PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS – PUC-CAMPINAS
CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

DIEGO BERLIM MARCUSSO

SISTEMÁTICA PARA IMPLEMENTAÇÃO DE REDES DEFINIDAS POR *SOFTWARE* EM *DATA CENTER*

Campinas, SP
2017

DIEGO BERLIM MARCUSSO

SISTEMÁTICA PARA IMPLEMENTAÇÃO DE REDES DEFINIDAS POR *SOFTWARE* EM *DATA CENTER*

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Engenharia Elétrica, do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas, como requisito para obtenção do Título de Mestre em Engenharia Elétrica.

Orientador: Prof. Dr. Eric Alberto de Mello Fagotto

Campinas, SP

2017

DIEGO BERLIM MARCUSSO

SISTEMÁTICA PARA IMPLEMENTAÇÃO DE REDES DEFINIDAS POR SOFTWARE EM DATA CENTER

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre em Gestão de Redes de Telecomunicações.
Área de Concentração: Engenharia Elétrica.
Orientador: Prof. Dr. Eric Alberto de Mello Fagotto

Dissertação defendida e aprovada em 31 de agosto de 2017 pela Comissão Examinadora constituída dos seguintes professores:

Prof. Dr. Eric Alberto de Mello Fagotto
Orientador da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

Prof. Dr. Antônio Carlos Demanboro
Pontifícia Universidade Católica de Campinas

Prof. Dr. Edson Luiz Ursini
Universidade Estadual de Campinas

Ficha Catalográfica
Elaborada pelo Sistema de Bibliotecas e
Informação - SBI - PUC-Campinas

t621.382
M322s

Marcusso,Diego Berlim.
Sistemática para implementação de redes definidas por software em Data Center / Diego Berlim Marcusso. – Campinas: PUC-Campinas 2017
78p.

Orientador: Eric Alberto de Mello Fagotto.
Dissertação (mestrado) – Pontifícia Universidade Católica de Campinas, Centro de Ciências Exatas, Ambientais e de Tecnologias, Pós-Graduação em Engenharia Elétrica.
Inclui bibliografia

1. Sistema de telecomunicações. 2. Gestão de redes e serviços. 3. Redes de computadores. I Fagotto, Eric Alberto de Mello II. Pontifícia Universidade Católica de Campinas Centro de Ciências Exatas, Ambientais e de Tecnologias. Pós-Graduação em Engenharia Elétrica. III. Título.

22.ed. CDD – t621.382

Dedico este trabalho a Deus e à minha família,
responsáveis por tornarem meus sonhos realidade.

Agradeço ao meu orientador, Professor Doutor Eric Alberto de Mello Fagotto,
pelo estímulo e apoio durante esta trajetória;

À Pontifícia Universidade Católica de Campinas,
pela concessão da bolsa de estudos no Programa de Mestrado, sem a qual não seria possível finalizar este curso.

À IBM Brasil,
pelo tempo concedido para estudo e elaboração deste trabalho;

À Cisco Brasil,
pela concessão dos equipamentos durante a realização dos testes.

"O que sabemos é uma gota.
O que ignoramos é um océano."

Isaac Newton (1643-1727)

RESUMO

MARCUSSI, Diego Berlim. ***Sistemática para implementação de Redes Definidas por* Software *em* Data Center.** 78 f. Dissertação (Mestrado em Gestão de Redes de Telecomunicações) – Pontifícia Universidade Católica de Campinas. Centro de Ciências Exatas, Ambientais e de Tecnologias, Programa de Pós-Graduação em Engenharia Elétrica, Campinas, 2017.

O presente trabalho de dissertação tem como principal objetivo analisar as redes de comunicação de dados para *Data Centers*, que sofreram grande evolução técnica nos últimos anos devido a problemas e limitações das redes convencionais, como falta de disponibilidade na rede, baixo desempenho, utilização ineficiente dos componentes de rede instalados, complexidade e atraso no provisionamento de novas aplicações. Esses e outros problemas motivaram o desenvolvimento de novas tecnologias mais flexíveis e configuráveis de acordo com a necessidade particular de cada cliente. A tecnologia *Software Defined Networking* (SDN), presente na maioria dos fabricantes de equipamentos e soluções de rede, endereça esses problemas e traz mais eficiência e simplicidade no provisionamento de novos recursos de rede. Neste trabalho, será apresentada uma sistemática para implementação de SDN. O resultado obtido ilustra que tal sistemática pode ser aplicada em clientes que desejam implementar novas redes para *Data Center* ou migrar suas redes convencionais para o modelo SDN de forma estruturada, mapeando todas as necessidades técnicas e de negócio para implementação da rede, criando uma base de testes, determinando a solução mais adequada ao ambiente e testando-a em ambiente controlado.

Palavras-chave: Sistema de Telecomuicações, Gestão de redes, Redes de computadores.

ABSTRACT

MARCUSSO, Diego Berlim. ***Systematics for Implementation of Software Defined Networks in "Data Centers".*** 78 f. *Dissertation (Master in Management of Telecommunications Networks)* - Pontifícia Universidade Católica de Campinas. *Center for Exact, Environmental and Technological Sciences, Post-Graduation Program in Electrical Engineering*, Campinas, 2017.

The present dissertation work has as main objective analyses the Data communication networks for Data Centers, that *have undergone a major technical evolution in recent years due to problems and limitations of conventional networks, such as lack of network availability, poor performance, inefficient use of installed network components, complexity and agility in the provision of new applications. These and other problems motivated the development of new technologies more flexible and configurable according to the particular need of each client.* Software Defined Networking *(SDN) technology found in most network equipment and vendors addresses these issues and brings more efficiency and simplicity to the provisioning of new network resources. This work presents a method for implementing SDN in* Data Center *in Brazil and also a comparative that analyzes the conventional network model and the SDN based model. This comparison is made based on functional aspects such as provisioning,* Quality of Service *(QoS), security and others. In order to compare the two technologies, a scenario was created with several network nodes and simulated the provisioning of a new application with several network requirements. The result obtained shows that the systematics can be applied to clients that wish to implement new networks for* Data Center *or migrate their conventional networks to the SDN model in a structured way, mapping all technical and business needs for network implementation, creating a* database t*esting, determining the most appropriate solution for the environment and testing it in a controlled environment.*

Keywords: *Telecommunication Systems.* Network management. Computer Networks.

LISTA DE FIGURAS

Figura 1. Arquitetura Hierárquica para Redes Convencionais....22
Figura 2. Diagrama Conceitual do VSS....23
Figura 3. Modelo de Referência SDN....25
Figura 4. Modelo Clos (*Spine and Leaf*)....25
Figura 5. Estrutura do VXLAN....27
Figura 6. Construção da Política no ACI....31
Figura 7. VRF's....32
Figura 8. *Endpoint Groups*....33
Figura 9. *Endpoint como VLANs*....33
Figura 10. Contratos....34
Figura 11. Criação de Contratos....35
Figura 12. Fluxograma da Sistemática....37
Figura 13. Diagrama de Rede Convencional Testada....43
Figura 14. Diagrama de Rede SDN testada....44
Figura 15. Fluxograma para Ativação de *Switches*....50
Figura 16. Painel de Configuração dos *Switches*....52
Figura 17. Fluxograma para Ativação de Análise de Tráfego....53
Figura 18. Fluxo de Comunicação da Aplicação de Desenvolvimento....54
Figura 19. Uso de Portas TCP e UDP da Aplicação....54
Figura 20. Fluxograma para Ativação de Análise de Tráfego....56
Figura 21. Medição da Qualidade de Tráfego da Aplicação....58
Figura 22. Gráfico de Pacotes Enviados e Recebidos....58
Figura 23. Latência da Aplicação....59
Figura 24. Detalhes do Fluxo de Comunicação....59
Figura 25. Fluxograma para Implementação de Segurança....61
Figura 26. Funcionalidade para Simulação de Regras....62
Figura 27. Criação de Contrato....62
Figura 28. Painel de Verificação dos *Switches*....65
Figura 29. Painel de Situação do Sistema....65
Figura 30. Programação por XML....69
Figura 31. Configuração de *Policy Group*....70
Figura 32. Capacidade no ACI....71
Figura 33. Criação de Filtros de Segurança no ACI (contratos)....72
Figura 34. Diagrama de Rede implementado no Cliente Varejo....73

LISTA DE TABELAS

Tabela 1. Tabela de Classificação de Porte de *Data Center* 38
Tabela 2. Relevância Técnica e Operacional.....39
Tabela 3. Base de Testes 40

LISTA DE GRÁFICOS

Gráfico 1. Pesquisa de Relevância com DC's Pequenos 47
Gráfico 2. Pesquisa de Relevância com DC's Médio 48
Gráfico 3. Pesquisa de Relevância com DC's Grandes 48
Gráfico 4. Resultado da Pesquisa.....67

LISTA DE ABREVIATURAS E SIGLAS

SDN	=	*Software Defined Networking*
DC	=	*Data Center*
DCN	=	*Data Center Networking*
LAN	=	*Local Area Network*
QoS	=	*Quality of Services*
ACI	=	*Application Centric Infrastructure*
APIC	=	*Application Policy Infrastructure Controller*
BYOD	=	*Bring Your Own Device*
VSS	=	*Virtual Switching System*
IRF	=	*Intelligent Resilient Framework*
ONF	=	*Open Network Foundation*
VNI	=	*VXLAN Network Identifier*
VXLAN	=	*Virtual Extensible Local Area Network*
NFV	=	*Network Function Virtualization*
VNF	=	*Virtual Network Function*

SUMÁRIO

1 INTRODUÇÃO ..... ERRO! INDICADOR NÃO DEFINIDO.
1.1 Motivação ..... Erro! Indicador não definido.
1.2 Objetivos **16**
1.3 Organização do trabalho **16**

2. CAPÍTULO I - TRABALHOS RELACIONADOS **18**

3. CAPÍTULO II - EVOLUÇÃO DE REDES PARA *DATA CENTER* **20**

4. CAPÍTULO III - REDES CONVENCIONAIS E DEFINIDAS POR *SOFTWARE* **21**
4.1 Modelo de redes convencionais (Classical Ethernet) **21**
4.2 Modelo de redes SDN **23**
4.2.1 Modelo Imperativo e Declarativo de Controle 27
4.2.2 *Openflow* e *Opflex* 28
4.2.3 *Underlay* e *Overlay* 28

5. CAPÍTULO IV - CISCO ACI **30**

6. CAPÍTULO V - SISTEMÁTICA PARA IMPLEMENTAÇÃO DE REDES DEFINIDAS POR *SOFTWARE* EM *DATA CENTER* **36**
6.1 Sistemática **36**
6.1.1 Pesquisa 38
6.1.2 Criação de Base de Testes 39
6.1.3 Definição da solução e fabricante 40
6.1.4 Preparação dos Testes 41
6.1.5 Execução dos Testes 44

7. RESULTADOS **47**
7.1 Pesquisa **47**
7.2 Testes em ambiente de emulação **49**
7.2.1 Primeiro Teste – Automação e Provisionamento de Rede 49
7.2.2 Segundo Teste – Fluxo de Comunicações 52
7.2.3 Terceiro Teste – Medição de QoS 55
7.2.4 Quarto Teste – Microssegmentação de Rede 60
7.2.5 Quinto Teste – Gerenciamento de Rede e Depuração de Problemas 63
7.3 Sistemática em ambiente real **66**

CONSIDERAÇÕES FINAIS **74**

REFERÊNCIAS **76**

1 INTRODUÇÃO

As redes de comunicação de dados para *Data Centers* (DCs) apresentaram pouca evolução até 2013 na perspectiva de provisionamento e automação. Alguns mecanismos proprietários foram desenvolvidos, mas nenhum foi amplamente adotado e aceito pelo mercado pelo fato de depender do desenvolvimento de código e equipamentos próprios de cada fabricante.

O modelo convencional de rede existente há mais de 20 anos e ainda está presente na grande maioria dos DC's, pois é um modelo estável com os problemas conhecidos, controlados e também pelo fato do alto investimento realizado no passado. Esse modelo exige intervenção manual das configurações para o provisionamento e administração, possui deficiências técnicas em termos de convergência, escalabilidade, Qualidade de Serviço (QoS), segurança, além de não tirar proveito de todos os recursos de rede devido a limitações de protocolos existentes. Esse problema agrava-se ainda mais quando se trata de DC's com grande volume de servidores instalados por exigir intervenção de diversos equipamentos da rede e envolver múltiplas equipes com diversas competências técnicas.

Para solucionar os desafios apresentados no modelo convencional, os principais fabricantes desenvolveram a tecnologia *Software Defined Network* (SDN), que consegue suprir todos esses problemas técnicos.

Neste trabalho, será apresentada uma sistemática para implementação de Redes Definidas por *Software* (SDN) em *Data Center*.

A sistemática permite estruturar a implementação de SDN para *Data Center* mapeando os requisitos técnicos e de negócio a partir de uma pesquisa. Essa pesquisa cria uma base de testes e, por meio de alguns critérios específicos, é definida a solução SDN que será adotada. Por fim, é aplicada a base de testes em um ambiente controlado com a solução escolhida.

1.1 Motivação

A tecnologia SDN mostra-se muito promissora em diversas áreas de telecomunicações, desde provedores de serviços a empresas fora do ramo de

tecnologia. Contudo, sua maior aplicação ainda se encontra no ramo acadêmico e de pesquisas.

Empresas de diversos ramos de atuação já estão interessadas em atualizar suas redes ou estão analisando as ofertas de SDN no mercado para uma futura implementação. No entanto, as empresas ainda desconhecem os benefícios diretos e indiretos da tecnologia e buscam desenvolver seu próprio método para implementação, sendo que muitas vezes investem em soluções que não atendem suas necessidades e exigências.

Este trabalho desenvolve uma sistemática para implementação de SDN que auxilia as empresas a estruturarem suas necessidades técnicas, comerciais e operacionais, avaliar as soluções existentes e a planejar a melhor forma de implementar uma rede SDN para o *Data Center*.

1.2 Objetivos

O objetivo principal deste trabalho é apresentar uma sistemática para implementação de redes SDN. Apesar de haver muitas tecnologias e fabricantes desenvolvendo soluções SDN no mercado, não existe uma sistemática definida que independa do fabricante e auxilie as empresas na implementação de redes SDN.

Este trabalho apresenta uma sistemática que permite às empresas mapearem quais são os problemas, dificuldades, requisitos técnicos e operacionais em sua rede de *Data Center,* a partir de uma pesquisa e, com base no resultado dessa pesquisa, forma-se uma base de testes que possibilita avaliar qual solução de rede melhor adequa-se ao seu negócio.

1.3 Organização do trabalho

O restante do trabalho está organizado da seguinte forma:

- Capítulo 1: Apresenta trabalhos acadêmicos relacionados;
- Capítulo 2: Apresenta uma introdução do conceito de redes para *Data Center* e os dois modelos existentes;

- Capítulo 3: Trata dos conceitos de redes convencionais e SDN;
- Capítulo 4: Descreve a tecnologia SDN da Cisco chamada de ACI;
- Capítulo 5: Apresenta a proposta deste trabalho, a sistemática para implementação de redes SDN e a implementação da sistemática em um ambiente de emulação e um cliente real;
- Resultados: Apresenta os resultados obtidos da sistemática;
- Considerações finais: Apresenta as conclusões finais e perspectivas de trabalhos futuros.

2 CAPÍTULO I - TRABALHOS RELACIONADOS

Como neste trabalho será apresentada uma proposta para implementação de Redes Definidas por *Software*, optou-se por pesquisar na literatura trabalhos semelhantes que compartilhassem esse aspecto.

No trabalho *On the Practical Applicability of SDN Research* [1], são destacados inúmeros problemas relacionados a implementações SDN e também as limitações de fabricantes que suportam *OpenFlow*. Foram pesquisadas as principais limitações em *OpenFlow* nos equipamentos dos fabricantes Arista, Brocade, DELL, Extreme e HP por meio de manuais e criada uma metodologia de testes com ambiente de simulação. Constatou-se que os fabricantes ainda possuem diversas dificuldades e limitações nos equipamentos para implementações SDN, apesar do protocolo *OpenFlow* já estar bem desenvolvido. Problemas de memória para as tabelas de comutação, falta de suporte a tecnologias existentes e flexibilidade para configuração híbrida são as principais deficiências encontradas nos testes.

O artigo *Towards a Tactical Software Defined Network* [2] apresenta uma metodologia para implementação de redes SDN em ambiente militar. As redes de dados militares possuem diversos problemas e limitações relacionados à instalação, desempenho, qualidade de serviço (QoS), integração dos equipamentos e gestão dos ativos. Desenvolveu-se uma metodologia estruturada em duas fases: a primeira fase visava a desenvolver e refinar os algoritmos e, a segunda fase, a analisar de forma quantitativa e qualitativa a aplicação de SDN para redes militares. A metodologia foi desenvolvida para quantificar os benefícios oferecidos por SDN em redes militares e a desenvolver um plano de adoção futuro.

O artigo *SDN and NFV Benchmarking for Performance and Reliability* [3] introduz uma metodologia de testes para SDN, *Network Function Virtualization* (NFV), que virtualiza componentes de rede como *Firewall*, IPS e roteadores e *Virtual Network Function* (VNF), que implementa funções de rede usando *software* desmembrado do *hardware*, na perspectiva de desempenho e “confiabilidade” dos sistemas, para um operador de rede. Criou-se uma base de testes com nove métricas de desempenho para SDN, cinco métricas para NFV e duas para VNF, além de duas métricas para testes de confiabilidade em SDN. Além da avaliação

das métricas, está apontada a necessidade de um padrão de arquitetura que traga o benefício de desempenho e confiabilidade. O trabalho auxilia os operadores na adoção e implementação de SDN, NFV e VNF.

Por sua vez, o artigo *Mathematical Tools and Methods for Analysis of SDN: A Comprehensive Survey* [4] provê insumos sobre várias ferramentas matemáticas e método de verificação que pode ser usado para análise de SDN. É apresentada uma ferramenta de predição de desempenho como *Queuing Theory* e o *Calculus,* que auxilia os planejadores de redes a entender como o desempenho da rede é afetado pela consumo e utilização dela.

3 CAPÍTULO II - EVOLUÇÃO DE REDES PARA *DATA CENTER*

O conceito de *Data Center* surgiu para concentrar todo o ambiente computacional da empresa, ou seja, em vez dos servidores e aplicações serem distribuídos em cada escritório remoto, é criado um único ambiente centralizado. Essa centralização reduz o custo da empresa em termos de investimento em equipamentos, administração e consolidação dos recursos.

As redes para *Data Center* tornam-se fundamentais para a operação do negócio, na medida em que os servidores e aplicações necessitam de acesso à rede para se comunicar com usuários e outras empresas. A interrupção da comunicação por falha de equipamento físico, lógico ou ameaça de segurança pode impactar diretamente no funcionamento da empresa.

As redes para *Data Center* estão sofrendo muitas mudanças nas perspectivas de equipamentos, soluções e arquitetura, porque as aplicações e interesse de tráfego na rede mudaram. O maior volume de tráfego nos *Data Centers* antigamente era no sentido de entrada e saída, enquanto, nos dias atuais, o maior volume é entre aplicações dentro do *Data Center,* exigindo novas características da rede, como maior desempenho, disponibilidade, convergência e programabilidade independentemente do fabricante.

4 CAPÍTULO III - REDES CONVENCIONAIS E DEFINIDAS POR *SOFTWARE*

4.1 Modelo de redes convencionais (*Classical Ethernet*)

O modelo de rede convencional, também conhecido como *Classical Ethernet*, faz uso da arquitetura hierárquica virtual LANs (VLANs) para segregação das redes, *Spanning-tree* um protocolo de camada dois do modelo OSI para controle de caminhos infinitos e roteamento como forma de melhor caminho para entrega de pacotes, sendo, ainda, o modelo predominante nos *Data Centers*.

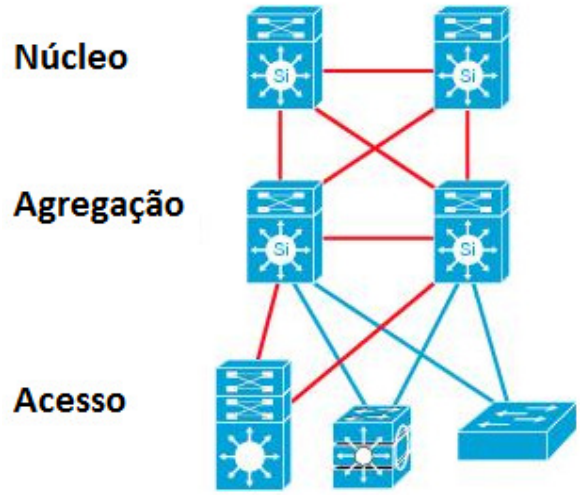
As implementações de redes de dados para *Data Center* sofreram pouca evolução até 2006. Sob a perspectiva de arquitetura, o modelo em três camadas, conhecido como modelo hierárquico, era utilizado como arquitetura única para as redes de *Data Center* e corporativa, ou seja, não havia praticamente diferenças nos equipamentos e implementações dessas redes.

O modelo hierárquico era amplamente utilizado em redes para *Data Center* e ainda utilizado em redes corporativas devido à sua hierarquia, modularidade, resiliência e flexibilidade. Esse modelo propõe-se a dividir a rede em três camadas: o núcleo da rede, a camada de agregação e o acesso. Vejam-se:

;

- A camada núcleo de rede provê transporte rápido entre os *switches* da camada de agregação e conectividade externa da rede;
- A camada de agregação provê conectividade e controle entre a camada de acesso e o núcleo;
- A camada de acesso provê acesso à rede para os servidores e aplicações. [5]

Figura 1. Arquitetura Hierárquica para redes convencionais



Fonte: Adaptada de Cisco Systems [6]

As redes convencionais utilizam o conceito de virtual LAN (VLAN) para criar um domínio de *broadcast* particionado e isolado. As VLANs são utilizadas para criar agrupamentos lógicos de equipamentos na rede. O padrão IEEE 802.1Q permite definir até 4096 VLANs em uma rede.

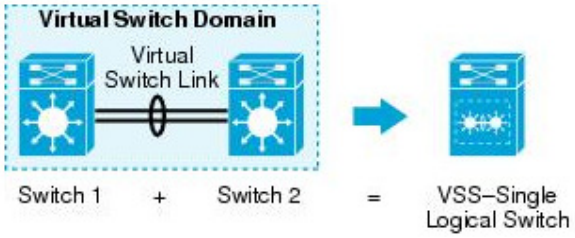
O algoritmo *Spanning-Tree* (STP) é utilizado pelas redes convencionais como protocolo principal para controle do tráfego *Ethernet* dentro do *Data Center*. O *Spanning-tree*, quando executado pelos equipamentos de rede, permite calcular uma topologia ou caminho com saltos limitados na rede. [7]

Apesar de trazer mais estabilidade à rede, o STP bloqueia caminhos alternativos e possui convergência lenta, padrão que não é aceito nas redes atuais, que exigem alto desempenho e convergência rápida.

A partir de 2009, começaram a surgir tecnologias que eliminavam ou mascaravam o *Spanning-Tree*. O protocolo *Inter-Chassis Communication Protocol (ICCP)* surgiu como um mecanismo de redundância entre *switches* para alta disponibilidade. A partir dele, fabricantes como Brocade, Cisco, HP e Juniper desenvolveram seus próprios padrões como *Virtual Switching System (VSS)* e *virtual Port-channel* (vPC) da Cisco e o *Intelligent Resilient Framework* (IRF) da HP, para a utilização de caminhos redundantes, aumentando a disponibilidade e velocidade de comutação dos pacotes.

A Fig. 2 ilustra o funcionamento do protocolo VSS da Cisco:

Figura 2. Diagrama conceitual do VSS



Fonte: Cisco Systems [8]

4.2 Modelo de redes SDN (SDN)

A partir de 2013, os fabricantes começaram a desenvolver soluções que utilizavam o conceito de redes definidas por *software*, ou mais conhecido como *Software Defined Networking* (SDN).

As tecnologias SDN surgiram para ser mais independentes do desenvolvimento dos fabricantes e trabalharem com novos padrões e protocolos, além de oferecem mais desempenho, disponibilidade, estabilidade e crescimento simplificado da rede.

SDN tornou-se uma peça fundamental para os problemas computacionais, como:

- Mudança comportamental do tráfego: as aplicações distribuídas em nuvem pública ou privada requerem acessos à banda sob demanda;
- "Consumerização" de TI: tendência de *Bring Your Own Devices* (BYOD) requer que as redes sejam flexíveis e seguras;
- Aumento de serviços em nuvem: acesso sob demanda de aplicações e infraestrutura;
- Largura de banda: grande massa de dados requer mais processamento e velocidade para serem processados;
- Complexidade: adicionar ou movimentar equipamentos torna-se complexo, consome tempo e cria riscos de indisponibilidade do sistema;

- Dificuldade de crescimento: a técnica de “oversubscription”, cálculo de dimensionamento acima do esperado, não funciona mais para o novo tráfego dinâmico em redes virtualizadas, devido ao processamento em escala paralela;
- Independência de fabricante: a falta de padronização e interfaces abertas limitam a implementação de ambientes individuais. [9]

A *Open Network Foundation* (ONF) [10] é um consórcio sem fins lucrativos dedicado ao desenvolvimento e padronização de SDN.

A ONF define *Software Defined Networking* como uma arquitetura emergente, cujo plano de controle é desacoplado do plano de dados e é diretamente programável.

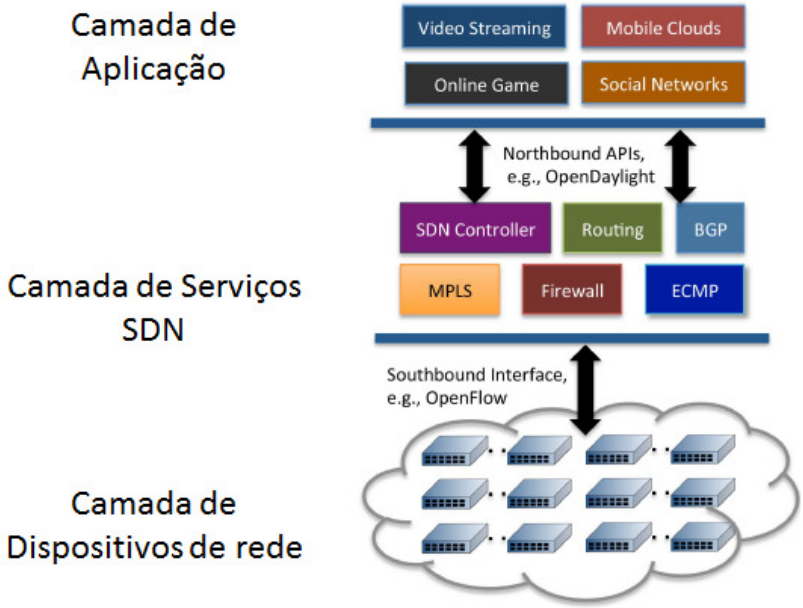
Com essa arquitetura, o plano de controle pode ser separado do plano de dados sem afetar o desempenho do fluxo de dados.

SDN é baseado em três princípios:

- Desacoplamento do plano de dados ao plano de controle;
- Controle centralizado logicamente;
- Programabilidade dos serviços de rede. [11]

A Fig. 3 ilustra o modelo de referência SDN:

Figura 3. Modelo de Referência SDN



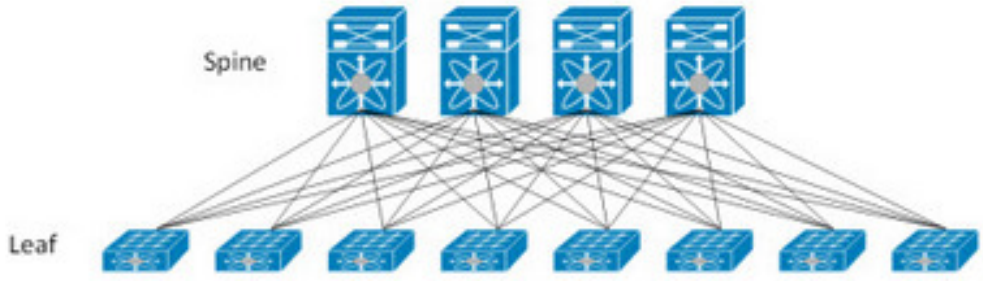
Fonte: Adaptada de [12]

Charles Clos, um pesquisador da Bell Labs [13], publicou um artigo que descreve como uma chamada telefônica poderia ser comutada por um equipamento que usasse múltiplos estágios de interconexão para permitir que uma chamada telefônica seja completada.

Em meados de 1990, o conceito de *Clos Networks* foi reutilizado nas redes *Ethernet*, como um conceito de criar conectividade entre qualquer interface *Ethernet* do *switch*, permitindo a troca de quadros dentro daquele *switch*.

A Fig. 4 representa a nova arquitetura de *Data Center* baseada no modelo Clos:

Figura 4. Modelo Clos (*Spine and Leaf*)



Fonte: [14]

As redes SDN utilizam-se dessa arquitetura para criar uma rede com, no máximo, dois saltos da origem ao destino com múltiplos caminhos sendo utilizados simultaneamente. Essa arquitetura reduz o tempo de atraso na entrega do tráfego, reduz o tempo de convergência, a possibilidade de falhas e aumenta o desempenho da rede.

O novo conceito de Clos divide a rede de dados em duas camadas: a *Spine e Leaf*.

A camada do *Leaf* consiste nos *switches* de acesso que conectam servidores, *firewalls*, roteadores e demais elementos de rede e computacionais. Não existe comunicação direta entre os *Leafs* sem passar pelo *Spine*.

A camada do *Spine* consiste na interconexão dos *Leafs*, nenhum outro equipamento é conectado diretamente ao *Spine*.

O *OpenFlow* foi originado na Universidade de Stanford e, atualmente, está em fase de desenvolvimento dos padrões por meio da ONF.

O objetivo inicial era prover um caminho para os pesquisadores realizarem experimentos de protocolos em uma rede em produção.

O *OpenFlow* define um protocolo, que, de forma centralizada, pode controlar *switches* e outros elementos de rede. O *OpenFlow* surgiu como primeiro protocolo de controle para redes SDN, havendo, ainda, confusão entre o conceito de SDN com a definição do *OpenFlow*.

Um conceito muito importante na nova arquitetura SDN é o VxLAN, cujo protocolo surgiu com o intuito de endereçar problemas e dificuldades do *Spanning-Tree* e VLANs, como escalabilidade, uso de múltiplos caminhos e convergência rápida.

A *Virtual extensible Local Area Network* (VxLAN) é um *overlay* (uma camada de virtualização) na Camada 2 do modelo OSI sobre uma Camada 3. Apenas máquinas virtuais e equipamentos no mesmo segmento VxLAN podem comunicar-se.

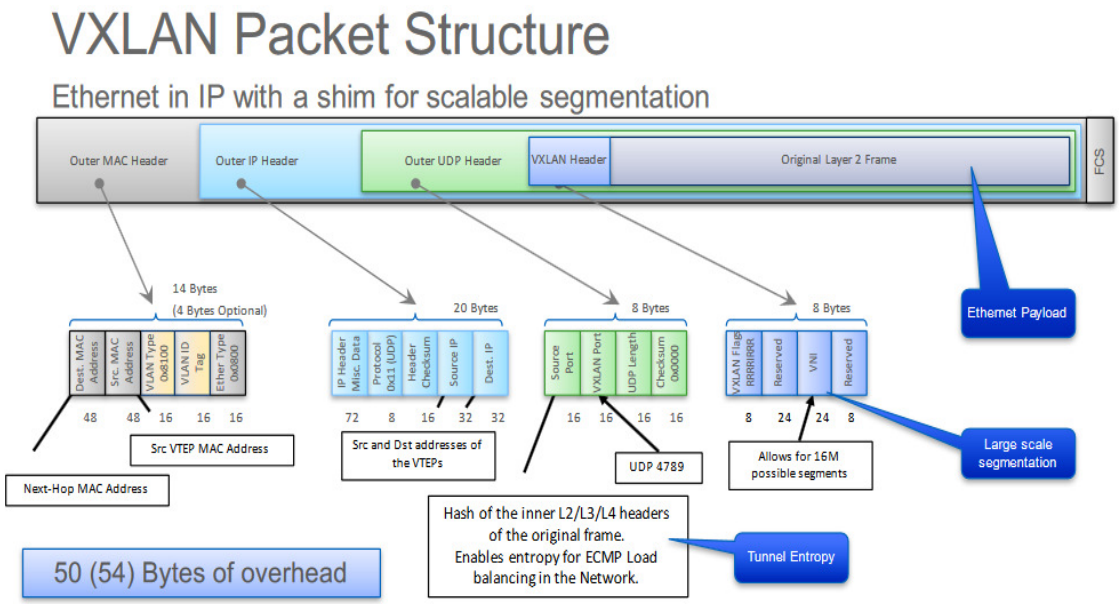
Os segmentos VxLAN são encapsulados em pacotes IP, o que permite estendê-lo entre *Data Centers* através de roteamento.

Cada segmento VxLAN é identificado por meio de um segmento de 24 bits denominado *VxLAN Network Identifier* (VNI), o que permite a criação de 16 milhões de segmentos VxLAN. [15]

O VxLAN pode ser considerado uma evolução do conceito de VLAN, porém, com maior escalabilidade, resiliência por usar roteamento e não depender do *Spanning-Tree* e por permitir a utilização de múltiplos caminhos.

A Fig. 5 ilustra os campos do pacote VxLAN:

Figura 5. Estrutura do VXLAN



Fonte: [16]

4.2.1 Modelo Imperativo e Declarativo de Controle

No modelo imperativo o controlador SDN atua como o cérebro da rede SDN. O controlador SDN recebe as solicitações das aplicações via uma interface de programação de programação de aplicação (API) e impõe ao plano de encaminhamento como os switches e roteadores precisam ser configurados para responder as necessidades da aplicação. Dessa forma, o controlador centralizado pode se tornar um único ponto de falha na rede, sem qualquer controle embutido no caminho dos dados.

No modelo declarativo o controlador SDN declara o que a aplicação necessita e envia a mensagem para a rede, de modo que os *switches* e roteadores determinem como atender aquelas necessidades. O controle declarativo permite uma inteligência mais distribuída. A política é aplicada de forma centralizada, mas

os switches e roteadores possuem mais autonomia para decidir como executá-las[17].

4.2.2 *Openflow* e *Opflex*

OpenFlow é um protocolo baseado em controle imperativo, o qual define um controlador centralizado logicamente para controlar um *switch OpenFlow*. Cada *switch* na arquitetura *OpenFlow* mantém uma ou mais tabelas de fluxos, as quais são utilizadas para realizar pesquisas de pacotes. Ações distintas são tomadas em relação à pesquisa e encaminhamento de pacotes [18].

Um administrador pode modificar a tabela de fluxos através do controlador SDN para controlar o fluxo, ou seja, a rota que os pacotes devem seguir [19].

A arquitetura (OpFlex) provê um sistema de controle distribuído, baseada em um modelo declarativo de controle. As políticas são definidas em um repositório central e são enviados comandos aos elementos distribuídos através do protocolo OpFlex. Esse protocolo permite a comunicação bidirecional das políticas, eventos, estatísticas e erros [20].

OpFlex é um protocolo aberto e de políticas extensivas para transmitir políticas em XML ou JSON entre o controlador SDN e qualquer outro equipamento, incluindo Hypervisor, uma camada de software entre o hardware e sistema operacional, switches físico ou virtual, *firewalls* e outros.

4.2.3 *Underlay* e *Overlay*

Existem dois tipos de soluções SDN oferecidas no mercado: a solução SDN, baseada em *hardware* físico (*underlay*), e a solução de virtualização de rede (*overlay*). A rede *overlay* é construída sob uma rede *underlay*.

A rede *underlay* é constituída de *hardware*, mais precisamente *switches, qu*e podem abrir e fechar túneis VxLAN ou NVGRE, os quais são usados para criação de *overlays*.

A rede *overlay* como é criada, independentemente dos *switches* que estão sendo utilizados na rede, exigem alguns requisitos mínimos para o funcionamento dela, porém, a dependência dos *switches* implementados é baixa.

A rede *overlay*, por sua vez, termina túneis VXLAN ou NVGRE sem a utilização de *hardware*, apenas utilizando seu *software* de virtualização de rede.

A rede *overlay* propõe-se a criar uma camada de virtualização de rede e a implementar novos serviços com alto grau de transparência e desacoplamento da rede *underlay*.

A rede *overlay* foi definida com quatro características [21]:

- Deve garantir a segregação de tráfego entre clientes;
- Deve suportar independência do espaço de endereço IP entre clientes;
- Deve permitir a implementação ou movimentação de servidores e máquinas virtuais independentemente do esquema de endereçamento IP da rede *underlay*;
- Deve suportar os três itens anteriores em grande escala, com milhões de servidores ou máquinas virtuais.

5 CAPÍTULO IV - CISCO ACI

A principal tecnologia desenvolvida pela Cisco e utilizada como plataforma SDN durante os testes neste trabalho foi a *Application Center Infrastructure* (ACI).

O Cisco ACI é uma nova arquitetura desenhada SDN da Cisco para endereçar os requisitos atuais das redes tradicionais.

O Cisco ACI consiste em:

- Linha de *switches* Cisco Nexus 9000 Series;
- Um gerenciamento de políticas centralizado através do controlador SDN Cisco *Application Policy Infrastructure Controller* (APIC);
- Um *switch* virtual de aplicativos (AVS) para a borda da rede virtual;
- Integração das infraestruturas física e virtual;
- Um ecossistema aberto de fornecedores de rede, armazenamento, gerenciamento e orquestração.

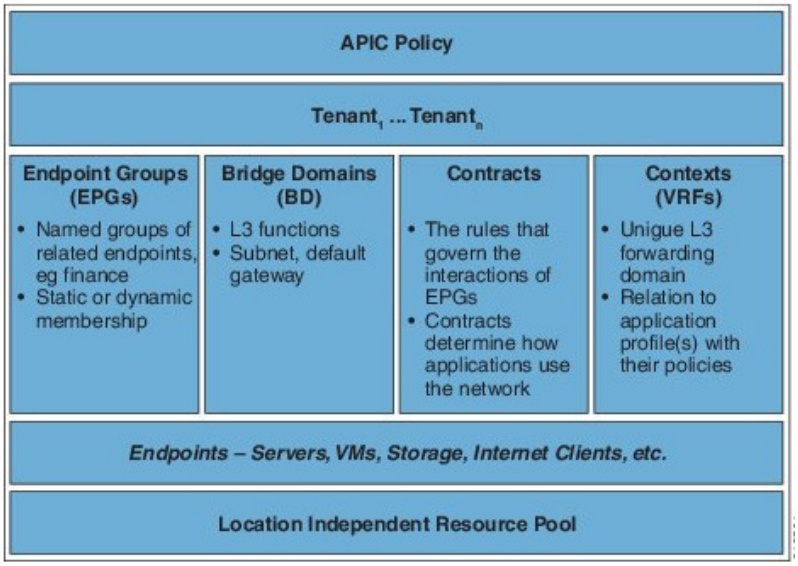
Entre as principais características do ACI, estão [22]:

- Automação simplificada por meio de um modelo de políticas orientado por aplicativos;
- Visibilidade centralizada com monitoramento de integridade de aplicativos em tempo real;
- Flexibilidade de *software* aberto para integração entre equipes de desenvolvimento e operações e o ecossistema de parceiros;
- Desempenho dimensionável.

Construção lógica do ACI

O modelo de política gerencia o ACI completo, incluindo a infraestrutura, autenticação, segurança, serviços, aplicações e diagnóstico. O modelo de construção lógica define como o fabricante alcança as necessidades de qualquer função dentro dele. A Fig. 6 ilustra a construção do modelo de política do ACI [23]:

Figura 6. Construção da política no ACI



Fonte: [23]

Tenant

Tenant é um *container* lógico para aplicação de políticas que permitem ao administrador aplicar controle baseado em domínio. Um *tenant* representa uma unidade de isolamento sob a perspectiva de política.

O *Tenant* pode representar um cliente para um provedor de serviços, uma organização ou simplesmente um agrupamento de políticas.

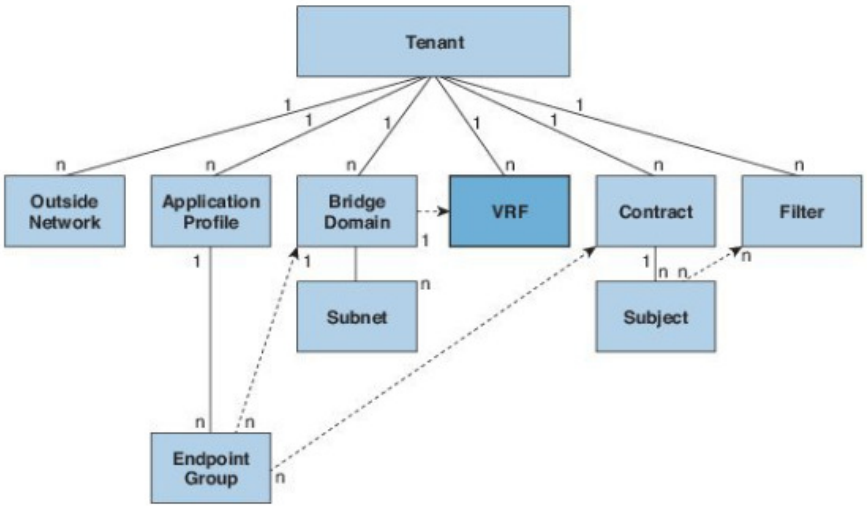
Os *Tenants* podem ser isolados uns dos outros ou compartilhar recursos. Os primeiros elementos que um *tenant* contém são filtros, contratos, redes externas, *Bridge Domains*, VRFs e EPGs, que serão descritos mais à frente. [23]

VRF

A *Virtual Routing and Forwarding* (VRF) define um domínio L3, sendo que um ou mais *Bridge Domains* são associados a uma VRF.

Todos os *endpoints* dentro de uma VRF precisam possuir um endereço IP único, pois é possível enviar pacotes diretamente entre esses equipamentos se a política permitir [23]:

Figura 7. VRFs



Fonte: [23]

Bridges Domain* e *Subnets

No ACI, o domínio de *broadcast* de camada 2 do modelo OSI é representado como uma entidade lógica chamada de *Bridge Domain* (BD). O BD é uma construção de encaminhamento baseada em cada 2 do modelo OSI usado para forçar a distribuição de tráfego *broadcast* e *multicast*.

Endpoints são sempre mapeados para um BDs, entretanto, eles podem sem agrupados em subgrupos chamados de *Endpoint Groups* (EPGs) e definidos como um único BD [23].

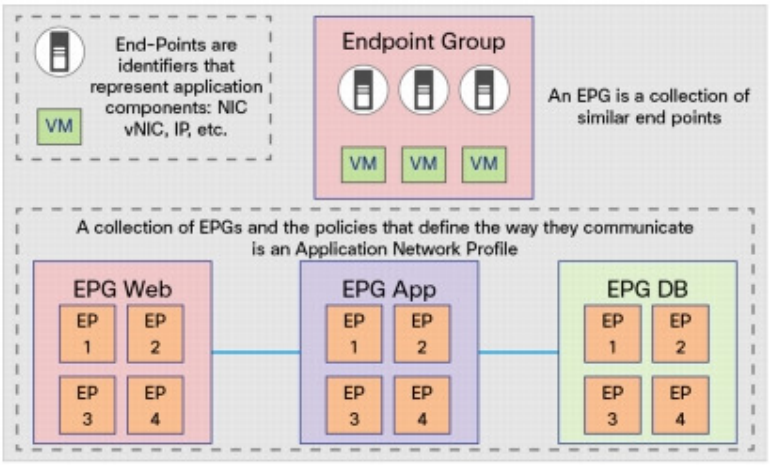
Endpoint Groups

O EPG provê um novo modelo para mapeamento de aplicações para redes. Em vez de utilizar uma estrutura com endereçamento de camada 2 ou 3 do modelo OSI para aplicar políticas de segurança, o EPG usa um agrupamento de aplicações para *endpoints*.

EPGs funcionam como *containers* de aplicações e são classificados baseados em vários critérios e requisitos de controle de acesso. Os EPGs são equivalentes a *security zones* e todos os equipamentos dentro de um EPG podem falar entre si, a menos que o isolamento dentro do EPG seja habilitado [23].

A Fig. 8 ilustra o agrupamento de dispositivos por meio do EPG:

Figura 8. *Endpoint Groups*



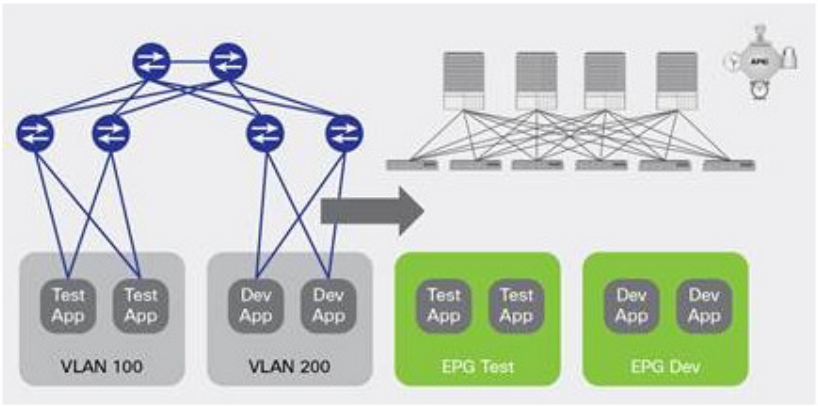
Fonte: [24]

Esse agrupamento é independente do endereçamento IP e da vlan. Dentro de um EPG, os dispositivos podem coexistir em várias redes e essas redes podem coexistir em vários EPGs consequentemente.

Os EPGs podem ser mapeados de várias formas: as mais utilizadas são EPGs como uma vlan, rede, VxLAN, VMware *Port Group*, agrupamento de aplicações ou zonas de segurança.

A forma mais utilizada e fácil de implementar um EPG é por meio do mapeamento de VLANs, de forma que todos os equipamentos são mapeados para um EPG. Esse formato permite a migração simplificada do ambiente existente da forma estruturada conforme a representação da Fig. 9 [23]:

Figura 9. *Endpoint* como VLANs



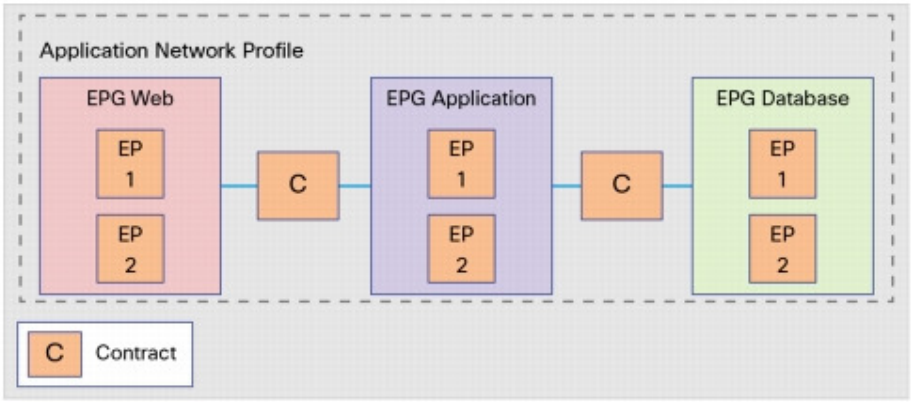
Fonte: [25]

Contratos

Contratos são restrições de segurança aplicados na comunicação entre os EPG's. Sem um contrato estabelecido entre o EPG, nenhuma comunicação é permitida, a menos que a instância de VRF seja configurada como sem restrições. Dentro de um EPG, não é requerido um contrato, pois a comunicação interna é sempre permitida.

A Fig.10 representa a relação entre EPG e Contratos:

Figura 10. Contratos



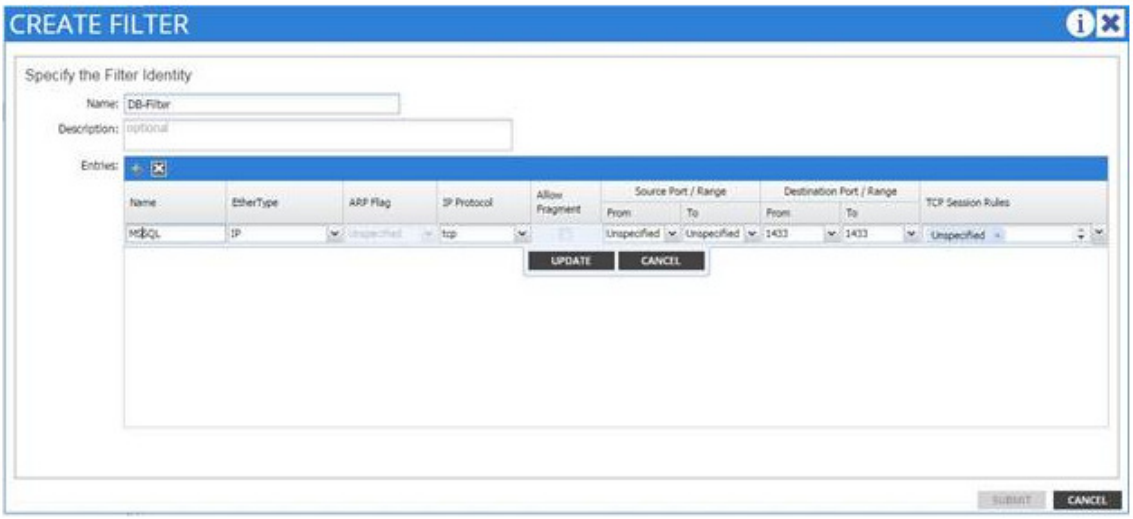
Fonte: [24]

Um EPG pode utilizar um único ou múltiplos contratos. Por exemplo: o EPG *Web* pode utilizar um contrato para acesso ao EPG *App* ou, similarmente, o EPG DB poderia utilizar um único contrato para acesso ao EPG *APP* e *Web*.

Os contratos funcionam como filtros, que especificam portas TCP, UDP e tipos de protocolos [23].

A Fig. 11 ilustra o painel de criação dos contratos:

Figura 11. Criação de Contratos



Fonte: [26]

6 CAPÍTULO V - SISTEMÁTICA PARA IMPLEMENTAÇÃO DE REDES DEFINIDAS POR *SOFTWARE* EM *DATA CENTER*

Neste trabalho, é proposta uma sistemática para a implementação de redes definidas por *software*. Em virtude do interesse dos clientes em implementar redes mais modernas que se adequem às necessidades de negócio e devido ao número elevado de fabricantes e soluções existentes no mercado, este trabalho vem apresentar uma sistemática para implementação de SDN em *Data Center* que permite levantar os requisitos das empresas, requisitos de rede, definir qual solução implementar e avaliar se a solução atende as exigências. A forma como era desenhada e implementada uma rede e como algumas empresas ainda implementam é através de um mapeamento básico do número de interfaces *Ethernet* no *Data Center* com velocidades de 1 Gbps ou 10 Gbps e definindo quais serviços de rede são necessários, como *firewall*, balanceador de aplicações, *proxy* reverso e outros.

Esse método mostra-se ineficiente para as novas redes para *Data Center*, porque as aplicações atualizaram-se e possuem requisitos e comportamentos diferentes. O fluxo principal de tráfego de um *Data Center* era no sentido norte-sul, ou seja, tráfego que entrava e saia do *Data Center* e as aplicações tinham poucas dependências uma das outras.

As redes atuais são orientadas para aplicação, o que se faz necessário entender o seu funcionamento, os requisitos de funcionamento e, então, definir como os serviços e funções de rede devem ser implementados. Grande parte das aplicações em *Data Centers* são virtualizadas, sendo assim, devem ser consideradas funções de *switches, firewalls*, balanceadores e outros elementos, distribuídos entre equipamentos físicos e virtualizados, para que exista menos tráfego circulando no *Data Center*, reduza o tempo de atraso de comutação dos pacotes, aumente o nível de segurança lógica e exija menos recursos de *hardware*.

6.1 Sistemática

A sistemática desenvolvida no projeto para implementação de redes definidas por *software* envolve o entendimento das principais necessidades

técnicas para redes de *Data Center* por meio de uma pesquisa. É, então, criada uma base de testes, definida a solução e o fabricante, em seguida, executados os testes em ambiente controlado.

O entendimento das necessidades técnicas e de negócio para as redes de *Data Center* é conduzido por meio de uma pesquisa enviada a diversas empresas de diferentes ramos de atuação, a fim de entender quais são as principais preocupações e dificuldades encontradas nas redes para *Data Centers* (DCN).

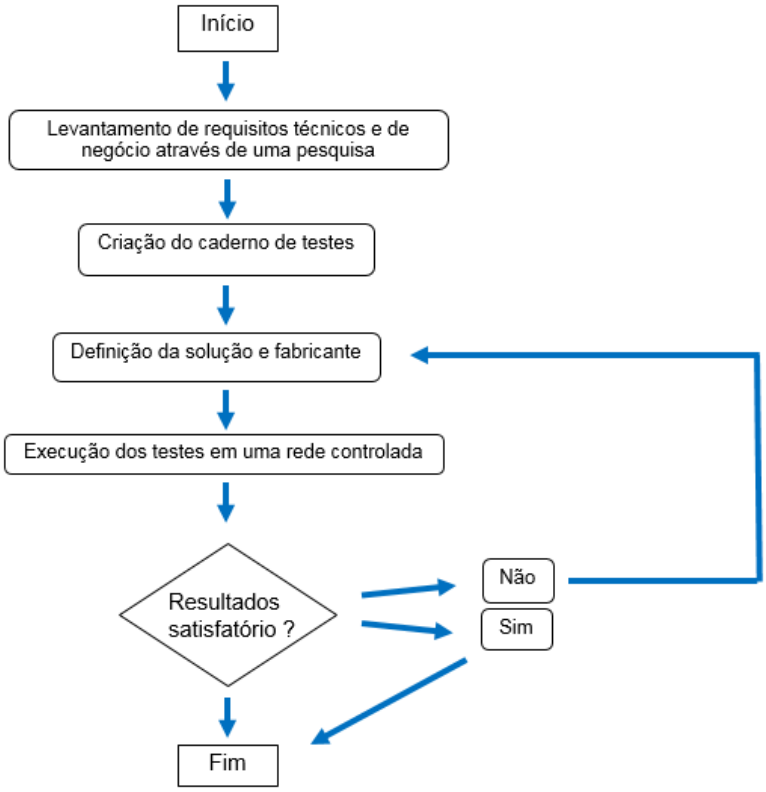
A partir das informações coletadas na pesquisa, foi elaborada uma base de testes relacionada às dificuldades e características de DCN destacadas na pesquisa.

Na sequência, foi selecionada uma solução SDN definida por alguns critérios técnicos e específicos e, então, foram executados os testes para analisar se a solução secadequava às necessidades da empresa.

O último estágio aplica à sistemática em um cliente real que deseja migrar de uma rede tradicional para SDN.

A Fig. 12 ilustra um fluxograma de desenvolvimento do trabalho:

Figura 12. Fluxograma da sistemática



Fonte: Elaboração própria

6.1.1 Pesquisa

A pesquisa foi elaborada para analisar os níveis de relevância dos aspectos técnicos, operacionais e comerciais das redes para *Data Center* em diversos clientes

Para uma avaliação mais abrangente, foram considerados, na pesquisa, 30 clientes do mercado de varejo, financeiro e fabril, sendo 10 clientes com *Data Center* de pequeno porte, 10 clientes com *Data Center* de médio porte e 10 clientes com *Data Center* de grande porte, de acordo com classificação da Tab. 1:

Tabela 1. Tabela de Classificação de Porte de *Data Center*

Clientes alvo	Classificação
Pequeno	Até 100 servidores físicos/virtuais
Medio	101 até 500 servidores físicos/virtuais
Grande	(+500) servidores físicos/virtuais

Fonte: Elaboração própria

Foram feitas a cada um dos clientes as seguintes perguntas:

- Quais características são essenciais em uma rede de *Data Center*?
- Quais as limitações encontradas nas redes atuais de *Data Center*?
- Quais as principais dificuldades enfrentadas nas redes de *Data Center*?
- Quais funções e funcionalidades deveriam ser aperfeiçoadas nas redes de *Data Center*?
- Quais funções ou funcionalidades deveriam ser desenvolvidas nas redes de *Data Center*?

Com os insumos obtidos, foi criada a Tab. 2 com cada assunto discutido e classificado por tamanho do *Data Center* e grau de relevância.

Os aspectos avaliados foram classificados em 3 (três) grandezas, sendo baixo, médio e alto grau de relevância:

Tabela 2. Relevância técnica e operacional

Grau de Relevância em Data Center Pequeno			
Aspectos Analisados	**Classificação**		
	Baixo	**Médio**	**Alto**
Programabilidade			
Automação, provisionamento e simplicidade de configuração			
Alta disponibilidade de rede			
Convergência			
Eliminação de Spanning-Tree e utilização de múltiplos caminhos (Multipath)			
Desempenho 40/100 Gb			
Escalabilidade			
Interoperabilidade de fabricantes			
Simplicidade de configuração			
Data Center Interconnect (DCI)			
Implementação unificada de serviços de Segurança (Firewall e IPS) para ambientes físico e virtual			
Implementação de microsegmentação			
Análise de fluxo e interdependências de aplicações			
Implementação e medição de QoS e análise de tráfego			
Overlay networks			
Flexibilidade para adoção de novas tecnologias			
Gerenciamento de rede e depuração de problemas			

Fonte: Elaboração própria

6.1.2 Criação de Base de Testes

A base de testes foi elaborada com apoio da pesquisa de relevância técnica e operacional. Desse modo, foram criados diversos aspectos e critérios de avaliação por meio dos insumos obtidos.

O objetivo dos testes é evidenciar a necessidade do uso de SDN em *Data Centers* e avaliar se a solução definida pelo cliente atende os requisitos técnicos e operacionais exigidos.

Na Tab. 3, está apresentada a base de testes:

Tabela 3. Base de testes

Características	Critérios
Programabilidade	- Programação de acordo com as necessidades de negócio; - Programação independendente de fabricante; - Compatível com algum protocolo de controle como OpenFlow, OpFlex, RESTFUL, OVSDB.
Provisionamento e automação de rede	- Configuração sem tocar no hardware "zero-touch"; - Configuração dos elementos de rede de forma centralizada; - Provisionamento da rede de acordo com os requisitos de aplicação.
Alta disponibilidade de rede	- Alta disponibilidade de hardware e software; - Compatível com protocolos de alta disponibilidade FHRP.
Convergência	- Redes com covergência automática em microsegundos quando ocorrer falha; - Protocolos padronizados e abertos para atingir a convergência entre os fabricantes; - Soluções que permitam a implementação de rede física e virtual de forma única e transparente.
Eliminação de Spanning-Tree e utilização de múltiplos caminhos (Multipath)	- Comunicação dos switches em L3; - Utilização de todos os caminhos L3 simultâneos; - Implementação de tecnologias de agregação de links (Multi-chassis Link-aggregation).
Desempenho 40/100 Gbps	- Hardware e software disponíveis para o acesso a velocidades de 40 Gbps e 100 Gbps; - Dependência apenas do hardware para suportar velocidades acima de 10 Gbps.
Escalabilidade	- Flexibilidade de crescimento da rede física ou virtual de forma simplificada; - Implementação de VxLAN.
Interoperabilidade	- Plataforma de hardware e software que permite integrar diversos fabricantes; - Plataforma que não depende do desenvolvimento do fabricante.
Simplicidade de configuração	- Configuração através de uma interface gráfica (GUI); - Configuração de switching, roteamento, balanceamento de carga e segurança de forma unificada e centralizada; - Configuração unificada da rede física e virtual.
Data Center Interconnect (DCI)	- Compatível com VPLS ou protocolos proprietários de extensão de vlans; - Extensão de vlans via VxLAN; - Extensão de vlans via Fabric nativo.
Implementação unificada de serviços de Segurança (Firewall e IPS) para ambientes físico e virtual	- Plataforma única de configuração e administração de firewall e IPS físico ou virtual; - Implementação de Firewall e IPS Norte-Sul e Leste-Oeste; - Integração com fabricantes de segurança.
Implementação de microsegmentação	- Implementação de firewall layer 3, layer 4 (modelo de camadas OSI) para controle de tráfego horizontal ou leste-oeste. - Implementação de firewall distribuído; - Centralização da configuração e gerenciamento das políticas de acesso.
Análise de fluxo e interdependências de aplicações	- Ferramenta nativa ou integração simplificada com a solução; - Análise do fluxo de aplicação e interdependência; - Auxílio na implementação de regras de segurança.
Implementação e medição de QoS e análise de tráfego	- Função nativa nos equipamentos através do licenciamento; - Exibição de níveis de SLA por aplicação; - Integração do *template* de provisionamento da aplicação com os requerimentos de QoS.
Overlay networks	- Implementação de rede virtualizada; - Independência da rede física para implementação de redes virtualizadas.
Flexibilidade para adoção de novas tecnologias	- Desenvolvimento próprio de automação e processos; - independência de fabricantes para implementação de novas tecnologias e integrações.
Conexão com cloud	- Plataforma que se integre com a cloud; - Plataforma que permita a extensão da solução e administração unificada.
Gerenciamento de rede e depuração de problemas	- Plataforma integrada de gerenciamento; - Gerenciamento dos ativos de rede como “saúde” dos equipamentos, alertas críticos e configuração centralizada. - Ferramentas para depuração de problemas e diagnóstico; - Planejamento de capacidade futura.

Fonte: Elaboração própria

6.1.3 Definição da solução e do fabricante

Para a definição da solução e do fabricante aplicando a sistemática em um cenário real, é necessária uma análise rigorosa considerando os seguintes aspectos:

- Existência de uma padronização de fabricante na rede;

- Preferência de fabricante;
- Casos de referência em clientes do mesmo ramo;
- Estado de maturidade da solução;
- Fabricantes que desenvolvem solução apenas de *hardware* (*overlay*) e *software (underlay*);
- Custo de aquisição do *hardware, software* e implementação.

Para a definição de fabricante e modelos de equipamentos nos testes de emulação, foram considerados fatores de *market share*, ou seja, o fabricante que tem a maior porção de equipamentos de rede para *Data Center* e que também oferece soluções convencionais e SDN de rede para *Data Center*.

O fabricante Cisco Systems foi escolhido neste projeto, mas outros fabricantes alternativos, como Arista e HP, poderiam ter sido analisados devido à competência e produtos reconhecidos no mercado.

Para os testes em modelo convencional, foram utilizados equipamentos Nexus 9508 com 36 interfaces de 40 GE como núcleo da rede, Nexus 93108TC-EX com 48 interfaces 1/10 GE como agregação de servidores, *firewalls* e balanceadores de carga. Ambos os modelos rodaram o sistema operacional da Cisco NX-OS.

Para os testes em modelo SDN, foram utilizados os mesmos modelos, porém, com o *software* ACI instalado.

6.1.4 Preparação dos Testes

A arquitetura utilizada para o cenário de testes em redes convencional e SDN foram similares, sendo uma arquitetura baseada em duas camadas, com a única diferença na nomenclatura das camadas que, para o modelo convencional, é conhecido como núcleo e agregação e, no modelo SDN, *Spine* e *Lea*f.

Em uma rede convencional, os serviços de *firewall*, balanceamento de carga e outros podem estar posicionados na camada núcleo da rede ou agregação. A definição é feita, normalmente, levando-se em consideração o posicionamento do *gateway* de servidores. Se eles forem os *switches* de agregação, deve-se colocar os *firewalls* e demais serviços conectados a essa camada e, caso o *gateway*

termine nos *switches* núcleo de rede, os *firewalls* e demais serviços devem conectar-se a essa camada.

Em uma rede SDN, os serviços de rede são sempre conectados aos *switches Leafs*, enquanto os *Spines* possuem concentração apenas das conexões dos *Leafs*.

Foram utilizados os mesmos modelos de equipamentos, porém, para os testes em SDN, os *switches* foram convertidos para o modo ACI.

Foram expostas cinco dimensões a cada um dos modelos, conforme apresentados nas seções de testes a seguir.

6.1.4.1 Ambiente preparado para testes em reder convencionais

O ambiente de testes criado para redes convencionais foi composto por seis *switches* Cisco, sendo dois *switches* com função de *core* de rede, quatro *switches* com a função de agregação e *firewalls* ASA *Firepower* com a função de controle de aplicações.

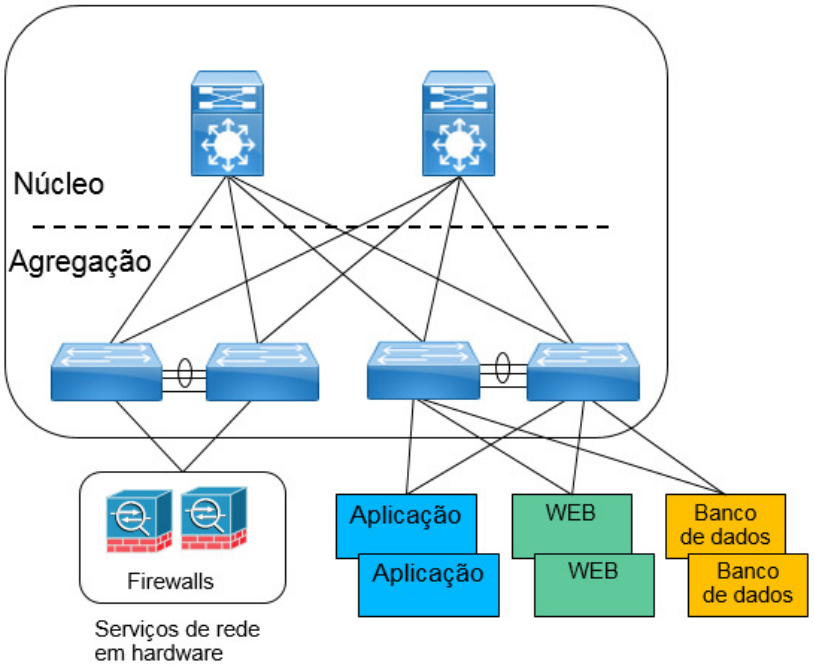
Os *switches* com função de core foram configurados como gateway da rede, portanto todo o roteamento entre as redes internas e externas era executado pelo par de *switches* Nexus 9500.

Os *switches* com função de agregação modelo família 9300 foram conectados em modo *bridge*, ou também conhecido como *layer* 2, no qual o equipamento não tem função de roteamento, apenas comutação de quadros.

Os servidores de aplicação, interface *web* e o banco de dados ficaram conectados aos *switches* de agregação.

A Fig. 13 apresenta o diagrama de rede convencional testada:

Figura 13. Diagrama de rede convencional testada



Fonte: Elaboração própria

6.1.4.2 Ambiente preparado para testes em SDN

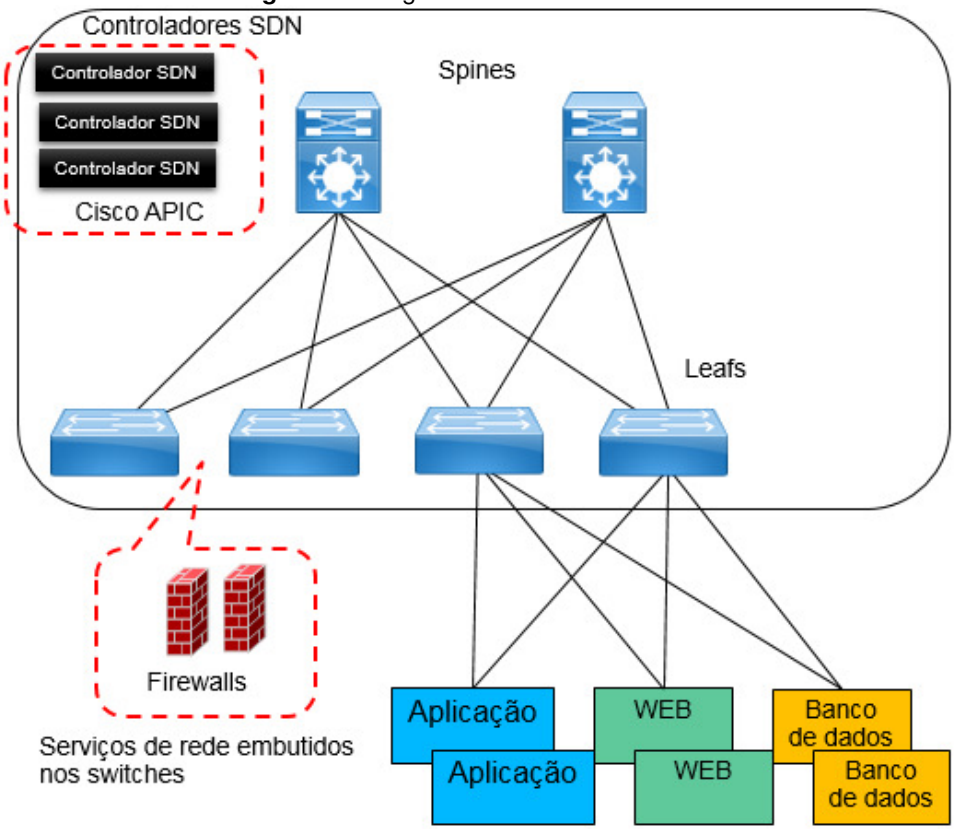
O ambiente de testes criado para redes SDN foi composto por seis *switches* Cisco, sendo dois *switches* com função de *Spines*, quatro *switches* com a função de *Leaf* e três controladores SDN Cisco APIC.

Os *switches Spines* modelo Nexus 9500 implementados em SDN foram configurados através do APIC e têm como funções principais a interconexão dos *Leafs* e a comutação dos pacotes IP leste-oeste.

Os *switches Leafs* modelo Nexus 9300 têm como funções principais as conexões de servidores, máquinas virtuais, aplicações e *gateway* da rede.

A Fig. 14 apresenta o diagrama de rede SDN testado:

Figura 14. Diagrama de rede SDN testado



Fonte: Elaboração própria

6.1.5 Execução dos testes

Os testes foram executados em ambiente de emulação e, também, num cliente real que desejava migrar sua rede para um modelo mais atual.

A necessidade de um ambiente de testes emulado é relevante para o entendimento da melhor forma de aplicação e também para o aprimoramento da sistemática.

Os testes para emulação levaram em consideração cinco aspectos, isso porque o objetivo era testar a sistemática para entender como aplicá-la em ambiente real, aperfeiçoá-la e, também, para evidenciar a necessidade de SDN em redes de *Data Center*.

O primeiro teste foi de automação e provisionamento dos equipamentos de rede. Para essa dimensão, foram testados:

- Configuração sem tocar no *hardware* "zero-touch";

- Configuração dos elementos de rede de forma centralizada;
- Provisionamento da rede de acordo com os requisitos de aplicação.

O segundo teste analisou o fluxo de comunicação e se propôs a avaliar as dimensões de:

- Ferramenta nativa ou integração simplificada com a solução;
- Análise do fluxo de aplicação e interdependência;
- Auxílio na implementação de regras de segurança.

O terceiro teste foi a implementação e medição da Qualidade de Serviço (QoS) na rede do *Data Center.* Para essa dimensão, foram avaliados:

- Função nativa nos equipamentos por meio do licenciamento;
- Exibição de níveis de SLA por aplicação;
- Integração do *template* de provisionamento da aplicação com os requisitos de QoS.

O quarto teste foi a microssegmentação de rede. Para essa dimensão, foram avaliados:

- Implementação de regras de *firewall* para camada 3 do modelo OSI e camada 4 do modelo OSI) para controle de tráfego horizontal ou leste-oeste;
- Implementação de *firewall* distribuído;
- Centralização da configuração e gerenciamento das políticas de acesso.

O quinto e último teste avaliou o gerenciamento da rede e a depuração de problemas nos seguintes aspectos:

- Plataforma integrada de gerenciamento;

- Gerenciamento dos ativos de rede como “saúde” dos equipamentos, alertas críticos e configuração centralizada;
- Ferramentas para depuração de problemas e diagnóstico;
- Planejamento de capacidade futura.

Para a execução dos testes em ambiente real, é necessário aplicar os testes para cada item crítico apontado na pesquisa, a fim de avaliar se a solução SDN escolhida atende os requisitos necessários.

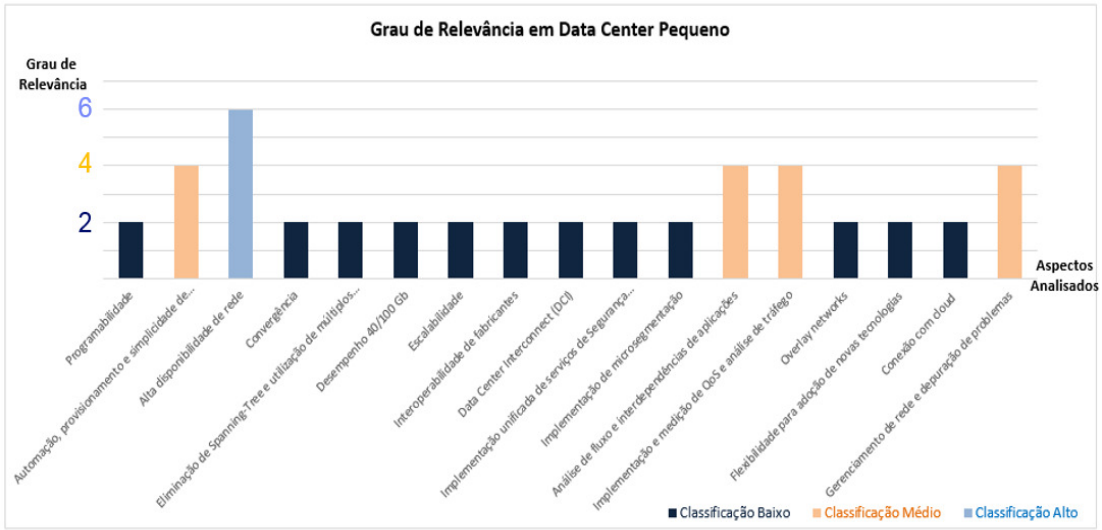
7 RESULTADOS

7.1 Pesquisa

As respostas das cinco perguntas realizadas, conforme o supcapítulo 6.1.1, foram consolidadas e agrupadas de acordo com a classificação dos *Data Centers* de grande, médio ou pequeno porte, definidos pelo número de servidores.

A pesquisa apontou que clientes com *Data Centers* pequenos estão mais interessados em simplificar a configuração e administração da rede, precisam da rede altamente disponível, possuem dificuldades para mapear os requisitos necessários para implementação da aplicação, dificuldades para aplicar e medir o QoS na rede e também necessitam de ferramentas simples, mas eficientes para o gerenciamento da rede e depuração de problemas. Apenas o aspecto de alta disponibilidade foi classificado com alta relevância ou importância para esses clientes.

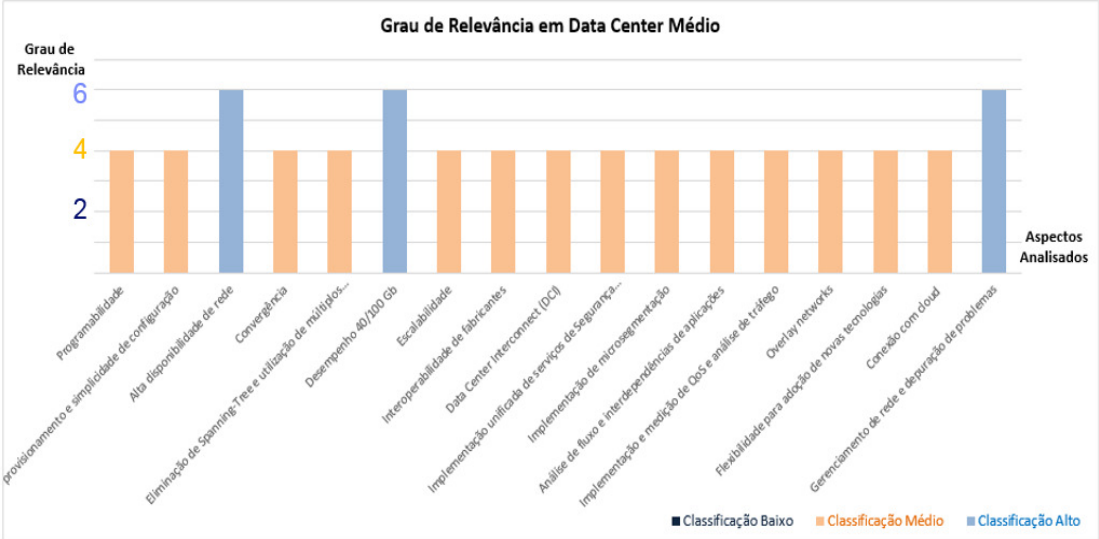
Gráfico 1. Pesquisa de Relevância com DC's Pequenos



Fonte: Elaboração própria

Clientes com *Data Centers* médios, conforme Gráf. 2, demonstraram interesse em todos os aspectos analisados e apontaram como áreas de maior interesse e relevância a alta disponibilidade de rede, a necessidade de conexão a 10 Gbps e 40 Gbps e as ferramentas para gerenciamento e depuração de falhas:

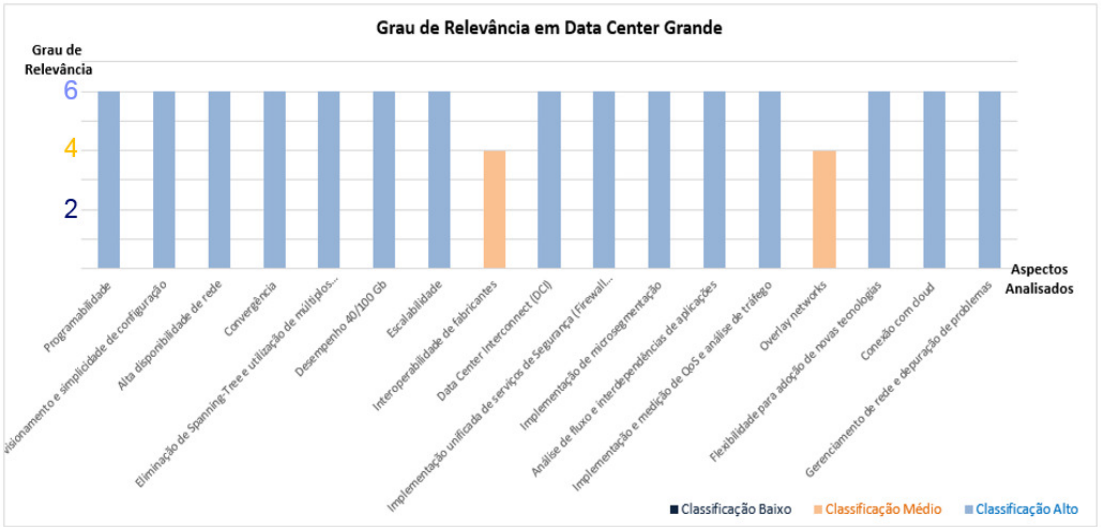
Gráfico 2. Pesquisa de Relevância com DC's Médio



Fonte: Elaboração própria

Clientes com *Data Centers* grandes, conforme Gráf. 3, demonstraram interesse e preocupação em todos os aspectos e apontaram apenas a interoperabilidade de fabricantes e o uso de redes *overlay* como relevância média. Todos os demais aspectos foram classificados como críticos:

Gráfico 3. Pesquisa de Relevância com DC's Grandes



Fonte: Elaboração própria

7.2 Testes em ambiente de emulação

Foram aplicados cinco testes nos modelos convencionais e SDN e coletados os resultados. Foram aplicados apenas cinco testes, pois o resultado já permitiu evidenciar a necessidade do uso de SDN em *Data Center* e possibilitou aprimorar a sistemática.

As cinco dimensões analisadas foram escolhidas de forma particular, porém, todos os demais testes da base de testes poderiam ser aplicados.

7.2.1 Primeiro Teste – Automação e Provisionamento de Rede

A configuração inicial de equipamentos de rede é uma atividade repetitiva e demorada por depender do acesso particular via console em cada equipamento de rede.

Após a configuração inicial, os equipamentos sofrem configurações remotas de forma unitária, até que toda a rede esteja configurada.

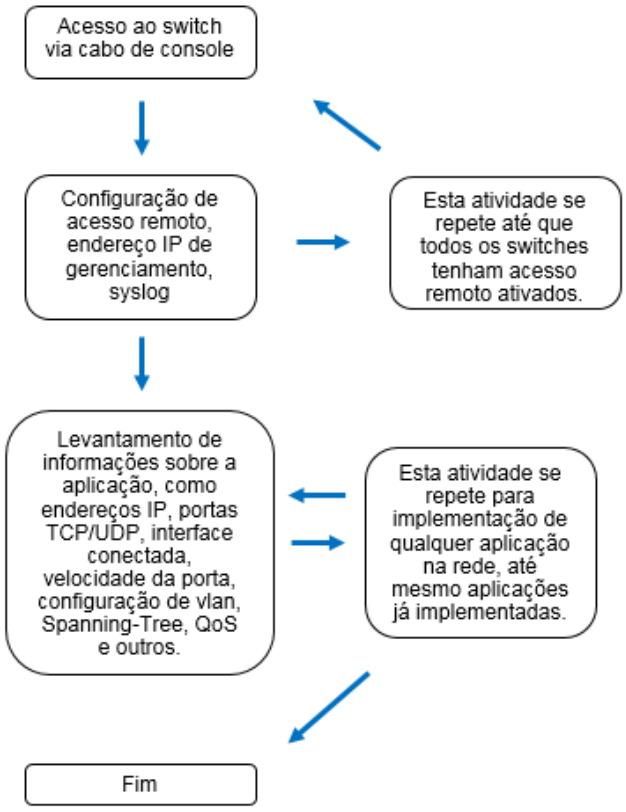
O provisionamento e automação nas redes permite ao administrador configurar inúmeros equipamentos de forma centralizada, por meio de um único painel de configuração, sem ter de realizar qualquer configuração prévia no equipamento.

REDES CONVENCIONAIS

Todos os equipamentos foram configurados de forma manual e unitariamente sem automatizar o provisionamento, pois as ferramentas são limitadas ou complexas de manusear.

O fluxograma da Fig. 15 apresenta os esforços para provisionar e configurar um novo *switch* na rede:

Figura 15. Fluxograma para ativação de *switches*



Fonte: Elaboração própria

Cada *switch* no modelo convencional precisou ser acessado unitariamente, de forma que houve a necessidade de conhecer a linguagem de configuração do equipamento em questão. Foi preciso mapear uma série de informações para implementação, configurar o *switch* e sincronizar as configurações de vlan, *Spanning-Tree*, *gateway* de rede, roteamento, QoS e outros, para que não ocorressem falta de acesso, perdas de pacotes ou comportamento indevido da rede que prejudicasse o desempenho da aplicação.

A seguir, são detalhadas algumas das configurações básicas para configuração dos *switches* de agregação:

Configuração de acesso Remoto

interface mgmt0

ip address 192.168.10.1

ssh server enable

```
ssh key rsa 2048
username admin01 sshkey ssh-rsa
```

Configuração de Spanning-Tree

```
spanning-tree mst configuration
name dc1
revision 1
instance 1 vlan 1-1000
```

Configuração de rede para interface física do servidor

```
interface ethernet 1/3
switchport mode access
switchport access vlan 2
```

Como pode ser observado na configuração apresentada, são diversos os comandos que precisam ser executados de forma unitária. Os requisitos técnicos da aplicação precisam ser mapeados manualmente, além de demandar um conhecimento aprofundado da linguagem de configuração do equipamento.

REDES DEFINIDAS POR *SOFTWARE*

Todos os equipamentos foram implementados de forma centralizada e automatizada através do APIC (*Application Policy Infrastructure Controller*).

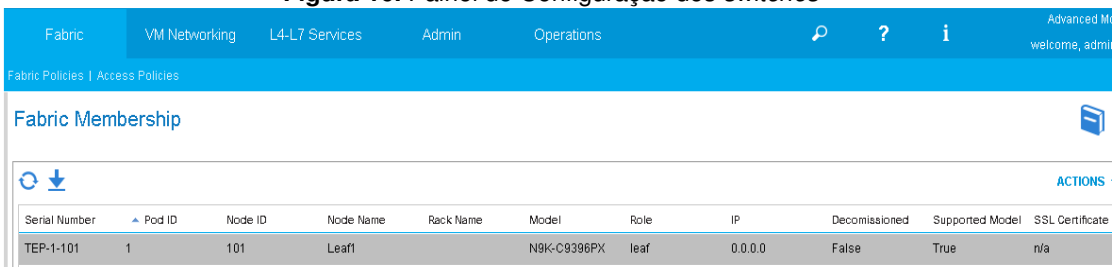
O controlador SDN ficou encarregado de automatizar a rede física.

Os três controladores implementados APIC proveram serviços de DHCP para todos os *switches*, configuração de *bootstrap* (configuração de inicialização), gerenciamento de imagem e atualizações de todos os nós do ACI (Spines e Leafs).

Cada APIC utilizou um endereço interno para se comunicar com outros APIC's, cujo endereço IP foi colocado manualmente.

Os nós do ACI (*Spines e Leafs*) foram descobertos automaticamente pelo APIC por meio do protocolo LLDP e foram configurados dinamicamente com o endereçamento IP. A Fig. 16 ilustra o painel de provisionamento e gerenciamento dos nós de rede dentro do ACI:

Figura 16. Painel de Configuração dos *switches*



Fonte: APIC

7.2.2 Segundo Teste – Fluxo de Comunicações

O entendimento do fluxo de comunicação na rede do *Data Center* é determinante na configuração apropriada de regras de *firewall* e *Quality of Service* (QoS) nos *switches*.

A análise do fluxo de comunicação é realizada nos *switches* onde as aplicações residem. Para tal, o *switch* faz uma coleta por meio de diversos protocolos existentes e exporta amostras ou fluxos para determinadas ferramentas analisarem.

REDES CONVENCIONAIS

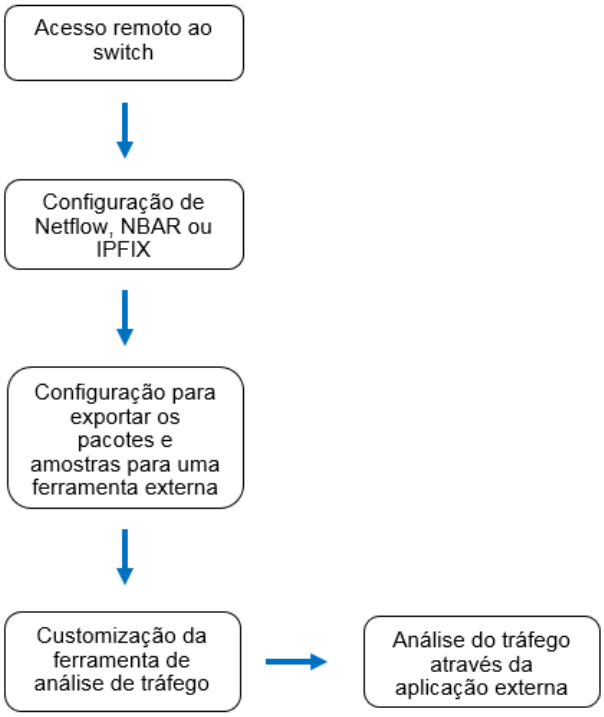
Para análise do fluxo de comunicação, foi necessário configurar os *switches* manualmente e ativar os protocolos NetFlow [27], NBAR [28] e IPFIX [29], além de provisionar uma ferramenta para coleta e análise dos fluxos de comunicação.

Os equipamentos de rede não possuem ferramentas embutidas para análise de tráfego, portanto, é necessário exportar a coleta de tráfego por meio de um dos protocolos destacados e analisá-los por meio de uma ferramenta separada.

As ferramentas para análise de fluxo em redes convencionais apresentam um custo elevado e, na maioria das vezes, não exibem informações completas das aplicações. Esse mapeamento acaba sendo desenvolvido em conjunto com um levantamento manual com o desenvolvedor.

O fluxograma da Fig. 17 representa os esforços para ativar os protocolos para coleta e análise dos fluxos de comunicação na rede:

Figura 17. Fluxograma para ativação de análise de tráfego



Fonte: Elaboração própria

REDES DEFINIDAS POR *SOFTWARE*

Para os testes em redes SDN, foi utilizada a plataforma *Tetration*, que consiste numa ferramenta da Cisco utilizada para análise de tráfego.

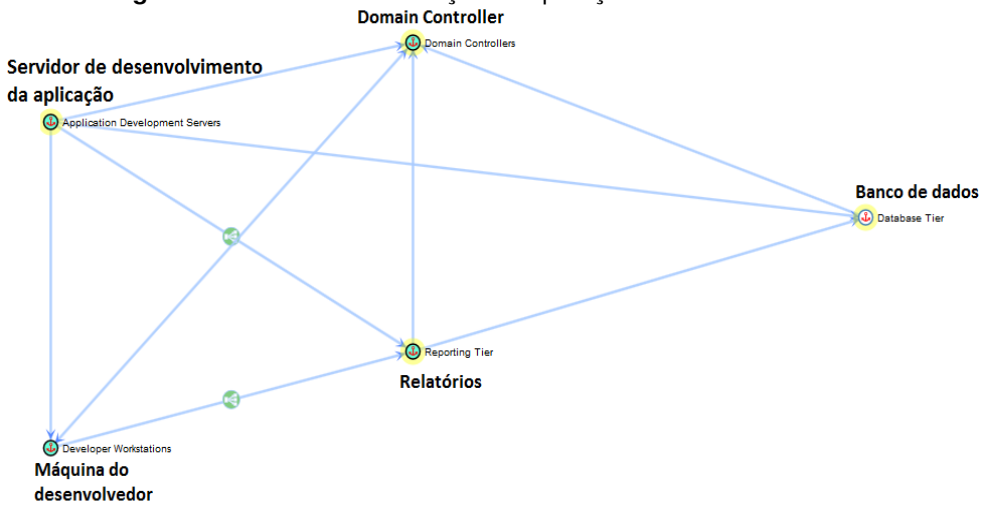
O *Tetration* é uma plataforma de análise de tráfego que se integra ao controlador SDN através de uma interface de programação de aplicativos (API).

Por meio do funcionamento em conjunto do Controlador APIC e *Tetration*, foi possível identificar as dependências da aplicação, como base de dados, controlador do domínio e também as portas TCP, UDP e protocolos para a comunicação da aplicação.

Não houve necessidade alguma de interação com o desenvolvedor da aplicação para entender os requisitos de rede para aplicação.

A Fig. 18 apresenta um fluxograma de relações com outras aplicações e interfaces:

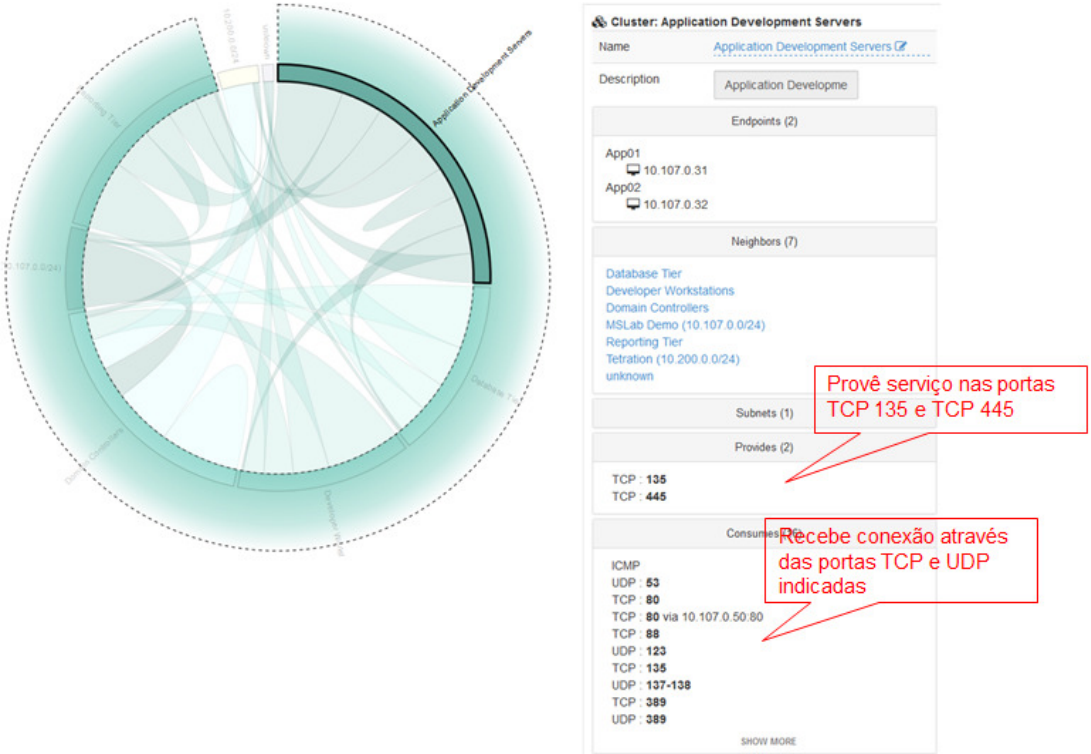
Figura 18. Fluxo de comunicação da aplicação de desenvolvimento



Fonte: Cisco Tetration

A Fig. 19 apresenta as portas TCP e UDP utilizadas durante a comunicação da aplicação:

Figura 19. Uso de portas TCP e UDP da aplicação



Fonte: Cisco Tetration

7.2.3 Terceiro Teste – Medição de QoS

O *Quality of Service* (QoS) é uma implementação fundamental nas redes atuais, porque a banda disponível na *Internet*, WAN ou nas redes de *Data Center* são limitadas e o tráfego crítico precisa ser priorizado em relação ao restante.

O QoS é implementado no *Data Center* para priorizar as aplicações mais críticas, reduzindo o *delay* (tempo de atraso) na entrega e reservando banda em momentos de congestionamento.

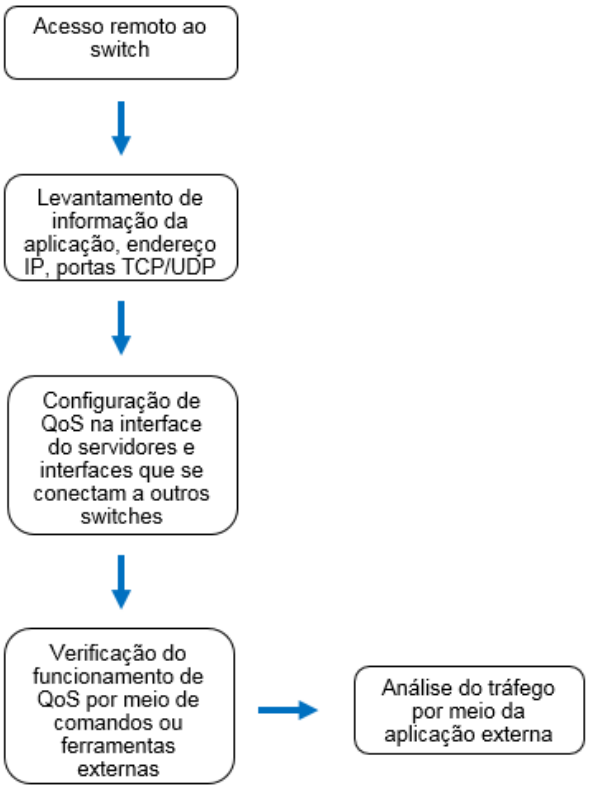
REDES CONVENCIONAIS

A implementação de QoS em redes convencionais ainda é feita de forma manual nos equipamentos, o que significa que o mapeamento e configuração são realizados de forma unitária sem qualquer ou pouca automatização.

O planejamento e implementação de QoS em redes convencionais depende do *hardware* instalado. Cada equipamento suporta um número determinado de classes e modelo proprietário de implementação.

O fluxograma da Fig. 20 representa os esforços para implementar QoS:

Figura 20. Fluxograma para ativação de análise de tráfego



Fonte: Elaboração própria

Para o teste, foi configurada uma política de QoS chamada de Critical_APP, que classifica a aplicação de desenvolvimento e reserva 10% da velocidade da interface no sentido de saída do tráfego.

Percebe-se que essa implementação é inviável em redes extensas. Muitas vezes, as empresas preferem não implementar QoS no *Data Center* devido à complexidade da implementação e gerenciamento das políticas.

A seguir, são detalhadas algumas das configurações básicas para configuração de QoS nos *switches*:

Configuração de QoS para a aplicação

ip access-list name Critical_App

permit tcp 138 any any

permit tcp 138 any any

class type qos Critical_App

```
match access-group Critical_App

policy-map type qos Critical_App
class Critical_App
bandwidth percent 10
set qos-group 4

interface ethernet 1/1
service-policy type qos Critical_App
```

REDES DEFINIDAS POR *SOFTWARE*

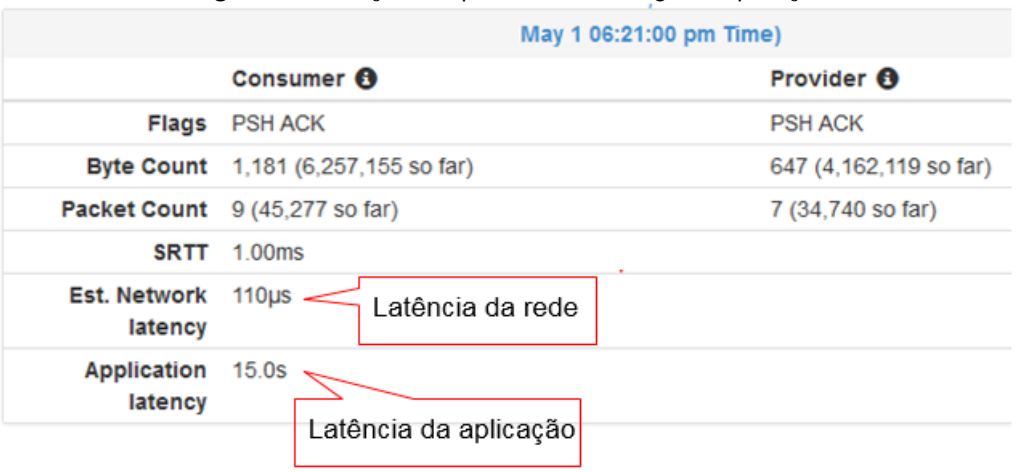
Em redes SDN, o provisionamento e gerenciamento das políticas de QoS estão embutidas no controlador. Com isso, é possível aplicar as configurações de forma centralizada e unificada, independentemente do modelo de equipamento implementado.

O controlador SDN também permite criar *templates* por tipo de máquina virtual ou aplicação. Assim, quando uma nova máquina ou aplicação são implementadas, o *template* pode ser reutilizado, trazendo agilidade na implementação e evitando erros de configuração.

As Fig. 21 e 22 apresentam algumas telas do ACI, mostrando a medição da qualidade da aplicação, uma vez que já foi mostrado como é feito o mapeamento por meio do *Tetration*.

A Fig. 21 apresenta o tempo de resposta da aplicação:

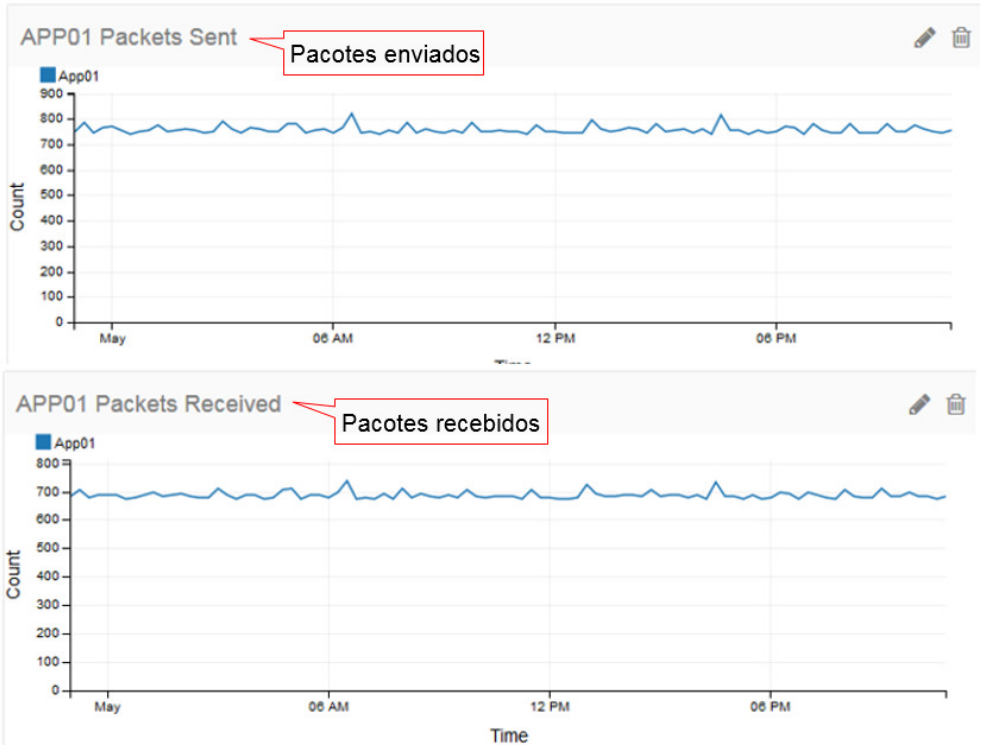
Figura 21. Medição da qualidade de tráfego da aplicação



Fonte: Tetration

A Fig. 22 apresenta os pacotes enviados e recebidos da aplicação de desenvolvimento:

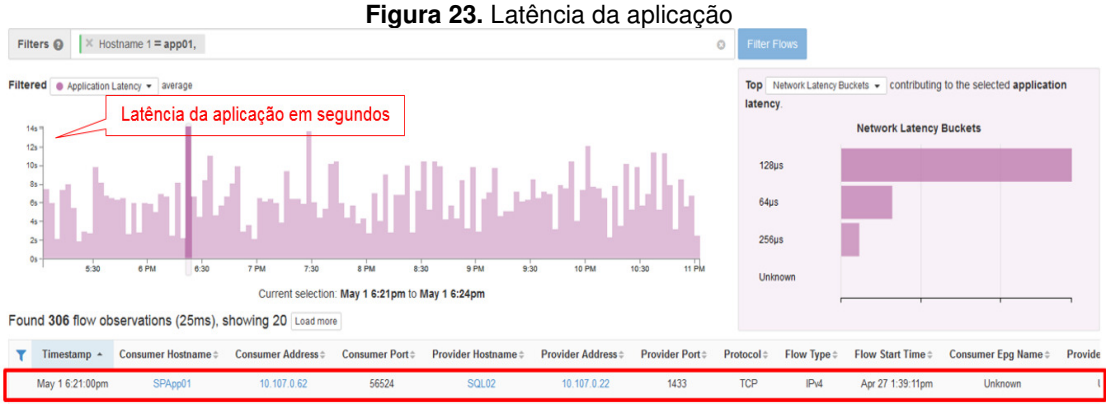
Figura 22. Gráfico de pacotes enviados e recebidos



Fonte: Tetration

A Fig. 23 apresenta a latência (atraso) da aplicação na rede tendo como referência o endereço IP do usuário que utiliza a aplicação:

Figura 23. Latência da aplicação



Fonte: Tetration

A Fig. 24 apresenta detalhes da qualidade do fluxo de comunicação entre a aplicação e o banco de dados, pacotes enviados e recebidos por intervalo de tempo.

Figura 24. Detalhes do fluxo de comunicação

Fonte: APIC

7.2.4 Quarto Teste – Microssegmentação de Rede

O perfil de tráfego nos *Data Centers* vem apresentando mudanças nos últimos anos. Isso porque a maior parcela de tráfego era de dentro para fora. Esse cenário mudou e, atualmente, o principal tráfego é interno e entre aplicações dentro do próprio *Data Center*. Essa mudança foi constatada pelo Gartner, IDC e pelos fabricantes de soluções de rede.

A implementação apenas de *firewalls* externos para controle perimetral da rede já não é tão efetiva, pois a maior parte do tráfego no *Data Center* é virtualizado. As dificuldades de controlar o tráfego virtualizado são como enviar o tráfego para um elemento centralizado, inspecioná-lo e a capacidade exigida das máquinas para processá-los.

A microssegmentação é uma funcionalidade de segurança que apareceu há pouco tempo. A pioneira no desenvolvimento de segurança em microssegmentos foi a VMWare, com o lançamento da plataforma SDN chamada de NSX, que permite criar regras de acesso distribuídas na direção leste-oeste, entre aplicações [30].

Essa função é conhecida como *firewall* distribuído (DFW), que consiste na implementação de *firewall* com alto desempenho diretamente no Kernel do *hypervisor*.

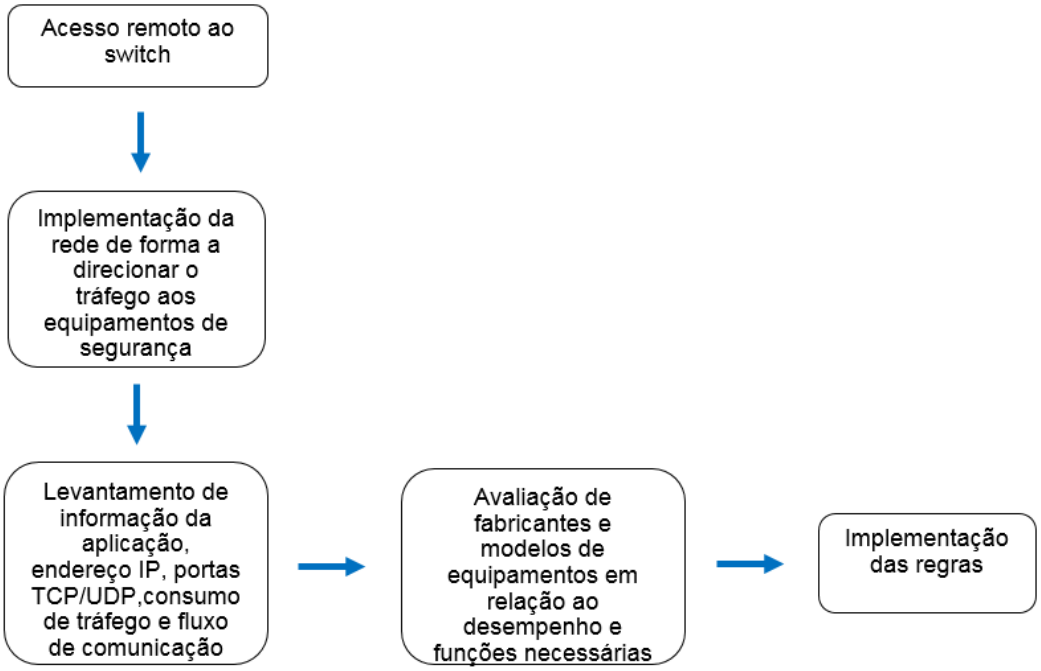
A partir dele, é possível criar regras com IP de origem, destino, porta de origem, destino e aplicação (com uso de atributos das máquinas virtuais) diretamente na camada de virtualização, sem que o tráfego saia do ambiente virtualizado e seja tratado por um *firewall* externo.

REDES CONVENCIONAIS

As redes convencionais utilizam o método clássico de utilizar *firewalls* com grande capacidade para controle do perímetro externo e interno. Esses *firewalls* utilizam o conceito de contextos para separar o controle externo e interno ou os separam por meio de equipamentos fisicamente distintos.

O fluxograma da Figura 25 apresenta os esforços necessários para implementação de tráfego externo e interno:

Figura 25. Fluxograma para implementação de segurança



Fonte: Elaboração própria

Conforme apresentado no fluxograma da Fig. 25, é muito trabalhoso, custa caro e, muitas vezes, ineficiente a implementação apenas de *firewalls* físicos no *Data Center*.

Os *firewalls* para controle em redes convencionais se tornam um gargalo (limitador) de tráfego e também um ponto único de falha na rede.

REDES DEFINIDAS POR *SOFTWARE*

Em redes definidas por *software*, os *firewalls* distribuídos ou a implementação de regras distribuídas, como acontece no ACI, são nativas. Para implementação de segurança perimetral externa ainda se utilizam de *firewalls* físicos, porém, para controle de tráfego entre as aplicações no sentido leste-oeste, é utilizado o conceito de microssegmentação.

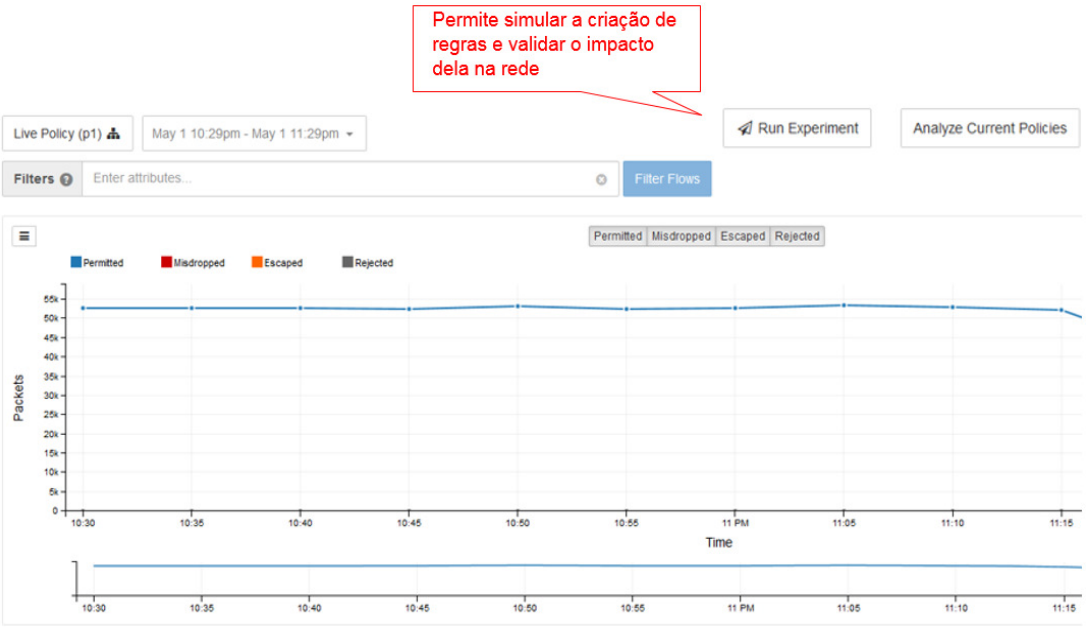
A microssegmentação pode ser implementada por meio de uma função nativa de *firewall* virtualizado, como é o caso do NSX com o componente *Distributed Firewall* (DFW) [31] ou o com o conceito de contratos como no ACI.

Para os testes em redes SDN, foi utilizado o conceito de contratos para bloquear o tráfego lateral entre as aplicações.

As Fig. 26 e 27 ilustram o procedimento a ser executado para criação das regras.

A Figura 26 permite simular a criação de regra para avaliar o impacto da regra na rede:

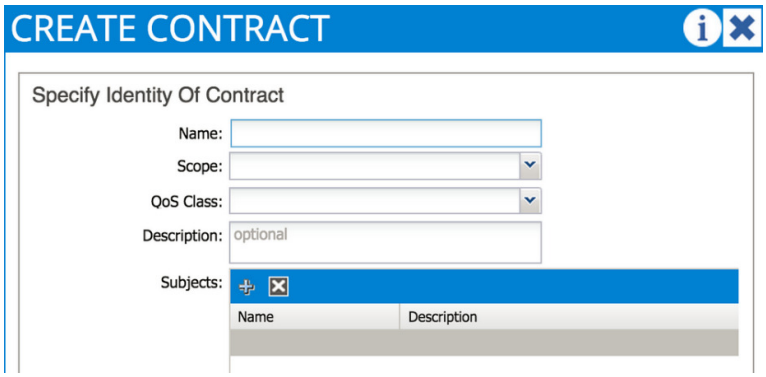
Figura 26. Funcionalidade para simulação de regras



Fonte: APIC

A Figura 27 apresenta a tela de configuração do contrato:

Figura 27. Criação de Contrato



Fonte: APIC

7.2.5 Quinto Teste – Gerenciamento de Rede e Depuração de Problemas

O gerenciamento da rede é crucial para a operação dos *Data Centers*. O gerenciamento da rede apurado ajuda a prevenir problemas, identificá-los de forma proativa e a resolvê-los mais rapidamente.

A gerência de rede, além de detectar e resolver problemas, permite à empresa planejar o crescimento de sua infraestrutura.

REDES CONVENCIONAIS

Os *switches* em redes convencionais possuem funcionalidades embutidas limitadas para o gerenciamento e depuração de problemas. Para verificação de utilização elevada de CPU, memória, erros ou utilização de interfaces e *logs*, é necessária uma série de comandos que, muitas vezes, guardam as informações temporariamente. Em muitos casos, se faz necessária a identificação de algum sintoma ou problema na rede num horário específico em que não é possível ser verificado diretamente nos equipamentos. Muitas vezes, são utilizadas plataformas de gerenciamento do próprio fabricante ou também outros fabricantes que possuam suporte.

Foram utilizadas nos testes apenas funções embutidas nos equipamentos e mostradas por meio de comandos de verificação.

O comando *show system resource* apresenta a média de consumo de CPU e memória do *switch*.

switch# **show system resources**
Load average: 1 minute: 0.00 5 minutes: 0.03 15 minutes: 0.05
Processes : 355 total, 1 running
CPU states : 0.0% user, 0.3% kernel, 99.7% idle
CPU0 states : 0.0% user, 1.0% kernel, 99.0% idle
CPU1 states : 0.0% user, 0.0% kernel, 100.0% idle
CPU2 states : 0.0% user, 0.0% kernel, 100.0% idle
CPU3 states : 0.0% user, 0.0% kernel, 100.0% idle
Memory usage: 16402560K total, 2564208K used, 13838352K free
Current memory status: OK

O comando *show processes cpu history* apresenta o consumo de cpu do *switch* por segundo e nas últimas 72 horas.

```
switch(config)# show processes cpu history

100
 90
 80
 70
 60
 50
 40
 30
 20                          #                       #       #
 10    ##            #     #   ##                    #       ##
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5

100
 90
 80
 70
 60
 50
 40
 30
 20
 10**************************************************************************

0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0

                CPU% per hour (last 72 hours)
               * = maximum CPU%   # = average CPU%
```

Porcentagem de utilização da CPU a cada 5 segundos

Porcentagem de utilização da CPU a cada 5 horas

REDES DEFINIDAS POR *SOFTWARE*

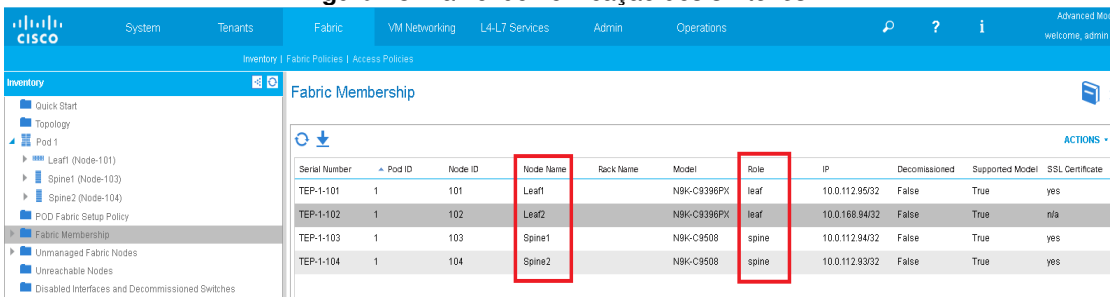
O gerenciamento da rede SDN é nativo, sendo que, por meio do controlador SDN, é possível identificar falhas nos equipamentos, como fonte ou ventoinha

danificados, alta utilização dos recursos de *hardware*, como memória e CPU em tempo real, além de manter os arquivos de configuração atualizados e o histórico de alertas e falhas nos equipamentos.

As Fig. 28 e 29 apresentam os painéis básicos de gerenciamento do ACI.

A Fig. 28 apresenta informações dos *switches*, como endereços IP, nome dos equipamentos e função na rede:

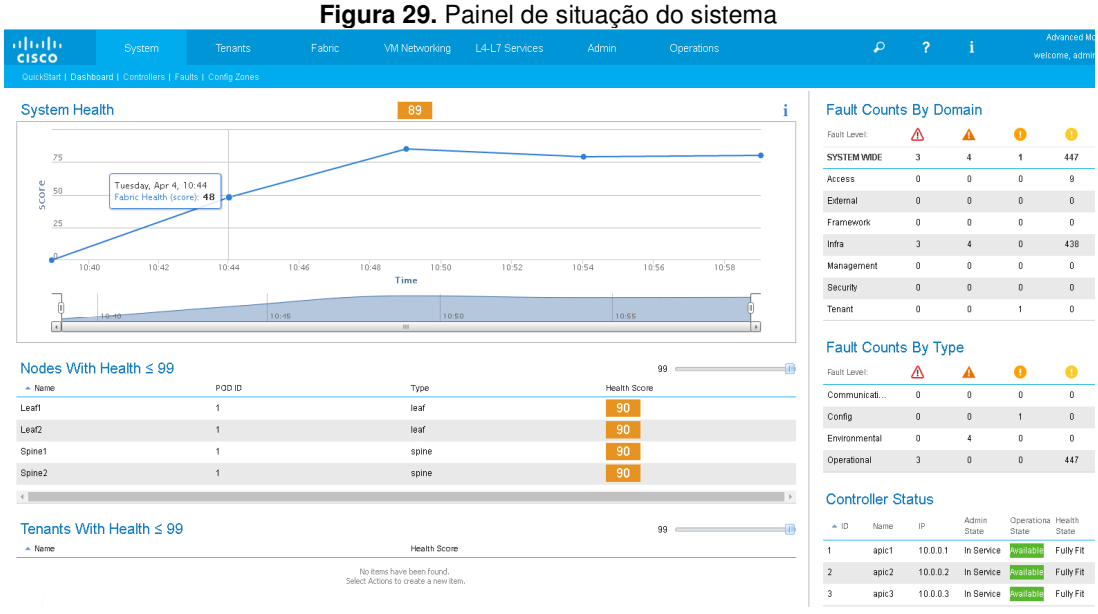
Figura 28. Painel de verificação dos *switches*



Fonte: Imagem do APIC

A Fig. 29 apresenta informações dos *switches*, como tempo de disponibilidade, alertas e utilização de recursos como memória e CPU:

Figura 29. Painel de situação do sistema



Fonte: Imagem do APIC

7.3 Sistemática em ambiente real

A sistemática foi aplicada em um cliente real de grande porte do mercado varejista depois de ser testada em ambiente de emulação. O teste em ambiente de emulação serviu para aperfeiçoar os questionamentos, permitindo identificar as perguntas que conseguiriam obter mais informações de forma genérica, enriquecer a base de testes e direcionar melhor a seleção da solução SDN.

A fim de avaliar o método na prática, ou seja, em um cliente real que desejava implementar SDN em seu *Data Center*, o método foi aplicado com a permissão do cliente.

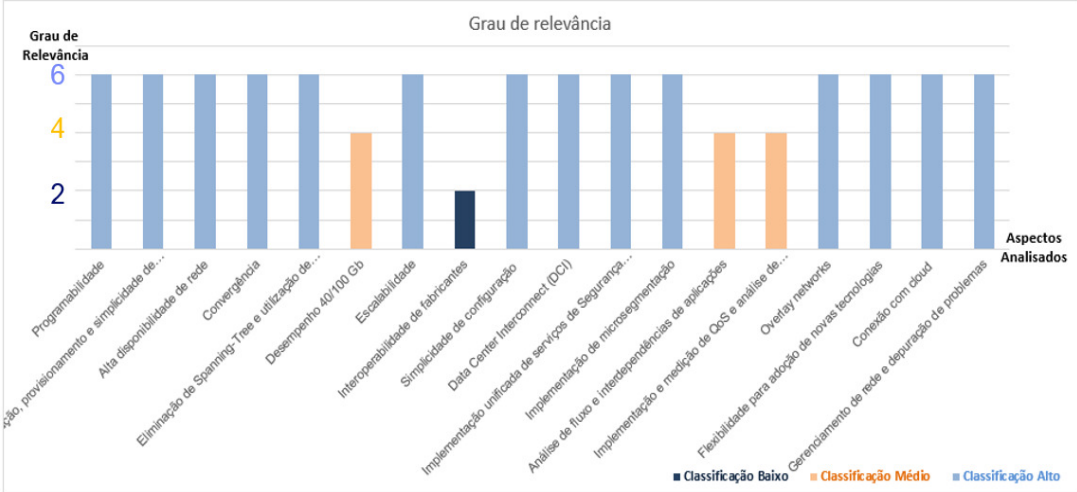
O cliente real é um dos maiores varejistas no Brasil e possuía, em média, 2000 servidores físicos e virtuais espalhados em três *Data Centers* na mesma localidade, ou seja, separados apenas por salas.

Esse cliente desejava atualizar sua rede por um modelo mais atualizado, pois sua rede tinha sido implementada há mais de 10 anos, houve poucas atualizações e inovações desde então e a rede não permitia mais que o cliente crescesse de forma estruturada sem a paralisação da comunicação.

Foi executada a metodologia da sistemática por meio da pesquisa, depois apresentado o caderno de testes, foi selecionado em conjunto com o cliente a solução mais adequada, realizados testes em ambiente controlado do cliente e a elaboração de um relatório com os resultados e conclusões.

Para a etapa da pesquisa, foi aplicado o mesmo questionário e observou-se que apenas quatro aspectos não eram tão críticos e relevantes ao cliente: o primeiro era a adoção de interfaces 10 Gbps ou 40 Gbps para os servidores, isso porque 90% das interfaces de servidores eram de 1 Gbps e não consumiam 40% da carga, dados constatados em uma ferramenta de monitoração dos *switches*. O segundo, de que não havia restrições em utilizar um único fabricante como já era feito. O terceiro, de que não havia dificuldades para o mapeamento de requisitos da aplicação (fluxo de comunicação das aplicações). O quarto, de aplicação de QoS na rede, pois havia um processo bem definido para levantamento de requisitos da aplicação, sendo que cada uma que aplicada era desenvolvida e passava por um processo de homologação na rede antes de ser implementada e, durante o processo, eram mapeados os requisitos da aplicação por meio de ferramentas.

Gráfico 4. Resultado da pesquisa



Fonte: Elaboração própria

O cliente apontou que todos os demais aspectos eram críticos para seu ambiente porque tinha limitações de crescimento, faltavam ferramentas para gerenciamento, a rede física não comportava mais o crescimento “vegetatitvo” sem criar gargalos, o protocolo *Spanning-Tree* era de difícil administração. O cliente precisava estender sua rede até outro D*ata Center*, cuja extensão da rede é chamada de *Data Center Interconnect* (DCI), para aplicar *VMotion*, mas tinha receio de prolongar seus problemas para o outro *Data Center*, entre outras dificuldades.

Com base nas informações levantadas na pesquisa e considerações finais do cliente, foi produzida uma base de testes que avaliou os seguintes aspectos críticos:

- Programabilidade;
- Automação, provisionamento e simplicidade de configuração;
- Alta disponibilidade de rede;
- Convergência;
- Eliminação de *Spanning-Tree* e utilização de múltiplos caminhos (*Multipath*);
- Escalabilidade;
- Simplicidade de configuração;
- *Data Center Interconnect* (DCI);

- Implementação unificada de serviços de Segurança (*Firewall* e IPS) para ambientes físico e virtual;
- Implementação de microssegmentação;
- *Overlay networks*;
- Flexibilidade para adoção de novas tecnologias;
- Conexão com *cloud*;
- Gerenciamento de rede e depuração de problemas.

A escolha da solução foi realizada com base nos seguintes critérios:

- O cliente tinha preferência de um fabricante, contanto que este atendesse os seus requisitos;
- Conheceu outros clientes do mesmo ramo que tinham implementado a solução com sucesso;
- Precisava atualizar sua rede física (*underlay*) e, ao mesmo tempo, gostaria de iniciar sua implementação de redes virtualizadas (*overlay*);
- A solução tinha sido desenvolvida há mais de 5 anos e possuía maturidade suficiente para implementação em sua rede;
- Atendia o orçamento reservado de 7 milhões de reais.

Por meio do teste de programabilidade, o cliente identificou que conseguia criar redes adaptáveis ao seu negócio e também a criar processos e automatizações por meio de API's que agilizariam o provisionamento e a depuração de problemas.

Os testes de automação, provisionamento, simplicidade e flexibilidade de adoção de novas tecnologias permitiram ao cliente identificar a essência de SDN, a agilidade, redução no tempo de provisionamento da rede e a integração com outras soluções por meio de API's.

A Fig. 30 apresenta algumas linhas de código XML usadas para programação e automação dos *switches* dentro do ACI. Nesse exemplo, foram configurados os objetos nomeados de *Policy Group* (infraAccBndlGrp), o perfil das interfaces nomeado de *Interface Profile* (infraAccPortP) e o perifil dos *switches*

nomeado de *Switch Profile* (infraNodeP) via programação XML, isso para acelerar o processo de provisionamento dos *switches* e portas que se conectam aos servidores:

Figura 30. Programação por XML

```
<polUni dn="uni">
      <infraInfra dn="uni/infra" ownerKey="" ownerTag="">
            <infraNodeP descr="" dn="" name="<NOME_SWITCH_PROFILE_VPC>" ownerKey=""
ownerTag="">
                  <infraLeafS descr="" dn="" name="<NOME_NODES_SWITCHES_VPC>"
ownerKey="" ownerTag="" type="range">
                        <infraNodeBlk descr="" dn="" from_="<SWITCH_NODE_ID_1_VPC>"
to_="<SWITCH_NODE_ID_2_VPC>"/>
                  </infraLeafS>
                  <infraRsAccPortP dn="" tDn="uni/infra/accportprof-
<NOME_INTERFACE_PROFILE>"/>
            </infraNodeP>
            <infraFuncP descr="" dn="" name="default" ownerKey="" ownerTag="">
                  <infraAccBndlGrp descr="" dn="" lagT="node"
name="<NOME_POLICY_GROUP>" ownerKey="" ownerTag="">
```

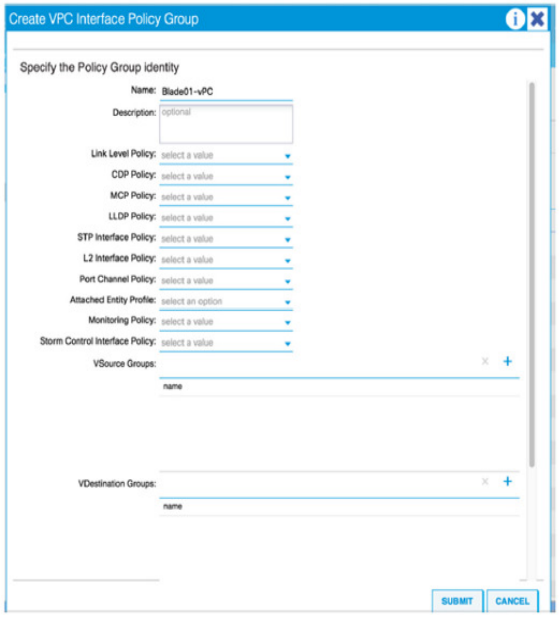
REST

Método	Ação
POST	Criar/Atualizar
GET	Ler
DELETE	Deletar

Fonte: Elaboração própria

A Fig. 31 apresenta o processo gráfico utilizado para configuração padronizada das interfaces que se conectam a dispositivos de rede. Nesse exemplo, os protocolos CDP e LLDP utilizados para descoberta de informações do dispositivo diretamente conectado estão habilitados, o protocolo LACP, utilizado para agregação de vários *links* físicos como um único lógico, está habilitado e a velocidade da interface está configurada em 10 Gbps em *full duplex*. Essa configuração foi aplicada de modo gráfico em todas as interfaces que se conectam a roteadores, *firewalls* e balanceadores de carga:

Figura 31. Configuração de Policy Group



CDP_Enabled – Protocolo CDP Habilitado
LLDP_Enabled – Protocolo LLDP Habilitado
LACP_Active – Procoloco LACP configurado como Ativo
10G_Auto – Link Level definido como 10Gbps Auto Negociação
10G_Full – Link Level definido como 10Gbps Full Duplex

Fonte: ACI – Policy Group

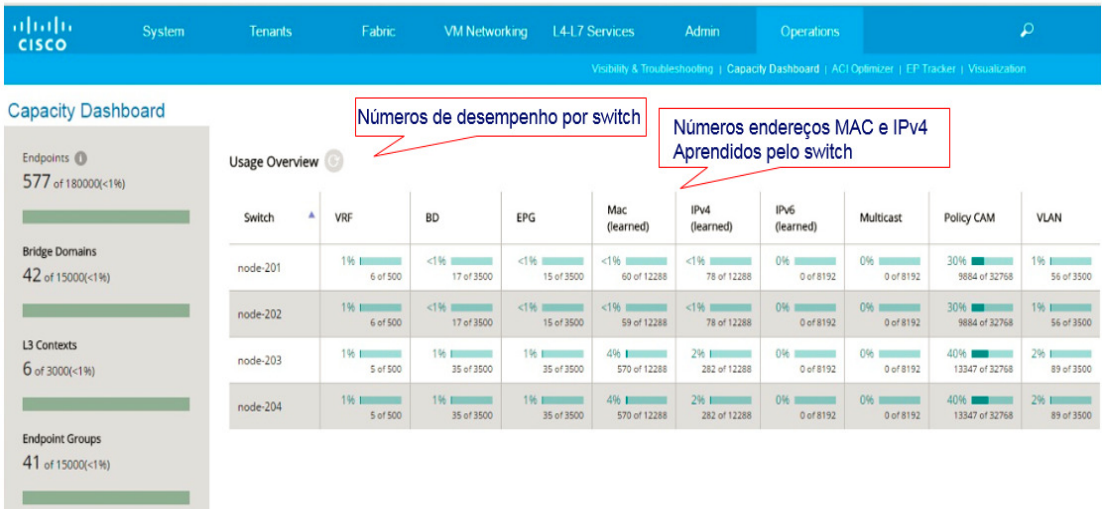
O teste de alta disponibilidade autenticou a alta disponibilidade oferecida pelo *hardware* e *software*, além de destacar a função de *anycast* nos *Leafs*, uma função que traz o *gateway* de rede para cada *Leaf* como se fosse um grande *switch* distribuído.

O teste de convergência demonstrou a continuidade do funcionamento da rede com a queda de um *link* porque as conexões dos *Spines* e *Leafs* são roteáveis e possuem balanceamento entre todos os *links* ativos.

O teste de eliminação de *Spanning-Tree* demonstrou que os equipamentos utilizam interfaces roteáveis para conexão entre os *Spines* e *Leafs* e a funcionalidade de vPC permitiu conectar ao servidor através de dois *Leafs* com balanceamento de carga.

O teste de escalabilidade permitiu avaliar, por meio da interface gráfica, a capacidade utilizada dos *switches* em termos de endereços MAC, IPv4, número de *Bridge Domains* e EPG e planejar a capacidade futura, conforme a Fig. 32:

Figura 32. Capacidade no ACI



Fonte: ACI – *Capacity Dashboard*

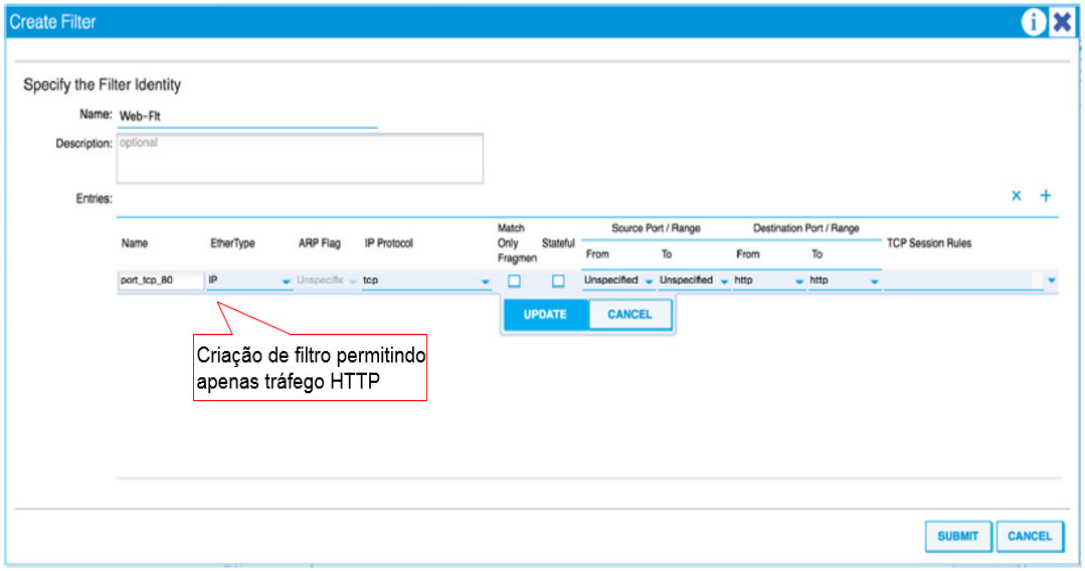
O teste de DCI foi relevante para testar a melhor forma de estender vlans entre *Data Center* de forma controlada por meio do protocolo MP-BGP, que consiste num protocolo de roteamento utilizado para controle do VxLAN.

A implementação de serviços de segurança permitiu testar o gerenciamento unificado das soluções de segurança em *hardware* e em *software* por meio de *Network Function virtualization* (NFV).

A implementação da microssegmentação foi extremamente importante, pois o cliente desejava criar regras de controle na camada de virtualização, sem que o tráfego saísse da rede virtualizada e fosse controlado num equipamento físico.

A Fig. 33 ilustra a criação de um contrato, permitindo apenas tráfego HTTP para um servidor:

Figura 33. Criação de filtros de segurança no ACI (contratos)



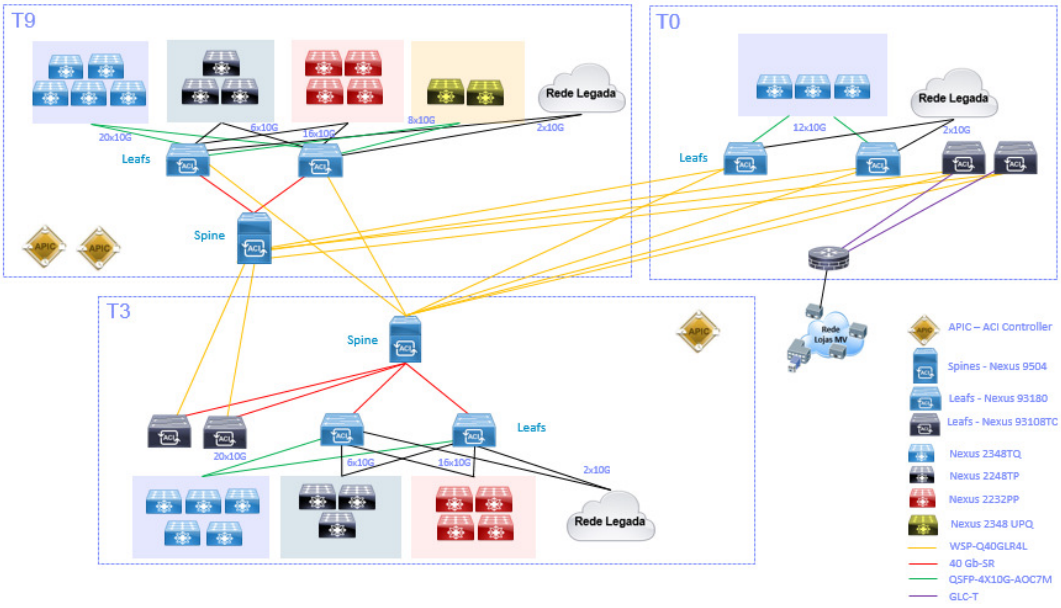
Fonte: ACI – *Create filters*

O teste de conexão com a *cloud* avaliou a integração da solução com *cloud* pública, permitindo a extensão da rede de *Data Center* até a *cloud* pública de forma simplificada e controlada.

Por fim, o teste de gerenciamento apresentou toda a gama de recursos embutida no controlador SDN, desde a identificação proativa de problemas à resolução de forma centralizada e simplificada.

O resultado apresentado evidenciou a facilidade, flexibilidade e redução do tempo gasto para implementação de uma aplicação com o uso de SDN.

Figura 34. Diagrama de rede implementado no cliente varejo



Fonte: Elaboração própria

O uso da sistemática permitiu estruturar e evidenciar a escolha do modelo de implementação de rede e, também, quais são os estágios necessários para implementar uma rede SDN no cliente. Isso porque a pesquisa apresentou todas as dificuldades do cliente, direcionou a criação da base de testes e os resultados dos testes confirmou a escolha do modelo mais adequado de rede para esse cliente.

O cliente comprou a solução sem riscos de perder o investimento realizado e implementou-a sem a necessidade de outros testes, o que trouxe maior agilidade na implementação e redução do ciclo de projeto.

CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo apresentar uma sistemática para implementação de redes definidas por *software*. A sua contribuição deve-se ao fato de as empresas estarem interessadas em implementar SDN em seus *Data Centers*, porém, com a inexistência de uma sistemática neutra a fabricantes que avaliem se a empresa deve, ou não, migrar para uma rede baseada em SDN e quais etapas deveria percorrer. Portanto, acaba postergando ou não encontrando justificativas técnicas e financeiras para investir na tecnologia.

A tecnologia SDN mostrou-se vantajosa em relação às redes convencionais, visto que apresentaram vantagens no primeiro teste de automação e provisionamento, no segundo teste de análise do fluxo de comunicação das aplicações, no terceiro, para implementação e medição de QoS e, no quinto teste, para o gerenciamento e depuração de falhas, mostrando que está mais preparada para a atual evolução computacional e aos desafios futuros em redes de comunicação de dados.

A sistemática apresentou resultados significativos em relação ao método antigo, que mapeava apenas o número de interfaces 1 Gbps e 10 Gbps, permitindo, por meio da pesquisa, identificar os requisitos técnicos e comerciais dos clientes, criar uma base de testes genérica e agnóstica ao fabricante, auxiliou na seleção da solução desejada, estruturou a base de testes, avaliou se a solução escolhida se adequava aos requisitos. Por fim, gerou um caminho mais compreensível e estruturado para a implementação de SDN em *Data Center*.

Essa sistemática permite às empresas a adoção da solução de rede mais adequada ao seu *Data Center* e a investir fundamentada numa sistemática estruturada, mapeando e endereçando eventuais problemas e dificuldades antes de adquirir e implementar uma nova solução.

A sistemática implementada foi benéfica à empresa em que o autor desta dissertação trabalha, visto que também foi aplicada em outros dois clientes que desejavam migrar suas redes convencionais para redes baseadas em SDN, precisavam avaliar seu ambiente existente e definir uma metodologia para migração. A sistemática foi utilizada nos dois casos com êxito por outras pessoas que trabalham no mesmo setor e se mostrou eficiente, mapeando todas as

necessidades dos clientes e direcionando a seleção e adoção da solução mais adequada, apesar dos diferentes portes e ramos das empresas.

A sistemática foi padronizada pelo time nacional para implementação de novas redes SDN e também motivou a criação de outra sistemática para implementação de redes *Wi-Fi*.

É importante que a sistemática seja aperfeiçoada em trabalhos futuros, visto que a tecnologia SDN está em desenvolvimento e constante evolução, o que pode implicar a criação de novas etapas e novos testes.

REFERÊNCIAS

[1] Roberto di Lallo,m, Mirko Gradillo, Gabriele Lospoto, Claudio Pisa, Massimo Rimondini, “On the Practical Applicability of SDN Research”, 2016

[2] Towards a Tactical Software Defined Network

[3] SDN and NFV Benchmarking for Performance and Reliability

[4] Girish L, Sridhar K. N. Rao, “Mathematical Tools and Methods for Analysis of SDN: A Comprehensive Survey”.

[5] Cisco Network Academy “Connecting Networks Companion Guide, Capítulo 1” 2014.

[6] Cisco, “Enterprise Campus 3.0 Architecture”. [Online]. Available:http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html

[7] M. Zhang, H. Wen e J. Hu, RFC7727, "Spanning Tree Protocol (STP) Application of the Inter-Chassis Communication Protocol (ICCP)", 2016.

[8] Cisco, Chapter: “Virtual Switching Systems Design Introduction”. [Online]. Available:http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/VSS30dg/campusVSS_DG/VSS-dg_ch1.html

[9] ONF, “SDN Architecture”. [Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR-521_SDN_Architecture_issue_1.1.pdf

[10] Open Networking Foundation (ONF). [Online]. Available: https://www.opennetworking.org.

[11] “Software-defined networking: The new norm for networks,” Palo Alto, CA, USA, White Paper, Apr. 2012. [Online]. Available: https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf

[12] Longbin Chen, Meikang Qiu , Jian Xiong, “An SDN-Based Fabric For Flexible Data-Center Networks”

[13] Charles Clos “A study of non-blocking switching networks”, 1996.

[14] Network World. [Online]. Available: http://www.networkworld.com/article/2226122/cisco-subnet/clos-networks--what-s-old-is-new-again.html.

[15] M. Mahalingam, D. Dutt, K. Duda, RFC 7348 , Virtual eXtensible Local Area Network (VXLAN). [Online]. Available: https://datatracker.ietf.org/doc/rfc7348/?include_text=1.

[16] Marian Klas, “VXLAN Design and Deployment”. [Online]. Available: https://www.cisco.com/c/dam/m/sl_si/events/2016/cisco_dan_inovativnih_resitev/pdf/cisco_day_slovenia_2016_vxlan_marian_klas_final.pdf.

[17] Navaid Shamsee, David Klebanov, Hesham Fayed, Ahmed Afrose, Ozden Karakok. “CCNA Data Center DCICT 200-155 Official Cert Guide” 2017.

[18] E. Haleplidis, K. Pentikousis, S. Denazis, J. Hadi Salim, “Software-Defined Networking (SDN): Layers and Architecture Terminology” 2015

[19] Hailog Zhang, Xiao Guo, Jinyao Yan, Bo Liu, Qianjun Shuai, “SDN-Based ECMP Algorithm for Data Center Networks”, 2014.

[20] 24M. Smith, M. Dvorkin, Y. Laribi, V. Pandey, P. Garg e N. Weidenbacher. “OpFlex Control Protocol draft-smith-opflex-00”. [Online]. Available: https://tools.ietf.org/html/draft-smith-opflex-00, 2014.

[21] Samer Salam, "Overlays, Underlays and the New World Order". [Online]. Available: https://blogs.cisco.com/getyourbuildon/overlays-underlays-and-the-new-world-order

[22] Cisco Systems, "Application Centric Infrastructure (ACI)". [Online]. Available: http://www.cisco.com/c/en_au/solutions/data-center-virtualization/aci.html

[23] Cisco Systems. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/aci-fundamentals/b_ACI-Fundamentals.pdf.

[24] Cisco Systems. [Online]. Available: http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps13004/ps13460/white-paper-c11-729906_ns1261_Networking_Solutions_White_Paper.html.

[25] Cisco Systems. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731630.html

[26] Lauren Malhoit, “Cisco ACI – Creating Contracts”. [Online]. Available: http://techgenix.com/cisco-aci-creating-contracts/.

[27] B. Claise, Ed. Cisco Systems, RFC 3954. [Online]. Available: https://www.ietf.org/rfc/rfc3954.txt.

[28] Cisco Systems, “Network Based Application Recognition (NBAR)” [Online]. Available: “http://www.cisco.com/c/en/us/products/ios-nx-os-software/network-based-application-recognition-nbar/index.html”

[29] B. Claise, B. Trammell, Cisco Systems, RFC 7011, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information"

[30] VMWare. [Online]. Available: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-microsegmentation.pdf, páginas 6-8.

[31] VMWare. [Online]. Available: https://pubs.vmware.com/NSX-6/topic/com.vmware.nsx.admin.doc/GUID-42EA8F48-8F13-4504-9FD1-3BE48D8B2F9E.html.