Redes Virtuais

Cecília L. Osório[1], Lucas G. Queiroz[1], Rafael A. de Andrade[1], Vitória V. de O. Freitas[1]

[1]Faculdade de Computação – Universidade Federal de Mato Grosso Sul (UFMS)
Caixa Postal 549 – 79.070-900 – Campo Grande – MS – Brazil

cecilialosorio@gmail.com, lucasgq71@gmail.com, acioli.rafael@gmail.com, vitoriafreita

Abstract. *This paper presents the general concept of Virtual Networks, an alternative to regular LANs that has many advantages. It describes many types: VLANs, VPNs and networks based on virtual devices. It describes their main features and uses.*

Resumo. *Este trabalho apresenta o conceito geral de Redes Virtuais, uma alternativa a LANs convencionais que possui diversas vantagens. São apresentados diversos tipos: VLANs, VPNs e redes baseadas em dispositivos virtuais. São descritas suas principais características e seus usos.*

1. Introdução

Redes Virtuais são redes de computadores que consistem, principalmente, de ligações lógicas. Um link de rede virtual é uma ligação que não consiste em uma conexão física (com ou sem fio) entre dois dispositivos de computação, mas sim numa implementação usando métodos de virtualização de rede.

As duas formas mais comuns de virtualização de rede são as redes virtuais baseadas em protocolo (VLANs, VPNs e VPLSs) e as redes virtuais baseadas em dispositivos virtuais (como as redes que ligam as máquinas virtuais dentro de um $hypervisor$). Na prática, as duas formas podem até ser utilizadas em conjunto. Neste artigo abordaremos estas quatro tecnologias de virtualização de redes de computadores.

2. LAN - Local Area Network

A Local Area Network (LAN) é uma rede do tipo local, que ocupa uma área geográfica limitada, geralmente um prédio ou um campus. As LANs costumam ser utilizadas para conectar computadores numa organização com o propósito de compartilhar recursos. Administradores de rede gostam de agrupar os usuários em LANs que refletem sua estrutura organizacional. Isso pode ser feito por diversos motivos, alguns deles são:

- Segurança: numa empresa, por exemplo, uma LAN pode guardar os dados com acesso público enquanto outra guarda os dados privados.
- Carga: uma operação realizada pelo grupo usuário de uma LAN pode deixar a rede sobrecarregada enquanto outro grupo, em outra LAN, pode utilizar a rede para outra operação.
- Tráfico de $broadcast$: se houver uma LAN contendo todos os participantes de um grupo de $broadcast$, enviar uma mensagem de $broadcast$ a esse grupo equivale a enviar uma mensagem para toda a LAN. É logico que, se a LAN for muito grande, o $broadcast$ fica muito caro.

No intuito de solucionar este e outros problemas, foram criadas as redes virtuais. [Tanenbaum et al. 2003]

3. Redes virtuais

O presente trabalho apresenta e explica quatro tipos de tecnologias de redes virtuais existentes: VLAN, VPN, VPLS e redes virtuais baseadas em dispositivos virtuais.

3.1. VLAN - Virtual Local Area Network

As Virtual Local Area Networks surgiram como resposta a um recorrente problema estrtural das LANs. Tal problema pode ser ilustrado no seguinte exemplo:

No prédio de uma empresa ou organização, dez estações, ou computadores, estão agrupados em três LANs, cada uma numa sala, interconectadas por um $switch$. As estações de cada grupo de máquinas estão ligadas entre si enquanto cada grupo está fisicamente separado do outro, como ilustrado na seguinte figura:

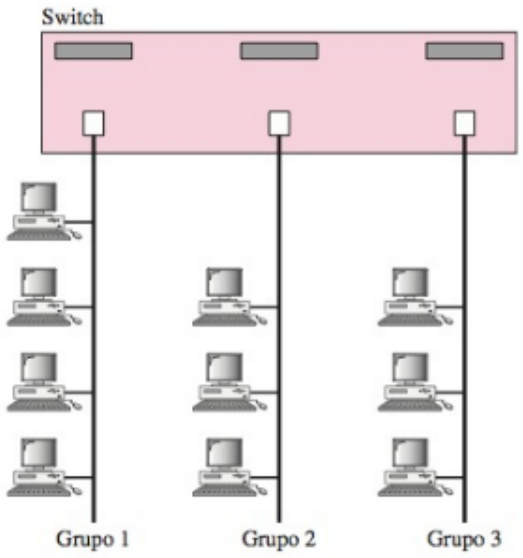

Figura 1. Ilustração de três LANs conectadas por um $switch$

Em tal configuração, se um funcionário do Grupo 1 for escolhido para participar de um projeto do Grupo 2 e, portanto, precisar ser transferido para a sala deste, a sua estação também deverá ser transferida para o Grupo 2. Essa mudança exigirá alteração na configuração física da rede, pois o técnico de rede terá que refazer a ligação dos computadores. Essa é uma operação custosa e terá que ser repetida toda vez que um funcionário migrar para outro grupo.

A solução para esse problema surgiu com a criação das VLANs. Numa VLAN, os computadores são divididos em grupos lógicos, e não físicos. Uma LAN pode ser dividida em várias LANs que passam a ser chamadas de VLANs. No exemplo, cada VLAN continuará sendo um grupo de trabalho, mas eles já não estarão necessariamente em salas separadas.

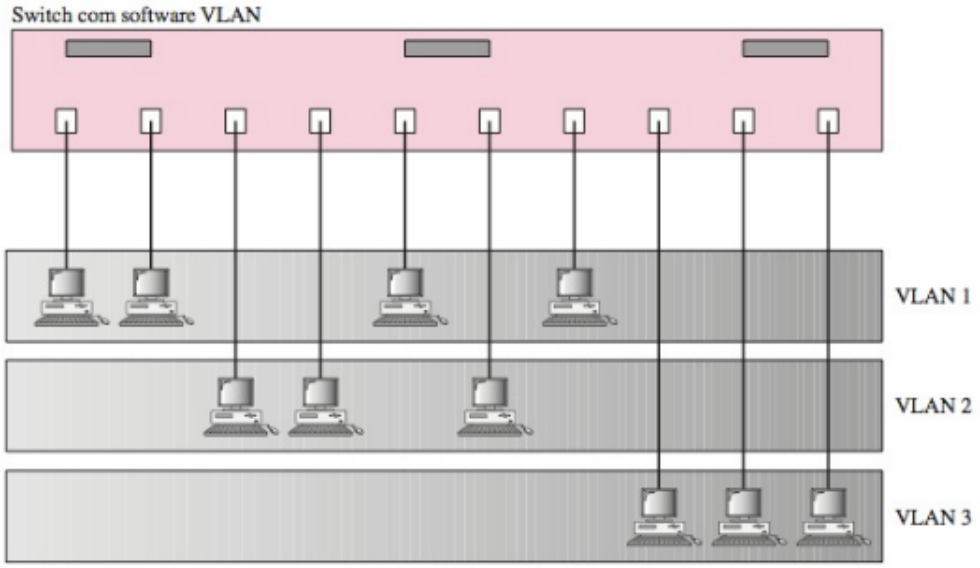

Figura 2. Ilustração de três VLANs construídas sobre uma única LAN

Se um funcionário precisar trocar de grupo, não será preciso trocar a sala de seu computador, ou seja, a configuração física da rede não terá que ser alterada. Na VLAN, a participação do computador em um grupo é definida pelo software, e não pelo hardware, então basta mover o computador logicamente para outra VLAN. [Tanenbaum et al. 2003]

Uma VLAN pode ser definida das seguintes diferentes formas, ou por combinações delas:

- Endereço (número) de porta: pode-se definir, por exemplo, que as portas 1, 3 e 4 pertencem à VLAN 1 e as 2, 5 e 6 pertencem à VLAN 2.
- MAC Address: pode-se definir, por exemplo, que estações com os endereços MAC E21342A12334 e F2A123BCD341 pertençam à VLAN 1.
- Endereço IP: pode-se definir, por exemplo, que as estações com os endereços IP 181.34.23.67, 181.34.23.72, 181.34.23.98 e 181.34.23.112 pertençam à VLAN 1.
- Endereço IP de multicast: o endereço de multicast define a qual VLAN a máquina pertence.

Para se configurar uma VLAN, existem três formas. Na **configuração automática**, as estações são automaticamente conectadas (e desconectadas) a uma VLAN seguindo um critério definido pelo administrador. Se o critério for, por exemplo, o número do projeto em que um funcionário está trabalhando e este repentinamente mudar de projeto, sua estação será automaticamente migrada para a VLAN correspondente ao novo projeto. Na **configuração manual**, o administrador de sistema seta manualmente (digita uma por uma) num software as portas ou demais características que definem a qual VLAN cada estação pertence, e qualquer migração ocorrida posteriormente também é feita de forma manual. Existe também a **configuração semi-automática**, na qual geralmente a inicialização é manual e as migrações são automáticas.

O uso de VLANs permite a criação de grupos de *broadcast* com custo e tempo reduzidos quando comparado ao uso de uma LAN convencional. Além disso, também traz uma segurança a mais para os grupos criados. [Forouzan and Mukhopadhyay 2011]

3.2. VPN - Virtual Private Network

A tecnologia VPN também faz frente a um problema estrutural, dessa vez concernente à segurança. Imagina-se o dono de uma empresa com vários escritórios espalhados pelo mundo. Como ele os interligaria de modo a garantir a segurança e a privacidade das informações? Dentre as possibilidade algumas seriam: lançar satélites próprios, pagar por uma rede física privada ou utilizar uma VPN.

Uma rede privada é desenvolvida para uso interno em uma organização. Ela possibilita acesso a recursos compartilhados e, ao mesmo tempo, fornece privacidade. Existem dois termos que estão comumente relacionados às redes privadas:

- **Intranet**: uma rede privada que usa o modelo Internet mas possui acesso limitado aos usuários dentro da organização.
- **Extranet**: o mesmo que intranet, mas alguns recursos estão disponíveis para grupos específicos fora da organização, sob controle do administrador de redes.

Para se obter privacidade de informações, as organizações podem usar umas das seguintes estratégias:

1. **Redes privadas**: organizações podem interligar suas LANs através de linhas alugadas e roteadores, assim criando sua própria internet. Não há acesso a redes externas.
2. **Redes Híbridas**: permite às empresas trocar dados entre si e ainda manter a conexão com a Internet global, fator necessário para a maioria das organizações.
3. **Redes Privadas Virtuais**: criadas como forma de garantir conexão interna e externa solucionando um problema gerado pelas duas alternativas anteriores: o custo.

A Rede Privada Virtual (VPN) utiliza uma infraestrutura pública, como a Internet global por exemplo, ou compartilhada para criar conexões privadas, oferecendo funcionalidade, segurança e gestão. Além disso, a VPN oferece, como ilustrado na figura a seguir, transparência de conexão, dando ao usuário, ou à estação, a sensação de estar conectado apenas a uma rede interna, como uma LAN, e não à Internet.

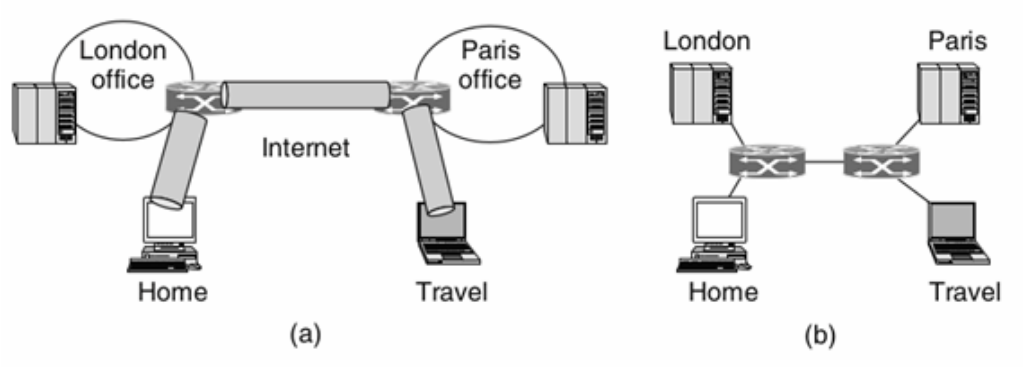

Figura 3. (a) Uma rede privada virtual. (b) Como a topologia é vista

3.2.1. Tecnologia VPN - IPSec

O IPSec (IP Security) é um conjunto de protocolos desenvolvido pela Internet Engineering Task Force (IETF) para ofercer segurança a um pacote no nível de rede. O IPSec ajuda a

criar pacotes confidenciais e autenticados para a camada IP, conforme mostrado na figura a seguir:

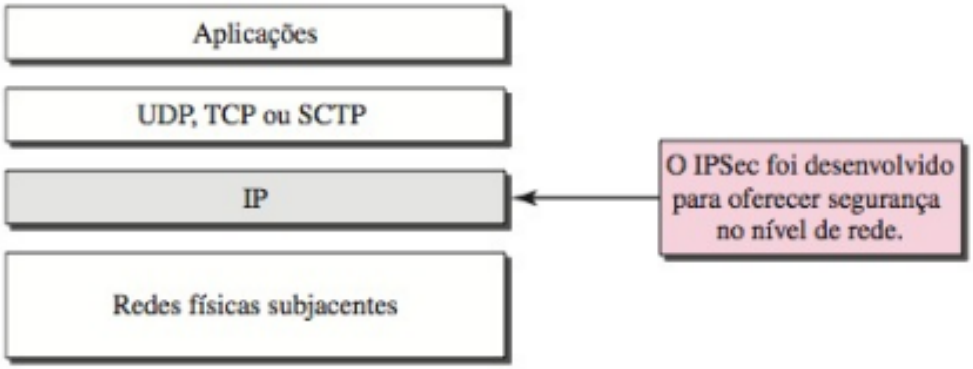

Figura 4. O IPSec é implementado na camada IP

O conjunto IPSec pode operar em um dos dois modos distintos: o modo de transporte ou o modo túnel, como mostrado na figura seguinte.

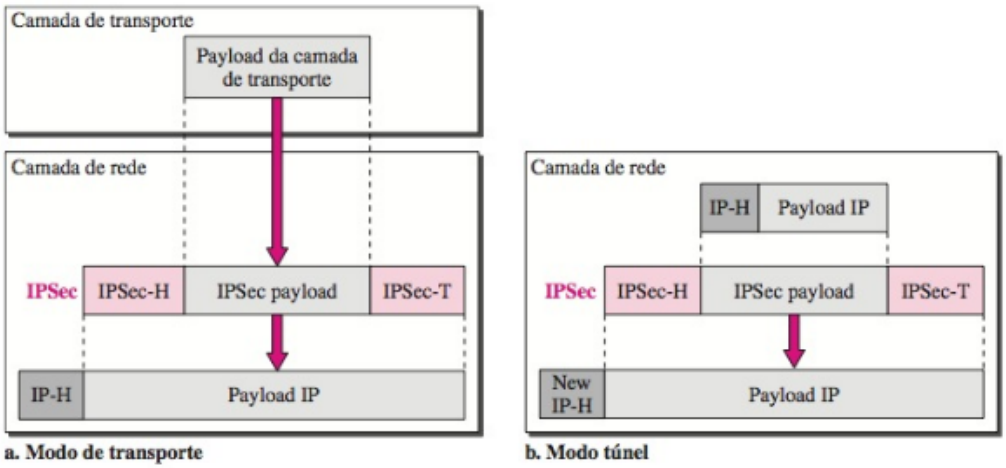

Figura 5. Modos de trabalho do IPSec

A tecnologia VPN usa IPSec no modo túnel para fornecer autenticação, integridade e privacidade. Nesse modo, cada datagrama IP destinado ao uso privado na organização é encapsulado em outro datagrama. A figura a seguir demonstra o processo de tunelamento:

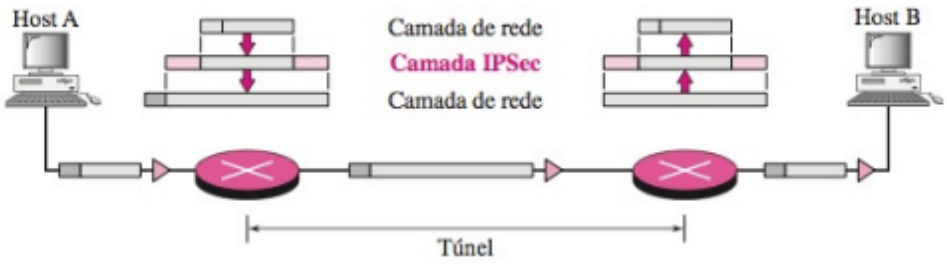

Figura 6. Processo de tunelamento

Uma rede privada que usa o modelo Internet deve utilizar endereços IP. Sendo assim, existem três opções para determinar os endereços a se utilizar. A primeira é solicitar endereços das autoridades Internet e usá-los sem estar conectada à Internet. Assim, se a empresa decidir se conectar à Internet no futuro, não terá tantos problemas. A segunda forma consiste em usar qualquer endereço da Internet sem solicitar às autoridades da Internet, o que pode causar confusão ao acessar os endereços. E uma terceira opção é usar endereços reservados (10/8, 172.16/12 ou 192.168/16).

Para empregar IPSec no tunelamento, as VPNs precisam usar dois conjuntos de endereçamento, como mostrado a seguir:

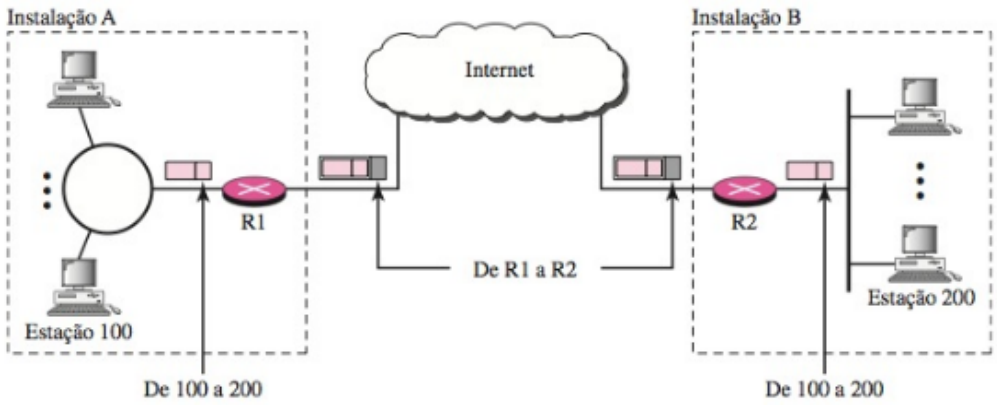

Figura 7. Endereçamento de uma VPN.

[Richardson et al. 1998]

3.3. VPLS - Virtual Private LAN Service

O VPLS, ou Virtual Private LAN Service, é usado para emular uma rede local sobre uma rede MPLS (Multiprotocol Label Switching), usando PWs (pseudowires). O MPLS facilita a implantação e o gerenciamento de redes privadas virtuais (VPNs). Ou seja, O VPLS torna possível aos clientes criar uma rede lógica de área local (estrutura de LAN) entre locais geograficamente separados. Todos os serviços em um VPLS parecem estar na mesma rede local, independentemente da localização.

Ao contrário da tradicional WAN ou das Redes Virtuais Privadas (VPN) baseadas

em IP, um VPLS pode ser usado para transportar o tráfego não-IP, sem necessidade de conversão ou encapsulamento.

Um VPLS tem topologia de rede do tipo malha, o que significa que pode fornecer serviços ponto-a-ponto, multiponto e *broadcast*. O VPLS cria uma Ethernet virtualizada na borda do prestador de serviços, ligando vários locais remotos como se estivessem no mesmo *switch* físico.[3.3]

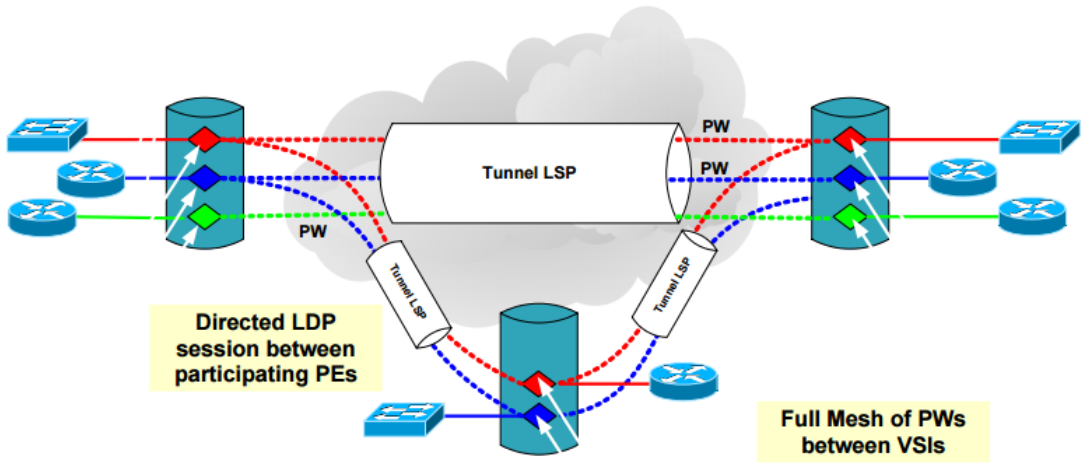

Figura 8. Rede VPLS implementando PWs e VSs.

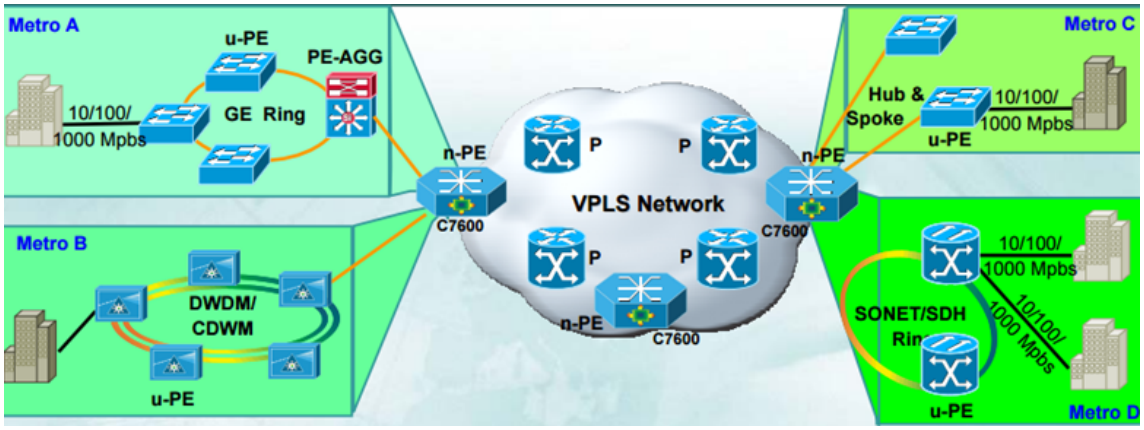

Figura 9. Visão geral de uma implementação de VPLS.

[Sugerman et al. 2001]

3.4. Redes virtuais baseadas em dispositivos virtuais

Uma rede virtual baseada em dispositivos virtuais possui as mesmas características de uma rede com máquinas físicas, porém utiliza máquinas virtuais. É possível construir redes complexas com apenas um único *host* ou vários *hosts*. Esse tipo de rede é útil para implementações de produção ou para fins de desenvolvimento e testes.

Essas redes virtuais possuem dois componentes chaves: adaptadores Ethernet virtuais, utilizados por determinadas máquinas virtuais; e *switches* virtuais, que ligam as

máquinas virtuais e o console de serviço ESX Server para redes externas. *Switches* virtuais permitem que máquinas virtuais no mesmo host ESX Server possam se comunicar umas com as outras usando os mesmos protocolos que seriam utilizados em *switches* físicos, sem a necessidade de hardware de rede adicional. O *switches* virtuais ESX Server também suportam VLANs que são compatíveis com implementações de VLAN padrão.

Uma máquina virtual pode ser configurada com um ou mais adaptadores virtuais Ethernet, cada um tendo seu próprio endereço IP e seu endereço MAC. Como resultado, as máquinas virtuais têm a mesma propriedades de máquinas físicas do ponto de vista de rede.

O controle da rede é centralizado, o que reduz o custo e a complexidade de operação e manutenção de hardware e software, se comparado com a administração de numerosos dispositivos separados em diversas localizações. A figura a seguir ilustra a estrutura desse tipo de rede virtual.

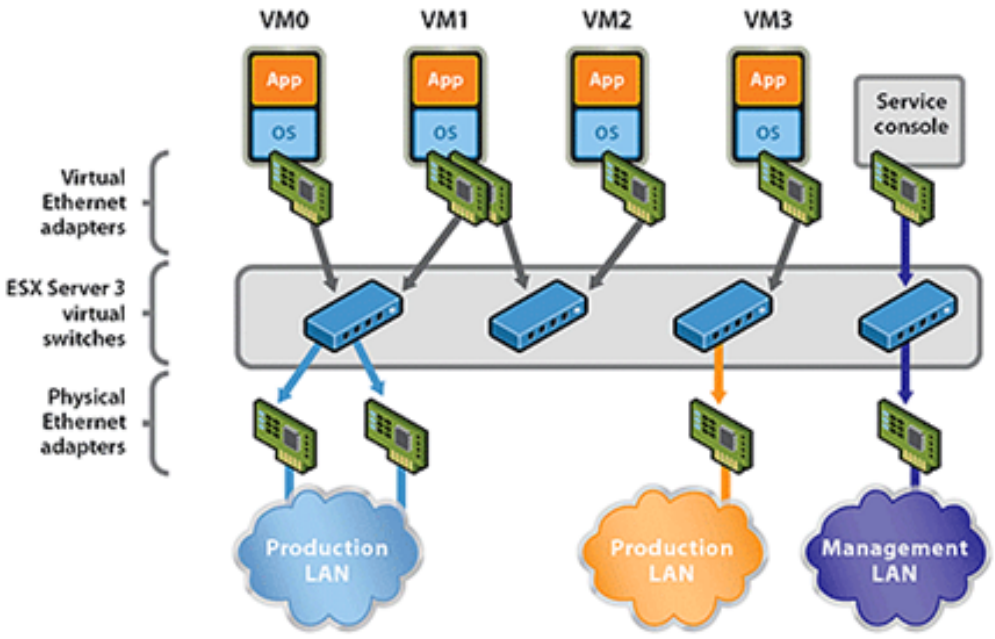

Figura 10. Estrutura de uma rede virtual com maquinas virtuais.

Apesar das muitas vantagens oferecidas por essa tecnologia, uma rede virtual baseada em dispositivos virtuais possui limitações, e a principal delas é o fato de certos problemas serem possíveis de ser solucionados apenas através do contato físico com o hardware envolvido. [Rosenblum 1999]

4. Conclusão

Este artigo apresentou o conceito de redes virtuais e alguns de seus tipos: VLANs, VPNs, VPLSs e redes virtuais baseadas em dispositivos virtuais. As redes virtuais foram concebidas para expandir as capacidades das redes físicas a partir do ponto em que estas não conseguiam mais crescer sem acarretar numa série de complicações.

A tecnologia VLAN, que pode ser considerada com um dos tipos mais básicos de rede virtual, fornece praticidade de mudança de configuração de rede a grandes ou pequenas organizações usuárias de redes internas. Enquanto isso, os tipos de rede virtual VPN e VPLS geram formas baratas e seguras de se transmitir informações privadas por redes em longas distâncias, mantendo ao usuário a impressão de que a máquina com a qual se comunica está na sala ao lado, e não na cidade vizinha. Por fim, as redes virtuais baseadas em dispositivos virtuais transcendem as redes físicas com ligações e aparelhos concretos, ampliando não só o alcance como a concepção de uma rede.

A evolução gerada pelas redes virtuais tende, portanto, a se tornar cada vez maior e mais expressiva, não se pode ainda traçar os limites dessa tecnologia.

Referências

Forouzan, B. A. and Mukhopadhyay, D. (2011). *Cryptography and Network Security (Sie)*. McGraw-Hill Education.

Muller, S., Yeung, L., and Hendel, A. (2000). Distributed vlan mechanism for packet field replacement in a multi-layered switched network element using a control field/signal for indicating modification of a packet with a database search engine. US Patent 6,128,666.

Richardson, T., Stafford-Fraser, Q., Wood, K. R., and Hopper, A. (1998). Virtual network computing. *IEEE Internet Computing*, 2(1):33–38.

Rosenblum, M. (1999). Vmware's virtual platform™. In *Proceedings of hot chips*, volume 1999, pages 185–196.

Sugerman, J., Venkitachalam, G., and Lim, B.-H. (2001). Virtualizing i/o devices on vmware workstation's hosted virtual machine monitor. In *USENIX Annual Technical Conference, General Track*, pages 1–14.

Tanenbaum, A. S. et al. (2003). Computer networks, 4-th edition. *ed: Prentice Hall*.

Waldspurger, C. A. (2002). Memory resource management in vmware esx server. *ACM SIGOPS Operating Systems Review*, 36(SI):181–194.