3rd October 2016

Assignment 3 - Protocols

Assignment Report

Course: Computer Networks (CO300)

Instructor: Prof. K. Chandrasekaran

Degree / Semester: B.Tech. / Fifth

Department: Computer Science and Engineering

Submitted by

S. No	Reg. No	Name	Signature
1.			
2.	14CO203	Anirudh Sriram	
3.	14CO204	Aparna R Joshi	

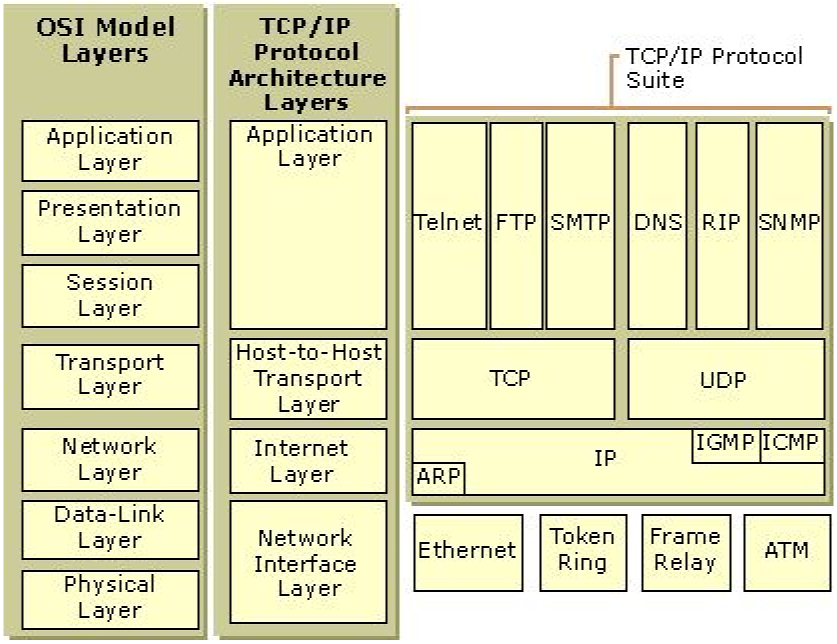
4.	14CO205	B. Sandhya Rani	
5.	14CO206	C.B.Yuvaraj	
6.			
7.	14CO208	Deepak Srikanth	

Table of Contents

Assignment 3 - Protocols

Assignment Report

1. Protocols in IEEE and OSI Models



Layer	Model(s)	Protocols	Explanation

Physical Layer	● OSI ● IEEE	Ethernet physical layer 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX and other varieties	The most common ethernet which is used to control the handling of data at the lowest layer of the network model is 802.3 ethernet. 802.3 ethernet provides a means of encapsulating data frames to be sent between computers. It specifies how network data collisions are handled along with hardware addressing of network cards.
		SONET/SDH	Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized protocols that transfer multiple digital bit streams synchronously over optical fiber using lasers or highly coherent light from light-emitting diodes (LEDs).
Data Link Layer	● OSI ● IEEE	SLIP	Serial Line Internet Protocol. This protocol places data packets into data frames in preparation for transport across network hardware media. This protocol is used for sending data across serial lines. There is no error correction, addressing or packet identification. There is no authentication or negotiation capabilities with SLIP. SLIP will only support transport of IP packets.
		PPP	Point to Point Protocol is a form of serial

			line data encapsulation that is an improvement over SLIP which provides serial bi-directional communication.
		CSLIP	Compressed SLIP is essentially data compression of the SLIP protocol. It uses Van Jacobson compression to drastically reduce the overhead of packet overhead. This may also be used with PPP and called CPPP.
Network Layer	● OSI ● IEEE	ARP	Address Resolution Protocol enables the packaging of IP data into ethernet packages. It is the system and messaging protocol that is used to find the ethernet (hardware) address from a specific IP number. Without this protocol, the ethernet package could not be generated from the IP package, because the ethernet address could not be determined.
		RARP	Reverse address resolution protocol is used to allow a computer without a local permanent data storage media to determine its IP address from its ethernet address.
		IP	Internet Protocol. Except for ARP and RARP all protocols' data packets will be packaged into an IP data packet. IP

			provides the mechanism to use software to address and manage data packets being sent to computers.
		ICMP	Internet control message protocol (ICMP) provides management and error reporting to help manage the process of sending data between computers. (Management). This protocol is used to report connection status back to computers that are trying to connect other computers. For example, it may report that a destination host is not reachable.
		IGMP	Internet Group Management Protocol used to support multicasting. IGMP messages are used by multicast routers to track group memberships on each of its networks.
Transport Layer	● OSI ● IEEE	TCP	TCP provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.
		UDP	UDP provides a one-to-one or

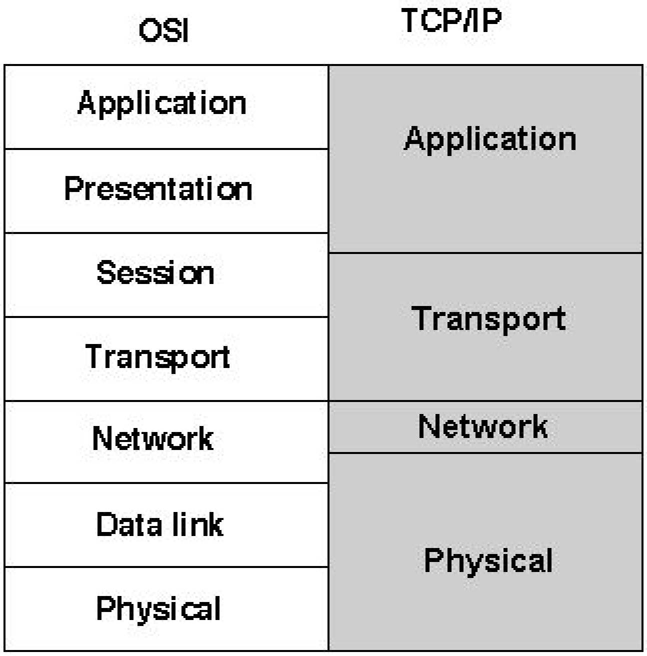
			one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.
Session Layer	● OSI	BGP	Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.
		NetBIOS	NetBIOS is an acronym for Network Basic Input/Output System. It provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.
		NFS	Network File System (NFS) is a distributed file system protocol allowing a user on a client computer to access files over a computer network much like local storage is accessed.
		TLS	Transport Layer Security (TLS) and its

Presentation Layer	• OSI		predecessor, Secure Sockets Layer (SSL), both frequently referred to as "SSL", are cryptographic protocols that provide communications security over a computer network.
Application Layer	• OSI • IEEE	FTP	File Transfer Protocol allows file transfer between two computers with login required.
		SMTP	Simple Mail Transfer Protocol is used to transport mail. Simple Mail Transport Protocol is used on the internet, it is not a transport layer protocol but is an application layer protocol.
		HTTP	Hypertext Transfer Protocol is used to transport HTML pages from web servers to web browsers. The protocol used to communicate between web servers and web browser software clients.
		BOOTP	Bootstrap protocol is used to assign an IP address to diskless computers and tell it what server and file to load which will provide it with an operating system.

		DHCP	Dynamic host configuration protocol is a method of assigning and controlling the IP addresses of computers on a given network. It is a server based service that automatically assigns IP numbers when a computer boots. This way the IP address of a computer does not need to be assigned manually. This makes changing networks easier to manage. DHCP can perform all the functions of BOOTP.
		Telnet	Telnet is used to remotely open a session on another computer. It relies on TCP for transport.

2. Comparison between OSI and IEEE Architecture

The mapping between layers in the IEEE TCP/IP and OSI layers is shown below.



As seen, the physical layer(Network access layer) in the TCP/IP model corresponds to the data link and physical layers in the OSI model. The Network(IP) layer is equivalent to the Network layer of the OSI model, the transport (or host-to-host or TCP layer) is equivalent to the Transport layer of the OSI model.Some functionality of this layer is also similar to the session layer in the OSI model. the Applications layer maps to the upper three layers in the OSI model

The following are the major similarities and differences between the models

Similarities:

- Both models share a similar, layered architecture.
- The lower layers- up to and including the transport layer- combine together to provide the same functionality in both models i.e. end-to-end transport service.
- The upper layers in both model are application oriented and use the functionality provided by the lower layers.

Differences:

- Reliability/Error handling: In the OSI model, each layer handles and detects errors. Each layer uses checksums to detect errors. On the other hand, error detection and handling in the TCP/IP model is concentrated in the Transport layer. Checksums, acknowledgements and timeouts are used to verify data integrity.

- The OSI model has a higher level of abstraction. Protocols in this model can be easily replaced as and when better protocols are made. In the TCP/IP model, changing protocols is not as easy.
- The OSI model is a more flexible model and can be used for different application. The TCP/IP model on the other hand can be used only for the Internet or similar applications.
- The role of the session layer in OSI model is to allow and maintain ongoing communications between two parties. This is called a session. In the TCP/IP model, there is no specific session layer. Its functionality is provided by the Transport/TCP layer.
- The Network layer (layer 3) of the OSI model provides functionality for both connection-oriented as well as connection-less networking. The IEEE model on the other hand only allows for exclusively connectionless networks.
- Unlike in the OSI model, when UDP protocol is used, delivery of packets is not guaranteed

3. TCP/IP Protocols for the Proposed Solution

TCP/IP protocols for MPLS:

MPLS is a protocol used to provide high speed data carrying technique that can be used with a range of access technologies such as ATM (Asynchronous Transfer Mode) and DSL (Digital Subscriber Line). It makes use of path labels to route packets through the network as opposed to long addresses. This makes routing more efficient and quicker. It is protocol and medium independent and thereby, versatile. When an unlabeled packet enters the ingress router and needs to be passed on to an MPLS tunnel, the router first determines the forwarding equivalence class (FEC) for the packet and then inserts one or more labels in the packet's newly created MPLS header. The packet is then passed on to the next hop router for this tunnel.

MPLS operates at a layer which is considered to be in between the second and third layers of the traditional OSI model, i.e. between the data link and transport layer. It is sometimes referred to as a layer 2.5 protocol.It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model.

Label Distribution Protocol:

A label switch router(LSR) is an MPLS router which performs routing based only on the label.This router is located in the middle of an MPLS network and responsible for switching the labels used to route packets.

A label edge router (LER) is an MPLS router that operates at the edge of an MPLS network and acts as the entry and exit points for the network.It is also known as edge LSR .LERs push an MPLS label onto an incoming packet and pop it off the outgoing packet.

In Label Distribution Protocol, labels are distributed between label switch routers and label edge routers.Label Distribution Protocol (LDP) is a protocol in which routers capable of Multiprotocol Label Switching (MPLS) exchange label mapping information. Two routers with an established session are called LDP peers and the information exchange is bi-directional. LDP is used to build and maintain LSP databases(Label Switched Paths, established by the network operator for a various purposes, such as to create network-based IP vpn)that are used to forward traffic through MPLS networks.

It is the protocol defined by the IETF for the purpose of distribution of labels in an MPLS environment. Label Distribution Protocol relies on the underlying routing information present in order to forward label packets. The router FIB(Forwarding information Base), determines the hop-by-hop path through the network. Unlike Traffic engineered paths, which use constraints and explicit routes to establish end-to-end Label Switched Paths (LSPs), LDP is used only for signaling label Switched Paths.

Border Gateway Protocol:

The Border Gateway Protocol (BGP) is a path vector protocol which acts as a core routing protocol of the Internet. BGP is an important internet protocol used by ISP to establish routing between one another. It maintains a table of IP networks or prefixes and assigns network reachability to autonomous systems; as a result it is indirectly used by the Internet users. iBGP protocol is used among the routers in autonomous system to command the internal routers.

When MPLS cloud is utilized at core, BGP can be deployed at the network edges with the core routers carrying just the information about the BGP’s next step. BGP establishes loop-free routes and share routing information among the group of routers (autonomous systems). MPLS cloud does not scatter BGP across the network. MPLS provides end to end transport for BGP routes. This can be done by running BGP everywhere, redistributing BGP into Interior Gateway Protocol and running GRE tunnel from PE to PE. In case of large scale network, run an MPLS free BGP core. Make sure to always use single area if open shortest path first option is implemented in network.

MPLS labels are added to the update messages that a router sends. Routers exchange the following types of BGP messages:

1. Open messages— once a TCP connection is established between routers they start transferring open messages. Every message contains IP address of the message sender and the AS number to which the router is connected.
2. Update messages— if the route is new, modified or broken then the router sends update message to the adjacent router. Update message includes both functioning and non functioning paths. The Network Layer Reachability Information (NLRI) in the message tracks the IP address of functioning routes.
3. Keepalive messages— Router sends signal to check the availability of nearby router. The signal is the Keepalive message which contains only the message header.
4. Notification messages— Router sends a notification message if an error is detected.

There are 2 kinds of notification messages:

1. Error notifications; these signal fatal errors and cause termination of the session
2. Advisory notifications; these are used to pass on LSR information about the LDP session or the status of some previous message received from the peer.

All LDP messages have a common structure that uses a Type-Length-Value (TLV) encoding scheme. This TLV encoding is used to encode much of the information carried in LDP messages. The Value part of a TLV-encoded object (TLV), may itself contain one or more TLVs.

The RSVP-TE (traffic extension) protocol is an addition to the RSVP protocol with special extensions to allows it to set up optical paths in an agile optical network.
The RSVP protocol defines a session as a data flow with a particular destination and transport-layer protocol. However, when RSVP and MPLS are combined, a flow or session can be defined with greater flexibility and generality

TCP/IP Protocols for Carrier Ethernet:

Ethernet is everyone’s favorite networking technology. Its ubiquity and popularity have pushed it outside the LAN and across almost all aspects of network infrastructure. When a way to naturally extend the Ethernet protocol to provide WAN connectivity was looked for, back in the early 2000s, the industry introduced Carrier Ethernet. It isn’t *just* for carriers—it’s a reliable and feature-rich solution perfect for all network operators who provide networking services to end-users.

The Carrier Ethernet is therefore, a marketing term for extensions to Ethernet to enable telecommunications network providers to provide Ethernet services to customers and to utilize Ethernet technology in their networks.

It is important to understand that all protocols found on ethernet links are true for carrier ethernet as well. The TCP/IP IEEE model is used as a model for developing data network protocols.Each layer works with the layers above and below them to enable communication with the same layer of another stack instance.\

Application Layer:

Telnet is a client-server protocol, based on a reliable connection-oriented transport. Generally, this protocol is used to establish a connection to Transmission Control Protocol(TCP) port number 23, where a Telnet server application (telnet) is listening.

The TELNET protocol is based upon the notion of a virtual teletype, employing a 7-bit ASCII character set. The primary function of a User TELNET, then, is to provide the means by which its users can 'hit' all the keys on that virtual teletype

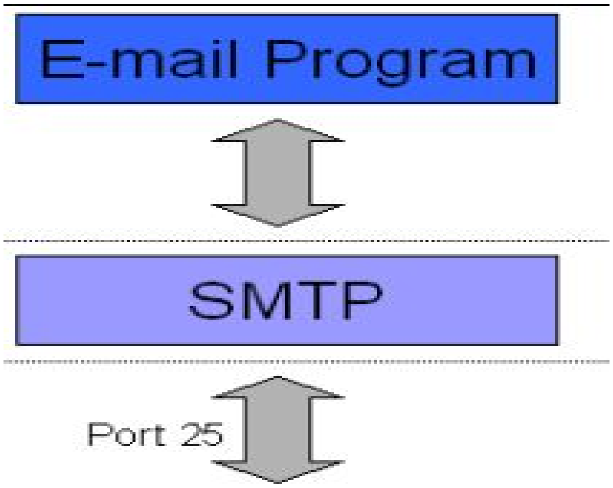
Telnet is used to remotely connect to the target of evaluation via the Ethernet management port. Telnet is not a part of the evaluated configuration as it is an insecure communication protocol. Telnet is to be disabled and SSH is to be used in its place.

Secure Shell (SSH), meanwhile is employed using a cryptographic network protocol for operating network services securely over an unsecured network. The best known example application is for remote login to computer systems by users.

SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server. Any network service can be secured with SSH. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.

Thus SSH was designed as a replacement for Telnet and for unsecured remote shell protocols such as the Berkeley rlogin, rsh, and rexecprotocols. Those protocols send information, notably passwords, in plaintext, rendering them susceptible to interception and disclosure using packet analysis.

SMTP is an electronic messaging protocol used to send e-mail messages and files from a user on the local network to a user on a remote network.SMTP defines the interchange between two SMTP processes. It does not define how mail is to passed from sender to SMTP, or how the mail is passed from the SMTP to the recipient. The SMTP process with mail to send is called the SMTP client, and the SMTP process recieving it is called the SMTP server. SMTP default port of communication is port 25.



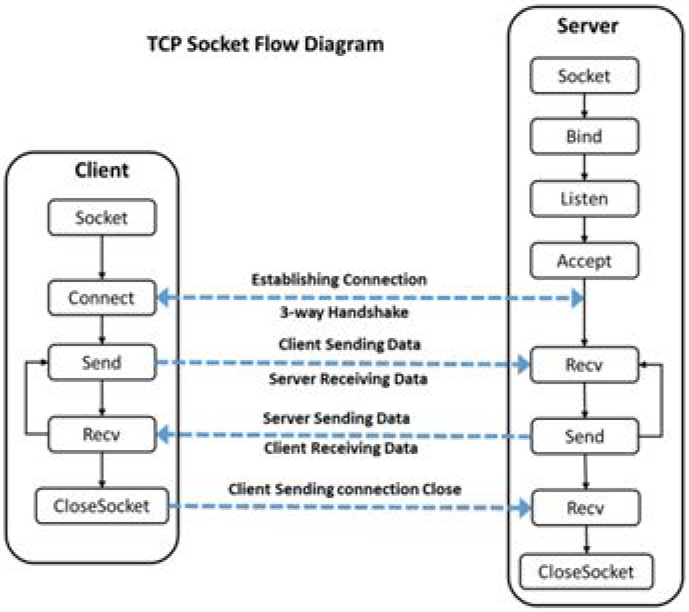
Host-to-Host transport Layer:

Sockets generally relies upon client/server architecture. For TCP communications, one host listens for incoming connection requests. When a request arrives, the server host accepts it and data is transferred between the hosts. The socket API makes use of two mechanisms to deliver data to the application level:

ports and sockets. All TCP/IP stacks have 65,536 ports for both TCP and UDP. A port is not a physical interface. It is a concept that simplifies the concept of internet communication. Applications can create sockets, which allow them to attach to a port. When an application has created a socket and bind it to a port, data destined to that port will be delivered to the application. If there is no application listening on that port, the packet is discarded and an error may be returned to the sender.

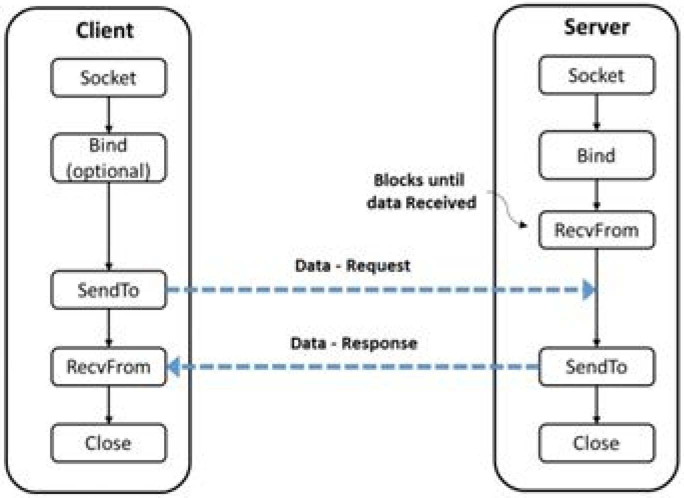
TCP is used for many protocols, including HTTP web browsing and email transfer. UDP may be used for multicasting and broadcasting, since retransmissions are not possible to a large amount of hosts. UDP typically gives higher throughput and shorter latency, and is therefore often used for real-time multimedia communication where packet loss occasionally can be accepted, for example IP-TV and IP-telephony, and for online computer games.

Socket based TCP Server-Client



Socket based UDP Server-Client

Socket APIs for UDP



Internet Layer:

IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.)

The Internet Protocol is responsible for addressing hosts and for routing datagrams (packets) from a source host to a destination host across one or more IP networks. For this purpose, the Internet Protocol defines the format of packets and provides an addressing system that has two functions: Identifying hosts and providing a logical location service.

The most widely used version of IP today is Internet Protocol Version 4 (IPv4).

The **Internet Control Message Protocol** (**ICMP**) is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.

The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. It is used when IPv4 is used over Carrier Ethernet.

The Carrier Ethernet address is a link layer address and is dependent on the interface card which is used. IP operates at the network layer and is not concerned with the link addresses of individual nodes which are to be used.The address resolution protocol (ARP) is therefore used to translate between the two types of address.

Network Interface Layer:

ATM:

ATM provides functionality that is similar to both circuit switching and packet switching networks: ATM uses asynchronous time-division multiplexing and encodes data into small, fixed-sized packets (ISO-OSI frames) called *cells.*This differs from approaches such as the Internet Protocol or Ethernet that use variable sized packets and frames.

Token Ring:

Token ring local area network technology is a communications protocol for local area networks. It uses a special three-byte frame called a "token" that travels around a logical "ring" of workstations or servers. This token passing is a channel access method providing fair access for all stations, and eliminating the collisions of contention-based access methods.

TCP/IP Protocols for SDN:

SDN forwarding methods are based on flows, through a protocol like OpenFlow, which operates in contrast to conventional networking device methods, such as TCP/IP routing table and MAC learning table.

OpenFlow Protocol:

OpenFlow is predominant set of protocols that provide a standard interface for programming the data plane switches. The OpenFlow protocol is layered on top of the Transmission Control Protocol (TCP), and prescribes the use of Transport Layer Security (TLS). Controllers should listen on TCP port 6653 for switches that want to set up a connection.

OpenFlow mainly considers switches, whereas other SDN approaches consider other network elements, such as routers. It is like an x86 instruction set for the network. An OpenFlow controller installs flow table entries in switches, so that these switches can forward traffic according to these entries. Thus, OpenFlow switches depend on configuration by controllers.

OpenFlow Protocol Messages

1. Controller-to-Switch: initiated by the controller and used to directly manage or inspect the state of the switch

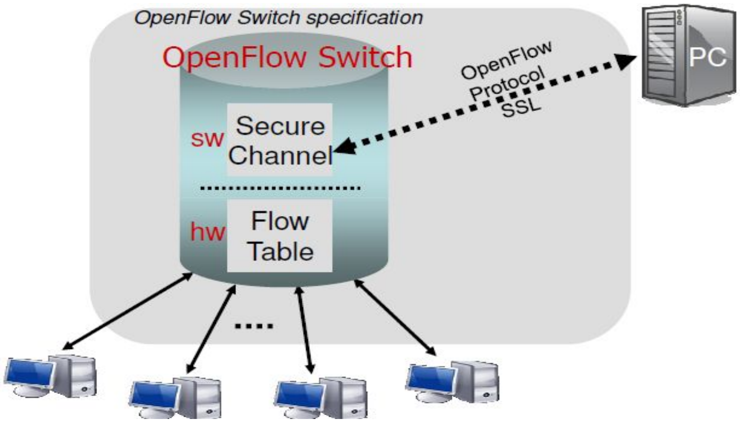
- Features, Config, Modify State, Read-State, Packet-Out, Barrier

2. Asynchronous: Asynchronous messages are sent without the controller soliciting them from a switch

- Packet-in, Flow Removed / Expiration, Port-status, Error

3. Symmetric: Symmetric messages are sent without solicitation, in either direction

- Hello, Echo, Experimenter / Vendor

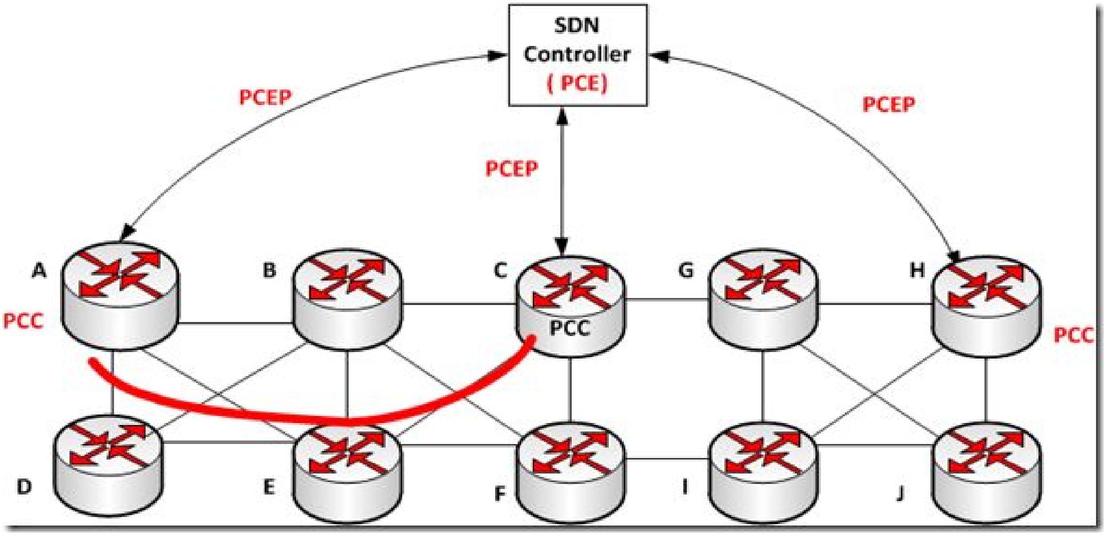


Forwarding and Control Element Separation Protocol:

ForCES is not only a protocol but also a framework; the ForCES also separates the control plane and data plane, but is considered more flexible and more powerful than OpenFlow. Forwarding devices are modeled using logical function blocks (LFB) that can be composed in a modular way to form complex forwarding mechanisms. Each LFB provides a given functionality, such as IP routing. The LFBs model a forwarding device and cooperate to form even more complex network devices. Control elements use the ForCES protocol to configure the interconnected LFBs to modify the behavior of the forwarding elements.

Path Computation Element Protocol (PCE):

PCE is embedded in controller for path computation. It is connected to infrastructure and client-controller. PCEP operates over TCP using a registered TCP port (4189). The PCEP messaging mechanism facilitates the specification of computation endpoints (source and destination node addresses), objective functions (requested algorithm and optimization criteria), and the associated constraints such as traffic parameters (e.g. requested bandwidth), the switching capability, and encoding type.



PCE is a control-plane service that provides services for control-plane applications. PCEP may be used as an east-west interface between PCEs that may act as domain control entities (services and applications).

Locator/ID Separation Protocol (LISP):

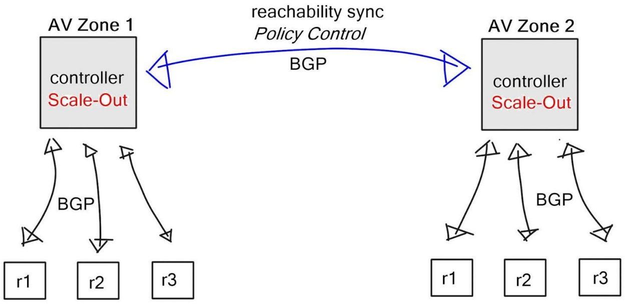
LISP splits current IP addresses overlapping semantics of identity and location into two separate paces namely, EIDs (Endpoint Identifiers) and RLOC (Routing Locator), this EID can be attached to many RLOC, the LISP Protocol provides mapping between them. The LISP protocol operating in an SDN deployment manages network traffic in terms of flows.

LISP allows a node (devices: Endpoint, Servers, VM, Smartphone, etc.) to keep the same IP address even when its location changes because it keeps its EID while mapping to multiple RLOCs. LISP-enabled edge routers can aggregate EID prefixes with closely aligned RLOCs, making it easier for a core router to quickly determine where to send data. It’s like “Enhanced DNS for IP addressing”. Usage of LISP for SDN results in a set of benefits like incremental deployment, scalability, flexibility, interoperability, and inter-domain support and drawbacks like extra headers and some initial delay.

Border Gateway Protocol (BGP):

BGP is a well-known core Internet routing protocol used for exchanging routing information between gateway hosts in a network of autonomous systems.

BGP is looked into use in hybrid software-defined networking. Considering the operational agility and programmability that SDN offers, with or without OpenFlow, as a result, BGP is identified as an SDN protocol with potential to enable network programmability promised by SDN.



NETCONF/YANG:

NETCONF is a network management protocol. It provides an administrator or network engineer with a secure way to configure a firewall, switch, router, or other network device. It is based on remote procedure call (RPC) and was designed to resolve issues that exist with the Simple Network Management Protocol and Command-Line Interface protocols, as they relate to the configuration of network devices.

NETCONF is now mandatory for the configuration of OpenFlow-enabled devices. The specification, called OF-CONFIG (named in Openflow), requires that devices supporting it must implement the NETCONF protocol as the transport.NETCONF is suitable for Management Plane Southbound Interfaces(MPSI) in SDN.

Bidirectional Forwarding Detection (BFD):

BFD is a network protocol designed for detecting path failures between two forwarding elements, with potentially very low latency. BFD can provide low-overhead failure detection on any kind of path between systems.

In SDN, a BFD agent can be implemented as a control-plane service or application that would help the forwarding plane to send/receive BFD packets. However, a BFD agent is usually implemented as an application on the device and uses the forwarding plane to send/receive BFD packets and update the operational-plane resources accordingly.

MPLS Transport Profile (MPLS-TP):

MPLS-TP is designed to be used as a network layer technology in transport networks. Certain changes to MPLS are proposed that include the use of the standard MPLS data-plane with a simpler control-plane based on SDN and OpenFlow. By having a simplified control plane that de-coupled from the data plane, it's able to globally optimize services, make services more dynamic, and create new services by programming networking applications on top of the SDN controller.

4. Members Contributions

S. No	Reg. No	Name	Contribution(s)
1.	14co202	Alla Pranathi	TCP/IP protocols over carrier Ethernet
2.	14CO203	Anirudh Sriram	MPLS description and protocols.
3.	14CO204	Aparna R Joshi	Enlisting and explaining various layer protocols in IEEE and OSI models.
4.	14CO207	Chiranjeevi AR Hegde	Protocols in MPLS
5.	14CO206	C.B.Yuvaraj	Description about LDP protocol and BGP protocol in MPLs.
6.	14CO208	Deepak Srikanth	Comparison between IEEE and OSI models
7.	14co209	Devanga Teja Sri	TCP/IP protocols over carrier Ethernet
8.	14CO205	B. Sandhya Rani	Description of TCP/IP protocols in SDN

5. References

[1] https://technet.microsoft.com/en-us/library/cc958821.aspx

[2] https://en.wikipedia.org/wiki/List_of_network_protocols_(OSI_model)
[3] http://www.comptechdoc.org/independent/networking/protocol/protnet.html
[4] http://ieeexplore.ieee.org/document/7158286/?reload=true
[5] https://www.clear.rice.edu/comp529/www/papers/tutorial_4.pdf
[6] https://tools.ietf.org/html/rfc7426#section-4.2
[7] http://searchsdn.techtarget.com/news/2240227714/Five-SDN-protocols-other-than-OpenFlow
[8] https://tools.ietf.org/html/draft-rodrigueznatal-lisp-sdn-00#section-5
[9] http://searchnetworking.techtarget.com/answer/What-is-the-difference-between-OSI-model-and-TCP-IP-other-than-the-number-of-layers
[10] http://www.mplsinfo.org/border-gateway-protocol-bgp.html