Architecture for Technology Transformation

Service Providers Leverage SDN/NFV to Empower Change

Table of Contents

Executive Summary

Software-defined networking (SDN) and Network Functions Virtualization (NFV) have revolutionized the traditional communication network architectures and have transformed the way communication service providers (CSPs) design their network infrastructure and services. SDN and NFV use standard virtualization technologies to virtualize entire classes of network functions that can be connected or chained together to create network services. The initial interest in introducing SDN and NFV into communication services has been driven by the desire to lower capital costs by replacing dedicated network hardware with generic x86 platforms, and to lower operating costs by leveraging cloud automation tools. As the revolution has progressed, focus has shifted towards a foundational transformation in managed communication services, a migration toward a telecommunication (telco) cloud, and the emergence of distributed virtualized infrastructures.

This paper outlines Juniper's view on the NFV architecture, including the standard architecture developed by European Telecommunications Standards Industry Specification Group (ETSI ISG), as well as the open architectural principles that Juniper provides to enable CSPs to achieve shorter innovation cycles and expedite service deployments with managed services, telco cloud, and distributed virtualized infrastructures.

Introduction

NFV is a network architecture concept that uses the technologies of IT virtualization to virtualize entire classes of network node functions into building blocks that can be connected, or chained together, to create communication services. The NFV architecture is based on the requirements derived from the ETSI ISG, where Juniper has been an active and contributing member. The NFV architecture consists of three main components: management and orchestration (MANO) layer, NFV Infrastructure (NFVI), and virtualized network functions (VNFs).

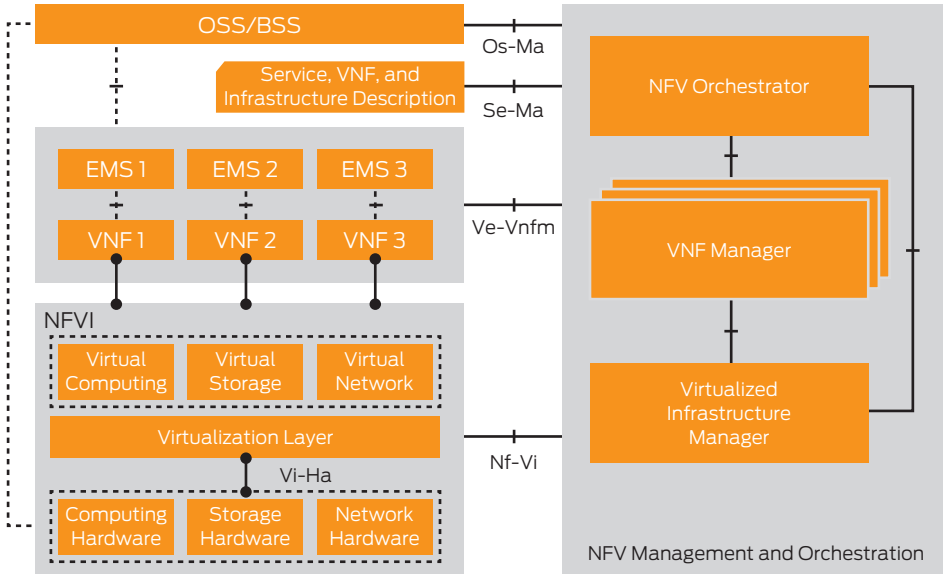

Figure 1: ETSI NFV standard architecture

Management and Orchestration

MANO provides an architectural framework for management and orchestration of all resources in the cloud data center (compute, network, storage), distributed virtualized infrastructures, NFVI, VNFs, and network services. MANO architecture includes three main functions:

- NFV Orchestrator onboards and coordinates the life cycle of VNFs that jointly instantiate a network service. This includes managing the services graphs that define associations between different VNFs, and when applicable between VNFs and physical network functions (PNFs), as well as the topology of the network services. NFV Orchestrator is also responsible for global resource management, including validation and authorization of NFVI resource requests.
- VNF Manager is responsible for service life-cycle management, including instantiating, scaling, upgrading, downgrading, modifying, and terminating VNFs. The VNF Manager functions take into consideration specific service requirements, constraints, policies, key performance indicators (KPIs), as well as service assurance parameters for scaling network operations.
- Virtualized Infrastructure Manager (VIM) controls and manages the NFVI compute, storage, and network resources in the cloud data center.

NFV Infrastructures

NFV aims to leverage virtualization technology to consolidate dedicated network equipment into standard off-the-shelf commercial servers, switches, and storage, which could be located in data centers, network nodes, and at customer premises. The desire to "mix and match" hardware for a common infrastructure stems from the CSPs' relentless drive toward service agility and operational efficiency. The NFVI are designed to interoperate with existing legacy infrastructures where the MANO layer enables a seamless integration and orchestration across NFVI and legacy infrastructures.

VNFs

Virtual network functions are specific network functions that run on one or more virtual machines (VMs), on bare-metal servers, or on top of the physical networking infrastructure. VNFs range from applications such as firewall or application-level gateways (ALGs) that reside on customer premises equipment (CPE) to complex network functions such as Service Gateways, broadband network gateways (BNGs), and Packet Data Network Gateways (PGWs) found in mobile networks.

Juniper's End-to-End NFV Solution

Juniper's automated, programmable, end-to-end NFV solution combines carrier-grade reliability, security, and scalability to simplify the CSPs' transformation of their current infrastructure into an NFV architecture. Juniper's open NFV solution is based on ETSI open-source architecture and can be delivered as a converged end-to-end solution or as a simpler, well designed componentized solution to address a particular CSP use case, such as virtual CPE (vCPE).

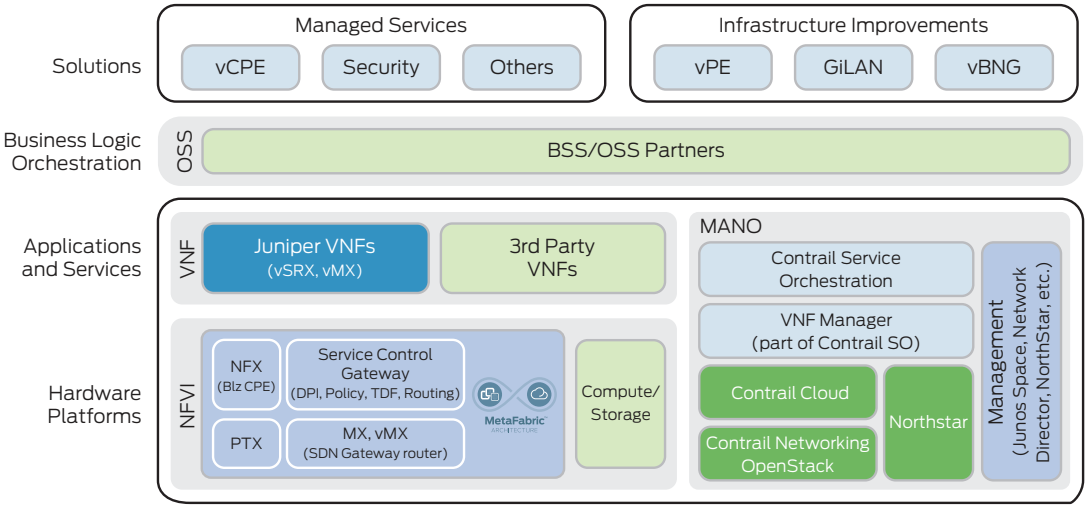

Figure 2: Juniper NFV solution architecture

Management and Orchestration

Juniper's MANO layer consists of Juniper Networks® Contrail Service Orchestration, Contrail Cloud Platform, Contrail Networking, and NorthStar Controller.

Contrail Service Orchestration is a comprehensive management and orchestration platform that simplifies service design and creation, reducing network services delivery from months to just minutes. Based on a web-scalable microservice architecture platform, each service is stateless and the states are maintained in web-scale databases that scale on demand. With Contrail Service Orchestration, CSPs can manage the entire service life cycle and orchestrate services across centralized, distributed, and hybrid deployment models. Contrail Service Orchestration also provides an intuitive and streamlined user experience to manage the service life cycle for various roles. For service designers, it enables a rich service creation and definition platform to create the service catalog. For network administrators, it provides a robust service management and troubleshooting vantage point. For end users, it delivers a personalized self-service portal for service design and performance monitoring.

Contrail Cloud Platform is a foundational element of Juniper's open cloud networking and NFV solutions. Based on open-source technologies, it leverages OpenStack and OpenContrail for cloud management, Ceph distributed storage system, and Puppet server management. Combined with the policy-based automation capabilities of Contrail Networking, Contrail Cloud Platform delivers a robust, multitenant, and elastic cloud for predictable economies of scale, with enhanced interoperability, security, performance, and resiliency.

The NorthStar Controller is a powerful SDN controller and WAN traffic engineering solution that enables granular visibility and control of IP and MPLS flows in large communication networks. It enables CSPs to optimize their network infrastructure through proactive monitoring, planning, and explicit routing of large traffic loads based on the

constraints specified and service-level guarantees. NorthStar Controller is the industry's first multilayer controller that can dynamically interact with transport and optical controllers, reroute IP and MPLS flows, provide time-based path scheduling, and adapt to real-time changes in multiple layers.

NFV Infrastructure

Juniper's NFVI consists of the Juniper Networks NFX250 Network Services Platform, MX Series 3D Universal Edge Routers, Service Control Gateway, PTX Series Packet Transport Routers, and data center and cloud networks built on Juniper Networks MetaFabric™ architecture.

The NFX250 Network Services Platform eliminates the operational complexities of deploying diverse types of CPE to meet multiple customer service needs. As part of Juniper's Cloud CPE solution, the NFX250 gives CSPs and enterprises the flexibility to deploy secure, high-performance virtual services on-premises in a single CPE device.

The SDN-ready MX Series 3D Universal Edge Routers provide universal gateways that interconnect both virtual and physical networks. Key enabling features include support for Multiprotocol BGP (MBGP), dynamic tunnels using MPLS-over-GRE or Virtual Extensible LAN (VXLAN) encapsulation, virtual routing and forwarding (VRF) tables or Ethernet VPNs (E-VPNs), and Network Configuration Protocol (NETCONF), as well as mechanisms to send traffic between VRF and global routing tables based on configuration and policy.

The Service Control Gateway utilizes subscriber awareness, deep packet inspection (DPI), and policy management to determine traffic treatment on a per-subscriber and per-application basis, enabling highly customizable and differentiated services. Implemented on MX Series routers, the Service Control Gateway solution supports multiple services organically, including carrier-grade Network Address Translation (NAT), firewall, server load balancing, IP/MPLS VPNs, switching, and routing. Working with Contrail Cloud Platform, the Service Control Gateway can steer traffic into complex VNF and PNF service chains hosted within the NFVI or existing physical appliances. This granular understanding of traffic flows provides a rich set of data to analytics engines and back-office systems to permit real-time charging and end-user engagement at the application and content level.

The PTX Series Packet Transport Routers bring physical and virtual innovations to the core network. These directly address concerns about operational expenditures, while scaling organically to keep pace with growing traffic demands. The ability to address core networking requirements of performance, deployability, and SDN control begins with the silicon. Juniper's ExpressPlus™ is the first purpose-built telecommunications silicon to engineer a 3D memory architecture into the base design for over 1.6 billion filter operations per second, dynamic table memory allocation for mammoth IP routing scale, and enormous power efficiency gains. CSPs can now deploy a Converged Supercore® architecture with the efficiency of a lean core deployment with NorthStar Controller SDN control, a robust full-featured Internet backbone router, and a converged regional IP and MPLS core router with integrated 100GbE coherent transport for superior performance, elegant deployment, and SDN programmability.

Juniper's MetaFabric™ architecture delivers a simple and open blueprint for building high-performance data centers and cloud networks. It enables CSPs and enterprises to deploy new applications, services, and technologies quickly and easily, with secure, always-on access to data. The MetaFabric architecture delivers an agile and highly efficient network foundation for complex physical and virtual data centers and cloud networks. MetaFabric architecture is not a single product or technology. It is a complete cloud solution that includes a combination of powerful switching, routing, and security platforms, programmable systems, adaptable software, orchestration, SDN, and open APIs that enable integration with the technology ecosystem.

Virtual Network Functions

Juniper is one of the first vendors to introduce VNFs for rapid deployment and scale-out environments. Juniper's VNF solutions include the vSRX virtual firewall and the vMX virtual routing solution.

The vSRX delivers core firewall, networking, and advanced security management capabilities. The industry's fastest virtual security platform, the vSRX offers firewall speeds up to 100 Gbps, providing scalable, secure protection across private, public, and hybrid clouds. A containerized version, the cSRX container firewall, is also available. By leveraging Docker, the cSRX provides an easy and flexible security solution for containerized environments.

The vMX is a full-featured, carrier-grade virtual router with complete control, forwarding, and management planes. It supports sophisticated routing services, and it is ideally suited for rapid service scale-out and agile service introduction and modification for both CSPs and enterprise applications. With its granular, "pay as you grow" licensing model, the vMX reduces the risk associated with new market entry and service innovation; it allows you to start small, move fast, and stay profitable.

The vSRX and vMX serve as a versatile programmatic platform supporting multiple advanced security and routing services. With the CSO's built in service design capability, the vSRX and vMX can be easily configured to provide IP VPN, Software-defined WAN (SD-WAN), firewall, content filtering, antivirus, unified threat management (UTM), virtual provider edge router (vPE), and vBNGs.

Juniper's NFV solution is backed by the Juniper Networks Professional Services organization which, with deployments with the world's leading CSPs, offers extensive experience in planning, building, and migrating to NFV cloud architectures while minimizing risk and delivering results.

Key Benefits

Juniper's end-to-end NFV solution enables a simple and open architecture that accelerates service deployment. Our reference architecture can deliver the following key technical benefits:

- Automation
- Open integration
- Extensibility
- Security
- Dynamic scaling
- Third-party VNFs
- Dynamic service chaining
- Customization

Automation

One of the greatest advantages of NFV as a software-based solution is the ability to automate the entire service life cycle. The service life cycle encompasses all of the steps involved in managing service delivery, including configuration, deployment, policy and security enforcement, assurance, monitoring, scaling, and healing of service usage and performance.

Contrail Service Orchestration leverages OpenStack Heat templates, the OpenStack Neutron plugin, as well as Contrail APIs to automate the task of service life-cycle management based on a logical workflow, with the following primary tasks:

1. Onboard, validate, and catalog network service using VNFs and descriptors.
2. Create, associate, and manage users, roles, and policies.
3. Instantiate network service from GUI self-care portal.
4. Orchestrate policy-based network service workflows.
5. Check and allocate resources based on policies, performance KPIs, and SLAs.
6. Create and update network services configuration, forwarding graphs, and inter-VNF instance connectivity.
7. Configure virtualized network functions using VNF Manager.
8. Monitor network service resource usage and analyze performance KPIs and auto healing.
9. Policy-based auto scaling of network service by allocating additional resources from the resource pool.

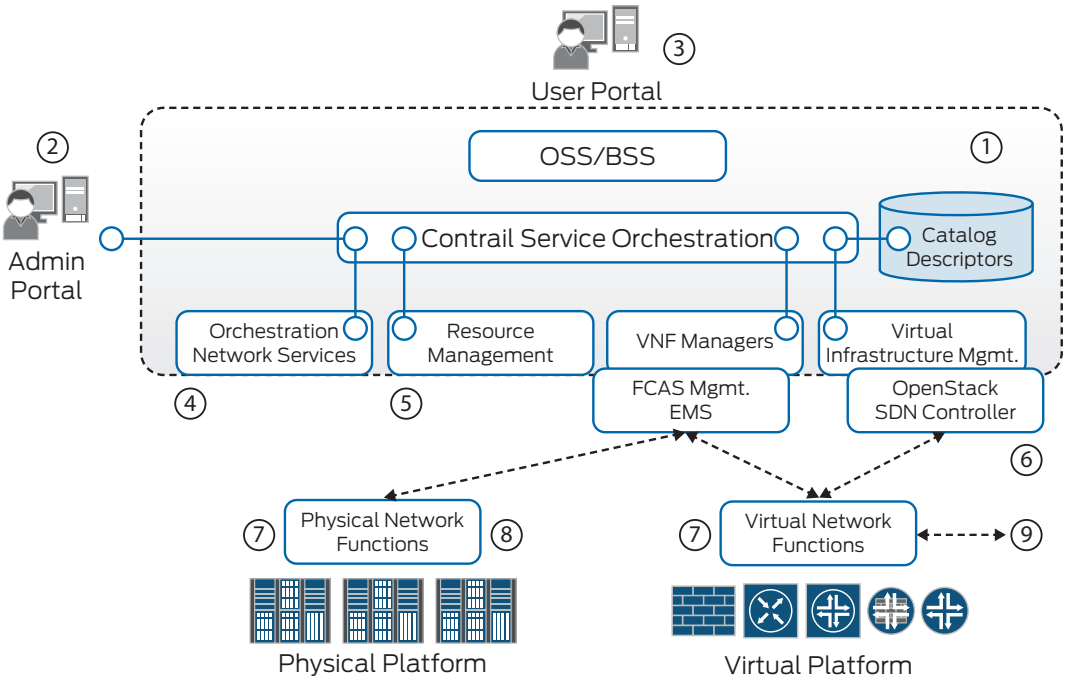

Figure 3: End-to-end service instantiation workflow

Open Integration

The Juniper NFV solution has been developed based on open standards and open-source communities. It uses OpenStack for VIM management and the ETSI specification framework for open architecture. Contributions and projects with industry bodies such as OpenStack and OpenContrail have played a primary role in developing capabilities associated with the Juniper reference architecture. Juniper's NFV solution can easily integrate with existing physical infrastructures, enabling freedom of choice and avoiding vendor lock-in.

Contrail Service Orchestration fully supports open protocols and seamless API integration. The northbound API towards operations and business support systems (OSS/BSS) is an open and standardized REST and RESTConf API, enabling third-party OSS and BSS vendors to integrate business workflow and management applications. Contrail Service Orchestration also provides a network service design toolset, self-service application, and associated APIs, which could be easily integrated into a customer-facing portal—a critical component for a managed service platform.

Contrail Service Orchestration's southbound API supports integration with the VIM layer based on OpenStack, as well as kernel-based virtual machine (KVM) virtualization. Contrail Service Orchestration is also able to support different VIMs, including VMware and other SDN controllers. And, it supports the configuration of virtual and physical functions via VNF and PNF managers with Netconf and RESTconf protocols.

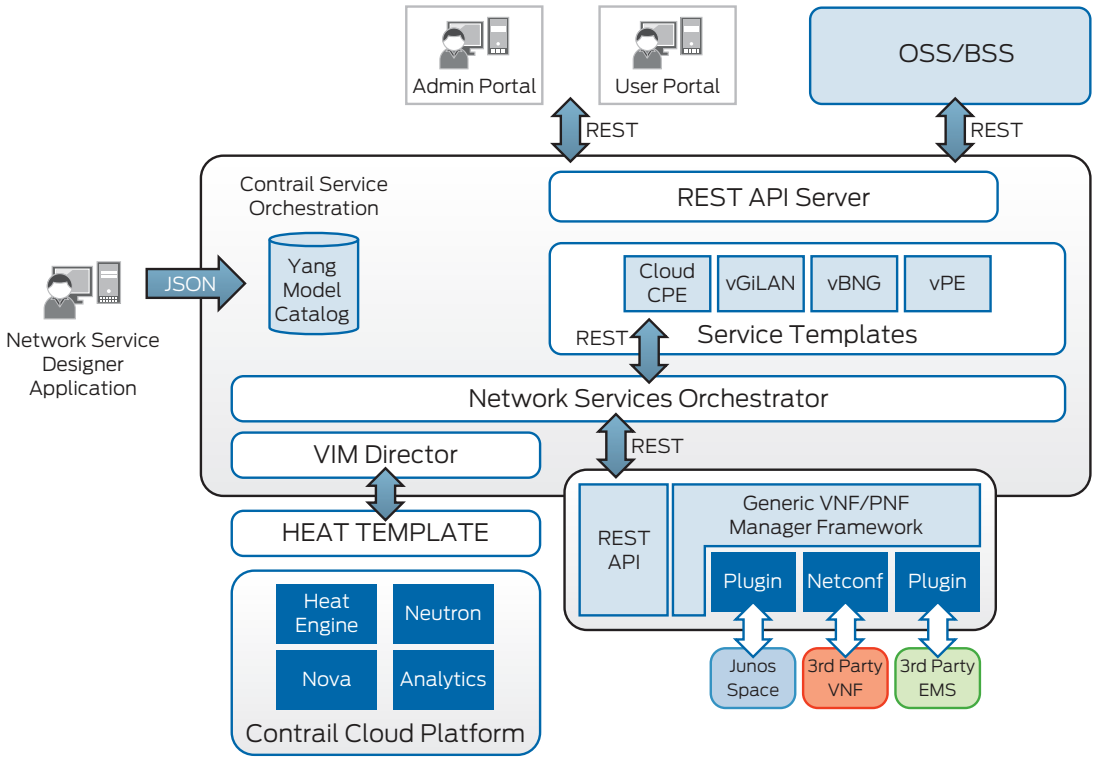

Figure 4: Open integration

Extensible Across Virtual and Physical Environments

Juniper's NFV solution is designed to support multiple deployments where functions and features are consistent across physical and virtual environments. This is exemplified by the vMX virtual router and vSRX virtual firewall. The vMX is a virtual version of MX Series routers that is optimized for x86 servers. The vSRX is a virtual security solution that offers the rich functionality of SRX Series Services Gateways in a virtual format. Both vMX and vSRX are powered by the Juniper Networks Junos® operating system and support advanced release synchronization to ensure ongoing feature parity.

Virtual and physical solutions can be selected based on specific business goals and objectives without any operational penalty or risk, empowering CSPs to completely control the pace of network evolution without disrupting established operating environments.

End-to-End Security

Unlike tightly integrated physical network devices, virtualized networks consisting of many software subcomponents require end-to-end security that keeps pace with evolving threats without sacrificing the reliability, visibility, or control that virtualized environments demand.

Juniper's NFV solution leverages OpenStack Keystone to provide automated identity management, authentication, role-based access control, and policy enforcement. It also uses secure HTTP communication for REST API interconnectivity. End-to-end security enhancement on the Juniper NFV solution can be classified in the following three layers:

- **Infrastructure layer:** Communication and interaction between network components and subscriber database are secured where only authenticated profiles are allowed access to the network. Automation proactively uses real-time feeds on emerging threats so that security enforcement points within the network can automatically filter malicious traffic and denial-of-service (DoS) type attacks without requiring any human interaction.
- **VNFs and applications layer:** Access to VNF Manager and application data is secure, controlled, and isolated as defined by the policy-driven user profiles.
- **Users**: Automated security provides encryption and key management, where only authorized users can access network management and control functions.

Dynamic Scaling

Juniper's NFV reference architecture addresses the challenge of network elasticity, enabling dynamic allocation of network resources and network services (VNFs) to fit changing capacity and traffic conditions.

Contrail Service Orchestration automates the management of network resources. When a predefined threshold is reached, automatic scaling is initiated. Additional CPU cores and virtual machines (VMs) are commissioned as traffic volume increases (scale-up), and are later scaled back when traffic load becomes lighter (scale-down). New services can also be rapidly introduced and expanded by adding new VNF resources (scale-out).

Third-Party VNFs Ecosystem

Contrail Service Orchestration is based on a modular architecture with multiple subcomponents such as a service catalog and service templates. This modular architecture facilitates the integration of relevant components for a solution to meet the business objectives of CSPs. It also enables integration, hosting, and support of third-party VNFs, allowing CSPs to rapidly deploy innovative services. Third-party vendors or developers can easily deploy VNFs on Juniper's NFV solution with minimal integration using standard APIs.

Contrail Service Orchestration provides automated life-cycle management for all VNF applications. As part of the application onboarding process, a VNF descriptor is created. The descriptor outlines the components of the application, the dependencies between its components, application performance parameters, and the actions taken when certain life-cycle events occur.

Third-party VNFs with their descriptors are onboarded as network service templates and published in the NFV service catalog. The descriptors for VNFs and network services are defined using the YANG data model. Contrail Service Orchestration converts YANG data for OpenStack Heat templates to deploy virtual network services and also converts to NETCONF for physical network function support. It also leverages available virtual components, including virtual links, virtual ports, forwarding graphs, and other network constructs in the NFV service catalog to create repeatable instances.

Dynamic Service Chaining

Traditionally, building service chain to support new network applications was a complicated process. Each new service required specialized hardware devices provisioned to support the maximum level of demand. Devices had to be individually configured where the chance of errors was high, and an issue in one component could disrupt the entire network. Service chains were also often built to support multiple applications. As a result, data sometimes passed through unnecessary network devices or servers and consumed extra bandwidth and CPU cycles.

Contrail Service Orchestration enables dynamic service chaining. A GUI-based network service designer simplifies the creation and configuration of service chains. An automated framework intelligently manages service chaining where the path for any packet traffic can be dynamically managed based on policy, subscriber, or a particular set of service parameters as defined by CSPs.

Dynamic service chaining expedites service creation, eliminates human errors, and reduces the chances for inconsistent device configuration and network interruptions.

Customized Service Delivery

Juniper's NFV solution simplifies service creation and supports highly customized service delivery. A built-in network service designer with functional drag-and-drop designer tools enables CSPs to quickly create and deliver customized services. The highly intuitive portal dashboard, modeled after the SlipStream UI design, comprises a set of primary horizontal top menu options and vertical sub-menu options on the left side of the screen. The network service designer provides the flexibility to choose appropriate VNFs, design functional service chains, specify interface data paths, and implement policies and quality-of-service (QoS) rules designed to meet overall performance goals.

Telecommunication Cloud

A traditional telco service can be described as a set of solutions distributed over multiple domains. These domains, in turn, are supported by transport layers consisting of resources such as switches, routers, and firewalls. These resources perform complex and sophisticated interconnection functions in support of telco services. Functions often require multiple dedicated VPNs and VLANs, extensive load balancers, security, address translators, proxies, redundancy, latency control, policy-based routing, as well as carrier-grade QoS.

In traditional networks, transport layers are provided by dedicated site infrastructure incorporating purpose-built proprietary hardware. In the telco cloud and NFV environment, domains become a tenant of a federated cloud infrastructure where many transport layer functionalities can be replaced with VNFs.

The basic networking capabilities provided through VNFs can range in complexity from basic routing to multi-network routing and forwarding capabilities. Advanced capabilities include virtual private cloud (VPC), vBNG as well as carrier-grade NAT, virtual evolved packed core (vEPC), virtual service control gateway (vSCG), GiLAN services, and DPI and traffic detection-steering function (DPT/TDSF).

The evolution of virtualization technologies, as well as the Central Office Re-Architected as a Datacenter (CORD) movement, have expanded the boundary of telco cloud beyond centralized data centers. Juniper's end-to-end NFV solution offers a flexible architecture that fully addresses the unique idiosyncrasies of multi-dimensional deployment models.

The path toward NFV and telco cloud will likely be an evolutionary approach. CSPs will retain existing infrastructures while expanding selected new network infrastructures based on virtual capabilities and deployment models. This gradual approach minimizes the risk of network migration, empowering the CSPs to completely control the pace of network evolution without disrupting established operating environments, while achieving substantial network efficiency, operational flexibility, CapEx savings, as well as a faster time to market for new network services.

Managed Services

Managed communication services have become a critical requirement for today's market environment as enterprises have become increasingly reliant on CSPs to support business operations and transactions. CPE has been one of the most important connectivity services from CSPs to enterprise customers.

While the traditional CPE service delivery model has served the market well for years, there are a number of challenges associated with deploying, managing, and evolving these managed services. The ability to innovate in the area of managed services is dependent on the hardware and software platforms deployed with the CPE device. CSPs typically employ diverse and closed platforms that inhibit scalability and require large upfront investments. As new services and locations are added or extended, hardware costs continue to multiply. CPE deployment is a time-consuming process. Each CPE device needs to be manually configured and provisioned, resulting in substantial delays and business interruptions. Any subsequent CPE device repair and upgrade involves costly updates across databases and network elements. Chances of errors that could severely impact services for the enterprise customers are high.

NFV revolutionizes managed service delivery and life cycle operation. CSPs are less dependent on device-centric service delivery and manual workflows, making them more relevant to their customers. Enterprise customers can choose from a wide variety of customized services, available on demand. NFV empowers CSPs to move from a device-centric and manual-intensive business model to a software-based cloud model, accelerating service innovation that ultimately increases their competitiveness, revenue, and profitability.

Use Case—Juniper Networks Cloud CPE Solution

Juniper Networks Cloud CPE is a scalable virtualized CPE solution that replaces dedicated CPE hardware with multiple routing and security VNFs, such as Juniper's vSRX virtual firewall and vMX virtual router, into a highly scalable end-to-end solution. Built on Juniper's NFV architecture, the Juniper Cloud CPE solution automates service delivery consistently and coherently across distributed, centralized, and overlay deployment models.

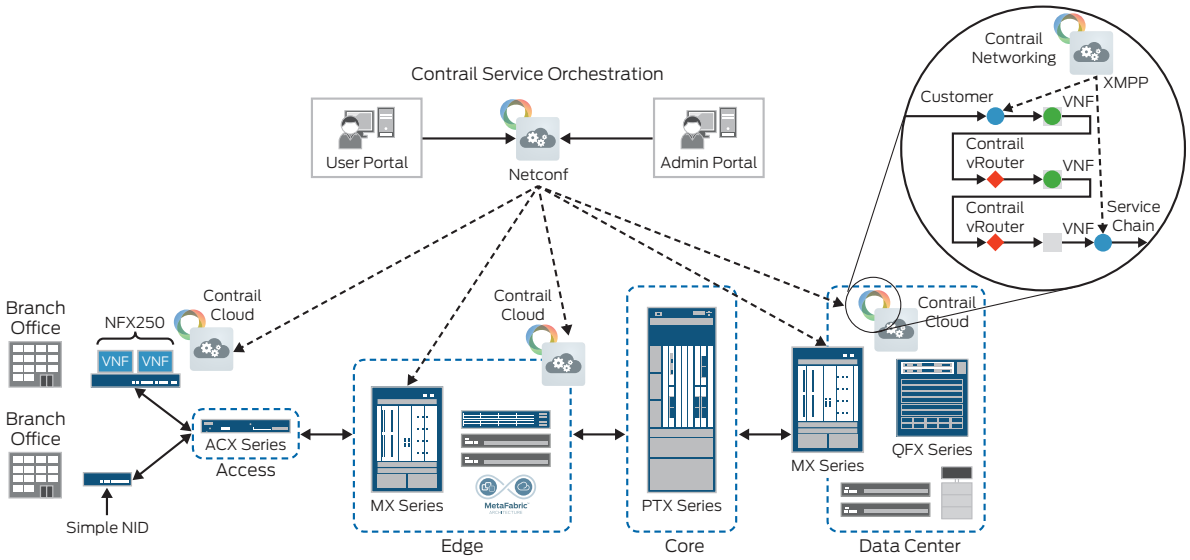

Figure 5: Juniper Cloud CPE solution

Juniper's Cloud CPE solution incorporates Contrail Service Orchestration, a modular service orchestration and service assurance layer with a robust resource management and control layer on an open framework. Automated service creation simplifies the service life cycle, enabling CSPs to quickly conceive and create highly customizable services in minutes. Services and capacities can be dynamically updated, improving the scalability and flexibility of managed CPE services. Subsequent service additions, changes, and expansions can be fully automated, replacing traditional manual processes; this not only reduces the risk of human error, it virtually eliminates network interruptions.

The Juniper Cloud CPE solution supports a variety of use cases, including IP VPN, SD-WAN, firewall, content filtering, antivirus, and UTM, as well as the integration of third-party VNF applications.

Conclusion

Given the explosive growth of new communication applications and unpredictable traffic patterns, it is no longer practical for CSPs to build dedicated network infrastructures that serve one network function and scale only as far as allotted capacity. Rather, CSPs require a dynamic open architecture that is agile, flexible, and can improve infrastructure growth based on the demand and traffic patterns of different communication services.

The emergence of SDN, NFV, and virtualization technologies has promised a new era of innovation. In the face of these innovations and opportunities, CSPs can maximize business outcomes by undergoing a technology transformation. Instead of relying on the physical preprovisioning of infrastructure, CSPs can now leverage NFV and SDN solutions to implement a new generation of network architecture. This new architecture will be able to actively respond to shifting market conditions with application-agnostic processing resources, automated orchestration, and dynamic scalability that will reduce time to deploy new services, increase operational agility, and immediately unlock market opportunities in this increasingly competitive market.

Juniper Networks has an unwavering commitment to innovative transformation. With our field-proven SDN and NFV end-to-end solution as well as our experience from deployments with global CSPs, Juniper has been a collaborative partner for unlocking market opportunities while driving sustainable long-term competitive advantages. We are the leaders that have helped CSPs complete the shift into IP platforms, and we will continue to facilitate their transformation journey into NFV and beyond.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

2000633-002-EN Feb 2017