Assignment 4

R1. Let’s review some of the terminology used in this textbook. Recall that the name of a transport-layer packet is segment and that the name of a link-layer packet is frame. What is the name of a network-layer packet? Recall that both routers and link-layer switches are called packet switches. What is the fundamental difference between a router and link-layer switch?

The name of a network-layer packet is “Datagram”. The fundamental difference between a router and link-layer switch as

* A router forwards a packet based on the packet’s IP (layer 3) address.
* A link-layer switch forwards a packet based on the packet’s MAC (layer address).

R2. We noted that network layer functionality can be broadly divided into data plane functionality and control plane functionality. What are the main functions of the data plane? Of the control plane?

Data Plane: forwards traffic, does switching, and goes through the router.

Control plane: makes decisions where traffic is sent and has routing protocols.

R3. We made a distinction between the forwarding function and the routing function performed in the network layer. What are the key differences between routing and forwarding?

Forwarding: move packets from router's input to appropriate router output.

Routing: determine route taken by packets from source to destination.

Usually routing runs continuously to establish the routing tables before the packets are forwarded and in anticipation of packets.

R4. What is the role of the forwarding table within a router?

The routing table resides in the control plane. It contains routing information received through routing protocols and from configuration. There may be more than one entry for a given prefix if multiple routing information is received by the control plane. The forwarding table has the definitive destination information where a packet is routed for any given IP prefix.

R5. We said that a network layer’s service model “defines the characteristics of end-to-end transport of packets between sending and receiving hosts.” What is the service model of the Internet’s network layer? What guarantees are made by the Internet’s service model regarding the host-to-host delivery of datagrams?

Best-effort. Packets are not guaranteed to be received in order they are sent. Eventual delivery not guaranteed. No end-to-end guarantee or minimal bandwidth guarantee.

R6. In Section 4.2 , we saw that a router typically consists of input ports, output ports, a switching fabric and a routing processor. Which of these are implemented in hardware and which are implemented in software? Why? Returning to the notion of the network layer’s data plane and control plane, which are implemented in hardware and which are implemented in software? Why?

Data plane (hardware): needs greater speeds to avoid traffic in the network.

The control plane (software): No speed restrictions, which is why it is done in software.

R7. Discuss why each input port in a high-speed router stores a shadow copy of the forwarding table.

With the shadow copy, the forwarding decision is made locally, at each input port, without invoking the centralized routing processor. Such decentralized forwarding avoids creating a forwarding processing bottleneck at a single point within the router.

R8. What is meant by destination-based forwarding? How does this differ from generalized forwarding (assuming you’ve read Section 4.4 , which of the two approaches are adopted by Software-Defined Networking)?

Destination-based: router forwards datagram based on destination IP address.

Generalized: router forwards based on other factors too, like header field values (TCP/UDP source/destination port numbers, etc.)

R9. Suppose that an arriving packet matches two or more entries in a router’s forwarding table. With traditional destination-based forwarding, what rule does a router apply to determine which of these rules should be applied to determine the output port to which the arriving packet should be switched?

A router uses longest prefix matching to determine which link interface a packet will be forwarded to if the packet's destination address matches two or more entries in the forwarding table.

R10. Three types of switching fabrics are discussed in Section 4.2 . List and briefly describe each type. Which, if any, can send multiple packets across the fabric in parallel?

Switching via memory: Fabric switching with the use of CPU

Switching via a bus: Fabric switching via shared buses on input and output port

Switching via interconnection network: fragmenting datagrams into fixed length cells, switch cells through fabric.

R11. Describe how packet loss can occur at input ports. Describe how packet loss at input ports can be eliminated (without using infinite buffers).

Packet loss occurs if the queue size at the input port grows large because of slow switching fabric speed and thus exhausting the router's buffer space. It can be eliminated if the switching fabric speed is at least n times as fast as the input line speed, where n is the number of input ports.

R12. Describe how packet loss can occur at output ports. Can this loss be prevented by increasing the switch fabric speed?

If the queue size at the input port grows large because of slow switching fabric speed and thus exhausting the router's buffer space. It can be eliminated if the switching fabric speed is not smaller than the speed of the number of input ports time.

R13. What is HOL blocking? Does it occur in input ports or output ports?

Head of Line blocking, a queued packet in an input queue must wait for transfer through the fabric because it is blocked by another packet at the head of the line. It occurs at the input port.

R14. In Section 4.2 , we studied FIFO, Priority, Round Robin (RR), and Weighted Fair Queueing (WFQ) packet scheduling disciplines? Which of these queueing disciplines ensure that all packets depart in the order in which they arrived?

FIFO stands for First In First Out. In this type of handling approach the oldest (first) entry, or 'head' of the queue, is processed first. Round Robin assigns time slices to each process in equal portions and in circular order and there is no priority in the processes. FIFO is the one that ensures that all packets depart in the order in which they arrived.

R15. Give an example showing why a network operator might want one class of packets to be given priority over another class of packets.

Packets that are being transmitted contain different kinds of information, depending on the type of the information the packets are carrying packets are classified in classes of high priority and low priority.

R16. What is an essential different between RR and WFQ packet scheduling? Is there a case (Hint: Consider the WFQ weights) where RR and WFQ will behave exactly the same?

RR classifies the packets into classes and rotates the scheduler to have all packets get equal priority. RR and WFQ will work the same way if WFQ has all the packets that are the same weight.

R17. Suppose Host A sends Host B a TCP segment encapsulated in an IP datagram. When Host B receives the datagram, how does the network layer in Host B know it should pass the segment (that is, the payload of the datagram) to TCP rather than to UDP or to some other upper-layer protocol?

The 8-bit protocol field in the IP datagram contains info about which protocol to choose.

R18. What field in the IP header can be used to ensure that a packet is forwarded through no more than N routers?

TTL (time to live).

R19. Recall that we saw the Internet checksum being used in both transport-layer segment (in UDP and TCP headers, Figures 3.7 and 3.29 respectively) and in network-layer datagrams (IP header, Figure 4.16 ). Now consider a transport layer segment encapsulated in an IP datagram. Are the checksums in the segment header and datagram header computed over any common bytes in the IP datagram? Explain your answer.

Yes, because it can identify errors if there is any mismatch between the bytes.

R20. When a large datagram is fragmented into multiple smaller datagrams, where are these smaller datagrams reassembled into a single larger datagram?

The smaller datagrams are reassembled at the destination, before being passed into the transport layer.

R21. Do routers have IP addresses? If so, how many?

Routers have only one IP address

R22. What is the 32-bit binary equivalent of the IP address 223.1.3.27?

11011111 00000001 00000011 00011100

R23. Visit a host that uses DHCP to obtain its IP address, network mask, default router, and IP address of its local DNS server. List these values.

The solution may vary for different hosts that use DHCP.

IP address: 192.168.1.111

Subnet mask: 255.255.255.0

Default router: 192.168.1.254

Local DNS server: 192.168.1.2

R24. Suppose there are three routers between a source host and a destination host. Ignoring fragmentation, an IP datagram sent from the source host to the destination host will travel over how many interfaces? How many forwarding tables will be indexed to move the datagram from the source to the ­destination?

(Number of routers) \* (2 per router) + 2 = 6 + 2 = 8

3 routers means three forwarding tables will be indexed

R25. Suppose an application generates chunks of 40 bytes of data every 20 msec, and each chunk gets encapsulated in a TCP segment and then an IP datagram. What percentage of each datagram will be overhead, and what percentage will be application data?

TCP and IP are 20 bytes each. Added to the 40 byte data chunk makes 80 total bytes. The overhead is 40 of the 80 total, so that's 50%.

R26. Suppose you purchase a wireless router and connect it to your cable modem. Also suppose that your ISP dynamically assigns your connected device (that is, your wireless router) one IP address. Also suppose that you have five PCs at home that use 802.11 to wirelessly connect to your wireless router. How are IP addresses assigned to the five PCs? Does the wireless router use NAT? Why or why not?

Typically the wireless router includes a DHCP server. DHCP is used to assign IP addresses to the 5 PCs and to the router interface. Yes, the wireless router also uses NAT as it obtains only one IP address from the ISP.

R27. What is meant by the term “route aggregation”? Why is it useful for a router to perform route aggregation?

It is a method used to minimize the number of routing tables required in an IP network. Route aggregation works extremely well when addresses are allocated in blocks to ISPs and then from ISPs to client organizations.

R28. What is meant by a “plug-and-play” or “zeroconf” protocol?

Plug and play is a configuration of a host to a network and Zeroconf is an automatic configuration.

R29. What is a private network address? Should a datagram with a private network address ever be present in the larger public Internet? Explain.

A private network address of a device in a network refers to a network address that is only meaningful to those devices within that network. A datagram with a private network address should never be present in the larger public Internet, because the private network address is potentially used by many network devices within their own private networks.

R30. Compare and contrast the IPv4 and the IPv6 header fields. Do they have any fields in common?

IPv6 has a fixed length header, which does not include most of the options an IPv4 header can include. Even though the IPv6 header contains two 128 bit addresses (source and destination IP address) the whole header has a fixed length of 40 bytes only. Several of the fields are similar in spirit. Traffic class, payload length, next header and hop limit in IPv6 are respectively similar to type of service, datagram length, upper-layer protocol and time to live in IPv4.

R31. It has been said that when IPv6 tunnels through IPv4 routers, IPv6 treats the IPv4 tunnels as link-layer protocols. Do you agree with this statement? Why or why not?

Yes, under tunnelling, the entire IPv6 is encapsulated in an IPv4 datagram and passed through the link-layer.

R32. How does generalized forwarding differ from destination-based ­forwarding?

In destination-based forwarding the router forwards datagram based on destination IP address. In generalized forwarding it forwards based on other factors too, like header field values (TCP/UDP source/destination port numbers, etc.)

R33. What is the difference between a forwarding table that we encountered in destination based forwarding in Section 4.1 and OpenFlow’s flow table that we encountered in Section 4.4 ?

Each entry in the forwarding table of a destination-based forwarding contains only an IP header field value and the outgoing link interface to which a packet (that matches the IP header field value) is to be forwarded. Each entry of the flow table in OpenFlow includes a set of header field values to which an incoming packet will be matched, a set of counters that are updated as packets are matched to flow table entries, and a set of actions to be taken when a packet matches a flow table entry.

R34. What is meant by the “match plus action” operation of a router or switch? In the case of destination-based forwarding packet switch, what is matched and what is the action taken? In the case of an SDN, name three fields that can be matched, and three actions that can be taken.

"Match plus action" means that a router or a switch tries to find a match between some of the header values of a packet with some entry in a flow table, and then based on that match, the router decides to which interface(s) the packet will be forwarded and even some more operations on the packet. In the case of destination-based forwarding packet switch, a router only tries to find a match between a flow table entry with the destination IP address of an arriving packet, and the action is to decide to which interface(s) the packet will be forwarded. In the case of an SDN, there are many fields that can be matched, for example, IP source address, TCP source port, and source MAC address; there are also many actions that can be taken, for example, forwarding, dropping, and modifying a field value.

R35. Name three header fields in an IP datagram that can be “matched” in OpenFlow 1.0 generalized forwarding. What are three IP datagram header fields that cannot be “matched” in OpenFlow?

Three example header fields in an IP datagram that can be matched in OpenFlow 1.0 generalized forwarding are IP source address, TCP source port, and source MAC address. Three fields that cannot be matched are: TTL field, datagram length field, header checksum (which depends on TTL field).

**Work Cited**

<https://networkengineering.stackexchange.com/questions/52150/what-is-the-different-between-routing-table-and-forwarding-table>

<https://brainly.com/>

<https://quizlet.com/ca/462248263/ch-4-review-flash-cards/>

<https://quizlet.com/340406487/chapter-4-network-layer-flash-cards/>

<https://www.studyblue.com/?src_url=https://www.studyblue.com/notes/note/n/networking-ch4/deck/21882790#flashcard/review/21882790>