



## Executive Summary

Traditional network designs are failing to meet service providers' business requirements. The designs lead to complex hardware stacks, over-provisioning of capacity, lengthy service cycles, and expensive truck rolls. Adherence to these designs, which results in high cost, broken business processes, and lagging innovation, is eroding service providers' competitive positions.

Juniper Networks has launched High-IQ, a programmable networking approach, that leverages network function virtualization (NFV) and software defined networking (SDN) to create networks that are automated, scalable, and customizable, enabling rapid service provisioning based upon actionable intelligence. Programmable networks allow service providers to automate network operations for simplicity and agility in response to dynamic service needs while reducing operational costs; scale the network infrastructure with silicon, SDN, and network fabric virtualization to deliver the performance and efficiency needed to economically meet demand; and rapidly create new, customizable services to increase revenue and brand equity.

ACG Research analyzes three programmable High-IQ network use cases that were created by Juniper Networks. The analyses show the benefits derived from the deployment of programmable networks for service providers. A cloud customer premise equipment (CPE) and virtual firewall (vCPE) use case replaces physical CPE with a simple on-premise Ethernet device and moves IP virtual private network (VPN) and firewall functions to the cloud. This produces a 36 percent five-year net present value (NPV) increase as compared to the physical CPE solution. A real-time network self-optimization use case replaces manual traffic engineering processes. This produces a 27 percent five-year total cost of ownership (TCO) savings compared to the manual processes. An elastic traffic engineering use case for a national all IP core network demonstrates the advantages of an SDN solution as compared to the present mode of operations. The SDN solution reduces bandwidth and associated link capital expenses (capex) by 35 percent while maintaining all network service level agreements.

### KEY FINDINGS

Juniper Networks' programmable NFV/SDN networks enable service providers to automate network operations for an agile response to dynamic service needs, reduce operational costs, and scale the network.

Three Juniper Networks' use cases are analyzed. Compared to the present mode of operations, programmable High-IQ networks:

- Increase NPV by 36% using virtualized CPE and firewall (vCPE)
- Reduce TCO by 27% via real-time network self-optimization
- Reduce network link capex by 35% using elastic traffic engineering

## Introduction

Traditional network designs are impairing service providers' competitive positions. Their dependence on purpose-built hardware and use of manual systems interfaces are driving costs to uncompetitive levels and eroding customer satisfaction. Networks have become inflexible and rigid with stranded assets and low-capacity utilization. In addition, service innovation has failed to keep pace with that of new cloud-based market entrants.

A new approach to network architecture and design is needed to restore competitiveness. It must allow service providers to:

- Increase customer satisfaction and customer retention
- Increase revenues by accelerating delivery of new and differentiated services
- Reduce upfront capital expenditures and improve asset utilization
- Provide customized, on-demand service delivery through customer focused portals

Juniper Networks' programmable High-IQ networks leverage network function virtualization (NFV) and software defined networking (SDN) to provide a vehicle that addresses these needs. The combination of a unified control plane with programmable virtualized network resources enables extensive automation of service provisioning and network management processes across many devices, multiple layers, and multiple vendors. Programmable High-IQ networks reduce capital expenses (capex) by improving network utilization. Specifically, utilization is improved through the elimination of over-provisioning and near real-time network optimization. In addition, faster service delivery and increased automation reduce personnel costs and contribute to operational efficiency. Accelerated new service introduction and rapid customer order completion contribute to the delivery of innovative, customized experiences, culminating in higher revenue, customer retention, and increased margins.

## Use Cases

The benefits of the programmable High-IQ networks approach are illustrated by three use cases:

1. Cloud customer premise equipment (CPE) and virtual firewall (vCPE)
2. Real-time network self-optimization
3. Elastic traffic engineering

### **Cloud CPE and Virtual Firewall**

Existing business services implemented in CPE, such as IP-VPN and security services, are high cost, require long installation intervals, and are difficult to modify and upgrade. This slow and rigid process creates customer dissatisfaction and impairs the service provider's ability to innovate and upsell services.

The CPE equipment stack is the root cause of the high cost, inflexibility, and long installation intervals. Adds, moves or changes frequently require replacement of the CPE with associated truck rolls and several manual updates to databases and network elements on site, at the network operations center and at the customer services center.

Cloud CPE and virtual firewall reduce field equipment installation and support costs. More importantly, service providers can rapidly deploy new cloud-based services that are free of traditional physical CPE

installation and maintenance limitations. Figure 1 shows the architecture for the new virtualized solution.

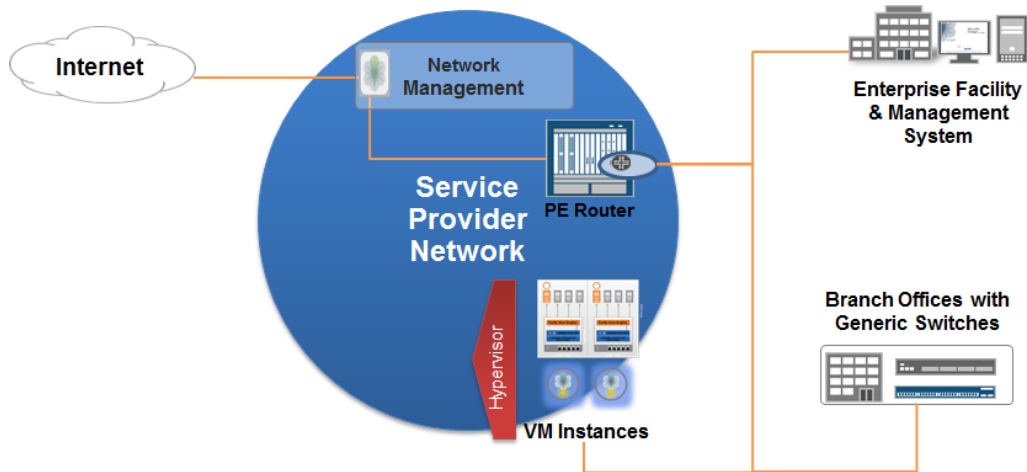


Figure 1 – Cloud CPE and Virtual Firewall Architecture

Cloud CPE and virtual firewall simplify CPE via an Ethernet network interface device. Functions such as IPv6 NAT<sup>1</sup>, DPI based functions, and firewall capabilities are moved to the provider edge router and to virtualized data centers. A self-care portal allows the customer to set IP VPN data rates, use network management tools, make policy-level choices for firewall and threat management security services, and monitor the services in real time.

Figure 2 shows a single-site cost comparison achieved by virtualizing CPE.

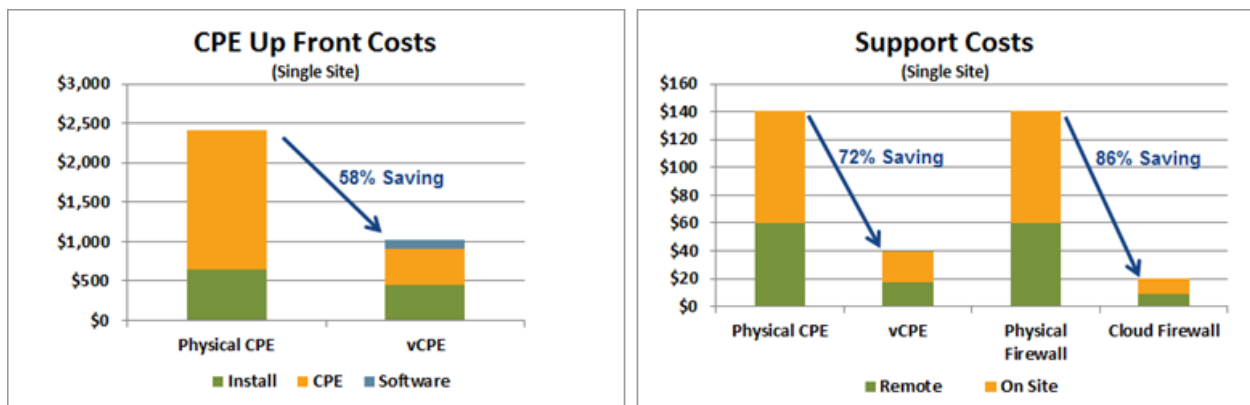
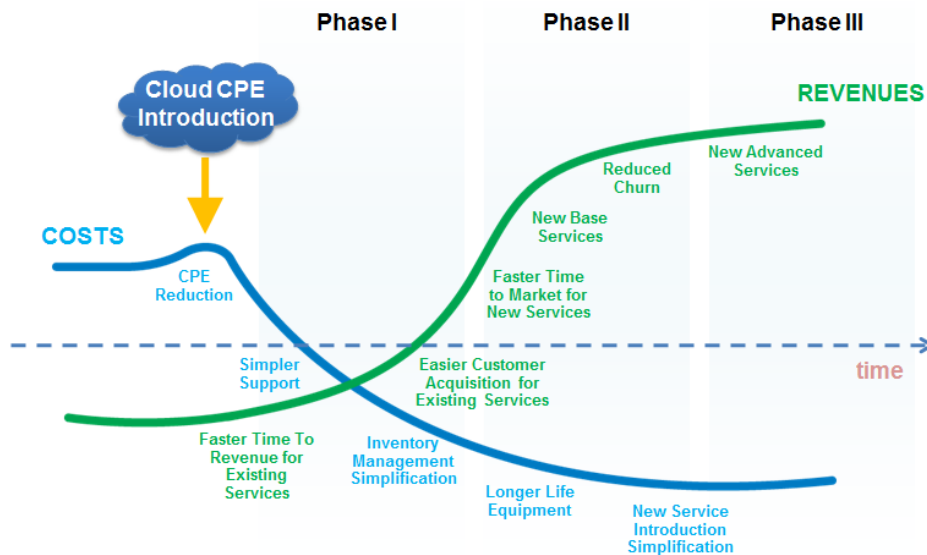


Figure 2 – Single-Site Cost Comparison

Up-front CPE costs are reduced by 58 percent because of virtualization, which exploits the better scale economies of the data center. Virtualization also reduces support costs: 72 percent CPE savings and 86 percent firewall savings.

Figure 3 Figure 1 displays a comprehensive view of the benefits of cloud CPE and virtual firewall.

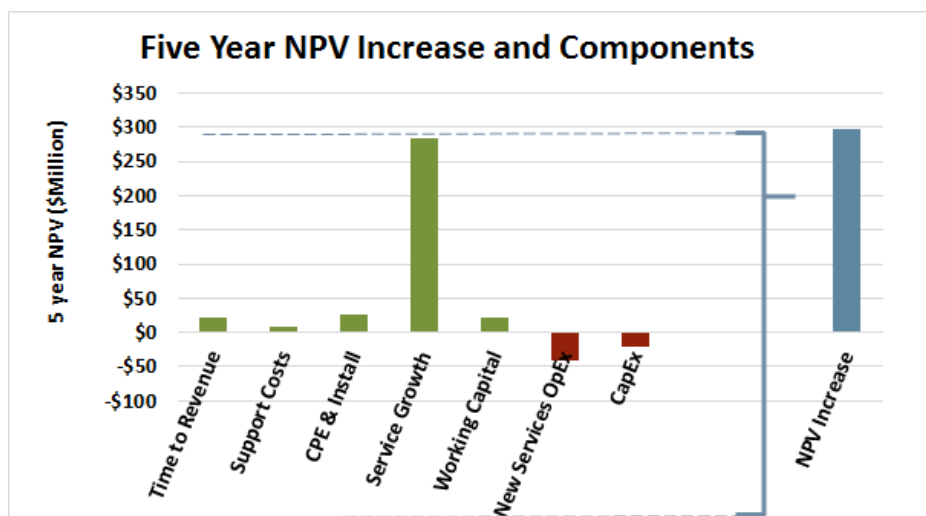
<sup>1</sup> Network Address Translation



Simpler CPE results in significantly lower setup costs and reduces inventory, maintenance, and support costs. Cloud CPE automation and orchestration capabilities eliminate many manual processes. Consequently, services become faster to develop, deploy, and contribute revenue.

A detailed financial comparison is made between cloud CPE with virtual firewall and traditional physical CPE and firewall for a US service provider serving 75,000 small, 5,000 medium, and 2,000 large businesses.

Modeling assumptions include average monthly recurring charges: IP Virtual Private Network (VPN) \$250/site and firewall \$75/site; average nonrecurring charges: IP VPN \$500/site and firewall \$300/site; and cloud startup costs: \$5 million. Figure 4 shows the additional net present value (NPV) contributions of cloud CPE and virtual firewall compared to the physical CPE solution.



**Figure 4 – Increase NPV Showing Individual Component Contributions<sup>2</sup>**

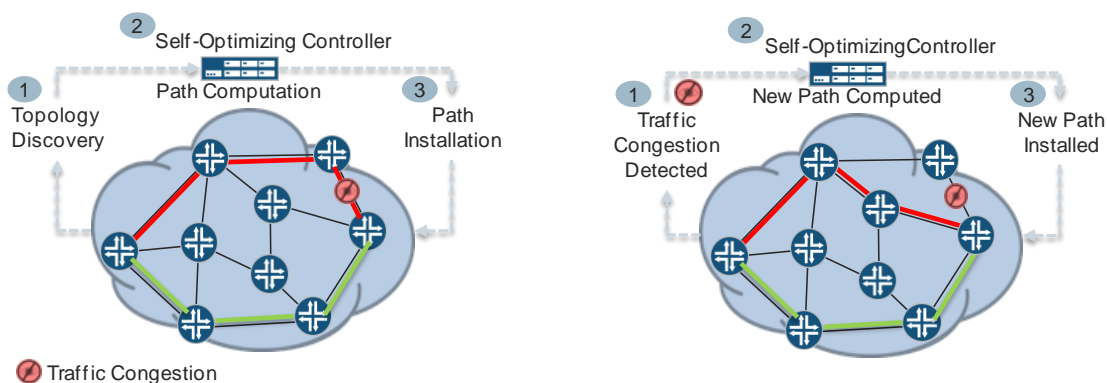
<sup>2</sup> Capex has negative NPV because many additional service contracts are sold for the virtual solution. The unit cost of virtual CPE is 72 percent lower than traditional CPE.

Cloud CPE with virtual firewall provides a five-year NPV increase of 36 percent (\$298 million) as compared to the physical CPE solution.

### Real-Time Network Self-Optimization

Real-time network optimization is not feasible using traditional network architectures because many manual interventions are required in the optimization process. The manual interventions prevent rapid response to changing traffic flows and therefore force operators to throw bandwidth at the problem as a hedge against possible service outages and service level agreement violations. The result is high cost due to wasted network capacity.

Real-time network self-optimization automatically identifies the optimal network path in near real time, allowing service providers to continually optimize traffic flows and thereby increase utilization and avoid capex caused by over-provisioning. Figure 5 shows an example of a self-optimization response to traffic congestion on a single link. The self-optimizing controller uses real-time traffic flows to adjust the network model of the controller, identify a new optimized path that avoids the congestion, and then program the new optimized route.



**Figure 5 – Example Real-Time Self-Optimizing Network Response to Traffic Congestion**

A financial comparison is made for a 15 node core network. The self-optimizing network with dynamic traffic engineering capability and converged control plane is compared to a traditional network with manual traffic engineering and separate IP and optical control planes. Key assumptions and inputs include the number, cost, growth, and environmental costs of 10GE and 100GE ports.

The self-optimizing network shows a 27 percent total cost of ownership (TCO) savings compared to the manually engineered network. The main benefits of an optimized network are lower costs per port, transport and edge power savings derived from increased network utilization and avoidance of over-provisioning. The automation of many network capacity and optimization processes also reduces network engineering labor expenses.

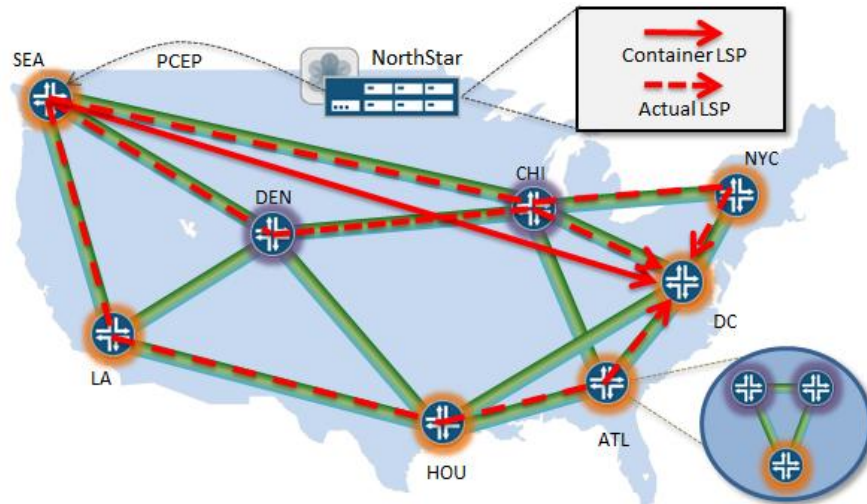
### Elastic Traffic Engineering

Traditional traffic engineering practices lack a real-time global view of traffic and employ many manual steps to reconfigure network paths and capacity allocations. As a result each Label Switched Path (LSP) is traffic engineered separately. Modern mesh networks provide many economically attractive alternative paths to connect a traffic source to its destination. One at a time engineering of each LSP evaluates only

a fraction of the possible alternatives. Suboptimal path assignments are made, resulting in significant waste of capacity and unnecessary cost.

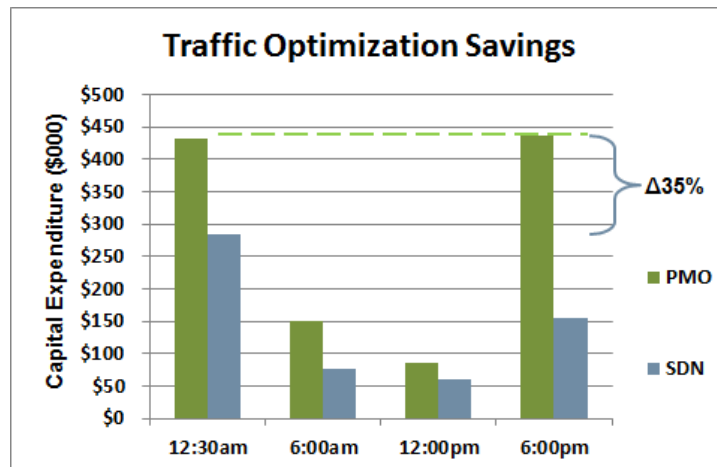
An SDN solution employs elastic traffic engineering to globally and dynamically optimize traffic on all LSPs on a national backbone network. This reduces network link capacity and its associated capex as compared to the present mode of operations that traffic engineers each LSP separately.

Figure 6 illustrates the elastic traffic engineering concept.



**Figure 6 – Elastic Traffic Engineering**

Juniper Networks NorthStar controller provides visibility of traffic flows on all LSPs in real time. It uses this information to globally optimize traffic capacity on all links. Furthermore, it has the flexibility to use multiple network paths to provision traffic requirements for individual LSPs. For example, Figure 6 shows an LSP between Seattle and Washington, DC. This is treated as a container with capacity requirement that is met by three actual LSPs traversing three separate network paths. Figure 7 shows the link capex benefit of the elastic traffic engineering solution compared to the present mode of operations.



**Figure 7 – Capex Savings for Elastic Traffic Engineering**

Elastic traffic engineering produces a link capex savings of 35 percent as compared to the present mode of operations (PMO). The savings is compared for the capacity required at peak time because this requirement is used to provision the Layer 3 equipment. The savings are produced by the optimization ability of SDN to find a global optimum for all LSPs as compared to the one LSP at a time method used by the PMO and by the elastic traffic engineering technique of meeting container LSP requirements by assigning multiple, actual LSPs.

## Conclusion

Service providers need a new approach to network architecture and design to restore competitiveness. Programmable High-IQ networks address this need by enabling service providers to automate network operations for an agile response to dynamic service needs, reduce operational costs, and scale the network.

Three use cases created by Juniper Networks demonstrate the economic contributions of programmable High-IQ networks as compared to the present mode of operations:

1. Cloud CPE and virtual firewall: 36 percent five-year NPV increase
2. Real-time network self-optimization: 27 percent five-year TCO savings
3. Elastic traffic engineering: 35 percent link capex savings

ACG Research is an analyst and consulting company that focuses in the networking and telecom space. We offer comprehensive, high-quality, end-to-end business consulting and syndicated research services. Copyright © 2014 ACG Research. [www.acgresearch.net](http://www.acgresearch.net).