31 August 2016

Managing WANs in MNC Enterprises

Layer 2 and Layer 3 Switching

Assignment Report

Course: Computer Networks (CO300)

Degree / Semester: B.Tech. / Fifth

Department: Computer Science and Engineering

Submitted by

S. No	Reg. No	Name	Signature
1.	14CO202	Alla Pranathi	
2.	14CO203	Anirudh Sriram	

3.	14CO204	Aparna R Joshi	
4.	14CO205	B. Sandhya Rani	
5.	14CO206	C.B.Yuvaraj	
6.	14CO207	Chiranjeevi A.R.Hegde	
7.	14CO208	Deepak Srikanth	
8.	14CO209	D. Teja Sri	

Table of Contents

Managing WANs in MNC Enterprises - Layer 2 and Layer 3 Switching

Assignment Report

1. Overview

A network switch (also called switching hub or bridging hub) is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI Model. Switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality that most commonly uses IP addresses to perform packet forwarding; such switches are commonly known as layer-3 switches or multilayer switches.

1.1. Layer 2 Switching

Layer 2 switching uses the media access control access (MAC address) from the host's network interface cards (NICs) to decide where to forward frames. Layer 2 switching is hardware-based, which means switches use application-specific integrated circuits (ASICs) to build and maintain filter tables (also known as MAC address tables or CAM tables. One way to think of a layer 2 switch is as multiport bridge.

Layer 2 switching provides the following

- Hardware-based bridging (MAC)
- Wire speed/non-blocking forwarding
- Low latency

Layer 2 switching is highly efficient because there is no modification to the data packet and the frame encapsulation of the packet changes only when the data packet is passing through dissimilar media (such as from Ethernet to FDDI).

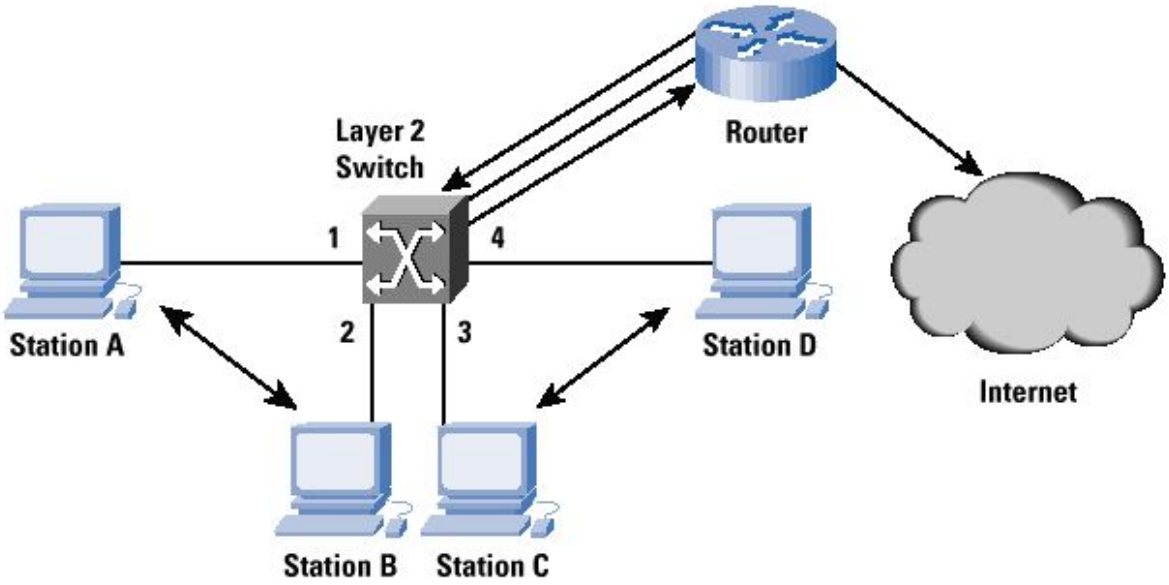
They are similar to multiport bridges in that they learn and forward frames on each port. The major difference is the involvement of hardware that ensures that multiple switching paths inside the switch can be active at the same time.

Layer 2 switches learn MAC addresses automatically, building a table which can be used to selectively forward packets. For example, if a switch receives packets from MAC address X on Port 1 it then knows that packets destined for MAC address X can simply be forwarded out of that port rather than having to try each available port in turn.

Because Layer 2 information is easily retrieved, packets can be forwarded (switched) very quickly, typically, at the wire speed of the network. Layer 2 switching, therefore, has little or no impact on network performance or bandwidth. And because they are relatively dumb devices, no setup or management is required, making them cheap and easy to deploy.

However, Layer 2 switches cannot use any intelligence when they forward packets. They cannot forward packets based on IP address or prioritise packets sent by particular applications. For example, layer 2 switches cannot guarantee bandwidth to VoIP users.

The information required for such switching only starts to become available at Layer 3 (the Network Layer).



Layer 2 switch with External Router for Inter-VLAN traffic and connecting to the Internet

1.2. Layer 3 Switching

Layer 3 switching is solely based on (destination) IP address stored in the header of IP datagram. The difference between a layer 3 switch and a router is the way the device is making the routing decision. Traditionally, routers use microprocessors to make forwarding decisions in software, while the switch performs only hardware-based packet switching.

Because many layer 3 switches offer the same functionality as traditional routers they can be used as cheaper, lower latency replacements in some networks. Layer 3 switches can perform the following actions that can also be performed by routers:

- Determine paths based on logical addressing
- Run layer 3 checksums (on header only)
- Use Time to Live (TTL)
- Process and respond to any option information
- Update Simple Network Management Protocol (SNMP) managers with Management Information Base (MIB) information
- Provide Security

Intelligent packet forwarding (routing) based on Layer 3 information is traditionally the function of routers. It's here that IP addresses are found, for example, enabling a router to link different subnets together. Specialised routing protocols also use Layer 3, enabling routers to "learn" routes between networks.

In recent years, however, that same functionality has also been built into network switches. Routers are still used to forward packets across (relatively) slow WAN (Wide Area Network) connections but on local networks, high-performance Layer 3 switches - sometimes referred to as "switch routers" or "routing switches" - have largely replaced them.

Other intelligence commonly found in Layer 3 switches, includes the ability to logically segment a network into two or more Virtual LANs (VLANs) plus enhanced security controls to prevent unauthorised setup changes. Facilities to prioritise different types of traffic are also commonplace, to provide guaranteed Quality of Service (QoS) when, for example, building converged voice and data networks.

2. MPLS Networking

Multiprotocol Label Switching (MPLS) is a protocol for speeding up and shaping network traffic flows.

MPLS allows most packets to be forwarded at Layer 2 (the switching level) rather than having to be passed up to Layer 3 (the routing level). Each packet gets labeled on entry into the service provider's network by the ingress router. All the subsequent routing switches perform packet forwarding based only on those labels—they never look as far as the IP header. Finally, the egress router removes the label(s) and forwards the original IP packet toward its final destination.

MPLS works by prefixing packets with an MPLS header containing one or more labels – a label stack. The label itself is a four-byte, fixed-length identifier which is used to identify a Forwarding Equivalence Class (FEC). An FEC is a group of IP packets which are forwarded in the same manner, over the same path, with the same priority and the same label. The label on a particular packet indicates the FEC to which that packet is assigned.

The label is imposed between the data link layer header and network layer header. Since the label resides between Layer 2 and Layer 3 in the OSI model, MPLS can sometimes be referred to as a **“Layer 2.5”** protocol.

2.1. Layer 2 Switching

One ought to keep in mind that when we talk about MPLS it is a technique, not a service — so it can be used to deliver anything from IP VPNs to metro Ethernet service. Thus although carriers build MPLS backbones, the services that users purchase may not be called “MPLS”. They could be called anything from “IP VPN” to metro Ethernet. One such label is the MPLS VPN.

A Layer 2 MPLS VPN is a term in computer networking. It is a method that Internet service providers use to segregate their network for their customers, to allow them to transmit data over an IP network. This is often sold as a service to businesses.

Layer 2 VPNs are a type of Virtual Private Network (VPN) that uses MPLS labels to transport data. The communication occurs between routers that are known as Provider Edge routers (PEs), as they sit on the edge of the provider's network, next to the customer's network.

Layer 2 (L2) MPLS VPNs resemble a virtual circuit type service and are very effectively used by service providers in the Metro Ethernet field. There are two main RFCs that define two L2 MPLS VPN topologies:

1. The concept of virtual circuits as another overlay label switched path (LSP) inside a tunnel LSP. It addresses the problem of point-to-point VPN connections in MPLS VPNs.
2. The second important RFC on the label distribution protocol (LDP), specifies the virtual private LAN service (VPLS), which presents a solution for multipoint connectivity for the Layer 2 MPLS VPN.It expands the concept to a full mesh network topology. VPLS is commonly marketed under the name "Enterprise Private LAN."

In discovering MPLS VPN types, we may also encounter the term pseudowire. Pseudowires offer point-to-point WAN transport. A pseudowire is an industry term for transport of any frame over an MPLS network that uses MPLS to encapsulate packets and uses LDP as a signaling mechanism. Cisco calls pseudowires Any Transport over MPLS (AToM). This is the building block of Layer 2 VPNs over MPLS.

2.2. Layer 3 Switching

MPLS-based VPNs are created in Layer 3 and are based on the peer model. The peer model enables the service provider and the customer to exchange Layer 3 routing information. The service provider relays the data between the customer sites without the customer's involvement. When a new site is added to an MPLS VPN, only the service provider's edge device that provides services to the customer site needs to be updated. Hence making MPLS VPNs easy to manage.

Centralized routers and edge-based access devices, which had to interface with protocols other than Ethernet, added management intelligence and MPLS support to their core switch chips, thus making these devices Layer 3 switches.

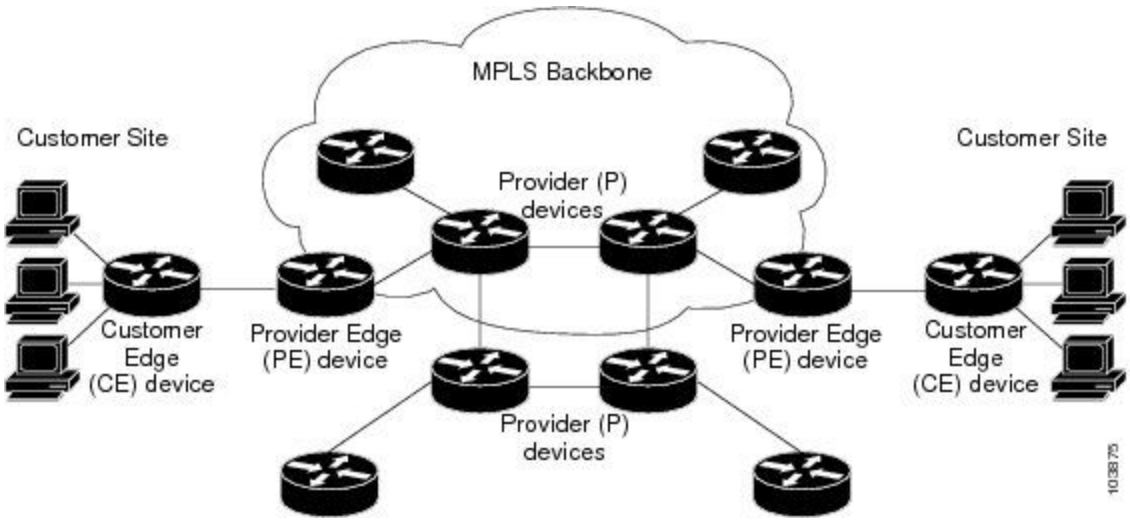
The different parts of the MPLS VPN are described as follows:

- Provider (P) device—Device in the core of the provider network. P devices run MPLS switching, and do not attach VPN labels to routed packets. The MPLS label in each route is assigned by the provider edge (PE) device. VPN labels are used to direct data packets to the correct egress device.
- PE device—Device that attaches the VPN label to incoming packets based on the interface or subinterface on which they are received. A PE device attaches directly to a customer edge (CE) device.
- Customer (C) device—Device in the ISP or enterprise network.
- CE device—Edge device on the network of the ISP that connects to the PE device on the network. A CE device must interface with a PE device.

The CE routers exchange their routing tables with the PE routers via standard routing protocols (RIP, OSPF, EIGRP and BGP).

The PE routers store the routing updates from each customer's CE router in a virtual router field or VRF. Each CE router has its own VRF on the PE. The customer then advertises all routes associated with that location to the PE. Once all the PE routers that connect to a particular customer have the customer's routing information in a VRF, the PE routers exchange information using multiprotocol BGP. These routes and the corresponding VRFs make up the customer VPN.

Basic MPLS VPN Terminology



3. Carrier Ethernet

Carrier Ethernet is the use of high-bandwidth Ethernet technology for Internet access and for communication among business, academic and government local area networks (LANs).

Carrier ethernet vs. traditional ethernet:

Traditional ethernet is most commonly used for the implementation of local area networks (LANs). Traditional ethernet is augmented with features to provide additional features that can help the provider build network infrastructure or build MANs and WANs.

To implement WAN or MAN, an entire organization connects to a Carrier Ethernet “port” at a given subscriber location. The Carrier Ethernet network serves many organizations or branches of organizations.

Carrier Ethernet services can be delivered not only over traditional (native) Ethernet-based networks but can also over other transport technologies. Examples of underlying transport mechanisms that could be used are:

- Native Ethernet
- MPLS-based Layer 2 Virtual Private Networks (VPNs)
- IEEE 802.1ad Provider Bridges
- Ethernet over SONET

By this uniform approach, carrier ethernet extends the benefits of ethernet to provide cost efficiency.

Here, we examine carrier ethernet using the underlying transport mechanism of native ethernet.

3.1 Carrier Ethernet: Layer 2

At layer 2, switches have access to MAC addresses, which can be used to build tables for selective forwarding of frames. This allows extremely fast forwarding/switching of packets, which leads to negligible impact on network performance and bandwidth.

The layer 2 transport service over MPLS is implemented using two level label switching between the edge routers. The label used to route the packet over the MPLS backbone to the destination is called the “tunnel label” while the label used to determine the egress interface is called the “VC label”. It encapsulates Ethernet protocol data units (PDUs) inside MPLS packets and forwards the packets, using label stacking, across the MPLS network. This technology has applications in service provider, enterprise and datacenter environments.

Further, layer two switches are generally passive devices, making them easy to manage and cheap to deploy. However, they lack the ability to make decisions or apply intelligence in directing packets. This functionality is only available in layer 3.

3.2 Carrier Ethernet: Layer 3

Unlike layer 2 switching which uses hardware addresses such as MAC addresses for forwarding, layer 3 switching uses IP address for forwarding packets.Traditional routes traffic between its ports according to MAC addresses of connected devices. Layer 3 switches improve on this by using IP address to route when managing traffic in network.

Carrier Ethernet, is the extension of Ethernet that enables service providers to provide premium Ethernet services. In a Carrier Ethernet network, data is transported across point to point and multipoint to multipoint using ethernet virtual connections. Let us look at different carrier Ethernet services:

· Ethernet Virtual Private Line or E-Line: a service connecting two customer Ethernet ports over a WAN.

· Ethernet Virtual Private LAN or E-LAN: a multipoint service connecting a set of customer endpoints, giving the appearance to the customer of a bridged Ethernet network connecting the sites.

· Ethernet Virtual Private Tree or E-Tree: a multipoint service connecting one or more roots and a set of leaves, but preventing inter-leaf communication.

Now let us see whether we can implement layer 3 VPNs in Carrier Ethernet Services.

Layer 3 VPN is a technology where the traffic will be carried over pseudowires (PW) over MPLS Label Switch Paths (LSPs) tunnels. Forwarding is based on IP addresses, thereby making it layer 3 based and hence the name layer 3 VPN.The network infrastructure comprises routers that are MPLS-capable. Such a network can provide connectivity service to subscribers, in a similar manner to the way CEN provides ethernet services.

These services provided by layer 3 VPN are non-standard and at present there is no organisation (standard development) attempting to create standards for such services.

In contrast to Layer 3 VPN, ethernet services are built on the concept of ethernet based forwarding, hence can be referred to as layer 2 VPN. In some cases a global solution may result in a combination of L2VPN and L3VPN services. The main reason is that for long haul, forwarding based on Ethernet addresses sometimes does not scale sufficiently, whereas L3 VPNs are available throughout the globe on international links.

Summary:

The advantages of layer 2 switching lie in its low level of latency and high speed switching. However, layer 3 switches are capable of intelligent routing and provide a scalable platform for MPLS implementation.

4. SDN Architecture

An SD-WAN is a Wide Area Network (WAN) managed using the principles of software-defined networking. The main drive of SD-WAN is to lower WAN costs using less expensive leased lines, as an alternative or partial replacement of more expensive MPLS lines. Control and

management is separated from the hardware, with central controllers allowing easier configuration and administration.

Figure 1 illustrates the logical structure of an SDN. A central controller performs all complex functions, including routing, naming, policy declaration, and security checks. This plane constitutes the *SDN Control Plane,* and consists of one or more SDN servers.

The *SDN Controller* defines the data flows that occur in the *SDN Data Plane*. Each flow through the network must first get permission from the controller, which verifies that the communication is permissible by the network policy. If the controller allows a flow, it computes a route for the flow to take, and adds an entry for that flow in each of the switches along the path. With all complex functions subsumed by the controller, switches simply manage flow tables whose entries can be populated only by the controller. Communication between the controller and the switches uses a standardized protocol and API. Most commonly this interface is the OpenFlow specification, discussed subsequently.

SDN at different layers:

The SDN architecture is remarkably flexible; it can operate with different types of switches and at different protocol layers. SDN controllers and switches can be implemented for ethernet switches (Layer 2), internet routers (Layer 3), transport (Layer 4) switching, or application layer switching and routing. SDN relies on the common functions found on networking devices, which essentially involve forwarding packets based on some form of flow definition.

New Generation of Layer-2 and Layer-3 switches and routers – network devices that are scalable, fault tolerant with high availability, performance on par with wiring closets along with investment protection against technological advancements. Layer-2, Layer-3 control protocols would run as Controller Applications and make the converged flow entries into data path through controller.

Within each switch, a series of tables—typically implemented in hardware or firmware—are used to manage the flows of packets through the switch.In an SDN architecture, a switch performs the following functions:

- The switch encapsulates and forwards the first packet of a flow to an SDN controller, enabling the controller to decide whether the flow should be added to the switch flow table.
- The switch forwards incoming packets out the appropriate port based on the flow table. The flow table may include priority information dictated by the controller.

- The switch can drop packets on a particular flow, temporarily or permanently, as dictated by the controller. Packet dropping can be used for security purposes, curbing Denial-of-Service (DoS) attacks or traffic management requirements.

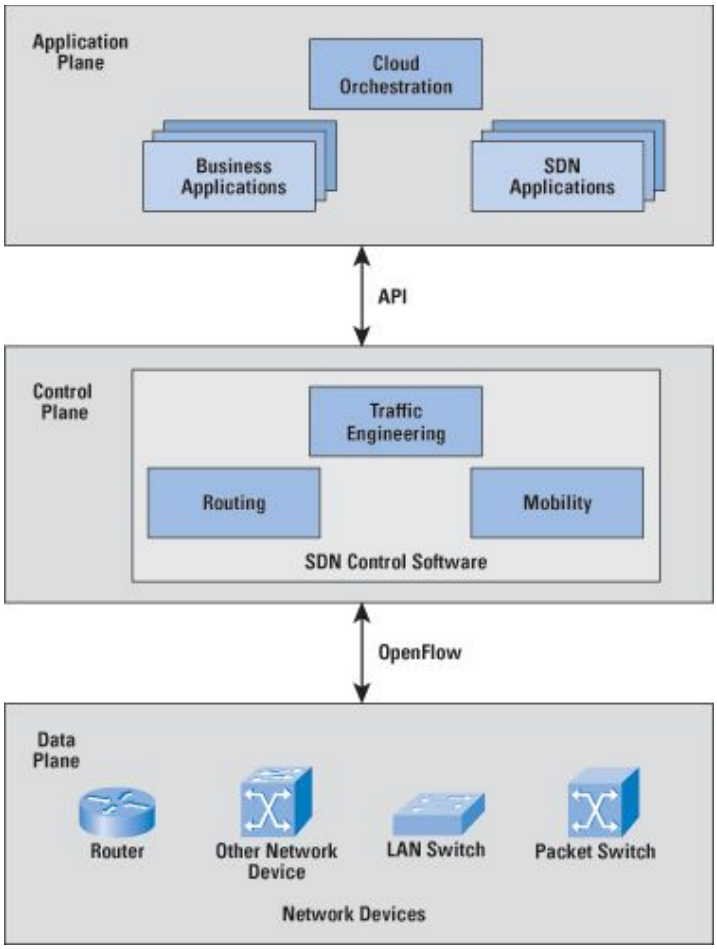
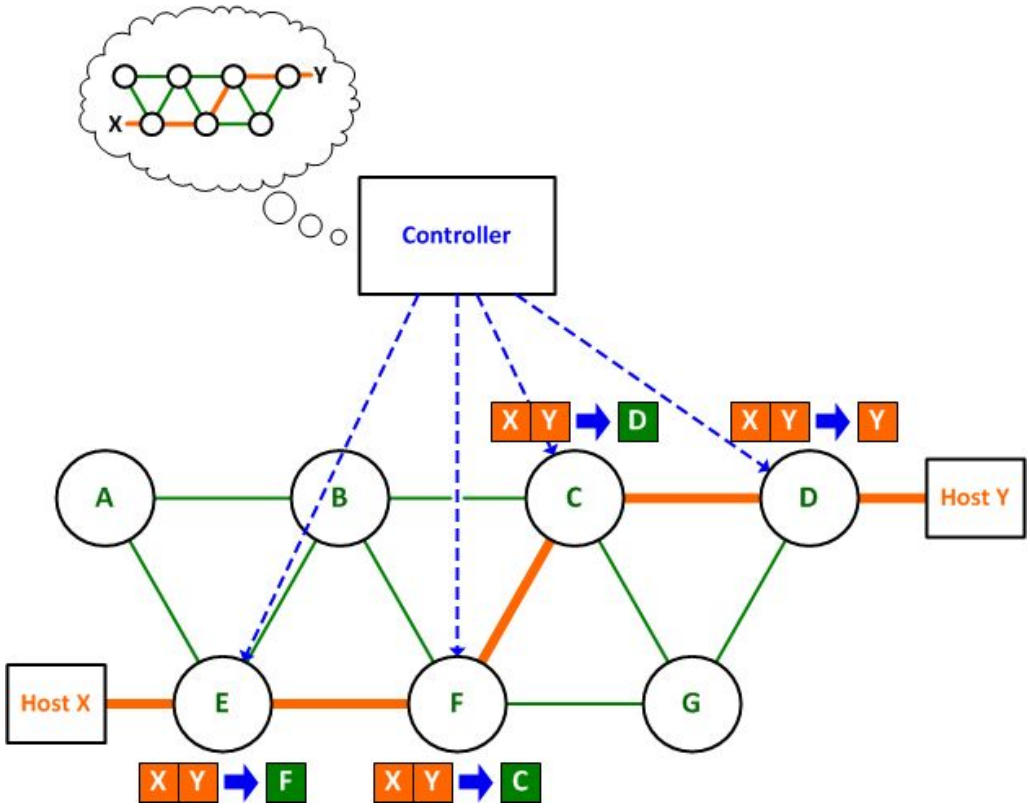


Figure 1

Consider a layer two switching topology with redundant paths. Normally, spanning tree (a control plane process) is needed to guard against loops because no individual switch knows what the entire network looks like. However, if the control plane functions for all switches are offloaded to a central controller as in SDN, that controller can "see" the entire network and install forwarding decisions to each subordinate switch based upon the desired end-to-end path for each destination or flow while keeping all links active.

SDN appears to be an abstraction of DNS for packet switching, designed for the network. In the SDN switch model, the controller does have that visibility - just like a root DNS service - and can provide a definitive answer to the question as to where should it send the packet.



The SDN controller manages the forwarding state of the switches in the SDN.With the decoupling of the control and data planes, SDN enables applications to deal with a single abstracted network device without concern for the details of how the device operates. Network applications see a single API to the controller. Thus it is possible to quickly create and deploy new applications to orchestrate network traffic flow to meet specific enterprise requirements for performance or security.

Reasons for using SDN domains include Scalability, privacy, incremental deployment,coordinate flow setup originated by applications containing information such as path requirement, QoS, data rate, latency and service-level agreements across multiple SDN domains, exchange reachability information to facilitate inter-SDN routing etc.

Summary:

SDNs, implemented using OpenFlow, provide a powerful, vendor-independent approach to managing complex networks with dynamic demands. The software-defined network can continue to use many of the useful network technologies already in place, such as virtual LANs and an MPLS infrastructure. SDNs and OpenFlow are likely to become commonplace in

large carrier networks, cloud infrastructures, and other networks that support the use of big data.

5. Open Networking

In OpenStack network architecture, Layer-2 decisions involve those made at the data-link layer, such as the decision to use Ethernet or Token Ring. Layer-3 decisions involve those made about the protocol layer and the point when IP comes into the picture.

Two competing trends in networking one of which leans towards building data center network architectures based on layer-2 networking whereas the other treats the cloud environment essentially as a miniature version of the Internet. The Internet only uses layer-3 routing rather than layer-2 switching.

A network designed on layer-2 protocols has advantages over one designed on layer-3 protocols. In spite of the difficulties of using a bridge to perform the network role of a router, many vendors, customers, and service providers choose to use Ethernet in as many parts of their networks as possible. The benefits of selecting a layer-2 design are:

- Ethernet frames contain all the essentials for networking. These include globally unique source addresses and destination addresses, and error control.
- Ethernet frames can carry any kind of packet. Networking at layer-2 is independent of the layer-3 protocol.
- Adding more layers to the Ethernet frame only slows the networking process down. This is known as ‘nodal processing delay’.

Most information starts and ends inside Ethernet frames. Today this applies to data, voice (for example, VoIP), and video (for example, web cameras). The concept is that if more of the end-to-end transfer of information from a source to a destination in the form of Ethernet frames can be performed, the network benefits more from the advantages of Ethernet. Although it is not a substitute for IP networking, networking at layer-2 can be a powerful adjunct to IP networking.

Layer-2 Ethernet usage has these advantages over layer-3 IP network usage:

- Speed
- Reduced overhead of the IP hierarchy.
- No need to keep track of address configuration as systems move around. Whereas the simplicity of layer-2 protocols might work well in a data center with hundreds of physical machines, cloud data centers have the additional burden of needing to keep track of all virtual machine addresses and networks. In these data centers, it is not uncommon for one physical node to support 30-40 instances.

Layer-2 architecture limitations

Outside of the traditional data center the limitations of layer-2 network architectures become more obvious.

- The number of MACs stored in switch tables is limited.
- One must accommodate the need to maintain a set of layer-4 devices to handle traffic control.
- MLAG, often used for switch redundancy, is a proprietary solution that does not scale beyond two devices and forces vendor lock-in.
- It can be difficult to troubleshoot a network without IP addresses and ICMP.
- Configuring ARP can be complicated on large layer-2 networks.

Layer-3 architecture advantages

In the layer-3, there is no churn in the routing tables due to instances starting and stopping. The only time there would be a routing state change is in the case of a Top of Rack (ToR) switch failure or a link failure in the backbone itself. Other advantages of using a layer-3 architecture include:

- Layer-3 networks provide the same level of resiliency and scalability as the Internet.
- Controlling traffic with routing metrics is straightforward.
- Routing takes instance MAC and IP addresses out of the network core, reducing state churn. Routing state changes only occur in the case of a ToR switch failure or backbone link failure.
- There are a variety of well tested tools, for example ICMP, to monitor and manage traffic.
- Layer-3 architectures enable the use of *quality of service (QoS)* to manage network performance.

OpenStack Networking:

- Complex, multiple agents
- Newer, maturing
- Flat, VLAN, Overlays, L2-L3, SDN
- Plug-in support for 3rd parties
- Scaling requires third party plugins
- Multi-tier topologies

6. Members Contributions

S. No	Reg. No	Name	Contribution(s)
1.	14co202	Alla Pranathi	MPLS Layer 3 architecture description
2.	14co203	Anirudh Sriram	Layer 2 and Layer 3 carrier ethernet architecture. Advantages and disadvantages of either.
3.	14co204	Aparna R Joshi	Overview of Layer 2 and Layer 3 switching, and description about Layer 2 switching in MPLS.
4.	14co205	B.Sandhya Rani	Details about SDN architecture and Open networking - Layer 2,3 architectures.
5.	14co206	C.B.Yuvaraj	Description about Layer 3 switching in Carrier Ethernet and about carrier ethernet services.
6.	14co207	Chiranjeevi A.R.Hegde	Layer 3 switching in Carrier Ethernet and its services.
7.	14co208	Deepak Srikanth	Carrier Ethernet Description and layer 2 switching.
8.	14co209	D.Teja Sri	Description about the architecture implemented in the MPLS Layer 3 Switching.

7. References

[1] http://www.warwicknet.com/blog/multiprotocol-label-switching-mpls-part-2
[2] https://www.fujitsu.com/us/Images/CarrierEthernetEssentials.pdf
[3] http://packetlife.net/blog/2013/may/2/what-hell-sdn/
[4] http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-59/161-sdn.html
[5] http://docs.openstack.org/arch-design/network-focus-technical-considerations.html
[6] https://devcentral.f5.com/articles/sdn-is-dns-for-packet-switching

[7] https://wiki.mef.net/pages/viewpage.action?pageId=29229129