ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 14, May 2016

Software Defined Networking: Vision Architecture, Tools

Ms. Joharan Beevi. M PG Student
Dept. of CSE
Valliammai Engineering College
Kancheepuram, India

Mrs. S. Suma Assistant Professor (Sr.G)
Dept. of CSE
Valliammai Engineering College
Kancheepuram, India

Abstract: -- In modern business environment networking is an important concept in order to improve our communications. This network will be on premises, cloud or hybrid of two. It provides various communication links that can be used to run the applications, delivery services and be competitive. All the organizations need new technologies for configuring, controlling and operating to their networks. So in this paper will discuss how the network will be implemented, controlled easily by introducing SDN. It is an approach to build a network that splits the elements which is used for systems. All processes in the SDN are not happening in the same devices inside. In additionally virtual machines are moved between the servers dynamically in certain minutes or seconds for improving server virtualization. But it can take several weeks or days for movement of virtual machine, it also provides some difficulties for reconfiguring the network. Hence SDN promises in overcome these limitations in the network.

Keywords: - SDN, On premises, Cloud, Server Virtualization

I. INTRODUCTION

Open Network Foundation (ONF) point of view SDN is a network architecture that separates Control plane and Data plane. Control plane is moving to an application known as Controller. In commonly SDN is network that controlled by the software applications, it can holds many characteristics such as Agile, Directly programmable, Managed Centrally, programmatically configured.

A. Traditional Network

Most of the networks are implemented by using dedicated application like switches, routers etc. and hardware applications are implemented by using Application Specific Integrated Circuit. The main limitations of the traditional networks are Complexity, Inconsistency policies, Inability to scale.

➢ Inability to Scale

The IT department either wants to connect with static network as oversubscribed or must grow with demand of many organizations when increasing bandwidth and application workloads. Moreover bandwidth requiring statistical planning and reconfiguring the network.

➢ Incompatible policies

All operations in the network environment are manually configured and scripted among the hundreds and thousands of network applications mainly security and quality policies are configured manually. This makes complicated to the organizations during implementation without providing significant investment of scripting skills or knowledge. It is difficult to predict which one is entered incorrect and which one is incorrect access control list on a given device. So this makes complex to removing the all associated policies where one application is removed from the device then complexity is increased further.

➢ Complexity

Network is increased because plenty of network protocols and features are used so traditional network can increases network and hardware complexity to the users. These features are executed via vendor or customer specific commands so that increases complexity [3].

B. Innovation of SDN

The development and standardization of the SDN can be derived by using Open Networking Foundation (ONF). It is mainly provides a policy based flow management within a network and particularly suitable for implementing network segmentation. This makes simple quality of service and flow metering. The SDN contains Open Flow, Standard South Band API, and Centralization of Control Plane, separation of Control and data planes. These are mechanisms but SDN is not a mechanism this is also called as a framework to rectify set of problems. It is the physical decouple of control plane from the forwarding plane where the control plane can be controlled to other devices. Network Administrators can automatically control and dynamically managing the services, routers, paths, applications, packet handling policies with the help of high level languages. In the networking environment management holds provisioning, operating, optimizing and managing (faults, configuration accounting, performance, and security)[1,3]. Software Defined Networking is needed for several reasons such as

➢ Virtualization

It is used for remotely monitoring the device without need of the physical location for storing the elements. All services, resources, applications, protocols are handled by remotely in the server.

➢ Orchestration

This makes controlling and managing the whole devices by giving one command by the user or client. It requires less amount of resources and easily manageable.

➢ Programmable

It can be easily programmed by the clients or network administrators, which should be change the behavior of the networking environment. It requires networking skills to managing the network.

➢ Dynamic Scaling

Depending upon the user needs the size and quantity of the network components should be changeable. So in any situation the administrator can change the networking environment periodically.

➢ Performance

Utilization of optimized network devices. It consists of Bandwidth management, traffic engineering, Load balancing, high utilization, Fault tolerance capacity.

➢ Mutli-tenancy

Each users in the network need accessing capability for that they also have permission for accessing the data. So it requires complete control of addresses, topology, routing and security.

➢ Service Integration

Many network services are integrated in the multi-tenancy environment there are Load balancers, Intrusion Detection Systems (Ids), Firewalls.

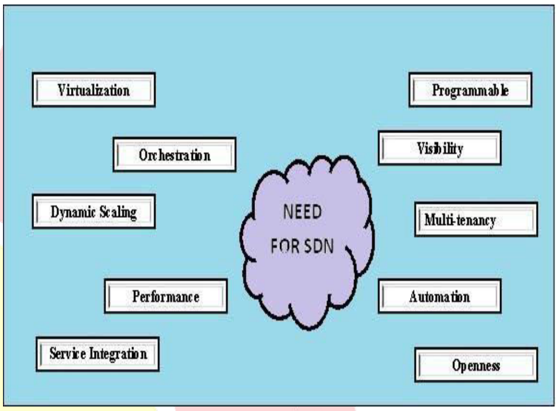

Fig 1. SDN Needs

II. Understanding The SDN Technology

C. *SDN Controllers*

It is a centralized storage of policy and control of all instructions for applications or networks infrastructures. These controllers are consistently and provide information of the network, analytical information among the all resources. For example WAN and LAN, wired and wireless network and physical, virtual infrastructures. When you are writing the controller by using API policies. The controller can join the gap between network elements and applications they also provide communication between them then supplies to the network, applications and services in automated manner. Network has to translating the number of protocols and features for the application so increasing burden in the network, in order to reducing the burden the network communication to translating the control policy into the network level policy by the controller. So compliance, checking, enforcing network technologies will be automate in the networking environment.

Controller also provides the programmatic interfaces, supplying services for the setting polices among the network. Using this we have to eliminate the network complexities and automatically run our virtual and physical network. SDN controller is based various types of protocols such as Open flow that is used to sending the packets in the servers by providing the commands. The SDN controller is the core part of an SDN network. It is sitting between the network devices and the applications [1].

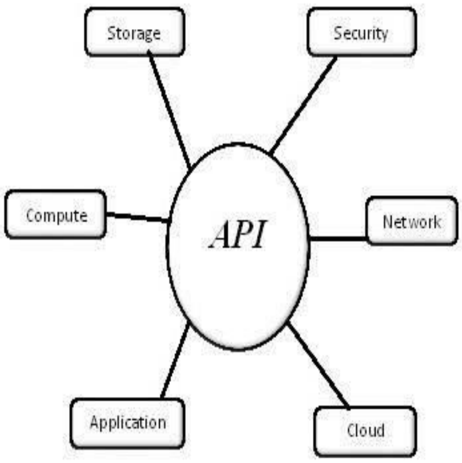

Fig 2. Various fields of API

A controller also provides:

- ➢ Consistency across the enterprise network that keeps downtime to a minimum and lowers operational complexity and associated cost
- ➢ Automated end-to-end provisioning and configuration to enable rapid deployment of applications and services
- ➢ Support for both existing and new deployments that lets you implement programmability and automation with the infrastructure[1]

The Vendors of the SDN Controller is the Big Switch network, HP, IBM, Juniper. It holds huge collection of pluggable modules and being used for the different performance tasks such as gathering network statistics, what devices are allowed within the network etc.

D. SDN Policies

In networking environment all businesses are required to implement, scale up and optimize the application when we need so it increases network complexity and maximize manual operations. To overcome these limitations SDN policies are implemented in the network then the software can accomplish the task by using these policies.

S.no	Controller name	Working principle	License	Features	Shortcomings
1	NOX	First SDN Controller. Written in C++.	GPL	Understandable language	Lack of documentation Heavily implemented.
2	POX	Written in Python Working with API and documentation	Opel flow reference	Platform Independent, Provides Web based GUI documentation	Lack with experimental and developmental life cycles.
3	Beacon	Written in java, highly integrated with Eclipse IDE	GPL, FOSS license for your code	Have ability to start and stop new applications.	No loops, Limited to star topologies
4	Flood Light	It is controlled by Big switch network. It is made by using Apache Ant	Apache Ant	.Easier Flexible Very active community	Most of the functionality exposed only API.
5	Open Day Light	It can be implemented on variety of networking environment within the JVM. Written in Java	Cisco	Web based API GUI based API Pluggable modules	Load Balancer and Firewall services are missing
6	Open Contrail	It is a platform for multi networking function Providing NV and Network Function Virtualization	Apache 2.0	Well written product Own commercial Control	Not supported compared with Open daylight

Table 1. Different SDN Controller

This makes reduction of thousands of servers and millions of workloads. Cisco's policies provide the instructions that say how the network elements are interacted with network and application traffic.

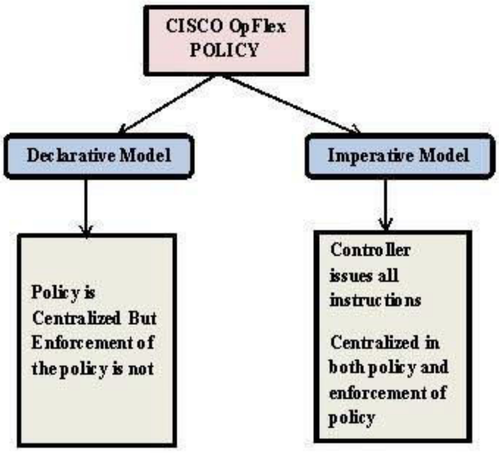
CISCO OpFlex POLICY
Declarative Model
Imperative Model
Policy is Centralized But Enforcement of the policy is not
Controller issues all instructions
Centralized in both policy and enforcement of policy

Fig 3. Models of OpFlex

To deploying this policies CISCO is used separate architecture for improving SDN networking. OpFlex is the example of Cisco policy. It is an extensible communication protocol model that is used to transfer the abstract policy between the controller and collection of network devices. It is an application centric policy and provides the distributed environment. This makes automation of entire infrastructure without failure that is tolerating the scalability in the cloud infrastructure. OpFlex is placed on the information model which the agents are understood the controller and devices. It must be based on the abstraction policy and providing each device with freedom and rendering the policy of the abstraction then flexibility in nature. It has basic advantages such as can support any devices like physical switches, hypervisor switches.

E. SDN Environment

Increasing number of server virtualization and network in virtual wants data centers and cloud infrastructures more important. SDN mainly involves the Cloud servers and virtual network so this reason SDN take advantages of the Virtual network. This virtual network is also called as the overlay network. Top of the physical network holds new logical topology for that the virtual network is also called as the overlay network. From the interconnected nodes of virtual network can be separated virtual network overlays under the supervision of physical network when they will be deploy the applications without modifying the underlying network which requires only topologies. It should separate the tenants and applications. User of shared cloud resources is also known as tenant they might be applications or group of applications which are connected in logically. This overlying network supplies number of uses that can rectify the some of the burden of the datacenters. There are Flexibility, Fabric Scalability, Layer 2 connectivity over layer 3, Isolating roles and responsibilities, Address Overlapping. Various Networking environments are available in the SDN for example VXLAN.

The VXLAN is the Software defined Networking Environment that is abbreviated by Virtual Extensible Local Area Network developed by Cisco. It is an open source protocol which is promoted by virtualization vendors such as Red Hat, Citrix and VMware. VxLAN is an encapsulation protocol which is running on layer 2 infrastructures which provides the extension of virtual LAN address space by adding the segments ID and maximizing the number of available IDs. VLAN ID is defined by 12 bit attribute of the VLANs in the previous network but nowadays increasing multitenant consuming large connectivity during creating their own networks. So it is not scalable to the datacenter. VXLAN has several components in the VMware environment. There are VTEP, VCNs manager, VCNs Gateway.

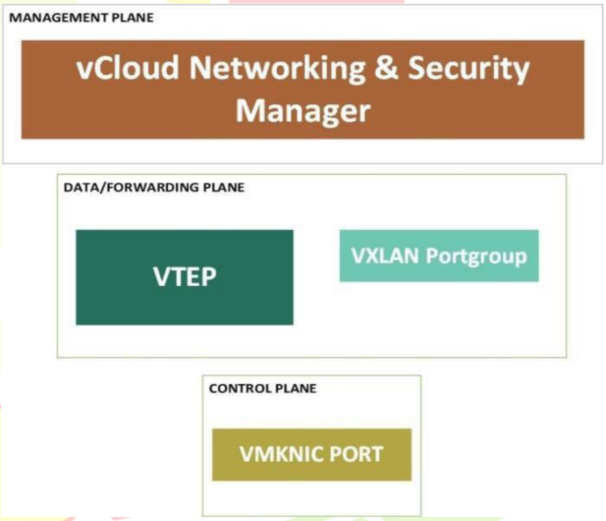

Fig 4. VXLAN modules

VTEP is expanded as VXLAN Tunnel Endpoint which is start and end of the process of tunnel which is executed on the ESIX host and holds following sub components there are VM kernel module, VM knic adapter, and VXLAN port group.

1. VM kernel is used to managing the routing tables, handles encapsulation and decapsulation of packets in the data plane.
2. VM knic adapter: - This provides clustering effect to the VLAN which is installed on one host that transporting VXLAN traffic control.
3. VXLAN port group: - When deploying the network at each time and VXLAN segment, the Newport group is created.

VCNs Manager makes the centralized management of all VXLAN segments and preparing the VXLAN

clusters in the VM knic interfaces. It holds the VXLAN implementation in the VCenter domains.
VCNs Gateway is managed by VCNs manager, which provides security and connectivity. This is an important element in the architecture because it connects the VMLAN and Outside world.

III. Key Requirements and Protocols of SDN

F. SDN Architecture

SDN towards operating system for network. It is often considered as the north and south band interfaces that communicate with the applications, network systems and services. A North Band interface is used to connect the controller and applications then the South band interface is used to connect the controller and physical environment. SDN provides virtualized architecture which is not located in the physical place.

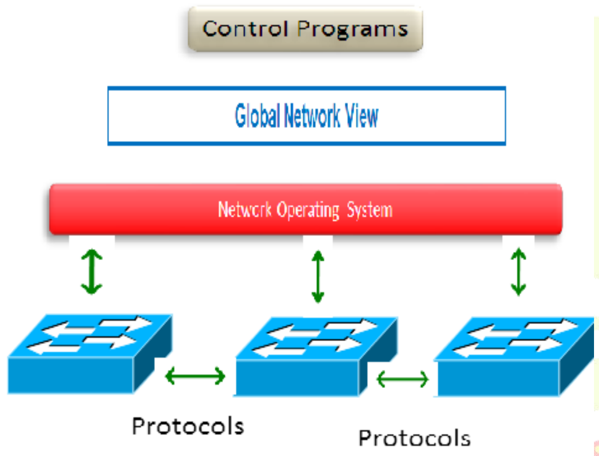

Fig 5. Overview of SDN

In the SDN architecture decoupling the control and data planes and network and states are centralized. Underlying infrastructure is derived from the applications [4].
SDN defines network architecture as a four pillars
Decoupling Control and data plane: - To remove the functionality of network from the devices in network, then
It will forward the elements such as packets. The decisions are represented as the flow based these values are defined by set of field values as a filter and instructions.
The External entity of the network holds the control logic for this reason is called as the Network Operating System (NOS) or SDN controller which can be run on commodity hardware. A software application provides the programmable environment to the network on top of the NOS that interacts with the data plane devices.

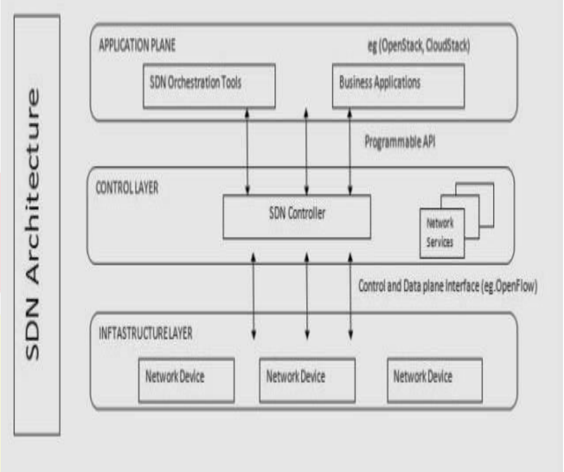

Fig 6. Architecture of SDN

In order to identify the various elements in the SDN such as forwarding devices, Data plane, South bound Interface, North bound Interface, Control plane, management plane [5].

Forwarding Devices and Data plane:-
Forwarding devices are well defined instructions set which can be used to take actions for forwarding the incoming packets. By using wireless or wired network channels the forwarding devices are connected that represents data plane.

South and North Bound Interfaces (SI and NI)
Forwarding device's instruction set can be defined by using southbound API, here communication protocol will be used for interaction between forwarding devices and control plane elements. Application Programming Interfaces for the NOS could provide the North band Interface.

Control Plane and Management Plane
By using control plane elements forwarding devices are programmed. Control logic in the application and controllers built the control plane. It is used to implement the network control and operation logic. It includes various applications such as firewalls, load balancers, monitoring.

G. SDN Protocols

Various protocols are used to communicate and connect the data between the control and data plane [6]. There are

1. Border Gateway Protocol (BGP)
This protocol is used for exchanging the information about routing among the gateway hosts

in a network. It is considered as the exterior gateway protocol.

2. NETCONF

It defines Internet Engineering task Force network management protocol. This protocols are based on RPC and SNMP.

3. XMPP and VSDB

Extensible Messaging and Presence Protocol is defined by extensible markup language. It is an alternative SDN protocols. Open Switch Database Management protocol refers Open flow configuration protocol. It refers the open switch implementation which can be distributed among multiple servers.

IV. Conclusion

In traditionally network devices are hard to manage and control those devices are very difficult to the users. Each product in the network have own configuration and management, long duration implies late upgrades or updates. So overcoming these limitations Software Defined Networking will be implemented. It is decoupled between the Control and Data plane but SDN has some of the problems there are hardware infrastructure, southbound interfaces, network virtualization, network programming languages, and northbound interfaces. SDN interfaces can transform the static networks into flexible, programmable platforms, allocation of resources dynamically, highly automated and secure cloud environment. Hence software Defined Networking can change the future networks

REFERENCES

[1] Bring Underdahl, Gary Kinghom, "Software Defined Networking for dummies" John willey and sons., 2015.

[2] Diego Keutz, M. V Ramos, Paulo Verissimo, Christian Esteve Rothernberg, Azodolmolky, " Software Defined Networking: A Comprehensive Survey, Version 2.01 Oct 2014.

[3] Cisco white paper-"Software Defined Networking: Why We like it and How We are Building" On It,2013.

[4] SDN 101. An Introduction to Software Defined Networking,citrix.com/sdn.

[5] Open Networking Foundation," SDN Architecture Overview" Version 1.0, Dec 12, 2013.

[6] Article title: http://searchsdn.techtarget.com