Chapter 1

Network Function Virtualization: Perspectivas, Realidades e Desafios

Raphael Vicente Rosa (Unicamp), Marcos Antonio de Siqueira (Unicamp), Christian Esteve Rothenberg (Unicamp), Emerson Barea (UFSCar), Cesar Augusto Cavalheiro Marcondes (UFSCar)

Abstract

Approximately a year after its conception, the Network Function Virtualization (NFV) concept has been shown prominent in telecom operators scenario. It brings the opportunity to innovate communication networks on an unimaginable time scale, the concept brought together currently about 150 members in a group of industry specifications (Industry Specification Group - ISG) within the European Telecommunication Standards Institute (ETSI). The rapid evolution of the concept comes from numerous isolated use cases of telecommunications operators, which were driven to jointly develop new concepts and standards that today constitute the core of NFV. A number of factors brought good reasons for this cause, such as operating costs and energy, time to implement and deploy new technologies to market, scalable and dynamic management of network services and availability of shared network resources through services and different platforms. Complementary to the promise of Software Defined Networks (SDN) to automate the orchestration and network configuration, NFV proposes automate the deployment and control of network functions, which will run on platforms with virtualized servers. In this context, challenges become inherent in this NFV proposal, which address topics such as interoperability of network platforms, performance tradeoffs, security and resilience. This short course aims to: introduce the concepts and principles of NFV; elucidate the different perspectives that guide its development today, focusing on the ETSI and its working groups, addressing the challenges inherent in its creation and emancipation in the telecommunications operators; raise research topics and works until now published on the subject as well as their main references, and finally, present a demonstration of the network function virtualization technology. Through these objectives, we show both an overview of the state of the art of NFV, and how progress has been made in research since its inception. Afterwards, we will raise a discussion focused on trends in current lines of research around the topic covered in this short course, raising questions that might be addressed in future research by undergraduate and postgraduate, as well as IT professionals.

Resumo

Com aproximadamente um ano após sua criação, o conceito Network Function Virtualization (NFV) tem se mostrado proeminente no cenário de operadoras de telecomunicação. Trazendo a oportunidade de inovar redes de comunicação em uma escala de tempo inimaginável, o conceito já traz consigo atualmente cerca de 150 membros em um grupo de especificações para a indústria (Industry Specification Group – ISG) dentro do European Telecommunication Standards Institute (ETSI). A evolução rápida do conceito advém dos inúmeros casos de uso isolados de operadoras de telecomunicação, as quais foram impulsionadas a desenvolver em conjunto novos conceitos e padrões que hoje constituem o cerne de NFV. Inúmeros fatores trouxeram boas razões para esta causa, tais como: custos de operação e energia, tempo de implementação de novas tecnologias para o mercado, gerenciamento escalável e dinâmico de serviços de rede e disponibilidade de compartilhamento de recursos de rede por meio de serviços e diferentes plataformas. Complementar à promessa de Software Defined Networks (SDN) de automatizar a orquestração e configuração da rede, NFV propõe automatizar a implantação e controle de funções de rede, as quais serão executadas em plataformas com servidores virtualizados. Neste contexto, desafios se tornam inerentes a esta proposta, os quais abordam tópicos como interoperabilidade de plataformas de rede, trade-offs de desempenho, segurança e resiliência. Este minicurso tem como objetivos: apresentar os conceitos e princípios de NFV; elucidar as diferentes perspectivas que hoje guiam seu desenvolvimento, tendo como foco o ETSI e seus grupos de trabalho; abordar os desafios inerentes a sua criação e emancipação nas operadoras de telecomunicação; levantar os tópicos de pesquisa e trabalhos até então publicados sobre o tema assim como suas principais referências; e por fim, apresentar uma demonstração de uma tecnologia de virtualização de função de rede. Por meio destes objetivos, mostraremos tanto uma visão do estado da arte em que se encontra NFV quanto os progressos em pesquisas realizados desde a sua criação. Logo, teremos como foco levantar uma discussão sobre as tendências das atuais linhas de pesquisa em torno do tema abordado neste minicurso, levantando questionamentos que possam ser tratados em futuras pesquisas por estudantes de graduação e pós-graduação assim como profissionais de TI.

Acrônimos

BSS	Business Support Systems
BYOD	Bring Your Own Device
CAPEX	Capital Expenditure
CDN	Content Delivery Network
COTS	Comercial Off-the Shelf
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
IAAS	Infrastructure as a Service
IMS	IP Multimedia Subsystem
ISG	Industry Specification Group
N-POP	Network Point of Presence
NAAS	Network as a Service
NF	Network Function
NFV	Network Function Virtualization
NFV-RES	NFV Resource
NFVI	Network Functions Virtualisation Infrastructure
NFVI-POP	Network Function Virtualisation Infrastructure Point of Presence
NFVIAAS	Network Functions Virtualisation Infrastructure as a Service
NVGRE	Network Virtualisation using Generic Routing Encapsulation
OPEX	Operational Expenditure
OSS	Operational Support Systems
PE	Provider Edge
PNF	Physical Network Function
POP	Point of Presence
SAAS	Software as a Service
SDP	Service Discovery Protocol
SG	Study Group
SLA	Service Level Agreement
VA	Virtual Application

vE-CPE	virtualized Enterprise - Customer Premises Equipament
VNF	Virtual Network Function
VNF FG	VNF Forwarding Graph
VNFaaS	Virtual Network Function as a Service
VNPaaS	Virtual Network Platform as a Service
VxLAN	Virtual Extensible Local Area Network

1.1. Introdução ao conceito de *Network Functions Virtualization*

Há tempos a qualidade no provimento de serviços de redes de computadores e de telecomunicações está atrelada às grandes marcas de fabricantes, responsáveis pelo fornecimento conjunto de software e hardware aos data centers das operadoras. Essa dependência dá-se principalmente pelo fato das tecnologias oferecidas por esses fabricantes atenderem às necessidades de desempenho, estabilidade e disponibilidade requiridas nesse tipo de negócio. Cada fabricante explora ao máximo sua tecnologia, tornando seus softwares somente compatíveis com hardwares cada vez mais específicos, aproveitando ao máximo os detalhes de suas plataformas na busca de maior eficiência de todo ambiente.

Obviamente, essa abordagem contribui para que as tecnologias de fabricantes diferentes sejam incompatíveis umas com as outras. Por exemplo, dificilmente é possível implantar o software de um fabricante na plataforma de outro. O acoplamento entre software e hardware de um mesmo fabricante é tão forte que a migração de plataforma pode ser inviável. Códigos fontes proprietários e restrições de licenciamento também contribuem para essa limitação.

Situações como essas tornaram a tecnologia cara e de difícil acesso às empresas consumidoras. Uma vez que a dependência a essas plataformas existe, manter um ambiente funcional corresponde à necessidade de instalação de diversos equipamentos proprietários (ex: middleboxes), cada um responsável por uma fatia pequena do processamento total, mas que necessitam de todo um gerenciamento e licenciamento específicos. Também são comuns a falta de integração entre as tecnologias, visto que nem sempre um mesmo fabricante atende todas as áreas de interesse da empresa; o desenvolvimento de soluções específicas para as necessidades do cliente fica prejudicada, devido ao fato de naturalmente as tecnologias fornecidas serem projetadas para atender às necessidades gerais de vários clientes; dificuldades na operacionalização do ambiente, uma vez que há necessidade de mão-de-obra qualificada para cada tipo de tecnologia, pois, mesmo que a função base seja a mesma, as diferenças e detalhes de cada implementação tornam o processo diferente o suficiente entre fabricantes, sendo necessário profissionais com perfis específicos para operar plataformas de fabricantes diferentes. Problemas como alto custo de espaço, implantação e consumo energético também são comuns a esse tipo de ambiente.

Por estas e outras razões históricas, as principais empresas de telecomunicações do mundo se uniram para construir a definição de um novo conceito para o provimento dos serviços de redes e telecomunicações: *Network Function Virtualization* (NFV). Em sua essência, NFV é responsável pelo oferecimento das funções de rede através de serviços virtualizados em servidores de uso geral. As vantagens proporcionadas por NFV vão de encontro às limitações impostas pelas tecnologias proprietárias convencionais expostas anteriormente, porém, novos requisitos se fazem presentes aos seus desenvolvedores, como a necessidade de garantir interoperabilidade, alto desempenho e portabilidade das funções de rede. Na mesma linha, novos desafios também devem ser superados para que o NFV possa ser considerado maduro suficiente para sua implantação em ambientes reais.

Com base nas definições do NFV, esse minicurso apresenta de forma aprofundada as características técnicas do NFV, seus requisitos, desafios e atual situação dos trabalhos relacionados à evolução dessa tecnologia. De forma específica, a seção 2 apresenta

os fundamentos e aspectos teóricos do NFV, sendo responsável por detalhar sua terminologia e estrutura. A seção 3 apresenta os desafios dessa plataforma com base em seus requisitos, sendo seguido pela seção 4 que traz o detalhamento do esforço desenvolvido para evolução do NFV, através dos casos de uso e provas de conceito atualmente em desenvolvimento. Essa seção é complementada pela apresentação de algumas tecnologias habilitadoras aos NFV. Finalizando, a seção 5 conclui o assunto abordado nesse minicurso.

1.2. Fundamentos e Aspectos Teóricos

Esta sessão aborda a terminologia básica da Virtualização de Funções de Redes, ou *Network Function Virtualization (*NFV*)*. A idéia é apresentar seus principais conceitos, objetivos e metas em torno do desenvolvimento deste conceito surgido da iniciativa da indústria de operadoras de redes de telecomunições. Serão expostos os principais termos como NFV *Forwarding Graphs*, *Physical Network Function*, NFV *Network Infrastructure*, entre outros, que formam o vocabulário dessa nova tecnologia. Estes fundamentos formarão os alicerces para entender os requisitos e desafios de NFV, na seção posterior. Além disso, a explicação dessa nomenclatura tem como foco o grupo de trabalho em NFV dentro da *European Telecommunications Standards Institute (*ETSI*)* e a proposta de arquitetura de referência (ainda em desenvolvimento) que permitirá entender como são constituídos cada um dos elementos de uma infraestrutura de NFV, como eles interagem entre si e com a infraestrutura subjacente.

1.2.1. Principais objetivos e Metas de NFV

NFV possui os seguintes objetivos principais:

Melhor eficiência nos gastos de capital (CAPEX) comparando-se a implementações com hardware dedicado. Isto é alcançado utilizando hardware comercial de uso geral (ex: servidores e *storage*) para prover funções de dispositivos de rede através de técnicas de virtualização. O compartilhamento de hardware para realização de diferentes funções, bem como a redução dos tipos de dispositivos utilizados na rede, podem auxiliar na redução de CAPEX.

Flexibilidade na designação das funções de rede para um hardware de propósito geral. Isto permite obter escalabilidade, já que desacopla as funcionalidades de hardware e locais específicos, permitido que as funções (software) virtualizadas sejam posicionados de forma flexível nos locais mais apropriados. Esses locais são chamados de NFVI-PoPs, e as funcionalidades migram para esses locais, dependendo das condições externas como demanda, falhas, horário do dia, política de compartilhamento de recursos, ciclo de liberação (Ex.: versões alfa, beta, produção). Os NFVI-PoPs podem incluir sites de clientes, pontos de troca de tráfego (PTTs), centrais de operadoras, data centers, entre outros.

Rápida implementação de novos serviços sem necessidade de alterações em plataformas de hardware.

Melhora de eficiência nos processos operacionais através da automatização destes processos, resultando em uma drástica redução em custos operacionais (OPEX).

Redução na utilização de energia elétrica contribuindo com as iniciativas *green networks*, já que permite a migração de cargas e desligamento de hardware não utilizado.

Padronização e abertura de interfaces entre funções virtualizadas e a infraestrutura com as entidades de gerenciamento, de forma que os diferentes elementos possam ser oferecidos por diferentes fornecedores de forma desacoplada.

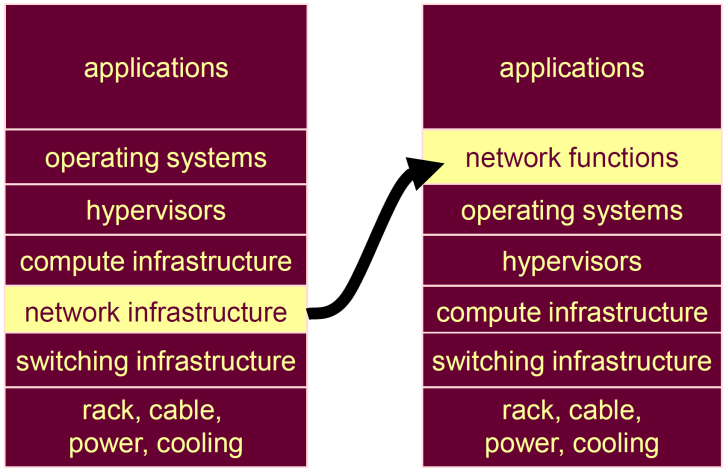


Figure 1.1. Mudança do modelo em camadas introduzido pelo paradigma NFV. Fonte: [1]

1.2.2. Modelo em camadas

A introdução da funcionalidade da rede como implementação em ambientes de computação virtualizados traz mudanças no modelo de camadas OSI comumente usado para descrever arquiteturas de redes e computadores. A Figura 1.1 ilustra a dependência de uma aplicação na pilha de sistemas das camadas inferiores. No modelo NFV (Fig. 1.1 à direita) as funções de rede não mais dependem diretamente da infraestrutura física de comunicações e são implementadas no domínio de software como aplicações de alto nível que dependem do sistema operacional e das camadas de virtualização presentes na infraestrutura computacional. O trade-off entre desempenho e flexibilidade (assim como as implicações de segurança) do modelo NFV é um dos aspectos principais introduzidos nesse novo paradigma de redes.

1.2.3. Terminologia

A seguir são introduzidos os principais termos debativos nos trabalhos de padronização de NFV (ex: [2]).

NFV Framework A totalidade das entidades, pontos de referência, modelos de informação e outras formas de construção definidas por especificações publicadas pelo ISG NFV do ETSI.

Network Function (NF) Um bloco de construção funcional dentro de uma infraestrutura de rede, a qual tem *interfaces* externas e comportamento funcional bem definido. Em termos práticos, uma NF é hoje frequentemente um nó da rede (ex: switch, roteador) ou um *appliance* físico (ex: firewall, IDS).

Physical Network Function (PNF) Uma implementação de uma NF via um sistema de hardware e software bem acoplados.

Virtualised Network Function (VNF) Uma implementação de uma NF que possa ser implantada em uma infraestrutura de NFV.

NF Set Um conjunto de NFs com conexões entre si não especificadas.

NF Forwarding Graph Um grafo com enlaces lógicos conectando nós NF com a finalidade de descrever um fluxo de tráfego entre estas funções de rede.

VNF Forwarding Graph (VNF FG) É definido como um grafo de encaminhamento onde pelo menos um de seus nós seja uma VNF. Define uma cadeia de serviços quando a ordem de conectividade na rede é importante, tais como firewall, NAT, ou balanceador de carga.

Virtual Application (VA) Uma aplicação virtual é um termo mais geral para um pedaço de software que pode ser carregado em uma máquina virtual. Por exemplo, uma VNF é um tipo de VA.

NFV Service Um serviço de rede utilizando NFs, onde ao menos algumas NFs são VNFs. Um grafo de encaminhamento VNF é um exemplo de tal serviço.

NFV Infrastructure (NFVI) É a totalidade de todos os componentes de hardware e software que constituem o ambiente no qual VNFs são implementadas. A NFVI pode estar constituída através de várias localizações, i.e. múltiplos N-PoPs. A rede provendo conectividade entre estas localizações define-se como parte da NFVI.

Network Function Virtualisation Infrastructure Point of Presence (NFVI-PoP) Constituí o local onde funções de rede estão ou poderiam ser implementadas como VNFs.

Network Point of Presence (N-PoP) A localidade onde uma função de rede (NF) é implementada ou como função física (PNF) ou virtual de rede (VNF).

NFV-Resource (NFV-Res) Recursos de NFV existem dentro de uma infraestrutura de NFV e podem ser utilizados por VNFs a fim de permitir que elas sejam executadas propriamente.

VNF Descriptor (VNFD) Uma abstração (*template*) de configuração que descreve uma VNF em termos de seus comportamentos de implementação e operacional. Essa abstração é utilizada no processo de implantação e instanciação de uma VNF. O comportamento de instanciação descreve os recursos de NFVI que uma instancia de VNF requer, enquanto que o comportamento operacional descreve as operações de instâncias, de topologia e de ciclo de vida, da VNF.

NFV Orchestrator O orquestrador de NFV tem a responsabilidade de orquestrar e gerenciar de forma ampla os recursos de NFV (infraestrutura e software), e ter conhecimento da topologia de serviços sobre a NFVI[1].

[1] O NFVO opera, gerencia, e automatiza a infraestrutura distribuída de NFV. Ele tem controle e visibilidade de todas as VNFs sendo executadas dentro da NFVI. Além disso, ele faz uso intenso do sistema operacional de NFV para realizar as tarefas de automação e operação, logo, estendendo as capacidades básicas deste sistema para um ambiente operacionalmente diversificado.

1.2.4. Arquitetura de Referência para NFV

A virtualização de funções de rede (NFV) visa a implementação de funções de rede (NF) como entidades de software que rodam sobre a infraestrutura NFV (NFVI). Portanto, foi definida uma arquitetura de referência para a implementação de NFV pelo ETSI [3] que objetiva permitir a instanciação dinâmica de funções de rede virtuais (ou seja, as instâncias de VNFs), bem como a relação entre estas relacionado a dados, controle, dependências, conectividade, entre outros atributos.

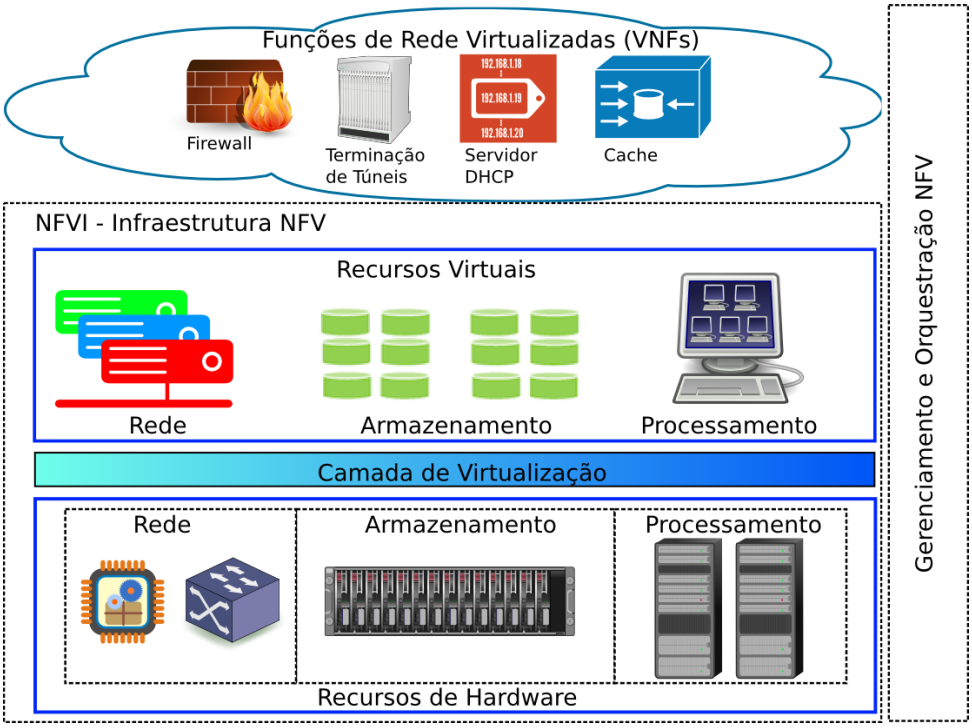


Figure 1.2. Arquitetura de alto nível para NFV.

Observa-se que pode existir relação de conectividade de rede entre diferentes VNFs, sendo esta definida como grafos de encaminhamento entre VNFs (VNF-FG), os quais podem definir, por exemplo, a conectividade lógica entre VNFs relativas a *firewalls*, balanceadores de carga, NAT, servidores Web, entre outros para o provimento de um serviço.

A Figura 1.2, a seguir, ilustra a arquitetura de alto nível para virtualização de funções de redes. A Arquitetura é dividida em três blocos funcionais principais, que serão mais detalhados a seguir:

- Funções de rede virtualizadas (VNFs)
- Infraestrutura NFV (NFVI)
- Gerenciamento e orquestração NFV.

1.2.4.1. Blocos funcionais

Funções de Rede Virtualizadas (VNF). VNF é a virtualização de funções de redes. Exemplos de funções de rede incluem as desempenhadas por roteadores, *firewalls*, *gateways* residenciais, elementos da arquitetura 3GPP como o MME (*Mobility Management Entity*), PGW (*Packet Data Network Gateway*), servidores de autenticação, servidores DHCP, entre outros. Uma função de rede pode ser decomposta em diferentes componentes externos, os quais podem sem implementados em diferentes máquinas virtuais. No entanto, o comportamento funcional de uma função de rede deve ser independente, se tal função é virtualizada em múltiplas VMs, em uma única VM ou não é virtualizada.

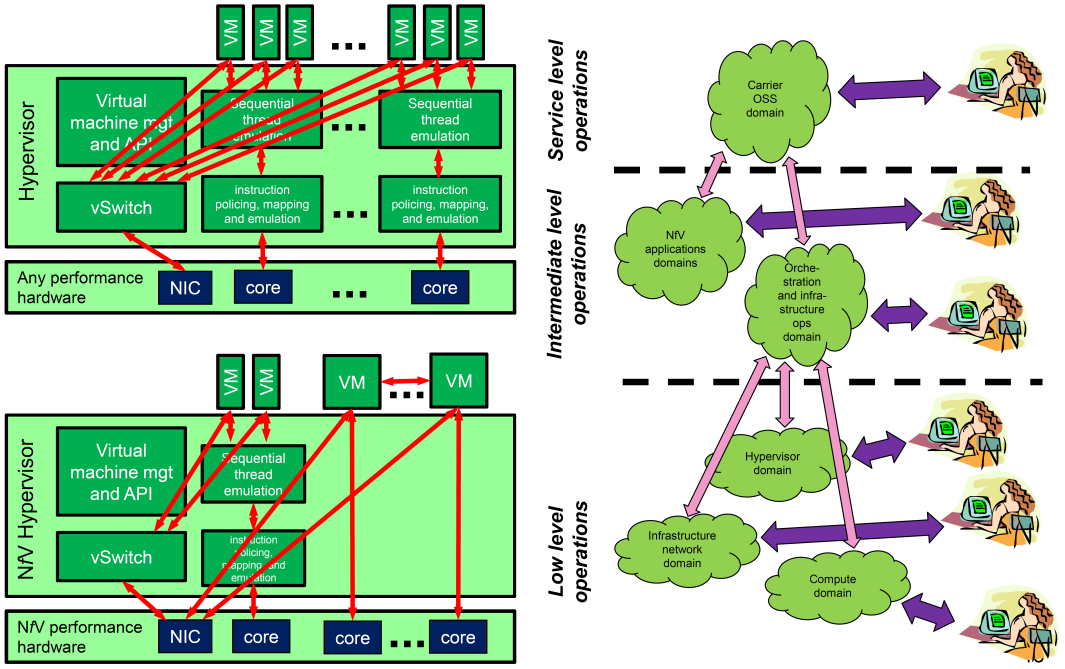
Infraestrutura para NFV (NFVI). NFVI é a composição dos recursos de hardware e software necessários para a implementação, execução, e gerenciamento das VNFs. A infraestrutura para o provimento de NFVI pode ser distribuída em diferentes localidades (Ex.: diferentes NFVI-PoPs), de forma que a rede que provê conectividade entre os NFVI-PoPs faz parte da NFVI. No entanto, a camada de virtualização para os recursos de hardware visto pelas VNFs permite que a NFVI possa ser vista como uma entidade única.

Ainda dentro da NFVI, os **recursos de hardware** incluem recursos que provêm processamento, armazenamento e conectividade para as VNFs, através da camada de virtualização. É fundamental que os recursos de hardware sejam de propósito geral, referidos como COTS (*Commercial off-the-shelf*). Interconectando esses recursos, há dois tipos de redes: as redes internas dos NFVI-PoP e as redes de transporte que os interconectam.

Além disso, a **camada de virtualização** também é importante em NFVI, pois ela abstrai os recursos de hardware, desacoplando o software das VNFs de hardware especializado, portanto garantindo independência do tipo de hardware a ser utilizado. Isto é feito através do particionamento lógico dos recursos (*slicing*) entre VNFs. Dessa forma, provendo os recursos lógicos para as VNFs através de uma camada de abstração de hardware. Tipicamente, o desacoplamento dos recursos de computação e armazenamento do software é realizado através de *hypervisors*, como Xen, VMWare, etc, que permitem a execução de diversas máquinas virtuais (VMs) em hardware de propósito geral.

No entanto, é importante notar que uma VNF poderia ser executada em uma ou mais VMs. Desse modo, na arquitetura de referência para NFV definida pelo ETSI [3] (Figura 1.2), não é definida uma solução específica para a camada de virtualização. Ou seja, espera-se que seja definida uma padronização mais adequada para a abstração do hardware. De qualquer modo, o uso de *hypervisors* é uma das soluções atuais para tal camada. No domínio da conectividade dessa camada de virtualização, várias técnicas têm sido utilizadas para a virtualização de recursos de rede, de forma a prover conectividade entre as VMs de uma mesma VNF, incluindo VxLANs (*Virtual Extensible Local Area Network*), NVGRE (*Network Virtualisation using Generic Routing Encapsulation*) e OpenFlow.

A implementação de funções de rede em *hypervisors* pela prestação de serviços de rede pela computação em nuvem. Nesse caso, como visto na Figura 1.3(a), a diferença entre a proposta de um NfV hypervisor e outro comum, é a permissividade de acesso direto às funções de processamento e rede, ou mesmo pela permissão de comunicação direta entre VMs. Tais avanços em tecnologias de hypervisor adequadas para o modelo



(a) Domínio de hypervisor (b) Orquestração de NFs a nível de hypervisors

Figure 1.3. Composição de NFs por orquestração em hypervisors [1].

NFV são atualmente ativos alvos de pesquisa (ex: ClickOS, VALE, etc.) [4].

Os esforços em novos projetos de *hypervisors* incluem também a utilização de técnicas de virtualização leve (*Lightweight Virtualisation*). O modelo tradicional de VMs (virtualização completa ou paravirtualização) implica um alto custo em termos de recursos (memória, CPU, disco) para cada máquina virtual. Tal abordagem limita o número máximo de VMs que podem ser executadas em paralelo em cada servidor (na ordem de dezenas) assim como introduz restrições em relação ao tempo mínimo para inicio (*bootup*) das VMs.

A figura 1.4 apresenta as diferentes hierarquias de virtualização que oferecem múltiplos ambientes de execução possíveis (servidor, VM, Linux contêineres, processo, thread). Cada ambiente virtualizado traz diferentes níveis de desempenho e isolação (incluindo aspectos de segurança). Avanços recentes em tecnologias de virtualização (mais detalhes na seção 1.4.0.3) tem reduzido o *overhead* de consumo de recursos de cada instancia virtual, fato que abre novas oportunidades para a escalabilidade das soluções de NFV com base a um mapeamento otimizado entre a aplicação que implementa a função de rede é a "máquina virtual" onde é executada.

Gerenciamento e Orquestração.

Os gerenciadores da infraestrutura virtualizada controlam a interação da VNF com os recursos físicos sob sua autoridade, realizando gerenciamento de recursos (ex: alocação, desalocação e inventário), além de operações como visibilidade da infraestrutura, coleta de informações para gerência de falhas e desempenho. Por outro lado, os gerenciadores das VNFs são responsáveis pelo gerenciamento do ciclo de vida das VNFs,

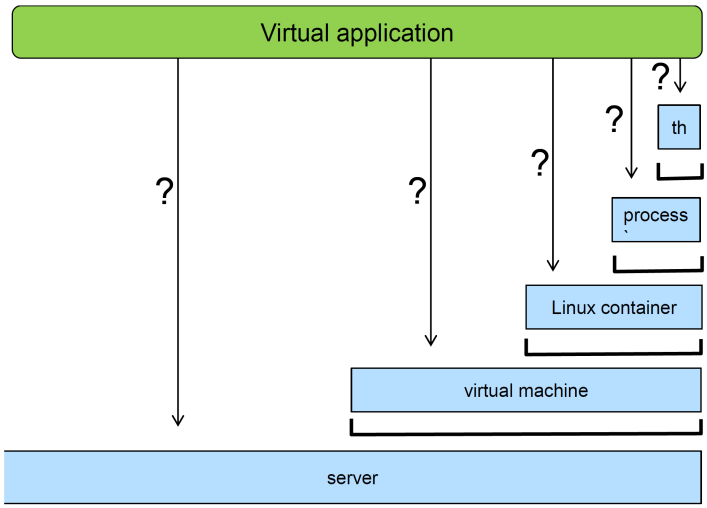


Figure 1.4. Diferentes opções disponíveis para implementar aplicações virtualizadas.

incluindo operações como instanciação, atualização e finalização.

A constituição de aplicações de NFV sobre o modelo de *hypervisor* permite que softwares de orquestração (ex: vSphere, OpenStack, CloudStack) selecionem, configurem e inicializem VMs e hosts de acordo com operações de serviço de alto nível (vide Figura 1.3(b)) para especificação de perfis de aplicações com configurações específicas segundo sua localização e serviço de rede. Dessa maneira as tarefas de orquestração e gerenciamento se tornam flexíveis a ponto de constituírem cadeias de serviços facilmente por meio da programação de elementos nas bordas da rede.

Outras entidades envolvidas no Gerenciamento de NFV, incluem o **EMS** (*Element Management System*) que provê funções típicas de gerenciamento para uma ou mais VNFs, e também o **Orquestrador**, responsável pelo gerenciamento dos serviços, orquestrando recursos de infraestrutura e de software para as VNFs. Finalmente, temos a **Base de Configuração** que inclui informações de configuração dos serviços, das VNFs e da infraestrutura, e também inclui *templates* para a implementação de VNFs, grafos de encaminhamento das VNFs e informações relativas aos serviços e infraestrutura.

1.2.4.2. Pontos de Referência

Após uma explicação sucinta da arquitetura em alto nível. Descreveremos detalhes da Arquitetura de Referência sendo definida pelo ETSI [3] na Figura 1.5. Nesta figura, além dos blocos funcionais, vistos anteriormente, foram incluídos o posicionamento dos Sistemas de Suporte Operacional (*Operational Support Systems - OSS*) que são responsáveis por suporar processos internos da operadora como inventório de rede, provisionamento de serviços, configuração de elementos de rede e gerenciamento de falhas. Bem como, em complemento, os Sistems de Suporte ao Negócio (*Business Support Systems - BSS*) que são os sistemas que lidam com solicitações dos usuários, suportando processos como processamento de cobranças, ordens de serviço, entre outros.

Finalmente, na figura também aparecem os chamados, pontos de referência, ou seja, os pontos de *interface* entre os diferentes componentes e/ou camadas na arquitetura. Os pontos de interface tem os nomes compostos pelas iniciais dos sistemas que eles interligam. Por exemplo, o ponto de referência **Os-Ma** interconecta o sistema OSS com o sistema de gerenciamento e orquestração de NFV. A seguir, apresentaremos em detalhes os pontos de referência, começando pela interação dos elementos internos e depois os elementos com o gerenciamento.

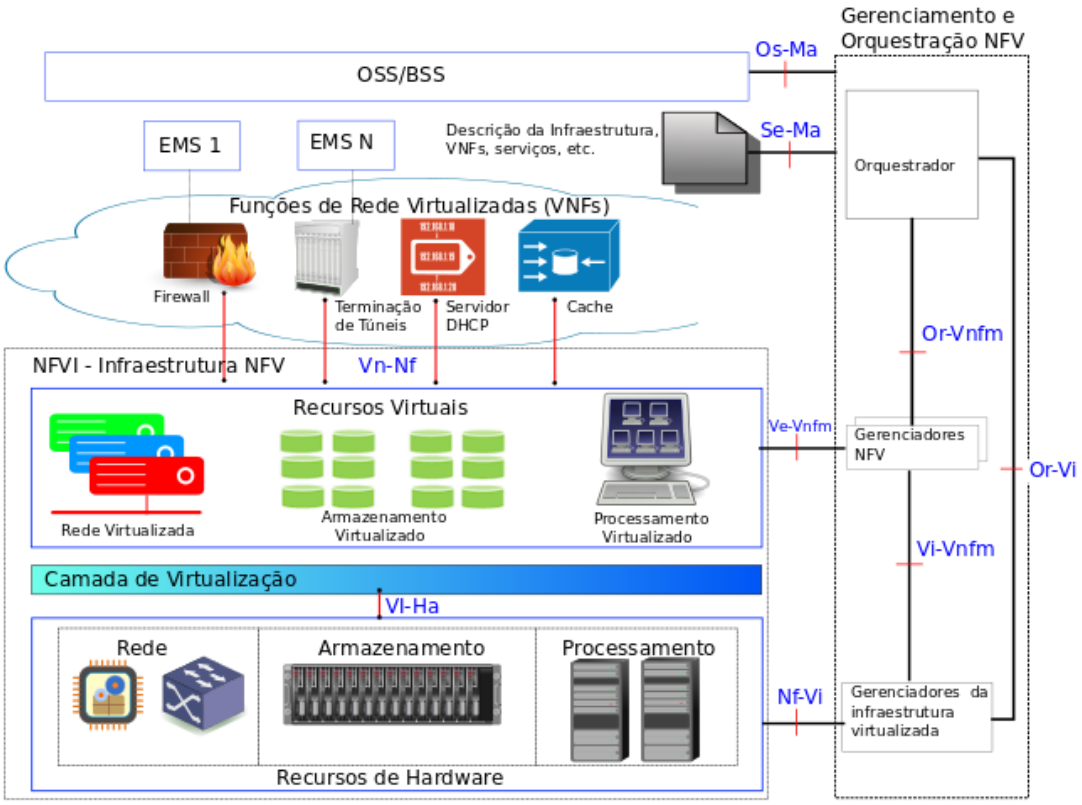


Figure 1.5. Arquitetura detalhada proposta pelo ETSI SG NFV.

Vl-Ha – Camada de Virtualização – Recursos de Hardware. O ponto de referência Vl-Ha faz a interface entre a camada de virtualização e os recursos de hardware, criando um ambiente para a execução das VNFs, independente de plataformas de hardware específicas.

Vn-Nf : VNF – Infraestrutura NFV. O ponto de referência Vn-Nf representa o ambiente de execução provido pela NFVI às VNFs, garantindo um ciclo de vida independente de tipo de hardware, atendendo aos requisitos de desempenho, portabilidade, entre outros das VNFs.

Or-Vnfm : Orquestrador – Gerenciador de VNFs. O ponto de referência Or-Vnfm é responsável pelas seguintes funções:

- Requisições relativas a recursos, como autorização, validação, reserva e alocação pelos gerenciadores de VNFs;

- Envio de informações de configuração ao gerenciador de VNFs, de forma que a VNF possa ser configurada de forma apropriada para sua função específica no Grafo de Encaminhamento de Funções de Rede (NF Forwarding Graph);
- Coleta de informações de estado das VNFs, necessário para gerenciamento do ciclo de vida da rede.

Vi-Vnfm : Gerenciador de Infraestrutura Virtualizada – Gerenciador de VNFs. O ponto de referência Vi-Vnfm é responsável por:

- Requisições de alocação de recursos realizadas pelo gerenciador de VNFs;
- Configuração de recursos de hardware virtualizado e troca de informações de estado (ex: eventos).

Or-Vi : Orquestrador - Gerenciador de Infraestrutura Virtualizada O ponto de referência Or-Vi é utilizado para:

- Reserva de recursos e/ou requisições de alocação pelo orquestrador;
- Configuração de recursos de hardware virtualizado e troca de informações de estado (ex: eventos).

Nf-Vi : NFVI - Gerenciador de Infraestrutura Virtualizada O ponto de referência Nf-Vi é utilizado para:

- Designação específica de recursos em função de requisições de alocação;
- Encaminhamento de informações de estado de recursos virtualizados;
- Configuração de recursos de hardware e a troca de informações de estado (ex: eventos).

Os-Ma : OSS/BSS – Gerenciamento e Orquestração de NFV O ponto de referência Os-Ma é utilizado para:

- Requisições para gerenciamento do ciclo de vida dos serviços de rede;
- Requisições para gerenciamento do ciclo de vida das VNFs;
- Encaminhamento de informações de estado das VNFs;
- Trocas de informações de políticas e dados analíticos;
- Encaminhamento de registros de utilização (contabilização);
- Troca de informações de inventário e capacidade da NFVI.

Ve-Vnfm – VNF/EMS – VNF Manager O ponto de referência Ve-Vnfm é utilizado para:

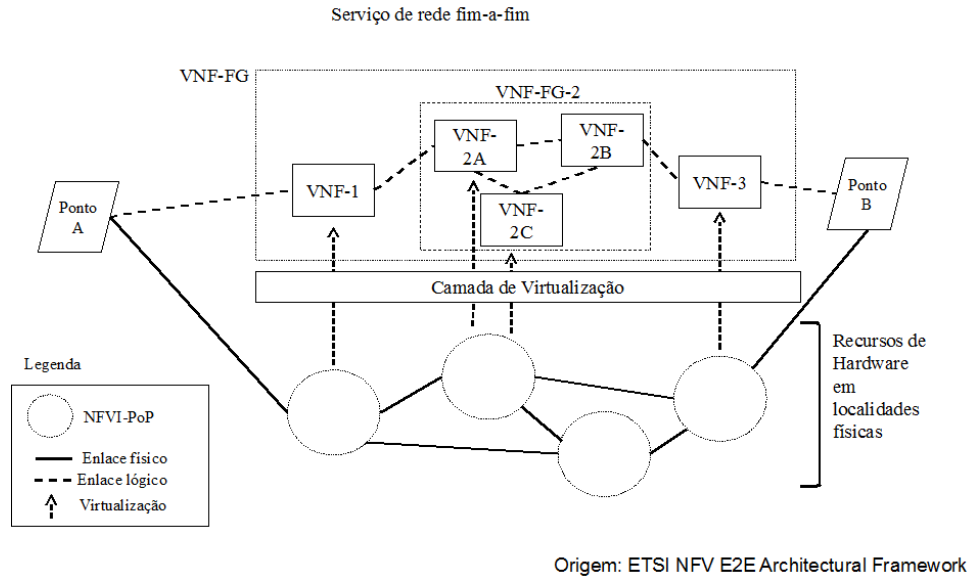


Figure 1.6. Exemplo de um serviço de rede fim-a-fim com VNFs e VNF-FGs aninhados.

- Requisições para gerenciamento do ciclo de vida de VNFs;
- Troca de informações de configuração;
- Troca de informações de estado necessárias para o gerenciamento do ciclo de vida dos serviços de rede.

1.2.5. Composição de Serviços de Redes

Para demonstrar a arquitetura de referência em execução, é preciso definir os serviços de rede (ex: Acesso Internet banda larga, VPN, serviço web). Esses serviços fim-a-fim podem ser descritos no ambiente NFV, por um Grafo de Encaminhamento de Funções de Rede (*NF Forwarding Graph*). Desta forma, o comportamento de um serviço de rede é a combinação do comportamento de seus blocos funcionais, que podem incluir Funções de Rede (NFs) individuais, conjuntos de NFs, outros Grafos de Encaminhamento de NFs, e/ou infraestrutura de rede.

A Figura 1.6 mostra um exemplo de um serviço de rede fim-a-fim e as diferentes camadas envolvidas no processo de virtualização deste. Os NFVI-PoPs possuem recursos de armazenamento, processamento e rede, bem como conectividade entre estes. O VNF-FG é composto por duas VNFs (VNF-1 e VNF-3) interconectadas por um VNF-FG aninhado (VNF-FG-2) que é composto por três VNFs (VNF-2A, 2B e 2C). As funções de virtualização são instanciadas sobre a Camada de Virtualização, permitindo que a localização física e quais recursos físicos estão utilizados para o provimento das VNFs e do serviço sejam abstraídos.

1.2.6. Reflexões sobre a Arquitetura de Referência NFV

A arquitetura de referência NFV apresenta muita flexibilidade na construção de serviços de rede distintos, sob-demanda, com rápida implantação. Algumas provas de conceito

dessa arquitetura estão sendo propostas, e abordaremos alguns exemplos na seção 1.4. Porém, será que ela atende bem os desafios e expectativas da comunidade de operadoras de rede, na próxima seção abordaremos alguns desses questionamentos, explicando os requisitos e desafios.

1.3. Requisitos e Desafios de NFV

Diante das perspectivas de crescimento dos atuais planos de implementação dos fundamentos de NFV em provas de conceito, alguns questionamentos surgem e levantam requisitos de resolução ainda estão não observados pelas empresas de telecomunicação. Por exemplo, a virtualização de redes de acesso fixas (vCPE), onde equipamentos de rede situam-se na fronteira entre usuários e provedores de serviços, traz consigo as propriedades de portabilidade e elasticidade, as quais irão suprimir custos de serviços operacionais das empresas de telecomunicação. No entanto, tais primitivas por si só já se tornam desafios em um ambiente com necessidades de resiliência e segurança [20].

Nesta seção, abordaremos os principais desafios que NFV vem construindo com a definição de requisitos [6] e provas de conceito de virtualização de funções de rede [7]. O foco será dado a contextualização dos conceitos fundamentais de NFV e como seus requisitos implicam o surgimento de diversos desafios. Estes podem ser definidos em tópicos como: cadeias de serviços; trade-offs de desempenho; portabilidade, interoperabilidade de plataformas NFV e coexistência de plataformas legadas; gerenciamento, orquestração e automação de arquiteturas e funções de rede; segurança; resiliência; e integração de SDN e NFV.

1.3.1. Especificações de VFNGs (cadeias de serviços) e VNFs em VNFGs

O desenvolvimento de padrões de NFs bem como de suas diferentes funcionalidades e interfaces de comunicação, seja com outras NFs e/ou recursos físicos, é uma tarefa que abrange a terminologia recomendada pelo ETSI, a qual permite um amplo espectro de características a serem propostas em PoCs [19]. Como estipulado pela terminologia anteriormente definida, relações de VNFs constituem VNFGs os quais definem a composição de um ou mais serviços de rede. Logo, agregar serviços a ponto de permitir a formação de cadeias é uma tarefa que exige não só a definição de características de NFs e suas respectivas interfaces como também de ações e suas respectivas propriedades que irão ser executadas sobre o tráfego a ser conduzido em um VNFG. Em termos simples, tornar uma cadeia de NFs funcional a ponto de ser utilizada em um domínio específico de rede, seria, por exemplo, agregar e orientar determinadas funcionalidades de DHCP, firewall e roteamento em gateways residenciais (ex: BRAS) [9]. Este é um requisito de NFV que agrega em si praticamente todos os desafios descritos nesta seção, os quais estão sendo já discutidos pela comunidade acadêmica [10] e pelo IETF [11]. A figura 1.7 abaixo, representa a dualidade entre o modelo atual (em linha alaranjada) de cadeias de serviços e o modelo proposto por NFV (em linha preta pontilhada).

Como requisitos gerais, VNFGs podem ser compostos por VNFs e PNFs, definindo um framework NFV o qual pode compor diversos serviços. Além disso, tal implementação pode ser constituída sobre um ambiente com múltiplos provedores de serviços em N-POPs compartilhando um ambiente de NFVI com um ou mais operadores. Tomando como base este exemplo, podemos notar os desafios que se agregam em tal ambiente. As relações entre VNFs e PNFs constituem particularidades que podem repercutir em outros desafios, como elasticidade e desempenho. Tais particularidades, que interfaces entre NFs podem trazer, estão suscetíveis ao ambiente em que elas são implementadas, como equipamentos BRAS e v-CPE.

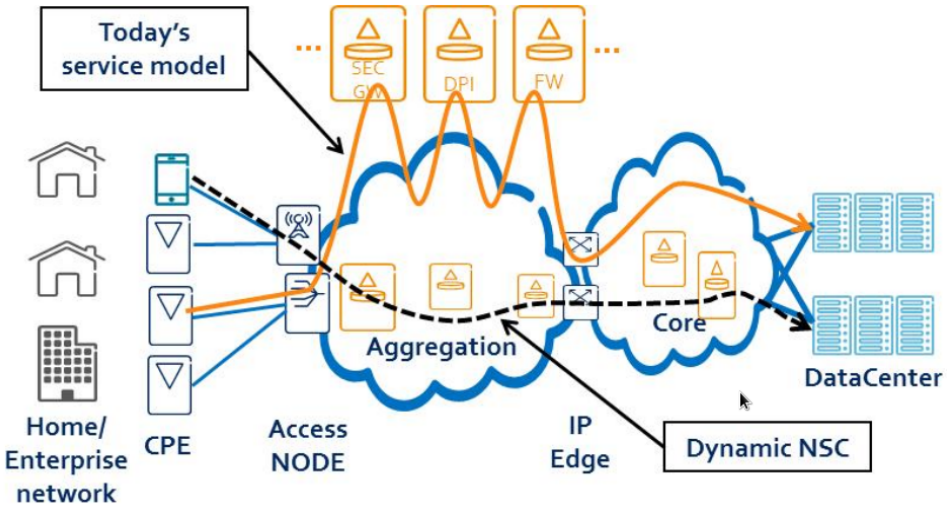


Figure 1.7. Comparação entre cadeias de serviços atual e de NFV.

Além dos fatores de interfaces entre NFs, a própria constituição de cadeias de serviços pode trazer desafios na construção de VNFGs. Isto envolve a repartição e montagem de uma função de rede por diversas subdivisões de tarefas, como por exemplo, a tarefa de DPI subdividida em um componente complexo de classificação de tráfego, um componente de cache de fluxos que mantém registro do tráfego já identificado, e outro componente aplica as políticas pré configuradas. Nesse sentido, tais desafios, de forma semelhante a terceirização de funções de rede por subcomponentes de rede, podem ser definidos por três critérios: semânticas de processamento; garantias de desempenho; e verificações de custos [12]. Nas subseções seguintes, outros desafios relacionados a cadeias de serviços também serão tratados nos seus devidos pormenores, tais como segurança e resiliência. Abaixo seguem alguns exemplos dos desafios citados.

Semânticas de processamento dizem respeito a operações que NFs podem realizar em fluxos de tráfego, tornando estes suscetíveis a falhas de processamento por outras NFs. Por exemplo, em uma cadeia de NFs (NF1, NF2, ...), NF1 sendo um balanceador de carga pode realizar modificações nos pacotes com a consequência de que NF2, sendo por exemplo um IDS, descarte-os. Nesse caso, um provedor de serviço, utilizando esta cadeia de NFs, não terá informações se o descarte dos pacotes foi causado pela rede (ex: buffers cheios) ou pela constituição errada de NFs.

No caso de garantias de desempenho, um provedor de serviço necessita saber que suas aplicações não sofram perda de desempenho por overheads inseridos pela comunicação entre NFs de um VNFG requisitado. O desafio, neste caso, surge da ocorrência de efeitos não determinísticos causados por operações em nível de rede e pela própria rede. No caso de operações, NFs podem realizar processamento de pacotes em batch ou atrasá-los para eliminação de redundâncias. No segundo caso, congestionamentos por filas cheias ou falhas em computações de rotas podem ser os causadores comumente vistos em ambientes não virtualizados.

As cobranças realizadas sobre serviços prestados por NFs também podem ser afetadas caso VNFGs que as contenham possuam inconsistências em medições de cargas de

trabalho das funcionalidades contratadas. Um cliente não é capaz de medir o consumo de recursos contratado em uma determinada NF caso esta esteja operando com anormalidades que estejam sendo geradas por outras NFs do mesmo VNFG em que todas elas se inserem. Nesse caso, segue como critério rígido a definição de métodos de medição e validação de NFs bem como de suas interações com outras NFs para a definição de uma cadeia de serviços. Portanto, segue destes tópicos a relevância na construção de provas de conceito (PoCs) bem detalhadas e especificadas para NFV.

1.3.2. Desempenho e escalabilidade

A grande premissa de NFV é o suporte de grande volume de servidores de baixo custo desempenhando papéis diversos a NFVI para tornar eficiente a alocação dinâmica de recursos a diferentes VNFs. Abordar a utilização eficiente de recursos virtualizados requer que estes sejam escaláveis às dimensões dos serviços oferecidos por VNFs assim como que estas, definidas em uma vasta heterogeneidade (ex: firewall, DPI, BRAS), possam utilizar aplicações do plano de dados de maneira customizada às suas necessidades [6].

Em escalas geográficas diferentes, partindo de data centers a WANs, a capacidade de adequação das atuais tecnologias de virtualização, principalmente no que se diz respeito a equipamentos de rede, pode possuir diferentes peculiaridades. Por exemplo, atualmente roteadores de grandes domínios da Internet, cerca de milhares em todo mundo, possuem grandes buffers, fazem uso de grandes quantidades de memória para armazenamento de suas tabelas BGP, e logo se diferenciam de equipamentos de rede de data centers, cerca de 100 mil em um único data center, onde se preza por filas e tabelas de encaminhamento pequenas devido a natureza do tráfego deste ambiente. Essa diferença de cenários, em termos de escala e requisitos de operações, é um dentre os fatores discutidos nesta subseção que tornam complexo o desenvolvimento de tecnologias de virtualização de funções de rede flexíveis e elásticas [13].

Em requisitos de desempenho de tecnologias de virtualização de NFs, os seguintes parâmetros se destacam: uma instância de VNF deve ter suas especificações de desempenho bem definidas para operar conforme os recursos disponíveis da infraestrutura compartilhada/isolada em que for instanciada; e formas de coletar informações sobre armazenamento, rede e processamento de VNFs devem ser bem definidas e consequentemente realizadas em diferentes níveis de infraestrutura (ex: hypervisor, servidores, VMs). Estes requisitos irão influenciar muito na continuidade de existência de NFs e do próprio conceito de NFV. No caso, tecnologias de virtualização terão possivelmente, e inicialmente, comportamentos não tão bons quanto middleboxes dedicadas, mas trarão a flexibilidade necessária para fornecer elasticidade a funções de rede (ex: BRASes [9]). Nesse caso, bem melhores estabelecidas e garantidas, caso elas possam ser monitoradas de forma escalável em diversos níveis de operação e granularidade, fornecendo portanto, estados consistentes de NFs e seus respectivos ambientes.

Tecnologias já existentes e habilitadoras (ex: DPDK, ClickOS) trarão os requisitos de operação esperados a atender diferentes escalas de usuários e NFs para dar suporte aos demais desafios de NFV, tais como balanceamento de carga dinâmico e automatizado. É importante analisar, como na figura 1.8 (eixo x em escala contínua e eixo y em escala logarítmica), observações interessantes sobre a complexidade de uso versus a eficiência

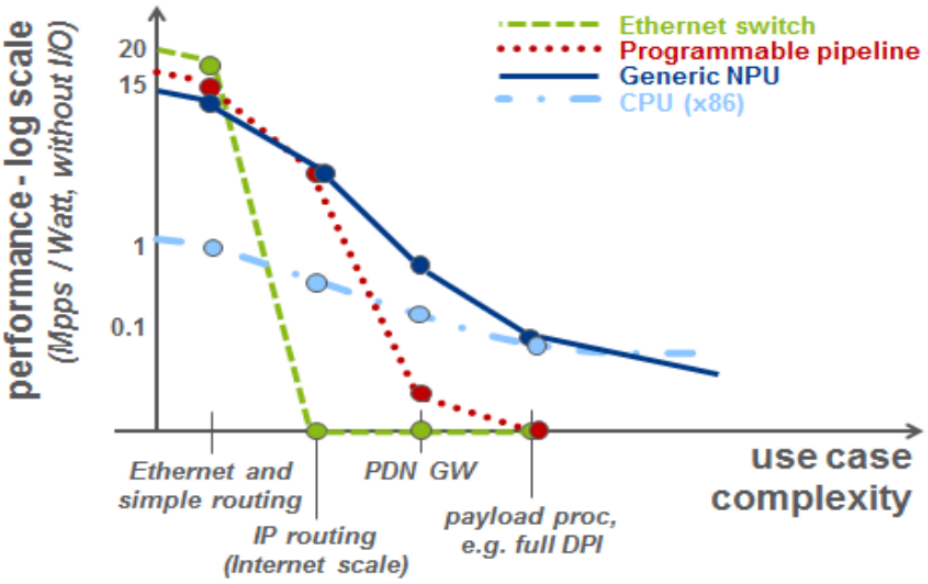


Figure 1.8. Eficiência de chip vs. complexidade de caso de uso [14].

de chips utilizados em redes que estão permitindo e irão habilitar o conceito de NFV, tais como: a complexidade de uso cresce conforme o desempenho de todas as soluções decrescem; chipsets de propósito único são limitados, e não podem ser usados em cenários com tarefas mais complexas; e CPUs genéricas podem se sobressair em desempenho sobre NPUs em casos de uso complexos, tais como métricas baseadas em classificação de pacotes (ex: DPI).

1.3.3. Gerenciamento, Orquestração e Automação de funções de rede

Em um ambiente onde funções de rede se tornam objetos com propriedades de mobilidade podendo ser inseridas em diversos contextos e ambientes conforme demanda ou requisitos de operação, gerenciamento e orquestração de NFs são tarefas críticas que podem levar a rede a obter agilidade para desempenhar a tradução de objetivos de alto nível em procedimentos e operações consistentemente cadenciadas as quais podem ser até mesmo automatizadas.

Em um primeiro plano a descoberta de serviços se torna uma tarefa inerente a operação e gerenciamento dos mesmos. Em um ambiente de NFVI onde uma heterogeneidade de tecnologias de hypervisors, NFs e provedores de serviços não dispõem de uma linguagem única de comunicação, protocolos de descoberta de serviços (Service Discovery Protocols - SDPs) detém a tarefa crucial de serem arquitetados a operar com os seguintes parâmetros/desafios: linguagem de descrição de serviços; formato de mensagens; arquitetura de diretórios; e comportamentos de operação e comunicação em rede.

Como abordado na subseção 1.3.1 serviços de NFV podem ser arquitetados desde a constituição de VMs até a programação de cadeias de regras em switches para direcionamentos de fluxos de tráfego para NFs/PFs em servidores ou middleboxes. A necessidade de abstrações consistentes para a elaboração de NFs parte do pressuposto da tradução de

objetivos lógicos de alto nível para funções de APIs que podem desencadear séries de comandos na infraestrutura de rede subjacente. Esta compilação, propriamente definida como orquestração, requer o uso de interfaces (ex: REST, JSON, XML) que abstraiam visões amplas da rede (ex: topologia, recursos/características de enlaces) abrindo espaço a implementações de algoritmos que possam levar a automatizações de funções de gerenciamento de rede.

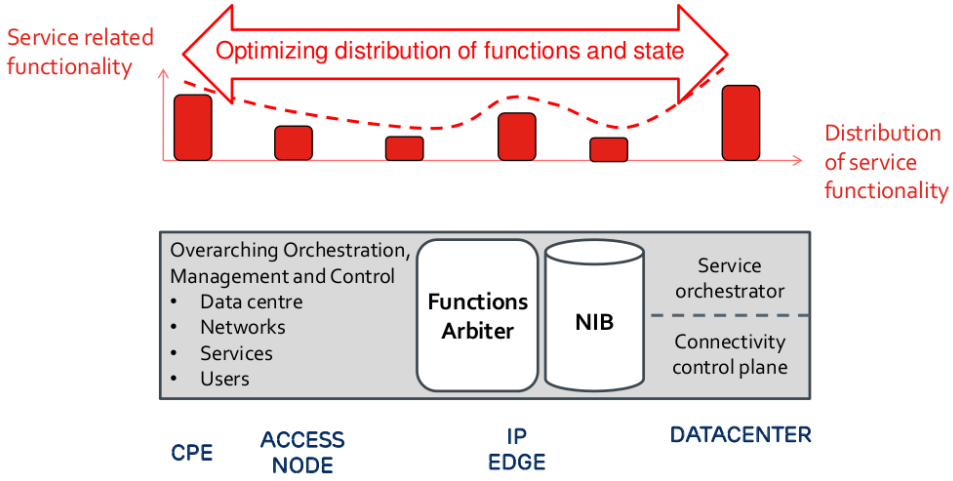


Figure 1.9. Visão lógica de gerenciamento [15].

Um framework de NFV pode requerer alocações dinâmicas de recursos de hardware conforme carga de operação de NFs sobre ele, o que deve tornar a tarefa de orquestração aberta a capacidade de scale up/down. Conforme visto na Figura 1.9 visões amplas de rede devem ser fornecidas ao controle de gerencia e orquestração da rede para que a distribuição de NFs bem como das cadeias de serviços que elas constituam estejam otimizadas em suas funcionalidades e de acordo com o ambiente em que se encontram, podendo este ser homogêneo ou mesmo heterogêneo [16]. E neste caso, sendo estas funções desempenhadas para escalar em ambientes desconexos, a migração de NFs tem como desafio a manutenção de seu estado durante sua realocação, replicação e qualquer tipo de gerenciamento de escalabilidade. Este requisito, traz consigo a necessidade de mecanismos de coordenação e arbitragem em requisições de aplicações a provedores de infraestrutura, como em [17]. Além disso, para que estes estados sejam corretamente implementados, formas de checagem de configurações designam papel crucial na determinação de consistências de NFs que permitirão o cumprimento dos requisitos de desempenho e escalabilidade levantados anteriormente na subseção 1.3.2.

Agregadas ao serviço de provimento dinâmico de capacidade a NFs e checagens de consistências destas operações, estão as tarefas de detecção, diagnóstico e recuperação de falhas. Cabe a função de gerenciamento verificar se uma infraestrutura de NFV está operacional em seus diversos níveis. Nesse caso, tal monitoramento deve estar atrelado a cumprimentos de contratos de SLA fim-a-fim que podem levar em consideração requisitos de tempo, espaço e custo. Granularidades de monitoramento, bem como de reatividade em caso de falhas são tópicos importantes que serão melhor discutidos na subseção 1.3.6.

1.3.4. Portabilidade e Interoperabilidade com plataformas legadas

Diante da prevista evolução continua de implementação dos conceitos de NFV em redes de produção, a interoperabilidade com redes legadas se torna um ponto chave onde a permissão de coexistência entre VFs e PFs estará amplamente atrelada as interfaces de comunicação disponíveis a estas funções, como por exemplo, em tunelamentos utilizando SDNs [18]. Nesse aspecto, uma visão ampla de rede possibilitada por plataformas de gerenciamento podem definir cadeias de serviços constituídas por middleboxes dedicadas e NFs em equipamentos comoditizados. A verificação do impacto de cadeias de serviços de plataformas legadas em novas funções de rede e vice-versa é um desafio que pode ser avaliado com base nas condições de construção de cadeias de serviços como mencionado na subseção 1.3.1.

O desenvolvimento de sistemas de comunicação espontâneos para interoperabilidade dinâmica e universal entre sistemas legados e novas tecnologias tem as seguintes dificuldades quando determinados em uma única e padronizada solução: formular um sistema desta forma que disponha de maneira *one size fits all* pode não conseguir lidar com a heterogeneidade das diversas tecnologias existentes em ambientes NFVI; padrões de desenvolvimento e comunicação são lentos e construídos em processos incrementais enquanto que novas aplicações e sistemas distribuídos surgem constantemente e podem tornar as soluções existentes rapidamente obsoletas; plataformas legadas continuam úteis aos serviços atuais, enquanto que novos padrões nem sempre levam em consideração questões de interoperabilidade com soluções antigas, ainda operacionais.

Como requisito de operação de NFs, é necessário na visualização de informações sobre a rede tornar transparente, por parte do operador de rede ao cliente, a utilização ou não de VFs ou PFs bem como o impacto de desempenho causado no serviço requisitado pela utilização destas funções [6]. Tal fato, implica em outro desafio a ser avaliado na determinação de cadeias de serviços fim-a-fim onde múltiplos provedores de NFVI intermediários possuem diferentes tecnologias de virtualização de funções de rede necessitando de interoperabilidade, não só das funções de rede em si, mas também de negociações de parâmetros de SLAs nas diversas cadeias heterogêneas de serviços que serão constituídas entre eles. Por este aspecto, necessitam ser especificadas ás tecnologias utilizadas ao longo do serviço fim-a-fim constituído, por exemplo, se houve utilização de comutação de pacotes ou estabelecimento de circuitos ópticos. Além disso, composições de redes legadas e novas tecnologias envolvem parâmetros diversificados de controles de procedimentos, protocolos, consumo de energia, entre outros parâmetros de rede (ex: uso de largura de banda e latência em operações) as quais devem ser dimensionadas corretamente para atender as demandas de cadeias de serviços fim-a-fim [16].

1.3.5. Estabilidade da rede: segurança

Da mesma forma que a existência de virtualização em servidores cria brechas para o surgimento de vulnerabilidades em suas camadas de operação (ex: OS, hypervisor, hardware), a determinação de funções de rede sobre um conjunto de servidores/switches COTS ou definidos pelo modelo BYOD também podem propiciar o surgimento de falhas de segurança em novos níveis de virtualização advindos de NFV, tais como sistemas operacionais de rede, cadeias de serviços de VNFGs e interfaces entre NFs [19]. Dessa maneira, em

uma infraestrutura de NFVI, assim como em data centers com milhares de servidores, diversos provedores de serviços e operadores de rede podem utilizar serviços compartilhados, e requisitam como principal funcionalidade o isolamento de desempenho entre suas tenants a fim de que não tenham seus contratos de SLA violados.

Clientes requisitando operações de gerenciamento de NFs ou de NFVIs podem requerer controle sobre os serviços que contratam, e logo, possuir a necessidade de gerenciá-los em seus diferentes níveis de operação. Em seu pleno funcionamento, NFV deve fornecer a clientes a exposição segura de APIs com as quais se possa gerenciar NFs de acordo com os níveis de serviço contratados. Consequentemente, a estas APIs não devem ser dadas as permissões de clientes constituirem NFs ou cadeias destas que interfiram no funcionamento de NFs ou serviços de outros clientes e, portanto, da própria NFVI. Exemplo este visto em proposta de caso de uso de plataforma de rede virtual como serviço (VNPaaS) na atribuição de políticas de segurança em firewalls para que empresas implementem aplicações de acesso a internet por através de provedores de serviços [20] ou requisitos de segurança já existentes em SDN [**?**], a serem futuramente utilizados em funções de orquestração de cadeias de serviços em NFV.

Entre outros fatores, como o grande impacto que políticas de alto nível causam atualmente a middleboxes e suas respectivas funções de rede, em um ambiente de NFV cadeias de serviços fim-a-fim trarão consigo a presença de inúmeras determinações de cumprimentos de SLAs. Adicionalmente a este fato, as cadeias de políticas que estas poderão definir, serão de grande relevância, e de certa forma mais importante do que os próprios requisitos de segurança de NFs e suas interfaces. A determinação de consistências em políticas de alto nível podem levar funções de gerenciamento a operar de acordo com requisitos de provedores de serviço de modo que elas desempenhem papel fundamental no uso correto de NFVIs. Portanto, tanto em redes legadas quanto em novas tecnologias que irão surgir de PoCs de NFV, a constituição de políticas de segurança de alto nível é um fator preponderante na existência de funções de orquestração e gerenciamento consistentes a atender contratos de SLA de forma segura para clientes e para os próprios provedores de infraestrutura [6].

1.3.6. Estabilidade da rede: resiliência

Em um ambiente de NFV, há requisitos de determinação de recriação de NFs caso estas venham a falhar. Tal recriação pode ocorrer de modo automático ou manual, conforme requisitos de operação do serviço dependente dessas NFs. Além disso, para que esta tarefa seja possível de ser realizada, a determinação de níveis de requisitos de confiabilidade/disponibilidade deve ser feita para o agrupamento de VNFs em diferentes categorias de resiliência. Consequentemente, a determinação de funções necessárias a continuidade de serviços, constituídos por orquestração de NFVs devem facilitar aos planos de controle e de dados formas seguras de disponibilidade e continuidade de serviços, e não se tornarem um ponto único de falhas [6].

Não obstante, NFVs devem permitir que seus dados possam ser replicados para preservação de suas integridades com a devida performance necessária ao cumprimento de SLAs. Estas devem definir métricas que determinem valores e a variabilidade de padrões de estabilidade de VNFs, inerentes a determinação das características de con-

fiabilidade de um framework NFV [19]. Nesse aspecto, diferentes métricas podem ser estabelecidas, tais como: taxa máxima de perdas de pacotes não intencional; variação máxima de atraso e latência baseada em fluxo de dados; tempo máximo para detectar e recuperar falhas; e taxa máxima de falhas de transações válidas e que não invalidam outras transações. Estes parâmetros podem variar bastante conforme a determinação de serviços específicos (ex: voz e vídeo, transações financeiras, aplicações relacionadas a saúde) que podem requerer confiabilidade/disponibilidade maior do que SLAs de melhor esforço.

Um tópico interessante no que diz respeito a constituição de cadeias de serviços é a determinação de suas falhas e correlações entre elas e as diferentes NFs que as constituem, sejam elas físicas ou virtuais, como no caso de uso de uma infraestrutura de NFV como serviço [20]. Para isso, todo o potencial da flexibilidade provida pela virtualização e portabilidade de funções de rede deve ser utilizada para atingir a confiabilidade necessária a disponibilidade e continuidade de serviços. Esta tarefa pode ser feita pela determinação clara de interfaces entre cadeias de serviços, estimativas bem definidas de desempenho de NFs, técnicas de verificações constantes de SLAs, checagem de dependência entre NFs, e por fim, formas de atribuições de correlações entre falhas conforme a determinação de conjuntos de NFs em grupos semelhantes de requisitos de SLA.

1.3.7. NFV e SDN

Redes Definidas por Software (SDNs) [21] se baseiam na separação dos planos de dados e de controle da rede, sendo que este se refere ao conjunto de funções, logicamente centralizado em controladores de rede, que influencia em como os pacotes são encaminhados a destinos na rede por elementos que aquele define para realizar tal tarefa por meio de uma interface de comunicação bem definida. Dessa forma, a inteligência da rede se concentra em sua maior parte no plano de controle, o qual pode potencialmente abrigar qualquer aplicação de rede que possibilite a implementação de melhores estratégias para encaminhamento de tráfego por inúmeros atuadores em diferentes granularidades. Consequentemente, SDN pode estabelecer algoritmos eficientes no plano de dados para atuar no balanceamento de carga em enlaces, tendo como critérios políticas que contenham quaisquer critérios que sejam úteis a esta tarefa.

É muito importante ressaltar que SDN e NFV são independentes, mas podem ser complementares, como visto na Figura 1.10 no que diz respeito principalmente as tarefas de gerenciamento [23] e orquestração [24]. A customização de funções de rede, bem como de suas programações no plano de dados, carecem de atenção no que diz respeito a permissividade de agentes, sejam estes usuários finais ou operadores de rede. Isto pois, segundo requisitos de portabilidade de NFV, tais agentes podem requerer a instalação de aplicações e funções de rede em dispositivos genéricos (ex: BYOD) de modo semelhante ao que existe na computação, em sistemas operacionais. Dessa maneira, a padronização de interfaces, northbound e southbound, para programabilidade de rede por parte de SDN, necessitam ser estipuladas, seja por hardware ou software em diferentes linguagens de baixo e/ou alto nível (ex: python, java, procera, pyretic), para que a orquestração e gerenciamento da rede defina NFs, e consequentemente, VNFGs, como proposto em [25] e [26] na programação de caminhos em núcleos de rede sem fio. Estas interfaces, ao mesmo tempo que facilitam a diversificação de aplicações e utilização por parte de agentes também podem prejudicar modelos de desenvolvimento e de negócios. Pois a evolução

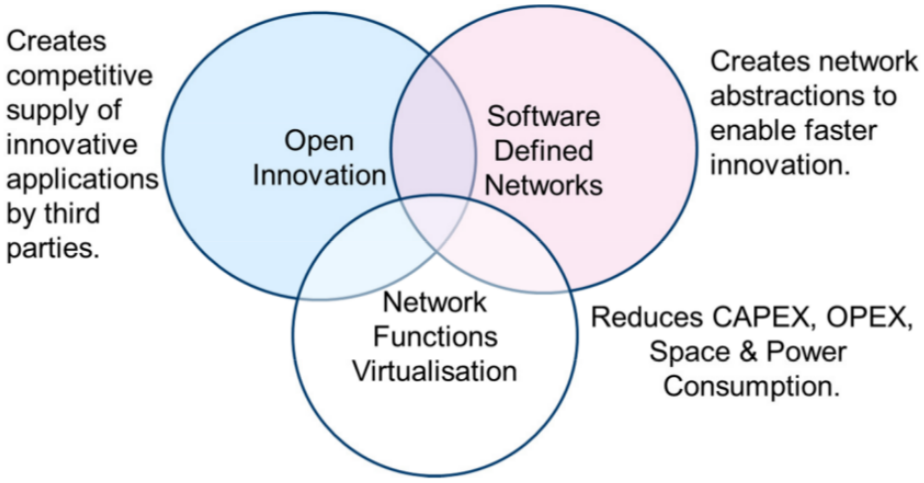


Figure 1.10. Relação entre SDN e NFV [22].

de diferentes plataformas de hardware e software por diferentes fabricantes de hardware podem ser limitadas em sua evolução caso a padronização de interfaces não possibilite formas de diferenciação de produtos, sejam eles controladores de rede ou dispositivos BYOD [27].

Diante dos atuais investimentos em padronizações de interfaces northbound do plano de controle pela Open Networking Foundation (ONF), algumas críticas se apresentam à determinação do ambiente principal de suporte às SDNs, definido como plano de dados. Estas se concentram em abordar tanto que tanto a programabilidade atualmente almejada em SDNs quanto o atual modelo de negócio em redes de comunicação não se adequam as atuais tecnologias habilitadoras a um plano de dados coerente às atuais demandas de escalabilidade e desempenho (ex: balanceamento de carga, IDS). Consequentemente, tais críticas se empregam a NFV, pois características de orquestração e gerenciamento, principalmente no que diz respeito a criação de cadeias de serviços, não encontram características suficientes que as habilitem a ser implementadas na atualidade [28]. Além disso, ainda existem incertezas sobre quais funcionalidades realmente devem ser separadas nos planos de dados e controle, que ainda decorrem principalmente em problemas de escalabilidade e desempenho.

1.4. Casos de Uso, Provas de Conceito e Tecnologias Habilitadoras

O objetivo desta seção é identificar e descrever um conjunto de modelos de serviços e casos de uso de alto nível que representam, na visão do NFV ISG, importantes modelos e campos de aplicação para NFV. Também são apresentadas algumas provas de conceito em resposta aos casos de uso NFV ISG, bem como resultados de trabalhos independentes. Por fim, são apresentadas tecnologias habilitadoras importantes ao NFV.

1.4.0.1. Casos de Uso NFV ISG

Buscando o desenvolvimento do NFV, o NFV ISG lançou em outubro de 2010 [20] uma primeira proposta de casos de uso que apresentaram um conjunto de modelos de serviços e campos de aplicação para o NFV. Essa iniciativa teve como objetivo contribuir para o estudo e desenvolvimento do NFV, viabilizando sua utilização em ambientes reais. Em alto nível, os casos de uso buscam atender as seguintes necessidades:

- Rápida inovação de serviços através da implantação baseada em software e operacionalização das funções de rede e serviços fim-a-fim;
- Eficiência operacional melhorada resultante da automação de procedimentos operacionais comuns;
- Redução do consumo de energia, migrando cargas de trabalho ou desligando hardware não utilizado;
- Interfaces padronizadas e abertas entre as funções de rede, possibilitando o fornecimento por diferentes fabricantes;
- Flexibilidade na relação da VNF com o hardware;
- Eficiência do capital empregado em comparação às implementações de hardware dedicado.

Ao todo, [20] definiu 9 casos de uso, sendo que [29] dividiu-os em 5 áreas comuns. Tabela 1.1.

Abaixo são apresentados os casos de uso definidos por [20], agrupados por [29], possibilitando uma visão geral sobre as características de cada um. Complementando, ao final dos casos de uso é apresentada uma relação entre os requisitos e desafios discutidos na seção 1.3 com os casos de uso propostos por NFV ISG.

Cloud Use Case

NFV Infrastructure as a Service (IaaS) (NFVIaaS): NFVIaaS é a capacidade de um provedor Cloud em fornecer uma estrutura que suporte NFV. Os recursos computacionais disponibilizados são comparáveis aos alocados pelo IaaS, bem como os serviços de conectividade de redes dinâmicas são comparados ao NaaS oferecido pelos provedores Cloud.

Um cenário onde o NFVIaaS torna-se importante é quando um provedor NFV possui clientes distribuídos por regiões remotas. Nesse caso, manter uma estrutura própria

Table 1.1. Casos de Uso NFV [29].

Cloud Use Cases	Mobile Use Cases	Data Center Use Cases	Access/ Residential
NFV Infrastructure as a Service (IaaS) (NFVIaaS)	Virtualization of the Mobile Core Network and IMS	Virtualization of CDNs	Virtualization of the Home Environment
Virtual Network Functions as a Service (VNFaaS)	Virtualization of Mobile Base Station		Fixed Access Network Functions Virtualization
Service Chairs (VNF Forwarding Graphs)			
Virtual Network Platform as a Service (VNPaaS)			

próximo aos clientes ou impor que eles utilizem seus serviços através de longas distâncias pode ser inviável econômica e tecnicamente, portanto, a contratação de infraestrutura NFV de provedores locais pode ser uma boa opção.

A figura 1.11 apresenta a estrutura formadora do NFVIaaS, composta pelos recursos IaaS e NaaS dos provedores. TambÃ©m apresenta um ambiente em que as VNFs de um provedor (#2) são executadas utilizando os recursos de outro provedor (#1).

Virtual Network Functions as a Service (VNFaaS): Atualmente muitas empresas estão implantando mais serviços nas bordas de suas redes. Apesar desse comportamento, a utilização de equipamentos dedicados e seu alto custo, inflexibilidade tecnológica, demora na instalação e dificuldade de manutenção, dificultam esse processo. Como as necessidades tecnológicas continuam evoluindo, mais serviços e aplicações migram para os centros de dados ou nuvens públicas, provocando constantes mudanças na estrutura das redes corporativas. Todas essas mudanças requerem constantes investimentos, forçando as empresas a procurarem alternativas de terceirização do fornecimento dos serviços de tecnologia. Nesse cenário, a virtualização do CPE nos provedores de serviço tornou-se uma alternativa, visto que os clientes não precisam mais arcar com os custos do ciclo de vida da tecnologia, enquanto os provedores aproveitam eficientemente os recursos existentes em seus centros de dados, virtualizando recursos com o NFV.

No VNFaaS, o serviço NFV fornecido pelo provedor é semelhante ao SaaS da computação em nuvem. A VNF é a aplicação do provedor, a empresa é o cliente do serviço e ela não tem acesso direto ou administrativo ao NFVI ou NFV, sendo apenas a consumidora do VNFaaS. Nesse ambiente, as operadoras podem virtualizar o próprio roteador de borda (PE), apesar de que há maiores vantagens em virtualizar o CPE por motivos de haver um número muito maior de CPEs e sua atuação ser apenas local.

O vE-CPE pode substituir todo um conjunto de equipamentos existentes no lado do cliente por soluções de NFV localizados nos provedores de nuvem ou nos centros de dados dos provedores de serviços. o vE-CPE é capaz de prover serviços de roteamento

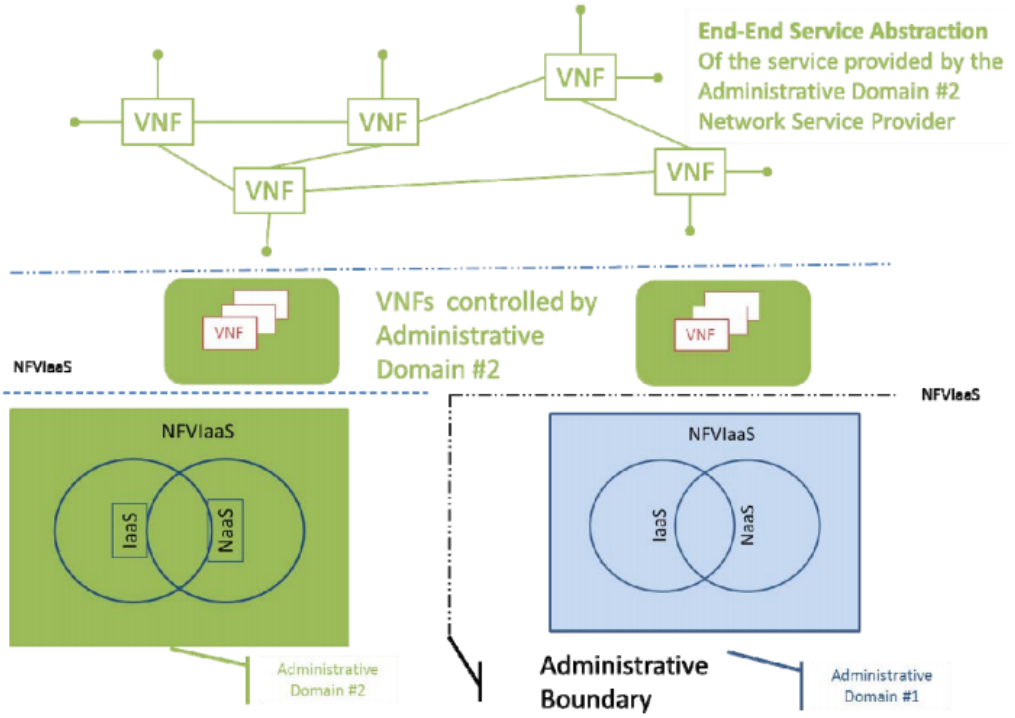


Figure 1.11. Exemplo de um Domínio Administrativo #2 Executando VNFs na Infraestrutura NFV disponibilizada pelo Domínio Administrativo #1 [20].

com QoS, firewall nas 7 camadas, detecção e prevenção de intrusão, aceleração de aplicativos e muito mais, tudo isso sem a necessidade de incluir hardwares especiais.

A figura 1.12 apresenta um exemplo de topologia com CPE virtualizado e não virtualizado. No CPE virtualizado, o provedor garante apenas a conectividade L2 ou L3 com o cliente, virtualizando os serviços de firewall, QOS, VPN etc, em seu centro de dados.

Virtual Network Platform as a Service (VNPaaS): Em computação em nuvem, PaaS caracteriza-se pela possibilidade do cliente implantar suas próprias aplicações utilizando a plataforma fornecida pelo provedor de serviço. O cliente controla o aplicativo, mas não a rede ou a infraestrutura de nuvem. Seguindo essa linha, o VNPaaS corresponde ao conjunto de aplicações disponibilizadas pela operadora de serviço como plataforma para que seus clientes desenvolvam seus próprios serviços de rede customizados de acordo com suas necessidades. Um exemplo de aplicação do VNPaaS é quando uma empresa fornece um *Access Point Name* (APN) aos seus funcionários hospedado por uma operadora móvel. O APN é o ponto de entrada lógico da rede privada da empresa, e como ele é hospedado por uma operadora, este pode fornecer funcionalidades de rede avançadas à empresa.

A operadora pode permitir que a empresa disponibilize serviços virtualizados de rede como firewall, DHCP, DNS, proxy, cache, email próximos à APN. Serviços de firewall, por exemplo, permitem sair da APN diretamente para internet com todas as políticas de segurança e monitoramento da empresa aplicadas, bem como o tráfego direcionado a Internet pode ser roteado diretamente sem ter que passar pela rede interna da empresa. Já serviços de cache podem disponibilizar determinados dados de aplicações próximos à

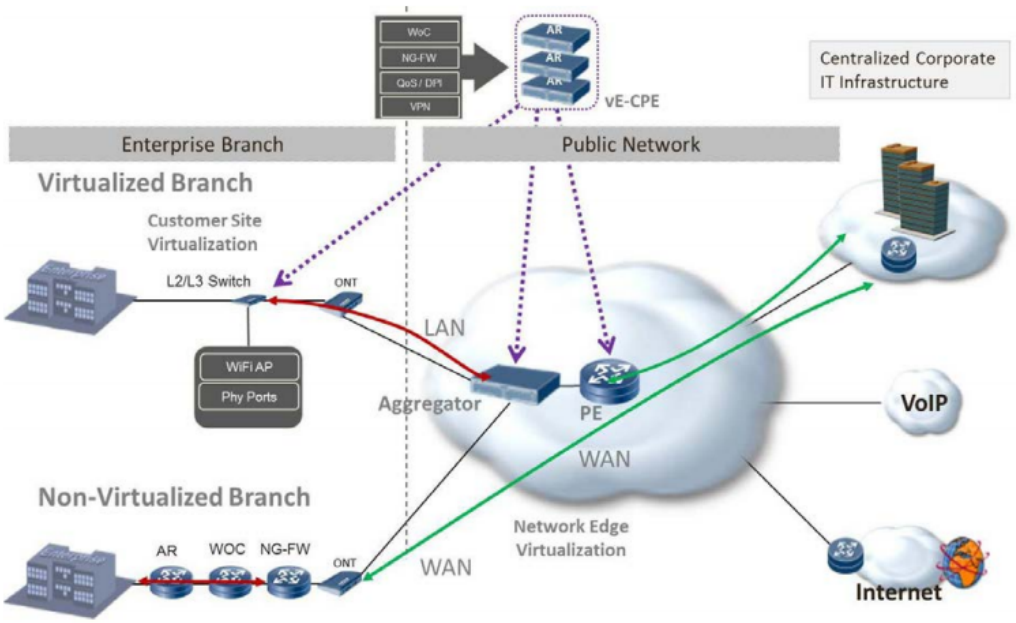


Figure 1.12. CPE não virtulizado e vE-CPE [20].

APN, permitindo o acesso com menor latência e carga sobre os links da empresa.

O VNPaaS é similar ao VNFaaS (vE-CPE), mas difere na escala de serviço e escopo de controle oferecidos ao consumidor do serviço. o VNPaaS oferece um serviço de maior escala, fornecendo uma rede virtual em vez de uma única função de rede virtual.

Service Chains (VNF Forwarding Graphs): VNF *Forwarding Graphs* corresponde à sequência de NFs que um pacote atravessa, sendo responsável pela comunicação entre os elementos do NFV. São como os cabos que conectam equipamentos físicos numa estrutura de rede, entretanto, provêem a conectividade lógica entre os equipamentos virtuais do NFV, além de interconectar o ambiente lógico às redes físicas.

A figura 1.13 apresenta um exemplo de VNF FG. Neste exemplo, o provedor criou um serviço de rede fim a fim entre duas funções de rede física que envolve vários VNFs. É possível que estes VNFs sejam fornecidos por um ou mais provedores.

Cada VNF possui alguns metadados associados a ele que descrevem suas características essenciais. O serviço de rede real é composto pelo conjunto de todos os fluxos de pacotes que atravessam o plano de encaminhamento NFV e físico.

As características do VNF FG permitem a resolução de uma série de problemas existentes em topologias físicas. A tabela 1.2 apresenta a relação entre os problemas enfrentados por equipamentos físicos e como eles são contornados por ambientes NFV.

Mobile Use Cases

Virtualization of the Mobile Core Network and IMS: Em tratando-se do núcleo da rede para sistemas de celular, o *Evolved Packet Core* (EPC) é a principal e mais recente arquitetura desenvolvida pelo 3GPPtm. Nesse caso, o MM e S/P-GW são exemplos de funções de rede existentes nessa arquitetura. Já o *IP Multimedia Subsystem* (IMS), que é

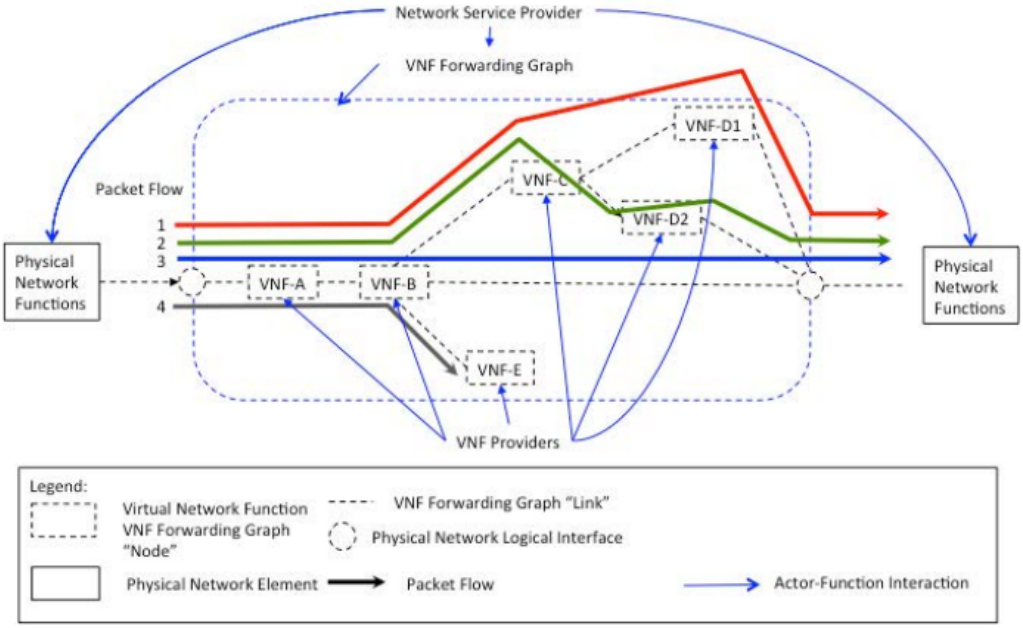


Figure 1.13. Visualização Lógica do VNF FG [20].

o responsável pelo controle de sessão no fornecimento de serviços multimídia sobre EPC ou outras redes baseadas em IP, possui o P-CSCF e S-CSCF como exemplos de funções de rede. HSS e PCRF são outras funções de rede do 3GPPtm requeridas na arquitetura fim-a-fim da prestação de serviço em conjunto com o EPC e IMS. Similarmente, os sistemas de tarifamento *online* e *offline* (OCS e CFO) são sistemas que captam os registros de utilização do usuário para tarifação dos serviços consumidos. Nessa linha, este caso de uso trata da virtualização do EPC, IMS e outras funções de rede mencionadas.

A figura 1.14 apresenta um ambiente onde serviços como HSS, P/SGW e MME são virtualizados. Essas VNFs podem escalar independetemente de acordo com suas necessidades específicas de recursos, pois, podem haver situações em que é necessário aumentar os recursos do plano do usuários sem afetar o plano de controle e vice-versa. VNFs que lidam com plano de dados também podem exigir um número diferente de recursos NFV do que aquelas que lidam só com VNFs de sinalização, portanto, a facilidade no gerenciamento de recursos possibilitado pelo NFV é de grande valia nesse ambiente.

Virtualization of Mobile Base Station: A virtualização de estação-base móvel possibilita que pelo menos uma parte da rede de acesso via rádio (RAN) possa ser oferecida através de servidores, storages e switches padrão de mercado. Espera-se com isso a diminuição do consumo de energia através da alocação dinâmica de recursos e balanceamento da carga de tráfego, falicidade de gerenciamento e operação, e menor tempo entre a concepção de novas tecnologias e sua implementação. Além disso, a virtualização permitirá consolidar tecnologias diferentes, como por exemplo 3G, LTE e WiMAX, numa mesma estação base virtualizada.

A utilização média de uma RAN geralmente é muito menor do que sua capacidade máxima. Esse comportamento é devido às RANs tradicionais serem projetadas para cobrir a carga de pico, fato que provoca ociosidade do ambiente que não pode ser compartilhado

Table 1.2. Comparação entre as Vantagens e Desvantagens dos Equipamentos Físicos e VNF FG [20].

Atributo	Equipamentos Físicos	VNF FG
Eficiência	Funcionalidade e capacidade dimensionada para o pico de carga	Funcionalidade e capacidade dinamicamente dimensionados pela utilização corrente
Resiliência	Backups utilizam hardware específico e redes dedicadas	Backups podem compartilhar hardware e recursos de rede
Flexibilidade	Lentidão em ativações de novas capacidades quando baseado em hardware	Pequeno tempo para atualizações ou ativações de novas funcionalidades por ser baseado em software
Complexidade	Necessário adicionar novas configurações, interfaces físicas e/ou suportar novos sistemas para implementar novos grafos de encaminhamento	Virtualização da função de encaminhamento e/ou configuração de VNF implementam grafos de encaminhamento mais facilmente
Ativação	Ativação em outras operadoras requer equipamentos físicos, interfaces e configurações para conectar usuários finais	Virtualização de funções e comutação torna o processo de ativação mais simples

com outros nós. Nesse caso, a virtualização da RAN pode garantir maior eficiência na utilização dos recursos entre diferentes estações base.

Algumas funções alvo de virtualização em estações base são a PHY, MAC, RLC, RRC e PDCP. A camada PHY inclui o maior número de tarefas intensivas computacionalmente, tais como canal de codificação/decodificação, FFT/IFFT, merecendo atenção especial falando-se em NFV.

Data Center Use Cases

Virtualization of CDNs: Integrar os nós das redes de distribuição de conteúdo com as redes de operadoras pode ser uma forma eficiente de responder aos desafios do fornecimento de tráfego de vídeo. Hospedar conteúdos multimídia mais perto dos usuários acarreta na economia de links e equipamentos concentradores, permitindo entregar fluxos de dados com maior largura de banda e melhor qualidade.

Em implementações tradicionais, os cache CDN são máquinas físicas ou software dedicados com requisitos específicos de hardware, muitas vezes instalados lado a lado, porém, sem compatibilidade ou integração entre eles ou outros serviços. Essa estrutura apresenta desvantagens conhecidas aos provedores de serviço CDN, portanto, a virtualização da função de cache CDN representa diminuição do custo operacional dos provedores e contribui para a evolução do CDN.

Access/ Residential

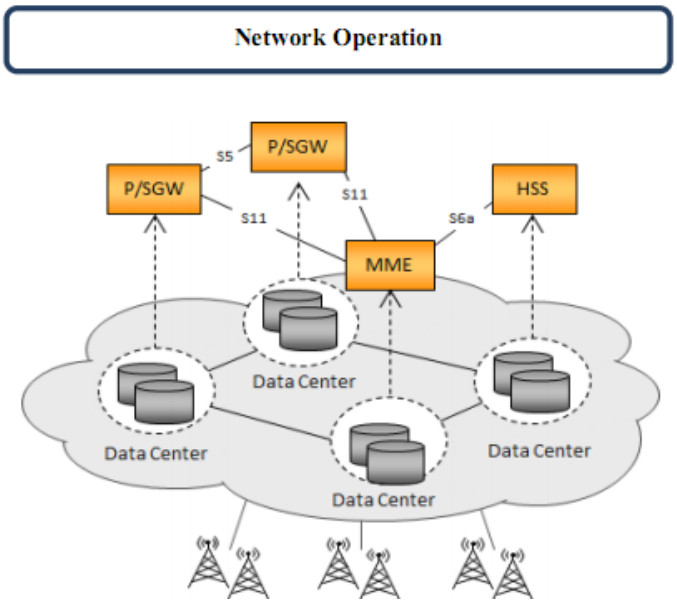


Figure 1.14. Virtualização do EPC. VNFs como HSS, P/SGW e MME podem ser virtualizadas [20].

Virtualization of the Home Environment: A arquitetura atual para acesso aos serviços oferecidos pelas operadoras aos clientes finais é composta por um CPE dedicado localizado na rede doméstica, suportado por sistemas existentes na rede da operadora. O CPE representa a presença da operadora ou provedor nas instalações do cliente, geralmente incluindo um gateway de roteamento (RGW) para serviços de Internet e VOIP, e um gateway de mídia (STB), responsável por oferecer suporte e armazenamento de mídia local.

Nesse ambiente, o NFV é importante para clientes e operadoras, concentrando os serviços a custo mínimo e apresentando maior capacidade e facilidade de atualização ou disponibilização de novas tecnologias. Todo CPE do usuário pode ser substituído por apenas um cabo responsável por criar a conectividade local, migrando as funções da rede para o ambiente da operadora.

A figura 1.15 apresenta uma proposta de VNF onde é mantido uma réplica virtualizada do dispositivo original, de modo que o RGW migra para um vRGW e o STB migra para vSTB. Ao manter essa estrutura, matem-se também as interfaces originais para os dispositivos virtualizados.

Fixed Access Network Functions Virtualization: O maior custo e gargalo das redes geralmente está no acesso. Em redes de acesso cabeadas, a tecnologia mais comumente utilizada é o DSL, mas sua implantação depende do desenvolvimento e instalação de equipamentos eletrônicos em nós remotos localizados na rua ou em armários de telecomunicações existentes em prédios de uso comum. Esses sistemas devem ter eficiência energética para minimizar problemas térmicos e ainda fornecer energia para os equipamentos hospedados nos clientes. Além disso, devem utilizar tecnologia simples e ter vida operacional longa.

Nas redes de acesso, a virtualização permite mover o processamento de dados complexo do usuário para áreas mais internas da rede do provedor, permitindo o com-

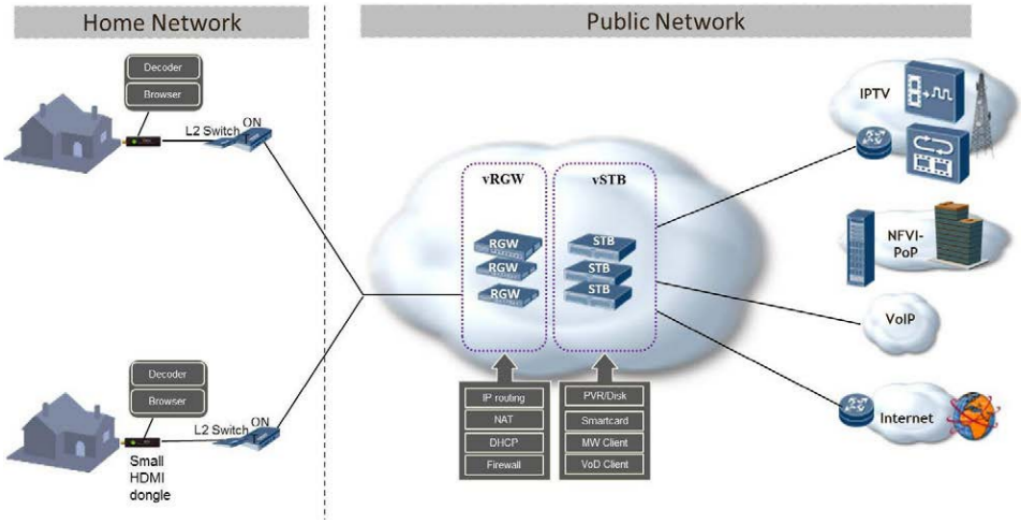


Figure 1.15. Virtualização das funções do ambiente doméstico. A criação do vRGW e vSTB permitiu a transferência de funções de rede e mídia para o centro da rede [20].

partilhamento da estrutura com outros usuários. Complementando, a simplificação do nó remoto contribui para a diminuição de seu custo e consumo energético.

A figura 1.16 apresenta um cenário onde a virtualização de funcionalidades da camada 2 e planos de controle, como ONT, ONU, MDU, DSLAM e ETH Switch, são realizadas no centro de operações da operadora.

Casos de Uso versus Requisitos e Desafios do NFV

Como apresentado na seção 1.3, algumas propostas de virtualização de funções de rede no NFV apresentam requisitos e desafios que devem ser atendidos e superados para garantir a evolução da tecnologia. Com intuito de tornar a informação mais clara e de fácil acesso, a tabela 1.3 sintetiza os requisitos e desafios apresentados na seção 1.3, relacionando-os aos casos de uso propostos pelo NFV ISG.

Apesar de não explícito, a integração com SDN, segurança e resiliência podem ser considerados como requisitos para todos casos de uso NFV ISG.

1.4.0.2. Provas de Conceito

Além de definir casos de uso que apresentam a viabilidade do NFV, o NFV ISG também definiu um modelo de desenvolvimento de Provas de Conceito (PoC) [19], cuja finalidade é garantir a qualidade dos resultados obtidos pelas PoCs. Esse modelo é definido no Diagrama de Fases da PoC. Figura 1.17

O Diagrama de Fases da PoC apresenta todas etapas de seu desenvolvimento. Em linhas gerais, o processo inicia-se com a chamada para submissão de PoCs realizado pelo próprio NFV ISG, onde grupos formados por pesquisadores, operadoras e empresas de telecomunicações interessadas no desenvolvimento do NFV, unem-se com o objetivo de desenvolver e demonstrar tecnologias que atendam aos casos de uso NFV ISG.

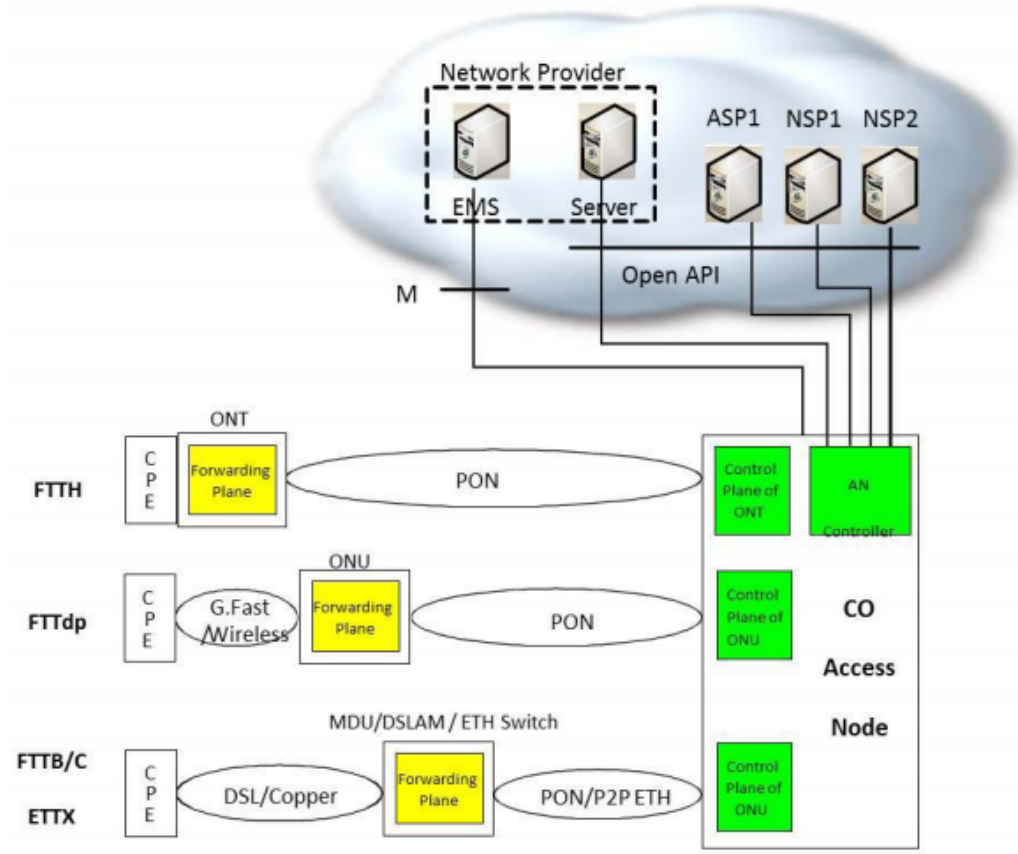


Figure 1.16. Virtualização da Rede de Acesso [20].

As propostas de PoC geradas são então submetidas à aprovação do NFV ISG, e após sua validação, todo desenvolvimento e resultados são acompanhados através de relatórios disponibilizados durante o desenvolvimento ou através da demonstração final.

Abaixo são apresentadas PoCs autorizadas e reconhecidas pelo NFV ISG, que seguem seu modelo proposto, como também algumas PoCs considerados indepentendes, que na maioria das vezes tem como objetivo principal apresentar uma determinada tecnologia NFV.

PoCs NFV ISG

CloudNFV Open NFV Framework Project: O grupo CloudNFV [30] foi o primeiro a obter aprovação de seu projeto para desenvolvimento de uma PoC junto ao NFV ISG [31]. O projeto [32] define 16 cenários que apoiam oito objetivos gerais, visando uma implementação que integra a criação, implantação e gestão de serviços NFV.

O foco da PoC é atender ao caso de uso IMS, baseando-se no projeto de código aberto Clearwater do Metaswitch IMS [33]. A proposta também busca introduzir duas aplicações adicionais, sendo uma baseada no caso de uso VNFaaS, para inspeção profunda de pacotes (DPI), e outra direcionada a prover teste e monitoramento como serviço (T/MaaS). As três aplicações evoluirão independentemente, mas serão combinadas em um único caso de uso IMS.

Table 1.3. Casos de Uso versus Requisitos e Desafios do NFV

Casos de Uso	Requisitos	Desafios
NFVIaaS	Desempenho e interoperabilidade	Gerenciamento, orquestração e automação de arquiteturas e funções de rede
VNFaaS	Elasticidade e desempenho	Segurança e resiliência
VNF FG	Interoperabilidade e coexistência de plataformas legadas	Elasticidade e desempenho
VNPaaS	Desempenho, interoperabilidade e orquestração	Gerenciamento e segurança
Mobile Core e IMS	Desempenho, interoperabilidade, gerenciamento e orquestração	Elasticidade, segurança e resiliência
CDNs	Interoperabilidade, elasticidade	Gerenciamento e desempenho
Home Environment	Portabilidade e interoperabilidade	Elasticidade e desempenho
Mobile BS	Desempenho e interoperabilidade	Segurança, resiliência e automação de arquitetura e funções de rede
Fixed Access	Portabilidade e elasticidade	Segurança e resiliência

O projeto é dividido em 5 fases [34]. A primeira (Modelagem de Serviços e Recursos) é responsável por definir a arquitetura CloudNFV, as regras estruturais do modelo de dados e a descrição da integração das funções CloudNFV, considerada uma introdução às outras quatro fases. A fase 2 (Node Builder), é responsável por descrever a integração de recursos e funções virtuais bem como fornecer uma modelagem básica para ambos. A fase 3 (Service Builder) é responsável pela construção de modelos de serviços para os nós definidos pelo Node Builder, criando um inventário de serviços disponíveis. A fase 4 (Service Broker), é responsável pelo desenvolvimento do mecanismo de seleção de um modelo de serviço de inventário, gerado a partir do Service Builder, e implantá-lo em recursos disponibilizados pelo Node Builder. A fase 5 (Service Manager), interliga o CloudNFV e NMS, OSS, BSS, bem como fornece as ferramentas e processos de operações para essa integração. Todas fases são repetidas para os três aplicativos propostos na PoC (IMS, DPI e T/MaaS).

O desenvolvimento da PoC é realizado no laboratório da Dell em Santa Clara, e conta com a participação de empresas de expressão que atuam em partes específicas do processo.

A figura 1.18 apresenta a estrutura do laboratório CloudNFVl, identificando a função de cada membro do processo de desenvolvimento da PoC. Nessa estrutura, a Dell é responsável pelo hardware, a 6WIND pela aceleração do plano de dados; Overture provê a orquestração entre os requisitos de implantação e de conectividade junto ao OpenStack. A Qosmos faz o monitoramento de tráfego que permite a otimização da utilização e per-

Figure 1.17. Diagrama de Fases das PoCs NFV ISG [19].

formance do ambiente; a Metaswitch provê o IMS Clearwater, a Mellanox é responsável pelas interfaces de alto desempenho para o ambiente e por fim a Shenick faz a injeção de dados para execução dos testes.

Service Chaining for NW Function Selection in Carrier Networks: A Nippon Telegraph and Telephone Corporation (NTT), Cisco Systems, Juniper Networks e a HP japonesa propuseram um caso de uso [35] que apresenta um método de encadeamento de serviço que permite ao cliente selecionar e aplicar várias funções virtualizadas de rede de acordo com suas necessidades. Nessa implementação, a interoperabilidade entre as tecnologias utilizadas demonstrou a viabilidade do NFV nesse tipo de aplicação.

Para a demonstração, o NTT desenvolveu um método de encadeamento de serviços no qual cada pacote recebe um identificador que permite ao usuário selecionar e aplicar funções virtualizadas sob demanda. Cada identificador é responsável por identificar uma cadeia de funções de rede virtualizada, bem como encaminhar pacotes a elas quando necessário. Na demonstração foram virtualizados serviços de rede como vCPE, vDPI, vFW no ambiente suportado pela Cisco, Juniper e HP. Como resultados, verificou-se que

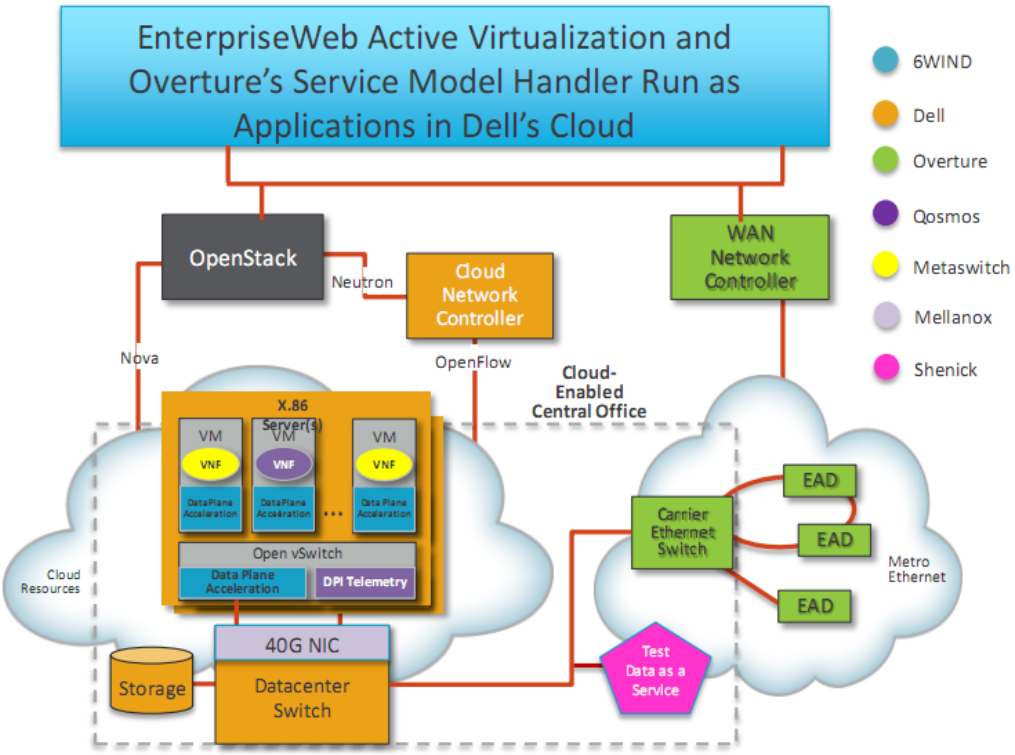


Figure 1.18. Estrutura do Laboratório Dell para uso do grupo CloudNFV [32].

o método de encadeamento permitiu aos usuários selecionar e utilizar os serviços de rede de acordo com suas necessidades.

Como demonstrado na figura 1.19, o roteamento IP possui limitações quanto ao encaminhamento de pacotes por aplicação e usuário, enquanto o processo de identificação de encadeamento de funções permite controle total do caminho por onde tráfegos específicos das aplicações do usuário devem ser encaminhados.

A PoC em questão atendeu aos casos de uso VNF *Forwarding Graph*, a partir da demonstração do encadeamento virtualizado dos serviços, e o VNFaaS, através da virtualização de serviços de rede como o vCPE, vDPI e vFW.

Virtual Function State Migration and Interoperability: O objetivo desta PoC [36] foi demonstrar que uma função de rede devidamente desenvolvida utilizando ferramentas de desenvolvimento modernas, sistemas operacionais e hypervisors de código-aberto, pode ser implantada de forma transparente em duas máquinas com hardware totalmente diferente. Nesse caso específico, um mesmo código fonte foi executado tanto na arquitetura x86 quanto na MIPS-64, além disso, a aplicação da PoC foi desenvolvida separando o estado da aplicação, permitindo a migração do estado entre instâncias diferentes do mesmo sistema rodando em máquinas com plataformas diferentes.

Nesta PoC foram utilizados o KVM como hypervisor, o Linux como sistema operacional virtualizado e interfaces padrão para o plano de dados, como DPDK ou Linaro ODP. Como compilador foi utilizado o compilador GNU C ou GCC, porém são esperadas implementaç oes utilizando *Low-Level Virtual Machine* (LLVM), permitindo a inde-

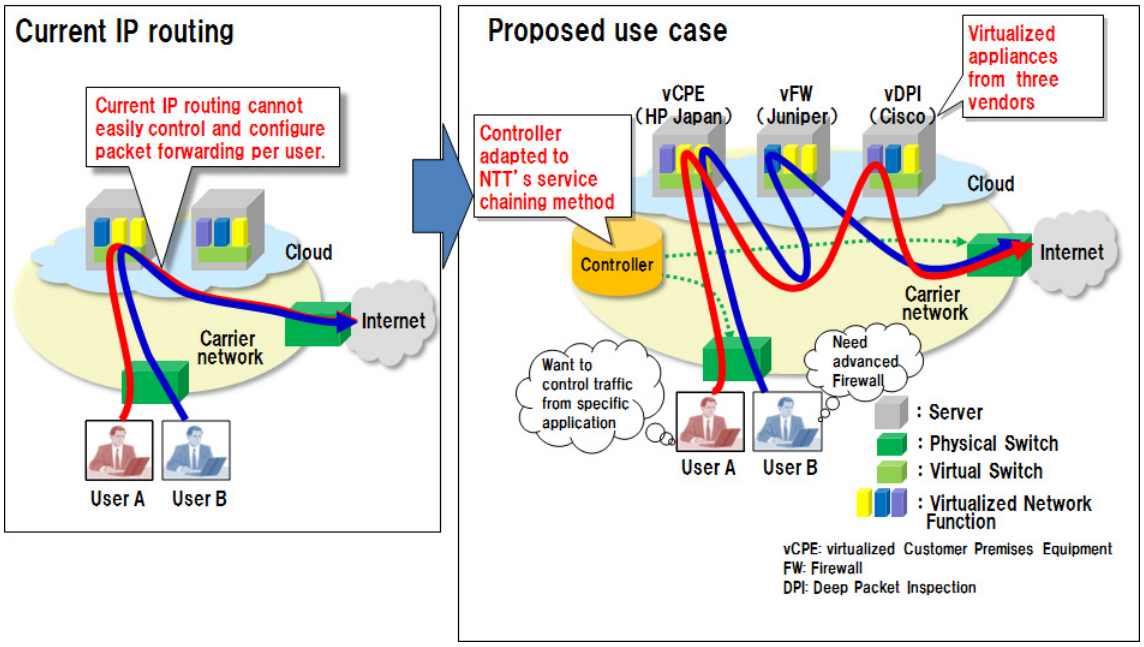


Figure 1.19. Método de Encadeamento de Serviço. As limitações impostas pelo roteamento IP convencional e as possibilidades de encadeamento de serviços possibilitadas pela identificação de encadeamento [35].

pendência do "*byte-code*" em relação à arquitetura.

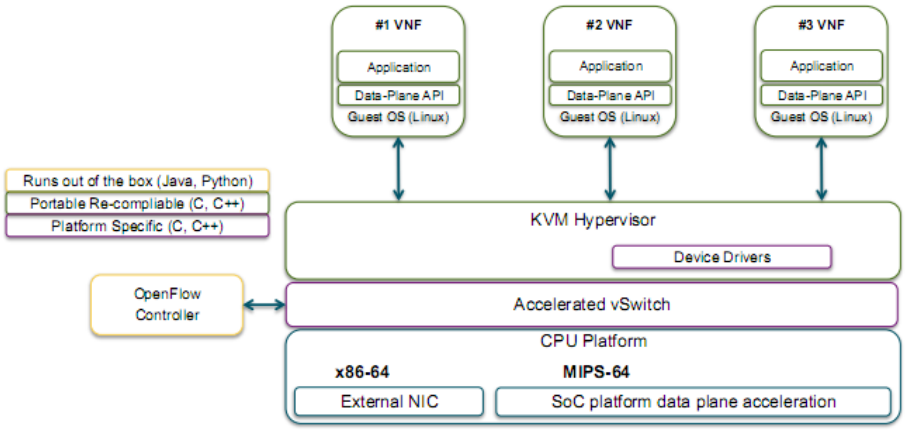


Figure 1.20. Arquitetura de Software e Servidores. Apesar da arquitetura de hardware ser diferente, o software deve ser exatamente igual entre elas [36].

Como apresentado na figura 1.20, os componentes da plataforma NFV escolhida são de código aberto e disponível em x86 e MIPS-64. A plataforma de software em ambas arquiteturas precisam estar alinhadas, incluindo as ferramentas de desenvolvimento, como compiladores, hypervisores e sistemas operacionais. Para ser eficiente, fabricantes devem ser capazes de desenvolver funções de rede utilizando ferramentas que suportem a compilação para diferentes arquiteturas, bem como a implantação desses sistemas em ambientes padronizados.

A demonstração da PoC consiste na transmissão de um vídeo a partir de um servi-

dor para o vECP em execução na plataforma x86. O vídeo flui através do vECP para uma vBTS e, finalmente, para o equipamento do usuário final. Durante a transmissão do vídeo, há migração do vECP para a plataforma MIPS-64, sendo que para isso, o fluxo que passa através do vECP x86 é pausado e o estado da transferência migrado para o vECP MIPS-64. A partir daí o fluxo é retomado com base no estado anterior. Figura 1.21.

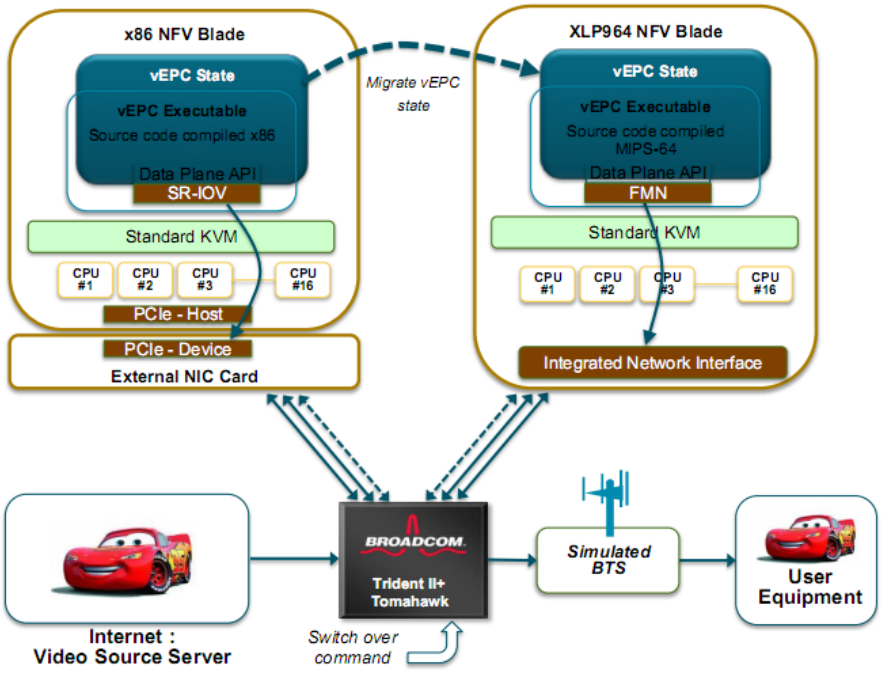


Figure 1.21. Migração de VNF com estado entre as plataformas x86 e MIPS-64 [36].

Esta PoC está diretamente relacionada ao estudo de caso NFVIaaS, pois demonstra IaaS através de duas arquiteturas diferentes. Além disso, a portabilidade condiz com a proposta do estudo de caso do IMS e de Virtualização dos Recursos da Rede de Acesso.

Multi-vendor Distributed NFV: Esta PoC [37] visa validar os requisitos, comportamento e arquitetura geral de uma implantação de NFV distribuído (D-NFV), composto por fornecedores diversos que fornecem componentes físicos e virtuais, bem como VNFs de uma ou múltiplas funções implantadas em grande escala.

Participam dessa PoC empresas como a Cyan, responsável pelo orquestrador que gerencia e coordena uma rede composta por elementos físicos (interfaces de rede e infraestrutura de virtualização) e virtuais (firewall e criptografia). A Cyan e a CenturyLink também hospedaram os laboratórios para o desenvolvimento da PoC. A RAD NID, responsável pela infraestrutura de computação embutida que integra componentes físicos e virtuais, permitindo a implantação de NFV na borda da rede (lado do cliente). A Fortinet, responsável por fornecer VNFs que suportem funções de firewall e IPS, através do FortiGate, bem como suporte ao IPv4, IPv6, BGP, OSPF e outros recursos de rede através do VDOM. A Certes Network, responsável pelos encriptadores virtuais para os vCEPs, possibilitando criptografar e descriptografar tráfego L2, L3 ou L4 utilizando criptografia AES 256 bits, ponto a ponto ou multiponto. O controle das chaves e as políticas puderam ser gerenciados pelo usuário final atravÃ©s do *Certes Networks TrustNet Manager*. As

VNFs fornecidas pela Fortinet (Firewall) e Certes Network (encriptador) permitem a co-existência entre VNFs em um mesmo vCEP.

Essa PoC é dividida em duas fases. Os principais objetivos da fase 1 são demonstrar implantações reais de VNFs e a orquestração necessária, especialmente em vE-CPE baseados em D-NFV, com a implantação de firewall e criptografia do lado do cliente. Demonstrar o encadeamento de funções entre a rede física e a virtualizada, testar e documentar a interação e co-existência entre VNF de fabricantes diferentes e, por fim, validar a capacidade do OpenStack de suportar a infraestrutura D-NFV.

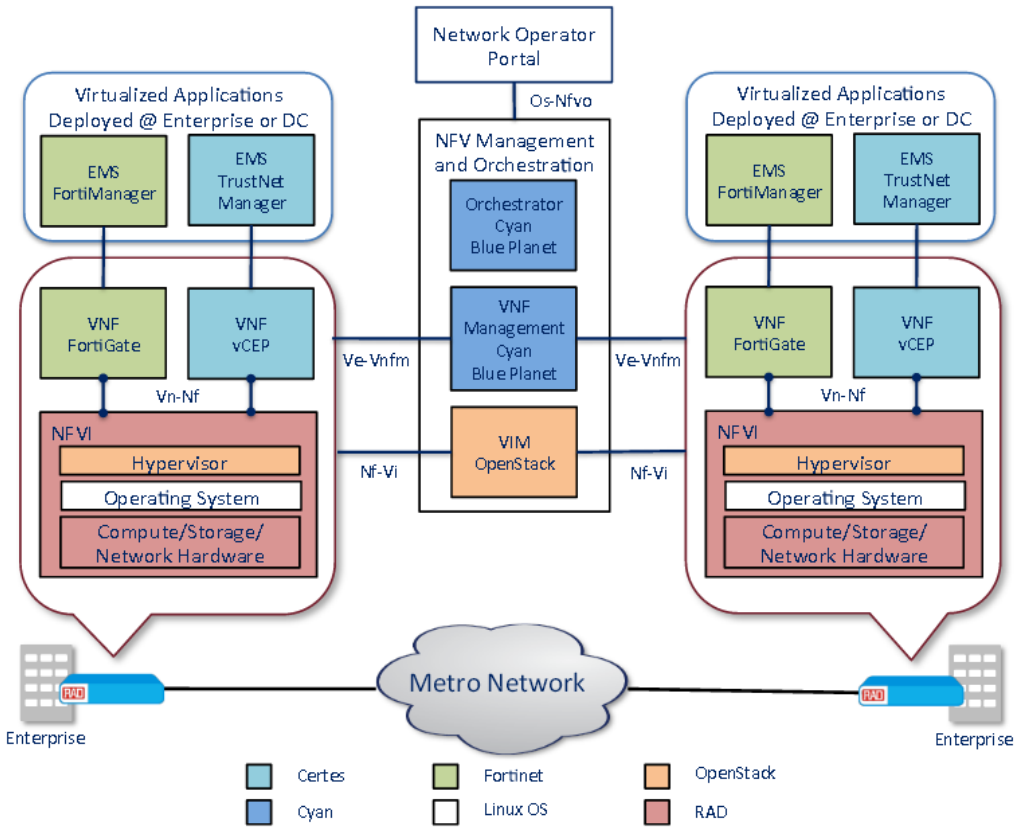


Figure 1.22. Quadro geral da arquitetura para fase 1. Apresenta todas funções e seus responsáveis [37].

A figura 1.22 apresenta as funções exercidas pelas tecnologias oferecidas pelos membros do grupo. Também apresenta a estrutura do vE-CPE composto pelas VNFs de firewall e criptografia hospedadas no cliente.

A fase 2 da PoC é responsável por demonstrar o funcionamento e integração do D-NFV com o vE-CPE centralizado no centro de dados da operadora e distribuído nos clientes.

Esta PoC atende aos casos de uso VNFaaS, por demonstrar um vE-CPE, e o VNF-FG, por apresentar o encadeamento de VNFs entre diferentes fabricantes.

E2E vEPC Orchestration in a multi-vendor open NFVI environment: Esta PoC [38] demonstra uma infraestrutura NFV composta por vários fornecedores com um único orquestrador responsável por disponibilizar, implementar e gerenciar uma rede de serviço

móvel composta por um vE-ECP em uma infraestrutura de hardware padrão e uma rede *backhaul* L2 móvel.

A PoC está dividida em duas fases, sendo que os principais objetivos da primeira são validar o modelo de arquitetura NFV ISG [20] e demonstrar a integração entre múltiplos fabricantes NFV, incluindo Intel, Dell, Red Hat, Cyan e Connectem. A segunda fase é responsável pela busca da melhora do desempenho do ambiente, identificando e solucionando possíveis deficiências do OpenStack e implementando o Intel DPDK para melhora na velocidade de comunicação entre as VMs e entre as VMs e a NIC.

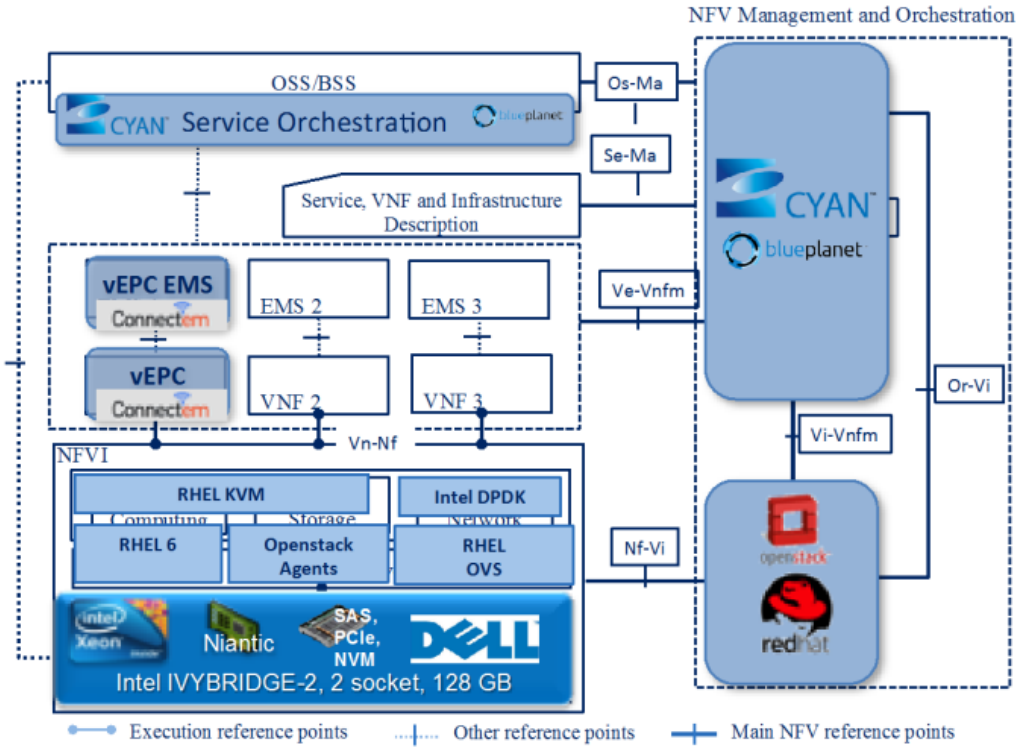


Figure 1.23. Componentes da PoC. Lista de fabricantes e componentes funcionais correspondentes [38].

A figura 1.23 apresenta a lista de fabricantes envolvidos na PoC e os componentes funcionais que compõem o NFVI, VNF e camada de orquestração NFV.

A PoC atende diretamente aos casos de uso NFVIaaS, por disponibilizar um conjunto de recursos de infraestrutura utilizados no NFV; virtualização de rede móvel e IMS, por implementar um vE-CPE, além de implementar a orquestração fim-a-fim, implementar co-existência de funções de rede virtuais e não-virtuais e gerenciamento de VNFs.

Outras PoCs NFV ISG: Alguns outros grupos também tiveram suas PoCs submetidas e aprovadas pelo NFV ISG [39], porém ainda não tiveram seus projetos e resultados publicados abertamente.

PoCs Independentes

OpenNaas: OpenNaaS [40] é o resultado do projeto Mantychore FP7 [41] e surgiu com o objetivo de criar uma comunidade de software de código aberto interessada no desen-

volvimento de software NaaS. é uma plataforma de provisionamento dinâmico de recursos de rede e permite a implantação e configuração automática de infraestrutura de rede independente de fornecedores de hardware para o acesso.

OpenNaaS permite a criação de representações virtuais de recursos físicos como switches ópticos, roteadores, redes IP e BoD-domains, além de permitir a inclusão de novos recursos como uma extensão às suas capacidades.

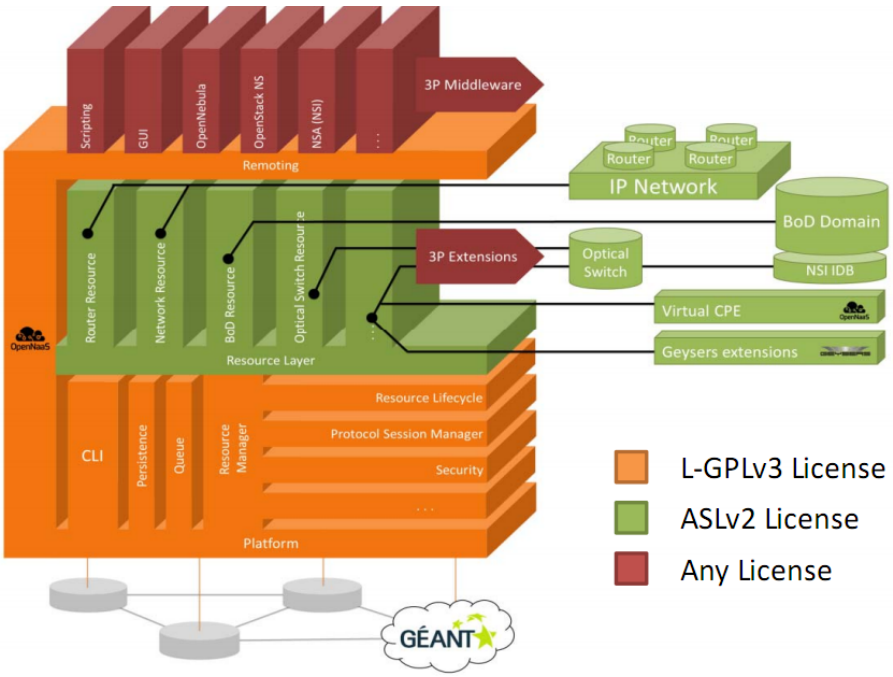


Figure 1.24. Arquitetura em Camadas OpenNaas [42].

Sua arquitetura [42] é dividida em três camadas: Plataforma, NaaS e Inteligência da Rede (figura 1.24). A camada de Plataforma corresponde às tecnologias base do OpenNaas, como por exemplo, o OSGi, Java 6, Apache SF, Scala etc. Os recursos são considerados blocos reutilizáveis por todas extensões do OpenNaas e controla o acesso à infraestrutura. A camada NaaS é responsável pela abstração da infraestrutura e disponibiliza o controle de uma fatia dos recursos ao usuário. A Inteligência de Rede corresponde às aplicações de gerência de rede que podem ser construídas na parte superior da abstração. É nessa camada que as políticas de gestão do ambiente são definidas, mas geralmente esses aplicativos não são distribuídos com o OpenNaas.

Para demonstração do OpenNaas, [43] trouxe duas aplicações para virtualização de CPEs em um ambiente educacional, onde uma Rede Nacional de Pesquisa e Educação (NREN) é o provedor e as instituições educacionais são os clientes da topologia. A primeira demonstração enfatiza a estrutura entre um provedor e um cliente apenas, enquanto a segunda apresenta a utilização de múltiplos provedores, num ambiente em que dois provedores comunicam-se com um mesmo cliente. Figura 1.25.

O principal benefício da virtualização do CPE é a redução no custo e impacto ambiental provocado pelo equipamento entre a NREN e o cliente, economizando espaço, energia e refrigeração necessários ao ambiente, além de permitir que os recursos sejam

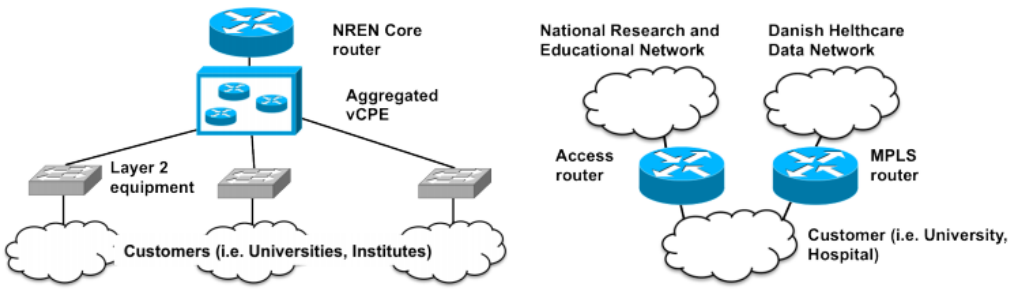


Figure 1.25. Ambiente vCPE com suporte a apenas um provedor e outro com gerenciamento múltiplo [43].

utilizados por mais de um cliente.

Como análise final, [43] apresenta o detalhamento das economias esperadas na fase de testes. A configuração escolhida é baseada em roteadores Juniper MX-240, que suportam até 16 roteadores lógicos, sendo dois deles reservados para controle e conectividade com um roteador backup. Nesse ambiente são criados 7 pares de roteadores, sendo um para o cliente e outro para o NREN. A configuração é duplicada em um roteador secundário para fins de backup e essa configuração é então comparada com o CPEs tradicionais baseado em equipamentos Cisco e Juniper. Figura 1.26.

CPE SETUP COMPARISON

	Virtual CPE MX 240	Multiple CPE ASR1002-F	Multiple CPE MX 10
Manufacturer	Juniper	Cisco	Juniper
# Users Supported	7	7	7
NREN CPE	Yes	Yes	Yes
Space	5 U	14U	14U
Power (kw)	2000	3290	2632
Weight (kg)	58.97	127	96

VIRTUAL CPE SETUP SAVINGS FOR 7 CUSTOMERS

	MX 240	ASR1002-F	MX 10
Manufacturer	Juniper	Cisco	Juniper
Space Saving	-	560%	560%
Power Saving	-	329%	263%
Weight Saving	-	430%	325%

Figure 1.26. Comparação Entre CPEs Físicos e Ganho com Utilização de vCPE [43].

Intel/HP/Wind River Accelerated vSwitch: O cerne do NFV é a virtualização das funções de rede em hardware padrão, mas para que essa tecnologia seja realmente aplicável às operações das operadoras de telecomunicação, é necessário que a qualidade do serviço seja garantida.

Entre outras características importantes, é necessário que a velocidade de acesso aos recursos virtualizados seja o mais próximo possível das obtidas em ambientes dedicados, não degradando a percepção de desempenho do usuário ao compará-lo ao mesmo serviço oferecido nos moldes convencionais.

Nessa linha, Intel, HP e Wind River uniram-se em uma prova de conceito para construção de um ambiente NFV de alto desempenho [44]. O objetivo é demonstrar que o desempenho do Open vSwitch [45] pode ser melhorado a partir da união do Intel DPDK [46] com o *Open Virtualization Profile* (OVP) [47] da Wind River, utilizando-se um servidor HP padrão de mercado como base.

Em sua distribuição original, o Open vSwitch é um switch de produção baseado em software de código aberto, projetado para rodar em ambiente virtualizado em hard-

ware padrão. O suporte ao Open vSwitch foi adicionado ao kernel do Linux a partir da versão 3.3 e sua função é encaminhar tráfego entre VMs no mesmo servidor físico ou entre VMs em uma mesma rede física mas em servidores distintos. Opera no L2 ou L3 e foi desenvolvido para utilizar os módulos do kernel para atingir melhor desempenho na comutação, apesar de também poder operar no espaço de memória do usuário, sem assistência do módulo do kernel.

Testes realizados com o Open vSwitch apresentaram desempenho insatisfatório para comutação de dados entre VMs, além disso, o Open vSwitch mostrou-se não escalável quanto ao aumento do número de VMs, condição fundamental à viabilidade do NFV. Essas deficiências motivaram a Intel e Wind River a projetar uma solução de virtualização que levou o Open vSwitch a montar seu plano de dados no espaço de memória do usuário do Linux, através da construção de um comutador lógico utilizando as bibliotecas Intel DPDK.

A solução proposta representou um grande ganho de desempenho na comunicação entre VMs. Intel e Wind River desenharam uma solução de virtualização que retirou inteiramente o Open vSwitch do Kernel para melhorar o desempenho. O plano de dados foi então recriado no espaço de memória do usuário, no topo das bibliotecas do DPDK, e Intel e Wind River utilizaram um modelo de memória compartilhada que possibilitou que os pacotes que chegam ao vSwitch tenham seus cabeçalhos analisados e, a partir daí, seja passado apenas um ponteiro para o destinatário, evitando a cópia do dado para sua área de mem'oria.

EANTC-NFV Multi-Vendor NFV Showcase: O *European Advanced Networking Test Center* (EANTC) é uma consultoria em telecomunicações, de tecnologia neutra, membro do ETSI NFV. Seus clientes são fabricantes de equipamentos de rede e provedores de serviço em redes e telecomunicações e suas áreas de negócio incluem a interoperabilidade, conformidade e testes de desempenho para Ethernet, IP/MPLS, redes concentradoras e *backhaul* móveis, redes convergentes *Triple Play* e tecnologias e aplicações de provedores de computação em nuvem.

Em 2013, a EANTC propôs [48] que fabricantes se unissem para uma demonstração de implementação real de NFV. A proposta visava abranger características do NFV como a instanciação e provisionamento de recursos, portabilidade e elasticidade do ambiente.

As empresas participantes da demonstração [49] foram a Huawei, responsável pelas funções relacionadas ao cliente, como NAT, DPI e controle de acesso, a Metaswitch que apresentou o *Perimeta Session Border Controller*, responsável por implementar níveis de segurança entras VNFs; a Procera, que trouxe o tecnologias de DPI e a Ixia, que ficou responsável por gerar tráfego para as demonstrações.

A figura 1.27 apresenta a topologia lógica do ambiente, com a especificação das funções necessárias aos testes.

Como resultados, no âmbito de instanciação e provisionamento, todas VNFs puderam ser instaladas remotamente em hardware padrão via interface de comando ou web. Os testes utilizaram hardware x86 padrão e os hypervisores KVM, OpenStack e VMware. Um desafio em comum foi a abstração das interfaces de rede, onde constatou-se que o

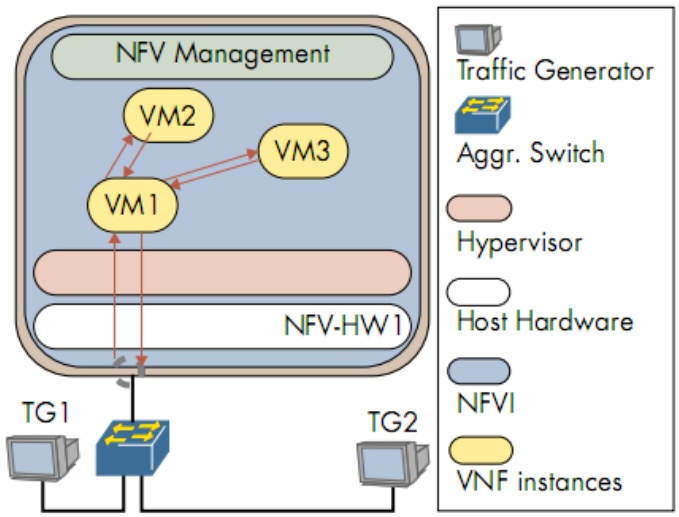


Figure 1.27. Topologia Lógica Especificada por Funções [49].

switch virtual causou gargalho na comunicação entre as VMs. Como orquestrador foram utilizadas tecnologias proprietárias e desenvolvidas especificamente para a PoC, além do *VMWare vCloud Director/vShield* e o OpenStack.

Quanto a portabilidade, ocorreram situações onde foi possível migrar VNFs sem qualquer parada do ambiente, enquanto em outras, houve a necessitade que uma segunda instância da VNF já estivesse funcionando para a portabilidade acontecer, nesse caso havendo apenas a migração de tráfego com manutenção do estado. Quanto a elasticidade, foi demonstrado que alguns fabricantes são capazes de fazer compartilhamento de carga entre VNFs ou criar novas instâncias de VNFs automaticamente de acordo com a necessidade do ambiente.

Segundo os participantes da PoC, o objetivo proposto foi atingido ao se verificar que a integração entre as tecnologias utilizadas obtiveram êxito no âmbito do NFV.

1.4.0.3. Tecnologias Habilitadoras

Esta seção tem por objetivo apresentar algumas tecnologias consideradas habilitadoras à implantação do NFV em ambientes reais. Segundo [50], são tecnologias habilitadoras os servidores de alto desempenho e grande volume de dados baseados em hardware padrão e a computação em nuvem. Os servidores de hardware padrão são a base física do NFV, que presa pela independência de hardware específico em sua arquitetura. A computação em nuvem contribui com o conceito de virtualização e todo aparato tecnológico também necessário ao NFV.

Em geral, as tecnologias de computação em nuvem podem ser divididas por grupos de funções, onde algumas são responsáveis pela orquestração do ambiente, outras garantem que o hardware padrão obtenha desempenho compatível com o hardware dedicado e outras tentam assegurar que as VNFs utilizem o mínimo possível de recursos do hardware, viabilizando a instanciação de grande quantidade de VNFs por recurso alocado.

Abaixo são apresentadas algumas tecnologias responsáveis por essas funções.

OpenStack: O OpenStack [51] é uma plataforma de computação em nuvem pública e privada de código aberto. Consiste em uma série de projetos inter-relacionados que entregam uma solução completa de infraestrutura de nuvem totalmente compatível com as plataformas de servidores de hardware genérico. Objetiva ser reconhecido pela simplicidade de implantação, alta escalabilidade e riqueza em recursos. Originalmente era desenvolvido pela Rackspace e NASA, mas atualmente é mantido por uma comunidade global de desenvolvedores.

Como apresentado na figura 1.28, os projetos do OpenStack são responsáveis por controlar grupos de computadores, storage, recursos de rede e outras funções básicas ou que complementam essas atividades principais, tudo gerenciado por uma interface dedicada.

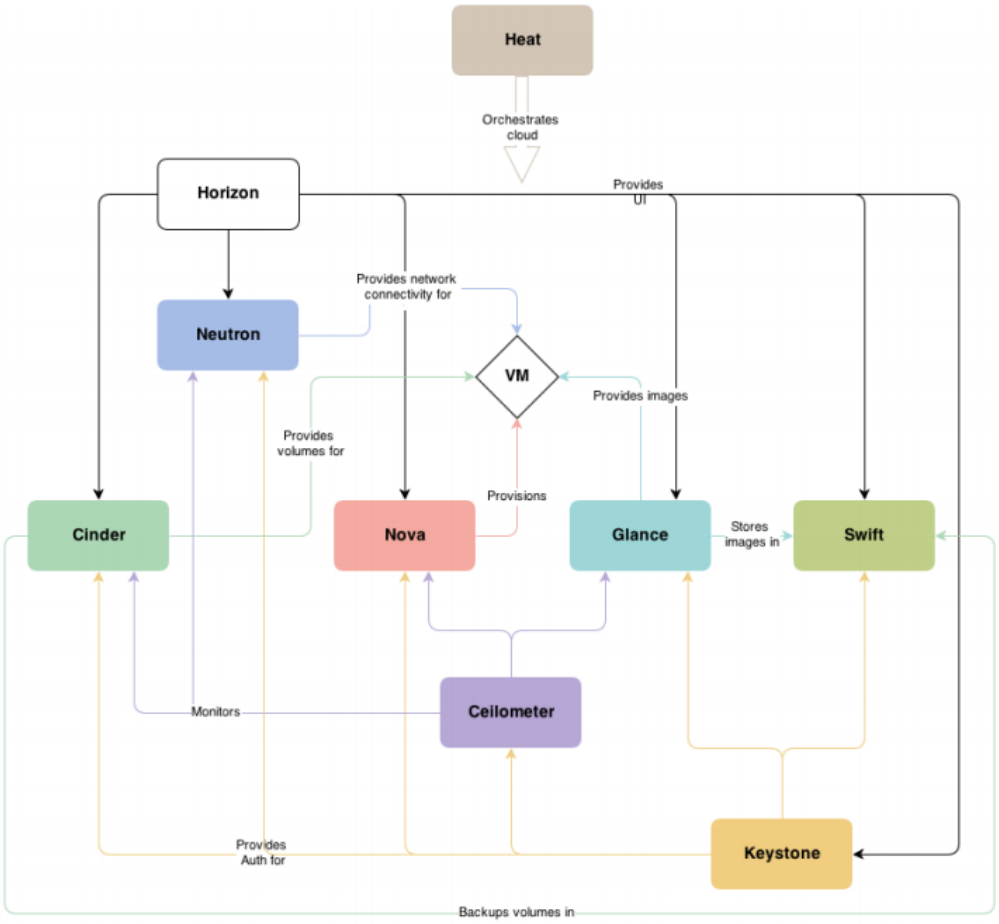


Figure 1.28. OpenStack - Arquitetura Conceitual. Apresenta os projetos OpenStack suas funções e interações com outros projetos [51].

Dentre os principais projetos do OpenStack, o Nova é responsável por gerenciar o ciclo de vida de instâncias de computadores e suporta hypervisores como o KVM, XEN, VMware vSphere, containers LXC, etc. Suas funções incluem a instanciação, desclassificação e inutilização de máquinas de acordo com a demanda. É a parte principal do IaaS.

O Neutron, formalmente denominado Quantum, é o projeto de rede. Fornece conectividade como um serviço entre interfaces (ex. vNICs) e outros serviços OpenStack (ex. Nova). Fornece APIs para que usuários possam definir e conectar-se às redes, bem como suporta integração com tecnologias de vários fabricantes.

Dos outros projetos, o Swift e o Cinder fazem parte do módulo de storage. O Horizon corresponde à interface de acesso e gerenciamento, enquanto o Heat é responsável pela orquestração do ambiente. O Glance, Ceilometer e Keystone são responsáveis, respectivamente, pelas funções de gerenciamento de imagens, telemetria e identidade.

Tanto o Nova quando o Neutron são os projetos OpenStack mais relevantes ao NFV, pois, gerenciamento de recursos dos servidores, escalabilidade dos computadores, gerenciamento de instâncias de VMs, usuários e grupos são atividades desempenhadas pelo Nova, enquanto o Neutron é responsável pelo gerenciamento de VLANs, IDS, VPN, integração com SDN entre outras funções específicas de rede.

Como exemplo da utilização do OpenStack nas PoCs NFV ISG, *CloudNFV*, por exemplo, utilizou o Nova no gerenciamento das VNFs, enquanto o Neutron ficou responsável pela interface com o controlador OpenFlow [52]. Na PoC *Multi-vendor Distributed NFV*, O OpenStack foi avaliado junto ao hypervisor KVM para ambientes D-NFV [37], enquanto em *E2E vEPC Orchestration in an multi-vendor open NFVI environment*, o Neutron foi avaliado através do desenvolvimento de novas VNFs para arquiteturas de hardware padrão, enquanto o Heat era responsável pela orquestração do ambiente [38].

A cada cenário de teste de uma PoC em que o OpenStack é utilizado, seu comportamento e limitações são analisados para que essa plataforma evolua com o NFV, visto que ele é considerado a base para o NFV por muitos.

Intel Data Plane Development Kit (Intel DPDK): O principal objetivo do *Intel Data Plane Development Kit* (DPDK) [46] é fornecer um ambiente simples e completo que suporte o processamento rápido de pacotes para aplicações que necessitam de alto desempenho.

A Intel publicou os resultados de testes em uma plataforma com suporte ao DPDK composta por um Intel Xeon E5-2600 de 1 soquete, memória DDR3 e controlador PCI Express, que atingiu a marca de 80Mpps no processamento L3 de pacotes de 64 Bytes. Os resultados representam uma diminuição na latência de memória de 120ns para 70ns aproximadamente, incluindo o tempo de recebimento do pacote.

O DPDK possui vários recursos que contribuem para a diminuição da sobrecarga do ambiente, como a desativação de interrupções geradas pelo I/O, alinhamento de cache, utilização de *huge pages* para diminuição de falhas na consulta à tabela de páginas da memória (TLB), pré-busca, entre outros. O DPDK roda no espaço de memória do usuário, eliminando a sobrecarga proveniente da cópia de dados entre o kernel e a memória do usuário.

Projetado para acelerar o desempenho do processamento de pacotes, o DPDK contém um número crescente de bibliotecas cujo código fonte está disponível para que desenvolvedores possam utilizá-las ou modificá-las conforme suas necessidades. As aplicações podem ser desenvolvidas utilizando bibliotecas que seguem os modelos *pipeline*

ou *run-to-completion*, que contribuem para a ausência de interrupções de I/O nesse ambiente.

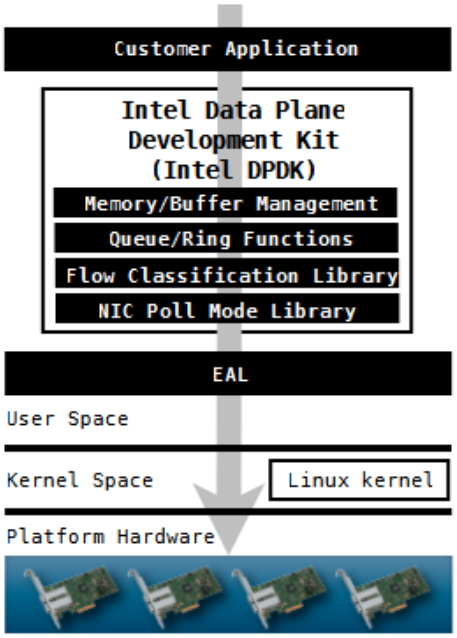


Figure 1.29. Intel DPDK - Arquitetura de bibliotecas [46].

A figura 1.29 apresenta a arquitetura de bibliotecas do DPDK e sua relação com o restante do ambiente. As aplicações dos usuários utilizam as interfaces disponibilizadas pelas bibliotecas para acesso aos recursos da plataforma através da camada de abstração do ambiente (EAL).

Quanto às suas funções, as bibliotecas de gerenciamento de memória e buffer são responsáveis principalmente pelo gerenciamento da alocação de objetos não NUMA em *huge pages*, diminuindo o TLB, bem como realizam a pré-alocação de espaços fixos de buffers para cada core. O gerenciamento de fila implementa filas livres ao invés de *spinloks*, evitando espera desnecessária para o processamento dos pacotes. O classificador de fluxo provê mecanismos de geração de *hash* utilizados na combinação de pacotes em fluxos, melhorando a vazão.

O DPDK ainda possui uma grande quantidade de outras bibliotecas, como as relacionadas à multiprocessamento, temporizadores, logs, debug e criptografia. Além disso, a Intel planeja desenvolver novas bibliotecas seguindo a evolução do DPDK.

Das PoCs apresentadas, *Virtual Function State Migration and Interoperability* [36] e *E2E vEPC Orchestration in an multi-vendor open NFVI environment* [38] implementaram ou pretendem implementar o DPDK diretamente em seus ambientes, já *Intel/HP/Wind River Accelerated vSwitch* fez uso do DPDK através do OVP da Wind River para melhorar o desempenho do Open vSwitch [44]. Por sua vez, *CloudNFV* utiliza-se do DPDK através do 6WINDGate [52].

Netmap: Netmap [53] é a uma estrutura que permite sistemas operacionais genéricos suportarem taxas de comunicação de milhões de pacotes por segundo com interfaces de

1 à 10 Gbps, sem a necessidade de hardware personalizado ou alterações nos aplicativos. Apesar de desempenhar função equivalente ao Intel DPDK, o Netmap procurou diferenciar-se deste pela facilidade de implementação e portabilidade, apesar de testes apontarem uma pequena vantagem de desempenho para o DPDK.

No desenvolvimento do Netmap, foram identificadas e tratadas três características que correspondiam à custos no processamento de pacotes: a alocação de memória dinâmica por pacote, trocada por recursos de pré-alocação; custos de chamadas de sistemas, amenizado com processamento em lote; e cópias de memória, eliminadas através da partilha de buffers e metadados entre o kernel e o espaço do usuário, ao mesmo tempo que protege o acesso aos registos de dispositivos e outras áreas de memória do kernel.

Netmap foi testado em FreeBSD e Linux com adaptadores diversos de rede de 1 à 10 Gbps. O protótipo desenvolvido em [53], apontou que um único núcleo rodando a 900 MHz, pode enviar ou receber 14,88 Mpps, o que corresponde à taxa de pico em links de 10 Gbps. Esse resultado foi considerado mais de 20 vezes mais rápido do que o obtido com APIs convencionais. Testes ainda apontam que foi possível obter aumentos de velocidade de 5 vezes ou mais no Click e em outras aplicações de encaminhamento de pacotes, utilizando uma biblioteca de emulação Pcap rodando sobre no Netmap.

Além do desempenho, o Netmap considera a segurança da operação e a facilidade de uso como métricas importantes. No Netmap, clientes não podem travar o sistema porque os registos de dispositivos e regiões críticas de memória do kernel não são expostos, além de não poderem injetar ponteiros de memória falsos no kernel, o que muitas vezes representa vulnerabilidade de outros sistemas baseados em memória compartilhada.

Como exemplo de aplicação do Netmap, [54] apresentou o *Virtual Local Ethernet* (VALE), switch virtual responsável por prover portas de acesso à múltiplos clientes, sendo eles hypervisores ou processos de hosts. Da perspectiva de um usuário, o VALE é capaz de oferecer a cada usuário uma estrutura independente, com NICs virtuais conectadas a um switch e acessível através da API Netmap. Segundo [54], o VALE foi utilizado para testar versões modificadas para alto desempenho do *ipfw* e *Dummynet Traffic Shaper*, atingindo taxa de operação que excederam os 6 Mpps.

ClickOS: O ClickOS [55] é uma arquitetura modular de software responsável pela construção de *middleboxes*. Cada bloco formador do Click é denominado Elemento e representa uma unidade de processamento em toda sua estrutura. A conexão de um conjunto desses elementos em forma de grafo corresponde à configuração do *middlebox*, representando o conjunto de funções desempenhadas por ele. Nessa estrutura, a execução dessas funções decorre do movimento dos pacotes de um elemento para o outro através das arestas do grafo.

A estensão das configurações de um *middlebox* é possível através do desenvolvimento e acréscimo de novos elementos ou mesmo a modificação dos já existentes ao grafo correspondente. Sobre o desempenho do Click, [55] demonstrou que ele funciona bem apesar de sua modularidade. Os testes realizados apresentaram taxa de encaminhamento IP de 73.000 pacotes por segundo, o que equivale dizer que ele é 90% mais rápido que o Linux no mesmo hardware e alguns roteadores comerciais simples de custo equivalente, como o Cisco 2621, por exemplo.

Para que o Click possa ser utilizado em VNFs variadas e desempenhe funções além de um roteador comum, em muitos casos é necessário que os módulos correspondentes ainda sejam desenvolvidos, o que pode levar algum tempo e corresponder ao enfrentamento de problemas ainda desconhecidos na plataforma Click, mesmo assim, sua adoção em ambientes NFV vem sendo apontada como possível e positiva em alguns trabalhos, como [56], que aponta suas características de instanciação rápida, pequena utilização de memória, isolamento entre instâncias, alto desempenho e flexibilidade como sendo necessárias ao NFV.

Para que o Click desempenhe funções além de um roteador comum, pode ser necessário o desenvolvimento dos módulos correspondentes às novas funções. Esse processo pode levar algum tempo ou ser prejudicado por incompatibilidades ainda desconhecidos da plataforma Click, porém é visto como possível e positiva em alguns trabalhos, como [56], que aponta suas características de instanciação rápida, pequena utilização de memória, isolamento entre instâncias, alto desempenho e flexibilidade como sendo interessantes ao NFV.

Outras Tecnologias Habilitadoras: Obviamente, que as tecnologias habilitadoras ao NFV não limitam-se apenas às apresentadas aqui. Como as próprias PoCs, NFV ISG ou independentes, vêm mostrando, os estudos em NFV ainda são iniciais e muitas barreiras devem ser superadas para que essa tecnologia atinja a maturidade necessária. Com a evolução do NFV, é natural que outras tecnologias sejam incluídas gradativamente a esta lista, dependendo apenas das limitações diagnosticadas ou necessidades surgidas.

1.5. Conclusões e Trabalhos Futuros

O modelo de rede atual baseada em software e hardware proprietários vem mostrando-se não escalável para os provedores de serviços de redes e telecomunicações devido às limitações impostas pela dependência de plataformas disponibilizadas pelos fabricantes, o que corresponde a um alto custo de implementação e manutenção dos ambientes de data centers, falta de integração entre tecnologias diferentes, dificuldade na obtenção de mão-de-obra especializada, entre outras.

Nessa linha, apesar de ser um conceito novo, NFV vem sendo apontado como capaz de mudar essa realidade, pois, a virtualização das funções de rede permite a utilização de hardware genérico no lugar de plataformas específicas e dedicadas, o que corresponde a possibilidade de diminuição no custo direto com aquisição de novos equipamentos proprietários e redução do consumo energético por conta da virtualização, o que permite agregar diversas funções de rede em um único hardware. Porém, a viabilidade da adoção do NFV ainda depende de requisitos que devem ser atendidos, como por exemplo a interoperabilidade e portabilidade entre as tecnologias baseadas em recursos físicos e virtualizados, bem como necessita que alguns desafios sejam superados, como garantia de desempenho próximo ao obtido em hardware dedicado.

Atualmente, diversos estudos estão sendo realizados com o objetivo de garantir o desenvolvimento confiável dessa tecnologia, o que garantirá a viabilidade da adoção do NFV em ambientes reais. Exemplos de recentes workshops acadêmicos com foco em NFV incluem: Sessão de demos no Globecom 2013[2], Globecom NFV Demo, ACM CoNEXT 2013 HotMiddlebox Workshop[3], e 2013 Software Defined Networks for Future Networks and Services (SDN4FNS)[4]. Alguns trabalhos que merecem destaque e devem trazer importantes avanços para o estado da arte em NFV são os projetos europeus CHANGE[5], Unify[6], e Trilogy 2[7]. Esse último em particular (Trilogy2), com o motto de "*Building the Liquid Net´´*, é um dos principais contribuidores para os grupos de estudo do ETSI NFV e outros trabalhos relacionados de padronização no IETF (ex: SFC - Service Function Chaining)[8].

[2]http://www.ieee-globecom.org/2013/demos.html
[3]http://conferences.sigcomm.org/co-next/2013/workshops/HotMiddlebox/program.html
[4]http://sites.ieee.org/sdn4fns/
[5]http://www.change-project.eu/
[6]http://www.fp7-unify.eu/
[7]http://www.trilogy2.org/
[8]https://tools.ietf.org/wg/sfc/

References

[1] B. Briscoe, "Network functions virtualisation," November 2013. [Online]. Available: http://www.ietf.org/proceedings/86/slides/slides-86-sdnrg-1.pdf

[2] W. Xu, Y. Jiang, and C. Zhou, "Data models for network functions virtualization," Internet Engineering Task Force, September 2013. [Online]. Available: http://tools.ietf.org/html/draft-xjz-nfv-model-datamodel-00

[3] "Network Functions Virtualization (NFV); Architectural Framework"," ETSI, 2013.

[4] "EU FP7 Trilogy2 project: Building the Liquid Net," http://www.trilogy2.org/, 2014.

[5] GS, "ETSI GS NFV 004 V1.1.1: Network Functions Virtualisation (NFV); Virtualisation Requirements," 10 2013, http://www.etsi.org/deliver/etsi_gs/NFV/001_099/004/01.01.01_60/gs_NFV004v010101p.pdf.

[6] ——, "ETSI NFV Proofs of Concept," 02 2014, http://www.etsi.org/technologies-clusters/technologies/nfv/nfv-poc.

[7] R. Bifulco, T. Dietz, F. Huici, M. Ahmed, J. Martins, S. Niccolini, and H.-J. Kolbe, "Rethinking access networks with high performance virtual software brases," in *Software Defined Networks (EWSDN), 2013 Second European Workshop on*, Oct 2013, pp. 7–12.

[8] W. John, K. Pentikousis, G. Agapiou, E. Jacob, M. Kind, A. Manzalini, F. Risso, D. Staessens, R. Steinert, and C. Meirosu, "Research directions in network service chaining," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Nov 2013, pp. 1–7.

[9] E. P. Quinn and E. T. Nadeau, "Service function chaining problem statement," Informational Draft, IETF Secretariat, Internet-Draft draft-quinn-sfc-problem-statement-02.txt, Feb. 2013.

[10] S. K. Fayazbakhsh, M. K. Reiter, and V. Sekar, "Verifiable network function outsourcing: Requirements, challenges, and roadmap," in *Proceedings of the 2013 Workshop on Hot Topics in Middleboxes and Network Function Virtualization*, ser. HotMiddlebox '13. New York, NY, USA: ACM, 2013, pp. 25–30. [Online]. Available: http://doi.acm.org/10.1145/2535828.2535831

[11] A. Manzalini and R. Saracco, "Software networks at the edge: A shift of paradigm," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Nov 2013, pp. 1–6.

[12] G. Pongrácz, L. Molnár, Z. L. Kis, and Z. Turányi, "Cheap silicon: A myth or reality? picking the right data plane hardware for software defined networking," in *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, ser. HotSDN '13. New York, NY, USA: ACM, 2013, pp. 103–108. [Online]. Available: http://doi.acm.org/10.1145/2491185.2491204

[13] A. Császár, W. John, M. Kind, C. Meirosu, G. Pongrácz, D. Staessens, A. Takács, and F.-J. Westphal, "Unifying cloud and carrier network: Eu fp7 project unify," in *Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing*, ser. UCC '13. Washington, DC, USA: IEEE Computer Society, 2013, pp. 452–457. [Online]. Available: http://dx.doi.org/10.1109/UCC.2013.89

[14] D. Siracusa, E. Salvadori, and T. Rasheed, "Edge-to-edge virtualization and orchestration in heterogeneous transport networks," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Nov 2013, pp. 1–6.

[15] K. Samdanis, A. Kunz, M. I. Hossain, and T. Taleb, "Virtual bearer management for efficient mtc radio and backhaul sharing in lte networks," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*, Sept 2013, pp. 2780–2785.

[16] M. Kobayashi, S. Seetharaman, G. Parulkar, G. Appenzeller, J. Little, J. van Reijendam, P. Weissmann, and N. McKeown, "Maturing of openflow and software-defined networking through deployments," *Computer Networks*, no. 0, pp. –, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912861300371X

[17] GS, "ETSI GS NFV 002 V1.1.1: Network Functions Virtualisation (NFV); Architectural Framework," 10 2013, http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf.

[18] ——, "ETSI GS NFV 001 V1.1.1: Network Functions Virtualisation (NFV); Use Cases," 10 2013, http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf.

[19] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "Sdn security: A survey," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Nov 2013, pp. 1–7.

[20] N. Feamster, J. Rexford, and E. Zegura, "The road to sdn," *Queue*, vol. 11, no. 12, pp. 20:20–20:40, Dec. 2013. [Online]. Available: http://doi.acm.org/10.1145/2559899.2560327

[21] [Online]. Available: http://portal.etsi.org/NFV/NFV_White_Paper.pdf

[22] H. Kim and N. Feamster, "Improving network management with software defined networking," *Communications Magazine, IEEE*, vol. 51, no. 2, pp. 114–119, February 2013.

[23] ONF, "OpenFlow-enabled SDN and Network Functions Virtualization," 02 2014, https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-sdn-nvf-solution.pdf.

[24] K. Pentikousis, Y. Wang, and W. Hu, "Mobileflow: Toward software-defined mobile networks," *Communications Magazine, IEEE*, vol. 51, no. 7, pp. 44–53, July 2013.

[25] X. Jin, L. E. Li, L. Vanbever, and J. Rexford, "Softcell: Scalable and flexible cellular core network architecture," in *Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies*, ser. CoNEXT '13. New York, NY, USA: ACM, 2013, pp. 163–174. [Online]. Available: http://doi.acm.org/10.1145/2535372.2535377

[26] F. Risso, A. Manzalini, and M. Nemirovsky, "Some controversial opinions on software-defined data plane services," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Nov 2013, pp. 1–7.

[27] S. Sezer, S. Scott-Hayward, P. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for sdn? implementation challenges for software-defined networks," *Communications Magazine, IEEE*, vol. 51, no. 7, pp. 36–43, July 2013.

[28] M. Cohn, "NFV Insider's Perspective, Part 2: There's a Network in NFV - The Business Case for SDN," Setembro 2013, http://www.sdncentral.com/education/nfv-insiders-perspective-part-2-theres-network-nfv-business-case-sdn/2013/09/.

[29] CloudNFV, "CloudNFV," http://www.cloudnfv.com/.

[30] CIMI Corporation, "The CloudNFV Proof-of-Concept Was Approved by the ETSI ISG," Dezembro 2013, http://blog.cimicorp.com/?p=1553.

[31] CloudNFV, "CloudNFV Open NFV Framework," 2014, http://www.cloudnfv.com/CloudNFVPoCAsApproved.pdf\#page=1&zoom=auto,0,800.

[32] Project Clearwater, "Project Clearwater - IMS in the Cloud," http://www.projectclearwater.org/.

[33] CloudNFV, "CloudNFV PoC Test Plan," http://www.cloudnfv.com/CloudNFVPoCTestPlan.pdf.

[34] NTT; Cisco; HP; Juniper Networks, "Service Chaining for NW Function Selection in Carrier Networks," Fevereiro 2014, http://nfvwiki.etsi.org/index.php?title=Service_Chaining_for_NW_Function_Selection_in_Carrier_Networks.

[35] AT&T; BT; Broadcom Corporation; Tieto Corporation, "Virtual Function State Migration and Interoperability," Fevereiro 2014, http://nfvwiki.etsi.org/index.php?title=Virtual_Function_State_Migration_and_Interoperability.

[36] CenturyLink; Certes; Cyan; Fortinet; RAD, "Multi-vendor Distributed NFV," Fevereiro 2014, http://nfvwiki.etsi.org/images/NFVPER%2814%29000011_NFV_ISG_PoC_Proposal_-_Multi-vendor_Distributed_NFV.pdf.

[37] Telefonica; Sprint; Intel; Cyan; Red Hat; Dell; Connectem, "E2E vEPC Orchestration in a multi-vendor open NFVI environment," Fevereiro 2014, http://nfvwiki.etsi.org/images/NFVPER%2814%29000010r2_NFV_ISG_PoC_Proposal-E2E_vEPC_Orchestration.pdf.

[38] NFV ISG, “On-going PoCs,” http://nfvwiki.etsi.org/index.php?title=On-going_PoCs.

[39] OpenNaaS Community, “OpenNaaS: Open Platform For Network as a Service,” http://new.opennaas.org/.

[40] P. Minoves, “Mantychore FP7: IP Networks as a Service,” novembro 2010, http://dana.i2cat.net/mantychore-fp7-ip-networks-as-a-service/software/.

[41] OpenNaaS Community, “OpenNaaS: Architecture,” http://new.opennaas.org/wp-content/uploads/2013/11/ONP_Sep2012.pdf.

[42] P. Minoves, F. Ole, B. Peng, M. Andrew, and W. Dave, “Virtual cpe: Enhancing cpe’s deployment and operations through virtualization,” *Cloud Computing Technology and Science (CloudCom)*, vol. 2012 IEEE 4th International Conference, Dezembro 2012. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6427560&isnumber=6427477

[43] S. Perrin and S. Hubbard, “White Paper: Practical Implementation of SDN & NFV in the WAN,” Outubro 2013, http://networkbuilders.intel.com/docs/HR-Intel-SDN-WP.pdf.

[44] Open vSwitch, “Open vSwitch: An Open Virtual Switch,” http://openvswitch.org/.

[45] Intel Corporation, “Impressive Packet Processing Performance Enables Greater Workload Consolidation,” 2012, http://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/communications-packet-processing-brief.pdf.

[46] Wind River, “Wind River Open Virtualization: Enabling Network Functions Virtualization Without Compromises,” 2014, http://www.windriver.com/products/open-virtualization-profile/.

[47] EANTC, “NFV World Showcase at the SDN & OpenFlow World Congress,” Outubro 2013, http://www.eantc.com/showcases/NFV_Showcase/intro/.

[48] C. Rossenhï¿½vel, “White Paper: NFV World Showcase 2013 - Provisioning, Portability and Elasticity,” Outubro 2013, http://www.eantc.de/fileadmin/eantc/downloads/events/2011-2015/SDNOF2013/EANTC-NFV2013-WhitePaper_Final.pdf.

[49] NFV White Paper, “Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & C all for Action. Issue 1,” Outubro 2012, http://portal.etsi.org/NFV/NFV_White_Paper.pdf.

[50] OpenStack, “OpenStack: Cloud Software,” https://www.openstack.org/.

[51] CloudNFV, “CloudNFV PoC Test Phase One,” http://www.cloudnfv.com/CloudNFVPoCTestPhaseOne.pdf.

[52] L. Rizzo, “netmap: a novel framework for fast packet I/O,” usenix ATC’12 (Best paper award), Boston, USA, Junho, 2012.

[53] L. Rizzo and G. Lettieri, "VALE: a switched ethernet for virtual machines," in *ACM CoNEXT'2012, Nice, France*, Dezembro 2012, http://conferences.sigcomm.org/co-next/2012/program.html.

[54] E. Kohler, R. Morris, B. Chen, J. Jannotti, and M. F. Kaashoek, "The click modular router," *ACM Trans. Comput. Syst.*, vol. 18, no. 3, pp. 263–297, Aug. 2000. [Online]. Available: http://doi.acm.org/10.1145/354871.354874

[55] J. Martins, M. Ahmed, C. Raiciu, and F. Huici, "Enabling fast, dynamic network processing with clickos," in *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, ser. HotSDN '13. New York, NY, USA: ACM, 2013, pp. 67–72. [Online]. Available: http://doi.acm.org/10.1145/2491185.2491195