COMPUTER NETWORK

ECAP256

ABHEY S 5/15/23 LPU

Computer Network Viva Questions

1. Define a network.

A network is a collection of networks joined together by physical media linkages. Recursively, a network is any physical link connecting two or more nodes or any two or more networks connected by one or more nodes.

---

2. How do links work?

Two or more computers connected directly to one another via a physical media, such as ***a coaxial cable or optical fibre,*** can perform work at the lowest level. A *link* is an example of a physical medium.

---

3. Describe a Node.

A ***network*** can be made up of two or more computers that are physically linked together, such as by ***coaxial cable or optical fibre***. Such ***physical media*** is known as a ***link***, and the computer that connects to it is referred to as a ***node***.

---

4. What is a router or gateway?

A node linked to two or more networks is referred to as a ***gateway or router***. In most cases, it transmits the message from one network to another.

---

5. Describe the point-to-point link.

We refer to physical connections as point-to-point links if they can only connect two nodes.

---

6. What is multiple access, exactly?

If two or more nodes share the physical links, it is referred to as multiple accesses.

---

7. What benefits do distributed processing systems offer?

Distributed processing systems offer various benefits, including distributed databases, collaborative processing, encapsulation or security, quicker problem solution, and security through redundancy.

---

8. What are the names of the variables that impact the performance of the network?

Hardware, software, users, and various transmission mediums are all factors.

---

9. What standards must a network meet to be effective and efficient?

Reliability:

The amount of time it takes a link to recover from a failure, how often failures occur, and how robust the network is are all indicators of how reliable a system is.

Security:

Security concerns include guarding data from viruses and illegal access.

Performance:

A network's performance can be evaluated in a number of ways, including through metrics like reaction time and transmit time.

---

10. Talk about the elements that affect the network's dependability.

There are mainly two elements that affect the network's dependability:

- Frequency of failures;
- Network recovery time after a failure.

---

11. What are the factors that affect the security of the network?

There are several factors that affect network security, including viruses, unauthorized access, and many more.

---

12. What is the protocol?

A ***protocol*** is a collection of guidelines that governs all facets of information communication.

---

13. What is the essential component of protocol?

Key components of the protocol are:

Semantics:

It speaks of the significance of each bit in a segment.

The format and structure of the data, or the manner in which they are presented, make up a protocol's syntax.

Timing:

It has the following two qualities:

- When should the information we send
- How quickly can data be sent?

---

14 Discuss the key design issues of a computer network.

There are various key design issues of a computer network, including:

- Support for common services
- Cost-effective resource sharing
- Performance
- Connectivity

---

15. What are latency and bandwidth?

Latency and bandwidth are used to gauge the network's performance. The number of beads that may be transmitted through the network in a specific amount of time is referred to as the ***network's bandwidth***. In contrast, ***latency*** describes the length of time it takes a message to transit over a network in terms of bits.

---

16. Talk about routing.

The act of methodically forwarding a message to a destination node depending on its address is known as ***routing*** in a network.

---

17. What is a peer-to-peer process?

Each process that communicates between machines at a specific network layer is known as a ***peer-to-peer process***.

---

18. What is the congested switch?

A switch may receive packets quicker than a card link that can hold them and store them in memory for a longer amount of time. If this occurs, the switch may eventually run out of buffer space, forcing some packets from it to be lost in a particular state. The situation of the network is referred to as the ***"congested condition of the network"***.

---

19. Address the network's semantic gap.

Understanding the requirement applications and being aware of the technological constraints might help to define a useful channel. Therefore, the gap between application characteristics and the underlying technology can be described as the semantic gap in the network.

---

20. How long is the round trip?

The ***Round-trip time*** is the amount of time it takes to send a message from one end of a network to the other and vice versa.

---

21. Talk about broadcasting, unicasting, and multicasting.

Multicasting is a method by which the message is sent to some subset of other nodes.

Unicasting is a method by which the message is sent from a source to a single destination node.

Finally, ***broadcasting*** is a method by which the message is sent to all the nodes in the network.

---

22. Talk about multiplexing.

Multiplexing is the process through which numerous signals are sent simultaneously over a single data channel.

---

23. Go over the different types of multiplexing.

There are several types of multiplexing, including:

A. Time division multiplexing

- Synchronous TDM
- Asynchronous TDM or statistical TDM

B. Frequency division multiplexing

C. Wave division multiplexing

---

24. Talk about FDM.

FDM is an analogue method that can be used when a link's bandwidth is greater than the total bandwidth of the signals to be transferred.

---

25. How does WDM work?

This method is comparable to ***FDM***. Additionally, multiplexing and demultiplexing include the transmission of light signals across fibre optic channels.

---

26. What is TDM?

TDM involves digital technology, and it can be used when the transmission medium's data rate capacity exceeds the data rate needed by the transmitting and receiving devices.

---

27. Discuss Synchronous TDM.

The multiplexer always assigns each device the exact same time slot in the synchronous time division multiplexing technique. The device might or might not have anything to communicate.

---

28. What are the OSI layers?

There are several layers in the OSI Model, including,

1. Physical layer
2. Datalink layer
3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer

---

29. Which is the network-supported layer?

Network-supported layers are,

1. Network layer
2. Physical layer
3. Datalink layer

---

30. Which is the user-supported layer?

User-supported layers are,

1. Application layer

2. Presentation layer
3. Session layer

---

31. Which layer in the OSI stack connects the user-supported and network-supported layers?

The user-supported layer and the network-supported layer are connected via the transport layer.

---

32. Talk about the issues with the physical layer.

The physical layer coordinates the operations necessary for the transmission of a bit stream across a physical medium.

1. Representation of bits
2. physical characteristics of interfaces and media
3. data rate
4. bits synchronization
5. a line configuration
6. transmission mode
7. physical topology

---

33. Discuss the responsibilities of the data link layer.

The data link layer transmits information to the physical layer. The data link layer is in charge of node-to-node distribution and conveys a raw facility to a dependable link.

- physical addressing
- flow control
- framing
- error control
- access control

---

34. Explain the functions of the network layer.

Several functions of the network layer are,

1. The network layer is responsible for routing and logical addressing.
2. The network layer is in charge of delivering packets from source to destination, maybe through several networks.

---

35. Explain the functions of the transport layer.

The transport layer is in charge of sending the full message from source to destination. Some other functions of the transport layer are,

1. Connection control
2. error control
3. segmentation and reassembly
4. service point addressing
5. flow control

---

36. Explain the function of the session layer.

The network dialogue controller is treated as a session layer. It upholds, establishes, and synchronizes communication between systems.

- Synchronization
- Dialogue management

---

37. Explain the responsibilities of the presentation layer role.

The presentation layer is in charge of sharing information on the syntax and semantics between two systems. Other functions include ***translation, encryption, and compression***.

---

38. Describe the responsibility of the application layer.

The application layer decides whether software or humans will access the network. The application layer provides user interfaces and supports, like shared database management, e-mail, and other types of distributed Information Services.

---

39. What are the two categories of hardware components?

There are two categories of hardware components, i.e., **Nodes and Links**.

---

40. What different kinds of links can be employed to construct a computer network?

- leased lines
- Cables
- last mile links
- wireless links

---

41. Discuss the various categories of transmission media.

There are various categories of transmission media, including:

I) guided media

A) twisted pair cable

1. shielded TP
2. Unshielded TP

B) coaxial cable

C) fiber optics cable

II) unguided media

1. terrestrial microwave
2. Satellite communication

---

42. What kinds of errors are there?

There are mainly two types of error, including:

- **Single bit error:** In this error, only one bit in the data unit is altered.
- **Burst error:** two or more data bits will be altered in this error.

---

43. What is computer network error detection, and what are its methods?

During transmission, there may be the possibility of corruption of data. For reliable communication, errors must be deducted and corrected. The concept of redundancy is used by error detection in a computer network, which means adding extra bits to detect errors at the destination. There are some common error detection methods which are as follows

- **Longitudinal redundancy check**
- **Vertical redundancy check**
- **Cyclic redundancy check**
- **Checksum**

---

44. Describe redundancy.

Redundancy is a method by which we might transmit more information merely for comparison purposes.

---

45. What is a vertical redundancy check?

It is one of the simplest and most prevalent procedures used in mistake detection techniques. In vertical redundancy check, a parity bit is added to every data unit so that the total number of 1s becomes even for

even parity. It has a single-bit error detection capability and can only detect burst faults if there are an odd number of overall errors in each data unit.

---

46. How do you perform a longitudinal redundancy check?

In the ***longitudinal redundancy check***, bits are broken up into blocks called rows, and a redundant row of bits is added to the original block. It is capable of detecting burst mistakes. Let's say two bits in a data unit are broken, and bits in the exact same locations in another data unit are likewise broken. In that situation, the longitudinal redundancy checker won't pick up on a mistake. The data unit comes after n data units in the logical redundancy check.

---

47. What does cyclic redundancy check mean?

It is one of the most powerful redundancy-checking methods. The cyclic redundancy check is based on binary division.

---

48. What is the checksum?

The ***checksum approach*** is used by higher layer protocols to assist with error detection.

---

49. Describe the steps involved in creating the checksum.

- The data is divided into sections
- Using 1's complement arithmetic, these sections are added together
- Finally, the complement is taken for the final sum. It is the checksum.

---

50. Describe the data link protocols.

Data link protocols refer to the set of specifications required to implement the data link layer. The following are some categories of data link protocols:

A. Asynchronous protocol

B. Synchronous protocol

1. **Character-oriented protocol**
2. **Bit oriented protocol**

---

51. What is the difference between error correction and error detection?

Error detection is easy and simple than error correction, and it is examined for error detection when any error occurs. Additionally, only the corrupted bits are verified during error correction. The number of mistakes and the size of the messages is key components in key correction.

---

52. Define forward error correction.

Forward error detection is the method through which the receiver makes an attempt to understand the message using redundant bits.

---

53. What is retransmission?

Retransmission is the process by which a message is requested to be sent again after an error has been found by the recipient. The message is sent again and again until it is received and the recipient accepts it as an ***error-free transmission***.

---

54. Define data words.

The messages are separated into blocks when using block coding. A ***data word*** is referred to as each of the ***K beats. Block coding*** is a ***one-to-one method***, and the same data word is consistently encoded using the same code word.

---

55. What are code words?

Each block is given an additional ***"r"*** redundant bit to make the length ***n = k + r***. These resultant n-bit blocks are known as ***codewords***. The codewords ***2n*** and ***2k*** are rarely used, and these terms have no legitimate use.

---

56. Define linear block code.

A ***linear block code*** is one in which another valid code word is created by the ***exclusive OR*** of two valid code words.

---

57. What is cyclic code?

It is a particular variety of additional ***linear block code***. A ***code word*** will yield another code word if it is ***rotated or sorted*** in cyclic code.

---

58. What is an encoder?

It is a program or device that applies specified algorithms to video or audio data to compress or encode it for usage in storage or transmission. Analog video to digital video conversion is accomplished with this circuit.

---

59. What is a decoder?

The encoded data is translated into its original format by a program or device. This expression is frequently used to describe ***MPEG-2 sound*** and video data, which needs to be encoded before output.

---

60. What is framing?

Framing is the process by which the data connection layer divides a message into its additional centre address and destination address while it is being sent from one source to another or from one destination to another. The sender address enables the recipient to acknowledge receipt of the packet, and the destination address specifies where the packet must go.

---

61. What is fixed-size framing?

In ***fixed-size framing***, the frame borders are not specified. A delimiter could be the size itself.

---

62. What is character stuffing?

The ***character stuffing*** or ***bite stuffing*** approach involves adding a special kind of byte to the frame's data section along with a character or pattern that matches the flag. The data area is filled with the aid of an additional byte. This bite is frequently referred to as the escape character, which has a predetermined bit pattern. When the receiver comes across the escape character, it is deleted from the data section and it sees the following character as data rather than a delimiting indicator.

---

63. What is bit stuffing?

It is a process in which one extra ***0*** is added when five consecutive ***1*** s follow a ***0*** in the data, get there will be no mistake when the receiver makes a pattern ***0111110*** for a flag.

---

64. How does flow control work?

Flow control refers to a collection of methods that is used to limit how much data a sender can send before having to wait for an acknowledgment.

---

65. Define error control.

Error control is the combination of ***error detection and correction***. It allows the receiver to inform the sender of any frames lost or damaged and transmission, and it coordinates the transmission of those frames by the sender. In the data link layer, error detection is referred to as ***"error control and retransmission methods"***.

---

66. Define automatic repeat request.

Error control is the combination of error detection and correction. The data link layer frequently implements error control. When an exchange error is discovered, the required programmes are sent again. An ***automatic repeat request (ARQ)*** is the name given to the entire process.

---

67. Define stop-and-wait protocol.

In the ***stop-and-wait protocol***, the sender sends the first frame and waits for the receiver to affirm, ***"OK, go ahead"***, before sending the next frame.

---

68. What is an automatic stop-and-wait repeat request?

By keeping the copy of the sent frame, the ***error correction*** is done in a ***stop-and-wait automatic repeat request***, and when the timer expires, the transmission of the frame is done.

---

69. What is the use of sequence number in reliable transmission?

This protocol stipulates that each frame must have a unique number. This method is done with the help of sequence numbers. The data frame is given a pill to carry the frame's sequence number. We wish to reduce its frame size, so the smallest range offers clear communication. The numbers in the series can circle.

---

70. Discuss pipelining.

Pipelining is a ***networking technique*** or other application where a task frequently starts before the previous activity has finished.

---

71. What is a sliding window?

The range of sequence numbers is described by an ***abstract idea***. Also, it is a concern of the sender and receiver. On the other hand, the receiver and the sender should deal with it if they only have access to a portion of the possible sequence number.

---

72. Discuss piggybacking.

Piggybacking is the term for the method that is used to increase the effectiveness of more extensive external treatments. A frame can control information about lost frames from ***Q*** when it conveys data from ***P to Q***, and it can control information about the arrived frame from ***P*** when it carries data from ***Q to P***.

---

73. What are the types of transmission technology available?

There are two types of transmission technology, including:

1. Point to point
2. Broadcast

---

74. Define subnet.

The ***subnet*** is a generic term that is used for the section of a large network, usually separated by a bridge or a router.

---

75. What are the differences between transmission and communication?

Communication defines the full exchange of information between two communication media.

---

76. Describe the possible ways of data exchange.

There are several ways of data exchange, including:

1. Simplex
2. Half duplex
3. Full duplex

---

77. Define SAP.

It is a series of interface points that allows other computers to communicate with other network protocol stack layers.

---

78. Define triple X in the computer network.

A document called ***X.3*** describes the function of a packet ***assembler disassembler***. The standard protocol has been defined between the ***PAD*** and terminal called ***X.28***, and another standard protocol exists between the network and PAD known as ***X.29***. These three combined are recommended as triple X.

---

79. Define frame relay and in which layer it comes under.

It is a packet-switching technology that will operate in the data link layer.

---

80. Define terminal emulation and in which layer it comes under.

Terminal emulation is called telnet, and it comes under the application layer.

81. Define beaconing.

Beaconing is a process in which it permeates a network to self-repair the problems in that network. The network on the station alerts the other stations in the ring when these are not receiving the transmission. In addition, it is utilised in ***token rings*** and ***FDDI networks***.

---

82. Define redirector.

It is software that converts files into network requests, prints I/O requests, or intercepts files. It belongs to the presentation layer.

---

83. Define the terms NETBEUI and NETBIOS.

NETBEUI:

It is the netbios programming interface's extended user interface. Companies like ***Microsoft and IBM*** created this transport protocol for the use of tiny subnets.

NETBIOS:

It is a programming interface that enables I/O requests to be sent and received from remote computers while concealing the networking hardware from applications.

---

84. What is RAID?

Multiple hard discs are used in this strategy to provide fault tolerance.

---

85. Define the term passive topology.

When the computers on the network listen and receive the signal, the signals we call are passive. It is because they increase the signal's volume. The best illustration of passive topology is the linear bus.

---

86. What is cladding?

It is a layer of glass that encircles the central fibre of glass in a fibre optic cable.

---

87. Define point-to-point protocol.

It is a communication protocol. It is used to connect computers to remote networking services, including Internet service providers.

---

88. How is the gateway different from routers?

At the upper levels of the OSI model, a gateway always operates, and it translates information between two completely different data formats or network architectures.

---

89. What is a Mac address?

For a device, the address is defined at the ***media access control (Mac)*** layer in the network architecture. ***Mac address*** is unique. It's usually stored in ROM on the network.

---

90. What is the difference between bit rate and baud rate?

The number of bits transmitted during one second is called as ***Bit rate***. At the same time, the number of signal units per second required to represent those bits is called the ***baud rate***.

Baud rate = bit rate/ N

Where N is the number of bits represented by its signals shift.

---

91. Discuss the types of transmission media.

Usually, signals are transmitted over some transmission media. These transmission media are basically classified into two categories;

A. Guided media:

In guided media, it conducts conduction between one device to another, including twisted pair, fiber optic cable, and a coaxial cable. The signal which travels along any of these media is directed and is contained by the physical limits of the medium. Coaxial cable and twisted pair use metallic that accepts and transports signals in the form of electrical current. In the form of light, the optical fiber, which is a Plastic or a glass cable, transports under accepted signals?

B. Unguided media:

It is a wireless media. It transports electromagnetic waves without the help of a physical conductor. These are done through satellite communication, radio communication, and cellular telephony.

---

92. Define project 802.

It is a project that is started by ***IEEE***. It has started to set standards to enable intercommunication between equipment from various manufacturers. To allow the interconnectivity of major LAN protocols, it is preferred to specify functions after the physical layer, the data link layer, and the person's extent to the network layer.

It consists of the following:

A. For compatibility of different mans and lans across protocols, 802.1 is an internal networking standard.

B. 802.3 is the ***logical link control (LLC),*** the upper sublayer of the datalink layer, which is non-architecture specific. It remains the same for all ***IEEE-defined lans***.

C. The lower sublayer of the data link layer, which is media access control, contains some distinct modules, each carrying proprietary information specific to the LAN product being used. These modules are Ethernet LAN, i.e., ***802.3, a token ring LAN, i.e., 802.4, and a token bus LAN, i.e., 802.5***.

D. ***802.6*** is a ***distributed dual queue bus (DQDB)*** designed to use in mans.

---

93. Define protocol data unit.

The ***protocol data unit (PDU)*** is the data unit at the ***LLC level***. Four fields are contained by the protocol data units: a source service access point (SSAP), a destination service access point (DSAP), a control field, and an information field. Source service access point and destination service access point add the addresses which are used by LLC for identification of the protocol stacks and the receiving and sending machines that generate and use the data. Whether the PDU frame is an information frame or a supervisory frame, or an unnumbered frame is specified by the control field.

---

94. Discuss the different types of networking or networking devices.

There are various types of networking or networking device, including:

A. Repeater:

The ***Repeater*** is also called a ***regenerator***. It is an electronic device that operates only at the physical layer. Before it becomes weak, it receives the signal in the network, regenerates the signal bit pattern, and puts the refreshed copy back into the link.

B. Bridges:

Bridges operate in both the data link layer and physical layer of lans of the same type. A large network is divided by the bridges into smaller segments. Bridges contain logic that allows them to keep the traffic for each segment separate, and for that, the repeaters relay frame inside the segment containing the intended recipient and control congestion.

C. Routers:

Among multiple interconnected networks, the packets are relayed by the routers. Routers operate in data link, physical, and network layers. Router's content software enables them to the determination of several possible paths, i.e., which path is best for a particular transmission.

D. Gateway:

A gateway is a networked device that acts as an entry point into another network when discussing networking (network devices gateway). For example, a wireless router is typically utilized as the default gateway in a home network. In a nutshell, a gateway serves as a messenger agent, receiving data from one network, interpreting it, and transmitting it to another. Gateways may function at any layer of the OSI model and are also known as protocol converters.

---

95. Define ICMP.

ICMP stands for ***"Internet control message protocol"***. It is a network layer protocol of the ***TCP/IP protocol*** that is used by hosts and gateways for sending notifications of datagram problems back to the sender. ICMP uses an echo test or reply to test whether a destination is reachable and responding. ICMP handles both control and error messages.

---

96. Describe the data units at different TCP/ IP protocol suite layers.

The message is the data unit that is created at the application layer. A segment or a user datagram is the data unit that is created at the transport layer. At the network layer, the datagram unit is created. At the data link layer, the datagram is encapsulated and finally transmitted as signals along the transmission media.

---

97. Describe the difference between ARP and RARP?

Basically, the ***address resolution protocol*** (ARP) is used for the association of the 32-bit IP address with the 48-bit physical address. By sending an ARP query packet, it is used by a host or a router to find the physical address of another host on its network, which includes The IP address of the receiver.

On the other hand, The ***reverse address resolution protocol (RARP)*** permits a host to discover its Internet address when it knows only its physical address.

---

98. What is the minimum and maximum length of the header in the TCP segmentand the IP datagram?

There should be a minimum length of the header of up to ***20 bytes***, and the length can have a maximum of ***60 bytes***.

---

99. What is the range of addresses in the class of Internet address?

Class A - 0.0.0.0 - 127.255.255.255

Class B - 128.0.0.0 - 191.255.255.255

Class C - 192.0.0.0 - 223.255.255.255

Class D - 224.0.0.0 - 239.255.255.255

Class E - 240.0.0.0 - 247.255.255.255

---

100. What are the differences between FTP and TFTF application layer protocols?

The file transfer protocol is one of the standard mechanisms provided by TCP IP for the purpose of a copy of a file from one host to another. It is very secure and reliable. It uses the services offered by TCP. Two connections are established between the host, which is one for ***data transfer*** and another for ***control information***.

The ***trivial file transfer protocol (TFTP)*** lodges a local host open files from a remote host. But here, the host does not provide reliability or security. Fundamental packet delivery services are used by TFTP, which is offered by UDP.

---

101. Describe the major types of networks and explain them.

There are several types of networks, including:

1. Peer-to-peer network:

In this type of network, the computers can act as the client using the resources, and servers share the resources.

2. Server-based network:

In this network, it provides centralized control of network resources which rely on server computers for providing security and network administration.

---

102. Describe the important topologies for networks.

There are several topologies for networks, including:

1. Star topology:

In the star topology network, all computers had connected using a central hub. It can be inexpensive. It is very easy to install, and then we can easily reconfigure it, and it is very easy to detect physical problems.

2. Bus topology:

In this topology network, each computer is directly connected to a primary network cable with the help of a single line. It is also inexpensive, and it is very easy to install. We can understand it simply, and they can extend easily.

3. Ring topology:

In this topology, all the computers are connected in a loop. In this, the computers have equal access to network media. In this system, the installation process is simple. As much as in other topologies, the signal does not degrade because each computer regenerates it.

---

103. What is a mesh network?

In the mesh network, there are multiple network links available. This network links the computers to provide multiple paths to travel for the data.

---

104. Describe the differences between broadband and basebandtransmission.

According to broadband transmission on multiple frequencies, the signals are sent by allowing multiple signals simultaneously.

On the other hand, a single cable consumes the entire bandwidth of the cable in baseband transmission.

---

105. What is the 5-4-3 rule?

In the ***Ethernet network***, there cannot be more than five network segments between any two points on the network. In the same way, there cannot be four repeaters, well. Only three of segments upper pipe segments can be populated.

---

106. What is MAU?

The hub is called the ***multistation access unit (MAU)*** in the token ring.

---

107. Describe the difference between non-routable and routable protocols.

A routing protocol is a network protocol that transports data from one network to another via a router and is delivered to a system on that remote network. On the other hand, the data from a non-routable protocol cannot be routed through a router. It is primarily due to the protocol's lack of capacity.

---

108. What is the importance of the OSI reference model?

OSI reference model provides a framework for discussing network design and operations.

---

109. Describe the logical link control.

The ***logical link control (LLC)*** is the highest sublayer of the data link layer in the open system interconnections (OSI) data transmission reference model. It serves as an interface between the network layer and the data link layer's media access control (MAC) sublayer.

---

110. Define the virtual channel.

It is a connection from one source to one destination. However, multicast connections are also permitted. The circuit is another name for a virtual channel.

---

111. Define the virtual path.

A group of virtual circuits can be grouped together along any transmission path from a given source to the destination. This destination path is called a ***virtual path***.

---

112. Define packet filtering.

Packet filtering is a firewall technique that is utilized for controlling network access by monitoring outgoing and incoming packets and enabling them to pass or fail based on the source and destination IP addresses, protocols, and ports.

---

113. Define multicasting routing.

Multicast routing is a networking technique for distributing one-to-many traffic efficiently. A multicast source transmits traffic to a multicast group in a single stream like a live video conference. Receivers in the multicast group include computers, gadgets, and IP phones.

---

114. Define silly window syndrome.

Silly Window Syndrome is a problem caused by bad TCP implementation. It reduces TCP throughput and renders data delivery wasteful.

---

115. Describes trigrams and diagrams.

A trigram is the combination of three letters, for example, the ing and ion. On the other hand, a diagram is the combination of two letters, e.g., the, in, re, er, and an.