Chapter 4

1. What are the functions of the Network Layer?
   - Transport segments from the sending to receiving host. Encapsulate the segment into a datagram on the sending side and deliver the segment on the receiving side.
   - Two key network layer functions are:
     i. Forwarding (Data Plane): Move packets from one router's input to appropriate router output.
     ii. Routing (Control Plane): Determine the route taken by the packet from source to destination.

*Note: The routing algorithm determines the contents of the router's forwarding tables.

2. What is traditional Control plane approach?
   The routing algorithm runs in each and every router and both forwarding and routing functions are contained within a router. The routing algorithm function in one router communicates with the routing algorithm function in other routers to compute the values for its forwarding table by exchanging routing messages containing routing information according to a routing protocol.

3. What is software defined networking?
   Instead of running the routing algorithm on each and every router, control-plane routing functionality is separated from the physical router—the routing device performs forwarding only, while the remote controller computes and distributes forwarding tables. The remote controller might be implemented in a remote data centre with high reliability and redundancy, and might be managed by the ISP or some third party. The router and the remote controller communicate by exchanging messages containing forwarding tables and other pieces of routing information.

4. What are the components of the router?
   - Input Ports: An input port performs several key functions:
     i. It performs the physical layer function of terminating an incoming physical link at a router.
     ii. An input port also performs link-layer functions needed to interoperate with the link layer at the other side of the incoming link.
     iii. A lookup function is also performed at the input port. The forwarding table is consulted to determine the router output port to which an arriving packet will be forwarded via the switching fabric.
     iv. Queueing: If datagram arrive faster than the forwarding rate.
     v. Destination-based forwarding: Forward based on the IP address. (Traditional).
     vi. Generalized forwarding: Forward based on any set of header values.
   - Switching Fabric: The switching fabric connects the router's input ports to its output ports. This switching fabric is completely contained within the

router—a network inside of a network router. There are 3 types of switching fabrics:

i. Switching via Memory: The input packed is first copied into the memory. The routing processor then extracts the destination IP from the packet header and transfers it to the appropriate output buffer. 2 packets cannot be forwarded at the same time since only one memory read/write can be done.
ii. Switching via Bus: In this approach, an input port transfers a packet directly to the output port over a shared bus, without intervention by the routing processor. This is done by the input pre-pend the label of the output link it has to send to. All output ports receive the packet, but only the port that matches the label will keep the packet. If multiple packets arrive to the router at the same time, each at a different input port, all but one must wait since only one packet can cross the bus at a time.
iii. Switching via an interconnection network: To overcome the bandwidth limitation, the input and output links are connected in a more sophisticated interconnection network. When A wants to send to Y, the switch controller closes the cross-bar at Y so only Y can pick up the packet. And B can send packet to X at the same time since they're using different bus.

- Output ports: An output port stores packets received from the switching fabric and transmits these packets on the outgoing link by performing the necessary link-layer and physical-layer functions. When a link is bidirectional (that is, carries traffic in both directions), an output port will typically be paired with the input port for that link on the same line card.
- Routing processor: The routing processor performs control-plane functions. In traditional routers, it executes the routing protocols, maintains routing tables and attached link state information, and computes the forwarding table for the router. In SDN routers, the routing processor is responsible for communicating with the remote controller in order to receive forwarding table entries computed by the remote controller, and install these entries in the router's input ports. The routing processor also performs the network management functions.

*Note: Refer Head-of-the-line (HOL) blocking on Page 368.

5. What is Scheduling?
There are 3 types of scheduling:

- FIFO: The most basic one first in first out.
- Priority Queueing: There are different queues depending on the number of classes and the class with the priority is send first. Packets inside a particular class are sent FIFO.
- Round Robin and Weighted Fair Queueing: Assuming there are 2 classes, one packet is sent from class 1 and one packet is sent from class 2.

Weighted fair is different from round robin in the form that each class is given a different amount of service in any interval of time.

6. What is Checksum?
   The header checksum aids a router in detecting bit errors in a received IP datagram. The header checksum is computed by treating each 2 bytes in the header as a number and summing these numbers using 1s complement arithmetic. A router computes the header checksum for each received IP datagram and detects an error condition if the checksum carried in the datagram header does not equal the computed checksum. Routers typically discard datagrams for which an error has been detected.

7. What is tunnelling?
   When 2 IPv6 capable routers want to communicate with each other but they're connected through an IPv4 router. So, what the sending does is that takes the entire IPv6 datagram and puts it into the data field of the IPv4 datagram. The IPv4 is addressed to the receiving end of the tunnel and sent to the first node in the tunnel. The IPv4 router will route this IPv4 datagram completely unaware of the fact that it is IPv6 datagram. The IPv6 node on the receiving side of the tunnel eventually receives the IPv4 datagram (it is the destination of the IPv4 datagram!), determines that the IPv4 datagram contains an IPv6 datagram (by observing that the protocol number field in the IPv4 datagram is 41 [RFC 4213], indicating that the IPv4 payload is a IPv6 datagram), extracts the IPv6 datagram, and then routes the IPv6 datagram exactly as it would if it had received the IPv6 datagram from a directly connected IPv6 neighbour.

8. What is fragmentation?
   The maximum amount of data that a link-layer frame can carry is called the maximum transmission unit (MTU). Large IP datagrams divided ('fragmented') and they're reassembled only at the final destination.
   Each fragment has source and destination IP and an identification number of the original datagram. All the fragments have a flag bit set to 1 except for the last bit which is set to 0 so the receiver can determine the last the fragment.

*Topics left: Subnet designing, Fragmentation table, Generalized forwarding and SDN.

Chapter 5

1. What is a routing algorithm? And explain its classification.
   The goal of a routing algorithm is to calculate the least cost path from the sender to the receiver. The routing algorithm can be classified into 4 types:
   I. Centralized routing algorithm: This algorithm calculates the least cost between the sender and the receiver using the all the nodes and edges as input. That means that the routing has complete global knowledge about the network. The router has to obtain all this information before doing the

calculation. Algorithms with global state information are knows as link state algorithms.

II. Decentralized routing algorithm: Here, no node has the complete information about all the routers in network. Instead, each node begins with only the knowledge of the costs of its own directly attached links. Then the router calculates the least cost path and exchanges information with its neighbouring nodes, and the node gradually calculates the least-cost path to the destination or a set of destinations.

III. Static routing algorithms: These routes change very slowly with time and are often changed as a result of human intervention.

IV. Dynamic routing: These change the routing paths as the topology changes. These algorithms can be run periodically or when there's a change in the topology.

2. What is link state algorithm?
   The link state algorithm also known as the Dijkstra's algorithm is classified as a centralized routing algorithm since it has complete knowledge of the all the nodes and their costs currently in the network.
   Formula: D(v) = min(D(v), D(w) + c (w, v))

3. What is distance vector algorithm?
   Unlike the link state algorithm, the distance vector does not have complete gobal information about all the nodes in the network. Distance vector is asynchronous and distributed.
   Formula: $D_x(y) \leftarrow min_v\{c(x,v) + D_v(y)\}$ *for each node* $y \in N$

Some common terms

Autonomous Systems (AS): A group of routers under the same administrative control.

Autonomous system number (ASN): An Autonomous system is identified by its globally unique ASN

4. What is OSPF?
   Open shortest path first: OSPF is a link-state protocol that uses flooding of link-state information and a Dijkstra's least-cost path algorithm. With OSPF, each router constructs a complete topological map (that is, a graph) of the entire autonomous system. Each router then locally runs Dijkstra's shortest-path algorithm to determine a shortest-path tree to all subnets, with itself as the root node.
   Some advanced features of OSPF are:

   i. Security: Exchanges between OSPF routers (for example, link-state updates) can be authenticated. With authentication, only trusted routers can participate in the OSPF protocol within an AS, thus preventing malicious intruders (or networking students taking their newfound

knowledge out for a joyride) from injecting incorrect information into router tables.

ii. Multiple same-cost paths: When multiple paths to a destination have the same cost, OSPF allows multiple paths to be used.

iii. Provide Hierarchy within a single AS: An OSPF autonomous system can be configured hierarchically into areas. Each area runs its own OSPF link-state routing algorithm, with each router in an area broadcasting its link state to all other routers in that area. Within each area, one or more area border routers are responsible for routing packets outside the area. Lastly, exactly one OSPF area in the AS is configured to be the backbone area. The primary role of the backbone area is to route traffic between the other areas in the AS. The backbone always contains all area border routers in the AS and may contain non-border routers as well. Inter-area routing within the AS requires that the packet be first routed to an area border router (intra-area routing), then routed through the backbone to the area border router that is in the destination area, and then routed to the final destination.

5. What is BGP?

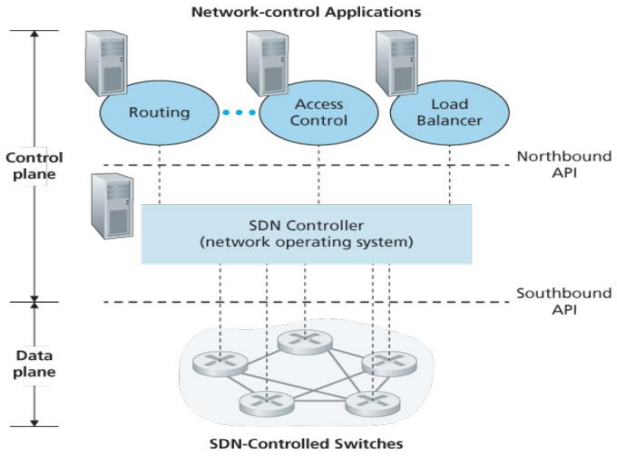
Border gateway protocol is used for calculating routes between inter-AS domains. The 2 main functionality of BGP are:

i. Obtain prefix reachability information from neighbouring ASs: In particular the BGP allows each subnet to advertise its existence to the rest of the ASs. It does this over a BGP connection, i.e., a semi-permanent TCP connection on port 179 where the routers can exchange routing information. Furthermore, a BGP connection that spans two ASs is called an external BGP (eBGP) connection, and a BGP session between routers in the same AS is called an internal BGP (iBGP) connection.

ii. Determine the best route: For this BGP uses an algorithm that incorporates hot potato routing. If there are 2 or more paths to the destination, the BGP invokes the elimination rules:

   a. Local preference: Path with the highest preference is selected.
   b. From all the remaining path, the path with the shortest AS-PATH is selected.
   c. For the remaining routes, hot potato routing is used.
   d. Other identifiers.

6. Explain SDN architecture.



The SDN architecture has 2 planes:

i. Data Plane: The data plane consists of all the switches; data plane is generally the hardware part of the SDN architecture while control is the software part of it. The flow tables in these switches are installed by the SDN controller. The controller and the switches communicate using an Open Flow protocol they use a southbound API to communicate with each other.

ii. Control Plane: The control plane further consists of 2 parts:

a. The SDN controller:
   i. It maintains the network state information.
   ii. Interacts with the network control application above via a northbound API.
   iii. Interacts with the network switches below above via a northbound API.
   iv. It is implemented as a distributed system for better performance, scalability, fault tolerance and robustness.

b. Network control applications: These are the "brains" of control: implement control functions using lower-level services, API provided by SDN controller.

7. Explain Open Flow Protocol.

The Open Flow protocol operates between the SDN controller and SDN controlled switches in the data plane. It is implemented using the Open Flow API. It operates over the TCP layer with a default port number of 6653.

These are some of the few important messages flowing from controller to the controlled switch:

i. Configure: To the configure the switch.

ii. Modify: To add, delete or modify flow table entries.

These are some of the few important messages flowing from controlled switch to the controller:

i. Flow-removed: To notify the controller that a flow table entry is removed.

ii. Port status: To notify the controller of the port change.

8. Explain ICMP.

Internet Control Message Protocol is used to by hosts and routers to send network layer information, typically to send error messages to each other. Like for example, when we visit a site and it says that the host is unreachable, that is a ICMP error message sent from the router.

ICMP lies above the IP, and ICMP are carried inside the IP datagram, which means the ICMP messages are sent inside the data payload of the IP datagram. ICMP messages have a type and code field to point out what caused the error. Some basic examples of these are:

Type	Code	Description
3	0	Destination network unreachable
3	1	Destination host unreachable
3	2	Destination protocol unreachable
3	3	Destination port unreachable

How it works using traceroute?

Traceroute is used to calculate the routers between the source and the destination. It does so by sending datagram with an UDP segment to an unlikely UDP port with a TTL 1, datagram 2 with TTL 2, and so on. When the host sends the Nth packet to the Nth router, the TTL just expires and the router discards the packet and sends an ICMP error message to host with the name of the router and it's IP address. When this message is received by the host, it calculates the round-trip time and obtains the name and the IP address of the router.

Eventually one of the datagrams will make all the way to the destination but since the UDP port number is unusual, the destination responds with an ICMP error message (type 3 code 3) back to the source. The source receives this ICMP message and it knows that it does not need send additional probes.

9. Explain Network Management and SNMP.

The Network Management framework consists of a number of components:

i. Managing Server: The managing server is an application that is run on a centralized Network Management station. The managing server controls the collection, processing, analysis and display the Network Management Information.

ii. Managed Device: A Managed Device is a piece of network equipment in the Managed Network. A managed device could be a host, router, switch or modem. There may be several Managed Objects within the Managed Agent, the Managed Object is an actual piece of hardware, such as Network Interface Card etc.

iii. Management Information Base: The data related to Managed Object is collected into the Management Information Base (MIB). A MIB object could be a counter, such as the number of datagrams packets discarded etc.

iv. Network Management Agent: Apart from the Managed Object, Network Management Agent also reside in the Managed Device. It communicates with the Managing Server and takes action at the Managed Device.

v. Network Management Protocol: The protocol runs between the Managing Server and the Managed Device. It allows the Managing Server to communicate with the Managed Device and allows the Managing Server to take action on the Managed Device via the Agent.

Simple Network Message Protocol (SNMP): It is an application layer protocol used to send network management control and information messages between the Managing Server and the Managed Device. There are 2 types of modes:

i. Request-Response: Here, the Managing Server sends a request to the Managed Device, The Managed Device upon receiving this request, performs some action and sends a response to the Managing Server.
ii. Trap: These are usually sent by the Managing Device to the Managing Server. Trap messages are used to notify the Managing Server of an exceptional situation that has resulted changes in the MIB values.