SDN 2.0: Monitoring, Analytics, and Automation

Building closed-loop automated networks with software-defined tools

Featuring: Pluribus NETWORKS

Key Findings

- **The software-defined networking (SDN) market is entering a new stage that will integrate telemetry, monitoring, and analytics to deliver increased automation.** Large network operators are now moving toward platforms that can collect large amounts of telemetry data to drive analytics and automation.
- **Service providers see SDN 2.0 as a key driver of automation.** Interviews with leading service provider architects indicates they see the marriage of SDN platforms with real-time monitoring and big data analytics as a key driver for automation.
- **SDN integration with hardware underlay is a critical feature.** SDN software-only overlays are important, but integration with the hardware and OS will be critical to delivering automation and self-healing networks, as indicated by recent adoption plans.
- **Monitoring tools are being integrated with leading SDN platforms.** The drive to automate large-scale service provider networks will drive more integration between monitoring and telemetry tools with SDN platforms.
- **Network monitoring and network packet broker (NPB) functions are now SDN features.** This trend is likely to accelerate, therefore look for monitoring and NPB vendors to partner or seek integration deals with leading SDN platforms.
- **Intent-based networking (IBN) will be a key function that will enable further automation of SDN platforms.** Higher level analytics functions will set the state for IBN and automation.
- **SDN startups such as Apstra, Big Switch, and Pluribus Networks are making inroads.** Despite long-held skepticism of SDN startups, these companies are gaining traction with both large enterprises and service providers. They could be prime acquisition or IPO candidates as operators accelerate their interest in fully featured SDN solutions that aren't tied to specific hardware platforms.

Table of Contents

I. Introduction: What's Next for SDN

The revolution will be automated

Big changes have come to networks, driven by the cloud and a boom in web applications. This has changed the game for large network operators, making networks larger, more complex, and mission-critical than ever before. Cloud-scale operators such as Amazon, Facebook, and Google, and Microsoft pioneered techniques in software-defined networking (SDN), including the separation of the forwarding and control plane for networking as well as the "disaggregation of hardware and software components, to scale their networks and become less reliant on proprietary hardware. This trend has now taken hold with large enterprises and service providers, who have adopted cloud-scale SDN techniques to deploy new services with more agility and scalability, using cloud-based platforms known as network functions virtualization (NFV).

But what's missing — and what's next? As service providers and large network operators such as cable companies and large enterprises look to mimic the accomplishments of the cloud-scale providers, they have significant challenges in building SDN and NFV networks. The end-goal is higher levels of automation in the network, whereby a network can monitor and detect faults and resolve them with less human intervention. Futuriom calls this evolution SDN 2.0, which will require the following components:

- Integration of monitoring and telemetry with SDN and NFV to aggregate network intelligence and give a full view of what's happening with network connections and applications
- Analytics platforms to process network telemetry and drive automation
- A move to intent-based networking (IBN) and intent-based analytics (IBA) models that enable network programmability based on the intent, rather than state
- Further integration between SDN software and network hardware (underlay) to create fully programmable network fabric

As vendors ramp up their marketing efforts, everybody is making sure to include many of these buzzwords — telemetry, IBN, underlay, and SDN — in their slides. The truth is, however, that this is a mammoth undertaking that will require many years as well as integration and cooperation among vendors in the industry.

Large network operators such as communications service providers say that progress has been made in driving automation and analytics into networks. For example, AT&T recently said it plans to have 75% of its network virtualized by 2020. However, many large service provider technologists point to the complexity and size of this undertaking as they seek to "cloudify" their networks and drive automation.

Futuriom has spent months studying these trends, talking to dozens of vendors and end- users at major network operators. While it's clear that end users are accepting some of the vendor vision for where SDN and NFV will go to achieve SDN 2.0, they are challenged by integration tasks that require them to meld sophisticated monitoring, telemetry, analytics with the network underlay to create full-fledged SDN 2.0 and achieve real network automation.

"The telcos need to focus on operations and let's face it we're behind," said Deutsche Telekom VP Axel Clauberg in a Futuriom interview. "We need to revisit how we are operating the network and managing services and it is part of a large transformation."

A key to achieving these goals will be the role of network telemetry and monitoring as they are integrated into the network hardware and software. "I see more embedded monitoring going forward," says Clauberg.

This process will require further integration of network hardware, software, analytics, and monitoring functionality. End users have three choices in this process: 1) Buy existing solutions from vendors 2) Build their own software 3) Use some combination of the two. In our discussions and surveys of end-user sentiment, it's clear that many network operators — including both enterprises and service providers — do not feel they have the resources or expertise to build their own network hardware and software, so they will look to the vendor community to integrate tools to drive telemetry, real-time monitoring, and analytics into SDN platforms to help them achieve SDN 2.0.

How will that happen? Let's delve into the drivers and requirements.

II. Market Drivers for SDN 2.0

The original vision of SDN derived from a need to scale out hardware more quickly, without requiring the complex provisioning required by many proprietary network schemes. Google was among the first to detail its SDN scheme, which involved stringing together hundreds if not thousands of commodity-based networking boxes and controlling them with software. The growth of Google's back-end (east-west) network quickly surpassed the demand of user-facing network. This growth was expensive because the network didn't scale as economically as storage and compute. Google believe that by separating hardware from software, the company could choose hardware based on required features while being able to innovate and deploy on software timelines. Second, it provided a more deterministic and fault-tolerant networking platform. It also allowed Google to drive automation with monitoring, management and operation of the individual boxes and applications.

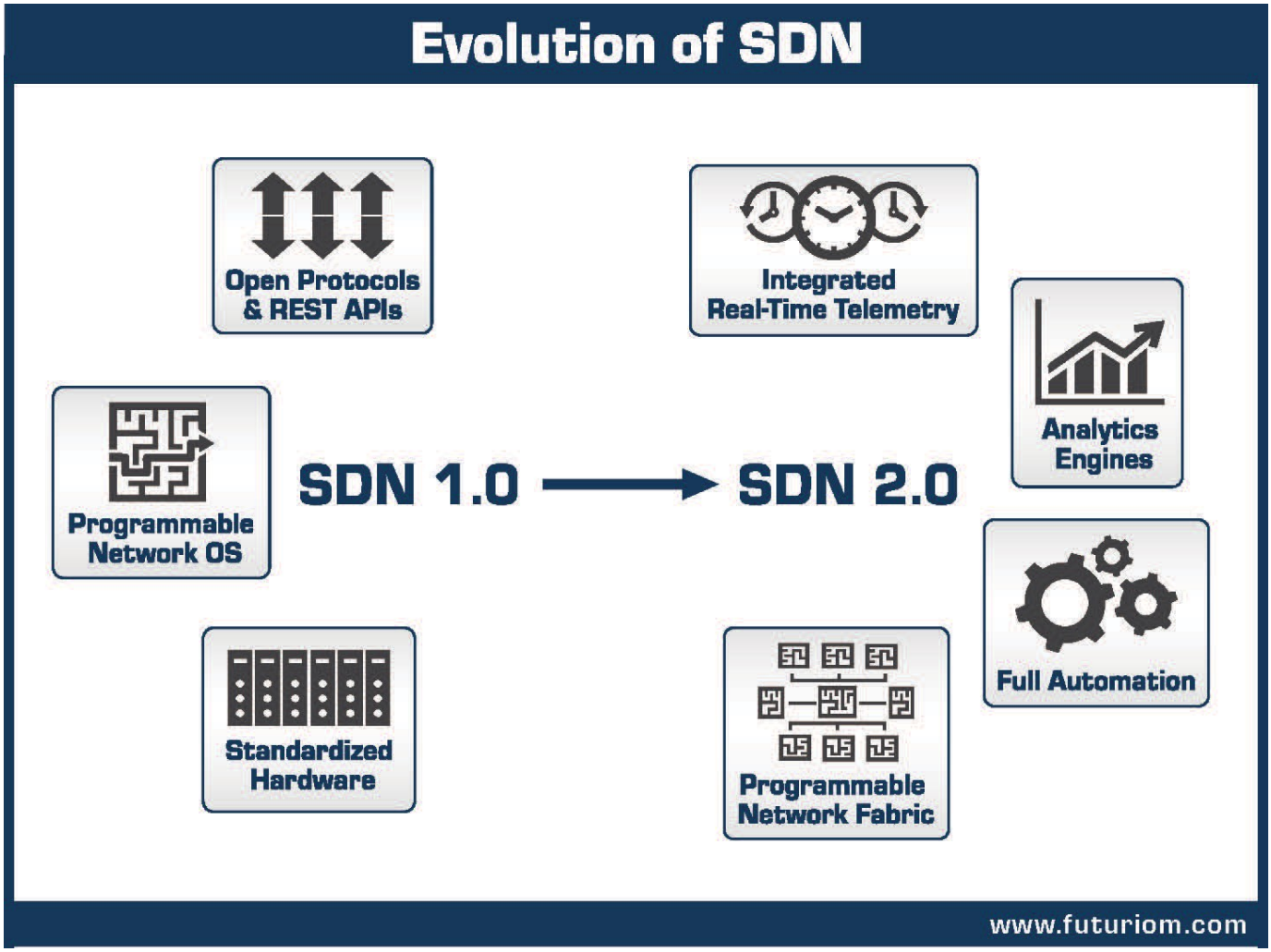
Most of this vision is still intact, but the service provider and large enterprise network operators have found that this goal more challenging, without the resources or technical expertise of a cloud operator such as Google. Additionally, service providers have more legacy network infrastructure to support, rather than just focusing on building new greenfield data centers.

The feedback that Futuriom has heard from the service providers and large network operator community over last three months is that they are just starting to push SDN toward more extensive network automation. But this will require more integration between the variety of SDN tools, including SDN network fabrics, monitoring products, and analytics.

We're just in the start of the SDN journey," Mattias Fridström, Chief Analyst of Telia Carrier, told us recently. "If you talk to us in three months time we will be much more automated." Fridström says the enables will be connecting real-time telemetry to analytics to drive automation

Most enterprises, except for the largest ones, don't have the resources or scale to build their own custom SDNs. Even services providers, regardless of size, are rethinking whether they want to be in the cloud software design business — and they are working closely with startups and vendors to deliver integrated SDN 2.0 solutions.

The vision is for large network operators to deliver a heterogenous networking environment with real-time monitoring and telemetry, which can connect with analytics sotware to enable more sophisticated automation. In achieving these goals, network operators hope to save significant amounts of money in both capital expense (capex) and operating expense (opex). The chart below shows how SDN is evolving



In conclusion, here are the drivers and goals for SDN 2.0:

SDN 2.0 Drivers

- Need for standardized network hardware with open APIs to drive a scale-out architecture
- Need for more pervasive, integrated real-time monitoring and network telemetry
- Direct connection and communication to hardware fabric (underlay)
- Need for automation through configuration, analytics, and programmability
- Providing software-based agility to launch new services.

SDN 2.0 Goals

- Improved visibility
- Improved security
- Reduced opex through simplified operations, including integration with cloud
- Capacity and resource planning
- Cost control by optimizing network resources
- Improved user experience

III: Requirements for SDN 2.0

Telemetry, APIs, and Standards

The SDN and network landscape has become complex. Part of that has been brought about by the messy migration to virtualized networks in which they are no longer defined by a set of management interfaces (often proprietary) on a specific manufacturer's box but by a wide range of data protocols and APIs, often stretching the boundaries between traditional networks and the cloud.

At the same time, network managers are suffering a cultural revolution, in which the tools of cloud, such as DevOps and open-source Linux programming, have started to infiltrate the network world, which has long depended on knowledge of specific hardware management platforms and command-line interfaces (CLIs). The cloud world has pushed the network world toward more flexibility — moving from closed, proprietary systems that don't like to share to more open systems to consume and exchange data.

So how does all of this work together? It comes down to wiring up the network with a wide range of capabilities to exchange data and configuration information with networking standards and application programming interfaces (APIs). This data exchange is the connective tissue of SDN — the capability to share data and configuration information between platforms.

Data Models for SDN 2.0

One of the key trends in service provider and large enterprise networks is the move toward data-driven infrastructure to make it easier to program and configure hardware. These data models also make it easier to feed analytics programs to build an automated system.

The data-model trend means there is more configuration, traffic, and flow data available than ever before -- whether the networking platform is open or proprietary. This information comes from a wide variety of standardized network protocols and data models such as SNMP, YANG, Netconf, NetFlow, and vendor APIs. This data can include hardware information from the CPU or memory, data on jitter and packet loss, or error log messages. The key is the capability to collect as much data as possible and then program a way to process and react to this data in an automated fashion, rather than requiring network operators to respond to error logs manually. With the advent of cloud and SDN, networks are propagating more data than even, including applications data from APIs. SDN 2.0 solutions will aim to solve this by being programmed with traffic analytics, and eventually intent, that can analyze this data in real-time and make automated decisions to respond to problems. All this means a trend toward real-time data collection and analytics to improve security, capacity planning, monitoring, and troubleshooting

"The first step was to get into data-model driven management," DT's Clauberg told us. "We started with YANG and Netconf. The point was how to build on top of that. How to build end-to-end service orchestration. Once you have the foundation with the data models, you bring in big data event management, automation remediation with AI, and in the end you will have full automation."

So what, specifically, is being used? Based on survey data gathered by interviewing end users and vendors, Futuriom has determined that the following network protocols, data models, and APIs are the most commonly used to gather the network telemetry and configuration data needed to drive network analytics and automation:

APIs: Networks are using a wide range of APIs, including vendor-specific REST APIs allowing access to confirmation and operational data for specific vendor hardware. The opening of REST APIs to proprietary hardware has been one of the key enablers of SDN 2.0, facilitating the programmability of a heterogeneous network.

Data Models: Data models such as Netconf, YANG, and TOSCA have risen in popularity by enabling orchestration tools to automate configuration of network devices and software.

Network Management & Monitoring Protocols: Network protocols and standards such as SNMP, NetFlow, OpenFlow, SFlow and JFlow have enabled open, shareable data on network status. This data can be used by SDN, NFV, management and service assurance platform to build real-time status information on the network.

Unix Tools: The cloud world has infiltrated networking. SDN systems are increasing leveraging data generated by the systems of the server world, using Syslog and other Unix tools.

What's interesting is that this movement has blurred the lines between an "open" and "proprietary" platform. Even the most proprietary platforms have become more open through the publishing of APIs and the adoption of common data models. Some network operators may standardize on one platform. Others build customized monitoring and analysis interface. As one service provider network architect told, it boils down to one thing: Building networks with more data gathering capabilities.

"I want streaming data about the status of the box and don’t wait to wait for it to fail," Bill Walker, director of network architecture at CenturyLink, told us in an interview. "We use Syslog (and other Linux tools), SNMP, and we are looking at NetFlow, Netconfig, even OpenFlow telemetry. We are spending a lot of time around localized information so that we can keep the data localized and not send it to a central place to be analyzed."

Operators want as much data and telemetry from boxes as possible. This data forms the basis for more advanced goals such as analytics, IBN, and automation.

Standards Groups Developments to Watch

In addition to the extensive use of APIs and network management protocols, a number of standards organizations are working on create new standards for interoperability among service providers. These will be important for enabling SDNs that can span the WAN, from data center to data center or across clouds. It's easier to create an SDN in the closed environment of one cloud platform, but harder to manage an SDN that spans multiple service provider networks. To provide full automation, network service and control will need to be implemented across domains and clouds (e.g. carrier-to-carrier, or IP to optical), which requires industry standards.

Several groups are working on such standards. One of the more recent industry developments is the MEF's introduction of the MEF 3.0 framework at its annual event in November of 2017, the MEF introduced a new group of standards for carrier-to-carrier networks for dynamic Carrier Ethernet, wavelength, IP, SD-WAN, Security-as-a-Service, and other virtualized services that will be orchestrated over programmable networks using Lifecycle Service Orchestration (LSO) APIs. The goal is to enable service orchestration of across multiple providers and over multiple network technology domains (e.g., Packet WAN, Optical Transport, SD-WAN, 5G, etc.). This will be important for implementing SDN automation in cloud-to-cloud configurations.

A large number of service providers have embraced the effort, including CenturyLink, Charter Communications, Colt, Orange Business Services, PCCW Global, Tata Communications, and Verizon, among others.

Jeffrey Schwartz, Associate Vice President, Managed Network Services and Cloud Enablement, Tata Communications, summarized the goals of MEF 3.0, in a recent statement for the MEF conference held in Orlando, Fla. in November:

“At Tata Communications, we want to make cloud adoption more seamless for enterprises through the automation of service delivery and greater application-level control. We’re committed to the development of industry standards such as MEF 3.0, harnessing our networking and cloud expertise and partnerships in the global technology ecosystem to help accelerate digital transformation in enterprises worldwide.”

Some of the key industry standards organizations focused on large enterprise and service provider networks are outlined below.

ETSI

The European Telecommunications Standards Institute this year published six new specifications governing the use of network functions virtualization (NFV) services, which enable operators to deploy services on a virtualized infrastructure. Because SDN will be used to configure and connect NFV platforms, it is important to track how NFV platforms connect to SDNs for management, monitoring, and analytics.

For example, the new ETSI NFV specifications defines APIs enabling multivendor interoperability for service deployments, according to ETSI. For example, these standards could be used to define how to configure security and SD-WAN services using NFV. ETSI says it is also working on standards for interoperability with Operations and Support Systems (OSS) in carrier networks, with the formation of a new Zero-Touch ISG group.

IETF

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers that has guided the Internet architecture and development of important standards. The most famous of these, of course, is Internet Protocol (IP). The IETF is involved in a wide range of standards governing the developing of the Internet. Some of the important networking standards it has created include MPLS, OSPF, and SIP.

While the IETF largely concerns itself with IP-based technology, it has a group looking at SDN, known as I2RS, which has done some work on southbound programming protocols, NFV and network service chains.

The Linux Foundation

The Linux Foundation oversees an immense range of open-source projects and standards focused on cloud computing and open-source software. Many of these are focused on SDN in the operator environment, including the carrier operating system project ONAP, SDN controller Open Daylight (ODL), OpenFlow, and CORD, which is a model for building cloud platforms for NFV.

The Linux Foundation has been consolidating many SDN projects and tools, most notably OpenFlow, CORD, ONAP, and ODL, which are being used to build virtualized infrastructure in carrier environments. This is an important role and further consolidation is welcome as it can help operators try to manage "standards sprawl" with open-source projects proliferating

MEF

The MEF is working with many of the world's leading service and technology providers, open source projects, standards associations, and enterprises to realize dynamic services orchestrated across automated networks.

The MEF 3.0 services framework family includes dynamic Carrier Ethernet, wavelength, IP, SD-WAN, Security-as-a-Service, and other virtualized services that will be orchestrated over programmable networks using LSO (Lifecycle Service Orchestration) APIs. The LSO Reference Architecture enables the standardized of LSO APIs that enable orchestration of services across multiple providers and multiple technology domains (e.g., Packet WAN, Optical Transport, SD-WAN, 5G, etc.). This will be important for implementing SDN automation in cloud-to-cloud configurations.

The Open Compute Project (OCP)

The Open Compute Project (OCP), is a community of technology leaders in the cloud computing environment which has been driving standardized hardware, software, and equipment design for cloud data centers.

The OCP's original focus is pure hardware, with standards for elements such as power supplies, server racks, and battery backup systems. But it has branched out into other areas, such as a universal customer premises equipment (CPE). The main goal of OCP is to drive standardized components that can be used to build cloud services.

TM Forum

The TM Forum works closely with service providers and other carrier standards groups such as the MEF to define carrier interoperability, which as discussed will be increasingly important to guiding connectivity of SDN and automation between clouds and carrier networks. The TM Forum maintains a suite of 50+ REST-based Open APIs collaboratively developed to be used in service provider networks. Many of these APIs are useful for monitoring and fault management. Some examples of the TM Forum APIs include the Alarm Management API, Customer Management API, Performance Management API, and Resource Function Activation and Control API.

In an important recent development, the TM Forum is cooperating to insure interoperability between the MEF's LSO and MEF 3.0 framework and TM Forum's Open API framework. The goal is to create standardized APIs to enable SDN architectures from different network service providers to interoperate with each other. The increased cooperation between the MEF and the TM Forum is encouraging because many service provider experts have regularly expressed concern about the volume of standards organizations and consolidation and cooperation should help streamline the process.

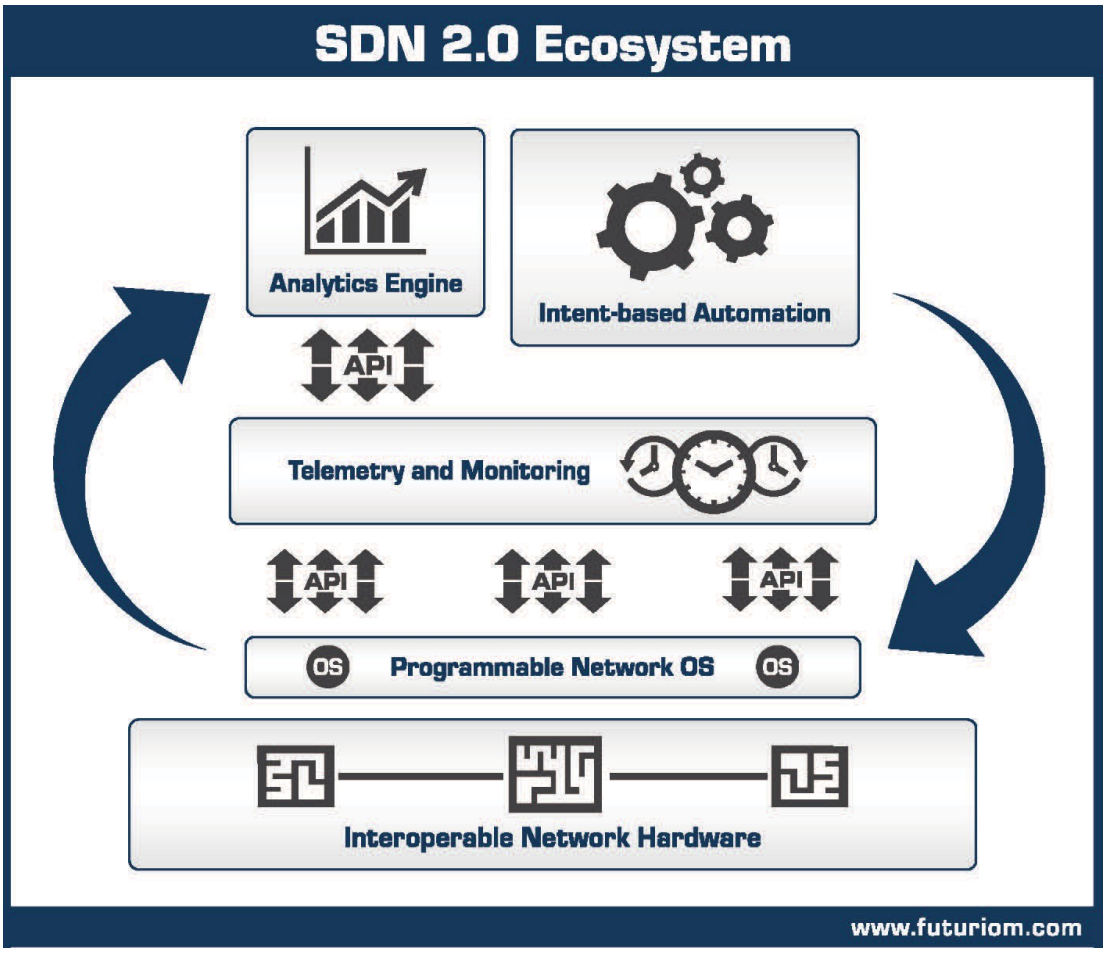
IV: The SDN 2.0 Ecosystem

Technology component and functions

Putting all the components together to create a close-loop automated SDN is no easy task. Right now, large operators are accomplishing this by integrated a collection of monitoring, analytics, and networking tools -- including both open-source and vendor products.

Futuriom believes it's likely that SDNs will evolve over time much like the Linux server and virtualization ecosystem: Vendors will emerge as integrators for the operators, helping to package and test elements to work together.

The chart below describes how the SDN ecosystem is being built for large network operators and service providers. The following section provides detail on recent vendor developments in particular areas.



Networking Fabric Systems and OSes

SDN networking systems help integrate monitoring, analytics, and network fabric functionality to build a living and breathing network than can respond to changes in applications flows and faults. To build this, you first need an integrated SDN fabric with as much telemetry and network "awareness" as possible. The trend in the industry is increased integration between the softare overlay and the underlying networking hardware OS (underlay).

Initially SDN was about disaggregating software and hardware components so that heterogeneous systems could be built using software overlays, mixing and matching a hardware box, OS, and software networking overlay. **VMware**'s NSX was the first dominant SDN software overlay, and it is still a leader today with a billion-dollar run rate. However, **Cisco Systems** has made strides with its applications centric infrastructure (ACI), which integrates an SDN system with a hardware underlay. But in some cases these two systems are used together, to integrate the functionality of both the underlay and the overly.

Some operators have concluded to full control and visibility requires integration with the hardware underlay. This has led a resurgence in SDN startups that provide both a software overlay with integrated OS underlay.

Startups such as **Pluribus Networks** have gone all-in on underlay integration, featuring its own OS that runs the network fabric and is integrated with analytics and monitoring applications. Recently, Pluribus made waves when it was revealed that it was the underlying networking infrastructure for **Ericsson**'s HDS8000 network functions virtualization (NFV) platform.

Big Switch Networks also implements a proprietary OS on commodity hardware, producing integrated systems including a partnership with Dell. It is using a modular approach to delivering its SDN, which splits its Big Cloud Fabric, the networking software, and the Big Monitoring Fabric (or "Big Mon"), which delivers monitoring and security applications.

Arista Networks has been focused on selling its own switching systems rather than loading SDN software on commodity hardware, which makes some SDN purists say it's not an "real" SDN company. But one could argue that Arista's operating system, EOS, was the first to enable interoperability with other hardware by enabling the extensive use of APIs. Arista has delivered a series of monitoring applications, including CloudVision Analytics and Telemetry Apps. It uses open APIs and networking protocols including eAPI, YANG, NETCONF, RESTCONF, and gRPCand.

Orchestration and Automation Platforms

Anuta Networks markets the NCX Network Service Orchestrator platform, which abstracts configuration information by accessing IETF standard YANG service models on network devices. It allows operators and network managers to orchestrate devices from 35+ vendors using their individual API and CLIs. NCX also enables custom device, service, and operational models with YANG. Once the network is mapped, the software generates up-to-date configuration and topology diagrams for audit and compliance initiatives. Then, specific applications monitor and analyze network behavior, including the verification of connectivity and security policies.

Apstra is one of the newer SDN startups on the scene, delivering a management and automation platform that abstracts network data and sits above the hardware layer. Apstra pioneered the concept of IBN, which uses a combination of telemetry and analytics to drive the network programmatically. It also has the capability to integrate layer 2 overlay running on a layer 3 underlay using hardware APIs, acting as a configuration platform for heterogeneous networks. Sources have told Futuriom that some leading service providers are looking at Apstra to automate the configuration of underlay networks as they move to cloud-based platforms such as NFV.

Forward Networks is another SDN 2.0 software and automation company that is looking to use IBN to model the automation of network configuration. Forward Networks securely collects data about configuration and network state from all network devices via SSH, issuing a series of CLI commands. Once the network is mapped, the software generates up-to-date configuration and topology diagrams for audit and compliance initiatives. Then, specific applications monitor and analyze network behavior, including the verification of connectivity and security policies.

Network Monitoring, Performance Management (NPM), and NPBs

Network monitoring systems and telemetry are key to the collecting the right data on network functions and applications that can be used by analytics programs to drive network automation. This has been a particularly active area for vendors in recent years, as they position themselves to sell sophisticated monitoring products that can be adopted for SDN and NFV products. It's also a large and complicated space that includes sometimes discrete components such as network performance management (NPM), TAPs, networking monitoring tools, and NPBs -- only a small segment will be adapted for SDN and NFV. The foremost requirement is functionality that can be delivered in software, which is limiting to many of the monitoring companies that are geared toward specialized hardware devices.

NPM is a gigantic category that includes many performance monitoring and management tools. For the purposes of this report, we will only comment on the general trend of this category and how it relates to SDN with specific recent developments. Futuriom believes that packet flow data will eventually be built into the SDN fabric, obviating the need for these tools in many networks. As of

today, many SDN platforms require third-party NPM and monitoring tools. Some key provider of NPM products include **CA**, **Cisco**, **NETSCOUT**, **Viavi**, and **SevOne**. Many of these products focus on collecting network and flow data supplied by protocols such as SNMP, Netow, or Sflow, analyzing the network performance, and helping to diagnose problems and possible solutions.

A packet broker can be a discrete network component that literally brokers packets — it has the capability to duplicate packet traffic from the network and manage how it is processed in valued-added applications such as NPM analytics and security products. Some of the leading packet broker solutions come from **Big Switch**, **Gigamon**, **Viavi**, and **NETSCOUT**. The packet broker market has grown fast, driven by the need for monitoring packet data, especially for security purposes. While the packet broker product category is likely to be viable for some time in enterprise, it will likely be threatened in larger enterprise networks and service provider networks by SDN products that are integrated the functionality into the network fabric itself. This is already happening as products such as **Pluribus Networks**' Netvisor, which integrates packet visibility, and **Big Switch**'s strategy to sell packet broker as a separate application that can be used with its SDN fabric. The question this leaves is whether packet broker is a separate product category in the SDN world, or merely a feature. Over time it's more likely to be subsumed into SDN fabric capabilities.

Service Assurance Tools

Service provider networks often require highly specialized service monitoring and service assurance products to deliver Quality of Service (QoS) and enforce service-level agreements (SLAs). Some of the vendors in this category include **Accedian**, **CENX**, **Infovista**, and **NETSCOUT**. Sometimes these products include special software probes or even specialized hardware (network interface cards) to be plugged into the network to provide granular network telemetry. This category is also at risk at being integrated into an SDN fabric, and Futuriom believes that the value proposition for SDN is to incorporate this functionality in the future, though these functions are highly specilalized. The near-term trajectory is you will see a lot of activity in partnerships, integration, and even mergers between SDN fabrics in partner-built service-assurance solutions.

NPM, Monitoring, and NPB Integration Trends for SDN

Many monitoring and NPM companies have positioned themselves for SDN. As the SDN pure-play companies (all mentioned above) add monitoring, analytics, NPM, NPB, and service assurance functions to their networking suites, pure-play NPM and monitoring products are looking to partner or integrate with these virtualized network environments. This has led to some rapid consolidation and also financial moves involving many monitoring and NPB companies.

For example, **NETSCOUT** has been aggressively rolling up many different categories, purchasing Arbor Networks (security), Fluke Networks (troubleshooting and analytics), Tektronix Communications (traffic inspection, customer experience management and analytics) and VSS Monitoring (network packet brokers). NPB provider **Gigamon** was recently taken private.

Other networking monitoring companies that specialize in service assurance are positioning themselves as tools for SDN 2.0. For example, **EXFO** is a broad-based networking test and measurement company that is rolling out a suite of software monitoring products geared for SDN and NFV platforms. A cadre of service assurance specialists including **InfoVista** and **CENX** are targeting SDN in the service provider networking market. **Cisco** has been emphasizing its Tetration product line, which is designed to monitor and collect data to drive analytics functionality that will integrate with Cisco's ACI platform, though the company is in the early stages of integrating these functions and did not respond to specific requests for information in this report. You can see the appendix for more information on these companies.

With a myriad of monitoring and analysis products on the market -- NPMs, TAPs, monitoring, service assurance and NPBs -- only a small segment will be adapted for SDN and NFV. The foremost requirement is functionality that can be delivered in software, which is limiting to many of the monitoring companies that are geared toward specialized hardware devices. To give a real-world picture of how this is happening, the next section zeros in on real world deploy

IV .Conclusion

SDN Fabrics & Open Data Yield Integrated Platforms

Since its introduction in the 2010 timeframe, SDN has come a long way. Initially defined by disaggregated hardware and software as well as by new networking protocols such OpenFlow, SDN has expanded to become a much broader system comprising many platforms, management, monitoring, and automaton functions.

The emergence of fully functioning SDN fabrics that can create virtualized switching environments creates new opportunity to integrate software-based monitoring and analytics functions. This is enabling SDN to scale to larger networks, particularly those in service provider operations, which are in need of more open and scalable platforms. Further interoperability and configuration tools are needed to integrate multi-vendor service-provider environments. In addition, new data models needed to standardize operations and streamline the adoption of APIs.

Our research into the large enterprise and service-provider market indicates a resurgence in interest in SDN platforms, particularly those addressing platform automation and orchestration for the service-provider space. The reason for this is that creating interoperability and automation in larger enterprise and service provider networks is exceedingly complex and will require cooperation in the vendor community as well as strong innovation from the startup community. At the same time, leading standards organizations such as the ONF, MEF, and TM Forum have realized the need to coordinate data and standards models to guide interoperability.

As this innovation moves forward, open data models, APIs, and SDN platforms will open up new opportunities for real-time monitoring and analytics of SDN. Data-driven models will pave the way for the automation that large network operators are looking for to reduce the operating expenses and increase the capacity of their networks.

Pluribus NETWORKS

Product Type: SDN Fabric and OS **Target Market:** Service providers, enterprises

Description: Netvisor operating system software from Pluribus Networks is a scalable data center-class Network Operating System (OS) that virtualizes open networking hardware to build a holistic, distributed network that's intelligent, automated, and resilient. Enabling operational flexibility, the Netvisor OS combines best-in-class layer 2 and layer 3 networking foundation, the highly scalable distributed Adaptive Cloud Fabric architecture, and embedded network performance monitoring telemetry. Being software-enabled and built on open networking platforms, Netvisor OS has benefits over first generation SDN architectures and technology. In addition to being the foundation for Adaptive Cloud Fabric architecture, Netvisor helps build a distributed network that brings the benefits of cloud-scale and adaptability to the modern data center without a controller.

- Eliminates the SDN controller, radically simplifying the network architecture with no proprietary protocols
- Virtualizes underlying switch hardware, enabling multiple network instances on a single switch
- Plug and play operation with automated provisioning and management
- Supports a geographically distributed operating environment
- Fully interoperable with existing network deployments to support brownfield environments

Analytics Details: Pluribus Insight Analytics delivers Flow and Packet analysis capabilities with an easy-to-use dashboard to visualize key network and application performance metrics. Extensive filtering, and correlation capabilities enables users to quickly drill-down to visualize connections for detailed analysis workflows. Users can tag specific assets, such as IP addresses, VLANs, MAC addresses, and switch ports, with context to easily aggregate and filter flows. Integrated alerting capabilities enable quick notification of critical events based on connection attributes as they occur. With Insight Analytics, the IT Operations team can understand how users and services are consuming the infrastructure and conversely how the infrastructure is supporting the users and services.

Customers: Pluribus Networks is not disclosing customer names. However, the company says it has customers at two of the top five global banks, two of the top computing companies, as well as customers in the insurance, electricity, and electronics industries. Pluribus Networks also has 10+ service providers including Swisscom and Telstra.

Company URL: http://www.pluribusnetworks.com