Software Defined Network Researching Report

1. What is Software Defined Networking?

Software Defined Networking(SDN) has two main features. First, SDN separates the networking device's control planes from their data planes.[1] Control planes is the logical or intelligence of a networking. Control Planes make decision where the data or packets go when a router trying to forward the data or table to next router. Data plane carries the packets to the destination through the router based on the decision that control plane made. Second, SDN makes the whole networking programmable. In other words, SDN simplifies the process to manage a networking by providing a control panel to the networking administrator and allowing dynamical configures the networking based on its needs.[1] SDN has three major layers, infrastructure layer, control layer and application layer. These three layers structured from bottom to the top. The south-bound exists between control layer and infrastructure layer, and the north-bound exists between the control layer and application layer. Infrastructure layer includes data plane, memory, switch devices, and transmission media. This layer plays a "Do and implement" role in SDN networking. [1] All the four components are hardware level in SDN networking. The control layer is the intelligence of the SDN networking and the bridge between infrastructure layer and application layer. The reason control layer viewed as an intelligence layer is because it provides the decision where the packets should go, how the traffic should be processed, and whole SDN networking status through the rules and programming language such as C++, Java and Python.[1] Application layer with well-defined Application Programming Interface (API) connects the apps to the control layer and allows the apps directly to control the SDN networking. SDN application will allow user to easily monitor, configure and manage the infrastructure layer through the control layer. Two practical examples are adaptive routing and load balancing. Traditionally, switches and routers have their own forwarding table based on distribution needs. However, such designs are hard to reconfigure, complex to implement and may cause whole network goes down when one node goes wrong. In SDN, since it provides the whole networking's status such as bandwidth, traffic statistics, packet numbers and data size to SDN controllor, the SDN applications will dynamically adapt the networking and adjust its configuration based on the status. In other words, SDN applications control the whole networking.[1]

2. Why do we use Software Defined Networking?

Networking has become more and more complicated and hard to manage in today's world. Big data, high bandwidth, real-time streaming, and cloud computing, all of them require a stable and dynamic networking to keep them running smoothly. However, tradition networking cannot meet those needs when it comes with non-dynamic and difficult to reconfigure. In tradition networking or as known Quality of Service (QOS) networking, the bandwidth for each

---

[1] Olorunosebi, J. "A Beginner's Guide to Software-Defined Networking(SDN)", *Intense School*, Oct 30,2015, Web, Jan 24,2018 accessed, http://resources.intenseschool.com/software-de%EF%AC%81ned-networking-sdn/ .

service are fixed and it usually has high latency. But SDN provides app on-demand for devices in networking. For example, if employees need to communicate with his or her boss, but his or her devices does not have an app to support the communication, he or she needs to download the app first. When their devices connect to the API in SDN networking, FTP will be the first priority on their devices to improve the speed of downloading. Another advantage to use SDN networking is low latency when needed. For instance, a stocker trading house needs to have low-latency networking between 6 am to 6 pm because stock trading needs to be done in seconds, although low-latency is expensive but they would like to pay for it. However, after the 7 pm, the trade house might want high-latency because of offsite maintenance does not require low-latency speeds. In short, SDN networking provides a lot more flexibility compares with the tradition networking because it allows devices to control the networking based on the networking traffic and needs.

3. Security of Software defined Networking

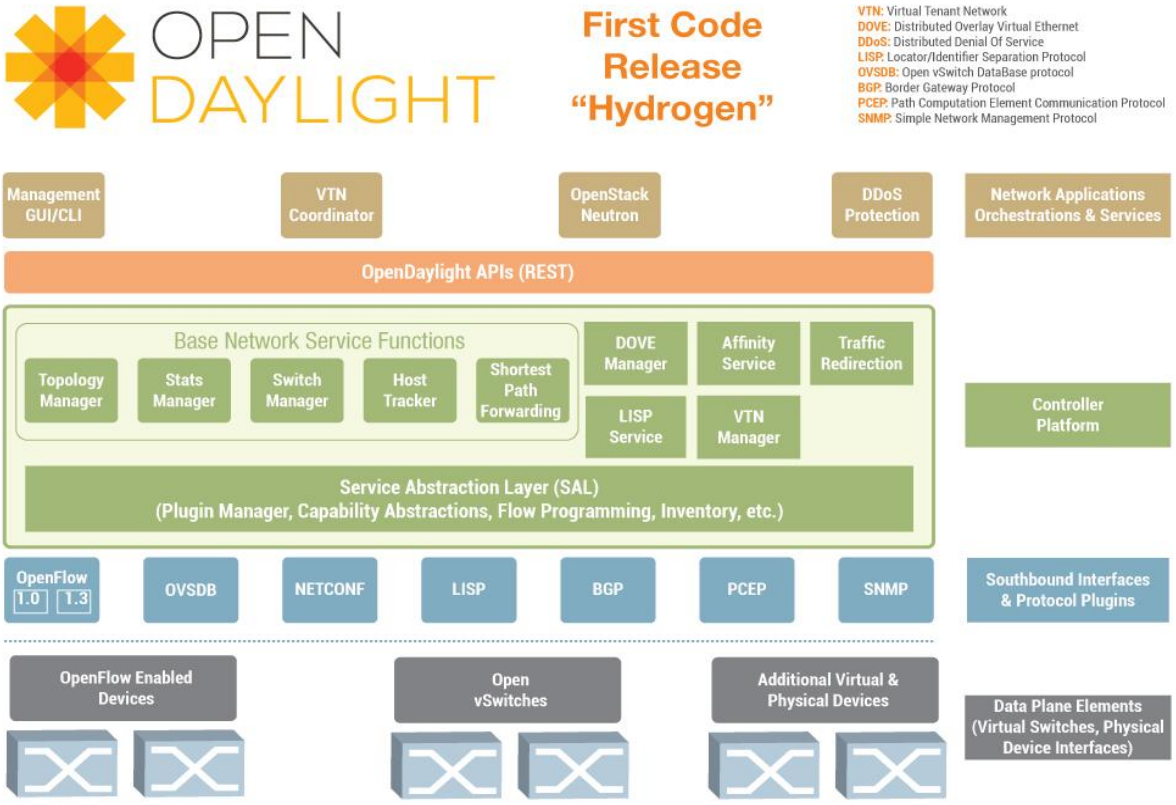
Compares with the traditional networking security, SDN provides an easy way to manage and configure the security policy and rules among the whole networking. In traditional networking, due to massive proxy servers, firewalls, and IOT devices, configuring the security rules and letting networking meets required standard are extremely hard and tedious. With SDN, configuring, monitoring and access control can be done in one platform, which is a better way to defend and detect cyber-attacks.[1] However, because SDN applications and controller has the ability to control the whole networking, SDN can also be vulnerable to many cyber-attacks. For example, if an attacker successfully spoofing a controller's address, he or she could define their own policies and rules on forwarding nodes and devices and take over the whole networking in just few minutes. Also, attackers could guess the forwarding rules in the controller and increasing the number of packets eventually the whole SDN networking will become overwhelmed.[1] In short, one vulnerability in controller or any bad code designs in SDN applications could result the whole SDN be compromised by attackers. Shorter timeout, packet dropping and rate limits can be applied on controller and forwarding devices to decrease wide range threats. Access control, selective filtering, troubleshooting, firewall, and intrusion detection system these tradition techniques could also mitigate threats in SDN networking.[1]

4. What is OpenFlow Protocol and how does it works?

OpenFlow widely used in many SDN solutions today. In the earlier ages, Openflow was used for easy control and manage campus networking. OpenFlow SDN standard includes two parts, OpenFlow switch and OpenFlow controller. In a OpenFlow networking, the data remains on the OpenFlow switch but the high-level decision is separated to the OpenFlow controller, typically a controller server.[2] The OpenFlow controller and switch communicate through the OpenFlow protocol, which defines message such as packet-received, send-packet-out, modify-forwarding-table, and get-stats. In OpenFlow switch, it contains flow tables, group tables and OpenFlow channel. In each flow table, it contains flow entries and actions which tells where the packet goes. When OpenFlow switch receives a packet, it compares if there are any matches flow entries, if not, the switch sends that packet to OpenFlow controller to let it make a decision

what to do with that packet such as dropping that packet or add a flow entry. If the packet has matching flow entry, switch will forward that packet based on the existing flow entry. [2]

5.What is Open Day Light(ODL) platform?
Open Day Light controller is one of the popular open source SDN controllers. SDN controller is the "brain" of the networking. It controls the southbound API such as switchers, routers and northbound API in applications. ODL was announced in 2013 by Linux Foundation and they released their first code, Hydrogen. [3]



Reference

1. Olorunosebi, J. "A Beginner's Guide to Software-Defined Networking(SDN)", *Intense School*,

[2] "OpenFlow Learn More", n.n,n.n, Web , Jan 24 2018 accessed, http://archive.openflow.org/wp/learnmore/

[3] "What are SDN Controllers (or SDN controller platform)?", sdx central, n.n, Web, Jan 24,2018 accessed, https://www.sdxcentral.com/sdn/definitions/sdn-controllers/

Oct 30,2015, Web, Jan 24,2018 accessed, http://resources.intenseschool.com/software-de%EF%AC%81ned-networking-sdn/
2. “OpenFlow Learn More”, n.n,n.n, Web , Jan 24 2018 accessed, http://archive.openflow.org/wp/learnmore/
3. “What are SDN Controllers (or SDN controller platform)?”, sdx central, n.n, Web, Jan 24,2018 accessed, https://www.sdxcentral.com/sdn/definitions/sdn-controllers/