INFONETICS RESEARCH SPECIAL REPORT

The Evolution of SDN and NFV Orchestration

February 2015

By Principal Analyst Michael Howard

Table of Contents

List of Exhibits

INTRODUCTION

Although the telecom industry is still in the early days of network functions virtualization (NFV) and software-defined networking (SDN), we see orchestration technology starting to bloom. SDN and NFV are designed to allow service providers to increase automation of their networks while avoiding “vendor lock-in” by enabling multi-vendor solutions. This is all well and good; however, the pathway from today to that Nirvana requires pragmatic steps. This means starting with SDN and NFV in projects within “contained domains” to make technology work in real, but small, parts of carrier networks before advancing to orchestrate larger multi-domain areas.

In this technology paper, we examine:

- Types of orchestration for SDN and NFV
- The orchestrator of orchestrators
- Where we are now—orchestration for each contained domain
- The evolution of orchestration through 2020
- Considerations for choosing orchestration software

MANY TYPES OF ORCHESTRATION FOR SDN AND NFV

Each NFV use case or SDN network domain requires an orchestration system, and when the operator wants to coordinate 2 or more domains, a multi-domain or cross-domain orchestration system is required. And therein lies the fertile ground for the growth of layers of orchestration systems that will inevitably spring forth to help automate network operation from services to the physical network.

The ultimate multi domain is the entire network and all the services delivered, which will require a master uber orchestrator or orchestrator of orchestrators. Orchestration systems will coordinate multiple vendors' software and hardware, and therefore vendors want to be in the controlling position of providing the uber orchestrator; if not careful, operators can find themselves in a vendor lock-in situation once again...but more about this later. In a few years, it will be obvious that a few giants will be competing for this uber orchestration position as the orchestrator of orchestrators in service provider networks.

Orchestration has been around a long time, but it's just more complicated with the heterogeneous physical network systems found in operator networks. Orchestration increases automation by coordinating the interactions and services flows among various parts of the network, giving guidance to other orchestrators and controllers. It's the controllers that tell the equipment what to do. The orchestration-controller hierarchy is similar to the change from 3G to LTE: in 3G, the Radio Network Controller (RNC) tells the NodeB what to do, but in LTE, this has changed to having no RNC; the RNC function is directly in eNodeBs and is coordinated through a distributed self-organizing network (SON) acting as orchestrator, and a centralized SON acts as orchestrator of orchestrators.

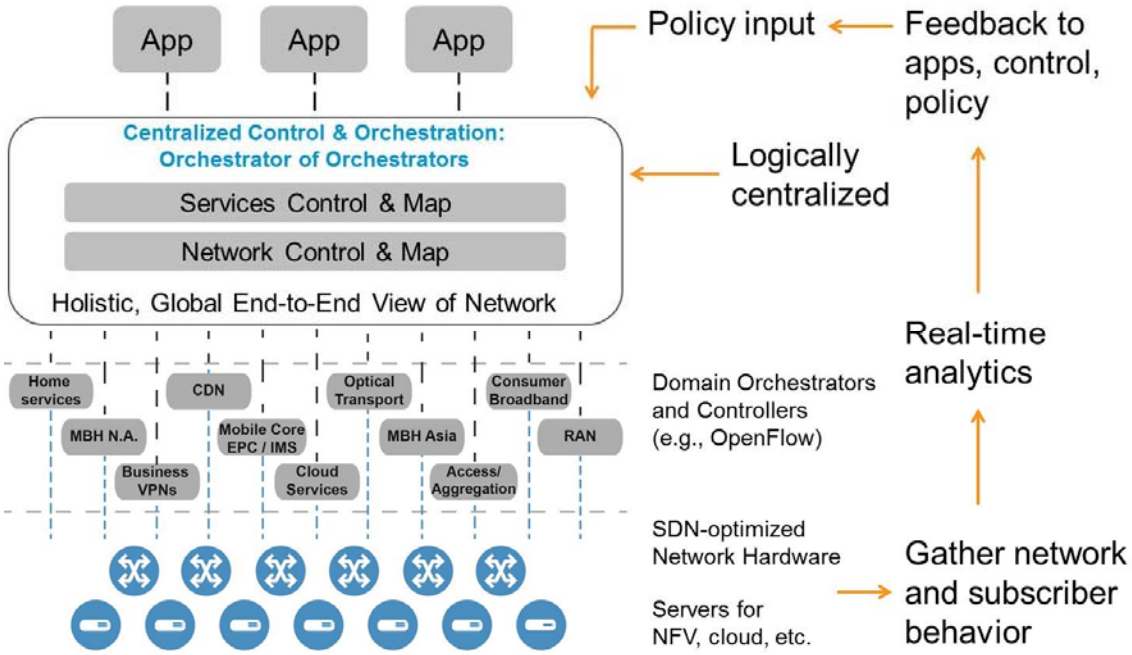
SDN and NFV orchestration can be organized into 2 types:

- *Service* orchestration; e.g., setting up an IP VPN among several sites of a business or delivering a specific set of firewall and IPS/IDS service options to a customer
- *Infrastructure* orchestration; e.g., using Open Stack for servers, storage, and switches

ORCHESTRATOR OF ORCHESTRATORS—THE GRAND VIEW THROUGH 2020

During the past 3 years, we have worked on what markets will look like as SDN and NFV matures. By 2020, we believe that the SDN network architecture will start to resemble the diagram in Exhibit 1 below. I vetted this architectural view in 2012 and 2013 with many SDN and NFV experts at key service providers and manufacturers in the industry, so we believe it is sound. (See our April 2013 analyst note, *2020 Foresight: SDN Network Architecture; SDN ≠ OpenFlow.)*

Exhibit 1 **SDN/NFV 2020+ Architectural Roadmap**



Service provider goals for SDN and NFV include achieving a holistic view of their networks and service agility across their networks. But to do this, the network "control constructs" must be distributed. In fact, with the multitude of applications and domains (e.g., consumer broadband, mobile backhaul, mobile packet core, and business VPNs), control cannot reside in a single monolithic magic software orchestrator or controller; rather, a hybrid architecture is required with distributed domain orchestrators sharing a global view of the services and network provided by an orchestrator of orchestrators or controllers.

By 2020, we believe that the SDN and NFV network architecture will comprise 5 key components:

1. Network applications
2. Centralized control and orchestration—an Orchestrator of Orchestrators
3. Distributed domain orchestrators and controllers
4. Network infrastructure—SDN-optimized network hardware, servers/storage/switches used for NFV
5. Instrumentation, data analytics, and feedback to policy, apps, and control—key to automation

Network Applications

A major purpose of SDN and NFV abstractions is to bury complexity and make services and the use of the network simpler without invoking the management and provisioning software of the many manufacturers deployed in the network. The goal of SDN and NFV is to make the construction and/or writing of applications and creation of services simpler and more direct.

Centralized Control and Orchestration Has the Global Holistic View of the Network for Services and Infrastructure

Applications will make requests to the services control and map layer for services or information; this layer must have knowledge of the existing network services. Apps will not connect directly to the network infrastructure to obtain information such as “what is the status of port 3 on the module in slot 5 of a router in Los Angeles,” so there must be a services layer. Of course, to deploy services in a network, such as an IP VPN among various sites for a business, a network services control and map is needed to put the IP VPN in place across the physical network of router and optical layers.

Distributed Domain Orchestrators Direct the Controllers

Although the "big view" orchestrator of orchestrators has network-wide, end-to-end overview, all the intelligence of a carrier network cannot be assembled into a single piece of software. The principle of "divide and conquer" applies here, and a domain orchestrator has the network intelligence necessary for its contained domain, such as mobile backhaul, transport network, IP VPNs, content delivery networks (CDNs), and the like. After the services control and map translates service requests from apps into network requests to the network control and map, then requests are made to a distributed set of "contained domain" orchestrators. The domain orchestrator communicates with a set of SDN controllers that communicate commands to the equipment. OpenFlow could be used as the SDN protocol by any of the SDN controllers in that layer of our diagram to send OpenFlow commands to SDN-capable network hardware.

The Physical Network Architecture Is Composed of Network Hardware Such as Switches, Routers, and Optical Transport

By 2020, most networks will have optimized SDN-capable hardware. Controllers will make requests to the hardware to direct traffic flows or extract status information. To ensure that the hardware is SDN-capable at high levels of performance, there will need to be changes made to the silicon, and this process is already underway.

Servers and storage are also a critical part of this infrastructure where the virtual network functions (VNFs) of NFV will be executed.

Instrumentation, Data Analytics, and Feedback to Policy, Apps, and Control Are Key to Automation

To achieve automation, the network must be instrumented in the data plane to track bulk and application traffic flow patterns and subscriber behavior. Real-time analytics will be used to extract, mine, and refine pertinent information, which goes to the policy functions to send policy directions back into the orchestration layers to self-regulate, self-optimize, and relay important network status changes, as well as deliver SLAs and good QoE to paying customers.

SDN controllers based on Open Flow were the catalyst that forced operators and vendors to examine SDNs as a way to gain a global view of the networks and move control and network functions to servers and software for increased agility. Once the industry accepted this view, the need became obvious for orchestration, a services control layer, and a network control layer that communicate to distributed domain orchestrators, which in turn must ride SDN controllers. In this new view of the network, a set of distributed domain orchestrators communicates with SDN controllers that communicate directly with equipment. OpenFlow-based SDN controllers are just one type of domain controller, which are part of this much bigger 2020 architecture picture.

BUT WHERE ARE WE NOW? ORCHESTRATION FOR CONTAINED DOMAINS

Service provider networks are so complex and are composed of so many different network service domains that there is no feasible way to deploy a single “orchestrator of orchestrators” today. To achieve that broad end-goal, vendors would have to somehow embed the intelligence of running a comprehensive carrier network into that orchestrator, and that’s simply too big a task.

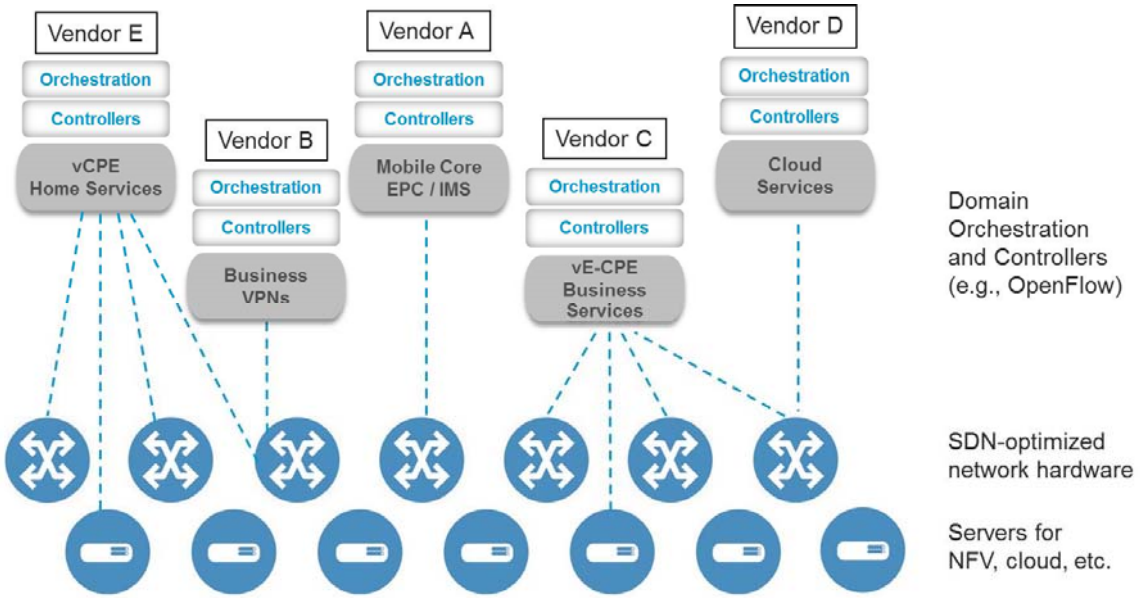
This complexity is solved by distributed domain orchestrators, whose purpose is twofold:

1. The intelligence of each domain needs to be in a separate orchestrator.
2. The best way to solve specific problems is by decomposing the problem into smaller parts covering specific network segments. Carriers have taken this approach to the point that the ETSI has catalogued 20+ proof of concept (PoC) tests, tens of private and public tests, and field tests that are localized in a contained domain.

An example of this is in Exhibit 2. For each of the domains in which carriers are doing PoC tests, it appears that they are selecting the orchestration system from a single vendor even though most often software and hardware from multiple vendors is involved. We believe that this multi-vendor, multi-layer situation in a single domain, with a single orchestration tool, will be commonplace for the next 2 to 3 years. For this reason, almost every manufacturer that has entered the SDN/NFV market has its own orchestration software, or they are partnering with another vendor that does.

We are seeing some PoC trials that are combining 2 domains, but those will be very limited over the next few years. Ciena, NEC, and Cyan have demonstrated the ability to deliver a single orchestration system that can manage at least 2 domains.

Exhibit 2 SDN-NFV 2014–2017 Steps toward 2020—The Evolution Begins



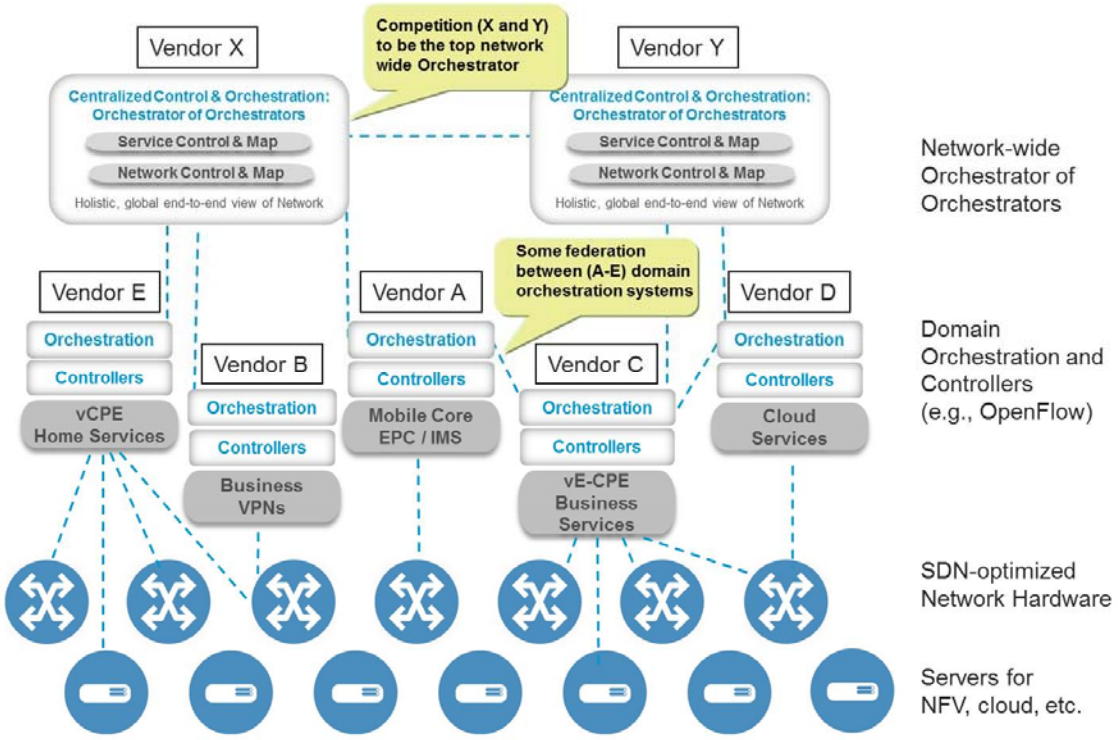
EVOLUTION OF ORCHESTRATION TOWARD 2020+

In Exhibit 1, we showed that the goal is to have orchestration and control across the entire network. It is not yet known exactly how the industry will achieve that. In Exhibit 3, we show how vendors' orchestration systems will have to be able to communicate with the orchestration systems of other vendors. We believe there are 2 likely scenarios as the orchestration evolution shakes out:

1. Software companies will have no hardware bias. This is where NFV is the initial logical focus. Prominent vendors in this scenario will include AMDOCS, Oracle, IBM, VMware, and some smaller companies such as Clearpath and others. Other players will include the OPNFV group and ON.Lab.
2. Large hardware vendors will deliver SDN and NFV orchestration. We believe that Huawei and Ericsson are among the top contenders in this scenario, though many other companies—like NEC, Cisco, Brocade, Alcatel-Lucent (Nuage and CloudBand), HP, Nokia Networks, Juniper, ZTE, and smaller manufacturers, such as Cyan, Overture Networks, Telco Systems, and MRV—are already playing in the NFV/SDN orchestration space.

Federation will occur between domains through a pair of orchestrators—essentially to coordinate from one domain to the next. More likely, a multi-domain orchestrator will be used to coordinate the domain orchestrators. The next step is to build a multi-domain orchestrator that coordinates many domains, which would be needed, for example, to effect an IP VPN for multiple customer locations across router, CPE, access, aggregation, and optical.

Exhibit 3 **2017–2020 Orchestration Evolution toward an Orchestrator of Orchestrators**



CONSIDERATIONS WHEN CHOOSING ORCHESTRATION SOFTWARE

Many carriers are currently in the midst of PoC tests or field trials, with the goal of moving toward commercial deployments of SDN and NFV. In 2014, about 10 commercial SDN- and NFV-based services were deployed, and we expect another 15 in 2015. These early trials are most commonly in contained domains—initially implementing the technology in just a small part of their network—which gives carriers the opportunity to see how the technology interacts in the network and learn more about the practical applications they may run into.

As carriers develop and refine SDN and NFV in these contained domains, they often choose an orchestration system from a single vendor. However, they must be cautious that they don't get locked in to a specific vendor when their longer-term goal is having an orchestrator of orchestrators that can work across a variety of domains. In these contained domains, once an orchestration system is installed, it's difficult to change once it's being used to actually serve customers. If the orchestration system is proprietary in any way, then the carrier has just bought into vendor lock-in, and it will be a significant challenge to unlock the system for something more open as SDN and NFV implementations grow.

To prevent vendor lock-in when choosing an orchestration vendor and/or platform for a single contained domain, we recommend the following considerations:

- Make sure the orchestration software is open in terms of industry standard interfaces, including northbound, southbound, and east-west for federation with other orchestrators
- Evaluate orchestrators based on open source software
- Be aware of the many flavors and types of openness; e.g., a vendor's own APIs can be open to others even though they are not industry standard or industry accepted (such as in open source)
- Look for vendors that embrace the principles of openness, fully supporting industry accepted APIs and best practices

We recommend that service providers evaluate vendors in light of the above considerations, including how public/published the interfaces are and the vendor's stance on these interfaces.

BOTTOM LINE

Service providers want to leverage SDN and NFV to achieve a holistic, global view of their network—with visibility up and down the network layers and across the various domains of the network—regardless if the underlying equipment is from multiple vendors.

Service providers are reaching for agility to deploy new services or service variants with dramatically shorter time-to-market and for the ability to optimize network traffic, increase automation, and reduce capex. Enough said for the grand goals of NFV and SDN—now we have to get there from here.

To learn more, join Infonetics and Juniper Networks **Thursday, February 12, 2015 at 11:00 a.m. Eastern** for a free, live webinar, *Choosing the Right SDN-NFV Orchestration Platform for the Job*, or watch the replay. Both can be accessed at:

http://w.on24.com/r.htm?e=916853&s=1&k=6BDA738384AF3BD6DDE5CD9FDB4B1376

REPORT AUTHOR

Michael Howard

Principal Analyst, Carrier Networks

Infonetics Research / IHS Inc.

Michael.Howard@ihs.com +1 408.583.3351

Twitter: @michaelvhoward

ABOUT INFONETICS RESEARCH

Infonetics Research, now part of IHS Inc. (NYSE: IHS), is an international market research and consulting analyst firm serving the communications industry since 1990. A leader in defining and tracking emerging and established technologies in all world regions, Infonetics helps clients plan, strategize, and compete more effectively.

REPORT REPRINTS AND CUSTOM RESEARCH

To learn about distributing excerpts from Infonetics reports or custom research, please contact:

North America (West) and Asia Pacific
Larry Howard, Vice President
Larry.Howard@ihs.com +1 408.583.3335

North America (East, Midwest, Texas), Latin America and EMEA
Scott Coyne, Senior Account Director
Scott.Coyne@ihs.com +1 408.583.3395

Greater China, Southeast Asia, and India 大中华区及东南亚地区
Jeffrey Song, Market Analyst and Account Manager 市场分析师及客户经理
Jeffrey.Song@ihs.com +86 21.3919.8505