Distributed Data Centers within the Juniper Networks Mobile Cloud Architecture

White Paper

June 2017

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

The information in this document is current as of the date on the title page.

Copyright © 2017, Juniper Networks, Inc. All rights reserved.

Contents

© 2017 Juniper Networks, Inc.

© 2017 Juniper Networks, Inc.

Executive Summary

This white paper covers distributed data centers, which is one solution area within the Juniper Networks Mobile Cloud Architecture. It includes:

- Challenges and trends that are driving the need for distributed data centers.
- Types and architectures of distributed data centers from micro data centers to large data centers with 10,000 or more devices.
- Products and services that Juniper offers to create distributed data centers, including underlay and overlay technologies.
- How to combine mobile and fixed networks in an enterprise use case.
- How Juniper has partnered with Saguna Networks to provide multi-access edge computing (MEC).
- The flexibility of Juniper Networks Cloud CPE architecture.
- How to use secure SD-WAN in your enterprise.
- Customer references and awards that Juniper has received, and a summary of the benefits of using Juniper Networks products in distributed data centers.
- An overview of the five solutions areas of the Juniper Networks Mobile Cloud Architecture.

The content in this white paper is also available in PPT (blueprint) and video formats at Network Design and Architecture Center: Mobile Cloud.

Challenges and Trends

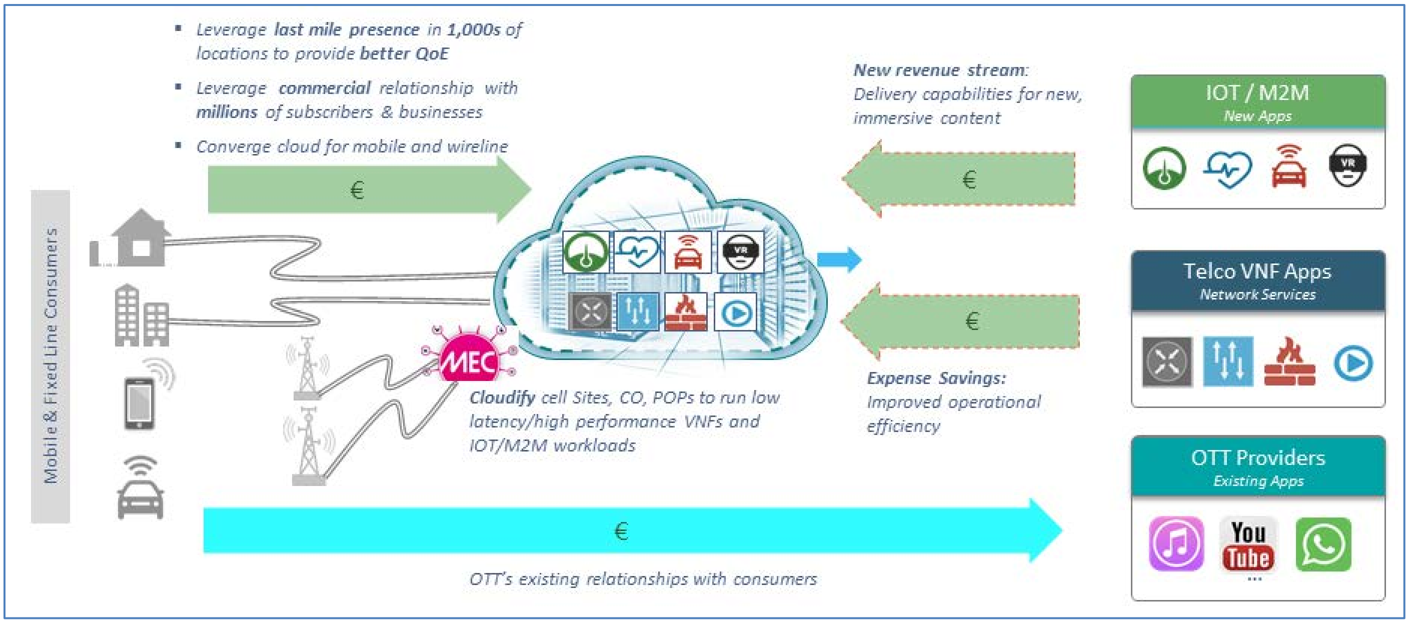
This section covers the challenges and trends in the distributed data center market.

Challenge: Monetize Assets with Distributed Data Centers

One of the main challenges that service providers face is how to monetize their assets. One way for them to do that is to move computing of traffic closer to the edge of the network. Moving computing for services closer to the edge is called multi-access edge computing (MEC).

Service providers need to create the same types of service offerings that are currently running in the cloud, and move them closer to the edge of the network. Applications at the edge require high bandwidth and fast latency, and service providers can achieve that by creating distributed data centers. Service provider locations are already perfectly suited for this technology.

© 2017 Juniper Networks, Inc.



- Leverage **last mile presence** in **1,000s** of locations to provide **better QoE**
- Leverage **commercial** relationship with **millions** of subscribers & businesses
- Converge cloud for mobile and wireline

New revenue stream: Delivery capabilities for new, immersive content

Cloudify cell Sites, CO, POPs to run low latency/high performance VNFs and IOT/M2M workloads

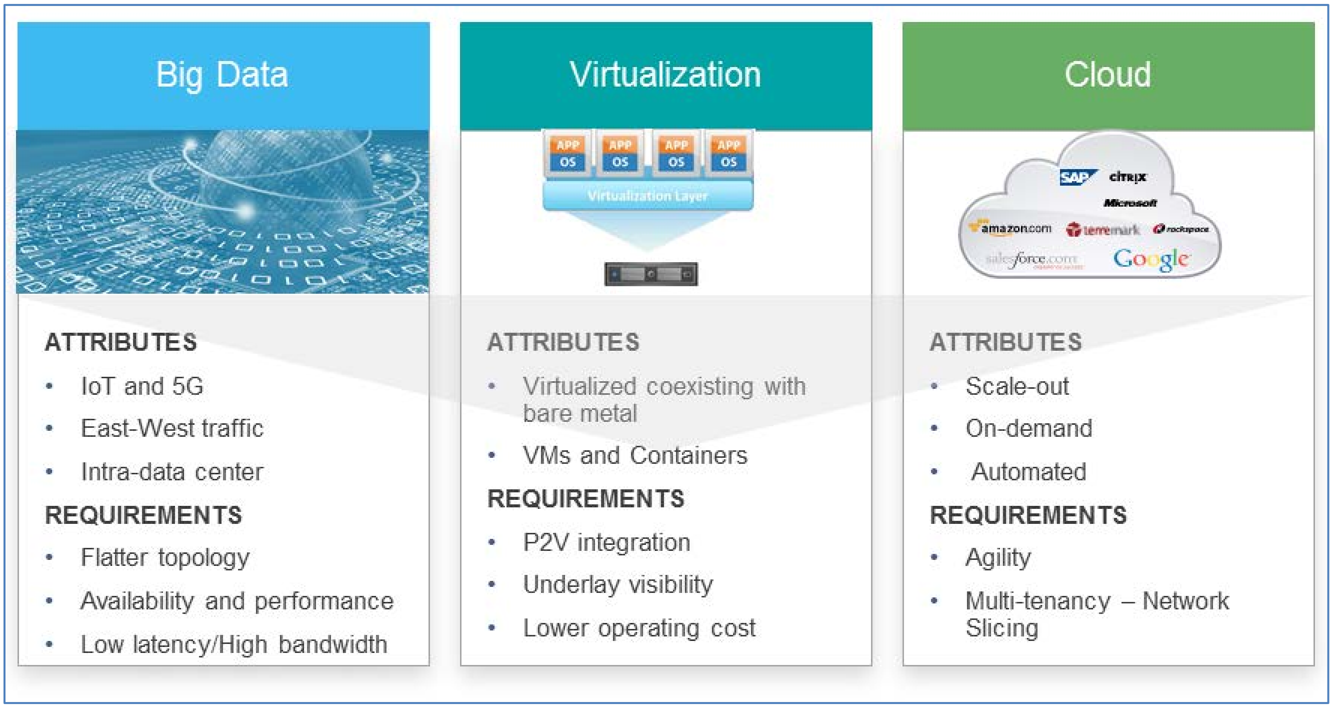
Expense Savings: Improved operational efficiency

OTT's existing relationships with consumers

Figure 1 : Monetizing Assets with Distributed Data Centers

Trends Driving Distributed Data Centers

At Juniper Networks, we are seeing the following trends that are driving the need for distributed data centers:



Big Data

ATTRIBUTES
- IoT and 5G
- East-West traffic
- Intra-data center

REQUIREMENTS
- Flatter topology
- Availability and performance
- Low latency/High bandwidth

Virtualization

ATTRIBUTES
- Virtualized coexisting with bare metal
- VMs and Containers

REQUIREMENTS
- P2V integration
- Underlay visibility
- Lower operating cost

Cloud

ATTRIBUTES
- Scale-out
- On-demand
- Automated

REQUIREMENTS
- Agility
- Multi-tenancy – Network Slicing

Figure 2 : Trends Driving Distributed Data Centers

© 2017 Juniper Networks, Inc.

Big Data

With the Internet of things (IoT) and more equipment being connected to networks in general, there are large amounts of data being generated. The information collected will only increase as more things are connected to networks.

Instead of this traffic going to a data center in the cloud, much of this data needs to travel across the network in an east-west fashion. This means that data can be processed at the edge of the network, and only certain types of information need to go to cloud data centers. This trend leads to requirements of high bandwidth, low latency, better availability, and flatter topologies than we see today.

Virtualization

Virtualization is replacing the trend of running applications on bare metal servers. Virtualization lowers costs by sharing compute resources for several purposes instead of using a single server or network application for each function.

Juniper Networks has the products that can virtualize the network and extend the physical network seamlessly to the virtual network. In this paper, we will cover the underlay network that uses Juniper Networks switching and routing infrastructure that compute nodes run on, and that host the virtual machines and containers that Juniper Contrail controls.

Cloud

With the cloud, we have the ability to scale out virtual machines to meet any need. Instead of adding hardware to scale out and then scaling it back when you do not need as many resources or capacity, you can use virtual machines. You no longer need to place orders for new equipment and wait, perhaps weeks, for it to arrive. You can automate the process of scaling in and scaling out your network with virtual machines.

Automation and Juniper Contrail solution allows for a multi-tenancy within cloud environments. You can slice the network and then provide those slices with the security that Juniper offers, on top of the agility to order on-demand services to scale in and scale out as needed.

Summary

Juniper Networks can meet the demands of big data, virtualization, and distributed or centralized cloud. Juniper Networks pulls them together to create the networks of today and tomorrow.

Distributed Data Center Architectures

Figure 3 shows Juniper Networks distributed data center architectures. These are the underlay network architectures, and start from a cloud CPE device (NFX Series) on the left to larger and larger data centers up to a data center with 10,000 or more devices on the right. Juniper Networks portfolio covers all of these architectures from our NFX Series platform that can run as a router, switch, and server up to the EX Series or QFX Series with 1-GbE and 10-GbE ports, and then up to QFX10000s with its 100-GbE ports.

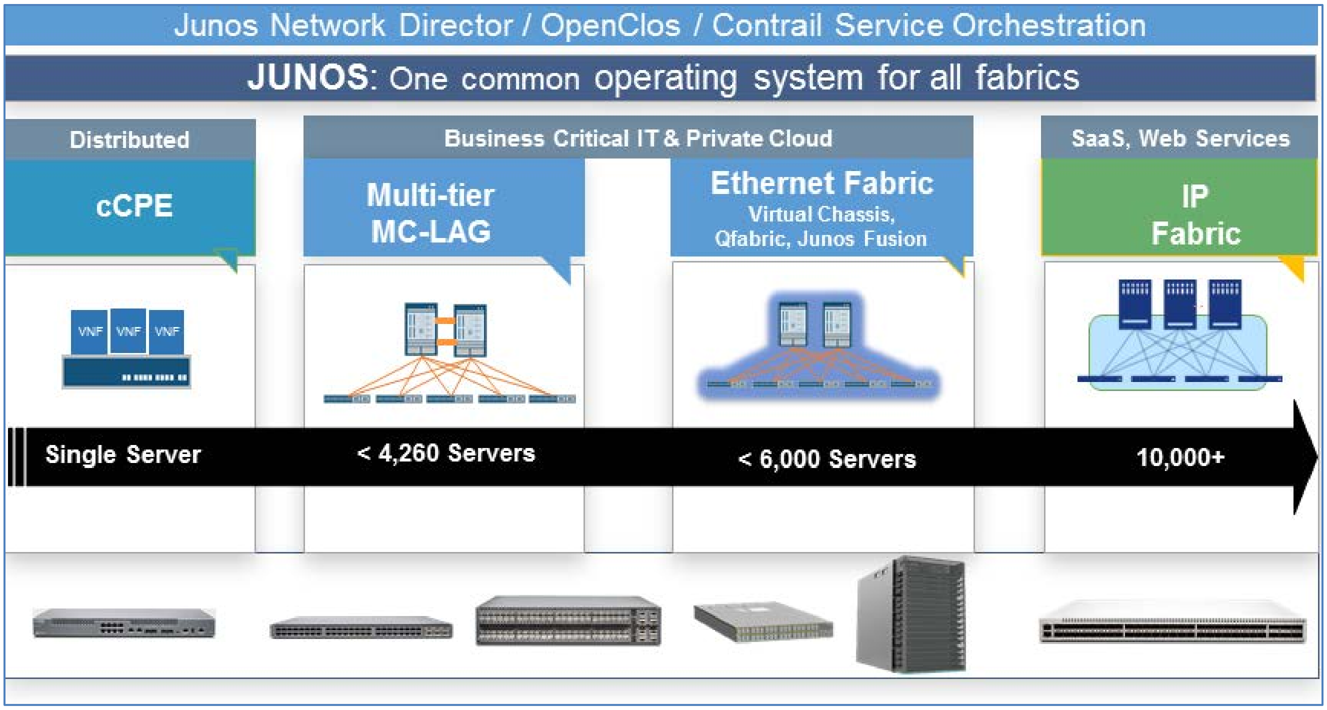

Junos Network Director / OpenClos / Contrail Service Orchestration
JUNOS: One common operating system for all fabrics
Distributed
cCPE
Business Critical IT & Private Cloud
Multi-tier MC-LAG
Ethernet Fabric
Virtual Chassis, Qfabric, Junos Fusion
SaaS, Web Services
IP Fabric
VNF
VNF
VNF
Single Server
< 4,260 Servers
< 6,000 Servers
10,000+

Figure 3 : Overview of Distributed Data Center Architectures

The types of data center architectures include:

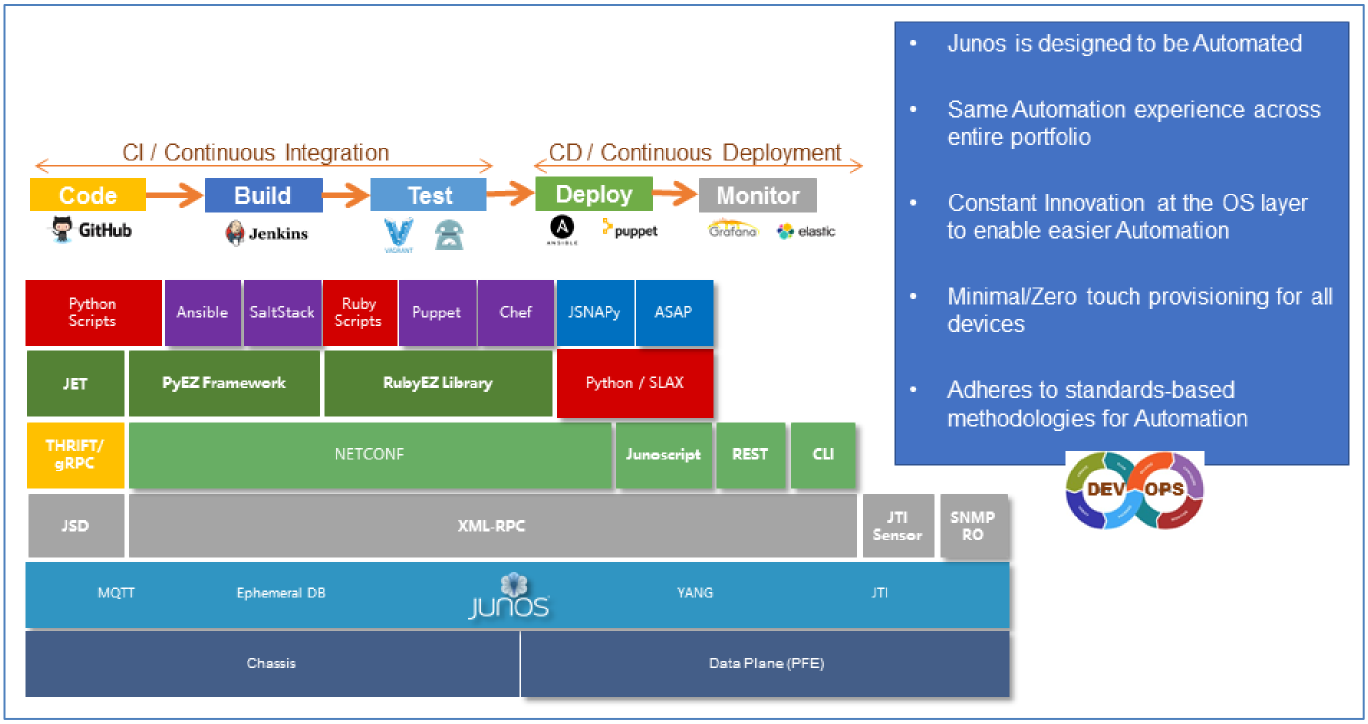
- **Distributed Cloud CPE.** This is a micro data center with a single server that is located at a customer site.
- **Multi-Tier, Multi-Chassis-Link Aggregation (MC-LAG).** As your edge network gets larger and your data centers grow, you can use MC-LAG to aggregate your links so that none of your links are wasted.
- **Ethernet Fabric.** As we move into larger, more cohesive data centers, Ethernet fabric provides a way of managing all of your devices as one.
- **IP Fabric.** As data centers become very large, and cloud providers are running software-as-a-service and Web services, you would typically use IP fabric to manage your site.

The following sections cover each of the data center architectures in more detail.

At the top of our data center architecture in Figure 3 is Junos Network Director, OpenClos, Contrail, and Contrail Service Orchestration to provide true automation, as well as the orchestration and monitoring of services that are running in these data centers.

Next is our one JUNOS operating system, which allows you to take advantage of the programmability of JUNOS. If you need to configure an NFX 250 or a QFX 10000, the same API calls in the same code can configure and monitor these devices. Figure 4 shows the Junos automation stack with its standards-based programmability.

© 2017 Juniper Networks, Inc.

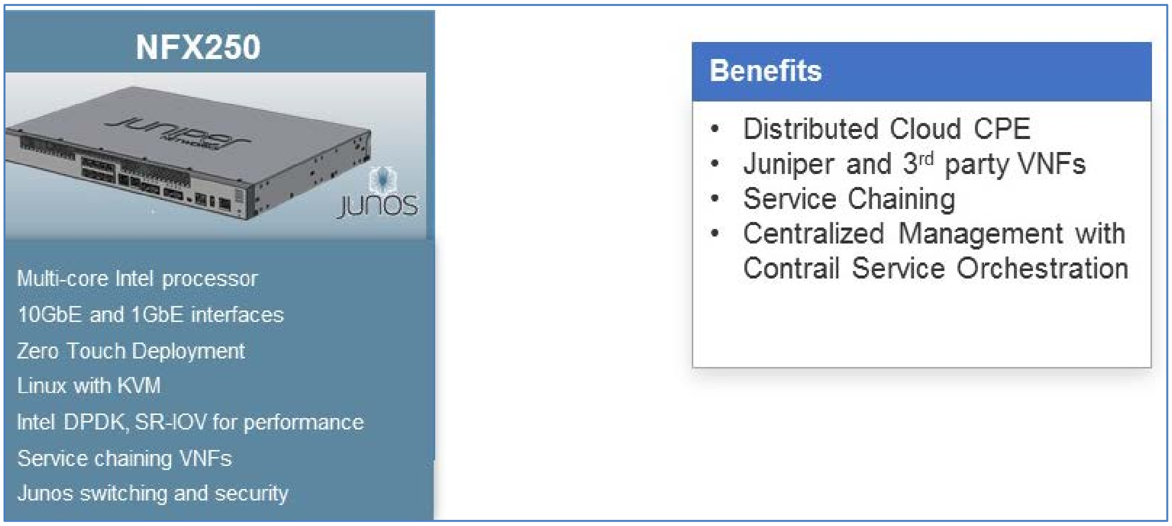


- Junos is designed to be Automated
- Same Automation experience across entire portfolio
- Constant Innovation at the OS layer to enable easier Automation
- Minimal/Zero touch provisioning for all devices
- Adheres to standards-based methodologies for Automation

Figure 4 : Junos Automation Stack with Standards-Based On-Box Programmability

Distributed Micro Data Center

Figure 5 shows the first data center type:



Multi-core Intel processor
10GbE and 1GbE interfaces
Zero Touch Deployment
Linux with KVM
Intel DPDK, SR-IOV for performance
Service chaining VNFs
Junos switching and security

Benefits

- Distributed Cloud CPE
- Juniper and 3rd party VNFs
- Service Chaining
- Centralized Management with Contrail Service Orchestration

Figure 5 : Distributed Micro Data Center with the NFX 250 Network Services Platform

A distributed micro data center has virtual network functions (VNFs), which are virtual machines (VMs), running on a server that could be Juniper Networks NFX 250 distributed cloud CPE platform, or it could be an x86 box. This data center type provides computing power where it is needed, which could be at a branch office or on a Radio Access Network (RAN). Wherever computing power is needed on the network, you can run VMs.

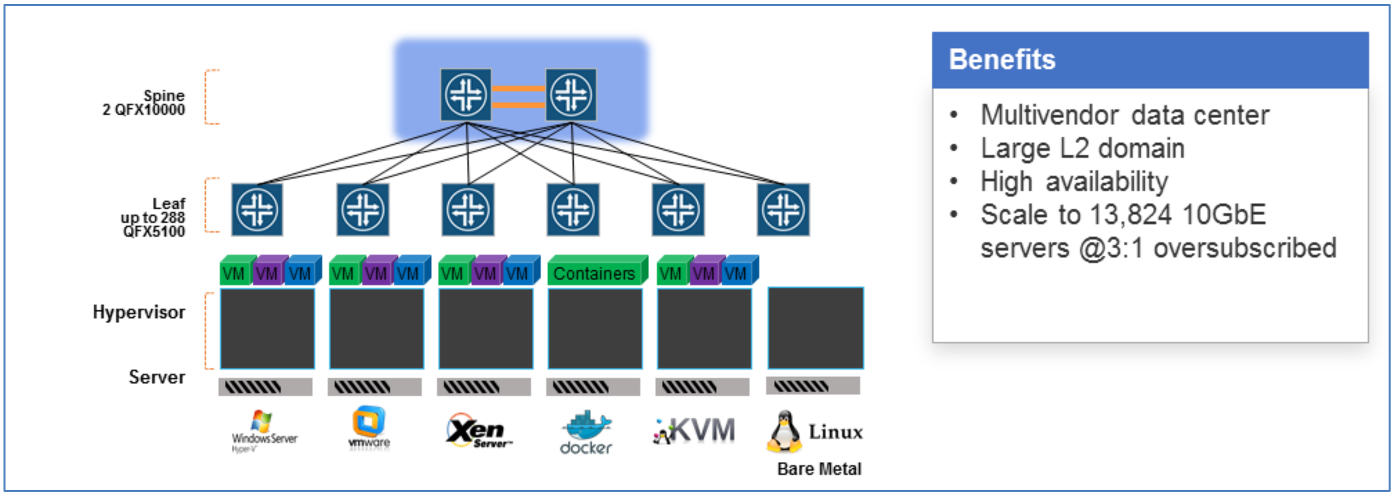
© 2017 Juniper Networks, Inc.

The NFX 250 features include:

- Gigabit Ethernet LAN ports and 10GbE WAN ports
- Full zero-touch provisioning
- Linux as the host operating system, with the Kernel-based Virtual Machine (KVM) hypervisor to host VNFs from Juniper or from third parties. Third party VNFs are needed because Juniper does not make all network functions. For features such as WAN optimization, Juniper relies on partners to supply those VNFs. Juniper supports an open ecosystem where third-party products work seamlessly with our VNFs to provide agility and choice to customers.
- Support for the Data Plane Development Kit (DPDK) from Intel and single root input/output virtualization (SR-IOV) for performance
- Support for creation of service chains of your VNFs. If you need deep packet inspection and a firewall, instead of having multiple hardware devices, you simply run them as the VMs on the NFX platform. Service chaining makes sure that the data path goes through all the VNFs in the proper order, and that the return path works the same way.
- Centralized management using Contrail Service Orchestration

Multi-Tier MC-LAG Data Center

Figure 6 shows the multi-tier MC-LAG data center design, which is used in large Layer 2 domains. If a switch is supplying multiple connections to servers, you want to use all of the links so that you do not waste bandwidth or waste utilization of circuits in your data center.



Benefits

- Multivendor data center
- Large L2 domain
- High availability
- Scale to 13,824 10GbE servers @3:1 oversubscribed

Figure 6 : Multi-Tier MC-LAG with QFX10000s and QFX5100s

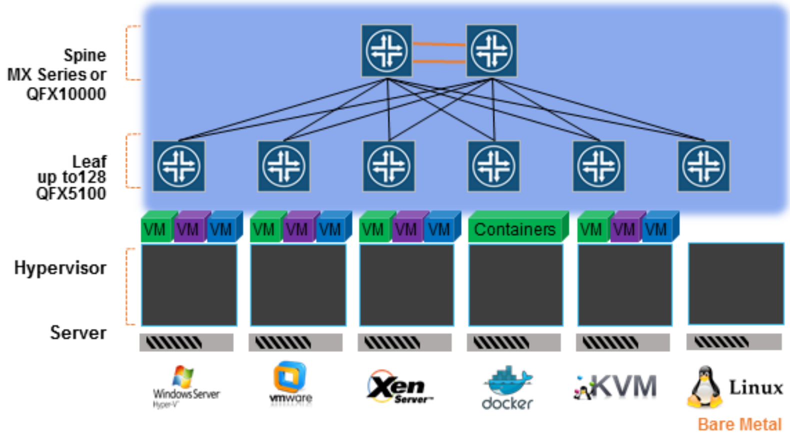
This design uses a spine and leaf architecture. In the spine are two QFX10000s that can appear to be a single node. In the leaf are QFX5100s. With MC-LAG, the QFX10000s can send traffic across any of the links, without the need for a Spanning Tree protocol. Spanning Tree would turn off certain links, and you would not be taking full advantage of link utilization.

This MC-LAG topology can scale to 13,000 10-GbE ports plus oversubscription. You need to consider what your VMs require to determine what your own oversubscription would be.

© 2017 Juniper Networks, Inc.

Ethernet Fabric Data Center

In the next architectures, we are moving away from Layer 2 domains because of the policy capabilities of IP routing at Layer 3. The Ethernet fabric, shown in Figure 7, uses both Layer 2 and Layer 3.



Virtual Chassis Fabric Benefits:

- Single point of management
- Mixed 1GbE/10GbE/40GbE
- Scale up to 28 leaf nodes
- Overlay Support

Qfabric Benefits

- Single point of management
- 10GbE and 40GbE optimized
- Scale up to 128 member switches
- Performance at scale
- Broad customer base

Junos Fusion Benefits

- Plug-and-play provisioning
- Multi-version support
- Open Standards & programmability
  - IEEE 802.1BR and JSON-RPC APIs
- 1GbE/10GbE/40GbE/100GbE
- Scale up to 128 leaf switches

Figure 7 : Layer 2 and Layer 3 Ethernet Fabric

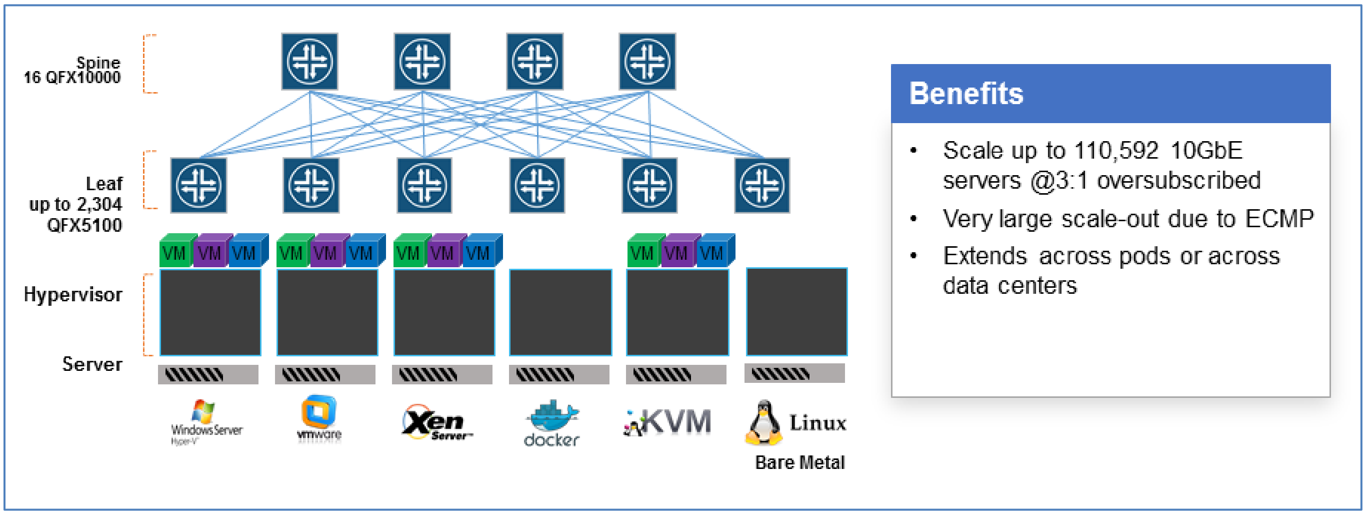
The Ethernet fabric architecture scales to about 6,000 devices. It uses a spine-and-leaf architecture, where the spines control the leaf nodes as well as each port from the leafs to the servers. You can use a mix of EX Series switches or QFX Series switches at the leafs to support 1-GbE, 10-GbE, or 40-GbE links.

To manage the Ethernet fabric, you can use a virtual chassis or a Q Fabric, where all devices look as one. From JunosSpace Network Director, the spine appears as one large switch that can have up to 128 leafs coming off it. Alternatively, you can use Junos Fusion to manage many devices from a single platform.

The QFabric can scale to 128 member switches that support open standards of programmability for automation. You can use the Junos Snapshot Administrator (JSNAP) automation tool to test the entire fabric to see how many ports are up and what MAC addresses are on those ports for inventory control. By automating testing, you can check and monitor your environment much easier on Junos platforms than on any other vendor on the market. Juniper Professional Services can assist in the automation of your data center.

IP Fabric Data Center Architecture

Figure 8 shows the IP fabric architecture. It scales to over 10,000 devices, and we see it used in large, hyperscale data centers. This architecture uses Equal-Cost Multipath (ECMP) as the routing protocol between the spines and leafs, so that all spine devices know about all leaf devices.



Benefits

- Scale up to 110,592 10GbE servers @3:1 oversubscribed
- Very large scale-out due to ECMP
- Extends across pods or across data centers

Figure 8 : IP Fabric Data Center Architecture

With IP fabric, you can run policies and get all the benefits of IP routing protocols that you cannot get with just switching technologies.

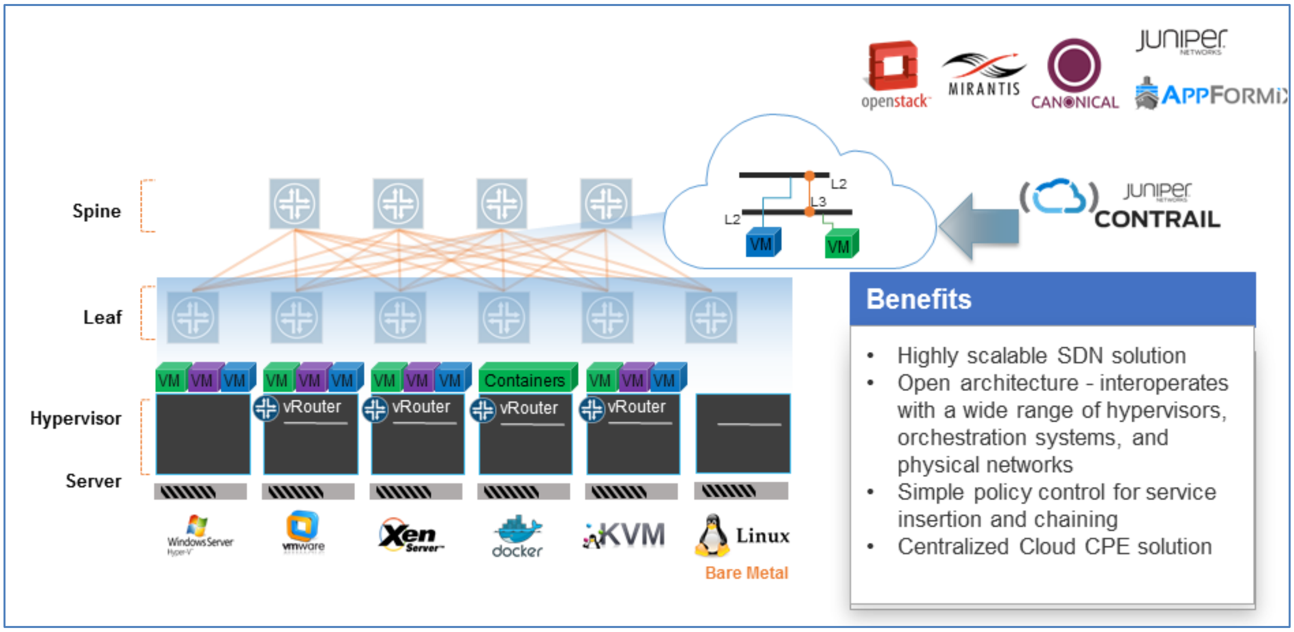
Similar to MC-LAG, traffic can go across multiple links. With the ECMP methodology, traffic is split by hashing the flow of packets that are coming from VMs running on bare metal servers. This traffic can go either up the network or across the network to other VM servers that run in the same data center. You can scale to over 110,000 10-GbE ports with up to a 3:1 over subscription.

We are seeing data centers that are this large in production today. Even with the size of this data center, you can still use a single management entity, such as JunosSpace Network Director and Contrail, to manage the data center.

Overlay Networking with the Contrail SDN Platform

The previous sections covered our underlay network infrastructure, and now we will cover the overlay network infrastructure, which is shown in Figure 9. Once the spine and leaf network underlays are built, we can introduce a Contrail SDN platform that is used as our overlay for Contrail networking.

© 2017 Juniper Networks, Inc.



Benefits

- Highly scalable SDN solution
- Open architecture - interoperates with a wide range of hypervisors, orchestration systems, and physical networks
- Simple policy control for service insertion and chaining
- Centralized Cloud CPE solution

Figure 9 : Overlay Networking with the Contrail SDN Platform

The SDN controller takes the VMs in the servers and extends the virtual network between servers, or stretches the virtual network outside the scope of a server. The servers have tunnels between then. For example, in Figure 9 a purple VM can communicate with another purple VM even though they are on different servers. The Contrail networking component makes that connection seamless. In the cloud diagram in our figure, there is a blue VM and a green VM. In order for these VMs to communicate, they need a policy that links them. When a policy links them, we have services, such as firewalls, in a truly micro-segmented network versus having each host prone to cross talk between networks.

This Contrail architecture eliminates the need for VLANs. Once your data center infrastructure is set up, you simply put the Contrail virtual router on servers. The virtual router can do the network slicing and the multi-tenancy needed to support networks of today and the future.

Connecting the Physical and Virtual Worlds

To connect our data centers to the outside world, we need an SDN gateway router, such as the MX Series 3D Universal Edge router. The SDN gateway routers translate between the virtual environment and the outside world, and they communicate with each other over a WAN or the Internet to connect seamlessly with cloud providers.

© 2017 Juniper Networks, Inc.

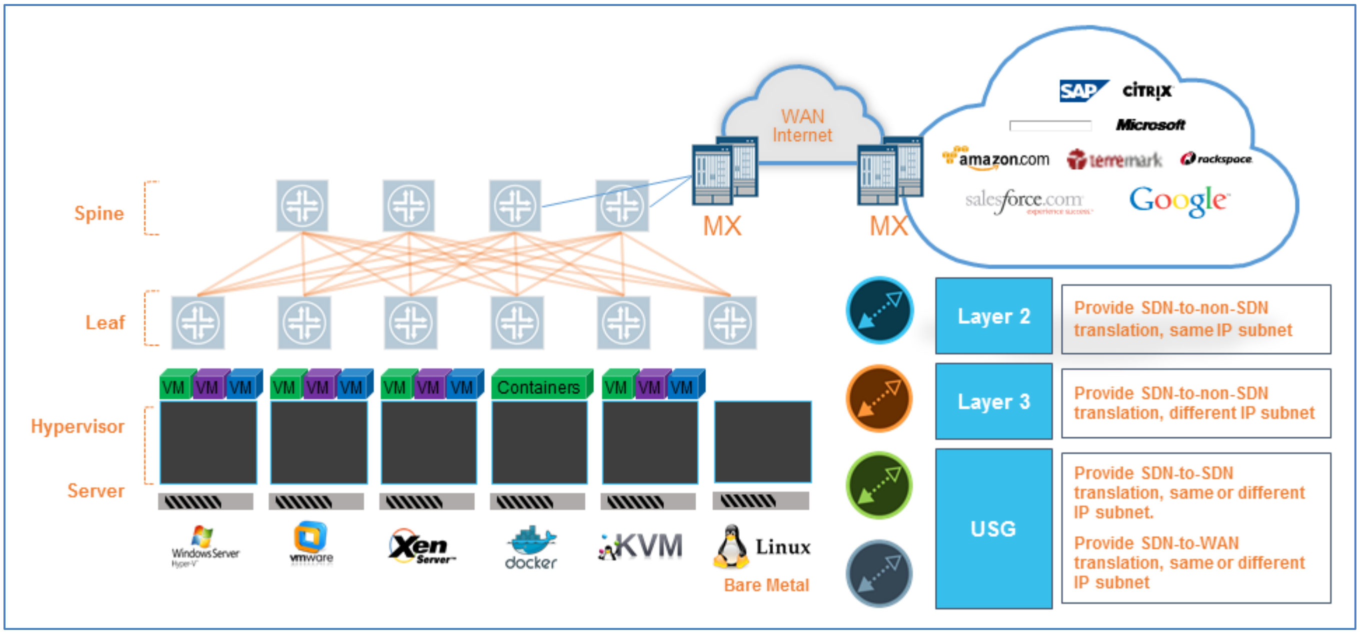

WAN
Internet
SAP
CITRIX
Microsoft
amazon.com
terremark
rackspace
salesforce.com
Google
Spine
MX
MX
Leaf
Layer 2
Provide SDN-to-non-SDN translation, same IP subnet
Layer 3
Provide SDN-to-non-SDN translation, different IP subnet
USG
Provide SDN-to-SDN translation, same or different IP subnet.
Provide SDN-to-WAN translation, same or different IP subnet
Hypervisor
Server
VM
Containers
Windows Server
vmware
Xen Server
docker
KVM
Linux
Bare Metal

Figure 10: Connecting the Physical and Virtual Worlds

Between the virtual Contrail environment and the SDN gateway routers, we use standard routing protocols so that there is a seamless architecture between the physical and virtual networks. This architecture is easy to implement, scales, and connects Layer 2 networks, Layer 3 networks, and it connects clouds.

Juniper has the products from the switching infrastructure, to the virtual networking on the servers, to the SDN gateways, to the data center interconnections needed to build scalable distributed data centers.

Enterprise Solution Architecture Use Case

In the past, mobile and the fixed wireline networks were kept separate. They were each built on their own, and were running as ships passing in the night. Figure 11 is an example of what is possible when we combine the mobile and fixed worlds.

© 2017 Juniper Networks, Inc.

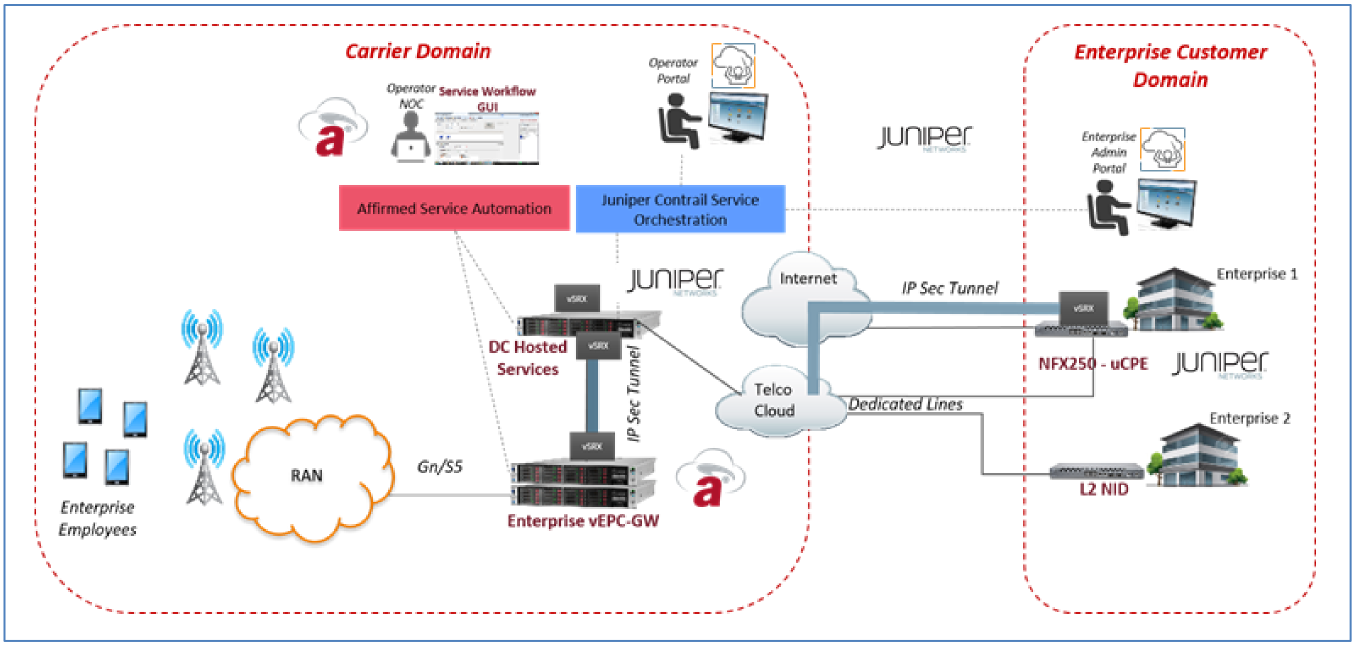


Figure 11: Enterprise Solution Architecture

In this section, we show how to use the virtual Evolved Packet Core gateway (vEPC-GW), provided by Affirmed Networks, and connected to the RAN to identify specific employees in an enterprise.

The enterprise users can be assigned either an access point name, which specifies the point where a mobile device can access an IP network, or an IP address pool that has policies on it. If traffic from these users needs to get to an enterprise site, whether that site is a branch or headquarters, we use policies with the virtual SRX Series Services Gateways to create IPsec tunnels. The IPsec tunnels secure traffic from mobile subscribers to the enterprise.

The enterprise can use either Layer 2 or Layer 3 to bring traffic from the Internet directly into the Telco cloud or the service provider cloud. This means that mobile users and Layer 2 or Layer 3 facilities that are connected to the Internet or directly connected to the service provider can all be managed as one enterprise.

Mobile users do not need to install VPN software. When there is machine-to-machine communication, the network identifies mobile users and uses policy-based routing to steer their traffic into the Enterprise VPN. It can then add the traffic to the Enterprise VPN so that machine-to-machine communications can be processed.

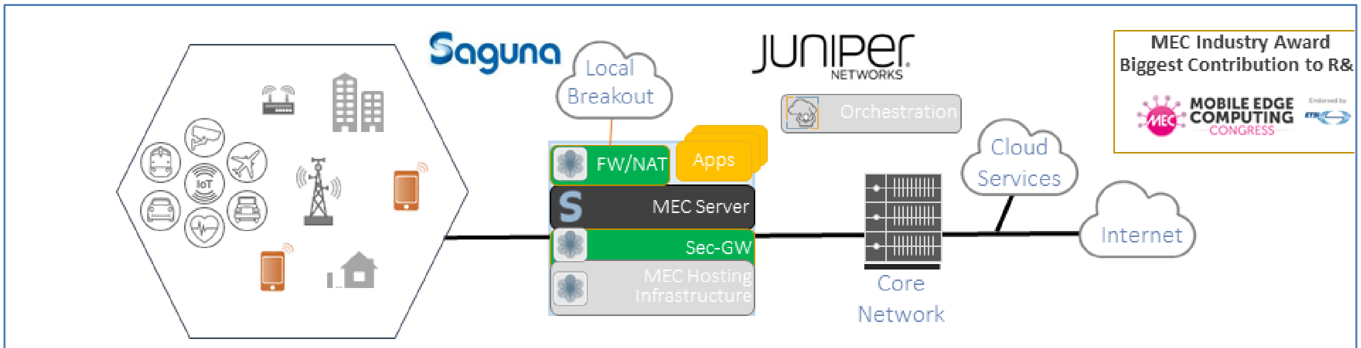
This is accomplished by distributing the data center out to where the EPC and virtual EPC are and creating secure tunnels into the Enterprise VPN. You can distribute small, medium, or large data centers across the network, and use the same architecture to turn up virtual machines to scale out applications, such as vEPC components, during congestion.

There can also be communication between millions of endpoints that will be on RANs, on wireline networks, or on Wi-Fi networks. You can use open protocols and standards that are agnostic of how endpoints connect into the network, but use the same technologies, such as IPsec.

Juniper Enables the Service-Aware RAN

Juniper Networks has partnered with Saguna Networks to provide multi-access edge computing (MEC), as shown in Figure 12.

© 2017 Juniper Networks, Inc.



Value proposition	Characteristics		Use Cases		
Improved user experience	Cloud computing and IT service environment at the edge		Local content cache	Compute offload for AR, Cognitive assistance	Edge Security
Better use of network resources	Reduced latency	High bandwidth	IOT Analytics and Security	Device location tracking	Location-based content and applications
New network monetization opportunities	Real-time radio network information	Location awareness	Mobile Throughput Guidance for video delivery optimization	RAN optimization for video	V2V, V2I

Figure 12: Service-Aware RAN

Here is an example of being service-aware within the RAN. The general packet radio service (GPRS) Tunneling protocol (GTP) traffic, which is encapsulated, must be de-encapsulated. To make traffic secure, we use a security gateway (Sec-GW). We use the MEC hosting infrastructure to offload processing or for content delivery. A good example is a download of an update on a phone. You can have the download a very short distance from the consumer of the content. This is where the benefits of distributed data centers come in. Our objective is to improve the user experience. We can do that by keeping content local to the user, instead of in a data center that can be hundreds or thousands of miles away.

While there needs to be a fast turnaround on data, you cannot store all of your data at the edge. Collected data needs to be processed locally, and then just required data can be sent to cloud. An IoT example, is if a user is constantly taking sensor readings of railroad tracks. Most of those readings will be the same, and do not need to be sent to the cloud. The readings need to be processed locally, and only changes in readings need to be sent to the cloud. There are many examples like this, where IoT applications require immediate communication, and as time goes on, more applications of this type will be developed creating a truly connected world.

Our goal is a better use of network resources. Obviously, if traffic is not sent to the core of the network, that will save bandwidth in the core. The key is to use distributed data centers at the edge. Juniper has the solutions with our partners to supply distributed data centers that are required in the network going forward.

Another goal is to monetize the network. Service providers need to recover the money spent to create and support these distributed data centers. They need a way to drive revenues to pay for them and to add services that customers are requesting.

Cloud CPE Architecture

Figure 13 shows the Juniper Networks Cloud CPE architecture.

© 2017 Juniper Networks, Inc.

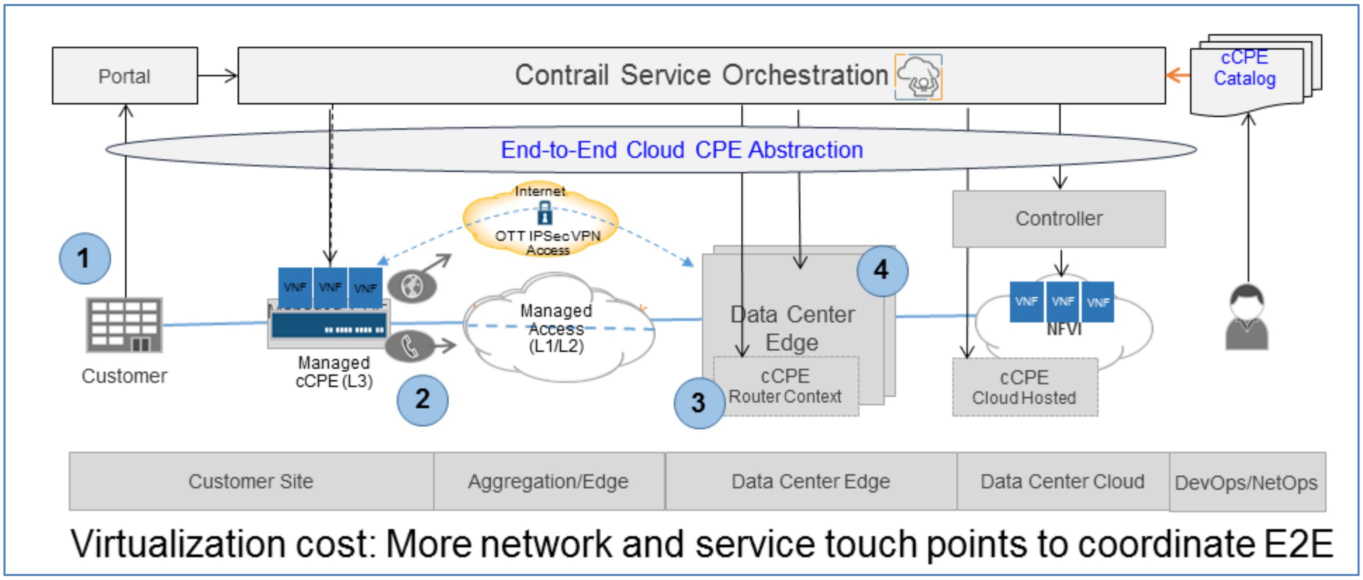


Figure 13 : Cloud CPE with Contrail Service Orchestration

Here is an example of how flexible this architecture is:

1. To start, there is a customer portal that is communicating with Contrail Service Orchestration.

   Contrail Service Orchestration is controlling not only the VMs that are running within distributed clouds, but it is also communicating with SRX Series devices and third-party devices on the network, such as a managed cCPE and DCE.

2. There are two links from the managed cloud CPE. One is an over-the-top (OTT) Internet access, and the other is a managed access link, which is a secure, managed line on the service provider's MPLS access network. Traffic is split across these links in what is known as software defined wide area networks (SD-WANs).

3. In our illustration, there is a Layer 3 cCPE that is also running VMs. We might need the following VMs:

   - Local VMs to run deep packet inspection.
   - Virtual SRXs that can interface with Juniper Networks Sky ATP platform to do localized malware protection.
   - Firewall and NAT.
   - Policies that can track Layer 7 applications, and decide which traffic can use the OTT links, and which traffic should use the managed access link. Normal Internet traffic can go over the OTT link, but voice and other important traffic needs to go over the managed link.

4. At the data center edge, we want to supply other services that may run at the customer site. These can be value-added services, such as VMs, for backup services or other types of sophisticated protection or business applications. You can put these services in a private cloud, but also make them accessible to customers or your end sites. Instead of installing hardware for these services, you can use VNFs.

As an alternative to the customer building in the figure, you could have the Gi-LAN side of the RAN or the virtual EPC or the EPC that the mobile world is accustomed to.

© 2017 Juniper Networks, Inc.

Secured SD-WAN Infrastructure

Figure 14 shows a secured SD-WAN infrastructure.

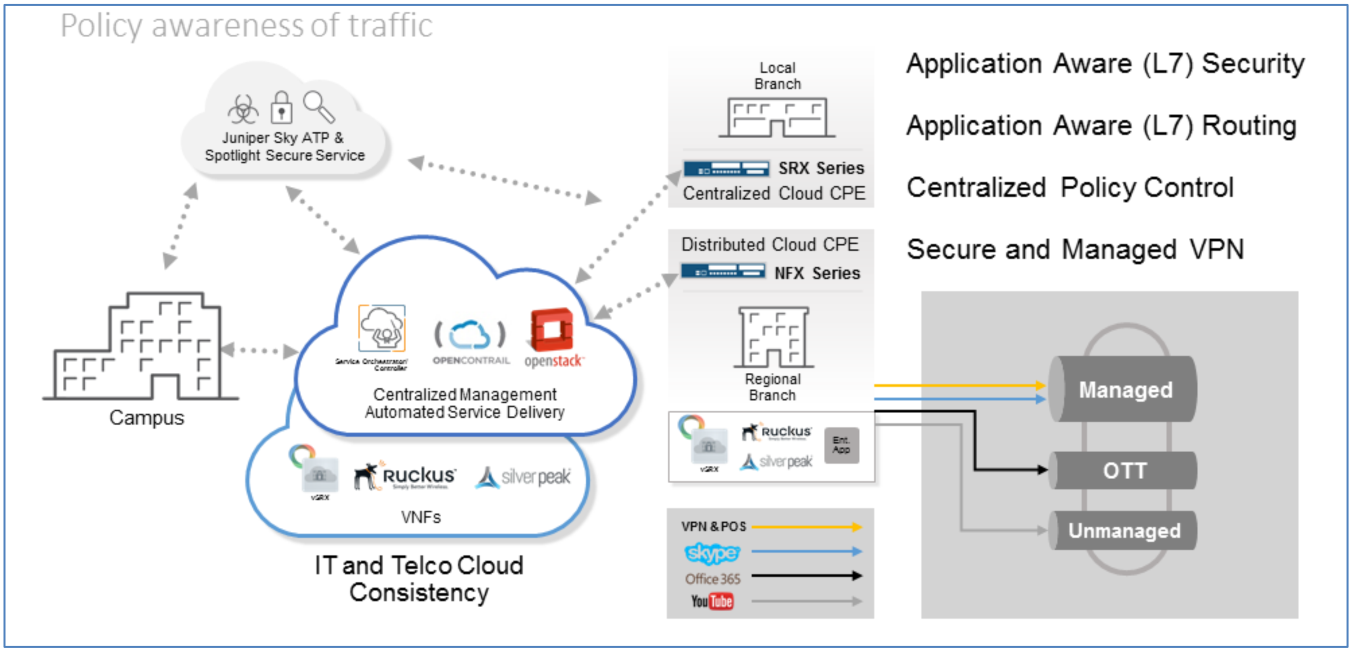


Figure 14: Secured SD-WAN Infrastructure

With Juniper Networks SD-WAN feature, we do not want to secure the network, we want to build secure networks. To do so, we want to put security everywhere, such as at the local branches, or within the network. Figure 14 shows just a couple of examples where we have our SRX Series with a centralized Cloud CPE at the branch and our distributed Cloud CPE on the NFX Series at the regional office.

With our SRX or virtual SRX Series that can run as a VM on the NFX250 Series, the AppSecure feature set tracks and applies security to Layer 7. AppSecure is a suite of application security capabilities for the SRX Series that identifies applications for greater visibility, enforcement, control, and protection of the network. AppSecure understands application behaviors and vulnerabilities, and it can prevent application-borne security threats that are difficult to detect and stop.

The right side of the illustration has three types of links: Managed, OTT, and Unmanaged. The managed link would probably be an MPLS circuit, and you could use it for voice traffic with Skype, VPN access, and other types of important traffic. Office 365 traffic could go over the OTT link, but through a tunnel, so that there is a defined path that you can secure. Other traffic, such as YouTube or general Internet traffic could go over the unmanaged link.

Once the network is application aware, you can decide which applications you want to send over which link. To do this, you can use centralized policy control, security, and managed VPN services.

For traffic that comes from the RAN across the Gi-LAN, you can also make choices on what traffic you want to put where. All based Juniper Networks cloud-based services, such as AppSecure, Sky Advanced Threat Prevention (ATP), and the Spotlight Secure Threat Intelligence platform. The SRX Series—virtual SRX as well as physical SRX— can use these cloud services to protect your network against malware and other threats beyond basic firewall security threats.

© 2017 Juniper Networks, Inc.

Juniper Networks Cloud and Data Center Portfolio

Figure 15 shows Juniper Networks portfolio for distributed data centers, including data center interconnect (DCI) and Data Center Edge (DCE).

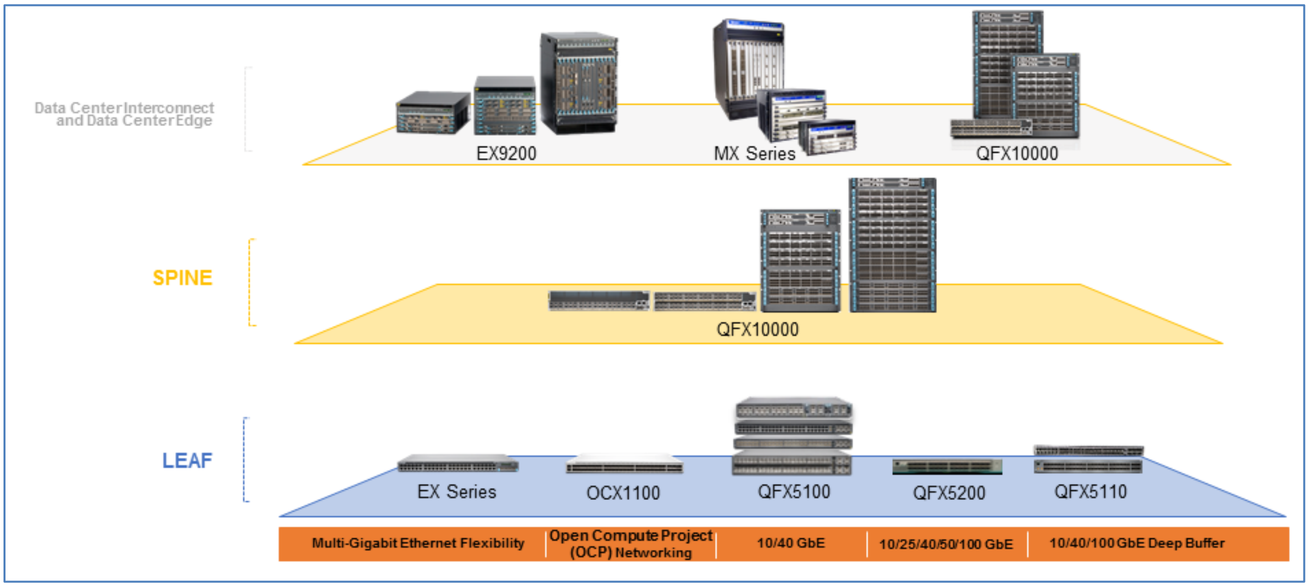

Data Center Interconnect and Data Center Edge
EX9200
MX Series
QFX10000
SPINE
QFX10000
LEAF
EX Series
OCX1100
QFX5100
QFX5200
QFX5110
Multi-Gigabit Ethernet Flexibility
Open Compute Project (OCP) Networking
10/40 GbE
10/25/40/50/100 GbE
10/40/100 GbE Deep Buffer

Figure 15 : Juniper Portfolio for Distributed Data Centers

For data centers that use the spine-and-leaf topology, options at the leaf layer include:

- EX Series switches with multi-gigabit ports
- OCX open compute switch, which provides the option of a white box (hardware and software provided by different vendors) or an Open Compute Project (OCP) integrated switch that comes bundled with the Junos operating system.
- QFX Series switches with 10GbE and higher ports. If you need deep buffers, you can get that with specific QFX Series switches.

For the spine, we recommend the QFX10000, which has 100GbE downlinks that let you build a data center with 10,000+ ports.

At the DCE or DCI, we recommend any one of the following products for ingress and egress of the data center:

- EX9200
- QFX10000
- MX Series routers

We also recommend that you use larger SRX Series as a front-end node to build security all the way through the network.

Planning, Building, and Operating

We recommend that you follow the steps in Figure 16 to plan, build, and operate your distributed data centers.

© 2017 Juniper Networks, Inc.

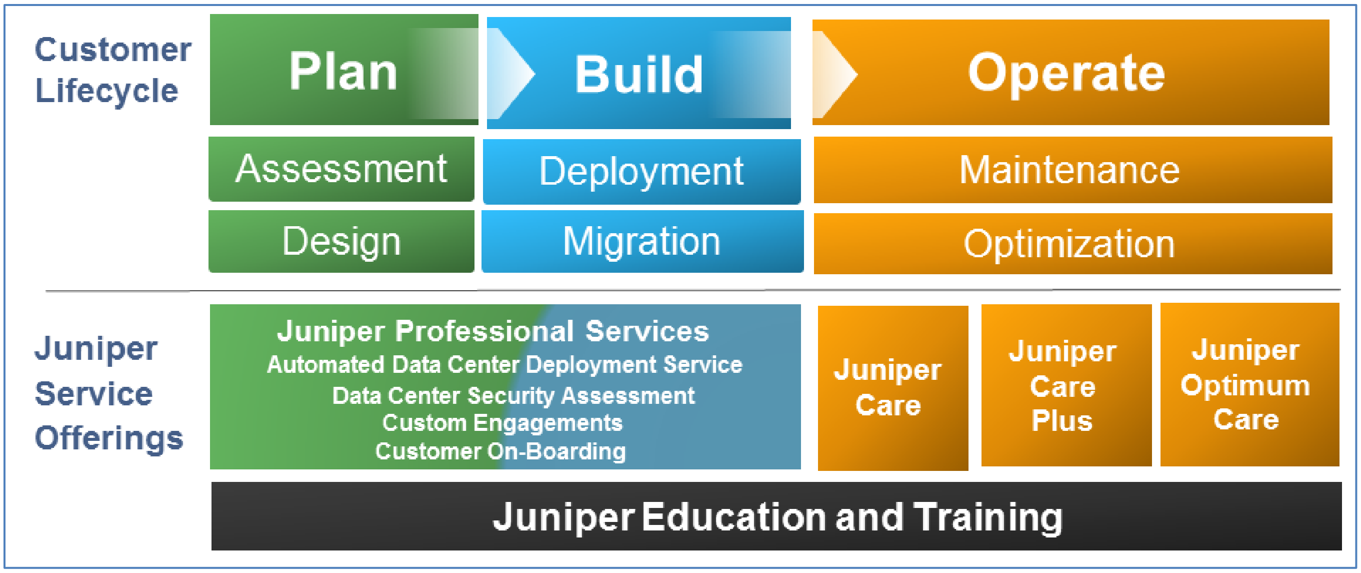


Figure 16: Planning, Building, and Operating Distributed Data Centers with Juniper Networks

Up front planning is essential to a successful deployment that meets your business requirements. Without proper planning, operations will become a big challenge.

You can use Juniper Professional Services group to provide assessment services to assist you in the design of your data center. Juniper Networks can also help in the building stage with deployment services. If you need to customize services outside of our standard packages, Juniper Networks can customize any type of deployment. Whether it is the build-out of a distributed data center all the way to onboarding customers, look to Juniper Professional Services to help.

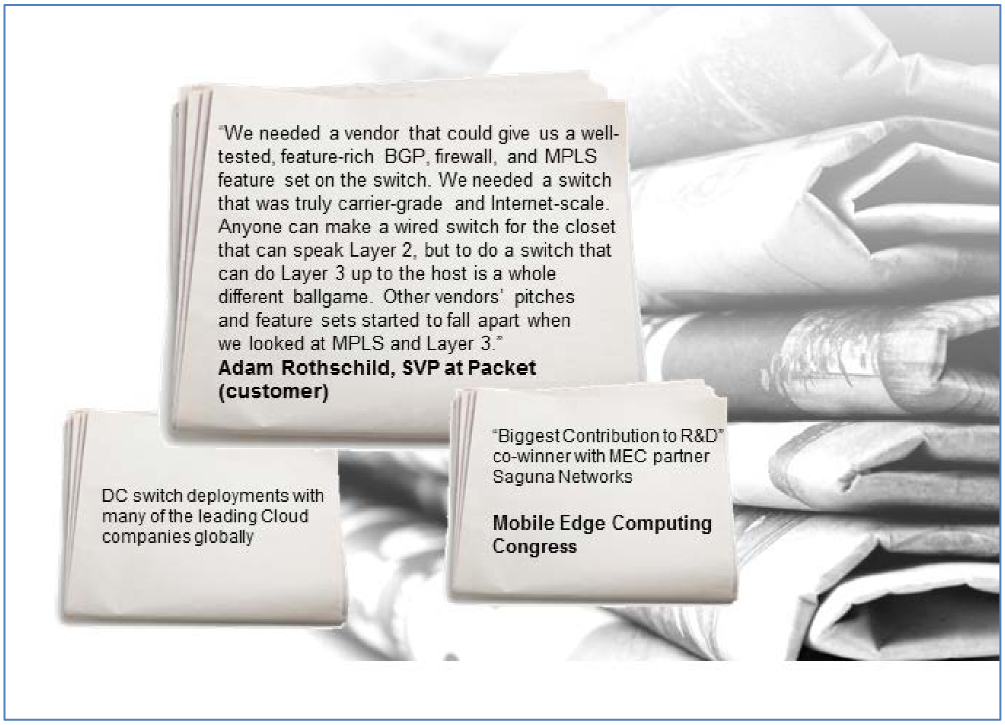
For assistance with operations, Juniper offers Juniper Care, Juniper Care Plus, and Juniper Optimum Care. Juniper is very proud of our services organization, and what they bring to the table.

Juniper Networks Education Services are for everyone. They get you up to speed throughout the processes of planning, building, and operations. Learn the details of our products, and keep up to speed on new products, new developments, and new features.

Juniper Networks References and Awards

Figure 17 shows just a couple of the many customer references that we receive. It also shows an award that Juniper Networks and our partner Saguna Networks from the Mobile Edge Computing Congress.

© 2017 Juniper Networks, Inc.



"We needed a vendor that could give us a well-tested, feature-rich BGP, firewall, and MPLS feature set on the switch. We needed a switch that was truly carrier-grade and Internet-scale. Anyone can make a wired switch for the closet that can speak Layer 2, but to do a switch that can do Layer 3 up to the host is a whole different ballgame. Other vendors' pitches and feature sets started to fall apart when we looked at MPLS and Layer 3."
Adam Rothschild, SVP at Packet (customer)

DC switch deployments with many of the leading Cloud companies globally

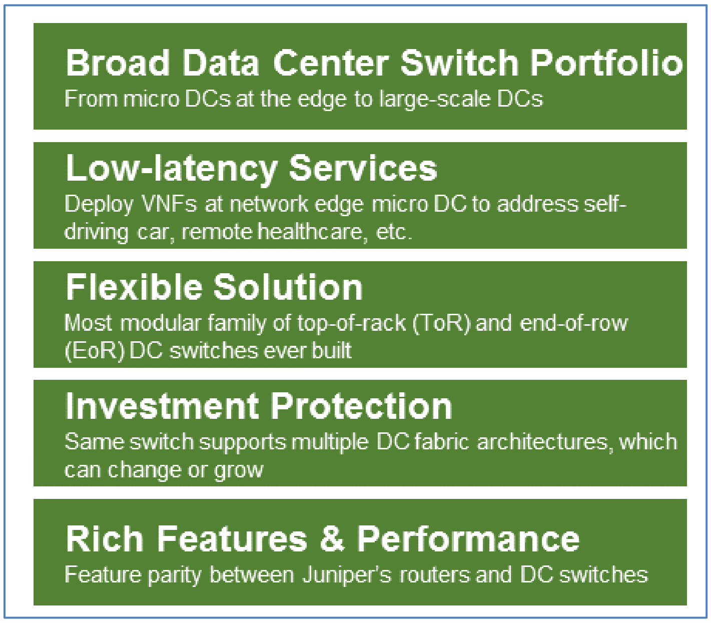
"Biggest Contribution to R&D" co-winner with MEC partner Saguna Networks

Mobile Edge Computing Congress

Figure 17 : Juniper Networks References and Awards

Benefits of Juniper Networks Products in Distributed Data Centers

Figure 18 summarizes the benefits that Juniper Networks products provide to build distributed data centers.



Broad Data Center Switch Portfolio
From micro DCs at the edge to large-scale DCs

Low-latency Services
Deploy VNFs at network edge micro DC to address self-driving car, remote healthcare, etc.

Flexible Solution
Most modular family of top-of-rack (ToR) and end-of-row (EoR) DC switches ever built

Investment Protection
Same switch supports multiple DC fabric architectures, which can change or grow

Rich Features & Performance
Feature parity between Juniper's routers and DC switches

Figure 18 : Summary of Juniper Networks Data Center Portfolio Benefits

As you saw, we have a broad portfolio from micro data centers to large hyper-cloud data centers.

© 2017 Juniper Networks, Inc.

The key to low latency will be very important with things like self-driving cars and remote healthcare. There are many other examples where low-latency requirements drive the need to have compute power moved out to the edge. These requirements show why building distributed data centers is important, and why they need to be flexible from the top of the rack to the end of the row.

In addition to other benefits of Juniper Networks products is the Junos OS. Junos provides investment protection because when training employees, they need to learn only one operating system. This means significant saving on OPEX just from running Juniper products. Another investment protection is that the same switch can support multiple architectures. It can be run as an MC-LAG that is transitioned to a Qfabric and Junos Fusion, and can then transition directly to an IP fabric. The products that you are purchasing are supported in the same infrastructure so you are protecting your investment going forward.

Multi-Access Edge Computing

Figure 19 shows the Juniper Networks Multi-Access Edge Computing (MEC) architecture. With the distributed data center, you can have data centers anywhere or everywhere. The MEC architecture includes service gateways (S-GWs) and Packet Data Network Gateways (P-GWs), along with security gateways, which are firewall, NAT, and VPN service types. This design includes a virtual infrastructure and distributed data centers.

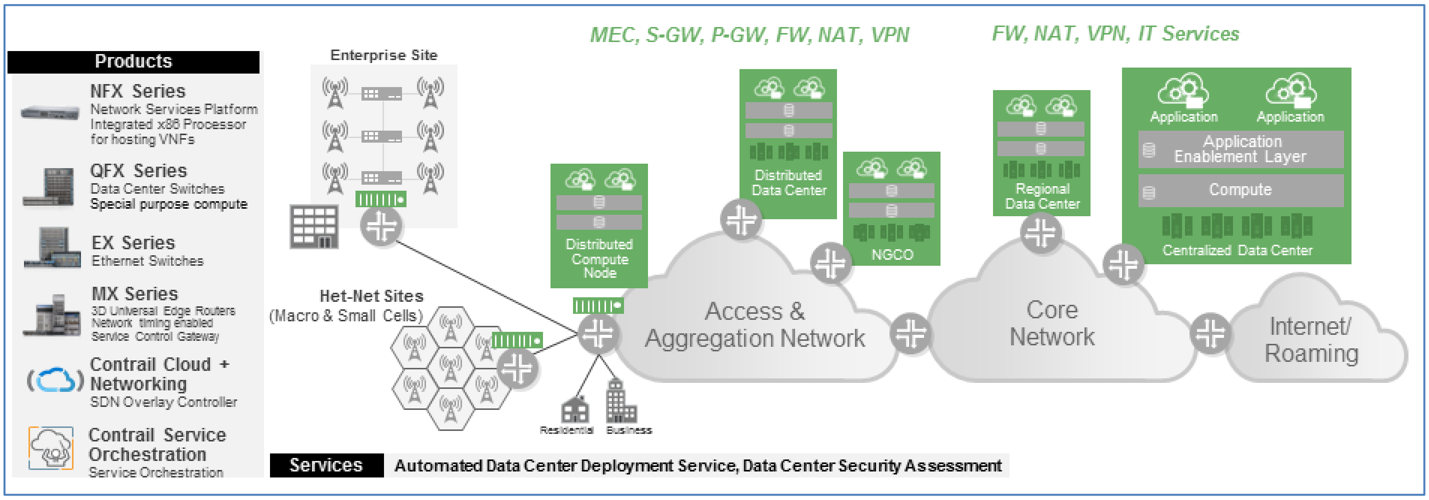


Figure 19: Multi-Access Edge Computing

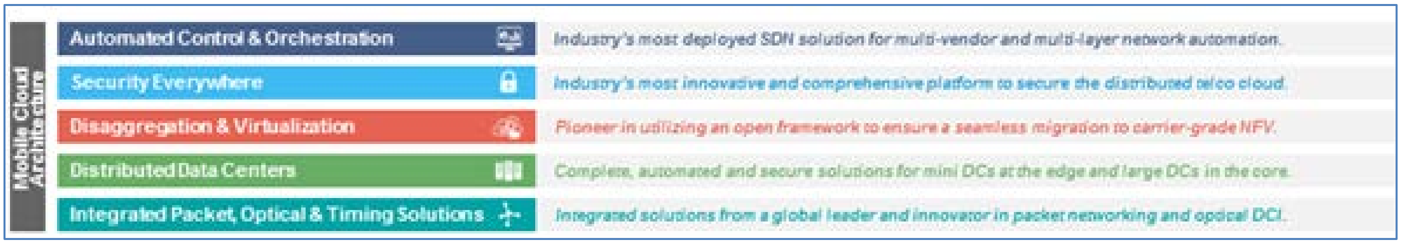
If you want centralized data centers, you can have ten thousand or a hundred thousand servers in your data centers. If you want a micro data center, you can use the Cloud CPE or NFX platform.

The key is the infrastructure that we can build and the distributed data centers—from our NFX series, to our EX series, to our QFX leaf switches, and our QFX 10000 spine switches, our data center interconnect, and our MX Series router universal SDN gateways. Then we can use Contrail networking to marry the virtual world with the physical world and Contrail Service orchestration as an overarching orchestrator for all of these components.

For More Information

The distributed data center is one of five solution areas within the Juniper Networks mobile cloud architecture, as shown in Figure 20.

© 2017 Juniper Networks, Inc.



Mobile Cloud Architecture	Automated Control & Orchestration	Industry's most deployed SDN solution for multi-vendor and multi-layer network automation.
	Security Everywhere	Industry's most innovative and comprehensive platform to secure the distributed telco cloud.
	Disaggregation & Virtualization	Pioneer in utilizing an open framework to ensure a seamless migration to carrier-grade NFV.
	Distributed Data Centers	Complete, automated and secure solutions for mini DCs at the edge and large DCs in the core.
	Integrated Packet, Optical & Timing Solutions	Integrated solutions from a global leader and innovator in packet networking and optical DCI.

Figure 20 : Juniper Networks Mobile Cloud Architecture–Solution Areas

For further detail on the other solution areas, see Network Design and Architecture Center: Mobile Cloud.

© 2017 Juniper Networks, Inc.