Instituto Politécnico de Setúbal

Escola Superior de Ciências Empresariais

Redes Definidas por Software

do estado da arte tecnológico à identificação de um conjunto de boas práticas

José Augusto Moreiras

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de

MESTRE EM SISTEMAS DE INFORMAÇÂO ORGANIZACIONAIS

Orientador: Hernani Raul Vergueiro Monteiro Cidade Mourão

Setúbal, 2016

Agradecimentos

No final este trabalho, não posso deixar de manifestar os meus agradecimentos a todos os que direta ou indiretamente ajudaram na sua execução.

À Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal, nas pessoas dos professores do Mestrado em Sistemas de Informação Organizacionais, com quem muito conhecimento, regras e valores absorvi durante os últimos dois anos.

Aos meus colegas de curso e camaradas de trabalho que me ajudaram com o seu tempo, disponibilidade e paciência para a discussão do tema.

Ao professor orientador de dissertação, o Professor Hernani Raul Vergueiro Monteiro Cidade Mourão, que com sugestões, propostas de adaptação e correções muito contribuiu para o esclarecimento das ideias que acabam por ficar registadas. Nas muitas reuniões de fim de sexta-feira, durante praticamente um ano, o professor contribuiu com um valoroso apoio profissional e com a sua vontade e força inspirou-me e motivou-me na evolução do trabalho.

Aos meus filhos, que muito me tem apoiado neste caminho académico que escolhi nos últimos cinco anos

A todos, um muito obrigado!

Índice:

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Acrónimos

ACL *Access Control List*
ACS *Access Control System*
AP *Access Point*
API *Application Programming Interface*
ARP *Address Resolution Protocol*
AS *Autonomous Systems*
ASIC *Application Specific Integrated Circuits*
BYOD *Bring Your Own Device*
CD Centro de Dados
CDP *Cisco Discover Protocol*
CIDR *Classless Interdomain Routing*
CLI *Command Line Interface*
CPD Centro de Processamento de Dados
DC *Domain Controller*
DDOS *Distributed Denial of Service*
DHCP *Dynamic Host Configuration Protocol*
DNS *Domain Name System*
DoS *Denial of Service*
DSL *Digital Subscribed Line*
ESCE Escola Superior de Ciências Empresariais
ETSI *European Telecommunications Standards Institute*
FDDI *Fibber Distribution Data Interface*
FIB *Flow Information Base*
HP *Hewlett-Packard*
IaaS *Infrastructure as a Service*
IDS *Intrusion Detection Systems*
IOE *Internet of Everything*
IOS *Internetworking Operating System*
IP *Internet Protocol*
IPS *Intrusion Protection Systems*
ISDN *Infrastructered Service Digital Network*
ISMS *Information Security Management System*
ISO *International Standard Organisation*
ISP *Internet Service Providers*
LAN *Local Area Network*
LSM *Local Switch Manager*
MAC *Media Access Control*
NaaS *Network as a Service*
NAT *Network Address Translation*
NFV *Network Functions Virtualization*
NSD *Network Service Directory*

NVT *Network Virtual Terminal*
ONF *Open Networking Foundation*
OSI *Open Standard Interconnection*
PaaS *Plataform as Service*
QOS *Quality of Service*
RFC *Request for Comments*
SaaS *Software as a Service*
SDN *Software Defined Network*
SNMP *Simple Network Management Protocol*
SSH *Secure SHell*
STP *Spanning Tree Protocol*
TCP *Transmission Control Protocol*
TI Tecnologias de Informação
VDS *Virtual Distributed Switch*
VLAN *Virtual* LAN
VoIP *Voice over Internet Protocol*
VPN *Virtual Private Network*
WAN *Wide Area Network*

Resumo

Perante a estática e praticamente imutável estrutura das arquiteturas de redes IP os administradores procuram soluções para a escalabilidade crescente do número de aplicações que emergem na área do *software* de administração de rede a que se chamou *Software Defined Networking* (SDN). Os principais objetivos desta promissora arquitetura são simplificar as operações da rede, reduzir custos e acelerar a entrega de serviços, dando aos administradores da rede a opção de alterar as redes para uma arquitetura aberta e com um novo tipo de interfaces. A SDN suporta a natureza dinâmica das funções de rede e aplicações. *Hardware*, *software* e gestão da estrutura convergem para uma solução de rede capaz de atender à enorme procura incessante de tráfego no futuro próximo por novos paradigmas de TI: mobilidade, *Interne of Everything* (IOE), computação em nuvem e "*Big Data"*.

A SDN requer a utilização de *software* em código aberto, para alavancar o seu crescimento e para tirar vantagem das diferentes topologias e modelos de arquiteturas de redes físicas, projetadas para diferentes fins. Aborda-se ainda a utilização da arquitetura OpenFlow, protocolo de trabalho do nível inferior do *framework* SDN, bem como a sua utilização e evolução pelas grandes organizações tecnológicas do ramo de negócio tendo em vista a sua utilização em grande escala nos centros de dados e sistemas de computação em nuvem.

Porque a maior parte dos clientes confia num único fornecedor e solução, ou pelo menos num fornecedor dominante, podemos concluir que o foco principal para os administradores de rede será projetar e implementar uma estratégia de SDN. Isto levá-los-á a escolher uma gama de soluções desenvolvidas por uma plataforma em código aberto. Se tivermos em conta a forte evolução dos últimos dois anos e o esforço realizado pelas empresas do setor nesta arquitetura tecnológica, podemos afirmar que esta arquitetura de rede tomará conta da gestão e administração das redes num futuro próximo.

Palavras-chave: gestão, redes, arquitetura, SDN, OpenFlow, *software*

Abstract

Software Defined Networking (SDN) is an emerging topic and discussed as one of the most promising network architecture that could simplify network operations, reduce costs and accelerate services delivery. Facing the static and virtually unchanging structure of the traditional IP network architecture, administrators seek solutions to the growing scale of the number of network administration applications. SDN gives network customers a choice to change their networks for open architecture and new type of interfaces. SDN supports dynamic nature of network functions and applications while lowering costs. Hardware, software, and management converge to a networking capable of meeting the huge traffic delivery demand in the near future by new paradigms of IT, mobility, Internet of Everything, cloud and Big Data.

SDN requires the use of open source software, to leverage its growth and to take advantage of different topologies and models of physical network architectures, designed for different purposes. This work also addresses the using of OpenFlow architecture, level of work protocol lower SDN *framework*, as well as their use and development by large technology organizations and business branch with a view to its use in large-scale datacenter and cloud computing systems.

Because most customers rely on a single supplier and solution, or at least a dominant supplier, we can conclude that the main focus for network administrators will be designing and implement an SDN strategy. This will lead them to choose a full range of solutions developed by an open source platform. Taking into account the strong growth the past two years and the efforts made by companies in the industry in this technology architecture, we can say that this network architecture will take care of the management and administration of networks in the near future.

Key-words: *management*, *networking*, *architecture*, *software*, SDN, *OpenFlow*

1. Introdução

Quando um arquiteto planeia uma obra, a arquitetura deve encorajar a colaboração entre as componentes, caso contrário a arquitetura deixará de fazer sentido. O próprio conceito de arquitetura pressupõe um conjunto de elementos organizados para um determinado objetivo ou funcionalidade, em que cada um dos elementos desempenha uma função específica. Estas funções devem colaborar na obtenção do objetivo comum. Da mesma forma, se uma arquitetura de rede não encorajar a colaboração entre tecnologias, então não atingirá os objetivos para que foi criada. Quanto maior for a capacidade que uma arquitetura de rede tem para projetar os sistemas existentes, de modo a satisfazer os utilizadores, maior será o seu sucesso. Para cumprir os requisitos de exigência e desempenho, o seu funcionamento tem que adaptar-se às mudanças. As arquiteturas de rede baseadas em *software*, ou *Software Defined Networks* (SDN) de acordo com a designação utilizada na bibliografia, têm como objetivo principal a separação física da camada de gestão e da camada de controlo da rede. Nesta separação utiliza-se um plano de controlo que gere vários dispositivos de rede físicos ou lógicos e que assegura o encaminhamento do fluxo da informação.

As atuais arquiteturas da rede apresentam uma série de limitações, por exemplo, o nível da escalabilidade, da segurança e da mobilidade. Por outro lado, as infraestruturas de rede tronaram-se obrigatórias e foram um sucesso nas empresas, nas escolas ou mesmo nas nossas casas. Nesta altura apresentam limitações que já são críticas para a inovação e a entrada de novas ideias para lá da pesquisa tradicional, pois consistem num emaranhado de protocolos e de sistemas em funcionamento. A configuração dos serviços que definem o funcionamento da rede é realizada através de variados subsistemas. São tecnologias, protocolos, técnicas e processos de gestão tais como sub-redes, *Autonomous Systems*[1] (AS), Sistemas Autónomos, *Classless Interdomain Routing*[2], (CIDR) ou *Network Address Translation*[3] (NAT), para que os administradores consigam fazer face aos requisitos atuais e futuras aplicações (McKeown at al, 2008). A SDN pode revolucionar esta forma de gerir e administrar redes, com as configurações a serem realizados através de uma abstração de *software* e com um sistema de controlo a funcionar a partir de um único ponto.

1.1. Problemática

A principal razão para a existência das redes informáticas é o facto de existirem serviços a prestar a clientes e utilizadores. Num passado recente as redes ligavam-se a redes para aumentar o seu raio de ação. Foi assim que nasceu a internet, a maior de todas as redes existentes e, por isso, conhecida como a "rede das redes". Com o crescimento das redes a nível global, nasceram variadas topologias e arquiteturas. A tecnologia de

[1] Conjunto de prefixos de routing ligados e controlados por endereçamento IP
[2] Capacidade de agregar os endereçamentos em classes de rede (RFC 1519)
[3] Forma de mapear um IP externo na rede interna e permitir acesso a IPS internos.

ligação *ethernet*[4] ganhou vantagem sobre as tecnologias concorrentes apoiadas pelas topologias *novell* e *tokenring*. A razão fundamental deste sucesso aparenta ser a facilidade com que esta topologia alavanca a escalabilidade e faz uso da arquitetura TCP/IP[5] de que falaremos mais adiante. Os problemas gerados pelo crescimento exponencial foram tratados com recurso a novos protocolos, padrões de rede e equipamentos ativos de rede. Devido às necessidades criadas por negócios e empresas, os grandes fabricantes e fornecedores de ativos de rede cresceram rapidamente. Os equipamentos de comutação e reencaminhamento, vulgarmente conhecidos pelos termos em inglês *switches*[6] *and routers*[7], tornaram-se vitais para a os planos de negócio. A estrutura física das redes tem permanecido praticamente imutável ao longo da última década, tendo apenas sido registadas alterações significativas nos meios de transmissão. A comunicação, que anteriormente se suportava nas tecnologias suportadas em cabo de cobre *Infrastructered Service Digital Network* (ISDN) e *Digital Subscribed Line (DSL*), viu surgir a distribuição de sinais por fibra ótica, conhecida por *Fibber Distribution Data Interface* (FDDI) com o consequente aumento no limite de velocidade de transmissão.

O problema a resolver agora é conseguir que o tráfego flua o mais rápido e ordenado possível pelo caminho certo através da estrutura existente. Isso só é possível se configurarmos alterações na arquitetura física da rede e obrigarmos o fluxo da informação a caminhar pelos locais mais adequados através de controlos feitos pela parte programável da rede.

Os fabricantes e fornecedores dos serviços de rede estão atentos à problemática, desenvolvendo e vendendo soluções e serviços de configuração que incluem a resolução do problema. As grandes organizações, que possuem estrutura própria e fornecimento de serviços, adaptam-se à nova realidade, introduzindo os conceitos desenvolvidos por si ou pela academia. Nem todas podem optar por contratar os serviços de configuração a terceiros, quer por que estão fora do seu orçamento quer pela dificuldade em adaptá-las à sua realidade. Algumas destas organizações possuem administração e configuração própria da sua estrutura de rede, baseada em quadros técnicos especializados nas tecnologias e modelos de configuração. Quer a administração da rede seja feita por contrato de serviços, quer por quadros da empresa, a resolução desta problemática é sempre uma preocupação empresarial. Por vezes, as dificuldades não se manifestam nalgumas organizações, porque possuem uma estrutura física tão sobredimensionada que dá a ideia que não são necessárias intervenções nem configurações para resolver um problema inexistente. Esta última abordagem tende a ser temporária porque, mais tarde ou mais cedo, a organização percebe que a estrutura não é suficiente para suportar novos requisitos de mobilidade, virtualização ou *framework* de vídeo.

[4] Tecnologia de ligação de redes e equipamentos em rede mais utilizada
[5] Um dos modelos de desenho e implementação de redes.
[6] Equipamento de rede com a função de comutação de pacotes
[7] Equipamento de rede com a função de reencaminhamento de tráfego

Os serviços são normalmente fornecidos a partir de pontos específicos da rede, os denominados centros de dados. Estes locais, por vezes também conhecidos como *server farm*s, possuem um conjunto de servidores da organização. A presença desta infraestrutura faz aumentar o tráfego na rede, assim como os requisitos de processamento de informação. A resolução destas necessidades passa pela substituição dos equipamentos existentes por outros mais modernos e eficientes. Este conjunto de equipamentos pode variar de número e funções conforme a dimensão da organização. Quando uma infraestrutura aumenta, pode sentir-se a necessidade de melhorar a segurança da infraestrutura. Os servidores e equipamentos têm que ser mantidos em condições de funcionamento adequadas e com o intuito de fornecer aos seus utilizadores um ambiente de trabalho com garantia e vantagens sobre o mesmo tipo de serviço obtido através de fornecedores de serviço de internet. Face a utilização de aplicações e equipamentos, cujo funcionamento deficiente pode por em causa o normal funcionamento da empresa, é necessário um ponto de intervenção rápido para controlar e repor a situação de funcionamento normal. Mais tarde analisamos este aspeto no subcapítulo 2.7 - SDN no Centro de Dados.

1.2. Objetivos

A arquitetura tradicional de gestão da rede é, fundamentalmente, baseada na sua arquitetura física. O propósito deste trabalho é abordar uma realidade recente, que está associada ao desenvolvimento e evolução da arquitetura de gestão e administração das de redes e que está, neste momento, a expandir-se - a arquitetura de rede baseada em *software*. Embora a evolução da SDN tenha sido de vulto nos últimos cinco ou seis anos, aos profissionais de gestão e de administração de redes a desempenhar funções em pequenas e médias empresas chegou pouca informação sobre os seus conceitos fundamentais.

O objetivo geral deste trabalho consiste no levantamento **do estado da arte das tecnologias SDN** que estão a ser desenvolvidas pelas empresas do setor de administração e gestão das redes, para tentar **compreender porque em redes de grande dimensão a procura das causas de um incidente é um conjunto de processos lentos e complexos**, criando-se assim nos utilizadores uma ideia errada de um mau funcionamento sem causas aparentes. A problemática acerca do defeituoso funcionamento das redes tradicionais foi detetada primeiramente nos meios académicos dedicados ao estudo desta temática. Sendo assim, também não é de admirar que a solução tivesse surgido nos mesmos meios.

De uma forma mais específica, este trabalho pretende ainda atingir os seguintes objetivos específicos:

- Acelerar os processos de resolução de incidentes na gestão das redes tradicionais e redes definidas por *software*;

- Trazer, novamente, o assunto para a discussão académica e tentar explicar o que se entende por SDN e o que é o protocolo OpenFlow que grandes organizações tecnológicas de administração e desenvolvimento de *hardware* e *software* de redes estão neste momento a utilizar;
- Perceber a importância do SDN e OpenFlow para a evolução e o conhecimento da arquitetura de gestão de redes por *software*, assim como da forma como estão a ser publicitadas, desenvolvidas e implementadas as soluções SDN pelas referidas organizações;
- Efetuar uma análise destes conceitos e de soluções desenvolvidas ou já implementadas por algumas empresas;
- Propor algumas sugestões de boas práticas a adotar na implementação da SDN nas redes tradicionais. Em específico, apresentar boas práticas:
    - Na implementação controladora SDN;
    - Na configuração da rede;
    - Na gestão e administração da rede;
    - E na segurança da rede.

1.3.Metodologia

Utilizamos uma metodologia qualitativa porque se trata de matéria de investigação feita através de uma "variedade de técnicas interpretativas que têm por fim descrever, descodificar, traduzir certos fenómenos" (Guerra 2006). No nosso caso estamos à procura de alternativas para os problemas que a gestão e a administração das redes tradicionais enfrentam. Nesse sentido criamos um processo de pesquisa e análise documental a partir de trabalhos científicos e páginas da internet das organizações profissionais que desenvolvem na área das tecnologias SDN. Procuramos primeiro identificar o estado da arte e determinar amplitude da área a estudar. Em seguida orientamos as técnicas de pesquisa na procura de material com significado que nos permitisse a tomada da decisão sobre o conteúdo e a sua importância.

Este estudo baseia-se na investigação e na experiência que as organizações mais representativas das tecnologias SDN tem feito nos últimos anos. É por isso também uma fonte das características dos métodos do estudo qualitativo, fruto da experimentação e da investigação situacional (Stake 2011).

1.4.Estrutura do Trabalho

Este trabalho está estruturado segundo as normas da ESCE para os trabalhos académicos dos mestrados. Esta estrutura inclui cinco capítulos compostos por subcapítulos e estes por seções.

Depois deste capítulo introdutório temos o capítulo dois que é dedicado à revisão da bibliografia mais relevante publicada sobre o assunto que se pretende abordar. Faz-se, em primeiro lugar, a identificação da problemática e o que tem sido realizado pela comunidade académica e profissional para a resolução dos problemas identificados. O capítulo está

dividido em 8 subcapítulos cada um deles com um tema considerado importante para a perceção da SDN atual e do seu desenvolvimento nos últimos cinco anos. Os subcapítulos estão ordenados por ordem cronológica para melhor se perceber a evolução do paradigma SDN. Do primeiro até ao oitavo são: **SANE, ETHANE, SDN, SDN e OpenFlow, Interfaces Northbound e Southbound, SDN no Centro de Dados e SDN na Computação em Nuvem.**

No terceiro capítulo, designado **Da Gestão das Redes Tradicionais à Gestão das Redes SDN,** descreve-se a forma como se está a fazer a gestão redes e dos seus equipamentos nas arquiteturas tradicionais. Faz-se ainda uma caracterização de alguns aspetos considerados fundamentais para a compreensão da realidade existente. O capítulo está dividido em seis subcapítulos:

- **A arquitetura –** onde se analisa como funcionam as arquiteturas tradicionais;
- **A administração –** como são desenvolvidos os esforços de administração das redes tradicionais e o papel dos administradores de rede;
- **A configuração –** onde se apresentam as configurações necessárias e o trabalho que as arquiteturas tradicionais exigem para esta parte importante da administração das redes;
- **Gestão das redes SDN –** descreve as práticas que estão a ser utilizadas para a gestão de redes pelas organizações académicas e empresariais na área das redes definidas por *software*. O objetivo consiste em que o novo paradigma substitua com vantagem a gestão e administração tradicional das redes IP;
- **A SDN e a Virtualização –** analisa como a SDN e a virtualização evoluem em conjunto e se complementam na gestão e administração das redes;
- **As soluções empresariais na SDN -** investiga-se o papel que as principais organizações envolvidas na SDN desempenham no desenvolvimento da nova arquitetura tecnológica da gestão das redes. Está dividido em seis seções em que se analisam cinco soluções SDN das principais empresas da área e se faz um pequeno apanhado de outras empresas a desenvolver e experimentar soluções. Do primeiro até ao sexto eis os nomes das seis seções:
  - ONF,
  - OpenDaylight,
  - Cisco,
  - HP-VMware,
  - IBM,
  - Outras organizações.

Em cada uma destas seções apresentamos trabalhos que constam no endereço eletrónico destas empresas e que estão a desenvolver para o desenvolvimento da SDN.

No quarto capítulo chamado **Boas Práticas na Implementação da SDN**, apresenta-se uma proposta de boas práticas e métodos para a implementação da SDN na estrutura de rede

duma organização. Está dividido em quatro subcapítulos e em cada um deles aponta-se um conjunto de boas práticas para a implementação do componente analisado. Os títulos são: **Boas Práticas na Implementação da Controladora**, **Boas Práticas na Configuração de Equipamentos**, **Boas Práticas na Administração da Rede** e **Boas Práticas na Implementação da Segurança da Rede**.

O quinto e último capítulo, designado **Conclusões e Perspetivas,** foi dividido nestas duas seções com o intuito de colocar em conclusões, as ilações retiradas da parte de investigação do trabalho e em perspetivas em que se aponta as perspetivas futuras de profissionalmente, o autor, vir a implementar ou trabalhar com soluções SDN, apoiando-se no conhecimento adquirido ao longo da elaboração deste trabalho.

2. Revisão da Literatura

A história das arquiteturas de redes baseadas em *software* remonta a 2006, quando um grupo de estudantes da Universidade de Stanford, Califórnia, desenvolveram em associação com dois estudantes da universidade de Berkeley, um trabalho que designaram "*SANE: A Protection Architecture for Enterprise Networks*", que tinha como objetivo propor uma solução para simplificar o processo de implementação das políticas de segurança da rede, sem a obrigatoriedade de visitar todos os equipamentos de *routing*, *switching* e *firewalling*, como acontece na administração tradicional de redes (Casado et al, 2006, 1). Este trabalho conjuntamente com um outro conceito fundamental designado "*collaborative open source*" (código aberto em ambiente colaborativo), ou seja, código aberto a toda a comunidade de pesquisadores de tecnologias e soluções de rede que quisessem criar a partir dele. A colaboração entre as duas universidades acima citadas nestes projetos acabou por ser o impulso necessário que permitiu aos utilizadores das respetivas redes definirem fluxos de dados e determinarem os caminhos desses fluxos, usando *software* independentemente daquele que controlava o *hardware*. Criou-se assim uma outra forma de tornar o mercado mais competitivo, pois deixou de ser necessário adquirir um *software* específico para o controlo de um determinado *hardware*.

2.1. SANE

A forma tradicional de implementação de políticas de segurança nas arquiteturas de rede tradicionais é executada através de múltiplos mecanismos. De entre eles, destacam-se os mais conhecidos e utilizados: *Virtual Lans* (VLANs), *Access Control Lists* (ACLs), *firewalls* e NAT. São processos meticulosos e de elevado grau de dificuldade que requerem atenção redobrada por parte dos executantes. Qualquer falha na execução do processo põe em causa a implementação correta das políticas de segurança da empresa. O processo de segurar a rede pode alterar a sua topologia lógica, alterando convergência dos processos de *switching* e de *routing* provocada pelas novas configurações, provocando atrasos e gerando ruído na comunicação. As reconfigurações específicas, na maioria das vezes, dão azo a quebras temporárias de serviço e geram processos comprometedores nas políticas de segurança da organização (Casado et al,2006, 2).

A arquitetura tradicional é um campo fértil aos ataques de utilizadores mais hábeis, mais experimentados e com menos escrúpulos. Este tipo de utilizadores pode, com alguma facilidade, explorar as vulnerabilidades com ataques típicos como *Denial of Service* (DoS), disrupção ou *man-in-the-midle*. Com ataques como estes pode-se frequentemente tornar a rede não utilizável ou redirecionar o tráfego para análise e espionagem. A proliferação da informação não controlada é também um recurso que facilita a vida aos atacantes, porque lhes permite identificar serviços, bases de dados ou equipamentos de proteção da rede (IDS, *firewall*,…). Com este conhecimento está facilitada a identificação da topologia de rede e, por conseguinte, a identificação da metodologia de ataque. SANE, foi a primeira abordagem ao estudo da fragilidade e à vulnerabilidade da arquitetura de redes IP tradicionais. Como objetivo inicial o trabalho pretendia fornecer uma arquitetura de proteção para redes

corporativas. A forma encontrada seria definir uma única camada de proteção, que tinha como princípio ser o ponto de controlo e de onde se regeriam todos os acessos e permissões existentes dentro da rede empresarial. Todas as decisões de roteamento e controlo de acesso passariam a ser realizadas por um servidor logicamente centralizado que forneceria serviços de distribuição e proteção dos recursos. Tudo isto numa camada de abstração única que controlaria todas as ligações feitas de e com a empresa. Os autores identificaram as falhas primárias das arquiteturas de redes IP existentes e apresentaram soluções para as suas resoluções imediatas (Casado et al, 2006:1-3).

A **Tabela 1** apresenta uma síntese com as principais falhas encontradas e soluções propostas pelo SANE.

Rede atual	Fragilidade	SANE
Complexidade de mecanismos (VLANs, NATs, ACLs, *Firewalls*)	Disperso e a requerer permanente atenção	Resposta comum com uma política de segurança por *software*
Parâmetros por omissão ativados; mais privilégios menos segurança.	Conhecidos de todos, logo fáceis de manipular	Parâmetros por omissão desativados; menos privilégios; capacidades instaladas providenciam acessos.
Pontos de controlo descentralizados	Difíceis de administrar e fáceis de encontrar pelos invasores	Pontos de controlo centralizados
Rede permissiva entre ligações; Controlo de passos inexistente	Intrusão no meio; disrupção.	Segurança aplicada por níveis; controlo do tráfego; economia de esforços dos sistemas
Endereçamentos sem ligação ou sentido entre níveis de acesso a core	Dificuldade na gestão e controlo	Endereçamento de acesso à rede, distribuição e core fortemente ligados
Princípio da proliferação da informação	Recurso facilmente utilizado por atacante	Princípio da informação restrita
Demasiados protocolos de broadcast sem autenticação; uPNP; CDP; e DHCP	Trafego desnecessário e não autenticado na rede;	Utilização de *gateways* SANE DCs distribuídos;
Serviços não tolerantes a falhas	Falha de serviço por inoperância de servidor	Replicação de DCs com métodos de consistência de serviços

Tabela 1 - Arquitetura tradicional (fragilidades) vs SANE (soluções propostas)

A implementação da maioria das soluções apresentadas consegue ser realizada utilizando as arquiteturas simples e existentes em quase todas as redes tradicionais, desde que implementem o serviço de *Active Directory* (AD), que a Microsoft tinha lançado com o sistema operativo Windows 2000. De facto, a AD implementa um serviço centralizado de controlo de políticas de acesso a recursos de uma rede distribuída que permite aplicar as soluções propostas pelo SANE.

A **Figura 1** representa a arquitetura que o SANE identificou como necessária à implementação das soluções propostas (Casado et al, 2006:4).

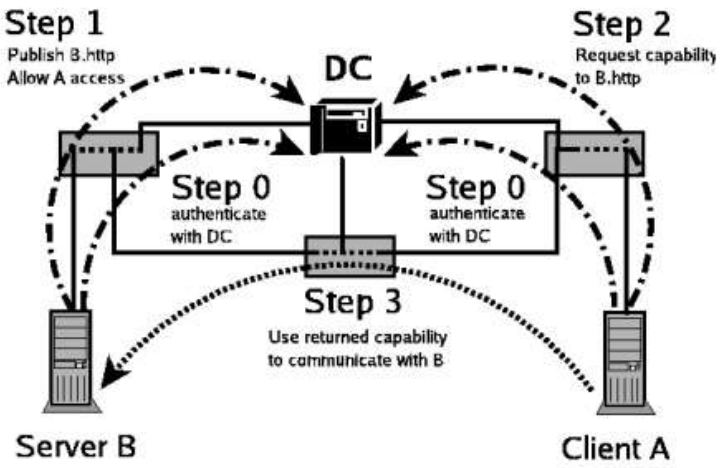

Figura 1 **- Primeira arquitetura SANE (Casado et al, 2006)**

Quando um novo utilizador ou equipamento se conectam na rede em que funciona a arquitetura SANE, esta apenas permite a comunicação do cliente com o Controlador de Domínio – *Domain Controller,* (DC). Este DC é o responsável por autenticar todos os utilizadores e serviços. A comunicação existente entre quaisquer outros componentes da rede pode então acontecer. Esta comunicação seguirá os seguintes passos:

- Primeiro passo (*Step 0*) - Cliente e Servidor autenticam-se no DC e estabelecem um canal seguro para comunicação futura;
- Segundo passo (*Step 1*) - Servidor publica serviços sob um único nome no *Network Service Directory* (NSD), *Server.http*;
- Terceiro passo (*Step 2*) – Cliente A requer permissão para aceder ao serviço de B;
- Quarto passo (*Step 3*) – Se o cliente tem permissão para o serviço *Server.http* passa a aceder diretamente.

Esta é uma arquitetura dos sistemas de autenticação que passou a ser utilizada por todos os sistemas de autenticação única. Nestes sistemas cada cliente apenas se autentica uma vez no DC e são-lhe atribuídas as autorizações associadas ao seu perfil registadas nas políticas implementadas pelas políticas de serviço de diretório.

O SANE apresentou ainda capacidades adicionais, que os autores consideraram essenciais para o bom funcionamento a rede IP. Os serviços adicionais e considerados fundamentais incluíam a capacidade de registo centralizado de todas as ações da rede, controladores intermédios, *proxies* e mobilidade.

Após esta primeira incursão pelo estado da arte das redes tradicionais e suas arquiteturas, segundo as próprias conclusões dos autores, o SANE revelou ser um *framework* não suficientemente testado e apresentando algumas dificuldades na implementação. Embora a análise feita pelo SANE apresentasse as fragilidades a que as estruturas de rede estavam sujeitas e fornecesse as suas soluções, a implementação das correções não surgia com facilidade esperada (Casado et al, 2006, 7-8).

2.2.ETHANE

Num outro trabalho realizado em 2007, designado Ethane, foi apresentada uma arquitetura de gestão de redes empresariais baseada em fluxos de pacotes e programada através de uma linguagem de alto-nível. Praticamente o mesmo conjunto de autores (Casado et al, 2007), faz uma análise das fragilidades encontradas nas arquiteturas, e apresenta soluções para as ameaças identificadas. No trabalho anterior estas fragilidades não tinham sido detetadas e, consequentemente, não tinham sido resolvidas. Mas a proposta deste trabalho é responder à questão: "**Como podemos alterar a arquitetura da rede de forma a torná-la mais facilmente administrável?**". Como exemplo do que este trabalho identificou, apresentam-se algumas das fragilidades mais relevantes existentes em protocolos de utilização generalizada. Os três exemplos da ***Tabela 2*** (Casado et al, 2007) são bem conhecidos de administradores de sistemas e redes.

Protocolo	Fragilidade	Ataque
Address Resolution Protocol (ARP)	Não autenticado	Mapear o IP para *Media Access Control* (MAC) errado
Dynamic Host Configuration Protocol (DHCP)	Não autenticado	Alterar *gateway* para IP errado
Domínio Name System (DNS)	*Caches* persistentes quando os clientes saem da rede	*Redirecionar informação da cache*

Tabela 2 - Algumas fragilidades e ataques identificados pelo ETHANE

Os protocolos acima citados, embora analisados pelo SANE não foram tratados nessse trabalho. Sendo a sua execução desencadeada de forma dinâmica[8] e posteriormente revistos no ETHANE, foram encontradas as falhas identificadas na nova análise dos processos. Estas falhas permitiam aos atacantes da rede aproveitar as fragilidades inerentes e desencadear ataques maliciosos. Para colmatar estas falhas a rede necessitava da intervenção atempada dos administradores. Procurou-se usar endereços IP fixos de forma a tornar o protocolo *Address Resolution Protocol* (ARP) estático e limpar ciclicamente *caches* do DNS para evitar a sua utilização maliciosa. Estes processos adulteravam, de alguma forma, os princípios da criação e do funcionamento dos próprios protocolos e as razões porque tinham sido desenvolvidos. Os processos reativos eram assim implementados com a criação de novos procedimentos e regras de utilização. Como consequência a arquitetura da rede ficou menos flexível e funcional. Por outro lado, se em qualquer equipamento da rede,

[8] Um protocolo de execução dinâmica é aquele cuja execução é desencadeada por um processo automatizado na rede e sem iniciativa de terceiros

em qualquer posição da arquitetura, fosse tomado por um invasor que desviasse o tráfego por um outro caminho, essa ação poderia ter consequências desastrosas para a organização. A administração da rede estaria comprometida e o administrador não conseguiria gerir o efeito das ações anteriores.

O estado da arte na administração de redes empresariais obriga a executar uma ampla variedade de aplicações e protocolos, que tipicamente operam sob confiabilidade restrita (Casado et al, 2007). A fim de proteger a rede e a informação que nela viaja Ethane estipula três princípios fundamentais para tornar a rede mais facilmente administrável.

- A rede deve ser gerida tendo em conta políticas de segurança estabelecidas a um nível mais elevado e a partir de pontos de acesso que não envolvam os equipamentos ativos de rede;
- Devem também ser as políticas a determinar todo o caminho que os pacotes percorrem ao longo da rede, ainda que forçosamente sejam obrigados a passar por um destino intermédio específico;
- A rede deve impor uma forte ligação entre os pacotes e a sua origem, de forma a poderem ser sempre rastreados.

Embora com semelhanças fundamentais com SANE, principalmente a nível de análise, em que mais uma vez se verificou a dificuldade de implementação, o ETHANE vem estender o anterior trabalho e impor três princípios fundamentais (Casado et al,2007, 3).

- A segurança segue a gestão - segurança da empresa é um subconjunto da gestão de rede. Ambos requerem uma rede com controlo e formas de monitorizar, identificar, isolar e diagnosticar os erros, assim como controlar o fluxo de informação, ou seja, quem comunica com quem;
- Implementação incremental – uma abordagem ampla da rede pode parecer a melhor forma mas em alguns casos as mudanças são um entrave significativo. ETHANE pode ser implementado por fases sem que a organização necessite de mudanças significativas na arquitetura. Os ativos de rede podem ir sendo integrados na nova estrutura ao lado dos equipamentos existentes e a funcionar em conjunto;
- Experiência de implementação significativa – Ao contrário de SANE, ETHANE foi largamente testado em *hardware* e *software*, em meios de transmissão a Gbit Ethernet e com experiência alargada de gestão em mais de 300 *hosts*.

É com o ETHANE que emerge a primeira arquitetura de rede, que mais tarde se consolidou na arquitetura SDN, descrita na secção seguinte. Os nomes e as definições dos seus componentes também foram exportados para as definições SDN. Quando se fala de um *Switch* ETHANE, por exemplo, estamos a falar de um *switch ethernet* simplificado, que não precisa de aprender *mac-addresses*, suportar VLANs ou construir e guardar estatísticas de tráfego. Todas estas tarefas já são realizadas pela controladora ETHANE. O que um *switch* ETHANE necessita é de uma tabela de controlo de fluxo que contenha os cabeçalhos dos

pacotes e uma ação que lhe é imposta pela controladora. Na verdade, existem dois tipos comuns de entrada na tabela de fluxo:

- *Perflow* entradas que descrevem fluxos dos pacotes que devem ser reencaminhados;
- *Perhost* entradas que descrevem mau comportamento dos originadores dos pacotes que devem ser descartados.

Apenas a controladora pode acrescentar entradas na tabela de controlo de fluxo. As entradas podem ser removidas pelo controlador local do *switch* por excesso de tempo e inatividade ou então revogadas pela controladora. A ação de autorizar tráfego ou de descartá-lo não é a única atribuição dum *switch* ETHANE. Quando a rede tem implementada o *Quality of Service* (QoS) ou NAT, o *switch* terá variadas filas de classificação de tráfego e tabelas de tradução de endereços que a controladora gere de acordo com a política implementada. Nestas condições, a tabela de controlo de fluxo não é, portanto, a única tabela existente no *switch*. Para gerir estas tarefas, manter a comunicação com a controladora e informar o estado da ligação, um switch ETHANE possui um nível de *software* a que se chama *Local Switch Manager* (LSM). Este *software* é também responsável por estabelecer inicialmente a comunicação segura entre o *switch* e a controladora. A ***Figura 2*** apresenta a arquitetura típica duma rede ETHANE de acordo com o documento original (Casado et al, 2007:6).

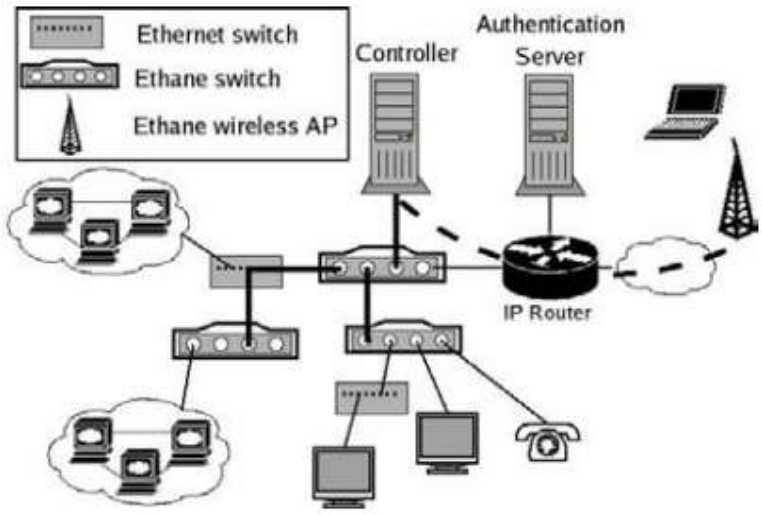

Figura 2 - Arquitetura duma rede ETHANE (Casado et al, 2007)

A arquitetura é uma arquitetura física que apresenta componentes típicos duma rede local com tecnologia *ethernet* e composta de vários elementos utilizados em 2007. Foi com esta arquitetura de rede que os estudos deste trabalho foram desenvolvidos. Já a arquitetura de comunicação na rede local é bem mais simples e restringida e utilizadores, PCs e servidores. A comunicação prevista pela arquitetura que o ETHANE é resumida em cinco etapas

distintas. O seu funcionamento é descrito abaixo e exemplificado pela ***Figura 3*** (Casado et al, 2007:5-6). Decorre a seguinte sequência de acontecimentos:

- **Registo** – utilizadores e *switches* ETHANE registam-se na controladora com as suas credenciais de autenticação. Estas credenciais podem variar por tipologia ou dispositivo, por exemplo, utilizadores podem usar o par de credenciais *user* e *password*, enquanto ativos de rede e computadores podem utilizar *mac-addresses* ou certificados;
- **Inicialização** – os *switches*, no arranque, criam uma rota de *spanning-tree* por omissão com a Controladora ETHANE. Terminada esta etapa criam um canal seguro por onde se autenticam e registam. A partir deste momento toda a comunicação entre os dois componentes do sistema é feita por este canal. A controladora atualiza o estado dos equipamentos ativos e refaz a topologia;
- **Autenticação** – o par *userA/hostA* entram na rede. Não existe tráfego para este conjunto, então o *switch* envia o tráfego vindo deste conjunto para a controladora, que inicia um novo fluxo, verifica credenciais e atribui IP ao *mac-address* respetivo à porta do *switch*. O utilizador autentica-se e começa a sessão na rede. O mesmo se passa com o par *userB/hostB*. A partir do momento que *userN/hostN* estão autenticados na rede, podem começar a utilizar os serviços. Sempre que iniciam uma comunicação nova, esta é automaticamente redirecionada para a controladora ETHANE com a finalidade de verificar as autorizações;
- **Configuração de fluxo** – *UserA* inicia comunicação com *userB*. O *switch* encaminha o pacote para a controladora depois de verificar que não coincide com nenhuma entrada ativa na tabela de fluxo. A controladora decide se deve permitir ou negar o fluxo, ou obrigá-lo a percorrer um conjunto de pontos intermédios na rede. Se o fluxo for permitido, a controladora insere a rota em todos os pontos intermédios do caminho e adiciona uma nova entrada nas tabelas de fluxo de todos os *switches* ao longo do caminho;
- **Encaminhamento** – se a controladora permitiu o caminho, envia o pacote de retorno e acrescenta as entradas simétricas nas tabelas de todos os *switches* do caminho. Os pacotes subsequentes passam a ser encaminhadas diretamente entre *switches* sem a necessidade de serem enviados á controladora. A entrada é mantida em cada *switch* até que ela expire, devido a inatividade ou seja revogada pela Controladora.

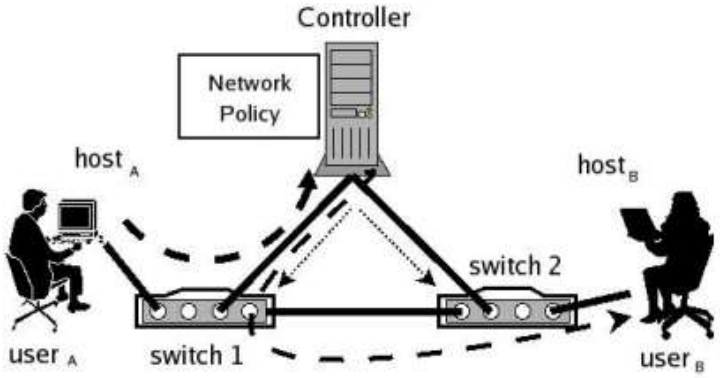

Figura 3 - Comunicação numa rede ETHANE (Casado et al, 2007)

Como a controladora conhece a topologia da rede, ao passo que cada *switch* só conhece uma parte dela, cada novo elemento deve autenticar-se na controladora. Na perspetiva do *switch*, cada novo pacote é um novo fluxo, pelo que é automaticamente encaminhado para a controladora através do canal seguro. A controladora é, pois, o elemento fundamental do controlo duma rede ETHANE, funcionando como um cérebro que distribui a inteligência pela rede tornando-se a entidade responsável pelo funcionamento da arquitetura.

No âmbito deste trabalho não iremos fazer uma análise minuciosa de todos os componentes da controladora ETHANE, mas apenas reforçar a ideia das suas funções dentro da arquitetura e da importância vital que têm dentro das arquiteturas SDN. Podemos verificar quais os elementos importantes que compõem a controladora, se atentarmos na ***Figura 4***, (Casado et al, 2007), onde aparecem componentes como: "*File, Network Topology, Switch Manager, Route Computation*", cujos nomes deixam antever as funções que cada um deles desempenha na gestão da rede.

Os componentes não precisam estar localizados no mesmo computador, podendo funcionar como controladora distribuída. Pela componente de autenticação passa todo o tráfego não autenticado, autenticando utilizadores e PCS com as credenciais conhecidas na Base de Dados. Após autenticados, a controladora mantém registo sobre a porta do switch onde cada um deles está ligado à rede e aplica-lhes as respetivas políticas empresariais. O cálculo da rota utiliza o conhecimento acerca da topologia da rede para orientar o fluxo. A topologia é mantida pelo *Local Switch Manager*, recebendo as atualizações das ligações existentes a partir dos switches.

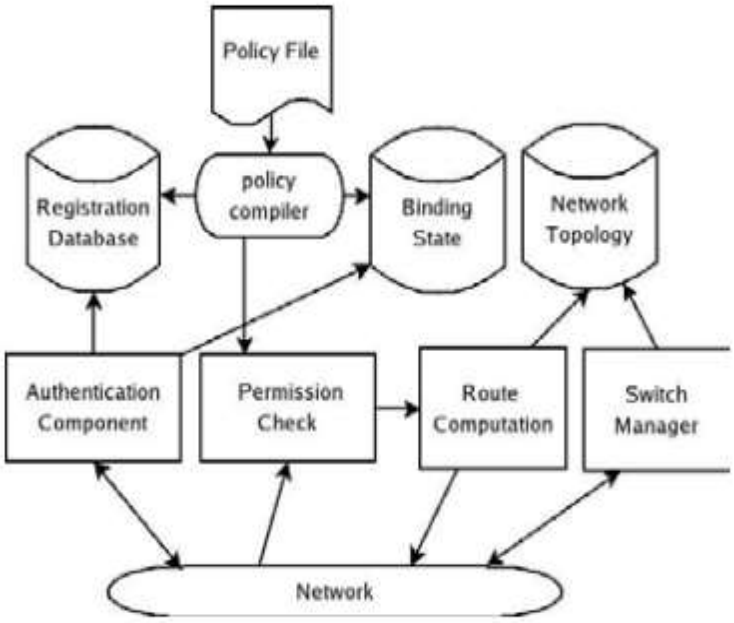

Figura 4 - Controladora ETHANE (Casado et al, 2007)

Mais funcionalidades e atribuições da controladora ETHANE podem ser consultadas em detalhe no documento original (Casado et al,2007, 10-18).

2.3.SDN

Os princípios e as regras do que se viria a designar por SDN surgem após a apresentação do ETHANE, como um novo paradigma e uma nova forma de abordar a gestão das redes. Procura-se uma nova abordagem para a administração da rede, em que o controlo é dissociado da função de transmissão da informação ou da arquitetura utilizada na infraestrutura. O papel que a controladora ETHANE representa, como dispositivo distribuído, corresponde a um elemento pertencente a um conjunto formado por várias controladoras ou aplicações distribuídas pela arquitetura, em que cada uma é responsável pelo controlo e gestão da rede que lhe compete, enquanto o todo implementa a arquitetura de gestão e administração global da rede. A divisão da infraestrutura em domínios de administração é uma função que surge cada vez que se implementam arquiteturas ETHANE.

A SDN é uma arquitetura emergente, dinâmica e adaptável que favorece arquiteturas físicas de rede em que a largura de banda é uma exigência constante pela natureza dinâmica das aplicações atuais SDN (ONF, 2016). Como caraterísticas fundamentais desta arquitetura a ONF elenca:

- **Diretamente programável** – o controlo de rede é diretamente programável pelos administradores. Permite configurar, gerir, proteger e otimizar os recursos da rede através de programas e normas SDN, sem a necessidade de acrescentar nenhuma licença do proprietário dos ativos de rede;

- **Ágil** – porque permite aos administradores ajustar o tráfego da rede de forma a adaptá-lo às necessidades da mudança;
- **Centralmente gerida** – a inteligência lógica da rede é centralizada nos controladores baseados em *software*, que mantêm uma visão global da rede;
- ***Open standards* independentes do fabricante** – como é implementada através de padrões abertos de *software*, a SDN pode vir a simplificar em muito a administração e operação da rede. As instruções são fornecidas pelos controladores de SDN em vez de dispositivos ou protocolos, específicos de fornecedores.

As tecnologias de rede existentes nem sempre suprem as exigências das empresas, muitas vezes devido à sua complexidade e à quantidade de protocolos utilizados. O desenvolvimento de soluções à medida, de forma isolada, pode dificultar ainda mais porque os grandes fabricantes dos componentes da infraestrutura utilizam protocolos proprietários. A dificuldade é maior quando existe a necessidade de escalar a rede e adicionar mais dispositivos, porque a interoperabilidade entre os dispositivos existentes e os novos que se adquirem é mínima. Novas aplicações de gestão e utilização de instalações podem ser um processo lento, e até inviabilizar a implantação de novas tecnologias nas arquiteturas de rede existentes. Os administradores e investigadores da área de redes testam soluções e ideias mas os *routers* e *switches* existentes no mercado possuem protocolos fechados e com *software* pertencente às empresas fabricantes. Testar soluções em ambientes de produção é inaceitável para as empresas pelas mais diversas razões.

Ao conseguir a separação entre o nível de controlo e nível de dados, a SDN permite que existam em simultâneo *routers* e *switches* com as regras da nova arquitetura e das arquiteturas existentes, tal como se de um verdadeiro laboratório se tratasse, não violando as regras de reencaminhamento e sem causar problemas de funcionamento das redes já em produção. Para dar resposta e apoio ao desenvolvimento da SDN foi criada, em 2011, uma organização sem fins lucrativos, apoiada por algumas empresas de dimensão global, em que se destacam a Nicira, Big Switch Networks, Google, Facebook, Verizon, Deustsche Telekom e Microsoft. Esta organização, denominada "*Open Networking Foundation"* (ONF), é uma organização orientada para o utilizador e dedicada à promoção, adoção e implementação de SDN por meio de padrões abertos, que são necessários para mover a indústria de *networking* para a frente dessas normas, atendendo às necessidades dos clientes." A ONF desenvolveu o protocolo OpenFlow de comunicação padrão, independente de vendedor, que implementa as regras da SDN. Esta organização foi a primeira a definir a SDN (ONF 2016):

"*The physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices*", ou seja, a separação física da camada de controlo de rede, da camada de reencaminhamento, e onde o plano de controlo tem a capacidade de controlar vários dispositivos. Uma arquitetura dinâmica, programável, controlável e cujo custo-benefício seja favorável à sua implementação. Implementar a SDN por meio de um padrão aberto permite reduzir os custos operacionais e desenvolver os

serviços, ao mesmo tempo que liberta os administradores de rede para integrar a restante tecnologia à medida que é desenvolvida (ONF 2016).

Mais tarde a ONF veio a ser apoiada no desenvolvimento desta arquitetura por outras grandes organizações na área de redes e sistemas de informação, das quais se destacam a Citrix, Cisco, Dell, HP, F5 Networks, IBM, NEC, Huawei, Juniper Networks, Oracle and VMware. Na página da ONF podem ser encontradas grupos de empresas que apoiam o desenvolvimento da SDN. Em junho de 2014 eram já mais de 150 empresas em que 24 delas eram especificamente dedicadas às tecnologias SDN (Quintero et al, IBM 2015, 725).

A virtualização com a sua exigência de processamento e a utilização de algoritmos mais rápidos exige eficiência e rapidez por parte da rede. A mobilidade exige políticas de manuseamento e segurança da informação a uma escala nunca antes vista. A evolução das arquiteturas de redes tem que satisfazer a complexidade das exigências dos dados, utilizadores e serviços, sem nunca esquecer o controlo da informação. Cada vez mais se sente a necessidade de orientar o tráfego específico que aumenta de uma forma exponencial. Aumentar sempre e cada vez mais a capacidade física da rede não é solução porque se torna demasiado cara. Em alternativa pode pensar-se numa solução que adapte a rede às necessidades do tráfego sem necessidade de intervenção em todos os equipamentos. É aqui que o método programático das arquiteturas de redes SDN se torna fundamental, permitindo o controlo e alteração do funcionamento da rede. Os administradores da rede podem programá-la de forma a cumprir os seus objetivos de negócio. Por exemplo, quando determinado fluxo na rede necessita de uma restrição de segurança, o próprio profissional poderá implementar esse requisito sem ter de esperar uma solução do fabricante. As empresas com maiores dimensões e com estruturas de rede próprias, assim como gestão e administração própria, tornam-se mais independentes dos fornecedores da estrutura e dos serviços, sem nunca menosprezar a vantagem de associação a esses profissionais.

As necessidades de manuseamento de informação têm forçado, na última década, as arquiteturas de rede tradicionais aos seus limites. O aumento de processamento exponencial para satisfazer as necessidades da mobilidade, virtualização, *Internet of Things* (IoT) e computação na nuvem exigem, da rede e dos seus administradores, a execução de tarefas cada vez mais complexas. Alguns fabricantes criaram soluções em tudo idênticas às preconizadas pela ONF, para manter as suas estruturas e equipamentos em funcionamento. É o caso da CISCO, NICIRA e VMWare que tem aproximações à SDN diferentes.

- A Cisco desenvolveu uma estratégia SDN que integrou numa solução em que apela a programação aberta de rede da camada de transporte por todo o caminho até às camadas de aplicação. A solução SDN Cisco será apresentada em pormenor no Capítulo 3.6.3;
- A IBM, embora não desenvolva uma solução SDN completa, está envolvida em várias soluções através de parcerias com várias empresas (Citrix, Juniper Networks, PaloAlto Networks e Plexxi) na conceção de soluções em quase todas as áreas de WAN Networking (balanceamento, segurança, reencaminhamento e otimização de

recursos. Abordaremos estas soluções sumariamente no capítulo 3.6.5. (IBM 2016, August 15);

- A NICIRA resolveu retirar a virtualização de rede nos controladores que interagiam diretamente com *routers* e *switches* que utilizavam o protocolo OpenFlow – protocolo da camada de infraestrutura da SDN. A sua função será analisada em pormenor no capítulo 2.4. No entanto a empresa destacou que o OpenFlow iria ser substituído por um protocolo proprietário que faria o mesmo trabalho sem que os clientes notassem a diferença, ou seja, pormenores de fabricante e compatibilidade com padrões;
- A VMWare, proprietária da vSpfere, que tem um mercado significativo no campo da virtualização, aposta na virtualização de todo o centro de dados. Na tentativa da obtenção de algo para atingir este objetivo, tomou como evolução normal a criação de protocolos e *software* proprietário. A maioria dos seus conceitos de virtualização de rede, e algumas das noções de SDN, são aplicáveis em toda a rede, computação, armazenamento e segurança;
- A HP desenvolveu o *HPE SDN solutions* que pretende ser uma solução completa de SDN. Para melhor completar a solução, a HP estabeleceu uma parceria com a VMWare em 2014, que, entretanto, tinha adquirido a NICIRA. Este consórcio tornou-se num dos primeiros e maiores fornecedores de serviços SDN em larga escala. A solução SDN das duas últimas empresas citadas irá ser apresentada no Capítulo 3.6.4.

Todas as organizações acima referenciadas estiveram ativamente envolvidas no desenvolvimento do OpenFlow e normas SDN através do *Open Research Center Networking* e da ONF, o que significa que todos sabem que a mudança de arquitetura e protocolos é demasiado importante e, por isso, desenvolveram alterações do protocolo OpenFlow ou protocolos equivalentes nos seus equipamentos.

2.4. OpenFlow

O protocolo OpenFlow foi desenvolvido pela ONF, para criar uma camada de abstração da infraestrutura de rede que permita executar as tarefas de gestão da rede nas camadas de infraestrutura e abstraindo totalmente o *firmware* e o *software* do fabricante. É considerado o primeiro protocolo padrão SDN, permitindo que a controladora SDN possa interagir diretamente com o plano de encaminhamento de dispositivos de *routers* e *switches*, tanto físicos como virtuais, facilitando a adaptação da arquitetura e das dinâmicas de gestão da rede.

As tendências que estão a alavancar o novo paradigma de arquitetura de gestão e administração da rede IP e que requerem a necessidade das tecnologias e metodologias SDN incluem (ONF, 2016):

- A mudança dos padrões de tráfego – tradicionalmente as aplicações servem-se da informação nas bases de dados geograficamente distribuídas e através da nova

tecnologia de computação em nuvem. Este paradigma recente e ainda em expansão necessita de largura de banda à medida mas, essencialmente, o que possibilita o funcionamento é a capacidade de gestão de tráfego à medida. A cada um as suas necessidades em cada momento é um lema que só pôde ser seguido depois da mobilidade passar a ser gerida por *software*;

- A necessidade permanente de consumir TI – em todo o lado e utilizando o seu próprio dispositivo é uma tendência cada vez mais alargada e que requer que as redes sejam flexíveis e seguras de forma a dar confiança a utilizadores e prestadores de serviços *Bring Your Own Device* (BYOD);
- O aumento de serviços na nuvem – os utilizadores esperam ter acesso à infraestrutura e outros recursos de Tecnologias de Informação (TI) - empresariais de forma imediata e segura para as suas aplicações;
- Mais necessidade de dados, maior largura de banda – a manipulação de conjuntos de dados de hoje exige muito processamento para uma constante satisfação do cliente, quer seja para ligações dedicadas, quer para as referidas capacidades adicionais de conectividade e tráfego à medida.

A pensar nestas exigências, os arquitetos das redes SDN quiseram satisfazer os requisitos de rede colocados pela evolução das necessidades, de maneira a que a infraestrutura da rede se mantenha confiável mesmo quando escalada e que não aumente o grau de complexidade da gestão. Melhorar os aspetos da convergência que aparece sempre como algo que altera o funcionamento da rede sempre que são realizadas alterações de configurações de equipamentos. Quer seja na convergência de *switching* ou de *routing* existem momentos de verdadeiro desespero para os administradores, muitas vezes por problemas não identificados na convergência da rede. Estas razões condicionam a administração e funcionamento das arquiteturas das redes tradicionais (Faughnan, 2016):

- Complexidade que leva a erros - a falta de capacidade para fazer cumprir a aplicação de políticas de segurança em toda a rede. Falta de capacidade para adicionar componentes móveis e aplicacionais, sem ser com processos muito demorados e complexos e que levavam normalmente a interrupções do serviço, desencorajando as mudanças na rede. Estas alterações eram, na maioria das vezes, realizadas de forma manual;
- Incapacidade para escalar - a abordagem à escalabilidade estava condicionada pelo tempo da ligação e não cumpria as funções básicas para a execução dos padrões de tráfego dinâmicos nas redes. Os fornecedores dos serviços ficavam portanto sem capacidade para escalar o processamento dos algoritmos necessários em larga escala.
- Dependência do fornecedor – existência de equipamentos de fornecedores específicos com falta de padrão a nível protocolar e de interfaces, limitando a capacidade dos operadores para se adaptarem aos seus ambientes individuais.

Estas limitações viriam a ser resolvidas pela nova metodologia e arquitetura a implementar, seguindo as regras da SDN. Esta metodologia levou à criação do protocolo

OpenFlow, um protocolo padrão de código aberto e que como ficou dito permite criar uma camada de abstração da infraestrutura de rede para que se possa executar as tarefas de gestão da rede, abstraindo totalmente o *firmware* e o *software* do fabricante.

Tanto o OpenFlow como as regras da SDN são resultado de anos de pesquisa e colaboração entre as Universidades de Stanford e de Berkeley com a ONF. Ainda que os equipamentos ativos sejam comercializados com *software* proprietário, este protocolo permite serviços de configuração sem a necessidade de aceder diretamente a cada um dos *routers* e *switches*. O protocolo OpenFlow destaca-se porque permite acesso direto a manipulação das tabelas de encaminhamento dos equipamentos ativos, sejam eles físicos ou virtuais. Os *routers* e *switches* que suportam OpenFlow registam as estatísticas de tráfego IP nos interfaces onde o Openflow está configurado e exportam-nas. Este conteúdo é entregue a um servidor aplicacional, para que seja feita a análise de tráfego em tempo real.

As tecnologias SDN usam o OpenFlow para poderem manipular a largura de banda de forma dinâmica, através de aplicações, adaptando as redes às diferentes necessidades do negócio que vão surgindo, reduzindo a complexidade da gestão e da administração da rede. A construção de soluções SDN passa pelo uso do protocolo OpenFlow como ferramenta central da interação entre os níveis mais baixos da arquitetura, permitindo visualizar o funcionamento global da arquitetura de rede. Segundo a ONF, a SDN irá conduzir-nos para o futuro das tecnologias de informação.

A ***Figura 5*** apresenta o *framework* que a *Open Network Foundation* criou para a utilização e implementação do protocolo OpenFlow. Sendo este esquema o esquema de abstração da arquitetura SDN, este releva a posição onde o protocolo se encaixa no *framework* e onde realiza o seu trabalho.

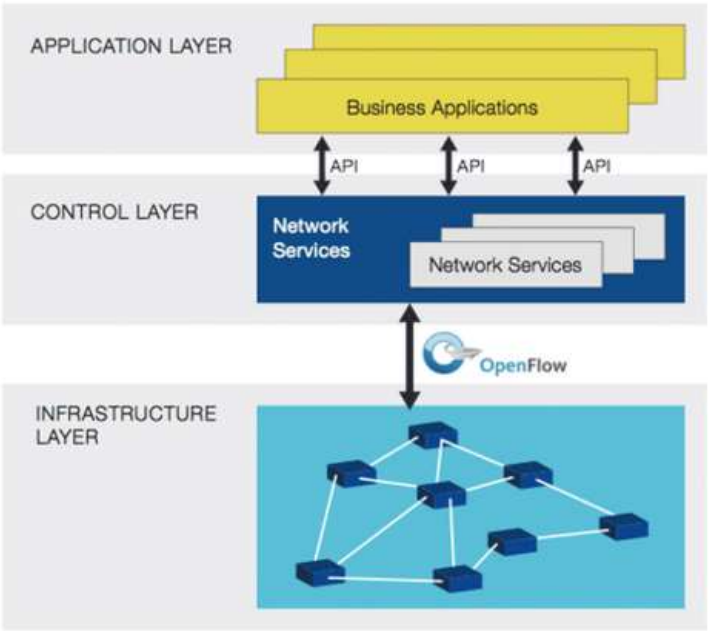

Figura 5 - OpenFlow na arquitetura SDN (ONF, 2016)

Cada uma das camadas é uma abstração da infraestrutura da rede, não importando qual é o sistema operativo, o equipamento ou o fabricante. Na sua arquitetura de funcionamento o *framework* divide-se em três níveis - Aplicação, Controlo e Infraestrutura, em que as funções e cada um deles pode ser resumida da seguinte forma (ONF, 2016):

- **Nível de aplicação** (*application layer*) – este nível permite aos clientes SDN a programação da rede de forma a permitir diferenciação, inovando e acelerando as funcionalidades dos serviços. Esta programação pode ser feita através de *Application Programming Interface* (API), *scripts*, ou outro qualquer ambiente que em termos de *software* permita ao cliente utilizar rotinas e padrões estabelecidos para a gestão e administração da rede sem se envolver muito em detalhes técnicos ou de implementação, quer de *software* quer de serviços. Na documentação da ONF também é referido muitas vezes como pelo "*northbound interface"* da arquitetura, exatamente porque em termos de posição geográfica se encontra localizado acima da controladora;
- **Nível de controlo** (*control layer*) – é o nível central de inteligência e controlo da rede. Está dissociado da quantidade de elementos que controla ou do desempenho de cada um deles. O papel fundamental é o de simplificar e otimizar o desempenho da rede no encaminhamento dos pacotes. As políticas da empresa determinam a gestão e operação deste nível. A função de controlo de rede pode estar fisicamente distribuída, mas é logicamente centralizada. As funções alojadas na controladora exercem o controlo programático direto no comportamento do tráfego e reencaminhamento do mesmo. Conhece a topologia lógica da rede, influencia o seu desempenho e configura as alterações;
- **Nível de infraestrutura** (*infrastructure layer*) – como o nome indica é o interface através do qual se faz a entrada de unidades externas à arquitetura. Pode conter elementos físicos e virtuais. É um nível de abstração que junta e separa ***hardware*** (elementos de rede a serem geridos e que originam e recebem tráfego), e de ***software*** **(**serviços de rede e configurações como OpenFlow, SNMP, *firewalls, load-balancers ou* qualquer outra ferramenta que implemente controlo ou outras tarefas associadas à gestão e funções da rede. Podem ser usadas configurações físicas e lógicas neste nível da arquitetura. Na documentação da ONF também é referido muitas vezes como "*southbound interface"* da arquitetura, exatamente porque em termos de posição geográfica se encontra localizado abaixo da controladora.

Como se pode ver pelo *framework* SDN, o protocolo OpenFlow funciona como uma camada de abstração entre o nível de controlo e o nível de infraestrutura. Altera o *design* da arquitetura de gestão da rede abstraindo uma parte dos modelos de estudo das redes, como são o caso do modelo *Open Systems Interconnection* (OSI) e do modelo *Transmission Control Protocol* /*Internet Protocol* (TCP/IP). Estes são os modelos utilizados para estudo e implementação das redes tradicionais durante várias décadas. O primeiro foi desenvolvido na década de 70 do século passado, mas só foi formalizado em 1983. É o modelo de estudo mais conhecido e pretende ser um modelo *standard* para protocolos de comunicação entre

os mais diversos sistemas. Composto por sete níveis em que cada um deles implementa uma funcionalidade da rede através de um nível de abstração. Os níveis do modelo OSI são:

- Físico - define especificações elétricas e físicas dos dispositivos;
- Ligação de Dados - deteta e corrige erros que possam acontecer no nível físico;
- Rede - fornece os meios funcionais e de procedimento de transferência dados; roteamento de funções;
- Transporte - proporciona um serviço de transporte dos dados que se retende eficiente, confiável e de baixo custo;
- Sessão - responsável pela troca de dados e a comunicação entre *hosts;*
- Apresentação - converte o formato dos dados vindos do nível de sessão para o nível de Aplicação e vice-versa;
- Aplicação - camada correspondente aos programas e aplicações que o utilizador desencadeia.

O segundo modelo conhecido por TCP/IP, ou modelo de internet, é o mais utilizado em implementações de arquiteturas de rede. Devido ao crescimento explosivo de redes foi necessário que a *International Organization for Standardization* (ISO) encontrasse um modelo único de implementação de redes a nível mundial. Este modelo já era utilizado pelo Departamento de Defesa dos Estados Unidos e várias vezes testado. É um modelo diferente do modelo OSI e mais simplificado pois possui apenas 4 níveis ou camadas.

- Aplicação – que substitui as camadas 5,6 e 7 do modelo OSI criando algumas abstrações.
- Transporte – proporciona um serviço de transporte dos dados que se retende eficiente, confiável e de baixo custo; equivalente ao mesmo nível no modelo OSI.
- Internet – desempenhas as funções da camada de rede
- Acesso à rede – substitui em funções as camadas de ligação de dados e física.

Figura 6 - Comparação de modelos OSI e TCP/IP

A ***Figura 6*** apresenta uma comparação gráfica entre os modelos de implementação de redes tradicionais referidos anteriormente. Como se verificou, existem diferenças fundamentais entre os modelos apresentados e o modelo SDN, discutido ao longo de todo o

documento e, em particular, neste capítulo. No modelo de gestão SDN a infraestrutura engloba os níveis 1 a 3 do modelo OSI, em que a controladora corresponde a uma abstração que passa a envolver o controlo da rede e da informação entre níveis 2 e 6 do mesmo modelo. Desta forma, as funções de administração da rede passam a estar redefinidas, mudando para as camadas de aplicação e de controlo do modelo SDN funções específicas de várias camadas do modelo OSI.

Para operar nos níveis das necessidades de telecomunicações tradicionais são necessários conhecimentos muito específicos e que exigem recursos humanos altamente especializados. Esta dificuldade torna-se ainda mais evidente quando se utiliza equipamentos de fabricantes diferentes. A infraestrutura SDN é semelhante à infraestrutura duma rede tradicional, composta por um conjunto de equipamentos de rede (*routers e switches*), com a diferença que estes elementos são apenas utilizados para o encaminhamento do tráfego cabendo ao *software* de controlo tomar as decisões. A inteligência de rede é removida dos dispositivos da infraestrutura e centralizado logicamente no sistema de controlo – a controladora SDN.

Implementar uma arquitetura SDN também não é trivial e exige a necessidade dum conhecimento detalhado da estrutura física e lógica existente. A implementação de mecanismos como *tunneling*, *routing*, *load-balancing* e outras caraterísticas típicas das novas arquiteturas de rede, parecem ter muito a ganhar com a implementação da SDN. As regras de reencaminhamento de um *switch* ou *router* da rede, quando necessário, podem ser prioritizadas ou bloqueadas por um nível de controlo baseado em *software* externo e num ambiente mais amigável. Esta zona da comunicação está em desenvolvimento e é ainda muito cedo para que possa ser associada a protocolos ou fabricantes específicos. Analisar o desempenho de uma topologia ou de uma determinada arquitetura de rede requer conhecimento da infraestrutura e isso pode ser muito difícil para um analista externo. No entanto, com uma camada de abstração como OpenFlow implementado por *software* pode tornar este trabalho mais fácil. Uma outra forma de resolver esta situação pode consistir na utilização de uma API do cliente ou de um ISP.

2.5. Interfaces Northbound vs Southbound

Sem dúvida alguma que o componente fundamental da arquitetura SDN é o sistema inteligente que agrega os sistemas de controlo, ou seja, a controladora SDN. Podemos olhar para este componente como o controlo da rede que abstrai a infraestrutura da arquitetura tradicional e permite a aplicação das políticas de gestão e segurança a um nível global, mas que precisa de interfaces de ligações à rede. Quer se trate de uma só controladora ou de uma controladora distribuída, existem dois conceitos que devemos ter presente quando falamos de interfaces de comunicação da controladora com o resto da arquitetura.

A designação de um interface Norte (*northbound*) dá-se a um qualquer interface da rede que comunica com um outro componente de nível mais elevado, por outro lado um interface Sul (*southbound*) corresponde a um interface que comunica com um componente de um nível inferior. Num sentido mais amplo, pode dizer-se que se o fluxo está acima do componente é fluxo norte e logo northbound, se o fluxo está abaixo do componente então é

fluxo sul e, portanto, *southbound*. Embora estes conceitos sejam aplicados a todo o tipo de componentes, redes e arquiteturas, ultimamente têm sido mais utilizados na arquitetura de redes definidas por *software*.

Segundo a ONF, associa-se duma maneira mais natural *southbound interface* às especificações que têm a ver com o protocolo OpenFlow e que permitem a comunicação entre a controladora SDN e os nós de rede da infraestrutura. Este interface, além de fornecer uma ligação entre os elementos do controlo e a funcionalidade dos dados, simultaneamente fornece uma separação entre eles. É aqui que se fornece a informação sobre o fluxo de informação para a controladora SDN, que permite a utilização de estatísticas de tráfego.

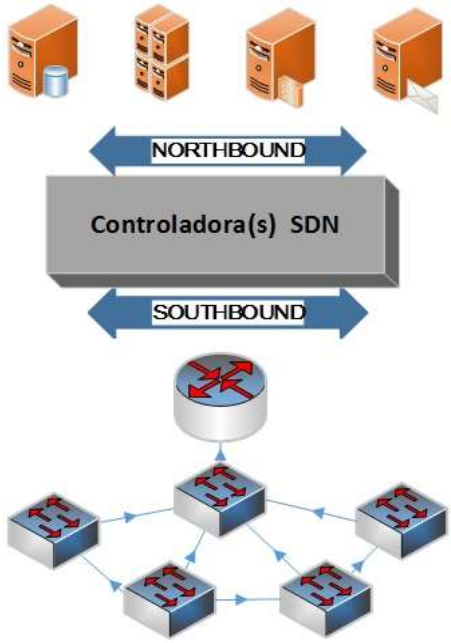

Figura 7 - Interfaces *Northbound vs Southbound* (baseado na definição ONF)

Por outro lado, associa-se *northbound interface* à comunicação entre a controladora e as APIs de *software* que funcionam na zona de comunicação aplicacional. Neste momento, parece ser demasiado cedo para definir uma interface *northbound* padrão. Existem demasiados trabalhos a ser desenvolvidos e muitas aplicações para testar e demonstrar sem certezas do caminho que o desenvolvimento da SDN tomará (Ramos et al, 2015, pp 3).

2.6. OpenFlow em funcionamento

Descrever as especificações e arquiteturas SDN pode ser demasiado abstrato. As arquiteturas OpenFlow e SDN confundem-se pela forma como nasceram e cresceram em conjunto, porque, na realidade, neste estágio atual de desenvolvimento desta tecnologia, o Open SDN apenas existe em *southbound interface*. O protocolo OpenFlow é o *standard* vigente no funcionamento dos dois níveis inferiores da arquitetura, os níveis de controlo e infraestrutura. Já a relação entre os dois níveis superiores, nível de aplicação e nível de

controlo, apresenta maiores alterações porque as aplicações utilizadas são desenvolvidas à medida do cliente pelos programadores do lado do cliente face às necessidades de cada um. Estas especificidades são, por vezes, tão diferentes que transformam as arquiteturas utilizadas, acabando por necessitar de licenças ou especificidades típicas que só os proprietários possuem.

Para exemplificarmos o funcionamento da arquitetura SDN, apresentamos uma pequena análise do funcionamento do protocolo OpenFlow, numa rede real e comunicação entre os dois níveis inferiores. Neste caso tomamos, por exemplo, uma pequena arquitetura de rede composta por quatro computadores, um *switch* e uma controladora. A controladora C0, como foi dito na seção 2.2 é desempenhado por um servidor munido de *software* específico para o efeito. O *switch* S1 é um componente certificado OpenFlow e os elementos H1 a H4 são computadores ligados em rede. É importante mais uma vez reforçar que se trata de uma arquitetura OpenFlow e recapitulando:

- C0 - Controladora de *software* OpenFlow
- S1- *switch* OpenFlow
- H1- H4 – *hosts* em comunicação

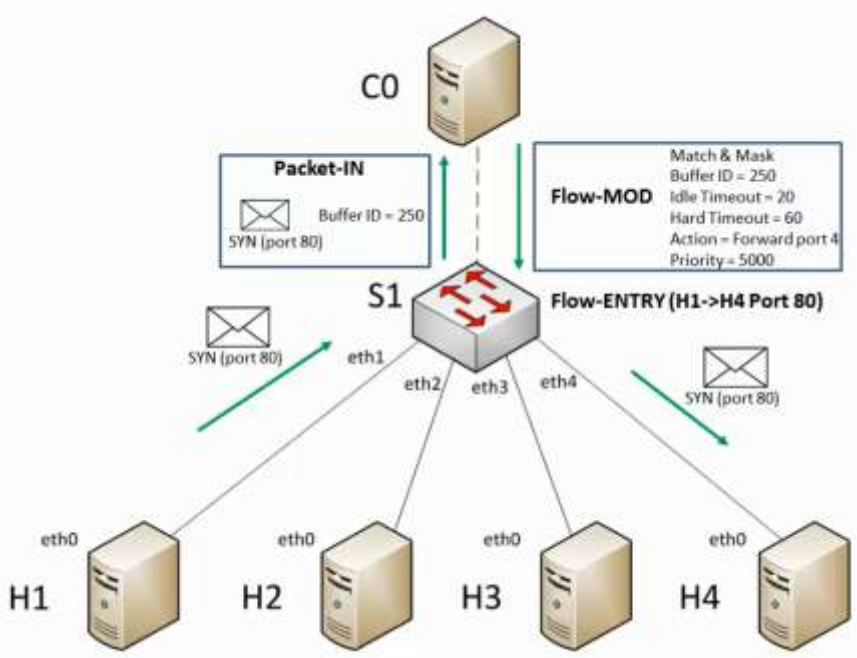

Figura 8 - OpenFlow, início de fluxo de informação

Quando é desencadeado um pedido *http (TCP port 80)* a partir do host H1 é iniciado um novo fluxo de informação. Como S1 não possui na tabela *Flow Information Base* (FIB) informação sobre este tráfego envia o pacote à controladora C0. Se a controladora tiver nas suas regras de funcionamento a informação do que fazer age de acordo, senão cria um *buffer*

com ID=250 e um FLOW-MOD com toda a informação acerca do que fazer com tráfego deste tipo e reenvia a S1. A controladora alimenta o *buffer* id=250 com os seguintes campos:

- *Action* = O que fazer com o pacote de dados (*Forward port 4*)
- *Idle Timeout* = Tempo, em segundos, que a entrada se manterá na tabela FIB sem tráfego
- *Hard Timeout* = Tempo máximo, em segundos, que a entrada se manterá na tabela FIB
- *Priority* = Ordem de prioridade da entrada na tabela FIB

A partir do momento em que exista a entrada H1→H4 na tabela, o *switch* deixa de consultar a controladora C0 e envia o tráfego diretamente.

A criação da entrada na tabela de acordo com a ação especificada pela controladora é normalmente iniciada pelo envio do pacote HTTP *request* SYN. A entrada na tabela FIB H4→H1 será construída na mesma tabela pelo HTTP *response* SYN ACK. Estes são os primeiros pacotes iniciais da especificação de abertura de comunicação em TCP. A partir deste momento passa a existir na arquitetura uma regra de retorno, que está exemplificada na ***Figura 9***. O fluxo de informação entre H1 e H4 será concretizado com recurso a estas regras.

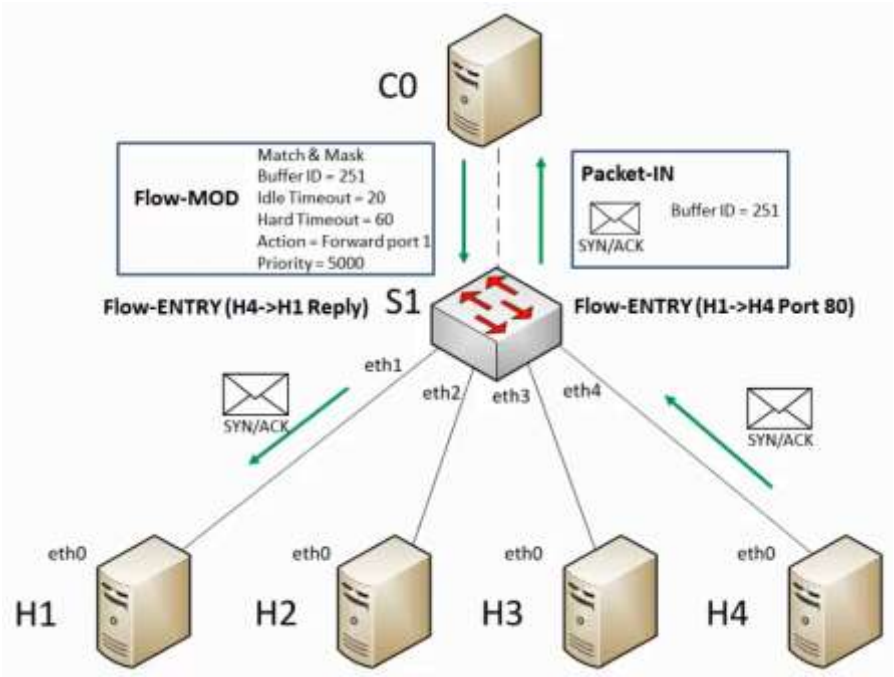

Figura 9 - OpenFlow, criação de fluxo de retorno

Esta é apenas um pequeno exemplo serve para ilustrar o funcionamento do OpenFlow. Num *switch* tradicional este trabalho seria executado por si próprio na consulta ou atualização das tabelas MAC e ARP. Se H1 e H4 estivessem em redes diferentes, haveria a utilização do protocolo e das tabelas de *routing*. A comunicação seria mais lenta, não só porque o *switch*

teria de consultar ou atualizar duas ou mais tabelas, mas também porque teria que desencadear dois ou mais subprocessos, um para cada protocolo.

2.7. SDN no Centro de Dados

O Centro de Dados (CD) ou Centro de Processamento de Dados (CPD), como também é conhecido, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e equipamentos ativos de rede, como *switches* e *routers*. Albergando centenas de servidores para fornecimento à rede dos mais variados serviços, processando grandes quantidades de informação e fornecendo acesso a milhares de utilizadores, os servidores e equipamentos de rede do centro de dados, normalmente instalados em bastidores metálicos e montados em pilha (*rack)*, são o suporte da informação das organizações e, portanto, centros nevrálgicos das grandes empresas. Por essas razões requerem instalações com proteção contra incêndios e sistemas de refrigeração tecnicamente avançados, para manter o ambiente com uma temperatura estável e dentro dos parâmetros de operação dos aparelhos. São espaços fundamentais para a continuidade do negócio em vários setores económicos em que a segurança física é implementada de forma a fazer cumprir normas rigorosas de acesso e permanência. Setores como a banca, a saúde, as telecomunicações, a energia, os transportes ou o setor militar possuem CD nestas condições de que depende em grande parte o seu normal funcionamento. A ***Figura 10*** mostra um exemplo de bastidores de *rack* num centro de dados da Cisco.

Figura 10 - Conjunto de bastidores de *rack* num CD (Cisco)

Se pensarmos na utilização das tecnologias SDN num CD, nomeadamente na sua capacidade para interagir com a rede e servidores através de *software* aberto, podemos imediatamente pensar na racionalização do controlo de serviços servidor-servidor ou servidor-memória. Uma aplicação de controlo de servidores pode controlar estes serviços em vários servidores independentemente do fabricante. As organizações estão sempre a criar novas aplicações virtualizadas, que requerem vastos recursos de memória, processamento e rede. O seu controlo através das ferramentas do sistema não é óbvio nem trivial, já que requerem a ligação permanente aos servidores. A utilização de SDN, através de

controladoras de *software,* que permitam ter uma abrangência total do controlo das aplicações, pode ser considerada importante para a correta gestão do centro, sobretudo na forma como a nova arquitetura permite o controlo do impacto que o crescente número de aplicações têm na utilização da rede. Uma vez que o número de aplicações virtualizadas continua a crescer, aumentam as necessidades de gestão e administração da rede e das aplicações. A necessidade de transitar a administração para tecnologias SDN parece ser evidente tanto por razões de custo como por disponibilidade de recursos (Cisco 2016, September 6).

A preocupação das organizações é fornecer serviços de qualidade sem correr o risco de perder o acesso aos dados durante a transição. A infraestrutura de rede deve primeiro garantir a continuidade no funcionamento dos serviços atuais e, de seguida, suportar o desenvolvimento crescente nas áreas de mobilidade e transação de dados. A virtualização das funções de rede é uma abordagem que foi implementada com sucesso em centros de dados pela VMWare com a virtualização de *switches* de topo através dos novos recursos do *Virtual Distributed Switch* (VDS). Os prestadores de serviços tentam agora ser mais ágeis e flexíveis nos serviços aos clientes alterando os seus modelos económicos. A SDN associada à virtualização pode influenciar estes modelos reduzindo os recursos de *software* e *hardware* de gestão da rede nos centros de dados. Também na segurança e correção a falhas o modelo pode ser muito importante, já que por serem importantes pontos de prestação de serviços, se tornam pontos críticos de falhas. Se a solução, de momento, parece ser manter os equipamentos de rede na última geração de *hardware* de forma a colmatar as falhas que o *software* não resolve, com a implementação de arquiteturas SDN, os prestadores de serviços resolvem as enormes exigências que a explosão de necessidades impostas com a chegada da mobilidade, vídeo, *big-data* e a panóplia de aplicações baseadas nos serviços da nuvem. A necessidade essencial é prover a estrutura do centro de dados com a capacidade de virtualizar melhores e mais rápidos equipamentos físicos, quer em termos de rede, quer em termos de processamento e memória. Só após estas necessidades satisfeitas começa o investimento em virtualização a ser recuperado.

2.8.SDN na Computação em Nuvem

O conceito de computação em nuvem (em inglês, *cloud computing*) refere-se a um modelo que permite acesso conveniente e em simultâneo em rede partilhada a um conjunto de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente fornecidos e com um esforço de gestão mínimo e sem interação do provedor de serviço (NIST 2016). A ***Figura 11*** representa um esquema básico duma arquitetura de programação em nuvem e foi retirada da página da internet da Cisco.

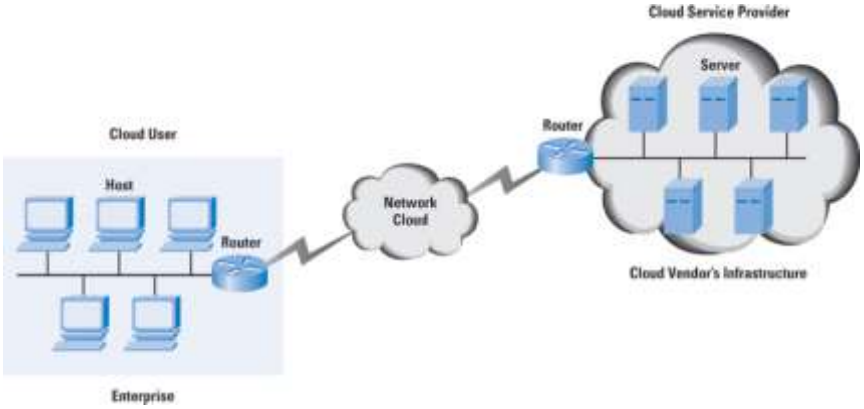

Figura 11 - Esquema funcional da computação em nuvem (Cisco)

Embora não esteja no âmbito deste trabalho fazer uma análise profunda do modelo de computação em nuvem, para que tenhamos um melhor entendimento dos termos utilizados apresentamos as definições do *National Institute of Standards and Technology* (NIST). É um instituto americano responsável por desenvolver padrões e boas práticas para fornecer inovação e competitividade às tecnologias e segurança da informação. Segundo a definição daquele instituto, o serviço de computação em nuvem deve ser composto por:

- Cinco caraterísticas essenciais (*self-service* à medida, amplo acesso à rede, acesso a um conjunto alargado de serviços, rápida escalabilidade e elasticidade e capacidade para medir e controlar os recursos consumidos);
- Três modelos de fornecimento de serviços (o *software* como um serviço, *Software as a Service* (SaaS), a plataforma como serviço, *Plataform as Service* (PaaS) e infraestrutura como serviço, *Infrastructure as a Service* (IaaS);
- Quatro modelos de implementação (nuvem privada, nuvem comunitária, nuvem pública e nuvem híbrida).

Do ponto de vista de infraestrutura, a computação em nuvem é muito semelhante aos serviços que os fornecedores dos serviços de internet *Internet Service Providers* (ISP) vêm fornecendo ao longo dos anos. Nos serviços, servidores, armazenamento e infraestrutura de rede são compartilhados entre vários clientes e utilizadores. A ligação remota através de serviços de rede também é escalável, mas esta capacidade de redimensionamento pode ser feita através de telefone ou *e-mail* com o fornecedor dos serviços. A computação em nuvem é diferente na medida em que oferece um modelo rápido e automático de redimensionamento e em que o cliente só paga o que consome. Os recursos quando deixam de ser utilizados por um cliente ficam livres para serem alocados a outro que deles necessite. Curiosamente, alguns grupos de fornecedores e analistas dos serviços utilizam a computação em nuvem para hospedar os seus próprios serviços e mercados (Cisco *cloud* 2016).

Tanto a computação em nuvem como a comunicação nos CD, ganharam um avanço significativo quando um novo conceito chamado *Network Functions Virtualization* (NFV) foi apresentado por um consórcio da indústria de telecomunicações, o *European Telecommunications Standard Institute* (ETSI), numa conferência sobre a SDN em

Darmstad na Alemanha em 2012. O NFV propõe-se virtualizar diversos tipos de funções dos componentes da rede, desvinculando-as de vez de *hardware* dedicado. Este novo conceito e a SDN tornaram-se assim abordagens praticamente complementares e estão claramente relacionadas. Enquanto a SDN foi criada pelos investigadores, a NFV foi criada por um consórcio de fornecedores de serviços. Muitos fornecedores de serviços na nuvem estão ainda curiosos sobre a escalabilidade da arquitetura SDN e aguardam a evolução. Migrar a arquitetura para SDN ou adaptar a infraestrutura à utilização do OpenFlow representa uma grande mudança de paradigma para a maioria dos fornecedores e grandes clientes. Qualquer grande infraestrutura leva sempre muito tempo para se adaptar às mudanças. A mudança desencadeada na rede para a utilização de OpenFlow nos centros de dados, pode ter grande impacto na utilização dos novos paradigmas da mobilidade e virtualização, com os clientes a saírem beneficiados pela utilização destes serviços. A virtualização dos recursos já transformou em grande parte o centro de dados num centro de criação automático e flexível de servidores. Mas a rede e infraestrutura não cresceram a esse ritmo. A relação entre a rede e o centro de dados pode ficar a ganhar com a implementação da SDN.

3. Da Gestão das Redes Tradicionais à Gestão das Redes SDN

As redes de computadores são parte integrante da realidade de milhares de utilizadores e consequentemente utilizam milhares de equipamentos ativos de rede onde correm algumas dezenas de protocolos. Correm tanto protocolos padrão como protocolos proprietários do fabricante dos equipamentos e que neste caso são específicos das funcionalidades requeridas. Vistos à imagem do explicado pelo modelo OSI, os três níveis inferiores, físico, ligação de dados e rede, são as camadas que fornecem serviços às camadas superiores. É aqui que a administração da rede realiza a maior parte do seu trabalho, quer seja no redireccionamento e análise do tráfego, na segurança da rede e da informação ou na correção de erros. Os protocolos destas camadas são ferramentas de trabalho dos administradores da rede, na execução das funções atrás referidas. Protocolos de *routing* e *switching* são vários, alguns dependem da ação específica do fabricante para a sua configuração e implementação. Requerem para a sua configuração acesso local ou remoto aos equipamentos de rede. Este acesso pode ser feito através de protocolos como o *Simple Network Management Protocol* (SNMP), *Network Virtual Terminal* (NVT), vulgo telnet ou *Secure Shell* (SSH). Alguns fabricantes mantêm como principal ambiente de configuração a utilização de *Command Line Interface* (CLI), acompanhado ou não de menus de ajuda à decisão. Não podemos esquecer que se trata de sistemas operativos proprietários e que são feitos para soluções específicas, exigindo *hardware* dedicado para suportar muitas vezes protocolos igualmente proprietários. O fabricante justifica a sua utilização garantindo que o desempenho é superior aos *standards* equivalentes. A sua configuração e implementação exige conhecimento técnico específico, caso contrário a organização perde a capacidade de comando e controlo associada ao desempenho da sua estrutura de comunicações.

Sabemos que as redes de telecomunicações são o caminho preferencial para as principais fontes de informação, sejam elas fontes públicas, acedidas via internet ou fontes privadas acedidas através de meios de comunicação e armazenamento próprios da empresa. Tornaram-se, por estas e outras razões, demasiados importantes para que se possa deixar a sua administração e gestão ao acaso. Cresceram exponencialmente e em consequência do seu sucesso cresceram os problemas para manter a qualidade de serviço desejada nos serviços essenciais. Se o aumento de tráfego aparentava não ser um problema, passou a sê-lo com a utilização em massa do *stream* de vídeo e todas as tecnologias digitais em expansão de que ressalta a mobilidade. O serviço *Voice over Internet Protocol* (VoIP), serviço de telefone em que a transmissão é suportada pela rede de dados, cujo tráfego parece irrisório exige elevada qualidade de serviço para sinalização e controlo. Os utilizadores do telefone não vão utilizá-lo se tiverem que esperar segundos que o retorno da voz do interlocutor chegue. A conversa entre os interlocutores terá que decorrer como se de uma conversa presencial se tratasse. Para que isto aconteça é necessário a existência de uma funcional para as redes e serviços, que englobe a administração e configuração.

3.1.A arquitetura

A gestão das redes tradicionais está muito dependente do *hardware* utilizado. Dependendo da qualidade, que estará obviamente relacionada com o custo, os equipamentos podem apresentar baixa eficiência e estar sujeitas a erros que por vezes se tornam difíceis de identificar. O modelo de arquitetura de redes WAN, que acabou por ficar conhecido como o modelo Cisco e que divide a arquitetura em 3 níveis foi desenhado por aquela organização para implementação dos seus equipamentos e soluções:

- Acesso (*access*) – É a camada em que são ligados os dispositivos finais, aqui estão *switches* que interligam os computadores, servidores, câmaras IP, telefones IP, pontos de acesso de redes sem fios. *Access Points* (AP), ou outros equipamentos finais. É neste nível de acesso que se criam VLANs, para separação virtual da panóplia de redes e serviços das redes IP.
- Distribuição (*distribution*) – Liga os diversos edifícios e dispositivos da camada de acesso ao núcleo. É na camada de distribuição que é implementada políticas de segurança, normalmente através de ACLs. Neste nível começa o roteamento, porque os equipamentos aqui instalados suportam L3 do modelo OSI e fazem o roteamento entre VLANs ou *inter-vlan routing*, porque é mais conhecido pela designação em inglês.
- Núcleo (*core*) - O núcleo é a camada mais alta no modelo de 3 camadas. Como área central da arquitetura, é a preferencial para que se façam aqui as ligações entre grupos de redes ou o acesso à internet. Requer processamento elevado, alta disponibilidade, redundância e os melhores meios de comunicação. De forma a disponibilizar os serviços da rede rapidamente encontra-se ligado diretamente ao nível de distribuição via IP e liga as outras LANs. Não pode falhar ou toda a arquitetura entra em colapso.

A ***Figura 12*** representa o modelo de arquitetura Cisco de 3 camadas e foi retirada do *site* desta organização.

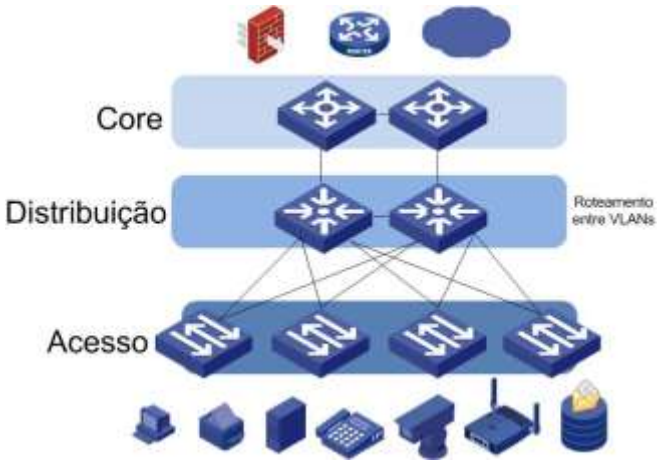

Figura 12 - Modelo de arquitetura de 3 camadas (Cisco)

O modelo pode ser utilizado em redes mais pequenas, porque a forma de ligação entre os níveis pode ser aproveitada para ligar redes com muitos ou poucos ativos de rede, mesmo aquelas em que o segundo ou terceiro nível não existam. Estas caraterísticas tornaram o modelo praticamente universal e que foi utilizado durante os últimos dez anos por todas as grandes empresas da área. Apenas as arquiteturas com objetivos muito específicos acabaram por criar a sua própria arquitetura de rede.

3.2. A administração

Baseado no contexto do crescimento de tráfego na rede, os administradores das redes corporativas sentem a responsabilidade de manter a qualidade e a segurança da informação. Considerando que todos os dias são adicionadas novas aplicações e funcionalidades, o papel da gestão e administração da rede é cada vez mais difícil de ser executado com sucesso. São construídos cenários novos todos os dias, que criam uma quantidade relevante de problemas e logo exigem a mesma quantidade de soluções. As funções do administrador da rede estão constantemente a ser redefinidas. Uma tarefa para nunca é igual à outra, ainda que inicialmente assim possa parecer. As análises de tráfego requerem configurações de ferramentas diferentes conforme se trate de mau funcionamento de aplicações, vírus, falha de segurança ou degradação da performance (Duong, 2015). De cada vez que um destes problemas surge o administrador tem que viajar, ainda que remotamente, através de todos os equipamentos ativos de rede envolvidos. Por uma questão de segurança o acesso remoto é normalmente controlado por um qualquer sistema de controlo de acessos. A Cisco, por exemplo, utilizou desde 2006 o Cisco *Secure Access Control System* (ACS), que complementava a infraestrutura dos seus clientes. Trata-se de um produto proprietário que usa protocolos de encriptação proprietários, outros fornecedores possuem outras soluções. Usar um sistema destes dá maior capacidade de gestão e controlo ao administrador e aumenta a segurança da rede em toda a sua extensão. Para que este controlo e segurança funcionem, a administração da rede tem que manualmente configurar acessos e formas de controlo seguro no servidor e em cada um dos ativos de rede. O controlo via ACS é um serviço apenas disponível nas redes e equipamentos da marca, visto utilizar protocolos de encriptação proprietários da Cisco.

Usar a máxima “dividir para reinar”, também se aplica na administração e gestão de redes. Assim, para que seja mais fácil identificar situações anómalas o administrador divide a rede em partes como se fossem silos independentes. De um lado o acesso, o cliente; do outro os serviços, o fornecedor; e no meio o trajeto que a informação percorre através da rede. Nas ações desenvolvidas pelo administrador da rede para a resolução de um problema, este nunca tem uma visão clara e permanente de toda a rede, pelo que a técnica ajuda na identificação e posterior resolução dos problemas. Cada dispositivo ou ferramenta é configurado isoladamente e de forma manual. Uma simples mudança na política da organização necessita uma série de ajustes em *routers*, *switches*, aplicações de gestão, de análise, de segurança ou de desempenho de rede. Porque a rede é distribuída por vários locais e por vezes a grandes distâncias uns dos outros e como o acesso remoto nem sempre resolve o problema. "Se um local remoto está a necessitar de intervenção da administração da rede,

significa que é necessário entrar em contato com o responsável de TI local rapidamente e agir de forma a resolver o problema. Por vezes pode mesmo ser necessária deslocação ao local e lá está o administrador da rede a apanhar transporte para ir resolver o problema" (Duong, 2015).

Um administrador de rede demora muitos anos a formar técnica e profissionalmente. É importante para as organizações manter os administradores de rede que acumularam o conhecimento durante anos, assim como o funcionamento dos processos para solucionar os problemas diários no domínio da rede WAN, quer sejam rotineiros ou menos habituais, fáceis ou complexos. Quando os ativos humanos do setor de administração de rede se tornam impossíveis de manter, a administração da rede fica seriamente comprometida ou limitada. Embora exista um conjunto de ferramentas que ajudam no trabalho existe sempre a limitação da aprendizagem até se dominarem convenientemente (McKeown at al, 2013). Uma abordagem mais estruturada para a análise dos problemas e a implementação da solução ajuda muito na administração da rede, mas isso só pode ser conseguido com a experiência e o conhecimento da rede. Quando este conhecimento e processos de resolução estão centralizados nas pessoas a dependência delas passa a ser maior.

3.3. A configuração

A primeira etapa para a configuração de um equipamento de rede começa com o novo equipamento a ser escolhido e configurado para o papel específico que vai desempenhar. O administrador possui uma lista de ações que fazem parte da configuração do equipamento para que funcione convenientemente, no local aonde vai ser instalado e desempenhe as funções desejadas. Este *checklist* pode ser automatizado com *scripts* de forma a facilitar o trabalho do administrador, mas não evita que seja confirmada manualmente.

Equipamentos diferentes podem requerer configurações diferentes mesmo que desempenhem funções idênticas, por diversas razões como seja o *firmware*, o modelo ou os interfaces de comunicação existentes. A lista de verificações é interminável. A título de exemplo apresentamos na ***Tabela 3*** a *checklist* fornecida pela Cisco nos manuais de configuração para um equipamento NEXUS 5000, um *switch* típico para funcionamento em CPD. Os passos são os descritos no manual de configuração do equipamento e na tabela apenas apresentamos as configurações de "*LAN Switching*" até à 3ª fase de profundidade de configurações, entre parenteses (n) à frente da cada item apresentamos desta fase, identificamos o número de passos para a fase quatro a partir da qual se começam a introduzir comandos efetivos de configuração. Os comandos de *Internetworking Operating System* (IOS), o SO que corre nos equipamentos Cisco, são executados a partir do interface CLI (Cisco 2016, September 7).

A referida tabela apenas apresenta um fragmento do conjunto das tabelas de configurações e que se refere apenas ao capítulo das configurações de "*LAN Switching*". Todas as funções secundárias são configuradas individualmente porque se trata de subsistemas a operar no nível 2 do modelo OSI. Cada um destes subsistemas engloba várias fases de configuração e verificação com comandos dos subsistemas específicos, que tem

como função enquadrar o equipamento nas particularidades de funcionamento na LAN em que o equipamento está a ser inserido. Recordamos que estamos a falar de um *switch* a instalar num CPD, área com especificidades e requisitos exigentes para que não se degrada a performance na transferência da informação.

Main Functions	**Secondary functions**	**Configuration phases**
LAN Switching	*Configuring Ethernet Interfaces;*	*Information About Ethernet Interfaces(5);* *Configuring Ethernet Interfaces(6);* *Displaying Interface Information*
	Configuring VLANs	*Information About VLANs(3);* *Configuring a VLAN()(3);* *Verifying VLAN Configuration*
	Configuring Private VLANs	*Information About Private VLANs* *Configuring a Private VLAN(6);* *Verifying Private VLAN Configuration*
	Configuring Rapid PVST+	*Information About Rapid PVST+(4);* *Configuring Rapid PVST+(12);* *Verifying Rapid PVST+ Configurations*
	Configuring Multiple Spanning Tree	*Information About MST(11);* *Configuring MST(20)*
	Configuring Spanning Tree Protocol (STP) Extensions	*Information About STP Extensions(6);* *Configuring STP Extensions(10);* *Verifying STP Extension Configuration*
	Configuring Port Channels	*Information About Port Channels(4);* *Configuring Port Channels(7);* *Verifying Port-Channel Configuration*
	Configuring Access and Trunk Interfaces	*About Access and Trunk Interfaces(5);* *Configuring Access & Trunk Interfaces(5);* *Verifying Interface Configuration*
	Configuring the MAC Address Table	*Information About MAC Addresses;* *Configuring MAC Addresses(3);* *Verifying MAC Address Configuration;*
	Configuring IGMP Snooping	*Information About IGMP Snooping;* *Configuring IGMP Snooping Parameters;* *Verifying IGMP Snooping Configuration*
	Configuring Traffic Storm Control	*Information About Traffic Storm Control* *Guidelines and Limitations* *Configuring Traffic Storm Control* *Configuring Traffic Storm Control* *Displaying Traffic Storm Control Counters* *Traffic Storm Control Example Configuration* *Default Settings*

Tabela 3 - Passos da configuração (*switch* cisco NEXUS 5000**)**

Estas tabelas como estamos a referir servem apenas como exemplo do caminho típico que um administrador de redes com arquitetura tradicional tem que seguir para executar o seu trabalho conforme o fabricante indica. A escolha de equipamentos Cisco é também apenas como exemplo. Não existe preferência por marcas, mas apenas porque a experiência profissional do autor como administrador de redes nas arquiteturas tradicionais está mais ligada a estes equipamentos, o que traz vantagem para a investigação e compreensão da matéria pretendida. Duma forma mais ampla a configuração de equipamentos engloba muito mais do que a configuração da LAN. Para que possamos ter uma mais completa compreensão da tarefa árdua que o administrador enfrenta, apresentamos na ***Tabela 4***, a tabela de configurações do nível superior, com todos os passos necessários à configuração completa.

Chapter	Title	Description
1	*Product Overview*	*Presents an overview of the Cisco Nexus 5000*
2	*Configuration Fundamentals*	*Contains chapters on using the CLI and initial switch configuration.*
3	*LAN Switching*	*Contains chapters on how to configure Ethernet interfaces, VLANs, STP, Port Channels, trunks, the MAC address table and IGMP snooping.*
4	*Switch Security Features*	*Contains chapters on how to configure AAA, Radius, TACACS+, SSH/Telnet and ACLs*
5	*System Management*	*Contains chapters on how to configure CFS, RBAC, System Message Logging, Call Home, SNMP, RMON, network management interfaces, storm control and SPAN.*
6	*Fibre Channel over Ethernet*	*Contains chapters on how to configure FCoE and virtual interfaces*
7	*Quality of Service*	*Contains chapters on how to configure QoS.*
8	*SAN Switching*	*Contains chapters on how to configure Fibre Channel interfaces and Fibre Channel capabilities (such as NPV, SAN-Port Channels, Zones, DDAS, FSPF and security features).*
9	*Troubleshooting*	*Contains chapters on how to perform basic troubleshooting*

Tabela 4 - Capítulos do manual de configuração (Cisco Nexus 5000)

Com a apresentação e interpretação das tabelas julgamos ter conseguido explicar a complexidade de um mundo da administração nas redes tradicionais. Obviamente que esta tarefa será tão mais complexa quão complexa seja a arquitetura e o tamanho da rede.

3.4. Gestão das redes SDN

Se a administração das redes tradicionais apresenta falta de automatismos para auxílio nas configurações, então a administração por SDN deve configurar novos dispositivos e novas aplicações para que os serviços de configuração deixem de ser feitos manual e individualmente. Este princípio facilitará a vida aos administradores da rede, que criarão automatismos para aplicação das políticas de segurança e das configurações. Com apenas alguns cliques aplicar, por exemplo, *Quality of Service* (QoS) em setores específicos de rede, monitorizar serviços, executar configurações e analisar tráfego. Criar e manter relatórios de toda a rede com gestão centralizada. Possuir um único painel de bordo em que se visualizar toda rede: topologia, tráfego, caminhos e dispositivos num único interface amigável desenhado por *software*. Ter a possibilidade de trabalhar as fontes da informação para obter os resultados desejados a partir do dito interface. Sem a necessidade de visitar todos os ativos de rede, libertar-se do tempo que passa normalmente na análise individual dos equipamentos e com as ferramentas da SDN inovar de forma a reduzir o tempo médio da resolução de incidentes, quer na fase da identificação, quer na apresentação da solução. Trabalhar na melhoria dos processos de execução destas ações, para reduzir tempo na sua execução, tornando-os mais precisos e rápidos através de novos automatismos. Isto seria o sonho de qualquer administrador de rede (Cisco, Duong, 2015).

O protocolo OpenFlow é um protocolo de comunicação, que permite que os investigadores desenvolvam e testem novos protocolos, trata-se do primeiro *interface* de comunicações *standard* entre as camadas de controlo e infraestrutura do *framework* SDN. Como foi referido anteriormente, permite o acesso direto e a manipulação do plano de encaminhamento dos dispositivos da rede, como *switches* e *routers*, quer eles sejam físicos ou virtuais. Em 2012 dizia-se que um protocolo como o OpenFlow era essencial para tornar possível a mudança do controlo da rede para fora dos equipamentos ativos de rede, mudando a lógica do controlo e centralizando-a num único ponto onde pudesse ser controlada através de *software* (ONF, 2012).

O OpenFlow pode ser implementado diretamente nos dispositivos físicos da infraestrutura da rede e nesse caso serão equipamentos compatíveis coma a implementação da SDN, como numa abstração acima dos equipamentos físicos independente do fabricante. Até ao momento, é o único protocolo *standard* para SDN que permite manipulações diretas no plano de encaminhamento dos dispositivos da rede. Está a ser cada vez mais adotado por parte dos fabricantes, sendo implementado no *firmware* dos dispositivos ou recorrendo a atualizações de *software*.

Segundo a ONF o OpenFlow apresenta benefícios no controlo generalizado da rede, não só pelo facto de permitir centralizar o controlo dos ativos de rede num único ponto, a controladora SDN, mas também pelas ações que consegue realizar através dela na área de segurança e monitorização. Após a implementação da controladora SDN e Openflow, deixa de ser importante o fabricante, o *firmware* e o grau de complexidade da operação dos equipamentos. Através de automatismos feitos por *software* facilita-se a administração dos ativos deixando mais tempo livre para a inovação. A confiança da gestão dada pela compreensão e implementação das políticas de segurança na rede é também aumentada.

Cresce a utilização de focos de SDN nos vários fabricantes de tecnologias de redes de grande dimensão, quer seja através da certificação de equipamentos compatíveis, quer com a utilização de *software* de controlo das várias seções da gestão da rede. Estas ações elevam o grau de confiança do mercado, para que novos clientes apareçam e reforcem a importância da ONF. Juntando os princípios de *software* aberto da SDN e a utilização do OpenFlow no encaminhamento na rede, esta pode tornar-se mais estável e bem definida. O futuro das redes irá assentar cada vez mais no *software* como ferramenta de automatização na programação e configuração das redes.

3.5. A SDN com Virtualização

Nas ciências da computação entende-se como virtualização a capacidade de simular uma plataforma de *hardware*, sistema operativo, capacidade de armazenamento ou equipamentos ativos de rede. A necessidade de virtualizar estes recursos pode estar associada aos custos ou à complexidade em armazenar ou alimentar energeticamente estes recursos. Em Outubro de 2012, o *European Telecommunications Standards Institute* (ETSI), entidade reconhecida pela União Europeia aprovou o padrão para a virtualização, o *Network Functions Virtualization* (NFV). É uma iniciativa padrão para virtualizar e desvincular os serviços de rede de *hardware* dedicado. O conceito utiliza a substituição de funções de configuração de *hardware* como *routers, firewalls, switches* ou quaisquer outros dispositivos de *hardware* dedicado, para serem executadas em máquinas virtuais (ETSI 2012).

A SDN e a NFV são abordagens praticamente complementares e estão claramente relacionadas. Enquanto a SDN foi criada pelos investigadores, a NFV foi criada por um consórcio de fornecedores de serviços e produtos na área das tecnologias. Na tentativa de acelerar a implantação de novos serviços de rede, a fim de avançar com os seus planos de receita e crescimento verificaram que os aparelhos baseados em *hardware* limitavam a sua capacidade de atingir tais metas e objetivos. Analisaram as tecnologias de virtualização de TI padrão e partiram para o desenvolvimento de tecnologia semelhante para os equipamentos de rede, a NFV, que os ajudou a acelerar a inovação na área dos serviços. Os operadores de serviços de rede e telecomunicações encontravam-se a cargo com alguns problemas na escalabilidade das redes e CD, dos quais sobressaía a crescente variedade de dispositivos de *hardware* proprietários. Para lançar um novo serviço de rede, por vezes, encontravam limitações de espaço, energia, custos, e desafios de investimento necessários à instalação de cada vez mais equipamentos físicos. A dificuldade para instalar, integrar e operar os aparelhos baseados em *hardware* era cada vez maior. Por outro estes equipamentos entravam rapidamente em processos de fim de venda ou de fim de vida, exigindo muito de um ciclo de vida curto e com pouco ou nenhum benefício na receita. A NFV visa resolver estes problemas, alavancando a tecnologia de virtualização de TI padrão e em simultâneo permitir que vários tipos de equipamentos de rede, servidores e equipamentos de armazenamento, convivem lado a lado no CD se virtualizados. Utilizando o padrão NFV a virtualização é aplicável a qualquer função de nível de processamento de pacotes, quer estejamos a trabalhar no nível de dados, quer no nível de controlo ou nos níveis de infraestruturas de rede fixa e móvel (SDXCentral, 2013).

Para que melhor possamos entender as funções e interações da SDN e a NFV, façamos a análise e interpretação da ***Figura 13*** propriedade da SDXCentral. Segundo esta organização, as duas tecnologias aliadas funcionam em mutualismo. O terceiro elemento que aparece na figura, a inovação aberta, é um conceito que consiste em partilhar a inovação interna do nossa área de desenvolvimento com o exterior através de licenciamento ou outros, com a finalidade de melhorarmos o nosso setor de desenvolvimento de produtos, fornecer melhores serviços aos clientes, aumentar a eficiência e reforçar o valor agregado. Como é mostrado na figura, as funções de virtualização da rede e as funções da SDN não são dependentes uma da outra, mas podem favorecer o mútuo desempenho. Os dois conceitos e logo as duas soluções podem ser combinados e potencialmente gerar maior valor acumulado para uma organização.

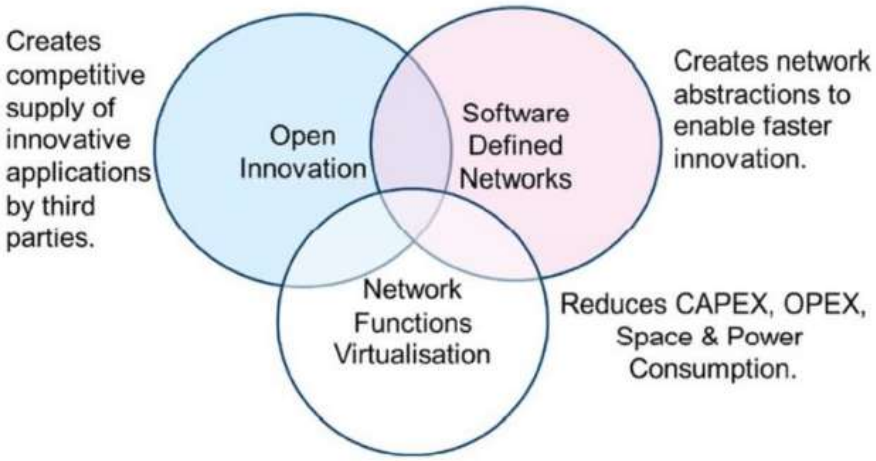

Figura 13 - Relação entre SDN e NSV (SDXCentral)

Embora as metas da virtualização da rede possam ser atingidas sem recurso ao protocolo padrão Openflow, a utilização plena do paradigma SDN não parece ser totalmente conseguido sem as abordagens de encaminhamento realizadas pela controladora SDN. A separação dos planos de controlo e encaminhamento de dados proposta pelo SDN pode melhorar o desempenho, simplificar a compatibilidade com implementações existentes, e facilitar os procedimentos de operação e manutenção. As funções de virtualização da rede são compatíveis com a SDN, fornecendo a infraestrutura sobre a qual o *software* SDN pode ser executado (SDXCentral, 2013).

A virtualização de rede é a reprodução completa de uma rede física em *software*. As aplicações são executados na rede virtual exatamente da mesma forma como se estivessem a ser executadas numa rede física. A virtualização de rede apresenta serviços e dispositivos lógicos do sistema de rede como portas lógicas, *switches*, *routers*, *firewalls*, balanceadores de carga, *Virtual Private Networks (*VPN). Os benefícios fazem-se sentir para cargas de

trabalho elevadas e permanentemente ligadas em rede. As redes virtuais oferecem os mesmos recursos e garantias que uma rede física e ainda fornecem, o que poderemos considerar como benefícios operacionais da independência de *hardware* (VMWare 2016).

3.6. Soluções Empresariais na SDN

Algumas organizações empresariais estão a desenvolver individualmente ou em parcerias soluções SDN que propõem à comunidade e aos seus clientes e parceiros. A execução deste trabalho prolonga-se por vários meses e as evoluções na área do desenvolvimento de *software* aberto para SDN parece ter evoluído significativamente. Muitas organizações desenvolveram APIs para execução de tarefas na área da SDN. Em quase todas é notória a tentativa de promover os padrões de código aberto, a intenção de cumprir as normas de interoperabilidade no desenvolvimento de novos recursos, ampliando os benefícios SDN. Como é humanamente possível referi-las todas, iremos investigar e estudar o que algumas das mais proeminentes empresas desta área de negócio estão a desenvolver. Incluímos aqui empresas de telecomunicações e serviços com a Cisco, HP, IBM e VMware, assim como as duas principais organizações de suporte à SDN OpenDaylight e ONF.

3.6.1. ONF

A *Open Networking Foundation* (ONF) é uma organização sem fins lucrativos, voltada para o utilizador e que tem por objetivo principal a acelerar os processos de adoção da SDN por parte das organizações clientes. Para a ONF a SDN é uma abordagem que mudará a forma de operação de todas as empresas relacionadas com redes, sejam eles fabricantes, operadores ou clientes. A ONF dá enfase aos processos de desenvolvimento abertos e colaborativos e que são orientados para a perspetiva do utilizador final do produto.

A ***Figura 14*** exemplifica a forma como a organização pretende desempenhar as funções que lhe estão atribuídas para a obtenção dos objetivos.

Figura 14 - *Framework* de trabalho ONF (ONF)

A ONF conseguiu introdução do OpenFlow® *Standard*, que foi a primeira ferramenta SDN padrão e se tornou num elemento vital das arquiteturas de rede definidas por *software*. Como entidade responsável pelo OpenFlow, a ONF é igualmente responsável por testar as soluções empresariais que pretendem a obtenção de certificação de conformidade com o

OpenFlow *Standard*. Esta Certificação de Conformidade OpenFlow para fornecedores de equipamentos de serviços de rede demonstra conformidade com a especificação OpenFlow de *hardware*, como *switches* e *routers*, bem como o *software* de rede. Atualmente os clientes procuram soluções de implementação prontas a funcionar nos seus ambientes, por isso procuram cada vez mais a compatibilidade com soluções SDN. Um certificado de Conformidade ONF OpenFlow é o mais alto nível de segurança disponível no mercado. Para validar a conformidade do produto com uma versão específica da especificação OpenFlow, são feitos testes de conformidade em laboratórios de testes independentes acreditados em todo o mundo, proporcionando a validação imparcial da ONF. Ainda recentemente, a organização anunciou a expansão do programa de Teste de Conformidade para incluir testes para membros não-ONF, desta forma pequenas empresas que desenvolvam *software* ou fabriquem *hardware* na área, podem não só adotar as regras, mas obter certificação da ONF. É uma forma que a organização encontrou de preencher lacunas na área de desenvolvimento da SDN, que não controlaria de outra forma, ao mesmo tempo que permite uma adoção mais ampla do Open SDN.

Figura 15 - Certificado de conformidade OpenFlow (ONF)

O logotipo identifica a versão da especificação OpenFlow a que o produto foi sujeito a testes de conformidade. Pode ser usado em produtos físicos, documentação de *software*, sites e material de marketing. As diretrizes do logotipo e os testes estão descritos no endereço eletrónico da ONF, assim como a lista de vendedores com Certificados de Conformidade, proporcionando uma vantagem competitiva adicional ONF (2016, September 9, (1,2)).

Além da certificação ONF OpenFlow para as empresas a organização certifica também pessoas. O programa fornece uma base sólida de validação de conhecimentos profissionais de engenharia que desejem melhorar as suas capacidades na área da SDN. O programa visa proporcionar a validação de conhecimento, quer para operadores quer profissionais que trabalham em ambientes SDN, sejam eles de desenvolvimento ou implementação.

3.6.2. OpenDaylight

Um grupo de fabricantes de equipamentos de redes, criou em 2013, um projeto denominado consórcio SDN OpenDaylight. Funciona da seguinte forma: diferentes patrocinadores propõem diferentes partes da linha de produto. A Cisco, VMware, Juniper e Ericsson contribuem com esforços de desenvolvimento de código e engenharia para disponibilizar uma infraestrutura de *software* comum. A OpenDaylight é uma plataforma modular gerida pelo *Linux Foundation*, que tem como objetivos desenvolver através de plataformas corporativas e em ambientes de código aberto aplicações que projetem e

aceleram a adoção das arquiteturas SDN. Ao adotar a utilização de padrões abertos, como o OpenFlow, a OpenDaylight pretende criar uma plataforma totalmente aberta para a SDN em toda a indústria da área, sejam eles clientes, parceiros ou programadores de aplicações. O primeiro código do Projeto OpenDaylight, chamado *Hydrogen 1.0*, foi lançado em fevereiro 2014.

O OpenDaylight Hydrogen é uma plataforma SDN que visa fornecer às empresas de TI, os vários casos de utilização dos serviços fornecidos pelas arquiteturas de serviços na nuvem. Faz uso de protocolos padrão, inclui métodos para virtualização da rede e auxilia na implementação e gestão das políticas de segurança, nomeadamente com processos de combate a ataques de Distributed Denial of Service (DDoS). O OpenDaylight Hydrogen inclui o OpenStack Neutron, um plugin em código aberto que permite a gestão dos equipamentos ativos de rede. Segundo o próprio consórcio OpenDaylight, "quando os engenheiros de *software* duma empresa experimentarem o Hydrogen, não devem esperar recursos com um de nível de robustez empresarial nem apoio comercial para o *software* pois trata-se de um produto em fase experimental e com o intuito de auxiliar na aprendizagem da SDN" (OpenDaylight, 2016 september 9).

A ***Figura 16*** representa o *framework* da arquitetura OpenDaylight para a sua plataforma SDN, o Hydrogen.

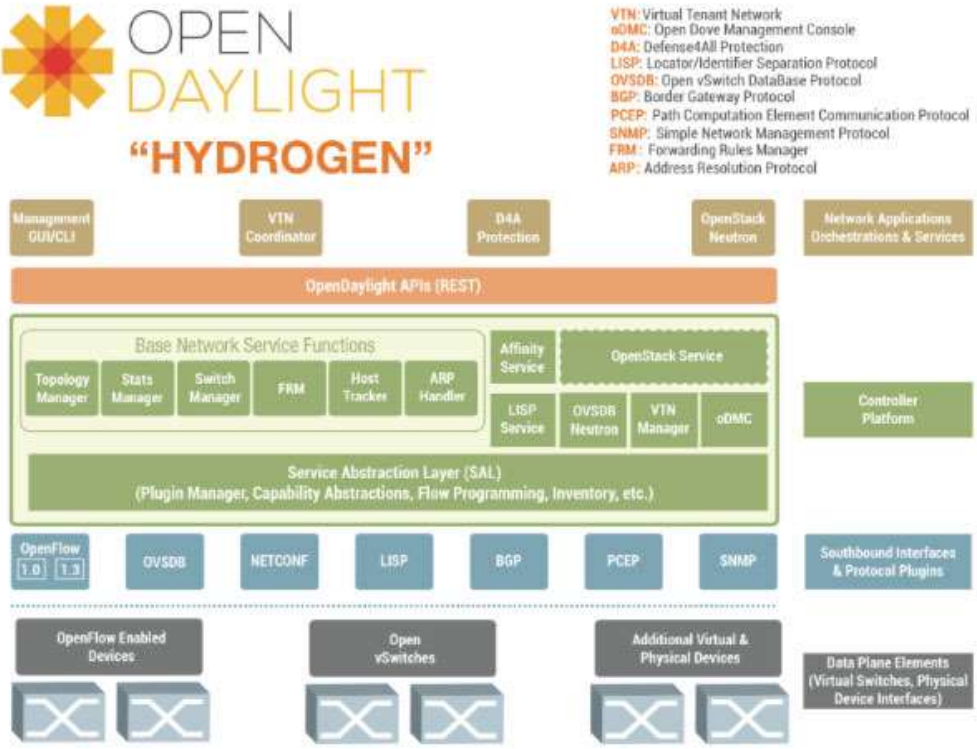

Figura 16 - OpenDaylight Hydrogen framework (sdxCentral)

As redes tradicionais são projetadas para acomodar as necessidades e as cargas de trabalho do momento, com algum grau de inovação e previsão futura, a arquitetura SDN pode otimizar as redes existentes para que consigam fazer face às necessidades de hoje, e facilmente adaptá-las às necessidades da mudança. O OpenDaylight integra código fonte aberto, apoiado em padrões abertos, contribuindo assim para o desenvolvimento dos princípios da SDN e tornando a gestão da rede mais programável, inteligente e adaptável.

3.6.3. Cisco

As redes definidas por *software* possibilitam que as empresas acelerem a implantação e a distribuição de aplicações, reduzindo drasticamente custos de TI por meio da automação de fluxos de trabalho compatíveis com políticas. A tecnologia SDN ativa arquiteturas de nuvem, disponibilizando distribuição e mobilidade de aplicativos de forma automatizada, aprimoram os benefícios da virtualização do CD aumentando a flexibilidade e a utilização de recursos e reduzindo as sobrecargas de infraestrutura. As SDN alcançam esses objetivos empresariais com a convergência da gestão e administração dos serviços de rede e de aplicações em plataformas de orquestração centralizadas e extensíveis que podem automatizar o provisionamento e a configuração de toda a infraestrutura. O resultado é uma infraestrutura moderna que pode fornecer novas aplicações e serviços em minutos, em vez dos dias ou semanas necessários anteriormente (Cisco 2016).

A solução SDN da Cisco designa-se *Cisco Open SDN Controller*. Segundo a própria empresa "é um produto *OpenDaylight* que fornece agilidade e automatismos para a infraestrutura SDN padrão. Construída com alta escalabilidade para plataformas SDN, abstrai toda a complexidade da gestão das redes, aumenta a capacidade no fornecimento dos serviços e reduz os custos operacionais" (Cisco, 2016 September 9).

Como *software* baseado em código aberto, a *Open SDN Controller* está continuamente em evolução, alavancada em simultâneo pelas comunidades Cisco e *OpenDaylight*. A solução está otimizada para os inovadores de código aberto que valorizam as tecnologias SDN como programadores de aplicações baseados em código aberto. Estão abrangidos nesta comunidade a *OpenDaylight* , os utilizadores Linux e os ambientes como o ensino superior que usam tecnologias OpenFlow para apoiar a gestão da rede composta por elementos heterogêneos quer em tempo de fabricante quer de *firmware* e sistemas operativos.

A ***Figura 17*** representa o *framework* da arquitetura da plataforma de desenvolvimento SDN da Cisco retirado do *site* da organização.

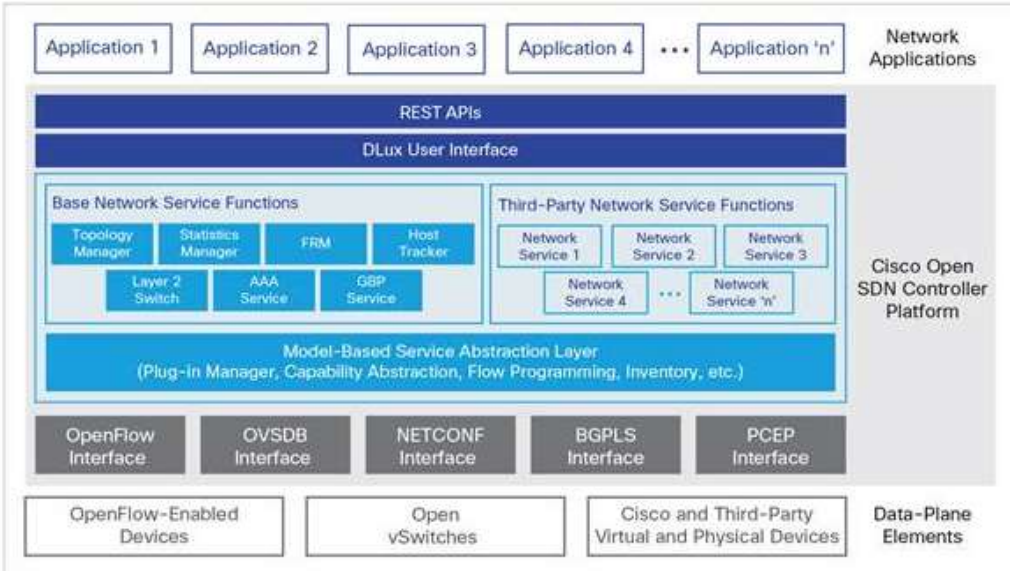

Figura 17 - *Framework* da Cisco *Open Standard Plataform* (Cisco)

A ideia da Cisco é alavancar a procura de aplicações SDN e empurrar os níveis de serviços para uma nova escala para lá do que é possível nas redes tradicionais. Com a *Open SDN Controller* a Cisco espera ainda acelerar os processos nas TI e os processos de configuração, operação e monitorização das redes. Isto será feito automatizando os instrumentos através dos quais são executado os processos e através da abstração baseada em inteligência e controlo. Criação robusta, baseada num controlador de aplicações, a integração e suporte de verificação são fornecidos em de ambiente de desenvolvimento abrangente através de um *software* desenvolvido para o efeito, o Cisco DevNet.

3.6.4. HP-VMware

A HP e a VMware anunciaram em 2013 que tinham planos para colaborar na criação da primeira solução de rede SDN integrada do mercado, desenhada para fornecer aos clientes a automatização e a visibilidade unificadas das suas redes físicas e virtuais nos seus centros e dados. Garantiram na altura aos seus clientes que não haveria perda na agilidade de negócios e aperfeiçoamento da continuidade das operações. As empresas integravam mobilidade e computação em nuvem, no entanto os dispositivos físicos do CD ainda não tinham automatizados os procedimentos de configuração. A solução é composta pela *HP Virtual Application Networks SDN Controller* fornecido pela HP e pela plataforma de virtualização de rede *VMware NSX™* de forma a fornecer aos clientes uma abordagem integrada para a automatização da sua infraestrutura de rede física e virtual (VMWare 2013).

Sendo a HP e a VMware duas das grandes empresas na área das ciências da computação e os primeiros a apresentar uma solução SDN praticamente completa, começaram a comercializar aplicações para monitorização gestão e administração da rede. A solução anunciada começou a ser comercializada com a arquitetura que a ***Figura 18*** documenta.

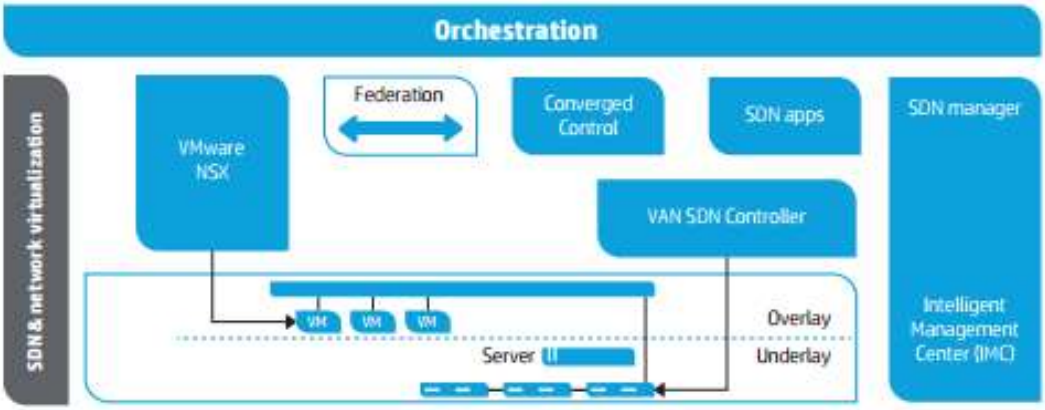

Figura 18 - Solução SDN, HP-Vmware (HP)

A solução SDN VMware-HP Networking oferece automação unificada e visibilidade das redes de centros de dados físicos e virtuais, permitindo a agilidade e continuidade dos negócios. Da solução fazem parte os componentes que a seguir se identificam e dos quais se escrevem as principais funções:

- *HP Virtual Application Networks SDN Controller* - fornece um ponto único para controlo da rede SDN, simplificando a gestão tanto da infraestrutura de comunicações como entrega dos serviços.
- *HP ConvergedControl SDN Application* - camada aplicacional onde, se encontram todas as aplicações desenvolvidas pela HP exclusivamente para o mercado do SDN.
- *HP FlexFabric 5930 Top-of-Rack Switch* - oferece recursos avançados e alto desempenho exigidos por um *switch* de um CD. Ocupa fisicamente 1U no Rack e possui 32 portas a 40GbE.
- *VMware NSX network virtualization Platform* - é uma plataforma de virtualização de rede que consegue virtualizar todos os modelos de rede e segurança a partir do *software*.

Em 2015 a VMware continuou a desenvolver *software* da linha NSX de forma virtualizar os componentes da arquitetura SDN dos quais se destacam:

vSphere - Plataforma unificada que ajuda a escolher o que há de melhor na área da virtualização, permitindo comparar desempenho, disponibilidade e eficiência da infraestrutura e das aplicações.

VMware Integrated OpenStack - permitir entregar acesso aberto via APIs à infraestrutura VMware, para que o cliente encontre e consuma os recursos que procura.

vSphere with Operations Management – gestão inteligente das operações de virtualização. Fornece informações mais detalhadas, do desempenho e disponibilidade aprimorados.

VMware vCloud Air - plataforma segura, dedicada às ações e serviços na nuvem construída no âmbito da *VMware vSphere*.

3.6.5. IBM

A IBM não apresenta soluções SDN únicas e proprietárias completas, mas ao invés disso, apresenta várias soluções com vários parceiros para enfrentar os desafios da SDN no mercado. Os parceiros da IBM nos projetos SDN estão identificados na ***Figura 19*** retirada do *site* da empresa em que se identificam os parceiros e se descreve as soluções.

Figura 19 - Parceiros SDN da IBM (IBM)

Como a variedade de soluções e aplicações da IBM é grande referenciamos aqui a arquitetura que a empresa chamou *IBM Software Defined Network for Virtual Environments VMware Edition*, nome de código (IBM SDN VE), que nos pareceu ser a que melhor se encaixava nos requisitos deste trabalho. Aproveitando a virtualização da VMware e KVM, a IBM apresenta uma arquitetura típica de SDN para uma plataforma única, que lhe permite entregar soluções integradas. É capaz de implementar dispositivos físicos e virtuais nas instalações dos clientes e com suporte para uma ampla gama de aplicações para os mais variados ramos de negócio e as variadas gamas de equipamentos (IBM, 2016 September 8).

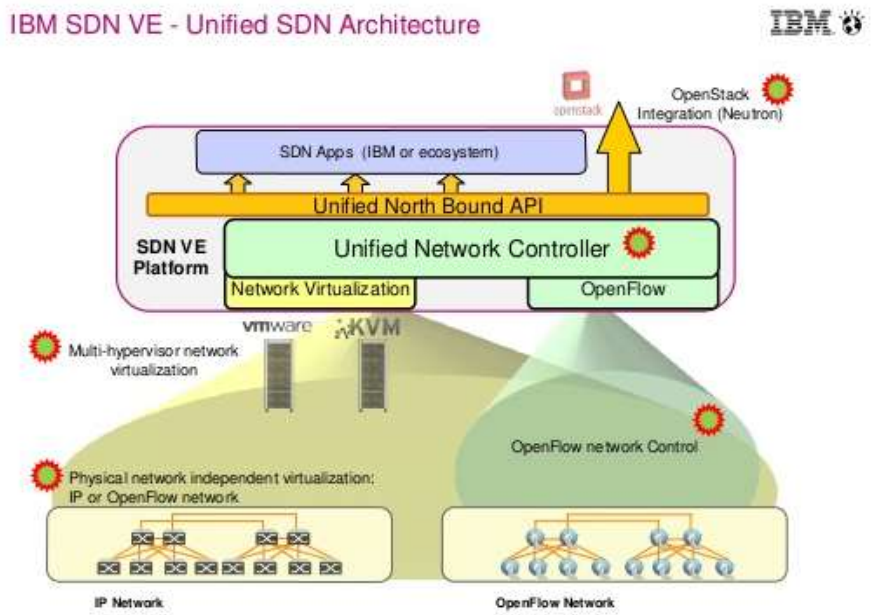

Figura 20 - Arquitetura IBM SDN VE (IBM)

Não explicaremos os componentes e suas funções detalhadamente, porque isso apenas mudaria o nome dos componentes por serem de fabricante diferente. As funções são as funções típicas da arquitetura SDN. Segundo a própria IBM “a solução IBM SDN VE cria uma rede mais flexível, criando uma rede virtualizada, como se fosse apenas uma máquina virtual separada do *hardware* utlizado. A IBM SDN VE atinge um nível de abstração de rede tão avançado, que permite a concorrência de serviços de rede em nível de aplicações e em ambientes multifornecedor em grande escala” (IBM, 2016 September 9).

3.6.6. Outras organizações

Além das organizações referidas nos subcapítulos 4.2.1 a 4.2.6 existem outras que estão a desenvolver soluções de SDN de forma isolada ou em parceria. Algumas desenvolvem mais que uma solução com diferentes parcerias de acordo com a estratégia de negócio. Na ***Tabela 5*** apresentamos uma das soluções adotadas em cada empresa, tendo sido selecionada a que nos pareceram mais relevantes durante este trabalho. Mais pormenores podem ser consultados nos endereços de internet respetivos.

Empresa	Nome da Solução	Descrição
Facebook	*Open Compute Project*	*Open redesigning hardware technology*
Microsoft	*Windows Server SDN*	*Windows Server Technologies for SDN*
Google	*Open Networking Summit*	*OpenFlow to optimize its data center interconnects*
Juniper Networks	*Contrail*	*Open-source network virtualization platform for the cloud*
Citrix	*Citrix NetScaler*	*Platform for cloud Application Control*
Big Switch Networks	*Big Network Controller*	*OpenFlow® controller based, Project Floodlight*
Huawey	*SoftCOM*	*SDN cloud based solution*
Alcatel-Lucent	*Intelligent Fabric*	*Data Center Switching*
Digital China Networks Ltd	*DCRS-7604 series*	*Hardware, L3 OpenFlow Ethernet Switch*
NEC Corporation	*EC PF5240 Series*	*Hardware, OpenFlow Ethernet Switch*

Tabela 5 - Empresas e soluções SDN

De uma maneira geral, a implementação destas soluções significa que o ciente pode utilizar uma solução à sua medida se endereçar as suas reais questões de negócios, nomeadamente o treino dos utilizadores, a mudança de processos e diferentes maneiras de usar a tecnologia.

4. Boas Práticas na Implementação da SDN

Gerir e administrar uma rede de grande dimensão, que possui um número elevado de equipamentos ativos e que presta uma significativa variedade serviços, ainda é uma tarefa com elevado grau de dificuldade. A ameaça permanente de quebra da segurança da informação obriga a manter altos padrões nas políticas de segurança. Os ativos de rede estão permanentemente a requerer ação por parte dos administradores, quer em alterações de configuração, quer em adaptações de tráfego. A utilização da SDN possibilita uma abordagem diferente à gestão e administração das redes, suportada por sistemas de gestão com um elevado grau de adaptação às realidades de cada organização.

No entanto, uma vez que este novo modelo SDN de gestão de redes ainda não está devidamente testado e que apresenta alguma complexidade na implementação por ser significativamente diferente dos modelos atualmente existentes, tem-se verificado alguma resistência por parte dos gestores da rede em aceitarem e explorarem esta nova tecnologia. A grande quantidade de APIs existentes na área do negócio obrigam a um controlo permanente do *software* que se pretende utilizar em *northbound*. Por outro lado, os administradores da rede olham para a SDN com algum apreço. Os projetos de desenvolvimento em *software* destinados a ajudar na administração da rede, também pode representar uma oportunidade para alavancar a utilização das tecnologias SDN. Iniciam-se assim novos processos de execução, baseados em novas práticas de implementação, quer no *software* quer na expansão do *hardware* da rede. A administração das redes SDN é uma abordagem evolutiva da arquitetura de gestão das redes, que procura simplificar as operações, tornando mais fáceis as tarefas de configuração e alteração do comportamento dos dispositivos de rede.

4.1. Boas Práticas na Implementação da Controladora SDN

A implementação da SDN na gestão e administração da nossa rede deve ser precedida duma análise a toda a estrutura e funcionamento da rede. Conhecer o comportamento do tráfego gerado pelas soluções de negócio e pelas tecnologias emergentes, pode elucidar-nos na procura de estrangulamentos provocados pela estrutura ou configurações. Começamos por analisar cada uma das vertentes de gestão nos três níveis do *framework* SDN. Por exemplo, se a infraestrutura é composta por equipamentos com o modelo de gestão das redes tradicionais, então é necessário verificar como se pode uniformizar a infraestrutura para a tornar compatível com a SDN. O primeiro passo consiste, assim, em uniformizar os ativos da rede e, se possível, com equipamentos que tenham obtido Certificação de Conformidade OpenFlow para fornecedores de equipamentos de serviços de rede.

O passo seguinte corresponde à análise de implementação da controladora SDN. Nesta fase é muito importante desenvolver uma análise de custos e benefícios que suportem a definição das características que controladora deverá ter para se adequar da melhor forma à estrutura existente. Para que esta fase possa ter sucesso é importante que estejamos capacitados a responder a perguntas do tipo:

- Como vamos distribuir a controladora pela estrutura da rede?
- Que tipos de controlo a rede vai ter (segurança, administração, configuração)?
- Onde serão colocados cada um dos elementos e tipos de controlo?
- Se implementarmos mais que uma controladora, que ativos controla cada uma?

Sendo a controladora SDN um conjunto de servidores distribuídos a análise de implementação deve orientar-nos para onde cada um deles deve ser colocado. Por exemplo, se a organização possuir mais que uma equipa de gestão e mais que um centro de dados sediados em diferentes locais, distantes um do outro, pode ser vantajoso distribuir os serviços de monitorização e administração por centros de dados diferentes. Torna-se assim mais fácil o acesso e deslocações das equipas aos locais quando necessário. Dependendo do orçamento devemos escolher criteriosamente que tipos de controlo são prioritários para nossa gestão e administração da rede.

Por fim, é necessário proceder à implementação das APIs e das regras do negócio. A área de negócio define que aplicações criadas neste nível devem executar de forma a darem à gestão de topo um aspeto da monitorização e gestão da rede. Objetivos diferentes prestam-se a cenários diferentes. A forma como estas aplicações interagem com a controladora são verdadeiros problemas de inteligência artificial porque fornecem ao mesmo tempo o estado da rede mas também são repositórios de aprendizagem, como se máquinas de inferência se tratasse.

4.2. Boas Práticas na Configuração da Rede

O administrador das redes tradicionais possui um conjunto de processos para a configuração de um equipamento. Para implementar regras SDN na configuração da rede devemos analisar esse conjunto de processos tradicionais e melhorá-los implementando automatismos. Embora os modelos existentes atualmente funcionem, a administração dos processos é complexa e morosa, de acordo com a discussão sobre a configuração de equipamentos nas redes tradicionais analisada na seção 3.3 deste trabalho. No equipamento tradicional é necessário percorrer várias listas de verificações e configurar cada um dos serviços percorrendo as várias etapas e protocolos padrão ou do fabricante. Na SDN a configuração deve ser automatizada a partir da controladora SDN. A Figura 21 ilustra a transição na execução das configurações, tendo em conta a gestão da rede tradicional e a gestão com recurso à SDN.

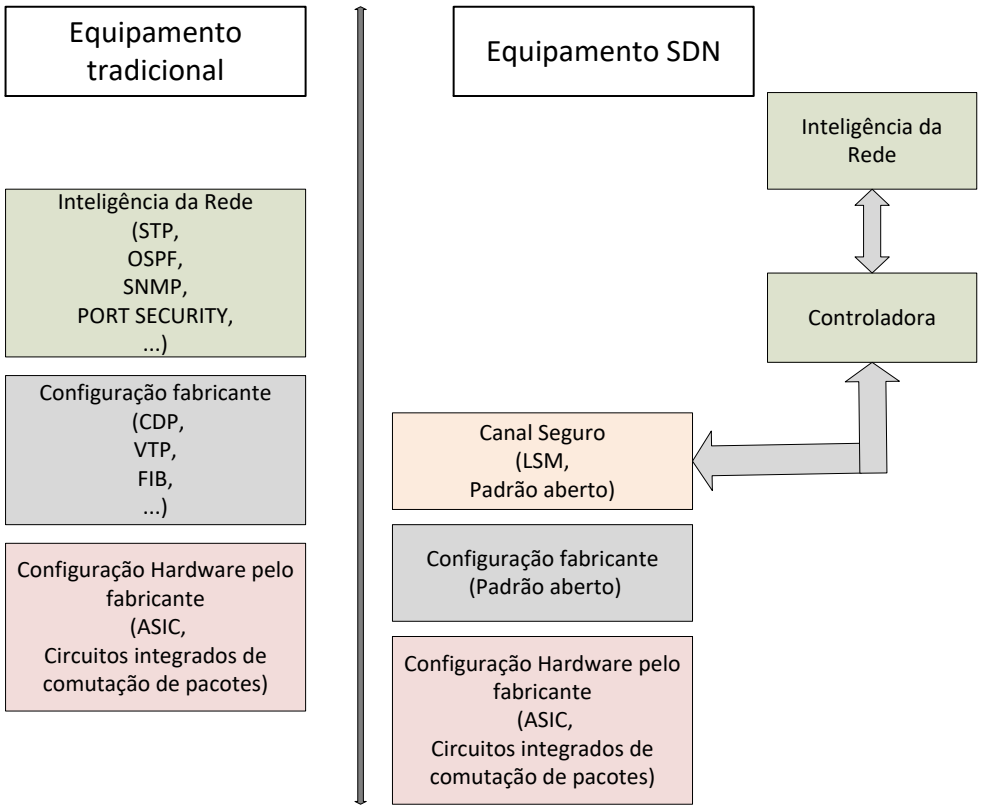

Figura 21 - Esquemas de configurações SDN vs tradicional

Enquanto na configuração tradicional, toda a inteligência da rede tem que ser configurada pelo administrador, viajando por cada equipamento, configurando protocolos para reencaminhamento, comutação, gestão, administração e segurança. Continuando ainda com os protocolos específicos do fabricante para descoberta da topologia, domínio e comutação. Nas redes que recorrem à gestão SDN todas estas funções são configuradas por *software* na controladora em código aberto, sendo depois enviadas para o equipamento. O equipamento compatível com SDN é dotado dum *software* inicial de gestão e controlo destinado a procurar a controladora de onde receberá os automatismos para a execução das tarefas de configuração inicial e reconhecimento na rede.

Como a configuração do fabricante é realizada em código aberto, requisito da compatibilidade com a implementação SDN, o administrador pode utilizar a controladora para adaptá-lo à realidade da organização codificando alterações de acordo com os equipamentos utlizados. Esta prática pode ser utilizada tanto nas configurações iniciais de um novo equipamento a instalar na rede, como nas alterações das configurações dos equipamentos existentes. Desta forma, torna-se mais prático executar configurações que requeriam muito tempo e que tinham de ser executadas com recurso a acessos a vários equipamentos como alterações e análise de tráfego, implementação de qualidade de serviço, túneis de reencaminhamento ou aplicação de políticas de segurança.

4.3.Boas Práticas na Administração da Rede

Para a gestão e administração da rede SDN os objetivos não se alteram muito dos objetivos da gestão e administração tradicional das redes. Os gestores pretendem ter monitorização centrada da rede e os administradores uma visão integrada de toda a rede, com o foco nos incidentes do momento. Aos gestores importa a visibilidade ponto a ponto dos fluxos da informação, para análise e satisfação do cliente ou utilizador, sendo de pouca importância as infraestruturas utilizadas ou os caminhos percorridos, enquanto aos administradores importa o trajeto dos fluxos e os possíveis caminhos alternativos, assim como a existência de falhas e as formas de recuperação. Se os objectivos finais são comuns entre gestores e administradores, mas os caminhos que cada um deles tem que percorrer para os atingir são diferentes, então para exigências diferentes, soluções diferentes. A criação e modificação desses caminhos cria alternativas nos processos. Essas alternativas são mais rápidas e eficazes quando executadas por *software*. Mais uma vez as necessidades e requisitos encaixam-se nas bases da arquitetura SDN.

É requisito de uma eficaz administração a utilização de uma controladora SDN que suporte multiplataformas, nomeadamente as da estrutura e fabricantes existentes na rede tradicional. Desta forma, durante a implementação da SDN podem monitorizar-se as evoluções. Estas evoluções permitem comparações entre os dois métodos de administração de redes a funcionar em simultâneo, quer em termos de avaliação de desempenho quer de custos. Os parâmetros a avaliar devem incluir:

- Simplicidade de processos – Controlo centralizado e automatizado da rede, que permita eliminar a complexidade dos protocolos e a irradicação dos erros associados à gestão das redes tradicionais;
- Rapidez de execução nos processos – Nomeadamente na capacidade para monitorar e alterar os caminhos dos fluxos da informação;

Facilidade de programação – essencialmente na função de eliminar estrangulamentos de tráfego. Recorrendo a otimizações de reencaminhamento se possível utilizando virtualização das funções de *routing* e *switching*.

- Código aberto – Funções de suporte para as versões padrão do OpenFlow, 1.0 a 1.3[9] e, se possível, com certificação ONF.
- Segurança – Cada uma das vertentes de segurança utilizadas tanto na gestão SDN como na tradicional devem ser perfeitamente isoladas. No caso de serem implementadas em VLANS, estas devem ser seguras, eliminando possíveis misturas e conflitos entre os dois ambientes. As boas práticas da segurança aplicada nas redes tradicionais devem manter-se em simultâneo com as novas políticas de segurança de implementação SDN discutidas na seção seguinte deste capítulo.

[9] Segundo informação do *site* da ONF, a versão 1.4 do Openflow será lançada ainda em 2016.

Os requisitos para fazer cumprir estes parâmetros devem ser perfeitamente identificados e resolvidos na fase de desenho. As correções na fase de implementação tornar-se-ão muito mais difíceis de executar.

Na SDN a rede não é controlada por *routers* e *switches*, mas por *software*. A grande vantagem desta mudança é a capacidade de melhorar a monitorização e o desempenho da infraestrutura, controlada de forma centralizada. Para implementar, por exemplo, a gestão do tráfego na arquitetura SDN, pensamos na forma como queremos orientá-lo dentro da nossa rede. Se possuímos um tráfego específico como *multicast* a maneira mais fácil é criar uma política por engenharia de tráfego e fazê-lo fluir por túneis através da estrutura da rede. Por exemplo e existe tráfego específico que queremos saia da nossa estrutura até à estrutura de um parceiro de negócios, usando um fornecedor de estrutura e serviços da internet, podemos encriptá-lo e enviá-lo através de um túnel até à estrutura do nosso parceiro de negócios. Usar esta capacidade tecnológica da criação de túneis, seguros ou não, para levar o tráfego de um ponto ao outro não importando a estrutura utilizada, é uma forma cada vez mais utilizada na programação da rede e logo melhora com a implementação da SDN.

4.4. Boas Práticas na Segurança da Rede

As ameaças para a segurança da rede têm aumentado em número e grau de complexidade. Existem algumas tecnologias e comportamentos dos utilizadores que favorecem o curto-circuito dos pontos de segurança da rede tradicional, expondo assim a segurança da rede:

- O aumento das aplicações distribuídas pela rede e em diversos casos a ser desenvolvidas dinamicamente e sem o controlo da administração da rede;
- As necessidades das empresas se associarem em diversas áreas do negócio, partilhando informação e recursos técnicos;
- O aumento da utilização dos dispositivos móveis quer em diversidade, quer nos locais aonde podem ser utilizados;
- A adoção ou não das regras do paradigma do BYOD.

Estes e outros pontos são preocupações bastantes para a equipa responsável pela segurança da rede, não fora já a dificuldade de manter a segurança da rede. No modelo de gestão de redes tradicional os administradores configuram a segurança em cada um dos níveis do modelo OSI. No nível físico a segurança pode ser melhorada através de um sistema de controlo de acessos, por exemplo, ainda que a codificação deste sistema não seja em código aberto e, portanto, compatível com o modelo SDN, já está implementado por *software*. Nos níveis da infraestrutura, e mesmo no nível 4 do modelo OSI, onde a aplicação das políticas de segurança é exclusivamente da responsabilidade da administração da rede, as listas de controlo de acessos (ACLs) foram sempre consideradas um meio eficiente. Com a arquitetura SDN implementada e a utilização de APIs, consegue automatizar-se os processos da aplicação das políticas de segurança da rede que gestão definiu. O primeiro nível de segurança corresponde à aplicação ao nível do sistema operativo dos ativos de rede.

As ACLs aplicadas a este nível devem ter em conta a própria definição do plano de dados, de maneira a que a aplicação da segurança não impeça a interoperabilidade e a performance da rede. A aplicação das políticas de segurança, a partir da controladora SDN, podem ser executadas em qualquer ponto da rede de forma célere, libertando os administradores da tarefa de percorrerem cada um dos equipamentos. As aplicações, sejam as que cumprem as tarefas de gestão da rede ou outras, devem ser seguras no seu próprio ambiente de execução.

As aplicações utilizadas na gestão da rede devem cumprir as normas da segurança ONF aplicáveis ao modelo SDN, quer desempenhem funções no interface *northbound* ou *southbound*. Os princípios e práticas da segurança para as controladoras SDN forma definidos pela ONF no documento em referência (ONF, 2015 B). No entanto, a segurança da rede é muito mais complicada, principalmente em tempos de implementação SDN ou quando as duas arquiteturas de gestão se misturam. É necessário pensar na segurança a implementar nos pontos de acesso externos à rede, sejam eles o acesso à internet ou a extensão da nossa estrutura para fora dos seus limites físicos. Estas situações estão referidas num recente documento da ONF de agosto de 2016. As regras de interoperabilidade no interface *east-westbound*, como esta zona de comunicação está a ser identificada na nova arquitetura SDN proposta pela ONF. Ainda que as previsões da ONF para 2016 tivessem sido que as preocupações maiores com a segurança da rede viessem do interface *northbound*, porque segundo a organização era aonde as inovações e evolução da SDN mais se faziam sentir. São os negócios e a interação dos fornecedores de serviços com a estrutura da rede da empresa a alavancar as leis de mercado.

4.5. Resumo das Boas Práticas

Não é objetivo deste trabalho substituir de alguma forma as normas internacionais da família ISO/IEC 27000. Cada uma das normas tem uma função específica na área dos sistemas de informação tendo como finalidade a sua criação, manutenção, funcionamento e análise. As normas podem ser adotadas independente do tamanho ou tipo da empresa. As suas orientações que fazem com que um *Information Security Management System* (ISMS) se adapte à empresa que deseja implementá-lo. Os administradores devem consultá-las para a realização das ações propostas. Por forma a facilitar uma orientação para a implementação das normas identificamos as principais no domínio das ISMS.

- **ISO/IEC 27000** - Informações básicas sobre as normas da série;
- **ISO/IEC 27001** - Bases para implementação de um ISMS numa organização;
- **ISO/IEC 27002** - Certificação profissional, códigos das práticas profissionais;
- **ISO/IEC 27003** - Diretrizes específicas de implementação dum ISMS;
- **ISO/IEC 27004** - Normas para as métricas e relatórios do ISMS;
- **ISO/IEC 27005** – Gestao de riscos e técnicas de segurança da informação.

Uma organização que cumpra estas normas e que esteja formalmente certificada, possui o reconhecimento dos seus parceiros, clientes e colaboradores. A certificação deve ser um

objetivo a atingir de forma a obter padrões e confiabilidade. Será assim também facilitada a tarefa de comunicar e integrar com outros sistemas.

A controladora SDN é responsável pelo controlo da arquitetura da rede e, por consequência, a entidade responsável pelo controlo da segurança da informação. Este controlo e a aplicação da política de segurança são conseguidos através de *software* específico de autenticação e autorização. A ONF emitiu em Julho de 2016 a norma TR-529 que especifica quais os requisitos de segurança para as controladoras SDN (ONF 2016, B). Nesta norma a organização identifica os requisitos críticos, as ameaças e os requisitos de segurança, fornecendo modelos e quadros que orientam os administradores para a implementação dos controlos.

De forma a facilitar a identificação dos componentes de boas práticas descritos nas seções anteriores deste capítulo apresenta-se a ***Tabela 6*** que lista sucintamente os elementos das boas práticas apresentadas neste trabalho e baseadas nele.

Funções	Análise	Ação	Parâmetro
Controladora	• Estrutura da rede • Tecnologias • Tráfego	• Como distribuir o controlo	• Tráfego • Arquitetura • Serviço pretendido
		• Tipos de controlo	• Segurança • Administração • Configuração • …
	• APIs	• Monitorização	• Serviços de visualização, quem e onde
		• Gestão da rede	• Regras • Políticas
Configuração	• Equipamentos	• Compatíveis Openflow • Virtuais	• Certificados • NFV • Tradicionais
	• Processos	• Gestão de tráfego seguro • Comutação	• Resolução de incidentes • Autenticação e especificidade
	• Inteligência da rede	• *Open software*	• Protocolos padrão • Linguagens de programação abertas
		• Pré-definida; • Testada	• Domínio • Autenticação
Administração	• Processos	• Simples • Sem erros	• Controlo centralizado e automatizado • Eliminar complexidade da gestão
		• Rápidos	• Na execução e monitorização
	• Programação	• Código aberto e seguro	• Suporte OpenFlow • Certificação ONF • Multilinguagem
Segurança	• Aplicações distribuídas	• Seguras • Controladas	• Controladas ou à revelia da administração
	• Informação	• Partilhada	• Parceiros • ISP • Interna
	• Mobilidade	• Regras	• BYOD • Locais • Diversidade
	• APIs	• Políticas	• Celeridade • Conjuntas

Tabela 6 - Orientação para boas práticas

5. Conclusões e Perspetivas

As conclusões finais deste trabalho são divididas em duas áreas distintas denominadas conclusões e perspetivas. O primeiro refere-se aos aspetos conclusivos acerca dos objetivos propostos, tendo em conta o trabalho de pesquisa efetuado e o segundo acerca das perspetivas futuras da SDN que parecem advir dos trabalhos de investigação e desenvolvimento que a organizações que analisamos estão a realizar.

5.1. Conclusões

A mudança é um processo complexo que depende em muito das características das organizações e dos indivíduos. Quando se trata de mudanças nas áreas tecnológicas, aumentam ainda as dificuldades e a resistência à mudança. A ansiedade e receio de não se conseguir lidar com as inovações e alterações atravessa a cabeça dos colaboradores. As chefias têm receio de perder o controlo das alterações e das pessoas. Por essas razões, a implementação da SDN nunca será tarefa fácil para os administradores da rede. No entanto, face à acentuada adoção das regras da ONF pelas grandes empresas do setor, a SDN pode vir a implementar-se de modo significativo nos ambientes de redes e serviços.

Na tentativa de compreender porque os processos de resolução de incidentes na gestão tradicional é lento e complexo, basta perceber a dificuldade que o administrador tem para analisar tráfego numa rede de elevada complexidade com muitos equipamentos ativos, que obriga a percorrer vários equipamentos na procura da informação pretendida. Na arquitetura SDN este trabalho pode ser realizado recorrendo ao *software* específico da controladora acelerando assim os processos, não só da procura, mas também da análise e resolução dos incidentes. O OpenFlow pode ser implementado tanto nos dispositivos da infraestrutura da rede como por *software*. Até ao momento, este é o único protocolo *standard* para SDN que aplica manipulações diretas ao plano de encaminhamento dos dispositivos da rede. Este protocolo está a ser muito adotado por parte dos fabricantes que o estão a implementar ou através do *firmware* dos dispositivos ou recorrendo a *upgrades* de *software* nos mesmos.

Segundo a ONF, o OpenFlow apresenta benefícios no controlo generalizado da rede, porque consegue centralizar a administração dos ativos de rede num único ponto controlado por *software*, a controladora SDN. Não importa a marca dos equipamentos nem o *firmware*, a complexidade e os automatismos ficam facilitados, deixando mais tempo livre para a inovação. A confiança da gestão dada pela compreensão e implementação das políticas de segurança na rede é também facilitada. A utilização dos focos de SDN, que vêm surgindo por vários fabricantes em redes de grande dimensão dão ainda outro grau de confiança. As regras da SDN, através do OpenFlow, manipulam o encaminhamento na rede, tornando-a mais estável e bem definida. O futuro da administração das redes irá assentar cada vez mais no *software* como ferramenta de automatização para a programação e configuração das redes.

Face às necessidades elencadas no primeiro parágrafo do Capítulo 4, para implementação da arquitetura SDN com a finalidade de gerir e administrar com eficiência uma rede de grande

dimensão, as propostas de boas práticas nas seções deste capítulo apresentam algumas soluções possíveis para ajudar os administradores nas suas funções. A ideia fundamental destas propostas é ajudar os administradores da rede:

- Na forma como pensar e agir na instalação da controladora SDN;
- Na mudança das ações a tomar nas configurações;
- Que caminhos tomar para facilitar a administração e gestão;
- E na forma como programar instalação e manutenção das políticas segurança da rede.

5.2. Perspetivas

Uma das preocupações dos serviços de TI das organizações é fornecerem aos clientes serviços de qualidade sem correr riscos de que se perca o acesso à informação. A infraestrutura de rede deve primeiro garantir a continuidade no funcionamento dos serviços atuais e, de seguida, suportar o desenvolvimento crescente nas áreas de mobilidade e transação de dados. A virtualização das funções de rede é uma abordagem que foi implementada com sucesso em centros de dados pela VMWare com a virtualização de *switches*. Os prestadores de serviços tentam agora ser mas ágeis e flexíveis nos serviços aos clientes, mudando os seus modelos económicos. A SDN pode influenciar estes modelos reduzindo os recursos de *software* e de gestão e administração da rede dos centros de dados, que por serem importantes pontos de prestação de serviços, se tornam pontos críticos de falhas. Embora a solução, de momento, ainda passe por manter os equipamentos de rede na última geração de *hardware* de forma a manter a empresa na vanguarda, a implementação de arquiteturas SDN tem vindo a resolver as enormes exigências impostas pela chegada da mobilidade, vídeo, big data e a panóplia de aplicações baseadas nos serviços da nuvem.

A tecnologia SDN, está em expansão e referenciada como inovadora tendo uma procura crescente de novos clientes. Uma das principais vantagens consiste na utilização de recursos configuráveis, à medida e sem preocupações de manutenção física ou custos associados. Algumas definições do serviço IaaS incluem infraestrutura de rede, conseguindo assim uma administração unificada que facilita a criação de regras de reencaminhamento dos pacotes, registos de utilização e volume de informação. Se as funções de rede forem virtualizadas, conceber e implementar arquiteturas SDN pode tornar-se mais ágil. Para os fornecedores dos serviços a mudança pode passar apenas pela alteração do modelo de negócio, porque necessitam possuir o mesmo nível de infraestrutura. Na perspetiva do cliente, a criação do NaaS permite consumir serviços de rede sem necessidade de possuir infraestrutura. Há operadores que consideram os serviços de aluguer de uma VPN e acessos de equipamentos móveis como serviços NaaS. A razão é porque o modelo de negócio é semelhante, já que ambos necessitam da infraestrutura e do serviço. O serviço NaaS, apenas exige ligação à internet, os clientes obtêm benefícios operacionais de um controlo de fluxo centralizado baseado em políticas de segurança e de tráfego que eles conhecem, podem desfrutar de uma maior flexibilidade, otimização de recursos, escalabilidade, eficiência da rede e redução de

custos. Além disso, garantem ao cliente opções mais robustas na recuperação da informação e que em certos casos são praticamente impossíveis nas estruturas de rede tradicionais.

Tendo o autor cerca de 30 anos de experiência na administração de sistemas e redes no Ministério da Defesa Nacional – Marinha, organização que possui uma infraestrutura de rede distribuída por todo o litoral de Portugal e pelas ilhas, toda esta temática tem uma importância acrescida. A estrutura de rede da Marinha destina-se a fornecer serviços de rede ao pessoal da organização que presta serviço nas unidades terrestres e navais e ainda aos militares e civis que guarnecem a Autoridade Marítima Nacional. Atualmente desempenha funções na administração da Rede de Comunicações da Marinha, cujas atribuições principais são a configuração e administração dos equipamentos de rede e ainda a segurança da informação. Os referidos serviços são fornecidos por servidores localizados em centros de dados na região de Lisboa e pretende-e que sejam entregues aos clientes em todas as unidades da Marinha. Nesta altura a administração é ainda muito baseada na arquitetura tradicional, mas aos poucos vão aparecendo soluções baseadas em *software*, que estão a ser incorporadas na arquitetura existente. Este facto é também uma das razões para a investigação realizada neste trabalho. Face a tudo o que foi descrito a possibilidade de continuar durante os próximos dez anos a trabalhar com as tecnologias SDN na área de administração e gestão de redes é muito elevada.

Bibliografia

B- On (2016), Repositório de Artigos Académicos, Biblioteca Online com Motor de Busca, retrieved from, http://www.b-on.pt/a-b-on-para/estudantes/

Big Switch Networks (2014), David Bombal, SDN and Openflow Overview, retrieved from, https://www.youtube.com/watch?v=l-DcbQhFAQs

Big Switch Networks (2014), David Bombal, SDN and OpenFlow Overview - Open, API and Overlay based SDN, retrieved from, https://www.youtube.com/watch?v=l-DcbQhFAQs

Casado, M., et al (2006), SANE: A Protection Architecture for Enterprise Networks (16(05), retrieved from, http://yuba.stanford.edu/~casado/sane.pdf

Casado, M., et al (2007), ETHANE: Taking Control of the Enterprise (05), retrieved from, http://www.sigcomm.org/sites/default/files/ccr/papers/2007/October/1282427-282382.pdf

CIENA (2015), Rob Tomkins, What is Software-Defined Networking, Chalk Talk: What is SDN?, retrieved from, https://www.youtube.com/watch?v=Np4p1CDIuzc

Cisco (2015 A, Anthony Sequeira, Cisco Cloud Fundamentals, SDN Fundamentals, retrieved from, https://www.youtube.com/watch?v=Np4p1CDIuzc

Cisco (2015 B), Jason Casey, Introduction to SDN & OpenFlow : SDN Key Ideas, retrieved from, https://www.youtube.com/watch?v=Np4p1CDIuzc

Cisco (2015 C), Jason Casey, INE course, Introduction to SDN & OpenFlow : SDN Key Ideas, retrieved from, https://www.youtube.com/watch?v=Np4p1CDIuzc

Cisco (2016, August 30), Access Control System, retrieved from http://www.cisco.com/c/-en/us/products/security/secure-access-control-system/index.html

Cisco (2016, September 6), The Journey to Unified Computing (pp, 1-2), retrieved from, http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/EMA_Cisco_UCS_Journey_0410_WP.pdf

Cisco cloud (2016, September 6), Cloud Computing Models and Technologies, retrieved from, http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-45/123-cloud1.html

Cisco (2016, September 7), Nexus 5000 Series NX-OS Software Configuration Guide, retrieved from, http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide.html

Cisco (2016, September 9), Cisco®Open SDN Controller, OpenDaylight software-defined networking, retrieved from, http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/open-sdn-controller/datasheet-c78-733458.html

Duong A., 3 Steps to WAN Management Nirvana (2015), A day in Life of a Network 15(08), retrieved from, http://blogs.cisco.com/enterprise/3-steps-to-wan-management-nirvana

Eli the computer guy (2013), Software Defined Networking (SDN) Introduction, retrieved from, https://www.youtube.com/watch?v=2BJyIIIYU8E

ETSI (2012), European Telecommunications Standard Institute, Network Functions Virtualization, retrieved from, http://www.etsi.org/technologies-clusters/technologies/nfv

Faughnan, L., Software Defined Network (2016), TechCentralie 13(05), retrieved from http://www.techcentral.ie/software-defined-networking

Google Académico (2016), Repositório de Artigos Académicos, Biblioteca online com Motor de Busca, retrieved from, https://scholar.google.pt/

Guerra, I., (2006), Pesquisa Qualitativa e Análise de Conteúdo, Sentidos e formas de uso, Principia Editora, Lda

HP (2016 September 8), Network Management/Security Software, HPE VAN SDN Controller Base Software, retrieved from, http://www8.hp.com/us/en/products/oas/product-detail.html?oid=5443917

IBM Software Group (2013 A), Jamie Thomas, Edge 2013, Software Defined Systems, retrieved from, https://www.youtube.com/watch?v=-BKYXBqFkk8

IBM Software Group (2013 B), Steve Kenniston, Edge 2013, Software Defined Storage, retrieved from, https://www.youtube.com/watch?v=-BKYXBqFkk8

IBM Software Group (2013 C), Oscar Addem, Edge 2013, Data Center Software Defined Environment, retrieved from, https://www.youtube.com/watch?v=-BKYXBqFkk8

IBM (2016, August 15), IBM SDN Applications Solutions, retrieved from, http://www-935.ibm.com/services/us/en/it-services/networking-services/software-defined-network/solutions/

IBM (2016, September 9), IBM Software Defined Network for Virtual Environments VMware Edition, retrieved from, http://www.redbooks.ibm.com/redbooks/pdfs/sg248203.pdf

IEEE (2015), Captain Morgan, Cutting-edge Seminar , An Introduction To Software Defined Networking, retrieved from, https://www.youtube.com/watch?v=Np4p1CDIuzc

Linux Foundation, Collaborative Projects (2016), OpenDayLight 16(01), (pp. 10 -23), retrieved from, https://www.opendaylight.org/

McKeown, N. at al (2008), OpenFlow: Enabling Innovation in Campus Networks, retrieved from, http://ccr.sigcomm.org/online/files/p69-v38n2n-mckeown.pdf

McKeown N., et al (2013), Leveraging SDN Layering to Systematically Troubleshoot Networks, retrieved from, http://dl.acm.org/citation.cfm?id=2491197

Mell, P., & Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, retrieved from, http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

NIST (2011, September), National Institute of Technology, The NIST Definition of Cloud Computing (pp 2), retrieved from, http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

ONF (2012 September 6), OpenFlow® Switch Specification, retrieved from, https://www-opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-1.2.pdf

ONF, (2015 A) Framework for SDN, Scope and Requirements, ONF- TR-516, retrieved from, https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Framework_for-SDN_-Scope_and_Requirements

ONF, (2015 B) “Principles and Practices for Securing Software-Defined Networks,” Issue 1, January,

2015, ONF TR-511, retrieved from: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technicalreports/Principles_and_Practices_for_Securing_SoftwareDefined_Networks_applied_to_OFv1.3.4_V1.0.pdf

ONF (2015 C), Dan Pitt, SDN and Openflow seminar, Introdution to Openflow and Software-Defined Network, retrieved from, https://www.youtube.com/watch?v=5-pLO4MZU3o

ONF, (2016 A, January, 16), Open Networking Foundation | Sitemap, SDN Defined, (pp.10-23), retrieved from, https://www.opennetworking.org/sdn-resources/sdn-definition

ONF (2016 B, July), Open Network Foundation, Security Foundatio Requirements for SDN Controllers, TR-529, retrieved from, https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Security_Foundation_Requirements_for_SDN_Controllers.pdf

ONF (2016, September 9 (A)), Open Network Foundation Overview, All about ONF, retrieved from, https://www.opennetworking.org/about/onf-overview

ONF (2016, September 9 (B)), Open Network Foundation, ONF Conformant Logo Guidelines, retrieved from, https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow-test/Conformant_Logo_Guidelines.pdf

OpenDaylight (2016, September 9), Linux Foundation, OpenDaylight: Open Source SDN Platform, retrieved from, https://www.opendaylight.org/news/foundation-news/2014/02/opendaylight-delivers-open-source-software-enable-software-defined Quintero, D. et al (2015), IBM Software Defined Environment, IBM Redbooks, retrieved from, https://play.google.com/books/reader?id=IWtfCgAAQBAJ&printsec=frontcover&output=reader&hl=pt_PT&pg=GBS.PP1

Raj Jain (2015), Washinton Uiversity in Saint Louis, Web Seminar, Tutorial on OpenFlow, Software Defined Networking (SDN) and Network Function Virtualization (NFV), retrieved from, https://www.youtube.com/watch?v=-OGvr0bjEkU

Ramos, F., Veríssimo P. & Kreutz D., (2015), Software-Defined Networks: on the road to the softwarization of networking, retrieved from, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=6994333

SDXCentral (2013 March), NFV and SDN: Whats the Difference?, retrieved from, https://www.sdxcentral.com/articles/contributed/nfv-and-sdn-whats-the-difference/2013/03/

Stake, R., (2010), Qualitative Research, Studying How Things Work, The Guilford Press

Stanford University (2013), Nick McKeown, SDN and Openflow seminar, How SDN will Shape Networking, retrieved from, https://www.youtube.com/watch?v=c9-K5O_qYgA

Stanford University (2013), Scott Shenker, Colloquium on Computer Systems Seminar Series (EE380), retrieved from, https://www.youtube.com/watch?v=WabdXYzCAOU

VMWare (2016, September 8), VMware vSphere with Operations Management, retrieved from, http://www.vmware.com/ products/vsphere.html