Application Layer

The application layer is where network applications and their application-layer protocols reside. The Internet's application layer includes many protocols, such as the HTTP

Transport Layer

The Internet's transport layer transports application-layer messages between application endpoints. In the Internet there are two transport protocols, TCP and

Network Layer

The Internet's network layer is responsible for moving network-layer packets known as **datagrams** from one host to another. The Internet transport-layer proto-

Link Layer

The Internet's network layer routes a datagram through a series of routers between the source and destination. To move a packet from one node (host or router) to the

Physical Layer

While the job of the link layer is to move entire frames from one network element to an adjacent network element, the job of the physical layer is to move the *individual bits* within the frame from one node to the next. The protocols in this layer are

1. The Web: HTTP; file transfer: FTP; remote login: Telnet; e-mail: SMTP; BitTorrent file sharing: BitTorrent protocol
2. Network architecture refers to the organization of the communication process into layers (e.g., the five-layer Internet architecture). Application architecture, on the other hand, is designed by an application developer and dictates the broad structure of the application (e.g., client-server or P2P).
3. The process which initiates the communication is the client; the process that waits to be contacted is the server.
4. No. In a P2P file-sharing application, the peer that is receiving a file is typically the client and the peer that is sending the file is typically the server.
5. The IP address of the destination host and the port number of the socket in the destination process.

10. A protocol uses handshaking if the two communicating entities first exchange control packets before sending data to each other. SMTP uses handshaking at the application layer whereas HTTP does not.
11. The applications associated with those protocols require that all application data be received in the correct order and without gaps. TCP provides this service whereas UDP does not.

$$D_{cs} = \max\left\{\frac{NF}{u_s}, \frac{F}{d_{min}}\right\} \qquad D_{P2P} = \max\left\{\frac{F}{u_s}, \frac{F}{d_{min}}, \frac{NF}{u_s + \sum_{i=1}^{N} u_i}\right\}$$

GBN: sequence number has k bits, window size is $[0, 2^k-1]$. One Timer.
If window size is 5, sequence number has at least 3 bits.
In GBN, the receiver has a window size of 1. Cumulative acknowledgment 累积确认(TCP 也是)
SR: In Selective Repeat, the sender window has the same size as the receiver window.
Every packet has it own Timer.
Window size must be less than or equal to half the size of the sequence number space.
For a 4-bit sequence number field in the packet header, the maximum window size for Selective Repeat is 8.
To speed up file transfers, a Selective Repeat implementation is using a window size of 8. The sequence number field in the packet header must be at least 4-bit long.

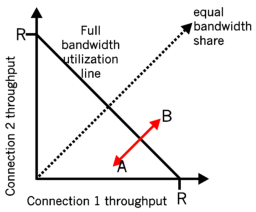
ISN(Initial Sequence Number) is random for security.

下一个ACK 等于上一个Seq 加上实际数据字节，下一个Seq 等于上一个ACK.
EstimatedRTT = (1 - 0.125) * EstimatedRTT + 0.125 * SampleRTT
DevRTT = (1 - 0.25) * DevRTT + 0.25 * | SampleRTT - EstimatedRTT |
TimeoutInterval = EstimatedRTT + 4 * DevRTT

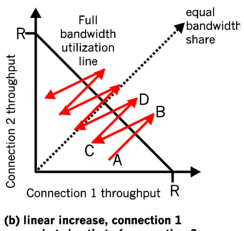
Sequence numbers are required for a receiver to find out whether an arriving packet contains new data or is a retransmission.

I. To handle losses in the channel. If the ACK for a transmitted packet is not received within the duration of the timer for the packet, the packet (or its ACK or NACK) is assumed to have been lost. Hence, the packet is retransmitted.

Refer to Figure below. In Figure (a), the ratio of the linear decrease on loss between connection 1 and connection 2 is the same - as ratio of the linear increases: unity. In this case, the throughputs never move off of the AB line segment. In Figure (b), the ratio of the linear decrease on loss between connection 1 and connection 2 is 2:1. That is, whenever there is a loss, connection 1 decreases its window by twice the amount of connection 2. We see that eventually, after enough losses, and subsequent increases, that connection 1's throughput will go to 0, and the full link bandwidth will be allocated to connection 2.



(a) linear increase, with equal linear decrease



(b) linear increase, connection 1 decrease is twice that of connection 2

a) GoBackN:
A sends 9 segments in total. They are initially sent segments 1, 2, 3, 4, 5 and later resent segments 2, 3, 4, and 5.
B sends 8 ACKs. They are 4 ACKS with sequence number 1, and 4 ACKS with sequence numbers 2, 3, 4, and 5.

Selective Repeat:
A sends 6 segments in total. They are initially sent segments 1, 2, 3, 4, 5 and later resent segments 2.
B sends 5 ACKs. They are 4 ACKS with sequence number 1, 3, 4, 5. And there is one ACK with sequence number 2.

22. Five generic tasks are error control, flow control, segmentation and reassembly, multiplexing, and connection setup. Yes, these tasks can be duplicated at different layers. For example, error control is often provided at more than one layer.

24. Application-layer message: data which an application wants to send and passed onto the transport layer; transport-layer segment: generated by the transport layer and encapsulates application-layer message with transport layer header; network-layer datagram: encapsulates transport-layer segment with a network-layer header; link-layer frame: encapsulates network-layer datagram with a link-layer header.

25. Routers process network, link and physical layers (layers 1 through 3). (This is a little bit of a white lie, as modern routers sometimes act as firewalls or caching components, and process Transport layer as well.) Link layer switches process link and physical layers (layers 1 through2). Hosts process all five layers.

- **Your computer first uses DHCP to obtain an IP address.** Your computer first creates a special IP datagram destined 255.255.255.255 in the DHCP server discovery step, and puts it in a Ethernet frame and broadcast it in the Ethernet. Then following the steps in the DHCP protocol, your computer is able to get an IP address with a given lease time.
- A DHCP server on the Ethernet also gives your computer a list of IP address of first-hop routers, the subnet mask of the subnet where your computer resides, and the addresses of local DNS servers(if they exist).
- Since your computer's ARP cache is initially empty, **your computer will use ARP protocol to get the MAC address of the first-hop router and the local DNS server.**
- Your computer first will get the IP address of the Web page you would like to download. If the local DNS server does not have the IP address, then **your computer will use DNS protocol to find the IP address of the Web page.**
- Once your computer has the IP address of the Web page, then it will send out the HTTP request via the first-hop router if the Web page does not reside in a local Web server. The HTTP request message will be segmented and encapsulated into TCP packets, and then further encapsulated into IP packets, and finally encapsulated into Ethernet frames. Your computer sends the Ethernet frames destined to the first-hop router. Once the router receive the frames, it passes them up into IP layer, checks its routing table, and then sends the packets to the right interface out of its all interfaces.
- Then your IP packets will be routed through the Internet until they reach the Web server.
- The server hosting the Web page will send back the Web page to your computer via HTTP response message. Those messages will be encapsulated into TCP packets and then further into IP packets. Those IP packets follow IP routers and finally reach your first-hop router, and then the router will forward those IP packets to your computer by encapsulating them into Ethernet frames.

A7. The maximum size of data field in each fragment = 480 (20 bytes IP header).
Thus the number of required fragments = (3000-20)/480 = 7

Each fragment will have Identification number 422. Each fragment except the last one will be of size 500 bytes (including IP header). The last datagram will be of size 120 bytes (including IP header). The offsets of the 7 fragments will be 0, 60, 120, 180, 240, 300, 360. Each of the first 6 fragments will have flag=1; the last fragment will have flag=0.

(a) NAT will not have an entry for a connection initiated from the WAN side, hence will drop incoming packets from Arnold.

(b) Bernard can know the IP address of Arnold through Cindy. Then, the p2p application can initiate a connection through NAT to Arnold and upload the file.

A9. 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.

1) The IP addresses of A and E would have to have the same network prefic since they are now part of the same subnet.
2) There is no need to change the physical (LAN) addresses.
3) The switch uses backward learning algorithm. When a host sent a frame through the switch, the switch would observe the LAN address of the sender and the interface through which it has arrived and record this value in its forwarding table.

No, without a public-private key pair or a pre-shared secret, Bob cannot verify that Alice created the message.

Yes, Alice simply encrypts the message with Bob's public key and sends the encrypted message to Bob.

(a) This is because Sheldon's NAT device is not recomputing the TCP and IP checksums after it changes the IP address and port numbers in each packet that passes through it. As a result, when routers in the Internet compute the checksum for these packets, they detect an error and hence, drop the packets

(b) Remember that FTP commands contain the port number and IP address of the end hosts (e.g. PORT). For FTP to work effectively through a NAT, the NAT must be configured to replace the IP addresses and port numbers used in accordance with the NAT translation table. Sheldon has not configured his NAT accordingly and hence he cannot use FTP. However, no such configuration is required for Web and hence he can successfully browse the Web.

TCP:
A sends 6 segments in total. They are initially sent segments 1, 2, 3, 4, 5 and later resent segments 2.
B sends 5 ACKs. They are 4 ACKS with sequence number 2. There is one ACK with sequence numbers 6. Note that TCP always send an ACK with expected sequence number.

b) TCP. This is because TCP uses fast retransmit without waiting until time out.

A1. framing: there is also framing in IP and TCP; link access; reliable delivery: there is also reliable delivery in TCP; flow control: there is also flow control in TCP; error detection: there is also error detection in IP and TCP; error correction; full duplex: TCP is also full duplex.

A2. An ARP query is sent in a broadcast frame because the querying host does not which adapter address corresponds to the IP address in question. For the response, the sending node knows the adapter address to which the response should be sent, so there is no need to send a broadcast frame (which would have to be processed by all the other nodes on the LAN).

A3. C's adapter will process the frames, but the adapter will not pass the datagrams up the protocol stack. If the LAN broadcast address is used, then C's adapter will both process the frames and pass the datagrams up the protocol stack.

Switch learns interface corresponding to Mac address of A
Since switch table is empty, so switch dose not know the interface corresponding to Mac address of D.

a) No. E can check the subnet prefix of Host F's IP address, and then learn that F is on the same LAN. Thus, E will not send the packet to the default router R1.
Ethernet frame from E to F:
Source IP = E's IP address
Destination IP = F's IP address
Source MAC = E's MAC address
Destination MAC = F's MAC address

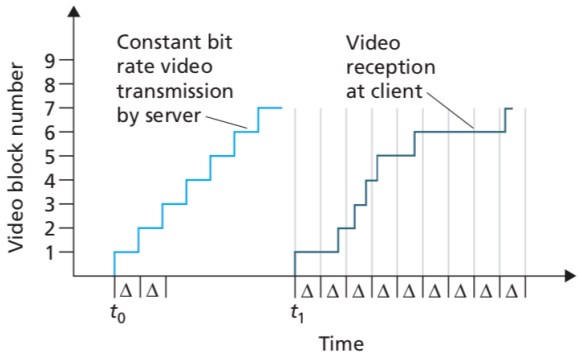
b) No, because they are not on the same LAN. E can find this out by checking B's IP address.
Ethernet frame from E to R1:
Source IP = E's IP address
Destination IP = B's IP address
Source MAC = E's MAC address
Destination MAC = The MAC address of R1's interface connecting to Subnet 3.

c) Switch S1 will broadcast the Ethernet frame via both its interfaces as the received ARP frame's destination address is a broadcast address. And it learns that A resides on Subnet 1 which is connected to S1 at the interface connecting to Subnet 1. And, S1 will update its forwarding table to include an entry for Host A.

Yes, router R1 also receives this ARP request message, but R1 won't forward the message to Subnet 3.

B won't send ARP query message asking for A's MAC address, as this address can be obtained from A's query message.

Once switch S1 receives B's response message, it will add an entry for host B in its forwarding table, and then drop the received frame as destination host A is on the same interface as host B (i.e., A and B are on the same LAN segment).



Problem 1

a) Client begins playout as soon as first block arrives at t1 and video blocks are to be played out over the fixed amount of time, d. So it follows that second video block should be arrived before time t1 + d to be played at right time, third block at t1 + 2d and so on. We can see from figure that only blocks numbered 1,4,5,6 arrive at receiver before their playout times.

b) Client begins playout at time t1 + d and video blocks are to be played out over the fixed amount of time, d. So it follows that second video block should be arrived before time t1 +2d to be played at right time, third block at t1 + 3d and so on. We can see from figure that video blocks numbered from 1 to 6 except 7 arrive at receiver before their playout times.

c) Maximum two video blocks are ever stored in the client buffer. Video blocks numbered 3 and 4 arrive before t1 + 3d and after t1 + 2d, hence these two blocks are stored in the client buffer. Video block numbered 5 arrives before time t1 + 4d and after t1 + 3d, which is stored in the client buffer along with already stored video block numbered 4.

d) The smallest playout at the client should be t1 + 3d to ensure that every block has arrived in time.

The energy magnitude of the signals from the sender may overwhelm other signals from other nodes, since the wireless signals decay very quickly in distance. It is thus hard to physically detect collision at the sender.

With those difficulties, 802.11 implements CSMA/CA (Collision Avoidance, with RTS/CTS) instead.

(a) C's packet would indeed arrive successfully at D, since D cannot hear A's transmission. Hence, there is no interference from the perspective of the receiver (i.e. D).
However, A's packet would not arrive successfully at B, since there will be a collision at B due to interference from C's transmission.

(b) C will not transmit while A is transmitting. This is because C would have overhead the CTS frame sent by B (in response to the RTS request from A). The CTS frame will contain the duration of time for which the on-going transmission between A and B will go on. Thus, C will know when A is transmitting.

(c) Same reason as above. The CTS contains the time and hence, C will know when A's transmission will end.

It is not possible to devise such a technique. In order to establish a direct TCP connection between Arnold and Bernard, either Arnold or Bob must initiate a connection to the other. But the NATs covering Arnold and Bob drop SYN packets arriving from the WAN side. Thus neither Arnold nor Bob can initiate a TCP connection to the other if they are both behind NATs.

吞吐量(throughout): rate at which bits transferred between sender and server (bits/time unit)
流量强度(traffic intensity): 到达的比特速率除以离开的比特速率 (aL/R)
平均排队时延会随流量强度增大而增大，界限为1.

发送方信道利用率(utilization): n倍。 $U_{\text{sender}} = \frac{L/R}{RTT + L/R}$

(iii) When link A-E fails, A realizes that the link has failed and tries to find a new neighbor to route through to E. A's routing table shows that the shortest available path to E is through neighbor B and has cost 4 (cost 3 to reach B and cost 1 from B to E). But now the path to B is through E and hence A will no select this option as A-E is down. A's routing table shows that the second shortest available path to E is through neighbor D and has cost 6 (cost 2 to reach D and cost 4 from D to E). Without realizing that D's next hop to E is A, A makes D the next hop neighbor for its route to C, and advertises a new cost of 6 to C in its routing advertisement. D then chooses the real shortest path of D-B-E. Though count to infinity occurs briefly due to the presence of an alternative path it is averted. Also if D advertises its path to C through B this situation will never have occurred. So this case may or may not cause count to infinity.

A solution to the count-to-infinity problem is poisoned reverse.