THIAGO FLORIANO WYKRET

SEGMENTAÇÃO VIRTUAL DE REDES DE COMPUTADORES

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para a obtenção do título de Bacharel em Ciência da Computação

Orientador
Prof. Dr. Luiz Henrique Andrade Correia

Lavras
Minas Gerais - Brasil
2009

THIAGO FLORIANO WYKRET

SEGMENTAÇÃO VIRTUAL DE REDES DE COMPUTADORES

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

Área de Concentração:

Redes de Computadores

Orientador:

Prof. Dr. Luiz Henrique Andrade Correia

LAVRAS
MINAS GERAIS – BRASIL
2009

Ficha Catalográfica

Wykret, Thiago Floriano

Segmentação Virtual de Redes de Computadores / Thiago Floriano Wykret. Lavras – Minas Gerais, 2009. 123p. :il.

Monografia de Graduação – Universidade Federal de Lavras. Departamento de Ciência da Computação

1. Redes de Computadores. 2. Segmentação Virtual. I. Wykret, T. F. II. Universidade Federal de Lavras. III. Título

THIAGO FLORIANO WYKRET

SEGMENTAÇÃO VIRTUAL DE REDES DE COMPUTADORES

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para a obtenção do título de Bacharel em Ciência da Computação

Aprovada em *26 de Novembro de 2009*

Prof. Dr. Bráulio Adriano de Mello

Prof. Dr. João Carlos Giacomin

Prof. Dr. Luiz Henrique Andrade Correia
(Orientador)

Lavras
Minas Gerais - Brasil
2009

Dedico este trabalho a minha namorada Bárbara e aos meus pais, Heron e Abadia, pelo apoio incondicional ao longo desta caminhada

Agradecimentos

Agradeço, primeiramente, a Deus, por ter me dado saúde e inteligência para concluir este trabalho.

À minha família, em especial aos meus pais, Heron e Abadia, que não mediram esforços para que eu chegasse até esta etapa da minha vida, pelo sacrifício, pela dedicação e base sólida que sempre me deu força. Pelo incentivo, pela confiança, pelo apoio em todos os momentos.

À minha namorada Bárbara, pelo amor, companheirismo, carinho e paciência, fundamentais para a concretização deste sonho e para seguir em frente. Pelo grande apoio e incentivo durante a época do vestibular, nos momentos difíceis durante a graduação e no desenvolvimento deste trabalho. Sem isso eu não teria conseguido chegar até aqui.

Aos meus avós, Laedy (em memória) e Diva, João (em memória) e Francisca, pelas orações, por todo apoio e carinho em todos os momentos.

Ao meu professor e orientador Luiz Henrique, pela confiança, apoio, dedicação e comprometimento com este trabalho. Pela paciência, pela excelente supervisão e as várias revisões até o término desta monografia. Superando as minhas mais altas expectativas em relação a um orientador, tornou-se um exemplo a ser seguido.

Aos professores e funcionários do DCC – Departamento de Ciência da Computação.

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

“Para grandes realizações devemos não somente agir, mas também sonhar; não somente planejar, mas também acreditar” Anatole France

Sumário

Lista de Figuras

Lista de Tabelas

SEGMENTAÇÃO VIRTUAL DE REDES DE COMPUTADORES

RESUMO

Este trabalho tem o objetivo de estudar e analisar o tráfego em redes de computadores usando segmentação virtual, ou mais especificamente, *Virtual Local Area Network* (VLAN). A técnica de segmentação de redes é um assunto pouco explorado na literatura, limitando-se, em geral, a pequenos trechos de livros, alguns guias de certificação e manuais de equipamentos. O material produzido por este trabalho apresenta uma síntese e exemplos de VLAN. O *software OPNET IT Guru Academic Edition* foi usado para analisar o tráfego de dados em *switches* utilizando VLANs. Essa ferramenta possibilita a criação de cenários para simulações em redes de computadores. Para a segmentação virtual de redes foi proposta a solução de *VLAN Trunking Protocol* (VTP). Essa solução permite a expansão de VLANs por múltiplos *switches* e também a configuração de mais de uma rede virtual em cada equipamento. Foram comparadas redes de computadores que utilizam ou não segmentação virtual. A partir da utilização de VLANs, o tráfego total da rede sofreu significativa redução que, aproximou-se, em algumas situações, a 70%.

Palavras-Chave: Redes de computadores, segmentação virtual, *Virtual Local Area Network*, simulação, *OPNET IT Guru Academic Edition.*

VIRTUAL SEGMENTATION OF COMPUTER NETWORKS

ABSTRACT

This dissertation has the objective to study and analyze the traffic in computer networks using virtual segmentation, or more specifically, Virtual Local Area Network (VLAN). The technique of network segmentation is a subject little explored in literature, merely, in general, small sections of books, some certification guides and equipment manuals. The material produced by this paper presents a synthesis and examples of VLAN. The software OPNET IT Guru Academic Edition was used to analyze the traffic data from switches utilizing VLANs. This tool enables the creation of scenarios for simulation in computer networks. For the virtual segmentation of networks was proposed solution VLAN Trunking Protocol (VTP). This solution allows the spanning of VLANs across multiple switches and also the configuration of more than one virtual network for each equipment. Computer networks utilizing virtual segmentation were compared. As from the use of VLANs, the total network traffic had significantly reduction, come near, in some situations, to 70%

Keywords: Computer networks, virtual segmentation, Virtual Local Area Network (VLAN), simulation, OPNET IT Guru Academic Edition.

Capítulo 1

INTRODUÇÃO

O rápido e, muitas vezes, desordenado crescimento das redes de computadores e seus serviços tem gerado nos últimos anos um grande aumento no fluxo de dados nas redes locais. Tais redes estão se tornando cada vez mais importantes no cotidiano de todas as pessoas e as exigências dos usuários em relação aos sistemas que utilizam redes de computadores estão tornando-se maiores (SHI; SJöDIN, 2007). A configuração e a localização de equipamentos e dos protocolos devem ser ajustados da melhor maneira possível com o intuito de criar uma rede de computadores que cumpra os propósitos para os quais ela foi projetada (DOOLEY, 2002). A infraestrutura de uma rede local pode, em algumas situações, não conseguir suprir a demanda computacional de seus usuários. Portanto, torna-se necessária uma reestruturação lógica de redes de computadores, de forma a aproveitar os recursos pré-existentes e proporcionar um melhor desempenho e maior facilidade nas atividades gerenciais. Tal reformulação é possível por meio de segmentação virtual de redes de computadores, ou seja, a criação de *Virtual Local Area Network* (VLAN). O termo VLAN refere-se à criação de redes locais virtuais em um mesmo equipamento ou conjunto de equipamentos de rede. Em segmentos de redes *Ethernet* muito extensos, as VLANs podem reduzir os

domínios de colisão, melhorando consideravelmente o desempenho (IEEE SOCIETY COMPUTER, 2006).

1.1 Objetivo

O presente trabalho tem como objetivos, a implantação e a análise dos resultados alcançados na segmentação de redes de computadores por meio de VLANs. Com base nas informações obtidas, apresentar soluções para melhor utilização dos recursos de redes pré-existentes. São apresentados os resultados das análises e propostas para reestruturação de infraestrutura lógica em redes de computadores, por meio de segmentação virtual, possibilitando a redução dos domínios de colisão e melhorando significativamente o desempenho e o funcionamento das redes de computadores. Outro objetivo do projeto é a criação de um tutorial sobre VLANs, pois o material é escasso, encontrado basicamente em manuais de equipamentos e guias de certificação.

1.2 Motivação

Uma grande parcela das atuais redes de computadores sofre com problemas de falta de estruturação e perda de desempenho, muitas vezes relacionados a ampliações rápidas e desorganizadasdes. A dependência de serviços automatizados e que necessitam da utilização das redes de computadores torna-se cada vez maior em universidades, empresas e diversos tipos de corporações. Dessa forma, são indispensáveis novas formas de implementação de redes de computadores que ofereçam suporte a toda essa demanda requisitada. Os custos para aquisição de equipamentos que possibilitem as reformulações necessárias muitas vezes são proibitivos, levando à inviabilidade dos projetos de reestruturação. Sendo assim, novas técnicas que reutilizam recursos já disponíveis se tornam mais utilizadas. A segmentação virtual de redes de computadores é uma das maneiras mais in-

dicadas. Este tipo de segmentação de redes é um assunto pouco explorado na literatura, resumindo-se, em geral, a apêndices e trechos de livros, guias de certificação, manuais de equipamentos e alguns sites na *Internet*.

1.3 Definição do problema

A formação de grandes domínios de colisão e o aumento de tráfego de dados em redes locais podem acarretar um maior número de colisões e consequentemente perda de informações. Além disso, a segurança e o desempenho de redes de computadores com grandes domínios de colisão ficam extremamente comprometidos. Com isso o uso de roteadores se torna necessário; e a reestruturação utilizando esse tipo de equipamento aumenta o grau de dificuldade de manutenção da rede e pode acarretar custos elevados, que muitas vezes tornam o projeto inviável.

1.4 Solução proposta

A segmentação virtual de redes de computadores permite a divisão de domínios de *broadcast* (divisão da rede local em vários segmentos lógicos), redução significativa de colisões, aumento de segurança, redução de custos com equipamentos e processos administrativos e facilidade nas atividades gerenciais. Uma das possíveis soluções na implementação de redes virtuais é o uso de *VLAN Trunking Protocol* (VTP). O VTP é um protocolo proprietário da *Cisco Systems*, usado na comunicação entre *switches* para a troca de informações sobre as configurações da VLAN. Essa solução permite que as VLANs realizem uma expansão por múltiplos *switches* e também a configuração de mais de uma rede virtual em cada equipamento.

1.5 Organização do trabalho

No capítulo 2, são apresentados os conceitos de VLAN, suas características e aplicações. Também são descritos seus benefícios, formas de implementação e uma proposta de solução por meio de *VLAN Trunking Protocol*. A metodologia utilizada neste trabalho é apresentada no capítulo 3, juntamente com informações sobre o processo de simulação utilizado. No capítulo 4 são descritos os detalhes dos processos de modelagem e simulação abordados neste trabalho, bem como os cenários utilizados no ambiente *OPNET IT Guru Academic Edition*. Os resultados obtidos com base nas simulações executadas são descritos no capítulo 5. Esses resultados são analisados comparando o desempenho de redes de computadores com e sem o uso de VLANs. No capítulo 6 são apresentadas as conclusões deste trabalho com a modelagem e simulação de redes com implantação de *Virtual LANs*. Além disso, são abordadas possibilidades para trabalhos futuros.

Capítulo 2

REFERENCIAL TEÓRICO

Uma rede local, LAN (*Local Area Network*), inicialmente era definida como sendo uma rede de computadores fisicamente conectados e localizados em uma mesma área geográfica. Atualmente, podemos defini-la como um único domínio de colisão e de mesma propriedade e tendo como limite geográfico o roteador da rede. Isso significa que um usuário da rede difunde informações através da LAN e estas podem ser recebidas por qualquer outro usuário dessa rede. Tais transmissões têm como limite o roteador da rede. Uma desvantagem do emprego de roteadores é o fato deles gastarem mais tempo para processar os dados do que, por exemplo, um *switch* (comutador de portas). Mais significativa ainda é a dependência de conexões físicas entre os dispositivos da rede para a formação dos domínios de *broadcast* em LANs, que são limitadas pelos roteadores. As VLANs surgiram da necessidade de uma maior flexibilidade nas redes de computadores atuais, por não possuírem limitações físicas, podendo ser organizadas de formas variadas. As redes virtuais oferecem meios flexíveis de segmentação de redes de computadores, sendo uma estratégia alternativa ao uso de roteadores. Uma VLAN, ou rede virtual, é um grupo de estações e servidores que se comunicam independente de sua localização física ou de topologia, como se fosse um único domínio de *broadcast*,

ou uma mesma rede lógica (MOLINARI, 2008), conforme mostra a Figura 2.1. A implantação de VLANs permite a criação de novos domínios de *broadcast*, possibilitando que usuários fisicamente distantes estejam conectados a uma mesma rede. As VLANs permitem que um mesmo grupo de usuários compartilhe a infraestrutura de uma rede local e cada pacote carregue uma identificação da rede virtual a qual pertence (PARSONS, 2007). Assim, o conceito de rede virtual se confunde com a ideia de "domínio de *broadcast*". Portanto, qualquer tecnologia utilizada para criar domínios de *broadcast* isolados pode ser considerada uma tecnologia para criação de redes virtuais (MOLINARI, 2008).

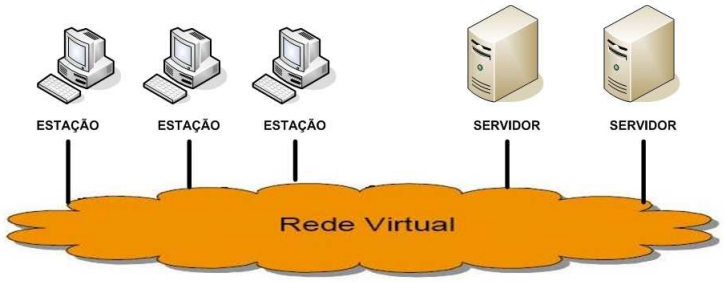

Figura 2.1: Rede Virtual.

É importante diferenciar os termos "domínio de colisão" e "domínio de *broadcast*". Um domínio de *broadcast* é uma área dentro de uma topologia de rede na qual a informação transmitida no domínio é recebida por todos os dispositivos dentro do mesmo domínio. Uma rede local é um domínio de *broadcast*, porque qualquer dispositivo conectado a essa rede pode transmitir quadros para qualquer outro dispositivo que esteja compartilhando a mídia de transmissão (CASTELLI, 2004). Já um domínio de colisão, refere-se a um segmento de rede *Ethernet*, *Fast Ethernet* ou *Gigabit Ethernet*, no qual fica contido o tráfego do grupo de estações desse segmento, assim como todas as colisões geradas por esse grupo (MOLINARI, 2008). Um *hub Ethernet* representa um único domínio de colisão; um *switch Ethernet* com 12 portas representa 12 domínios de colisão, mas ao mesmo tempo é um único domínio de *broadcast*, visto que os pacotes de *broadcast* podem

se propagar livremente para qualquer porta. É necessário um processo de nível 3 (Modelo OSI/ISO), como roteamento, ou filtros especiais para conter o tráfego dos pacotes de *broadcast*, criando-se, assim, domínios de *broadcast* separados, ou, em outras palavras, redes lógicas separadas, ou simplesmente redes virtuais separadas. Segundo (VELTE; VELTE, 2005), um domínio de *broadcast* é um ambiente em que todas as estações (dispositivos de rede e *hosts*) irão receber qualquer mensagem *broadcast* originária de qualquer dispositivo ou *host* dentro deste ambiente.

O uso de VLANs é coindicado, por exemplo, em empresas que obtiveram um crescimento muito rápido sem um projeto adequado para expansão da rede local. Com funcionários de diversos setores espalhados por uma grande área, uma solução possível para organizar os domínios seria a segmentação da rede interna em redes virtuais, uma para cada departamento. Outra aplicação interessante para VLANs é a criação de grupos de trabalhos desenvolvendo projetos durante um determinado tempo. Atualmente, é comum em empresas a realização de projetos envolvendo diferentes setores. Durante este período, a comunicação certamente se torna mais frequente e com maior troca de dados. Na intenção de conter o tráfego de *broadcast*, pode-se criar uma VLAN para este grupo de trabalho. Toda esta flexibilidade possibilitada pelo uso de VLANs é ideal para ambientes corporativos, em universidades e qualquer outro no qual sejam frequentes as trocas de funcionários, reestruturações internas, aumento no número de usuários, entre outras situações.

2.1 Segmentação de Redes de Computadores

Atualmente, profissionais que lidam frequentemente com redes de computadores se deparam com a necessidade de ampliação da rede, aumento do número de usuários ou da largura de banda disponível para atender a demanda requisitada. Alterações na infraestrutura física da rede não envolvem apenas substituições das interfaces de rede, mas também as substituições dos equipamentos pré-

existentes. Este tipo de atualização, ainda que bastante eficiente, pode tornar o projeto inviável devido aos seus custos elevados (CLARK; HAMILTON, 1999). Uma das principais tarefas em qualquer projeto de redes de computadores é reduzir todo o tráfego desnecessário, e isso pode ser conseguido limitando-se o alcance do tráfego (particularmente *broadcast*) apenas aos domínios para os quais ele é aplicável (KENYON, 2002). A segmentação é uma abordagem interessante para melhorar o desempenho da rede sem que haja a necessidade de substituir todos os seus equipamentos. Essa abordagem pode ser entendida como sendo o processo de divisão lógica de segmentos simples de *Ethernet* em múltiplos segmentos. Os *hubs* (repetidores), na verdade, não segmentam a rede e não gerenciam seus recursos. Eles simplesmente permitem ampliar a rede a uma certa distância. Os equipamentos mais apropriados para realizar tal reestruturação são *bridges* (pontes), *roteadores* e *switches*, conforme mostra a Tabela 2.1 (CLARK; HAMILTON, 1999). São várias as razões que tornam a segmentação de redes de computadores uma reorganização necessária. As principais são (MUELLER; OGLETREE, 2004):

- **Limitações topológicas:** quando é indispensável a inclusão de mais pontos em uma rede e, no entanto, existe impedimentos devido à limitação de distância ou o número de pontos por segmento já foi atingido.

- **Limitações no protocolo de rede:** quando é necessário agrupar dois ou mais segmentos de redes de endereços distintos em apenas um segmento.

- **Limitações na largura de banda da rede:** quando serviços de alto desempenho ou estações de trabalho consomem um grande volume de recursos da largura de banda do segmento.

- **Segurança:** quando se pretende limitar acessos externos à rede local e acessos internos à rede externa, ou até mesmo não permitir o acesso de determinadas estações de trabalho a outras do mesmo segmento.

- **Separação Geográfica:** quando se deseja impedir que o tráfego desnecessário não atinja uma conexão remota.

Tabela 2.1: Comparação entre Domínios de Colisão e de *Broadcast* criados por dispositivos de rede.

Dispositivos de Rede	Domínios de Colisão	Domínios de *Broadcast*
Hub	Um	Um
Bridge	Muitos	Um
Roteador	Muitos	Muitos
Switch	Muitos	Configurável

A localização do tráfego e a redução eficaz do número de estações de trabalho por segmento são medidas necessárias para evitar situações que reduzam o desempenho da rede, como colisões e *broadcasts*. Com a redução do número de *hosts* por segmento, a probabilidade de uma colisão decresce, porque menos estações podem transmitir em um determinado momento. Para a contenção de *broadcast*, a ideia é criar uma barreira na borda do segmento de rede de forma que tráfego *broadcast* não passe ou seja enviado (HUCABY, 2007). Os segmentos de uma LAN devem ser relativamente pequenos de forma a garantir a taxa de transmissão dos dados e limitar a frequência de colisões. Os segmentos menores são úteis quando se trata de flexibilidade, segurança e manutenção. Redes com um número cada vez maior de usuários estão gerando cada vez mais tráfego, com uma grande diversidade de tipos de dados. Esta combinação de fatores leva a uma maior necessidade de banda (VELTE; VELTE, 2005). A seguir são apresentadas algumas formas de expansão e segmentação de redes de computadores.

2.1.1 Uso de *Hubs* em redes de computadores

Os *hubs* são dispositivos de baixo custo e úteis quando a intenção é apenas estender a distância de um segmento de rede. Por serem equipamentos não inteligentes, não têm conhecimento dos dados que estão manipulando, retransmitindo os sinais de um segmento para todos os demais (CLARK; HAMILTON,

1999). Se um quadro enviado possui erros, ou viola o comprimento mínimo ou máximo de tamanho padrão, ainda assim o *hub* o repassa. Caso ocorra uma colisão em uma das portas (único segmento), ela ocorrerá em todas as outras portas do *hub*. Todas as estações conectadas ao *hub*, sem exceção, recebem todo o tráfego do segmento, seja ele útil ou desnecessário. Por isso, é preciso considerar algumas limitações dos *hubs* antes de utilizá-los para a ampliação de uma rede. De acordo com (CLARK; HAMILTON, 1999), algumas delas podem ser:

- **Compartilhamento de largura de banda entre dispositivos:** colisões em uma porta afetam estações em uma outra interface conectada ao *hub*. Outro efeito negativo do domínio de colisão é a propagação de *frames* (quadros) através da rede. Todas as estações enxergam todos os quadros. Ao adicionar mais estações à rede, a largura de banda disponível diminui e a possibilidade de colisão aumenta.

- **Número limitado de estações de trabalho:** toda a rede é formada por um único segmento compartilhado. Logo, a largura de banda disponível não cresce e deve ser compartilhada entre mais *hosts*, aumentando a possibilidade de saturação da rede.

- **Distância ponto-a-ponto:** uma outra limitação na ampliação de redes de computadores baseadas em *hubs* é a distância. Um segmento *Ethernet* pode se prolongar somente até não desrespeitar os padrões da mídia de transmissão. No caso de uma rede que utiliza cabos do tipo par trançado, o limite de comprimento é de 100 metros. Outra situação de não cumprimento das normas ocorre quando o tempo de contenção pelo meio é excedido.

Os *hubs* criam um único domínio de colisão e um único domínio de *broadcast* em toda a rede, conforme mostra a Figura 2.2.

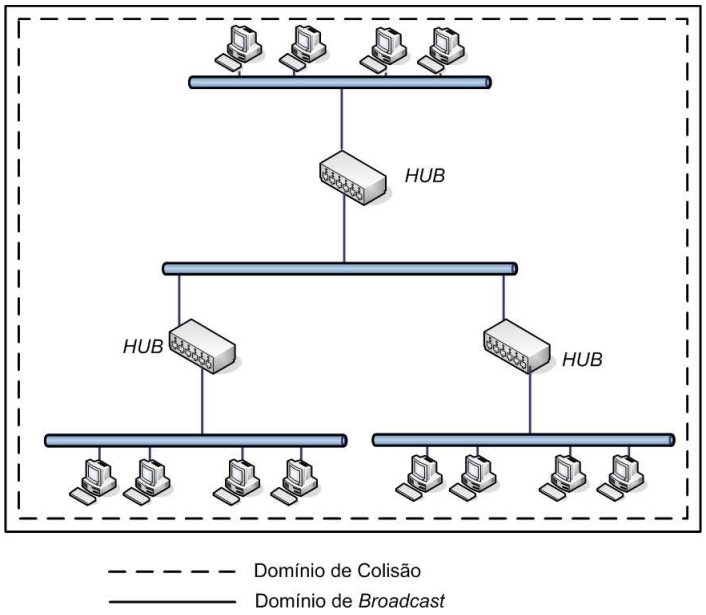

Figura 2.2: Domínios de Colisão e de *Broadcast* em uma Rede de Computadores com *Hubs*.

2.1.2 Segmentação de redes de computadores utilizando *Bridges*

Nas redes *Ethernet* a distância máxima de segmentos de rede e o número de estações conectadas são limitados. Sempre que dispositivos conectados em um mesmo segmento realizam alguma transmissão em uma rede baseada em *hubs*, os quadros aparecem em todos os outros segmentos da rede. No entanto, isto normalmente não acontece em uma rede com *bridges* (pontes) (CLARK; HAMILTON, 1999). Uma *bridge* é um dispositivo relativamente simples que consiste de pelo menos duas interfaces com *buffer* (memória). A *bridge* recebe um pacote em uma interface, o armazena no *buffer*, e, imediatamente o coloca na fila de transmissão para a outra interface. Os dispositivos interligados em barramento e conectados a uma das interfaces da *bridge* estão sujeitos a problemas de colisão (segmentos 1, 2 e 3, conforme mostra a Figura 2.3). Já os segmentos conectados às interfaces

da *bridge* não estão sujeitos a colisão. Eles estão em domínios de colisão separados. As *bridges* utilizam um processo de filtragem para determinar se um quadro será ou não encaminhado para outras interfaces (ODOM; NOTTINGHAM, 2000). Segundo (ODOM; NOTTINGHAM, 2000), uma *bridge* fornece basicamente três funções diferentes:

- Filtrar os quadros recebidos para determinar se ele deve ser transmitido.
- Encaminhar os quadros que devem ser enviados para a interface adequada.
- Reduzir atenuação e amplificar o sinal dos dados recebidos.

Todos os segmentos ligados à *bridge* pertencem ao mesmo domínio de *broadcast*.

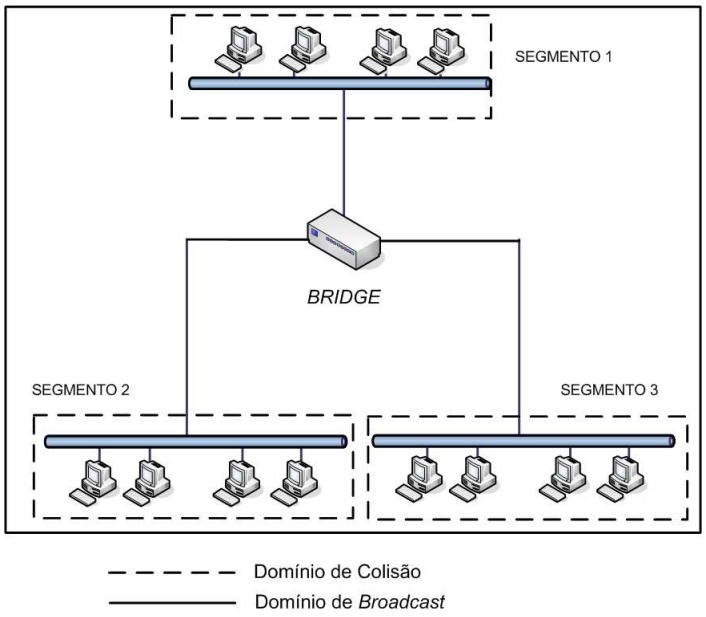

Figura 2.3: Domínios de Colisão e de *Broadcast* em uma Rede de Computadores com *Bridges*.

Outra vantagem das *bridges* é que elas impedem a transmissão de quadros com erros para outro segmento, já que são criados domínios de colisão isolados, conforme mostra a Figura 2.3. Se for detectado que um quadro possui erros ou tamanho que viola as regras de acesso ao meio, a *bridge* impede que este quadro prossiga na rede. Isso protege o segmento de rede destinatário de quadros com problemas, que nada mais fariam do que consumir largura de banda (CLARK; HAMILTON, 1999). No entanto, é importante entender que as *bridges* enviam o tráfego de *broadcast* em toda parte, e isto pode ser um sério problema que limita a escalabilidade de uma rede de computadores baseada em *bridge* (KENYON, 2002).

2.1.3 Segmentação de redes de computadores utilizando Roteadores

Os roteadores são dispositivos que operam na camada de rede (nível 3 do Modelo OSI/ISO), executam funções de transmitir informações, cálculo de rotas, filtragem entre múltiplos segmentos e conexão de mais de um segmento de rede com ou sem *bridges*. Roteadores, originalmente, foram introduzidos para conectar redes com tipos de mídias diferentes, e também para realizar encaminhamento de tráfego, filtrar transmissões de vários segmentos e melhorar o desempenho geral da rede. Na conexão de grandes redes ou para se conectar redes à WAN (*Wide Area Network*), os roteadores são muito utilizados. Eles realizam conversão de mídias, ajustando protocolos, quando necessário. A Figura 2.4 mostra um roteador conectando múltiplos segmentos de uma rede de computadores.

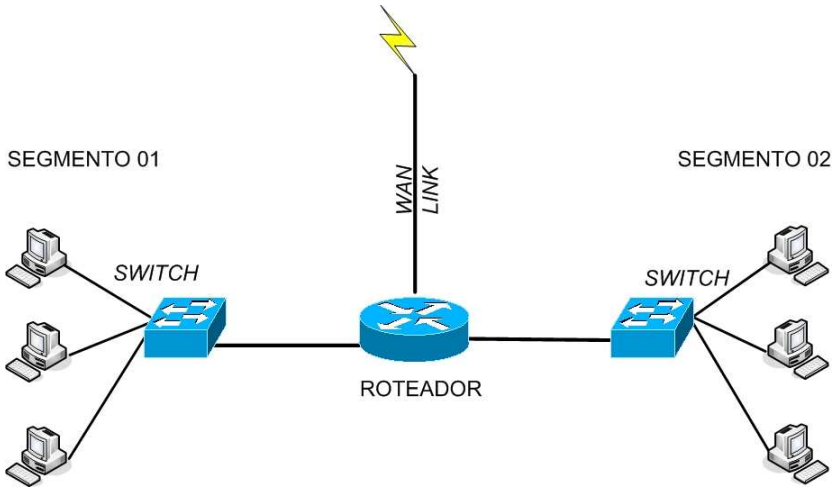

Figura 2.4: Roteador conectando múltiplos segmentos de uma rede de computadores.

Os roteadores têm algumas desvantagens. O custo dos equipamentos é alto em relação aos *switches*, logo são uma forma cara de segmentação de redes de computadores. A configuração é relativamente complexa, o que exige mais tempo e profissional especializado (ODOM; NOTTINGHAM, 2000). Os roteadores possuem capacidade de estender o diâmetro da rede, segmentar tanto domínios de colisão quanto domínios de *broadcast* e impedir que quadros de *broadcast* se propaguem pela rede. Conforme mostra a Figura 2.5, este isolamento de *broadcast* cria domínios de *broadcast* individuais, o que não é possível utilizando *bridges*. Com *hubs* ou *switches*, todas as estações de trabalho pertencem à mesma sub-rede, já que todas pertencem ao mesmo domínio de *broadcast*. No entanto, em redes baseadas em roteadores, são criados múltiplos domínios de *broadcast*, e desta forma cada segmento pertence a uma sub-rede diferente (CLARK; HAMILTON, 1999).

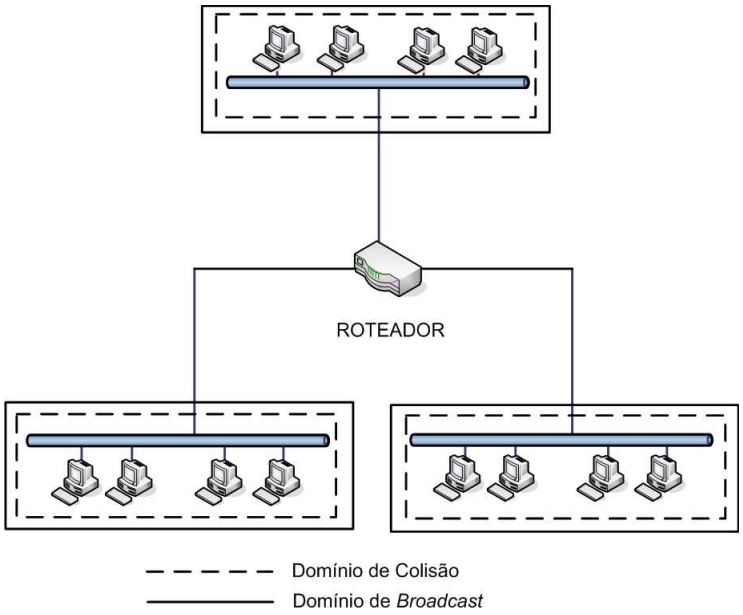

Figura 2.5: Domínios de Colisão e de *Broadcast* em uma Rede de Computadores com Roteador.

2.1.4 Segmentação de redes de computadores utilizando *Switches*

Segundo (FURUKAWA, 2004), o termo *switch* está relacionado aos dispositivos de alta velocidade de transmissão em redes de computadores, normalmente operando com comutação (ligação entre entrada e saída de um dispositivo com a largura de banda máxima dedicada). O *switch* é um dispositivo que gerencia e encaminha o tráfego através de suas portas. Cada porta é um canal de comunicação próprio, constituindo um domínio de colisão que pode receber uma única estação de trabalho, um *hub* ou outro *switch*. Ao fazer uso de *switches* para a interconexão de redes de computadores, surgem diferenças significativas quando comparadas às interconexões utilizando *hubs*. Um *switch* é uma *bridge* com múltiplas portas que permitem que muitas estações de trabalho conectadas diretamente a ele transmitam simultaneamente (CLARK; HAMILTON, 1999). Por exemplo, a Figura 2.6

mostra quatro estações de trabalho se comunicando ao mesmo tempo, algo impossível em um ambiente de rede compartilhada. Na Figura 2.6, o tráfego entre as estações 1 e 2 (sessão 01) é simultâneo ao tráfego entre as estações 3 e 4 (sessão 02).

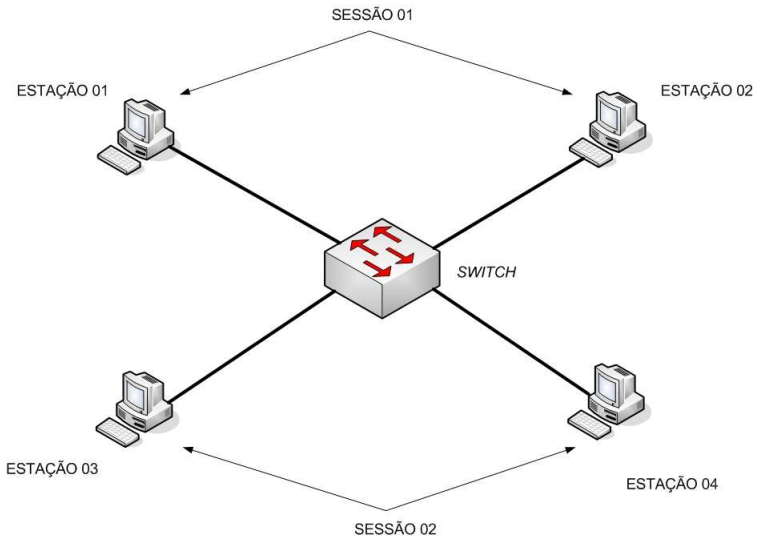

Figura 2.6: Várias sessões simultâneas através de um *switch*.

O *switch* é uma *bridge* mais complexa e com múltiplas interfaces, todas formando um único domínio de *broadcast*. Se a estação 01 envia um quadro de *broadcast*, todos os dispositivos conectados ao *switch* o recebem. Isto faz com que o *switch* não seja melhor do que *hubs* e *bridges* como forma de se conectar redes de computadores, quando se trata de quadros de *broadcast* ou *multicast*. No entanto, é possível projetar o *switch* para que suas portas possam pertencer a diferentes domínios de *broadcast* de acordo com a necessidade, criando, assim, isolamento de *broadcast*. Na Figura 2.7, algumas portas pertencem ao Domínio de *Broadcast* 1 (DB1), algumas ao Domínio de *Broadcast* 2 (DB2), e ainda outras pertencem ao Domínio de *Broadcast* 3 (DB3). Se uma estação conectada a uma interface no DB1 transmite um quadro de *broadcast*, o *switch* encaminha o *broadcast* somente para

as interfaces pertencentes ao mesmo domínio. Os outros domínios de *broadcast* não sofrem nenhum consumo de banda resultando do *broadcast* do DB1. Na verdade, é impossível para qualquer quadro atravessar de um domínio de *broadcast* para outro sem que o *switch* esteja configurado para permitir ou sem a introdução de outro dispositivo externo, como um roteador, para a interconexão dos domínios.

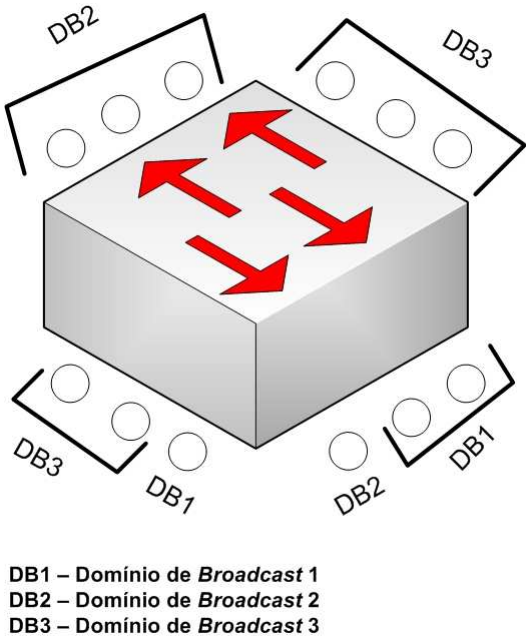

Figura 2.7: Múltiplos domínios de *broadcast* em um *switch* capaz de criar VLANs.

Os *switches* capazes de separar múltiplos domínios de *broadcast* definem as VLANs. Cada domínio de *broadcast* é uma VLAN. Um *switch* capaz de criar VLANs é um dispositivo que cria múltiplas *bridges* isoladas, como mostra a Figura 2.8. Se forem criadas três VLANs, passam a existir três *bridges* virtuais dentro do *switch*. Cada *bridge* virtual funciona isoladamente das demais.

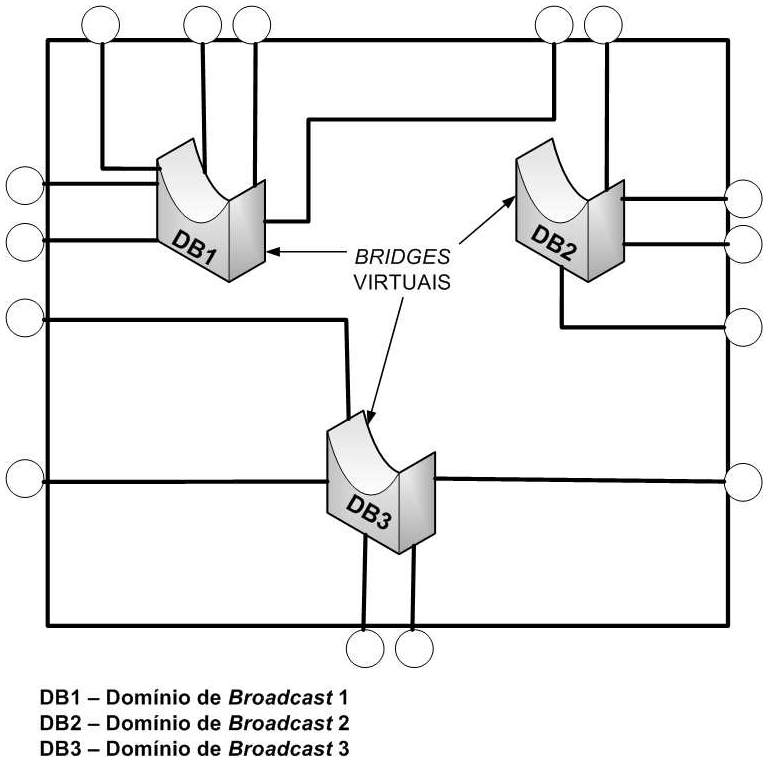

Figura 2.8: Representação interna lógica de um *switch* capaz de criar VLANs.

2.1.4.1 *Switches* Gerenciáveis e Não Gerenciáveis

Os *switches* não gerenciáveis são aqueles em que o administrador da rede não tem acesso a nenhum parâmetro ou estatística do equipamento. Não existe conexão local para configurar o equipamento e também não permite acesso pela própria rede. Já os *switches* gerenciáveis oferecem ao administrador de rede recursos para que esses controles sejam executados tanto localmente como remotamente por meio de interface WEB, SNMP (*Simple Network Management Protocol*) e *Telnet*. Normalmente, as redes são gerenciadas via SNMP, no qual o administrador utiliza programas de gerenciamento, baseados em interfaces gráficas, que apre-

sentam a topologia da rede com todas as suas interligações e permitem acessar cada *switch* e realizar a configuração de seus parâmetros de funcionamento (FURUKAWA, 2004).

2.1.4.2 *Switches* operando nas camadas 2 e 3

Segundo (ODOM; HEALY; MEHTA, 2008), *switching* (comutação) é o processo de capturar um quadro que chega de uma interface e entregá-lo direto para uma outra interface. Os roteadores utilizam *Layer 3 Switching* (operam na camada 3, ou seja, realizam roteamento) para determinar o caminho de um pacote, e os *switches* tradicionais utilizam *Layer 2 Switching* (operam na camada 2, ou seja, realizam encaminhamento) para transmitir os quadros. A diferença entre *Layer 2 Switching* e *Layer 3 Switching* é o tipo de informação contida no quadro que é usada para determinar a interface de saída correta. Com L*ayer 2 Switching*, os quadros são enviados com base no endereço MAC. Com *Layer 3 Switching*, os quadros são enviados com base em informação da camada de rede. *Layer 2 Switching* não enxerga as informações da camada de rede dentro do pacote. Ela verifica o endereço MAC de destino dentro do quadro e o envia para a interface apropriada. *Layer 2 Switching* constrói e mantém uma *switching table* (tabela de comutação) que realiza o controle de endereços MAC que pertencem a cada porta ou interface. *Layer 3 Switching* opera na camada de rede. Ela examina as informações dos pacotes e os transmite com base no endereço de destino da camada de rede. *Layer 3 Switching* também suporta funcionalidades de roteador.

2.1.5 Segmentação de redes de computadores utilizando Máscaras de Rede

O processo de subdividir faixas de endereços IP (*Internet Protocol*) em sub-redes utilizando máscaras de rede é denominado *subnetting* (sub-rede) (OSTERLOH, 2001). A *subnetting* permite a criação de redes lógicas diferentes através

de uma mesma rede física, ao contrário das VLANs que criam redes lógicas e físicas diferentes. Quando uma rede física é dividida em duas ou mais redes lógicas simplesmente são designadas redes IP diferentes, como 192.168.0.0/24, 192.168.1.0/24, e assim por diante. O problema é que mesmo criando-se redes diferentes todas elas usam o mesmo *backbone* (circuito de ligação principal), conforme ilustra a Figura 2.9. Os dados enviados trafegam através do *switch* e podem ser vistos por todos os outros *hosts*, mesmo que estejam em redes lógicas diferentes. O resultado é que a segurança é insignificante; dados confidenciais podem ser facilmente capturados; e haveria uma redução da largura de banda disponível, já que todos utilizam o mesmo *backbone*, acarretando um aumento do número de colisões (KUROSE; ROSS, 2007).

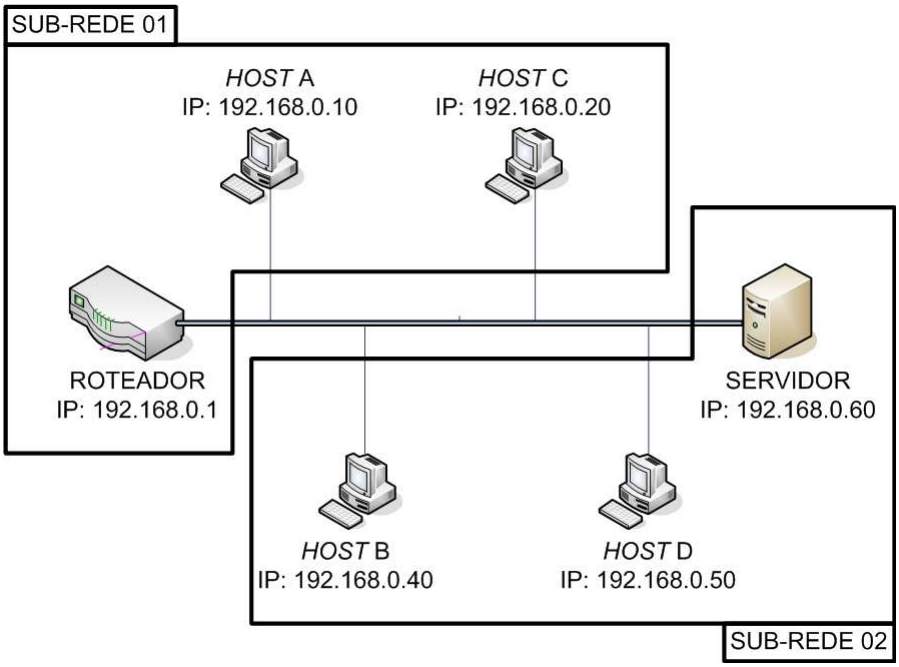

Figura 2.9: Criação de sub-redes utilizando máscaras de rede.

Então, com o intuito de amenizar os problemas das formas de segmentação de redes apresentados anteriormente, pode ser utilizada a segmentação através de VLANs. As *Virtual LANs* são descritas a seguir.

2.2 *Virtual Local Area Networks*

Instituições e organizações de médio e grande porte, geralmente, possuem muitas redes locais que devem suportar grande número de usuários e aplicações de rede. Cada usuário é conectado fisicamente a uma LAN; a característica dos dispositivos conectados a determinada LAN é definida pelas limitações dos dispositivos empregados (por exemplo, o número de portas do *switch*) e o tipo de conexões configuradas pelo administrador da rede. Uma vez que a rede de computadores está instalada e configurada, seu alcance é estabelecido. Alterar a configuração da rede local requer uma mudança nas conexões físicas. A conectividade lógica da LAN é igual a conectividade física (SEIFERT; EDWARDS, 2008). As LANs convencionais possuem limitações no que diz respeito a tamanho, distância e topologia física. O uso de *switches* para criar redes locais grandes resolve os problemas de domínios de *broadcast* e do número de dispositivos conectados à rede. Em um ambiente de rede de computadores moderno, existem outros fatores a serem considerados, como segurança, configuração e gerenciamento. Eventualmente, pode ser necessário conectar dispositivos em redes diferentes, embora eles estejam próximos e conectados ao mesmo *switch* da rede. As redes virtuais permitem o isolamento da topologia física e lógica. Assim, é possível se ter todos os dispositivos interconectados, usando um ou vários *switches* devidamente configurados, independente da topologia física (MUELLER; OGLETREE, 2004). A tecnologia de *Virtual LAN* (VLAN) permite a separação da conectividade lógica da conectividade física. Os usuários ainda estão conectados fisicamente, mas em relação a conectividade lógica da estação ou aplicação não há limites ou restrições quanto a topologia de rede adotada. Isto é, o conjunto de aplicações ou estações que podem se comunicar diretamente em uma LAN por meio de um *switch* de-

vidamente configurado. A rede local é virtual no sentido em que o conjunto de estações ou aplicações podem se comportar como se elas estivessem conectadas fisicamente a mesma LAN, mesmo que de fato elas não estejam (SEIFERT; EDWARDS, 2008). Para atingir esta flexibilidade, devem ser utilizados *switches* ao invés de *hubs* e *bridges* para a interconexão dos dispositivos. Além disso, os *switches* precisam suportar a criação de VLANs e são chamados de dispositivos *VLAN-aware*.

2.2.1 O padrão IEEE 802.1Q

O padrão que determina a forma de implementação das VLANs, IEEE 802.1Q, foi publicado em 1998. O esquema utilizado na identificação resulta em quatro novos *bytes* de informação sendo adicionados ao quadro entre os campos de endereço de origem e de tamanho/tipo. Isso aumenta o tamanho do quadro para 1522 *bytes* (caso o quadro esteja transportando 1500 *bytes* de dados) (SPURGEON, 2000). A Figura 2.10 mostra o que acontece quando a identificação de VLAN é adicionada ao quadro *Ethernet*. Com exceção do campo de tamanho/tipo, que aumenta em quatro *bytes*, os outros campos originais do quadro não sofrem alterações.

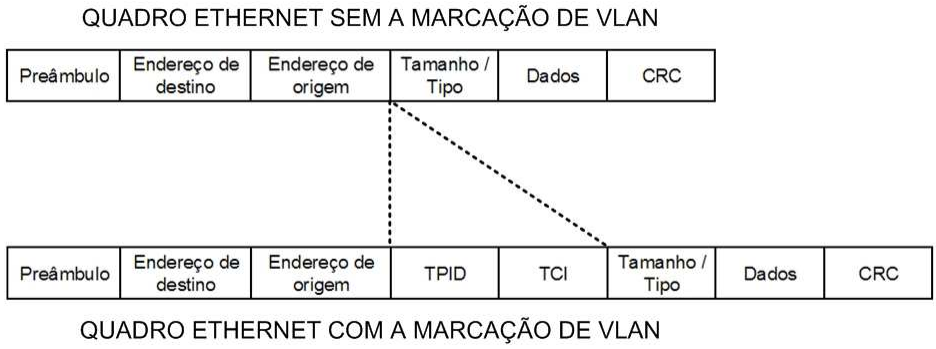

Figura 2.10: Quadros *Ethernet* sem e com marcação de VLAN.

Após ampla análise, engenheiros determinaram que todas as interfaces *Ethernet* poderiam acomodar quatro *bytes* extras de informação sem qualquer problema. A mudança no tamanho máximo do quadro foi especificada no suplemento IEEE 802.3ac, e adotada como parte do padrão *Ethernet* em 1998. A *Tag Protocol Identifier* (TPID) é um campo de dois *bytes* que identifica o quadro como um *frame tagged* (quadro identificado). Os próximos dois *bytes* contêm a *Tag Control Information* (TCI). Três *bits* desse campo são usados para transportar a informação de prioridade baseada nos valores definidos no padrão IEEE 802.1p. Portanto, o padrão 802.1Q estende a prioridade ao tratar aspectos do padrão 802.1p na *VLAN tag* (identificador de VLAN) para indicar a prioridade do tráfego. Isso permite que a informação de prioridade do tráfego seja enviada entre *switches* usando o protocolo VLAN. A TCI também transporta o *VLAN Identifier* (VID), que é um campo que identifica unicamente a VLAN a qual o quadro pertence (SPURGEON, 2000). O padrão IEEE 802.1Q também pode realizar associações de VLANs utilizando *Trunk Link* (Enlace Tronco). Ele permite que *switches*, roteadores e quaisquer outros dispositivos de rede enviem tráfego por múltiplas VLANs através de um único *link* (ODOM; HEALY; MEHTA, 2008). No entanto, esse método de identificação de quadro é padronizado, permitindo que *VLAN trunks* (troncos de VLAN) existam e operem em equipamentos de diferentes fabricantes. Em particular, o padrão 802.1Q define uma arquitetura para a implementação de VLANs, os serviços prestados, os protocolos e algoritmos utilizados (HUCABY, 2007).

2.2.2 Visão geral sobre VLANs

Tecnicamente, VLANs definem domínios de *broadcast* na camada de enlace. Redes legadas utilizam interfaces de roteador para definir os limites de domínios de *broadcast*. O comportamento característico dos roteadores previne que mensagens em *broadcast* se propaguem através de suas interfaces. Por consequência, roteadores automaticamente criam domínios de *broadcast*. Os *switches* nível 2, por outro lado, criam domínios de *broadcast* baseados na sua própria configura-

ção. Se um *switch* recebe tráfego em *broadcast* em uma porta, todas as outras o receberão (CLARK; HAMILTON, 1999).

2.2.3 Tipos de VLAN

As VLANs podem ser classificadas de acordo com a forma de agrupamento de seus elementos (ZHU; MOLLE; BRAHMAN, 2004). Destacam-se cinco tipos de agrupamento: portas, endereço MAC, protocolo, endereço IP, camadas superiores, como descritos a seguir.

- **Portas -** na Camada Física, os integrantes da rede virtual podem ser identificados de acordo com a porta do *switch* utilizada, conforme indica a Figura 2.11. É um método bastante utilizado devido a sua configuração simples e rápida. A principal desvantagem ocorre no caso de mudança física do usuário. Se for necessária a mudança na porta do *switch*, o administrador deve reconfigurar a 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

Figura 2.11: Associação de portas de um *switch* a diferentes VLANs.

- **Endereço MAC (*Media Access Control) -*** 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 2.12, o *switch* reconhece o MAC vinculado a cada rede virtual. Quando uma estação de trabalho sofre alteração na localização física, não é necessária qualquer mudança na configuração, já que o MAC faz parte da interface de rede. Uma desvantagem é que cada membro da VLAN deve ser inicialmente especificado, sem exceções. Em uma rede

com um grande número de dispositivos, esta identificação inicial torna-se um trabalho bastante custoso.

Endereço MAC	00-15-F2-C3-12-3D	1A-00-3F-11-B1-D4	00-53-D2-11-00-00	F2-00-3D-12-C3-B2
VLAN	0	1	1	0

Figura 2.12: Associação de Endereços MAC das interfaces de rede a diferentes VLANs.

- **Protocolo -** as estações de trabalho são identificadas de acordo com o tipo protocolo de rede ao qual obedecem, segundo exemplo da Figura 2.13.

Protocolo	IP	IPX	NetBios
VLAN	0	0	1

Figura 2.13: Associação de protocolos a diferentes VLANs.

- **Endereço IP -** na Camada de Rede, é utilizado o endereço IP. Embora a identificação ocorra na camada de rede, o processo não é realizado pelo roteador. Na Figura 2.14, o endereço IP é usado apenas para realizar um mapeamento dos usuários da VLAN.

Endereço IP	192.168.40.20	192.168.40.30	192.168.40.40	192.168.40.50
VLAN	1	0	1	0

Figura 2.14: Associação de Endereços IP a diferentes VLANs.

- **Camadas Superiores -** nas Camadas de Transporte e de Aplicação é possível a identificação dos membros da VLAN baseada nas aplicações e nos serviços, ou mesmo uma junção destes. Por exemplo, aplicações *File Transfer Protocol* (FTP) podem ser realizadas em uma rede virtual e aplicações *Telnet* em uma outra.

Segundo (COMER, 2007), VPN (*Virtual Private Network*) ou Rede Privada Virtual, é uma tecnologia que permite que uma companhia com múltiplas localizações tenha uma rede privada, mas use uma rede pública como uma portadora, conforme mostra a Figura 2.15. Em particular, embora a empresa possa usar a rede pública como um *link* entre seus centros, a tecnologia VPN restringe o tráfego de forma que os pacotes possam circular somente entre os centros da empresa. Além disso, mesmo que um estranho receba uma cópia de um pacote, o uso da tecnologia VPN permite que ele não entenda o seu conteúdo.

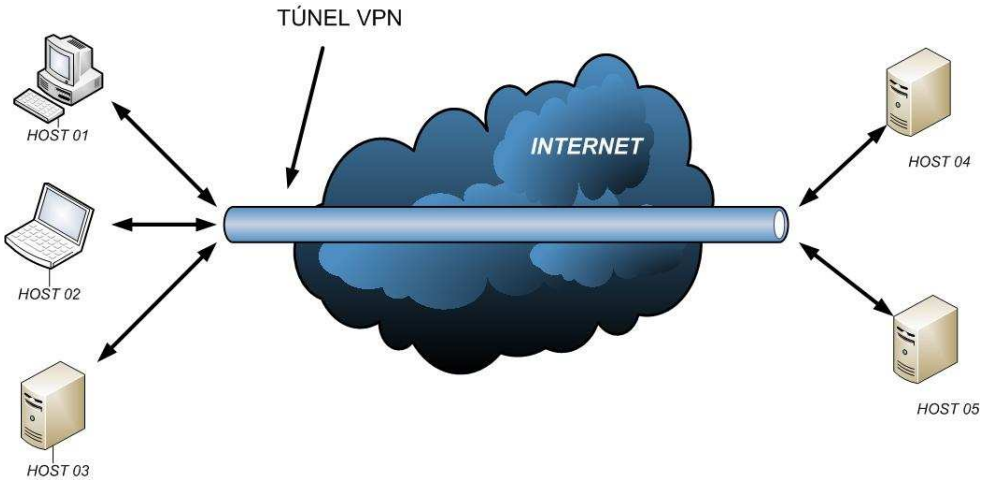

Figura 2.15: Redes privadas conectadas por um túnel VPN.

O uso de redes locais virtuais oferece muitas vantagens: controle de tráfego de *broadcast*, segmentação lógica da rede, redução de custos e facilidade de gerenciamento, independência da topologia física e maior segurança. Tais benefícios serão descritos a seguir.

2.3 Benefícios do uso de VLANs

Os benefícios de implantação de VLANs são inúmeros, dentre eles, destacam-se:

- **Controle de tráfego de *broadcast* -** em redes onde o tráfego *broadcast* é responsável por grande parte do tráfego total, as VLANs reduzem o envio de pacotes para endereços desnecessários, aumentando a capacidade de toda a rede.

- **Segmentação lógica da rede -** cada VLAN pode ser associada a um departamento ou grupo de trabalho, mesmo que seus membros estejam fisicamente distantes. Isto proporciona uma segmentação lógica da rede.

- **Redução de custos e facilidade de gerenciamento -** em uma VLAN, a adição e movimentação de usuários podem ser feitas remotamente pelo administrador da rede, sem a necessidade de modificações físicas, proporcionando uma alta flexibilidade.

- **Independência da topologia física -** VLANs proporcionam independência da topologia física da rede, permitindo que grupos de trabalho, fisicamente isolados, possam ser conectados logicamente a um único domínio *broadcast*.

- **Maior segurança -** o tráfego em uma VLAN não pode ser "escutado"por membros de outra rede virtual, já que estas não se comunicam sem que haja um dispositivo de rede desempenhando a função de roteador entre elas.

Os dispositivos conectados a uma VLAN também recebem uma classificação que será detalhada a seguir.

2.4 Tipos de conexão de dispositivos em VLANs

Os dispositivos em uma rede local virtual podem ser conectados de três maneiras diferentes, considerando se estes suportam ou não o padrão IEEE 802.1Q (IEEE SOCIETY COMPUTER, 2006). São elas:

- **Enlace Tronco (*Trunk Link*) -** todos os dispositivos ligados à rede virtual através deste tipo de enlace devem reconhecer quadros com a identificação de VLAN e poder inserir e remover informação no cabeçalho da *tag*, ou seja, ser *VLAN-aware*.
- **Enlace de Acesso (*Access Link*) -** este tipo de enlace conecta um dispositivo sem suporte a VLAN a uma porta *VLAN-aware*.
- **Enlace Híbrido (*Hybrid Link*) -** é uma união dos Enlaces Tronco e de Acesso. Nos enlaces híbridos são conectados tanto dispositivos *VLAN-aware* quanto dispositivos *VLAN-unaware* (não reconhece quadros com *VLAN tag*, isto é, não possuem suporte ao padrão IEEE 802.1Q).

Uma VLAN pode possuir simultaneamente os três tipos de enlaces citados anteriormente. Considerando as classificações de VLANs e os dispositivos que podem ser conectados a elas, torna-se possível propor uma solução para segmentação de redes de computadores. A seguir, será apresentada a solução chamada de *VLAN Trunking Protocol*.

2.5 Solução VTP (*VLAN Trunking Protocol*)

O VTP é um protocolo criado pela *Cisco Systems*, usado pelos switches para comunicação uns com os outros e troca de informações sobre as configurações da VLAN. Quando uma VLAN é configurada em um servidor VTP, essa configuração

é distribuída a todos os *switches* do domínio. Isso reduz a necessidade de aplicar a mesma configuração em vários lugares (CISCO SYSTEMS, 2002). É possível configurar um *switch* para operar em um dos seguintes modos de VTP:

- **Servidor VTP -** permite criar, modificar e deletar VLANs e especificar outros parâmetros de configuração tais como a versão do VTP e retirar configurações desnecessárias.
- **Cliente VTP -** se comporta da mesma maneira do Servidor VTP, porém não pode criar, modificar ou deletar VLANs.
- **VTP transparente -** *switches* transparentes não participam. Um *switch* transparente de VTP não é informado sobre a configuração da VLAN e não realiza a sincronização da configuração baseada nas informações recebidas. No entanto, ele repassa a configuração para fora da sua porta de *Trunking*.
- **VTP desligado -** nos três modos descritos anteriormente, as informações são recebidas e transmitidas logo que o *switch* entra em modo de gerenciamento. No modo VTP desligado, os *switches* se comportam da mesma forma que no modo VTP transparente, porém as informações recebidas não são transmitidas.

O VTP divulga as informações de configuração de VLAN aos *switches* vizinhos para que a configuração possa ser feita em cada um, com todos os outros *switches* na rede aprendendo a informação de VLAN dinamicamente. O VTP anuncia o VLAN ID, o nome e o tipo da VLAN para cada VLAN. Contudo, o VTP não divulga qualquer informação sobre em quais portas (interfaces) deveria estar cada VLAN, então a configuração para associar uma interface do *switch* a uma VLAN em particular ainda deve ser feita em cada *switch* individualmente. A Tabela 2.2 mostra, resumidamente, os modos de operação e características do VTP (ODOM; HEALY; MEHTA, 2008).

e

Tabela 2.2: 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

Na Figura 2.16, cada *switch* trabalha com duas VLANs. No primeiro *switch*, a VLAN A e a VLAN B passam através de uma única porta para o roteador e através de outra porta para o segundo *switch*. A VLAN C e a VLAN D utilizam *Trunking* do segundo para o primeiro *switch* e do primeiro *switch* para o roteador. Este processo de *Trunking* pode carregar tráfego de todas as quatro VLANs. O *link* de *Trunking* do primeiro *switch* para o roteador também pode carregar dados das quatro VLANs. Na verdade, esta conexão do roteador permite que este mesmo roteador apareça em todas as quatro VLANs, como se existissem quatro portas físicas diferentes conectadas ao *switch*.

As VLANs podem estabelecer comunicação entre si por meio da conexão *Trunking* entre os dois *switches* utilizando o roteador. Por exemplo, dados do computador na VLAN A que precisam ser transmitidos a um computador na VLAN B (ou VLAN C ou VLAN D) devem trafegar do *switch* para o roteador e novamente para o *switch*. Devido ao aprendizado 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, proporcionando

um aumento da largura de banda sem a necessidade de mudança de tecnologia do *backbone* (FURUKAWA, 2004).

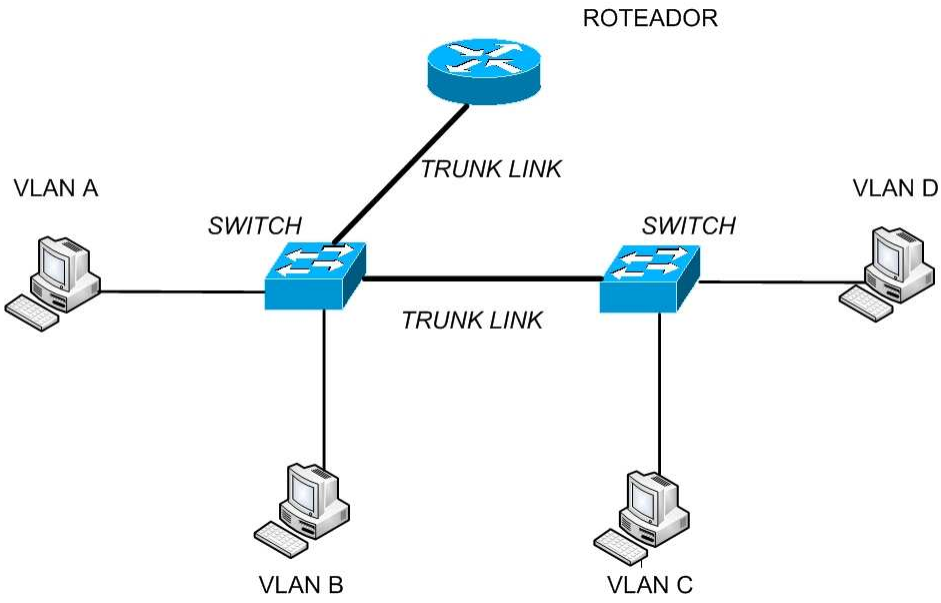

Figura 2.16: VLAN com uso de Trunking.

2.5.1 O Processo VTP e Números de Revisão

O número de revisão é um dos mais importantes componentes de um anúncio VTP. Todas as vezes em que um *switch* no modo VTP Servidor adiciona, deleta ou modifica a configuração de uma VLAN ele incrementa o número de revisão em uma unidade. O maior número de revisão dentro de um domínio VTP carrega a informação mais atualizada. Quando um *switch* em modo VTP Cliente recebe um número de revisão superior ao dele, deve atualizar sua configuração de VLAN sobrescrevendo suas informações com o banco de dados VTP do número de revisão mais alto. O processo de atualização começa quando um administrador de um *switch* no modo VTP Servidor modifica a configuração de uma VLAN. Quando

a nova configuração ocorre, o VTP Servidor incrementa o número de revisão e o anuncia junto com toda a configuração da VLAN. A Figura 2.17 mostra um exemplo de anúncio VTP com os seguintes passos: 1 – uma nova VLAN é adicionada; 2 - número de revisão antigo era 3 e é atualizado para 4; 3 – o VTP Servidor realiza o anúncio e propaga o banco de dados VTP para os outros *switches*; 4 – os VTP 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).

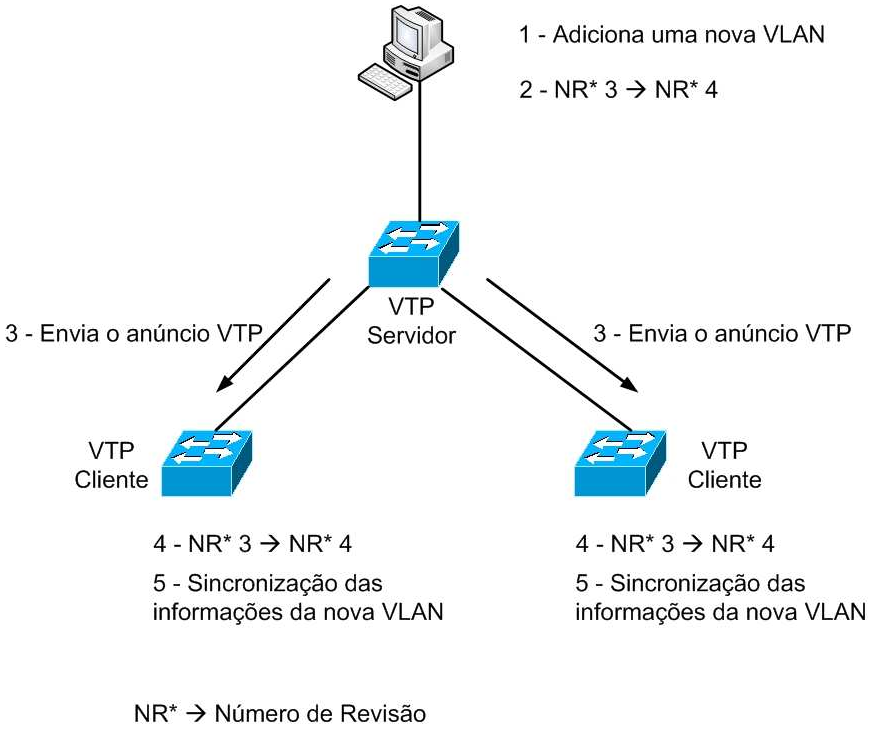

Figura 2.17: Processo VTP e Número de Revisão.

No próximo capítulo serão apresentados detalhes da metodologia adotada para a realização deste trabalho, assim como informações sobre o processo de simulação e sobre a análise dos resultados obtidos.

Capítulo 3

METODOLOGIA

Este capítulo descreve a metodologia utilizada no trabalho que permitiu que os objetivos da pesquisa fossem alcançados. Na primeira seção desse capítulo, será apresentada a classificação da pesquisa quanto à natureza, ao objetivo e aos procedimentos. Em seguida serão descritos os procedimentos metodológicos da pesquisa.

3.1 Tipo de pesquisa

Quanto à natureza da pesquisa, ela pode ser classificada como básica ou fundamental, pois tem como finalidade entender ou descobrir novos fenômenos. Baseando-se no objetivo geral da pesquisa do projeto, ela pode ser considerada como pesquisa descritiva, já que visa observar, registrar e analisar os fenômenos registrados em simulações na ferramenta *OPNET IT Guru Academic Edition*. Quanto aos procedimentos, a pesquisa é considerada experimental e em laboratório. Entende-se por uma pesquisa em laboratório aquela que permite o controle das variáveis que possam interferir no experimento (ZAMBALDE; PADUA; ALVES, 2008). A aquisição de referências foi realizada por meio de procedimentos de

pesquisa bibliográfica e documental. Esse tipo de pesquisa é desenvolvido a partir de livros e artigos científicos e de material já elaborado, existente na organização (GIL, 1991).

3.2 Procedimentos metodológicos

A pesquisa possui, basicamente, duas etapas. A primeira delas é a aquisição dos requisitos essenciais para o desenvolvimento e a evolução do trabalho. Nessa etapa ocorreu a definição do assunto abordado, a pesquisa bibliográfica e análise da documentação disponível encontrada, permitindo a obtenção de conhecimentos sobre segmentação de virtual de redes de computadores (suas características e possíveis formas de realização) e sobre o padrão IEEE 802.1Q. A segunda etapa é a implementação e avaliação dos resultados obtidos a partir da criação de cenários no simulador de redes de computadores *OPNET IT Guru Academic Edition*. A partir dos resultados das simulações realizadas, geração e análise de diversos gráficos, obedecendo a algumas métricas que serão descritas posteriormente.

3.3 O processo de simulação

A simulação tem como objetivo imitar uma situação do mundo real e, com base no modelo criado, realizar experimentos e testes com a finalidade de entender e avaliar o comportamento de determinado sistema (ALBERTI; NETO; MENDES, 1999). Existem três tipos principais de *softwares* de simulação para de redes de comunicação: linguagens de simulação de propósito geral, linguagens de simulação orientadas às redes de comunicações e simuladores orientados às redes de comunicações (LAW; MCCOMAS, 1994). Uma linguagem de simulação de propósito geral é um conjunto de simulação que, teoricamente, pode ser usado para qualquer tipo de sistema. No entanto, algumas dessas linguagens possuem características especiais para redes de comunicação, como módulos para *Ethernet*, redes sem fio

e outras. São exemplos dessas linguagens de simulação: Arena (HAMMANN; MARKOVITCH, 1995) e BONeS DESIGNER (COMDISCO SYSTEMS, INC., 1993). As linguagens de simulação orientadas às redes de comunicação têm como benefício a possibilidade da redução do tempo de programação e modelagem das construções voltas para as redes de comunicação. Como exemplos desse tipo de *software*, destacam-se o OPNET Modeler (SVENSSON; POPESCU, 2003) e GNS3 (GNS3, 2009). Os simuladores orientados às redes de comunicação são *softwares* que permitem a simulação de uma classe específica de redes de comunicação. Dentre as vantagens que esse tipo de simulador possui estão a facilidade de uso e a possibilidade de reduzir o tempo e a complexidade na criação dos modelos. São exemplos desse tipo de simulador: NIST (GOLMIE; KOENIG, 1995) e QUARTS-II (SIVABALAN; MOUFTAH, 1998).

3.4 Modelagem de redes de computadores

A modelagem é o processo de criação de modelos de sistemas reais para um ambiente de simulação específico, de forma que esses modelos representem, da maneira mais fiel possível, o comportamento desses sistemas diante de determinadas situações. Dentro de um contexto característico, por exemplo, a segmentação virtual de redes de computadores utilizando VLANs, a modelagem é uma tarefa que exige não apenas conhecimento do ambiente de simulação para o qual os modelos estão sendo desenvolvidos, mas também conhecimento teórico de VLANs, de detalhes dos componentes a serem modelados e de resultados a serem obtidos. Um fator importante a ser considerado quando se desenvolve modelos para ambientes de simulação é a distinção entre emulação e simulação. A emulação tem como propósito imitar a rede representando totalmente os detalhes envolvidos. Já a simulação visa obter resultados estatísticos que descrevam a operação dessas redes de computadores. Dessa forma, na simulação não é necessária a representação de todas as funcionalidades envolvidas, mas apenas aquelas, cujos

detalhes são importantes de acordo com as estatísticas de interesse (ALBERTI; NETO; MENDES, 1999).

3.5 A ferramenta de simulação *OPNET IT Modeler*

O *OPNET Modeler*, desenvolvida pela *OPNET Technologies Inc.*, é uma ferramenta de simulação que proporciona um ambiente virtual para modelagem, análise e prognóstico de desempenho de infraestruturas de TI, incluindo aplicações, servidores e tecnologias de redes de computadores. É um *software* utilizado por milhares de organizações, governos e universidades em todo o mundo. O OPNET é uma ferramenta com interface amigável e que oferece recursos gráficos e permite a criação de cenários de simulação de redes, nós, enlaces, sub-redes, protocolos, equipamentos e serviços (SVENSSON; POPESCU, 2003). A versão *OPNET IT Guru Academic Edition 9.1.A (Build 1998)*, destinada a fins acadêmicos, foi escolhida para a criação dos cenários, simulação e análise de resultados. A escolha deste simulador deve-se ao seu conjunto de ferramentas com os requisitos necessários para este trabalho, além de não exigir máquina com alto poder de processamento. A Figura 3.1 mostra a tela inicial do simulador OPNET.

Figura 3.1: Tela inicial do *software OPNET IT Guru Academic Edition*.

3.6 Escolha das Topologias

Muitas empresas, organizações e universidades têm um número significativo de computadores e dispositivos de rede. O modelo cliente/servidor é amplamente utilizado nas aplicações e serviços de rede e constitui a base de grande utilização das redes. Sendo assim, foi definido que os cenários seriam criados utilizando a ideia do modelo cliente/servidor (TANENBAUM, 2003). A Figura 3.2 ilustra uma rede local que se baseia no modelo cliente/servidor.

Os cenários construídos no OPNET têm por objetivo representar da maneira mais homogênea possível as situações nas quais as redes de computadores são projetadas, expandidas e utilizadas. Neste trabalho quatro tipos diferentes de modelos foram desenvolvidos, testados e analisados. Diferentes níveis de complexidade foram explorados em cada um dos cenários, desde uma rede com apenas um *switch* até cenários com algumas sub-redes utilizando vários *switches* e roteadores. Os modelos foram baseados em rede que utilizam ou não VLANs. Esses mode-

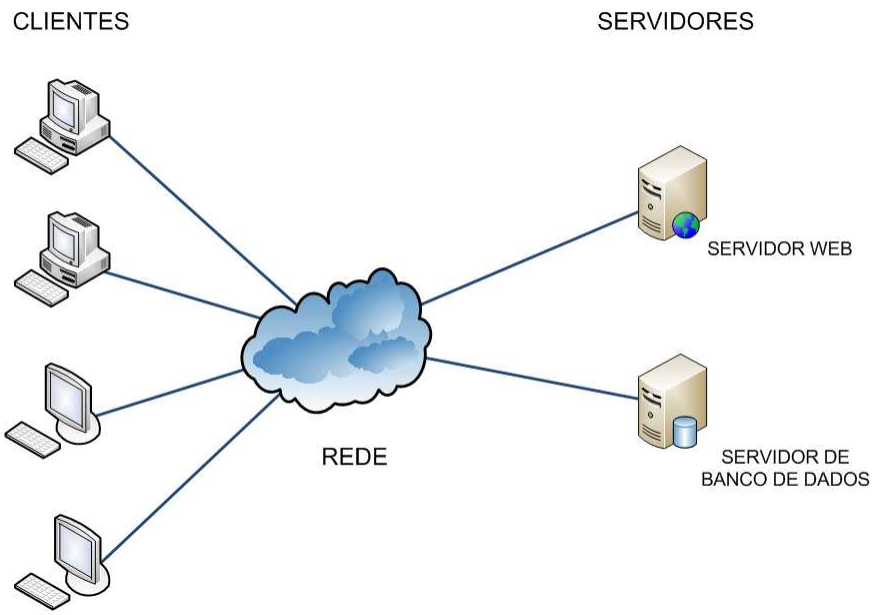

Figura 3.2: Rede de computadores utilizando o modelo cliente/servidor.

los foram comparados aos métodos tradicionais: segmentação por porta usando *switches* e segmentação por mascaramento de rede.

3.7 Definição das métricas e das aplicações

As métricas adotadas na coleta de dados das simulações, para comparação em redes locais sem e com segmentação virtual, foram as seguintes:

- Tráfego Recebido nos *switches* (pacotes/segundo)
- Tráfego Encaminhado nos *switches* (pacotes/segundo)
- *Throughput* entre roteador e *switch* (pacotes/segundo)

- Carga nos servidores (pacotes/segundo)

Cada uma das aplicações utilizadas durante as simulações podem ser configuradas em três níveis diferentes de carga de trabalho: *Low Load* (Carga Baixa), *Medium Load* (Carga Média) e *High Load* (Carga Alta). As possíveis aplicações que podem ser utilizadas no software de simulação adotado nesse trabalho são:

- Bando de Dados.
- E-mail.
- FTP.
- HTTP.
- Impressão.
- Acesso Remoto.
- Vídeo Conferência.
- Voz.

3.8 Análises dos resultados

Os resultados alcançados durante as simulações dos cenários no software *OPNET IT Guru Academic Edition* receberam uma análise comparativa com base nos modelos de redes de computadores que utilizam ou não a segmentação por VLANs. No próximo capítulo serão apresentados detalhes da modelagem dos cenários utilizados nos experimentos deste trabalho.

Capítulo 4

MODELOS DE SEGMENTAÇÃO EM REDES DE COMPUTADORES

Este capítulo apresenta a realização da modelagem dos cenários nos quais foram realizadas as simulações, sem nenhum tipo de segmentação virtual e com a utilização de VLANs.

4.1 Fluxo de trabalho do *OPNET Modeler*

A construção de modelos de redes de computadores no simulador OPNET segue, basicamente, um determinado fluxo de trabalho, conforme ilustra a Figura 4.1 (SVENSSON; POPESCU, 2003).

Inicialmente, são necessárias as informações referentes ao tráfego que será gerado pelos usuários e a topologia da rede a ser simulada. Cada uma das etapas é descrita a seguir.

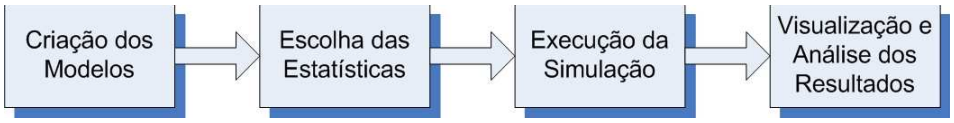

Figura 4.1: Fluxo de trabalho básico para construção de modelos no OPNET.

4.2 Criação dos Modelos

Os primeiros passos para qualquer simulação no OPNET são: a criação de um novo projeto, nomeação do projeto e do primeiro cenário, escolha da topologia inicial (um cenário vazio ou importação de um pré-existente), definição da escala da rede e especificação do tamanho do cenário, seleção das tecnologias que serão utilizadas no modelo e logo depois confirmar o resumo das especificações escolhidas para o modelo. No presente projeto, as especificações básicas definidas para todos os cenários foram:

- Nome do projeto: vlan-wykret
- Nome dos cenários: no-vlan-01, vlan-01, no-vlan-02, vlan-02, no-vlan-03, vlan-03, no-vlan-04, vlan-04
- Topologia inicial: Empty Scenario (Cenário Vazio)
- Escala da rede: *Office* (Escritório)
- Tamanho do cenário: 300 m x 300 m
- Tecnologias selecionadas: *applications* (aplicações), Cisco, *client-server* (cliente-servidor), *ethernet-advanced* (ethernet avançada), LANs, *links-advanced* (enlaces avançados), *routers-advanced* (roteadores avançados), VLANs
- Tempo simulado por cenário: 60 minutos

Após a definição das especificações citadas anteriormente, o simulador OPNET está pronto para que a rede de computadores seja modelada. A Figura 4.2 mostra o ambiente onde deve ser feita a modelagem da rede.

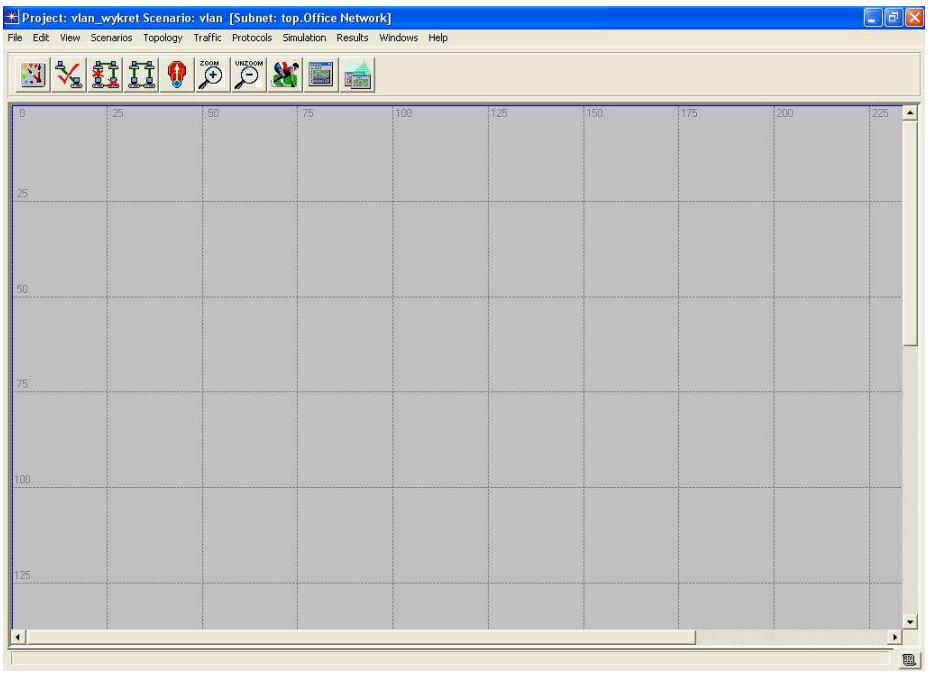

Figura 4.2: Ambiente do OPNET para modelagem do cenário.

Com o ambiente preparado, o próximo passo é abrir a Object Palette (Paleta de Objetos). A Object Palette contém todos os dispositivos pertencentes às tecnologias selecionadas no início do processo de criação do projeto. Na Figura 4.3 é possível verificar duas formas de abrir a Object Palette (no botão marcado com um ícone circulado e através do barra de menus – Topology $\rightarrow$ $OpenObjectPalette$).

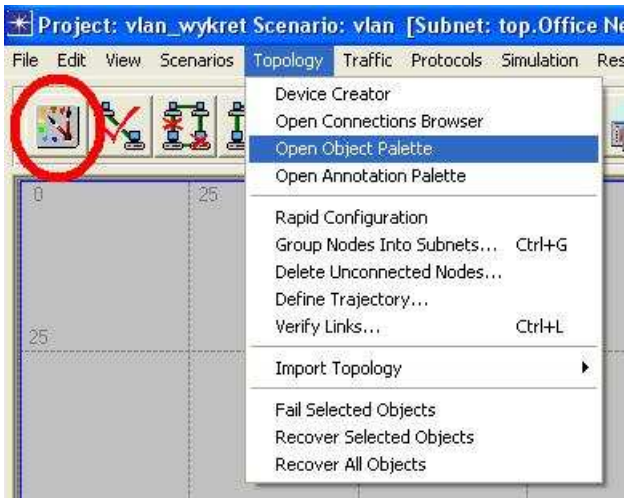

Figura 4.3: Formas de abrir a *Object Palette* do simulador OPNET.

A Figura 4.4 mostra a Object Palette e alguns de seus objetos.

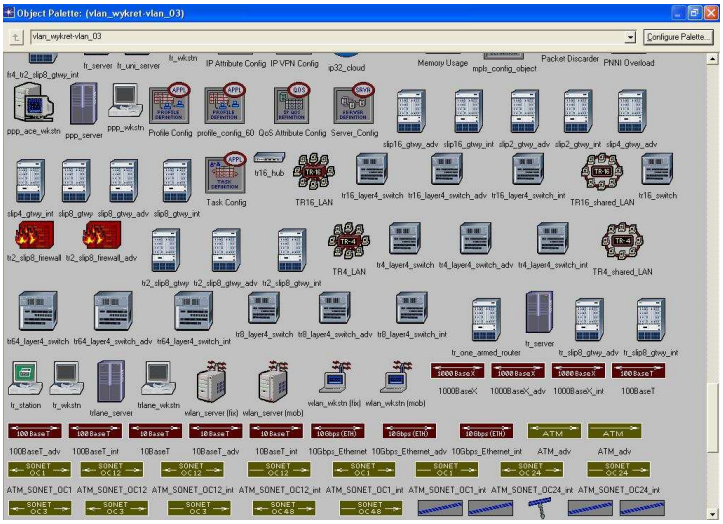

Figura 4.4: A *Object Palette* e alguns de seus objetos.

A *Object Palette* possui todos os componentes necessários para a modelagem da rede desejada. Além da escolha dos objetos é necessário definir as aplicações a serem executadas na rede. As aplicações são definidas e configuradas como objetos. Para a simulação são o *Application Definition* (Definição de Aplicação) e o *Profile Definition* (Definição de Perfil). O primeiro é utilizado para definir quais aplicações podem ser usadas durante a simulação. A Figura 4.5 mostra o objeto e sua janela de configurações.

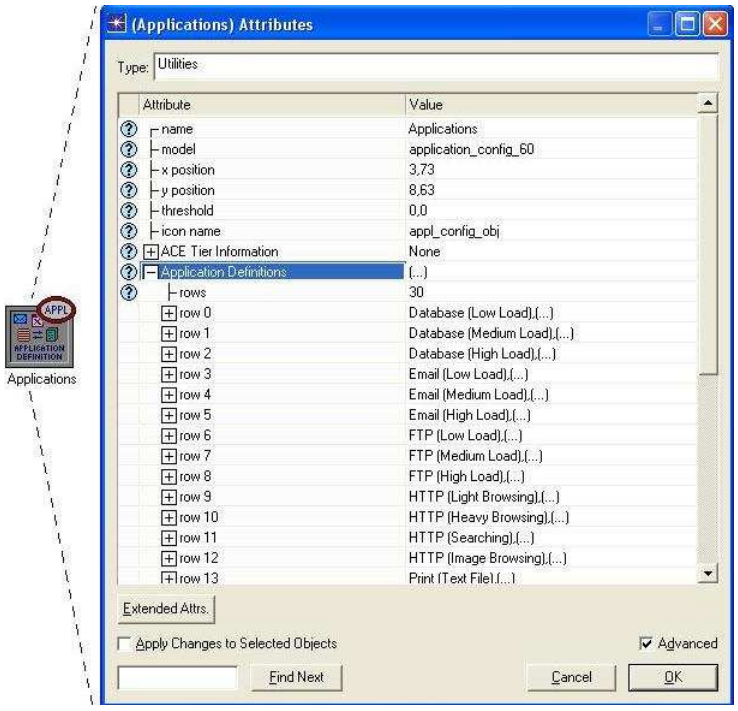

Figura 4.5: O objeto *Application Definition* e seus atributos.

Já o *Profile Definition* tem como função definir o perfil dos dispositivos da rede. Esse perfil carrega as informações sobre as aplicações com as quais o *host* irá trabalhar. Esse perfil está baseado nas aplicações disponíveis no *Application*

Definition. Na Figura 4.6 é possível observar o objeto *Profile Definition* e sua janela de configuração.

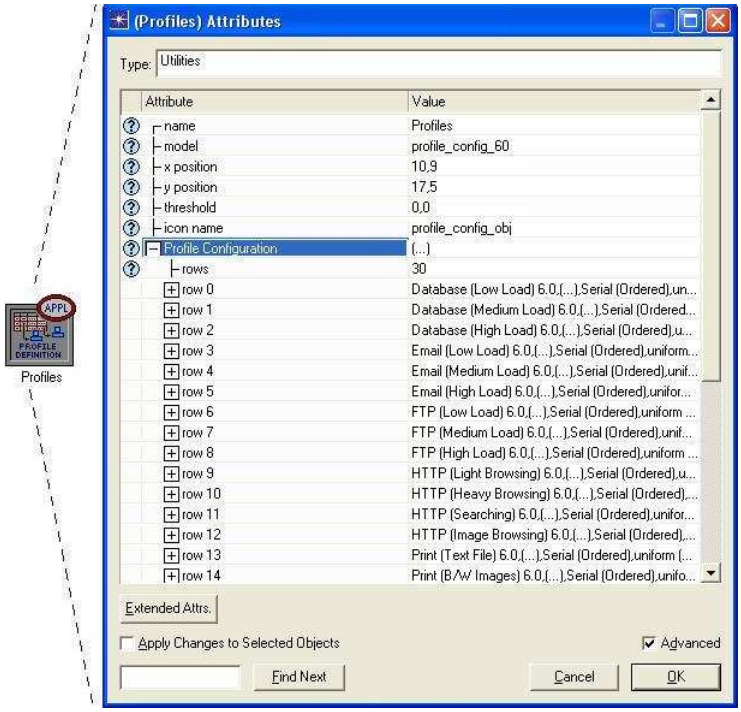

Figura 4.6: O objeto *Profile Definition* e seus atributos.

No presente trabalho, foi utilizado o objeto do tipo *Application Definition* já existente no simulador, *application config 60*, que por padrão possui todos os tipos de aplicações (citados anteriormente) em todos os níveis de carga de trabalho (baixa, média e alta). Também foi utilizado um objeto do tipo *Profile Definition* pré-existente, o *profile config 60*, que já possui configurados para uso todos os perfis baseados nas aplicações do objeto *application config 60*. A partir desses objetos foi possível configurar os servidores e estações de trabalhos com os serviços e perfis desejados.

A Figura 4.7 mostra a janela de configuração dos atributos de um dos servidores utilizados nas simulações.

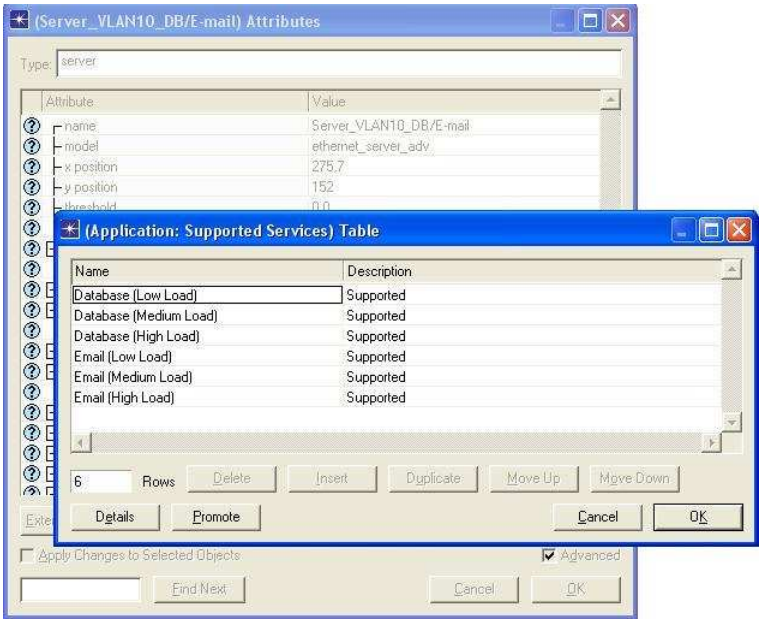

Figura 4.7: Janela de atributos de um dos servidores utilizados nas simulações.

Assim como na Figura 4.7, a Figura 4.8 exibe o mesmo tipo de janela pertencente a uma das estações de trabalho.

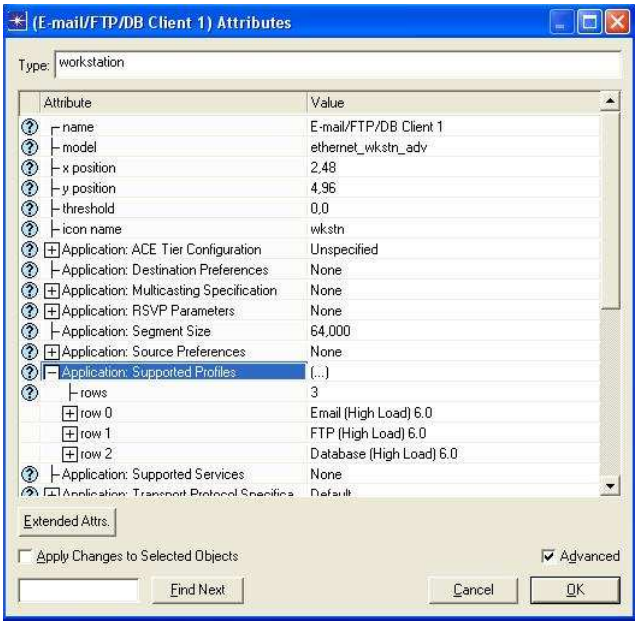

Figura 4.8: Janela de atributos de uma das estações de trabalho utilizadas nas simulações.

Para este trabalho foram definidas quatro topologias e oito cenários que serão descritos a seguir.

4.3 Topologias e Cenários

Inicialmente foram definidas informações referentes à topologia da rede, ao tráfego gerado pelos usuários, os tipos de enlaces físicos da rede e realizada a adequação de todos os requisitos da pesquisa para dar início a modelagem. Em todos os cenários os servidores forem preparados para dar suporte aos seus respectivos serviços em três níveis de carga (baixa, média e alta), para que os ambientes

simulados estejam próximos da realidade. Já as estações de trabalho foram configuradas para utilizarem suas aplicações com carga alta. Os circuitos utilizados em todos os enlaces foram configurados para operar a uma taxa de 100BaseT. Com todas as informações necessárias definidas, as topologias e os cenários modelados foram:

a.1) Cenário 1 – versão sem uso de segmentação virtual. Esse cenário possui topologia do tipo estrela, possuindo um switch como o nó central, formando um único domínio de broadcast. O cenário possui dois servidores (E-mail e FTP) e dois grupos de estações de trabalho, sendo um grupo cliente do Servidor de E-mail e o outro cliente do Servidor FTP. A Figura 4.9 mostra um esboço do cenário a ser modelado.

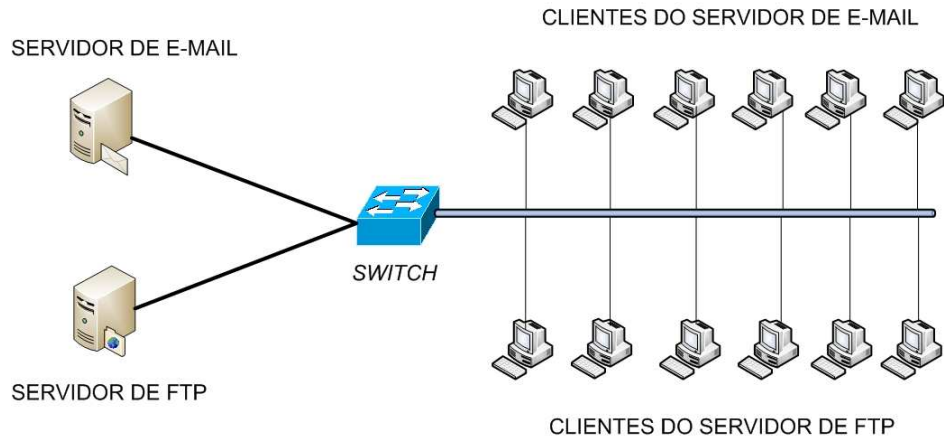

Figura 4.9: Esboço do Cenário a.1.

A partir do esboço foi possível a modelagem do cenário desejado usando o ambiente de simulação do OPNET, conforme a Figura 4.10.

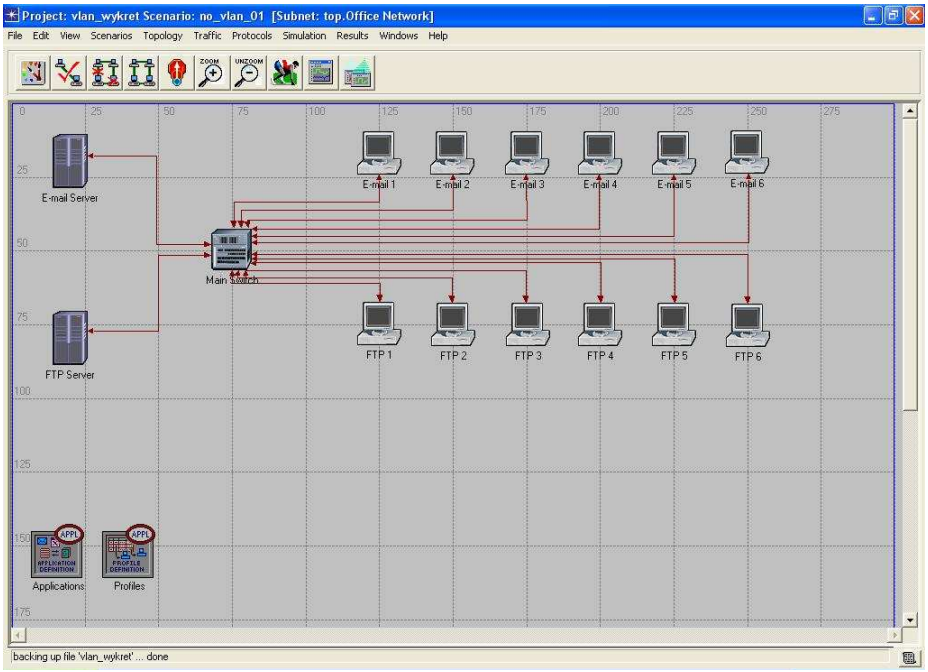

Figura 4.10: Cenário a.1 no OPNET.

a.2) Cenário 1 – versão utilizando VLANs. Esse cenário possui os mesmos dispositivos e aplicações utilizados no Cenário a.1. No entanto, duas VLANs foram criadas – VLAN 10 e VLAN 20 – criando uma segmentação lógica e dividindo a rede em dois domínios de *broadcast* independentes.

A Figura 4.11 mostra um esboço do cenário com a rede a ser modelada no OPNET.

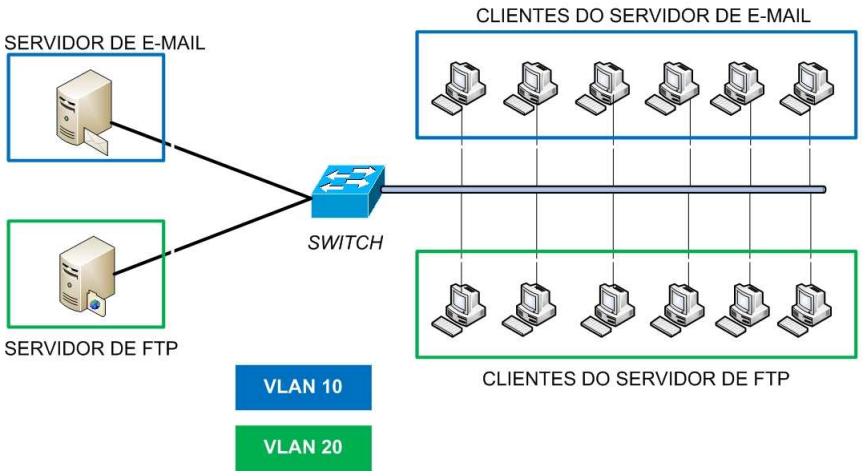

Figura 4.11: Esboço do Cenário a.2.

As aplicações utilizadas nesse caso foram as mesmas do ambiente anterior, E-mail e FTP.

A Figura 4.12 mostra o cenário com VLANs modelado no ambiente de simulação do OPNET.

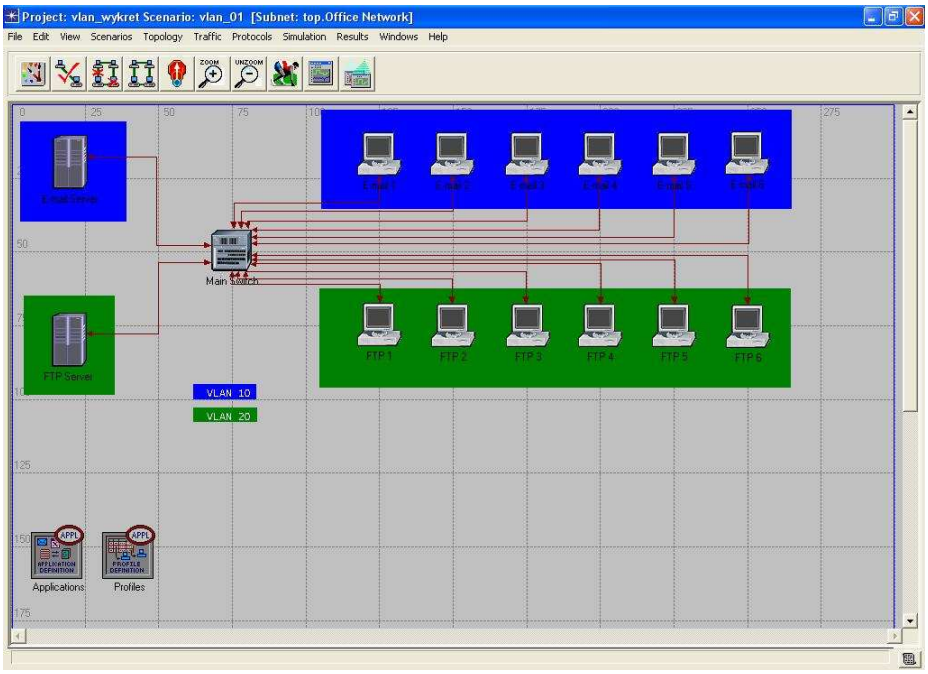

Figura 4.12: Cenário a.2 no OPNET.

b.1) Cenário 2 – versão sem uso de segmentação virtual. O Cenário b.1 simula um ambiente em que dois departamentos (Departamento A – DEP. A e Departamento B – DEP. B) de uma organização estão distribuídos em dois prédios diferentes (Prédio 1 e 2). Cada prédio possui um *switch* ao qual os dispositivos estão ligados. Existem servidores e estações de trabalho do Departamento A e do Departamento B em ambos os prédios. Isso significa que *hosts* pertencentes aos Departamentos A e B precisam ter acesso às redes dos dois prédios. A Figura 4.13 mostra um esboço do cenário antes de ser construído no simulador.

As aplicações utilizadas nos Cenários b.1 e b.2 foram: Banco de Dados (BD), FTP, E-mail e HTTP.

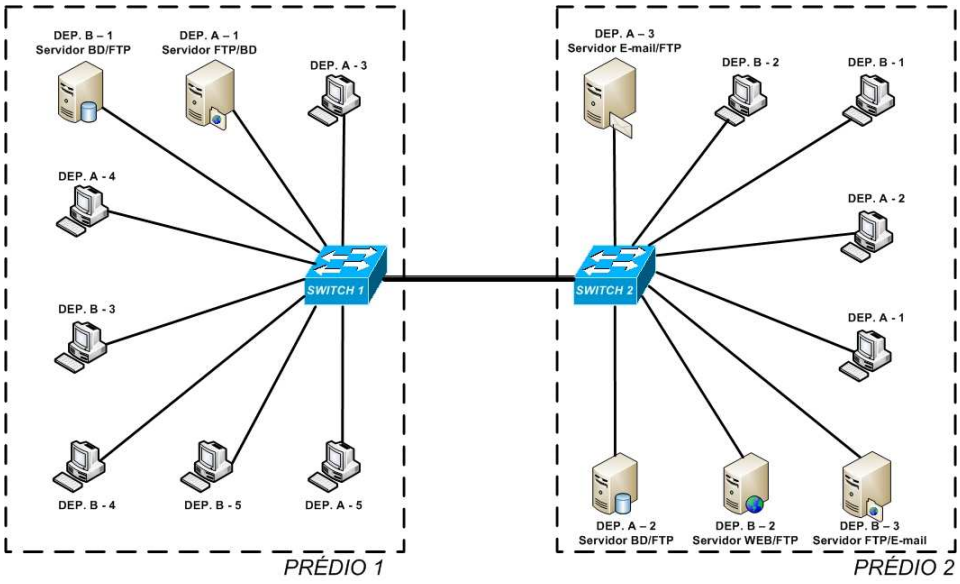

Figura 4.13: Esboço do Cenário b.1.

Com as aplicações e topologia definidas, o Cenário b.1 foi modelado no simulador OPNET, conforme mostra a Figura 4.14.

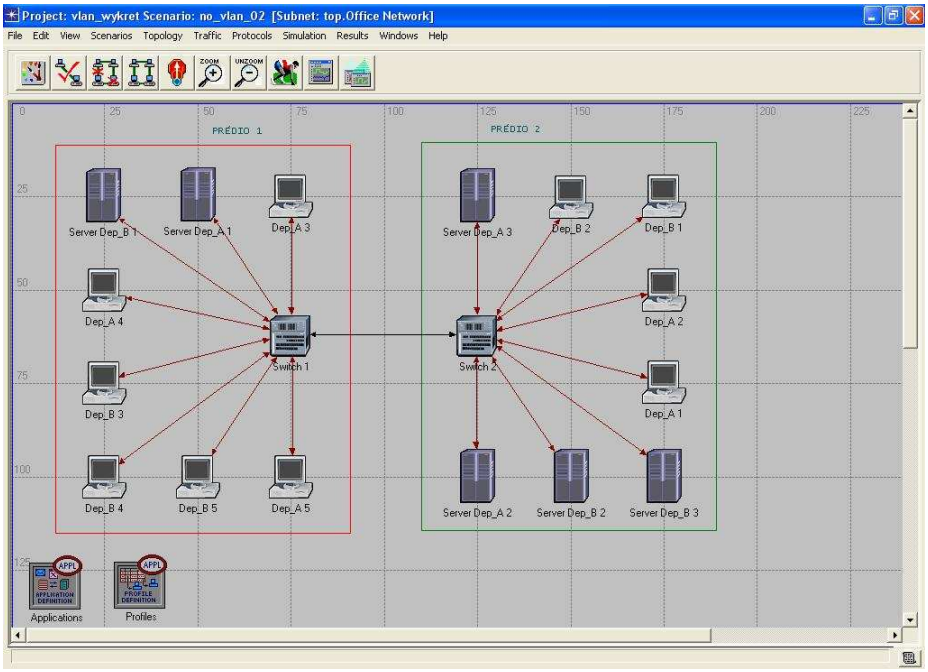

Figura 4.14: Cenário b.1 no OPNET.

b.2) Cenário 2 – versão utilizando VLANs. Esse cenário possui os mesmos dispositivos e aplicações utilizados no Cenário b.1. Porém, foram criadas duas redes virtuais: VLAN 10 para o Departamento A e VLAN 20 para o Departamento B.

A Figura 4.15 mostra um esboço do cenário antes da modelagem.

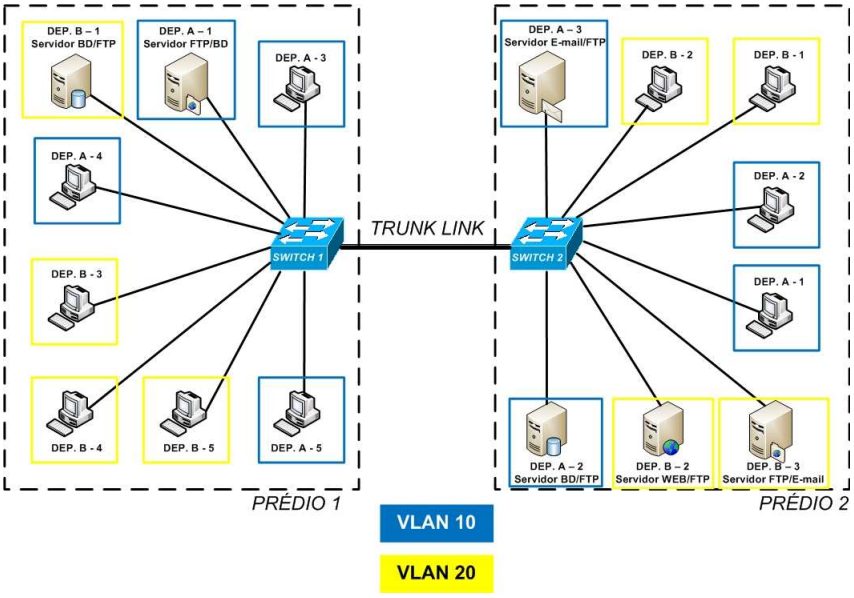

Figura 4.15: Esboço do Cenário b.2.

Nesse caso, dois *switches* foram utilizados e como todos os dispositivos precisam ter acesso a ambas as VLANs, foi necessário utilizar o *VLAN Trunking Protocol* (VTP). Isso tornou possível que os dois *switches* carregassem as informações das duas VLANs criadas.

A Figura 4.16 mostra o cenário b.2 criado no OPNET.

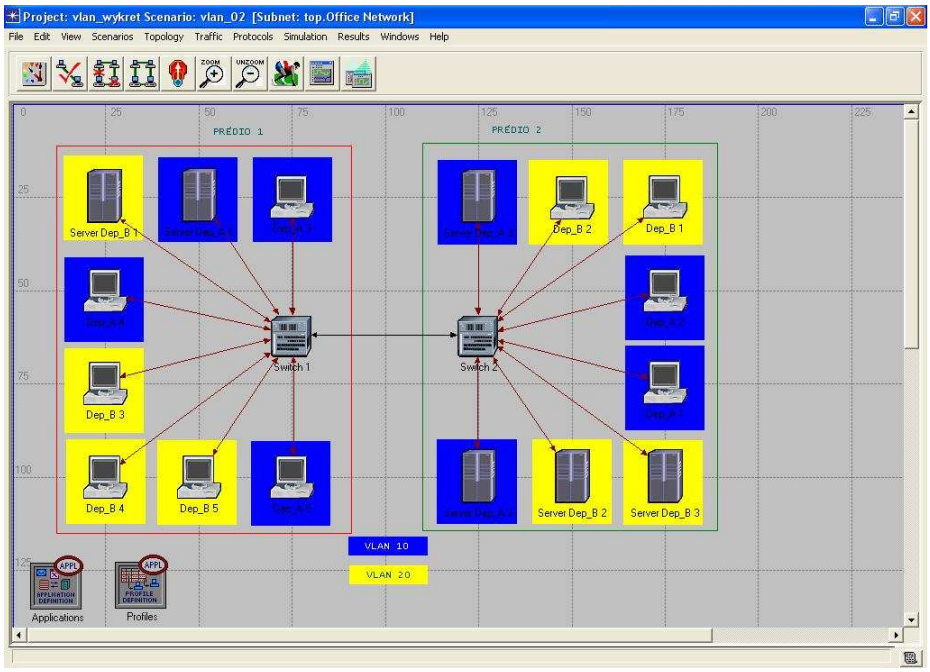

Figura 4.16: Cenário b.2 no OPNET.

c.1) Cenário 3 – versão sem uso de segmentação virtual. Esse cenário se refere uma grande rede local dividida em outras três sub-redes (LAN 1, 2 e 3). O *Switch* Principal (*Main Switch*) realiza a união das três sub-redes com os servidores disponíveis. Em cada um dos três níveis (Nível 1, 2 e 3) existem dispositivos de todas as três sub-redes. A descrição dos níveis é a seguinte:

- Nível 1 – possui um *switch* para cada uma das três sub-redes (LAN1-SW1, LAN2-SW1 e LAN3-SW1), quatro estações de trabalho da LAN 1 (LAN1-1, LAN1-2, LAN1-3 e LAN1-4), duas estações de trabalho da LAN 2 (LAN2-1 e LAN2-2) e duas estações de trabalho da LAN 3 (LAN3-1 e LAN3-2);
- Nível 2 – possui um *switch* para cada uma das três sub-redes (LAN1-SW2, LAN2-SW2 e LAN3-SW2), duas estações de trabalho da LAN 1 (LAN1-5 e LAN1-6), quatro estações de trabalho da LAN 2 (LAN2-3, LAN2-4, LAN2-5 e LAN2-6) e duas estações de trabalho da LAN 3 (LAN3-3 e LAN3-4);
- Nível 3 – possui um *switch* para cada uma das três sub-redes (LAN1-SW3, LAN2-SW3 e LAN3-SW3), duas estações de trabalho da LAN 1 (LAN1-7 e LAN1-8), duas estações de trabalho da LAN 2 (LAN2-7 e LAN2-8) e quatro estações de trabalho da LAN 3 (LAN3-5, LAN3-6, LAN3-7 e LAN3-8).

A Figura 4.18 ilustra o cenário descrito antes de ser modelado no OPNET.

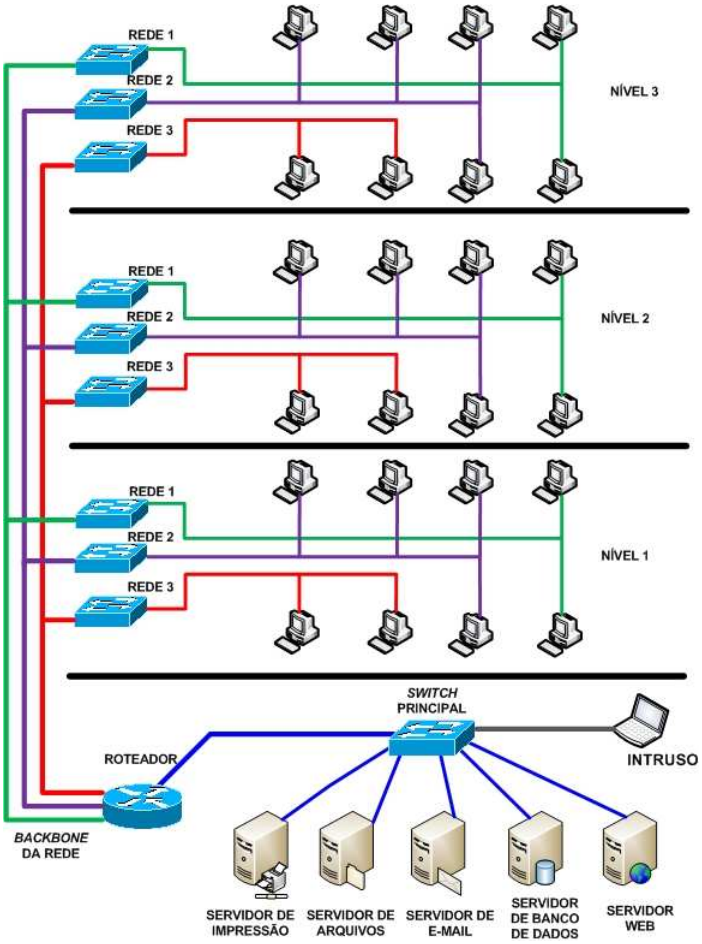

Figura 4.17: Esboço do Cenário c.1.

O Cenário c.1 conta ainda com servidores que disponibilizam serviços de Impressão, E-mail, FTP, HTTP e Banco de Dados. Na modelagem do OPNET, o cenário possui ainda uma estação de trabalho intrusa (*Hacker*), conectada ao *Main Switch*, que utiliza os serviços disponíveis e gera de tráfego desnecessário na rede.

A Figura 4.18 ilustra o cenário após ser construído no ambiente de simulação.

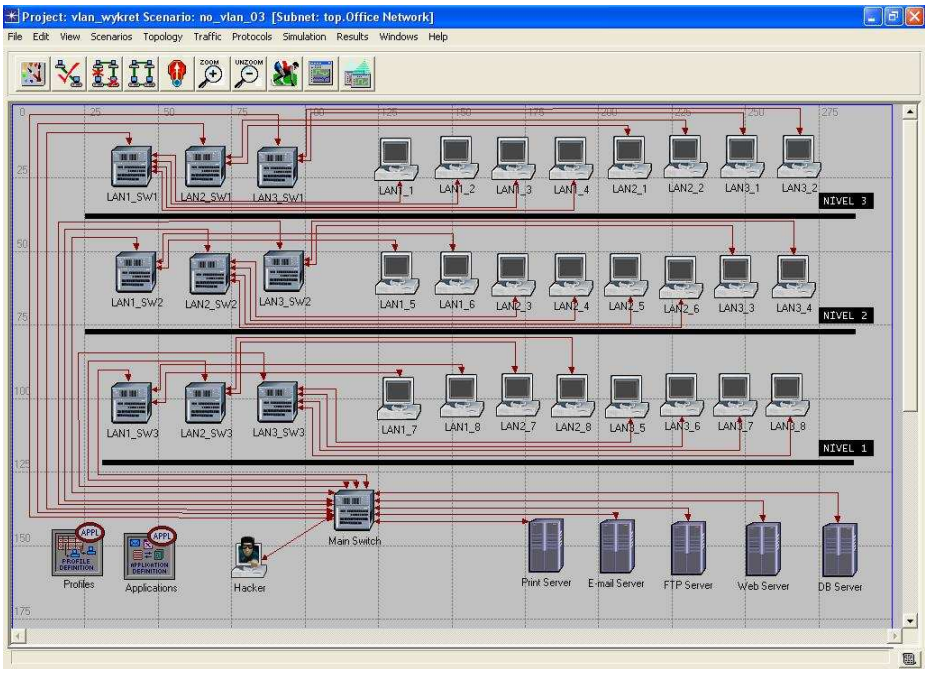

Figura 4.18: Cenário c.1 no OPNET.

c.2) Cenário 3 – versão utilizando VLANs. Essa versão do cenário possui as mesmas estações de trabalho, a estação intrusa e aplicações utilizadas no Cenário 3 – versão sem uso de segmentação virtual. O *Main Switch* é um *switch* de nível 3, capaz de realizar roteamento e permitindo assim que os integrantes de qualquer VLAN acessem qualquer um dos servidores. Após a criação de três redes virtuais (VLAN 10, VLAN 20 e VLAN 30) foi possível retirar dois *switches* de cada um dos níveis, pois apenas um *switch* configurado para suportar as três VLANs em cada nível é suficiente para controlar as três sub-redes, conforme indicado em esboço da Figura 4.19.

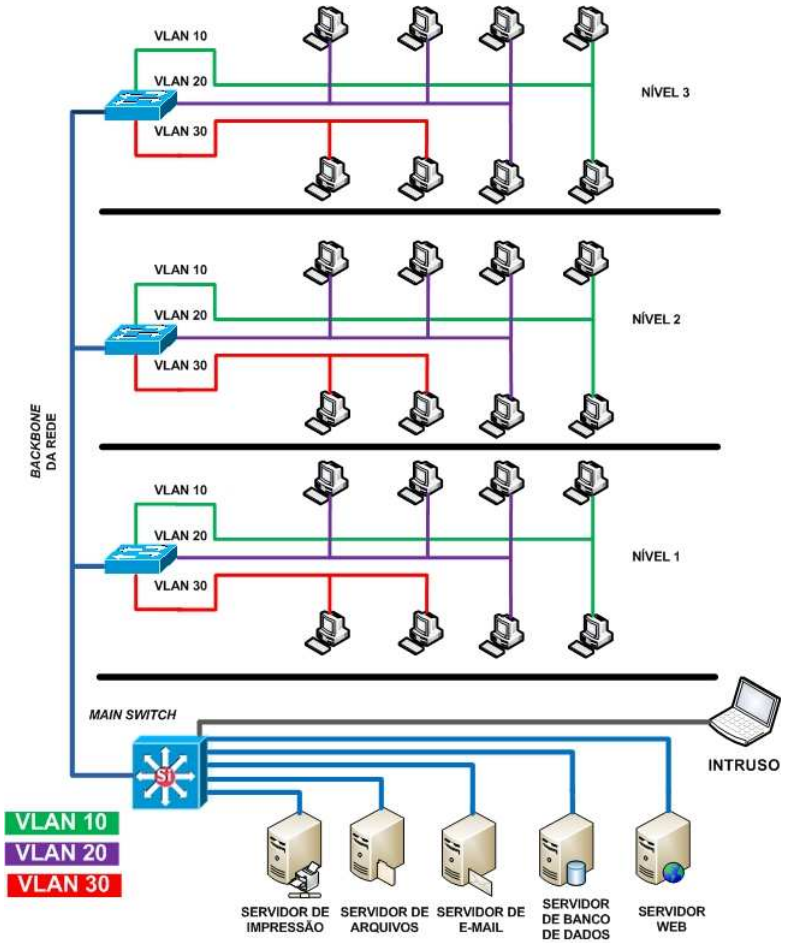

Figura 4.19: Esboço do Cenário c.2

Nesse cenário, todos os dispositivos precisam ter acesso aos servidores e, por isso, o *Main Switch* e os outros três *switches* devem dar suporte a todas as VLANs criadas. Assim, foi necessário utilizar o *VLAN Trunking Protocol* (VTP), conforme mostra a Figura 4.20. Dessa maneira, todos os *switches* carregam as informações das três VLANs existentes.

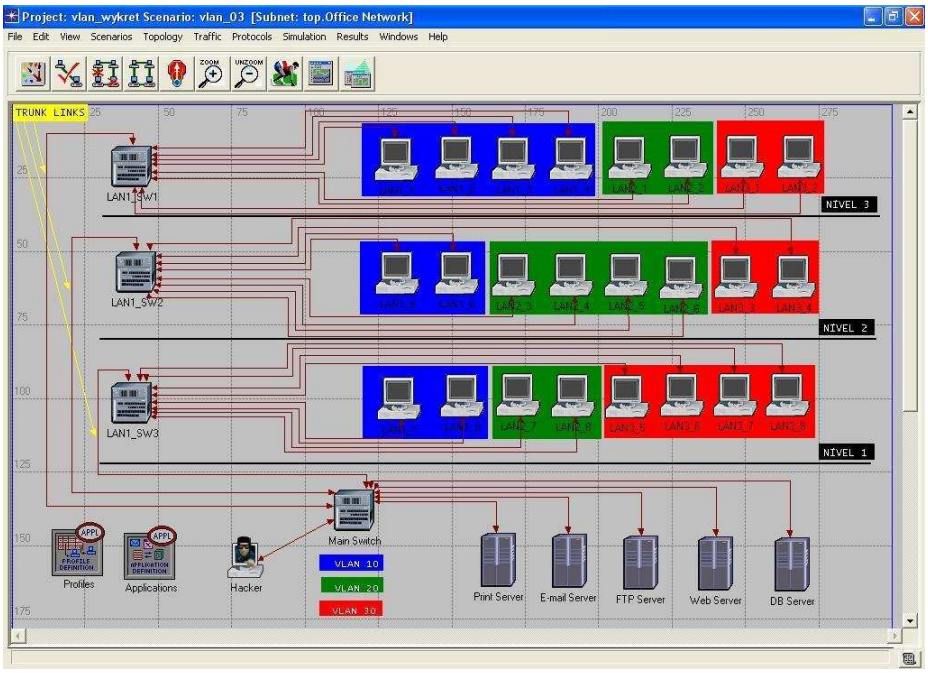

Figura 4.20: Cenário c.2 no OPNET.

d.1) Cenário 4 – versão sem uso de segmentação virtual. Esse cenário descreve uma situação em duas redes, em dois prédios (Prédio 1 e 2) separados que são conectadas através de um roteador. No Prédio 1, encontra-se um servidor de FTP e duas estações de trabalho, sendo que uma delas utiliza os serviços de E-mail, FTP e Banco de Dados, e a outra, apenas o serviço de E-mail e um *switch* (*Switch* 1) fazendo a conexão dos *hosts* com o roteador. No Prédio 2, existem dois servidores (um de E-mail e outro de Banco de Dados) e quatro estações de trabalho. Uma utilizando E-mail, FTP e Banco de Dados, outra utiliza Banco de Dados, a terceira Banco de Dados e FTP, e a última apenas o serviço de E-mail. Realizando a ligação entre os dispositivos do Prédio 2 estão dois *switches* (*Switches* 1 e 2), sendo um deles conectado direto ao roteador, conforme mostra a Figura 4.21.

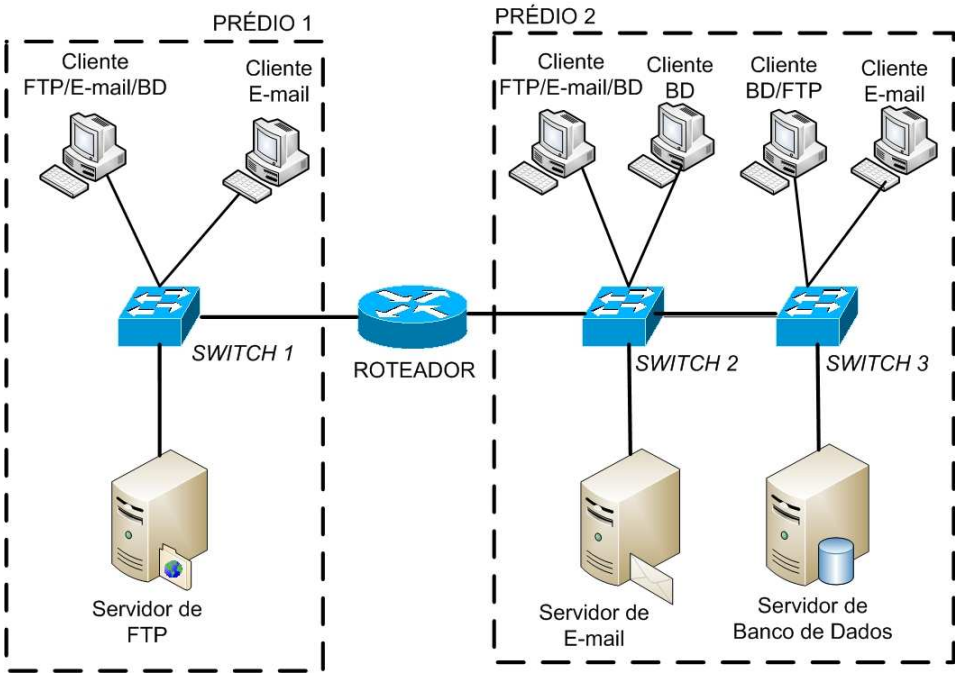

Figura 4.21: Esboço do Cenário d.1.

No Cenário d.1, as aplicações utilizadas durante a simulação foram FTP, E-mail e Banco de Dados. A interligação das redes dos Prédios 1 e 2 é realizada pelo roteador.

De acordo com a Figura 4.22, na modelagem da rede no OPNET, foi utilizado um roteador Cisco Série 4700.

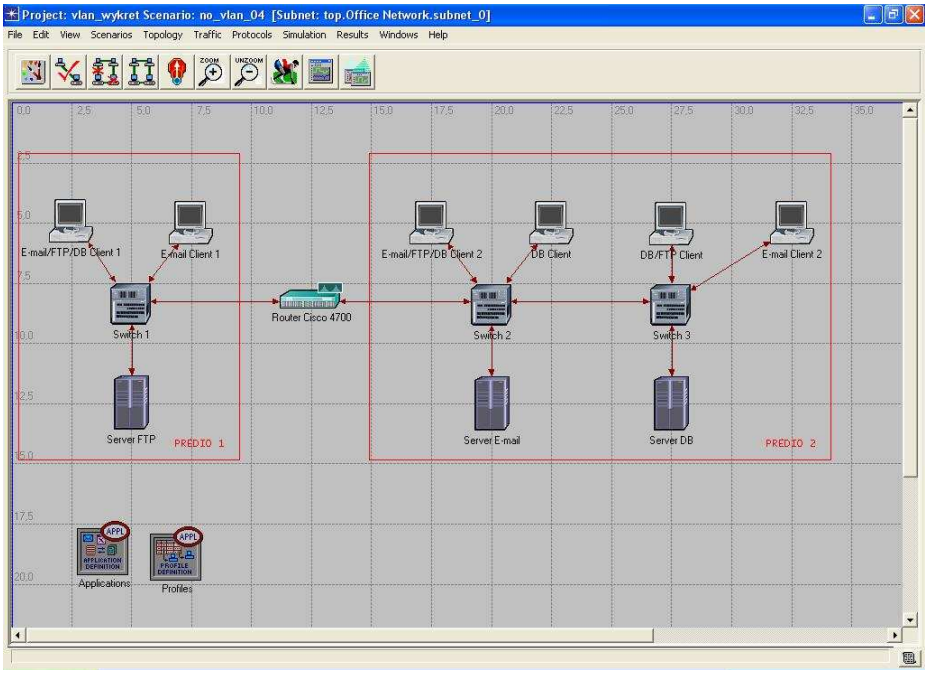

Figura 4.22: Cenário d.1 no OPNET.

d.2) Cenário 4 – versão utilizando VLANs. Nesse cenário estão presentes os mesmos dispositivos e aplicações do cenário anterior. No entanto, nesse caso, foi realizada uma segmentação virtual das redes. Foram criadas quatro VLANs (VLAN 10, VLAN 20 e VLAN 30), conforme Figura 4.23.

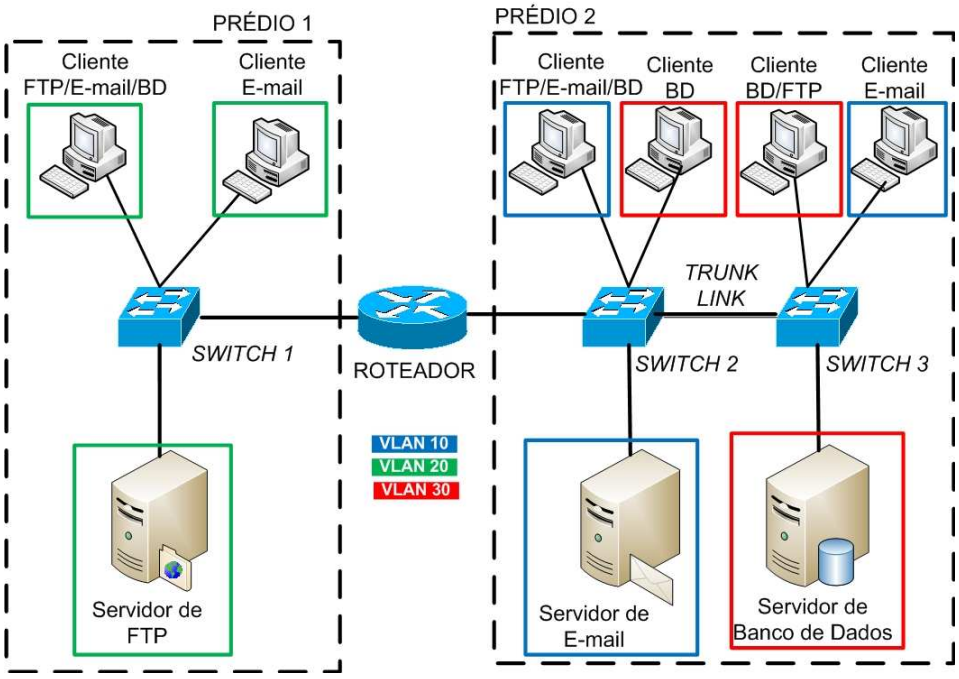

Figura 4.23: Esboço do Cenário d.2.

Para que todas as VLANs se comuniquem é necessário um equipamento que faça o roteamento dos pacotes, função do roteador Cisco 4700. Para que a rede fosse expandida do *Switch* 2 para o 3 e as VLANs mantidas, foi necessário utilizar o *VLAN Trunking Protocol* (VTP), conforme indica a Figura 4.24.

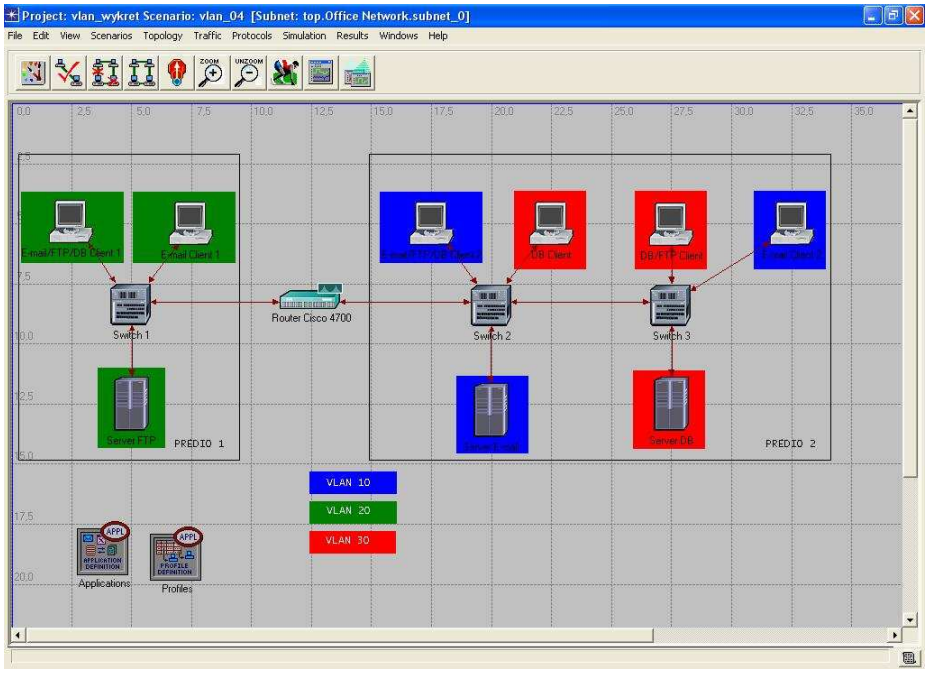

Figura 4.24: Cenário d.2 no OPNET.

4.4 Escolha das estatísticas

Após a modelagem dos cenários é necessário configurar as estatísticas a serem coletadas durante a simulação. Para esse trabalho foram coletadas estatísticas no *switches* e também estatísticas globais da rede.

A Figura 4.25 mostra a janela de seleção das estatísticas em um dos switches utilizados nas simulações.

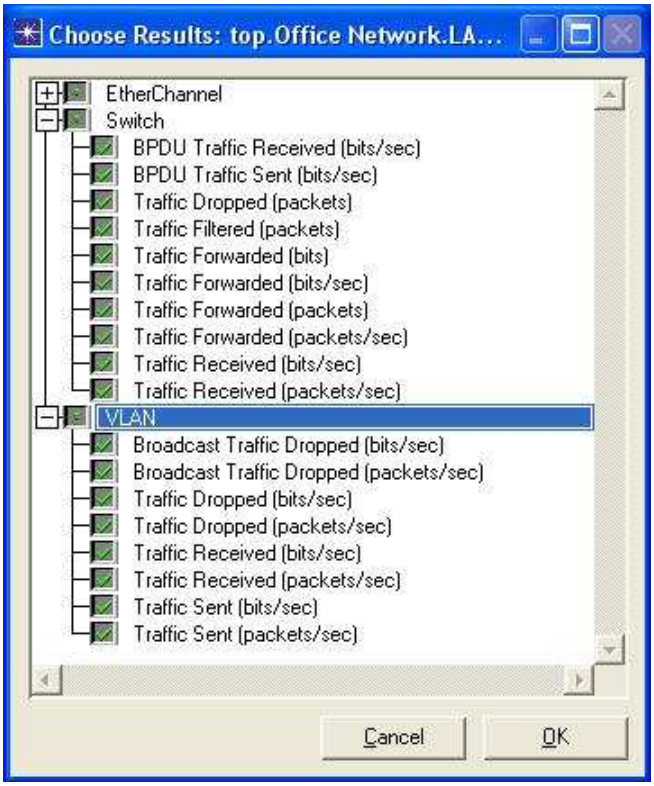

Figura 4.25: Janela de seleção das estatísticas de um switch a serem coletadas no OPNET.

A Figura 4.26 mostra a mesma janela da Figura 4.25, porém para estatísticas globais da rede.

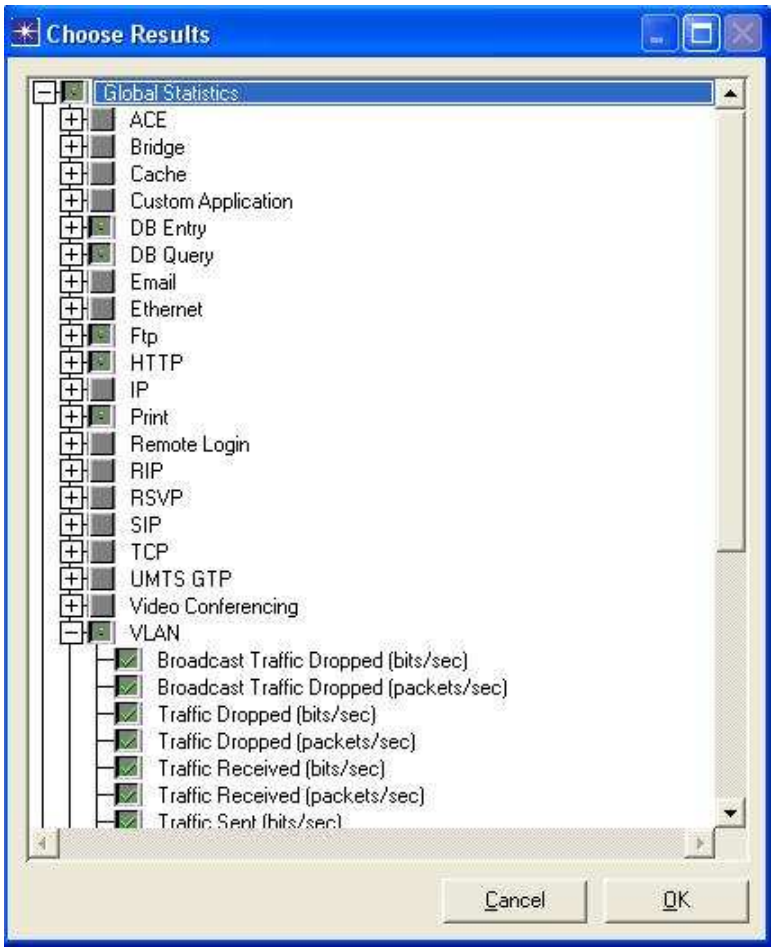

Figura 4.26: Janela de seleção das estatísticas globais a serem coletadas no OPNET.

4.5 Execução da simulação

Após a modelagem dos cenários e escolha das estatísticas, a simulação pode ser executada para que os dados sejam coletados e analisados. Antes de começar a simulação, é necessário abrir a janela de configuração desta, clicando no botão *configure/run simulation*, conforme mostra a Figura 4.27.

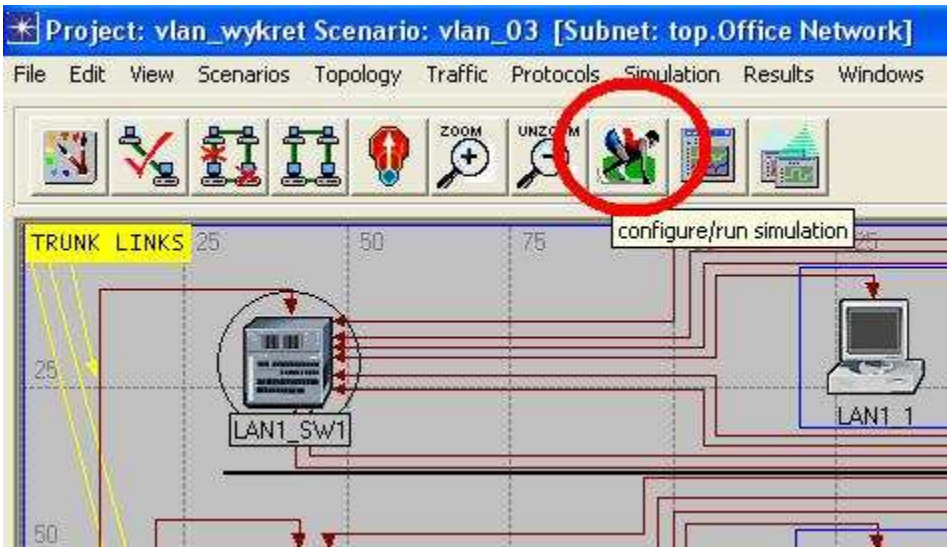

Figura 4.27: Botão *configure/run simulation* no ambiente de simulação OPNET.

Com a janela de configuração da simulação aberta, é feita a escolha do tempo a ser simulado pelo OPNET. O tempo pode ser definido em segundos, minutos, horas, dias e semanas, conforme ilustra a Figura 4.28. Ao acionar o botão *Run*, a simulação irá começar.

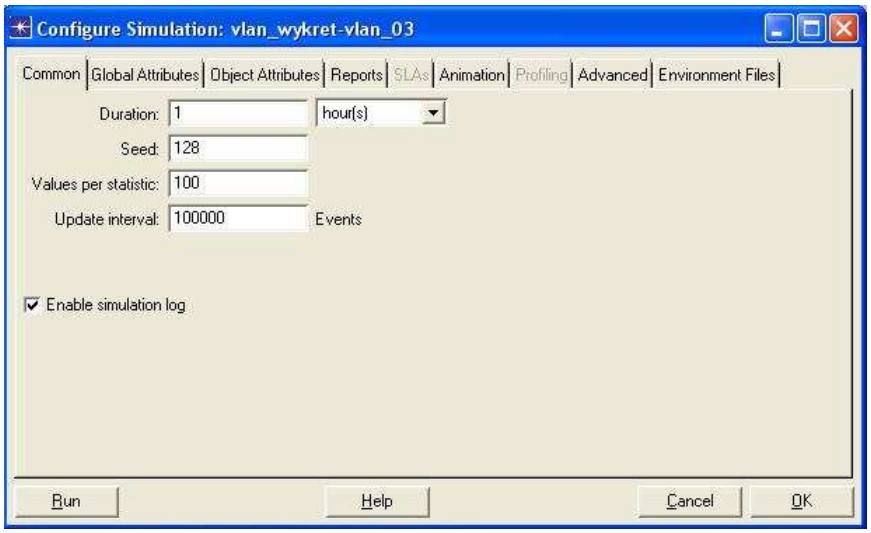

Figura 4.28: Janela de configuração da simulação no OPNET.

A Figura 4.29 mostra a janela que é exibida durante a simulação. Essa janela exibe as informações da simulação em execução (numericamente e em gráfico), tais como:

- *Elapsed Time* (Tempo Decorrido)
- *Estimated Remaining Time* (Tempo Restante Estimado)
- *Simulated Time* (Tempo Simulado)
- *Events* (Eventos)
- *Speed Average* (Velocidade Média, em eventos/segundo)

- *Speed Current* (Velocidade Atual, em eventos/segundo)

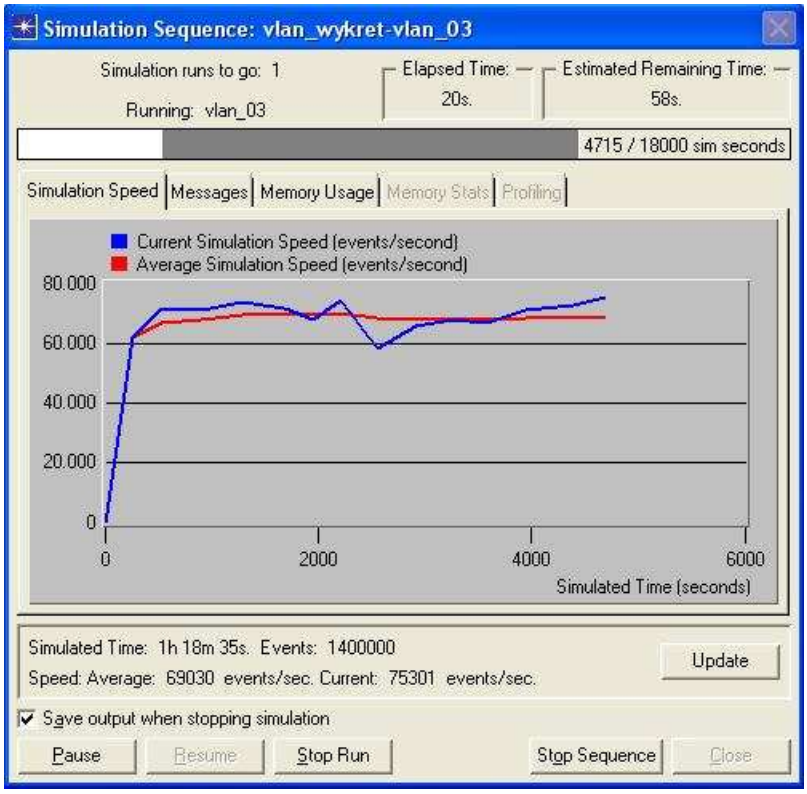

Figura 4.29: Janela com as informações da simulação em execução.

4.6 Visualização e Análise dos resultados

Quando a simulação termina é possível visualizar e analisar em forma de gráficos todas as informações que foram selecionadas antes da simulação. A Figura 4.30 mostra a janela de visualização dos resultados obtidos durante a simulação da rede.

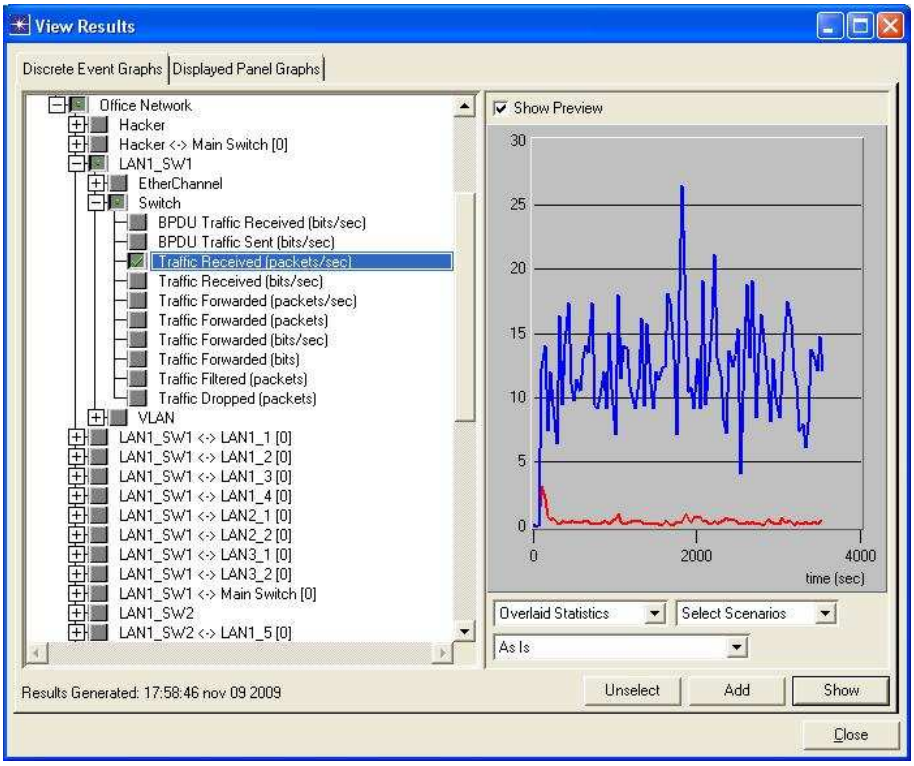

Figura 4.30: Janela de visualização de resultados obtidos na simulação do OPNET.

Os resultados obtidos e a análise dos gráficos gerados a partir das simulações realizadas no OPNET serão mostrados no capítulo a seguir. Serão avaliados os ganhos de desempenho na rede após a implantação das VLANs.

Capítulo 5

RESULTADOS E DISCUSSÃO

O objetivo deste capítulo é apresentar os resultados obtidos nas simulações de redes de computadores sem segmentação virtual e com a utilização de *Virtual Local Area Network* (VLAN). Após as simulações nos quatro tipos de cenários, os resultados alcançados serão comparados, comprovando a eficácia do método.

5.1 Cenários a.1 e a.2

Como nestes cenários é utilizado apenas um *switch*, não foi detectada melhoria em relação à redução do tráfego na rede, considerando a utilização ou não de VLANs. Esta situação se justifica pelo fato de todas as estações de trabalho estarem conectados ao mesmo *switch* em ambos os cenários. Assim todo o tráfego cenário, inevitavelmente, deve ser tratado por esse único *switch*.

A Figura 5.1 mostra o gráfico com o tráfego recebido (em pacotes/segundo) no *Main Switch* dos Cenários a.1 e a.2.

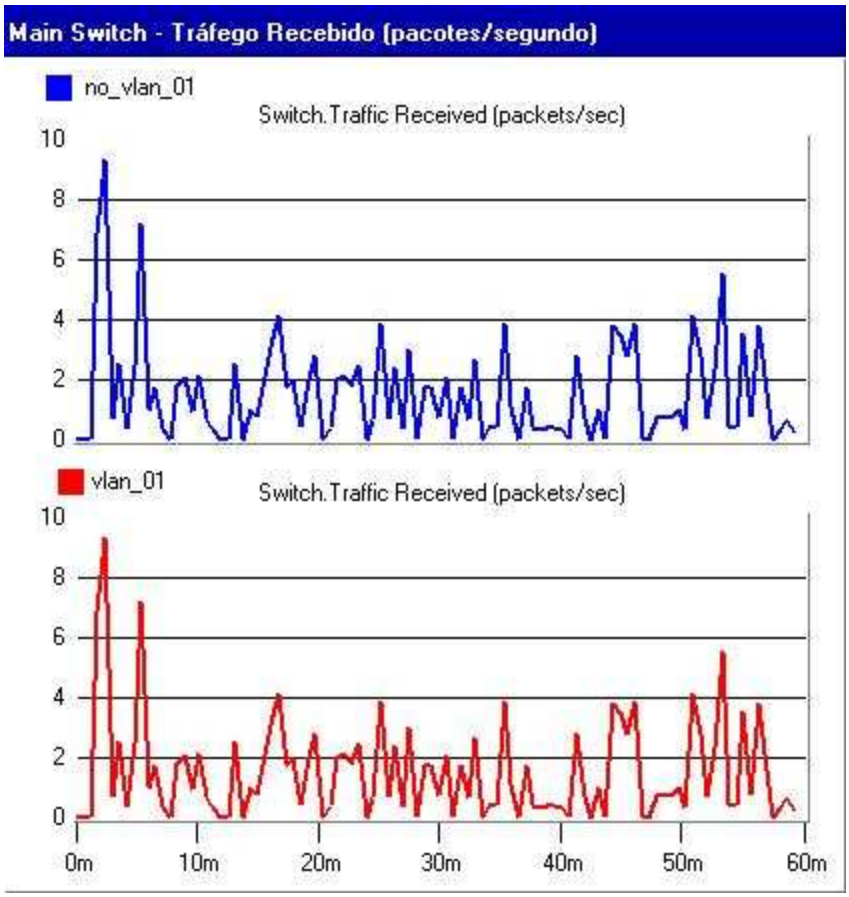

Figura 5.1: Gráfico de tráfego recebido do *Main Switch* dos Cenários a.1 e a.2.

Pelas mesmas razões que o tráfego recebido no *switch* se manteve o mesmo com ou sem o uso de VLANs, o tráfego encaminhado pelo *switch* também não se alterou devido à criação de VLANs, conforme mostra o gráfico de tráfego encaminhado (em pacotes/segundo) da Figura 5.2.

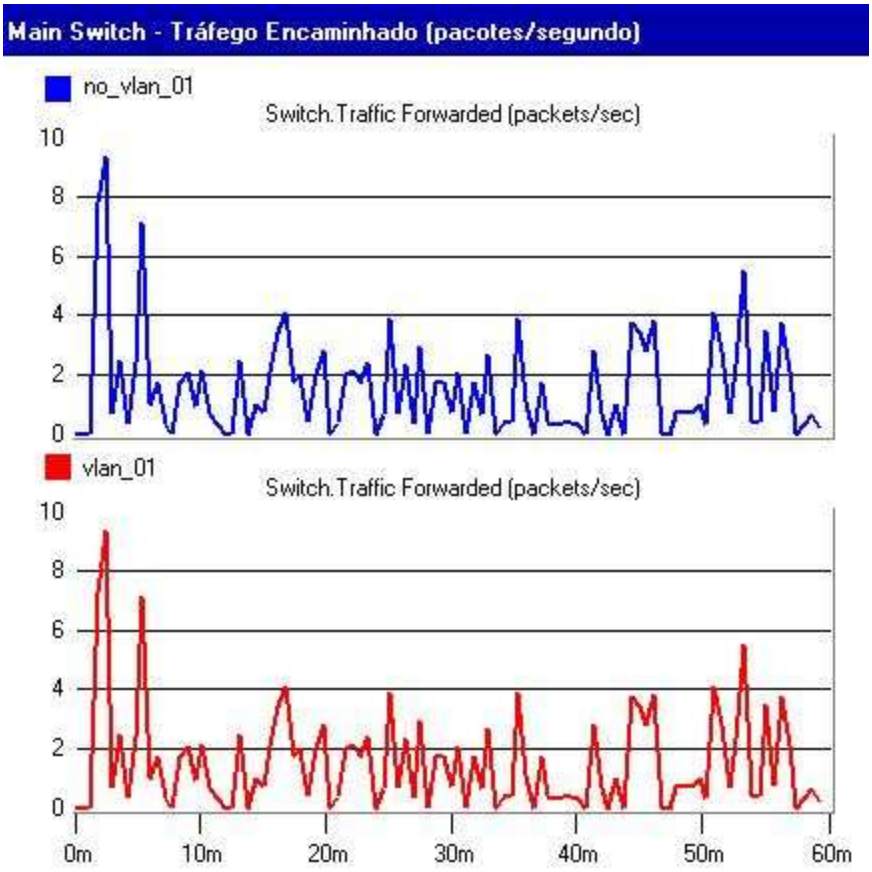

Figura 5.2: Gráfico de tráfego encaminhado do *Main Switch* dos Cenários a.1 e a.2.

A Tabela 5.1 contém as informações comparativas dos Cenários a.1 e a.2 referentes aos tráfegos recebidos e encaminhados.

Tabela 5.1: Tráfegos recebidos e encaminhados dos Cenários a.1 e a.2.

Dispositivo	Tráfego	Cenário	Tráfego em pacotes/segundo		
			Mínimo	Médio	Máximo
Main Switch	Recebido	a.1	0	1,51	9,33
	Recebido	a.2	0	1,51	9,33
	Encaminhado	a.1	0	1,52	9,33
	Encaminhado	a.2	0	1,51	9,33

Como já era esperado, devido aos resultados obtidos anteriormente, a carga nos servidores e a taxa de transferência dos enlaces também não apresentaram mudança significativa em relação aos Cenários a.1 e a.2. A Tabela 5.2 mostra a carga nos servidores nos dois cenários citados.

Tabela 5.2: Carga nos servidores dos Cenários a.1 e a.2.

Dispositivo	Cenário	Carga nos servidores em pacotes/segundo		
		Mínima	Média	Máxima
FTP Server	a.1	0	0,523	4,06
	a.2	0	0,523	4,06
E-mail Server	a.1	0	0,202	1,53
	a.2	0	0,202	1,53

Em redes de computadores com apenas um *switch* a utilização de VLANs não mostrou melhora em relação a redes em que nenhuma segmentação é realizada. No entanto, com o uso de VLANs, o gerenciamento da rede se torna mais fácil e esta se torna independente da topologia física, já que a manipulação dos usuários (adição e movimentação) pode ser feita remotamente e permite que grupo de trabalho fisicamente separados possam ser colocados em um único domínio de *broadcast*. Outro benefício importante a ser considerado é a segurança, pois o tráfego de uma VLAN não pode ser capturado por membros de outra rede virtual

sem a conexão do roteador. Os Cenários b.1 e b.2, mais complexos do que os anteriormente analisados, terão seus resultados discutidos a seguir.

5.2 Cenários b.1 e b.2

Os Cenários b.1 e b.2 possuem dois *switches* conectando duas sub-redes através de um *Trunk Link*, utilizando o *VLAN Trunking Protocol* (VTP). Como todos os dispositivos precisam acessar ambas as sub-redes e estão em um único domínio de *broadcast*, existe geração de tráfego desnecessário quando nenhum tipo de segmentação lógica é feita. Desta forma, a utilização de VLANs melhora consideravelmente o desempenho geral da rede.

Pelo gráfico mostrado na Figura 5.3, é possível perceber que tráfego recebido pelo *Switch* 1 quando a rede está segmenta com VLANs é menor do que sem uso de segmentação virtual.

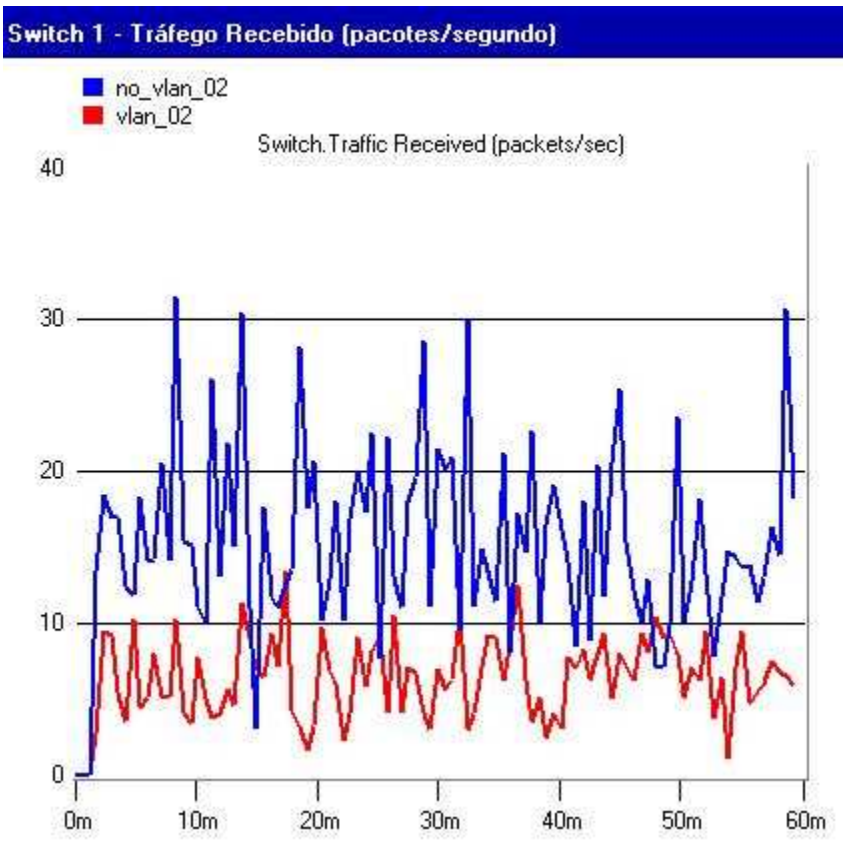

Figura 5.3: Gráfico de tráfego recebido do *Switch* 1 dos Cenários b.1 e b.2.

A Figura 5.4, referente ao gráfico de tráfego encaminhado do *Switch* 1, também mostra que houve diminuição dos pacotes enviados pelo *switch* após a segmentação virtual.

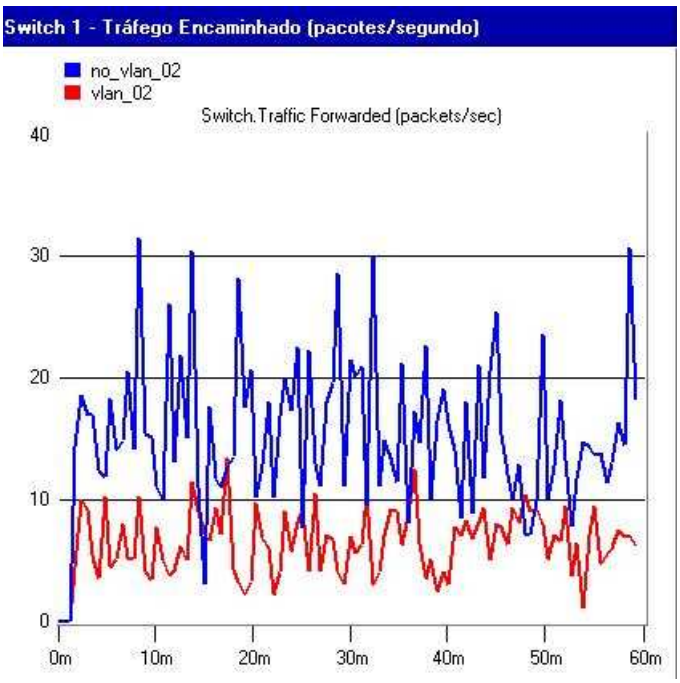

Figura 5.4: Gráfico de tráfego encaminhado do *Switch* 1 dos Cenários b.1 e b.2.

O gráfico da Figura 5.5 mostra que o *Switch 2* também obteve redução de tráfego recebido após a criação das VLANs.

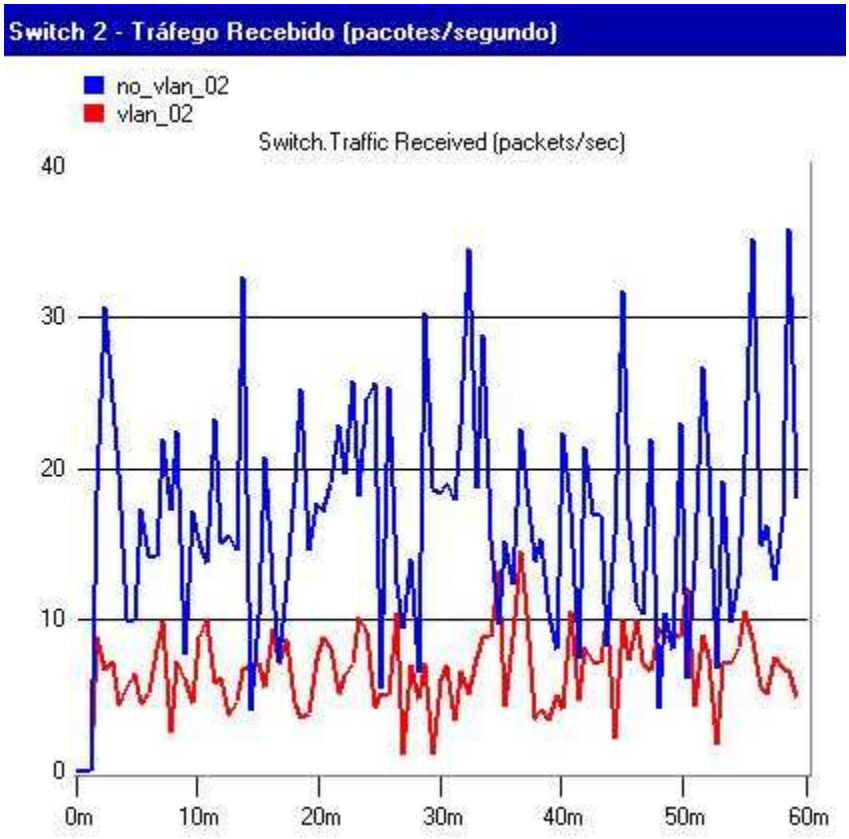

Figura 5.5: Gráfico de tráfego recebido do *Switch* 2 dos Cenários b.1 e b.2.

A Figura 5.6 mostra o gráfico que indica a diminuição do tráfego encaminhado pelo *Switch* 2 em relação aos Cenários b.1 e b.2.

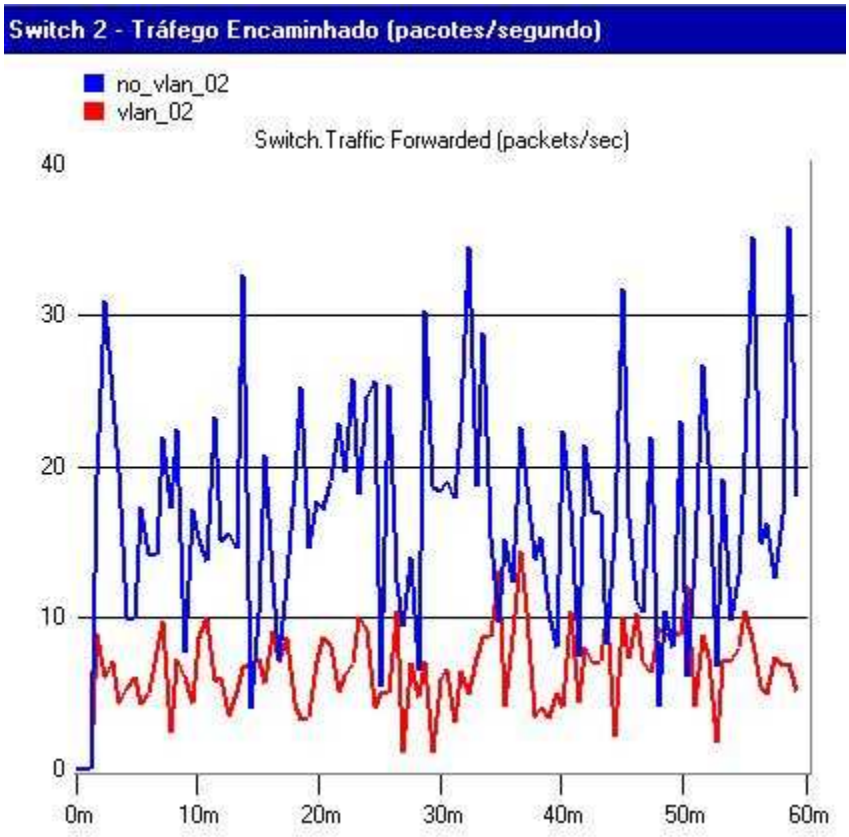

Figura 5.6: Gráfico de tráfego encaminhado do *Switch* 2 dos Cenários b.1 e b.2.

A Tabela 5.3 indica a redução de, aproximadamente, 58% no tráfego a ser tratado pelos *switches* dos Cenários b.1 e b.2.

Tabela 5.3: Tráfegos recebidos e encaminhados dos Cenários b.1 e b.2.

Dispositivo	Tráfego	Cenário	Tráfego em pacotes/segundo		
			Mínimo	Médio	Máximo
Switch 1	Recebido	b.1	0	15,2	31,4
	Recebido	b.2	0	6,3	13,4
	Encaminhado	b.1	0	15,3	31,4
	Encaminhado	b.2	0	6,38	13,4
Switch 2	Recebido	b.1	0	16,6	35,8
	Recebido	b.2	0	6,59	14,5
	Encaminhado	b.1	0	16,6	35,8
	Encaminhado	b.2	0	6,52	14,4

A Tabela 5.4 mostra a redução da carga nos servidores da rede que foi, em média, de 44% após a implantação das VLANs.

Tabela 5.4: Carga nos servidores dos Cenários b.1 e b.2.

Servidores	Cenários	Carga nos servidores em pacotes/segundo		
		Mínima	Média	Máxima
Dep_A 1 (BD e FTP)	b.1	0	1,88	5,8
	b.2	0	1,89	5,75
Dep_A 2 (BD e HTTP)	b.1	0	3,48	10,3
	b.2	0	1,89	5,17
Dep_A 3 (FTP e E-mail)	b.1	0	0,19	1,7
	b.2	0	0,18	1,69
Dep_B 1 (BD e FTP)	b.1	0	3,72	7,1
	b.2	0	1,9	5,14
Dep_B 2 (BD e HTTP)	b.1	0	4,03	16,5
	b.2	0	0	0
Dep_B 3 (FTP e E-mail)	b.1	0	0,22	2,1
	b.2	0	0,09	1,19

O próximo cenário a ser analisado é ainda mais complexo do que o anteriormente discutido. Será possível reduzir não apenas o tráfego na rede como também o número de equipamentos necessários.

5.3 Cenários c.1 e c.2

O cenário inicial (c.1) possui ao todo dez *switches*, sendo nove deles para conectar as três sub-redes existentes e outro *switch* principal que faz a conexão com os servidores. Após a segmentação utilizando VLANs, foi possível, além da redução significativa do tráfego, a eliminação de seis dos nove *switches* que estavam sendo usados pelas sub-redes. Isso pode ser feito já que as três sub-redes foram convertidas em três VLANs e somente um *switch* por nível possui capacidade suficiente para gerenciar todas as redes virtuais criadas. Ocorreu também a

inclusão de uma estação de trabalho intrusa, denominada *Hacker*, com o objetivo de utilizar os serviços e gerar tráfego desnecessário na rede do cenário modelado. O gráfico da Figura 5.7 mostra a redução ocorrida no tráfego recebido do *Main Switch*.

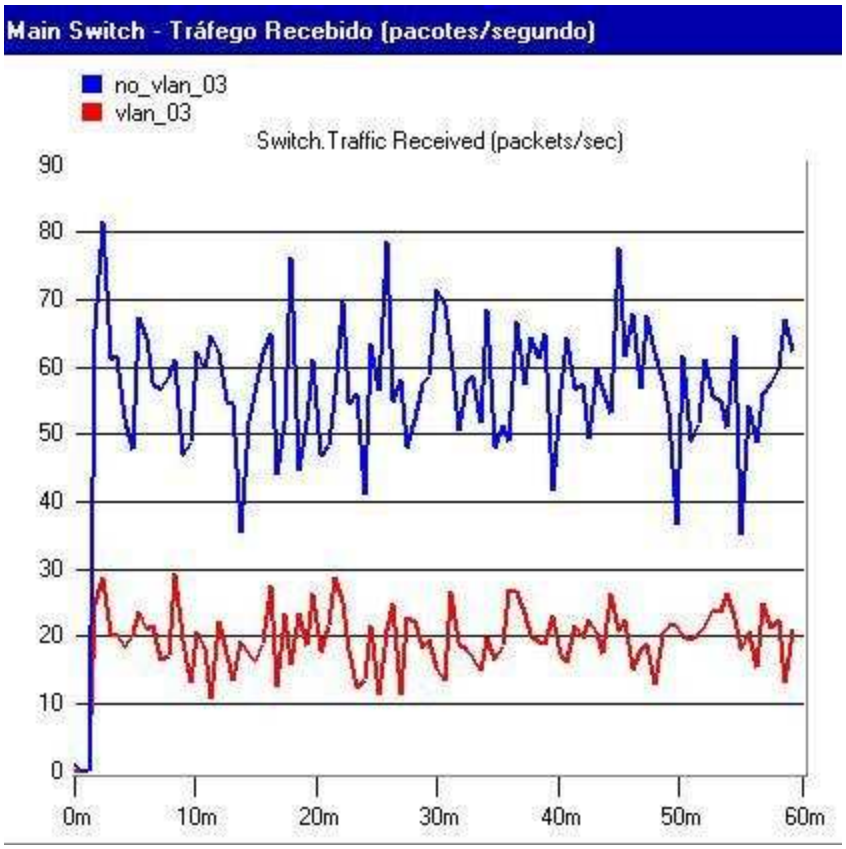

Figura 5.7: Gráfico de tráfego recebido do *Main Switch* dos Cenários c.1 e c.2.

Na Figura 5.8 é possível perceber a redução do tráfego a ser encaminhado pelo *Main Switch* dos Cenários c.1 e c.2 após realizar a segmentação virtual.

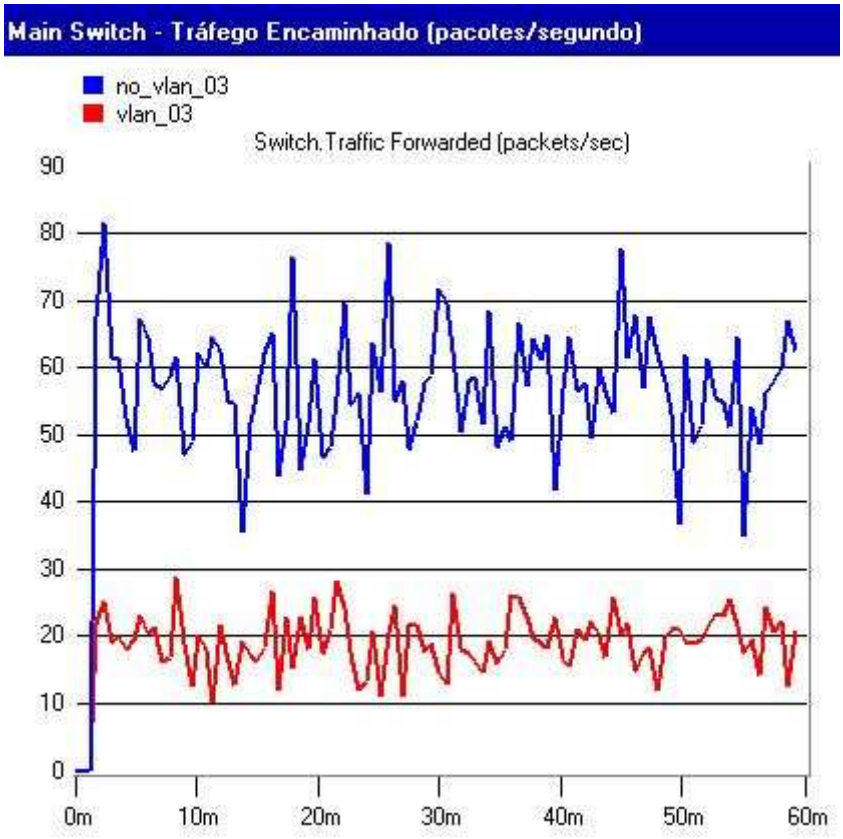

Figura 5.8: Gráfico de tráfego encaminhado do *Main Switch* dos Cenários c.1 e c.2.

O gráfico mostrado pela Figura 5.9 ilustra a situação do tráfego recebido pelo *switch* LAN1-SW1 com e sem o uso de VLANs nos Cenários c.1 e c.2 simulados no OPNET.

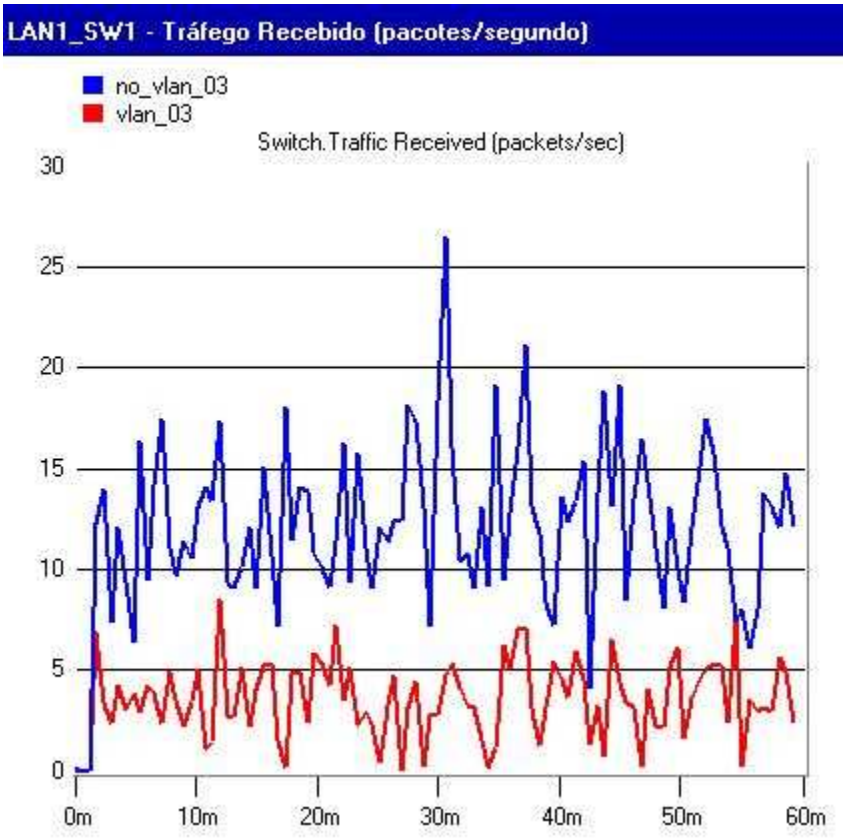

Figura 5.9: Gráfico de tráfego recebido do *switch* LAN1-SW1 dos Cenários c.1 e c.2.

O gráfico da Figura 5.10 indica que também houve a redução do tráfego encaminhado pelo *switch* LAN1-SW1 em relação aos Cenários c.1 e c.2.

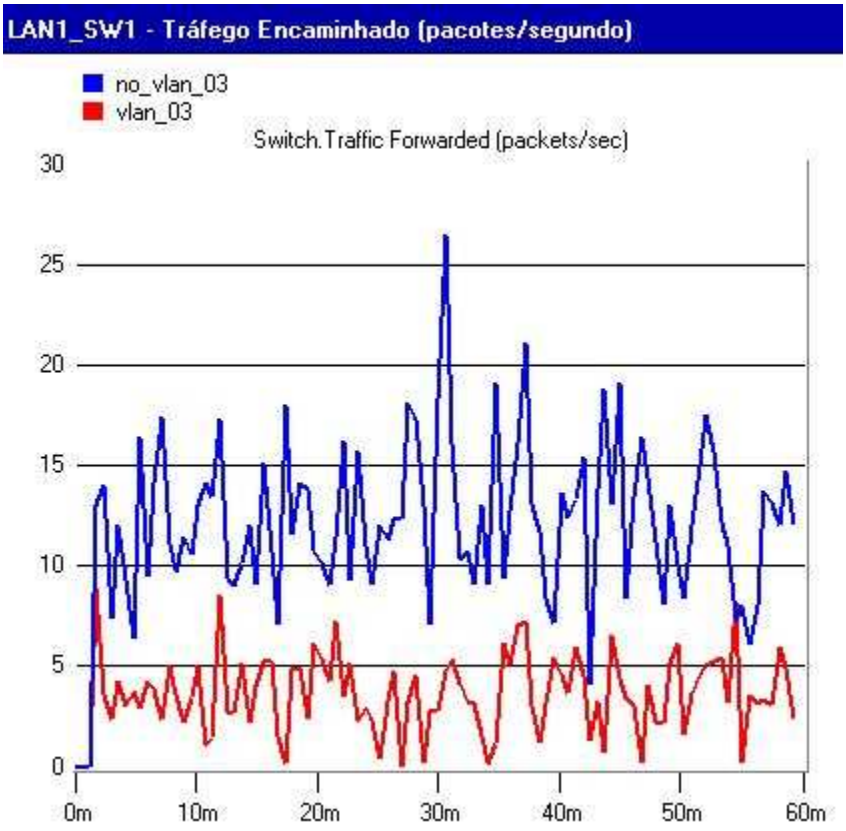

Figura 5.10: Gráfico de tráfego encaminhado do *switch* LAN1-SW1 dos Cenários c.1 e c.2.

Como citado anteriormente, alguns *switches* presentes no Cenário c.1 foram retirados do Cenário c.2. Os *switches* que foram mantidos no Cenário c.2 foram LAN2-SW2 e LAN3-SW3. Assim, no Nível 1 ficou o *switch* LAN1-SW1, no Nível 2 permaneceu o *switch* LAN2-SW2 e por último, no Nível 3 continuou o switch LAN3-SW3. E todos os *switches* relacionados estavam configurados para dar suporte às três VLANs criadas. As melhorias detectadas nos *switches* LAN2-SW 2 e LAN3-SW 3 foram semelhantes aos do *switch* LAN1-SW1. A Tabela 5.5 indica as reduções de tráfego conseguidas com o uso de VLANs, que chegam, em média, a 66%.

Tabela 5.5: Tráfegos recebidos e encaminhados dos Cenários c.1 e c.2.

Dispositivo	Tráfego	Cenário	Tráfego em pacotes/segundo		
			Mínimo	Médio	Máximo
Main Switch	Recebido	c.1	0	55,7	81,6
	Recebido	c.2	0	19,3	29,3
	Encaminhado	c.1	0	55,7	81,6
	Encaminhado	c.2	0	18,7	28,7
LAN1_SW1	Recebido	c.1	0	12,0	26,5
	Recebido	c.2	0	3,5	8,5
	Encaminhado	c.1	0	12,0	26,5
	Encaminhado	c.2	0	3,6	8,9

Outro benefício do uso de VLANs pode ser comprovado por meio das simulações. A segurança foi testada utilizando-se uma estação de trabalho intrusa, denominada *Hacker*, conectada ao switch principal da rede. No Cenário c.1, sem uso de VLANs, essa estação obteve sucesso em suas requisições e uso dos serviços da rede. No entanto, após a criação de VLANs, no Cenário c.2, o tráfego gerado pela pelo *Hacker* foi completamente descartado pelo *Main Switch*. Além disso, o intruso não pode "escutar" o tráfego de nenhuma das VLANs, pois a porta na qual ele está conectado não possui configuração de nenhuma das redes virtuais criadas.

A Figura 5.11 mostra o gráfico de tráfego recebido pelo *Hacker* nas situações descritas acima.

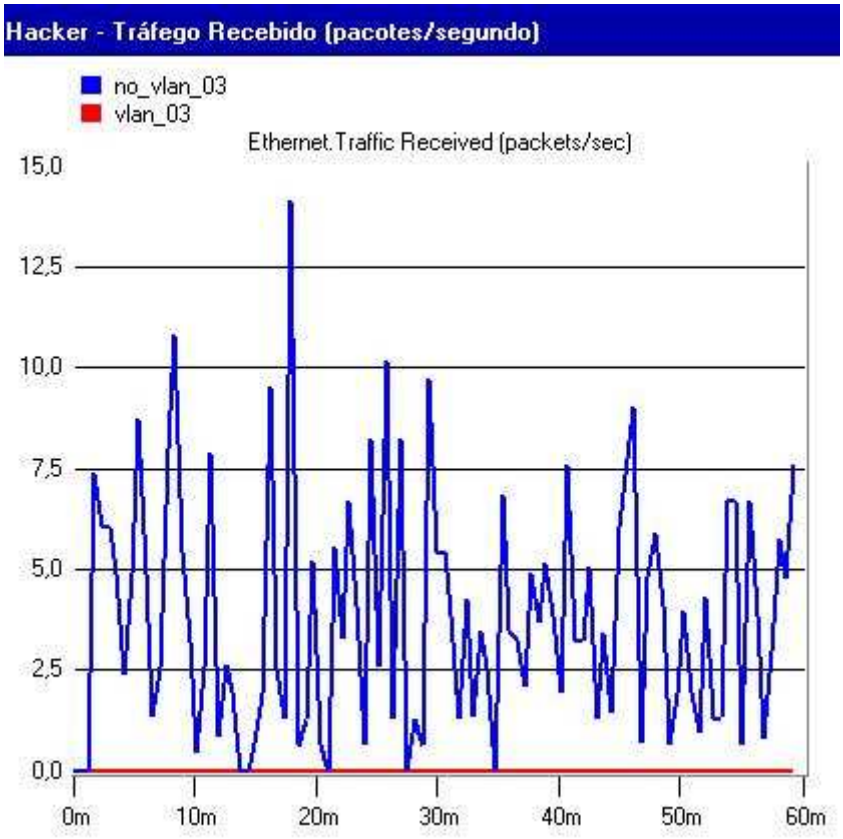

Figura 5.11: Gráfico do tráfego recebido pelo *Hacker* nos Cenários c.1 e c.2.

A Tabela 5.6 mostra as informações do tráfego recebido pelo *Hacker* nas situações em que a rede não contava com segmentação virtual (Cenário c.1) e após a implantação das VLAN (Cenário c.2).

Tabela 5.6: Tráfegos recebidos pelo *Hacker* dos Cenários c.1 e c.2.

Dispositivo	Cenário	Tráfego recebido em pacotes/segundo		
		Mínimo	Médio	Máximo
Hacker	c.1	0	3,8	14,1
	c.2	0	0	0

Em consequência do uso de VLANs na rede, houve também uma redução da carga de informações nos servidores utilizados, em média de 75%. A Tabela 5.7 mostra os dados da carga nos servidores nos Cenários c.1 e c.2, sem segmentação virtual e utilizando VLANs, respectivamente.

Tabela 5.7: Carga nos servidores dos Cenários c.1 e c.2.

Servidores	Cenários	Carga nos servidores em pacotes/segundo		
		Mínima	Média	Máxima
Banco de Bados	c.1	0	31,3	42,6
	c.2	0	7,27	12,8
WEB	c.1	0	1,8	10,5
	c.2	0	0,79	5,3
FTP	c.1	0	0,9	4,7
	c.2	0	0,39	2,7
E-mail	c.1	0	0,8	6,1
	c.2	0	0,4	3,2
Print	c.1	0	0	0,4
	c.2	0	0	0

Os últimos cenários, d.1 e d.2, que serão analisados a seguir, possuem um roteador ligando duas sub-redes que, por sua vez, possuem *switches* como nós centrais.

5.4 Cenários d.1 e d.2

Os cenários a serem analisados neste seção consistem de duas sub-redes conectadas por meio de um roteador Cisco 4700. Da mesma forma que nos cenários já analisados, a segmentação através de VLANs se mostrou um método que beneficia o desempenho da rede, eliminando tráfego desnecessário.

A Figura 5.12 mostra o gráfico do tráfego recebido pelo *Switch* 1 nos casos em que a rede contava ou não com segmentação virtual.

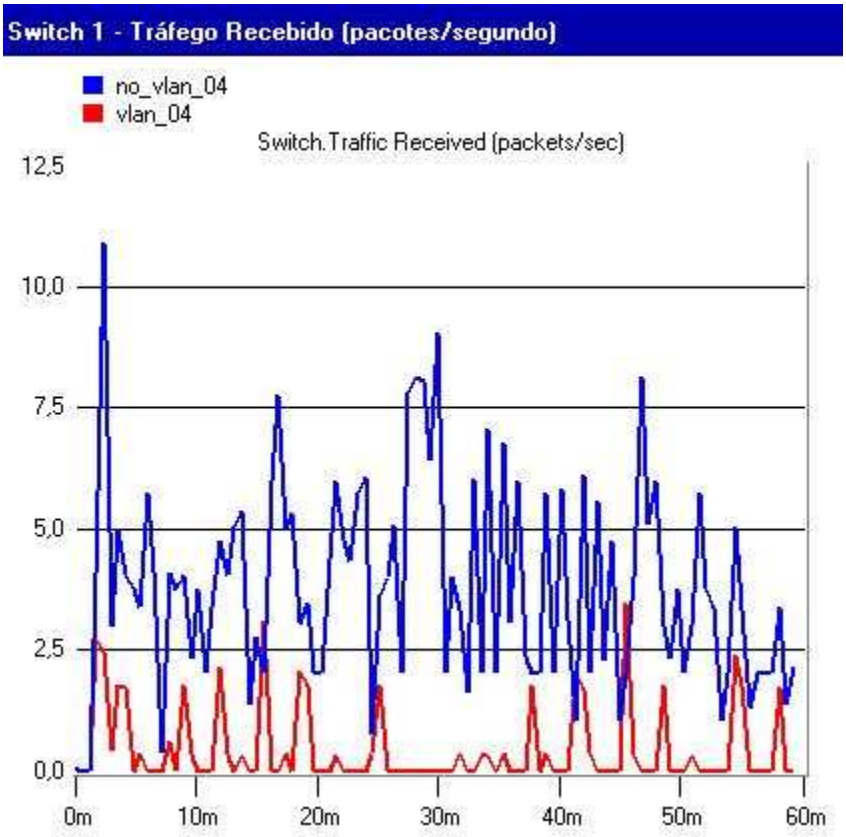

Figura 5.12: Tráfego recebido pelo *Switch* 1 nos Cenários d.1 e d.2.

Assim como no *Switch* 1, a utilização de VLANs também eliminou o tráfego desnecessário que seria tratado pelo *Switch* 2, conforme mostra a Figura 5.13.

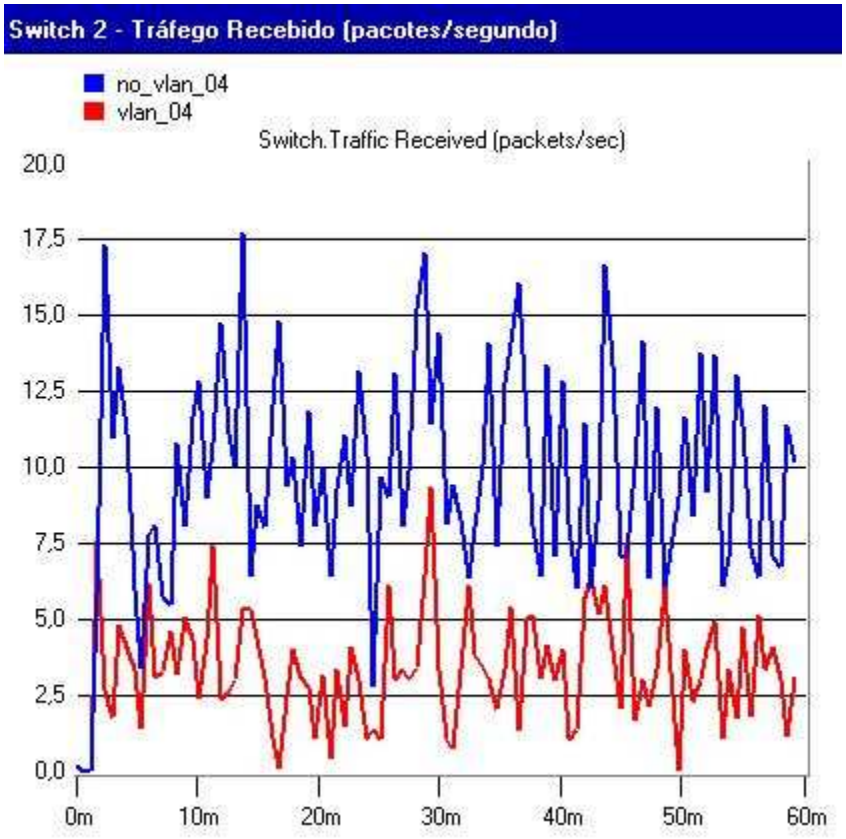

Figura 5.13: Tráfego recebido pelo *Switch* 2 nos Cenários d.1 e d.2.

Como esperado, o Switch 3 também se beneficiou da implantação de VLANs na rede. O gráfico da Figura 5.14 indica redução significativa no tráfego a ser tratado pelo *Switch* 3.

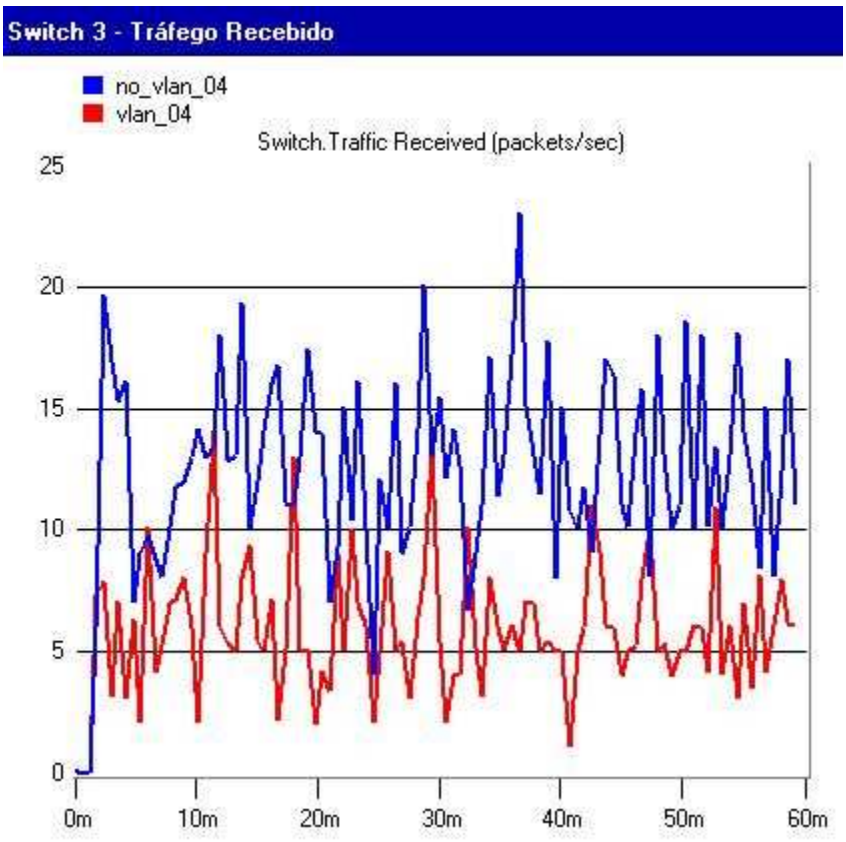

Figura 5.14: Tráfego recebido pelo *Switch* 3 nos Cenários d.1 e d.2.

Com os dados da Tabela 5.8, referente aos tráfegos recebidos pelos *Switches* 1, 2 e 3 dos Cenários d.1 e d.2, constata-se uma redução média do tráfego de 64%, chegando a mais de 88% no *Switch* 1.

Tabela 5.8: Tráfegos recebidos pelos *Switches* 1, 2 e 3 dos Cenários d.1 e d.2.

Dispositivo	Cenário	Tráfego recebido em pacotes/segundo		
		Mínimo	Médio	Máximo
Switch 1	d.1	0	3,8	10,9
	d.2	0	0,44	3,4
Switch 2	d.1	0	9,7	17,7
	d.2	0	3,33	9,4
Switch 3	d.1	0	12,5	23,1
	d.2	0	5,83	14,4

O roteador, mesmo sem participação direta nas VLANs, também teve seu tráfego reduzido. O gráfico da Figura 5.15 mostra o *throughput* do *Switch* 1 para o roteador, nas situações em que a rede estava ou não virtualmente segmentada.

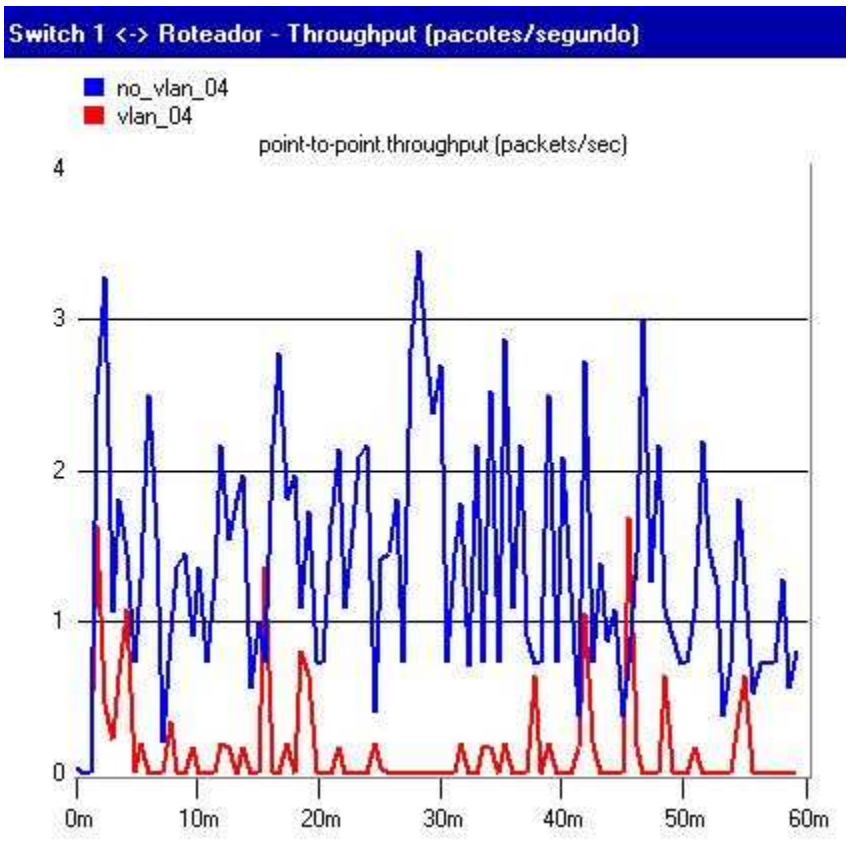

Figura 5.15: *Throughput* do *Switch* 1 para o roteador nos Cenários d.1 e d.2.

O gráfico da Figura 5.16 mostra o *throughput* do roteador para o *Switch* 1. Da mesma forma que o gráfico anterior, este indica redução de tráfego a ser processado pelo roteador da rede.

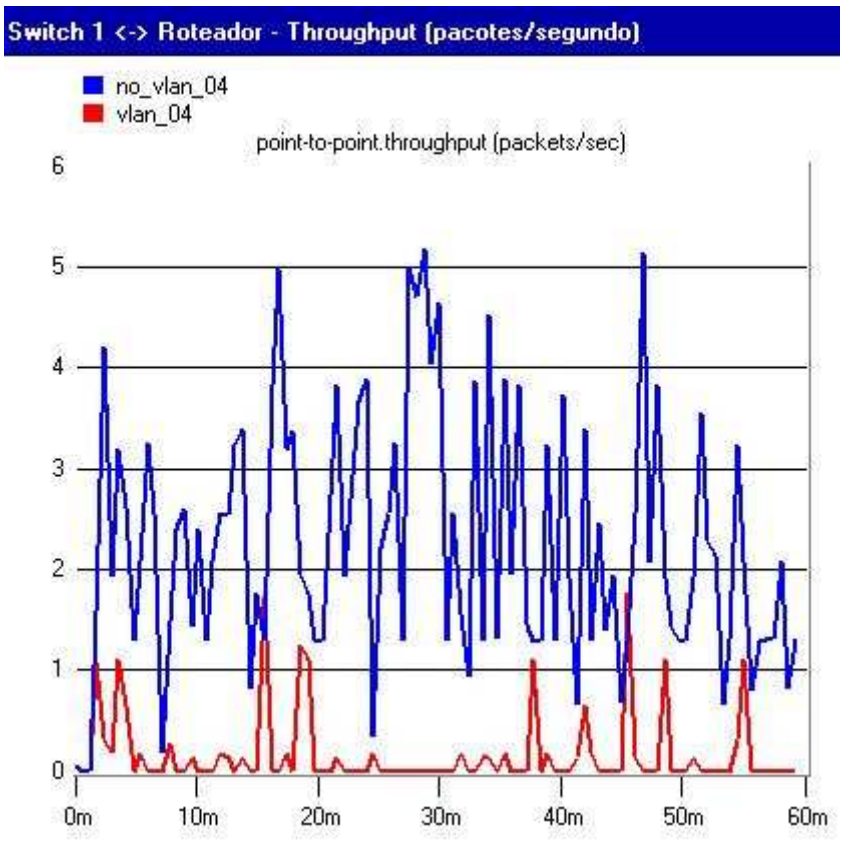

Figura 5.16: *Throughput* do roteador para o *Switch* 1 nos Cenários d.1 e d.2.

A partir dos dados da Tabela 5.9 é possível constatar uma redução média de tráfego entre o *Switch* 1 e o roteador de aproximadamente 83%. Este nível de redução de tráfego desnecessário também pode ser observada no *throughput* entre o roteador e o *Switch* 2.

Tabela 5.9: *Throughput* entre Roteador Cisco 4700 e Switch 1 dos Cenários d.1 e d.2.

Throughput	Cenário	Throughput em pacotes/segundo		
		Mínimo	Médio	Máximo
Switch 1 para Roteador	d.1	0	1,38	3,4
	d.2	0	0,15	1,69
Roteador para *Switch* 1	d.1	0	2,25	5,2
	d.2	0	0,16	1,75

Após a utilização de VLANs na rede de computadores dos cenários em análise, os servidores também obtiveram redução da carga de utilização, que foi próxima de 48%. A Tabela 5.10 mostra os dados da carga nos servidores nos Cenários d.1 e d.2.

Tabela 5.10: Carga nos servidores dos Cenários d.1 e d.2.

Servidores	Cenários	Carga nos servidores em pacotes/segundo		
		Mínima	Média	Máxima
Banco de Bados	d.1	0	7,76	14,8
	d.2	0	3,69	9,03
FTP	d.1	0	0,28	2,8
	d.2	0	0,16	1,69
E-mail	d.1	0	0,12	0,6
	d.2	0	0,11	0,75

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

Capítulo 6

CONCLUSÕES E TRABALHOS FUTUROS

Este capítulo apresenta as conclusões sobre os efeitos do uso de *Virtual Local Area Network* nas diferentes modelagens de redes de computadores analisadas. A utilização de VLANs demonstrou ser eficiente em relação ao controle de tráfego de *broadcast*, à possibilidade de segmentação lógica da rede, à redução de custos com reestruturações físicas e aquisições de novos equipamentos, à maior facilidade de gerenciamento, à independência da topologia física e à maior segurança.

6.1 Conclusões sobre a utilização de VLANs

Com base nas simulações realizadas, foi possível constatar que grande parte de todo o tráfego gerado nas redes de computadores é desnecessário. No entanto, a partir da utilização de VLANs como forma de segmentação lógica das redes, o tráfego total da rede sofreu significativa redução, aproximando-se, em algumas situações de 70%. No caso da comunicação entre roteador e *switch*, por exemplo,

a tráfego de dados diminui em até 83% do total na rede sem segmentação virtual. Isso foi possível, pois as VLANs tem a capacidade de reduzir o envio de pacotes para endereços diferentes do destinatário, aumentando a capacidade de toda a rede. Como cada VLAN pode ser associada a um departamento ou grupo de trabalho, é possível a realização de uma segmentação lógica da rede. Isso implica em melhorias para o controle do tráfego de *broadcast* e permite um melhor e mais fácil gerenciamento da rede. Em redes de computadores com VLANs, foi observado que, a adição ou movimentação de usuários pode ser feita de maneira remota pelo administrador, sem que sejam necessárias alterações na infraestrutura física da rede, proporcionando grande flexibilidade. Como foi observado durante a análise dos resultados, em alguns casos, é necessário um menor número de equipamentos em redes com VLANs do que nas tradicionais. Essa técnica de segmentação evita ainda a necessidade de uso de roteadores, diminuindo ainda mais os custos. Conforme comprovado durante a modelagem dos cenários, as VLANs proporcionam independência da topologia física da rede. Grupos de trabalho fisicamente isolados puderam ser conectados em um mesmo domínio de *broadcast* sem dificuldades. As simulações mostraram que a utilização de VLANs em redes de computadores as tornam mais seguras, pois o tráfego de uma VLAN não pode ser capturado por membros de outra (ainda que no mesmo *switch*) rede virtual. Mesmo quando intrusos tentaram utilizar a rede ou simplesmente gerar tráfego inútil, estes foram "ignorados" e não tiveram acesso a nenhum tipo de informação da rede. O tráfego desnecessário gerado foi descartado pelo *switch* não acarretando nenhum ônus ao desempenho da rede.

6.2 Trabalhos Futuros

Como trabalhos futuros pode-se apontar:

- Comparação da técnica de *VLAN Trunking* com o uso de *switches* nível 3 nas redes de computadores.
- Projetos utilizando o OPNET para testes e análises de novas topologias e modelos de redes.
- Análise de modelos a partir de outras métricas, como número de colisões, que não foi abordada por este trabalho devido à limitação da versão acadêmica do simulador OPNET.

Referências Bibliográficas

ALBERTI, A. M.; NETO, E. L. A.; MENDES, L. de S. Simulação de redes atm. In: XVII SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES. *Anais do XVII SBT*. Vila Velha, Brasil, 1999. p. 212–217.

CASTELLI, M. J. *LAN switching first-step*. 1. ed. Indianapolis, IN, USA: Cisco Press, 2004. 384 p. ISBN 1-58720-100-3.

CISCO SYSTEMS. *Cisco Understanding and Configuring VLAN Trunk Protocol (VTP) - Document ID: 10558*. [S.l.], 2002. Disponível em: <http://www.cisco.com/warp/public/473/21.pdf>.

CLARK, K.; HAMILTON, K. *Cisco LAN switching*. 1. ed. Indiana, IN, USA: Cisco Press, 1999. 926 p. ISBN 1-57870-094-9.

COMDISCO SYSTEMS, INC. *BONeS DESIGNER User's Guide. Version 2.5*. Foster City, CA, USA, 1993.

COMER, D. E. *Redes de Computadores e Internet*. 5. ed. São Paulo, SP: Artmed Editora SA., 2007. 720 p. ISBN 0-13-143351-2.

DOOLEY, K. *Designing Large-Scale LANs*. 1. ed. Sebastopol, CA, USA: O'Reilly Associates, Inc., 2002. 385 p. ISBN 0-596-00150-9.

FURUKAWA. *MF 102 Acessórios e Cabeamento para Redes*. 5. ed. [S.l.]: Furukawa Industrial S.A. Produtos Elétricos, 2004.

GIL, A. C. *Como elaborar projetos de pesquisa*. São Paulo, SP: Atlas, 1991. 159 p.

GNS3. *Graphical Network Simulator 3*. GNS3.net, 2009. Disponível em: <http://www.gns3.net/>.

GOLMIE, N.; KOENIG, A. *The NIST ATM Network Simulator, Operation and Programming. Version 1.0*. [S.l.], 1995.

HAMMANN, J. E.; MARKOVITCH, N. A. Introduction to Arena [simulation software]. In: *1995 Winter Simulation Conference (WSC'95)*. Arlington, VA, USA: [s.n.], 1995. p. 519–523. ISBN 0-7803-3018-8.

HUCABY, D. *CCNP Self-Study: CCNP BCMSN - Official Exam Certification Guide*. 4. ed. Indiana, IN, USA: Cisco Press, 2007. 598 p. ISBN 1-58720-171-2.

IEEE SOCIETY COMPUTER. IEEE Std 802.1Q. In: *IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks*. [S.l.: s.n.], 2006. p. 303. ISBN 0-7381-4877-6.

KENYON, T. *High-Performance Data Network Design: Design Techniques and Tools*. 1. ed. Daytona Beach, FL, USA: Digital Press, 2002. 926 p. ISBN 1-55558-207-9.

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a Internet: Uma abordagem top-down*. 3. ed. São Paulo, SP: Pearson Addison Wesley, 2007. 656 p. ISBN 978-85-88639-18-8.

LAW, A. M.; MCCOMAS, M. G. Simulation software for communications networks: The state of the art. *IEEE Communications Magazine*, p. 44–50, Março 1994.

MOLINARI, M. M. *Redes Virtuais: Tecnologias e Status da Padronização*. [S.l.], 2008. Disponível em: <http://lat.3com.com.br/>.

MUELLER, S.; OGLETREE, T. W. *Upgrading and Repairing Networks*. Indianapolis, IN, USA: Que Publishing, 2004. 1125 p. ISBN 0-7897-2817-6.

ODOM, S.; NOTTINGHAM, H. *Cisco Switching Black Book*. 1. ed. Scottsdale, AZ,USA: Coriolis Technology Press, 2000. 656 p. ISBN 157610706X.

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.

OSTERLOH, H. *IP Routing Primer Plus*. 1. ed. Indianapolis, IN, USA: Sams Publishing, 2001. 490 p. ISBN 0-672-32210-2.

PARSONS, G. Ethernet bridging architecture. *IEEE Communications Magazine*, p. 112–119, 2007.

SEIFERT, R.; EDWARDS, J. *The All-New Switch Book: The Complete Guide to LAN Switching Technology*. Indianapolis, IN, USA: Wiley Publishing, Inc., 2008. 816 p. ISBN 978-0-470-28715-6.

SHI, L.; SJöDIN, P. A VLAN Ethernet Backplane for Distributed. *IEEE Communications Magazine*, p. 42–45, 2007.

SIVABALAN, M.; MOUFTAH, H. T. QUARTS-II: A Routing Simulator for ATM Networks. *IEEE Communications Magazine*, p. 80,87, Maio 1998.

SPURGEON, C. E. *Ethernet: The Definitive Guide*. 1. ed. Sebastopol, CA, USA: O'Reilly Associates, Inc., 2000. 498 p. ISBN 1-56592-660-9.

SVENSSON, T.; POPESCU, A. *Development of laboratory exercises based on OPNET Modeler*. Dissertação (Mestrado) — Blekinge Institute of Technology, Junho 2003.

TANENBAUM, A. S. *Computer Networks*. 4. ed. Upper Saddle River, NJ, USA: Pearson Education, Inc., 2003. 891 p. ISBN 0-13-066102-3.

VELTE, T. J.; VELTE, A. T. *Cisco: A Beginner's Guide*. 4. ed. New York, NY, USA: McGraw-Hill Companies, 2005. 670 p. ISBN 0-07-226383-0.

ZAMBALDE, A. L.; PADUA, C. I. P. S.; ALVES, R. M. *O documento científico em Ciência da Computação e Sistemas de Informação*. Lavras, Minas Gerais: Notas de aula - rascunho, texto em construção sem revisão de português e citações, Departamento de Ciência da Computação, UFLA, 2008. 74 p.

ZHU, M.; MOLLE, M.; BRAHMAN, B. Design and implementation of application-based secure vlan. *Proceedings of the 29th Annual IEEE Internacional Conference on Local Computer Networks (LCN'04)*, 2004.