**Question 1**

Consider that you have joined a company and have been put on a project to design a communications network. A colleague on this project has little experience of the Internet but has heard of TCP/IP in this context. You need to convince this colleague of the advantages of using a layered protocol architecture.

1. Give four key points that summarize the advantages of using a layered protocol architecture in your design.  *[4 marks]*
2. *复杂问题分为很多块*
3. *问题可以在层内被定位*
4. *模块化问题，厂商可以各自发力*
5. *有更大的市场*
6. it can make complex problem divided into simple layers. --🡪Complex problem divided ; Easy to solve
7. once fix layer it can not influence the whole system, make problem separete. ----🡪
8. the layer problem solution also make a large market.-------🡪 more money
9. we can talk about it on a world around basis, so different teams from all over the world can have similar solutions or solution the similar problems, and also can understand eahc other easily ----🡪 modulization.

GPT答案

1. **Simplified Complexity**: A layered architecture breaks down the network communication process into manageable layers, each handling specific functions. This separation simplifies the complexity of network design and maintenance.
2. **Modularity and Flexibility**: Each layer can be developed, operated, and updated independently, allowing for greater flexibility in network design and easier integration of new technologies.
3. **Standardization and Interoperability**: Layered architecture promotes standardization, making it easier for different network components and systems to interoperate. It facilitates compatibility between hardware and software from various vendors.
4. **Easier Troubleshooting and Maintenance**: Issues within a network can be isolated within specific layers, simplifying the troubleshooting process. It also allows for targeted updates and improvements without overhauling the entire network.
5. Having convinced your colleague of the advantage of using a layered protocol architecture you now need to explain how this works. List four key points of the process of how layered protocols architectures operate. *[4 marks]*
6. **Layer-by-Layer Data Processing**: Each layer adds its specific information, like headers or footers, to the data as it passes downwards. During reception, each layer processes and removes its respective information.
7. **Encapsulation and Decapsulation**: Data is encapsulated with layer-specific control information as it descends through the layers. This encapsulation is reversed as data ascends, where each layer strips off its respective control information.
8. **Independent Layer Functions**: Every layer in the architecture has specific responsibilities, like error checking, encryption, or routing. Each layer operates independently, ensuring modularity in processing.
9. **Standardized Interfaces Between Layers**: Layers interact through standardized interfaces, allowing them to communicate and transfer data efficiently without needing to understand each other's internal workings.
10. Your colleague understands your description and asks about the ISO/OSI model layers. Provide the 7 layers of the ISO/OSI communications architecture in the correct order and provide **two** example functions provided by each layer. *[7 marks]*
11. **Physical Layer**:
    * Transmits raw bits over a physical medium.
    * Deals with the physical connection between devices and the transmission and reception of signals.
12. **Data Link Layer**:
    * Manages the physical addressing and frames for the physical transmission.
    * Handles error detection and correction from the physical layer.
13. **Network Layer**:
    * Manages the addressing and routing of data packets.
    * Ensures data packets are sent to the correct destination.
14. **Transport Layer**:
    * Ensures end-to-end communication and error recovery.
    * Manages flow control, ensuring data is sent at a rate suitable for both sender and receiver.
15. **Session Layer**:
    * Manages sessions between applications.
    * Controls the dialogues (connections) between computers.
16. **Presentation Layer**:
    * Translates data between the application layer and the network.
    * Manages data encryption and decryption.
17. **Application Layer**:
    * Closest to the end user.
    * Manages network-based services and applications
18. Your colleague has more experience of the TCP/IP operation and has heard of network address translation (NAT). Explain the purpose of network address translation (NAT) and how it works. *[4 marks]*
19. **Purpose of NAT**:

**Conserve IP Addresses**: NAT allows multiple devices on a private network to share a single public IP address. This is crucial given the limited availability of IPv4 addresses.

**Enhance Security**: By hiding private IP addresses from the public internet, NAT adds a layer of security, making it more difficult for external hosts to directly access internal devices.

1. **How NAT Works**:

**Translation Process**: When an internal device (like a computer within a home network) requests data from the internet, NAT translates the private IP address to the public IP address assigned to the router or NAT device. This translation is typically done at the router that connects the private network to the internet.

**Port Mapping**: NAT assigns a unique port number to each outgoing request. This way, when a response comes back to the router, NAT uses the port number to determine which internal device the response is for, and then forwards the response to the appropriate device.

**Types of NAT**:

**Static NAT**: Assigns a specific public IP address to a private IP address.

**Dynamic NAT**: Assigns any available public IP address from a pool.

**Port Address Translation (PAT)**: Allows multiple devices to share a single public IP address by differentiating them with unique port numbers.

1. Your colleague has heard that NAT addressing contravenes the ‘ISO/OSI layered protocol architecture rules’. Is this the case and if so how? *[1 mark]*
2. **Layer Crossing**: The ISO/OSI model clearly delineates functions across different layers from physical up to the application layer. NAT, however, operates at the network layer (Layer 3 - IP) but also makes use of transport layer (Layer 4 - TCP/UDP) information, specifically port numbers.
3. **Protocol Information Usage**: NAT involves modifying the IP addresses in the packet headers (a network layer function) and also often changes the TCP/UDP port numbers (a transport layer function). This intermingling of functionalities from different layers goes against the OSI model's principle of keeping layers separate and distinct.
4. **Impact on End-to-End Connectivity**: The OSI model advocates for maintaining the end-to-end principle, where communication should be directly managed by the end devices. NAT alters this by acting as an intermediary, modifying the IP addresses and potentially affecting the direct nature of the connections.

In essence, while NAT provides practical solutions for IP address scarcity and network security, it does so by operating in a way that doesn't fully align with the strict separation of concerns as outlined in the OSI model.

**Question 2**

You need to design two transport protocols for a communications network to provide respectively an unreliable connectionless service and a reliable connection oriented service; both will be using the services provided by an unreliable connectionless network.

1. Explain what an unreliable connectionless service is offering and how this could be provided. *[2 marks]*
2. **Definition and Offering**: An unreliable connectionless service provides a basic level of data transmission without guarantees on delivery, order, or error correction. It is typically characterized by its simplicity and speed.
3. **Provision Methods**:
   * **UDP (User Datagram Protocol)**: This is a common example of an unreliable connectionless protocol. UDP sends packets ("datagrams") without establishing a connection, making it suitable for applications where speed is more critical than reliability.
   * **No Acknowledgment**: There's no acknowledgment mechanism for the packets sent or received, which means the sender won't know if the data reaches the destination.
   * **Minimal Overhead**: Due to the lack of connection setup, maintenance, and teardown processes, the protocol introduces minimal overhead, contributing to faster data transmission.
   * **Best Effort Delivery**: The service offers "best effort" delivery, indicating that it attempts to deliver data but does not provide any guarantees or recovery methods for lost or corrupted packets.

[Simply a best effort service, i.e. data will be sent with no guarantees on delivery, (in-order or otherwise) or correctness. And there will be no feedback on whether or not data is delivered.]

1. Define what a ‘reliable connection oriented service’ is. *[3 marks]*

A 'reliable connection-oriented service' is a type of network communication where a dedicated connection is established between the sender and receiver before any data is transmitted. This service ensures the orderly and error-free delivery of data packets.

[Error free [1], in order delivery [1] of all data[1]. ]

A reliable connection-oriented service guarantees that all data is delivered correctly and in the order it was sent.

1. Explain the mechanisms which can provide a reliable connection oriented service when using an unreliable connectionless network. *[5 marks]*

The mechanisms that can provide a reliable connection-oriented service when using an unreliable connectionless network include error checking, acknowledgment, sequence numbers, timers, and flow control.

1. **Error Checking**: Ensures the data transmitted is error-free.
2. **Acknowledgment**: The receiver confirms the receipt of data, ensuring the sender is aware of the successful transmission.
3. **Sequence Numbers**: Used to order data packets, ensuring the sequential transmission of data.
4. **Timers**: Monitor the timing of data transmission and responses, helping to detect lost data packets.
5. **Flow Control**: Manages the rate of data transmission to prevent network congestion.
6. TCP is the Internet reliable connection oriented transport layer protocol. In addition to the mechanisms given in part ‘c’, TCP also provides ‘Congestion control’ and ‘Connection setup’.

(1)What is Congestion control aiming to achieve? *[1 mark]*

The objective of TCP's congestion control is to prevent traffic arriving at routers from overwhelming the input buffers and being discarded.

This is achieved by reducing the rate at which traffic is transmitted.

The aim is to ensure that the total aggregate traffic entering a network is less than the traffic leaving the network, addressing congestion as a fundamentally network-wide process.

(2)How does TCP detect congestion and are there any shortcomings in this detection mechanism? *[3 marks]*

TCP detects congestion primarily through timeouts and the Slow Start mechanism. A timeout occurs when the TCP sender does not receive any acknowledgements (ACKs) from the receiver for a certain period, leading the sender to assume that the segment is lost due to congestion, necessitating retransmission.

In the Slow Start phase, after establishing a connection, TCP begins with transmitting one segment. Upon receiving an ACK for this segment, TCP increases the congestion window (CongWin) by the size of the previously successful CongWin, effectively doubling the number of segments sent. This process continues as long as TCP receives corresponding ACKs or as allowed by the receive window (under flow control). The Slow Start phase concludes when CongWin reaches a predefined threshold or the receive window limit

(4)When a TCP connection has been established, TCP enters the ‘Slow Start’ mechanism. Describe the Slow Start mechanism. *[4 marks]*

The 'Slow Start' mechanism in TCP is a congestion control algorithm that gradually increases the amount of data transmitted over the network to avoid overwhelming the network. When a TCP connection is established, Slow Start begins with a small congestion window (CongWin), initially set to one or a few segments.

Here's how it works:

1. **Starting Small**: TCP starts with transmitting a small amount of data (typically one segment).
2. **Doubling**: For each acknowledgement (ACK) received, TCP increases the CongWin size, effectively doubling the window size for each round-trip time (RTT).
3. **Exponential Growth**: This process results in exponential growth of the congestion window, allowing TCP to quickly find the network's capacity limit.
4. **Threshold and Transition**: The Slow Start phase continues until the congestion window size reaches a threshold value, known as the slow start threshold (ssthresh). Upon reaching this threshold, TCP transitions to another phase, typically congestion avoidance, where the window growth becomes more conservative to avoid congestion.

Slow Start is crucial for TCP's ability to adapt to the network's capacity, ensuring efficient data transmission without causing congestion

(5)What action is taken by TCP when in the ‘Slow Start’ phase and congestion is detected? *[2 marks]*

[The CongWin threshold is halved, the CongWin is set to 1 MSS and the flow returns to the Slow Start mechanism.]

When TCP is in the 'Slow Start' phase and detects congestion, it takes the following action: the congestion window (CongWin) threshold is halved, and the CongWin is set to 1 Maximum Segment Size (MSS). After these adjustments, TCP returns to the Slow Start mechanism. This approach helps to alleviate congestion on the network by reducing the rate at which the sender transmits data, thereby preventing the network from being overwhelmed.

**Question 3**

This question is about addressing.

1. By completing a similar table to the following in your answer booklet, describe what (i) MAC addresses, (ii) IP addresses and (iii) Port Numbers are, the size of each in bits, how dynamic or permanent they are, and their purpose and the scope over which they act. *[15 marks]*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Used by: | Bit Size: | Permanence of assignment: | Purpose and scope: |
| MAC address | Link layer | 48-bit | No, fixed/permanent; hard wired at manufacture. | Forwarding frames on a LAN or subnet |
| IP address | Network layer | 32 bit(v4)  64 bit(v6) | Many different solutions exist, especially with v4 to allow for mobility and to extend the range of addresses.  With v6 and the vast number of available addresses they are predominantly assigned permanently. | Routing of packets across an internet. |
| Port Number | Transport layer | 16 bit | Assigned at call link establishment. There are commonly used port numbers  e.g. ftp = 20 & 21. | Addressing a segment to a particular process within a host. |

1. Explain how translation is done between MAC addresses and IP addresses and how and why attention is needed to keep the data up to date.  *[5 marks]*

使用地址解析协议（ARP）来执行MAC地址和IP地址之间的转换。ARP通过在网络上广播查询来找到与已知IP地址相对应的MAC地址。具有匹配IP地址的主机使用其MAC地址进行回复。该过程对于有效的网络通信至关重要，因为它将网络层（IP地址）链接到数据链路层（MAC地址）。需要注意保持ARP数据的最新状态，因为网络条件可能会发生变化，例如更换接口卡时。过时的ARP条目可能导致不正确的地址转换，从而导致网络上的通信问题。为了最大限度地减少流量并确保最新的信息，ARP条目会在一段超时时间内广播，之后它们会被更新或丢弃.

Hosts use the Address Resolution Protocol (ARP) to translate. Broadcasting of the entry on the network with a time out period for table entries is used to minimize the traffic generated and ensure information is kept up to date. The translation could change if for example an interface card failed and was replaced.

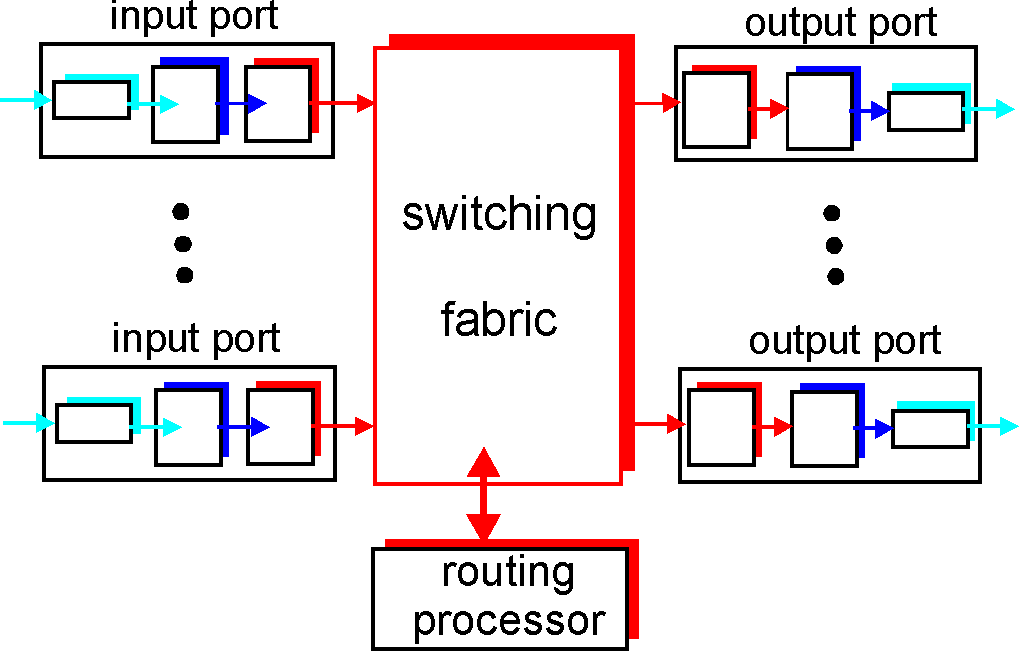
**Question 4**

This question is about routing.

1. Draw the key components of a router and indicate where queuing occurs, describing what causes it and the effects of queuing. *[8 marks]*

Four components :

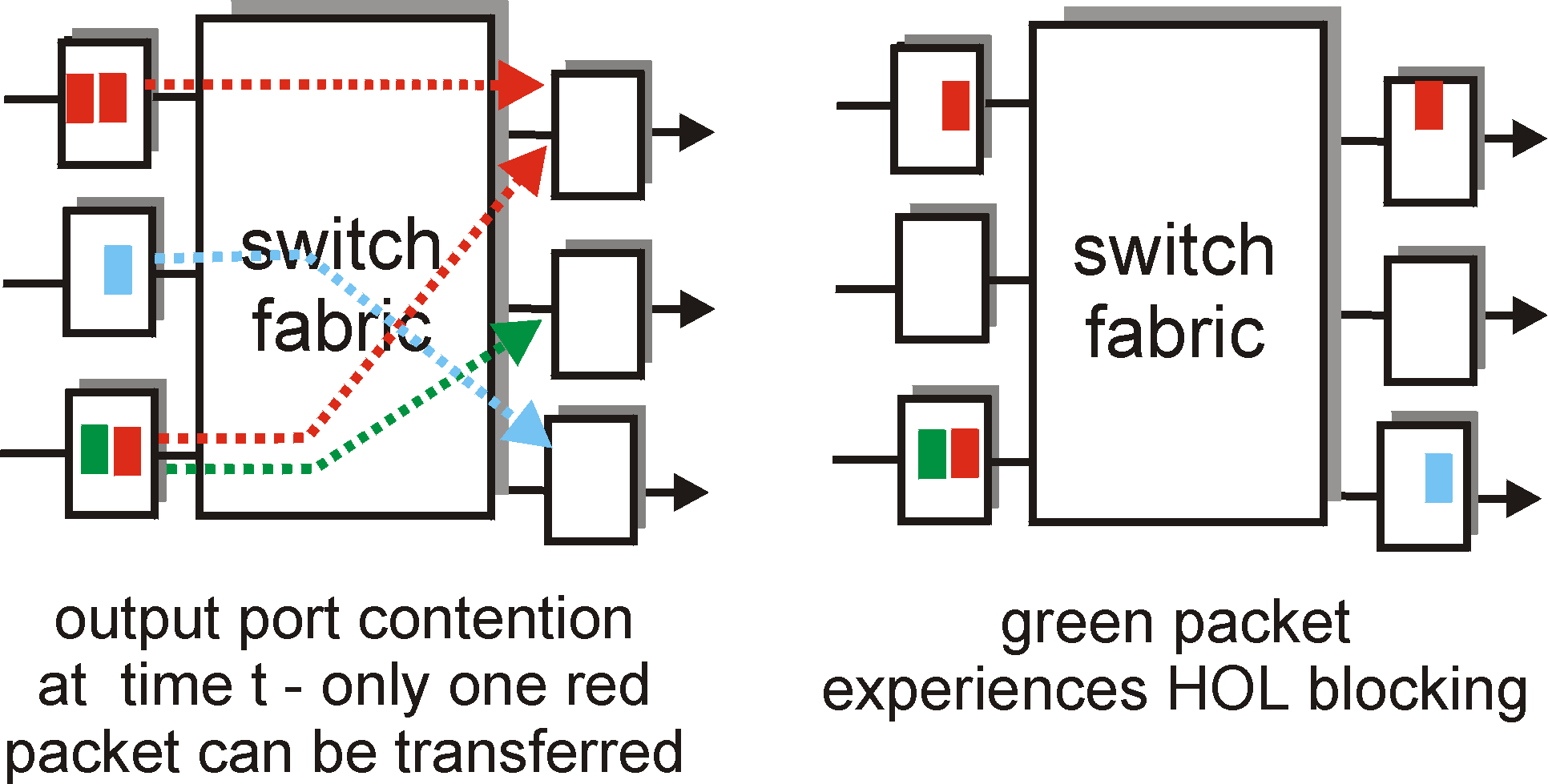
* Input Ports, Switching Fabric, Output Ports and Routing Processor



Queuing in routers

Fabric slower than input ports combined -> queuing may occur at input queues

Queuing delay and loss due to input buffer overflow!



1. Two fundamental routing algorithms are ‘Link state routing’ and ‘Distance Vector routing’. Describe how each one works. *[4 marks]*

**Link State Routing:**

Each router has complete knowledge of the network topology and link costs through link state broadcasts.

Routers compute the least cost paths from themselves to all other nodes.

The process is iterative, with routers updating their forwarding tables as they learn more about the network.

Notation includes c(xy) for link cost, D(v) for the cost of the path to destination v, and p(v) for the predecessor node along the path.

Distance Vector Routing:

Routers only know about their immediate neighbors and the cost to reach them.

They share their distance vectors with neighbors, which contain their best estimates of the distance to every other router.

The algorithm is decentralized and iterative, with each router updating its distance vector based on information from neighbors.

It uses the Bellman-Ford algorithm to calculate the best paths​​.

Both routing algorithms aim to find the most efficient paths for data packets, with Link State offering a more global view of the network and Distance Vector operating with more localized information.

1. Consider the following network.



With the indicated link delay (additive metric), use Dijkstra’s algorithm to compute the routing table for *x* to all network nodes. Show how the algorithm works by reproducing and completing the following table in your answer booklet (step 0 is given):

*[8 marks]*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **step**  **The End.** | **N’** | **D(y),p(y)** | **D(w),p(w)** | **D(v),p(v)** | **D(u),p(u)** | **D(t),p(t)** |
| 0  1  2  3  4  5 | x  xw  xwv  xwvu  xwvuy | 6, x  6,x  6,x  6,x  6,x | 1, x  1,x  1,x  1,x  1,x | 3, x  2,w  2,w  2,w  2,w | ∞  4,w  3,v  3,v  3,v | ∞  ∞  11,v  8,u  8,u |

Notation in the table:

* D(v): minimum delay of path from the source node to destination v, as of this iteration of the algorithm.
* p(v): previous node (neighbour of v) along the current minimum delay path from the source to v.
* N’: subset of nodes; v is in N’ if the minimum delay path from the source to v is definitively known.

**The End.**