HÃY PHARAPHARE NẾU MUỐN CÓ ĐIỂM NHÉ( MẤY CÂU LÝ THUYẾT, BÀI TẬP NẾU MUỐN AN TOÀN )

Câu 1: Explain the difference between connectionless unacknowledged service and connectionless acknowledged service. How do the protocols that provide these services differ?

A network communication service known as a "connectionless service" does not create a specific communication path between the sender and the receiver. The sender of a message delivers it through connectionless unacknowledged service, commonly referred to as "fire and forget" without verifying that the recipient has received it. The message may or may not be received by the intended recipient, and the sender is not provided with a confirmation.

By contrast, the sender of a message using a "connectionless acknowledged service" waits for the recipient to confirm receipt before sending another message. If the communication is received, the recipient replies with an acknowledgment to the sender. The sender may conclude that the message was not received if they do not receive an acknowledgment.

Different protocols used to deliver these services handle packet loss and protocol overhead in different ways. The delivery of messages is not guaranteed by "connectionless unacknowledged service" protocols like UDP (User Datagram Protocol), despite their short weight and low overhead. Although they have higher overhead, connectionless acknowledged service protocols like ICMP (Internet Control Message Protocol) and ARP (Address Resolution Protocol), which provide acknowledgments of successful message delivery, offer improved reliability.

Câu 2. Explain the difference between connection-oriented acknowledged service and connectionless acknowledged service. How do the protocols that provide these services differ?

* Connection-oriented acknowledged service:

+ It is a type of network communication that creates a special link between the sender and receiver before any data transmission happens.

+ In this service, the receiver sends an acknowledgment to the sender after receiving each packet of the data.

+ This service requires a stateful protocol, it used to monitor timers and sequence numbers.

* Connectionless acknowledged service:

+ There will be no prior context provided for transferring the information between sender and receiver.

+ The sender simply sends packets to the receiver, and the receiver sends acknowledgements back to the sender for each received packet.

- Different protocols used to deliver these services handle packet loss and protocol overhead in different ways.

Connection-oriented acknowledged service protocols, such as TCP

(Transmission Control Protocol), use a three-way handshake to establish a reliable connection between the sender and receiver. This protocol also uses congestion control and flow control methods to ensure effective data delivery and reduce packet loss.

Connectionless acknowledged service protocols, such as UDP (User Datagram Protocol), do not create a special relationship with the receiver. Instead, they just deliver the packets to the recipient without making any promises about delivery or buying it. These protocols are helpful in situations where speed is more important than accuracy, including online gaming and live broadcasting,

**Câu 3.** Explain the differences between PPP and HDLC.

|  |  |  |
| --- | --- | --- |
|  | PPP | HDLC |
| Full form | Point-to-Point Protocol | High-level Data Link Control |
| Flexibility | PPP is a more flexible protocol than HDLC. It can be used to carry multiple network layer protocols, including IP, IPX, and AppleTalk. | HDLC primarily designed for carrying only one protocol. |
| Error detection | PPP has a better error detection mechanism. PPP uses a cyclic redundancy check (CRC) for detecting errors. The CRC is considered more effective in detecting errors in data transmission. | HDLC uses a frame check sequence (FCS). |
| Configuration | PPP is easier to config. PPP uses a configuration protocol called LCP (Link Control Protocol), which automates the configuration process. | HDLC requires manual configuration of parameters, such as the address field and control field. |
| Authentication | PPP supports authentication mechanisms such as PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol), which authenticate the identity of the sender | HDLC does not support any authentication mechanism. |
| Sliding Window Protocol | PPP does not support any sliding window protocol. | HDLC uses a sliding window protocol for flow control. The sliding window protocol is used to optimize the flow of data between the sender and receiver, ensuring that the receiver is not overwhelmed with too much data at once. |

Câu 4. A 1.5 Mbps communications link is to use HDLC to transmit information to the moon. What is the smallest possible frame size that allows continuous transmission? The distance between Earth and the moon is approximately 375,000 km, and the speed of light is 3 × 10^8 meters/second

To determine the smallest possible frame size that allows continuous transmission, we need to calculate the round-trip time (RTT) to travel from Earth to the Moon and back.

Converting the distance between Earth and the Moon to meters:

375000 km = 3.75\*10^8 m

RTT = = 2.5 s

We have:

Trans time = -> Frame size= Trans time x Trans rate

To calculate the smallest possible frame size, we need to set the delay time so that it is less than 2.5s for optimal calculation. The value is usually taken as half.

So:

Trans time = 2.5/2 = 1.25s.

1.5Mbps = 1.5 \* 10^6 bps.

The smallest possible frame size = 1.25 \* 1.5 \* 10^6 = 1875000 bit.

**Câu 5.** Suppose HDLC is used over a 1.5 Mbps geostationary satellite link. Suppose that 250-byte frames are used in the data link control. What is the maximum rate at which information can be transmitted over the link?

**1 bản khác**

To calculate the maximum rate at which information can be transmitted over the link, we need to consider a few factors:

Link capacity: 1.5 Mbps (1,500,000 bits per second)

Frame size: 250 bytes (2000 bits, as there are 8 bits in a byte)

HDLC overhead: HDLC frames typically have a 6-byte overhead (1 byte for the flag, 2 bytes for the address and control fields, 2 bytes for the Frame Check Sequence, and 1 byte for the closing flag). This amounts to 48 bits of overhead.

First, let's determine the number of useful bits per frame by subtracting the overhead from the total frame size:

Useful bits per frame = Frame size - HDLC overhead

Useful bits per frame = 2000 bits - 48 bits

Useful bits per frame = 1952 bits

Next, we'll calculate the maximum number of frames that can be transmitted per second by dividing the link capacity by the frame size:

Frames per second = Link capacity / Frame size

Frames per second = 1,500,000 bits per second / 2000 bits per frame

Frames per second ≈ 750 frames per second

Now, we can determine the maximum rate at which information can be transmitted over the link by multiplying the number of useful bits per frame by the number of frames per second:

Maximum information rate = Useful bits per frame \* Frames per second

Maximum information rate = 1952 bits per frame \* 750 frames per second

Maximum information rate ≈ 1,464,000 bits per second

Thus, the maximum rate at which information can be transmitted over the link using 250-byte HDLC frames is approximately 1,464,000 bits per second (or about 1.464 Mbps)

**Bản của Kì trước :**

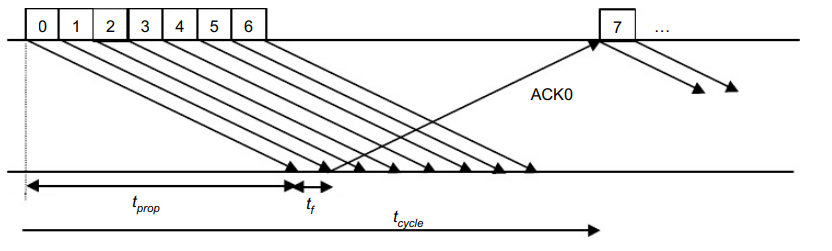
R = 1.5 Mbps or R = 1,5 x 106 bps, and nf =250 bytes or 2000 bits (250 x 8).

The distance that the information must travel is the earth-to-satellite distance, or D ≈ 36,000 km = 3,6 x 107 m.

The speed of light c is 3 x 108. We can calculate the propagation delay and processing rate as follows:

We can use either Go-Back-N or Selective Repeat ARQ. The default window size is N = 7 (with a 3- bit sequence number).





The maximum information rate is achieved with no error, and hence, no retransmission.

= minimum time to transmit a group of N packets

= + 2 = 1.33 + 2 x 120 = 241.33 ms

In which, is the minimum time to transmit a group of N packets.

n = no. of bits transmitted in a cycle = N.= 7 x 2000 = 14000 bits

= no. of bits sent in a cycle / minimum cycle time = n / = 58 kbps

In which, is the number of bits transmitted in a cycle, is number of bits sent in a cycle / minimum cycle time.

If the extended sequence numbering option (7-bit) is used, the maximum send window size would be N = 27– 1 = 127, and hence, the maximum information rate is:

**Câu 6:** Suppose that a multiplexer receives constant-length packet from N = 60 data sources. Each data source has a probability p = 0.1 of having a packet in a given T-second period. Suppose that the multiplexer has one line in which it can transmit eight packets every T seconds. It also has a second line where it directs any packets that cannot be transmitted in the first line in a T-second period. Find the average number of packets that are transmitted on the first line and the average number of packets that are transmitted on the second line.

First, find out the probability of the k packets that have reached the T- second. It can be computed with the help of binomial distribution that has parameters as N = 60 and shows the probability of p = 0.1. The multiplexer has one line in which it can transmit eight packets every T seconds.

The average number for the arrivals of the packets can be given as Np=6. Now, calculate the average number of packets received through the first line as below:

Now, the average number of packets received is 4.59 that gets transmitted through the first line. The remaining will get transmitted by the second line. Now, the average number of packets transmitted through the second line per T second can be obtained as below:

Therefore, it will transmit 1.41 packets on average per T second from the second line.

Câu 7 Consider the transfer of a single real-time telephone voice signal across a packet network. Suppose that each voice sample should not be delayed by more than 20 ms.

a. Discuss which of the following adaptation functions are relevant to meeting the requirements of this transfer: handling of arbitrary message size; reliability and sequencing; pacing and flow control; timing; addressing; and privacy, integrity and authentication.

b. Compare a hop-by-hop approach to an end-to-end approach to meeting the requirements of the voice signal.

a. The following adaptation functions are relevant to meeting the requirements of real-time telephone voice signal transfer across a packet network with a maximum delay of 20 ms:

Handling of arbitrary message size: Voice signals are continuous streams of data, and breaking them into smaller, fixed-size packets is essential for transmission over a packet network. This function ensures efficient transmission and prevents excessive delays.

Reliability and sequencing: While some degree of packet loss can be tolerated in voice communication, maintaining a minimum level of reliability is crucial to ensure voice quality. Sequencing is also essential, as voice packets need to be reassembled in the correct order at the destination to ensure intelligible speech.

Pacing and flow control: Pacing is the process of regulating the rate of data transmission to avoid overwhelming the network or the receiving end. Flow control ensures that the sending and receiving ends maintain a balanced rate of data transfer, preventing buffer overflow and underflow that could cause delays and degrade voice quality.

Timing: Precise timing is crucial for real-time voice communication, as it is necessary to maintain synchronization between the sender and receiver. A maximum delay of 20 ms should be maintained to ensure minimal impact on voice quality and user experience.

Addressing: Proper addressing is necessary for routing voice packets to the correct destination. It ensures that voice packets are delivered to the intended recipient, preventing miscommunication or loss of data.

Privacy, integrity, and authentication: While not directly related to the 20 ms delay requirement, these aspects are crucial for secure voice communication. Privacy ensures that only the intended recipient can access the voice data, integrity ensures that voice data is not tampered with during transmission, and authentication confirms the identities of the communicating parties.

b. Comparing hop-by-hop and end-to-end approaches for meeting the requirements of the voice signal:

Hop-by-hop approach: In this approach, each intermediate node (or hop) in the network is responsible for handling the voice packets, making decisions about routing, flow control, and error handling. This approach can provide better local optimization and quicker recovery from network issues, potentially reducing the impact of network congestion and keeping the delay below 20 ms. However, this approach adds complexity to the network and may require more resources to manage and maintain the intermediate nodes.

End-to-end approach: In the end-to-end approach, the responsibility for ensuring timely and reliable delivery of voice packets lies with the sender and receiver. Intermediate nodes only route packets without making decisions regarding flow control, error handling, or packet sequencing. This approach simplifies the network design and allows for easier scalability. However, it might be less effective in dealing with network congestion, and maintaining the 20 ms delay requirement might be more challenging.

In summary, both approaches have their merits and drawbacks. The choice between hop-by-hop and end-to-end approaches depends on the specific network architecture, requirements, and constraints. The hop-by-hop approach can offer better local optimization and quicker recovery from network issues, while the end-to-end approach simplifies network design and allows for easier scalability.

Câu 7 (câu trl) Consider the transfer of a single real-time telephone voice signal across a packet network. Suppose that each voice sample should not be delayed by more than 20 ms.

a. Discuss which of the following adaptation functions are relevant to meeting the requirements of this transfer: handling of arbitrary message size; reliability and sequencing; pacing and flow control; timing; addressing; and privacy, integrity and authentication.

b. Compare a hop-by-hop approach to an end-to-end approach to meeting the requirements of the voice signal.

a. The following adaptation functions are relevant to meeting the requirements of real-time telephone voice signal transfer across a packet network with a maximum delay of 20 ms:

Handling of arbitrary message size: Voice signals are continuous streams of data, and breaking them into smaller, fixed-size packets is essential for transmission over a packet network. This function ensures efficient transmission and prevents excessive delays.

Reliability and sequencing: While some degree of packet loss can be tolerated in voice communication, maintaining a minimum level of reliability is crucial to ensure voice quality. Sequencing is also essential, as voice packets need to be reassembled in the correct order at the destination to ensure intelligible speech.

Pacing and flow control: Pacing is the process of regulating the rate of data transmission to avoid overwhelming the network or the receiving end. Flow control ensures that the sending and receiving ends maintain a balanced rate of data transfer, preventing buffer overflow and underflow that could cause delays and degrade voice quality.

Timing: Precise timing is crucial for real-time voice communication, as it is necessary to maintain synchronization between the sender and receiver. A maximum delay of 20 ms should be maintained to ensure minimal impact on voice quality and user experience.

Addressing: Proper addressing is necessary for routing voice packets to the correct destination. It ensures that voice packets are delivered to the intended recipient, preventing miscommunication or loss of data.

Privacy, integrity, and authentication: While not directly related to the 20 ms delay requirement, these aspects are crucial for secure voice communication. Privacy ensures that only the intended recipient can access the voice data, integrity ensures that voice data is not tampered with during transmission, and authentication confirms the identities of the communicating parties.

b. Comparing hop-by-hop and end-to-end approaches for meeting the requirements of the voice signal:

Hop-by-hop approach: In this approach, each intermediate node (or hop) in the network is responsible for handling the voice packets, making decisions about routing, flow control, and error handling. This approach can provide better local optimization and quicker recovery from network issues, potentially reducing the impact of network congestion and keeping the delay below 20 ms. However, this approach adds complexity to the network and may require more resources to manage and maintain the intermediate nodes.

End-to-end approach: In the end-to-end approach, the responsibility for ensuring timely and reliable delivery of voice packets lies with the sender and receiver. Intermediate nodes only route packets without making decisions regarding flow control, error handling, or packet sequencing. This approach simplifies the network design and allows for easier scalability. However, it might be less effective in dealing with network congestion, and maintaining the 20 ms delay requirement might be more challenging.

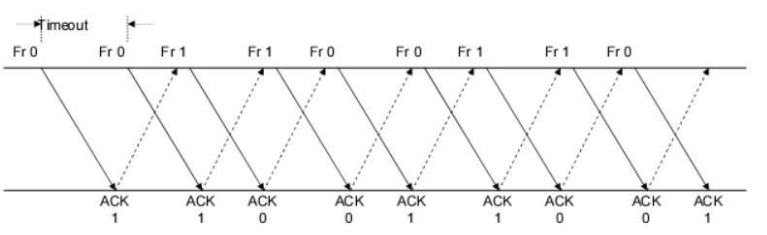
In summary, both approaches have their merits and drawbacks. The choice between hop-by-hop and end-to-end approaches depends on the specific network architecture, requirements, and constraints. The hop-by-hop approach can offer better local optimization and quicker recovery from network issues, while the end-to-end approach simplifies network design and allows for easier scalability.

**Câu 8.** Consider the Stop-and-Wait protocol as described. Suppose that the protocol is modified so that each time a frame is found in error at either the sender or receiver, the last transmitted frame is immediately resent.

a. Show that the protocol still operates correctly.

b. Does the state transition diagram need to be modified to describe the new operation?

c. What is the main effect of introducing the immediate-retransmission feature?



a. The modified Stop-and-Wait protocol still operates correctly because it ensures that every frame is received correctly before the next one is sent. If a frame is found in error, the sender immediately resends the last transmitted frame, which guarantees that the receiver will receive a correct copy of the frame.

b. The state transition diagram would need to be modified to reflect the new operation. Specifically, a new transition would need to be added from the "Frame Received, ACK/NAK Lost" state back to the "Frame Sent" state, indicating that the sender should immediately resend the last transmitted frame in response to the error.

**Bản hợp lí hơn cho câu b nhé:**

The state transition diagram for the original Stop-and-Wait protocol doesn't need to be modified to describe the new operation. The state transition diagram already considers the possibilities of frames being lost or arriving with errors. The only difference in the modified protocol is the immediate retransmission of the frame. However, this does not affect the sender or receiver's states, as they will still transition between "wait for ACK" and "wait for frame" states.

c. The main effect of introducing the immediate-retransmission feature is to improve the protocol's error recovery capabilities. With this feature, errors can be quickly corrected by resending the last transmitted frame. This reduces the time required for error recovery and increases the overall efficiency of the protocol. However, it also introduces additional network traffic, which could potentially increase congestion and delay.

**Câu 9.** Suppose that two peer-to-peer processes provide a service that involves the transfer of discrete messages. Suppose that the peer processes are allowed to exchange PDUs that have a maximum size of M bytes including H bytes of header. Suppose that a PDU is not allowed to carry information from more than one message.

a. Develop an approach that allows the peer processes to exchange messages of arbitrary size.

b. What essential control information needs to be exchanged between the peer processes?

c. Now suppose that the message transfer service provided by the peer processes is shared by several message source-destination pairs. Is additional control information required, and if so, where should it be placed?

a. To allow for the exchange of messages of arbitrary size within the given constraints, the peer processes can use a technique known as segmentation and reassembly. This involves dividing a message into smaller segments, each of which can fit within a single PDU, and then sending these segments over multiple PDUs. The receiver can then reassemble the segments back into the original message.

b. The essential control information that needs to be exchanged between the peer processes includes:

Sequence numbers: These are used to ensure that all segments are received in the correct order and that no segments are missing or duplicated.

Acknowledgment numbers: These are used to confirm that a segment has been successfully received by the receiver.

Window sizes: These are used to allow the sender to adjust the number of unacknowledged segments it can send at any given time based on how much space is available in the receiver's buffer.

c. If the message transfer service is shared by several source-destination pairs, additional control information may be required to differentiate between the different messages being sent. This information could be placed in the header of each PDU and could include the source and destination addresses, session identifiers, or any other information needed to identify the specific message being sent. Additionally, the control information used to manage the flow of PDUs between the sender and receiver may also need to be adjusted to account for multiple concurrent connections. For example, each connection may require its own sequence

and acknowledgment numbers to ensure that segments are properly tracked and acknowledged for each individual message.

**Câu 10.** A 1 Mbyte file is to be transmitted over a 1 Mbps communication line that has a bit error rate of p = .

a. What is the probability that the entire file is transmitted without errors? Note for n large and p very small, (1 − p)n ≈ e - np.

b. The file is broken up into N equal-sized blocks that are transmitted separately. What is the probability that all the blocks arrive correctly without error? Does dividing the file into blocks help?

c. Suppose the propagation delay is negligible, explain how Stop-and-Wait ARQ can help deliver the file in error-free form. On the average how long does it take to deliver the file if the ARQ transmits the entire file each time?

a. The probability that the entire 1 Mbyte file is transmitted without errors can be calculated as follows:

where p is the bit error rate and n is the number of bits in the file.

Since the file size is 1 Mbyte, which is equal to 8 million bits, we can calculate the probability as:

Therefore, the probability that the entire file is transmitted without errors is approximately , which is a very small probability.

b. If the file is broken up into N equal-sized blocks and transmitted separately, the probability that all blocks arrive correctly without error can be calculated as:

where p is the bit error rate, n is the number of bits in each block, and N is the total number of blocks.

Dividing the file into blocks does help because if an error occurs in one block, only that block needs to be retransmitted instead of the entire file.

Assuming each block is equally sized at 1/N Mbytes or 8/N million bits, the probability can be calculated as:

= 0.99992

Therefore, the probability that all blocks arrive correctly without error is approximately 0.999992.

c. Stop-and-Wait ARQ (Automatic Repeat Request) can help deliver the file in error-free form by ensuring that each block is successfully received before transmitting the next block. In this protocol, the sender transmits one block at a time and waits for an acknowledgment from the receiver before transmitting the next block.

Assuming the propagation delay is negligible, the time required to deliver the file using Stop-and-Wait ARQ can be calculated as follows:

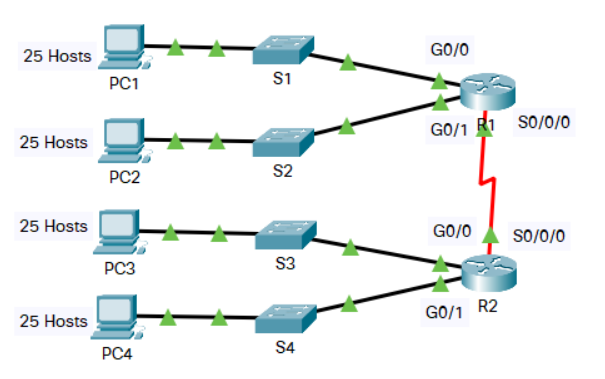
Time required to transmit one block = n/p, where n is the number of bits in each block and p is the bit rate of the communication line.

Since there are N blocks to be transmitted, the total time required to deliver the file would be N times the time required to transmit and receive one block:

Assuming a negligible propagation delay, the total time required to deliver the entire 1 Mbyte file would be:

However, this assumes no errors occur during transmission. If errors occur, additional time will be required for retransmission until all blocks are received correctly.

Câu 11: In this activity, you are given the network address of 192.168.11.0/24 to subnet and provide the IP addressing for the Packet Tracer network. Each LAN in the network requires at least 25 addresses for end devices, the switch and the router. The connection between R1 to R2 will require an IP address for each end of the link.



a. Based on the topology, how many subnets are needed?

b. How many bits must be borrowed to support the number of subnets in the topology table?

c. How many subnets does this create?

d. How many usable hosts does this create per subnet?

a) There are 5 subnets needed. Four for the LANs, and one for the link between the routers.

b) To support 5 subnets, we need to borrow three bits from the host portion of the IP address. This is because 2^3 = 8 > 5 (remember that the formula for calculating the number of subnets is 2^𝑛 , where n is the number of borrowed bits).

NOTE:

Cách trình bày số 2: To support 5 subnets, we need borrow ceil(log2(5)) or 3 bit. Because 2^3 = 8 > 5, it is enough for 5 subnets.

c) Because we borrowed 3 bits, the number of subnet is 2^3 or 8 subnets.

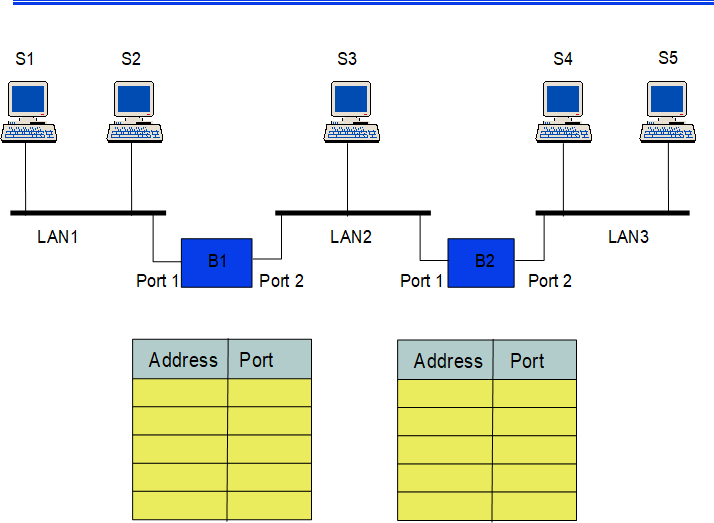
d) Because we have borrowed 3 bits for subnetting, subnet mask now is 27. We can calculate the usable hosts per subnet by hosts :

2^(32- subnet mask) - 2 = 2^5 - 2 = 30

So we have 30 usable hosts per subnet.

**Câu 12:**

Five stations (S1-S5) are connected to an extended LAN through transparent bridges (B1- B2), as shown in the following figure. Initially, the forwarding tables are empty. Suppose the following stations transmit frames: S1 transmits to S5, S3 transmit to S2, S4 transmits to S3, S2 transmits to S1, and S5 transmits to S4. Fill in the forwarding tables with appropriate entries after the frames have been completely transmitted.



Bridge 1

|  |  |
| --- | --- |
| Address | Port |
| S1 | 1 |
| S3 | 2 |
| S4 | 2 |
| S2 | 1 |
| S5 | 2 |

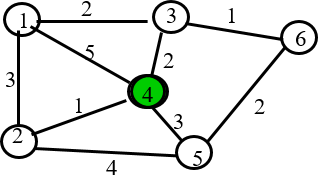
Bridge 2

|  |  |
| --- | --- |
| Address | Port |
| S1 | 2 |
| S3 | 1 |
| S4 | 1 |
| S2 | 1 |
| S5 | 2 |

S1 transmits to S5, S3 transmit to S2, S4 transmits to S3, S2 transmits to S1, and S5 transmits to S4.

**Câu 13:**

* 1. Consider the network in Figure.



1. Use the Dijkstra algorithm to find the set of shortest paths from node 4 to other nodes.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Iteration | N | D1 | D2 | D3 | D5 | D6 |
| Initial | {} |  |  |  |  |  |
| 1 | {} |  |  |  |  |  |
| 2 | {} |  |  |  |  |  |
| 3 | {} |  |  |  |  |  |
| 4 | {} |  |  |  |  |  |

1. Find the set of associated routing table entries (Destination, Next Hop, Cost)

|  |  |  |
| --- | --- | --- |
| Destination | Cost | Next Hop |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

ANSWER:

a, We define N is the node 4, D1, D2, D3, D5, D6 is the node 1,2,3,5,6.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Iteration | N | D1 | D2 | D3 | D5 | D6 |
| Initial | {N} | 5 | **1** | 2 | 3 | ~ |
| 1 | {N, D2} | 4, D2 |  | **2** | 3 | ~ |
| 2 | {N, D2, D3} | 4, D2 |  | - | **3** | **3, D3** |
| 3 | {N, D2, D3, D5, D6} | 4, D2 |  |  |  |  |
| 4 | {N, D2, D3, D5, D6, D1} | - | - | - | - | - |

So that, we can conclude that

+ The shortest part from N to D1 is 4, and pass D2.

+ The shortest part from N to D2 is 1.

+ The shortest part from N to D3 is 2.

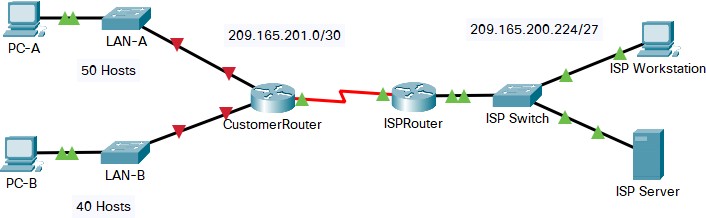
+ The shortest part from N to D5 is 3.

+ The shortest part from N to D6 is 3, and pass D3.

b,

|  |  |  |
| --- | --- | --- |
| Destination | Cost | Next Hop |
| D1 | 4 | D2 |
| D2 | 1 | D2 |
| D3 | 2 | D3 |
| D5 | 3 | D5 |
| D6 | 3 | D3 |

14)



You are a network technician assigned to install a new network for a customer. You must create multiple subnets out of the 192.168.0.0/24 network address space to meet the following requirements:

* The first subnet is the LAN-A network. You need a minimum of 50 host IP addresses.
* The second subnet is the LAN-B network. You need a minimum of 40 host IP addresses.
* You also need at least two additional unused subnets for future network expansion.

**Note**: Variable length subnet masks will not be used. All of the device subnet masks should be the same length.

Answer the following questions to help create a subnetting scheme that meets the stated network requirements:

* 1. How many host addresses are needed in the largest required subnet?
  2. What is the minimum number of subnets required?
  3. The network that you are tasked to subnet is 192.168.0.0/24. What is the /24 subnet mask in binary?
  4. The subnet mask is made up of two portions, the network portion, and the host portion. This is represented in the binary by the ones and the zeros in the subnet mask.

In the network mask, what do the ones and zeros represent?

* 1. When you have determined which subnet mask meets all of the stated network requirements, derive each of the subnets. List the subnets from first to last in the table. Remember that the first subnet is 192.168.0.0 with the chosen subnet mask.

a. The largest required subnet is LAN-A, which needs a minimum of 50 host IP addresses.

b. We need a minimum of 4 subnets - 2 for the required LANs and 2 additional unused subnets for future network expansion.

c. The /24 subnet mask in binary is 11111111 11111111 11111111 00000000.

d. In the subnet mask, the ones represent the network portion, and the zeros represent the host portion. The network portion identifies the network address, while the host portion identifies individual hosts within the network.

e. To meet the stated network requirements, we can use the following subnetting scheme:

Use a /26 subnet mask (255.255.255.192) for LAN-A to provide 62 host addresses per subnet.

Use a /26 subnet mask (255.255.255.192) for LAN-B to provide 62 host addresses per subnet.

Use a /27 subnet mask (255.255.255.224) for the first unused subnet to provide 30 host addresses per subnet.

Use a /27 subnet mask (255.255.255.224) for the second unused subnet to provide 30 host addresses per subnet.

The resulting subnets are:

Subnet 1: 192.168.0.0/26 (LAN-A)

Subnet 2: 192.168.0.64/26 (LAN-B)

Subnet 3: 192.168.0.128/27 (Unused)

Subnet 4: 192.168.0.160/27 (Unused)

Note that the first subnet is 192.168.0.0 with the chosen subnet mask, and the last usable address in each subnet is used as the broadcast address.

|  |  |  |
| --- | --- | --- |
| **Subnet Address** | **Prefix** | **Subnet Mask** |
| **192.168.12.0** | **/26** | **255.255.255.192** |
| **192.168.12.64** | **/26** | **255.255.255.192** |
| **192.168.12.128** | **/26** | **255.255.255.192** |
| **192.168.12.192** | **/26** | **255.255.255.192** |

**Câu 15:**

Suppose that Selective Repeat ARQ is modified so that ACK messages contain a list of the next m frames that it expects to receive.

1. How does the protocol need to be modified to accommodate this change?
2. What is the effect of the change on protocol performance?

a. To modify Selective Repeat ARQ so that ACK messages contain a list of the next m frames that it expects to receive, the protocol needs to be modified as follows:

The sender maintains a sliding window that includes all unacknowledged frames, as in the standard Selective Repeat ARQ protocol.

When the receiver receives a frame, it checks to see if it is the next expected frame in the sequence. If it is, the receiver sends an ACK message that contains a list of the next m frames that it expects to receive.

If there are gaps in the received frames, the receiver sends an ACK message that requests retransmission of the missing frames. The sender then retransmits the requested frames.

b. The effect of this change on protocol performance depends on the value of m and the characteristics of the network.

One potential benefit of this modification is improved efficiency, particularly in networks with high latency or high error rates. By including a list of expected frames in each ACK message, the receiver can help reduce the number of unnecessary retransmissions. For example, if the sender knows that the receiver is expecting frames 10-20, it can prioritize those frames for transmission instead of sending other frames that may not be needed.

However, there are also potential drawbacks to this modification. One concern is increased overhead due to the larger size of the ACK messages. Depending on the value of m, the size of each ACK message could be significantly larger than in the standard protocol, which could impact network performance. Additionally, the more frames that are included in each ACK message, the greater the risk of errors in the ACK message itself, which could lead to further retransmissions and delays.

# Q.16. (2 marks)

Suppose the size of an uncompressed text file is 1megabyte

***Note: Explain your answer in detail.***

1. How long does it take to download the file over a 32 kilobit/second modem?
2. How long does it take to take to download the file over a 1 megabit/second modem?
3. Suppose data compression is applied to the text file. How much do the transmission times in parts (a) and (b) change?

a) To download a 1-megabyte file over a 32 kilobit/second modem, we need to convert the file size from bytes to bits and then divide by the bit rate:

1 megabyte = 2^23 bits

32 kilobits = 32000 bits

Download time =

Download time = 262 seconds

Therefore, it would take approximately 262 seconds or 4 minutes and 22 seconds to download the file over a 32 kilobit/second modem.

b) To download a 1-megabyte file over a 32 kilobit/second modem, we need to convert the file size from bytes to bits and then divide by the bit rate:

1 megabyte = 2^23 bits

1 megabits = 10^6 bits

Download time =

Download time 8.4 seconds

Therefore, it would take approximately 8.4 seconds to download the file over a 32 kilobit/second modem.

c)

Suppose data compression is applied to the text file. The actual compression ratio depends on the compression algorithm and the content of the file. Let's denote the compression ratio as 'CR', where CR is the percentage of the original file size after compression (e.g CR = 50% means the file size is reduced to half its original size).

In this case, the size of the compressed file would be (CR \* original file size). The download times for the two modems would be:

32 kilobit/second modem: Download time = (CR \* 8,388,608 bits) / 32,000 bits/second

1 megabit/second modem: Download time = (CR \* 8,388,608 bits) / 1,000,000 bits/second

These results are illustrative and can vary depending on the actual compression algorithm and data content.

.

# Q17. (2 marks)

Let . Consider the information sequence 1001. Find the codeword corresponding to the preceding information sequence. Using polynomial arithmetic we obtain

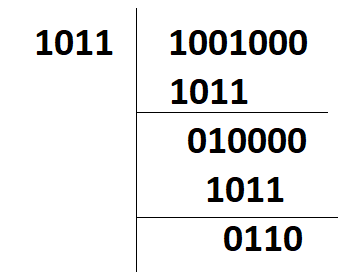
Given an information polynomial code is

Now we rewrite the polynomial code as  as 1011

Since the polynomial is of order  (3 is the highest power of g(x))

So, we add three zeros in the information sequence.

Therefore, the new polynomial code is



1011 | 1001000

| 1011

|-----------------

| 010000

| 1011

|------------------

| 0110

Then, we add 110 to the information sequence 1001 to get the codeword: 1001110.

Câu 18

A router has the following CIDR entries in its routing table:

Address/mask Next hop

135.46.56.0/22 Interface 0

135.46.60.0/22 Interface 1

192.53.40.0/23 Router 1

default Router 2

(a) What does the router do if a packet with an IP address 135.46.63.10 arrives?

(b) What does the router do if a packet with an IP address 135.46.57.14 arrives?

For a packet with IP address 135.46.63.10:

a)

We need to find the entry in the routing table that matches the destination IP address. To do this, we will apply the subnet mask of each entry and see if the result matches the network address.

For the 135.46.56.0/22 entry, the subnet mask is 255.255.252.0. If we apply this mask to the destination IP address (135.46.63.10) and the network address (135.46.56.0), we get:

135.46.63.10 & 255.255.252.0 = 135.46.60.0

135.46.56.0 & 255.255.252.0 = 135.46.56.0

These are not the same, so we move to the next entry.

For the 135.46.60.0/22 entry, the subnet mask is also 255.255.252.0. If we apply this mask to the destination IP address (135.46.63.10) and the network address (135.46.60.0), we get:

135.46.63.10 & 255.255.252.0 = 135.46.60.0

135.46.60.0 & 255.255.252.0 = 135.46.60.0

These are the same, so the router will forward the packet to Interface 1.

(b) For a packet with IP address 135.46.57.14:

Following the same process as before, we will check the destination IP address against each entry in the routing table.

For the 135.46.56.0/22 entry, applying the subnet mask (255.255.252.0) to the destination IP address (135.46.57.14) and the network address (135.46.56.0), we get:

135.46.57.14 & 255.255.252.0 = 135.46.56.0

135.46.56.0 & 255.255.252.0 = 135.46.56.0

These are the same, so the router will forward the packet to Interface 0

Câu 19: ( Note Hỏi thầy thứ tự A B C D )

A Large number of the consecutive IP address are available starting at 198.16.0.0. Suppose four organizations, A, B, C, and D request 4000, 2000, 4000, and 8000 addresses, respectively. For each of these organizations, give:

1. the first IP address assigned
2. the last IP address assigned
3. the mask in the w.x.y.z/s notation

The start address, the ending address, and the mask are as follows:

To allocate the requested number of IP addresses to each organization, we need to calculate the number of bits required to represent the maximum number of hosts for each organization. We can then use these bit counts to create subnet masks that provide enough addresses for each organization.

The number of bits required to represent x hosts is ceil(log2(x)), where ceil() is the ceiling function that rounds up to the nearest integer. Applying this formula to each of the four organizations, we get:

Organization A: 4000 hosts → ceil(log2(4000)) = 12 bits

Organization B: 2000 hosts → ceil(log2(2000)) = 11 bits

Organization C: 4000 hosts → ceil(log2(4000)) = 12 bits

Organization D: 8000 hosts → ceil(log2(8000)) = 13 bits

To allocate these address blocks, we can use the following approach:

Allocate an address block to Organization D, which requires the most addresses. We need a block with at least 8000 addresses, which requires a mask with at least 13 host bits. The closest subnet mask that provides enough addresses is /19, which has a mask of 255.255.224.0. This creates a block starting at 198.16.0.0 and ending at 198.16.31.255. The first IP address assigned to Organization D is 198.16.0.0, and the last IP address assigned is 198.16.31.255.

Allocate an address block to Organization A, which requires 4000 addresses. We need a block with at least 12 host bits, but since we've already allocated a /19 block, we have only 9 bits left for the next block. The closest subnet mask that provides enough addresses is /21, which has a mask of 255.255.248.0. This creates a block starting at 198.16.32.0 and ending at 198.16.39.255. The first IP address assigned to Organization A is 198.16.32.0, and the last IP address assigned is 198.16.39.255.

Allocate an address block to Organization C, which requires 4000 addresses. We can use the same /21 subnet mask that we used for Organization A since we still have enough addresses left in that block. This creates a block starting at 198.16.40.0 and ending at 198.16.47.255. The first IP address assigned to Organization C is 198.16.40.0, and the last IP address assigned is 198.16.47.255.

Allocate an address block to Organization B, which requires 2000 addresses. We need a block with at least 11 host bits, but we only have 3 bits left after allocating the previous two blocks. The closest subnet mask that provides enough addresses is /23, which has a mask of 255.255.254.0. This creates a block starting at 198.16.48.0 and ending at 198.16.49.255. The first IP address assigned to Organization B is 198.16.48.0, and the last IP address assigned is 198.16.49.255.

Therefore, the answer to the question is:

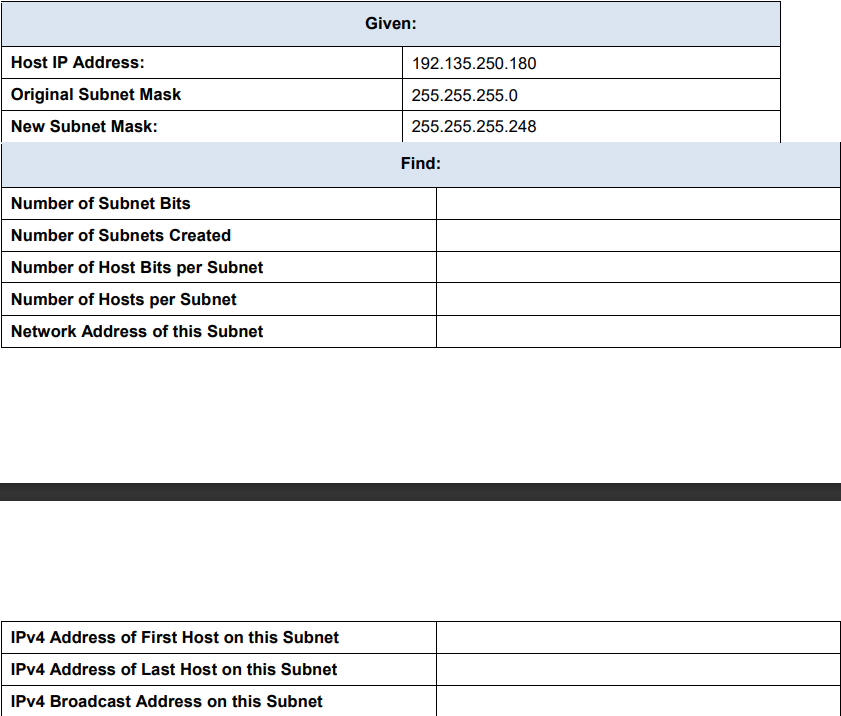
Organization A: First IP address = 198.16.32.0, Last IP address = 198.16.39.255, Mask = 255.255.248.0 of /21

Organization B: First IP address = 198.16.48.0, Last IP address = 198.16.49.255, Mask = 255.255.254.0 of /23

Organization C: First IP address = 198.16.40.0, Last IP address = 198.16.47.255, Mask = 255.255.248.0 of /21

Organization D: First IP address = 198.16.0.0, Last IP address = 198.16.31.255, Mask = 255.255.224.0 of /19

Câu 20: The ability to work with IPv4 subnets and determine network and host information based on a given IP address and subnet mask is critical to understanding how IPv4 networks operate. The first part is designed to reinforce how to compute network IP address information from a given IP address and subnet mask. When given an IP address and subnet mask, you will be able to determine other information about the subnet. Fill out the tables below with appropriate answers given the IPv4 address, original subnet mask, and new subnet mask



|  |  |
| --- | --- |
| Number of Subnet Bits | 5 |
| Number of Subnet Created | 2 ^5 = 32 |
| Number of Host Bits per Subnet | 3 |
| Number of Hosts per Subnet | 2^3 -2 = 6 |
| Network Address of this Subnet |  |
| Ipv4 Address of First Host on this Subnet |  |
| Ipv4 Address of Last Host on this Subnet |  |
| Ipv4 Broadcast Address on this Subnet |  |

Network Address of this Subnet = Host IP Address AND the new subnet mask

192.135.250.180 & 255.255.255.248 = 192.135.250.176

So 192.135.250.176 is the Network Address of this Subnet

Ipv4 Address of First Host on this Subnet: 192.135.250.177

IPv4 Address of Last Host on this Subnet: 192.135.250.182

IPv4 Broadcast Address on this Subnet: 192.135.250.183

Given:

Host IP Address: 192.135.250.180

Original Subnet Mask: 255.255.255.0

New Subnet Mask: 255.255.255.248

We'll first determine the number of subnet bits, the number of subnets created, the number of host bits per subnet, the number of hosts per subnet, and the network address of this subnet. Here's how we do it:

A number of Subnet Bits:

Original Subnet Mask: 255.255.255.0 (CIDR /24)

New Subnet Mask: 255.255.255.248 (CIDR /29)

Number of Subnet Bits = New CIDR notation - Original CIDR notation = 29 - 24 = 5 subnet bits

Number of Subnets Created:

Number of Subnets = 2 ^ (Number of Subnet Bits) = 2 ^ 5 = 32 subnets

Number of Host Bits per Subnet:

Host Bits per Subnet = 32 - New CIDR notation = 32 - 29 = 3 host bits

Number of Hosts per Subnet:

Number of Hosts = 2 ^ (Host Bits per Subnet) - 2 = 2 ^ 3 - 2 = 6 hosts

Network Address of this Subnet:

Host IP Address: 192.135.250.180

New Subnet Mask: 255.255.255.248

To find the network address, perform a bitwise AND operation between the IP address and the new subnet mask:

192.135.250.180 = 11000000.10000111.11111010.10110100

AND

255.255.255.248 = 11111111.11111111.11111111.11111000

11000000.10000111.11111010.10110000 = 192.135.250.176

So, the network address of this subnet is 192.135.250.176.

In summary:

Number of Subnet Bits: 5

Number of Subnets Created: 32

Number of Host Bits per Subnet: 3

Number of Hosts per Subnet: 6

Network Address of this Subnet: 192.135.250.176

To find the IPv4 address of the first host, last host, and the broadcast address on this subnet, we'll use the network address and the number of hosts per subnet we calculated earlier.

Network Address: 192.135.250.176

Number of Hosts per Subnet: 6

IPv4 Address of First Host on this Subnet: Add 1 to the network address: 192.135.250.176 + 1 = 192.135.250.177

IPv4 Address of Last Host on this Subnet: Since there are 6 hosts per subnet, add 6 - 1 to the first host address: 192.135.250.177 + (6 - 1) = 192.135.250.182

IPv4 Broadcast Address on this Subnet: Add 1 to the last host address: 192.135.250.182 + 1 = 192.135.250.183

In summary:

IPv4 Address of First Host on this Subnet: 192.135.250.177

IPv4 Address of Last Host on this Subnet: 192.135.250.182

IPv4 Broadcast Address on this Subnet: 192.135.250.183

**Đề câu 5 đã thi ở SP23 có đổi số liệu nhé**

Given:

Host IP Address: 192.168.200.139

Original Subnet Mask: 255.255.255.0

New Subnet Mask: 255.255.255.224

We'll first determine the number of subnet bits, the number of subnets created, the number of host bits per subnet, the number of hosts per subnet and the network address of this subnet. Here's how we do it:

A number of Subnet Bits:

Original Subnet Mask: 255.255.255.0 (CIDR /24)

New Subnet Mask: 255.255.255.224 (CIDR /27)

Number of Subnet Bits = New CIDR notation - Original CIDR notation = 27 - 24 = 3 subnet bits

Number of Subnets Created:

Number of Subnets = 2 ^ (Number of Subnet Bits) = 2 ^ 3 = 8 subnets

Number of Host Bits per Subnet:

Host Bits per Subnet = 32 - New CIDR notation = 32 - 27 = 5 host bits

Number of Hosts per Subnet:

Number of Hosts = 2 ^ (Host Bits per Subnet) - 2 = 2 ^ 5 - 2 = 30 hosts

Network Address of this Subnet:

Host IP Address: 192.168.200.139

New Subnet Mask: 255.255.255.224

To find the network address, perform a bitwise AND operation between the IP address and the new subnet mask:

192.168.200.139 = 11000000.10101000.11001000.10001011

AND

255.255.255.224 = 11111111.11111111.11111111.11100000

11000000.10101000.11001000.10000000 = 192.168.200.128

So, the network address of this subnet is 192.168.200.128

To find the IPv4 address of the first host, last host, and the broadcast address on this subnet, we'll use the network address and the number of hosts per subnet we calculated earlier.

Network Address: 192.168.200.128

Number of Hosts per Subnet: 30

IPv4 Address of First Host on this Subnet: Add 1 to the network address: 192.168.200.128 + 1 = 192.168.200.129

IPv4 Address of Last Host on this Subnet: Since there are 30 hosts per subnet, add 30 - 1 to the first host address:

192.168.200.128+ (30 - 1) = 192.168.200.157

IPv4 Broadcast Address on this Subnet: Add 1 to the last host address: 192.168.200.157+ 1 = 192.168.200.158

In summary:

IPv4 Address of First Host on this Subnet: 192.168.200.129

IPv4 Address of Last Host on this Subnet: 192.168.200.157

IPv4 Broadcast Address on this Subnet: 192.168.200.158

In summary,

|  |  |
| --- | --- |
| Number of Subnet Bits | 3 |
| Number of Subnet Created | 8 |
| Number of Host Bits per Subnet | 5 |
| Number of Hosts per Subnet | 30 |
| Network Address of this Subnet | 192.168.200.128 |
| Ipv4 Address of First Host on this Subnet | 192.168.200.129 |

**Câu Bổ sung.** A 1.5 Mbps communications link is to use HDLC to transmit information to the moon. What is the smallest possible frame size that allows continuous transmission? The distance between the earth and the Moon is approximately 375,000 km, and the speed of light is meters/second.

For continuous transmission: Use Go-Back-N or Selective Repeat ARQ

|  |  |  |
| --- | --- | --- |
|  | Maximum Send Window Size in Default HDLC Frame | Maximum Send Window Size in Extended HDLC Frame |
| Go-Back-N | 7 |  |
| Selective ARQ | 4 |  |

The round-trip propagation delay is

Call is the smallest possible frame size so that we got

Go-Back-N

If N = 7:

If N = 127:

Selective Repeat

If N = 4:

If N=64: