Architecting Data Centers for

SDN AND NFV

In 40G and 100G Environments

GARLAND
TECHNOLOGY

See every bit, byte, and packet®

Introduction

Software-Defined Networking: The Promises & The Reality

Back in 2013, the IT community was abuzz with excitement about software-defined networking (SDN). Hopeful IT professionals saw that network demands were increasing exponentially and were enamored by the promises of:

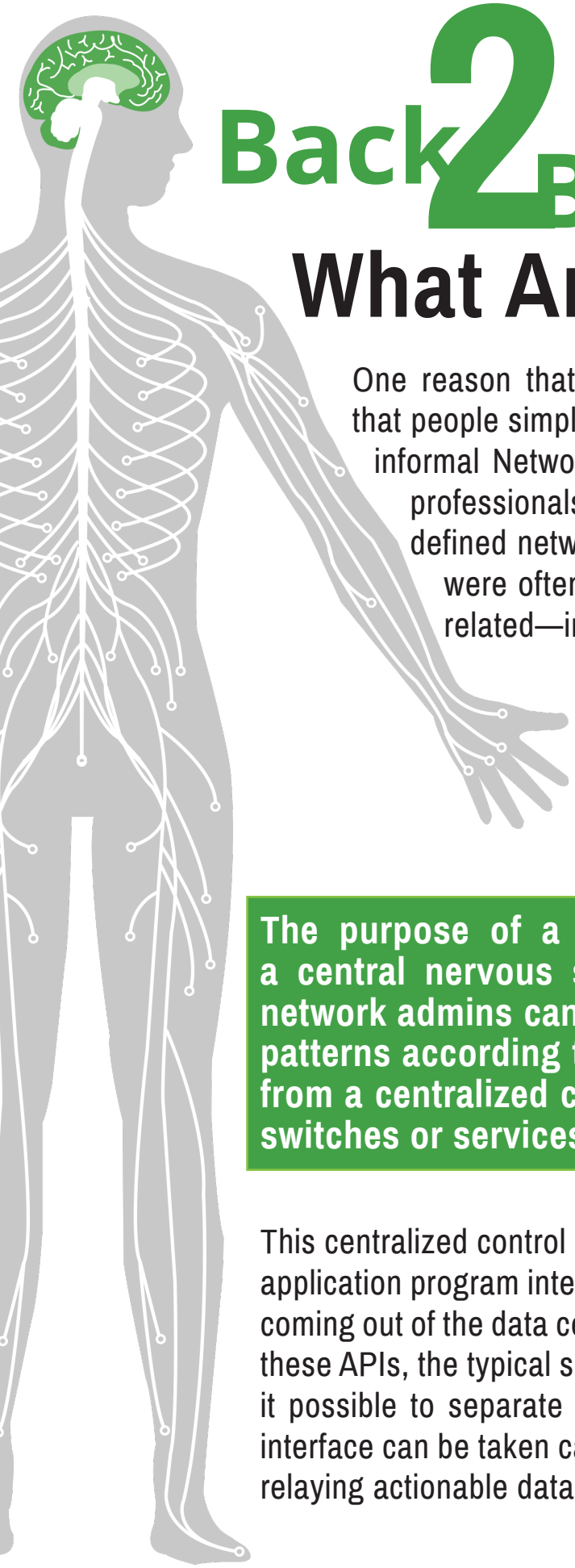
- Centralized, simplified control over network traffic
- Policy-driven priority supervision
- More accessible automation

However, almost on cue, SDN fell from its 2013 peak of inflated expectations on the Gartner Hype Cycle to what Gartner calls the "trough of disillusionment" in 2016.

What this means is that while many believed 2013 marked the year that SDN would start working its way into broad deployment, implementation proved more difficult than expected.

> **"During 2015, we started to see production adoption of SDN solutions, though broad deployments are still relatively rare. A variety of both established vendors and startups continue to develop SDN technologies, but full, robust, end-to-end enterprise-ready solutions are net yet fully established on the market."** *–According to Gartner's 2016 analysis*

Despite the fact that the hype has died down since 2013, now—seems to be the best time to start thinking seriously about software-defined networking and its companion technology, network functions virtualization (NFV). As 40G and 100G networks become more of the norm, SDN and NFV will help data centers keep pace with demands—but only if total traffic visibility is maintained throughout the evolution.



Back 2 Basics

What Are SDN and NFV?

One reason that SDN hype became so overblown in 2013 is that people simply didn't understand the technology. In fact, one informal Network World survey estimated that just 10% of IT professionals felt confident in their understanding of software-defined networking. To make matters worse, SDN and NFV were often lumped together because they are so closely related—in reality, they are separate yet complimentary.

So, before discussing the value of SDN and NFV in the 40G and 100G data centers of tomorrow (and today for some enterprises), it's important to truly understand what each technology is.

The purpose of a software-defined network is to create a central nervous system for traffic routing. This means network admins can use an SDN controller to change traffic patterns according to rapidly changing business needs—all from a centralized console without having to touch specific switches or services.

This centralized control is made possible by northbound and southbound application program interfaces (APIs) that command traffic going into and coming out of the data center. While the industry has not yet standardized these APIs, the typical southbound API is OpenFlow, a switch that makes it possible to separate data paths from control paths. The northbound interface can be taken care of by something like a network packet broker, relaying actionable data to virtual services.

These virtual services are where NFV comes into play. When centralized SDN control proved easier said than done, network architects worked to achieve the virtualization and automation goals of SDN on a smaller scale. This meant virtualizing some of the services in the data center, including load balancing, application firewalls, intrusion prevention, and monitoring tools.

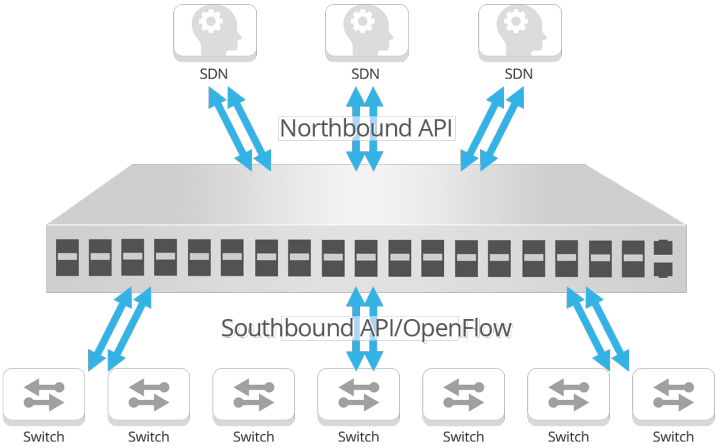
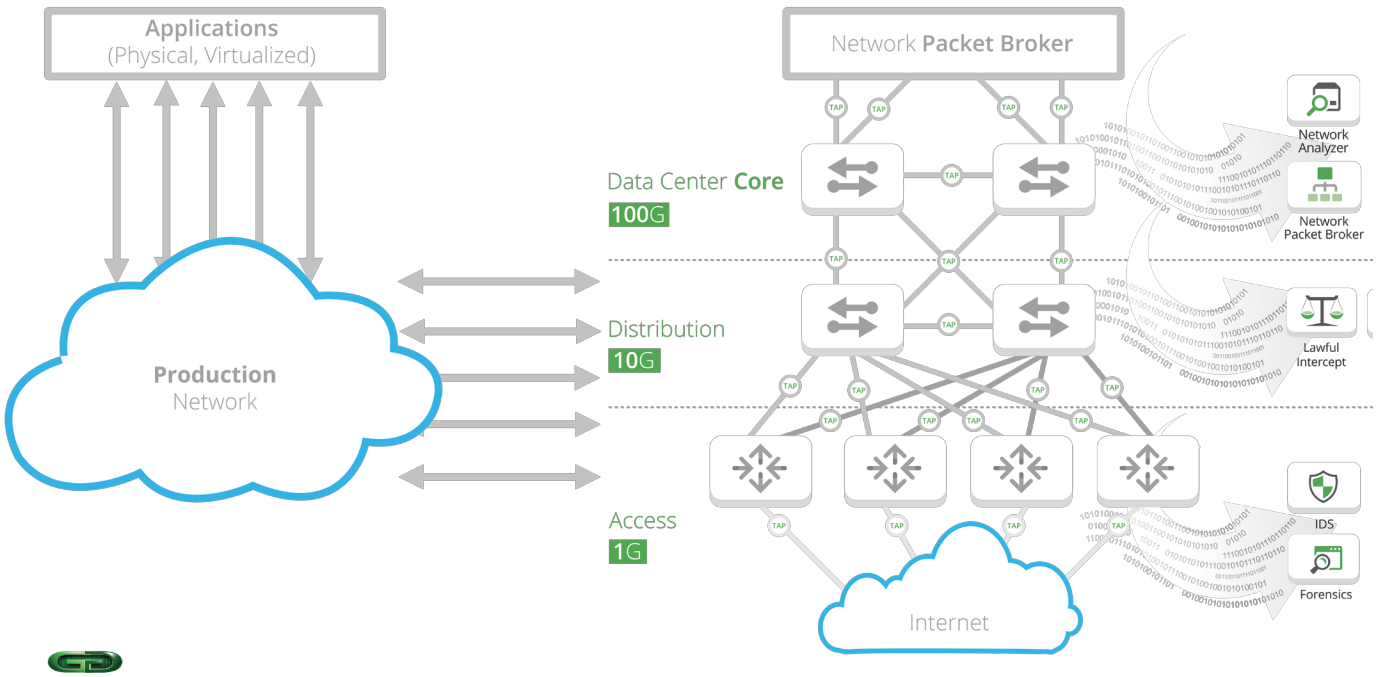


Diagram 1 - North/South API traffic

Widespread virtualization of applications and services—SDN and NFV working together—is the ultimate goal for efficient data centers at 40G and 100G speeds. However, SDN can be implemented without NFV simply as a series of switches, routers, and appliances that are controlled in an automated way.

SDN and NFV are complicated to say the least, which is likely why network architects at companies with 1G and 10G networks haven't pushed for widespread adoption—such extensive automation and virtualization isn't necessary at these lower speeds.

However, the external forces pushing enterprise networks and data centers to evolve will make the efficiency of SDN and NFV more of a necessity than an option moving forward.



As Data Center Demands Increase
Exponentially, SDN and NFV Will Go Mainstream

Google built the world's first true software-defined network to meet its global needs—but the company started building it in 2009 and only reached full-fledged SDN in March 2016. For years, this has been the use case for software-defined networking. The world's largest companies with the most demanding workloads on their networks and data centers.

However, today's business applications and systems are pushing even smaller enterprises away from the comfort of 1G and 10G networking.

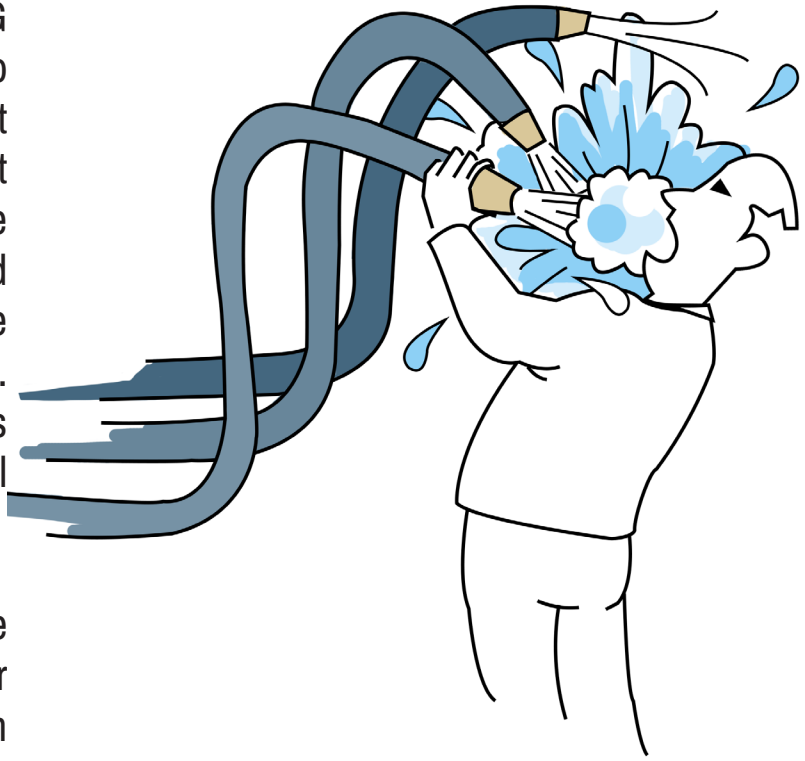
Bandwidth-intensive services such as videoconferencing, unified communications and collaboration, real-time data migration to the cloud, big data analytics and more will quickly overwhelm 10G networks, making 40G and 100G mainstream realities.

From a data center perspective, this will drastically increase east-west (server-to-server) traffic to the point that a new architecture will be a necessity.

In fact, recent Cisco research found that global data centers will see 31% increases in IP traffic annually through 2020.

The problem with rapidly-increasing east-west traffic is that it forces network architects to continuously increase monitoring capabilities. In a traditional architecture, each new east-west data center link would require new stacks of in-line security appliances and monitoring tools—especially given the fact that business-critical applications are going to the cloud and data centers must support high performance and availability.

At a certain point, purchasing new 40G or 100G appliances and software to meet east-west traffic demands won't just be economically inefficient—it will be impossible. But at the same time, persisting with existing 1G and 10G monitoring solutions will be like trying to drink water out of a firehose. Trying to monitor 40G or 100G links with oversubscribed 10G tools will inevitably lead to packet loss.



Implementing SDN will ease the challenges of east-west data center growth by introducing a north-south management and automation structure to maximize the potential of monitoring tools. However, SDN is only as effective as the visibility plane that supports it.

The Importance of Visibility with SDN

Keep In Mind

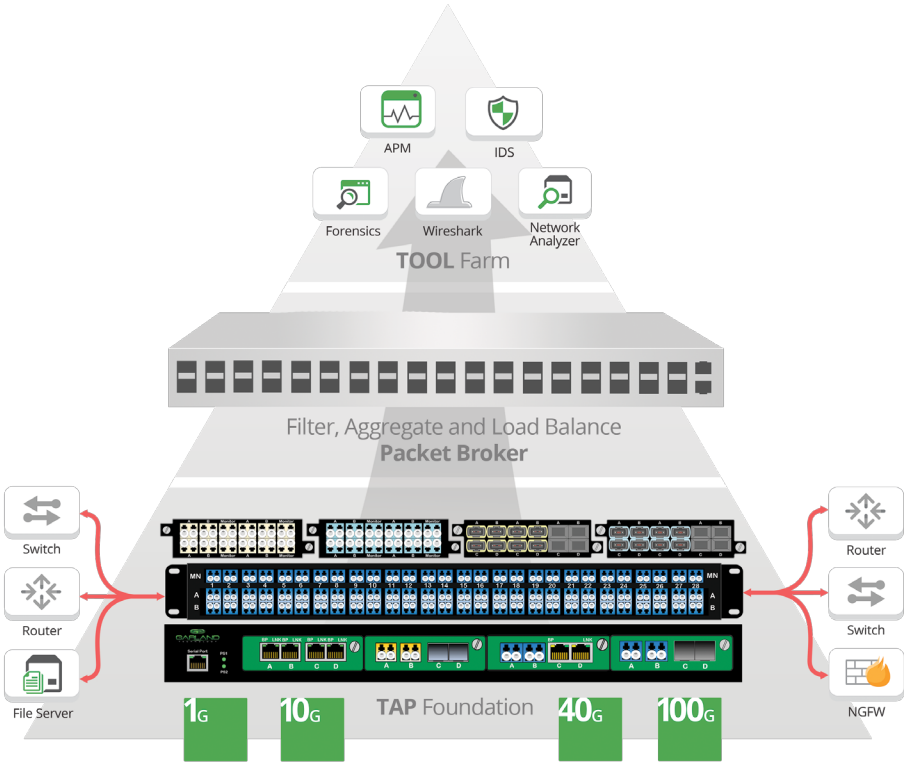
1. SDN decouples the data plane from the control plane
2. Visibility is required for both the data plane and the control plane

Centralized control of traffic flows will be critical for monitoring 40G and 100G networks. But before implementing SDN, network architects must ensure that they have a solid visibility plane that ensures 100% of packets will be seen by the SDN controller.

To achieve complete transparency with application monitoring tools, network architects must account for solutions and functions such as:

- Network analyzers
- Bandwidth management
- Computer forensic analysis and data capture
- Content filtering
- Data leakage prevention (DLP)
- Lawful interception
- Intrusion detection

Especially in 40G and 100G environments, capturing, filtering, aggregating and load balancing network traffic is paramount to achieving complete visibility. Without these functions, there will be holes in data regardless of whether the network is software-defined or not, making the enterprise more susceptible to data breaches and network intrusion.



It's important not to think traditionally when considering an approach to visibility that supports a software-defined network. Thinking in terms of 1G or even 10G networks might push network architects to rely on SPAN ports for connectivity, but this might be the most critical mistake when it comes to SDN visibility.

Mirroring traffic with SPAN ports requires CPU resources from switches and routers. At 1G speeds, companies may have been content with this CPU utilization because the demands weren't high enough to make a significant difference. However, CPU utilization is unpredictable and SPAN ports show blatant limitations on 10G networks as oversubscription leads to severe packet loss and diminished visibility. And if SPAN ports aren't viable for 10G network speeds, they certainly won't suffice for SDN visibility on 40G and 100G networks.

Rather than trying to force ineffective SPAN ports to work in a new SDN, enterprises must create a visibility plane with passive optical TAPs and network packet brokers to guarantee 100% packet capture for the centralized controller.

The Benefits of Passive Optical TAPs and Network Packet Brokers

The foundation of any visibility plane has to be passive optical TAPs. Rather than using SPAN ports that can become points of failure and unreliable for packet capture, passive optical TAPs guarantee 100% visibility without interrupting the data path. As east-west demands continue to increase, building out a foundation of passive optical TAPs helps scale traffic aggregation to support a centralized SDN controller.

Once network architects have a foundation of passive optical TAPs in place for all east-west traffic, network packet brokers can use these TAPs as a data source. Network packet brokers control the flow of traffic and make it possible to capture data as well as leverage monitoring tools and applications in 40G/100G environments.

However, there is often question as to whether these physical brokers will be effective in a virtual environment such as SDN. In addition, industry analysts wonder whether the functionalities of network packet brokers can be virtualized.

There are many variables that go into the ability of a packet broker to manage a visibility plane for an SDN solution, including individual protocols. As a Network World article points out:

> **"More important than any single protocol (especially with the ecosystem of protocols growing constantly) is the ability to inspect and identify packets from Layers 2 through 7, combined with the flexibility to configure and program the [network packet broker] to strip and slice packets to optimize monitoring applications, and to support emerging protocols, such as VXLAN."** *-Network World article*

Packet brokers must have supreme flexibility to be able to manage the many different APIs within a software-defined network. When flexible network packet brokers are in place to manage east-west traffic collected by TAPs, the SDN controller can proactively direct packets to proper monitoring tools and help realize the promised benefits of a software-defined network.

It Won't Pay to Lag Behind SDN and NFV

The rapidly increasing demands on enterprise data centers and networks are plain to see. It might seem cost effective to hang onto existing equipment, network architecture, and applications as long as possible. However, this will only hurt businesses in the long run.

Software-defined networks have received criticism in recent years because they have failed to live up to the 2013 hype. But SDN (and complementary NFV) are the future and enterprises will benefit from being proactive about transitioning from traditional 10G to a 40G/100G SDN.

While it's important to start adapting to software-defined networking and network functions virtualization, network architects must be careful not to dive in hastily. If you want help creating your visibility plane to prepare for a gradual transition to 40G/100G SDN, contact us today for a free Design-IT consultation.

Contact

Sales, quotations, product inquiries:
sales@garlandtechnology.com

Garland Technology, LLC.
New York | Texas | Germany