vMX

Francisco Sánchez

Iberia SE

October 2015

AGENDA

1	vMX Product Overview
2	Physical or Virtual MX
3	Use Cases and Deployment Models
4	Summary
5	Q & A

What is network functions virtualization

Network Functions Virtualization (NFV) falls within the realm of Software Defined Networks (SDN), so can be implemented on top of an SDN network, or other architecture, and has similar goals:

- Increased flexibility of the network
- Reduction in time-to-market of new services
- Optimization of capex and opex

Network functions virtualization (NFV) virtualizes network node functions so they can be put together as building blocks.

The idea of NFV emerged from the telecommunications industry in 2012.

More than 38 telecoms players have signed up to the European Telecommunications Standards Institute Network Functions Virtualization Industry Specific Group (ETSI NFV ISG).

Product overview

THE UNIVERSAL EDGE ROUTER

ONE TRIO CHIPSET
ONE UNIVERSAL EDGE

JUNOS®

one

N8A150   03D6
0806
90620013
PHILIPPINES

64 Tbps

32 Tbps

10 Tbps
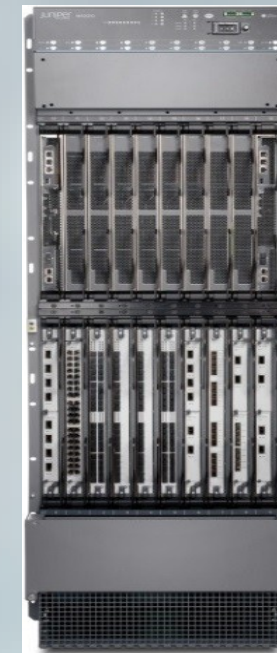
6 Tbps

2 Tbps

80 Gbps

80 Gbps

| MX 80 | MX 104 | MX 240 | MX 480 | MX 960 | MX 2010 | MX 2020 |

PORTFOLIO FOR ALL SIZES & CAPACITIES

MX Virtualization Strategy

Software

Applications

| Enterprise Edge/Mobile Edge | Aggregation/Metro/Metro core | Service Provider Edge/Core and EPC | Data center/Central Office |

Control Plane and OS: Virtual JUNOS, Forwarding Plane: Virtualized Trio

Virtual Routing Engine, Virtual Route Reflector

VCPE, Enterprise Router

Virtual PE, Virtual BNG/LNS, Hardware Virtualization

MX SDN Gateway

Cell Site Router

Branch Office

HQ

Carrier Ethernet Switch

Aggregation Router/ Metro Core

Service Edge Router

Core

Mobile & Packet GWs

DC/CO Edge Router

vBNG, vPE, vCPE

Leverage R&D effort and JUNOS feature velocity across all physical & virtualization initiatives

What is vMX?

- Virtualized Juniper MX platform with complete control, forwarding and management plane.

- Aiming for complete feature parity and function consistency between physical and virtual MX, to ease deployment and operation processes.

- Carrier grade routing feature support, plus superior new feature delivery method through release synchronization between physical & virtual.

vMX Product Overview - Components
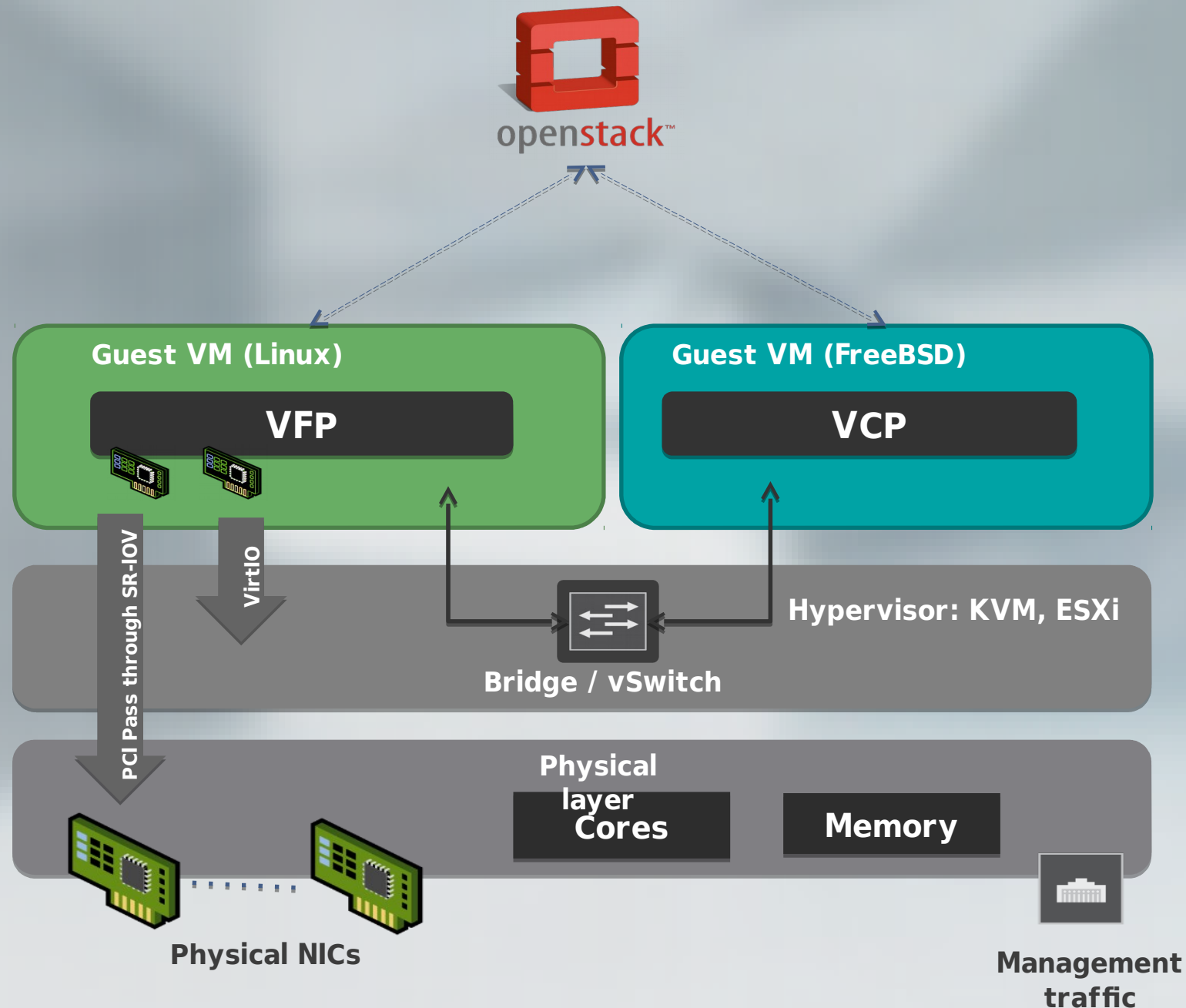
Virtual Control Plane (VCP)

- Virtual JUNOS hosted in a VM. Offers all the capabilities available in JUNOS
- Management remains the same as physical MX
- Follows standard JUNOS release cycles
- Software licenses for different applications and throughputs

Virtual Forwarding Plane (VFP)
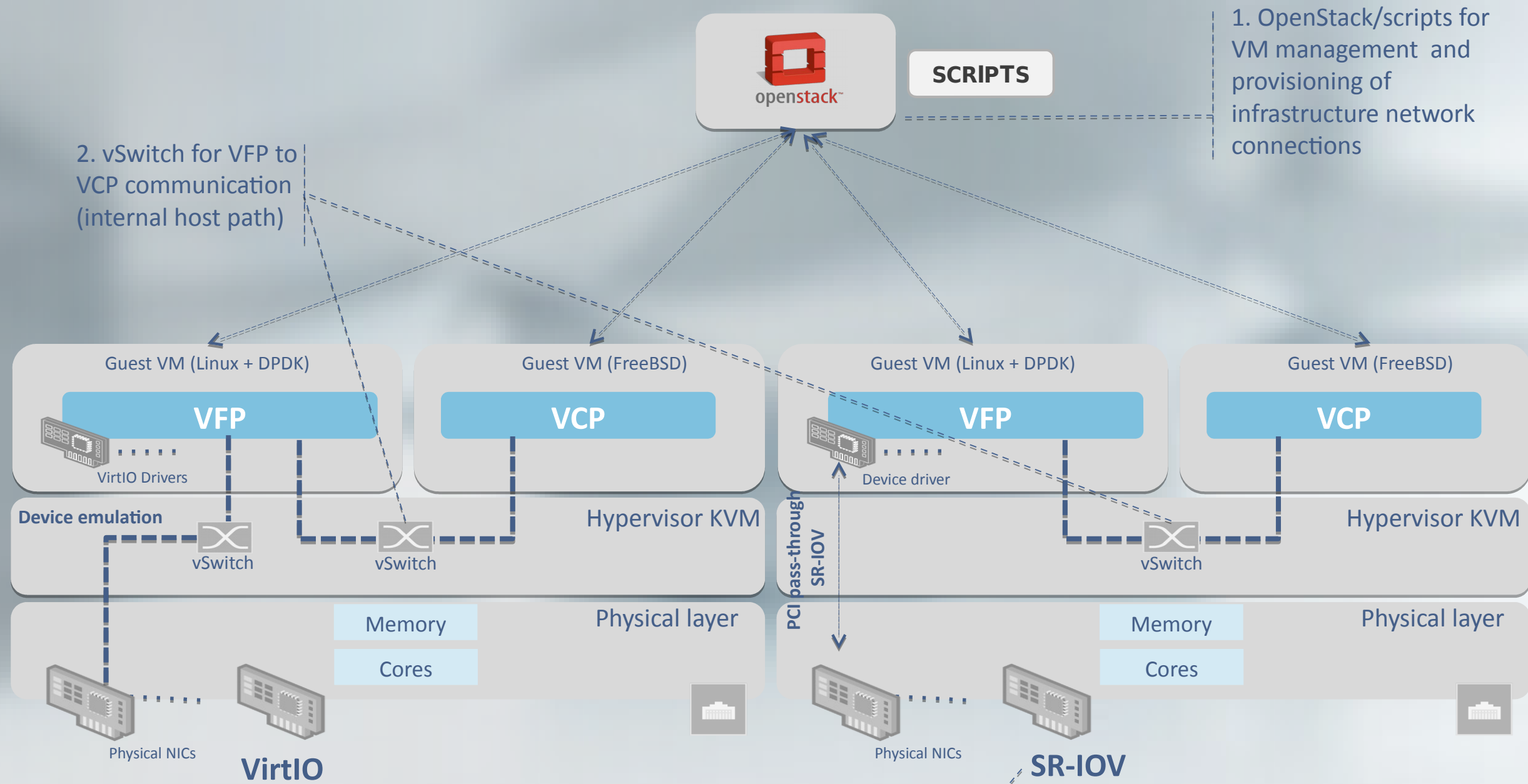
- Virtualized Trio software forwarding plane. Feature parity with physical MX. Utilizes Intel DPDK libraries
- Multi-threaded SMP implementation allows for elasticity
- VirtIO and SR-IOV capable for high throughput
- Can be hosted in VM or bare-metal

Orchestration

- vMX instance can be orchestrated through OpenStack Kilo HEAT templates
- Package comes with scripts to launch vMX instance

VMX system architecture - I/O Virtualization

1. OpenStack/scripts for VM management and provisioning of infrastructure network connections

2. vSwitch for VFP to VCP communication (internal host path)

SCRIPTS

Guest VM (Linux + DPDK)

VFP

VirtIO Drivers

Guest VM (FreeBSD)

VCP

Guest VM (Linux + DPDK)

VFP

Device driver

Guest VM (FreeBSD)

VCP

Device emulation

Hypervisor KVM

vSwitch

vSwitch

Hypervisor KVM

vSwitch

Physical layer

Memory

Cores

PCI pass-through SR-IOV

Physical layer

Memory

Cores

Physical NICs

VirtIO

Physical NICs

SR-IOV

3. Physical NIC can be assigned to the VM. Optimized data path from physical NIC to vNIC via SR-IOV (Single Root IO Virtualization).

Physical and Virtual MX

Physical

Virtual

CONTROL PLANE

DATA PLANE

ASIC/HARD WARE

JUNOS

PFE

TRIO UCODE

Microcode cross-compiled

JUNOS

VFP

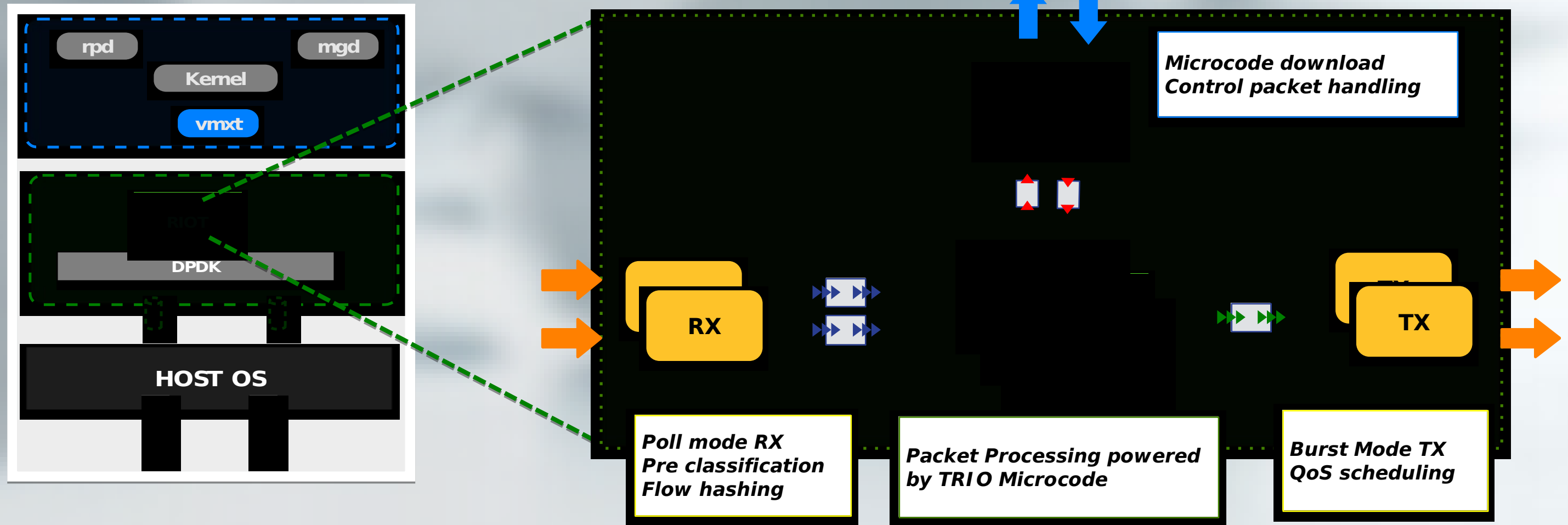**X86 instructions**
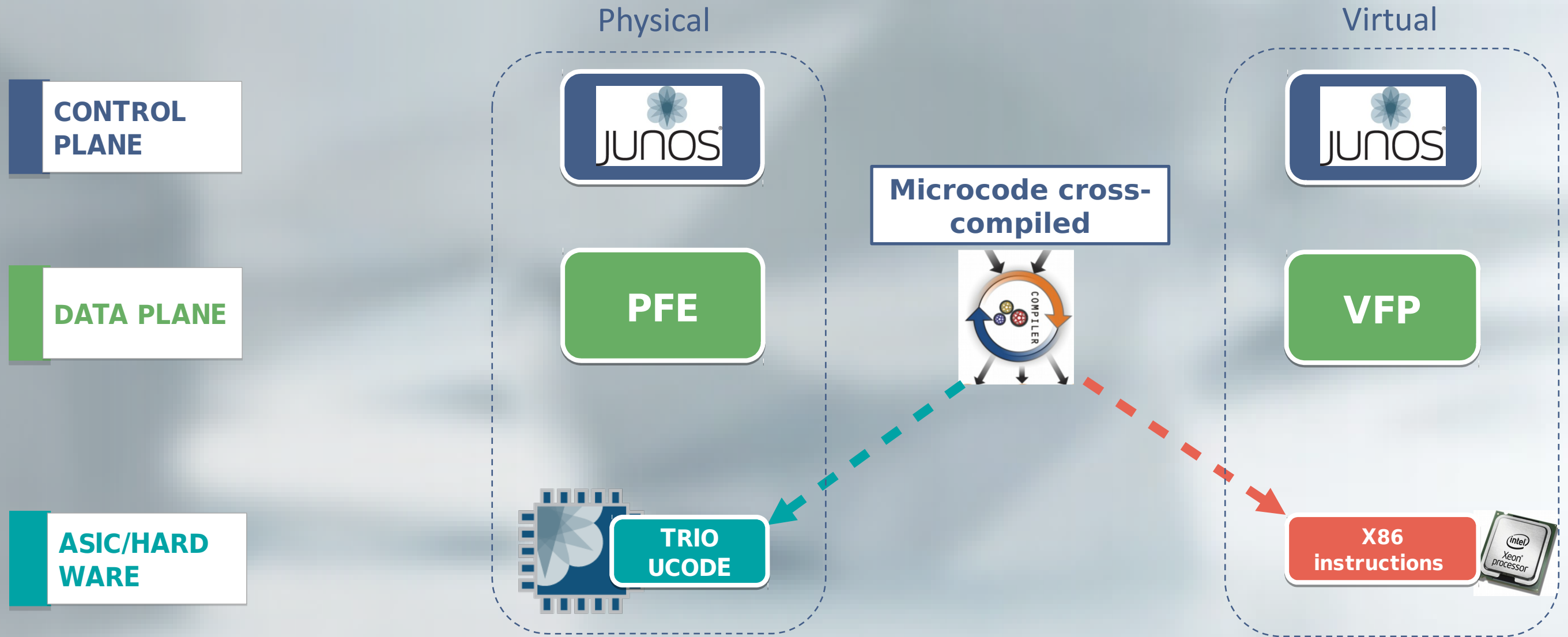
Cross compilation creates high leverage of features between Virtual and Physical with minimal re-work

Virtual TRIO Packet Flow

Virtual TRIO Packet Flow

rpd
mgd
Kernel
vmxt
RIOT
DPDK
HOST OS

Microcode download
Control packet handling

RX

TX

**Poll mode RX
Pre classification
Flow hashing**

**Packet Processing powered
by TRIO Microcode**

**Burst Mode TX
QoS scheduling**

VMX QoS model

LEVEL-1 **LEVEL-2** **LEVEL-3**

PORT

VLAN 1

VLAN 2

VLAN n

S I X   Q U E U E S

Q0 — High
Q1 — Medium
Q2
Q3
Q4 — Low
Q5
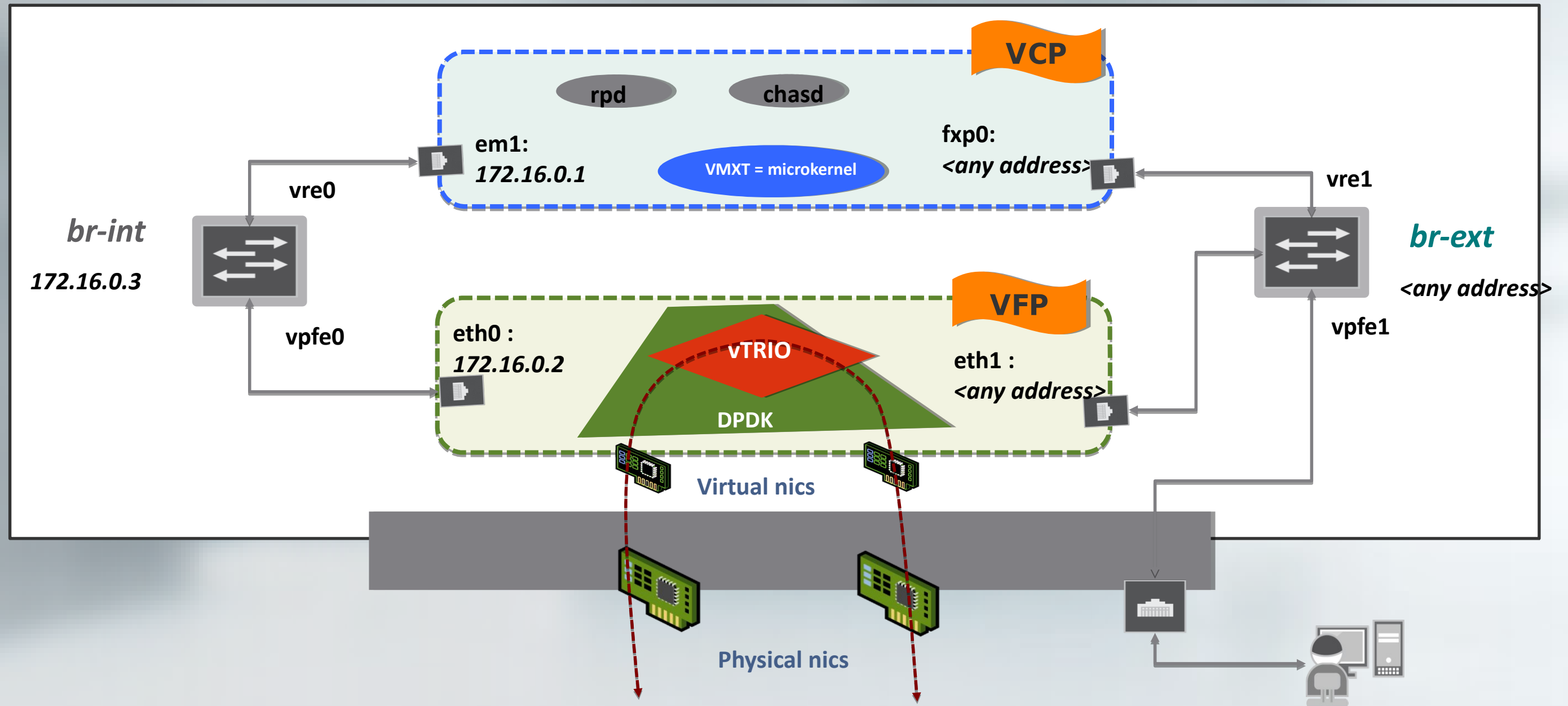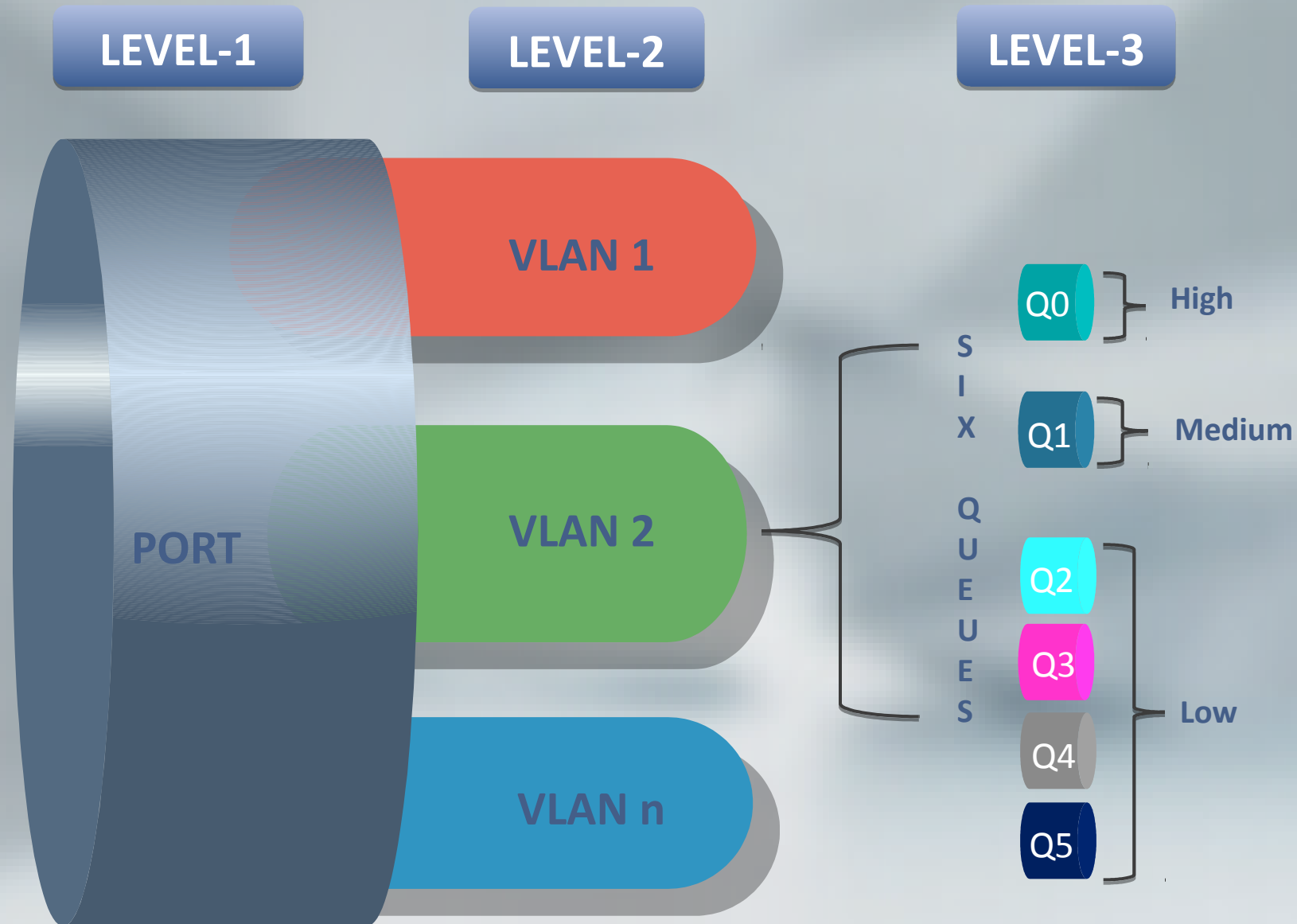
- Port:
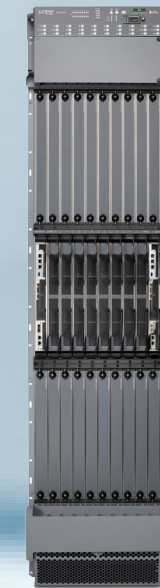 - Shaping-rate
- VLAN:
  - Shaping-rate
  - 4k per IFD
- Queues:
  - 6 queues
  - 3 priorities
    - 1 High
    - 1 medium
    - 4 low
- Priority groups scheduling follows strict priority for a given VLAN
- Queues of the same priority for a given VLAN use WRR
- High and medium queues are capped at transmit-rate

Physical or virtual MX

MX2020

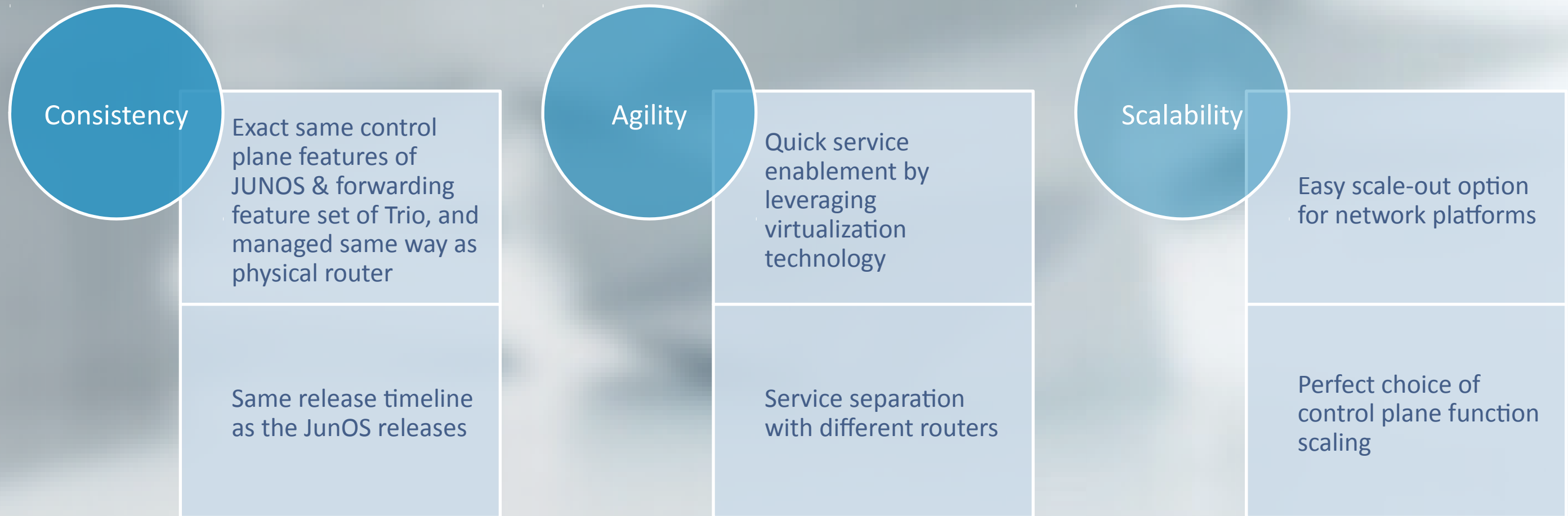**vMX**

Physical or non-virtualized technology

vMX is a new tool

- vMX is a new tool offered to the market
- Before we draw conclusion on where and how to use the tools or even thinking of replace another tool, let's understand their characteristics & capabilities first

Key Benefit of vMX

Consistency

Exact same control plane features of JUNOS & forwarding feature set of Trio, and managed same way as physical router

Same release timeline as the JunOS releases

Agility

Quick service enablement by leveraging virtualization technology

Service separation with different routers

Scalability

Easy scale-out option for network platforms

Perfect choice of control plane function scaling

Physical vs. Virtual

Physical	Virtual
High throughput, high density	Flexibility to reach higher scale in control plane and service plane
Guarantee of SLA	Agile, quick to start
Low power consumption per throughput	Low power consumption per control plan and service
Scale up	Scale out
Higher entry cost in $ and time	Lower entry cost in $ and time
Distributed or centralized model	Optimal in centralized cloud-centric deployment
Well development network mgmt system, OSS/BSS	Same platform mgmt as Physical, plus same VM mgmt as a SW on server in the cloud
Variety of network interfaces for flexibility	Cloud centric, Ethernet-only

Physical vs virtual

Physical MX

vMX @ the Cloud

CERTAINTY

UNCERTAINTY
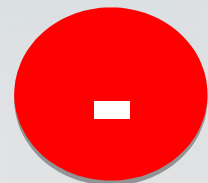
vMX

+
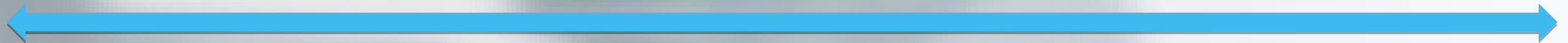
Up to 1Tbps/slot. 40Tbps
Deterministic performance
High speed interfaces (100G)
Very space & power efficient
Very good when there is certainty (on the demand)

Easy deployment of a VM
Flexibility
Low entry cost
Very good when there is uncertainty (on the demand)
Allows new business models.

-

Requires hardware deployment.
Large entry costs

Requires a DC & Cloud infrastructure
Requires Orchestration.
Space & power inneficient.
Lower scalability.
Lower scale interfaces

Cost perspective HW vs. SW

TCO $$$

SW IMPLEMENTATION (AKA VIRTUALIZED)

HW IMPLEMENTATION

The cross point will shift left or right as technology evolves

CAPACITY
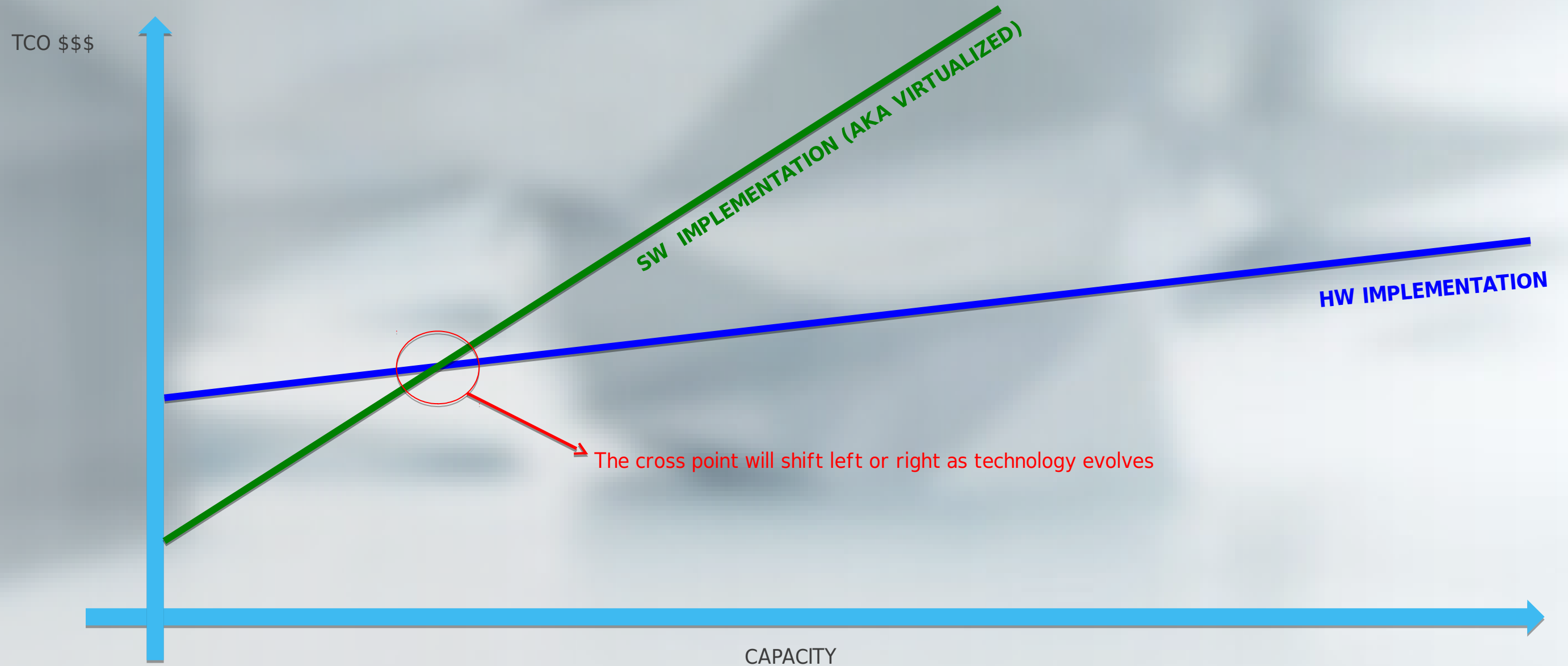
Organizational Implications

Business processes must be re-engineered, organizations must adopt and support a _more_ software-like environment

Organizational Impacts	Roles, Skills & Process Impacts	Cultural Impacts

• CIO organization increasingly takes on Network Ops
 	
• CTO responsibilities become future focused
 	
• CMO organization becomes more technical and feature focused
 	
• Sales organizations evolve to sell solutions regardless of network type or user equipment
	• "Chief Software Architect" – a new role under the CIO, that manages SDN "service creation teams"
	
	• SDN Engineering & NFV support roles added to IT organization
	
	• Agile methodology is used for software and service development, and realized via DevOps implementation
	
	• Shift from capacity planning to utilization management
		• Culture transitions from traditional silo-ed service provider functions to that of an ITSP Services Company in terms of:
		  - Solution Sales
		  - Customer Orientation
		  - Innovation
		  - Experimentation
		  - Accountability
		  - Talent acquisition and Development

Wait! there is another dimension!!

- Deployment in COs, requires hardware prepared for certain environmental conditions (temperature, humidity, …NEBS).
- So, it is not just x86 vs. ASICs, but "CO compliancy".
- "Usually" ASICs based devices are "CO compliant".
- x86 servers may or may not be compliant.
- But this must be taken into account:
  - A "CO located" x86 Cloud should be compliant.
  - A "Data Center located" Cloud could be non compliant.
  - This must be considered when deciding which functions can be centralized on a DC (latency acceptable) and which cannot, and must be deployed on a CO/PoP.

Physical or virtual, which one??

Physical or virtual, which one?

The answer is, why choose?
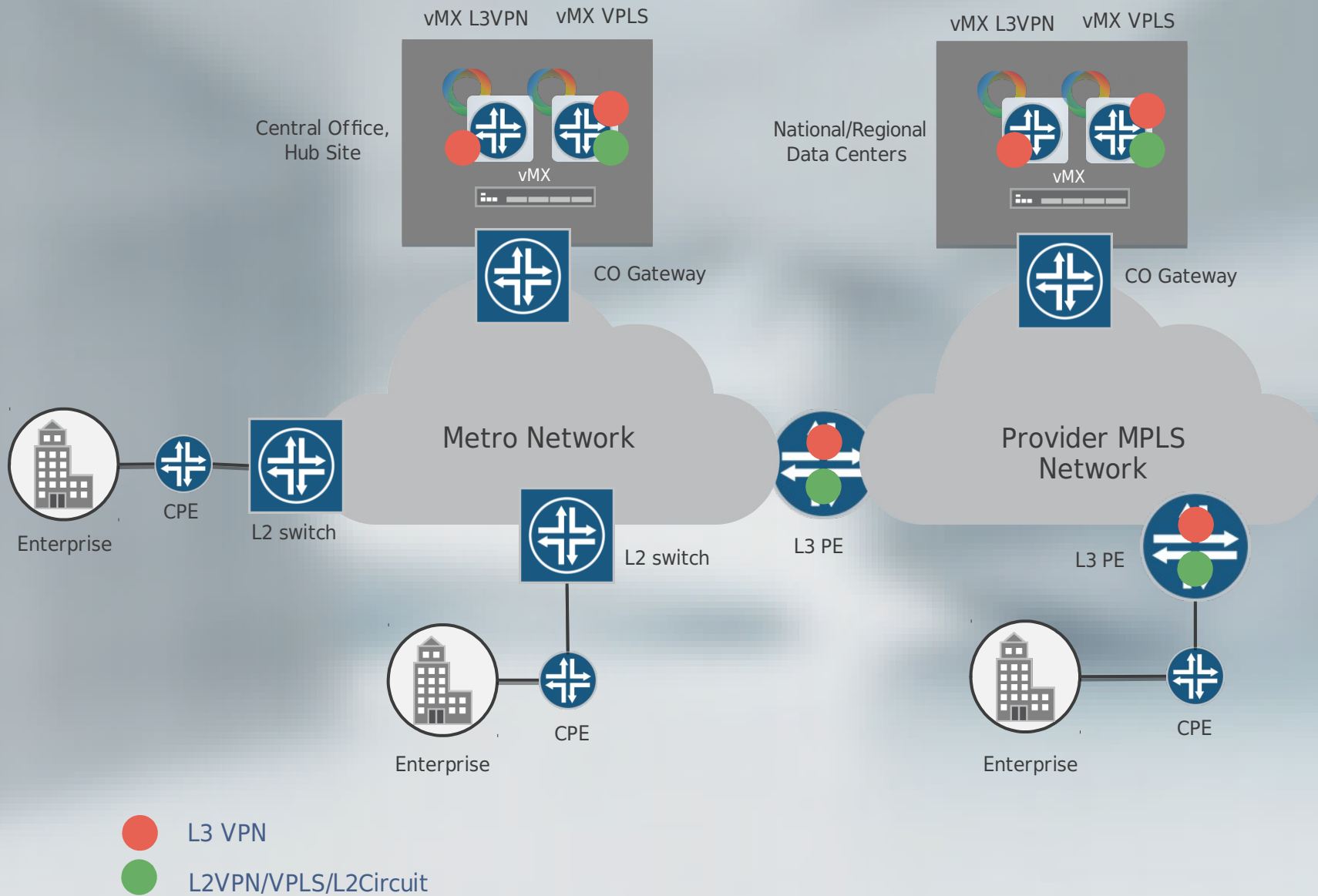
The ultimate choice is up to the needs of the customer, and Juniper provide both.

Beyond simple function mapping, why not think differently, and build the network differently to truly embrace the best of both worlds?

Use-Cases

vMX behaves the same way as the physical MX
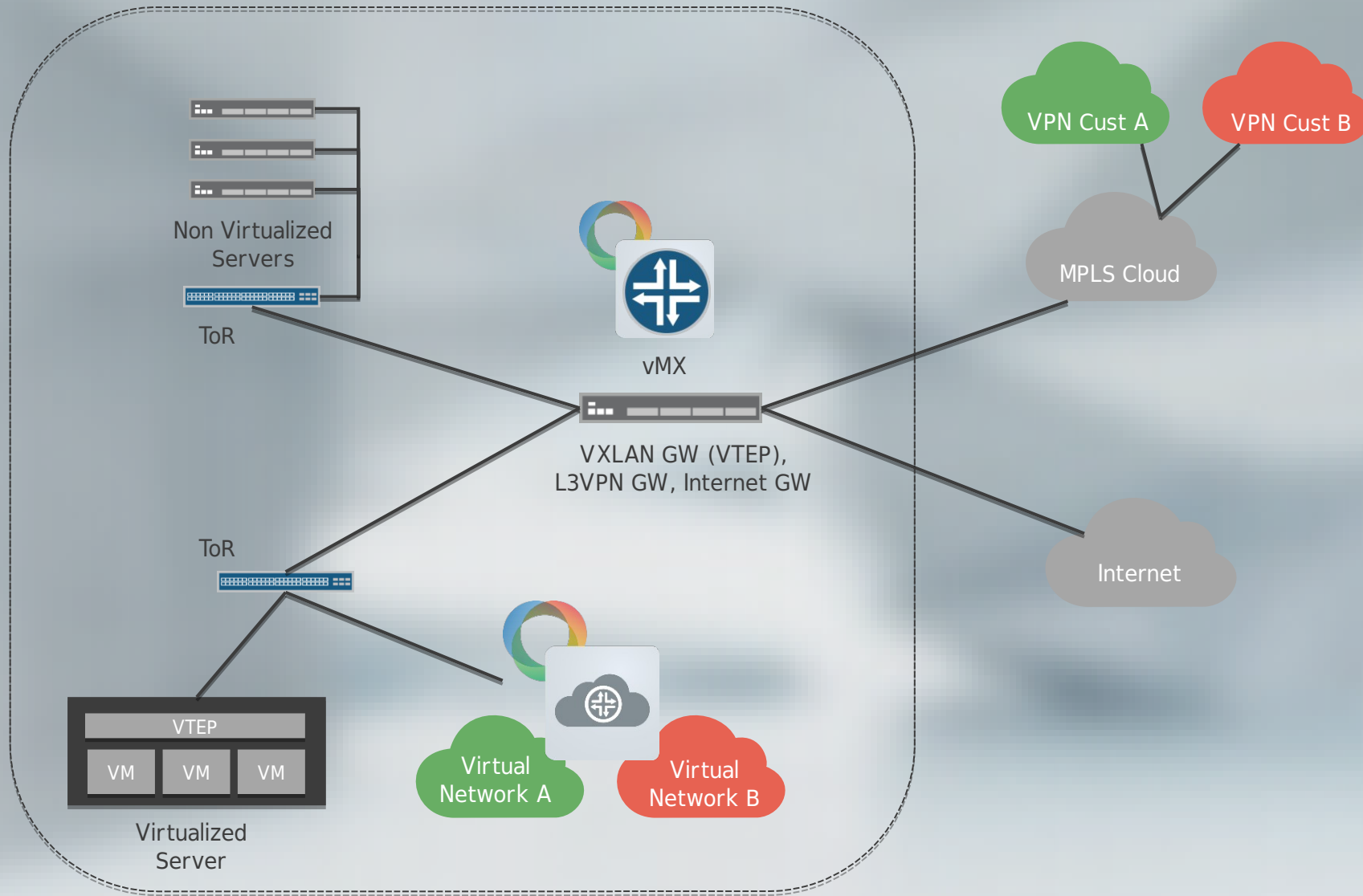
vMX Use-Case: Virtual PE

Use-case

- Scale-out deployment scenarios
- Low bandwidth, high control plane scale customers
- Dedicated PE per customer
- Small PE in a new market segment or geography with ability to support secure transport

vMX value proposition

- vMX is a virtual extension of a physical MX PE with all the capabilities of a carrier class PE router
- vMX offers IPSec and IPSec VPN capability
- Orchestration and management capabilities inherent to any virtualized application apply

Diagram labels:
- vMX L3VPN
- vMX VPLS
- Central Office, Hub Site
- vMX
- CO Gateway
- National/Regional Data Centers
- Enterprise
- CPE
- L2 switch
- Metro Network
- L2 switch
- CPE
- Enterprise
- L3 PE
- Provider MPLS Network
- L3 PE
- CPE
- Enterprise

Legend:
- 🔴 L3 VPN
- 🟢 L2VPN/VPLS/L2Circuit
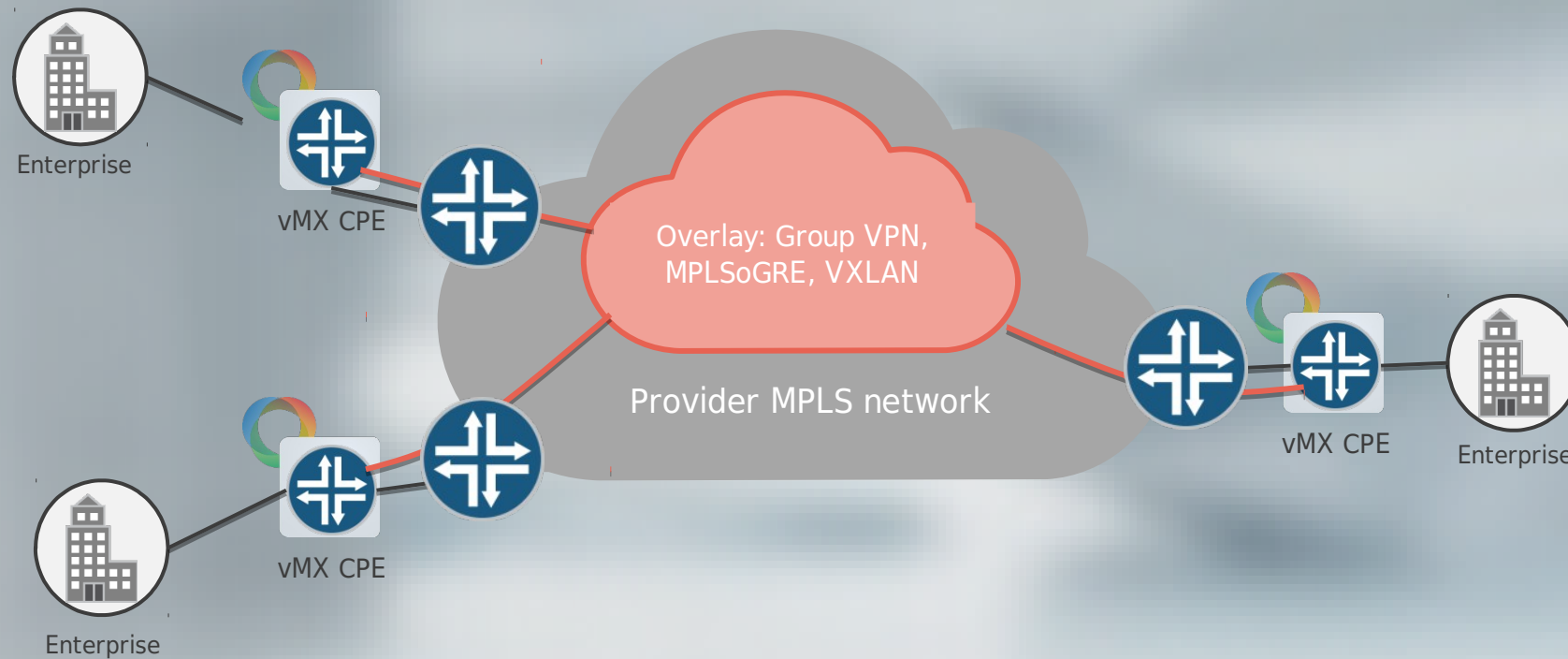
vMX Use-Case: Data Center Gateway

Use-case

- Service Providers need a gateway router to connect the virtual networks to the physical network
- Small hosting providers need a gateway route to connect to the internet
- Gateway should be capable of supporting different DC overlay, DC Interconnect and L2 technologies in the DC such as GRE, VXLAN, VPLS and EVPN

vMX value proposition

- VMX supports all the overlay, DCI and L2 technologies available on MX
- Scale-out control plane to scale up VRF instances and number of VPN routes

vMX Use-Case: Enterprise WAN Router

Overlay: Group VPN, MPLSoGRE, VXLAN

Provider MPLS network

Enterprise

vMX CPE

Enterprise

vMX CPE
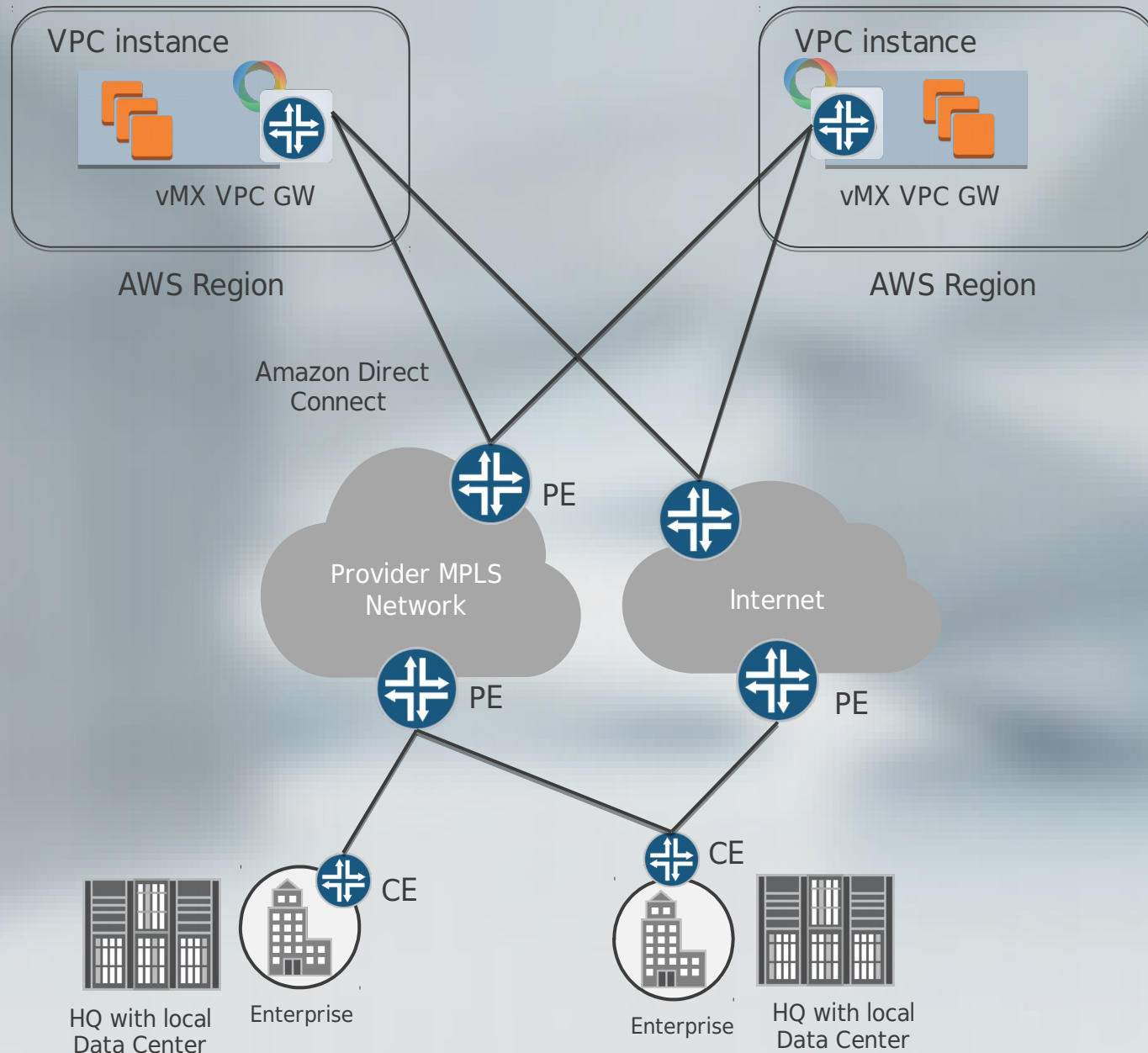
vMX CPE

Enterprise

Enterprise

Use-case

- Large Enterprises and Government institutions want to build their own overlay network over a Service Providers MPLS or Layer 2 network
- Transport for overlay network can be using encapsulation technologies such as MPLSoGRE, VXLAN and IPSec for secure transport

vMX value proposition

- vMX will offer IPSec VPNs using Group VPN technology for secure overlay transport
- All existing routing functionality available on vMX makes it a robust Enterprise WAN router

vMX Use-Case: Virtual Private Cloud Gateway

VPC instance

vMX VPC GW

AWS Region

VPC instance

vMX VPC GW

AWS Region

Amazon Direct Connect

PE

Provider MPLS Network

Internet

PE

PE

PE

CE

CE

HQ with local Data Center

Enterprise

Enterprise

HQ with local Data Center

Use-case

- Virtual Private Cloud (VPC) customers need a gateway router in the cloud to
    i. Route between subnets in a VPC instance
    ii. Route between VPC instances across geographies
    iii. Secure transport from a public or private network without scaling restrictions imposed by CSP
- Cloud Service Providers don't want to create specialized product offerings to meet these needs

vMX value proposition

- vMX as a VPC GW router can offer
    i. Ability for VPC customers to terminate IPSec tunnels with the scale & capacity they need
    ii. Create overlay topologies using IPSec and MPLS VPN technologies for Hybrid Cloud integration into the enterprise
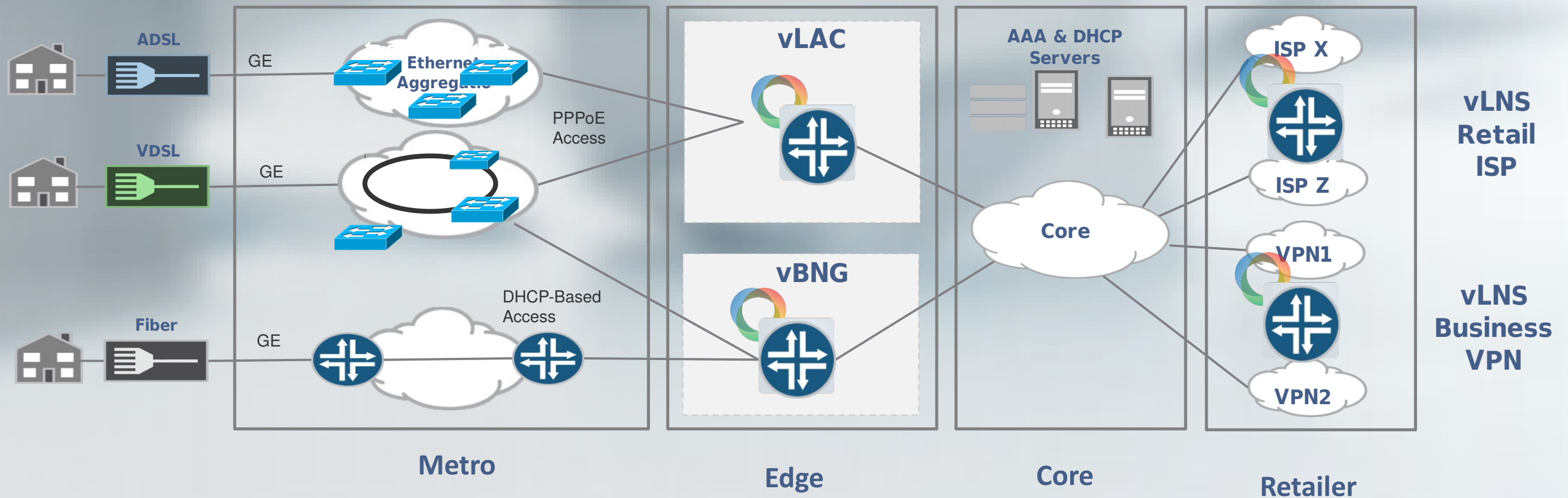
vMX Use-Case:Distributed vLNS & vBNG

Market Requirement

- vBNG and vLAC connect broadband subscribers via L2 from aggregation network, then assign IP and policies for L3 hand to the core or retail ISP
- vLNS deploys customized configurations for one or more retails ISPs or Business VPNs per instance

vMX + Porter Solution

- vBNG and vLAC allow just in time provisioning in small COs (<8K subscribers and <20 Gb/s) close to the access node
- vLNS deploys optimized instances for each Business VPN or Retail ISP with dynamic capacity management
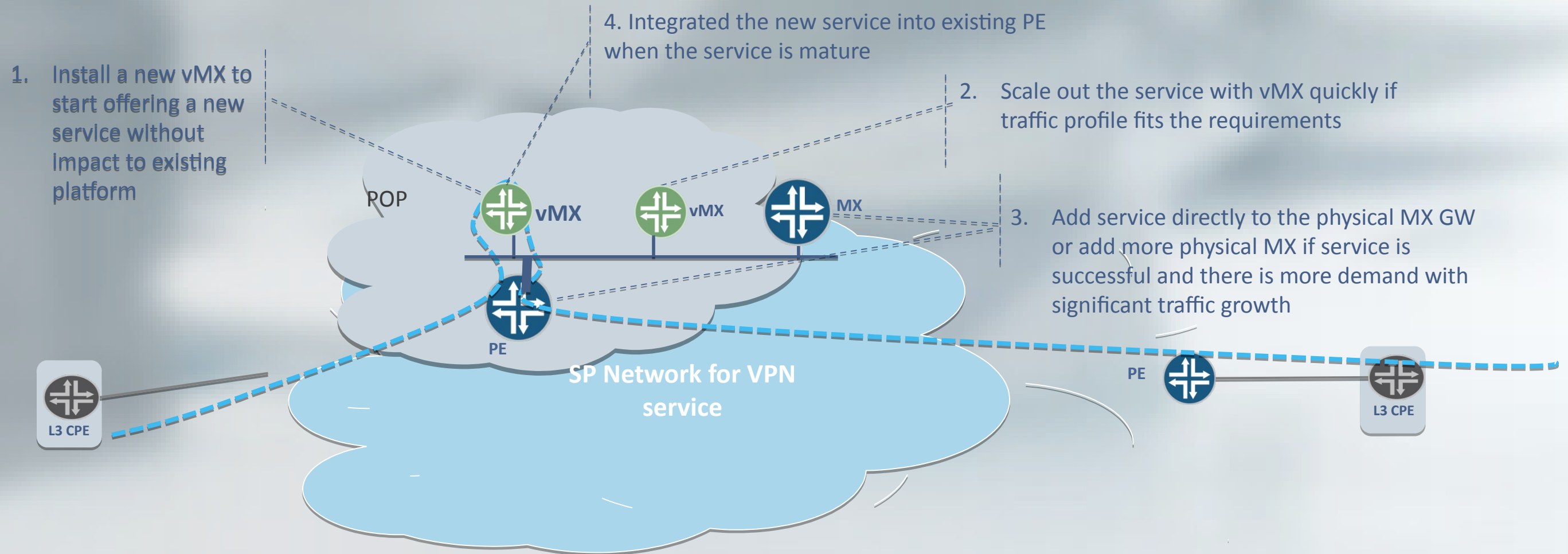

ADSL

VDSL

Fiber

GE

GE

GE

Ethernet Aggregate

PPPoE Access

DHCP-Based Access

vLAC

vBNG

AAA & DHCP Servers

Core

ISP X

ISP Z

VPN1

VPN2

vLNS Retail ISP

vLNS Business VPN

Metro

Edge

Core

Retailer

Reflection from physical to virtual world
Proof of concept lab validation or SW certification
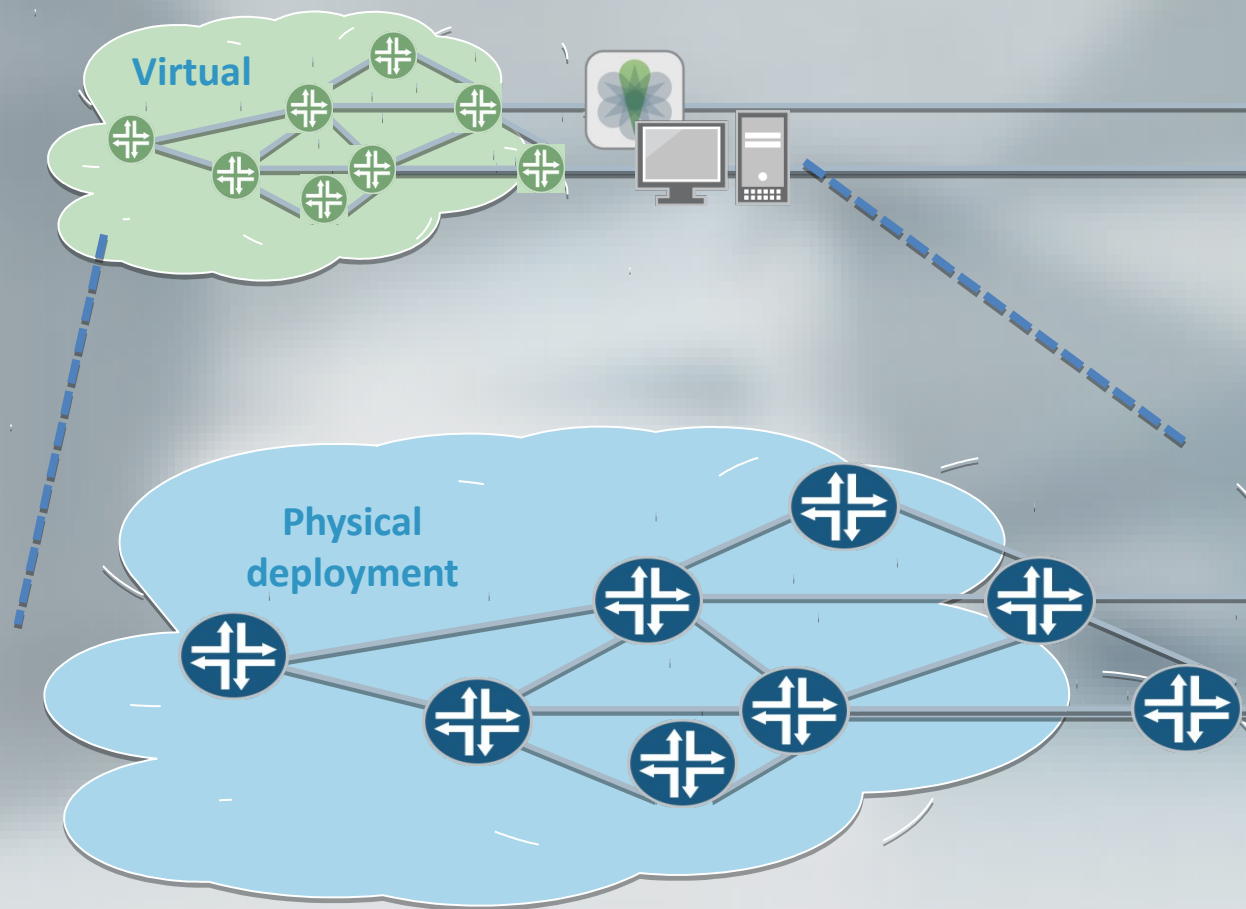
- Perfect mirroring effect between carrier grade physical platform & virtual router

- Can provide reflection effect of an actual deployment in virtual environment

- Ideal to support

  - Proof of Concept lab

  - New service configuration/operation preparation

  - SW release validation for an actual deployment

  - Training lab for operational team

  - Troubleshoot environment for a real network issue

- CAPEX or OPEX reduction for lab

- Quick turn around when lab network scale is required

Service Agility: Bring up a new service in a POP

4. Integrated the new service into existing PE when the service is mature

1. Install a new vMX to start offering a new service without impact to existing platform

2. Scale out the service with vMX quickly if traffic profile fits the requirements

3. Add service directly to the physical MX GW or add more physical MX if service is successful and there is more demand with significant traffic growth

POP

vMX

vMX

MX

PE

SP Network for VPN service

PE

L3 CPE

L3 CPE

Key takeways

- Virtualized technology: the gate to new revenue (new services, new locations, expanded footprint).

- non-Virtualized technology: the gate to scalability and efficiency.

- What is more sexy?
  - You need both.

- Benefits of virtualization are way beyond what it seems at first sight:
  - Flexibility, agility, lower entry barrier for new services and capabilities.

- Virtualization requires a transformation of the organization.

FINAL DISCLAIMER

- 1. We have discussed here about "**virtualization over x86**". Virtualization is a broader term with many other technical manifestations and applications.

- 2.Virtualization: **YES**. Juniper fully supports it and embraces it.

- 3. **Juniper portfolio** of Virtualized Network Functions **IS** the industry **BROADEST**:
  - vCPE, vPE, vBNG, vLNS, vRR, vCGNAT, vCDN, vFirewall, vIPS,vUTM, vRE, Contrail network virtualization, NFVO.

- 4. We believe it is important to **CAREFULLY** analyze **why, where and how** virtualization is used.
  - **It is a tool** and can be as positive as **harmful if not properly applied.**

- 5. The analysis must be done on the **SPECIFIC CONTEXT** of the customer.