International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 3 Ver. I || March 2018 || PP. 55-63

Efficient Network Management: A Software Defined Networking Approach

Shyam Patil[1], Pratik Kanani[2]
[1](*Information Technology Department, Dwarkadas J. Sanghvi College Of Engineering, India)*
[2](*Computer Engineering Department, Dwarkadas J. Sanghvi College Of Engineering, India)*
Corresponding Author: Shyam Patil

ABSTRACT: *Software-defined Networking is a network architecture that separates the data plane and control plane. Dynamic management, programmability and scalability problems are addressed by use of Software-defined Networking approach. In this paper we have a jest of Software-defined Networking approach and how it is implemented through use of OpenFlow standards. The implementation of this approach in various networks and its advantages are linked with existing protocols are further discussed in the paper. And finally we have discussed the scope and evaluated the advantages of this technology.*
KEYWORDS - *Software defined network, dynamic network management, OpenFlow standards.*

Date of Submission: 16-02-2018 Date of acceptance: 03-03-2018

I. INTRODUCTION

The rapid increase in network traffic in modern day data centers is quite acknowledged, with big companies expanding over large geographical areas. The amount of data that has to be stored is also increasing leading to rise in number of servers implemented for that purpose.

Advancements in the fields of Cloud Computing and Data Mining also require large data centers to continuously route traffic which is also a daunting task. Routing of such large scale requires dynamic protocols to run systems more efficiently. Hence the concept of Software Defined Networking is introduced.

II. SOFTWARE DEFINED NETWORKING

Software Defined Networking is defined as following:

"Software-defined networking (SDN) technology is a novel approach to cloud computing that facilitates network management and enables programmatically efficient network configuration in order to improve network performance and monitoring"[1].

This definition of Software Defined networking is far more sophisticated. In simple terms software defined networking allows a user to implement his/her own designed protocols suitable to the network in which it need to function.

SDN architectures decouple network control and forwarding functions, enabling network control to become directly programmable and the underlying infrastructure to be abstracted from applications and network services[2]. A Software-defined network controller or control plane is used decide where the received packets are supposed to be forwarded.

Some of the features of Software-defined programming are as follows:

1) Due to high cohesion and low coupling the SDN architecture is made directly programmable, which makes it dynamic and easy to handle.

2) Dynamic architecture allows the user to make necessary changes when required and also increases adaptability.

3) Being software based and programmable SDN architectures are centrally managed, providing the user full overview of the network.

4) SDN architecture also lets you manage network resources which are accomplished by dynamic and atomized SDN programs which can be user defined.

5) When implemented through open standards, the network design is simplified due to SDN controllers which makes network independent of vendor specific network switches and routers.

III. LITERATURE SURVEY

Now packet forwarding is the elementary motive of a router, throughout the network. Before use of centralised switches, there were various protocols used for this purpose i.e. transporting a packet from one location to other on the network with minimum time accounted for it.

Now these protocols are classified as namely IGP's(Interior Gateway Protocol) and EGP's(Exterior Gateway Protocols). These protocols have been used since mid of 80's and the oldest of them being the STP.

Now Interior Gateway Protocols lets the routers on the same network and under same administration exchange routing information, whereas the Exterior Gateway Protocols allow routers to connect to the router present on networks other than the existing network. The following protocols will be discussed in the segment for clearer idea as to what each of the protocol does. They are as follows:

- RIP (Routing Information Protocol)
- BGP (Border Gateway Protocol)
- STP (Spanning Tree Protocol)
- OSPF(Open Shortest Path First)

These protocols were mainly used until now for routing of packets in networks. But due to lack of time efficiency and to minimize the processing constraint required in the transmission of packets over network in large networks like data center's, these protocols have been replaced by Open Flow protocol.

I.1 ROUTING INFORMATION PROTOCOL

RIP or Routing information protocol is an example of Interior Gateway Protocol that is used to determine the number of hops i.e. number of network lines to be travelled in order to reach the desired destination in the network. It is generally used for small scale networks like homes and small offices.

RIP is based on distance-vector based routing which makes use of hop count as a parameter to identify the next route to be taken by the packet. A hop is in general the number of intermediate devices between the source and destinations.

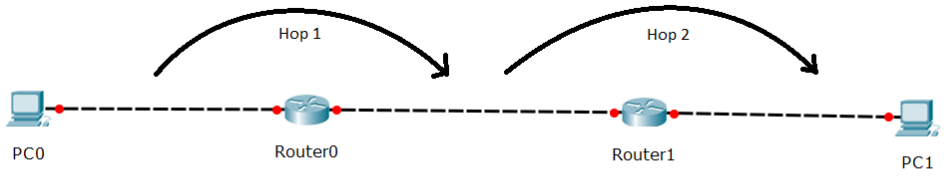

Fig. 1 Router Hops

The routing table is updated every 30 seconds by the Routing Information Protocol. This is achieved by sending request and response packages over the network to neighbouring routers which are RIP interface enabled.

Whenever online, the router sends out broadcast request packages to all the RIP interface routers and then it receives response packages from the corresponding routers. During update when the response packages are received it has three possibilities regarding hop count:

- The old entry does not exist for the corresponding entry received in the routing table.
- The hop count is less than the old entry in the routing table.
- The hop count is greater than the entry in the routing table.

In the first case, if the entry is not found then the entry is added to the routing table with the information that from which router has it originated and other information. In second case, if the hop count is less than the previous entry the routing table gets updated with the new and efficient route. In the last case the new route is not updated instead a Hold down timer is initiated.

Hold Down timer is nothing but the time period for which the router stops receiving any updates from the corresponding router and waits for the network to stabilize. If after timeout the response hop count is same then the hop count is updated in the corresponding routing table[3].

Also RIP uses methods like split-horizon and route poisoning to avoid loop routing and unreachable destinations.

In route poisoning, generally if a router discovers that a router is not reachable by path then all the routers on the network are informed by a response packet that the bad route has infinite route metric(hop count)[4].

In split-horizon the router only has table entries for routers which it is directly connected in the network. So if a neighbour of adjacent node fails it does not loop the packet between routers in order to reach the destination.

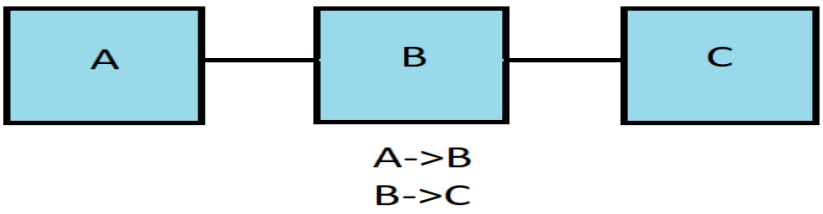

Fig. 2 Count to infinity scenario

Consider Fig. 2 where A is only connected to B and B to C. Assume A has an routing entry for node C and C fails. Then when B tries to transmit to C, node C is down and another possible route to C is via A. Now this a loop condition because the route to C from A is through B. Hence the packet is in a continuous loop.
Thus split-horizon is implemented to avoid such loop conditions[5].
Thus the drawbacks of Routing Information Protocol are:

- There is a hop count limit in order to implement route poisoning which is 15 after 16 hops RIP fails.
- RIP implementing network are generally flat meaning the have poor security, speed and non-redundant.
- RIP is susceptible to count to infinity problem.

Due this drawback of RIP, it is difficult to implement in large networks such as data center's. And due to hop count limit it is difficult to implement RIP in larger networks.

I.2 OPEN SHORTEST PATH FIRST

OSPF or Open Shortest Path First is an Interior Gateway Protocol. It is one of the most widely used protocol. It is generally implemented in large enterprise networks.
OSPF protocol is based on link-state routing algorithm. The main difference between distance-vector routing and link-state routing is that in distance-vector routing nodes i.e. routers share their routing tables with their neighbour and in link-state routing the information is shared about the link connectivity.
The link-state algorithm firstly creates an entire map of the network in which the routing is to be performed. The router checks all the physical connections through which it is connected to its neighbouring routers. Then it sends link-state advertisement packets to other routers to check all the active routers which participate in network. The packets only identify routers on the same network as OSPF is an example of IGP.After the router verifies the nodes and connections it creates a virtual map of the network.
For generating the router table entries the link state algorithm makes use of some variant of Djikstra's algorithm to find the shortest path available between two nodes in a given network. Since OSPF protocol is implemented on a large scale, it is not efficient to store the whole map of the network. Thus, the network is divide into different area's, where each area has its own identification notation similar to 32-bit notation of IP addresses.
OSPF does not use a transport protocol. It encapsulates its data directly in IP packets. This is in variance to other routing protocols, such as the Routing Information Protocol (RIP) and the Border Gateway Protocol (BGP). OSPF has its own transport layer error detection and correction functions which are implemented independently.
The main disadvantage of OSPF protocol is that it requires huge computing power and memory. It also requires large bandwidth to flood the network with link-state advertisement packets.

I.3 BORDER GATEWAY PROTOCOL

Border Gateway Protocol or BGP is a exterior gateway protocol. It is used to exchange routing information among networks. It falls under the classification of distance-vector routing protocol. The Border Gateway Protocol makes routing decisions based on policies set by the administrator and is responsible for making all the essential routing decisions. This decisions can also take into consideration the network architectue and rule-sets specified .
It can also be used to route information within a network. It's application is referred as Interior Broadway Protocol or iBGP. Large private IP networks make use of iBGP. The current BGP works on version 4(BGP4)[6].
BGP neighbours are known as peers. Peers are configured manually by the network administrator on port 179 to establish sessions. The BGP protocol makes use of 19-byte keep-alive message every 60 seconds to maintain connection between the peers[7]. When BGP runs between the protocols in the same network then it is called

iBGP, else if BGP runs between two edge or border router's it is called eBGP. These routers are also called as eBGP peers.

BGP peers make use of finite state machines to make decisions. They consist of six states:

- Idle
- Connect
- Active
- OpenSent
- OpenConfirm
- Established

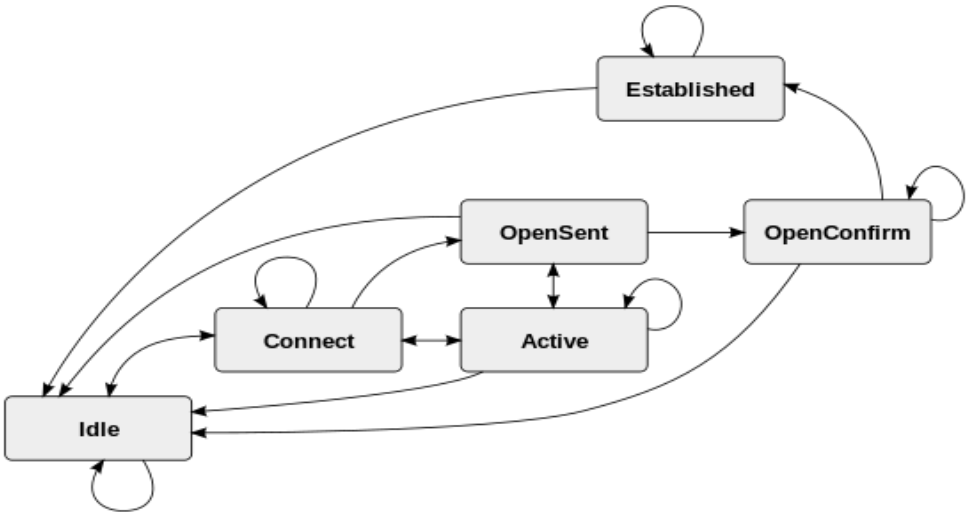

Fig. 3 BGP Finite State Machine[8]

For every BGP peer-to-peer session, itmaintains a state variable which keeps a track of which state the session is in. Generally Idle state, rejects incoming BGP requests and starts TCP connection with its configured BGP peer. A BGP peer does not stay long in connect state. In this state the peer waits for successful TCP negotiation with peer. If a peer is unable to establish a TCP connection then it goes into Active state. After a retry, if the peer connects successfully it sends a Open message to the peer, else it is reset to Idle state. In OpenSent state the peer listen to the Open message, if a valid message is received then peer move into OpenConfirm state. After confirmation, a keepalive message is received for time mentioned the peer stays in the Established state for packet exchange.

Drawbacks of Border Gateway Protocol are as follows:

- Due to pure inter-connectivity, the mesh topology is implemented and sessions in each router are to be maintained, which demand more processing power.
- If a router is misconfigured the changes in the network are not efficiently conveyed.
- The topology of Border Gateway Protocol demands more memory and CPU requirements, and if the global routing table size exceeds router capacity then they cannot serve as effective gateways.

Also implementation of Border Gateway protocol is not cost efficient as increased need for computing resources.

I.4 SPANNING TREE PROTOCOL

Spanning Tree Protocol or STP is a network protocol developed to avoid looping in networks. The basic function of STP is to prevent looping and Broadcast radiation. The term broadcast radiation refers to accumulation of multicast/broadcast packets on the network.

Spanning tree protocol as name suggests creates a spanning tree in the layer-2 bridges network and disables other inactive links leaving a single functional path between any two nodes. This spanning tree formed in the LAN need not necessarily be a minimum spanning tree.

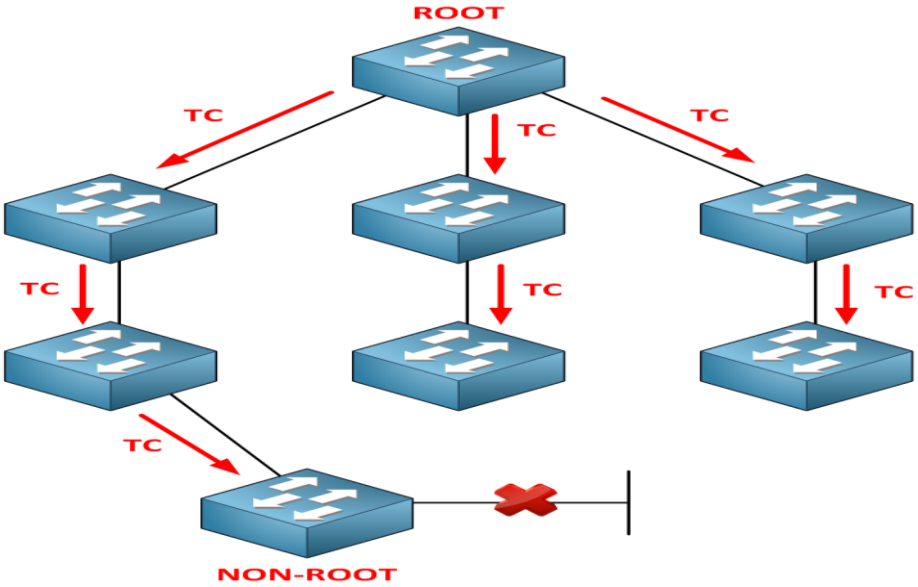

Fig. 4 STP topology

For the initial steps, a root bridge is selected in the network. This decision is based on the following parameters:

- Bridge priority
- MAC address

The concatenation of these two factors are termed as Bridge ID. And the bridge with lowest Bridge ID is the root. Then each bridge computes a least cost path to the root bridge. This is achieved by use of bridge Protocol Data Units (BPDU's). There are three types of BPDU's:

- Configuration BPDU
- Topology Change Notification (TCN)
- Topology Change Acknowledgement (TCA)[9]

BPDU's are sent every 2 seconds on the network. All the other root paths are later disabled. Sometimes it happens so that the root bridge has more than 1 port available on the network. In such cases a tie occurs. This is resolved by putting the lowest port number in Forwarding mode and all others are blocked.

When new devices such as computers or printers are added in the network they immediately do not start transmitting data. They go through various states and move to forwarding state in about 30 seconds. This delay is introduced due to learning and listening states of the switch. The following switch states are of Spanning tree protocol are:

- Blocking
- Listening
- Learning
- Forwarding
- Disabled

Blocking state is introduced on the port if the newly added device causes a loop in the network. BPDU data is still sent to the switch in blocking mode. Listening mode processes BPDU's and wait for possible information that can introduce a blocking state. In learning state, the port starts receiving frames and source addresses which are added to the MAC address table. In forwarding state the port starts sending and receiving frames like in a normal operation. Disabled state is generally introduced while spanning tree formation or that can be explicitly done by network administrator.

Spanning tree protocol has its own drawbacks. The delay in moving to forwarding state is to large. Improper configuration can lead to network disruptions. Blocking of available paths is not considered as a viable method in modern networks.

IV. Working Of Software Defined Networks

A SDN architecture comprises of an Application layer, Control layer and Architecture layer. SDN architecture can be implemented in two ways, either by use of Overlay networks or by implementation of Open Flow protocol. Most commonly used SDN architecture is Open Flow API based.

I.5 Overlay based SDN

An overlay network is a computer or storage network built on top of another network and connected by virtual or logical links. Overlay networks have the advantage over Open SDN that they are not limited by physical

connections between the switches and routers. This makes the network more agile and provides machine mobility. The only challenge faced in implementation in Overlay networks that network administrators are unable to visualize the network[10].

I.6 Open Flow SDN

In Open SDN, the different layers of architecture make use of API's for intercommunication. The problem with networking is that applications which act as user interfaces cannot directly communicate with the network devices. They require an intermediate layer to communicate with devices as they are proprietary vendor devices. So,the Application layer makes use of north bound API which is used to communicate with the Control Layer. These north bound API's may include REST or Java based API. These API's help communication between the Application layer which acts as a user interface and the control layer which consists of the Open Flow controller. This controller is responsible for routing the packets through the data center network. The controller on other hand communicates with the architecture layer using south bound API's. These API's consists of Open Flow API used for direct communication with network devices[11].

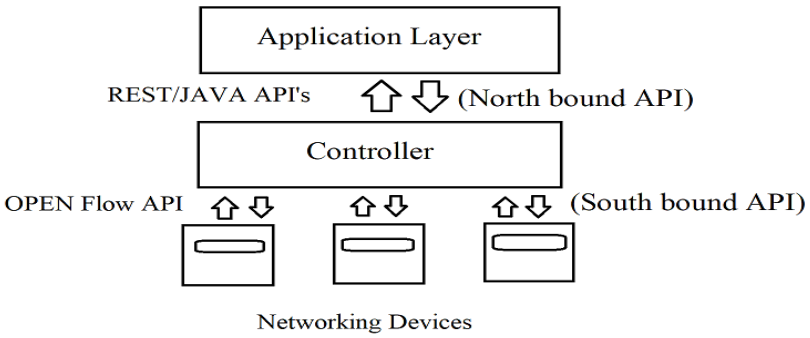

Fig 4. Open SDN Architecture

The Open Flow API comprises of the Open Flow protocol. This allows the controller to manipulate the flow tables in the switches. The Open Flow protocol does not allow users to update configuration of networking devices, thus it is used with other protocols like NETCONF or SNMP. The user does not need to know about the physical ASIC's of the switches in order to updates the flow tables. In a pure SDN architecture, the switches in the architecture layer do not posses any processing power.

A Open Flow switch consists of following components

1. Open Flow Channel
2. Group Table
3. Flow Table

Open Flow channel is used to connect the switch to the Open Flow controller. A group table is a special kind of flow table. It consists of group entries which comprise of a identifier and a action bucket. Action buckets consists of multiple forwarding addresses or actions to be carried out on a particular packet. On the other side flow table consists entries for single routing destinations throughout the network.

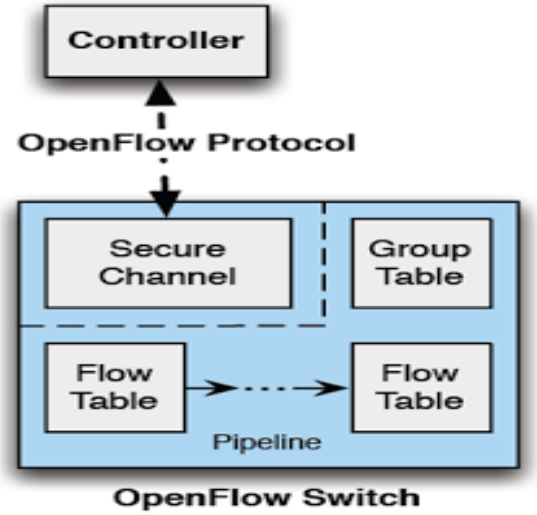

Fig. 5 Open Flow Switch

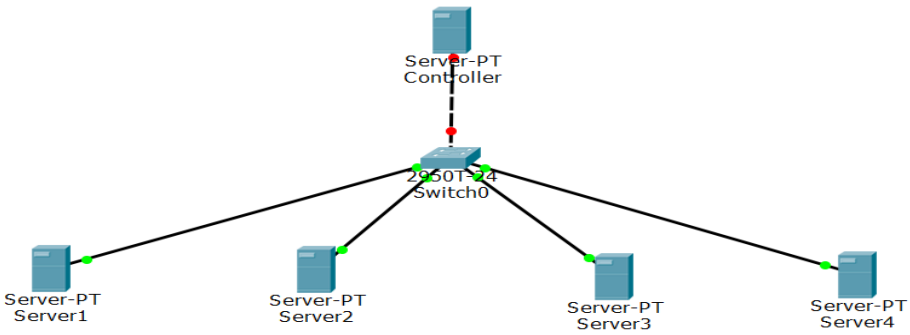

Fig. 6 Server setup in order to understand the Flow-MOD packet.

In above Fig. 6, consider a packet is to be sent from Server 1 to Server 4. Now the packet is first forwarded to the local switch. Since it is the first packet there are no corresponding matching values in the flow table for the following entry. Thus the switch caches a copy of the packet, and forwards a copy of the packet to the SDN controller a Packet-In message. The controller then processes the request according to user specified rules, and returns a message with a Packet-Out message. This Packet-Out message consists of the buffer id of the cached message and the action to be carried out with the packet. Another message the controller sends to the switch is the Flow-MOD packet. This Flow modification message which instructs the switch to add a new entry in the flow table. Another fields in the Flow modification message are timeouts. The timeouts in flow modification message are of two types.

1. Idle timeout
2. Hard timeout

Idle timeout indicates that if same flow entry is not available for the given time period then the flow entry is to be dropped from the table. Hard timeout indicates whether there is a request for the same flow entry or not, the entry is to be removed from the flow table. Each flow entry is also allocated some specific priority. So if two request for same destination are matched then the request with higher priority is serviced and the other packet is dropped[12].

V. APPLICATIONS OF SOFTWARE DEFINED NETWORKING

SDN technology is a flexible technology in networking and can be applied in various forms of networks due to its programmability which makes it more adaptable to any given network situation to work on. Following are some implementations of SDN technology.

- SDMN (Software Defined Mobile Networking)
- SD-WAN (Software Defined Wide Area Networks)
- SD-LAN (Software Defined Local Area Network)
- Security using SDN model
- Group Data delivery in SDN

I.7 SDMN

Mobile vendors often are interested in gaining access to the mobile user Internet of WI-FI access points in order to monitor their data usage activities. This may be for the purpose of increasing the QOS for the customers or as a part of data analysis as to how much a data traffic user generates. This can be achieved by doing the following

- Captive Portals
- Tunnelling
- Application policy

A web page is displayed to the new users which acts like a portal. These portals are commonly used as landing or log-in page which may require authentication. After authentication user is granted required levels of access. In tunnelling, after user has connected to the network access point, a Open Flow Enabled access point is already created by the vendor or the controller of your network. This tunnels the traffic to the vendor-network which then in turn diverts traffic to the internet. According to ONF's Wireless and Mobile Networking group ,there are various specific applications implemented in mobile systems through Open Flow Architecture. Some of them are as follows:

- Management and secured flow in LTE.
- Dynamic resource management in between the core and backbone wireless networks.
- Mobile traffic management.
- Security optimisation in wireless networks.
- Centralised access management for large enterprises or campuses.

I.8 SD-WAN

One of the drawbacks of traditional ethernet-based WAN's is that if a link fails between any two nodes there is loss of connectivity. Hence when a alternate route is selected for routing it is not necessarily optimal due to lack of central view of the overall network and other factors like bandwidth. Thus SDN controllers are a solution for these decisions and provide efficient routes in case of line failures. In industrial WAN's, they use applications like sFlow to monitor and manage network traffic and collect information to make routing optimal in the network, sFlow is an industry standard which makes use of truncated network packets with interface counters to monitor the network.

Multiprotocol label switching (MPLS) makes use of labels to route packets in network rather than using IP addresses and complex lookups in a routing table. The routes used in MPLS is called a *label switch paths* (LSP). They are also sometimes known as MPLS tunnels. Both of the abovementioned protocols are based on the working of SDN. Google has been using SDN technologies since its outset and all of its data centers have been implementing SDN Open Flow switches for optimal routing in consideration with the bandwidth and network traffic. Use of SDN architecture also makes the network management cost efficient[13].

I.9 SD-LAN

LAN's are generally implemented in area's like campuses, office or a large building. Connections in LAN are generally done by Wireless Access Points or through wire links. There are certain requirements that apply to specific Corporate/Office LAN networks. They are

- Various level of security access
- BYOD (Bring Your Own Device) connectivity
- Access control and security monitoring
- End-User Firewalls

In general, the daily users of any given campus network can be employees or guest users. The access level which is to be granted to a employee may not limit only to the internet but also the company database. On the other hand a guest user cannot be given access to such sensitive data. Also since employees are familiar and comfortable with working of their own devices like laptops and tablets, instead of the devices provided by the organisation. This increases the risk of affecting the network through an infected device. Thus the firewall rules of the employee devices also need to be properly defined. Now these requirements can be easily addressed by implementation of SDN in LAN's. Whenever a user tries to send in network traffic into the network, initially there is no policy assigned to the user's end so it's initial packets are forwarded to the central SDN controller. The controller gets the specific rules for the user firewall, which specifies the level of access for the user and also the firewall rules for the same[13].

I.10 Security based on SDN

As discussed in the above section of LAN and WAN implementations using SDN's, security in any network can also be handled by use of the same techniques as in LAN and WAN. Recent use of employee devices instead of organisation provided devices at various campuses is a technological trend. But an infected employee device can be a threat to the network. This is done through *captive portal* logins which assign the correct level of access. The SDN controller is situated at the end of the network where it can monitor the activities of the nodes consisted in the network. This how check take place

- A node makes a DHCP request to obtain IP address.
- When an DHCP response is received, a copy of it is sent to the controller.
- The controller matches the node's MAC address with user's database.
- If an entry is available then the HTTP traffic is forwarded to the node.
- Else the traffic is forwarded to the captive portal server and after the node is registered the traffic is routed back to the node in network.

Various research on SDN switches have been worked out to fight some of the well known internet threats. These threats include Distributed denial of service, botnets, and virus propagation. The idea is to keep check on the network traffic from the forwarding plane by use of some SDN protocol's which reprogram the data plane in order to handle anomalies, if detected.

SDN protocols also allow administrators to implement MTD algorithms(Moving Target Defence). These algorithms facilitate user to make periodic changes to important properties of network and the system. It is difficult to implement this strategy in orthodox networks as there is no established central authority. One of the key properties which can be changed are virtual IP's assigned to the hosts in the network. This makes it difficult for the attacker to penetrate the network[13].

I.11 Group Data Delivery in SDN

Data centres usually replicate data in order to have synchronisation and bring data closer to

the users. Data replication allows the system to continue working properly in case of failure or crash. It also makes data recovery easy. All these operations require data transmission from one machine to other machines. This process is termed as Reliable Group Data Delivery(RGDD).
RGDD can be implemented in SDN protocols by simply installing rules for multiport delivery. But such setups require to take into consideration the network congestion/load status to maximise its performance in real-time delivery.

VI. CONCLUSION

From the above information so far we can assume that the ease of network traffic management provided in Software-defined Networking approach is far more relaxed then existing protocols. User driven network with massive cost savings is a upper hand in this approach. Also centralized control and high granularity control of network flow enables efficiency. Dynamicity of this approach in future may allow more efficient ways of communication and also the and also programmability does not limit the application of Software-defined Networking.

REFERENCES

[1]. Benzekki Kamal et al.Software-defined networking (SDN): a survey, Security and Communication Networks 9, no. 18 (2016): 5803-5833.
[2]. "Software-Defined Networking (SDN) Definition". Opennetworking.org. Retrieved 26 October 2014.
[3]. Balchunas, Aaron. "Routing Information Protocol(RIP v1.03)". http://www.routeralley.com. Retrieved 25 April 2014.
[4]. Wick, Karl (18 April 2007). "What is route poisoning?". Retrieved 2009-01-23.
[5]. A Routing Procedure for the TIDAS Message-Switching Network, IEEE Transactions on communication 1975.
[6]. > "RFC 4271 - A Border Gateway Protocol 4 (BGP-4)". ietf.org.
[7]. "BGP Keepalive Messages - InetDaemon's IT Tutorials". inetdaemon.com.
[8]. BGPstate machine. https://en.wikipedia.org/wiki/File:BGP_FSM.svg
[9]. Cisco (October 2005). "Understanding Spanning-Tree Protocol Topology Changes". Retrieved 2014-06-10.
[10]. What is the difference between an overlay network and SDN". Techtarget.com. Retrieved 11 January 2018.
[11]. David Bombal ."SDN and OpenFlow Overview - Open, API and Overlay based SDN". Youtube.com, 28 October 2014.
[12]. David Mahler. "Introduction to OpenFlow". Youtube.com, 7 October 2013.
[13]. Paul Goransson, Chuck Black. SDN in Other Environments in *Software Defined Networking: A Comprehensive Approach*,(MA, Morgan Kaufmann, 2014)178-184.

International Journal of Engineering Science Invention (IJESI) is UGC approved Journal with Sl. No. 3822, Journal no. 43302.

Shyam Patil "Efficient Network Management: A Software Defined Networking Approach" International Journal of Engineering Science Invention (IJESI), vol. 07, no. 03, 2018, pp 55-63.