PRIFYSGOL
BANGOR
UNIVERSITY

ICP-2011 – Computer Networks

Assignment – Review Questions

16th April 2018

Dominik Harmim (eeub8c)

Answers

1. **Pure Time Division Multiplexing (TDM)** – The time slots are allocated on a constant basis. This means that user 1 always gets time slot 1, user 2 always gets time slot 2, and so no. Provided bandwidth is not used efficiently. There is guaranteed transmission path.

   Statistical Time Division Multiplexing (STDM) – Allocates bandwidth to each user on the basis of demands and needs. A user uses time slots only when they are actually transmitting data. When a user is not sending data, no time slots are allocated to it, and other users that are sending data can use these time slots. Time slots are allocated statistically.

   raw data rate of the user $= \boldsymbol{B \cdot \frac{1}{T}}$ **b**
   raw data rate of the entire TDM channel $= \boldsymbol{B \cdot N \cdot \frac{1}{T}}$ **b**

   user A transmission bandwidth $= 10 \cdot 2 =$ **20 Mb/s**
   user C transmission bandwidth $= \frac{10}{2} =$ **5 Mb/s**

2. Error digit correction in given information matrix with column/row even parity digits:

0	0	1	0	
0	1	1	1	1
0	1	1	0	0
1	0	0	0	1
1	0	1	1	1

Table 1: Information matrix with column/row even parity digits

   Parity checking-based error correction technique fails when even number of errors occur.

3. Data network architecture diagram:

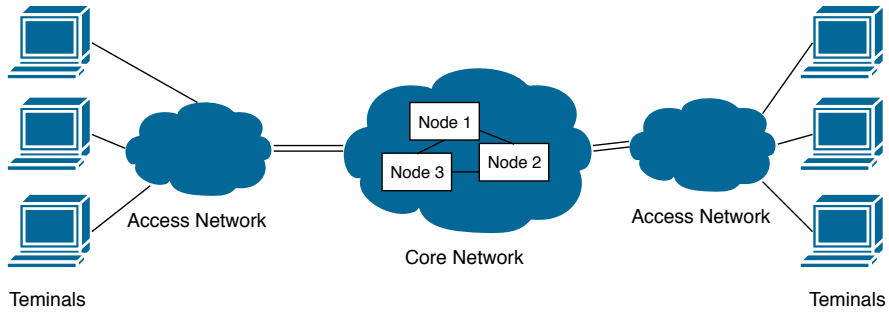

Figure 1: Data Network Architecture

   Communication protocol – Set of rules and procedures describing exchange the information within networks. Protocols enables devices to communicate by using set of rules.

   Communication architecture – Describes special functions that the computer hardware and software must perform to allow application programs to communicate with the outside world. Communication architecture is based on communication protocol.

4. OSI reference model layers:

   1 Physical Layer

   vi) Mechanical, electrical and functional interface.

2 Data Link Layer

i) Error correction and re-transmission.

iv) Responsibility for carrying frames between adjacent nodes.

vii) Flow control.

viv) Three packet switching technologies including X.25, Frame Relay and ATM.

3 Network Layer

iii) Route determination.

viv) Three packet switching technologies including X.25, Frame Relay and ATM.

4 Transport Layer

i) Error correction and re-transmission.

vii) Flow control.

viii) Reliable process-to-process message delivery.

5 Session Layer

ii) Establishing and monitoring an entire communication connection between users.

6 Presentation Layer

7 Application Layer

v) Communicates directly with user's application program.

5. Diagram shows content of packets when computer A sends data to computer D:

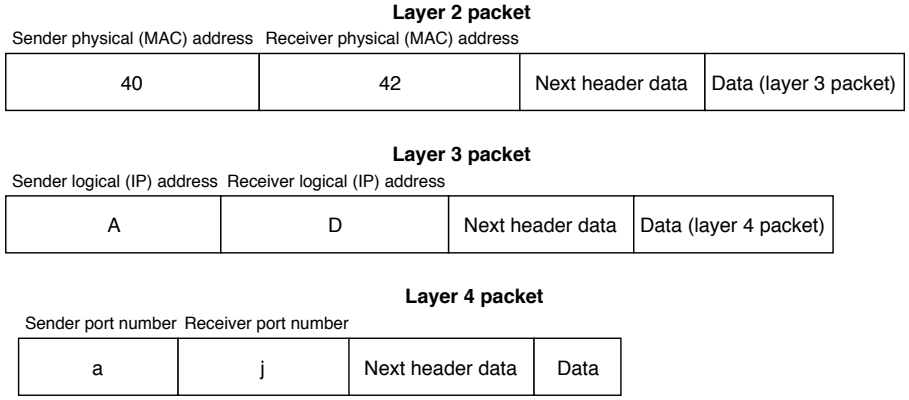

Figure 2: Computer A sends data to computer D

Diagram shows content of packets when computer D sends data to computer A:

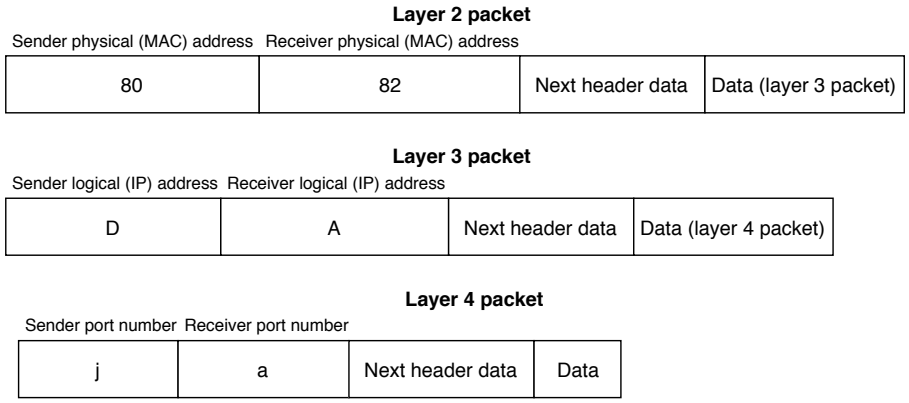

Figure 3: Computer D sends data to computer A

Data which sends computer A are encapsulated to layer 4 packet which in addition contains port numbers and other header information. Whole layer 4 packet is then encapsulated to layer 3 packet which in addition contains logical (IP) addresses and other header information. Finally is whole layer 3 packet encapsulated to layer 2 packet which in addition contains physical (MAC) addresses and other header information. This layer 2 packet is forwarded to layer 1.

If the physical destination address of a frame is corrupted during the transmission, the frame will be dropped and computer A can be informed about that either when receives this information from device that has received this corruption or computer A could waiting for some acknowledgment information which has not received.

Error control mechanisms are still required at layer 4 because sending data are basically divided on multiple packets and some of these packets may be dropped, lost or it could be lost their original order and such errors could be detected only at layer 4 of receiving side.

6. TCP in conjunction with IP can ensure the proper message delivery to the destination because TCP operates at layer 4 and ensures the reliability of user's message delivery, re-transmit data lost by the lower layers and IP operates at layer 3 and is responsible for routing and delivering individual packets.

   Diagram shows relationship between a TCP segment and an IP datagram:

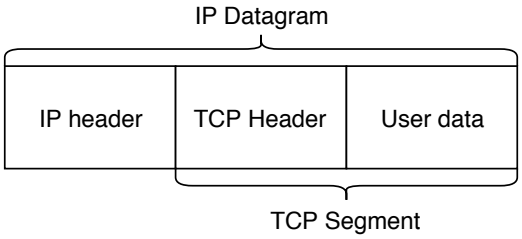

Figure 4: Relationship between a TCP segment and an IP datagram

7. Diagram of ATM switches:

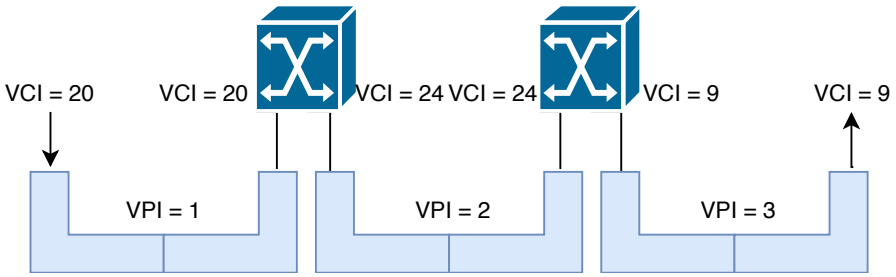

Figure 5: ATM switches using both VCI and VPI numbers

8. **TCP and UDP main differences** – TCP allows better error checking, more functionality and stability. UDP, however, lacks extensive error checking but is considered to be much faster than TCP. TCP, unlike UDP, establishes a virtual connection before transmission, guarantees the delivery of data over networks and if data is not received correctly, the sending computer will be notified and re-sends the information. TCP is connection-oriented protocol and UDP is connection-less protocol.

9. **Packet switching** – Information is divided into a number of specially formatted packets, each of which includes some addresses such as logical, physical and port addresses. These packets are routed by a

series of intermediate nodes of the network to the destination. At the destination, received packets are reassembled to form the original stream of data.

Connection-oriented packet switching – End-to-end virtual connection to the destination is established using single request packet that contains the source and destination addresses. The subsequent packets of the same message just need to carry the marking information, which defines the already established virtual connection. There is no need to look at addressing information to calculate a path for each packet, the intermediate nodes only read the marking information to route the packet to its destination.

Connection-less packet switching – Each packet of a message is an independent unit that contains the source and destination addresses. Each packet is independently routed at each intermediate nodes it crosses.

10. Routing table in a connection-less packet switched network **can not** have two entries with the same destination address because this routing table must unambiguously maps destination addresses to output ports.

    Switching table in a connection-oriented packet switched network

    i) **can** have two entries with the same input VPI,

    ii) **can** have two entries with the same incoming VCI and

    iii) **can not** have two entries with the same incoming VPI and VCI pair.

11. **Packet switching** – End-to-end virtual connection between two devices. Communication connection is always available and may be shared by many different users. Messages are split into a number of packets, which will be routed and switched separately. Cost-effective, because if no data is being transmitted, there are no transmission resources being wasted and bandwidth is shared with many users. Latency and loss of packets are the main concerns.

    Circuit switching – End-to-end physical connection between two devices. Established before the start of a communication section, shared by two users only and remains open for the entire communication section. Continuous data flow between two users. Not cost-effective, because stay on the line regardless of the usage of that line and bandwidth is no shared. A certain QoS can be guaranteed.

    Addressing mechanisms table:

Network Type	**Communication Stage**		
	Setup	**Data Transmission**	**Teardown**
Circuit Switching	end-to-end		local
Connection-less Packet Switching		end-to-end	
Connection-oriented Packet Switching	end-to-end	local	local

Table 2: Addressing mechanisms

12. Frame Relay can operate in a multi-protocol environment because it handles all protocols. It simply encapsulates another protocol into a Frame Relay envelope and carries it through the network.

13. **X.25:**

    Payload error control – Tight error control on every packet at every intermediate node.

    Latency – Large delay time. Error control increases transmission delay.

    Packet size – Relatively small packet size (128 bytes or 256 bytes long).

    Data transmission capacity – Operates at very low speeds ranging from 56 kb/s to 2 Mb/s.

    Types of traffic supported – For low speed data transmission only.

Frame Relay:

Payload error control – The intermediate nodes does not correct data errors. Error control at endpoints of networks.

Latency – Delay is reduced because the intermediate nodes does not correct data errors. Latency still could be a problem due to large packet size.

Packet size – Large packet size (up to 9 000 bytes and variable).

Data transmission capacity – Operates at a higher speed (45 Mb/s).

Types of traffic supported – Possible to carry voice and video.

Asynchronous Transfer Mode (ATM):

Payload error control – No payload error checking is made in the core of the networks. Payload error control at endpoints.

Latency – Latency is reduced due to uniform packet size. Time delay is minimized because no payload error checking is made in the core of the networks, routing time at each node across networks is minimizing and switching can be performed by hardware.

Packet size – Uniform 53-byte packet (5 bytes for addressing information and 48 bytes for payload).

Data transmission capacity – Speed can be very high (10 Gb/s to 160 Gb/s, Tb/s for some new products).

Types of traffic supported – Suitable for real-time traffic. Carries voice, data, multimedia, images, and other forms of traffic, so it is suitable for all kinds of traffic.

14. **Physical layer** – Provides the physical transportation of cells across network. It carries ATM cells rather than individual bits. These cells are multiplexed with other traffic for transmission. Physical layer defines transmission media, transmission rate, physical interface and coding schemes.

    ATM layer – Switches the cells around the network based on routing information. ATM layer provides routing, traffic management, switching and multiplexing services. Process outgoing traffic by accepting 48-byte segments from the AAL sub-layers and transforming them into 53-byte cells by adding a 5-byte header.

    ATM adaptation layer (AAL) – Assembles and disassembles broadband services into a stream of cells. The native traffic stream goes through the ALL, where it is segmented into 48-byte cells. ALL accepts any type of payload, both data frames and continuous stream of bits. AAL uses two sub-layers: the convergence sub-layer (CS) which guarantees the integrity of the data and the segmentation and reassembly sub-layer (SAR) where assembles and disassembles is performed. ATM defines four versions of the AAL: AAL1, AAL2, AAL3/4 and AAL5.

15. i) **1** padding byte is required. **1 087** data units are passed from SAR sub-layer to ATM layer. **1 087** ATM cells are produced.

    ii) Minimum number of ATM cells produced from an input packet may be **1** and maximum number may be **1 490**.

    iii) The value of `Btag` is repeated in each cell to identify all the cells belonging to the same packet. The value is the same as the value of `Etag`. So if there are 47 787 bytes of data, then the same `Btag/Etag` is repeated **2 174 times** and for maximum number of ATM cells, the same `Btag/Etag` is repeated **2 980 times**.

    iv) **LI (length indicator)** in CS header is the 6-bit field indicates how much of the final packet is data. **SF (start field)** in SAR header defines the offset from the beginning of the packet.

16. **Baseband transmission** – Transmits a digital signal directly through a cable, thus one signal is allowed at any given time. It is less expensive to implement but capacity and transmission length is limited.

    Broadband transmission – Signals are transmitted using carrier waves of different frequencies, thus multiple signals are allowed to transmit simultaneously. It is more expensive to purchase and maintain but bandwidth and length of transmission is not so limited.

    Topologies usage – The **tree** topology is commonly used in broadband LANs and the **bus**, **ring** and **star** topologies are used in basedband LANs.

17. Most common LAN topologies diagrams:

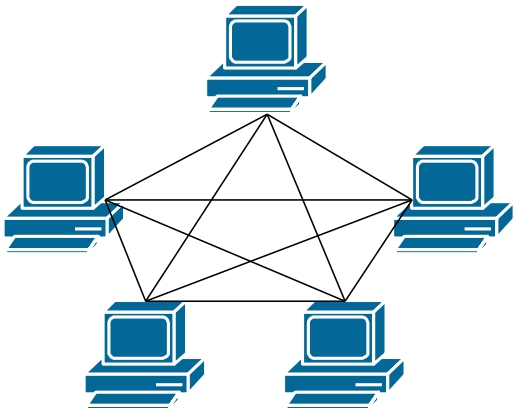

Figure 6: Mesh topology

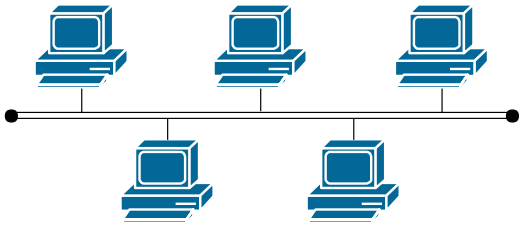

Figure 7: Bus topology

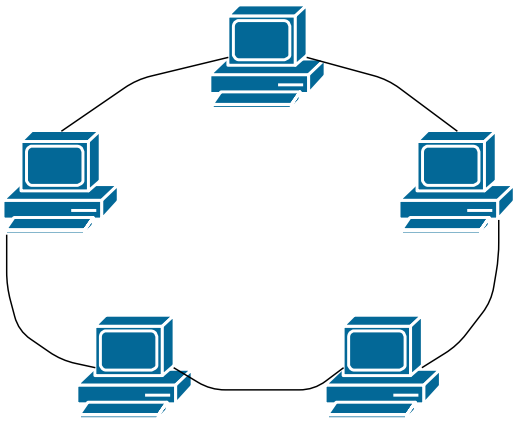

Figure 8: Ring topology

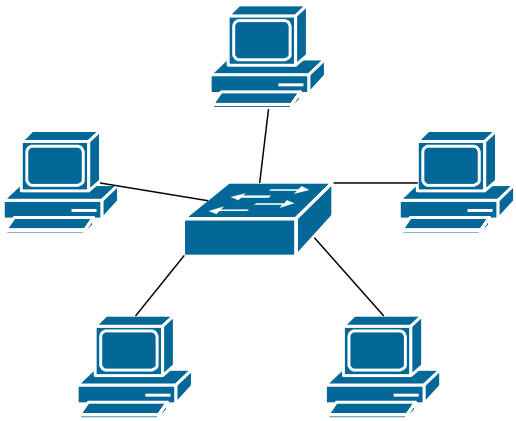

Figure 9: Star topology

    Tree topology – The tree topology has a root node, which forms the base of the network. The root node then communicates with a number of smaller nodes, and those in turn communicate with an even greater number of smaller nodes. Tree topology is actually combination of star and bus topology. Tree topology has binary tree structure. All transmission must pass through the root node.

18. Spanning trees diagrams (blocking ports are marked by dashed lines):

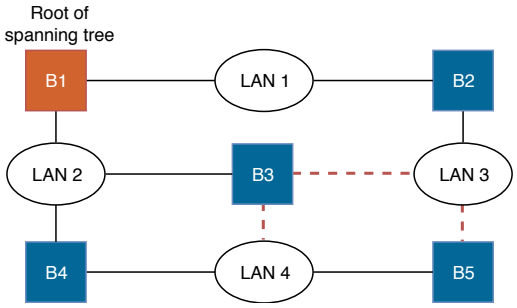

Figure 10: Spanning tree with bridge B1 as the root

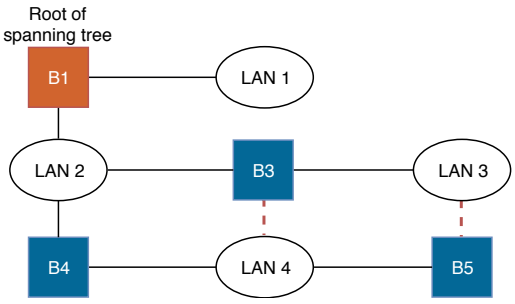

Figure 11: Spanning tree with bridge B1 as the root and bridge B2 is removed

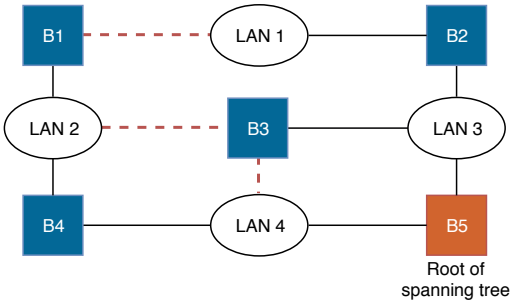

Figure 12: Spanning tree with bridge B5 as the root

19. **Token passing** – The master node inserts a token (specially formatted packet) into the ring. The token goes through the ring and is regenerated by each node it passes. When a node need to send a data, it waits for the token to pass by and grabs it off the circle. The node then can send the data. The data sent goes through the ring and are examined and regenerated by each node. Once the receiving node receives the data, it marks them as received then it regenerates them and re-injects them. This marks tells the sender that the data was received. The sender then generate a new token and injects it into the ring.

    CSMA/CD – When a node need to send a data, it set `attempt counter` to 1 and checks if there is some other transmitting node, if there is then it waits until there is no transmission and then it starts transmitting. Transmitting node also in meantime checks if there is collision, if there is not collision, it can transmit another data, checks for collision again until all data is transmitted. If there is collision, node waits some random time, increments `attempt counter` and then it could tries transmit again. If `attempt counter` is greater than maximum of possible attempts then there is something wrong and transmission is stopped.

20. The minimum frame size if we increase the data rate to 100 Mb/s will be $512 \cdot 10 = \mathbf{5\,120\ bits}$.

21. Bridges can solve traffic problems encountered in LANs because LANs can be divided into several parts using bridges and nodes on each part are said to be in separate collision domains. If nodes from different parts of the LAN, which are separated by bridges, transmit at the same time, they no longer collide witch each other.

    Procedure of building up bridge dynamic table that maps addresses to ports – Bridges inspects both the destination and source addresses. The source addresses are used for adding entries to the table and for updating purpose. If a packet arrives to the bridge, source address is mapped to the port from which the packed has arrived or if there already is port mapped to this source address, that port can be updated. Then if there is some port mapped to destination address, packet is forwarded to that port, otherwise packet is forwarded to all other bridge ports. After some amount of traffic on network, bridge should know where all addresses are located and no more forwarding to all ports is necessary.

22. **The key functionalities of bridges:**

    Filtering – Bridges have a table that maps addresses to ports. Based on this table, bridges checks destination addresses of incoming packets and decides whether the packets should be forwarded and to which port or dropped.

    Transparent and forwarding – If a bridge is transparent, other nodes don't know about its existence. Forwarding table is made automatically by learning packet movements in the network. Transparent bridges must correctly forward packets.

    Learning – Learning enables bridges to build up a dynamic table that maps addresses to ports automatically. Bridges inspects both the destination and source addresses. Procedure of bridges learning has been described in question number 21.

    Bridges and routers main differences:

    - Routers can support multiple protocols.
    - Routers do not require all nodes on connected LANs to have unique physical addresses.
    - Routers operate at the layer 3 and contain a virtual map of the network.
    - Routers use higher level (layer 3 - network) addresses. Bridges keep a table of layer 2 addresses of all active nodes on all connected networks. A routers know how to reach another routers. Routers know all only about LANs directly attached to that routers.

23. Three transmission windows may be used in optical fiber communications systems because these windows are created at different wavelengths (850 nm, 1 300 nm and 1 550 nm).

    A virtual communication path between two arbitrary users in an optical wide area network is created using both circuit switching and packet switching at one or more intermediate nodes. Circuit switching is achieved by connecting different WDM channels in the optical domain. Packet switching is achieved in the electrical domain by using protocols such as IP and ATM.

24. **Key functionalities of the optical layer** – Provide end-to-end optical connection between two nodes of the network and transmit data between two nodes at the bit rate at which individual channels of a WDM system operate.

    Sub-layers contained in the optical layer are

    - the optical transmission layer,
    - the optical multiplex layer and
    - optical channel layer.

25. If the maximum window size in TCP congestion control is 32 segments and threshold is 16 segments, than:

- The size of the congestion window after round 3 is **8** because congestion control starts in slow-start phase with windows size 1 and because the window size in this phase grows exponentially, in round 3 it is $2^3 = 8$.
- The size of the congestion window after round 5 is **17** because congestion control starts in slow-start phase with windows size 1 and because the window size in this phase grows exponentially, it reaches threshold in round 4, which is $2^4 = 16$ and then congestion control moves to congestion avoidance phase where window size is increasing linearly so in round 5, it is $16 + 1 = 17$.
- If a time-out occurs when the congestion window size is 20, the new threshold is **10**, because if a time-out occurs, threshold is set to one-half of the current window size, which is $20/2 = 10$. TCP congestion control should move to **slow-start phase**.
- The size of the congestion window after round 12 is **10**, because in round 8 when time-out occurs, congestion control starts again in slow-start phase and in round 12, congestion window size would reach 16, because round 12 is 4th round from round 8, which is $2^4 = 16$, but current threshold size is 10 so congestion window size is stopped in 10.
- If a three-acknowledgement event occurs when the congestion window size is 12, the new threshold is **6**, because if a three-acknowledgement event occurs, threshold is set to one-half of the current window size, which is $12/2 = 6$. TCP congestion control should move to **congestion avoidance phase**.