Questions and Problems for first part

1. Discuss the rationality behind the thinking of a layered structure for computer network software. What are the relationships between protocols, services and interfaces?

2. In your opinion, what is Intranet?

3. Describe briefly what is a virtual circuit. What kind of service will a virtual circuit offer?

4. To transmit at rate f_b requires approximately a bandwidth $B = f_b$. Someone cut the Department's Ethernet cable that connects workstations. You are doing repairing work and you find a replacement cable which is said to offer a bandwidth up to 16 MHz. Will this cable do the job? Why?

5. FDDI has a data rate of 100 Mbps. What is the actual rate going out to the fiber? Why the difference?

6. In Gigabit Ethernet, one of physical layer interface standards uses 1000Base-T with 4 pairs of category 5 twisted pair. Each category 5 twisted pair offers a bandwidth of 125 MHz, four pairs are used in each transmission direction, and a 5-levels line coding is employed. How can this interface achieves a data rate of 1 Gbps?

7. In broadband wireless physical layer interface, 64QAM is used for close-in subscribers, 16QAM is used for medium-distance subscribers, and QPSK is used for distant subscribers. With a typical 25 MHz bandwidth, what is the data rate offered to distant subscribers?

8. Describe the cell reception algorithm in ATM networks.

9. A data link layer protocol does flow and error controls. Can you think a single thing in the protocol design that make this possible?

10. In ATM network, will it be possible to implement flow and error controls at data link layer level?

11. A data link layer protocol uses sliding window flow control with 7-bit sequence number and go-back-n error control. What is the number of frames that a sender can transmit without the need for an ACK from receiver?

12. Discuss situations when you would prefer a full data link protocol to ensure error-free transmission and when you would want a light data link protocol and leave to higher layer to take care error-free transmission.

13. Describe three common techniques to provide frame flags for different data link layer protocols.

14. User A and user B are exchanging data using the HDLC protocol. User B received 6th I-frame from user A and finds it is erroneous. What should user B do to recover from this erroneous situation?

15. The efficiency of stop and wait protocol in the error-free case is given by

    $$U = \frac{1}{1 + 2a}$$

    where the link parameter a can be defined as the ratio of the propagation time to transmission time (frame time).

    Consider a satellite link, which has a round-trip propagation time of 300 ms. The average frame lasts 200 μs. What is the efficiency of this satellite link if the stop and wait protocol is used? Why the stop and wait protocol is inappropriate for links with long delay and short frame time?

16. From data link layer operation point of view, summarize the procedure of making an Internet point-to-point connection from a home PC using the point-to-point protocol (PPP). Notice how multiple network protocols can be supported in such an Internet connection.

17. The point-to-point protocol for Internet connection specifies a frame structure with a protocol field of 1 or 2 bytes. Explain what this protocol field is used for and why it is needed.

18. Ethernet uses the carrier sense multiple access with collision detection (CSMA/CD) protocol. Briefly summarize how this protocol works.

19. IEEE 802.3 specification has a minimum frame length of 64 bytes. Why 802.3 LANs need this specified minimum frame length?

20. The efficiency of Ethernet, under the heavy-load condition, is given by

$$U = \frac{1}{1 + 5.44a}$$

where

$$a = \frac{\text{medium length in bits}}{\text{frame length in bits}}$$

A 10 Mbps Ethernet has 1 km cable and an average frame length of 1024 bytes. Using the propagation speed of 2×10^8 m/s, calculate the efficiency U of this LAN.

21. A 1 km token ring operates at 16 Mbps. What is the physical length of a bit in meters? What is the physical length of this ring in bits? (The propagation speed is 200 m/μs). Why artificial delay may need to be inserted in a short ring?

22. In FDDI, an MAC mechanism called beacon process is used to locating failure station in a suspected broken ring. Can you describe how this beacon process works?

23. Use the hidden station problem and exposed station problem to explain why the carrier sense multiple access (CSMA) will not work for wireless LANs that use short range radio. What are the basic ideas of the medium access control protocol, MACA, for such wireless LANs?

24. Brief describe IEEE 802.11 wireless LANs medium access control.

25. Discuss why 802.3 – 802.5 MAC protocols are not suitable for MANs. Describe how distributed queue dual bus (DQDB) MAC protocol works.

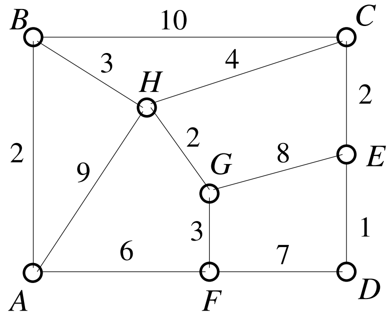
26. From the viewpoint of layered protocol structure, what is the difference between a bridge and a router?

27. Department has 3 Ethernet segments, connected by 2 transparent bridges into a linear network. One day, a new network administrator comes to work. He only knows IBM token rings, and notices that the ends of the network are not connected. So he orders a new transparent bridge and connects both loose ends of the network to the new bridge to make a closed ring. What happens next?

28. Describe how transparent bridge works.

29. In choosing best routes, the optimal principle can be very useful. What does the optimal principle say?

30. The topology of a network is given below, where the number on each line indicates the link cost.



What are the least-cost paths from A to F, from A to G, and from A to D, respectively? From these findings, draw a sink tree rooted at node A.

31. Link state routing is a widely used adaptive routing algorithm. Summarize how this routing algorithm works.

32. In broadcast routing, reverse path forwarding is often used. Describe briefly how this routing strategy works and explain why it is approximately optimal.

33. The concept of fixed home location or home agent makes the routing for mobile in a wide-area context easier. Describe how this routing strategy for mobile users works.

34. Alternative approach to fixed home agent is the mobile agent approach, which is an active research area in the ECS department. Can you seen any advantages and disadvantages of the mobile agent approach with respect to the fixed home agent approach?

35. Routing in ad hoc networks is typically done using the ad hoc one-dimensional distance vector algorithm. Basically, each node maintains a table, keyed by destination, giving information about that destination, including which neighbour to send packets in order to reach the destination. Describe how a node is able to build up this routine table.

36. Explain the differences between congestion control and flow control.

37. A computer on a 6-Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 1 Mbps. It is initially filled to capacity with 8 Mb. How long can the computer transmit at the full rate 6 Mbps?

38. Describe three congestion control policies that can be applied to virtual circuits subnets.

39. A network is heavily congested, and all the congestion control schemes in place have been tried but the congestion is not going away. A congested router decides to use its last resort, load shedding. It is carrying several virtual circuits for heavy file transfers. How should this router discards packets?

40. Explain how the congestion control based on hop-by-hop choke packets works.

41. Explain how the internetwork technique works in the case of both the source and destination host subnets are of the same type and the two ends are separated by some other WAN.

42. Is fragmentation needed in concatenated virtual-circuit internets or only in datagram systems?

43. Tunneling through a concatenated virtual-circuit subnet is straightforward: the multiprotocol router at one end just sets up a virtual circuit to the other end and passes packets through it. Can tunneling also be used in datagram subsets? If so, how?

Suggested answers and solutions for first part

1. A complete communication task across a computer network is very complicated. To make problem manageable, most network software are organized as a series of layers. Each layer at a machine performs a related subset of the functions required to communicate with another system. it relies on the next lower layer to perform more primitive functions and to conceal the details of how those functions are actually implemented.

   Logically, peer layers across the network talk to each other using protocols. The communication is actually carried out using some services provided by the lower lower. How a service can be accessed is via an interfaces. The peer protocols used in a layer are the layer's own business, as long as they get the job done. The service definition tells what a layer does. A layer's interface tells the layer above how to access it.

2. Intranet is just applying Internet services within an organization, like a company or a university department.

3. A full connection is set up between sender and receiver, but is implemented by packet switching, i.e. the route through the network is established prior to data exchange and is fixed for the duration of the logical connection but the connection is shared not dedicated. A virtual circuit offers connection-oriented service.

4. Ethernet data rate $R = 10$ Mbps. As Manchester encoding is used, the transmission rate or baud rate is

   $$f_b = 2R = 20 \text{ MHz}$$

   A bandwidth of 16 MHz is too small, and the cable cannot do the job properly.

5. 4b/5b encoding at physical layer, so the transmission rate is

   $$f_b = \frac{5}{4} \times R = \frac{5}{4} \times 100 \text{ Mbps} = 125 \text{ Mbps}$$

6. 5-levels line coding allows to transmit at 2 bits per symbol (with some spare). Since four pairs are used in each direction and each twisted pair can offer a bandwidth of 125 MHz. This provides at each direction the data rate

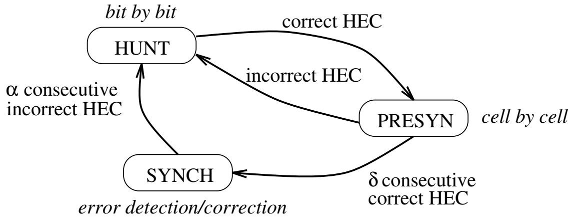
   $$R = 2 \times 4 \times 125 \text{ Mbps} = 1 \text{ Gbps}$$

7. QPSK allows to transmit at 2 bits per symbol. So 25 MHz of spectrum can provide the data rate

   $$R = 2 \times 25 \ \text{ Mbps} = 50 \ \text{ Mbps}$$

8. An ATM cell has a fixed length of 5-byte header followed by 48-byte payload. The 5-th byte of 5-byte header, HEC, is generated from the rest of header according to a known coding rule, and this forms the basis of cell reception algorithm:

   1. **HUNT**: a cell-delineation algorithm is performed bit by bit to determine if HEC coding law is observed. Once a match is achieved, it is assumed that one header has been found.



bit by bit
HUNT
correct HEC
incorrect HEC
α consecutive incorrect HEC
PRESYN
cell by cell
SYNCH
δ consecutive correct HEC
error detection/correction

   2. **PRESYN**: a cell structure is now assumed. Cell-delineation algorithm is performed cell by cell until encoding law has been confirmed δ times consecutively.

3. **SYNCH**: HEC is used for error detection and correction. Cell delineation is assumed to be lost if HEC coding law is recognized as incorrect α times consecutively.

9. Sequence number, which is essential in flow and error controls.

10. Flow and error controls are impossible at the data link layer level, as ATM cells do not contain a control field and thus no sequence number.

11. The maximum window size $N = 2^7 - 1 = 127$, the maximum number of frames allowed to send without the need to wait for an ACK.

12. A full data link protocol with its flow and error controls is very robust and can cope with networks with unreliable and noisy communications links, at the cost of introducing heavy overhead. So it is difficult to achieve high speed. To achieve high speed, a light data link protocol can be used for networks with reliable links. Error control may then be implemented within higher layer at an end-to-end basis.

13. Bit stuffing: Use 01111110 as frame flag, and make sure this pattern never appears inside a frame by bit stuffing – sender adds a 0 bit whenever it encounters five consecutive 1 bits in data, and receiver deletes the 0 bit that follows five consecutive 1 bits in the received data. An example is HDLC protocol.

    mb/nb ($n > m$) encoding: coding design ensure that some extra code bit patterns will be unique and never appear in coded data bit stream, thus provides frame flag. An example is FDDI 4b/5b encoding.

    Physical layer line coding violation: deliberate violating physical layer line coding rule to signify special event, i.e. the start of a frame. An example is ISDN BRI frame flag.

14. User B sends a supervisory frame REJ to user A with receive sequence number N(R) set to 6.

15. The link parameter

$$a = \frac{\text{propagation time}}{\text{frame time}} = \frac{300 \text{ ms}}{0.2 \text{ ms}} = 1500$$

    The efficiency of the link with the stop and wait protocol

$$U = \frac{1}{1 + 2 \times 1500} \approx 3 \times 10^{-4} = 0.3\%$$

    The stop and wait protocol is very inefficient for links with large value of a.

16. 1. Call the provider's router via a modem to set up a physical connection.
    2. Send a number of Link Control Protocol (LCP) packets, embedded inside PPP frames, to negotiate the options of PPP connection, such as

    - The maximum payload size in data frames
    - Do authentication (e.g. ask for password)
    - Monitor the link quality (e.g. how many frames did not get through)
    - Compress headers (which is useful for slow links between fast computers)

    3. Send a number of Network Control Protocol (NCP) packets, embedded inside PPP frames, to negotiate the network layer configuration.

    For example, if your PC wants to run TCP/IP, the NCP for IP is used to do IP address assignment.
    4. Your PC is now an Internet host, able to send and receive IP packets.

5. When you are finished, the NCP shuts down the network layer connection, free IP address; the LCP shuts down the data link layer connection; and finally, your PC tells the modem to hang up the phone, releasing physical layer connection.

Notice the stage 3, this makes it possible to support different network layer protocols.

17. The protocol field is used to tell what kind of network packet is in the payload. This is certainly needed as Internet consists of various different "networks" which may support different network layer protocols.

18. In CSMA/CD, a user wishing to transmit : **1.** Listens to see if the channel is free. If the channel is idle, it transmits. If the channel is busy, it keeps listening until the channel is free, then transmits immediately (1-persistent).
2. During the transmission, it keeps listening to the medium to detect collision. If a collision is detected, it stops transmitting immediately, and waits a random period of time before goes back to step **1**.

19. In CSMA/CD, an important rule is that frames must be long enough to allow collision detection prior to the end of transmission. Otherwise, CSMA/CD degrades to CMSA. The worst-case time to detect a collision is 2τ, τ being the end-to-end (two farthest stations) propagation time. The minimum frame must therefore last longer than 2τ. For IEEE 802.3 LAN standard, this gives rise to a minimum frame time of 51.2 μs, or 64 bytes.

20. $R = 10$ Mbps, $d = 1$ km, $L = 1024$ bytes, $V = 2 \times 10^8$ m/s

$$a = \frac{Rd}{LV} = \frac{10^7 \times 1 \times 10^3}{1024 \times 8 \times 2 \times 10^8} = 0.0061$$

$$U = \frac{1}{1 + 5.44 \times a} = 0.97$$

21. The physical length of a bit is

$$V \text{ m}/\mu\text{s} \times \frac{1}{R}\ \mu\text{s} = 200 \times \frac{1}{16} = 12.5 \text{ m}$$

The physical length of this ring in bits is

$$\frac{1 \text{ km} \times 16 \text{ Mbps}}{200 \text{ m}/\mu\text{s}} = 80 \text{ bits}$$

The ring physical length in bits must be large enough to contain the token. For short rings, this may not be the case, and artificial delay much be inserted.

22. The beacon process is used to locate a fault in a ring that is suspected of being broken. It results in identifying the station that is directly downstream from the break. The process begins with one or more stations sending streams of special MAC frames called *beacon frames*, which have a frame control value of 1100-0010. The destination address field is set to zero. The rules are:

1. Whenever any station suspects a fault in the ring, it starts the beacon process by sending a continuous streams of beacon frames. A token is not required to send these frames.

2. If a station receives beacon frames from another station, the ring is not broken between the station and its upstream neighbor. The station stops sending its own beacon frames and forwards the received beacon frames to the next stations.

3. If a station receives its own beacon frames, the ring is not broken. The station ends the beacon process and starts the claim process to recreate the token.

4. If a beaconing station does not hear either its own or anyone else's beacons for a long time (10 s or so), it concludes that the ring is broken just before it.

Beaconing is a MAC layer mechanism and generally detects failures internal to the stations. External failures such as broken cables are detected easily by the lower PHY and PMD layers and by means of other mechanisms.

23. Wireless LANs use short range radio. If CSMA is used – Hidden station problem: Station A, wishing to transmit to B, senses the medium. A may falsely conclude that it can transmit, when in fact another station, hidden behind B (and out of the range of A), is already transmitting to B. Exposed station problem: A senses an ongoing transmission and falsely conclude that it may not transmit, when in fact the transmitter is out of the range of B. A can in fact safely transmit to B.

    MACA: The basic idea is to sense any activity around the intended receiver in order to decide whether to send frames. This is done via Request-to-Send and Clear-to-Send mechanism.

24. IEEE 802.11 MAC supports two modes of operation: distributed coordination function with no central control (access point), and point coordination function with base station controlling activities in its cell.

    For DCF, medium access control protocol is based on MACA (multiple access with collision avoidance).

    - To cope with noisy wireless channels, 802.11 allows frames to be fragmented into smaller pieces, each with its own checksum.
    - Fragments are individually numbered and acknowledged using stop-and-wait.
    - Once channel has been acquired using RTS and CTS, multiple fragments can be sent in row.

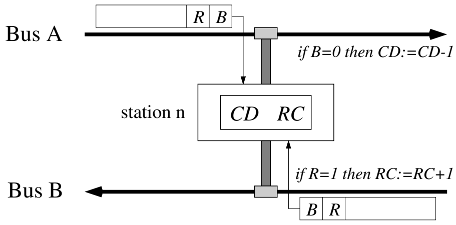
    For PDF, base station polls users, asking them if they have frames to send and controls transmission order. In this case, there is no collision, and a signed up user is guaranteed a certain fraction of bandwidth.

    - Base periodically broadcasts a beacon frame, which contains system parameters, such as hopping frequencies and dwell times (for FHSS), clock synchronization, etc., and it also invites new users to sign up for polling service.

    802.11 lets the two very different operation modes,PCF and DCF, to co-exist within a cell by carefully defining interframe time interval: after a frame has been sent, a certain dead time is required before any user may sent frame.

25. They are "greedy" based: if a station has a chance to transmit, it will do so regardless others. They are difficult to scale to larger MANs. For example, if 802.3 is used for MANs, because there are so many stations, collision will be so frequent that most of the bandwidth are wasted. For a token-ring protocol, token will take so long to go around (there are so many stations in the ring, they all want token for transmission), and a station will wait for too long for a chance to transmit.

    In a DQDB, stations are connected to dual buses with different flow directions. Direction of flow on a bus points to downstream. Fixed-size 53-byte cells with 44-byte payload are used. Each cell has a busy (B) bit and request (R) bit. Stream of cells flows down on a bus. If a cell is occupied, its B bit is 1. You make a request by setting a cell's R bit (if it is zero) to 1. DQDB MAC protocol is non greedy, and stations queue up in the order they became ready to send and transmit in FIFO order. Stations are polite to its downstream neighbors, and let them have go first if others make requests first. Consider the transmission on bus A (on bus B is similar):



Each station has a RC that counts the number of requests from its downstream stations. It also has a CD that counts the number of outstanding requests issued before its own request. Note that the downstream requests come from bus B, as you becomes "downstream" on bus B.

If a station wants to send something to its downstream (on bus A), it sets first available request bit in a cell on bus B to 1, and copies RC to CD. Assume that the value of CD at this moment is x. Then there are x requests from the station's downstream, and it has to let x free cells pass to the downstream. Also, the station must let its upstream stations on bus A know its request, that is why it uses bus B to make a **reservation**.

Each time a non-busy cell passes by, CD is reduced by 1. When CD drops to zero, the station can take the next non-busy cell on bus A to transmit.

26. Bridges operate at data link layer level, i.e. they do not examine the network layer header and simply pass network packets, unlike a router.

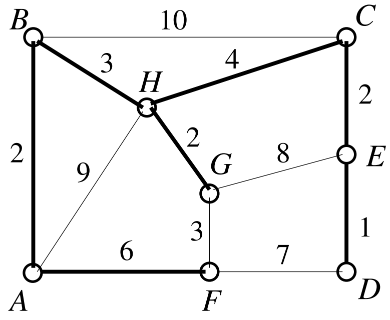
27. Nothing special. The new bridge announces itself and the spanning tree algorithm computes a spanning tree for the new configuration. The new topology will put one of the bridges into standby mode, so it will be available as a spare in case one of the others breaks. There is no looping problem.

28. Bridge must decide what to do with an incoming frame: discards it if destination and source LAN addresses in the frame are the same, or forwards it to destination LAN. Each bridge maintains a hash table, listing all the possible destination address/output line (LAN) pairs. When a bridge is first plug in, its hash table is empty, and this is how it figures out the configuration and keeps updating its hash table:

    - Flooding: incoming frames with unknown destinations are simply forwarded to all other LANs connected to the bridge.
    - Backward learning: bridge gradually learns which interface it can reach a host and builds up its hash table from incoming frames' source addresses.
    - Timeout: whenever a hash table entry is made, arrival time of the frame is noted in the entry. Whenever a frame whose source address already in the table arrives, its entry is updated with this new time. Periodically, bridge gets ride of those entries more than a few minutes old.

29. Optimality principle: If router B is on the optimal path from router A to router C, then the optimal path from B to C also falls along the same route.

30. The least-cost path from A to F: $A-F$; the least-cost path from A to G: $A-B-H-G$; the least-cost path from A to D: $A-B-H-C-E-D$. Sink tree rooted at node A:



It gives the optimal paths to every nodes.

31. Each router must:

    1. Find out its neighbours and get their network addresses. This is done by sending a HELLO packet on the router's each outgoing link, and getting a reply from the router at the other end.

    2. Measure the delay or cost to each of its neighbours. This is done by sending an ECHO packet to the neighbour and measure the round-trip delay.

    3. Construct a link state packet (LSP) to tell all it has just learnt. The LSP contains its identity, sequence number and age followed by the list of neighbours (identity and link cost).

    4. Send this packet to all the other routers. The LSPs are distributed by flooding but keep the flood in check with sequence number and age information.

    5. When a router has all the LSPs, it can construct the shortest path to all possible destinations, using the shortest path routing algorithm. The resulting sink tree is then used in routing decisions.

32. Assumption: In the normal operation, when router A forwards a packet to router B, it uses the outgoing link that lies on a sink tree rooted at B.

    Reverse path forwarding: When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending packets to the source of broadcast. If so, there is an excellent chance that the best route was used and this is the first copy to arrive at the router. The router then forwards the packet onto all lines except the one it arrived on. If, however, the packet arrived on a line other than the preferred one for reaching the source, the packet is discarded as a likely duplicate.

    Notice the assumption, it is normally true. This makes reverse path forwarding approximately optimal.

33. Routing strategy: Each mobile host has a permanent fixed home location. When a mobile host enters an area, it must register with the foreign agent in charge of the area. The foreign agent can then inform the mobile's home agent at the mobile's home location that the mobile is under its jurisdiction. When a packet is sent to a mobile host, it is routed to the mobile's home address. The mobile's home agent is then tunnelling it to the foreign agent where the mobile is currently in. The home agent can also inform the source where the mobile is, so that the subsequent packets can be sent directly to the foreign agent.

    The fixed home location or agent makes the things easier.

34. Fixed home address requires an expensive and huge investment, as in wireless mobile WANs. This is optional. Mobile agent is an active research area at ECS.

35. It is based on route discovery. Consider node A wants to send a packet to node I but it does not know how to do it. Node A broadcasts a ROUTE REQUEST (RReq) packet. When the RReq

packet arrives at A's neighbour node (A neighbour is one that can receive from you), it is checked to see if it is a duplicate or not (for flood control). If the packet is a duplicate, it is discarded. Otherwise, if the receiver knows a fresh route to the destination, it sends a ROUTE REPLY (RRep) packet back to the sender, giving routing information on how to reach the destination, and the process stop; otherwise it rebroadcasts the RReq packet to its neighbours.

So either node A gets the routing information back before the RReq packet reaches node I or, eventually, node I receives the RReq packet, and it replies with a RRep packet, which is sent back using the route that RReq packet came in and this provides A the routing information.

In route discovery, flooding is used, so many measures are employed to keep flood in check, and to make sure the route discovered is a fresh (live) one.

36. Congestion control is to do with making sure the subnet can carry the offered traffic. It is a global issue, involving all the hosts and routers. Flow control is related to the point-to-point traffic between given sender and receiver. Congestion control methods can be open-loop based or involving feedback. Flow control methods always involve direct feedback from receiver to sender.

37. $C = 8$ Mb, $M = 6$ Mb/s, $\rho = 1$ Mb/s,

$$S = \frac{C}{M - \rho} = \frac{8}{6 - 1} = 1.6 \text{ s}$$

38. 1. Admission control: Once congestion has been signaled, no more new virtual circuits can be set up until the problem has gone away. This is crude but simple and easy to do.

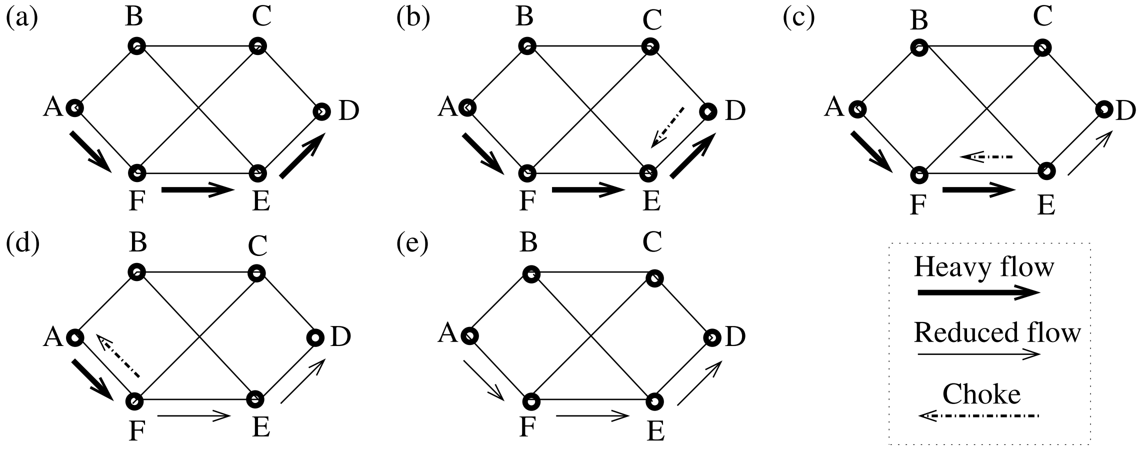
    2. Select alternative routes to avoid part of the network that is overloaded, i.e. temporarily rebuild your view of network by removing those congested routers, and from this "temporary" subnet, establish a virtual circuit to avoid congestion.

    3. Negotiate quality of connection in advance, so that the network provider can reserve buffers and other resources, guaranteed to be there.

39. It should adopt a wine policy, i.e. keeping old packets and drop new ones.

    For file transfer, an old packet is worth more than a new one. This is because dropping an old packet may force more packets to be retransmitted (since receiver will discard out-of-order packets). For this kind of applications, "the older the better".

40. The basic idea is that a congested router sends a choke packet to the source host who is causing the problem. The host is assumed to be cooperative and will slow down when received the "warning". To reduce the delay for responding to a choke packet, the hop-by-hop approach is adopted. Refer to the following figure. In (a), a host in San Francisco (router A) is sending heavy traffic to a host in New York (router D), and D is in trouble. In (b), D sends a choke packet back to source A. In (c), when the choke packet reaches the next router on the route E, it forwards the choke packet to the next router F as well as cuts the data traffic rate to router D immediately. Thus the congestion problem is "push-back" to E and D gets relief quickly. This process is repeated down the route until the "ball" is back to the "root" A, and it has to reduce the rate.



41. The technique is called tunneling. The multiprotocol router connecting the source subnet and the WAN simply encapsulates the packet in the payload field of the WAN packet and passes it to the multiprotocol router at the other end who retrieves the packet and injects it to the destination subnet. In this internetworking approach, the WAN in between acts like a serial line or "tunnel".

42. It is needed in both. Even in a concatenated virtual-circuit network, some networks along the path might accept 1024-byte packets, and others might only accept 48-byte packets. Fragmentation is still needed.

43. No problem. Just encapsulate the packet in the payload field of a datagram belonging to the subnet being passed through and send it.