RFC: Software Defined Wide Area Network (SD-WAN)

MANDAR RAJENDRA GHOGALE

Student ID: 47291378

Southern Methodist University

Spring 2018

EETS 8317

Switching and QoS Management in IP Networks

Dr. Kamakshi Sridhar

April 10 2018

# Abstract

This paper explores specific application of RFC 7426 Software-Defined Networking(SDN) applied to WAN connections.

This paper describes the purpose, implementation, benefits and further work of SD-WAN. The Software-Defined Wide Area Network (SD-WAN) is a specific application of Software Defined Networking (SDN) technology applied to WAN connections, which are used to connect enterprise networks – including branch offices and datacenters – over large geographic distances.

In the past, these WAN connections often used technology that required special proprietary hardware. In SD-WAN, the network control is moved into the “cloud,” using a software defined approach.

In other words, Software Defined Wide Area Network (SD-WAN) is an overlay technology in which the intelligence behind routing and switching and the movement of data and digital voice traffic is kept within software and removed from the hardware platforms that have traditionally controlled the flow of traffic in the network.

# Introduction

In the past, in order to obtain branch to branch connectivity between two branch offices of enterprise customer we need to rely on legacy IP/MPLS backhaul with WAN circuits which involves expensive, fixed circuits and proprietary hardware. In this particular WAN topology, it is really difficult to provision new green field deployment site with the possibility of failing this connection during peak time due to issues like fiber cut etc.

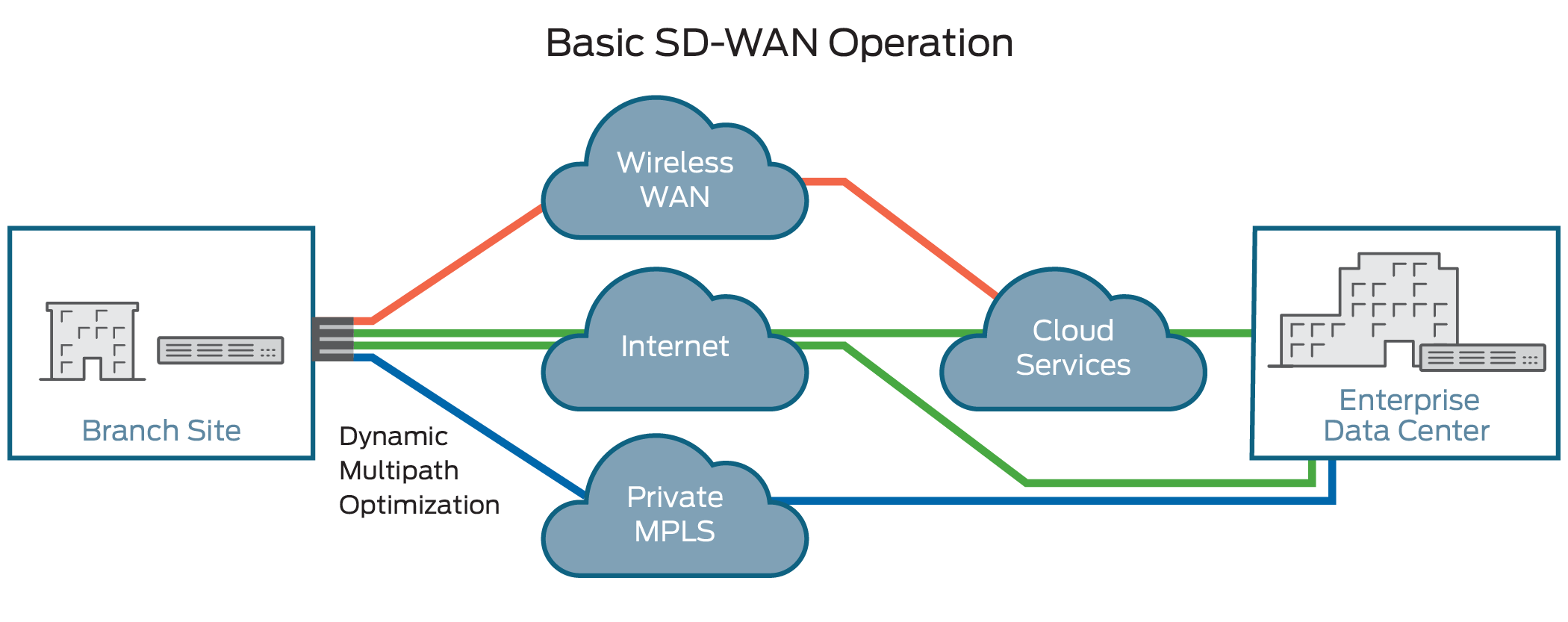
So, the software defined approach can be used to improve and secure internet connection. SD-WAN uses internet broadband connection to replace more expensive legacy hardware. Virtualization technology can apply to create GRE or VPN tunnel to broadband Internet connectivity or with the IPsec and DMVPN, making them more robust.

SD-WAN is important to extend WAN connectivity with the underlay of Internet broadband connection and overlay the VPN tunnel using virtual network function(VNF) by removing expensive routers and firewalls by provisioning via cloud services. In this report, we will see how customer can able to scale up connectivity during peak times of demand.

SD-WAN technology is differed by vendor to vendor, but a primary feature of SD-WAN is that it lets customers involve many connection types in their network, from multiprotocol label switching (MPLS) to broadband to wireless LTE. Customers can use primary path of expensive IP/MPLS network for priority traffic and backup path as cheaper public internet connection for less important traffic.

In this way, SD-WAN technology lets businesses switch carriers, mix and match them based on bandwidth availability, and quickly and easily spin up new connections to remote locations.

**Operation of Protocol**

****

Basically SD-WAN operates to provide connectivity between two branch offices over the internet broadband connection. It contains virtual CPE which is the white box which will be installed on customer branch offices. The vCPE contains virtual network functions such as virtual router, virtual firewall by using firewall we can create site to site VPN tunnel and forward the traffic in secured manner. In this service provider used its IP/MPLS private WAN circuit or Internet to build point to point tunnel between 2 branch offices of the customer. So, in this way, customer can have primary path(IP/MPLS) and backup path(Internet) to reach its branch office. The basic requirement is to know what the bandwidth requirement by the customer for connectivity purpose and which ISP will be they are using at each branch office such that service provider needs to create tunnel over third party internet. Also, we can apply QoS policies at the vCPE to throttle down the social media traffic and we can GUI access of the NFV orchestrator to monitor the traffic between two branch offices. If all the VNFs resides inside CPE, then that CPE will have called it as universal CPE (uCPE) if the VNFs are situated at the service provider data center and not on CPE then that CPE is called as virtual CPE(vCPE). vCPE is nothing but white box consisting of x86 processor. The OS will be based on Linux distributions, with standard transport layer functionality like routing, switching and bridging inbuilt in the OS itself. Premium functions like OAM, ZTP, Security, Tunnels and container support can be deployed on top of the base Linux kernel. Additionally, a hypervisor may be deployed to run any third party Virtual Network Function (VNF) on the CPE. There will be a protocol suite for management such as Netconf/Yang, OpenStack, OVSDB, OpenFlow CLI/SNMP etc. The SD-WAN controller is typically an application running on an x86 server in datacenter. It provides multiple capabilities like termination of VXLAN overlays on the vCPE, management of IPSEC tunnels within the L3 VPN and propagation of BGP routes across branch offices for branch to branch connectivity.

**Implementation**

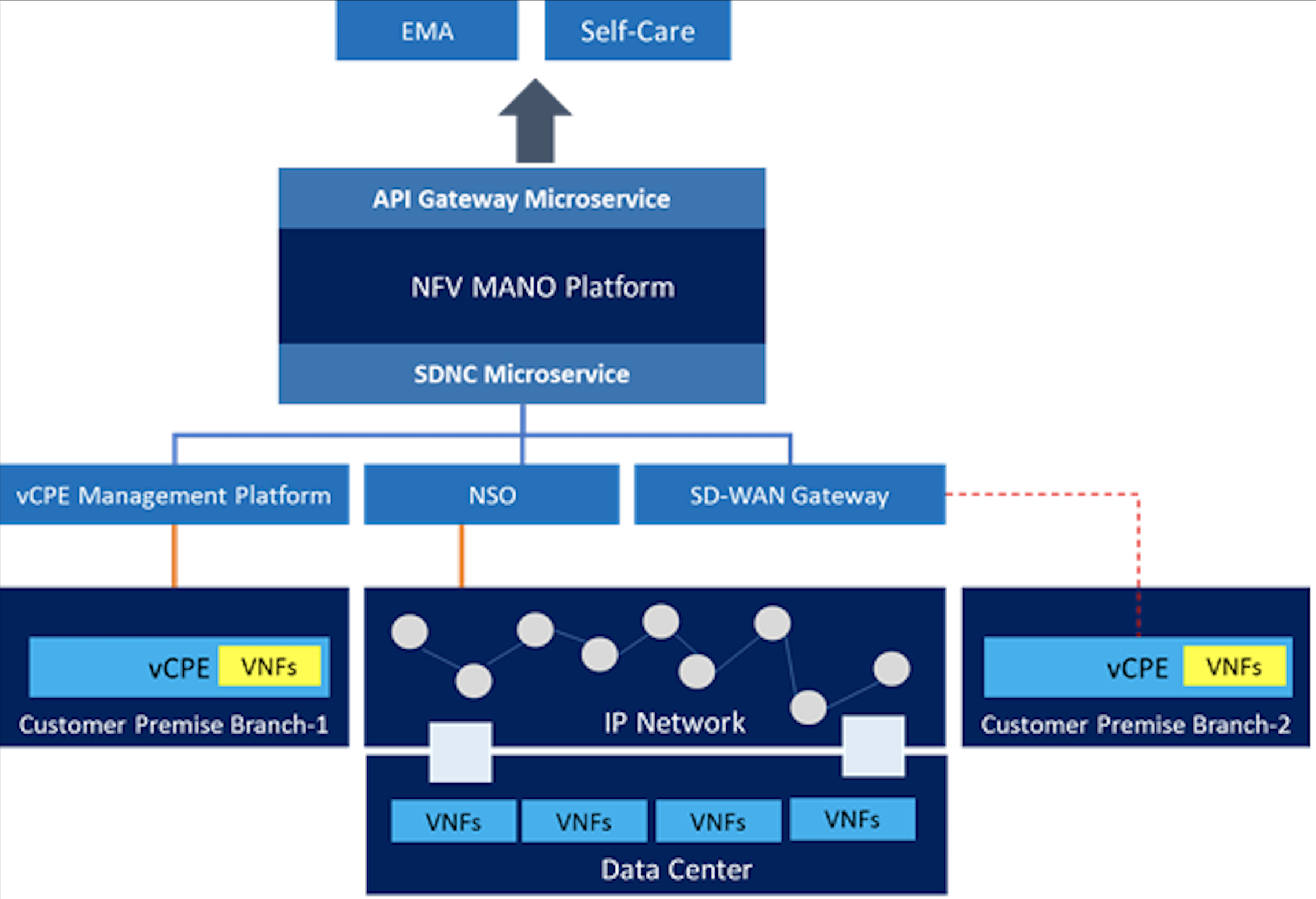


Figure 2 SD-WAN Architecture

The key features of the SD-WAN architecture are described below –

1. vCPE is installed at the customer premises. It can be both physical and virtual. VNFs such as Firewall, WAN Optimization, Application and Performance aware routing, NAT etc. will be hosted on the CPE or in the datacentre based on the customer requirements. These VNFs will be orchestrated through the NFV MANO Platform.
2. vCPE requires the SD-WAN gateway as a route reflector and an agent inside it for tunnelling IPSEC and other services within the CPE.
3. SDNC Microservice adapts between vCPE, NSO and SD-WAN Gateway APIs and plugs them into the MANO system workflow.
4. NFV MANO platform will do the end to end VNF Lifecycle management, SDN underlay/vCPE service orchestration.
5. Existing EMA/TIBCO, Self-Care and other Northbound applications will see a single pane of glass for SD-WAN. No CLI or sockets are required.

**Benefits**

One of the main SD-WAN as a service benefit is that most of the enterprise networks deploy SD-WAN is that it can reduce their WAN circuit costs by up to 90 percent because it supplements or replaces dedicated private WAN networks, which usually are private MPLS, and with regular internet broadband connectivity. That same cost-benefit can be applied to SD-WAN as a Service.  By using this, enterprises can get the flexibility and cost savings of SD-WAN and at the same time minimize the headache of managing the infrastructure and connectivity.

Also, we can have option of fully managed SD-WAN service by provider such that right from provisioning, installation, operation and maintenance handled by their NOC only. Most of the customers using SD-WAN for WAN acceleration and cloud security.

# Further work

Many new startup companies are going after the potential in the software-defined WAN [market](https://www.sdxcentral.com/reports/sdn-market-size-report-2013/), which is likely billions of dollars. Many of these startups have slightly different approaches to the market. For example, one of the vendor called Silver Peak has focused on accelerating [Software-as-a-Service(SaaS)](https://www.sdxcentral.com/term/software-service-saas/) applications in the cloud, VMWare’s [VeloCloud](https://www.sdxcentral.com/listings/velcloud-networks/) goes after branch-office connectivity, and Aryaka has built a global network so that companies can use WAN as a Network-as-a-Service (NaaS).

Incumbent WAN technology vendors such as Cisco and Riverbed, which make specialized appliances for WAN connectivity, are now focusing more on [cloud-based WAN](http://raynoreport.com/products/R003/) offerings in response to this new trend.

Expect the trend to accelerate over the next few years. What started as a solution for branch-office and data-center WAN connectivity requiring less proprietary equipment appears to be expanding into a wide range of SD-WAN (SDWAN) offerings and technologies including [VPN](https://www.sdxcentral.com/term/virtual-private-network-vpn/), [security](https://www.sdxcentral.com/security/definitions/security-challenges-sdn-software-defined-networks/), WAN optimization, NaaS, and application policy control.

New technologies such as segment routing, performance-based routing and intent based networking can plugin to the SD-WAN controller, also interesting to see how Linux foundation open source projects like CORD, ONAP will go after SD-WAN technology.

# Summary

SD-WAN is an emerging technology that offers several benefits compared with traditional, router-based WANs. Network decision makers can achieve cost savings, increased agility and simplification with an SD-WAN. This research defines SD-WAN and highlights its benefits, risks and alternatives. SD-WANs have the potential to disrupt the way enterprise WANs are built and managed. SD-WAN focus is connecting corporate headquarters to branch offices with centralized network management.   There are a lot of start-ups in that space using general purpose hardware with Intel Xeon processors.  A key advantage of SD-WAN was said to be software-based network reconfiguration.  It uses “SDN principles” like programmability and abstraction of functions, but not necessarily the classical SDN definitions of separate Control and Data planes with a Centralized SDN controller with global visibility and path selection.

# References

<https://www.juniper.net/us/en/products-services/what-is/sd-wan/> <https://www.sdxcentral.com/sd-wan/definitions/software-defined-sdn-wan/>

<http://techblog.comsoc.org/2016/10/10/summary-conclusions-of-sd-wan-sessions-at-telecom-councils-tc3-summit/>

<https://www.onecloudnetworks.co.uk/wp-content/uploads/2017/08/GARTNER-SD-WAN-TECHNOLOGY-OVERVIEW.pdf>

Jan 12, 2018, Architecture for Network Programmability with SDN and SD-WAN- Jio