**Question 1**

|  |  |
| --- | --- |
|  | 1. Describe the parameters monitored to provide Congestion Control and to provide Flow Control and how are they used? [10 marks]   List up the relevant parameters describing which is for each and how these are used.  Congestion Control:  Congestion control is aimed at preventing network congestion, which occurs when the demand for network resources exceeds its capacity. The key parameters monitored for congestion control include:  Packet Loss:  Monitoring: The number of lost or dropped packets is continuously monitored.  Usage: A sudden increase in packet loss is an indicator of network congestion. Congestion control algorithms react by adjusting the transmission rate to alleviate congestion.  Round-Trip Time (RTT):  Monitoring: The time it takes for a packet to travel from the sender to the receiver and back.  Usage: Increased RTT can indicate congestion. Congestion control algorithms may adjust the transmission rate based on changes in RTT to avoid overloading the network.  Network Buffer Utilization:  Monitoring: The level of occupancy in network buffers.  Usage: High buffer utilization may indicate congestion. Congestion control mechanisms may slow down transmission to prevent buffer overflow and subsequent packet loss.  Explicit Congestion Notification (ECN):  Monitoring: ECN marks in packet headers indicating congestion.  Usage: Routers can set ECN marks to inform endpoints of congestion. Endpoints respond by adjusting their transmission rates.  Throughput:  Monitoring: The rate at which data is successfully transmitted.  Usage: A decrease in throughput may indicate congestion. Algorithms can dynamically adjust transmission rates to optimize network usage.  Flow Control:  Flow control is focused on regulating the flow of data between the sender and the receiver to ensure that the receiver can handle the incoming data. The primary parameters monitored for flow control include:  Window Size:  Monitoring: The maximum number of unacknowledged packets allowed in the network at any given time.  Usage: Adjustments to the window size help regulate the amount of unacknowledged data, preventing the sender from overwhelming the receiver.  Acknowledgment (ACK) Timers:  Monitoring: The time it takes for the sender to receive acknowledgments for sent packets.  Usage: If acknowledgments are not received within a specified time, the sender may retransmit the data to ensure reliable delivery.  Credit-based Flow Control:  Monitoring: The amount of credit or buffer space available at the receiver.  Usage: The sender can only transmit as much data as there is available credit at the receiver, preventing overflow.  Explicit Signaling:  Monitoring: Explicit signals or flags exchanged between sender and receiver.  Usage: The receiver can signal the sender to slow down or speed up based on its ability to process incoming data.   1. Frames of length 1,000 bits are to be transmitted over the following links using the ‘stop and wait’ Flow Control mechanism. The velocity of propagation across these links is 2.5 x 108 m.s-1. For each link determine the link efficiency. 2. A 1,250 km link with a data transmission rate of 10 Gbps. [2 marks] 3. A 12.5m link with a transmission rate of 1 Mbps. [2 marks] 4. Propose a particular application for which the stop and wait flow control mechanism is suitable. Explain what advantages stop and wait has and suggest alternatives where stop and wait is not suitable. [6 marks]   i) Link Efficiency, U = {L/R}/ [RTT+ {L/R}]  L = 1000b, R=10 x109, d=2 x 1.25 x 106m = 2.5 x 106 m  {L/R} = 1x10-7s, RTT={2x1.25x106 /2.5x108} = 1x10-2.  U = {1x10-7}/{1x10-2 + 1x10-7} = ~1x10-5 ~ 0.001%]  ii) L =1000b, d = 25m, R = 1x106bps,  {L/R} = 103 / 106 = 10-3, RTT = 25/25 x107 = 1x10-7  U = 1x10-3/{1x10-3+1x10-7} = ~1 ~100%  iii)  Explain where Stop and Wait is efficient and mention which standard uses it. Describe what resources are needed to provide is compared to ‘go back n’ and ‘selective repeat’ and how and when they are better. Describe how these flow control mechanisms are used on the Internet. |
|  |  |

**Question 2**

|  |  |
| --- | --- |
|  | A key aspect of TCP is provision of a reliable data transfer (RDT) service. A ‘timeout interval’ is used in this provision.   1. Explain what part the ‘timeout interval’ plays in providing RDT. [4 marks]   Explain how timers are required and what part they play in providing RDT.  In the context of Reliable Data Transfer (RDT), the 'timeout interval' plays a crucial role in ensuring the reliable delivery of data across a communication channel, particularly in the presence of potential packet loss or corruption. RDT protocols, such as Stop-and-Wait or Go-Back-N, often use a timeout mechanism to handle situations where transmitted data may not be successfully received by the destination.   1. The round trip time (RTT) is measured and used in the calculation of the timeout interval. Explain what the RTT is, and how it is calculated. [7 marks]   Provide a description of how a useful RTT is calculated and the relationship used in this calculation.  Round Trip Time (RTT):  The Round Trip Time (RTT) is a critical metric in networking that measures the time it takes for a data packet to travel from the sender to the receiver and back again. RTT is often used in various networking protocols, including those that implement reliable data transfer mechanisms.  Calculation of RTT:  The RTT is calculated by measuring the time between sending a packet from the sender and receiving the acknowledgment (ACK) for that packet from the receiver. The RTT represents the total time taken for the packet to make the round trip between the sender and the receiver.  RTT=(Time ACK Received) - (Time Packet Was Sent)  Usefulness of RTT in Timeout Calculation:  The calculated RTT is often used in the determination of the timeout interval in protocols that implement reliable data transfer, such as the Transmission Control Protocol (TCP). The timeout interval is crucial for handling situations where a transmitted packet may be lost or corrupted, and retransmission is necessary.  Timeout Calculation Using RTT:  The calculated RTT is used to set the timeout interval (TO) based on the observed round trip times. The goal is to set a timeout that allows for a reasonable waiting period, taking into account potential network delays and variations in RTT. A common formula used is:  TO=RTT+Safety Margin   1. Explain how the duration of the timeout interval is determined with reference to the RTT and any other parameters (especially with reference to TCP). [9 marks]   Explain use of variation in RTT and the actual calculation of the Timeout interval itself.  1. Round Trip Time (RTT):  Role: RTT represents the time it takes for a packet to travel from the sender to the receiver and back. It is a crucial factor in determining the timeout interval.  2. Estimated Round Trip Time (ERTT):  Calculation:  ERTT=(1−α)×ERTT+α×RTT  Role: ERTT is a smoothed or averaged version of RTT, where α is a smoothing factor. It helps in adapting to variations in RTT and provides a more stable estimate.  3. Deviation Calculation:  Calculation:  Deviation=(1−β)×Deviation+β×∣RTT−ERTT∣  Role: Deviation measures the variation or fluctuation in RTT. It captures the difference between observed RTT and the smoothed ERTT.  4. Timeout Interval Calculation:  TO=ERTT+4×Deviation  Role: The timeout interval (TO) is calculated based on the ERTT and the deviation. The 4 times the deviation factor is an empirical constant that aims to provide a wide enough time window to cover potential fluctuations in the network.  5. Adaptive Timeout:  Role: The use of an adaptive timeout mechanism ensures that the timeout interval is dynamically adjusted based on observed variations in RTT over time.  Adaptation Process:  If RTT consistently increases, the adaptive mechanism may increase the timeout interval to accommodate the changing network conditions. Conversely, if RTT decreases, the timeout may be adjusted downward to avoid unnecessary delays.  6. Retransmission Mechanism:  Role: The calculated timeout interval is used in the retransmission mechanism of TCP. If an acknowledgment is not received within the timeout period, it is assumed that the packet was lost or corrupted, and TCP initiates retransmission. |

**Question 3**

|  |  |
| --- | --- |
|  | The Open Systems Interconnection (OSI) layered architectural model was developed by the International Standards Organisation (ISO) to describe communication systems.   1. What is the purpose of having such a layered model? [4 marks]   • Allow the whole problem to be sub-divided (reduce design complexity).  • Allow alternative options to be substituted in at each layer.  • Generate a bigger market for the solution at each layer.   1. Specify, in the correct order, the layers of the ISO open systems interconnect model, with example functions performed at each layer. [8 marks]   Physical Layer (Layer 1):  Function: Deals with the physical connection between devices and the transmission of raw binary data over a physical medium.  Example Functions:  Encoding/decoding of signals.  Physical topology (e.g., bus, ring, star).  Specification of cables, connectors, and hardware.  Data Link Layer (Layer 2):  Function: Responsible for reliable point-to-point and point-to-multipoint communication over the physical layer. It also handles error detection and correction.  Example Functions:  Framing: Creating and recognizing frame boundaries.  MAC (Media Access Control) addressing.  Error detection and correction (e.g., CRC).  Network Layer (Layer 3):  Function: Manages logical addressing, routing, and forwarding of data packets between devices on different networks.  Example Functions:  Logical addressing (e.g., IP addresses).  Routing: Determining the best path for data to travel.  Packet forwarding between different networks.  Transport Layer (Layer 4):  Function: Provides end-to-end communication and ensures the reliable and error-free transfer of data between devices.  Example Functions:  Segmentation and reassembly of data.  Flow control and error recovery.  Connection establishment, maintenance, and termination.  Session Layer (Layer 5):  Function: Establishes, maintains, and terminates sessions (dialogue) between applications on different devices.  Example Functions:  Session establishment, maintenance, and termination.  Synchronization of data exchange.  Dialog control between applications.  Presentation Layer (Layer 6):  Function: Translates data between the application layer and the lower layers, ensuring that data is in a readable format.  Example Functions:  Data compression and decompression.  Encryption and decryption.  Character set translation.  Application Layer (Layer 7):  Function: Provides network services directly to end-users or applications and supports network-aware applications.  Example Functions:  Network virtual terminal (providing a network interface for applications).  File transfer, email, and remote login protocols.  Network management and application-specific functionalities.   1. Are there disadvantages of using a layered architecture? [3 marks]   Overhead and Inefficiency:  The strict separation of layers may lead to additional overhead and inefficiency. Data may need to pass through multiple layers, each adding its own headers, which can increase processing time and consume additional resources.  Rigid Structure:  Layered architectures can be rigid, making it challenging to adapt to new technologies or changing requirements. Adding a new layer or modifying an existing one might be complex, and the entire architecture may need to be adjusted.  Duplication of Functionality:  Some layers may perform similar functions across different protocols or services. This duplication of functionality can be seen as wasteful, especially if a specific protocol does not require all the features provided by a particular layer.  Complexity:  Layered architectures can become complex, especially when multiple protocols are interacting across layers. Debugging and troubleshooting in such environments might be challenging.  Resource Consumption:  Each layer consumes system resources, and the cumulative effect of multiple layers can lead to increased resource consumption. This is especially important in resource-constrained environments.  Not Always Applicable:  Layered architectures may not be the most suitable choice for certain types of systems. In some cases, a more flexible or specialized architecture might be preferred.  Inter-Layer Dependencies:  Layers often depend on the proper functioning of layers beneath them. If a lower layer fails, it may impact the operation of higher layers. This dependency can make the system more vulnerable to failures.  Communication Overhead:  Communication between layers typically involves passing messages or data, which incurs additional overhead. In high-performance systems, minimizing this communication overhead is critical.  Difficulty in Integration:  Integrating third-party components or technologies into a layered architecture might be challenging, especially if they do not align well with the existing layering structure.   1. In contrast to the OSI model describe the TCP/IP architectural model. [5 marks]     application: supporting network  applications – FTP, SMTP, STTP  • transport: host-host data transfer – TCP, UDP  • network: routing of datagrams from  source to destination  – IP, routing protocols  • link: data transfer between neighboring  network elements – PPP, Ethernet  • physical: bits “on the wire”  Host to Network Layer:  Function: This layer is responsible for the physical connection between the network and the device. It includes the functions of both the Data Link and Physical layers in the OSI model.  Internet Layer:  Function: This layer is responsible for logical addressing, routing, and forwarding of packets between devices on different networks. It is equivalent to the OSI Network Layer.  Transport Layer:  Function: Similar to the OSI Transport Layer, this layer ensures end-to-end communication, reliability, and data flow control.  Application Layer:  Function: This layer provides network services directly to end-users or applications. It combines the functionalities of the OSI Application, Presentation, and Session layers.  • OSI model devised before protocols.  – Model very general not biased to a particular protocol.  – Designation of functionality to layers suspect! E.g. MAC in DLL.  – Convergence sub-layers needed to use existing protocols.  – No provision for internetworking.  – Transport layer offers only connection-oriented services. Network layer offers both  connection-oriented and connectionless services.  • TCP/IP model just a description of what already existed.  – Model doesn’t fit other systems.  – Doesn’t have Presentation, Session, Data link or Physical layers.  – Transport layer offers connectionless and connection- oriented services. Network layer  only offers connectionless services.  Question3.   1. List up the reasons for having layered communications hierarchies. 2. List the OSI layers with appropriate functions performed at each layer. 3. Provide things that can be disadvantageous about layering. 4. Compare OSI to the TCP/IP model by providing the TCP/IP layers with example functions and explanation of the differences. |

|  |  |
| --- | --- |
| **Question 4** | The Internet is in a state of transition as it changes from using IPv4 to using IPv6.   1. What is the binary equivalent of IPv4 address: ‘64.54.34.1’ [1 mark]   01000000 00110110 00100010 0000001 [1]   1. Compress the following IPv6 address (into the more compact form defined for IPv6 addresses): 47CD:0000:0000:0000:0000:0000:A456:0124 [1 mark]   47CD::A456:0124   1. Explain the reasons for this transition, the advantages it provides and how the transition is being implemented. [10 marks]   Explain the main and other reasons for IPv6, and explain the IETF anticipated transition from the IPv4 n/w to a IPv6 dominated n/w.  •Compared to IPv4 a number of fields have been dropped or made optional.  • Main/basic header is 40 bytes. – Version: 6 – Traffic class is similar to ToS of IPv4. 4-bit priority  • IPv6 not only offers more addresses it also provides better QoS support, more efficient service and better flexibility.  Reasons for Transition to IPv6:  IPv4 Address Exhaustion:  Main Reason: The primary driver for the transition is the exhaustion of IPv4 addresses. The 32-bit address space of IPv4 allows for approximately 4.3 billion unique addresses, which is no longer sufficient to accommodate the growing number of devices connected to the Internet.  Addressing Needs of Internet of Things (IoT):  Main Reason: The proliferation of IoT devices has significantly increased the demand for IP addresses. IPv6's larger address space (128-bit) provides an almost limitless number of unique addresses, making it well-suited for accommodating the vast number of IoT devices.  Addressing Challenges in Network Growth:  Main Reason: IPv6 helps overcome the limitations of IPv4, providing a larger address pool to support the continuous expansion of the Internet and the increasing number of connected devices.  Global Address Allocation Efficiency:  Other Reasons: IPv6 promotes more efficient global address allocation and eliminates the need for techniques like Network Address Translation (NAT) that were implemented in IPv4 to address address scarcity issues.  Simplified Network Management:  Other Reasons: IPv6 simplifies network management by eliminating the need for complex NAT configurations. Each device can have a globally unique address, simplifying end-to-end communication.  Improved Security Features:  Other Reasons: IPv6 incorporates enhanced security features, such as IPsec (Internet Protocol Security) support, which is optional in IPv4. This can improve the overall security posture of the Internet.  Advantages of IPv6:  Larger Address Space:  IPv6 provides a vastly larger address space compared to IPv4, ensuring a sufficient number of unique addresses for the growing number of devices.  Simplified Addressing and Routing:  IPv6 has a simplified header structure, which improves routing efficiency and simplifies the packet forwarding process.  Efficient Multicast and Anycast Support:  IPv6 incorporates improved support for multicast and anycast communication, facilitating more efficient data distribution and network services.  Auto-Configuration:  IPv6 includes built-in support for address auto-configuration, allowing devices to automatically configure their IPv6 addresses without the need for DHCP.  Enhanced Security Features:  IPv6 includes IPsec as a standard feature, providing built-in encryption and authentication for improved security.  Streamlined Network Management:  IPv6 simplifies network management by eliminating the need for NAT, making it easier to manage devices and track communication.  Implementation of the IPv6 Transition:  Dual Stack Deployment:  Organizations adopt a dual stack approach, where both IPv4 and IPv6 are deployed concurrently. This allows for a gradual transition, enabling devices to communicate using either protocol.  Tunneling Mechanisms:  Tunneling protocols like 6to4, 6in4, and Teredo are used to encapsulate IPv6 packets within IPv4, facilitating communication over IPv4 networks.  Network Address Translation (NAT) and IPv6-over-IPv4:  NAT64 allows IPv6 devices to communicate with IPv4 devices through translation mechanisms. This is particularly useful during the coexistence period.  IPv6-Enabled Internet Services:  Internet Service Providers (ISPs) and major online services are gradually transitioning to IPv6. This encourages the adoption of IPv6 as more services become available over the new protocol.  IPv6-Ready Hardware and Software:  Vendors are producing IPv6-compatible hardware and software, ensuring that new devices and applications support IPv6. This is crucial for the smooth integration of IPv6 into existing networks.  IETF Transition Guidelines:  The Internet Engineering Task Force (IETF) provides guidelines and standards to facilitate the transition. This includes best practices, transition mechanisms, and protocols that support the coexistence of IPv4 and IPv6.  Global Collaboration:  Organizations and governments globally collaborate to promote IPv6 adoption. Events like World IPv6 Day and World IPv6 Launch serve as initiatives to encourage the deployment of IPv6.   1. Detail the different IP exchanges necessary to allow the transition to take place.   [8 marks]  Explain the different exchanges which are needed to implement the transition with description of how each can be achieved.  Dual Stack Exchange:  Description: In a dual stack environment, both IPv4 and IPv6 protocols are supported simultaneously on network devices. This allows for a gradual transition without immediate dependence on IPv6-only infrastructure.  Implementation: Network devices are configured to run both IPv4 and IPv6 stacks concurrently. This enables communication with both IPv4 and IPv6-enabled systems. Over time, as the adoption of IPv6 increases, the reliance on IPv4 can be phased out.  Tunneling:  Description: Tunneling involves encapsulating IPv6 packets within IPv4 packets to traverse IPv4-only networks. This allows IPv6 communication across IPv4 infrastructure.  Implementation: Various tunneling protocols, such as 6to4, 6in4, and Teredo, can be employed. For instance, 6in4 encapsulates IPv6 packets in IPv4 headers and facilitates communication across IPv4 networks. This method is particularly useful during the coexistence period.  Translation (NAT64/DNS64):  Description: Network Address Translation IPv6 to IPv4 (NAT64) allows IPv6-only devices to communicate with IPv4-only devices. DNS64 assists in the translation of DNS queries and responses between IPv6 and IPv4.  Implementation: NAT64 translates IPv6 addresses to IPv4 addresses, enabling communication with IPv4 devices. DNS64 synthesizes AAAA records for IPv4-only domains, facilitating end-to-end communication. This approach is often used in scenarios where direct IPv6 connectivity is not possible.  Dual Stack Lite (DS-Lite):  Description: DS-Lite combines elements of tunneling and translation. IPv6 packets are tunneled over IPv4, and Network Address Translation (NAT) is used for IPv4 to IPv6 translation.  Implementation: In DS-Lite, the customer premises equipment (CPE) encapsulates IPv6 packets in IPv4, sending them over the IPv4 network to a Carrier-Grade NAT (CGN). The CGN performs the necessary address translation, allowing communication between IPv6 and IPv4 networks.  IPv6-over-IPv4 MPLS Networks:  Description: In Multiprotocol Label Switching (MPLS) networks, MPLS labels are used to route IPv6 traffic over an existing IPv4 infrastructure.  Implementation: MPLS routers in the network are configured to support both IPv4 and IPv6 traffic. MPLS labels are assigned to IPv6 packets, enabling them to traverse the MPLS network alongside IPv4 traffic.  IPv4 and IPv6 Peering:  Description: Internet Service Providers (ISPs) and network operators engage in bilateral agreements to facilitate direct peering between IPv4 and IPv6 networks.  Implementation: ISPs configure their routers to establish BGP (Border Gateway Protocol) sessions for both IPv4 and IPv6 prefixes. This allows efficient exchange of routing information and enables direct communication between networks using either protocol.  IPv6 Transition Mechanisms in Hosts:  Description: Hosts need to be capable of supporting IPv6, and various transition mechanisms, such as automatic tunneling or dual IP layer stacks, can be implemented at the host level.  Implementation: Operating systems and network stacks need to be IPv6-capable. Hosts can use mechanisms like 6to4, Teredo, or native dual stack support. Application developers should ensure that their software is compatible with both IPv4 and IPv6 addressing. |