problemas do ambiente, mas não sendo tão vantajoso em relação as redes lógicas (HUCABY, 2007).

3.1 VIRTUAL LOCAL AREA NETWORKS (VLAN)

Grande parte das instituições e organizações de porte médio e grande, possuem em seus ambientes muitas redes locais que precisam suportar um grande número de usuários e aplicações de rede, independentemente da localização geográfica da organização (TANEMBAUM; WETHERALL, 2011).

Uma *Virtual Local Area Network* (VLAN), é um agrupamento lógico de usuários e equipamentos que estão logicamente conectadas, podendo ser criadas e configuradas por meio de *switches* que possuem essa opção de serviço disponível. Com isso é possível criar e disponibilizar várias redes lógicas dentro de uma física, ou seja, cada usuário é conectado fisicamente a uma LAN, e as características dos equipamentos conectados a determinada LAN, é definida pelas limitações dos dispositivos utilizados (como o número de portas do *switch*) e o tipo de conexões configuradas pelo administrador de rede (MORAES, 2010).

Uma vez configurada as redes, e os computadores instalados e configurados, seu alcance é estabelecido. Para realizar alguma alteração da rede local requer uma mudança nas conexões físicas. A conectividade lógica da LAN é igual a conectividade física (SEIFERT; EDWARDS, 2008).

Um *switch* possui várias portas de comunicação. E através dessas portas locais são inseridos os cabos de rede para realizar a interligação dos equipamentos, sendo que cada porta pode ser conectada a apenas um único dispositivo. Esses

equipamentos fazem a troca de informações entre os equipamentos conectados a ele através de endereços que estão contidos nos pacotes transmitidos para o correto caminho do destinatário. Ainda é possível interligar *switches* para cobrir uma infraestrutura que abrigue uma quantidade maior de computadores na rede (TANENBAUM; WETHERALL, 2011).

A utilização de *switches* para implementar grandes redes locais resolve alguns importantes problemas, como o domínio de *broadcast* e o número de dispositivos conectados em uma rede, além de proporcionar melhorias também com a segurança, configuração e gerenciamento. As redes virtuais possibilitam o isolamento da topologia física e lógica. Assim, permitem ter computadores interconectados, usando um ou vários *switches* configurados corretamente, independente da topologia física (MUELLER; OGLETREE, 2004).

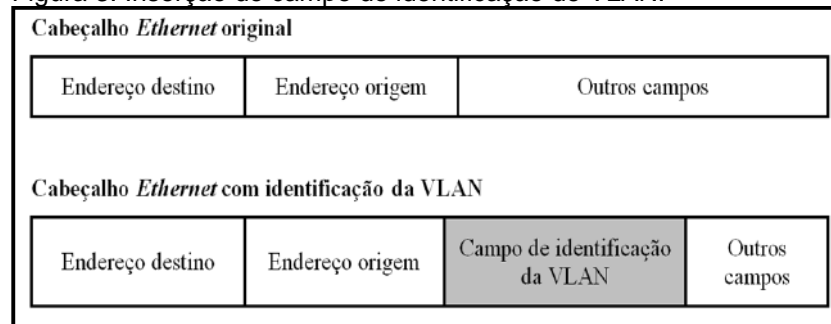
Caso possua vários *switches* em uma rede onde a VLAN é empregada, configurar todas as informações necessárias para o funcionamento manualmente, pode acarretar em um alto tempo caso seja necessário ser efetuadas alterações nessas configurações, pois todos os outros *switches* existentes na rede devem ser modificados também.

Para fazer a interligação de *switches* e propagar as configurações de VLAN em uma rede, é preciso criar um servidor de domínio *Virtual Trunk Protocol* (VTP), que será abordado detalhadamente mais adiante. Assim, o gerenciamento de VLAN pode ser centralizado em um único *switch* (servidor VTP) e os outros *switches* da rede devem fazer parte do mesmo domínio VTP para que possa obter as informações contidas no servidor (FILIPPETII, 2008).

Para os *hosts* se comunicarem em um ambiente de rede independente da VLAN que a pertença, são necessários alguns padrões de identificação que associem a VLAN de origem. Para que isso ocorra, o *switch* insere um *frame tagging* (que é um campo para identificação de VLAN) ao cabeçalho *Ethernet* (tecnologia de rede local baseado no envio de pacotes) original de modo que a mensagem possa ser recebida no dispositivo de destino. O método padrão para a identificação de *frames* foi desenvolvido pelo Institute of Electrical and Eletronics Engineers (IEEE) e é denominado 802.1q (FILLIPPETI, 2008)

A figura 3 demonstra os campos presentes em um cabeçalho *Ethernet* original e como fica o cabeçalho após a inserção do *frame* com a identificação da VLAN.

Figura 3. Inserção do campo de identificação de VLAN.

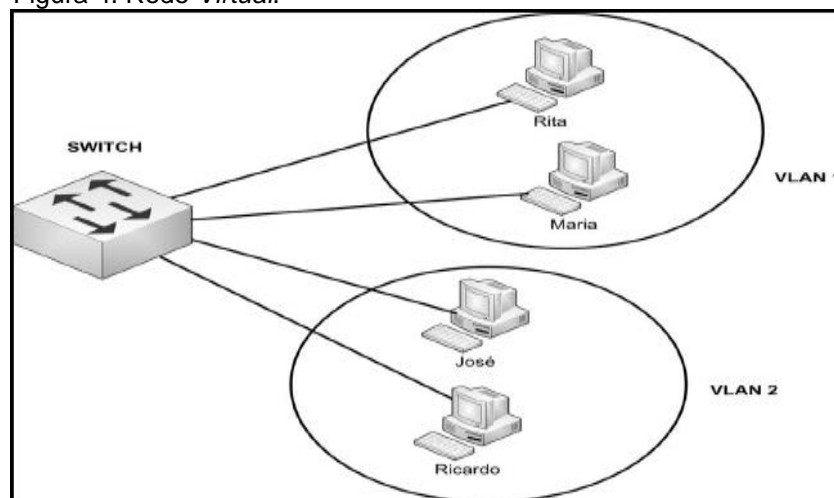


Fonte: Fillipeti (2008)

Em uma rede local, todos os dispositivos que estão ligados a um *switch* são entendidos por ele como pertencentes ao mesmo domínio de *broadcast*, ou na mesma LAN. Quando se utiliza VLAN é possível separar a rede local em múltiplos domínios de *broadcast* (ODOM, 2008)

Na figura 4 é possível observar um *switch* dividido em duas VLANs. No exemplo a seguir, na VLAN 1 estão alocados os usuários Rita e Maria. Na VLAN 2 estão os usuários José e Ricardo.

Figura 4. Rede *Virtual*.



Fonte: Moraes (2010).

A divisão da rede local em redes lógicas, possibilita ao administrador de rede uma maior facilidade para conseguir gerenciar os recursos que poderão fazer

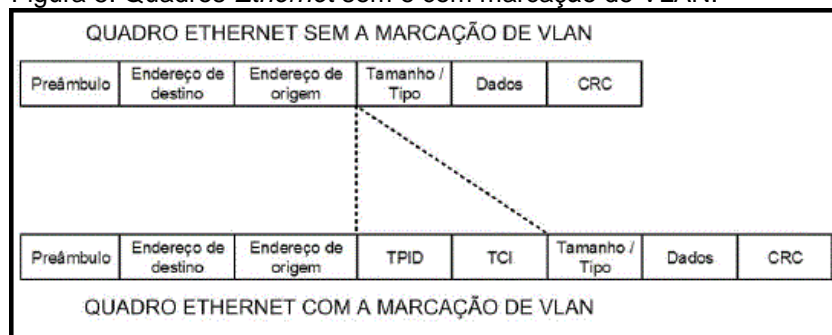
parte de determinados ambientes, assim conseguindo aplicar as devidas políticas de acordo com o grupo estabelecidos (CISCO SYSTEM, 2007)

3.1.1 O padrão IEEE 802.1Q

É o padrão que as VLAN seguem quando implementadas, e essa resolução foi publicada em 1998. O método que se é utilizado no reconhecimento resulta em quatro novos bytes de dados sendo anexados ao quadro entre os campos de endereço de origem e o de tamanho/tipo. Com isso o tamanho do quadro aumenta para 1522 bytes (SPURGEON, 2000).

Temos na figura 5 uma demonstração de como acontece na identificação de uma VLAN é adicionado ao quadro *Ethernet*. Os campos ficam com mesmo tamanho, exceto ao campo tamanho/tipo que é aumentado em quatro bytes.

Figura 5. Quadros *Ethernet* sem e com marcação de VLAN.



Fonte: Spurgeon (2000).

Após a realização de vários testes, foi chegada a uma conclusão que todas as interfaces *Ethernet* suportariam acomodar quatro bytes a mais do que já carregavam sem afetar o funcionamento. Essa mudança no tamanho do quadro, então foi especificada no padrão IEEE 802.3ac, e adotada como parte do padrão *Ethernet* a partir de 1998. A *Tag Protocol Identifier* (TPID) é um campo de dois bytes que identifica o quadro como sendo um *frame tagged* (quadro identificado). Os próximos dois bytes contem a *Tag Control Information* (TCI). Três bits desse campo são utilizados para poder transportar a informação de prioridade baseada nos valores definidos no padrão IEEE 802.1p. Com isso, o padrão 802.1Q surgiu para estender a prioridade ao tratar aspectos do padrão 802.1p na VLAN *tag* (identificador de VLAN) para direcionar a

prioridade do tráfego. Isso fez com que a informação de prioridade do tráfego possa ser enviada entre *switches* utilizando o protocolo VLAN (SPURGEON, 2000).

O padrão IEEE 802.1Q realiza também as associações de VLAN usando *Trunk Link* (Enlace Tronco). Isso permite que *switches*, roteadores ou qualquer outro equipamento de rede consiga enviar tráfego por várias redes virtuais utilizando um único caminho (ODOM; HEALY; MEHTA, 2008).

Esse método ainda por ser padronizado, permite que VLAN *Trunks*, possam operar em equipamentos de diferentes fabricantes. Em particular, o padrão 802.1Q define uma arquitetura para a implementação de redes virtuais, os serviços prestados, os protocolos e algoritmos utilizados (HUCABY, 2007).

3.1.2 Vantagem na utilização de VLAN

Ao trabalhar com rede *virtual*, reduz consideravelmente os problemas encontrados em uma rede de computadores, tornando muito mais eficiente e econômica, principalmente em redes corporativas, onde a qualquer momento pode haver a necessidade de reestruturação do sistema, ou mesmo o aumento no número de usuários, entre outras situações, que requerem uma flexibilidade, como pode se obter com VLAN para as redes locais (MORAIS, 2005).

Pode se observar algumas vantagens na utilização de redes virtuais. Os autores Fillipeti (2008), Moraes (2010) concordam que dentre essas vantagens podem ser citadas:

- a) **redução de domínios de *broadcast***: os *broadcasts* são responsáveis por grande parte do tráfego total da rede, tornando assim o desempenho das tradicionais redes locais inferior ao das VLAN. Com a rede segmentada *virtualmente* reduz o envio de pacotes para endereços desnecessários, aumentando a capacidade de toda a rede;
- b) **maior segurança**: com a divisão de redes virtuais se consegue mais segurança, já que estas só se comuniquem com os dispositivos que estão na mesma VLAN. Por exemplo, as redes do setor de administração são separadas do setor de marketing, diminuindo as chances de acesso a informações confidenciais. No caso somente através de um dispositivo

de rede com a função roteador é possível realizar a comunicação entre VLAN distintas;

- b) **maior eficiência para gerenciamento:** com rede *virtual* é possível para o administrador de rede ter um maior controle da rede, já que pode configurar as portas dos *switches* e alocar os usuários de maneira que facilite a organização da estrutura e seu controle;
- c) **topologia de rede independente:** além da facilidade do gerenciamento, é possível com a utilização de redes lógicas, obter uma topologia totalmente autônoma da rede física, e com isso vai proporcionar uma maior flexibilidade e escalabilidade caso a rede sofra mudanças estruturais.

3.1.3 Tipos de VLAN

É possível configurar a porta de um *switch* para pertencer a uma ou mais VLAN. Para fazer parte de uma rede *virtual*, a porta de um *switch* deve ser associada a uma rede lógica. O método de associação pode ser configurado para trabalhar de forma estática ou de forma dinâmica (CISCO SYSTEM, 2007).

O método de associação estática é o mais utilizado e fácil de monitorar, em um ambiente de rede onde há poucos usuários. Nesse modelo, as portas do *switch* são designadas a uma determinada rede lógica pertencendo a esta até que o administrador de rede altere estas configurações. É logo que um dispositivo entra na rede, o mesmo passa a fazer parte da rede virtual, onde é indicado a porta pertencente, e caso ocorra uma mudança de porta, o responsável pela rede terá que, manualmente associar a porta à VLAN (FILIPPETTI, 2008).

O método de associação dinâmica funciona de maneira em que um dispositivo conectado a um segmento de rede uma atribuição de VLAN de forma automatizada. Isso ocorre utilizando aplicações que realizem esse tipo de tarefa, é possível associar VLAN por meio de endereçamento de *hardware*, endereço MAC, por protocolos ou de forma autenticada (FILLIPETTI, 2008).

Na camada de enlace, os integrantes de uma VLAN são definidos através do endereço MAC ou físico. Um quadro enviado de um computador para outro deve conter o endereço MAC do receptor. Na figura 6 o *switch* reconhece o endereço de

hardware vinculado a cada rede virtual. Quando ocorrer uma alteração física do dispositivo, não é necessária qualquer mudança na configuração (ZHU; MOLLE; BRAHMAN, 2004). A desvantagem dessa configuração, é a exigência de que todos os utilizadores estejam configurados logo no início em pelo menos uma VLAN. Em uma rede com um grande número de dispositivos, esta identificação inicial torna-se um trabalho bastante custoso. A vantagem de uma configuração prévia obrigatória, impede que usuários não autorizados se conectem à rede apresentando uma maior segurança (CISCO SYSTEM, 2003).

Figura 6. Associação de portas de um *switch* a diferentes VLAN.

Portas	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
VLAN	0	0	0	0	1	1	2	2	2	1	1	0	1	1	2	0

Fonte: Cisco System (2003).

As VLAN baseado em protocolos, é ideal para ambientes que suportam múltiplas variedades de protocolos, ou que se baseiam em endereços da camada de rede. São identificadas de acordo com o tipo de protocolo ao qual obedecem, segundo o exemplo da figura 7 (ZHU; MOLLE; BRAHMAN, 2004).

Figura 7. Associação de protocolos a diferentes VLAN.

Protocolo	IP	IPX	NetBios
VLAN	0	0	1

Fonte: Zhu, Molle e Brahman (2004).

Entre as VLAN baseadas em protocolos destacam-se as redes virtuais baseadas no endereço IP, operam com base em informações da camada 3 do modelo OSI (Rede). Na figura 8, os membros de cada VLAN são determinados pelo cabeçalho de nível 3, podendo fazer uso do endereço IP para tal classificação (ZHU; MOLLE; BRAHMAN, 2004).

Figura 8. Associação de endereços IP às VLAN.

Endereço IP	172.16.4.8	172.16.12.16	172.16.5.9	172.16.5.10
VLAN	1	3	2	2

Fonte: Zhu, Molle e Brahman (2004).

A desvantagem de se utilizar este método, prende-se com o tempo para a transmissão de pacotes utilizando informações do nível de rede, que normalmente é maior do que o caso da utilização do endereço MAC. Porém, quando o usuário se deslocar para qualquer lugar dentro do mesmo ambiente, não há qualquer necessidade de reconfigurar os endereços, o que acaba sendo uma vantagem desse método (CISCO SYSTEM, 2003).

3.2 TIPOS DE CONEXÃO DE DISPOSITIVOS EM VLAN

Os computadores das redes virtuais podem ser conectados de três formas diferentes, considerando se estes suportam ou não o padrão IEEE 802.1Q (IEEE SOCIETY COMPUTER, 2006).

O Enlace Tronco (*Trunk Link*) é onde os equipamentos ligados à essa rede *virtual* devem reconhecer quadros com a identificação da rede lógica, e pode inserir e remover informação no cabeçalho da *tag*, ou seja, ser *VLAN-aware* (IEEE SOCIETY COMPUTER, 2006).

O Enlace de acesso (*Access Link*) é o tipo de enlace que o dispositivo conecta sem suporte a uma rede *virtual* a uma porta *Virtual Local Area Network aware* (IEEE SOCIETY COMPUTER, 2006).

Já o Enlace Híbrido (*Hybrid Link*) é uma junção dos Enlaces Tronco e de Acesso. No enlace híbrido são conectados tanto dispositivos *VLAN-aware* quanto equipamentos *VLAN-unaware* (não reconhece quadros com *Virtual Local Area Network tag*, isto é, não possuem suporte ao padrão IEEE 802.1Q) (IEEE SOCIETY COMPUTER, 2006).

Uma rede *virtual* pode possuir ao mesmo tempo os três tipos de enlaces citados sem problema algum. Considerando as classificações de rede *virtual* e os computadores que podem ser conectados a elas, torna-se possível propor uma solução para segmentação de redes de computadores (IEEE SOCIETY COMPUTER, 2006).

3.3 SOLUÇÃO VTP (VIRTUAL TRUNKING PROTOCOL)

Antes do protocolo VTP, para atualizar os parâmetros nos *switches*, era necessária uma tarefa manual para realizar as alterações em todos os *switches*, o que tornava um trabalho um pouco inviável em caso de uma rede de dimensões grandes. Com isso surgiu a necessidade de todo esse processo ser realizado de forma centralizada e gerenciada, garantindo que qualquer alteração nos parâmetros fosse reconhecida por todos os outros dispositivos (GOUVEIA; MAGALHÃES, 2005).

O VLAN *Trunking protocol* (VTP) é um protocolo criado pela Cisco System, criado para resolver o problema mencionado anteriormente (GOUVEIA; MAGALHÃES, 2005).

É possível configurar o *switch* para trabalhar em alguns modos de VLAN *Trunking Protocol* tais como servidor VTP, que permite criar, modificar e deletar redes virtuais e especificar outros parâmetros de configuração, como a versão do VTP e retirar configurações desnecessárias. Esses clientes, que é praticamente da mesma maneira do servidor de *Virtual Local Area Network Trunking Protocol*, porém não pode criar, modificar ou deletar *Virtual Local Area Network*. VTP transparente, onde um *switch* transparente de VLAN *Trunking Protocol* não é informado sobre a configuração da Rede Virtual e não realiza a sincronização da configuração baseada nas informações recebidas, mas ele repassa a configuração para fora da sua porta de *Trunking*. Com esse protocolo desligado, se comportam da mesma maneira do transparente, porém as informações recebidas não são transmitidas (CISCO SYSTEM, 2002).

O funcionamento desse protocolo acontece de maneira semelhante ao protocolo de roteamento, que faz com que o protocolo troque informações periódicas sobre atualização. Para um bom funcionamento da Rede Virtual baseado no protocolo VTP, cabe ao administrador começar primeiro a criação de um domínio no protocolo e determinar quais os *switches* que pertencem ao domínio (ODOM; HEALY; MEHTA, 2008).

Esse protocolo divulga as informações de configuração de Redes Virtuais aos *switches* próximos para que a configuração possa ser feita em cada um, com todos os outros *switches* no ambiente aprendendo a informação da rede lógica dinamicamente. O VTP anuncia o VLAN ID, o nome e o tipo da Rede *Virtual* para rede lógica. Contudo, o VLAN *Trunking Protocol* não divulga qualquer informação sobre em quais portas deveria estar cada Rede Virtual, então a configuração para associar uma

interface do *switch* a uma rede virtual em particular ainda deve ser feita em cada dispositivo individualmente. A tabela 2 mostra, de forma resumida, os modos de operação e características do VTP (ODOM; HEALY; MEHTA, 2008).

Tabela 2. Modos e características do VLAN Trunking Protocol (VTP).

Função	Modo Servidor	Modo Cliente	Modo Transparente
Origina anúncios VTP	Sim	Sim	Não
Processa anúncios recebidos para atualizar a configuração da VLAN	Sim	Sim	Não
Encaminha anúncios VTP recebidos	Sim	Sim	Sim
Cria, modifica e deleta VLANs	Sim	Não	Não

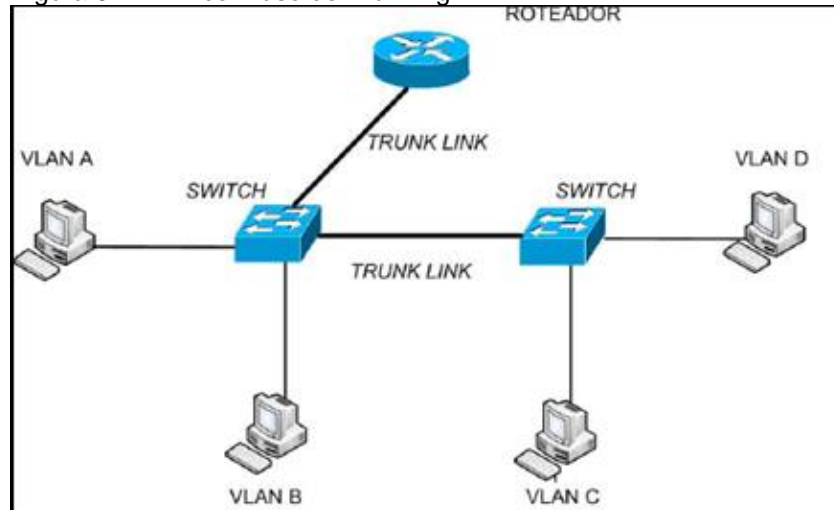
Fonte: Odom, Healy e Mehta (2008).

Na figura 9, cada *switch* trabalha com duas Redes Virtuais. No primeiro dispositivo, VLAN A e VLAN B passa através de uma única porta para o roteador e através de outra porta para o segundo *switch*. VLAN C e VLAN D utilizam *Trunking* do segundo para o primeiro *switch* e do primeiro *switch* para o roteador. O processo de *Trunking* pode carregar tráfego de todas as quatro VLAN. O *link* de *Trunking* do primeiro *switch* para o roteador também pode carregar os dados das quatro redes lógicas configuradas. O que acontece, é que esta conexão do roteador permite que este mesmo roteador apareça em todas as quatro Redes Virtuais, como se existissem quatro portas físicas diferentes conectadas ao *switch* (ODOM; HEALY; MEHTA, 2008).

O que também pode acontecer são que as redes virtuais podem estabelecer comunicação entre si por meio da conexão *Trunking* entre os dois dispositivos utilizando o roteador. Como exemplo temos um usuário que precisa enviar dados de seu dispositivo que se encontra na VLAN A para um computador pertencente a VLAN B, ou outra rede *virtual* ser for o caso, então as informações devem trafegar do *switch* para o roteador e novamente para o *switch*. Devido ao reconhecimento automático e ao *Trunking*, os computadores e o roteador acham que eles estão no mesmo segmento físico. O *Trunk* possibilita a união de várias interfaces físicas para

formar uma interface lógica, o que proporciona um aumento da largura de banda sem a necessidade de tecnologia do *backbone*³ (FURUKAWA, 2004).

Figura 9. VLAN com uso de Trunking.



Fonte: Furukawa (2004).

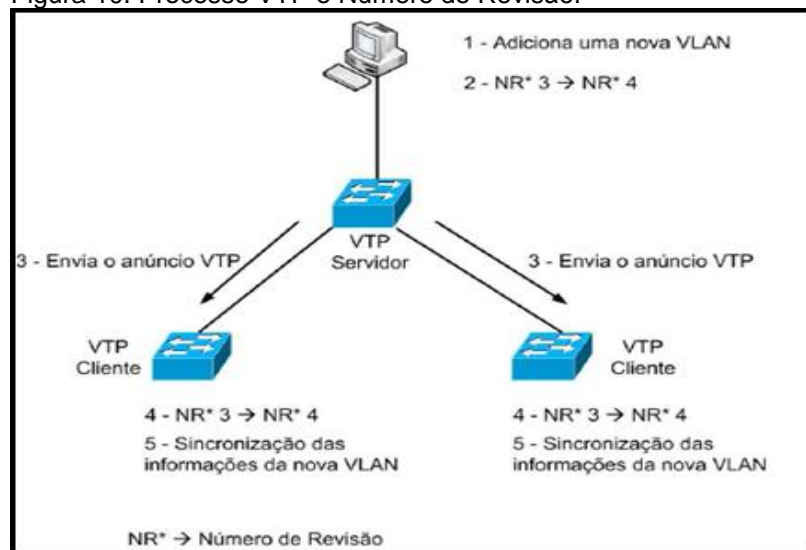
3.3.1 O Processo VTP e Números de Revisão

O número de revisão é um dos principais componentes de um anúncio VTP. É um número de 32 bits que tem o objetivo de indicar o nível de revisão para um quadro de uma rede lógica *trunking protocol*. O valor padrão de configuração para um *switch* é zero. Cada vez em que um *switch* no modo Servidor VTP faz alguma ação, como adicionar, deletar ou modificar alguma configuração de uma Rede *Virtual*, ele incrementa o número de revisão em uma unidade. O maior número de revisão dentro de um domínio de VLAN *Trunking Protocol* carrega a informação mais atualizada. Quando um *switch* em modo Cliente recebe um número de revisão superior o que possui, ele deve atualizar sua configuração de Rede *Virtual* sobrescrevendo suas informações com o banco de dados VTP do número de revisão mais alto. Quando há uma alteração do nome de domínio desse protocolo, não aumenta o número de revisão. Ao invés disso, o valor volta a ser zero. O processo de atualização começa quando o administrador configura um *switch* no modo servidor e modifica a configuração de uma rede lógica. A figura 10, mostra de forma exemplificada o

³ Backbone: é uma rede principal por onde os dados do cliente da Internet trafegam.

anuncio VTP com os seguintes passo: 1 – uma nova VLAN é adicionada; 2 – número de revisão antigo era 3 e é atualizado para 4; 3 - o Servidor VTP realiza o anúncio e propaga o banco de dados para os outros *switches*; 4 – os clientes recebem o anúncio e atualizam o número de revisão de 3 para 4; 5 – acontece a sincronização de informações da nova VLAN (ODOM; HEALY; MEHTA, 2008).

Figura 10. Processo VTP e Número de Revisão.



Fonte: Odom, Helay e Mehta (2008).

O número de revisão tem um papel de fundamental importância e complexa ao permitir que o VTP distribua e sincronize esse domínio e ainda as informações de configuração de VLAN.

Mesmo após fazer uma correta configuração de domínios VTP nos *switches*, podem aparecer outros fatores que podem negativamente afetar a funcionalidade (ODOM; HEALY; MEHTA, 2008).

4 SIMULAÇÃO

A simulação pode ser definida como uma técnica que pode ser utilizada por acontecer em um ambiente monitorado, onde os testes executados podem ser repetidos indeterminadas vezes sem que cause danos nenhum aos atores da cadeia. Tem dois importantes detalhes necessários a simulação, o primeiro refere-se ao ensino baseado em trabalhos, no qual se enfatiza o que se quer obter e como obter tal objetivo proposto, e o segundo é a relação com o simulador (ALECRIM, 2009).

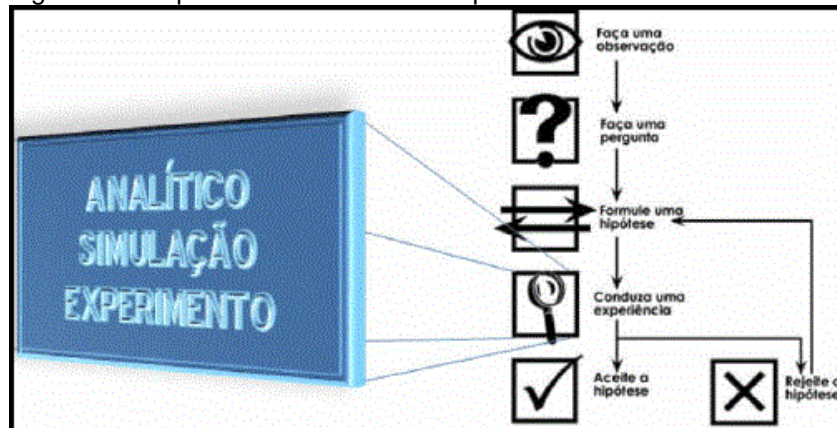
O início do uso dessa técnica foi no começo dos anos 60 coincidentemente com a entrada dos computadores no mercado mundial. A simulação é uma técnica que exige o uso de um computador, pois é uma tarefa que exige uma grande quantidade de cálculos matemáticos. No começo, a simulação foi utilizada pelos Estados Unidos, que utilizavam essa técnica para realizar planejamentos em operações militares. Já o seu início na indústria dos Estados Unidos ocorreu logo em seguida (UTZIG, 2007).

Com o grande avanço da Tecnologia da Informação, os desafios em se planejar novos projetos de rede aumentam no mesmo ritmo, e com isso, cada vez mais o uso da simulação em novos projetos, estão se tornando essenciais para determinar os cenários adequados a ser implementado, de acordo com as variáveis que podem fazer parte do ambiente, podendo realizar simulação de redes de filas simples até cenários mais complexos de acordo com a necessidade (MENDEZ; YUNUS; MUKHOPADHYAY, 2011).

4.1 OBJETIVOS DA SIMULAÇÃO EM REDES DE COMPUTADORES

A simulação se tornou uma ferramenta essencial para auxiliar na viabilidade ou não de uma determinada situação. Geralmente, uma experiência é a base para validar um cenário, mas para utilização de projetos de rede, uma hipótese pode ser validada baseado nas seguintes métricas: analítico, simulação e experimento controlado, a figura 11, ilustra as etapas do processo (ARAUJO; CASTRO; HOLANDA, 2009).

Figura 11. Etapas do método científico para cenários de rede



Fonte: Araujo; Castro e Holanda (2009).

Na validação de um cenário, a modelagem matemática analítica é baseada em cálculos e fórmulas matemáticas, já o experimento é baseado em uma análise em cima de uma situação real monitorada. Com as simulações, são planejados cenários virtuais, com o máximo de proximidade com a realidade, possuindo como base para os testes ferramentas de processamento de dados, para assim poder gerar informações e obter resultados antes de implementar o experimento real (ARAUJO; CASTRO; HOLANDA, 2009).

A utilização do método de simulação tem se mostrado muito eficaz, apresentando alguns benefícios, como o controle de detalhes, gastos reduzidos, segurança de que os objetivos de desempenho serão atendidos antes da compra do equipamento, identificação dos possíveis gargalos antes da implementação e redução do tempo na implementação. Algumas áreas vêm se destacando no uso dessa técnica, as companhias aéreas para aperfeiçoamento de seus pilotos, a área da medicina, com o objetivo de treinar médicos em procedimentos cirúrgicos (UTZIG, 2007).

Para realizar as simulações de rede, é necessário a utilização de programas de simulação ou simuladores, para que se possa realizar os testes de como um ambiente real irá se comportar com diferentes variáveis, e com isso produzir fielmente o sistema analisado. Assim é possível moldar o simulador para cumprir as tarefas especificadas, fazendo com que se tenha um comparativo do custo e tempo ao criar uma nova estrutura de rede. Também é possível testar situações e eventos

onde a emulação no *hardware* real não seria possível, mas que podem ser úteis a simulação de novos protocolos de rede (MENDEZ; YUNUS; MUKHOPADHYAY, 2011).

Pode-se classificar um modelo de simulação de acordo com alguns critérios a serem observados (TAVIERA, 1997):

- a) **determinísticos ou estocásticos:** modelos determinísticos não tratam as variáveis randômicas e as características operacionais trabalham com relações exatas. O modelo estocástico trata como uma variável do sistema se comporta de forma probabilística.
- b) **estáticos ou dinâmicos:** modelos estáticos não consideram explicitamente a variável tempo, tem relações determinísticas e normalmente são tratados por técnicas analíticas. Os modelos dinâmicos tratam com interações variáveis no tempo, o estudo do sistema em um certo instante interfere no estado do sistema no instante seguinte.
- c) **discreto ou contínuo:** o modelo discreto sofre alterações repentinas no tempo. As mudanças no sistema são expressas em termos do estado do sistema no início do período. As mudanças que ocorrem durante um intervalo de tempo são calculadas e é deduzido um novo estado do sistema para o final deste período e início do período. O modelo contínuo sofre constantes e suaves alterações no tempo.

4.2 SOFTWARES DE SIMULAÇÃO PARA REDES

As ferramentas de simulação de redes são muito importantes na hora de realizar os experimentos de forma a obter uma modelagem mais próxima possível do mundo real, e cada vez mais essas ferramentas estão evoluindo na área de redes de computadores (DOURADO; FILHO; MARQUES, 2011).

Além de ferramenta importante para profissionais administradores de rede que utilizam a simulação para minimizar ao máximo gastos desnecessários ao implementar uma nova estrutura, os simuladores tem outro objetivo, complementar o ensino de vários temas e conteúdo mais técnicos da área de redes, auxiliando aos estudantes no entendimento de conceitos abstratos e complexos de se compreender,

com isso, agregando no aprendizado do aluno e motivando os mesmos a apreender todo o processo de ensino (DOURADO; FILHO; MARQUES, 2011).

Para a realizar as experiências através de simulação, foi realizado uma pesquisa para se obter o software que cumprisse os requisitos necessários para realizar o projeto. Existem vários softwares disponíveis no mercado para tal finalidade, na qual podemos citar alguns como, Cloonix, Cisco *Packet Tracer*, Core, GNS3, IMUNES, LINE *Network Emulator*, Marionnet, Mininet, Netkit, NS-3, OPNET Riverbed *Modeler Academic Edition*, Psimulator2, Shadow, *Unified Networking Lab*, VNX, VNUML, onde cada software tem suas particularidades, vantagens e desvantagens na hora da escolha da melhor ferramenta a se utilizar em um experimento de simulação.

Muitas experiências em simulações exposta em artigos e trabalhos, apresenta o OPNET com um dos principais softwares de simulação. Apontando o OPNET como uma ferramenta poderosa para a obtenção de gráficos de análises para vários elementos, tais como *switches*, *links*, e também roteadores (AL-HADIDI, 2014).

Com o OPNET é possível realizar simulações de redes com configurações fiéis a realidade, possibilitando que sejam coletadas e analisadas diversas estatísticas a respeito da simulação, até como forma de complementar exercícios de laboratórios específicos para curso de redes. A uma comparação com outro software bastantes utilizado o GNS3, porém para a utilização desse software é necessário obter o IOS do roteador, caso contrário não é possível realizar as simulações, o que torna a utilização mais trabalhosa e complicada, além de outros softwares como Cnet que não tem versão para ambiente Windows, e outros software com suas particularidades (VOSS, 2012).

Com as informações obtidas, optou-se pela utilização do software OPNET para os experimentos a serem analisados, além de ter uma versão acadêmica que é disponibilizada gratuitamente, possuir documentos para o auxílio de sua utilização, também é uma ferramenta que não exige um hardware robusto para sua instalação.

O Opnet Riverbed *Modeler Academic Edition 17.5*, é desenvolvida pela Opnet IT *Techonogies Inc.*, é uma ferramenta de simulação que disponibiliza um ambiente virtual para modelagem, análise e assim poder obter prognóstico de desempenho de infraestrutura de TI, incluindo aplicações, servidores e tecnologias de redes de computadores. É um programa utilizado por milhares de organizações

comerciais e governamentais em todo o mundo, e por mais de 500 universidades, para a criação de cenários de simulação de redes, nós, enlaces, sub-redes, protocolos, equipamentos e serviços, disponibilizando recursos gráficos e uma interface amigável. Para executar o projeto proposto foi utilizado a versão OPNET IT *Riverbed Modeler Academic Edition* 17.5, lançado em 2014, destinada a fins acadêmicos, que possui todas as ferramentas necessárias para a execução do trabalho, e não exigir uma máquina com processamento muito alto para a sua utilização. Na figura 12 mostra a tela inicial do *software* OPNET.

Figura 12. Tela inicial do software OPNET IT Riverbed Modeler Academic Edition



Fonte: Autor.

4.3 PROJETO E ANÁLISE DE EXPERIMENTOS DE SIMULAÇÃO

Pelo fato das entradas da simulação ser aleatório, um modelo de simulação gera uma estatística estimada do resultado e não algo totalmente exato. Dentro dos resultados obtidos, para se ter um número estatisticamente preciso, com uma pequena variação, o analista deve especificar para configuração de rede algumas opções como, o tempo de cada execução de simulação, e a definição do número de simulações independentes a serem executados (HALSALL, 1996).

É necessário realizar algumas vezes as tarefas de simulação para cada configuração no intuito de que os resultados possam ser o mais confiável possível, baseado no intervalo de confiança que se deseja alcançar (PEGDEN; SHANNON; SADOWSKI, 1995).

Um intervalo de confiança é um intervalo numérico onde se tem $(1 - \alpha)$ chances de conter o real valor da medida a ser analisada, em que $(1 - \alpha)$ é o nível de confiança e α o erro permitido na probabilidade do aparecimento do valor real da variável no intervalo de confiança. Como base pode se levar em consideração um erro permitido de 5% do valor real da variável estar no intervalo, $\alpha = 0,05$, o que significa que há 95% de chance de o valor real estar contido no intervalo (MAHAJAN; INGALLS, 2004).

O cálculo do intervalo de confiança se dá em obter a média (μ) e o semi intervalo (h), onde o intervalo é limitado por $[\mu - h, \mu + h]$. Com o intervalo de confiança encontrado, é possível determinar o valor tabelado da variável normal padronizada (z), que será usado no cálculo do número de replicações. Então aplica-se a fórmula $n = \left(\frac{100z\sigma}{r\mu}\right)^2$ onde n é o número de replicações, z o valor da variável padronizada, σ o desvio padrão, r a precisão requerida e μ a média na amostra. Quando se obtém um valor decimal no resultado, o valor é arredondado para o próximo valor inteiro (MAHAJAN; INGALLS, 2004).

Com base na fórmula apresentada anteriormente, para o presente projeto temos a média (μ) 72103,44 GB/s, o desvio padrão (σ) de 171530,04 GB/s e a precisão requerida de 1800, empregando o nível de confiança de 95%, o valor de z é 1,96 (valor tabelado) e o número de replicações é de 22 replicações.

Realizar tarefas independentes significam usar diferentes números aleatórios para cada execução, começando cada uma delas no mesmo status inicial, e redefinir o modelo de contadores estatísticos ao estado inicial de zero no início de cada execução. A estimativa global deve ser mais preciso que desempenho estimado individualmente. Tem que se observar que as execuções independentes são necessárias para se obter estimativas de variância legítima e simples confiáveis nos intervalos (LAW, A. M., KELTON, W. D, 1991).

Ao simular certos tipos de sistema de comunicações, é dada importância mais para os resultados de longo prazo. No outro lado, simulações destes tipos de sistemas

geralmente começam com o sistema em um estado vazio e inativo. Isso resulta nos dados de saída não sendo muito relevantes. Portanto, simulações são muitas vezes executados por um determinado período de tempo, onde os são realmente usados para estimar a medida de desempenho desejado (PEGDEN; SHANNON; SADOWSKI, 1995).

5 TRABALHOS CORRELATOS

A segmentação *virtual* de redes de computadores pode ser utilizada em diferentes situações com o objetivo de melhorar o desempenho e a segurança de uma rede. A seguir serão descritos alguns trabalhos buscando destacar o foco de algumas das pesquisas.

5.1 PROJETO DE IMPLEMENTAÇÃO DE REDE LOCAL HIERÁRQUICA NO CAMPUS PONTA GROSSA DA UNIVERSIDADE TECNOLOGIA FEDERAL DO PARANÁ

Esta monografia foi desenvolvida por Fabian Maurice Malheiros Franco e apresentada à Universidade Tecnológica Federal do Paraná em 2012. O objetivo é apresentar e explorar os recursos disponíveis por meio da utilização do conceito de VLAN. Será proposto um modelo de implementação em uma rede, que apresenta lentidão ou até mesmo de indisponibilidade da rede.

Foi utilizado o conceito de VLAN, e foram apresentadas soluções para facilitar o gerenciamento e aumento da segurança da rede segmentada. A implementação ocorreu por meio da criação de um domínio VTP tornando mais fácil a administração das VLAN disponíveis em uma rede. Com isso, uma vez que as VLAN são criadas a partir de um *switch* configurado se propaga a configuração para todos os outros da rede (FRANCO, 2012).

5.2 VLAN: ESTUDO, TESTE E ANÁLISE DESTA TECNOLOGIA

Este trabalho foi desenvolvido por Ricardo Eleutério dos Santos e apresentado como Trabalho de Conclusão de Curso em Tecnologia em Sistemas de

Telecomunicações Instituto Federal de Santa Catarina em 2010. O objetivo é estudar os padrões IEEE 802.1Q, que define os padrões para o estabelecimento de VLAN, e IEEE 802.1X, que define os padrões de autenticação baseada em portas. Com o conhecimento destas normas permitirá a concepção de cenários de VLAN onde a autenticação do usuário irá definir a VLAN a qual ele pertence dentro de uma rede.

Em paralelo ao estudo de redes virtuais, foi estudado a autenticação de usuário e protocolos de rede como DHCP e RADIUS, que, junto com VLAN, permitem a criação de redes locais com bom grau de segurança e autonomia da rede.

Todos esses estudos foram realizados em cenários práticos de utilização, para poder chegar a um cenário que poderia ser implantado no Campus de São José do IFSC, mas que pode ser adaptado à outras instituições.

5.3 SEGURANÇA DE REDES LOCAIS COM A IMPLEMENTAÇÃO DE VLAN

Esta monografia foi desenvolvida por Odair Soares Barros e apresentado como Trabalho de Conclusão de Curso em Engenharia de Sistemas e Informática à Universidade Jean Piaget de Cabo Verde em 2006. Tem por finalidade compreender e relacionar a implementação de VLAN na rede local da Universidade perante os mecanismos de segurança nelas inseridas, e utiliza-las da melhor maneira possível.

No estudo de caso levantado no trabalho, foi optado realizar a implementação de VLAN através de *mac address*, por ter apresentado como a mais viável para o ambiente aplicado.

6 SIMULAÇÃO E SEGMENTAÇÃO VIRTUAL DE REDES DE COMPUTADORES

Este capítulo descreve a metodologia utilizada no trabalho que pode permitir que os objetivos propostos fossem alcançados. Nesse capítulo, será apresentado a classificação da pesquisa quanto a forma de desenvolvimento, ao objetivo e aos procedimentos. Logo depois serão descritos os procedimentos metodológicos utilizados na pesquisa.

6.1 METODOLOGIA

A metodologia da pesquisa, pode ser classificada como básica ou fundamental, pois tem como objetivo entender ou descobrir novos fenômenos. Com base no objetivo da pesquisa do projeto, ela pode ser considerada como pesquisa descritiva, já que visa observar, registrar e analisar através de experimentos com simulação baseado em ambientes reais pesquisado na literatura. Quanto aos procedimentos, a pesquisa é considerada experimental e em laboratório. Pesquisa em laboratório é aquela que permite o controle das variáveis que possam interferir o ambiente que se deseja realizar o experimento (ZAMBALDE; PADUA; ALVES, 2008).

6.2 PROCESSO DE SIMULAÇÃO

A simulação tem como objetivo imitar uma situação do mundo real e, com base no modelo criado, obter experimentos e testes com a proposta de poder compreender e avaliar o comportamento de uma determinada situação (ALBERTI; NETO; MENDES, 1999).

Além disso vem como um auxílio para profissionais da área de rede que precisam identificar e determinar até que ponto está o limite da infraestrutura de rede, que monitoram com ferramentas de capturas de pacotes como o PRTG, nagios, wireshark, entre outros, a realizar experimentos através de simulação com o objetivo de avaliar o custo benefício em implementar VLAN.

O projeto descreve a utilização de um simulador de rede de computadores associando o emprego das principais tecnologias de redes. Além disso, oferece uma abordagem prática do funcionamento destas redes por meio de simulação

computacional, que tem por objetivo possibilitar uma visão de prever o funcionamento em um ambiente real em produção. Podendo ter um planejamento sólido do ambiente a ser implementado. Por isso, a simulação computacional torna-se uma ferramenta essencial para se obter um modelo de rede econômica, evitando gastos com equipamentos desnecessários. A simulação computacional é altamente útil em um planejamento de redes e em projetos de remodelação de uma rede, por disponibilizar ambientes virtuais para uma variedade de características desejáveis, como poder modelar uma rede baseadas em critérios específicos e poder se obter teste em cenários diversos consultando os resultados (ALECRIM, 2009).

6.3 MODELAGEM DE REDES DE COMPUTADORES

A modelagem é processo de criação de modelos de sistemas reais para um ambiente de simulação que será utilizado, de forma que esses modelos representem, da maneira mais idêntica possível, o comportamento que se deseja em determinadas situações. Para isso possui algumas fases para realizar a modelagem de simulação (ALECRIM, 2009):

- a) **definição do problema:** é onde se defini o problema a ser estudado. Os principais pontos para identificar o problema são: o objetivo do projeto; o levantamento de equipamento e serviços disponíveis na rede; as métricas de desempenho; a identificação do problema ser estudado;
- b) **modelagem:** Nessa etapa vem a transcrição dos diversos fluxos lógicos do modelo, a modelagem da rede e dos serviços, visando identificar o escopo do ambiente, suas variáveis, indicadores de desempenho e os ambientes modelados.
- c) **seleção e Tratamento dos Dados de Entrada:** Após a definição do sistema a ser estudado, vem a etapa de coletar os dados, e fazer o tratamento estatístico.
- d) **simulação Computacional:** Tem como objetivo validar o modelo proposto anteriormente por meio de simulação.
- e) **apresentação e Análise de Resultados:** É a etapa que será feita as análises dos gráficos obtidos na simulação, em tem como tarefa estudar

os resultados obtidos, desenvolver as análises estatísticas dos dados de saída dos modelos e comparar os cenários desejados.

6.4 TOPOLOGIAS UTILIZADAS

Os cenários em organizações e universidades têm um grande número de dispositivos conectados em rede. O modelo cliente/servidor é muito utilizado nas aplicações e serviços de rede. Com isso o cenário definido para criar os cenários e realizar a simulação foi o modelo cliente/servidor.

Os cenários definidos no OPNET tem como meta representar da maneira mais semelhantes possíveis as situações nas quais as redes de computadores são construídas, expandidas e utilizadas. Nesse projeto foi abordado dois modelos diferentes para serem analisados e testados. Com níveis de complexidade diferentes de abordagem em cada um dos cenários.

Os modelos utilizados foram baseados em rede que utilizam VLANs e que não utilizam. Esses dois modelos foram comparados em modelo de segmentação por porta usando *switches*.

6.5 MÉTRICAS E APLICAÇÕES

As métricas utilizadas na coleta de dados das simulações, para comparação em redes locais sem e com segmentação *virtual*, foram analisados o comportamento dos *switches* e aplicações em servidores com as seguintes especificações:

- a) Tráfego recebido (bytes/segundo);
- b) Tráfego enviado (bytes/segundo);
- c) Tráfego encaminhado (bits/segundo);
- d) Tráfego recebido (bits/segundo);

Em cada aplicação utilizada durante as simulações pode ser configurada de três diferentes maneiras: *Low Load* (Carga Baixa), *Medium Load* (Carga Média), e *High Load* (Carga Alta). As aplicações utilizadas para a simulação nesse projeto foram:

- a) Banco de dados;

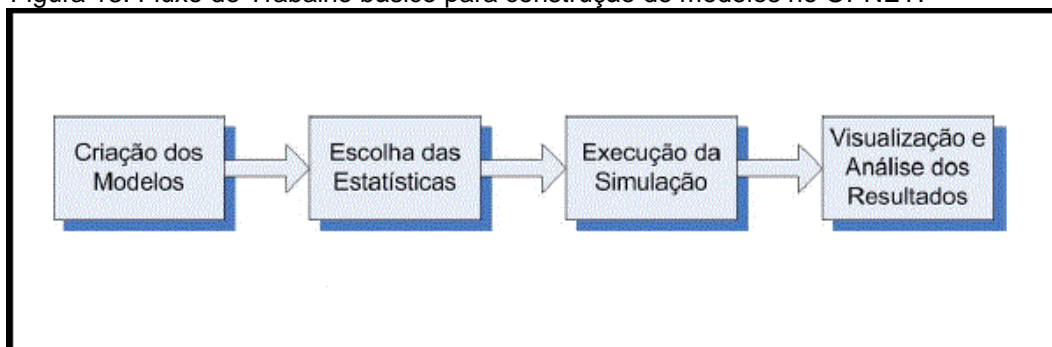
- b) Email;
- c) Voz;

6.6 FLUXO DE TRABALHO

A simulação tem sido constantemente abordada por alguns autores como uma técnica vantajosa para a representação de processos, pois, através desse processo é possível realizar análises de relações causais em tempo bastante curto e baixo custo.

Para construir o modelo de redes de computadores a ser simulado através do OPNET, foi utilizado basicamente, um fluxo de trabalho determinado, conforme ilustrado na figura 13 (SVENSSON; POPESCU, 2003).

Figura 13. Fluxo de Trabalho básico para construção de modelos no OPNET.



Fonte: Svensson e Popescu (2003).

6.7 MODELAGEM DO PROJETO

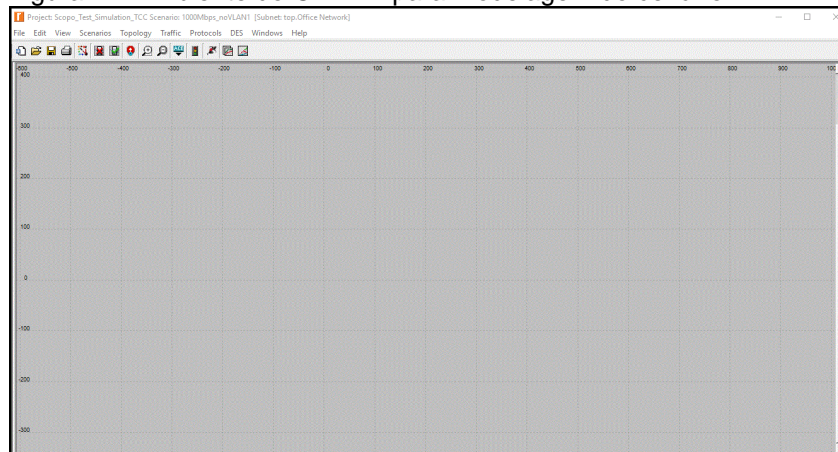
Para iniciar um projeto de simulação é necessário fazer o planejamento de todo o processo seguindo alguns passos: criar um novo projeto, definir a nomenclatura do projeto e dos cenários a serem elaborados, a escolha da topologia a ser utilizada, se será iniciado um cenário vazio ou importando um projeto pré-existente, a escala da rede e o tamanho do cenário que vai ser utilizado, selecionar as tecnologias a serem utilizadas no projeto, após a definição desses parâmetros é iniciado a implementação. Para o presente projeto, foi definido as seguintes especificações para os cenários construídos:

- a) **nome do projeto:** Scopo_Test_Simulation_TCC;

- b) **nome dos cenários:** Scopo_Test_Simulation_TCC-1000Mbps_no VLAN1; Scopo_Test_Simulation_TCC-1000Mbps_WithVLAN2;
- c) **topologia inicial:** cenário vazio;
- d) **escala da rede:** foi utilizado cenário de escritório;
- e) **tecnologias utilizadas:** aplicações, cliente servidor, *ethernet* avançada, roteadores avançados, LANs, enlaces avançados, VLANs;

Com as especificações definidas como descrito acima, o simulador OPNET utilizado nesse projeto, está pronta para iniciar a modelagem da rede de computadores. A figura 14 mostra onde a modelagem da rede será feita.

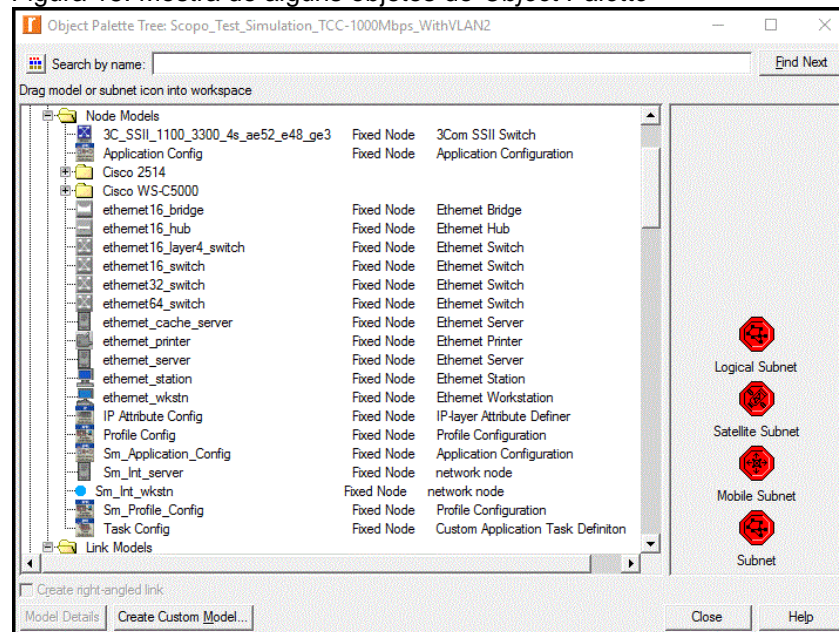
Figura 14. Ambiente do OPNET para modelagem do cenário.



Fonte: Autor.

Com o ambiente pronto para iniciar a configuração, o próximo passo é abrir a *Object Palette* (paleta de objetos). Essa opção contém todos os dispositivos que pertencem as tecnologias que foram selecionadas no início do processo da criação do projeto. A figura 15 mostra os objetos disponíveis no *Object Palette*.

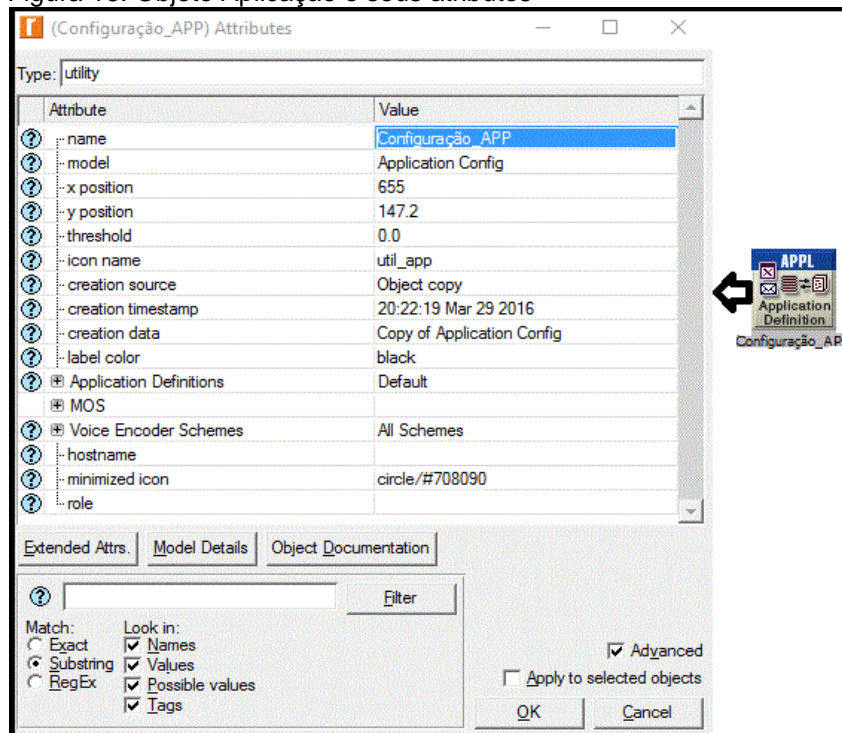
Figura 15. Mostra de alguns objetos do *Object Palette*



Fonte: Autor.

A *Object Palette* é onde possui todos os acessórios para montar a rede conforme o planejado, e também é onde que se defini as aplicações a serem executados na rede, e definidos e configurados como objetos. Para a simulação são o *Application Definition* (Definição de Aplicação) e o *Profile Definition* (Definição de Perfil). A figura 16 mostra a janela de configurações.

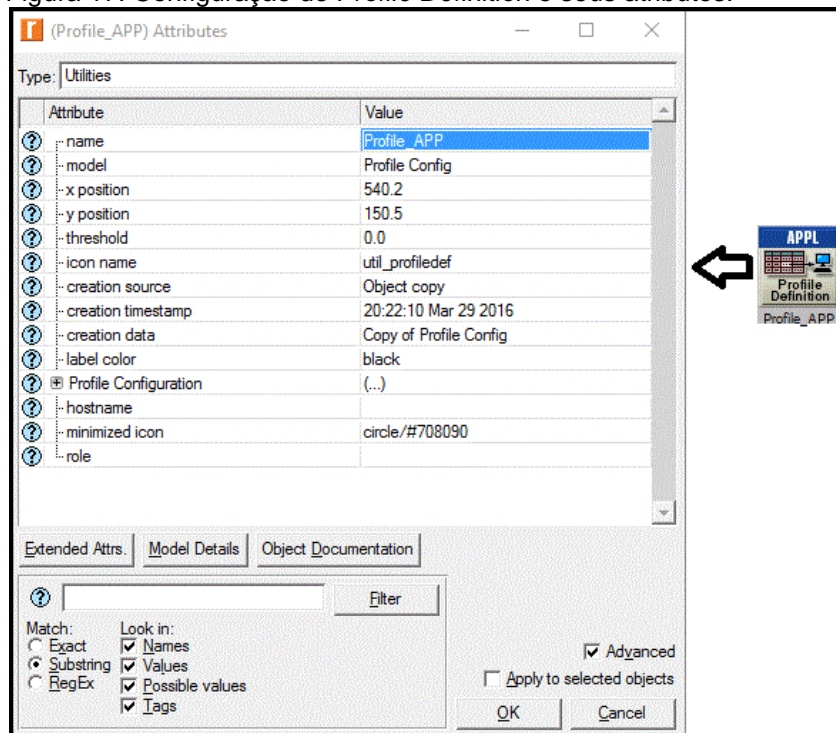
Figura 16. Objeto Aplicação e seus atributos



Fonte: Autor.

O *Profile Definition* faz a definição do perfil dos dispositivos da rede. O perfil tem o objetivo de carregar as informações sobre as aplicações com as quais o *host* irá trabalhar. A figura 17 é possível verificar o objeto *Profile Definition* e sua janela de configuração.

Figura 17. Configuração de *Profile Definition* e seus atributos.



Fonte: Autor.

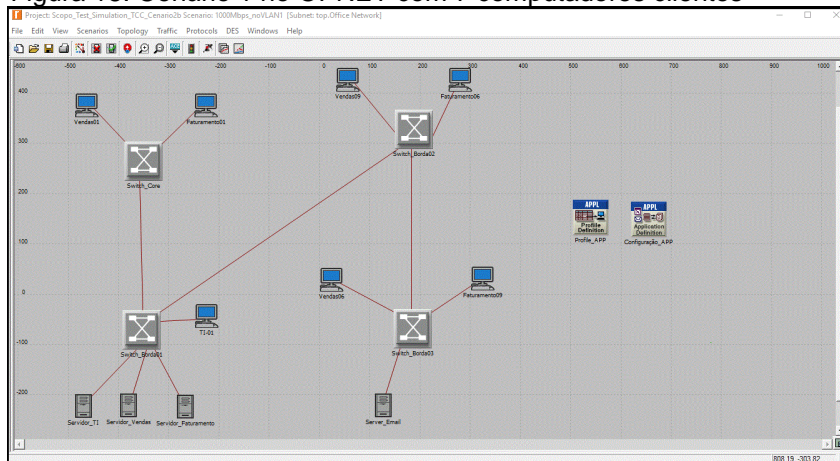
Para o projeto foram definidas topologias e os cenários que serão descritos a seguir.

6.8 CENÁRIOS E TOPOLOGIAS

Para a modelagem foi utilizado um cenário e topologia de um ambiente dividido em alguns setores. Para avaliar o tamanho do ambiente necessário para se implementar um VLAN, foram realizados diversos experimentos com a mesma configuração de cenário porém alterando em cada simulação a quantidade de dispositivos conectados em redes. Nesses cenários todos servidores foram preparados para dar suporte aos seus respectivos serviços em nível de carga alta, para que assim os ambientes simulados estejam próximos da realidade. Os computadores clientes foram configuradas para utilizarem suas aplicações com carga alta. Os circuitos utilizados em todos os enlaces foram configurados para operar a uma taxa de 1000BaseT. Com as informações definidas, foram modelados os seguintes cenários:

a) **cenário 1**: esse cenário consiste em uma configuração sem a utilização de segmentação *virtual*. É um cenário do tipo estrela, possuindo quatro *switches* como nó central. O cenário possui quatro servidores (E-mail, FTP, Banco de Dados e Voz) dividido em quatro grupos de estações de trabalho. Para melhor identificar o momento de implementar uma segmentação, foram simulados o mesmo cenário com quantidades diferentes de dispositivos interconectados a rede. A figura 18 mostra a modelagem do cenário usando o ambiente de simulação do OPNET com um ambiente com 7 computadores clientes trabalhando em rede.

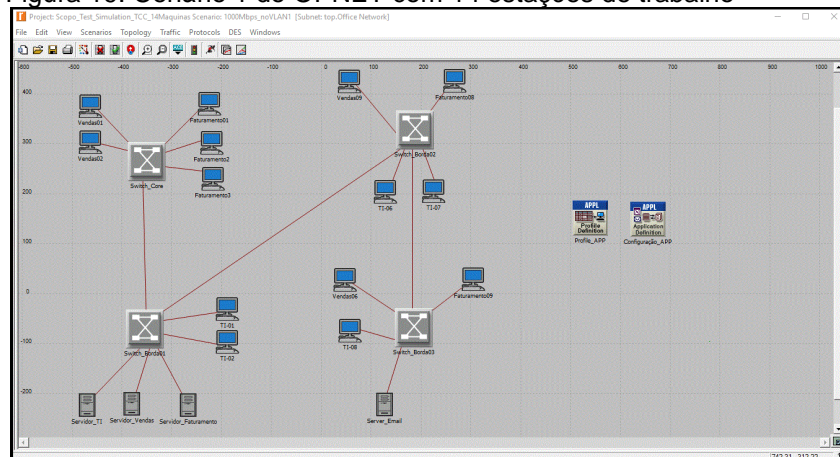
Figura 18. Cenário 1 no OPNET com 7 computadores clientes



Fonte: Autor.

A figura 19 mostra o cenário com um ambiente que possui 14 estações de trabalhos conectados à rede.

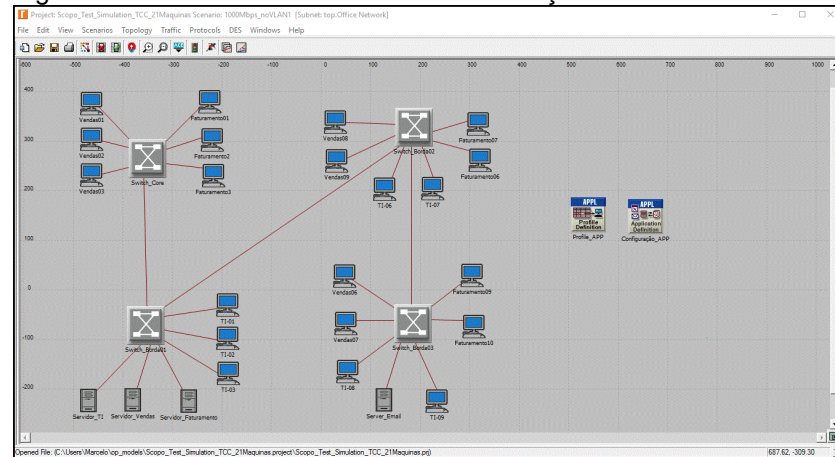
Figura 19. Cenário 1 do OPNET com 14 estações de trabalho



Fonte: Autor.

O ambiente modelado da figura 20 mostra a rede com 21 computadores clientes conectados.

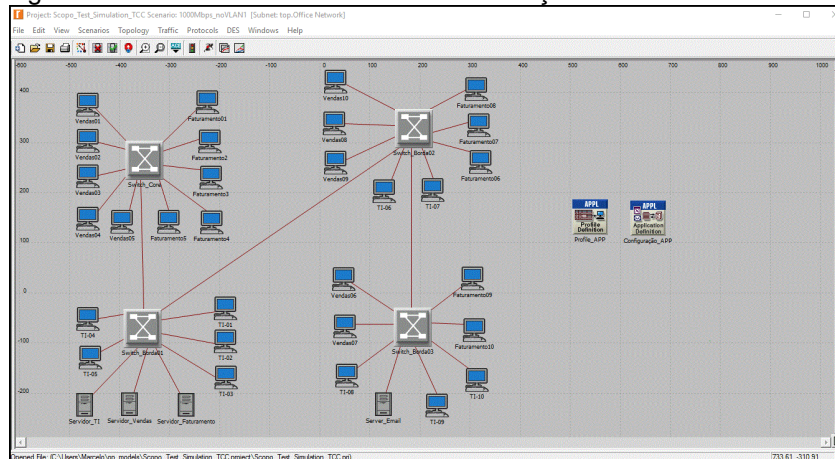
Figura 20. Cenário 1 do OPNET com 21 estações de trabalho.



Fonte: Autor.

O ambiente da figura 21 mostra a rede com 30 computadores conectados.

Figura 21. Cenário 1 do OPNET com 30 estações de trabalho.

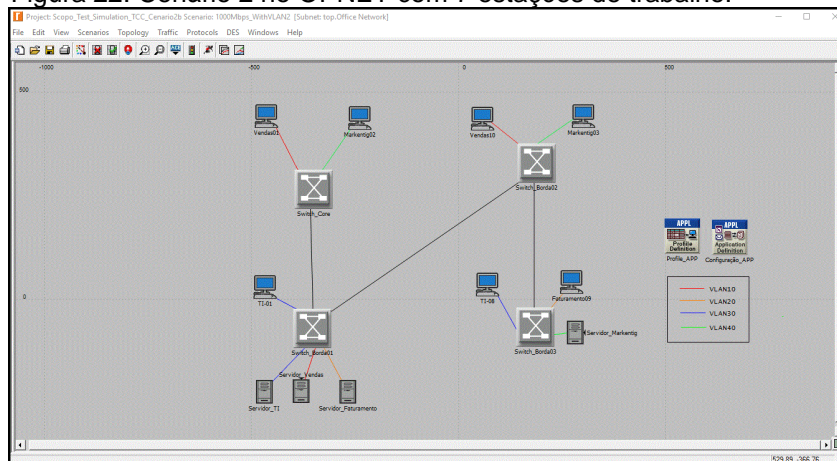


Fonte: Autor.

- b) **cenário 2:** esse cenário consiste em uma configuração utilizando segmentação. O cenário é semelhante ao do cenário 1. No entanto, quatro VLANs foram criadas, VLAN 10, VLAN20, VLAN30 e VLAN40, criando uma segmentação lógica e dividindo a rede em quatro domínios

de *broadcast* independentes. Para avaliar o tamanho do ambiente necessário para se implementar um VLAN, foram realizados diversos experimentos com a mesma configuração de cenário porem alterando em cada simulação a quantidade de dispositivos conectados em redes. A figura 22 mostra o cenário com VLANs modelados no ambiente de simulação do OPNET com 7 estações de trabalho conectados a essa rede.

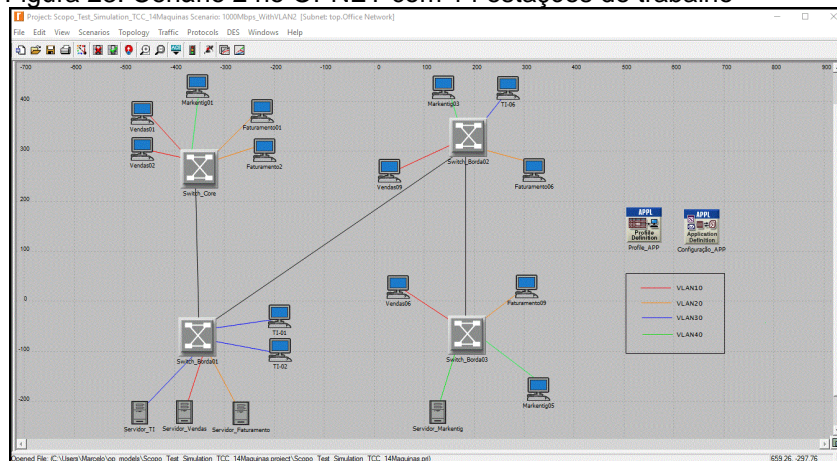
Figura 22. Cenário 2 no OPNET com 7 estações de trabalho.



Fonte: Autor.

A figura 23 mostra o cenário segmentado com um ambiente que possui 14 estações de trabalhos conectados à rede.

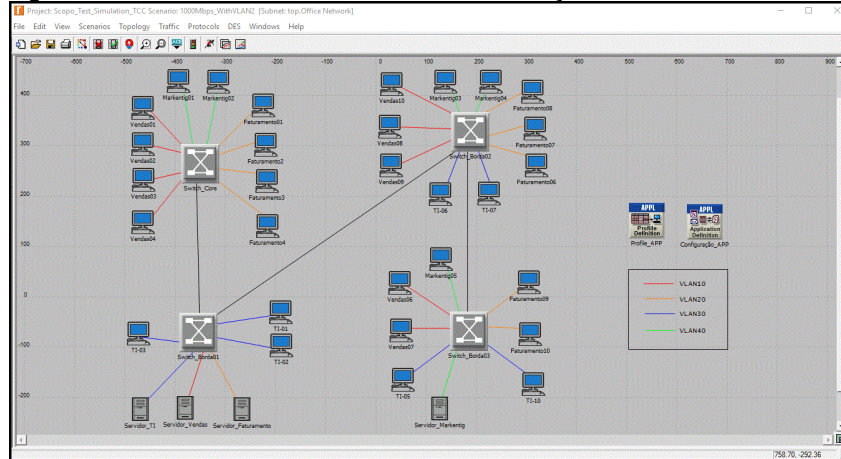
Figura 23. Cenário 2 no OPNET com 14 estações de trabalho



Fonte: Autor.

O ambiente da figura 24 mostra a rede segmentada com 30 computadores conectados.

Figura 244. Cenário 2 no OPNET com 24 estações de trabalho.



Fonte: Autor.

Para segmentar a rede é necessário configurar e atribuir as VLANs específicas nas portas do *switch*. As portas só podem suportar VLANs que são suportados pelo nó. As portas podem ser definidas como *Trunk*, *Access* ou *Hybrid*. A figura 25 mostra a configuração dos atributos da porta do *switch*.

Figura 25. Configuração de atributos na porta do switch.

The screenshot displays four configuration windows in OPNET:

- (Switch_Core) Attributes:** Shows general switch properties like name, model, position, and bridge parameters.
- (Supported VLANs) Table:** A table listing configured VLANs:

Identifier (VID)	Name	Cost	Priority	Tagging	Leaming Mode
10	VLAN_10	Same as Port	Same as Port	Send Tagged	Enable-Forward
20	VLAN_20	Same as Port	Same as Port	Send Tagged	Enable-Forward
30	VLAN_30	Same as Port	Same as Port	Send Tagged	Enable-Forward
40	VLAN_40	Same as Port	Same as Port	Send Tagged	Enable-Forward
- (Switch Port Configuration) Table:** A table listing 16 ports (P0-P15) with their status, operational status, speed, duplex mode, cost, priority, fast start mode, link type, and VLAN parameters.
- (VLAN Parameters) Table:** Shows configuration for a selected port, including port type, port VLAN identifier (PVID), supported VLANs, trunk negotiation parameters, and spanning tree configuration.

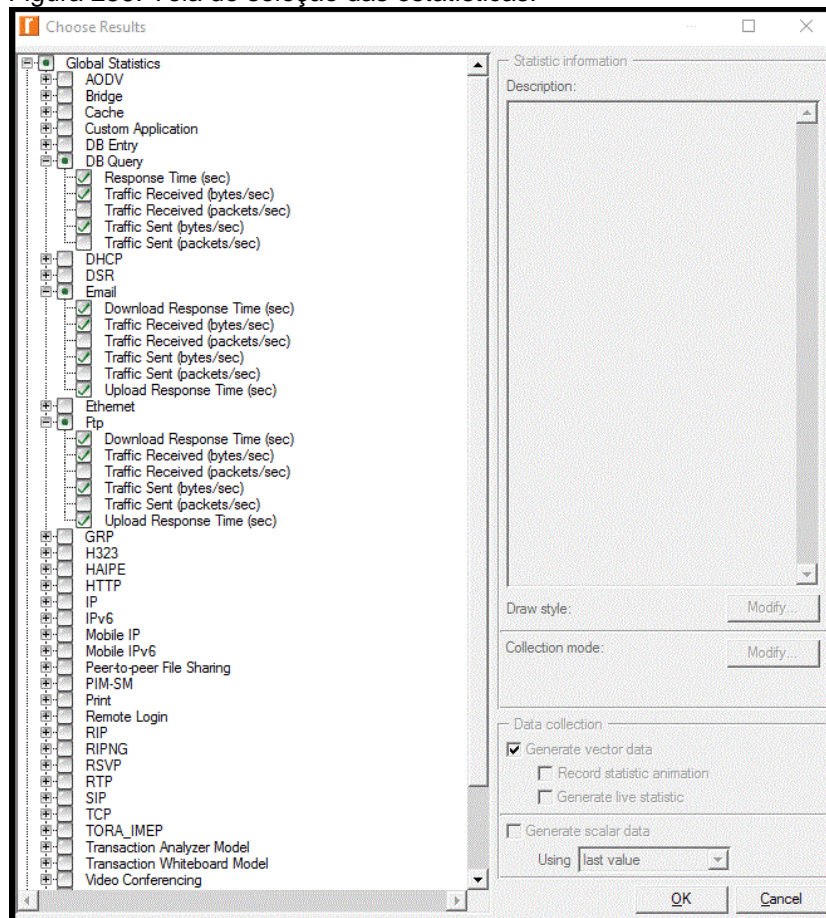
Fonte: Autor.

Com os cenários montados e configurados a próxima etapa é a definição dos dados a serem analisados.

6.9 ESCOLHAS DAS ESTATÍSTICAS

Com os cenários da simulação configurado, o próximo passo a ser realizado é configurar as estatísticas a serem coletadas durante a simulação. Para esse trabalho coletadas estatísticas globais da rede. A figura 26 mostra a janela de seleção das estatísticas dos aplicativos utilizados nas simulações e algumas das métricas definidas selecionadas para análises seguintes.

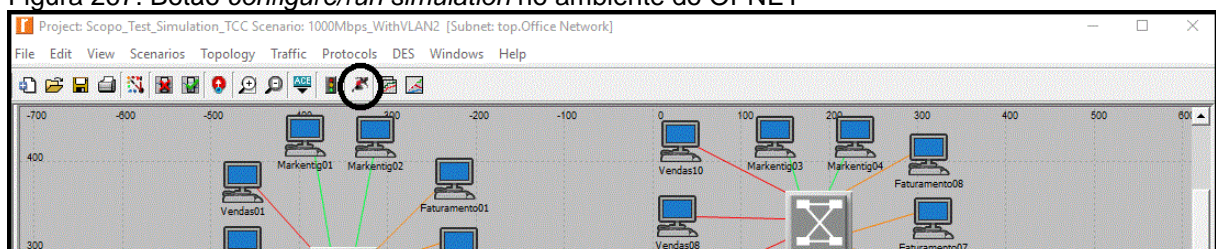
Figura 256. Tela de seleção das estatísticas.



Fonte: Autor.

6.10 EXECUÇÃO DA SIMULAÇÃO

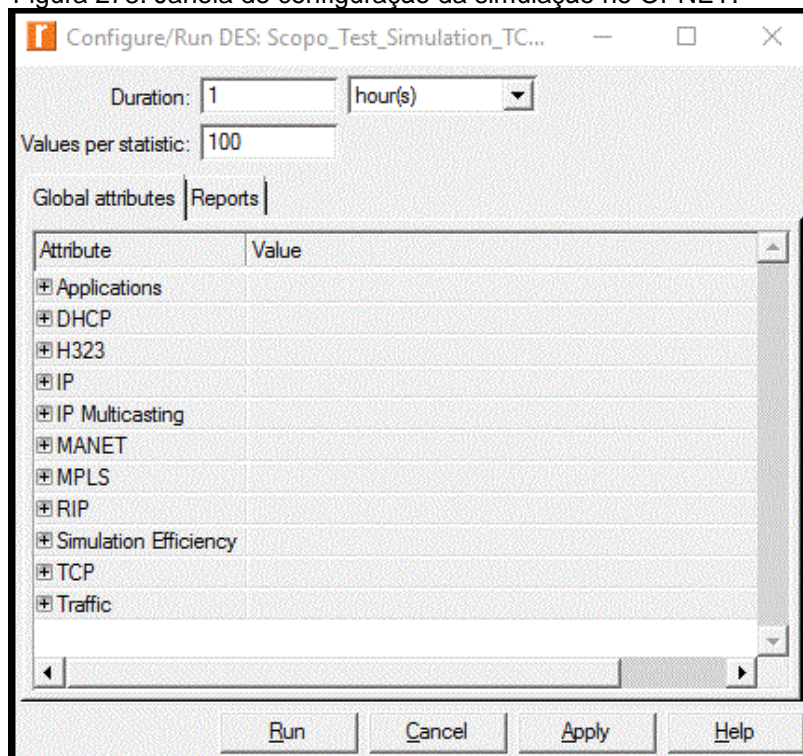
Com a modelagem dos cenários e também com as definições das estatísticas desejadas, a simulação pode ser executada para que assim os dados sejam coletados e analisados. Para executar a simulação é necessário primeiramente abrir a janela de configuração, clicando no botão *configure/run simulation*, como pode ser observado na figura 27.

Figura 267. Botão *configure/run simulation* no ambiente do OPNET

Fonte: Autor.

Após a janela de configuração da simulação abrir, é feita as escolhas do tempo a ser simulado pelo OPNET. O tempo pode ser escolhido em segundos, minutos, horas, dias e semanas como pode ser observado na figura 28. Com a definição das opções, a simulação irá começar.

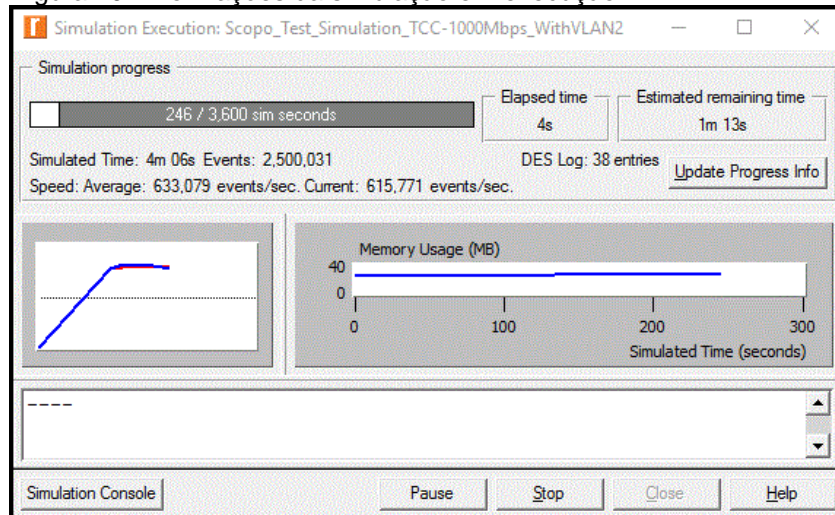
Figura 278. Janela de configuração da simulação no OPNET.



Fonte: Autor.

A figura 29 mostra a janela que aparece durante o processo de simulação. Nessa janela aparece algumas informações da simulação em execução como, tempo decorrido, tempo restante estimado, tempo simulado, eventos e velocidade média e velocidade atual.

Figura 29. Informações da simulação em execução.

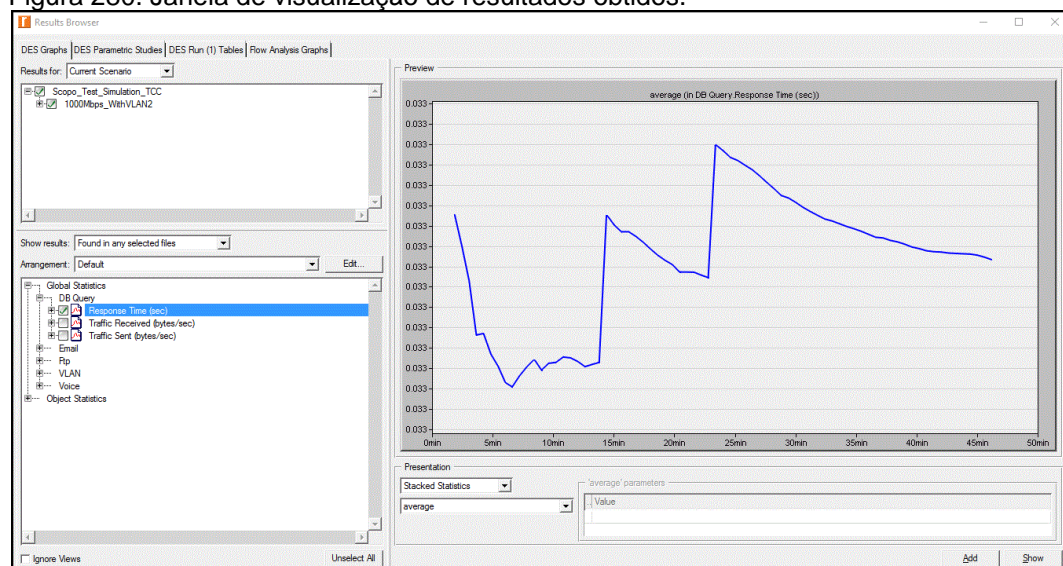


Fonte: Autor.

6.11 VISUALIZANDO E ANALISANDO RESULTADOS

Após o processo de simulação encerrar é possível visualizar e analisar nos gráficos todas as informações que foram selecionadas antes da simulação. Na figura 30 é possível observar a janela de visualizações dos resultados obtidos na simulação de rede.

Figura 280. Janela de visualização de resultados obtidos.



Fonte: Autor.

Os resultados obtidos e a análise dos gráficos obtidos com a execução das simulações serão mostrados a seguir. As avaliações com as diferenças do uso das duas redes serão abordadas posteriormente.

6.12 RESULTADOS OBTIDOS

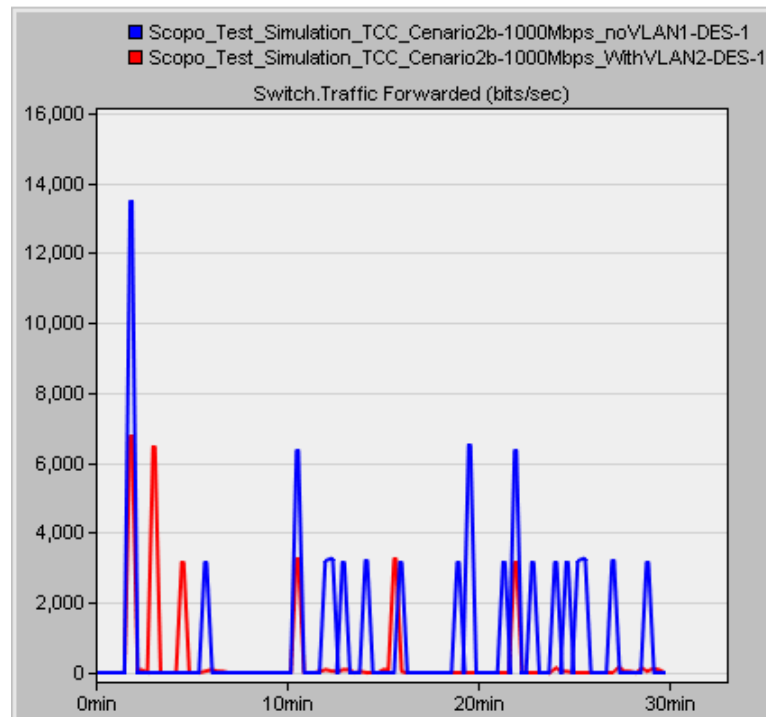
A partir desse tópico será apresentado os resultados obtidos nas simulações de redes de computadores sem segmentação virtual e com a aplicação de VLAN, após a simulação nos cenários apresentados, e os resultados alcançados foram comparados e analisados para identificar a melhora no desempenho. Assim observar a necessidade ou não de se implementar uma VLAN. E assim descrever o sobre os cenários analisados.

6.12.1 Cenários 1 e 2 com 7 máquinas

Este cenário consiste em uma análise de um ambiente onde contém 4 *switches* e algumas aplicações que estarão sendo disponibilizado para os computadores clientes. Na maior parte dos equipamentos pode se observar que a diferença da rede não segmentada com a rede segmentada não teve um aumento muito expressivo em relação a desempenho.

A figura 31 mostra o gráfico do *switch core* com o tráfego encaminhado (em bits/segundo).

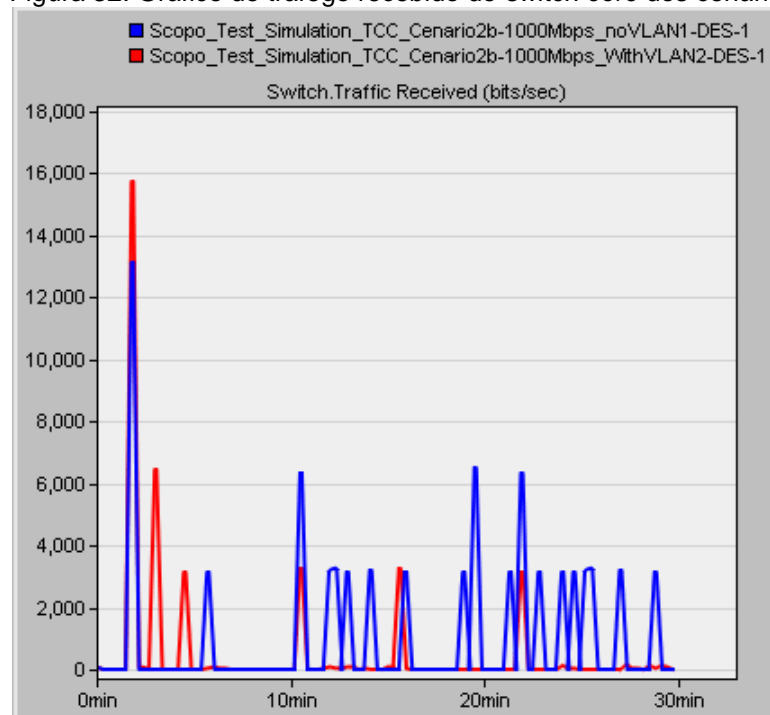
Figura 31. Gráfico de tráfego encaminhado do *switch core* dos cenários 1 e 2



Fonte: Autor.

Pelas mesmas razões que o tráfego encaminhado no *switch*, a diferença das redes segmentadas e não segmentadas não tiveram uma diferença de desempenho tão expressivo. Na figura 32 é mostrado o gráfico gerado com o tráfego recebido (em bits/segundo).

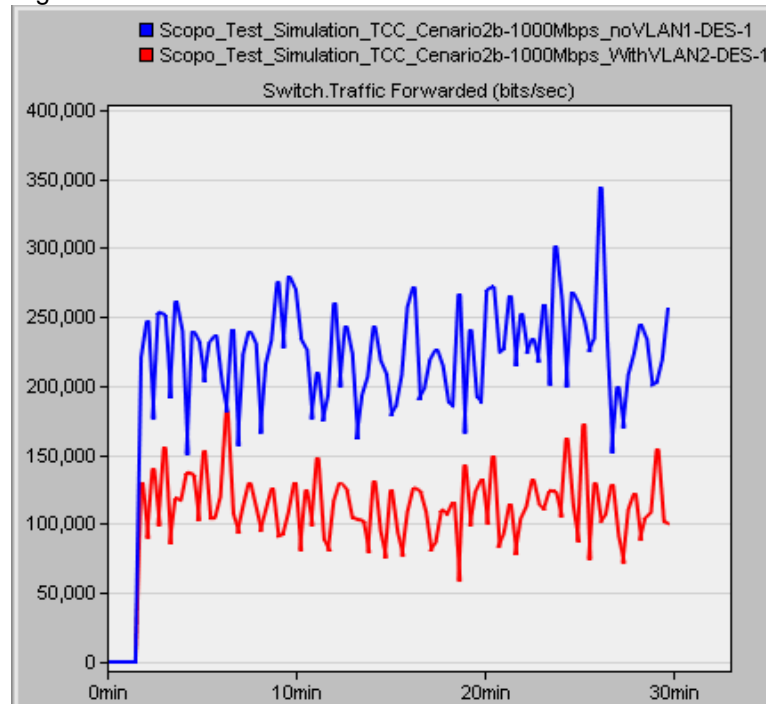
Figura 32. Gráfico de tráfego recebido do *switch core* dos cenários 1 e 2



Fonte: Autor.

A figura 33 mostra o gráfico de tráfego encaminhado (em bits/segundo) do *switch* de borda01 onde o tráfego encaminhado com a rede segmentada foi bem maior do que o tráfego da rede sem segmentação.

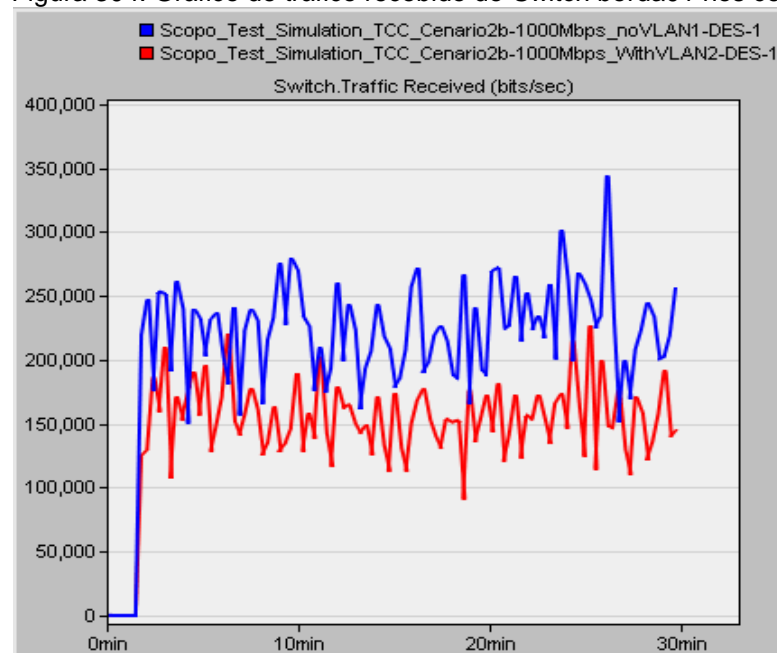
Figura 293. Gráfico de tráfego encaminhado do *Switch* borda01 nos cenários 1 e 2



Fonte: Autor.

A figura 34 mostra o gráfico de tráfego recebido (em bits/segundo) do *switch* borda01, onde podemos verificar um aumento pequeno de desempenho de uma rede com VLAN implementado.

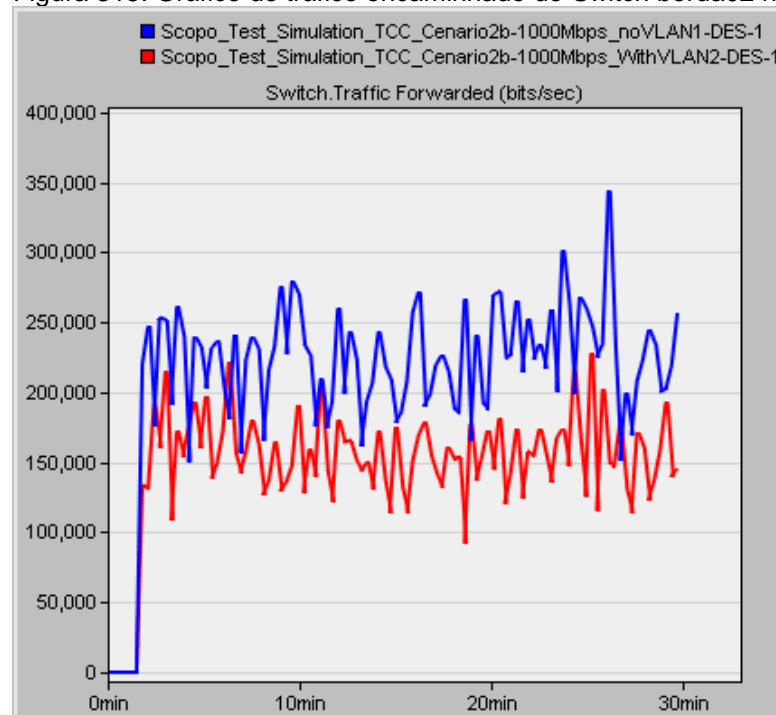
Figura 304. Gráfico de tráfego recebido do *Switch* borda01 nos cenários 1 e 2.



Fonte: Autor.

A figura 35 mostra o gráfico de tráfego encaminhado (em bits/segundo) do *switch* borda02, onde podemos verificar um aumento de desempenho não tão expressivo de uma rede com VLAN implementado.

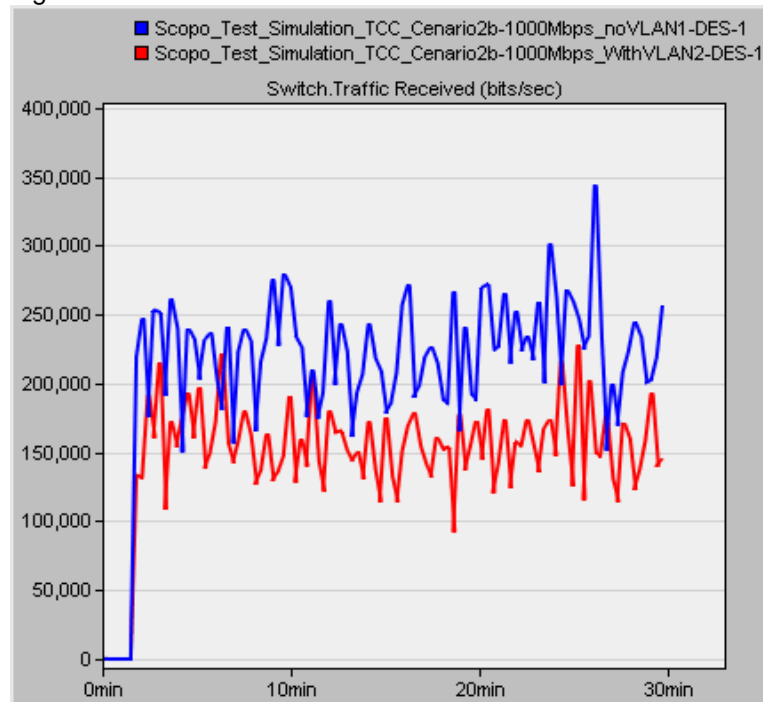
Figura 315. Gráfico de tráfego encaminhado do *Switch* borda02 nos cenários 1 e 2.



Fonte: Autor.

A figura 36 mostra o gráfico de tráfego recebido (em bits/segundo) do *switch* borda02, onde podemos verificar um aumento de desempenho também não tão expressivo de uma rede com VLAN implementado.

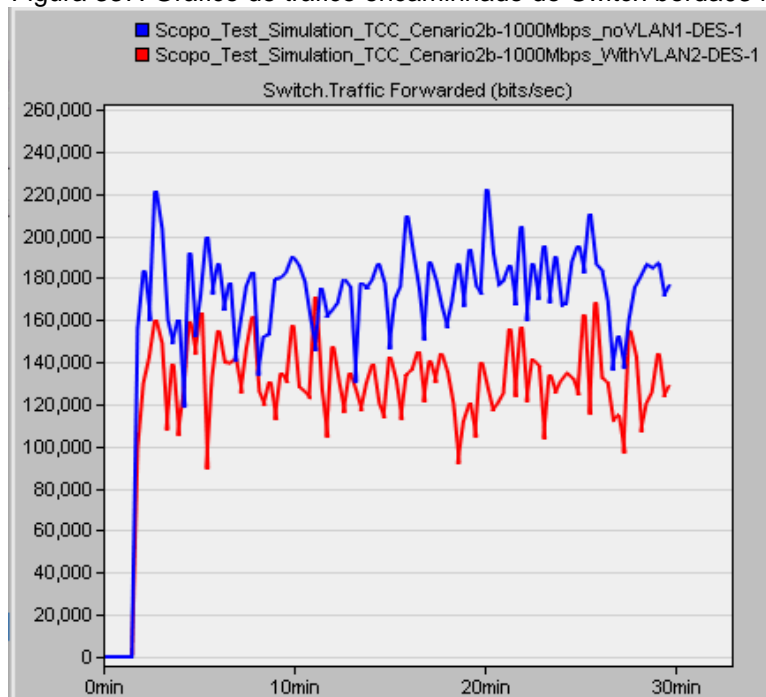
Figura 326. Gráfico de tráfego recebido do *Switch* borda02 nos cenários 1 e 2.



Fonte: Autor.

A figura 37 mostra o gráfico de tráfego encaminhado (em bits/segundo) do *switch* borda03, onde com a rede segmentada teve um tráfego maior do que a rede normal.

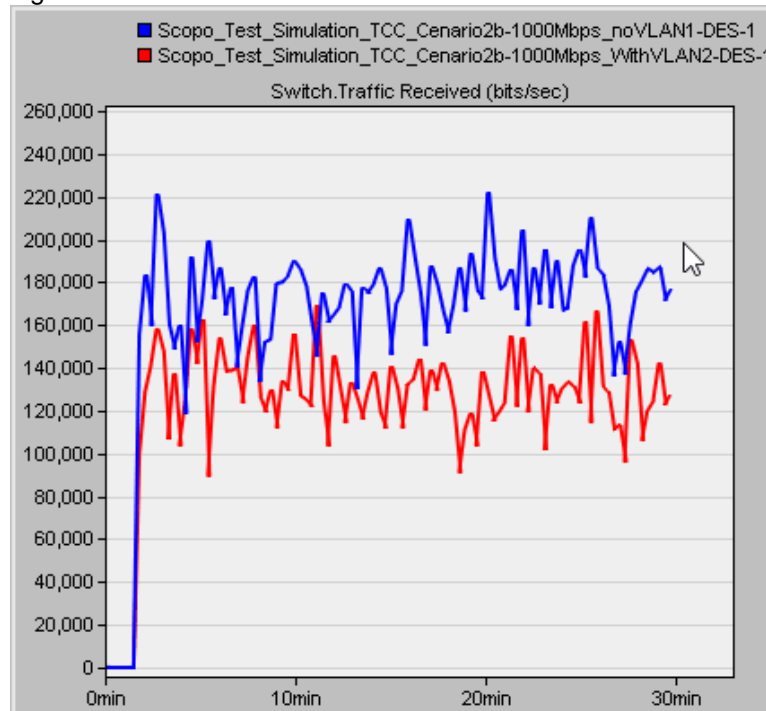
Figura 337. Gráfico de tráfego encaminhado do *Switch* borda03 nos cenários 1 e 2.



Fonte: Autor.

A figura 38 mostra o gráfico de tráfego recebido (em bits/segundo) do *switch* borda03, onde podemos verificar uma pequena diferença no desempenho das redes com VLAN e não segmentada da mesma maneira que o tráfego encaminhado.

Figura 348. Gráfico de tráfego recebido do *Switch* borda03 nos cenários 1 e 2.



Fonte: Autor.

Após os experimentos realizado em um ambiente com poucas máquinas, o ambiente com rede segmentada teve um desempenho médio de 20% a mais de desempenho em relação a rede não segmentada. A partir da tabela 3 é possível observar em números as comparações dos cenários e suas cargas de serviço referentes aos tráfegos encaminhados e recebidos.

Tabela 3. Tráfego recebido, encaminhados e enviados dos cenários 1 e 2 com 7 dispositivos clientes.

Dispositivo	Tipo de Tráfego	Performance com VLAN
<i>Switch Core</i>	Tráfego Encaminhado	28,69%
	Tráfego Recebido	11,83%
<i>Switch Borda01</i>	Tráfego Encaminhado	- 60,85%
	Tráfego Recebido	32.48%
<i>Switch Borda02</i>	Tráfego Encaminhado	30,87%
	Tráfego Recebido	31.57%
<i>Switch Borda03</i>	Tráfego Encaminhado	- 12,96%
	Tráfego Recebido	15,55%
Server Database	Tráfego Encaminhado	61,39%
	Tráfego Recebido	61,39%
<i>Email Server</i>	Tráfego Encaminhado	8%
	Tráfego Recebido	8%
<i>Voice Server</i>	Tráfego Encaminhado	25,30%
	Tráfego Recebido	48,25%

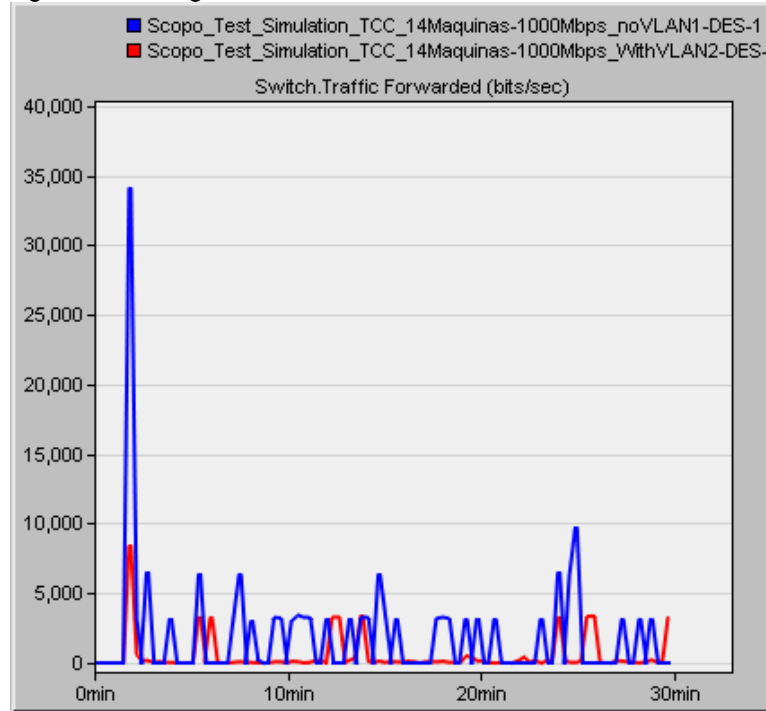
Fonte: Autor.

6.12.2 Cenários 1 e 2 com 14 máquinas

Este cenário a ser analisado contém 4 *switches* e algumas aplicações que estarão sendo disponibilizado para os computadores clientes. E com o aumento do número de computadores clientes na rede e conseqüentemente o acréscimo de pacotes trafegados, vamos observar a melhora do desempenho com a rede segmentada. Na maior parte dos equipamentos pode se observar que a diferença da rede não segmentada com a rede segmentada não teve um aumento muito expressivo em relação a desempenho.

A figura 39 mostra o gráfico de tráfego encaminhado (em bits/segundo) do *switch core*, com uma diferença considerável de uma rede segmentada em relação a rede não segmentada.

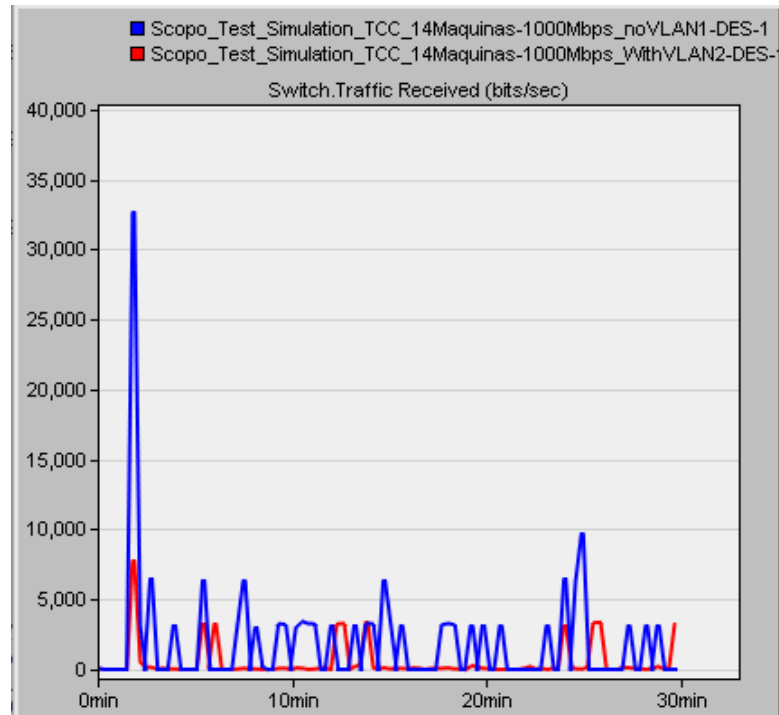
Figura39. Tráfego encaminhado *switch core* em ambiente com 14 computadores



Fonte: Autor.

A figura 40 mostra o gráfico de tráfego recebido (em bits/segundo) do *switch core*, com uma diferença considerável próximo do ocorrido com tráfego encaminhado de uma rede segmentada em relação a rede não segmentada.

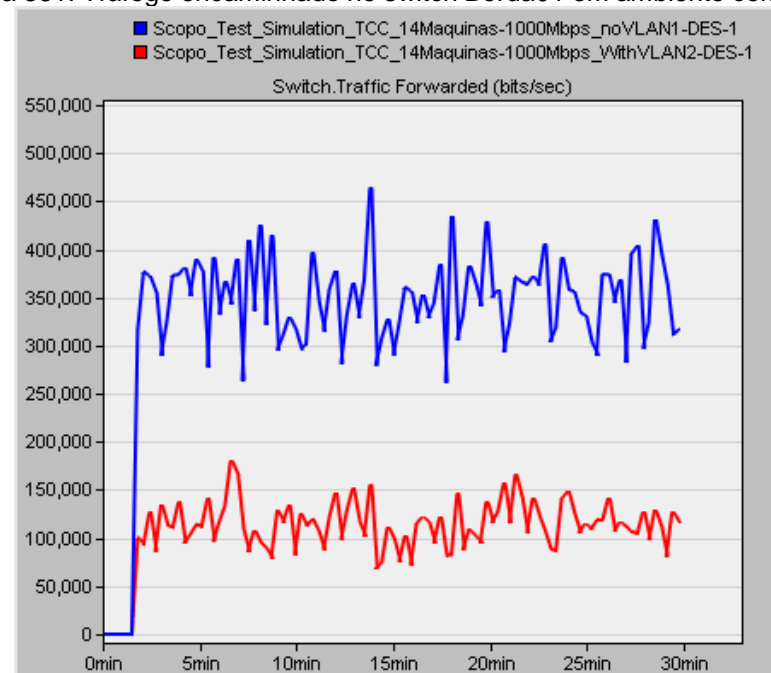
Figura 350. Tráfego recebido *switch core* em ambiente com 14 computadores.



Fonte: Autor.

A figura 41 mostra o gráfico de tráfego encaminhado (em bits/segundo) do *switch* borda01, com o aumento de equipamentos na rede já pode ser observado um pequeno aumento de desempenho com a configuração de uma rede segmentada em relação a rede sem VLAN.

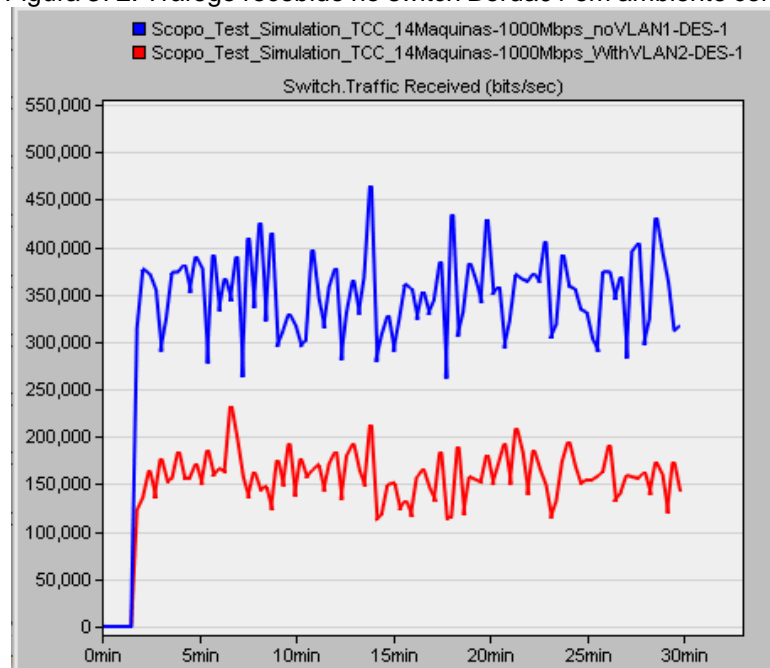
Figura 361. Tráfego encaminhado no switch Borda01 em ambiente com 14 computadores.



Fonte: Autor.

A figura 42 mostra o gráfico de tráfego recebido (em bits/segundo) do *switch* Borda01, com uma diferença da rede segmentada apresentar um maior desempenho em relação ao ambiente com menos computadores, e também em relação ao tráfego encaminhado.

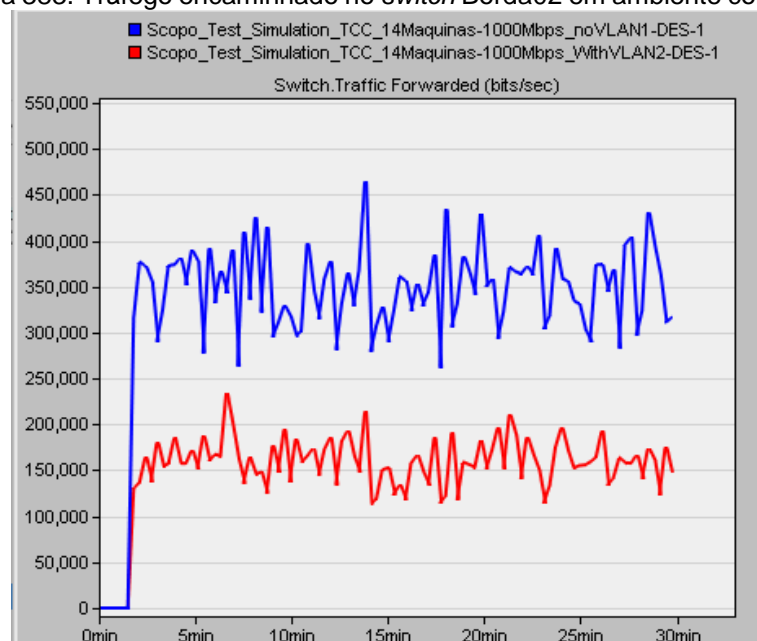
Figura 372. Tráfego recebido no *switch* Borda01 em ambiente com 14 computadores.



Fonte: Autor.

A figura 43 mostra o gráfico de tráfego encaminhado (em bits/segundo) do *switch* Borda02, com o aumento do número de computadores na rede pode-se observar um cenário mais favorável com uma rede segmentada, pelo melhor desempenho que proporciona em relação ao ambiente com menos máquinas.

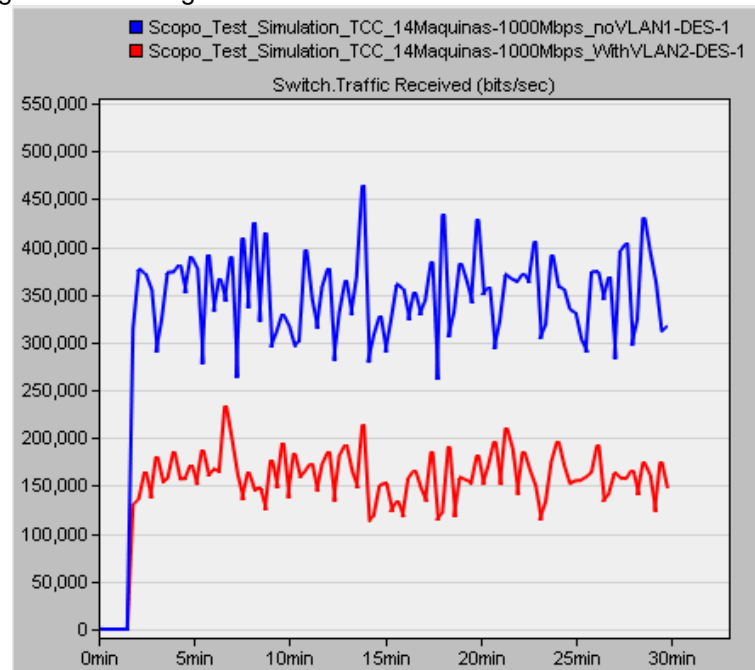
Figura 383. Tráfego encaminhado no *switch* Borda02 em ambiente com 14 computadores.



Fonte: Autor.

A figura 44 mostra o gráfico de tráfego recebido (em bits/segundo) do *switch* Borda02, com o aumento do número de computadores na rede pode-se observar um cenário mais favorável com uma rede segmentada, pelo melhor desempenho que proporciona em relação ao ambiente com menos máquinas.

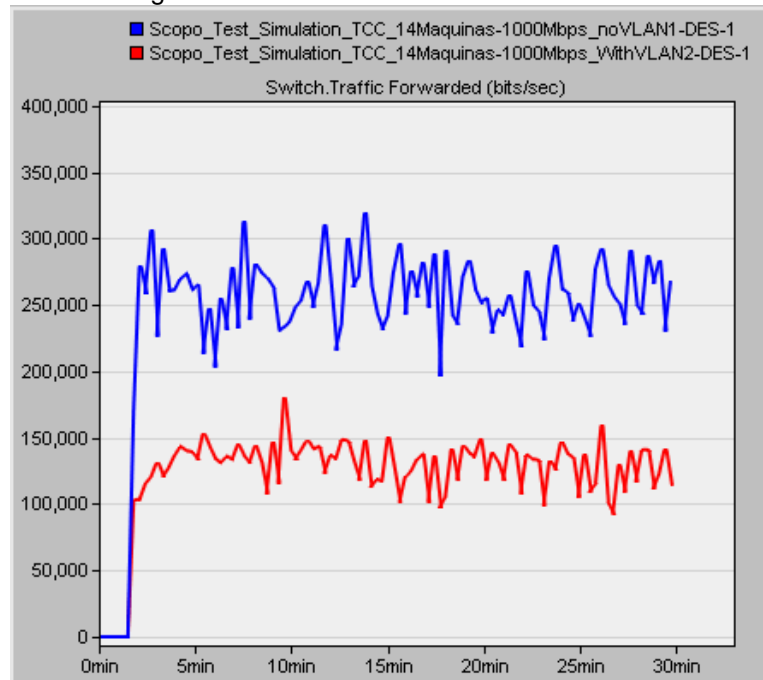
Figura 394. Tráfego recebido no *switch* Borda02 em ambiente com 14 computadores.



Fonte: Autor.

A figura 45 mostra o gráfico de tráfego encaminhado (em bits/segundo) do *switch* Borda03, com o aumento do número de computadores na rede pode-se observar um cenário mais favorável com uma rede segmentada em comparação com o ambiente com menor quantidade de dispositivo em rede, com a VLAN configurada o desempenho foi muito significativo em relação a rede normal.

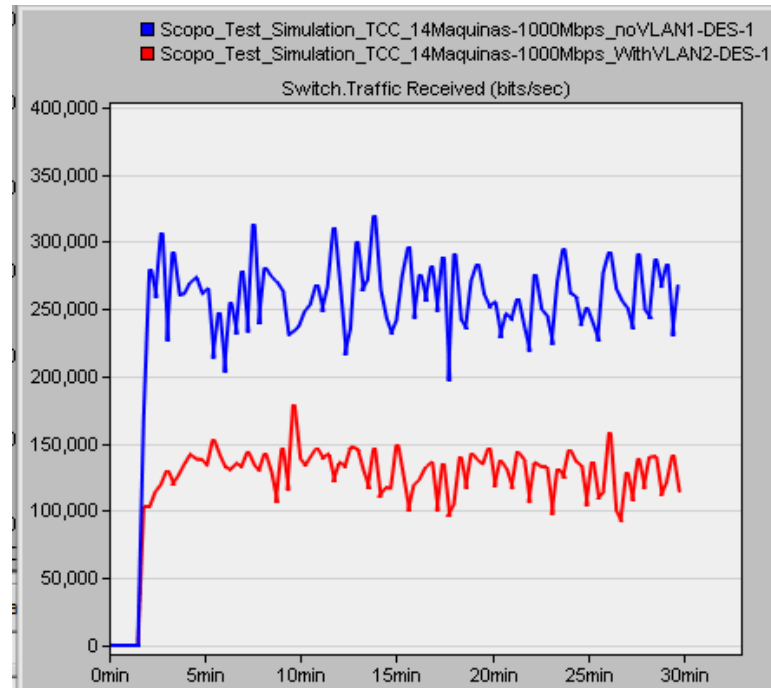
Figura 45. Tráfego encaminhado no *switch* Borda03 em ambiente com 14 computadores.



Fonte: Autor.

A figura 46 mostra o gráfico de tráfego recebido (em bits/segundo) do *switch* Borda02, pode-se observar que mesmo com o aumento do número de computadores na rede o tráfego recebido a rede segmentada não obteve um ganho tão expressivo em comparação a rede com menos máquinas.

Figura 406. Tráfego recebido no *switch* Borda03 em ambiente com 14 computadores.



Fonte: Autor.

Com o ambiente possuindo o dobro de computadores em relação ao anterior, a rede segmentada demonstrou ter um desempenho mais eficaz em comparação a rede não segmentada, demonstrando um ganho de desempenho médio de 54,90%. A partir da tabela 4 é possível observar em números dos equipamentos monitorados dos cenários e suas cargas de serviço referentes aos tráfegos encaminhados e recebidos.

Tabela 4. Tráfegos recebido, encaminhados e enviados dos cenários 1 e 2 com 14 dispositivos clientes.

Dispositivo	Tipo de Tráfego	Performance com VLAN
<i>Switch Core</i>	Tráfego Encaminhado	76,38%
	Tráfego Recebido	68,60%
<i>Switch Borda01</i>	Tráfego Encaminhado	6,63%
	Tráfego Recebido	59,16%
<i>Switch Borda02</i>	Tráfego Encaminhado	55,25%
	Tráfego Recebido	52,73%
<i>Switch Borda03</i>	Tráfego Encaminhado	41,36%
	Tráfego Recebido	37,74%
Server Database	Tráfego Encaminhado	72,82

	Tráfego Recebido	72,82
<i>Email Server</i>	Tráfego Encaminhado	21,57%
	Tráfego Recebido	21,57%
<i>Voice Server</i>	Tráfego Encaminhado	54,55%
	Tráfego Recebido	70,16%

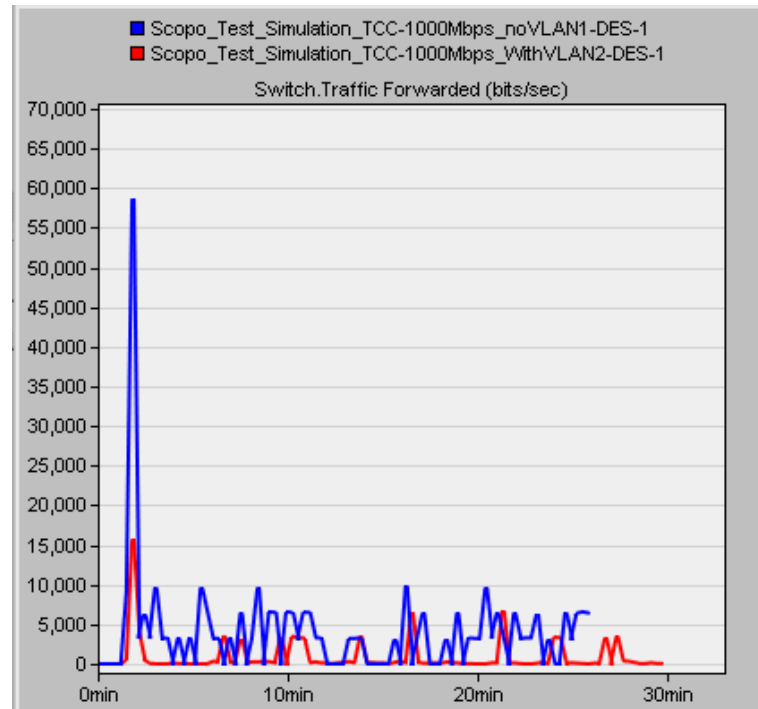
Fonte: Autor.

6.12.3 Cenários 1 e 2 com 30 máquinas

Este cenário a ser analisado contém 4 *switches* e algumas aplicações que estarão sendo disponibilizado para os computadores clientes. Para o experimento desse ambiente foi adicionado o dobro de computadores na rede em relação ao ambiente anterior, e com esse aumento dessas máquinas a requisição de serviços e pacotes trafegados vai ser maior, e então vai ser possível observar a melhora do desempenho com a rede segmentada.

A figura 47 mostra o gráfico de tráfego encaminhado (em bits/segundo) do *switch core*, com uma diferença considerável de uma rede segmentada em relação a rede não segmentada em comparação com ambientes com menor quantidade de computadores em rede.

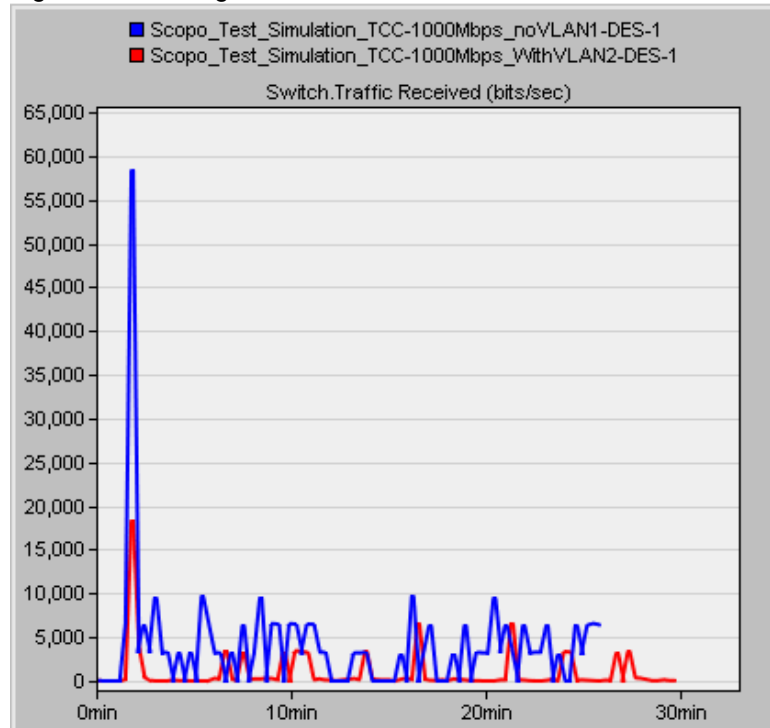
Figura 417. Tráfego encaminhado no *switch core* em ambiente com 30 computadores.



Fonte: Autor.

A figura 48 mostra o gráfico de tráfego recebido (em bits/segundo) do *switch core*, com o aumento de computadores na rede o desempenho com a rede segmentada ficou com um desempenho bastante expressivo, até em relação ao tráfego encaminhado.

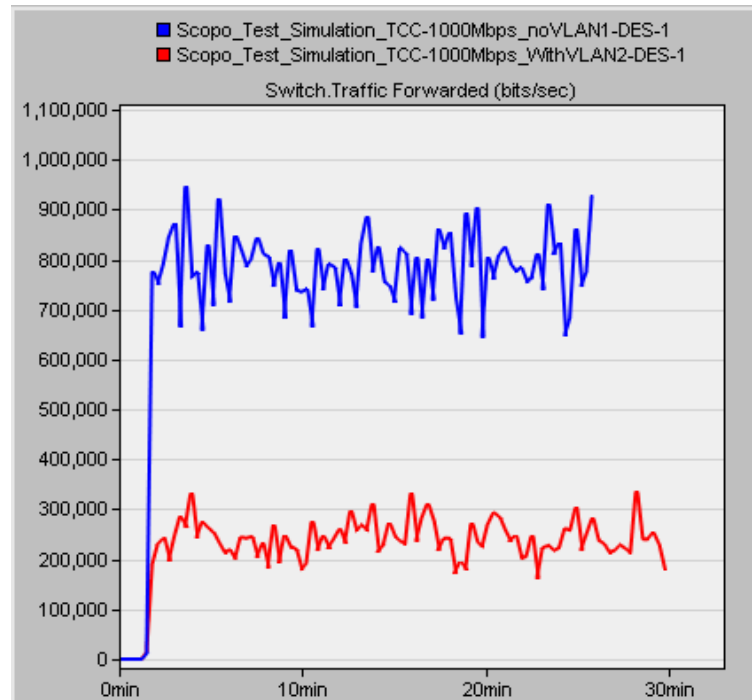
Figura 428. Tráfego recebido no *switch core* em ambiente com 30 computadores.



Fonte: Autor.

Com o *switch* de Borda01 a diferença em relação ao desempenho com o dobro de computadores não ocorreu de forma expressiva. A figura 49 mostra o gráfico de tráfego encaminhado (em bits/segundo).

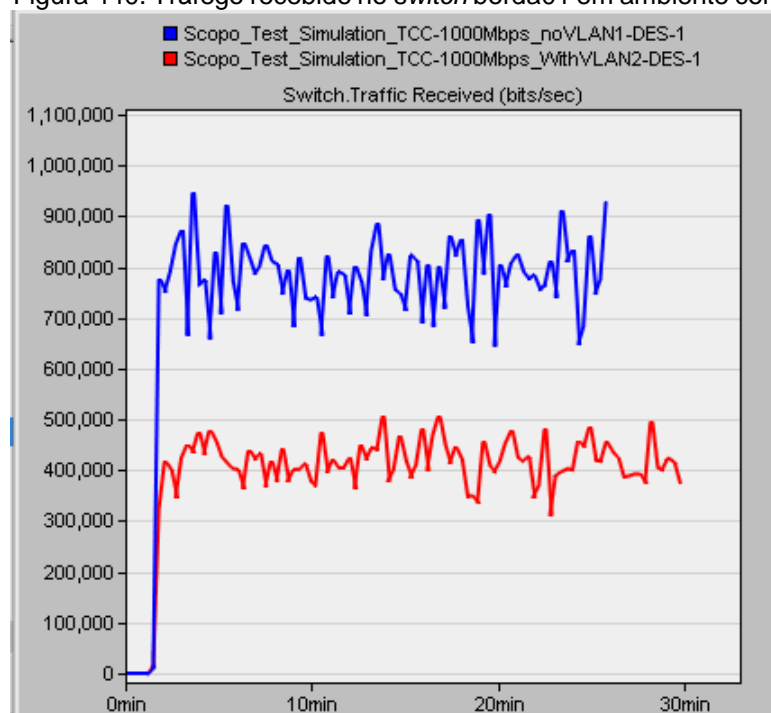
Figura 4943. Tráfego encaminhado no *switch* borda01 em ambiente com 30 computadores.



Fonte: Autor.

A figura 50 mostra o gráfico de tráfego recebido (em bits/segundo) do *switch* Borda01, com o aumento de computadores na rede o desempenho com a rede não teve muita alteração no desempenho com a segmentação da rede.

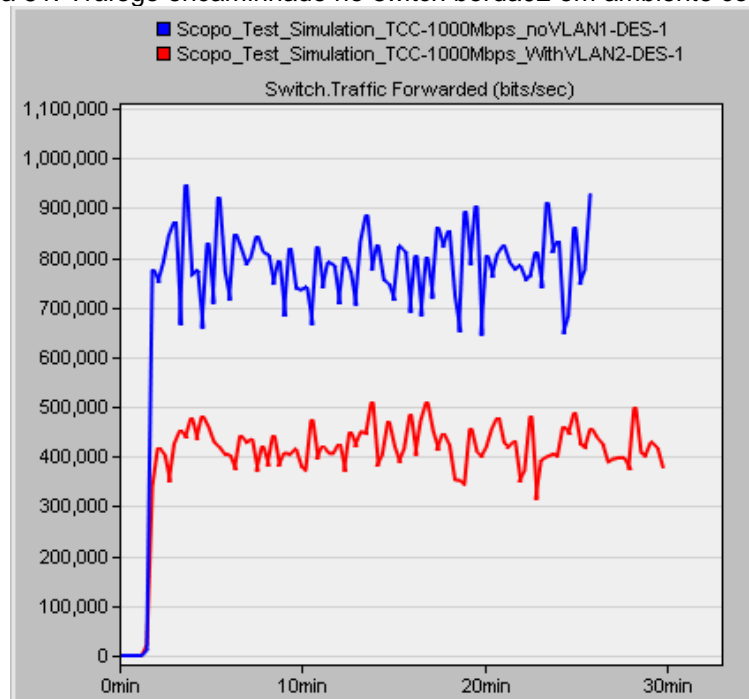
Figura 440. Tráfego recebido no *switch* borda01 em ambiente com 30 computadores.



Fonte: Autor.

A figura 51 mostra o gráfico de tráfego encaminhado do *switch* Borda02, onde a rede segmentada não trouxe um desempenho na rede tão expressivo.

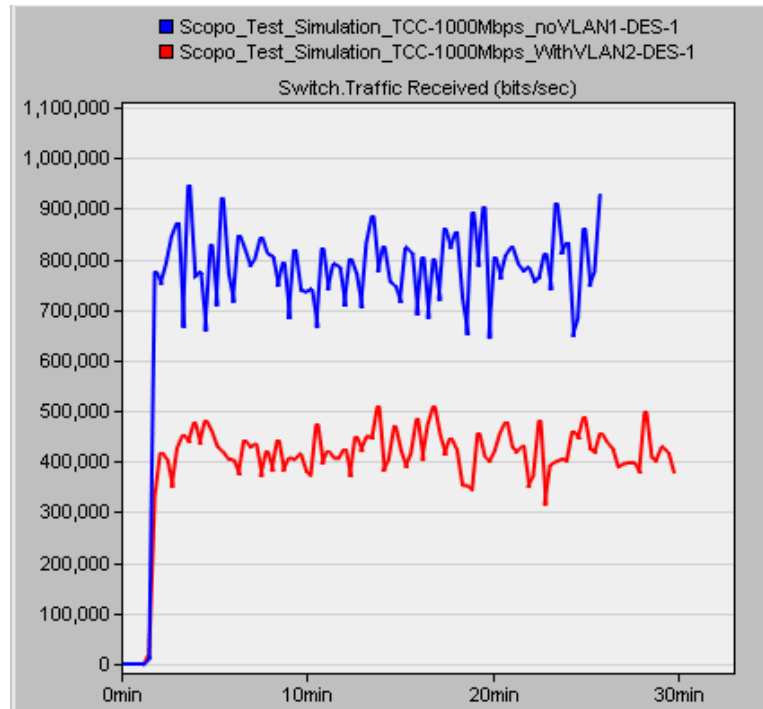
Figura 51. Tráfego encaminhado no *switch* borda02 em ambiente com 30 computadores.



Fonte: Autor.

O tráfego recebido obteve resultados muito próximos ao do tráfego encaminhado. A figura 52 mostra o gráfico do tráfego encaminhado (em bits/segundo).

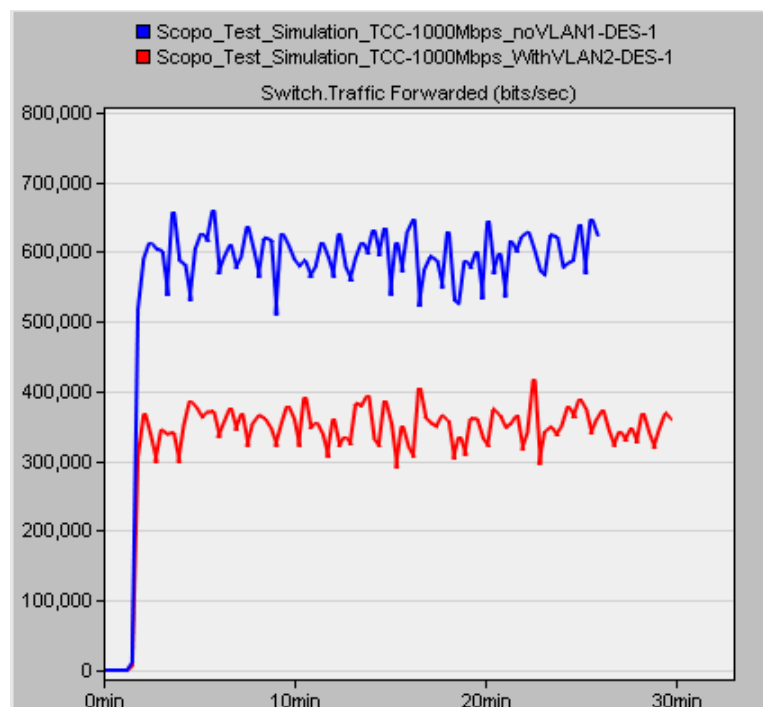
Figura 52. Tráfego recebido no *switch* borda02 em ambiente com 30 computadores.



Fonte: Autor.

Com o *switch* de Borda03 a diferença em relação ao desempenho com o dobro de computadores não obteve resultados de forma muito expressivo. A figura 53 mostra o gráfico de tráfego encaminhado (em bits/segundo).

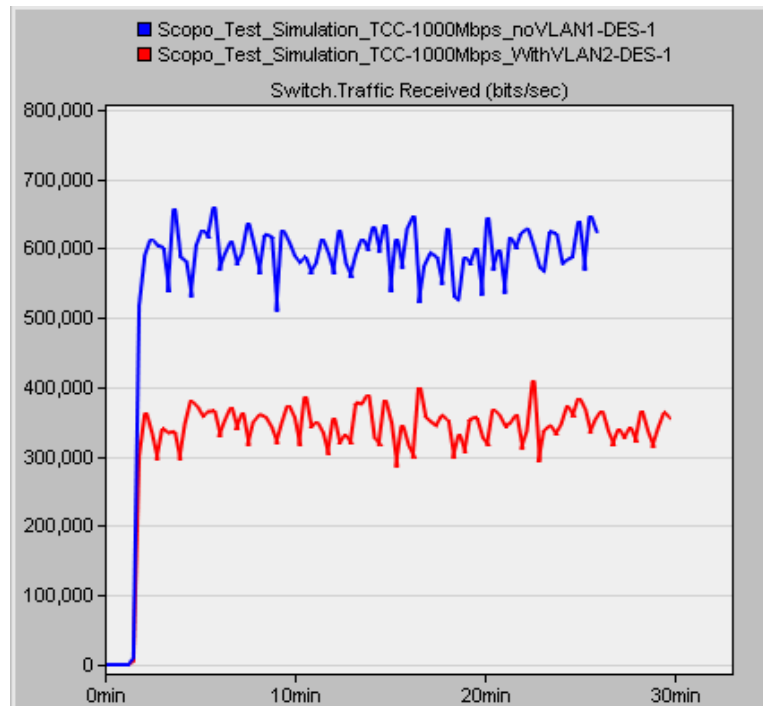
Figura 453. Tráfego encaminhado no *switch* borda03 em ambiente com 30 computadores.



Fonte: Autor.

O tráfego recebido obteve resultados muito próximos ao do tráfego encaminhado. A figura 54 mostra o gráfico do tráfego encaminhado do *switch* Borda03 (em bits/segundo).

Figura 464. Tráfego recebido no *switch* borda03 em ambiente com 30 computadores.



Fonte: Autor.

Conforme o número de computadores vai aumentando os resultados de uma rede segmentada se torna mais eficiente para um melhor desempenho. No ambiente com 30 máquinas o desempenho da rede com VLAN foi em média 66,71% em comparação a rede não segmentada. A partir da tabela 5 é possível observar em números, os equipamentos monitorados dos cenários e suas cargas de serviço referentes aos tráfegos encaminhados e recebidos.

Tabela 5. Tráfegos recebido, encaminhados e enviados dos cenários 1 e 2 com 30 dispositivos clientes

Dispositivo	Tipo de Tráfego	Performance com VLAN
<i>Switch Core</i>	Tráfego Encaminhado	96,95%
	Tráfego Recebido	102,37%
<i>Switch Borda01</i>	Tráfego Encaminhado	55,51%
	Tráfego Recebido	19,71%
<i>Switch Borda02</i>	Tráfego Encaminhado	21,85%
	Tráfego Recebido	20,87%
<i>Switch Borda03</i>	Tráfego Encaminhado	9,94%
	Tráfego Recebido	17,72%
Server Database	Tráfego Encaminhado	53,02%
	Tráfego Recebido	98,75%
<i>Email Server</i>	Tráfego Encaminhado	94,51%
	Tráfego Recebido	81,12%
<i>Voice Server</i>	Tráfego Encaminhado	93,52%
	Tráfego Recebido	66,71%

Fonte: Autor.

No próximo capítulo serão apresentadas as conclusões finais do projeto, com base nas análises apresentadas anteriormente, e possibilidades para trabalhos futuros.

7 CONCLUSÃO

As redes LANs são as infraestruturas básicas mínimas para um bom funcionamento de uma organização. Por isso a gestão das redes é um processo de extrema importância e ocupa uma boa parte do tempo do administrador da rede. Por isso a necessidade de uma nova tecnologia, para realizar isso de forma simples. O trabalho apresentou a VLAN como a tecnologia que auxilia na gestão, segurança e performance dessas redes, com a descrição detalhadas dessas vantagens dessa tecnologia em relação à uma rede normal. E de forma a ter maiores informações em relação a diferença de desempenho entre uma rede segmentada e uma rede não segmentada, sem a necessidade de investimento em equipamentos e interferir em um ambiente em produção antes de possuir relatórios, foi realizado um estudo que teve como objetivo avaliar através da simulação o melhor ambiente a segmentar uma rede. Com base nos experimentos foi possível observar que grande parte de todo tráfego gerado nas redes de computadores são desnecessário, e conforme o tamanho do ambiente com maior quantidade de dispositivos conectados, o tráfego desnecessário se torna maior ainda. Em experimentos realizados em ambientes menores o desempenho obtido em uma rede segmentada teve um acréscimo pouco expressivo, com um ganho de performance média de 20%, em ambientes menores pode não ser viável o investimento para a implantação de VLAN, dependendo do custo benefício a se ganhar com essa implementação. Porém, a partir da utilização de VLANs para segmentar essas redes maiores, o tráfego total da rede obteve uma significativa redução, isso se torna mais expressivo conforme o tamanho de computadores na rede, conseguindo um desempenho médio de 55% e 66% a mais com a segmentação da rede nos ambientes analisados nesse estudo, essa diferença de desempenho comparando essas duas redes ocorre pelo fato de que as redes segmentadas tem a capacidade de reduzir o envio de pacotes para endereços diferentes do destinatário, e conseqüentemente aumentado a capacidade de toda a rede. Como cada VLAN pode ser associado a um determinado grupo de trabalho, é possível a realização de uma segmentação lógica da rede. Essas melhorias com a VLAN configuradas foram possíveis pelo controle do tráfego de *broadcast* no que permite um melhor e mais fácil gerenciamento da rede. A utilização de VLAN em redes de computadores as tornam mais seguras, pelo fato do tráfego de uma VLAN não poder ser capturado por membro

de outra rede virtual, mesmo que estejam no mesmo *switch*. Assim a tentativa de acesso a uma VLAN não permitida o tráfego é “ignorado” e não consegue ter acesso a nenhum tipo de informação da rede. Com isso o tráfego desnecessário gerado é descartado pelo *switch* não acarretando nenhum prejuízo ao desempenho da rede. Como trabalho futuro pode ser realizar uma comparação de um cenário a ser trabalhado em ambiente real, montando o mesmo ambiente em um simulador, executando serviços iguais, capturando o tráfego tanto da rede real quanto a rede simulada e compará-los. Realizar um projeto a partir de outras métricas, novas topologias e modelos de redes.

REFERÊNCIAS

AL-HADIDI, M. R. A., Performance Analysis of EIGRP via OSPF Based on OPNET and GNS3. Disponível em < <http://maxwellsci.com/print/rjaset/v8-989-994.pdf>>. Acesso em: 30 de maio de 2016.

ALBERTI, A. M.; E. NETO, A. L.; MENDES, L. de S. Simulação de redes atm. In: XVII SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES, 17., 1999, Brasília. Anais. Vila Velha: Grafer, 1999. p. 212 - 217.

ALECRIM, P. D. Simulação computacional para redes de computadores. Rio de Janeiro: Ciência Moderna, 2009. 272 p.

ARAÚJO, H. S.; CASTRO, W. L. T.; HOLANDA FILHO, R. Simulação em RSSF para Protocolos de Roteamento usando uma Abordagem Geocast. ERCEMAPI, 2009. 90p.

BORGES, F. Redes de Comunicação Industrial - Documento técnico nº2. Edição de Setembro de 2007. Schneider Electric. Disponível em: <http://www.schneiderelectric.pt/paginas/Formacao/DOC_tecnicos/DOC_tecnicos/DocTecnico_redes.pdf> Acesso em 28 fevereiro 2015.

CAVALCANTE, Nayara Sá. A evolução do homem frente às novas tecnologias. Disponível em: < <http://www.artigonal.com/ensino-superior-artigos/a-evolucao-do-homem-frente-as-novas-tecnologias-909757.html> > Acesso em 05 de Abril de 2015.

CANTÚ, EVANDRO. REDES DE COMPUTADORES E INTERNET. SÃO JOSE, SC: CEFET, 2003. 75 P.

CARISSIMI, Alexandre da Silva; ROCHOL, J.; GRANVILLE, L. Z. Redes de Computadores. Porto Alegre: Bookman, 2010. 391p.

CECHIN, S. L. Avaliação de Desempenho em Redes de Computadores. 2005. Trabalho Individual (Doutorado em Ciência da Computação) – Instituto de Informática, UFRGS, Porto Alegre.

Cisco Systems. Cisco Understanding and Configuring VLAN Trunk Protocol (VTP) – Document ID: 10558. [S.1.], 2002. Disponível em: www.cisco.com/warp/public/473/21.pdf. Acessado em 13 de Abril de 2015.

Cisco Systems Inc. 2003. Cisco Networking Academy Program CCNA 3 and 4 Companion Guide, Third Edition. Hardcover.

CLARK, K.; HAMILTON, K. Cisco LAN *switching*. 1. Ed. Indiana, USA: Cisco Press, 1999 926 p.

COMER, Douglas E. Interligação de Redes com TCP/IP. 1. ed. Rio de Janeiro: Elsevier, 2006.

CORDEIRO, A. 2002. Introdução à Segurança dos Sistemas de Informação. Segurança um fator de sucesso – Auditoria, Políticas e Benefícios da Segurança, Lisboa, FCA – Editora de informática Ltda.

Dooley, k. Designing Large-Scale LANs. Sebastopol, CA, USA: O'Reilly Associates, Inc., 2002. 385 p.

E-COMMERCE cresce 24% e vende 35,8 bilhões em 2014. 2015. Disponível em: <<http://www.profissionaldeecommerce.com.br/e-commerce-cresce-24-e-vende-358-bilhoes-em-2014/>>. Acesso em: 10 abr. 2015.

FEY, Ademar Felipe; GAUER, Ricardo Raul. Desvendando VLAN. 2. ed. Caxias do Sul: Júlio Battisti, 2015. 140 p.

FILIPPETTI, Marco Aurélio. CCNA 4.1 (Exame 640-802): Guia Completo de Estudo. Florianópolis: Visual Books, 2008. 478 p

GOUVEIA, J., MAGALHÃES, A. (2005). *Redes de Computadores*. R. D. Estefânia, 138, R/C Dto., 1049-057 LISBOA: FCA - Editora de Informática, Ltda.

HALSALL, F. Data communications, computer networks and opens systems. 4. Ed. Nova York. Addison-Wesley, 1996. 928p.

HASSAN, Mahbub; JAIN, Raj. High Performance TCP/IP Networking: Concepts, Issues, and Solutions. New Jersey: Pearson Prentice Hall, 2004. 367 p.

HUCABU, D. CCNP BCMSN – Official Exam Certification Guide. 4. ed. Indiana, USA: Cisco Press, 2007. 598 p.

KENYON, T. High-Performance Data Network Design: Design Techniques and Tools. Daytona Beach, USA: Digital Press, 2002. 926 p.

KUROSE, James F.; ROSS, Keith W. Redes de computadores e a Internet: uma abordagem top-down. 5. ed. São Paulo: Addison Wesley, 2010.

LAW, A. M., KELTON, W. D. Simulation modeling and analysis. 2ed. Nova York, McGraw-Hill, 1991. 804p.

LEONARDO HAFFERMANN. Segmentação de Redes com VLAN. Disponível em <<http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Haffermann%20-%20artigo.pdf>>. Acesso em: 27 fevereiro 2015.

MAHAJAN, P. S.; INGALLS, R. G. Evaluation of methods used to detect warm-up period in steady state simulation. Oklahoma: Winter, 2004. 671p.

MENDEZ, G. R.; YUNUS, M. A.; MUKHOPADHYAY, S. C.; A WiFi based smart wireless sensor network for an agricultural environment. Sensing Technology, Berlin, 2011.

MIRANDA, Anibal D. A.. INTRODUÇÃO ÀS REDES DE COMPUTADORES. Vila Velha: Esab – Escola Superior Aberta do Brasil Ltda., 2008. 348 p.

MORAES, C. C. de; CASTRUCCI, P. L. Engenharia de Automação Industrial. 2. ed. LTC, 2007. IEEE SOCIETY COMPUTER. IEEE Std 802.1Q. In: IEEE Standard for local and metropolitan area network – *Virtual Bridged Local Area Networks*. [S.l.: s.n.], 2006. p. 303.

MORAES, Alexandre F. Redes de computadores: fundamentos. 7.ed. São Paulo: Érica, 2010.

ODEON, Wendell. CCENT/CCNA ICND 1: Guia Oficial de Certificação para o Exame. 2. ed. Rio de Janeiro: Alta Books, 2008. 488 p.

ODOM, W; HEALY, R.; MEHTA, N; CCIE Routing and Switching Exam Certification Guide. 3. Ed. Indianapolis, IN, USA: Cisco Press, 2008. 1057 p. ISBN 978-1-58720-196-7.

OLIVEIRA, Eliseu et al. MENTOR: A network performance recommendation tool. In: SALÃO DE FERRAMENTAS DO SBRC, 16. 2008, Florianópolis. Anais. Salvador: Universidade Salvador (unifacs), 2008. p. 43 - 44.

OPNET IT. Disponível em <http://br.riverbed.com/products/performance-management-control/network-performance-management/network-simulation.html#Modeler_University_Program>. Acesso em 01 de maio de 2016.

PEGDEN, C. D., SHANNON, R. E., SADOWSKI, R. P.; Introduction to simulation using SIMAN. 2. Ed. Nova York: McGraw-Hill, 1995. 600p.

SHI, L; SJÖDIN. P. A VLAN Ethernet Backplane for Distributed. IEEE Communications Magazine, p. 42-45, 2007.

SHRIRAM, Alok et al. Comparison of public end-to-end bandwidth estimation tools on high-speed links. In: PAM'05 PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE ON PASSIVE AND ACTIVE NETWORK MEASUREMENT, 6., 2005, Califórnia. Proceedings. Berlin: Springer-verlag, 2005. p. 306 - 320.

SOARES, Luiz Fernando Gomes. Redes de Computadores - das LANS, MANS e WANS às redes ATM. 2.Ed. - Rio de Janeiro: Editor Campus, 1995.

SVENSSON, Tommy; POPESCU, Alex. Development of laboratory exercises based on OPNET Modeler. 2003. 255 f. Dissertação (Mestrado) - Curso de Electrical Engineering, Blekinge Institute Of Technology, Karlskrona, 2003.

TANENBAUM, Andrew S.. Redes de Computadores. 4. ed. Amsterdam: Campus, 2010. 632 p.

TANENBAUM, Andrew S.; WETHERALL, David. Redes de computadores. 5. Ed. São Paulo: Pearson Prentice Hall, 2011

TANENBAUM, Andrew S. Redes de Computadores, editora Campus, 4ed., 2003. 968p.

TAVIERA, R. Uma metodologia para aperfeiçoamento da mudança para um sistema de produção just-in-time em uma indústria metalúrgica, usando simulação discreta e técnicas de projeto de experimentos de Taguchi. PPGEPS, Florianópolis, 1997. 123p.

VOSS, G. B., Proposta de utilização de laboratórios virtuais para o ensino de redes de computadores: articulando ferramentas, conteúdos e possibilidades. Disponível em <<http://www.cinted.ufrgs.br/ciclo20/artigos/5c-gleizer.pdf>>. Acesso em 30 de maio de 2016.

ZAMBALDE, A. L.; PADUA, C. I. P. S.; ALVES, R. M. O documento científico em Ciência da Computação e Sistemas de Informação. Minas Gerais: Departamento de Ciência da Computação, UFLA, 2008. 74p.

ZHU, M.; MOLLE, M.; BRAHAMAN, B. Design and implementation of application based secure VLAN. In: Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks., 2004, California. **Anais**... California: California Universidad, 2004. P.5-10.

ZHANG, Z. Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges. In: *Communications Surveys & Tutorials, IEEE*, 8., 2006, Guildford. P. 24-37

APÊNDICE

Simulação e Segmentação Virtual de Redes de Computadores

Marcelo Cechinel

³Departamento de Ciências de Computação
Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC – Brazil

Marcelocechinel2504@gmail.com

Abstract. *The article was developed in order to improve knowledge Concerning the implementation of Virtual Local Network (VLAN), in order to get through different environments simulations, performance results that a network will get compared to a non-segmented network. Through the study and its various features and settings can obtain the necessary knowledge to compare the different ways of implementing VLANs in order to master this technology that has stood out for its economy, flexibility and versatility..*

Resumo. *O artigo foi desenvolvido com o intuito de aprofundar os conhecimentos referentes a implementação de Redes Locais Virtuais (VLAN), com o propósito de obter através de simulações de ambientes diferentes, os resultados de desempenho que uma rede obterá em relação a uma rede não segmentada. Através do estudo e suas diversas características e configurações pode-se obter o conhecimento necessário para comparar as diferentes formas de implementação de VLANs, com o intuito de dominar esta tecnologia que vem se destacando por sua economia, flexibilidade e versatilidade.*

1. Introdução

Com o avanço da tecnologia e a expansão da internet, diversos serviços surgiram com o objetivo de facilitar a interação entre usuários conectados à rede de computadores. Com isso a quantidade das informações que trafegam pela rede tem apresentado um grande crescimento o que muitas vezes pode ocasionar lentidão na rede.

A implantação de VLANs (Virtual Local Area Network) tem a intenção de segmentar uma rede lógica afim de aumentar o controle de trafego da rede, diminuir o alcance de disseminação de pacotes (broadcast) e até o controle a locais não permitidos na rede, melhorando assim o desempenho e a segurança de uma determinada rede.

Como forma de avaliar o desempenho das redes, tem-se a implementação dessa tecnologia, de forma a trabalhar com *software* de simulação para os experimentos do modelo que rede não segmentado e segmento, procurando ser o mais fiel a realidade, gerando informações de desempenho para análise a fim de demonstrar a performance entre um ambiente normal de um ambiente segmentado.

E através dos resultados obtidos com a comparação entre as duas redes, é possível auxiliar o administrador de rede a tomar a melhor decisão em relação a estrutura de rede, e o possível investimento a ser feito na mesma.

2. Descrição do Problema

Uma infraestrutura de rede construída sem um bom planejamento, acaba ocasionando alguns fatores que podem prejudicar sua performance. Um dos fatores que pode influenciar o desempenho em uma infraestrutura de rede, são as escolhas dos equipamentos de interconexão. Dispositivos como hubs por exemplo, são produtos de baixo valor que tem como objetivo apenas estender a distância de uma rede. Porém, são equipamentos não inteligentes, e que não possuem mecanismos para identificar o tráfego de dados que está passando por ele, e apenas retransmitem os sinais de uma rede para todos os demais. Portanto se um quadro enviado possui erros, ou não cumpre o comprimento mínimo ou máximo padrão as informações são repassadas mesmo assim. Caso aconteça uma colisão em uma das portas, ela se estenderá para todas as outras portas do hub, pois toda as estações conectadas ao hub, sem exceção, recebem todo o tráfego, sendo útil ou não (CLARK; HAMILTON, 1999).

Quando há um aumento na quantidade de informações trafegando na rede, pode ocorrer problemas de perdas de pacotes, e quando isso ocorre pode se transformar em um grande problema na rede, pois as informações podem não chegar ao destino corretamente, e consequentemente tendo que reenviar os pacotes perdidos, resultando em mais congestionamento na rede (TANENBAUM, 2003).

Podem ocorrer em uma rede de computadores ameaças que podem ser classificadas como acidentais, ou intencionais, podendo ser ativas ou passivas. As ameaças acidentais são aquelas que não estão vinculadas a intenção premeditada, como bugs de *software* e *hardware*. As ameaças intencionais se definem pela variação desde a observação de dados com ferramentas simples de monitoramento de redes, ataques sofisticados baseados no conhecimento de como funciona o sistema. Ameaças passivas que são as que, quando aplicadas, não resultam em alteração de nenhuma informação contida na rede. E as ameaças ativas onde as informações são modificadas em seu sistema ou em seu estado de operação (SOARES, 1995).

2.1. Desempenho em Rede de Computadores

Para se obter um melhor desempenho das aplicações que é utilizado através da rede, é necessário conhecer seus requisitos, e também a situação atual dos canais de comunicação de testes e medições, a fim de inferir o melhor momento para utilização de determinada aplicação. Para determinar o estado momentâneo da rede, existem diversas ferramentas que realizam essa tarefa que trazem essas informações de várias maneiras. Porém, os dados apresentados, em geral, são muitas vezes, quase impossível de ser interpretado por usuários que não tenha tanta experiência na área, e acaba se tornando inacessíveis para esses profissionais. Com isso, além dos requisitos das aplicações e dos resultados obtidos através dos testes, tem que se levar em conta o tipo de usuário que vai analisar o resultado e suas preferências, podendo esses dados ser apresentado de maneira distinta e específica para cada indivíduo, obtendo assim um diagnóstico e, consequentemente, uma recomendação mais precisa e confiável (OLIVEIRA et al, 2008).

2.2. Modelagem de Redes de Computadores

A modelagem é o modelo de projeto de uma situação real de sistemas que se quer analisar para um ambiente de simulação específico, de maneira que fique o mais próximo de um ambiente real, o comportamento desses sistemas diante das situações simuladas. Com isso, por exemplo, a segmentação lógica de um ambiente de comunicação através de VLAN, a modelagem é uma tarefa que exige muito mais do que conhecer o ambiente de simulação que será utilizado, mas

também conhecimento teórico sobre VLAN, de detalhes dos componentes a serem modelados e dos objetivos que se quer alcançar com os testes. Um fator muito relevante é saber diferenciar emulação e simulação nos ambientes modelados. Pois a simulação é uma réplica da rede representando totalmente os detalhes envolvidos. Já a emulação tem o objetivo de extrair resultados da simulação, e transformar em estatísticas os dados obtidos. Com isso, na simulação não é necessário apresentar todas as funcionalidades, mas somente detalhes importantes de acordo com o que precisa saber (ALBERTI; SOUZA NETO; MENDES, 1999).

3. LAN, Segmentação e VLAN

Redes de computadores é um conjunto de dispositivos (locais ou remotos) que são interligados entre si por meio de roteadores, *switches* e entre outros, possibilitando a troca de informações entre os dispositivos, por meio de uma rede local, ou até mesmo remotamente, possibilitando a conexão de qualquer equipamento que esteja conectado em rede, como microcomputadores, notebooks, tablets, smartphones e outros. Para se caracterizar uma rede de computadores, precisa-se no mínimo de dois elementos interconectados, sendo que o número máximo não tem limite, pois teoricamente, todos os computadores do mundo poderiam estar interligados, a Internet é um exemplo (MIRANDA, 2008).

Local Area Network (LAN) é a tecnologia de rede local que liga os dispositivos em uma área geográfica limitada, como por exemplo, uma rede usada em um mesmo edifício, ou residência, e são utilizadas em conexão de computadores pessoais (TANENBAUM; WETHERALL, 2011).

O ambiente de uma organização de grande porte onde possuem mais de 300 dispositivos na rede por exemplo, ocorre uma exorbitante troca de informações em uma mesma rede física. Em uma empresa onde possuem muitos departamentos, certamente terá muitos setores em comuns mais também pouca comunicação entre diferentes departamentos. Com isso ocorre muito tráfego de dados congestionando a rede, conforme demonstra a figura. Além disso, o desempenho também é prejudicado devido ao grande número de domínios de *broadcast*. (FEY; GAUER, 2015).

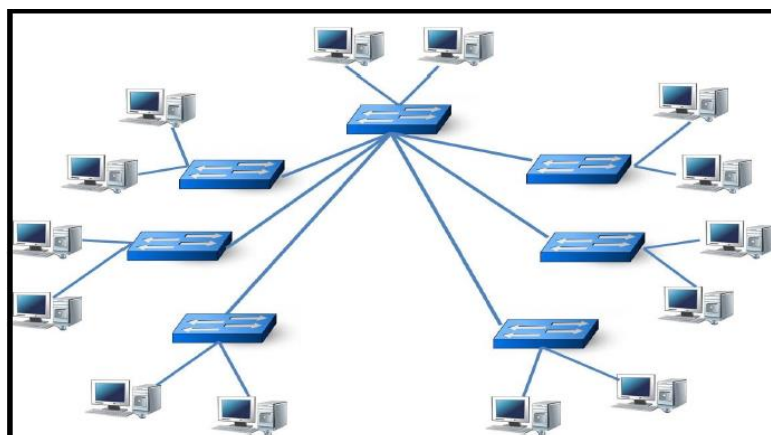


Figura 47. Rede LAN corporativa.

Para obter uma rede com um bom funcionamento, um dos principais objetivos ao realizar um projeto bem elaborado, é conseguir reduzir todo tráfego desnecessário, e uma das maneiras de se fazer isso, é limitando o alcance do tráfego (*broadcast*) somente para os domínios para os quais ele é aplicável (KENYON, 2002).

Uma boa opção para estruturação e funcionamento da rede sem que seja necessário a substituição de equipamentos é a segmentação da rede. Segmentar uma rede de computadores é fazer uma divisão lógica de segmentos simples de *Ethernet* em múltiplos segmentos, essa configuração é chamada de *Virtual Local Area Network* (VLAN) (WENDELL, 2008).

Uma *Virtual Local Area Network* (VLAN), é um agrupamento lógico de usuários e equipamentos que estão logicamente conectadas, podendo ser criadas e configuradas por meio de *switches* que possuem essa opção de serviço disponível. Com isso é possível criar e disponibilizar várias redes lógicas dentro de uma física, ou seja, cada usuário é conectado fisicamente a uma LAN, e as características dos equipamentos conectados a determinada LAN, é definida pelas limitações dos dispositivos utilizados (como o número de portas do *switch*) e o tipo de conexões configuradas pelo administrador de rede. Um exemplo básico de uma VLAN é apresentado na figura abaixo (MORAES, 2010).

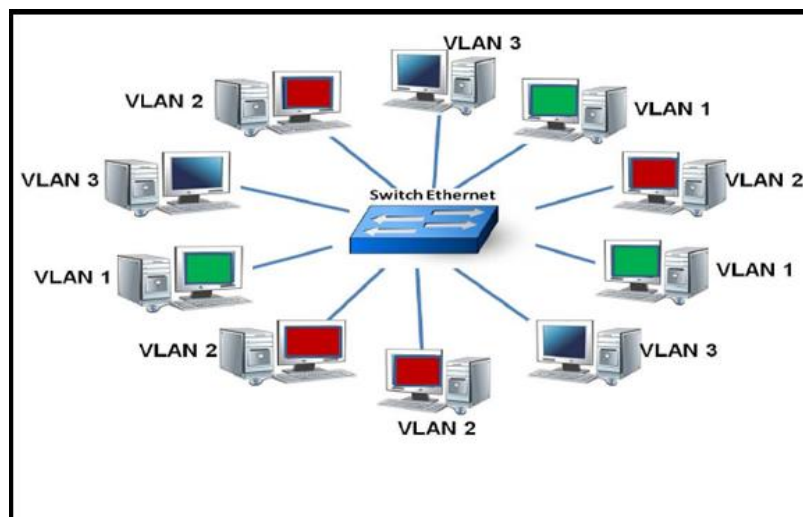


Figura 48. Rede LAN com diversas VLAN.

Uma vez configurada as redes, e os computadores instalados e configurados, seu alcance é estabelecido. Para realizar alguma alteração da rede local requer uma mudança nas conexões físicas. A conectividade lógica da LAN é igual a conectividade física (SEIFERT; EDWARDS, 2008).

Um *switch* possui várias portas de comunicação. E através dessas portas locais são inseridos os cabos de rede para realizar a interligação dos equipamentos, sendo que cada porta pode ser conectada a apenas um único dispositivo. Esses equipamentos fazem a troca de informações entre os equipamentos conectados a ele através de endereços que estão contidos nos pacotes transmitidos para o correto caminho do destinatário. Ainda é possível interligar *switches* para cobrir uma infraestrutura que abrigue uma quantidade maior de computadores na rede (TANENBAUM; WETHERALL, 2011).

3.1. Tipos de VLAN

É possível configurar a porta de um *switch* para pertencer a uma ou mais VLAN. Para fazer parte de uma rede *virtual*, a porta de um *switch* deve ser associada a uma rede lógica. O método de associação pode ser configurado para trabalhar de forma estática ou de forma dinâmica (CISCO SYSTEM, 2007).

O método de associação estática é o mais utilizado e fácil de monitorar, em um ambiente de rede onde há poucos usuários. Nesse modelo, as portas do *switch* são designadas a uma

determinada rede lógica pertencendo a esta até que o administrador de rede altere estas configurações. E logo que um dispositivo entra na rede, o mesmo passa a fazer parte da rede virtual, onde é indicado a porta pertencente, e caso ocorra uma mudança de porta, o responsável pela rede terá que, manualmente associar a porta à VLAN (FILIPPETTI, 2008).

O método de associação dinâmica funciona de maneira em que um dispositivo conectado a um segmento de rede uma atribuição de VLAN de forma automatizada. Isso ocorre utilizando aplicações que realizem esse tipo de tarefa, é possível associar VLAN por meio de endereçamento de *hardware*, endereço MAC, por protocolos ou de forma autenticada (FILLIPETTI, 2008).

3.2. Tipo de Conexão de Dispositivos em VLAN

Os computadores das redes virtuais podem ser conectados de três formas diferentes (IEEE SOCIETY COMPUTER, 2006).

Os computadores das redes virtuais podem ser conectados de três formas diferentes, considerando se estes suportam ou não o padrão IEEE 802.1Q (IEEE SOCIETY COMPUTER, 2006).

O Enlace Tronco (*Trunk Link*) é onde os equipamentos ligados à essa rede *virtual* devem reconhecer quadros com a identificação da rede lógica, e pode inserir e remover informação no cabeçalho da *tag*, ou seja, ser *VLAN-aware* (IEEE SOCIETY COMPUTER, 2006).

O Enlace de acesso (*Access Link*) é o tipo de enlace que o dispositivo conecta sem suporte a uma rede *virtual* a uma porta *Virtual Local Area Network aware* (IEEE SOCIETY COMPUTER, 2006).

Já o Enlace Híbrido (*Hybrid Link*) é uma junção dos Enlaces Tronco e de Acesso. No enlace híbrido são conectados tanto dispositivos *VLAN-aware* quanto equipamentos *VLAN-unaware* (não reconhece quadros com *Virtual Local Area Network tag*, isto é, não possuem suporte ao padrão IEEE 802.1Q) (IEEE SOCIETY COMPUTER, 2006).

Uma rede *virtual* pode possuir ao mesmo tempo os três tipos de enlaces citados sem problema algum. Considerando as classificações de rede *virtual* e os computadores que podem ser conectados a elas, torna-se possível propor uma solução para segmentação de redes de computadores (IEEE SOCIETY COMPUTER, 2006).

3.3. Solução VTP (Virtual Trunking Protocol)

O VLAN *Trunking protocol* (VTP) é um protocolo criado pela Cisco System, criado para resolver o problema mencionado anteriormente (GOUVEIA; MAGALHÃES, 2005).

É possível configurar o *switch* para trabalhar em alguns modos de VLAN *Trunking Protocol* tais como servidor VTP, que permite criar, modificar e deletar redes virtuais e especificar outros parâmetros de configuração, como a versão do VTP e retirar configurações desnecessárias. Esses clientes, que é praticamente da mesma maneira do servidor de *Virtual Local Area Network Trunking Protocol*, porém não pode criar, modificar ou deletar *Virtual Local Area Network*. VTP transparente, onde um *switch* transparente de VLAN *Trunking Protocol* não é informado sobre a configuração da Rede Virtual e não realiza a sincronização da configuração baseada nas informações recebidas, mas ele repassa a configuração para fora da sua porta de *Trunking*. Com esse protocolo desligado, se comportam da mesma maneira do transparente, porém as informações recebidas não são transmitidas (CISCO SYSTEM, 2002).

O funcionamento desse protocolo acontece de maneira semelhante ao protocolo de roteamento, que faz com que o protocolo troque informações periódicas sobre atualização. Para um bom funcionamento da Rede Virtual baseado no protocolo VTP, cabe ao administrador começar primeiro a criação de um domínio no protocolo e determinar quais os *switches* que pertencem ao domínio (ODOM; HEALY; MEHTA, 2008).

3.4. O Processo VTP e Números de Revisão

O número de revisão é um dos principais componentes de um anúncio VTP. É um número de 32 bits que tem o objetivo de indicar o nível de revisão para um quadro de uma rede lógica *trunking protocol*. O valor padrão de configuração para um *switch* é zero. Cada vez em que um *switch* no modo Servidor VTP faz alguma ação, como adicionar, deletar ou modificar alguma configuração de uma Rede *Virtual*, ele incrementa o número de revisão em uma unidade. O maior número de revisão dentro de um domínio de *VLAN Trunking Protocol* carrega a informação mais atualizada. Quando um *switch* em modo Cliente recebe um número de revisão superior o que possui, ele deve atualizar sua configuração de Rede *Virtual* sobrescrevendo suas informações com o banco de dados VTP do número de revisão mais alto. Quando há uma alteração do nome de domínio desse protocolo, não aumenta o número de revisão. Ao invés disso, o valor volta a ser zero. O processo de atualização começa quando o administrador configura um *switch* no modo servidor e modifica a configuração de uma rede lógica. A figura a seguir mostra de forma exemplificada o anúncio VTP (ODOM; HEALY; MEHTA, 2008).

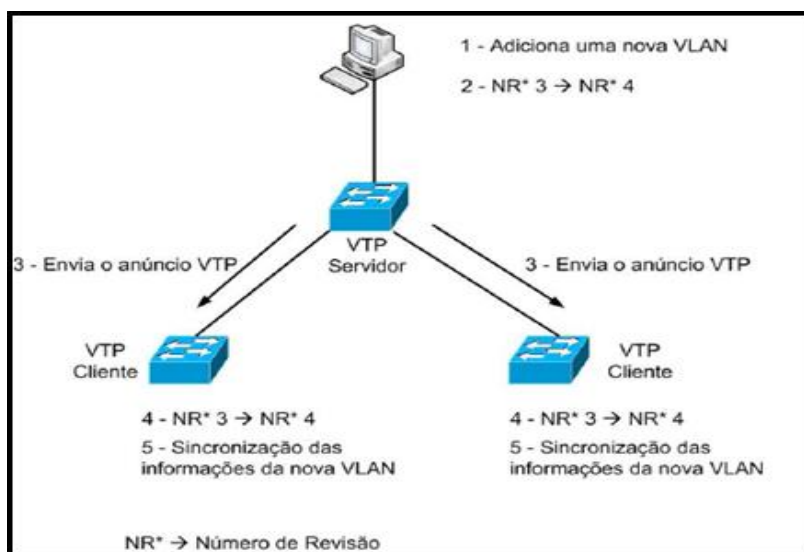


Figura 49. Processo VTP e Número de Revisão.

3.5. Vantagem na utilização de VLAN

Ao trabalhar com rede *virtual*, reduz consideravelmente os problemas encontrados em uma rede de computadores, tornando muito mais eficiente e econômica, principalmente em redes corporativas, onde a qualquer momento pode haver a necessidade de reestruturação do sistema, ou mesmo o aumento no número de usuários, entre outras situações, que requerem uma flexibilidade, como pode se obter com VLAN para as redes locais (MORAIS, 2005).

3.5.1. Redução de domínios de broadcast

Os *broadcasts* são responsáveis por grande parte do tráfego total da rede, tornando assim o desempenho das tradicionais redes locais inferior ao das VLAN. Com a rede segmentada

virtualmente reduz o envio de pacotes para endereços desnecessários, aumentando a capacidade de toda a rede (FILLIPETTI, 2008).

3.5.2. Segurança

Com a divisão de redes virtuais se consegue mais segurança, já que estas só se comunicam com os dispositivos que estão na mesma VLAN. Por exemplo, as redes do setor de administração são separadas do setor de marketing, diminuindo as chances de acesso a informações confidenciais. No caso somente através de um dispositivo de rede com a função roteador é possível realizar a comunicação entre VLAN distintas (MORAES, 2010).

3.5.3. Gerenciamento

Com rede *virtual* é possível para o administrador de rede ter um maior controle da rede, já que pode configurar as portas dos *switches* e alocar os usuários de maneira que facilite a organização da estrutura e seu controle (FILLIPETTI, 2008).

4. Simulação

A simulação pode ser definida como uma técnica que pode ser utilizada por acontecer em um ambiente monitorado, onde os testes executados podem ser repetidos indeterminadas vezes sem que cause danos nenhum aos atores da cadeia. Tem dois importantes detalhes necessários a simulação, o primeiro refere-se ao ensino baseado em trabalhos, no qual se enfatiza o que se quer obter e como obter tal objetivo proposto, e o segundo é a relação com o simulador (ALECRIM, 2009).

Com o grande avanço da Tecnologia da Informação, os desafios em se planejar novos projetos de rede aumentam no mesmo ritmo, e com isso, cada vez mais o uso da simulação em novos projetos, estão se tornando essenciais para determinar os cenários adequados a ser implementado, de acordo com as variáveis que podem fazer parte do ambiente, podendo realizar simulação de redes de filas simples até cenários mais complexos de acordo com a necessidade (MENDEZ; YUNUS; MUKHOPADHYAY, 2011).

4.1. Objetivos da Simulação em Redes de Computadores

A simulação se tornou uma ferramenta essencial para auxiliar na viabilidade ou não de uma determinada situação. Geralmente, uma experiência é a base para validar um cenário, mas para utilização de projetos de rede, uma hipótese pode ser validada baseado nas seguintes métricas: analítico, simulação e experimento controlado (ARAUJO; CASTRO; HOLANDA, 2009).

Na validação de um cenário, a modelagem matemática analítica é baseada em cálculos e fórmulas matemáticas, já o experimento é baseado em uma análise em cima de uma situação real monitorada. Com as simulações, são planejados cenários virtuais, com o máximo de proximidade com a realidade, possuindo como base para os testes ferramentas de processamento de dados, para assim poder gerar informações e obter resultados antes de implementar o experimento real (ARAUJO; CASTRO; HOLANDA, 2009).

Para realizar as simulações de rede, é necessário a utilização de programas de simulação ou simuladores, para que se possa realizar os testes de como um ambiente real irá se comportar com diferentes variáveis, e com isso produzir fielmente o sistema analisado. Assim é possível moldar o simulador para cumprir as tarefas especificadas, fazendo com que se tenha um comparativo do custo e tempo ao criar uma nova estrutura de rede. Também é possível testar situações e eventos onde a emulação no *hardware* real não seria possível, mas que podem ser

uteis a simulação de novos protocolos de rede (MENDEZ; YUNUS; MUKHOPADHYAY, 2011).

5. Conclusão

As redes LANs são as infraestruturas básicas mínimas para um bom funcionamento de uma organização. Por isso a gestão das redes é um processo de extrema importância e ocupa uma boa parte do tempo do administrador da rede. Por isso a necessidade de uma nova tecnologia, para realizar isso de forma simples. O artigo apresentou a VLAN como a tecnologia que auxilia na gestão, segurança e performance dessas redes, com a descrição detalhadas dessas vantagens dessa tecnologia em relação à uma rede normal. E de forma a ter maiores informações em relação a diferença de desempenho entre uma rede segmentada e uma rede não segmentada, sem a necessidade de investimento em equipamentos e interferir em um ambiente em produção antes de possuir relatórios, foi realizado um estudo que teve como objetivo avaliar através da simulação o melhor ambiente a segmentar uma rede. Com base nos experimentos foi possível observar que grande parte de todo tráfego gerado nas redes de computadores são desnecessário, e conforme o tamanho do ambiente com maior quantidade de dispositivos conectados, o tráfego desnecessário se torna maior ainda. A utilização de VLAN em redes de computadores as tornam mais seguras, pelo fato do tráfego de uma VLAN não poder ser capturado por membro de outra rede virtual, mesmo que estejam no mesmo *switch*. Assim a tentativa de acesso a uma VLAN não permitida o tráfego é “ignorado” e não consegue ter acesso a nenhum tipo de informação da rede. Com isso o tráfego desnecessário gerado é descartado pelo *switch* não acarretando nenhum prejuízo ao desempenho da rede. Como trabalho futuro pode ser realizar uma comparação de um cenário a ser trabalhado em ambiente real, montando o mesmo ambiente em um simulador, executando serviços iguais, capturando o tráfego tanto da rede real quanto a rede simulada e compará-los. Realizar um projeto a partir de outras métricas, novas topologias e modelos de redes.

6. Referências bibliográficas

- ALBERTI, A. M.; E. NETO, A. L.; MENDES, L. de S. Simulação de redes atm. In: XVII SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES, 17., 1999, Brasília. Anais. Vila Velha: Grafer, 1999. p. 212 - 217.
- ALECRIM, P. D. Simulação computacional para redes de computadores. Rio de Janeiro: Ciência Moderna, 2009. 272 p.
- ARAÚJO, H. S.; CASTRO, W. L. T.; HOLANDA FILHO, R. Simulação em RSSF para Protocolos de Roteamento usando uma Abordagem Geocast. ERCEMAPI, 2009. 90p.
- Cisco Systems. Cisco Understanding and Configuring VLAN Trunk Protocol (VTP) – Document ID: 10558. [S.l.], 2002. Disponível em: www.cisco.com/warp/public/473/21.pdf. Acessado em 13 de Abril de 2015.
- Cisco Systems Inc. 2003. Cisco Networking Academy Program CCNA 3 and 4 Companion Guide, Third Edition. Hardcover.
- CLARK, K.; HAMILTON, K. Cisco LAN *switching*. 1. Ed. Indiana, USA: Cisco Press, 1999 926 p.
- FEY, Ademar Felipe; GAUER, Ricardo Raul. Desvendando VLAN. 2. ed. Caxias do Sul: Júlio Battisti, 2015. 140 p.

FILIPPETTI, Marco Aurélio. CCNA 4.1 (Exame 640-802): Guia Completo de Estudo. Florianópolis: Visual Books, 2008. 478 p

GOUVEIA, J., MAGALHÃES, A. (2005). *Redes de Computadores*. R. D. Estefânia, 138, R/C Dto., 1049-057 LISBOA: FCA - Editora de Informática, Ltda.

KENYON, T. High-Performance Data Network Design: Design Techniques and Tools. Daytona Beach, USA: Digital Press, 2002. 926 p.

MENDEZ, G. R.; YUNUS, M. A.; MUKHOPADHYAY, S. C.; A WiFi based smart wireless sensor network for na agricultural environmet. Sensing Technology, Berlin, 2011.

MIRANDA, Anibal D. A. INTRODUÇÃO ÀS REDES DE COMPUTADORES. Vila Velha: Esab – Escola Superior Aberta do Brasil Ltda., 2008. 348 p.

MORAES, C. C. de; CASTRUCCHI, P. L. Engenharia de Automação Industrial. 2. ed. LTC, 2007. IEEE SOCIETY COMPUTER. IEEE Std 802.1Q. In: IEEE Standard for local and metropolitan area network – *Virtual Bridged Local Area Networks*. [S.l.: s.n.], 2006. p. 303.

MORAES, Alexandre F. Redes de computadores: fundamentos. 7.ed. São Paulo: Érica, 2010.

ODOM, W; HEALY, R.; MEHTA, N; CCIE Routing and Switching Exam Certification Guide. 3. Ed. Indianapolis, IN, USA: Cisco Press, 2008. 1057 p. ISBN 978-1-58720-196-7.

OLIVEIRA, Eliseu et al. MENTOR: A network performance recommendation tool. In: SALÃO DE FERRAMENTAS DO SBRC, 16. 2008, Florianópolis. Anais. Salvador: Universidade Salvador (unifacs), 2008. p. 43 - 44.

SOARES, Luiz Fernando Gomes. Redes de Computadores - das LANS, MANS e WANS às redes ATM. 2.Ed. - Rio de Janeiro: Editor Campus, 1995.

TANENBAUM, Andrew S.; WETHERALL, David. Redes de computadores. 5. Ed. São Paulo: Pearson Prentice Hall, 2011

TANEMBAUM, Andrew S. Redes de Computadores, editora Campus, 4ed., 2003. 968p.