Jeannie Cireus
4738446

R1. What is the difference between a host and an end system? List several different types of end systems. Is a Web server an end system?

There is no difference. Throughout this text, the words “host” and “end system” are used interchangeably. End systems include PCs, workstations, Web servers, mail servers, PDAs, Internet-connected game consoles, etc.

R2. The word protocol is often used to describe diplomatic relations. How does Wikipedia describe diplomatic protocol?

Diplomatic protocol is commonly described as a set of international courtesy rules. These well-established and time-honored rules have made it easier for nations and people to live and work together. Part of protocol has always been the acknowledgment of the hierarchical standing of all present. Protocol rules are based on the principles of civility.

R3. Why are standards important for protocols?

Standards are important for protocols so that people can create networking systems and products that interoperate.

R4. List six access technologies. Classify each one as home access, enterprise access, or wide-area wireless access.

1. DSL over telephone line: home or small office

2. Cable to HFC: home

3. 3G and 4G: wide-area wireless

4. Dial-up modem over telephone line: home

5. Ethernet: Enterprise

6. Wi-Fi

R5. Is HFC transmission rate dedicated or shared among users? Are collisions possible in a downstream HFC channel? Why or why not?

HFC bandwidth is shared among the users. On the downstream channel, all packets emanate from a single source, namely, the head end. Thus, there are no collisions in the downstream channel. Thus, there are no collisions in the downstream channel.

R6. List the available residential access technologies in your city. For each type of access, provide the advertised downstream rate, upstream rate, and monthly price.

dial-up; DSL; cable modem; fiber-to-the-home.

R7. What is the transmission rate of Ethernet LANs?

Ethernet LANs have transmission rates of 10 Mbps, 100 Mbps, 1 Gbps and 10 Gbps.

R8. What are some of the physical media that Ethernet can run over?

Ethernet most commonly runs over twisted-pair copper wire and “thin” coaxial cable.

R9. Dial-up modems, HFC, DSL and FTTH are all used for residential access. For each of these access technologies, provide a range of transmission rates and comment on whether the transmission rate is shared or dedicated.

Dial-up modems:

Transmission rate: 56 Kbps

Broad cast medium device.

HFC(Hybrid fiber-coaxial cable):

Transmission rate: 10 Mbps to 30 Mbps.

Shared broad cast medium.

DSL(Digital subscriber line):

Transmission rate: <5Mbps

Dedicated broad cast medium.

FTTH(Fiber To The Home):

Transmission rate: Approximately 20Mbps

Shared broad cast medium.

R10. Describe the most popular wireless Internet access technologies today. Compare and contrast them

Wifi (802.11) In a wireless LAN, wireless users transmit/receive packets to/from an base station (i.e., wireless access point) within a radius of few tens of meters. The base station is typically connected to the wired Internet and thus serves to connect wireless users to the wired network.

3G and 4G wide-area wireless access networks. In these systems, packets are transmitted over the same wireless infrastructure used for cellular telephony, with the base station thus being managed by a telecommunications provider. This provides wireless access to users within a radius of tens of kilometers of the base station.

R11. Suppose there is exactly one packet switch between a sending host and a receiving host. The transmission rates between the sending host and the switch and between the switch and the receiving host are R1 and R2, respectively. Assuming that the switch uses store-and-forward packet switching, what is the total end-to-end delay to send a packet of length L? (Ignore queuing, propagation delay, and processing delay.)

R1= Transmission rates between the sending host and the switch

R2= Transmission rates between the switch and the receiving host

L= Packet of length

Therefore, total end-to-end delay to send a packet of length L=L/R1+L/R2

R12. What advantage does a circuit-switched network have over a packet-switched network? What advantages does TDM have over FDM in a circuit-switched network?

A circuit-switched network can guarantee a certain amount of end-to-end bandwidth for the duration of a call. Most packet-switched networks today (including the Internet) cannot make any end-to-end guarantees for bandwidth. FDM requires sophisticated analog hardware to shift signal into appropriate frequency bands.

R13. Suppose users share a 2 Mbps link. Also suppose each user transmits continuously at 1 Mbps when transmitting, but each user transmits only 20 percent of the time.

a)When circuit switching is used, how many users can be supported?

Link size / transmitting size = 2Mbps / 1Mbps = 2 users can be supported

b) For the remainder of this problem, suppose packet switching is used. Why

will there be essentially no queuing delay before the link if two or fewer users transmit at the same time? Why will there be a queuing delay if three users transmit at the same time?

Since each user requires 1Mbps when transmitting, if two or fewer users transmit simultaneously, a maximum of 2Mbps will be required. This does not exceed the 2Mbps of available bandwidth in the shared link. If there is 3 users then the 3Mbps needed exceeds the 2 Mbps available. So there will be a queueing delay.

c) Find the probability that a given user is transmitting.

p = 20/100 = .2

d) Suppose now there are three users. Find the probability that at any given

time, all three users are transmitting simultaneously. Find the fraction of time during which the queue grows.

(3¦3) p^3 (1-p)^3-3 = (0.2)^3 = 0.008

R14. Why will two ISPs at the same level of the hierarchy often peer with each other? How does an IXP earn money?

Two ISPs at the same level of the hierarchy often peer with each other to send and receive traffic directly and avoid paying to the intermediate ISP provider.

• If two ISP's do not peer with each other, then they need an intermediate ISP provider to send traffic to each other.

• The two ISPs have to pay the intermediate ISP provider for carrying traffic for them.

• This would be an additional burden for the two ISPs.

• By peering with each other, two ISP's can reduce their cost and avoid paying to the intermediate ISP provider.

An Internet Exchange Points (IXP) is stand-alone building with its own switches.

• IXP enables multiple ISPs and peers to meet at a single point and exchange Internet traffic.

• An Internet Exchange Points (IXP) can earn money by charging each ISP that connects to it.

• The IXP charges

each ISP based on the amount of traffic sent to or received from the IXP.

R15. Some content providers have created their own networks. Describe Google's network. What motivates content providers to create these networks?

Google's network:

This network provides global data.

It is used to transfer content within the Google servers.

Its contains some Tier-1 ISP and interconnect with TCP/IP.

Motivates:

It is used to save money by transfer data and less time to travel content.

Content providers to control over the services.

R16. Consider sending a packet from a source host to a destination host over a fixed route. List the delay components in the end-to-end delay. Which of these delays are constant and which are variable?

Processing delay: Processing delay is fixed. ...

Transmission delay: Transmission delay is fixed. ...

Propagation delay: Propagation delay is fixed. ...

Queuing delay: Queuing delay is variable.

R17. Visit the Transmission Versus Propagation Delay applet at the companion Web site. Among the rates, propagation delay, and packet sizes available, find a combination for which the sender finishes transmitting before the first bit of the packet reaches the receiver. Find another combination for which the first bit of the packet reaches the receiver before the sender finishes transmitting.

a) 1000 km, 1 Mbps, 100 bytes
b) 100 km, 1 Mbps, 100 bytes

R18. How long does it take a packet of length 1,000 bytes to propagate over a link of distance 2,500 km, propagation speed $2.5 \cdot 10^8$ m/s, and transmission rate 2 Mbps? More generally, how long does it take a packet of length L to propagate over a link of distance d, propagation speed s, and transmission rate R bps? Does this delay depend on packet length? Does this delay depend on transmission rate?

1. 10msec
2. d/s

No, the delay depend on packet length is not true.

No, the delay depend on transmission rate is not true.

R19. Suppose Host A wants to send a large file to Host B. The path from Host A to Host B has three links, of rates R1 = 500 kbps, R2 = 2 Mbps, and R3 = 1 Mbps.

a) Assuming no other traffic in the network, what is the throughput for the file transfer?

b) Suppose the file is 4 million bytes. Dividing the file size by the throughput, roughly how long will it take to transfer the file to Host B?

c) Repeat (a) and (b), but now with R2 reduced to 100 kbps.

a)

Consider given data:R1 = 500 kbps, R2 = 2 Mbps, and R3 = 1 Mbps

The throughput for the file transfer=min{R1,R2,R3}

=min{500 kbps, 2 Mbps, 1 Mbps}

=500 kbps

b)

file size= 4 million bytes

Convert million bytes to bits

=32000000 bits.

From (a), Throughput for the file transfer=500 Kbps

=500000 bps

how long will it take to transfer the file to Host B:

=file size/throughput for the file transfer

=32000000 bits/500000 bps

=64 seconds

c)

R2=100 kbps , R1 = 500 kbps, and R3 = 1 Mbps

The throughput for the file transfer=min{R1,R2,R3}

=min{500 kbps, 100 kbps, 1 Mbps}

=file size/hroughput for the file transfer

=32000000 bits/100000 bps

=320 seconds

R20. Suppose end system A wants to send a large file to end system B. At a very high level, describe how end system A creates packets from the file. When one of these packets arrives to a packet switch, what information in the packet does the switch use to determine the link onto which the packet is forwarded? Why is packet switching in the Internet analogous to driving from one city to another and asking directions along the way?

The following steps to end System A creates packets from the file at very high level:

Divide file into chunks.

Create a packet by attach header to chunk.

Each packet maintain an address of the destination.

The following information in the packet does the switch use to determine the link onto which the packet is forwarded:

Switch uses the destination address.

It is easy to find which packet is forward to the header.

The following the packet switching in the Internet analogous to driving from one city to another and asking directions along the way:

Each packet maintain an address of the destination.

Reaching packet, packet display outgoing link which road to take to forwarded.

R21. Visit the Queuing and Loss applet at the companion Web site. What is the maximum emission rate and the minimum transmission rate? With those rates, what is the traffic intensity? Run the applet with these rates and determine how long it takes for packet loss to occur. Then repeat the experiment a second time and determine again how long it takes for packet loss to occur. Are the values different? Why or why not?

The maximum emission rate =500 packets/s

The minimum transmission rate=350 packets/s

The traffic intensity=500/350

$=1.43 > 1$

Loss will eventually occur for each experiment; but the time when loss first occurs will be different from one experiment to the next due to the randomness in the emission process.

R22. List five tasks that a layer can perform. Is it possible that one (or more) of these tasks could be performed by two (or more) layers?

Five generic tasks are error control, flow control, segmentation and reassembly, multiplexing, and connection setup. Yes, these tasks can be duplicated at different layers.

R23. What are the five layers in the Internet protocol stack? What are the principal responsibilities of each of these layers?

Application layer: HTTP, SMTP, and FTP protocols are used in application layer. it is used to send data over multiple end systems.

Transport layer: Transfer the content between two endpoints mainly. TCP and UDP protocols are used in transport layer.

Network layer: Move the packets between any two hosts in the network. IP protocol is used in network layer.

Link layer: Move the packets from one node to the next another node. Point-to-point protocol (ppp) used in data link layer.

Physical layer: Transfer the individual bits from one node to the next node with in the frame.

R24. What is an application-layer message? A transport-layer segment? A network-layer datagram? A link-layer frame?

Application layer message: HTTP, SMTP, and FTP protocols are used in application layer. it is used to send data over multiple end systems.

Transport layer segment: Transfer the content between two endpoints mainly. TCP and UDP protocols are used in transport layer.

Network layer datagram: Move the packets between any two hosts in the network. IP protocol is used in network layer.

link-layer frame: Move the packets from one node to the next another node. Point-to-point protocol (ppp) used in data link layer.

R25. Which layers in the Internet protocol stack does a router process? Which layers does a link-layer switch process? Which layers does a host process?

The layers in the internet protocol stack which does router processes are:-

Physical layer

Link layer

Network layer

The layer which does a link layer switch process are:-

Physical layer

Link layer

The layer which does a host process are all the five layers which are :-

Physical layer

Link layer

Network layer

Transport layer

Application layer

R26. What is the difference between a virus and a worm?

The primary difference between a virus and a worm is that viruses must be triggered by the activation of their host; whereas worms are stand-alone malicious programs that can self-replicate and propagate independently as soon as they have breached the system.

R27. Describe how a botnet can be created and how it can be used for a DDoS attack.

The following steps to create a botnet:

Prepare host systems to find the vulnerability attacker tries.

Using the Trojan to fight against attackers or compromises the host system.

This process is called botnet.

DDoS attack:

DDoS means Distributed Denial-of-Service.

The host systems can scan the environment and control the systems from the attacker.

R28. Suppose Alice and Bob are sending packets to each other over a computer network. Suppose Trudy positions herself in the network so that she can capture all the packets sent by Alice and Bob are sending packets to each other over a computer network.

Trudy positions herself in the network so that she can capture all the packets sent by Alice and send whatever she wants to Bob by pretending to be Bob.

The following steps to list some of the malicious things Trudy can do from this position:

She can observe the contents of all the packet and possibility to modify content of packets and sent appropriate receiver.

Trudy is chance to drop the packets from Alice to Bob or from Bob to Alice.

https://coursys.sfu.ca/2015su-cmpt-371-e1/pages/RVW_Sol_Ch1/view

Computer Networking: A Top-Down Approach Ross Keith and Kurose James Publisher, Edition, 7th Edition