|  |  |
| --- | --- |
| *This question paper consists of 5*  *printed pages, each of which is*  *identified by ELEC547101M* | *Drawing instruments and electronic calculators may be used.*  *Approved dictionaries may be used* |

**© University of Leeds**

**Examination for the Degree of MEng or MSc**

**(January 2014)**

**School of Electronic and Electrical Engineering**

**ELEC5471M: Data Communications and Network Security**

Time allowed: 3 hours

*Attempt any* **three** *questions*

**Do not write or draw with red ink or red pencil**

* *To obtain full marks candidates must show how answers are derived*
* *All symbols not specifically defined have their normally accepted meanings*

**Question 1**

1. Layered protocol architectures are used in communications network designs. Why?

[4 marks]

1. Because it can generate a bigger business and earn more money in different area.
2. It can divide the complex problem into several parts according to the layer, which can make it easier to address. -> Allow the whole problem to be sub-divided.
3. Allow alternative options to be substituted in at each layer. Allow different vendors to design their protocols within the same framework.
4. The design promotes modularity, simplify the design management and maintenance of networks.
5. List and describe disadvantages of using a layered protocol architecture in the design of a communications system.

[2 marks]

Disadvantages:

1. Some protocols span at serval layers, which may be difficult to define it at which layer. Leading to ambiguity in defining their specific layer.
2. The layered protocol has not bias at whatever network architecture, thus sometimes it would not be suitable for the certain design. The strict layer structure can be limiting in certain scenarios.
3. Communication between layers may introduce additional overhead in terms of processing time and resources.
4. The presence of multiple layers can contribute to the complexity of the protocol stack.
5. The International standards organisation (ISO) open systems interconnect (OSI) model is the generic architecture which is referred to worldwide. Name the layers, in the correct order of this architecture and give a key function performed at each layer.

[8 marks]

OSI:

1. Application layer
   1. Unit: message
   2. Key function: Transfer message between user and network device through application.
2. Presentation layer
   1. Unit: pPDU
   2. Key function: Encode and transfer the data to another type which can be read easily.
3. Session layer
   1. Unit: sPDU
   2. Key function: Establish, maintain and shutdown the session between the different entity.
4. Transport layer:
   1. Unit: segments
   2. Key function: Provide reliable communication and achieve the network congestion control and flow control to control the data send speed of the sender and receiver, which can better control the delay when transmit the data.
5. Network layer
   1. Unit: packages
   2. Key function: Achieve the route algorithm through such as Dijkstra to select the shortest route to destination and defined the logical addresses to the device such as IP address.
6. Data link layer
   1. Unit: frames
   2. Key function: Provide reliable transfer through bit such as correct and check the error.
7. Physical layer
   1. Unit: Bits
   2. Key function: Using the wire or wireless to connect the devices which is need to communicate in network.
8. Describe the main architectural differences between the ISO/OSI open systems interconnect architecture and the TCP/IP architecture.

[3 marks]

Differences:

1. OSI has the strict layer definition while TCP/IP architecture does not have. TCP/IP is more flexible.
2. The protocol in OSI is only for the certain layer, while span many layers in TCP/IP.
3. OSI does not bias any network design and thus people seldom use it to design network rather than TCP/IP. Because TCP/IP is more suitable for design particular networks. For example, OSI was developed by the International Organization for Standardization (ISO), aiming for a comprehensive and universal standard. TCP/IP, on the other hand, was developed by the U.S. Department of Defense with a focus on practical implementation in real-world networks.
4. Describe the advantages and disadvantages of adherence to the layering model in the TCP/IP architecture as compared to the ISO/OSI open systems interconnect architecture.

[3 marks]

Advantages:

1. Adherence to the layering model in the TCP/IP makes the complex problems more easily to address since it can be located in certain layer.
2. It encapsulates the details of the lower layer at certain layer which makes protocols can focus on providing services to upper layer.
3. Compared with OSI, the TCP/IP is more flexible and simple while the OSI is complex since it has seven layer.
4. Compared with OSI, the TCP/IP is widespread and more popular than OSI in real-world applications.

Disadvantages:

1. The layering model shadows the details of how the data transmit through the protocol and the sequence of the PDU.
2. The protocol spans many layers in TCP/IP may make confuse in locate the problem and implementation the protocol compared with OSI. It may limit modularity. Lacking of strict layer boundaries.
3. The TCP/IP sometimes may be too simple to handle the complex network scenarios.

**Question 2**

This question is about the Internet Protocol, IP.

1. What does an IP address refer to?

[1 mark]

The IP address refers to a logical address unique to the network device.

1. ‘128.85.170.3’ is a IPv4 Internet address expressed in dotted decimal notation. Give the binary equivalent of this address.

[1 mark]

1000 0000. 0101 0101. 1010 1010. 0000 0011

1. What is the binary equivalent of the following IPv6 address: ‘FFFF**::**5050**:**A0A**:**’

[1 mark]

IPV6: FFFF: 0000: 5050: A0A0

IPV4:

1111 1111 1111 1111

0000 0000 0000 0000

0101 0000 0101 0000

1010 0000 1010 0000

IPV6: FFFF: 0000: 0000: 0000: 0000: 0000: 5050: 0A0A

IPV4: 1111 1111 1111 1111:

0000 0000 0000 0000:

0000 0000 0000 0000:

0000 0000 0000 0000:

0000 0000 0000 0000:

0000 0000 0000 0000:

0101 0000 0101 0000:

0000 1010 0000 1010

The Internet Protocol is currently moving from version 4 to version 6.

1. List the improvements offered by IPv6 as compared to IPv4.

[7 marks]

Improvements:

1. IPV6 can provide more addresses than IPv4, which will address the problems of shortage of the IP address and improve the security. Larger Address space. IPV6 has 128 bits while the IPV4 has 32 bits.
2. IPV6 has more bit than IPV4, which can be used to express more status in IP addresses.
3. IPV6 can divided in wider range of use since it has more bits.
4. Efficient Routing and Aggregation: The IPV6 is designed with hierarchical addressing structure, which can facilitate more efficient routing and address aggregation.
5. Simplified Header Format: IPV6 has simplified and more efficient header format compared with IPV4.
6. Elimination of NAT: IPV6 has enough address to eliminate the need in use NAT at most of the cases.
7. Enhanced security features: IPV6 includes the security features such as IPSEC, which can significantly improve the security.
8. IPV6 supports the encapsulation of IPV6 packets within IPV4 packets, allowing for coexistence of IPV6 and IPV4 networks during the transition period.
9. IPV6 incorporates multicast as an intern part of the protocol, while IPV4 regard it as an extension.

During the transition period both IPv4 and IPv6 need to function on the Internet simultaneously.

1. How does a packet indicate that it needs to be processed as IPv4 or IPv6?

[1 mark]

It has an argument to point out whether it use the IPV6. It use the version field in the header to point out whether it use the IPV6, which is located in the first 4 bits of header both in the IPV4 and IPV6.

1. How can different IPv4 and IPv6 hosts both communicate with a single server?

[2 marks]

1. Dual Stack Configuration
   1. This configuration can make the server both support the IPV4 and the IPV6. When client initiates communication, it can choose the IPV4 or IPV6 to establish the connection.
2. IPV6-over-IPV4 Tunnelling
   1. If the server just supports the IPV4 or still don’t support IPV6. It can use the tunnel mechanism to communicate with the server who uses the IPV6.

1. How can two different hosts running only IPv6 communicate with one another across sections of the Internet which only use IPv4?

[2 marks]

The 6to4 tunneling mechanism allows IPv6 packets to be encapsulated within IPv4 packets, facilitating their transmission over IPv4-only networks.

Each host is assigned a unique IPv6 address that is constructed using its IPv4 address. This is done by combining the IPv6 prefix 2002::/16 with the IPv4 address of the host. For example, if the IPv4 address is A.B.C.D, the corresponding 6to4 IPv6 address would be 2002:ABCD::.

Hosts can then create tunnels between them by encapsulating IPv6 packets in IPv4 packets. These encapsulated packets can traverse IPv4-only sections of the Internet until they reach the destination host, where they are decapsulated.

1. Describe why two ways are needed for an IPv6 host to communicate with an IPv4 host and describe how these function.

[5 marks]

IPv6 hosts need two distinct methods to communicate with IPv4 hosts due to the incompatibility of the two IP versions. The primary reasons for the need for two ways are:

1. **IPv6-IPv4 Coexistence:**
   * IPv6 and IPv4 are different protocols with different addressing formats and structures. As the global transition to IPv6 takes place, both IPv4 and IPv6 networks coexist. During this coexistence period, some networks and hosts may still operate solely on IPv4, requiring mechanisms to enable communication between IPv6-only and IPv4-only entities.
2. **Addressing Format Incompatibility:**
   * IPv6 addresses are 128 bits long, while IPv4 addresses are 32 bits long. The addressing format and structure are fundamentally different. To facilitate communication, mechanisms are needed to bridge this gap and ensure compatibility between the two addressing schemes.

Two common methods for IPv6 hosts to communicate with IPv4 hosts are:

* **Dual Stack Configuration:**
  + In a dual-stack environment, an IPv6 host is configured to support both IPv6 and IPv4 simultaneously. The host is assigned both an IPv6 address and an IPv4 address, allowing it to communicate with both IPv6 and IPv4 hosts. Dual-stack hosts can seamlessly switch between IPv6 and IPv4 as needed.
* **Tunneling Mechanisms:**
  + Tunneling involves encapsulating IPv6 packets within IPv4 packets for transmission over an IPv4 network. This allows IPv6 traffic to traverse IPv4-only segments of the network.
  + Tunneling mechanisms, such as 6to4 and Teredo, create a virtual connection or tunnel between IPv6 hosts over an IPv4 network. These tunnels encapsulate IPv6 packets in IPv4 packets for transmission across IPv4-only sections, ensuring end-to-end communication between IPv6 and IPv4 hosts.

**Question 3**

1. In the operation of TCP what is the objective of Flow Control and what particular parameters does TCP use to provide it?

[3 marks]

The objective of Flow Control:

* + 1. Control the rate of the message send, which ensure the message sender send would not overwhelm the buffer of the receiver.
    2. Reduce the possibility of the message discarded since the data overwhelm the buffer

The parameters TCP use to provide:

1. Window size bit : It point out how much the receiver window has.
2. Finish bit : which point out whether this session is end.
3. Acknowledge bit : point out whether the receiver receive last message.
4. Syn bit: point out whether the receiver and the sender is synchronized.
5. Sequence number: point out what’s the turn of the message makes the message delivered in turn.
6. TCP provides Flow Control and Congestion Control. How do the objectives of Flow Control and Congestion Control differ?

[4 marks]

The difference between the Flow Control and Congestion control:

1. The Flow Control is aimed at addressing the problem the data transmission between the sender and receiver such as the overwhelm the buffer of the receiver.
2. The flow control is aimed at ensuring the data delivered in turn.
3. The Congestion control is aimed at making the route would not face the congestion dynamics.
4. The Congestion control is aimed at addressing the problem the data transmission among the networks such as network congestion and change the route of the network.
5. Using the ‘stop and wait’ Flow Control mechanism explain (with the aid of diagrams) how the loss of a corrupted information segment can be overcome.

[2 marks]

1. In the stop and wait Flow Control mechanism, if the sender send a information segment but it lost, the receiver would not send the acknowledgement back. And thus, the timer of the sender will over time and it will retransmission the data again.
2. Using the ‘stop and wait’ Flow Control mechanism explain (with the aid of diagrams) how the loss of a corrupted acknowledgement segment can be overcome.

[2 marks]

1. If the acknowledgement segment receiver send was lost, the sender would not receive the Acknowledgement segment and its timer will over time and then retransmission the segment again and the receiver will retransmit the Acknowledgement segment again.
2. A series of information frames of length 125 Bytes are transmitted over the following links using the ‘stop and wait’ Flow Control mechanism. The velocity of propagation across these links is 2 x 108 m.s-1. For each link determine the link efficiency.
3. a 1000 km link with a data transmission rate of 1 Gbps.

[3 marks]

The length of the frames = 125 \* 8 = 1000 bit

The distance of the link = 1000\*1000 = 10^6 m

The Transmission rate = 1 \* 10^9 bps

The link efficiency = s

1. a 10m link with a transmission rate of 1 Mbps.

[3 marks]

The link efficiency =

1. Comment on this result and use a table to compare alternative flow control mechanisms. Include the advantages and disadvantages of each mechanism in your table.

[3 marks]

**Question 4**

1. Describe the Internet data transfer service offered by TCP.

[3 marks]

1. The data transfer through TCP is responsible, which means the TCP will ensure the data transfer to the destination through flow control and congestion control.
2. The data transfer through TCP is in turn, TCP has the sequence number argument and the acknowledgement number and sync number to ensure the segment send from sender is in turn.
3. The TCP has the mechanism to detect and correct the error, TCP uses the checksum and retransmission mechanism to correct or detect the error.
4. Describe the Internet data transfer service offered by UDP.

[2 marks]

1. The UDP send the data is not responsible, since the transfer service not depend on the connection, which means the UDP would not establish the connection while it will send the data directly.
2. The data UDP send would not guarantee the sequence since it doesn’t has the mechanism.
3. The UDP has the simplest checksum mechanism to offer a minimum error detect mechanism.
4. Since both TCP and UDP provide their services using the same layer below. Describe how the difference in service provided by TCP, as compared to UDP, is achieved and any parameters used in provision.

[5 marks]

1. Compared with the TCP, the UDP has higher bandwidth, and it is suit for the live or game.
2. Compared with UDP, the rate of the TCP transmission would be lower since it has more mechanisms to ensure the data is responsible. UDP uses the checksum bit to implement this mechanism.
3. TCP has the window size to point out the size of the receiver buffer which is essential to the flow control.
4. TCP has the Acknowledgement bit, the Sequence number bit, finish bit and the synchronization bit to establish the connection through three steps hand-shake process.
5. TCP has the checksum bit, which is used to implement the mechanism of the detect and correct the error.
6. TCP’s header has the type bit to point out whether this segment is TCP.
7. Both TCP and UDP has the length bit to point out the size of the segment.
8. Describe the process within the TCP entity of establishing a TCP connection.

[6 marks]

It uses the three-steps handshake to establish a TCP connection:

1. The sender send a request segment to receiver and the sequence number is 1, the SYN number is 1.
2. After receiving the request segment, the receiver responds a ACK package, which point out the 1 of ACK bit.
3. The sender reply the ACK segment and after that it will begin to send messages.
4. What applications might chose to use UDP and why?

[4 marks]

1. The live application, since the live needs high bandwidth to play the video and it does not concern about the rate of the error.
2. The game application may choose the UDP also, since the UDP can has higher bandwidth compared with the TCP, when the user playing the game they prefer higher bandwidth and can admit a little error rate.

**The End**