CARLOS EDUARDO RIBAS

REDES DEFINIDAS POR SOFTWARE EM AMBIENTES ACADÊMICOS

Monografia apresentada ao PECE - Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para conclusão do curso de MBA em Tecnologia de Software.

São Paulo
2014

CARLOS EDUARDO RIBAS

REDES DEFINIDAS POR SOFTWARE EM AMBIENTES ACADÊMICOS

Monografia apresentada ao PECE - Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para conclusão do curso de MBA em Tecnologia de Software.

Área de Concentração: Tecnologia de Software

Orientador: Prof. Dr. Edson Gomi.

São Paulo

2014

DEDICATÓRIA

À minha família. Em especial para minha linda esposa Laila Massad Ribas e para a minha filha Isabela Massad Ribas. Amo vocês!

RESUMO

Com mais de um bilhão de usuários no mundo, a Internet se tornou uma infraestrutura essencial para a comunicação. Contudo, a atual arquitetura da internet enfrenta uma série de desafios relacionados com a segurança, escalabilidade, mobilidade, desempenho, etc. As universidades possuem hoje um dos ambientes mais desafiadores para a Tecnologia da Informação (TI), graças as pesquisas realizadas em grandes parcerias envolvendo professores, pesquisadores e estudantes do mundo inteiro. Redes Definidas por Software, em inglês *Software Defined Networking* (SDN), foram desenvolvidas para contornar as limitações das redes tradicionais. SDN oferece um novo paradigma para resolver os desafios existentes e ainda permite a inovação através da programação da rede. O conceito básico por trás de SDN é tirar a inteligência dos switches e roteadores e transferi-lo para um controlador ou para conjunto de controladores. Isto é feito com a dissociação do sistema que toma as decisões sobre onde o tráfego deve ser enviado (plano de controle) dos sistemas que encaminham o tráfego para o destino selecionado (plano de dados). Este estudo apresenta uma revisão de literatura sobre redes de computadores e sobre à Internet para compreender como elas funcionam e quais são as suas limitações. Em seguida, serão apresentados os conceitos de SDN e Openflow, será realizado uma comparação entre SDN e as redes tradicionais e será mostrado os prós e contras do uso de SDN em um ambiente acadêmico.

ABSTRACT

With more than one billion users worldwide, the Internet has become an essential communication infrastructure. However, current internet architecture is facing a number of challenges related to security, scalability, mobility, performance, etc. Universities are some of the most challenging Information Technology (IT) environments especially due to research conducted in large collaborative partnerships involving faculty, researchers and students worldwide. Software Defined Networking (SDN) was developed to solve the problems from the traditional network. SDN provides a new paradigm to solve many existing challenges and allows innovation through network programmability. The basic concept behind SDN is take off the network intelligence from switches and routers and shift it to a centralized controller or set of controllers. This is done by decoupling the system that makes decisions about where traffic is sent (the control plane) from the systems that forward traffic to the selected destination (the data plane). This study presents a literature review about computer networking and the Internet to understand how it works and what its limitations are. Then we present the concepts of SDN and Openflow and compare SDN with the traditional networks and show pros and cons of using SDN in an academic environment.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANSP	Rede acadêmica de São Paulo (*Academic Network at São Paulo*)
API	Interface de programação de aplicativos (*Application Programming Interfaces*)
ARPANet	*Advanced Research Projects Agency Network*
AT&T	*American Telephone and Telegraph*
BEEP	*Blocks Extensible Exchange Protocol*
BYOD	Traga o seu próprio dispositivo (*Bring Your Own Device*)
CapEx	Despesas de capital (*Capital Expenditure*)
CIDR	*Classless Inter-Domain Routing*
CLI	Interface de linha de comando (*Command Line Interface*)
CPU	Unidade central de processamento (*Central Processing Unit*)
DMZ	Zona desmilitarizada (*DeMilitarized Zone*)
DWDM	*Dense Wavelength Division Multiplexing*
ERP	*Enterprise Resource Planning*
ForCES	*Forwarding and Control Element Separation*
GB	*Gigabyte*
Gbps	Gigabits por segundo (*Gigabits per second*)
GHz	*Gigahertz*
GSMP	*Genaral Switch Management Protocol*
IANA	*Internet Assigned Numbers Authority*
IDS	Sistemas de detecção de intrusão (*Intrusion Detection System*)
IETF	*Internet Engineering Task Force*
IMS	*IP Multimedia Systems*
IP	Protocolo de internet (*Internet Protocol*)
IPv4	Protocolo de internet versão 4 (*Internet Protocol version 4*)
IPv6	Protocolo de internet versão 6 (*Internet Protocol version 6*)
IPTO	*Information Processing Techniques Office*
ISP	Provedores de serviço de internet (*Internet Service Provider*)
MAC	Endereço de controle de acesso (*Media Access Control*)
NAT	Tradução de endereços de rede (*Network Address Translation*)
NFV	Virtualização de Funções de Rede (*Network Functions Virtualization*)
NVGRE	*Network Virtualization using Generic Routing Encapsulation*
ONF	*Open Networking Foundation*

OpEx	Despesas operacionais (*Operational Expenditure*)
OSI	Interconexão de Sistemas Abertos (*Open Systems Interconnection*)
PC	Computador pessoal (*Personal Computer*)
PCE	*Path Computation Element*
QoS	Qualidade de serviço (*Quality of Service*)
RFC	*Request for Comments*
SAP	Ponto de acesso ao serviço (*Service Access Point*)
SDN	Redes definidas por software (*Software Defined Networking*)
SO	Sistema Operacinal
SOAP	Protocolo simples de acesso a objetos (*Simple Object Access Protocol*)
SSL	Protocolo de Camada de Sockets Segura (*Secure Socket Layer*)
STD	Padrão de Internet (*Internet Standard*)
TB	*Terabyte*
TCP	Protocolo de controle de transmissão (*Transmission Control Protocol*)
TDM	Multiplexação por divisão de tempo (*Time Division Multiplex*)
TI	Tecnologia da Informação
TLS	Segurança da Camada de Transporte (*Transport Layer Security*)
TTL	Tempo de vida *Time To Live*
VLAN	Rede local virtual (*Virtual Local Area Network*)
VNS	Serviço de rede virtual (*Virtual Network Service*)
VM	Máquina virtual (*Virtual Machine*)
VMM	Monitor de máquina virtual (*Virtual Machine Monitor*)
VPN	Rede privada virtual (*Virtual Private Network*)
VXLAN	*Virtual Extensible LAN*

SUMÁRIO

INTRODUÇÃO

Desde o surgimento das redes de computadores, que ocorreu no final da década de 60 e início da década de 70, até os dias atuais, não houveram grandes mudanças na forma como as redes funcionam. Equipamentos de rede como roteadores e switches continuam desempenhando seus papéis de leitura de endereço e transferência de pacotes para sistemas adjacentes.

As redes de computadores necessitam de estudos nas mais diversas áreas, tais como: segurança, consumo de energia, confiabilidade, escalabilidade e desempenho. Entretanto, muitos cientistas de rede não conseguem colocar em prática seus experimentos porque tem sido impossível testá-los em grande escala. Switches e roteadores do núcleo da internet, comumente chamados de roteadores de *core*, são fechados e fazem uso de programas proprietários.

As mesmas razões que tornaram possível o surgimento e o sucesso da Internet são hoje considerados uma barreira para o seu desenvolvimento. Para contornar este problema, as Redes Definidas por Software (SDN - Software Defined Network), particularmente por meio do seu carro-chefe a tecnologia OpenFlow, estão sendo amplamente estudadas, para, assim, tornar possível o crescimento e a evolução da Internet.

SDN é um conceito que vem para modificar a forma como as redes de hoje funcionam, onde os equipamentos de rede decidem quais ações devem ser tomadas. SDN é baseado em um modelo onde todos os switches movem a sua capacidade de decisão para um elemento central. Foi deste conceito que surgiu o OpenFlow, que é a tecnologia SDN de maior sucesso atualmente. Ao separar as funções de comutação e de engenharia, o OpenFlow reduziu a complexidade e permitiu que a rede passasse a ser programada por meio de um elemento central.

Embora a implantação das SDNs estejam em alta nos grandes *data centers*, isto não quer dizer que elas não possam ser utilizadas em outros tipos de ambientes. Redes acadêmicas também podem utilizar e se beneficiar com os recursos que as SDNs oferecem, tais como: criação de redes lógicas, otimização de recursos, gerência simplificada, etc.

1.1 Motivações

O início das redes de computadores ocorreu em um ambiente acadêmico e é natural imaginar que a sua evolução se dê neste mesmo ambiente. Redes Definidas por Software tem sido objeto de pesquisa por cientistas de redes na busca por maior agilidade à Internet, visando também a redução de custos por bit transmitido e maior segurança a todos os seus usuários. SDN permitirá que os pesquisadores saiam da cultura do fechado, proprietário e caro e passem a trabalhar com soluções abertas.

As SDNs já estão sendo utilizadas em alguns *data centers*, como, por exemplo, o do Google. Empresas que oferecem serviços de *cloud computing* (computação em nuvem) perceberam que a escalabilidade da rede não está acompanhando as demais áreas da TI. Hoje é possível ter uma máquina virtual rodando em questão de minutos, mas o aprovisionamento do resto da infraestrutura de rede (conexões, roteadores, firewalls, etc) ainda leva um longo tempo para ficar pronto.

Grandes universidades hoje possuem as mesmas necessidades e por vezes oferecem os mesmos serviços que grandes empresas do setor privado. A Universidade de São Paulo, por exemplo, possui um serviço de nuvem exclusivo para seus funcionários e pesquisadores. Portanto, se as SDNs já são consideradas vantajosas no setor privado, elas também podem ser vantajosas no meio acadêmico.

1.2 Objetivo

O objetivo deste trabalho é apresentar uma comparação entre as redes definidas por software e as redes tradicionais e realizar uma análise das vantagens e desvantagens da implantação de uma SDN num ambiente acadêmico (de ensino e pesquisa).

1.3 Justificativas

As redes acadêmicas estão cada vez mais complexas e novos desafios surgem a todo momento. Universidades e centros de pesquisa tentam encontrar soluções para problemas como o crescimento dos seus *data centers*, o expressivo aumento no tráfego gerado pela mobilidade, o fornecimento de redes alternativas para a execução de experimentos, métodos para facilitar a gerência de diversos equipamentos de rede, etc. SDN surge, então, como uma alternativa para as novas demandas do meio acadêmico e com a proposta de alterar a forma de implantar, controlar e gerenciar a rede.

1.4 Estrutura do Trabalho

O Capítulo 1 Introdução apresenta as motivações, o objetivo, as justificativas e a estrutura do trabalho.

O Capítulo 2 Redes de Computadores - Conceitos, Evolução e Tecnologias apresenta uma revisão sobre o início das redes de computadores e da Internet, as limitações da atual arquitetura, como funciona uma rede tradicional, o que é a virtualização de rede e a virtualização de computadores, cita exemplos de tecnologias de virtualização e apresenta as redes experimentais.

O Capítulo 3 Redes Definidas por Software apresenta como surgiram as SDNs, além de definir e citar seus conceitos gerais.

O Capítulo 4 OpenFlow apresenta os componentes de um switch OpenFlow, explica seu funcionamento e descreve o protocolo Openflow.

O Capitulo 5 SDN vs Redes Tradicionais compara as redes tradicionais com as SDNs.

O Capítulo 6 SDN em Ambiente Acadêmico apresenta os desafios das atuais redes acadêmicas, os possíveis cenários de uso e descreve as vantagens e desvantagens de utilizar SDN em um ambiente acadêmico.

O Capítulo 7 Considerações Finais apresenta as considerações finais e as contribuições deste trabalho.

As Referências Bibliográficas apresentam os artigos, os livros e os demais documentos utilizados na construção desta monografia.

REDES DE COMPUTADORES - CONCEITOS, EVOLUÇÃO E TECNOLOGIAS

O uso das redes de computadores revolucionou nossa sociedade da mesma forma que a máquina a vapor ou a eletricidade fizeram em seu tempo. Hoje é difícil imaginar nossa vida sem a rede. Tanenbaum (2002) cita em seu livro quatro motivos pelos quais as pessoas estão interessadas em redes de computadores e com que finalidade essas redes podem ser utilizadas. Os motivos são:

1. Aplicações comerciais: utilizado para o compartilhamento de recursos. O objetivo é fazer com que programas, equipamentos e os dados estejam acessíveis a todas as pessoas da rede, independente da localização física do recurso e do usuário. Além disso, uma rede oferece um eficiente meio de comunicação entre os funcionários. Outro fator importante é o comércio eletrônico, muitas empresas investem neste tipo de mercado.

2. Aplicações domésticas: talvez a maior motivação seja o acesso à Internet. Redes sociais, comércio eletrônico e entretenimento são alguns exemplos de uso de computadores dentro de casa.

3. Usuários móveis: celulares, tablets e notebooks são dispositivos muito utilizados hoje em dia, e as pessoas precisam utilizar seus equipamentos em todo lugar. Por este motivo, as redes sem fios estão sendo cada vez mais estudadas.

4. Questões sociais: as rede de computadores permitem que cidadãos comuns manifestem suas opiniões de um modo novo e para um público inteiramente diferente.

A Internet conta hoje com mais de um bilhão de usuários em todo o mundo e isto comprova o enorme sucesso que ela tem. No entanto, a Internet utilizada atualmente foi projetada a mais de 30 anos e, consequentemente, o uso que fazemos dela hoje pouco se parece com o que motivou a sua criação.

A tendência é que no futuro existam ainda mais usuários, objetos, serviços e aplicações rodando na Internet e os administradores de redes precisam fazer com que a rede consiga atender a estas novas demandas. Conhecer um pouco da história das redes pode ajudar a entender os problemas e as limitações da atual arquitetura e assim se preparar para este

crescimento de forma planejada e estruturada.

2.1 O Início das Redes de Computadores

A necessidade de se comunicar utilizando algum dispositivo não é novo. O sistema de telégrafo foi o primeiro sistema de comunicação digital e, junto com o telefone, foram os precursores da internet. Colpitts e Blackwell (1921) contam um pouco da história do telégrafo e do telefone.

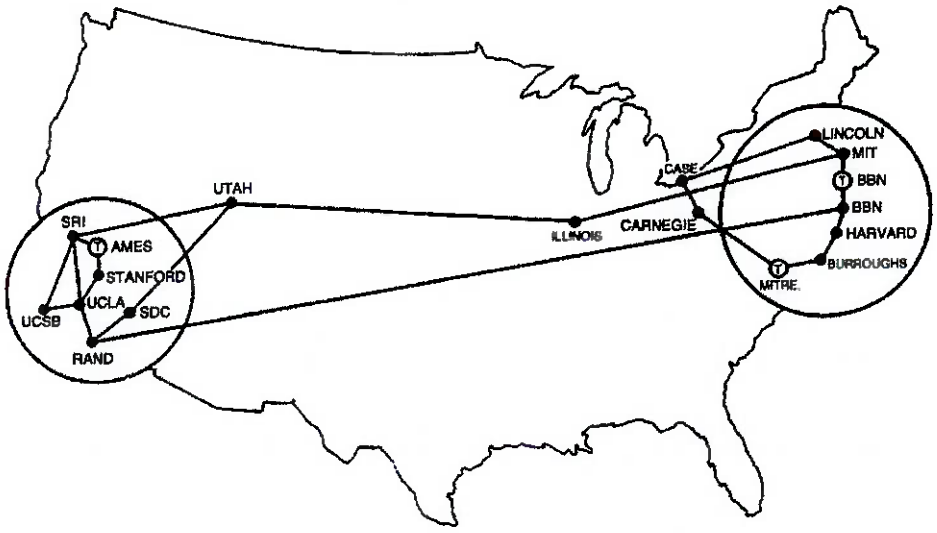
Um fator importante que possibilitou o surgimento das redes de computadores foi a invenção do microprocessador nos anos 70. Graças ao microprocessador, hoje é possível encontrar computadores e redes de computadores nos mais diversos locais, executando as mais diversas atividades. O microprocessador se tornou um ícone na era da informação e é utilizado não somente nos computadores, mas também em diversos outros tipos de dispositivos, tais como: celulares, automóveis, brinquedos, etc. A história do microprocessador é contada por Tredennick (1996).

Já a forma como os nós de uma rede são interconectados, chamada de topologia da rede, evoluiu junto com o sistema de telefonia. A Guerra Fria entre os Estados Unidos da América (EUA) e a extinta União das Repúblicas Socialistas Soviéticas (URSS) teve papel importante nesta evolução. Naquela época, a URSS já havia desenvolvido bombas atômicas, testado com sucesso o primeiro míssil balístico intercontinental e lançado o satélite Sputnick. Isto fez com que o setor de telecomunicações dos EUA começassem a se preparar para emergências. Duncan, então diretor adjunto de operações da *American Telephone and Telegraph Company* (AT&T), percebeu que um grande número de cidades e circuitos seriam destruídos caso um ataque nuclear se concretizasse e constatou que era preciso alterar a forma como as redes eram preparadas. Assim, a AT&T começou a prover rotas passando por fora das grandes cidades. Além disso, as redes passaram a ser projetadas e construídas para se tornarem altamente distribuídas e tolerantes as falhas (Grubesic e Murray, 2005).

2.2 O Início da Internet

A comunicação entre redes de computadores nasceu da ARPAnet, acrônimo em inglês de *Advanced Research Projects Agency Network* e evoluiu para o que se conhece hoje como Internet (Melcis, 1996). A figura 1 ilustra os diversos locais conectados pela ARPAnet em 1971. A rede ligava instituições na Califórnia e no nordeste dos Estados Unidos (Grubesic e Murray, 2005).

Figura 1: Rede ARPAnet em 1971



Fonte: (Grubesic e Murray, 2005)

Diversos livros e artigos afirmam que a ARPAnet foi desenvolvida para ajudar os militares. Contudo, Vea (2010) conta que recebeu a seguinte resposta sobre a origem da rede quando entrevistou Robert William Taylor, conhecido apenas como Bob Taylor, que era o então diretor da ARPA IPTO, em inglês, *ARPA Information Processing Techniques Office*: "A ARPAnet não foi construída com motivações militares, ela foi construída para permitir que as pessoas com acesso a computação interativa compartilhassem interesses em comuns".

Independente das motivações do seu surgimento, o fato é que a ARPAnet foi concebida para operar de forma descentralizada, o que de certa forma poderia proteger as informações de um ataque nuclear ou de desastres naturais, como furacão e tufão, uma vez que os dados não estariam concentrados em um único local (Severance, 2012).

Contudo, o crescimento e o surgimento de outras redes criaram uma complicação. A ARPAnet se mostrou inadequada para interconectar novas redes e, por este motivo, pesquisadores começaram a procurar alternativas. Deste problema surgiu o protocolo TCP/IP (Cerf e Kahn, 1974).

O TCP/IP se tornou o protocolo padrão da internet em 1981. Sua popularidade aumentou em 1983 quando ele foi utilizado na elaboração do Sistema Operacional UNIX (em particular, a versão Berkeley UNIX, implementado pela SUN-Microsystems). Este sistema foi amplamente utilizado por universidades e institutos de pesquisa (Maathuis e Smit, 2003).

O TCP/IP é na verdade um conjunto de protocolos de comunicação que definem como

tipos diferentes de computadores conversam uns com os outros. O Protocolo de Internet (IP) transmite dados na forma de datagramas. Os dados são divididos em pacotes e são enviados para os outros computadores via rede. O Protocolo de Controle de Transmissão (TCP) assegura que os datagramas em uma mensagem serão remontados na ordem correta em seu destino final e que os datagramas que estão faltando serão reenviados até que sejam corretamente recebidos (Ferreira, 2003).

Os primeiros serviços comerciais da Internet surgiram em 1989, após a conexão da Internet com provedores de e-mail. Neste mesmo ano foram criados três Provedores de Serviço de Internet (ISP) (Cerf, 2004). No Brasil, a Internet teve início por meio de um projeto FAPESP. Em fevereiro de 1989 um canal internacional de dados da Embratel entrou em funcionamento conectando o Fermilab, um laboratório especializado em física de partículas de alta energia localizado nos Estados Unidos, e a rede ANSP, uma rede acadêmica que era constituída na época por cinco nós: FAPESP, USP, UNICAMP, UNESP e IPT (ANSP, 2011).

A internet hoje pode ser vista como um conjunto interligado de domínios de roteamento. Cada domínio de roteamento é um grupo de nós (roteadores, switches e hosts), sob uma única administração (técnica), que compartilham políticas e informações de roteamento (Calvert *et al.*, 1997).

2.3 Limitações da Internet

O desenvolvimento e o crescimento da Internet trouxe uma série de desafios para seus pesquisadores. Para atender aos novos requisitos da Internet, diversas mudanças foram realizadas em sua arquitetura. As primeiras adaptações foram realizadas ainda na década de 80, para melhor interconectar o crescente número de redes que estavam surgindo. Desta situação, surgiram os conceitos de sub-redes (Mogul e Postel, 1985), do IP *multicasting* (Deering, 1986), dos sistemas de nomes de domínios (Mockapetris, 1987) e dos sistemas autônomos (Little, 1989). Além disso, na década de 90 foram criados o CIDR - *Classless Inter-Domain Routing* (Fuller *et al.*, 1993) e o NAT - *Network Address Translator* (Egevang e Francis, 1994).

A atual arquitetura da Internet suporta uma grande variedade de aplicações e executa diferentes tipos de tecnologias. Contudo, um dos pilares para o sucesso da Internet, o protocolo IP, é também considerado um obstáculo para o seu crescimento.

Alcober *et al.* (2013) afirmam que a Internet está enfrentando uma crise devido ao crescente número de usuários e aplicações. Por conta do grande número de adaptações reali-

zadas, a Internet tem se tornando cada vez mais complexa e os princípios originais estão cada vez mais distorcidos.

As redes de computadores de hoje podem ser comparadas aos *mainframes* dos anos 70. Na era do *mainframe*, os aplicativos, o Sistema Operacional (SO) e o hardware eram integrados e fornecidos pelo fabricante. Estes equipamentos eram proprietários e fechados, o que impedia a inovação. Atualmente, a maioria dos computadores utilizam o conjunto de instruções x86, o que permite que diferentes SOs, por exemplo, Windows, Linux e Mac OS, possam ser executados. O SO fornece APIs que permitem o desenvolvimento de novas aplicações, o que leva a uma rápida inovação e implantação.

Dentre as limitações que a atual arquitetura da Internet enfrenta, Jinzhou *et al.* (2010) citam o seguinte: segurança, flexibilidade, mobilidade e capacidade de gerenciamento. Haque *et al.* (2011) citam ainda a escalabilidade e a disponibilidade como fatores limitantes na atual arquitetura.

2.4 Redes Tradicionais

Como dito anteriormente, a arquitetura da Internet possui algumas limitações. Para compreender estas limitações e encontrar uma solução para este problema, é preciso primeiro conhecer como opera a rede atualmente.

Redes de computadores são dinâmicas e complexas. Uma rede tradicional pode ter um grande número de switches, roteadores, firewalls e diversos outros dispositivos de rede, com diferentes tipos de protocolos implementados, sendo cada um deles configurado individualmente (Kim *et al.*, 2011)(Kim e Feamster, 2013).

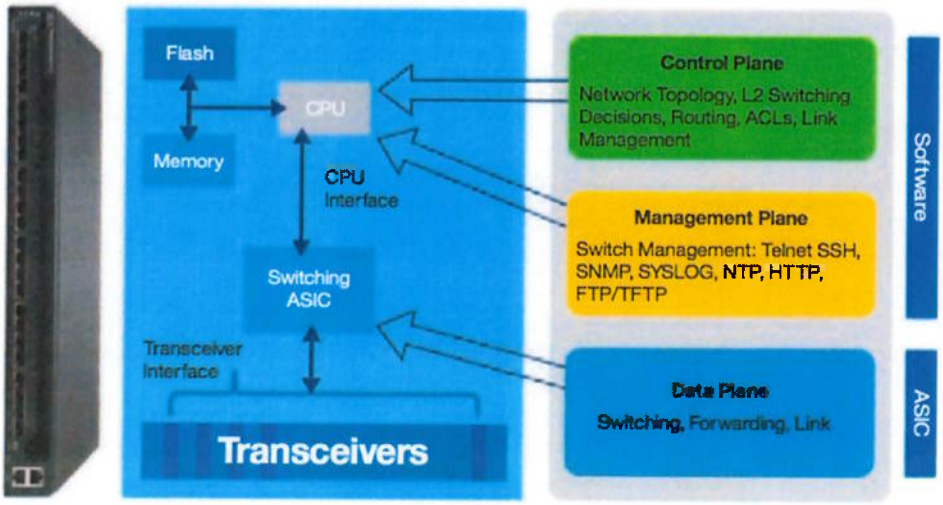
Comutador ou switch de rede é o dispositivo capaz de analisar os cabeçalhos dos pacotes recebidos e tomar decisões sobre como encaminhar estes pacotes pela rede. Existem diferentes tipos de switches, operando em diferentes camadas do modelo OSI: switch de camada 1 (HUB), switch de camada 2 (switch) e switch de camada 3 (roteador). Conforme pode ser visto na Figura 2, switches de camadas dois ou três possuem os seguintes elementos básicos (IBM, 2012):

a) Plano de dados: carrega fisicamente os pacotes de dados de uma porta para outra seguindo regras que são programadas dentro do hardware do equipamento.

b) Plano de controle: contém a lógica que o dispositivo utiliza para programar o plano de dados, assim os pacotes são redirecionados de forma correta pela rede.

c) Plano de gerência: permite que um usuário administrador acesse o equipamento para realizar as configurações básicas.

Figura 2: Arquitetura de um switch tradicional.



Fonte: (IBM, 2012)

Na arquitetura de uma rede clássica, o plano de dados e o plano de controle estão fisicamente dentro do mesmo dispositivo. Quando um switch convencional recebe um pacote, uma decisão é tomada no plano de controle e comunicada ao plano de dados, essa comunicação é feita através de um barramento interno.

Fabricantes costumam desenvolver software para o plano de controle para otimizar o fluxo de dados e assim conseguir alto desempenho e vantagem competitiva. Switch baseado no paradigma do plano de controle oferece pouca oportunidade para o administrador de rede aumentar a eficiência do fluxo de dados (IBM, 2012).

Os administradores de redes são os responsáveis pelas políticas de alto nível e por responderem ao grande número de eventos que podem ocorrer, como intrusões ou mudanças na troca de tráfego. Tarefas complexas são geralmente executadas com um limitado conjunto de comandos em uma interface de linha de comando. Como resultado, o gerenciamento da rede é bastante desafiador e, portanto, sujeito a erros.

Atualmente, as redes oferecem poucos mecanismos para responder automaticamente aos eventos que podem ocorrer. Devido a esta limitação, os administradores de redes utilizam ferramentas externas ou criam *scripts* para reconfigurar dinamicamente os dispositivos de rede quando ocorre algum evento (Kim e Feamster, 2013).

2.5 Virtualização

A virtualização tem sido amplamente estudada porque é considerada de fundamental importância para o desenvolvimento de uma nova arquitetura para Internet. O uso das técnicas de virtualização abrem novos horizontes e atendem a diversos requisitos de forma a contornar as dificuldades apresentadas pela rede atual.

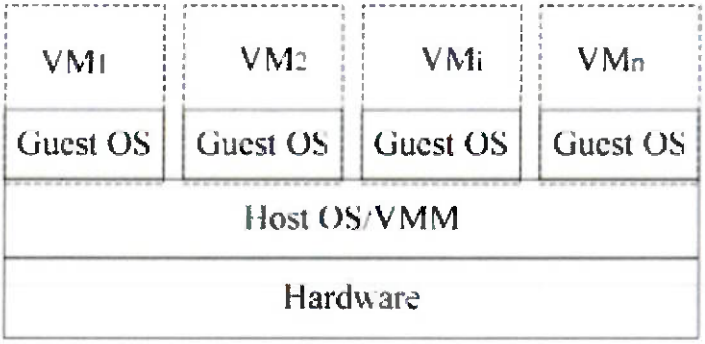
A virtualização é utilizada para gerar uma versão virtual de um dispositivo ou de um recurso, tal como um computador ou uma rede. Esta técnica passou a ser muita utilizada na última década, mas na verdade ela é muito mais antiga do que isso. Uma revisão sobre a virtualização é apresentada por Agarwal *et al.* (2012).

Os itens 2.5.1 e 2.5.2 fazem uma breve descrição do que é a virtualização de computadores e a virtualização de rede.

2.5.1 Virtualização de Computadores

Este tipo de virtualização utiliza-se de uma Máquina Virtual (VM) que nada mais é do que uma entidade abstrata que executa tarefas como se fosse uma máquina real. A figura 3 apresenta a arquitetura básica de uma VM.

Figura 3: Arquitetura de um sistema de máquina virtual.



Fonte: (Li *et al.*, 2010)

Nesta arquitetura, múltiplas VMs compartilham os recursos de uma mesma máquina física. As VMs são administradas pelo Monitor de Máquina Virtual (VMM). É o VMM que fornece a alocação de recursos, tais como CPU, memória e disco da máquina física para as máquinas virtuais. Uma máquina real pode hospedar diversas VMs e cada VM pode executar um SO distinto (Li *et al.*, 2010).

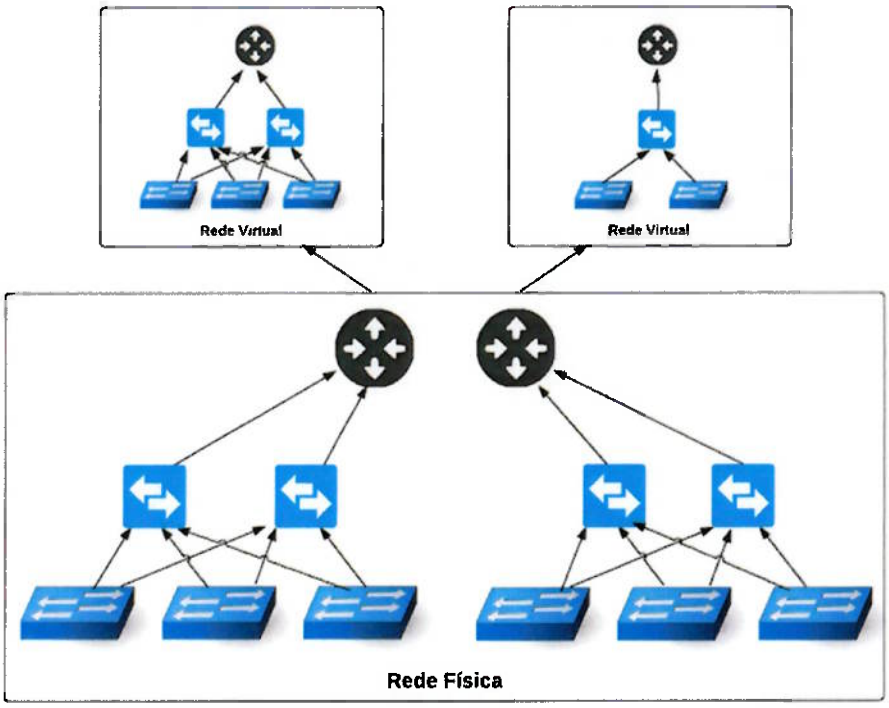
Existem diversas opções de software para utilizar na virtualização de servidores, sendo os

mais populares o Xen, o KVM, o OpenVZ e o VMware. Diversos artigos já foram escritos para comparar e avaliar cada um desses programas. Alguns autores que fizeram este tipo de trabalho foram: Che *et al.* (2010), Binu e Kumar (2011), Kolhe e Dhage (2012) e Wang *et al.* (2012).

2.5.2 Virtualização de Redes

Virtualização de rede é a tecnologia que permite a operação simultânea de múltiplas redes lógicas, sendo cada rede constituída de diversos nós e links virtuais, em uma única rede física (Figura 4).

Figura 4: Exemplo de virtualização de rede.



Fonte: produzido pelo autor

A virtualização de rede faz com que parte da infraestrutura física seja tratada como uma rede virtual. Esta abstração assegura que a rede virtual permaneça escondida do que acontece no resto da rede (Colle *et al.*, 2010).

Este método é considerado a melhor forma de afastar a "ossificação", ou como costumam falar os engenheiros de redes no Brasil, o "engessamento" da internet. Anderson *et al.* (2005) citam que a popularidade da internet acaba dificultando o seu próprio crescimento, uma vez que a adoção de uma nova arquitetura ou a modificação da arquitetura existente requer um consenso entre todas as partes envolvidas.

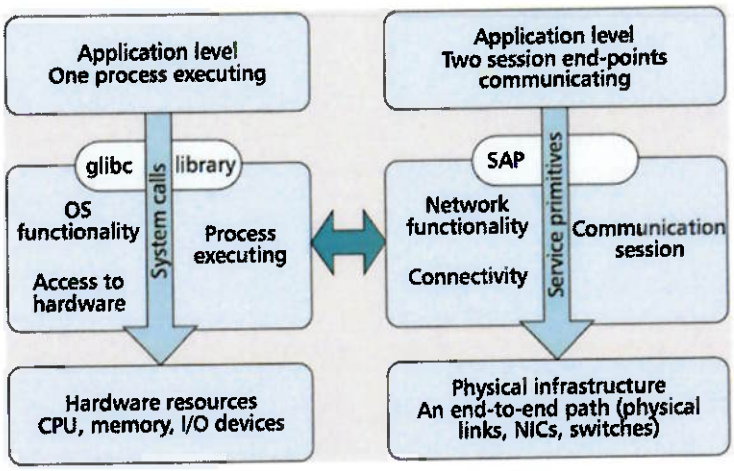
2.5.3 Analogia entre Virtualização de Redes e Virtualização de Computadores

Khan *et al.* (2012) fazem uma analogia entre o conceito de virtualização de rede e virtualização de computadores. Eles começam fazendo uma analogia entre as funcionalidades de um Sistema Operacional e de uma rede. Eles citam que a principal funcionalidade do SO é disponibilizar para a aplicação um simples conjunto de instruções. Um processo executando uma tarefa de uma determinada aplicação acessa os recursos de hardware desejados através deste conjunto de instruções. No caso da rede, eles citam que a sua principal função é a de prover conectividade entre dois pontos em uma sessão. A rede fornece um método simples para enviar informações de uma ponta para outra.

Assumindo uma equivalência entre a execução de um processo e a sessão de uma comunicação fim-a-fim, os autores fazem uma analogia entre o SO e a rede. O processo é a unidade de execução de um SO, que consome recursos de hardware e retorna a saída da execução para a aplicação que gerou o processo. De forma semelhante, uma sessão de comunicação fim-a-fim consome recursos da rede para permitir o fluxo de dados entre dois nós e uma saída é entregue para os pontos finais da comunicação. Deste ponto de vista, a principal função do SO, por exemplo, prover acesso aos recursos de hardware para um processo em execução, é semelhante à funcionalidade de uma rede, por exemplo, prover recursos da rede para a sessão de comunicação fim-a-fim.

Na figura 5 os autores fazem uma analogia em termos de funcionalidades. Chamadas de sistemas geradas pelo SO e executadas pela biblioteca *libc* são comparadas com o serviço oferecido na interface entre a aplicação e a rede através do ponto de acesso ao serviço, em inglês, *Service Access Point* (SAP).

Figura 5: Analogia conceitual entre um sistema operacional e uma rede.



Fonte: (Khan *et al.*, 2012)

O que os autores pretendem com esta analogia é trazer para a virtualização de rede alguns conceitos que já são bem conhecidos na virtualização de computadores. Eles argumentam que não há uma tecnologia superior à todas as outras e que alguns benefícios da virtualização de computadores, tais como: coexistência de diferentes tipos de SOs em uma mesma máquina, proteção da VM, utilização de VM para testes e experimentações, migração de VM entre diferentes máquinas físicas e otimização do uso dos recursos de hardware, também podem ser encontrados na virtualização de rede, porém na virtualização de rede esses benefícios seriam visto como: coexistência de diferentes redes, proteção da rede virtual, uso de redes virtuais para execução de testes, migração de um nó de rede para outro nó de rede e otimização do uso dos recursos da rede.

2.6 Tecnologias de Virtualização de Redes

É comum encontrar nas redes tradicionais algumas tecnologias de virtualização em funcionamento, contudo, estas tecnologias também são consideradas adaptações para contornar os problemas encontrados na arquitetura da Internet. Abaixo são descritos dois exemplos:

2.6.1 VLAN

Uma VLAN, acrônimo de *Virtual Local Area Network*, é uma rede logicamente independente que pode ser utilizada para agrupar várias máquinas de acordo com vários critérios, por exemplo: grupos de usuários ou tipos de tráfego.

Chowdhury e Boutaba (2010) descrevem que os clientes de uma VLAN são logicamente reunidos sob um único domínio de *broadcast*, independente da sua conectividade física. VLANs são entidades lógicas, ou seja, são configuradas via software. Elas são flexíveis em termos de administração de rede, gestão e reconfiguração. Além disso, VLANs proporcionam níveis elevados de confiança, segurança e isolamento. Esta tecnologia é geralmente configurada na camada 2, embora existam implementações em camadas diferentes. Todos os *frames* de uma VLAN recebem um identificador (ID). Este ID é inserido no cabeçalho e os switches utilizam este número, mais o endereço MAC de origem e de destino, para encaminhar os *frames*. Múltiplas VLANs podem ser conectadas usando *trunking*, o que permite que informações de múltiplas VLANs sejam transportadas por um único link entre diferentes switches.

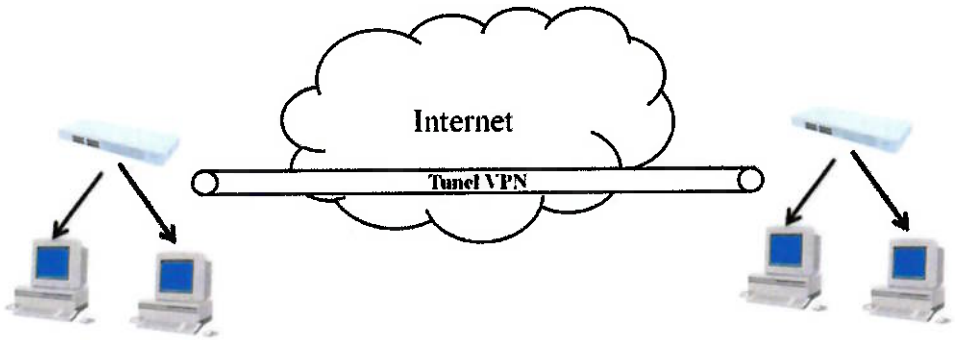
Existem três tipos básicos para determinar como um pacote é atribuído a uma VLAN: VLAN de nível 1, chamado de *Port-Based VLAN* (VLANs baseados em portas), VLAN de nível 2, chamado de *MAC Address-Based VLAN* (VLANs baseados em endereço MAC) e VLAN de nível 3, conhecidos por *Protocol-Based VLANs* (VLANs baseadas em protocolos) ou *Network Address-Based VLAN* (VLAN por sub-rede). Alguns motivos do porquê

se utilizar VLANs são: reduzir custos com operações de rede, aumentar a segurança com a divisão de dispositivos e usuários em domínios diferentes de *broadcast* e obter maior flexibilidade na administração e nas modificações da rede. Outras informações sobre VLANs, como agregação de VLANs e uso de VLANs em redes IPv6, podem ser encontradas em McPherson e Dykes (2001) e Chown (2006), respectivamente.

2.6.2 VPN

VPN é o acrônimo de *Virtual Private Network* - Rede Privada Virtual. Trata-se de uma rede privada que utiliza uma rede pública (normalmente a Internet) como meio de transporte de dados para conectar sites remotos ou usuários, porém em um contexto seguro, como se tudo estivesse em uma rede local (Figura 6). Por exemplo, organizações utilizam VPN para conectar escritórios que estão em locais geograficamente distantes ou, ainda, para que os funcionários que estejam fora da organização consigam acesso a rede interna da empresa.

Figura 6: Um túnel VPN utilizado para conectar duas redes privadas.



Fonte: produzido pelo autor

Os três principais protocolos utilizados para se estabelecer uma VPN são: *Point-to-Point Tunneling Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP) e *Internet Protocol Security* (IPSec). É possível, ainda, classificar as VPNs em diferentes categorias, as principais são: VPN de camada 2 (L2 VPN) e VPN de camada 3 (L3 VPN). Rosenbaun *et al.* (2003) e Wang *et al.* (2013) descrevem estas categorias.

2.7 Redes Experimentais

No meio universitário e de pesquisa, muitos acreditam que a solução para as limitações da Internet depende de um redesenho da arquitetura atual. Internet do Futuro (IF) é o termo que está sendo utilizado para definir a ampla iniciativa de pesquisadores ao redor do mundo para identificar os rumos tecnológicos que a rede deverá tomar nos próximos anos.

Entre as principais vertentes de pesquisa sobre IF estão as propostas *clean-slate* (limpa) e evolucionária. A primeira propõem que a nova arquitetura da rede seja pensada de forma independente, ou seja, com base nos conhecimentos sobre os problemas da Internet, um pesquisador poderia propor uma solução que não precisa ser necessariamente compatível com a atual arquitetura. A segunda vertente de pesquisa apoia que uma nova solução deva ser estabelecida com base na evolução da Internet atual. Em ambas as vertentes existe o consenso de que todas as novas propostas precisam ser testadas em larga escala e sob diferentes cenários, antes de se propor uma modificação no ambiente atual. Além disso, é necessário desenvolver um ambiente para a transição entre a Internet atual e a nova arquitetura (Moreira *et al.*, 2009).

Diante deste contexto, vários países estão desenvolvendo iniciativas que envolvem pesquisadores da academia e da indústria para projetar e testar novas propostas para a Internet. Redes experimentais (*testbeds*) já estão sendo utilizadas nos EUA com o programa GENI (GENI, 2006), na União Europeia (UE) com o programa FIRE (Gavras *et al.*, 2007), no Japão com o programa AKARI (Harai, 2009) e no Brasil com o projeto FIBRE (Sallent *et al.*, 2012).

2.8 Considerações do Capítulo

Este capítulo aborda o surgimento e a evolução das redes de computadores e da Internet com o intuito de apresentar os problemas e as limitações encontradas na atual arquitetura. Este capítulo também trata do funcionamento de uma rede tradicional e de conceitos como virtualização, tecnologias de virtualização de redes e redes experimentais. Estes conceitos formam a base para o entendimento da criação das SDNs.

REDES DEFINIDAS POR SOFTWARE

3.1 O Início

Enterasys (2012) cita que o conceito de SDN surgiu no início dos anos 90 com o protótipo VNS Seguro (*Virtual Network Service*) e com o GSMP (*Genaral Switch Management Protocol*). Já na comunidade dos Provedores de Serviço, o autor comenta que a ideia surgiu em torno da arquitetura IMS (*IP Multimedia Systems*) e as redes TDM (*Time Division Multiplex*), quando foi implementado o conceito de redes inteligentes.

Já para Sezer *et al.* (2013), o conceito de SDN vem evoluindo desde 1996 impulsionado pelo desejo de permitir que o usuário gerencie o funcionamento da rede. Essa evolução surgiu em torno das implementações realizadas por grupos de pesquisa e pela indústria, e incluem: o GSMP (1996), o *paper* criado por Rooney *et al.* (1998), os padrões ForCES (2000) e PCE (2004) criados pelo IETF - *Internet Engineering Task Force* - e, mais recentemente, os projetos Ethane (2007) e OpenFlow (2008).

Embora alguns conceitos utilizados em Redes Definidas por Software tenham surgido a mais de 20 anos, a sigla SDN surgiu apenas em 2008 com a descrição do projeto OpenFlow da Universidade de Stanford (Feamster *et al.*, 2013).

3.2 Definição

Existem diferentes tecnologias e abordagens que podem ser utilizadas para criar uma Rede Definida por Software, portanto, é possível encontrar na Internet a descrição de diferentes modelos de SDN. O modelo mais conhecido é o que foi proposto pela Universidade de Stanford, onde o plano de dados e o plano de controle são separados e o controle da rede passa a ser realizado por um elemento externo, denominado controlador. O controlador tem a responsabilidade de decidir o que deve ser realizado com as entradas na tabela de fluxos. Outro modelo que pode ser encontrado é o que faz uso de switches virtuais. Este modelo também separa o plano de dados e o plano de controle, mas ele faz isso utilizando switches virtuais gerenciados por um VMM. Usando protocolos como o VXLAN, descrito por Cai e Natarajan (2013) ou o NVGRE, criado por Sridharan *et al.* (2013), estes switches virtuais criam uma camada de abstração acima da rede física.

Por conta das diferentes abordagens que podem ser encontradas a respeito de Redes Definidas por Software, não existe um consenso quanto a definição do termo SDN. Para a ONF - *Open Networking Foundation* -, SDN é:

> uma nova abordagem para redes onde o controle da rede está desacoplado da função de transmissão de dados e é diretamente programável. O resultado é uma arquitetura dinâmica, gerenciável, adaptável e com bom custo-benefício, o que dá aos administradores a possibilidade para programar, automatizar e controlar a rede (ONF, 2012).

Já o IETF define SDN como:

> uma abordagem que permite que os aplicativos conversem e manipulem diretamente o software de controle dos dispositivos de rede e também os recursos da rede (Nadeau, 2011).

Existe também uma ambiguidade com a sigla SDN. Enquanto boa parte dos autores definem SDN como *Software-Defined Networking*, outros chamam de *Software-Driven Networks*.

O que é possível afirmar sobre SDN é que ela tem o objetivo de tornar as redes mais flexíveis, mais fáceis de serem operadas e gerenciadas e com capacidade para responder as novas demandas de serviços. É por este motivo que, apesar de toda a confusão em torno das SDNs, muitas empresas estão começando a explorar esta tecnologia e diversos fabricantes já implementam produtos com suporte a alguma forma de SDN.

Por outro lado, é possível afirmar o que SDN não é:

- SDN não é a definição de um novo protocolo de programação para plano de dados;
- SDN não é a definição de um novo software de controle;
- SDN não é apenas mais um sonho acadêmico.

3.3 Motivação

As SDNs surgiram por conta dos problemas enfrentados pela Internet, conforme já descrito na seção 2.3. Contudo, outros itens estão motivando a academia, as empresas, os fabricantes e os administradores de redes. Por exemplo, SDN é apontado como um método para tornar as redes mais expansíveis e flexíveis, mas o ponto que mais chama a atenção nas grandes empresas é a possibilidade de redução de custos com TI. Com a criação das

redes virtuais será possível otimizar o uso dos equipamentos que se encontram ociosos e, consequentemente, reduzir as despesas com novos dispositivos de rede. Também deverá ser possível reduzir os custos operacionais, automatizando um projeto de rede de acordo com a utilização do usuário. Esta é uma aposta que as empresas de computação em nuvem estão fazendo, principalmente por conta do crescimento que é esperado para este setor. A computação em nuvem vem crescendo significativamente no Brasil e deve ganhar ainda mais força nos próximos anos. Segundo uma pesquisa realizada pela Cisco (2013), o tráfego da Nuvem em *Data Center* na América Latina crescerá 3,9 vezes em 2017 em comparação com 2012. Estima-se que em 2017 os usuários finais serão os responsáveis por boa parte do tráfego, que deverá ser em boa parte para navegar na web, fazer *streaming* de vídeos e para fazer uso de diferentes dispositivos, o que vem de encontro com a "Internet das Coisas" - *Internet of Things* - (IoT). Para atender este crescimento e buscar a simplificação das redes, espera-se que as iniciativas de SDN, NFV - *Network Functions Virtualization* - e computação em nuvem caminhem juntas, retirando a complexidade da topologia e acelerando o processo de criação de novos serviços.

Na visão dos fabricantes, SDN surge como um novo negócio. Diversos fabricantes já anunciaram a intenção de dar suporte ao OpenFlow, entre eles estão: Alcatel-Lucent, Big Switch Networks, Brocade, Cisco, Datacom, HP, IBM, Juniper e VMware/Nicira. Existe também um trabalho conjunto entre fabricantes e academia, um exemplo disso é a parceria que existe entre a rede acadêmica de São Paulo (ANSP) e empresas nacionais de telecomunicações com o desenvolvimento de switches Openflow.

No mundo acadêmico, o que motiva o uso das SDNs é a possibilidade de inovar. Segundo McKeown *et al.* (2008), hoje não há quase nenhuma maneira prática de experimentar novos protocolos de rede (por exemplo, um novo protocolo de roteamento ou uma nova alternativa para o IP) em ambientes suficientemente realistas para ganhar a confiança necessária para a sua implantação. O resultado é que a maioria das novas ideias da comunidade de pesquisa não são devidamente testadas. Com SDN, os pesquisadores de redes enxergam uma possibilidade para separar o tráfego experimental do tráfego de produção e, assim, poder realizar qualquer tipo de teste. No Estado de São Paulo, as principais universidades começam a criar suas nuvens computacionais e seus centros de computação já há algum tempo discutem os conceitos de SDN (ANSP, 2014).

Para os administradores de redes, SDN é visto como uma alternativa para homogeneizar e simplificar a gerência das redes. Com a proliferação de equipamentos (firewalls, IDS, balanceadores de carga, etc) de diferentes fabricantes, SDN surge como uma alternativa para substituir a maioria deles por simples aplicativos. Outras áreas em que as SDNs devem contribuir é com a atual complexidade na administração de VLANs e no gerenciamento

de dispositivos pessoais nos ambientes de trabalho, o fenômeno BYOD (*Bring Your Own Device*).

3.4 Visão Geral

Este trabalho segue os conceitos que foram inicialmente apresentados pela Universidade de Stanford e que é mantido atualmente pela ONF. Neste contexto, SDN é uma arquitetura onde Plano de Controle é separado do Plano de Dados (itens "b" e "a" da seção 2.4) e é diretamente programável. Isto permite mover grande parte da lógica de tomada de decisão dos dispositivos de rede para controladores externos (item 3.5). A vantagem é que os controladores podem ser implementados com a tecnologia de servidores comerciais (PCs), um recurso abundante, escalável e barato (Rothenberg *et al.*, 2011).

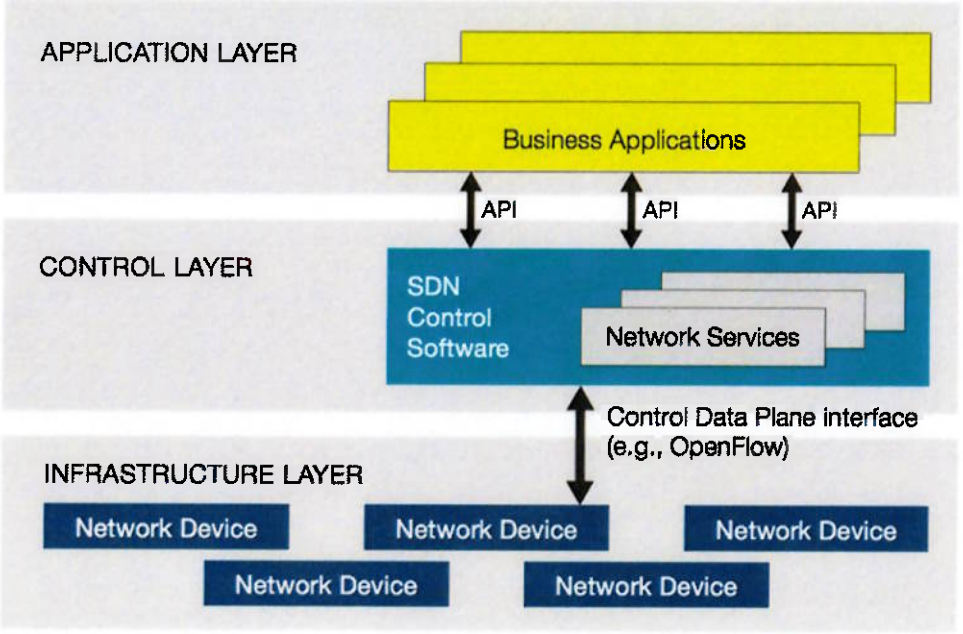
Em uma rede tradicional, as informações são transmitidas por meio de pacotes. Cada pacote contém as informações necessárias para que o switch consiga tomar as decisões necessárias para a sua transmissão. Este modelo não é apropriado para uma arquitetura SDN, pois se o controlador tiver que tratar cada pacote individualmente, isto poderia resultar em um alto *delay*. Ao invés disso, os dados em SDN são transmitidos por meio de fluxos ou por uma agregação de fluxos, onde a decisão do que será feito com o primeiro pacote de um fluxo é aplicado para os demais pacotes deste fluxo.

O SDN faz o Plano de Dados agir simplesmente como um comutador, onde sua principal função é o encaminhamento de pacotes. Já o Plano de Controle fica responsável pela inteligência da rede, definindo, entre outras coisas, qual será o próximo salto dos pacotes. Segundo Risdianto e Mulyana (2012), SDN possui os seguintes aspectos:

- Separação do Plano de Dados e Plano de Controle;
- Padrão, interface independente de fornecedor de equipamento de rede;
- Plano de controle centralizado logicamente (sistema operacional de rede);
- Virtualização para a operação simultânea de múltiplas redes lógicas.

A Figura 7 ilustra a visão lógica de uma arquitetura SDN. A inteligência da rede é (logicamente) centralizada em controladores baseados em programas que possuem uma visão global da rede. Como resultado, a rede é apresentada para as aplicações como um único switch lógico. SDN também simplifica os dispositivos de rede, já que eles não vão precisar compreender e processar diferentes tipos de protocolos, mas simplesmente aceitar as instruções dos controladores SDN (ONF, 2012).

Figura 7: Arquitetura de uma rede definida por software.



Fonte: (ONF, 2012)

A arquitetura SDN é bastante flexível, uma vez que ela pode operar em diferentes protocolos e em diferentes tipos de switch. Em uma arquitetura SDN, o switch desempenha as seguintes funções:

- Encapsula e encaminha o primeiro pacote de um fluxo para o controlador;
- Encaminha os pacotes para as portas apropriadas de acordo a tabela de fluxos;
- O switch também pode descartar, temporariamente ou permanentemente, os pacotes de um determinado fluxo.

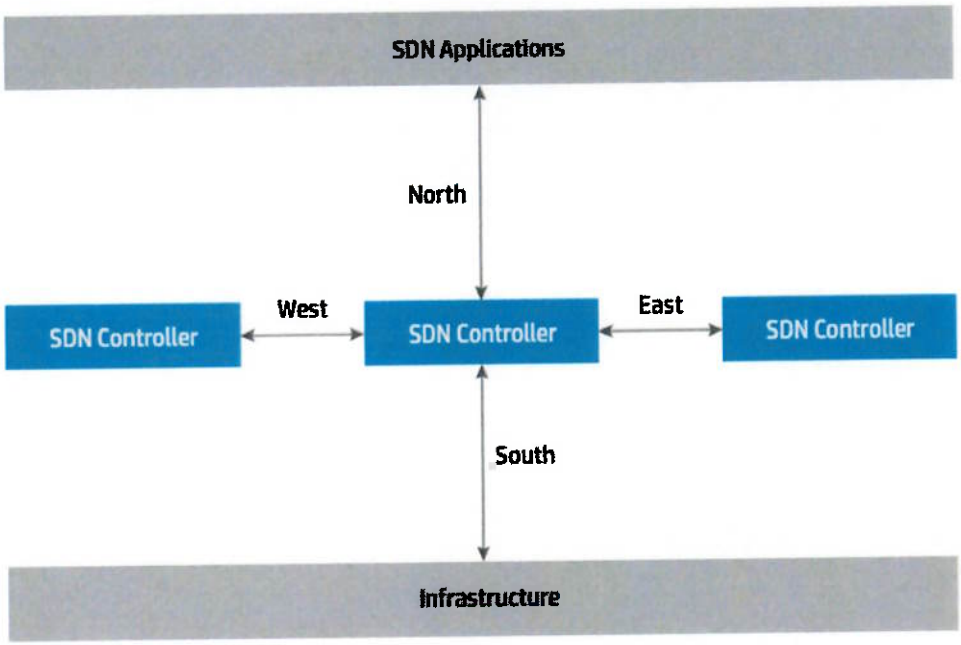
Pitt (2013) cita que SDN permite que operadores de redes programem o Plano de Controle a partir de uma interface central, usando métodos comuns de programação. Desta forma, não é necessário estar fisicamente nos locais onde se encontram os equipamentos para reconfigurar um dispositivo de rede. ONF (2012) cita também a vantagem dos operadores de redes não precisarem mais aguardar que as novas funcionalidades sejam inseridas nos programas fechados e proprietários dos fornecedores, uma vez que eles mesmos poderão programar as rotinas.

Arquiteturas SDNs possuem suporte a um conjunto de APIs (Application Programming Interfaces) que possibilitam a implementação de serviços comuns de rede, incluindo roteamento, *multicast*, segurança, controle de acesso, gerenciamento de largura de banda, engenharia de tráfego, qualidade de serviço, otimização de armazenamento e processamento, consumo de energia e todas as demais formas de política de gerenciamento, customizado

para atender aos objetivos de negócio.

Também existem APIs para a comunicação entre as camadas da pilha SDN. Estas APIs são agrupadas com base em sua função dentro da arquitetura. Na figura 8, *North* representa a comunicação entre controladores e aplicações, *South* representa a comunicação entre o controlador e a infraestrutura da rede e *East* e *West* representam a comunicação entre controladores (HP, 2012).

Figura 8: Grupos de APIs de acordo com a função exercida em SDN.



Fonte: (HP, 2012)

Existem alguns protocolos que foram especialmente desenvolvidos para concentrar as tarefas de manipulação direta dos dispositivos de rede dentro de uma arquitetura SDN. Já o gerenciamento de uma rede SDN é realizado em uma abstração de mais alto nível, por meio de um dispositivo chamado controlador.

3.5 O Controlador

O controlador de rede, também chamado de sistema operacional de rede, é responsável pela execução de tarefas complexas, como roteamento e verificações de segurança. Rothenberg *et al.* (2011) descrevem que o controlador exerce a função de uma camada de abstração da infraestrutura física, facilitando a criação de aplicações e serviços que gerenciem as entradas de fluxo de dados.

Em linhas gerais, o controlador define como o fluxo de dados deve se comportar dentro

do Plano de Dados. Cada fluxo que passa pela rede deve primeiro obter uma permissão do controlador. O controlador verifica se existe alguma regra referente a este fluxo na política da rede e, caso exista, ele traça o percurso que o fluxo deve tomar adicionando uma entrada para o fluxo em cada switch existente no caminho. A comunicação entre o controlador e o switch é feita por protocolos padronizados e por APIs.

As SDNs podem ser gerenciadas por um ou mais controladores. O uso de um único controlador representa um possível ponto de falha para toda a rede, portanto um provável cenário para uma rede com um grande número de *hosts* seria a separação da rede em diferentes domínios, sendo cada domínio gerenciado por um controlador. A existência de vários domínios obriga que os controladores utilizem um protocolo padronizado para que eles possam se comunicar, por isso o IETF está trabalhando no desenvolvimento do protocolo SDNi (Yin *et al.*, 2012).

Um controlador pode ser do tipo Reativo ou Pró-Ativo. No modelo Reativo o controlador precisa ser consultado cada vez que uma decisão precisa ser tomada, por exemplo quando o primeiro pacote de um fluxo chega ao switch. No modelo Pró-Ativo o controlador préconfigura uma tabela de fluxos no switch. A vantagem do modelo Reativo é que ele faz um uso eficiente da tabela de fluxos, mas tem a desvantagem de ter a funcionalidade limitada em caso de perda de conexão do controlador com a rede. Para o modelo Pró-Ativo a grande vantagem é a possibilidade de diminuir o *delay* e aumentar o *throughput* para novos fluxos, além de não ter o tráfego interrompido em caso de perda de conexão do controlador com a rede, por outro lado, a desvantagem deste modelo é que ele exige a criação de regras "coringas".

Existem diversos controladores que podem ser utilizados em uma arquitetura SDN. A escolha do controlador deve ser feita com base nas funcionalidades que o controlador oferece e na linguagem de programação que o desenvolvedor se sinta confortável em utilizar. Existem controladores em diferentes linguagens de programação, tais como: Java, C, Python e Ruby. A tabela 1 mostra os principais controladores já desenvolvidos.

Existe uma preocupação quanto à escalabilidade e o desempenho dos controladores. Tootoonchian *et al.* (2012) realizaram um experimento emulando 100.000 terminais e um número variado de switches (1, 4, 16, 32, 64 e 256) e constataram que os controladores NOX, NOX-MT, Maestro e Beacon conseguiram tratar ao menos 50 mil novos pedidos de fluxos por segundo. Neste estudo, os autores apresentaram o controlador NOX-MT[1]. Este controlador conseguiu tratar até 1 milhão e 600 mil novos pedidos de fluxos por segundo, com um tempo médio de resposta de 2 milissegundos. Este teste foi realizado

[1]Os conceitos apresentados no controlador NOX-MT foram incluídos na nova versão do NOX.

Tabela 1: Principais controladores SDN

Nome	Linguagem	Plataforma	*Open Source*	Desenvolvedor
NOX	C++/Python	Linux	Sim	Nicira
POX	Python	Multiplataforma	Sim	Nicira
MUL	C	Linux	Sim	Kulcloud
Maestro	Java	Multiplataforma	Sim	Rice University
Trema	Ruby/C	Linux	Sim	NEC
Beacon	Java	Multiplataforma	Sim	Stanford
Floodlight	Java	Multiplataforma	Sim	BigSwitch
SNAC	C++	Linux	Não	Nicira
Ryu	Python	Linux	Sim	NTT e OSRG
Flowvisor	C	Linux	Sim	Stanford e Nicira
RouteFlow	C++	Linux	Sim	CPQD

utilizando uma máquina de oito núcleos, com 2 GHz de processamento. O resultado deste estudo comprova que um único controlador poderia ser utilizado para gerenciar uma rede com um grande número de *hosts*, porém esta prática não é aconselhada uma vez que isto poderia comprometer a disponibilidade da rede. Além disso, utilizar dois ou mais controladores pode ajudar na obtenção de um menor tempo de resposta nas requisições feitas ao controlador.

3.6 Considerações do Capítulo

Este capítulo trata do surgimento das SDNs e da motivação, do ponto de vista de diferentes segmentos, em utilizar esta nova abordagem. São apresentadas também algumas definições e uma visão geral sobre o funcionamento das redes definidas por software. Neste estudo, foi considerado que SDN é uma arquitetura onde Plano de Controle é separado do Plano de Dados e é diretamente programável.

OPENFLOW

O OpenFlow foi apresentado em março de 2008 por professores da Universidade de Stanford como uma idéia inovadora para uma rede de um câmpus universitário. Este trabalho, intitulado "*OpenFlow: enabling innovation in campus networks*", foi o precursor de uma área que vem ganhando muito destaque no mundo das redes. O objetivo dos autores era incentivar que os fabricantes de equipamentos de rede incluíssem o OpenFlow em seus produtos, com isso os pesquisadores poderiam executar seus experimentos em diferentes tipos de switch e os vendedores não precisariam expor o funcionamento interno dos seus equipamentos (McKeown *et al.*, 2008). Seis anos após lançamento do OpenFlow, é possível afirmar que os autores conseguiram atingir o objetivo que foi inicialmente proposto.

Do nome OpenFlow, "*Open*" significa que a interface para o controle externo do switch é aberta, permitindo assim que qualquer pessoa consiga modificar as funções do switch. "*Flow*" significa que o controle é baseado em fluxos. Esses fluxos podem ser definidos arbitrariamente (Shimonishi *et al.*, 2012).

O OpenFlow é atualmente gerenciado pela *Open Networking Foundation* (ONF), uma organização sem fins lucrativos dedicada à promoção e adoção de Redes Definidas por Software através do desenvolvimento de padrões abertos. A tabela 2 mostra a evolução do OpenFlow nos últimos anos.

Tabela 2: Evolução do OpenFlow

Versão	Data	Algumas Características
0.1	Novembro de 2007	Versão inicial do OpenFlow
1.0	Dezembro de 2009	Tabela única; IPv4
1.1	Fevereiro de 2011	Múltiplas tabelas; MPLS; VLAN; ECMP
1.2	Dezembro de 2011	Múltiplos controladores; IPv6
1.3	Junho de 2012	Canais paralelos entre o switch e o controlador
1.4	Outubro de 2013	Monitoração de fluxos

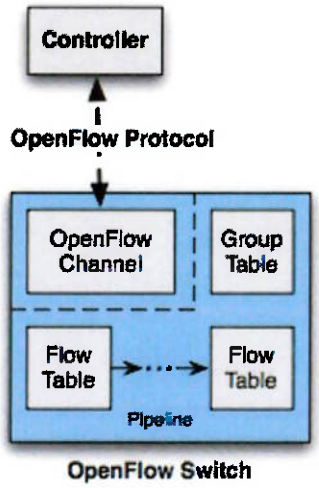
O OpenFlow chama atenção por se tratar de uma plataforma que pode resolver os problemas da geração de novos ambientes experimentais de rede, uma vez que sua principal característica é a separação do plano de dados do plano de controle. Utilizando meca-

nismos de virtualização de redes como o FlowVisor, que permite dividir a rede em fatias (*slices*), será possível manter separado a rede de experimentação da rede de produção (Kanaumi *et al.*, 2012).

4.1 Componentes de um Switch OpenFlow

Um switch OpenFlow possui uma ou mais tabelas de fluxos e uma tabela de grupo para a execução de pesquisas e encaminhamento de pacotes, além de um canal de comunicação com um controlador externo (Figura 9). O switch se comunica com o controlador e o controlador gerencia o switch por meio do protocolo OpenFlow (ONF, 2013b).

Figura 9: Principais componentes de um switch OpenFlow



Fonte: (ONF, 2013b)

Cabe a cada componente a execução de uma determinada tarefa. Abaixo é listado uma breve descrição de cada componente.

- Tabela de Fluxo: contém uma lista com as entradas de fluxos. É a responsável por indicar o tratamento que será dado aos pacotes de um determinado fluxo.
- Tabela de Grupo: contém entradas de grupo. Grupos fornecem uma maneira eficiente para direcionar um mesmo conjunto de ações para vários fluxos.
- Canal de Comunicação: conecta cada switch OpenFlow ao controlador. Pode fazer uso de criptografia (TLS ou SSL), mas também pode ser executado diretamente sobre o TCP.
- Controlador: responsável por adicionar, atualizar ou excluir entradas de fluxos em uma tabela de fluxos, de maneira reativa ou pró-ativa.

- Protocolo OpenFlow: protocolo utilizado para a comunicação entre o switch e o controlador.

Um switch OpenFlow se conecta com outros switches OpenFlows usando portas OpenFlow. Um switch OpenFlow deve ter suporte a três tipos de portas: porta física, porta lógica e porta reservada. Portas físicas correspondem diretamente a uma interface do hardware, enquanto as portas lógicas são abstrações de alto nível. Portas reservadas lidam com instruções de encaminhamento usando métodos de um switch tradicional. Existem no mercado switches do tipo *OpenFlow-Only*, que possuem suporte apenas as operações OpenFlow, e switches do tipo *OpenFlow-Hybrid*, que possuem suporte as operações OpenFlow e as operações de um switch *Ethernet*.

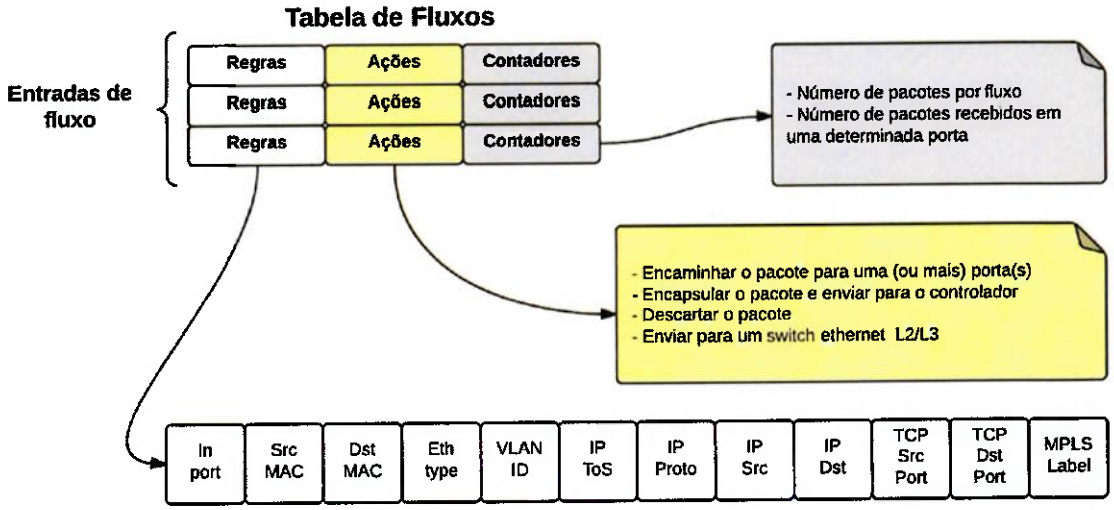
4.2 Funcionamento

O controlador é o responsável pela transmissão das regras e ações que definem o comportamento da rede. Ele transmite estas regras para todos os dispositivos com suporte OpenFlow, como comutadores, roteadores e pontos de acesso sem fio. Para que isso aconteça, o OpenFlow possui um protocolo padrão (Rothenberg *et al.*, 2011). Os equipamentos com suporte ao OpenFlow e o controlador se comunicam por meio do protocolo OpenFlow, que define mensagens como: *packet-received, send-packet-out, modify-forwarding-table,* e *get-stats*.

A partir da versão 1.1, o OpenFlow passou a permitir o uso de uma ou mais tabelas de fluxos, assim, o plano de dados passou a ser formado por um conjunto de tabelas, chamado *pipeline* do OpenFlow. Uma tabela de fluxo pode armazenar várias entradas de fluxo. Cada entrada na tabela de fluxo contém os seguintes itens: regra, ação e contador (Figura 10). A regra define o fluxo e é formada com base nos valores presentes nos campos do cabeçalho do pacote. As ações definem como os pacotes devem ser processados, por exemplo, encaminhar o pacote para uma determinada porta, descartar o pacote, modificar o TTL, VLAN, atribuir QoS, etc. O contador é utilizado para manter estatísticas de utilização, por exemplo, guardar o número de pacotes para cada fluxo ou a quantidade de pacotes ou bytes recebidos em uma determinada porta, além de registrar o tempo de armazenamento para cada fluxo.

O *pipeline* OpenFlow define como os pacotes vão interagir com as tabelas de fluxos (Figura 11). As tabelas de fluxos são numeradas sequencialmente, começando do zero, e os pacotes de entrada são primeiramente comparados com as entradas presentes na primeira tabela. Quando os pacotes de entrada correspondem a uma determinada tabela de fluxo, o contador é incrementado e as ações para aquele conjunto de instruções são realizadas. Essas instruções podem direcionar os pacotes para uma outra tabela de fluxo (apenas

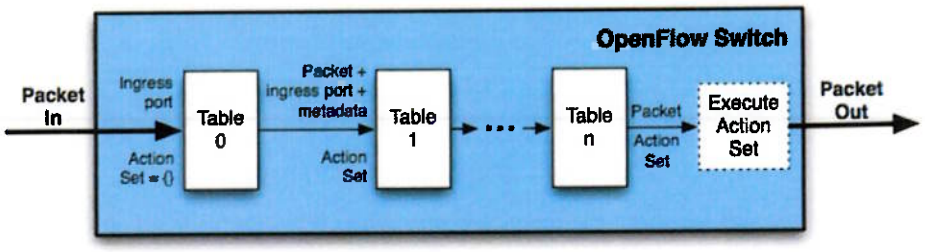
Figura 10: Estrutura da tabela de fluxos do OpenFlow



Fonte: (Stanford University, 2010) - Adaptado pelo autor.

para tabelas que possuem número maior que a tabela de origem), e assim uma nova busca por instruções será realizada. Um novo fluxo poderá ser criado quando um pacote não corresponder a nenhuma entrada na tabela de fluxo. Neste caso, o switch pode descartar o pacote ou então enviar o pacote para o controlador. O controlador então define um novo fluxo para esse pacote e cria uma ou mais entradas na tabela de fluxo. Essa entrada ou entradas são enviadas para os switches e, na sequencia, o pacote é enviado de volta para o switch para ser executado de acordo com esta nova regra.

Figura 11: Uma busca pode ser realizada em diferentes tabelas de fluxos

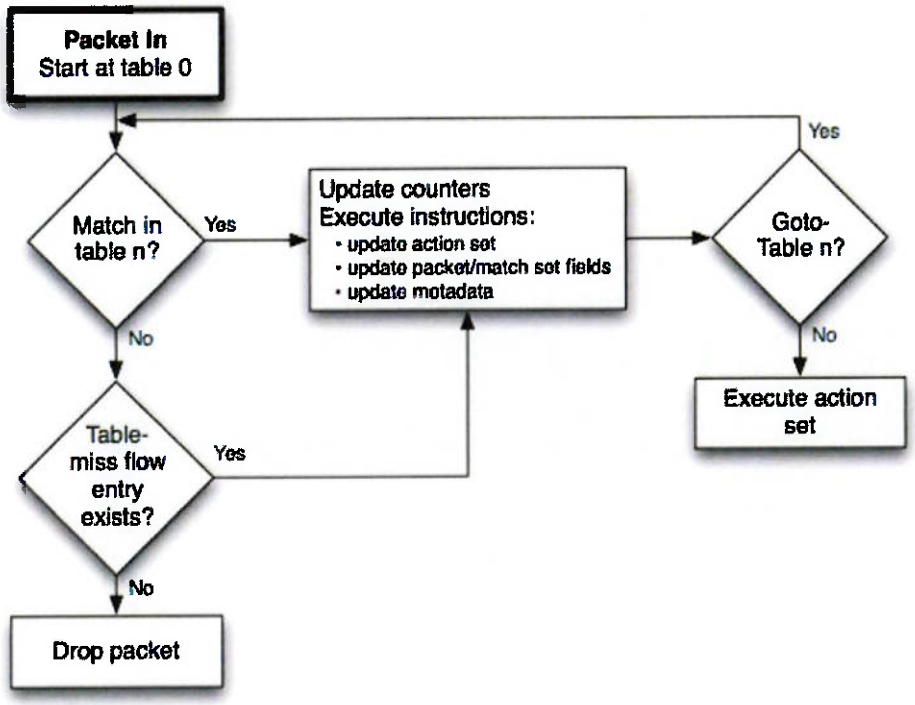


Fonte: (ONF, 2013b)

A figura 12 ilustra como um pacote é tratado em um Switch OpenFlow. Os campos usados para buscar uma entrada nas tabelas de fluxos dependem basicamente do tipo do pacote. Por exemplo, pode ser utilizado o endereço *Ethernet* de origem, o endereço IPv4 de destino ou a porta utilizada por determinado serviço.

Entradas de fluxo são retiradas das tabelas de fluxos em três ocasiões: através de um

Figura 12: Fluxo de um pacote em um switch OpenFlow



Fonte: (ONF, 2013b)

pedido do controlador, pelo mecanismo de expiração do fluxo ou por um mecanismo opcional de liberação de recursos. O controlador pode remover entradas de fluxos enviando mensagens para o switch ou então quando um grupo é apagado. O mecanismo de expiração é executado no switch independentemente de uma ação do controlador e é baseado no estado e na configuração de um fluxo de entrada. Já o mecanismo opcional é acionado apenas quando o switch necessita de recursos e ocorre somente na tabela de fluxo onde o mecanismo foi explicitamente configurado. A escolha de qual entrada de fluxo será desocupada é definido pelo switch e depende de parâmetros da entrada de fluxo.

4.3 Protocolo OpenFlow

A IANA - *Internet Assigned Numbers Authority* - atribuiu ao OpenFlow a porta TCP 6653. O uso das portas 6633 e 976, que eram anteriormente utilizadas, foram descontinuadas (ONF, 2013b). O protocolo OpenFlow possui suporte a três tipos de mensagens: *controller-to-switch* (controlador para switch), *asynchronous* (assíncronas), e *symmetric* (simétrica). Esses três tipos, mencionados por Fernandez (2013), Bakshi (2013) e ONF (2013b), são descritos abaixo:

- Mensagens do tipo controlador para switch são enviadas pelo controlador e pode ou não requisitar uma resposta do switch. Estas mensagens servem para:

  - Adicionar, excluir e modificar definições de fluxos e grupos;
  - Solicitar informações sobre as capacidades básicas do switch;
  - Coletar informações sobre as configurações atuais e algumas estatísticas;
  - Enviar de volta um pacote para o switch para que ele seja executado de acordo com as regras de um novo fluxo;
  - Tipos de mensagens: *Features, Configuration, Modify-State, Read-State, Packet-out, Barrier, Role-Request* e *Asynchronous-Configuration.*

- Mensagens assíncronas são enviadas pelo switch para:
  - Enviar para o controlador um pacote que não corresponde a um fluxo existente;
  - Informar o controlador que uma entrada de fluxo foi removida da tabela de fluxo;
  - Informar o controlador sobre uma mudança de status em uma porta ou de um erro ocorrido no switch;
  - Tipos de mensagens: *Packet-in, Flow-Removed* e *Port-status.*

- Mensagens simétricas podem ser enviadas pelo switch ou pelo controlador e são utilizadas para:
  - Trocar mensagens durante a inicialização;
  - Verificar se a conexão está ativa;
  - Checar a latência ou largura de banda;
  - Fornecer um caminho para futuras extensões e revisões da tecnologia OpenFlow;
  - Tipos de mensagens: *Hello, Echo, Error* e *Experimenter.*

4.4 Considerações do Capítulo

Este capítulo apresenta o desenvolvimento histórico e o funcionamento da principal tecnologia SDN da atualidade, o OpenFlow.

SDN VS REDES TRADICIONAIS

As SDNs mudaram completamente a forma de operação das redes de computadores. Consequentemente, uma série de vantagens e desvantagens podem ser observadas em cada modelo. O OpenFlow é a forma de SDN mais conhecida atualmente e ganhou ainda mais força depois que o Google anunciou que está utilizando este método para interligar seus *Data Centers* (Jain *et al.*, 2013). Contudo, o OpenFlow é uma abordagem recente e que ainda requer estudos, melhorias e testes. Diferente das SDNs, as redes tradicionais contam com uma gama de produtos e tecnologias comprovadamente testadas, certificadas e que estão em operação a muitos anos. Diante disso, enquanto alguns administradores de redes já estão realizando seus experimentos com SDN, outros, mais conservadores, preferem esperar o amadurecimento desta nova abordagem.

Este capítulo faz uma comparação entre as redes tradicionais e as SDNs de requisitos que são importantes em uma rede acadêmica. Um resumo de como determinados itens são obtidos nos dois modelos de rede são apresentados na tabela 3.

5.1 Inovação

A Internet possui atualmente um grande número de normas. Estas normas são descritas nas RFCs - *Request for Comments*. O processo de criação de um novo padrão costuma ser complexo e demorado. Antes de se tornar um padrão, o documento é chamado de *Internet Draft*. Esse documento passa por uma série de revisões até ser aceito e publicado. Algumas RFCs são consideradas Padrões de Internet (*Internet Standard - STD*), mas para isso elas devem obedecer o que está descrito em outra RFC, a RFC 2026 (Bradner, 1996). Após a publicação de uma RFC, ainda é preciso aguardar que os fabricantes façam a implantação em seus produtos. Este lento processo de padronização acaba frustrando os pesquisadores e desestimulando a inovação.

Com a adoção de SDN, os pesquisadores não ficam presos aos programas proprietários dos fabricantes, portanto, inovar não deverá ser um problema. Para implementar algo novo, basta programar a rotina no controlador.

Tabela 3: Solução tradicional vs solução em SDN

Item	Solução Tradicional	Solução em SDN
Inovação	Escrever um *Draft*, submeter ao IETF, aguardar ser aceito e publicado e depois aguardar que os fabricantes implementem a ideia.	Programar o que se deseja diretamente no controlador.
Gerência da rede	CLI, *scripts*, SNMP e ferramentas de gerência	Controlador com ferramenta de gestão para definir políticas e dar uma visão mais dinâmica de toda a rede. Sem configurações manuais nos dispositivos.
Custos	Switches possuem suporte a milhares de protocolos, o que encarece os dispositivos	Switches podem ser simples, pois a inteligência da rede estará no controlador. O controlador pode ser um PC comum.
Segurança	ACLs, IDS/IPS, 802.1X, autenticação via MAC, uso de diferentes ferramentas.	Regras mais granulares com base no contexto do usuário. Aplicação dinâmica das políticas de segurança. Permitir que as políticas sejam dissociadas do perímetro físico, o que é especialmente importante para usuários móveis. Garantir a segurança do controlador é de extrema importância.
Mobilidade e BYOD	IP Móvel, QoS e VLANs.	Uso de switches e APs que suportem SDN para reconhecer usuários e dispositivos e fornecer as mesmas políticas de acesso. Controle mais granular sobre o tráfego.

5.2 Gerência da rede

Gerenciar uma rede de grande porte é um desafio imenso. Uma rede tradicional pode fazer uso de dezenas ou centenas de equipamentos e o administrador de rede precisa configurar individualmente cada dispositivo. Portanto, a execução de determinadas tarefas, como aplicar parâmetros de QoS ou criação de uma nova VLAN, faz com que o administrador de rede tenha que manualmente alterar as configurações dos equipamentos envolvidos. Este tipo de tarefa seria simplificada em uma arquitetura SDN, pois o administrador de rede precisaria apenas configurar o controlador, ou dependendo da configuração utilizada, um pequeno conjunto de controladores. Uma vez configurado, o controlador ficaria responsável por encaminhar as nova regras para os dispositivos apropriados.

Outro problema comumente encontrado nas redes tradicionais é o uso de equipamentos de diferentes fabricantes. O problema é que não existe um padrão de sintaxe nas interfaces de linhas de comando, o que faz com que cada fabricante implemente seu próprio CLI. Embora os protocolos padrões possam ser implementados em dispositivos de diferentes marcas, o método utilizado para realizar a configuração pode ser diferente de um fabricante para outro.

Alternativas para facilitar a gerência em uma rede tradicional estão sendo difundidas. Algumas pessoas argumentam que tecnologias como o NETCONF e o YANG podem resolver parte do problema que o OpenFlow se propõem a fazer, mas sem a necessidade de mudanças significativas na rede. O NETCONF é um protocolo para troca de informações de configuração. Ele é baseado em XML, utiliza *Remote Procedure Calls* (RPC) e pode operar com o uso de protocolos como SSH, TLS, SOAP ou BEEP. O Yang é a linguagem de modelagem de dados utilizado pelo NETCONF. Apesar do protocolo NETCONF permitir a modificação e a configuração de dispositivos de rede, ele é diferente do OpenFlow que permite a modificação da tabela de encaminhamento. Schönwälder *et al.* (2010) descrevem o NETCONF e o YANG com maiores detalhes.

NETCONF e OpenFlow também podem trabalhar em conjunto dentro de uma SDN. A ONF tem difundido o *OpenFlow Management and Configuration Protocol* (OF-Config) com o objetivo de permitir a configuração remota de *datapaths* OpenFlow. Este protocolo exige que dispositivos com suporte ao OF-Config implementem o protocolo NETCONF (ONF, 2013a).

5.3 Custos

SDN tem sido apontado como uma alternativa para reduzir o CAPEX (despesas de capital) e o OPEX (despesas operacionais). Segundo Celentano (2008), CAPEX é uma das métricas mais utilizadas por empresas de telecomunicações para determinar a direção e o nível de investimento em equipamentos e serviços de rede.

Um dos itens que costumam ser estudados para a redução do CAPEX são os equipamentos de rede. Os equipamentos usados atualmente possuem um custo elevado, pois a inteligência da rede está toda depositada nestes dispositivos. A tendência é que os equipamentos de rede fiquem mais baratos com a introdução das SDNs, já que a inteligência da rede passará dos dispositivos para o controlador.

Com o uso das Redes Definidas por Software, os administradores de rede terão uma visão geral da topologia da rede e poderão avaliar com maior precisão a necessidade de atu-

alizações e melhorias, o que pode resultar em economia de CAPEX. Esta possibilidade já foi levantada por Naudts *et al.* (2012) em uma análise técnico-econômica de SDN em redes móveis. Neste estudo, os autores concluíram que os benefícios obtidos com SDN superaram os eventuais custos extras.

Os switches atuais precisam dar suporte a milhares de protocolos e, obviamente, alguém precisa saber configurá-los. Com equipamentos complexos, as equipes de operações acabam sendo sobrecarregadas. As equipes de TI precisam configurar, gerenciar e dar suporte em todas as camadas de rede. Com SDN será possível automatizar algumas operações de rede, portanto, é esperado que SDN auxilie também com a redução do OPEX.

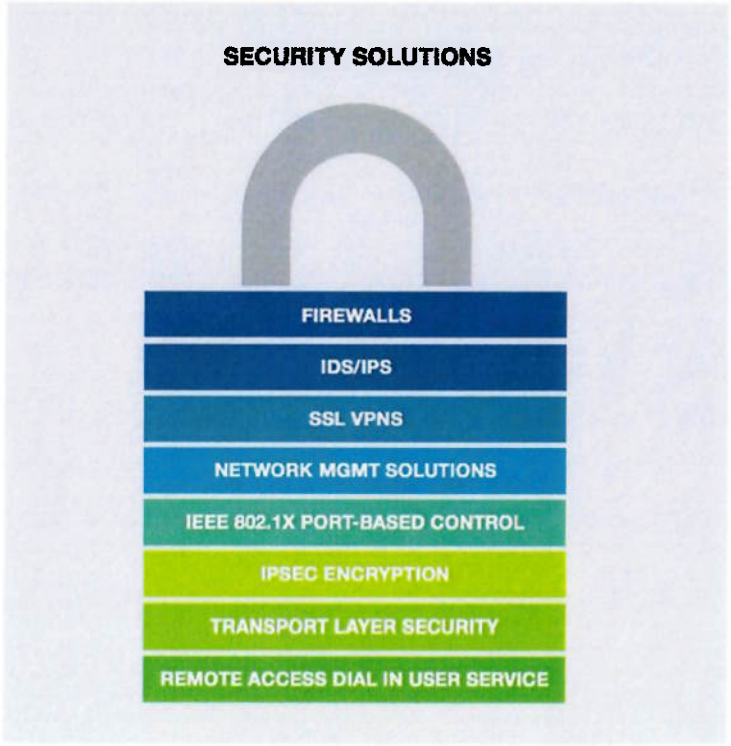
5.4 Segurança

Segundo a ISO (2005) a segurança da informação é obtida a partir da implementação de um conjunto de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Existe, porém, uma certa complexidade em encontrar um equilíbrio na hora de implementar soluções que atendam os princípios fundamentais da segurança da informação (confidencialidade, integridade e disponibilidade) e que tenham uma boa relação custo-benefício.

Nas redes tradicionais, inúmeras soluções de segurança, protocolos e equipamentos são utilizados na tentativa de se proteger contra diferentes tipos de ameaças (Figura 13). As políticas são geralmente definidas nos dispositivos, não nos serviços e aplicações. Consequentemente, as soluções de segurança se esforçam para mitigar os riscos de forma rápida, automatizada e em equipamentos de múltiplos fornecedores. Além disso, as soluções existentes nas redes atuais costumam ser caras, complexas, inflexíveis, altamente proprietárias e difíceis de serem implantadas e gerenciadas (ONF, 2013d).

Teoricamente, as SDNs vão deixar as redes mais seguras. Com a virtualização da rede, muitas operações poderão ser automatizadas, o que resultará em uma rede menos propensa as falhas humanas. Entretanto, assim como em qualquer outro sistema em desenvolvimento, novos riscos serão introduzidos. Em uma SDN, a segurança estará focada principalmente no controlador. Garantir a segurança do controlador será de fundamental importância, uma vez que ele será o elemento principal da rede. Onde colocar, para quem dar acesso e como configurar e auditar o controlador serão os desafios dos administradores de redes. Além disso, será preciso garantir a segurança entre controladores e dispositivos (usando,

Figura 13: Soluções de segurança disponíveis nas redes atuais.



Fonte: (ONF, 2013d)

por exemplo, certificados para a autenticação e criptografia para a segurança na conexão). Também será preciso prover métodos para garantir a disponibilidade dos controladores.

5.5 Mobilidade

Antigamente não era difícil prever a largura de banda necessária para uma determinada região. Os usuários utilizavam a internet discada, DSL ou cabo. Estes usuários eram fixos, o que fazia com que o número de usuários e o limite da banda fossem conhecidos. Com o advento das redes sem fios e dos diferentes tipos de dispositivos (celulares, tablets, notebooks, etc) que podem ser utilizados para acessar à Internet, fazer este tipo de estimativa e fornecer um serviço de qualidade deixou de ser uma tarefa trivial.

A mobilidade é um quesito que deixa a desejar nas redes tradicionais devido a forma como o TCP/IP opera. O protocolo IP atribui um endereço único para cada dispositivo conectado à Internet, mas da forma como o protocolo foi criado, se o dispositivo for levado para um outro local, existe a necessidade de alterar o endereço IP, o que resulta na quebra das conexões TCP já estabelecidas.

Para obter mobilidade nas redes tradicionais foi desenvolvido o IP Móvel (Perkins, 2010). O IP Móvel permite que os dispositivos mudem seu ponto de conexão com à Internet

mantendo todas as comunicações já estabelecidas e utilizando o mesmo endereço IP de origem. Os dispositivos são identificados por um *Home Address* independentemente do atual ponto de conexão com à Internet. Contudo, o IP Móvel possui alguns problemas de segurança e confiabilidade, além de limitações resultantes do roteamento triangular e de atrasos na entrega de pacotes dependendo da distância entre o *Home Agent* e o *Foreign Agent*.

Nas SDNs a mobilidade poderá ser obtida utilizando, por exemplo, pontos de acesso sem fio com suporte ao OpenFlow. Quando um dispositivo se mover e houver a necessidade de alterar seu ponto de conexão com à Internet, o controlador executará as ações necessárias para realizar a alteração dinâmica das tabelas de fluxos entre switches, permitindo assim a redefinição das rotas utilizadas.

As SDNs também podem auxiliar na mobilidade das VMs presentes nos grandes *data centers*. Estas organizações realizam com certa frequência a migração de VMs sem a interrupção do serviço e sem que os usuários percebam. Estas ações são conhecidas por *live* ou *hot migration*. Normalmente a migração em tempo real gera um aumento no domínio de *broadcast*, pois é preciso garantir que a VM possa ser alcançada após a migração usando o mesmo endereço. Esta prática resulta no aumento do número de VLANs e em um enorme desafio para os administradores de redes. O VLAN ID é limitado em 12 bits, o que permite a criação de um pouco mais do que 4000 VLANs, um número insuficiente para os grandes *datacenters*. Para contornar estes problemas, SDN e virtualização de redes estão sendo estudados. O uso de Redes Virtuais Sobrepostas (*Virtual Overlay Networks*) resolve o problema da limitação de VLANs permitindo que o tráfego de camada 2 passe a ser executado em camada 3. Desta forma, quando um dispositivo mudar de posição, será alterado também a sua rede virtual.

5.6 Considerações do Capítulo

Este capítulo apresentou uma comparação entre as redes tradicionais e as SDNs. Alguns quesitos considerados importantes para uma rede acadêmica foram analisados com o intuito de apoiar a análise das vantagens e desvantagens de se utilizar uma SDN em um ambiente acadêmico.

SDN EM AMBIENTE ACADÊMICO

Com o intuito de minimizar os problemas de consumo de energia, roteamento e virtualização, a adoção de SDN em *data centers* tem sido bastante utilizada. Contudo, SDN também pode ser utilizado em outros tipos de ambientes, tais como: redes móveis, redes domésticas, redes corporativas e redes acadêmicas (de ensino e pesquisa). Estes ambientes possuem necessidades distintas, mas que também podem ser atendidas por meio das SDNs.

Este capítulo abordará como os ambientes acadêmicos poderão se beneficiar com a adoção das redes definidas por software.

6.1 Desafios das atuais redes acadêmicas

As redes dos câmpus universitários possuem necessidades que obrigam as equipes de TI a atenderem diferentes tipos de usuários (alunos, professores, pesquisadores, funcionários, visitantes, etc), dispositivos (notebook, desktop, celular, tablet, etc), aplicações (internet, sistemas financeiros, educacionais e de segurança, etc) e conexões (cabeada, sem fio, VPN, 3G, etc).

Por se tratar de uma rede heterogênea, as redes acadêmicas são difíceis de serem gerenciadas. Isto costuma elevar os custos e prejudicar escalabilidade e a confiabilidade. Alterações nas configurações da rede podem ser demoradas e como elas precisam ser realizadas de forma individual, elas ainda estão sujeitas a erros (ONF, 2013c).

6.2 Cenários de uso

SDN pode ser utilizado em uma rede acadêmica para:

- obter uma infraestrutura de experimentação de novas arquiteturas de rede.
- melhor atender as necessidades de comunicação em aplicações científicas de alto desempenho (*Science DMZ*).
- facilitar a comunicação e o desenvolvimento de pesquisas científicas entre diferentes pesquisadores e instituições.

- lidar com grandes volumes de dados (*Big Data*) gerados nas áreas de ciências biológicas, astrofísica, física nuclear, etc.

6.3 Vantagens das SDNs

Abaixo são listados alguns benefícios que as redes definidas por software podem oferecer para as redes acadêmicas.

6.3.1 Redes lógicas

Bakshi (2013) cita que as universidades serão beneficiadas com o recurso de fatiamento de rede (*Networking Slice*) que as SDNs proporcionam. Este recurso permite a criação de redes lógicas isoladas que seriam particularmente úteis em ambientes acadêmicos que estão em constantes mudanças e que precisam atender cada vez mais usuários com diferentes necessidades. Além disso, o autor comenta que os centros de computação das universidades geralmente utilizam redes isoladas para a realização de experimentos, mas que muitas vezes existe a necessidade de se comunicar com outras redes acadêmicas. Assim, com a gerência do plano de controle fora dos dispositivos de rede e centralizado no controlador, SDN se torna um ajuste natural a essa necessidade. Flowvisor (Sherwood *et al.*, 2009), AutoSlice (Bozakov e Papadimitriou, 2012) e Pyretic (Reich *et al.*, 2013) são exemplos de tecnologias que as universidades poderão utilizar para criar os *slices* de rede mantendo a integridade da rede de produção.

Segundo (ONF, 2013c) a virtualização da rede também é vantajosa porque é rápida de ser criada e não impacta outras redes lógicas. Além disso, ela melhora a disponibilidade, uma vez que caminhos alternativos podem ser pré-populados.

6.3.2 Redução de custos

As universidades públicas do Brasil precisam lidar com a escassez de recursos financeiros, o que as obrigam a empregar com sabedoria os recursos destinados para TI. SDN deverá auxiliar na redução das despesas com a utilização da virtualização. A virtualização das redes maximiza o uso dos dispositivos e minimiza o espaço utilizado e o consumo de energia.

Outro aspecto importante é que as SDNs permitem a utilização de interfaces, padrões, APIs e programas de código aberto. Esse suporte a sistemas abertos e interoperáveis permitirá que os administradores de redes criem seus próprios programas ou façam uso de outros sistemas de código aberto, o que deverá contribuir para a redução dos custos.

6.3.3 Simplicidade

Poder programar todos os requisitos necessários e ter uma visão geral da rede a partir de um ponto central deve facilitar o trabalho dos administradores de rede. Configurações isoladas de dezenas de dispositivos de rede não serão mais necessários, o que deve contribuir para redução das falhas decorrentes de erros na configuração. Além disso, SDN promove a interoperabilidade entre dispositivos de diferentes fabricantes, o que simplifica a gerência da rede.

6.3.4 Desempenho e flexibilidade

Os avanços computacionais e a facilidade em se obter grande capacidade de armazenamento fazem com que novas formas de se comunicar sejam estudadas e desenvolvidas. Estes estudos serão particularmente úteis nos laboratórios de pesquisa devido as enormes quantidades de dados que muitos cientistas trabalham. Hoje em dia não é incomum encontrar projetos que precisem movimentar informações com tamanhos de algumas dezenas de *Gigabytes* até alguns *Terabytes*. Esta grande quantidade de dados gera um enorme impacto nas redes acadêmicas.

SDN também será útil para as instituições que queiram implementar uma *Science DMZ*. Uma *Science DMZ* é um um ambiente de rede otimizado para a transferência de dados com alto desempenho, voltado para aplicações científicas. Estas redes são implementadas dentro ou próximo das redes acadêmicas e possuem algumas configurações, principalmente as relacionadas com segurança, otimizadas para a obtenção de melhor desempenho. A tabela 4 mostra a diferença entre uma rede corporativa e uma rede científica.

Tabela 4: Redes corporativas vs redes científicas

Quesito	**Rede Corporativa**	**Rede Cientifica**
Tipo de uso	Web, e-mail, sistemas de ERP, finanças, educacionais, etc.	Transferência de dados.
Tipo de fluxo	Grande número de fluxos consumindo pouca banda cada fluxo.	Pequeno número de fluxos consumindo muita banda.
Perda de pacotes x desempenho	Pequena taxa de perda de pacotes não afeta o desempenho de forma significativa.	Pequena taxa de perda de pacotes afeta o desempenho de forma significativa.
Segurança	Filtragem complexa (uso de firewalls, IDS, proxies, etc).	Controle simples.

Dados científicos estão crescendo em volume e em valor, além disso, estes dados precisam ser analisados, e para isso eles são geralmente compartilhados entre diferentes cientistas. SDN pode fazer o gerenciamento de uma *Science DMZ* de forma mais fácil. A flexibili-

dade de uma SDN permitirá que as redes se adaptem mais facilmente e dinamicamente às mudanças de volume de dados quando comparado com as redes tradicionais.

6.3.5 Inovação e colaboração com outras universidades

Com a criação das redes virtuais, cientistas de redes poderão utilizar as SDNs para colocar em prática seus experimentos. Novas arquiteturas ou protocolos poderão ser testados sem comprometer a rede de produção.

Atualmente existe muita colaboração entre pesquisadores, professores e estudantes que trabalham em diferentes instituições e em diferentes países. Esse trabalho em conjunto, que muitas vezes envolvem a transferência de uma grande quantidade de dados, somado ao uso de vídeo-conferência para a discussão dos trabalhos, contribui substancialmente para o aumento da banda utilizada por cada instituição.

Novos projetos para a evolução das redes surgem a todo momento. Hoje já é possível encontrar redes com capacidade de operar a 100 Gbps. No Brasil, a rede ANSP fez no segundo semestre de 2013 uma demonstração de um sistema DWDM a 100 Gbps por canal óptico. Na ocasião, a conexão foi estabelecida entre a Unicamp e o CCE-USP, uma distância aproximada de 130 km.

O avanço da ciência depende cada vez mais do avanço da tecnologia e das redes de computadores. A criação de ambientes colaborativos deve auxiliar no desenvolvimento de novos projetos e as SDNs devem facilitar a criação destes ambientes e ajudar com a gerência das redes de alta capacidade.

6.4 Desvantagens das SDNs

Seja no meio acadêmico ou não, a principal preocupação dos administradores de redes em implantar uma SDN é o fato dela ainda não estar consolidada. Por se tratar de um conceito que altera radicalmente o modo de operação de uma rede, muitas dúvidas acabam surgindo. Abaixo estão listados as principais desvantagens das Redes Definidas por Software.

6.4.1 Incerteza

Apesar do Openflow ser o modelo de maior sucesso, ainda existe muita incerteza sobre o futuro das Redes Definidas por Software. Existem diferentes tecnologias e abordagens no mercado para criar uma SDN, porém algumas são tão imaturas que acabam contribuindo apenas para gerar mais dúvidas. Fabricantes e fornecedores possuem uma boa parcela de

culpa em toda esta confusão, pois cada um tem uma definição, um plano e um produto para oferecer.

Outra dúvida natural que surge com a criação de uma nova tecnologia é se ela é suficientemente segura e se ela traz os benefícios que são prometidos. É difícil encontrar materiais que descrevem como foi ou como está sendo a implantação de SDN nas universidades ou nas empresas, além disso, a implantação de SDN em um determinado ambiente pode não refletir as necessidades de outro ambiente.

6.4.2 Padrão não estabelecido

Os produtos e padrões em SDN são considerados imaturos, pois ainda estão em desenvolvimento. Alguns fabricantes criaram seus próprios padrões, o que obviamente limita a interoperabilidade. A arquitetura OpenFlow vista neste trabalho também não possui interoperabilidade garantida, pois os fabricantes ainda estão nos estágios iniciais de sua implantação.

A ONF, organização que gerencia o OpenFlow, concentrou esforços na padronização da comunicação da infraestrutura da rede com o controlador (*southbound*) e pouco fez para tentar buscar a padronização da comunicação entre o controlador e os aplicativos (*northbound*). Essa atitude tem um motivo relevante, os cientistas afirmam que a padronização da *northbound* pode inibir a inovação. Padrões são ótimos para garantir a interoperabilidade, mas para isso é preciso que os requisitos estejam bem definidos.

6.5 Considerações do Capítulo

Este capítulo apresentou os atuais desafios das redes acadêmicas e listou os possíveis cenários de uso para uma SDN em um ambiente acadêmico. Além disso, foram listadas algumas vantagens e algumas desvantagens das redes definidas por software.

CONSIDERAÇÕES FINAIS

Devido ao seu grande potencial de inovação, SDN é visto como a melhor alternativa para o futuro das redes de computadores. Embora ainda existam muitas dúvidas e a tecnologia ainda esteja em desenvolvimento, existe um grande otimismo que as SDNs deixem as redes mais flexíveis, dinâmicas, com melhor custo-benefício e mais fáceis de serem operadas e gerenciadas.

Obviamente, a transição de uma tecnologia já consolidada para outra ainda em desenvolvimento requer cuidados. Os administradores de redes devem definir estratégias para implementar SDN nas redes acadêmicas. O ideal é que seja realizado um projeto piloto para que a equipe de TI possa aprender e ganhar experiência com SDN.

Mesmo com toda a animação em torno das SDNs, é bem provável que sua introdução seja feita de forma gradual, devendo existir uma fase híbrida entre SDN e as redes tradicionais, assim como ocorre, por exemplo, com a implantação do IPv6, quando mecanismos de transição e de coexistência com a atual tecnologia IPv4 foram desenvolvidos. Este cenário deverá permitir o entendimento do SDN sem se expor completamente aos riscos de introduzir uma tecnologia que ainda não está totalmente consolidada.

7.1 Contribuições do Trabalho

Conforme pode ser visto nos capítulos Redes de Computadores - Conceitos, Evolução e Tecnologias, Redes Definidas por Software e OpenFlow, este trabalho apresentou conceitos, tecnologias e uma breve história das redes de computadores e das SDNs. No capítulo SDN vs Redes Tradicionais foi apresentado como cada tipo de rede lida com determinados requisitos, tais como: inovação, gerência da rede, custo, segurança e mobilidade. Este estudo mostrou que para os pesquisadores SDN terá grande utilidade no quesito inovação, já para os administradores de rede SDN será útil para a gerência da rede. No capítulo SDN em Ambiente Acadêmico foi apresentado as vantagens e as desvantagens das SDNs e listados os possíveis cenários de uso. No meio acadêmico, concluí-se que SDN poderá ser utilizado para a criação de uma infraestrutura de experimentação de novas arquiteturas de redes, para facilitar o desenvolvimento de pesquisas científicas entre diferentes instituições e para auxiliar no gerenciamento de uma *Science DMZ*. Para finalizar, este trabalho

mostrou que as redes acadêmicas podem aproveitar o que as SDNs têm de melhor e com isso facilitar o trabalho de professores, pesquisadores, alunos e funcionários.

7.2 Trabalhos Futuros

SDN não mudará apenas a forma como as redes de computadores serão operadas, ela mudará também o perfil dos engenheiros de rede. Um possível trabalho futuro seria investigar quais impactos SDN deverá trazer para os profissionais de redes. Alguns pontos que podem ser estudados é se SDN criará novas oportunidades ou se irá limitar os trabalhos dos profissionais de rede. Outras dúvidas que surgem com o advento das SDNs é se o conhecimento sobre as redes tradicionais deixará de ter valor e quais novas habilidades os profissionais de rede precisarão ter.

REFERÊNCIAS BIBLIOGRÁFICAS

Agarwal *et al.* **(2012)** A. Agarwal, R. Luniya, M. Bhatnagar, M. Gaikwad e V. R Inamdar. Reviewing the world of virtualization. Em *Third International Conference on Intelligent Systems, Modelling and Simulation, ISMS*, páginas 554–557. Citado na pág. 21

Alcober *et al.* **(2013)** J. Alcober, X. Hesselbach, A. de la Oliva, A. Garcia-Saavedra, D. Roldan e C. Bock. Internet future architectures for network and media independent services and protocols. Em *15th International Conference on Transparent Optical Networks, ICTON 2013*, páginas 1–4. Citado na pág. 18

Anderson *et al.* **(2005)** T. Anderson, L. Peterson, S. Shenker e J. Turner. Overcoming the Internet impasse through virtualization. *Computer*, 38(4):34–41. Citado na pág. 22

ANSP (2011) ANSP. Anuário ansp 2011. http://www.ansp.br/images/docs/publicacoes/ANUARIO_ANSP_2011_PT_TEXTO.pdf, 2011. Último acesso em 14/10/2013. Citado na pág. 18

ANSP (2014) ANSP. 5ª reunião semestral da ANSP, em São Paulo, coloca em debate a questão da segurança nas redes acadêmicas. http://www.ansp.br/images/docs/publicacoes/PORT_2014-05-06_Boletim%20ANSP%209.pdf, 2014. Último acesso em 29/06/2014. Citado na pág. 29

Bakshi (2013) K. Bakshi. Considerations for software defined networking (SDN): Approaches and use cases. Em *IEEE Aerospace Conference*, páginas 1–9. Citado na pág. 39, 48

Binu e Kumar (2011) A. Binu e G. S. Kumar. Virtualization techniques: A methodical review of XEN and KVM. Em *Advances in Computing and Communications - First International Conference, ACC*, volume 190, páginas 399–410. Citado na pág. 22

Bozakov e Papadimitriou (2012) Z. Bozakov e P. Papadimitriou. Autoslice: Automated and scalable slicing for software-defined networks. http://conferences.sigcomm.org/co-next/2012/eproceedings/student/p3.pdf, 2012. Último acesso em 03/07/2014. Citado na pág. 48

Bradner (1996) S. Bradner. RFC 2026: The internet standards process – revision 3, 1996. Citado na pág. 41

Cai e Natarajan (2013) D. Cai e S. Natarajan. The evolution of the carrier cloud networking. Em *Service Oriented System Engineering SOSE*, páginas 286–291. Citado na pág. 27

Calvert *et al.* **(1997)** K. Calvert, M. Doar, A. Nexion e E. Zegura. Modeling internet topology. *IEEE Communications Magazine*, 35(6):160 – 163. Citado na pág. 18

Celentano (2008) J. M. Celentano. Carrier capital expenditures. *IEEE Communications Magazine*, 46(7):82–88. Citado na pág. 43

Cerf (2004) V. G. Cerf. On the evolution of internet technologies. Em *Proceedings of the IEEE*, páginas 1360–1370. Citado na pág. 18

Cerf e Kahn (1974) V. G. Cerf e R. E. Kahn. A protocol for packet network intercommunication. *IEEE Transactions on Communications*, COM-22(5):637–648. Citado na pág. 17

Che *et al.* (2010) J. Che, C. Shi, Y. Yu e W. Lin. A synthetical performance evaluation of openVZ, xen and KVM. Em *IEEE Asia-Pacific Services Computing Conference, APSCC*, páginas 587–594. Citado na pág. 22

Chowdhury e Boutaba (2010) N. M. M. K. Chowdhury e R. Boutaba. A survey of network virtualization. *Computer Networks*, 54(5):862–876. Citado na pág. 24

Chown (2006) T. Chown. RFC 4554: Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks, 2006. Citado na pág. 25

Cisco (2013) Cisco. Cisco global cloud index: Forecast and methodology, 2012–2017. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.pdf, 2013. Último acesso em 02/11/2013. Citado na pág. 29

Colle *et al.* (2010) D. Colle, B. Jooris, P. Gurzi, M. Pickavet e P. Demeester. Network virtualization and programmability. Em *15th OptoeElectronics and Communications Conference, OECC*, páginas 414–415. Citado na pág. 22

Colpitts e Blackwell (1921) E. H. Colpitts e O. B. Blackwell. Carrier Current Telephony and Telegraphy. *Transactions of the American Institute of Electrical Engineers*, XL:205–300. Citado na pág. 16

Deering (1986) S. E. Deering. RFC 988: Host extensions for IP multicasting, 1986. Citado na pág. 18

Egevang e Francis (1994) K. Egevang e P. Francis. RFC 1631: The IP network address translator (NAT), 1994. Citado na pág. 18

Enterasys (2012) Enterasys. Software defined networking (SDN) in the enterprise. http://www.enterasys.com/company/literature/SDN_tsbrief.pdf, 2012. Último acesso em 18/10/2013. Citado na pág. 27

Feamster *et al.* (2013) N. Feamster, J. Rexford e E. Zegura. The road to SDN: An intellectual history of programmable networks. http://www.cs.princeton.edu/courses/archive/fall13/cos597E/papers/sdnhistory.pdf, 2013. Último acesso em 26/10/2013. Citado na pág. 27

Fernandez (2013) M. P. Fernandez. Comparing openflow controller paradigms scalability: Reactive and proactive. Em *27th IEEE International Conference on Advanced Information Networking and Applications, AINA*, páginas 1009–1016. Citado na pág. 39

Ferreira (2003) R. E. Ferreira. *Linux – Guia do Administrador do Sistema*. Novatec Editora. Citado na pág. 18

Fuller *et al.* (1993) V. Fuller, T. Li, J. Yu e K. Varadhan. RFC 1519: Classless inter-domain routing (CIDR): an address assignment and aggregation strategy, 1993. Citado na pág. 18

Gavras *et al.* (2007) A. Gavras, A. Karila, S. Fdida, M. May e M. Potts. Future internet research and experimentation: the FIRE initiative. *Computer Communication Review*, 37(3):89–92. Citado na pág. 26

GENI (2006) GENI. GENI design principles. *Computer*, 39(9):102–105. Citado na pág. 26

Grubesic e Murray (2005) T. H. Grubesic e A. T. Murray. Spatial–historical landscapes of telecommunication network survivability. *Telecommunications Policy*, 29(11): 801 – 820. Citado na pág. 16, 17

Haque *et al.* (2011) M. Haque, K. Pawlikowski e S. K. Ray. Challenges to development of multipurpose global federated testbed for future internet experimentation. Em *The 9th IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2011*, páginas 289–292. Citado na pág. 19

Harai (2009) H. Harai. Designing new-generation network - overview of akari architecture design. Em *Asia Communications and Photonics Conference and Exhibition, ACP*, páginas 1–2. Citado na pág. 26

HP (2012) HP. Realizing the power of SDN with HP virtual application networks. http://h17007.www1.hp.com/docs/interopny/4AA4-3871ENW.pdf, 2012. Último acesso em 24/10/2013. Citado na pág. 32

IBM (2012) IBM. Software defined networking: A new paradigm for virtual, dynamic, flexible networking. http://public.dhe.ibm.com/common/ssi/ecm/en/qcw03016usen/QCW03016USEN.PDF, 2012. Último acesso em 14/10/2013. Citado na pág. 19, 20

ISO (2005) ISO. Tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação, 2005. Citado na pág. 44

Jain *et al.* (2013) S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, J. Zolla, U. Hölzle, S. Stuart e A. Vahdat. B4: experience with a globally-deployed software defined wan. Em *ACM Special Interest Group on Data Communications, SIGCOMM'13*, páginas 3–14. Citado na pág. 41

Jinzhou *et al.* (2010) C. Jinzhou, W. Chunming, J. Ming e Z. A Dong. A review of future internet research programs and possible trends. Em *6th International Conference on Wireless Communications Networking and Mobile Computing, WiCOM 2010*, páginas 1–4. Citado na pág. 19

Kanaumi *et al.* (2012) Y. Kanaumi, S. Saito, E. Kawai, S. Ishii, K. Kobayashi e S. Shimojo. Deployment and operation of wide-area hybrid openflow networks. Em *Network Operations and Management Symposium*, páginas 1135–1142. Citado na pág. 36

Khan *et al.* (2012) A. Khan, A. Zugenmaier, D. Jurca e W. Kellerer. Network virtualization: a hypervisor for the internet? *IEEE Communications Magazine*, 50(1):136–143. Citado na pág. 23

Kim e Feamster (2013) H. Kim e N. Feamster. Improving network management with software defined networking. *IEEE Communications Magazine*, 51(2):114–119. Citado na pág. 19, 20

Kim *et al.* (2011) H. Kim, T. Benson, A. Akella e N. Feamster. The evolution of network configuration: a tale of two campuses. Em *Proceedings of the 11th ACM SIGCOMM Conference on Internet Measurement, IMC '11*, páginas 499–514. Citado na pág. 19

Kolhe e Dhage (2012) S. Kolhe e S. Dhage. Comparative study on virtual machine monitors for cloud. Em *World Congress on Information and Communication Technologies, WICT*, páginas 425–430. Citado na pág. 22

Li *et al.* (2010) Y. Li, W. Li e C. Jiang. A survey of virtual machine system: Current technology and future trends. Em *Third International Symposium on Electronic Commerce and Security, ISECS*, páginas 332–336. Citado na pág. 21

Little (1989) M. Little. RFC 1126: Goals and functional requirements for inter-autonomous system routing, 1989. Citado na pág. 18

Maathuis e Smit (2003) I. Maathuis e W. A. Smit. The battle between standards: TCP/IP vs OSI victory through path dependency or by quality? Em *The 3rd Conference on Standardization and Innovation in Information Technology*, páginas 161–176. Citado na pág. 17

McKeown *et al.* (2008) N. McKeown, T. Anderson, H. Balakrishnan, G. M. Parulkar, L. L. Peterson, J. Rexford, S. Shenker e J. S. Turner. Openflow: enabling innovation in campus networks. *Computer Communication Review*, 38(2):69–74. Citado na pág. 29, 35

McPherson e Dykes (2001) D. McPherson e B. Dykes. RFC 3069: VLAN Aggregation for Efficient IP Address Allocation, 2001. Citado na pág. 25

Meleis (1996) H. Meleis. Toward the information network. *IEEE Computer*, 29(10): 59–67. Citado na pág. 16

Mockapetris (1987) P. Mockapetris. RFC 988: Domain names - concepts and facilities., 1987. Citado na pág. 18

Mogul e Postel (1985) J. C. Mogul e J. Postel. RFC 950: Internet Standard Subnetting Procedure, 1985. Citado na pág. 18

Moreira *et al.* (2009) M. D. D. Moreira, N. C. Fernandes, L. H. M. K. Costa e O. C. M. B Duarte. Internet do futuro: Um novo horizonte. grupo de teleinformática e automação. http://www.gta.ufrj.br/ensino/cpe728/MFCD09.pdf, 2009. Último acesso em 15/10/2013. Citado na pág. 26

Nadeau (2011) T. Nadeau. Software driven networks problem statement. http://tools.ietf.org/html/draft-nadeau-sdn-problem-statement-00, 2011. Último acesso em 26/11/2013. Citado na pág. 28

Naudts *et al.* (2012) B. Naudts, M. Kind, F. Westphal, S. Verbrugge, D. Colle e M. Pickavet. Techno-economic analysis of software defined networking as architecture for the virtualization of a mobile network. Em *European Workshop on Software Defined Networking (EWSDN)*, páginas 67–72. Citado na pág. 44

ONF (2013a) ONF. Openflow management and configuration protocol (of-config 1.1.1). https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow-config/of-config-1-1-1.pdf, 2013a. Último acesso em 16/12/2013. Citado na pág. 43

ONF (2012) ONF. Software-defined networking: The new norm for networks. https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf, 2012. Último acesso em 18/10/2013. Citado na pág. 28, 30, 31

ONF (2013b) ONF. Openflow switch specification. https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.4.0.pdf, 2013b. Último acesso em 10/11/2013. Citado na pág. 36, 38, 39

ONF (2013c) ONF. SDN in the campus environment. https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-enterprise-campus.pdf, 2013c. Último acesso em 01/02/2014. Citado na pág. 47, 48

ONF (2013d) ONF. SDN security considerations in the data center. https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-security-data-center.pdf, 2013d. Último acesso em 17/12/2013. Citado na pág. 44, 45

Perkins (2010) C. Perkins. RFC 5944: Ip mobility support for ipv4, revised, 2010. Citado na pág. 45

Pitt (2013) D. Pitt. Trust in the cloud: the role of SDN. *Network Security*, 2013(3):5–6. Citado na pág. 31

Reich *et al.* (2013) J. Reich, C. Monsanto, N. Foster, J. Rexford e D. Walker. Modular SDN programming with pyretic. http://www.cs.princeton.edu/~jrex/papers/pyretic13.pdf, 2013. Último acesso em 03/07/2014. Citado na pág. 48

Risdianto e Mulyana (2012) A. C. Risdianto e E. Mulyana. Implementation and analysis of control and forwarding plane for SDN. Em *7th International Conference on Telecommunication Systems, Services, and Applications TSSA*, páginas 227–231. Citado na pág. 30

Rooney *et al.* (1998) S. Rooney, J. E. van der Merwe, S. A. Crosby e I. M. Leslie. The Tempest: A framework for safe, resource-assured programmable networks. *IEEE Communications Magazine*, 36(10):42–53. Citado na pág. 27

Rosenbaun *et al.* (2003) G. Rosenbaun, W. Lau e S. Jha. An analysis of virtual private network solutions. Em *28th Annual IEEE International Conference on Local Computer Networks, LCN '03*, páginas 395–404. Citado na pág. 25

Rothenberg *et al.* **(2011)** C. E. Rothenberg, M. R. Nascimento, M. R. Salvador e M. F. Magalhaes. Openflow e redes definidas por software: um novo paradigma de controle e inovação em redes de pacotes. *Cad. CPqD Tecnologia*, 37(1):65–76. Citado na pág. 30, 32, 37

Sallent *et al.* **(2012)** S. Sallent, A. Abelem, I. Machado, L. Bergesio, S. Fdida, J. F. Rezende, S. Azodolmolky, M. Salvador, L. N. Ciuffo e L. Tassiulas. FIBRE project: Brazil and europe unite forces and testbeds for the internet of the future. Em *Testbeds and Research Infrastructure. Development of Networks and Communities - 8th International ICST Conference, TridentCom 2012, Revised Selected Papers*, volume 44, página 372. Citado na pág. 26

Schönwälder *et al.* **(2010)** J. Schönwälder, M. Björklund e P. Shafer. Network configuration management using NETCONF and YANG. *IEEE Communications Magazine*, 48(9):166–173. Citado na pág. 43

Severance (2012) C. Severance. Vint cerf: A brief history of packets. *IEEE Computer*, 45(12):10–12. Citado na pág. 17

Sezer *et al.* **(2013)** S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller e N. Rao. Are we ready for SDN? implementation challenges for software-defined networks. *IEEE Communications Magazine*, 51(7):36–43. Citado na pág. 27

Sherwood *et al.* **(2009)** R. Sherwood, G. Gibby, K. Yapy, G. Appenzellery, M. Casado, N. McKeowny e G. Parulkary. Flowvisor: A network virtualization layer. http://archive.openflow.org/downloads/technicalreports/openflow-tr-2009-1-flowvisor.pdf, 2009. Último acesso em 01/02/2014. Citado na pág. 48

Shimonishi *et al.* **(2012)** H. Shimonishi, Y. Takamiya, Y. Chiba, K. Sugyo, Y. Hatano, K. Sonoda, K. Suzuki, D. Kotani e I. Akiyoshi. Programmable network using openflow for network researches and experiments. Em *The Sixth International Conference on Mobile Computing and Ubiquitous Networking*, páginas 164–171. Citado na pág. 35

Sridharan *et al.* **(2013)** M. Sridharan, A. Greenberg, Y. Wang, P. Garg, N. Venkataramiah, K. Duda, I. Ganga, G. Lin, M. Pearson, P. Thaler e C. Tumuluri. Nvgre: Network virtualization using generic routing encapsulation. http://tools.ietf.org/html/draft-sridharan-virtualization-nvgre-03, 2013. Último acesso em 25/11/2013. Citado na pág. 27

Stanford University (2010) Department of Computer Science Stanford University. Cs244 advanced topics in networking. http://yuba.stanford.edu/cs244wiki/index.php/Overview, 2010. Último acesso em 12/09/2014. Citado na pág. 38

Tanenbaum (2002) A. S. Tanenbaum. *Computer networks (4. ed.)*. Prentice Hall. Citado na pág. 15

Tootoonchian *et al.* **(2012)** A. Tootoonchian, S. Gorbunov, Y. Ganjali, M. Casado e R. Sherwood. On controller performance in software-defined networks. Em *Proceedings of the 2nd USENIX conference on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services*. Citado na pág. 33

Tredennick (1996) N. Tredennick. Microprocessor-based computers. *IEEE Computer*, 29(10):27–37. Citado na pág. 16

Vea (2010) A. Vea. The unknown history of the internet engineering the worldwide wiwiw project. Em *History of Telecommunications Conference (HISTELCON)*, páginas 1–9. Citado na pág. 17

Wang *et al.* (2013) A. Wang, M. Iyer, R. Dutta, G. N. Rouskas e I. N. Baldine. Network virtualization: Technologies, perspectives, and frontiers. *Lightwave Technology*, 31(4): 523–537. Citado na pág. 25

Wang *et al.* (2012) Q. Wang, D. Zhao e Z. Huang. Research on the performance of virtualization-based remote sensing data processing platform. Em *International Conference on Systems and Informatics, ICSAI*, páginas 900–904. Citado na pág. 22

Yin *et al.* (2012) H. Yin, H. Xie, T. Tsou, D. Lopez, P. Aranda e R. Sidi. SDNi: A message exchange protocol for software defined networks (SDNs) across multiple domains. http://tools.ietf.org/html/draft-yin-sdn-sdni-00, 2012. Último acesso em 25/10/2013. Citado na pág. 33