FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Clesio Guimarães Belizário Junior

SDN e Desafios de Segurança

Americana, SP

2020

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Clesio Guimarães Belizário Junior

SDN e Desafios de Segurança

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em 2020, sob a orientação do Prof. Esp. Marcus Vinícius Lahr Giraldi.

Área de concentração: Segurança da Informação.

Americana, SP.

2020

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

B38s BELIZÁRIO JÚNIOR, Clésio Guimarães

SDN e desafios de segurança. / Clésio Guimarães Belizário Júnior. – Americana, 2020.

52f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Marcus Vinícius Lahr Giraldi

1 Segurança em sistemas de informação I. GIRALDI, Marcus Vinícius Lahr II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.3.05

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Clesio Guimarães Belizário Junior

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pela Faculdade de Tecnologia de Americana.
Área de concentração: Segurança da Informação.

Americana, Dezembro de 2020.

Banca Examinadora:

_____
Marcus Vinicius Lahr Giraldi (Presidente)
Especialista
Fatec Americana Ministro Ralph Biasi

_____
José Martins Junior (Membro)
Doutor
Fatec Americana Ministro Ralph Biasi

_____
Daniele Junqueira Frosoni (Membro)
Especialista
Fatec Americana Ministro Ralph Biasi

AGRADECIMENTOS

Primeiramente a Deus, por iluminar sempre meu caminho colocando nele pessoas de bem.

Sou grato pela minha família, pelo amor, incentivo e apoio durante toda a vida.

Deixa-se um agradecimento especial ao orientador, Marcus Vinicius Lahr Giraldi pelo incentivo e pela dedicação do seu escasso tempo ao meu projeto de pesquisa.

Quero agradecer à Faculdade de Tecnologia de Americana e a todos os professores do curso pela elevada qualidade do ensino oferecido.

Também agradeço a British Telecom por me abrir as portas e tornar possível a realização deste projeto e a todas as pessoas que fizeram parte da minha experiencia profissional até hoje.

E mesmo em meio a tantos desafios no ano de 2020 em virtude da pandemia da Covid-19 enfrentada pelo mundo, espera-se que todos continuem com saúde e propósito sempre.

DEDICATÓRIA

Aos meus pais, amigos, esposa e filha. Grato pela compreensão de todos com as minhas horas de ausência. Vocês foram a mola propulsora que permitiu o meu avanço, mesmo durante os momentos mais difíceis. Agradeço do fundo do meu coração.

RESUMO

Este trabalho tem como objetivo apresentar a tecnologia SDN e suas propostas para a arquitetura de redes moderna.

Inicialmente será descrito como são as redes de computadores tradicionais, suas demandas e limitações e, também desafios existentes. Em seguida será mostrado SDN e sua arquitetura, ressaltando as propostas de melhoria que a tecnologia traz para o atual cenário de redes de computadores e como ela os cumpre.

Também será abordado questões de segurança sobre a tecnologia, mostrando que ainda existe um grande caminho a percorrer para alcançar a sua melhor forma, e que por mais que consiga resolver vários dos problemas que temos na arquitetura atual, também traz alguns novos e ainda revitaliza outros problemas antigos.

Palavras-Chave: SDN; Segurança; OpenFlow; Arquitetura de Redes.

ABSTRACT

This purpose of this work is to expose the difficulties of current computer networks and the factors that led to the need to develop a new architecture, the SDN.

Initially, it will be described how traditional computer networks are, their demands and limitations and also existing challenges. Next, SDN and its architecture will be showed, highlighting the improvement proposals that the technology brings to the current scenario of computer networks and how it fulfills them.

Technology security issues will also be addressed, showing that there is still a long way to go to achieve its goal, and despite being able to solve many of the problems we have in the current architecture, it also brings some new ones and revitalizes some old problems.

Keywords: SDN; Security; OpenFlow; Network Architecture.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE GRÁFICOS

1 INTRODUÇÃO

O aumento de tendências, demandas, fornecedores e tipos de serviços tem forçado as provedoras e usuários a repensarem na arquitetura tradicional de redes. Com o aumento de novas tendências e formas de se utilizar redes de computadores, houve um aumento na demanda das redes corporativas, na internet e em outras redes. Estas novas tendências são (STALLINGS, 2015): Aumento significativo de Computação na nuvem pelas empresas, tanto serviço público quanto privado; Aumento do processamento de grandes conjuntos de dados em vários servidores; Tráfego de dispositivos móveis e acesso a redes corporativas a partir deles tem crescido muito e, com isso o seu consumo também; IoT (*Internet of Things*) tem-se inserido um grande número de dispositivos que acessam as redes, consequentemente aumentando a movimentação de redes corporativas assim como os dispositivos móveis.

Uma pesquisa realizada *Internet World Stats* neste ano (2020) mostra o crescimento gigantesco que existe no número de usuários da internet desde 1995, no Gráfico 1 apresenta-se os números.

Gráfico 1 - Crescimento do número de usuários de internet

Fonte: Internet World Stats – Internet growth statistics (2020)

Além do aumento da demanda, o tráfego tem-se tornado cada vez mais complexos. A forma padrão de arquitetura de redes consistia em um campus local com uma ou mais redes LAN conectadas e uma saída conectando a WAN através de um ou mais roteadores, e estes campus teriam então acesso a outros campus através

disto. Esta arquitetura funciona bem para conexões cliente/servidor, o que também era mais utilizado.

Com este modelo, o tráfego ficava na maior parte do tempo entre um cliente e um servidor, a rede poderia ser configurada com servidores estáticos e os clientes com locações estáticas e o tráfego entre estes clientes e servidores era algo bem previsível. Hoje em dia, devido ao desenvolvimento da rede de computadores e da forma de utilizá-la, o tráfego se tornou muito mais complexo e dinâmico entre empresas, *data centers*, usuários e provedoras. Isso inclui (STALLINGS, 2015): Aplicações clientes e servidores criando um tráfego “horizontal” entre eles e os bancos de dados; A conversão e aumento de tráfego de dados, voz e vídeo tem deixado o fluxo de dados quase que imprevisível; O aumento da utilização de computação na nuvem tirou o tráfego que antes era interno das redes corporativas e o jogou na WAN.

2 REDE DE COMPUTADORES

Antes de falar de Redes de Computadores, é importante comentar um pouco sobre o conceito de comunicação de maneira geral. O dicionário da língua portuguesa a define como processo de emitir, transmitir e receber mensagens por meio de métodos e/ou processos convencionados (DICIONÁRIO AURÉLIO DIGITAL, 2019). Sendo assim, coloca-se foco em como a ação é realizada, podendo-se entender esses métodos convencionados como sendo qualquer mecanismo que se use para transmitir uma mensagem ou informação. A linguagem escrita, falada ou sinais gestuais produzidos com a mão podem ser exemplos disso. Exemplos mais sutis também podem ser apresentados, como o ato de piscar os olhos, que pode ser usado para comunicação e para isso basta apenas que todos os indivíduos envolvidos convencionem qual é o significado desse gesto, o mesmo vale para qualquer outro método mencionado anteriormente.

Tanenbaum (2011) define redes de computadores como um conjunto de computadores autônomos conectados por uma única tecnologia. Computadores só estão conectados quando podem trocar informações entre si. Considerando a definição acima, identifica-se os mesmos elementos presentes na definição do termo comunicação, onde os indivíduos que querem trocar informações são os sistemas autônomos e o método convencionado entre eles para a troca de mensagens é a tecnologia única, acessível a todos os envolvidos.

2.1 Arquitetura de Redes

Arquitetura de redes é o design de uma rede de computadores. É uma estrutura para especificações de componentes físicos de uma rede e toda a sua configuração funcional, bem como os protocolos utilizados para comunicação

Existem dois tipos de conexões entre redes e a partir da combinação delas surgem as demais topologias: (REDE NACIONAL DE ENSINO E PESQUISA, 2015)

- Conexão Ponto-a-Ponto - O tipo mais simples de conexão de redes, os equipamentos são conectados entre si por uma única linha de

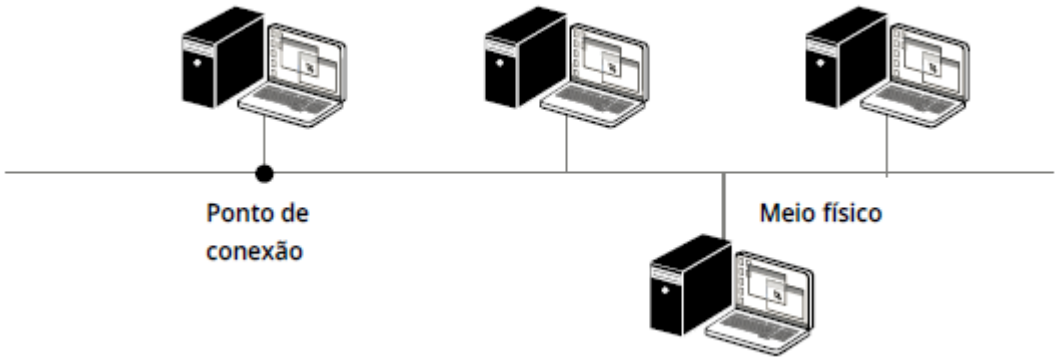
comunicação, quando algum deles tiver algo a transmitir a linha estará disponível, como apresenta a Figura 1.

Figura 1 - Exemplo de conexão ponto-a-ponto.

Fonte: RNP - Arquitetura e Protocolos de Rede TCP-IP (2015)

- Conexão Multiponto - Este tipo de conexão permite que todas as estações se comuniquem entre si diretamente, e não apresenta os problemas de escalabilidade da conexão ponto-a-ponto. Existe apenas um único meio de comunicação interligando todas as estações, através de muitos pontos de conexão, um para cada estação, como mostra a Figura 2.

Figura 2 - Exemplo de conexão Multiponto



Fonte: RNP - Arquitetura e Protocolos de Rede TCP-IP (2015)

As topologias clássicas são tipos de redes que usam das características dos dois tipos básicos citados acima.

2.1.1 Topologia

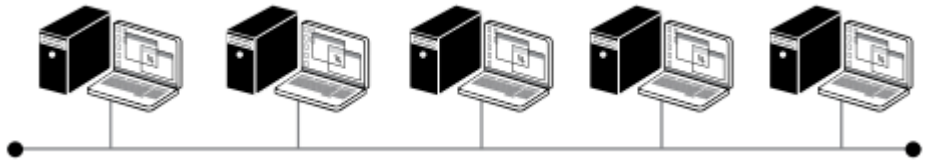
Topologia é a forma de ligação dos equipamentos em uma rede. A topologia se refere ao nível físico dessa conexão, sendo dependente do projeto e suas funções.

Ao planejar uma rede, muitos fatores devem ser considerados e um dos mais importantes é o tipo de participação dos nós.

Existem vários tipos de topologias, mas todas elas são derivadas de três tipos principais, sendo elas: (REDE NACIONAL DE ENSINO E PESQUISA, 2015)

- Topologia Barramento - Nessa topologia, todos os nós (estações) se conectam no mesmo meio de transmissão, geralmente compartilhada em tempo e frequência e o tráfego é bidirecional. A topologia é uma simples aplicação do tipo básico multiponto, utilizando normalmente cabo coaxial. Na topologia barramento a falha de uma única estação não causa a parada total do sistema, no entanto uma falha no barramento pode ocasionar esse problema. O tempo de resposta é totalmente dependente do protocolo de acesso utilizado. A Topologia Barramento é representada na Figura 3.

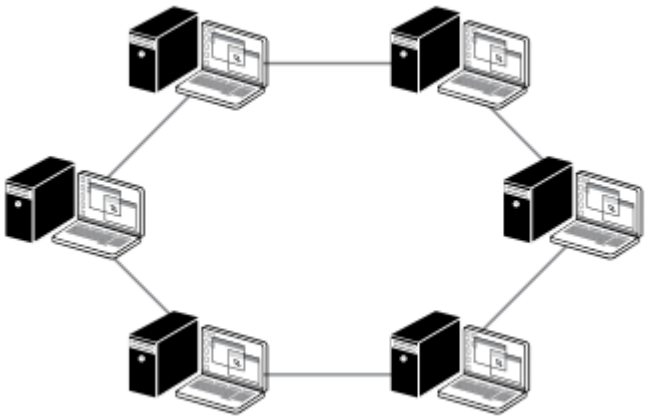
Figura 3 - Exemplo de Topologia Barramento.



Fonte: RNP - Arquitetura e Protocolos de Rede TCP-IP (2015)

- Topologia Anel - A topologia anel consiste em estações conectadas em um caminho fechado. Redes Anel são capazes de transmitir e receber informações de qualquer direção porem o mais utilizado é unidirecional, tornando menos sofisticados os protocolos que asseguram a entrega da mensagem corretamente e em sequência. A topologia nada mais é do que uma sucessão de conexões ponto-a-ponto entre estações formando um anel, acarretando uma rede com baixa tolerância a falha e erros de transmissão ainda podem fazer com que uma mensagem fique circulando o anel por longo tempo. A Topologia Anel é representada na Figura 4.

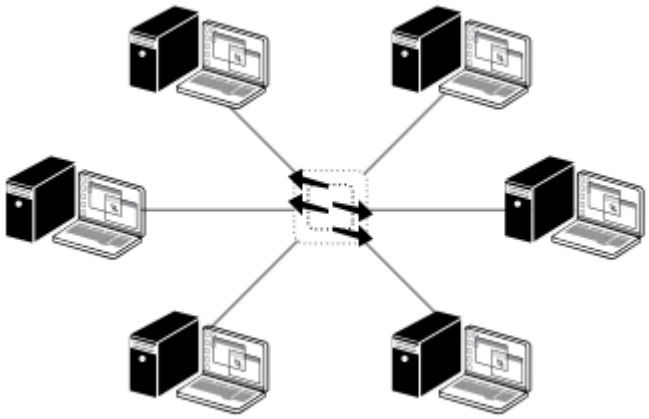
Figura 4 - Exemplo de Topologia Anel.



Fonte: RNP - Arquitetura e Protocolos de Rede TCP-IP (2015)

- Topologia Estrela - Na topologia estrela, todos usuários se comunicam em um nó central, também utilizando a conexão ponto-a-ponto e, através dele os usuários podem transmitir mensagens entre si. Essa topologia é a melhor escolha em situações onde o nó central está restrito a funções de comutação, porem ele pode fazer mais do que isso, por exemplo, pode atuar como conversor em caso dos envolvidos na comunicação usem protocolos diferentes ou estejam em redes distintas. Em caso de falha no nó central toda a rede estará comprometida, mas isso pode ser evitado utilizando nós redundantes na rede, porem isso acarretara em aumento considerável dos custos. O desempenho da rede está diretamente ligado a quantidade de tempo que o nó central leva para processar as mensagens. A Topologia Estrela é representada na **Erro! Fonte de referência não encontrada.**.

Figura 5 - Exemplo de Topologia Estrela



Fonte: RNP - Arquitetura e Protocolos de Rede TCP-IP (2015)

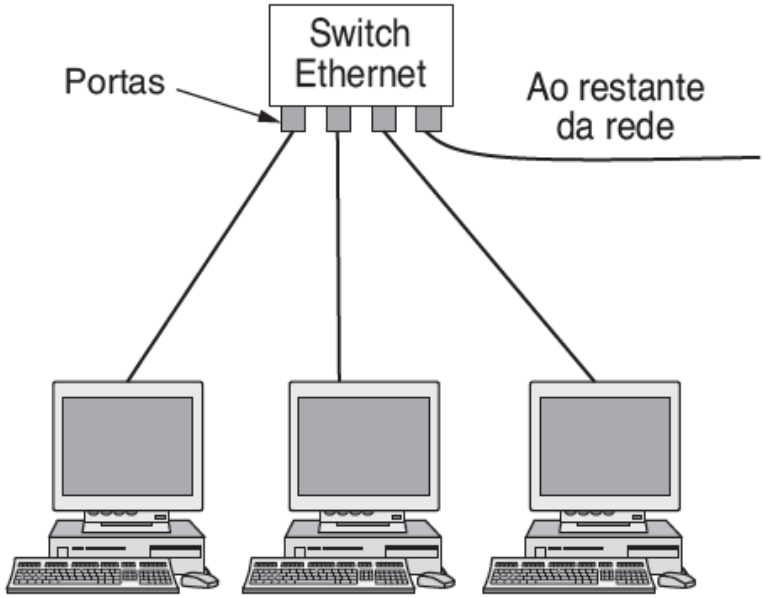
2.1.2 Redes definidas por área geográfica

Uma rede pode ser definida por um ou mais critérios, no entanto, olhando de uma forma mais abrangente além das topologias citadas no capítulo anterior, a classificação mais comum é feita por área geográfica ou organizacional. Nesse caso entra os vários termos LAN, MAN, WAN, PAN, WLAN etc. Porém, as mais comuns e mais usadas são: (TANENBAUM 2011)

- LAN – *Local Area Networks* – Redes privadas, com a cobertura restrita a prédios ou campus não maiores que alguns quilômetros, elas são amplamente usadas para a interconexão de computadores pessoais em empresas e residências. A principal tecnologia de transmissão utilizada nessas redes são as variações dos protocolos Ethernet. Um exemplo de rede LAN pode ser visto na

- **Figura 6**.

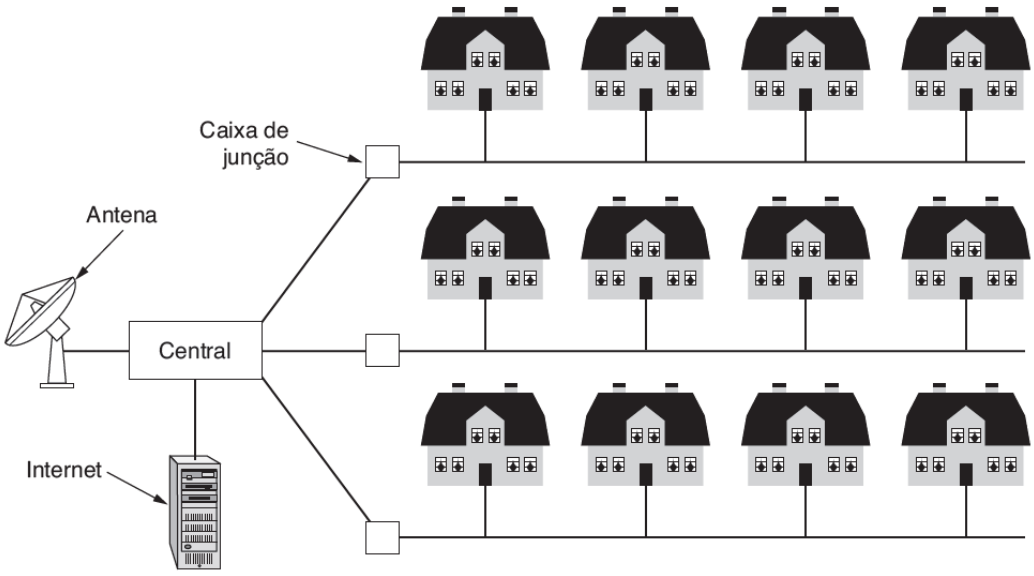
Figura 6 - Exemplo de uma rede LAN.



Fonte: ANDREW S. TANENBAUM – Redes de Computadores (2011)

- MAN – *Metropolitan Area Networks* – Basicamente são versões maiores de LANs, uma rede que abrange uma cidade. O exemplo mais conhecido de MANs é a rede de TV a cabo de uma cidade ou a interligação de escritórios em uma região específica. Um exemplo de Rede MAN pode ser visto na Figura 7.

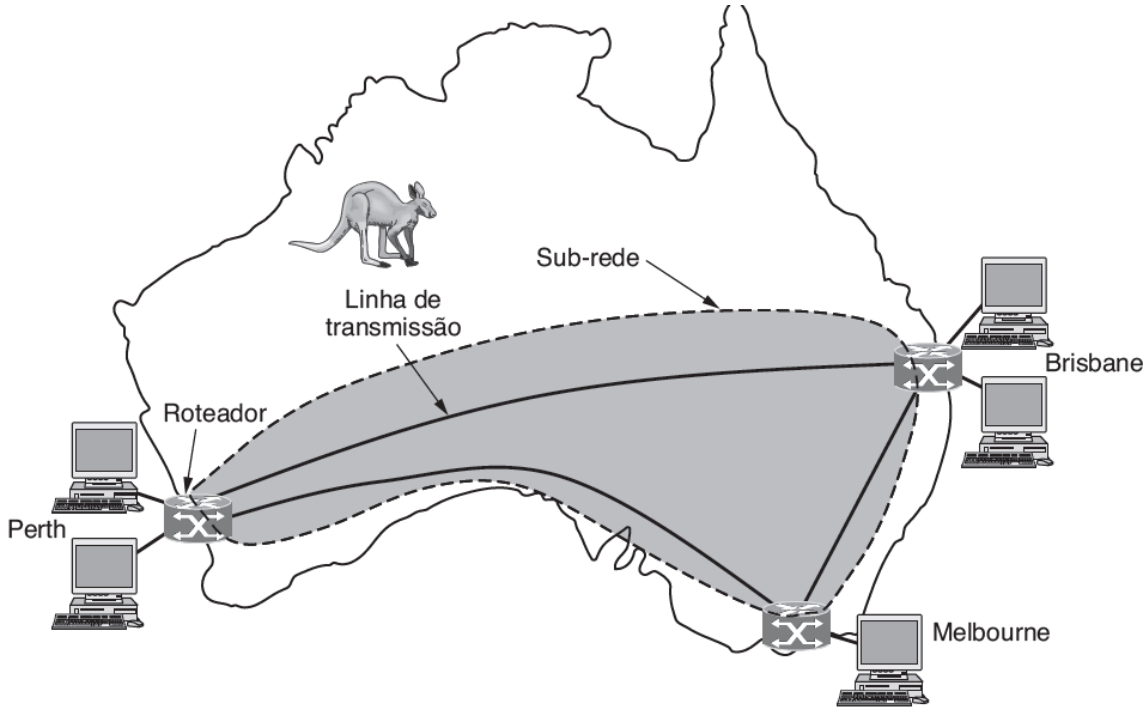
Figura 7 - Exemplo de uma rede MAN.



Fonte: ANDREW S. TANENBAUM – Redes de Computadores (2011)

- WAN – *Wide Area Neworks* – Redes de ampla cobertura geográfica, interligando países ou até continentes inteiros, essas redes são operadas por empresas prestadoras de serviços de telecomunicações e empregam as mais diversas tecnologias, ATM, Frame Relay, MPLS, MetroEthernet, etc. Um exemplo de uma rede WAN pode ser visto na Figura 8.

Figura 8 - Exemplo de uma rede WAN



Fonte: ANDREW S. TANENBAUM – Redes de Computadores (2011)

2.2 Arquitetura de Protocolos

Protocolo é um conjunto de regras que controla as máquinas e seus processos, como se fossem regras de conduta e comportamento. Os protocolos são estruturados e divididos em camadas, de forma a dividir e organizar suas funções. De modo geral, as camadas superiores obtêm informações e serviços das camadas inferiores.

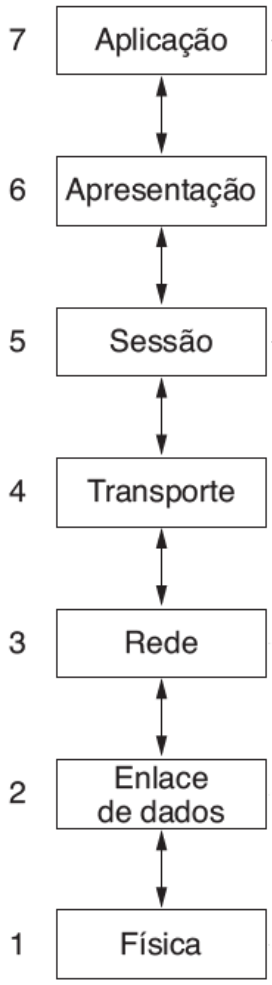
O principal objetivo da arquitetura em camadas é estruturar o *hardware* e o *software* de uma melhor forma, para isso acontecer as camadas são feitas de forma hierárquica e cada uma com uma função bem definida que é construída usando as informações das camadas inferiores. Além disso, o modelo estruturado em camadas

reduz a complexidade dos protocolos, simplificam o ensino e aprendizado dos usuários de redes e permite a interoperabilidade de tecnologias utilizadas nas diversas camadas do modelo.

2.2.1 Modelo de referência OSI

O modelo se baseia na proposta desenvolvida pela ISO (*International Standards Organization*) como o primeiro passo a direção a padronização internacional dos protocolos usados em várias camadas. Chama-se Modelo de Referência ISO OSI (*Open System Interconnection*), pois se trata de interconexão de sistemas abertos à comunicação com outros sistemas. Na Figura 9 pode-se ver a ordem das camadas do Modelo OSI

Figura 9 - Modelo de referência OSI



Fonte: ANDREW S. TANENBAUM – Redes de Computadores (2011)

De acordo com Tanenbaum (2011) os princípios utilizados para chegar ao modelo de sete camadas foram:

- Uma camada deve ser criada onde houver necessidade de abstração.
- Cada camada deve executar uma ação bem definida.
- A função de cada camada deve ser definida em função dos protocolos padronizados internacionalmente.
- O limite de camada deve ser escolhido para minimizar o fluxo de informações entre elas.
- O número de camadas deve ser grande o bastante para uma camada não ter funções distintas, mas também deve ser pequeno o suficiente para que a arquitetura não se torne difícil de controlar.

Deve ser lembrado que o Modelo OSI não foi feito como arquitetura de rede, como dito por Tanenbaum (2011), pois ele não especifica os serviços e protocolos exatos que devem ser usados em cada camada, ele apenas informa o que deve ser feito.

As sete camadas de baixo para cima:(Tanenbaum, 2011)

- Camada Física - A camada física trata da transmissão de bits normais por um canal de comunicação. Deve ser garantido que quando um lado enviar bit 1, o outro lado receberá bit 1 e não 0. O projeto lida em grande parte com interfaces mecânicas, elétricas e sincronização, também com o meio físico de transmissão que se situa abaixo da camada física.
- Camada de Enlace de Dados - A principal função da camada de enlace de dados é transformar o canal de transmissão em uma linha que pareça livre de erros de transmissão. Isso é feito fazendo o transmissor dividir os dados em quadros e transmitindo os sequencialmente. Se o serviço for confiável, o receptor confirmara a recepção correta de cada quadro enviando de volta um quadro de confirmação.
- Camada de Rede - A camada de rede controla as operações da sub-rede. É fundamental ser determinado a maneira como os pacotes são roteados da origem até o destino (rotas estáticas ou dinâmicas). Se houver muitos pacotes na sub-rede ao mesmo tempo, eles dividirão o mesmo caminho, formando gargalos. A responsabilidade pelo controle deste congestionamento também pertence a camada de rede, em

conjunto as camadas mais altas. De modo geral, a qualidade do serviço fornecido (atraso, tempo em trânsito, instabilidade etc.) também é uma questão da camada de rede.

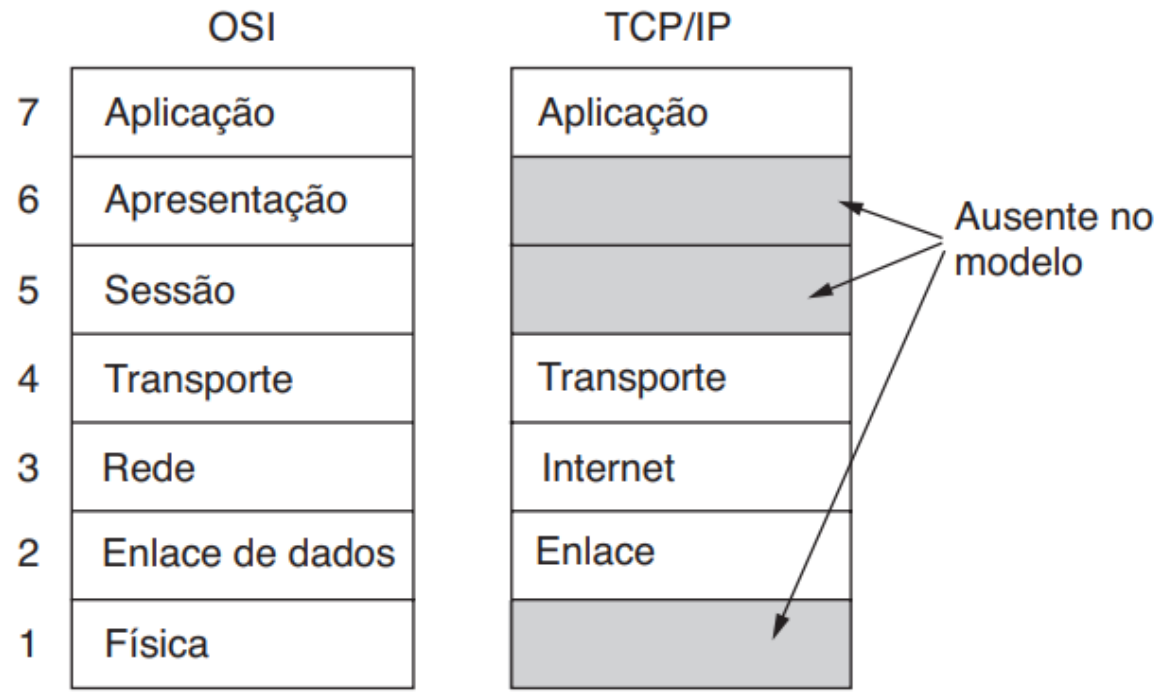
- Camada de Transporte - A função básica da camada de transporte é aceitar dados da camada acima, dividir em unidades menores e passar para a camada de rede e garantir a chegada na outra extremidade. Além disso deve ser feito de forma que as camadas superiores fiquem isoladas das mudanças de tecnologia de hardware com o passar do tempo. A camada de transporte também determina o tipo de serviço fornecido a camada de sessão.
- Camada de Sessão - A camada de sessão permite que os usuários estabeleçam sessões de comunicação entre eles, mantendo controle de quem deve transmitir em cada momento. Uma sessão oferece diversos serviços como controle de diálogo, gerenciamento de tokens e a sincronização.
- Camada de Apresentação - A apresentação está relacionada a sintaxe e semântica das informações transmitidas, para tornar possível a comunicação entre computadores com diferentes representações internas dos dados. A camada de apresentação gerencia essas estruturas de dados e permite o intercâmbio de dados de nível mais alto (por exemplo, registros bancários).
- Camada de Aplicação - Camada de aplicação contém uma série de protocolos necessário para os usuários, como por exemplo o HTTP (*Hyper Text Transfer Protocol*) que constitui a base da Word Wide Web. Outros protocolos de aplicação são usados para transferência de arquivos, correio eletrônico e transmissão de notícias pela rede.

2.2.2 TCP/IP

De acordo com Tanenbaum (2011) com o surgimento de redes de rádio e satélite, os protocolos já existentes começaram a ter problemas de interligação com elas, o que forçou a criação de uma nova arquitetura de referências. O modelo foi definido pela primeira vez em Cerf e Kahn (1974), depois melhorado e definido como padrão na comunidade da internet. A filosofia de projeto que o modelo se baseia é

discutida em Clark (1988), basicamente o Departamento de Defesa se preocupava em manter as conexões intactas enquanto máquinas de origem e destino estivessem funcionando mesmo que algo no de transmissão deixasse de operar repentinamente. Além disse era necessária uma arquitetura flexível para as aplicações com diversos requisitos diferentes, desde transferência de arquivos e a transmissão de dados de voz em tempo real. Na Figura 10 pode-se ver a diferença entre camadas do modelo OSI e TCP/IP.

Figura 10 - Diferenças do Modelo OSI e TCP/IP



Fonte: ANDREW S. TANENBAUM – Redes de Computadores (2011)

As quatro camadas de baixo para cima: (Tanenbaum, 2011)

- A Camada de Enlace - A camada de enlace descreve que os enlaces gerais como linhas seriais e Ethernet precisam cumprir os requisitos dessa camada de interconexão com serviço não orientado a conexões. Ela não é exatamente uma camada propriamente dita, mas uma interface entre os hosts e os enlaces de transmissão.
- A Camada de Internet (Camada de Rede) - Sua tarefa é permitir que *hosts* injetem pacotes em qualquer rede e garantir a entrega destes pacotes. A camada define um formato de pacote oficial e um protocolo chamado IP (*Internet Protocol*) mais um protocolo que o acompanha, chamado ICMP

(*Internet Control Message Protocol*). O roteamento de pacotes claramente é uma questão muito importante para essa camada, assim como o congestionamento.

- A Camada de Transporte - A finalidade dessa camada é permitir que as entidades pares dos hosts de origem e de destino mantenham uma conversação, exatamente como acontece na camada de transporte OSI. Dois protocolos de ponta a ponta foram definidos nesta camada, o primeiro é o TCP (*Transmission Control Protocol*), é um protocolo orientado a conexões confiável que permite a entrega dos pacotes sem erros. O segundo protocolo é o UDP (*User Datagram Protocol*), é um protocolo sem conexões, não confiável. Ele é utilizado para aplicações onde a entrega imediata é mais importante do que a entrega precisa, como voz e vídeo por exemplo.
- A Camada de Aplicação - TCP/IP não necessita de camadas de sessão ou apresentação já que são poucos usados na maioria das aplicações. A camada de aplicação do modelo TCP/IP engloba todas as funções de sessão e apresentação, ela também contém todos os protocolos de nível mais alto. Dentre eles estão o protocolo de terminal virtual (TELNET), transferência de arquivos (FTP) e de correio eletrônico (SMTP) além de muitos outros.

Ambos os modelos OSI e TCP/IP tem muito em comum, ambos se baseiam no mesmo conceito de uma pilha de protocolos independentes. Além disso, as camadas tem praticamente as mesmas funcionalidades.

2.3 Arquitetura Atual

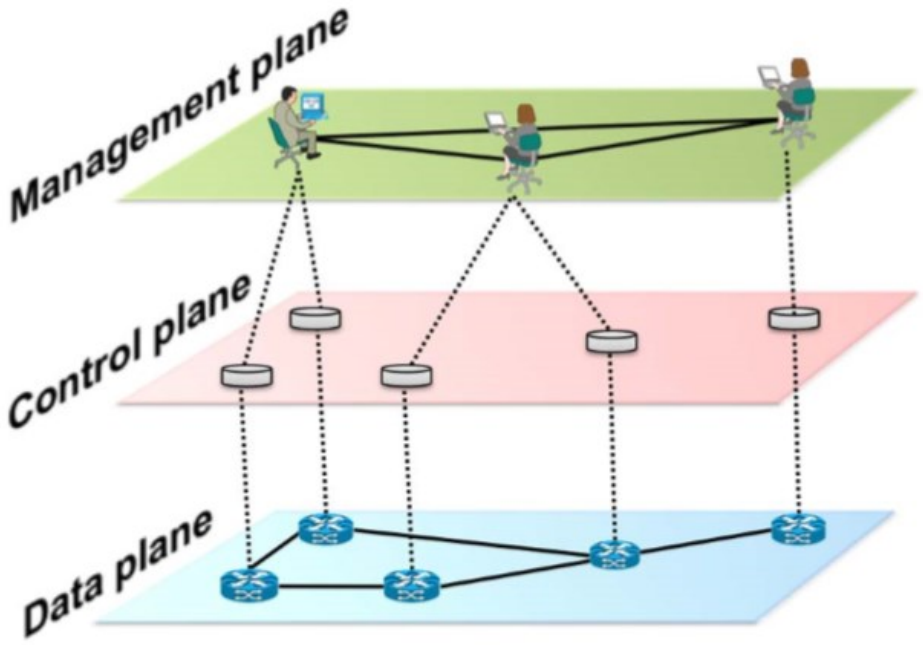
Redes de computadores podem ser divididas em tipos de funcionalidade: *Data Plane*, *Control Plane* e *Management Plane*. As funções de cada um destes planos são: (FELIPPETTI, 2019)

- *Data Plane*: Responsável por enviar, eficientemente, os pacotes e quadros pela rede.
- *Control Plane*: Responsável pelos protocolos de roteamento, popular as tabelas que serão utilizadas no *Data Plane*.

- *Management Plane*: Qualquer protocolo que esteja relacionado com gerenciamento remoto e configuração dos equipamentos como Telnet, SSH, SNMP etc.

Basicamente, as políticas da rede são criadas no *management plane*, o *control plane* as impõe e por último o *data plane* executa elas quando for encaminhar os dados pela rede. A Figura 11 - Camadas de funcionalidade da redeapresenta uma ilustração das camadas.

Figura 11 - Camadas de funcionalidade da rede



Fonte: Kreutz - Software-Defined Networking: A Comprehensive Survey (2015)

Nas redes tradicionais, o *control plane* e *data plane* são acoplados nos equipamentos. Por muito tempo, essa foi a melhor opção para a arquitetura das redes de computadores, já que dessa forma se garantia a maior resiliência possível, o que era de extrema importância.

Entretanto, o resultado era uma arquitetura extremamente complexa e estática e um dos principais motivos de redes tradicionais serem rígidas e difíceis de gerenciar. Erros de configurações e erros relacionados a isso são extremamente comuns hoje em dia. De acordo com Feamster e Balakrishnan (2005), mais de 1000 erros de BGP (*Border Gateway Protocol*) foram encontrados na internet, e cada um destes

equipamentos mal configurados podem resultar em vários comportamentos não desejados na rede global incluindo perda de pacote, *loop* de rede, lentidão e violação de contrato entre outros.

Além disso ainda existe o problema com as fornecedoras de *hardware*, devido aos equipamentos possuírem o *control plane* acoplado internamente, cada fornecedor possui suas próprias sintaxes de comandos e formas de configurar seus equipamentos, o que acaba fazendo com que o engenheiro de redes tenha que conhecer e gerenciar diversos equipamentos de forma diferente e muitas vezes não compatíveis com outros.

3 GERENCIAMENTO DE REDES

Assim como em uma empresa é necessário existir um gestor que conheça seus funcionários e entenda bem cada funcionalidade e relação entre eles, em redes de computadores é necessário ter conhecimento dos equipamentos, como eles se interconectam e suas funções para que a rede possa funcionar na melhor forma possível e suas falhas possam ser rapidamente identificadas e restauradas.

Neste capítulo vamos falar sobre o monitoramento de redes, alguns pontos importantes para que ele possa ser bem feito e até mesmo o protocolo mais utilizado.

3.1 Importância e Necessidade

O crescimento contínuo de componentes de redes tem tornado a atividade de gerenciamento cada vez mais complexa e necessária. As coisas ficam ainda piores com o número maior de fornecedores destes equipamentos, pois cada um tem suas particularidades. Uma falha de rede, por menor que seja, tem chances de causar um impacto na receita de uma empresa e até mesmo a impossibilidade de prestação de serviços, causando transtornos financeiros e consequências bastantes serias podendo até se tornar implicações de cunho legal.

O isolamento e o teste dos problemas das redes tornam-se mais difíceis devido a diversidade e níveis de pessoal envolvido, variação nas formas de monitoração usada pelos fornecedores e até mesmo protocolos utilizados.

Aqui temos alguns dos motivos que tornam Monitoramento importante e necessário: (REDE NACIONAL DE ENSINO E PESQUISA, 2015)

- Crescimento vertiginoso das LANs e WANs.
- Mais aplicações e usuários gerando complexidade: equipamentos*, hardware* e *software* heterogêneos; empresas dependentes das redes para elevar eficiência e lucros.
- Necessidade de gerenciamento visando a coordenação (controle de atividades e monitoração do uso) de recursos materiais (modems, roteadores, enlaces físicos etc.) e lógicos (protocolos, configurações etc.), fisicamente distribuídos na rede, assegurando, na medida do possível, confiabilidade e performance aceitáveis e segurança das informações.

Em vista desses fatores, o desafio de manter custos sob controle, treinar novamente a equipe, reter a equipe e recrutar novos profissionais é constante.

3.2 Atuação do Gerente de Redes

A atividade de gerenciamento de rede é usualmente exercida por um grupo de pessoas que inclui, no mínimo, um operador de rede e um administrador de rede. (REDE NACIONAL DE ENSINO E PESQUISA, 2015)

Normalmente, o operador controlador da rede realiza a contínua monitoração da rede a partir de uma estação onde são exibidos os dados sobre a situação da rede e de seus componentes.

O Gerenciamento visa ter controle e poder agir em função de informações coletadas que mostram situações determinadas. Por exemplo: Um *link* de dados pode apresentar atraso ou perda de pacotes; uma ação possível seria rotear o tráfego para outro *link*. Gerenciamento de redes de computadores é uma das áreas mais complexas quando falamos de T.I (Tecnologia da Informação), contratos de prestação de serviços de T.I estão cada vez mais criteriosos e com SLAs (*Service Level Agreement*) cada vez mais apertadas. Por isso é importante identificar todos os ativos de rede, monitorá-los, coletar informações relevantes e exibi-las das formas mais compreensíveis possível para que possam ser analisadas na medida em que são recebidas e que anomalias sejam fáceis de serem detectadas. Esses procedimentos visam facilitar a identificação e solução dos problemas de maneira rápida e eficaz.

Dentro das atividades comuns de gerenciamento de redes, as principais são monitoramento e controle (REDE NACIONAL DE ENSINO E PESQUISA, 2015). Para o monitoramento gerenciamento de redes, pode-se utilizar a própria infraestrutura existente para alcançar os elementos ou pontos definidos da rede. Outra opção seria montar uma rede paralela a rede existente, que tivesse intersecções nos pontos de interesse.

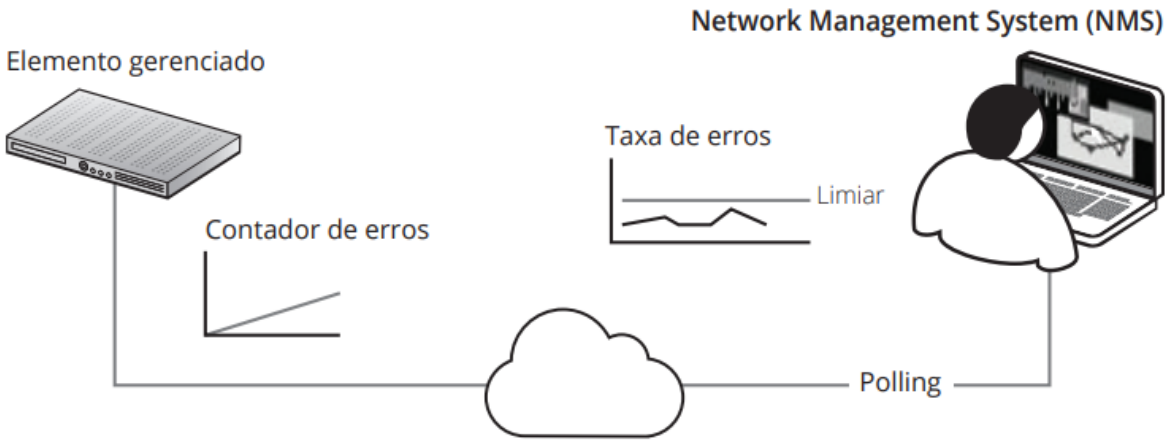
A situação atual das redes é que os equipamentos nela utilizados tem condição de prover uma grande quantidade de informações sobre seu próprio funcionamento, adicionando isso com fato dos *softwares* também serem estruturados utilizando a mesma estratégia (gerar informações sobre o próprio funcionamento) a quantidade e diversidade de informações sobre o funcionamento das redes cresce continuamente ocasionando mais dificuldades na determinação de problemas. Portanto existe a

necessidade de reconhecer, manipular e tratar todas estas informações, de forma a permitir o diagnóstico o mais rápido e preciso possível. A atividade de gerenciamento de rede envolve uma gama de atividades, tais como: (REDE NACIONAL DE ENSINO E PESQUISA, 2015)

- Registrar a ocorrência de eventos;
- Estabelecer critérios para o disparo de alarmes;
- Detectar e diagnosticar a ocorrência de falhas;
- Conhecer e controlar alterações nos equipamentos;
- Acompanhar o desempenho da rede e dos serviços de rede;
- Garantir a segurança;
- Contabilizar recursos;
- Verificar Acordo de Nível de Serviço (ANS) estipulado no contrato.

A Figura 12 ilustra uma situação típica nesse contexto.

Figura 12 - Visão geral do gerenciamento de redes



Fonte: RNP - Gerenciamento de Redes de Computadores (2015)

3.3 Protocolo SNMP

O SNMP (*Simple Network Management Protocol*) é um dos protocolos mais utilizados para auxiliar no gerenciamento de redes. Nesta parte do capítulo será apresentada uma breve introdução ao protocolo, citando suas funções, versões e suas operações.

3.3.1 O que é SNMP

Devido à complexidade das redes, como já dito no capítulo anterior, pode parecer assustador gerenciar todos os equipamentos de redes e ter certeza que eles não só estão funcionando, mas também trabalhando da maneira mais otimizada possível. Este é o ponto onde o protocolo SNMP nos ajuda. Criado em 1998, o protocolo SNMP fornece aos seus usuários um set de operações que permite esses equipamentos a serem gerenciados remotamente. (MAURO 2005)

A ponto principal do SNMP é o set de operações simples que permite ao administrador a possibilidade de mudar o estado de equipamentos compatíveis com o protocolo, por exemplo, é possível derrubar uma interface de um roteador ou verificar a velocidade que ela está operando sem precisar estar conectado fisicamente a ele. SNMP pode até mesmo monitorar temperatura e velocidade de rotação das ventoinhas e nos avisar se algo está fora do padrão definido.

SNMP geralmente está associado com o gerenciamento de Roteadores, porém ele foi desenvolvido para monitorar muitos tipos de equipamentos, alguns deles são: (O'Reilly 2005)

- Sistemas Linux
- Sistemas Windows
- Impressoras
- Modems
- Fontes de energia

Qualquer equipamento que tenha compatibilidade com o *software* pode ser monitorado e gerenciado, isso inclui não apenas equipamentos físicos, mas *softwares* como servidores e banco de dados.

3.3.2 Operações SNMP

Antes de falarmos das operações do SNMP (*Simple Network Management Protocol*), é importante definirmos que no mundo SNMP existe duas entidades: Agentes e Gerentes. (MAURO 2005)

- Gerente: O gerente é qualquer tipo de servidor rodando algum *software* que consegue lidar com as tarefas de gerenciamento de redes, muitas vezes são referenciados como NMS (*Network Management Station*). Gerentes são

responsáveis por requisitar e receber as mensagens dos agentes (roteadores, *switches*, servidores linux etc.)

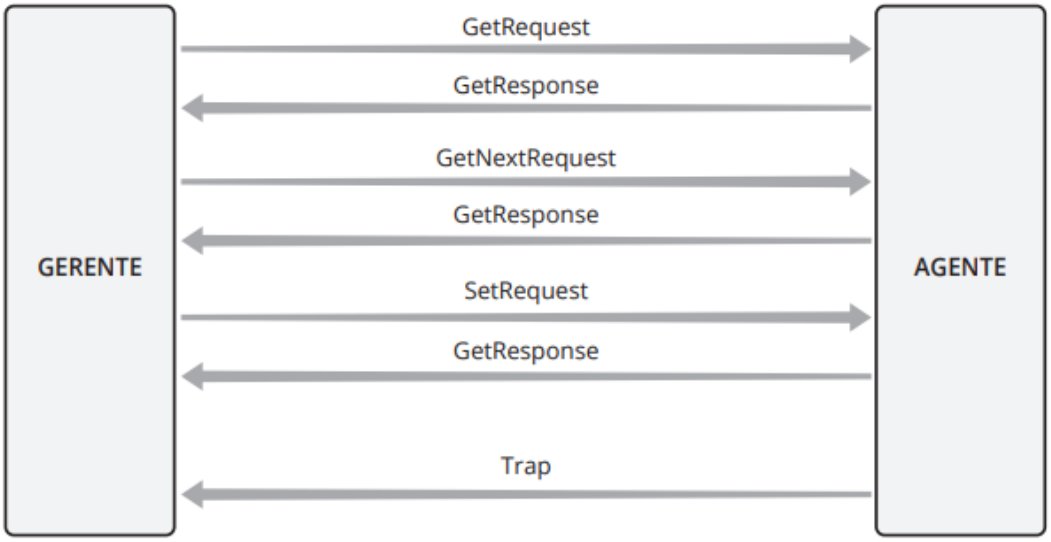
- Agente: É um *software* que roda em um equipamento gerenciável, pode ser um *software* a parte ou incorporado no Sistema Operacional. O agente provê informações para o Gerente, mantendo a monitoração de vários aspectos do equipamento, podendo mandar mensagens não solicitadas (*Trap*) quando algum problema é encontrado ou responder as requisições de informação do Gerente

O protocolo SNMP utiliza o seguinte conjunto de operações: (REDE NACIONAL DE ENSINO E PESQUISA, 2015) *GetRequest*: requisição para capturar o valor de uma variável;

- *SetRequest*: requisição de mudança de um valor de uma variável feita pelo gerente;
- *GetNextRequest*: requisição para capturar o valor da próxima variável;
- *Response*: mensagem de resposta do agente para as solicitações de Get e Set;
- *Trap*: notificação do agente ao gerente, comunicando o acontecimento de um evento predeterminado.

Estas mensagens são encapsuladas pelo protocolo UDP (*User Datagram Protocol*) e transportada através do protocolo IP. Através do uso delas, a estação de gerenciamento da rede pede informações para os agentes SNMP, altera os valores dos objetos gerenciados no agente e obtém respostas para estes comandos. Além disso, os agentes SNMP podem gerar mensagens de *Trap* quando alguma anomalia for notada no equipamento. A Figura 13 exemplifica a relação entre Gerente e Agente.

Figura 13 - Relação entre Gerente e Agente



Fonte: RNP - Gerenciamento de Redes de Computadores (2015)

3.3.3 Versões do Protocolo SNMP

O IETF (Internet *Engineering Task Force*) é a responsável por definir os padrões dos protocolos da internet, incluindo o SNMP. O IETF publica a RFCs (*Request for Comments*), que são as especificações destes protocolos. (MAURO 2005).

O protocolo SNMP foi inicialmente definido pelo RFC 1067 em 1988, mas sofreu uma evolução e a versão 2 foi publicada na RFC 1442 em 1993. Apesar do mecanismo de segurança ser melhorado na segunda versão, o mecanismo de criptografia das mensagens ainda não havia sido implementado, e foi somente na versão 3, definida pela RFC 1861 e publicada em 1995 que criptografia e autenticação foram implementadas. A Figura 14 mostra as diferenças de segurança entre as versões.

Figura 14 - Diferenças entre versões do SNMP

Versão	Nível	Autenticação	Criptografia	O que acontece?
SNMPv1	noAuthNoPriv			Usa o texto *community* para autenticar
SNMPv2c	noAuthNoPriv			Usa o texto *community* para autenticar
SNMPv3	noAuthNoPriv	Username		Usa o *username community* para autenticar
	authNoPriv	MD5ou SHA		Usa os algoritmos de autenticação - HMAC-MD5 e HMAC-SHA
	authPriv	MD5ou SHA	DES	Usa criptografia 56-bit DES

Fonte: RNP - Gerenciamento de Redes de Computadores (2015)

4 SDN (SOFTWARE DEFINED NETWORK)

Os protocolos de roteamento e de transporte dentro dos roteadores e dos *switches* são as chaves que permitem a informação ser transmitida ao redor do mundo. Apesar de extremamente utilizados, redes tradicionais são complicadas e muito difíceis de gerenciar, cada *device* deve ser configurado individualmente utilizando comandos de baixo nível e muitas vezes exclusivos para cada fornecedor específico (Juniper, Cisco, HP, etc.). Em adicional, redes tradicionais precisam lidar com falhas e se adaptar perante elas e já que reconfigurações automáticas e mecanismo de respostas para essas falhas são quase que não existentes, reforçando o requerimento de mais configurações e políticas nos equipamentos.

SDN (*Software Defined Network*) é o que dá esperança de mudar as limitações impostas pelas redes convencionais e neste capítulo será abordado como gerar isso e quais as vantagens de utilizá-la.

4.1 O que é SDN?

SDN originalmente refere-se a uma arquitetura de redes onde a *data plane* e o *control plane* são separados, mas com o passar do tempo a indústria da rede de computadores em muitas ocasiões mudaram a visão original de SDN referindo-a tudo aquilo que tenha *software* envolvido.

Kreutz (2015) junto de outros engenheiros da IEEE (*Institute of Electrical and Electronics Engineers*) definiram SDN como uma arquitetura de redes com quatro pilares principais:

- *Control plane* é retirado dos equipamentos de redes, deixando-os apenas como um dispositivo de encaminhamento.

- As decisões para o encaminhamento destes pacotes são feitas com base em fluxo invés de IP de destino. No contexto de SDN, um fluxo é a sequência de pacotes entre origem e destino, todos pacotes de um mesmo fluxo receberá as mesmas políticas no momento do encaminhamento. O tratamento de tráfego por fluxo permite identificar e unificar o comportamento de diferentes tipos de

equipamentos e a programação por fluxo permite uma flexibilidade maior do que a forma atual de encaminhamento.

O *control plane* é movido para uma entidade externa, chamada de controladora SDN ou NOS (NOS é uma plataforma que provê todos os recursos necessários para facilitar a programação dos dispositivos de encaminhamento baseado em uma lógica centralizada)

- A rede é programável a partir de aplicações que rodam em cima do NOS que interage diretamente com os dispositivos de encaminhamento. Esta é a característica fundamental da SDN, considerada o seu propósito principal

A centralização lógica do *control plane*, em particular, já oferece diversos benefícios, tais como: Menor probabilidade de erros ao modificar as políticas da rede através de linguagens de alto nível e *softwares*; Um programa de controle pode reagir a mudanças da rede e manter as políticas intactas; A centralização de *control plane* facilita o desenvolvimento de funções mais sofisticadas, serviços e aplicações.

Como mencionado previamente, manter o *control plane* e *data plane* acoplados acabava causando muita rigidez na arquitetura, era extremamente difícil criar e implementar novas funcionalidades já que teria de ser modificado o *control plane* não só de um, mas de todos equipamentos de redes quais as implementações fizessem parte, além disso seria necessário possíveis atualizações de *firmware* e até mesmo de *hardware*. Consequentemente, desacoplar a *data plane* do *control plane* trouxe diversas vantagens, como: (KREUTZ, 2015)

- Facilita a criação de novas aplicações e funcionalidades já que o *control plane* é centralizado e a mesma linguagem de programação pode ser compartilhada entre diversas fornecedoras

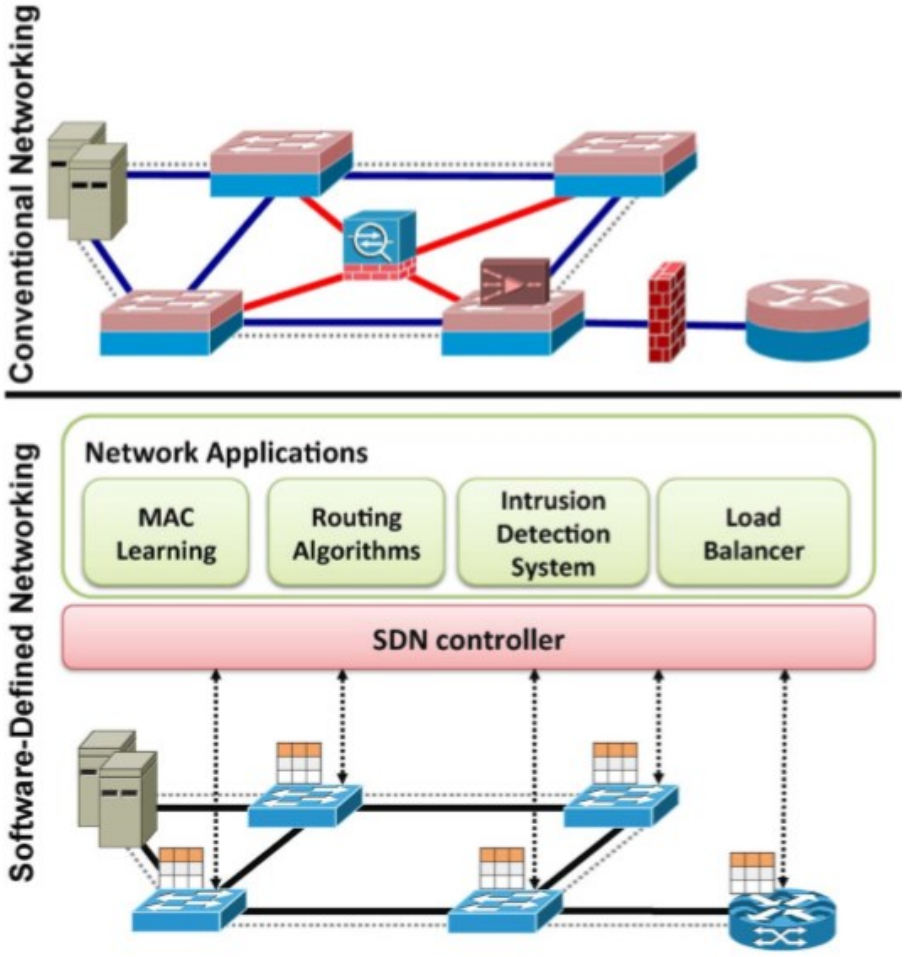
- Todas as aplicações utilizarão as mesmas informações da rede como um todo, podendo tomar decisões mais consistentes e eficientes.

- Estas aplicações poderão tomar ações em qualquer ponto da rede, não haverá necessidade de criar uma estratégia precisa em pontos específicos da rede.

- Integração de diferentes aplicações se tornam mais simples e diretas.

Na Figura 15 apresenta-se um comparativo entre redes de computadores convencionais e uma SDN (*Software Defined Network*).

Figura 15 - Comparação entre redes convencionais e SDN.



Fonte: Kreutz - Software-Defined Networking: A Comprehensive Survey (2015)

4.2 Terminologias

Para identificar elementos diferentes de SDN, será apresentado algumas Terminologias que serão usadas nos próximos capítulos com mais frequência:(KREUTZ, 2015)

- *Forwarding Devices* (FD): Já foi citado nesse trabalho como "Dispositivo de Encaminhamento". É basicamente o *hardware* ou *software* que fará a função

do *Data Plane*. os FDs tomarão as ações nos pacotes (encaminhar, descartar, reescrever algum cabeçalho, etc). Estas instruções são definidas pela *southbound interface* e são instaladas nos *forwarding devices* pela *SDN Controller.*

- *Data Plane* (DP): São conectados aos dispositivos de encaminhamento remotamente, por cabo, *wireless* ou via rádio.

- *Southbound Interface* (SI): As instruções aplicadas nos *forwarding devices* são definidas na *southbound API*, que faz parte da *southbound interface*. *Southbound interface* também define os protocolos entre os *forwarding devices* e o *control plane.*

- *Control Plane* (CP): Os *forwarding devices* são programados pelo *control plane*, toda lógica da rede fica nas aplicações e controladoras, que juntas formam o *control plan.*

- *Northbound Interface* (NI): O NOS é onde estão as API para desenvolver as aplicações. Estas API representam a *northbound interface*, apenas uma simples interface para desenvolver aplicações para rede.

- *Management Plane* (MP): o *Management plane* é o conjunto de aplicações que utilizam as funções oferecidas pelo *Northbound interface*, isto inclui aplicações como roteamento, *firewalls*, monitoração e etc. Essencialmente, *management plane* cria as políticas que serão traduzidas pela *southbound interface* e suas aplicações que programarão o comportamento dos *forwarding devices.*

4.3 Arquitetura

A Arquitetura SDN (*Software Defined Network*) possui algumas camadas importantes para o seu funcionamento e cada camada tem uma função específica e importante.

Os capítulos a seguir passarão pelas camadas mais importantes, explicando a sua função dentro da arquitetura.

4.3.1 Infraestrutura

Uma infraestrutura SDN não é muito diferente de uma rede convencional, ela também é composta por equipamentos como roteadores, *switches*, etc. A maior diferença, como já citado anteriormente, é que estes equipamentos servem apenas para encaminhar pacotes, ou seja são os FDs. Esta camada representa apenas o *Data Plane*, e toda a "inteligência" da rede foi retirada dela e estes equipamentos e centralizadas em um sistema de controle que veremos melhor mais à frente.

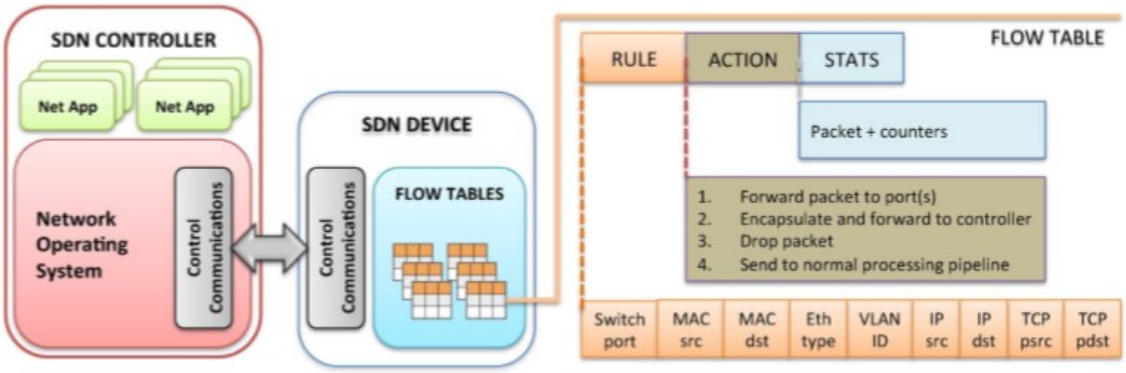
Mais importante, os FDs são implementados sob uma interface como o *OpenFlow* por exemplo, que garante a comunicação e interoperabilidade entre diferentes equipamentos com o *Control Plane*, em outras palavras, esta interface permite a programação dinâmica de diversos FDs independente de seus fabricantes, algo quase impossível de ser feito em redes de computadores tradicionais.

Na arquitetura SDN, os equipamentos do *Data Plane* são *hardwares* especializados em encaminhar pacotes enquanto os controladores são os *softwares* que rodam em uma plataforma especializada para isso. Os FDs implementados com *OpenFlow* fazem o encaminhamento de pacotes baseados em fluxo e não em destino, eles possuem tabelas de fluxos onde cada entrada dela possui 3 importantes informações: (KREUTZ, 2015)

- Regra de verificação
- Ações para ser executada nos pacotes que batem com a regra
- Contador para manter a estatísticas dos pacotes

Dentro de um equipamento *OpenFlow*, existe uma sequência de tabelas de fluxo que definem como o pacote é tratado, quando o pacote chega ele vai para a primeira tabela e vai para as seguintes até encontrar ruma regra que bata com o pacote ou passar por todas as regras. Uma regra de fluxo pode checar diferentes campos em um pacote, como mostra a Figura 16.

Figura 16 - Equipamento com OpenFlow habilitado



Fonte: Kreutz - Software-Defined Networking: A Comprehensive Survey (2015)

A sequência das regras segue a tabela de forma natural, como se fosse uma ACL (*Access Control List*) e as ações possíveis são: (KREUTZ, 2015)

- Encaminhar o pacote por uma porta de saída
- Encapsular e encaminhar para a controladora
- Descartar o pacote
- Envia-lo para o processamento normal
- Enviar para a próxima tabela de fluxo

4.3.2 Southbound Interface

Southbound interface (ou *Southbound API*) é a ponte entre a controladora e o FD, fazendo uma função muito importante na separação do *control* e *data plane*. Porém, estas APIs estão ligadas aos FDs e seus elementos físicos ou virtuais.

De acordo com McKeownetal (2008), de todas as APIs que rodam na *southbound*, *OpenFlow* é a mais aceita pela indústria, ela provê conectividade e interoperatividade entre diferentes equipamentos de diferentes fornecedoras logo se tornou a mais aceita e implementada nos padrões SDN.

O protocolo *OpenFlow* prove três fontes de informações para as controladoras (McKEOWNETAL, 2008).

- Informações baseadas em eventos que são enviados pelos FDs quando algo acontece com eles, por exemplo a queda de uma interface.

- Estatísticas de fluxo são geradas pelos FDs e enviados para a controladora.
- Pacotes são enviados dos FDs para as controladoras quando não sabem o que fazer com o fluxo que ele pertence ou caso exista uma regra explícita para enviar pacotes de determinado fluxo para a controladora.

Estes canais de informações são os meios principais de providenciar informações a nível de fluxo para as controladoras.

4.3.3 *Network Hypervisors*

Virtualização já é uma tecnologia muito consolidada em redes de computadores modernas. Baseado em Bittman (2016), mais de 80% dos servidores x86 no mundo já são virtualizados.

Hypervisors permitem que maquinas virtuais compartilhem dos mesmos recursos físicos. Em uma estrutura de *Infrastructure as a Service* (IaaS), cada usuário pode ter seus próprios recursos virtuais dentro de um armazenamento de computadores. Isso permite que recursos sejam alocados de acordo com demanda através da divisão de recursos físicos a um custo relativamente baixo, também permite que provedoras de serviços utilizem toda a capacidade de suas instalações físicas de uma forma muito mais eficiente.

Outro fato muito interessante sobre virtualização, é que um ambiente virtual pode ser facilmente migrado de uma localidade física para outra e pode ser criado ou deletado por demanda, deixando assim o serviço muito mais flexível a necessidade dos usuários.

Para que virtualização seja completa, a infraestrutura deve ser capaz de suportar topologias de redes arbitrárias e também endereçamentos diversos, os elementos físicos da rede devem ser capazes de configurar ambos, computadores e equipamentos de redes simultaneamente. Não existe em redes convencionais uma aplicação unificada que permita configurar ou reconfigurar a rede de maneira global e, como consequência disso, a virtualização de redes tradicionais para virtuais podem demorar meses para acontecer. (BITTMAN, 2016)

Existe uma esperança de que esse cenário mude com SDN e novas técnicas e tecnologias que já foram recentemente implementadas e testadas em ambientes virtuais, tais como:

Fatiando a rede*: FlowVisor* é a primeira tecnologia de virtualização de SDN. A ideia principal é permitir múltiplas redes logicas utilizar a mesma infraestrutura *OpenFlow*. Para esse propósito, ele providencia uma camada extra que torna fácil de fatiar a data plane baseado em *OpenFlow switches*, permitindo várias redes de coexistirem juntas. Atualmente cinco dimensões são consideradas pelo *FlowVision*: Banda, topologia, tráfego, CPU dos equipamentos e tabelas de encaminhamento. Também é possível que cada uma destas fatias tenha sua própria controladora e múltiplas controladoras podem coexistir dentro da mesma infraestrutura física, porém cada controladora pode agir somente na sua própria fatia da rede. (KREUTZ, 2015)

Hypervisors para *Colocation Datacenters: Colocation Datacenter* é o termo utilizado para se referenciar a um *Datacenter* onde empresas podem alugar a sua infraestrutura para uso próprio de acordo com suas necessidades. De tudo o que foi falado até agora, nada conseguiu endereçar os desafios que *Colocation Datacenter* trazem. Estes *Datacenters* tem a necessidade de migrar suas soluções para a nuvem sem que exista nenhuma modificação nas configurações de sua arquitetura física. As técnicas e tecnologias existentes hoje falham quando o assunto é a migração destes *datacenters* e de provedoras. O ambiente desse tipo de *Datacenter* deve possuir uma *hypervisor* capaz de separar os equipamentos e topologia física de acordo com a empresa que está utilizando. Mais ainda, cada uma destas empresas deve ter acesso e controle apenas aos seus próprios equipamentos virtuais e serem completamente isolado dos outros.

VMWare propôs uma plataforma de virtualização que supre todas estas necessidades de acordo com Koponen (2013). Ele permite a criação de redes virtuais independente em larga escala para ambientes de *colocation*. NVP (*Network Virtualization Plataform*) é uma solução completa de virtualização que permite a criação de redes virtuais, cada uma com seus modelos de serviços, topologia, arquitetura de endereçamento e muito mais individualmente e tudo isso dividindo o mesmo ambiente físico. Com a NVP os usuários não precisam se preocupar com o entendimento da topologia ou configurações dos FDs, ela mesmo traduz as configurações e requerimentos a um nível de instrução que possa ser instalado nos FDs. Para que isso seja possível, a plataforma usa conjuntos de controladoras SDN para manipular as tabelas de encaminhamento nas *hypervisors*, logo as decisões são todas tomadas por ela.

Até aqui, muitos dos problemas já foram endereçados, no entanto ainda existem alguns pontos a serem melhorados, como as técnicas de mapeamento de redes físicas para virtuais (GHORBANI; GODFREY, 2014). Porém, é previsto uma grande expansão de virtualizações no futuro e a tendência é que todos estes problemas sejam resolvidos.

4.3.4 *Northbound Interface*

Northbound interface e *Southbound interface* são duas partes importantes para o funcionamento da SDN. Já falamos sobre a SI em alguns capítulos atrás usando *OpenFlow* como exemplo de API mais utilizada, já na NI é um pouco mais difícil de definir algo do tipo.

A NI é como um ecossistema de softwares, diferente da SI que é mais voltada pra parte dos *hardwares*. Esse ecossistema é basicamente o responsável pela comunicação entre o *control plane* e o *management plane*, porém ainda é muito cedo para definir os *softwares* padrões desta camada, as experiências dos desenvolvedores em diferentes tipos de controladoras vão certamente encontrar uma aplicação mais adequada para isso. (KREUTZ, 2015)

Como descrito por Salisbury (2012), a maioria das controladoras possuem suas próprias NI, controladoras como *Floodlight*, Trema, NOX e *OpenDaylight* por exemplo, mas cada uma delas tem sua própria definição e suas próprias linguagens se programação, além de que as funções e comportamento do *data plane* são diferentes em cada uma delas. Eventualmente é difícil dizer que uma única NI apareça como vencedora, os requerimentos de cada aplicação são muito diferentes, APIs para segurança por exemplo são bem diferentes das voltadas para roteamento.

4.4 Pesquisas e Desafios

Nesta seção, serão evidenciados os pontos importantes que ainda precisam ser melhorados para que SDN atinja o seu potencial mais alto.

4.4.1 Arquitetura dos switches

Os *switches* baseados em *OpenFlow* existem em diferentes versões e todos eles possuem diferenças quando se trata de performance, interpretação e aderência

a protocolos específicos. Infelizmente ainda existem pontos a serem melhorados para implementar estes equipamentos em grande escala.

Capacidade da tabela de fluxo: Todas as regras de encaminhamento de pacotes de um fluxo estão guardadas nas tabelas de fluxo. Um desafio que os desenvolvedores encontram é em uma forma de criar um *switch* que tenha uma grande e eficiente tabela de fluxo para armazenar todas as regras necessárias.

A escolha mais comum para armazenar tabelas de fluxos é utilizar as TCAMs (*Ternary Content Addressable Memory*) que são um tipo especial de memória utilizada em roteadores ou *switches* para alcançar uma alta velocidade de encaminhamento de pacotes e classificação de pacotes baseada em regras escritas nas tabelas de roteamento e ACLs (Hwang e Murata, 2010). TCAM *(Ternary Content Addressable Memory)* são extremamente rápidas, podendo registrar até quinhentas mil entradas, porém elas são extremamente caras e possui um consumo de energia muito elevado e este é um dos motivos dos *switches* que utilizam *OpenFlow* utilizarem TCAM com apenas oito mil entradas, que torna desafiador o suporte de várias tabelas de fluxos em um único equipamento.

Outro estudo que está sendo feito é o de comprimir o número de regras inseridas nas TCAMs e conseguir a mesma performance. Wolfgang Braun e Michael Menth (2014) apresentam resultados significantes na utilização de *WildCards* na declaração das regras, conseguindo diminuir em até 17% o número de entradas em uma tabela de fluxo, ajudando a resolver o problema de exaustão de espaço nas tabelas.

Performance: A taxa de transferência dos *switches* comerciais (baseados em *OpenFlow*) varia de trinta e oito até mil fluxos por segundo, porém a maioria chega nem a quinhentos fluxos por segundo e isso é algo que precisará ser aprimorado conforme mais destes equipamentos começarem a ser implementados já que a necessidade de alta taxa de transferência serão mais evidentes. (KREUTZ, 2015)

Testes de implementações também tem revelado certos problemas com a CPU dos *switches* baseados nos mais comerciais, testes feitos por Kobayashi (2013) mostram que durante testes de roteamento ponto a ponto entre 2 VLANs diferentes, utilizando *links* virtuais, poderia causar picos de utilização de CPU o que pode acarretar em perda de pacotes e até mesmo queda na rede.

4.4.2 Controladoras

Quando se fala em SDN, controladora é um pilar crítico da arquitetura e é realmente importante e muito dos esforços em pesquisas são voltados para ela, porém ainda existem pontos que não estão 100% encaminhados

Interoperabilidade e portabilidade de aplicações: Similar aos FDs, é importante que exista interoperabilidade entre as controladoras, isto inclui portabilidade de linguagem de programação entre elas para que possam utilizar das mesmas aplicações sem serem amarradas a suas fabricantes. Contudo, isso ainda está longe de ser realizado. (KREUTZ, 2015)

Peng Sun (2014) apresentou o que ele chama de "*Statesman*", que seria um *framework* que permite múltiplas aplicações de redes operarem independentemente no mesmo control plane sem comprometer a performance e segurança da rede. Este *Framework* deixa o desenvolvimento de aplicações mais simples pois ele automaticamente resolve os conflitos que possa acontecer entre diferentes aplicações.

Alta Disponibilidade: Controladoras SDN são responsáveis pela maior parte da funcionalidade da rede, é necessário a garantia de que elas estão funcionando perfeitamente para evitar qualquer tipo de interrupção na rede e, quando se depende muito do funcionamento de um equipamento é evidente que ele se torna a maior vulnerabilidade da rede.

Kreutz (2013) evidencia que ataques e vulnerabilidade nas controladoras é a maior ameaça para SDN. Uma falha em uma controladora pode comprometer toda a rede. *Softwares* comuns de detecção de atividades maliciosas podem não ser o bastante, devido a quantia de eventos que acontecem em uma controladora pode ser difícil de isolar uma atividade e identifica-la como suspeita. As soluções propostas são: Replicação de controladoras, desta forma fica fácil a remoção de uma delas caso necessário ser feito alguma investigação de atividade maliciosa; Diversidade de protocolos, linguagem de programação e *softwares*; praticar periodicamente atividades de varredura e limpeza do sistema; Garantir segurança de toda informação sensível dentro de uma controladora (chaves de criptografias/senhas).

5 DESAFIOS DE SEGURANÇA

Ataques cibernéticos tem-se tornado uma ameaça para o governo e todos ao redor do mundo, em uma notícia publicada recentemente pelo site *Security Report*, com base em informações providas pela Fortnet, só no Brasil houveram mais de 3,4 bilhões de tentativas de ataques cibernéticos e já é mais do que evidente que estes ataques podem causar danos a uma nação inteira, como foi o caso publicado pela revista VEJA do ataque recentemente sofrido pelo STJ (Superior Tribunal de Justiça) no Brasil, onde toda sua base de dados, inclusive *backups* foram criptografados por cibercriminosos.

Devido a problemas com *cyber* ataques nos dias de hoje, segurança é a maior prioridade quando o assunto é SDN (KREUTZ, 2013) . Por mais que a maior parte das vulnerabilidades existam tanto em redes convencionais como SDN, existem algumas que são exclusivas.

5.1 Vulnerabilidades

Como dito, a segurança é a maior preocupação quando se fala no futuro de SDN. Existem muitas pesquisas que focam no desenvolvimento da segurança em termos de detecção de ataque e defesa, desafios e oportunidades.

Uma pesquisa feita por Drashti e Nagaraju em 2017 e publicada no livro "A pragmatic analysis of security and integrity in software defined networks" evidencia pontos de ataques no data plane e control plane e também revê os modelos de segurança na SDN em diferentes níveis incluindo autenticação, gerenciamento e até mesmo o uso de checagem de fluxo.

Hussein (2019) divide o assunto de segurança em SDN em diferentes sessões, incluindo vulnerabilidade em comunicação e gerais, e elas serão vistas a seguir.

5.1.1 Segurança na comunicação

A comunicação entre a controladora e os switches são feitas utilizando o protocolo TCP, e podem ser, opcionalmente, autenticadas por TLS.

Durner e Kellerer em 2015 analisaram os limites da comunicação em diferentes camadas entre equipamentos como terminal e switch, switch e switch e switch e controladora. Foi usado um modelo de teste que divide a SDN em arquiteturas tais

como acesso do usuário, transmissão de dados e distribuição de controle e, no final da análise, foi possível identificar diversas vulnerabilidades na conexão entre as entidades que fazem parte da SDN.

Os principais pontos fracos identificados na comunicação são:

- Comunicação na *northbound interface*: Fraca autenticação permite que o *spoofing* dos dados seja feito com mais facilidades; Autorizações incorretas que podem levar a acessos maliciosos nas aplicações

- Comunicação na *Southbound interface*: Falta de criptografia no trafego entre controladoras e switch pode causar o roubo de dados; fraca autenticação entre controladoras e switches facilitam o ataque man-in-the-middle; Autorizações incorretas que podem levar a acesso inapropriado para o *data plane*.

5.1.2 Vulnerabilidades Gerais

Originalmente, redes tradicionais ja possuem falhas de segurança não resolvidas, com a chegada da SDN algumas delas foram endereçadas, porem outras novas foram surgindo e algumas ainda foram herdadas das redes tradicionais. As vulnerabilidades principais de SDN são:(Hussein, 2019)

- Controle Centralizado: O controle centralizado logo indica um ponto único de falha, fazendo as controladoras muito vulnerável a ataques como: DoS (*Denial of Service*) ou DDoS (*Distributed Denial of Service*). Anda existe o fato que quando se tem um controle centralizado, a controladora é um alvo muito chamativo para ataques de intrusão, se levarmos em conta que com o controle dela qualquer coisa pode ser feita no control plane, inclusive alterar os fluxos da forma que quiser. As controladoras são o foco das pesquisas de segurança em SDN, uma solução solida ainda não foi desenvolvida, mas está a caminho. Usar backups também pode ajudar a mitigar as ameaças nesse quesito, ja que em caso de emergência, é possível desativar uma controladora e utilizar outra.

- Código Aberto: SDN é implementado por softwares de código aberto como *OpenFlow* e, consequentemente, os atacantes tem a vantagem de poder procurar por vulnerabilidade no código.
- Riscos da tabela de fluxo: Todas as tabelas de fluxo da rede são controladas pela controladora principal e backup, como ja dito anterior mente, são alvos muito chamativos para atacantes. É de extrema importância que as tabelas de fluxo permaneçam consistentes e protegidas de qualquer atualização maliciosa que venha de fora ou de controladoras comprometidas.
- Falta de funcionalidades importantes: Algumas funcionalidades de segurança como NAT (*Network Address Translation*) ainda não estão naturalmente bem definidas na arquitetura de SDN. Nas redes SDN operando atualmente, funcionalidade como esta e outras relacionadas à segurança são implementadas adicionando equipamentos específicos ou aplicações externas, porem geralmente a implementação deste tipo de tecnologia acaba sendo complexa e tem várias limitações como a inspeção de pacotes feita pelo OpenFlow.

5.2 Ataques a SDN

Seguindo os exemplos mostrados por Hussein (2019), nesse capitulo vamos falar de alguns dos possíveis ataques que uma rede SDN possa sofrer.

5.2.1 Camada Física

Primeiramente, vamos começar olhando alguns possíveis ataques que ameaçam a rede na sua parte física: (Hussein, 2019)

- *"Hijacking"* de controladora: *Hijacking* é um termo inglês que é utilizado quando alguém toma o controle fisicamente de algo que não pertence a ele de forma que se beneficie (*Cambridge Dictionary*). A controladora por ser a parte mais crítica e mais poderosa da rede SDN, qualquer pessoa que tenha acesso a ela pode facilmente roubar informações sensíveis sobre os fluxos que passam pela rede e também, manusear o tráfego e as aplicações da forma que bem entender.

- Má administração: Em uma rede convencional, uma administração mal feita em um dos equipamentos pode causar um grande impacto, ja em uma rede SDN, uma configuração errada nas controladoras (intencional ou não) pode causar danos ainda maiores do que em redes convencionais, podendo facilmente comprometer a disponibilidade da rede

5.2.2 *Control Plane*

Seguindo o mesmo estudo, vamos agora falar sobre alguns ataques dos ataques que afetam diretamente o control plane:(Hussein, 2019)

- *Spoofing*: Redes *openflow* são vulneráveis a *spoofing*, o que não é algo específico da tecnologia, porem pode causar um grande impacto nela. Como funciona o ataque, por exemplo, um atacante pode roubar o endereço IP da controladora e então todos os dados que seriam direcionados a ela iriam para o atacante, permitindo ele fazer uma análise dos dados e em seguida enviar para a verdadeira controladora, fazendo parecer que nada aconteceu.

- *Man-in-the-middle*: Conhecido como "homem-no-meio" é algo que pode ser simplesmente aplicado na comunicação entre a controladora e os switches. Como dito anteriormente, a comunicação entre eles é feita por TLS, e a autenticação criptografada é opcional, consequentemente, existe a possibilidade de eles estarem se comunicando por texto plano.

- DoS (*Denial of Service*): Negação de Serviço é um ataque bastante comum em redes tradicionais, porém é algo mais fácil de ser aplicado em redes SDN. Levando em consideração que todos os serviços estão centralizados na controladora, para afetar uma rede inteira o atacante ja sabe muito bem onde atacar para causar o maior impacto. Este é provavelmente o ataque com maior potencial de impacto em redes SDN.

5.2.3 *Data Plane*

Para finalizar, agora veremos alguns ataques que afetam o Data Plane:(Hussein, 2019)

- Roubo de informação: Através da injeção de falsas regras nas tabelas de fluxo utilizando aplicações maliciosas, os atacantes conseguem fazer com que os tráfegos originados por eles passem pelo firewall ou outros equipamentos e aplicações de segurança sem problema, invadindo a rede toda e podendo facilmente roubar informações sensíveis.

- Adulteração de informações: O mais comum é a criação de regras falsas devido à falta de verificação consistente nas mesmas. Um exemplo disso é a técnica utilizada para ser feito o ataque de roubo de informações citado anteriormente, onde o atacante utilizando aplicações maliciosas consegue injetar regras falsificadas nas tabelas de fluxo.

- Ataques a nível de TCP: TCP (*Transmission Control Protocol*) é utilizado na comunicação entre os equipamentos e a controladora, consequentemente o atacante pode utilizar qualquer técnica de quebra do protocolo que ja seja conhecida, podendo ser ataques direcionado ao ICMP (*Internet Control Message Protocol*), reset de negociação, predição de sequência e até mesmo DoS.

6 CONCLUSÃO

O objetivo deste trabalho foi apresentar a tecnologia SDN e suas propostas para a arquitetura de redes moderna utilizando artigos e livros de profissionais renomados da área.

Ao longo do projeto, podemos ver que SDN cumpre, se não todas, a maioria das propostas iniciais feita, auxiliando no gerenciamento de redes trazendo-o de forma centralizada e desprendendo da arquitetura proposta por cada fornecedor, tornando-se algo mais dinâmico e flexível tanto para quem está gerenciando quanto para quem precisa de seus serviços.

Contudo, é importante ressaltar que, ainda existe muito a melhorar, como lido no capítulo 5 deste trabalho, SDN por utilizar de aplicações e possuir um gerenciamento centralizado, trouxe várias vulnerabilidades novas e deu a oportunidade para atacantes explorarem vulnerabilidades já existentes nas redes de computadores tradicionais

Considerando todos os pontos expostos neste trabalho, podemos concluir que SDN é sim uma solução que resolve muitos dos problemas das redes de computadores tradicionais, porém ainda não podemos a considerar como o remédio para todos os problemas, visto que existem falhas de segurança que se exploradas podem expor a rede inteira e até mesmo trazê-las ao colapso. Ainda existe muitas pesquisas em andamento, principalmente quando o assunto é a segurança das controladoras, porém acredita-se que esta é a melhor aposta que existe para o futuro de redes de computadores e que com o tempo todos estes problemas atuais serão mitigados ou extintos.

REFERÊNCIAS BIBLIOGRÁFICAS

BITTMAN T.J. **Magic Quadrant for x86 server Virtualization Infrastructure,** 2016

BRAUN W.; MENTH M., **Wildcard compression of inter-domain routing tables for OpenFlow-based software-defined networking**, 2014

CAMBRIDGE, **Cambridge Virtual Dictionary** (https://dictionary.cambridge.org/pt/dicionario/ingles/hijacking), 2020

CERF, V. G; KAHN, R. E. **A Protocol for Packet Network Intercommunication**, 1974.

CLARK, D. D. **The Design Philosophy of the DARPA Internet Protocols**, 1988.

DAVE D.; NAGARAJU A., **A pragmatic analysis of security and integrity in software defined networks**, 2017.

DIERKS T. **The transport layer security (tls) protocol version 1.2** (https://www.ietf.org/rfc/rfc5246.txt), 2008.

DURNER R.; KELLERER W., **The cost of security in the SDN control plane**, 2015

ELIAS, G; LOBATO, L. C. **Arquitetura e Protocolos de Rede TCP-IP**, 2° Edição. Rio de Janeiro. Editora RNP/ESR, 2013.

FEAMSTER, N; BALAKRISHNAM H. **Detecting BGP Configuration Faults with Static Analysis**, MIT Computer Science and Artificial Intelligence Laboratory, 2005

FELIPPETTI, M. A. **CCNA 6.0**: Guia Completo de Estudo, 2ª Edição. Editora Alta Books, 2019.

GHORBANI S; GODFREY B. **Towards Correct Network Virtualization**, University of Illinois, 2014

Hussein A., **Software-Defined Networking (SDN): the security review, Journal of Cyber Security Technology**, 2019

HWANG H; MURATA M., **A New TCAM Architecture for Managing ACL in Routers**, 2010

INTERNET WORLD STATS, **INTERNET GROWTH STATISTICS** (https://www.internetworldstats.com/emarketing.htm), 2020

KOBAYASHI M**., Maturing of OpenFlow and software-defined networking through deployments**, 2013

KOPONEN T., **Network Virtualization in Multi-tenant Datacenters**, VMWare, 2013

KREUTZ D., **Towards secure and dependable software-defined networks**, 2013

KREUTZ, D. **Software-Defined Networking**: A Comprehensive Survey, 2015.

MAURO, D. R. **Essentials SNMP**, 2ª Edição. Editora O'Reilly Media, 2005.

MCKEOWNETAL N. **OpenFlow: Enabling innovation in campus network,** 2008.

POSITIVO SOLUÇÕES DIDÁTICAS. Dicionário Aurélio da língua Portuguesa, 2019.

REDE NACIONAL DE ENSINO E PESQUISA - **Gerenciamento de Redes de Computadores**, 2015.

REVISTA VEJA, **Brasil sofre seu maior ataque hacker da história**, (https://veja.abril.com.br/blog/radar-economico/brasil-sofre-seu-maior-ataque-hacker-da-historia/), 2020

SALISBURY B. **The northbound API: A big little problem,** 2012

SECURITY REPORT, **Mais de 3,4 bilhões de tentativas de ataques cibernéticos já atingiram o país em 2020** (https://www.securityreport.com.br/overview/mais-de-34-bilhoes-de-tentativas-de-ataques-ciberneticos-ja-atingiram-o-pais-em-2020/#.X6z6hshKiUk), 2020

STALLINGS, W. **Foundations of Modern Networking**: SDN, NFV, QoE, IoT, and Cloud, 1ª Edição. Editora Addison-Wesley Professional, 2015.

SUN P., **A network-state management,** service, 2014

TANENBAUM, A. S. **Redes de Computadores**, 5ª Edição. Editora Pearson Universidades, 2011.