Understanding networks by Mike Myers(LinkedIn Learning)

What is a model?

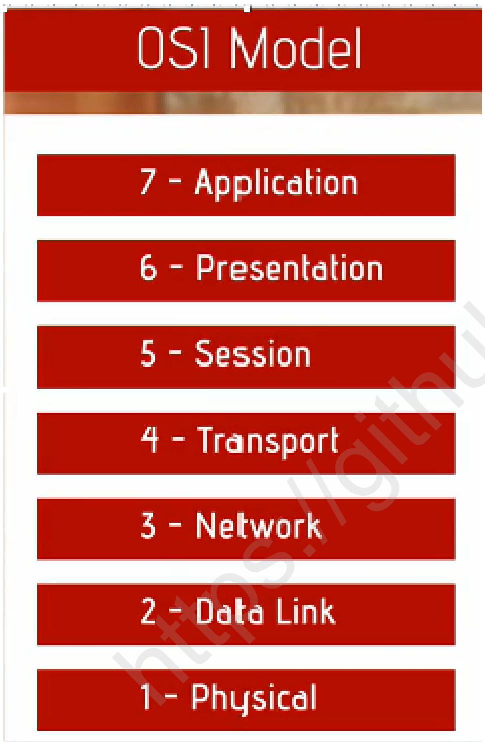
- A model is a way to organize a system’s functions and features to define its structural design.
- Models are used to represent how networks function.

Which are the two popular networking models?

- **OSI seven-layer** Model and **TCP /IP** Model

OSI model Vs TCP/IP model

Explain OSI model



1.Physical Layer

- The Physical Layer deals with the actual physical transmission medium that carries the digital signals between devices.
- This can include copper wires, fiber-optic cables etc.

2.Data Link Layer

- Manages the reliable and error-free transmission of data frames between directly connected network devices like switches, using hardware addresses, i.e. MAC addresses.

3.Network Layer

- It utilizes the logical addresses(e.g., IP addresses) and is responsible for routing data packets between devices in different networks. Routers, operating at this layer, determine the best path for data packets to reach their destination across interconnected networks, ensuring efficient and reliable communication.

4.Transport Layer

- It is responsible for the assembly of data for transmission, the disassembly of received data, and maintaining good order in data delivery.

5.Session Layer

- Is primarily responsible for managing communication sessions between devices for
- e.g. when you access a website using your web browser, a session is established at the Session Layer to manage the interaction between the browser and the web server or when you share files or folders between computers on a network, the Session Layer is involved in managing the file transfer session.

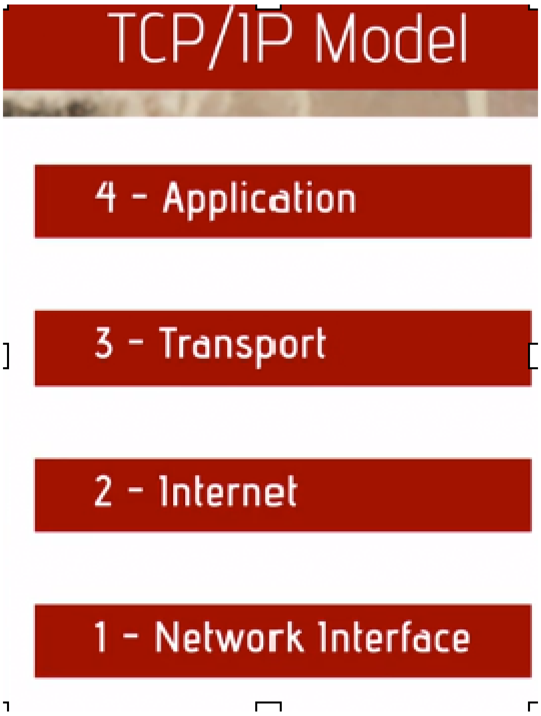
6.Presentation Layer

- Presentation Layer in the OSI model historically played a critical role in data format conversion and translation but Microsoft suite has made it easier for users to work with data across different platforms and applications.

7.Application Layer

- Application Programming Interfaces(APIs) in the Application Layer, serve as a bridge between applications and the network, making applications network-aware and allowing them to interact with various network services and protocols.

Explain TCP/IP model



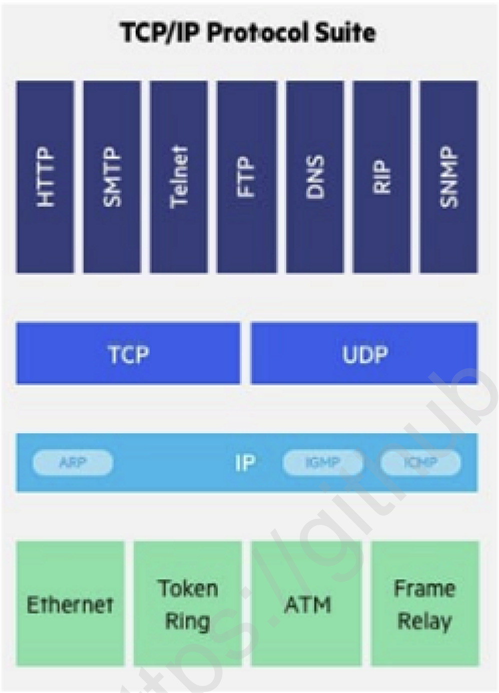
TCP/IP Model

4 - Application

3 - Transport

2 - Internet

1 - Network Interface



1.Network Interface Layer

- Also called the Link or Network Access layer. This layer combines the OSI model's L1 and L2(Physical and Data Link Layer).

2.Internet Layer

- This layer is similar to the OSI model's L3(Network Layer)

3.Transport Layer

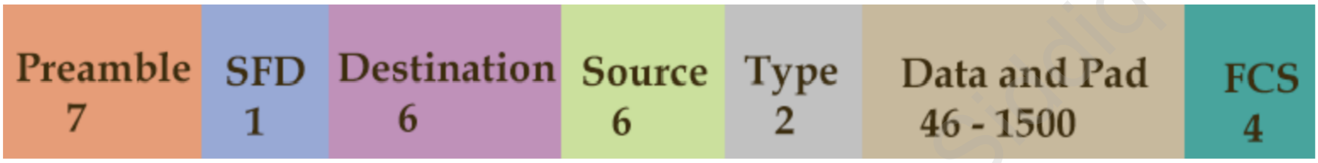
- Also called the Host-to-Host layer. This layer is similar to the OSI model's L4(Transport Layer).

4.Application Layer

- Also called the Process layer, this layer combines the OSI model's L5, L6, and L7(Session, Presentation and Application Layers).

What is an ethernet frame?

- An Ethernet frame is a piece of data along with the information that is required to transport and deliver that piece of data. In networking reference models, such as; OSI Seven Layers model and TCP/IP, the Ethernet frame is defined in the Data link layer.
- An Ethernet frame contains three parts; an Ethernet header (Preamble, SFD, Destination, Source, and Type), Encapsulated data (Data and Pad), and an Ethernet trailer (FCS).



Preamble	SFD	Destination	Source	Type	Data and Pad	FCS
7	1	6	6	2	46 - 1500	4

Walking through OSI and TCP/IP

Explain how an Ethernet frame is handled in the OSI model and TCP/IP model at both the sending and receiving ends.

Sending End: Consider a client system sends out a http request to open up a web page.
Physical Layer:

- Consider this to be the network card which waits for the data to be received as a frame.
- The job of the network card with the ethernet frame is to first take a look at the MAC addresses and verify if it belongs to the card.
  Data link Layer
- After successful verification , the card strips off the Frame Check Sequence (extra bits added to the frame for error detection) along with the MAC addresses.
- It saves the MAC addresses in the memory so it can send it back where it came from at a later stage. At this point the job of the network card is over and we are left with an IP packet.
- In case of the TCP/IP the above two steps are carried out by the Network Interface Layer or Link Layer.
  Network Layer(Internet layer for TCP/IP)
- The IP packet is now in the Network Layer in OSI model
- It verifies its own IP address , gets rid of it and retains the IP address that it came from.
- We are now left with the TCP segment and is passed to the Transport Layer
  Transport Layer(Same Layer for both OSI & TCP/IP)
- Acts as the assembler /disassembler of the data
- The job of the transport layer is to divide the data into bite size chunks when its going out and reassemble when its coming in.

- It does this with the help of the sequencing number.
- It retains the sequencing number and passes on the data (which is complete at this point) along with the port numbers up to the Session Layer
  Session/Presentation/Application(Application for TCP/IP):
- The session layer is designed to connect a server to a client on a remote system.
- The presentation layer was designed long ago where the data would be formatted to be presented to the applications which is redundant now.
- In the application layer it stores the port number that the data frame needs to be returned and passes the data frame to the applications.
  So here, we took the incoming data frame and turned it into data that can be used by the applications.

Receiving End (OSI Model): Here, we are going to start with some data and send out an ethernet frame and explain how a web server brings back all the information.
Session/Presentation/Application(Application for TCP/IP):
Application layer

- The data frame needs to be sent to the right destination and the port numbers now become source : Port 80 and destination : Port 1423.
  Transport Layer
- At the transport layer, a TCP segment is formed (When data is sent over a network, it is often divided into smaller, manageable pieces called segments). Each TCP segment consists of two main parts.
  a. Header: This portion of the segment contains control information, including source and destination port numbers, sequence numbers.
  b. Payload: The payload contains the actual data being transmitted. It can be a portion of a larger message, file, or application data.
- This TCP segment is passed on to the next lower layer i.e the Network Layer.
  Network Layer
- At this point the IP addresses are included in the packet headers. They serve as unique identifiers for devices on a network and are essential for routing data to its intended destination.
  Data Link Layer:
- At the Data Link Layer, each device on a local network is identified by a unique MAC address, also known as a hardware address or physical address. The sender's MAC address (source MAC) and the receiver's MAC address (destination MAC) are added to the header of the data frame. These MAC addresses are used for local network communication, helping network devices identify the source and destination of the data frame within the same network segment.
- The FCS is a field added to the Data Link Layer header that contains a checksum or cyclic redundancy check (CRC) value. The purpose of the FCS is to detect errors in the data frame during transmission.
  Physical Layer:

- The ethernet frame is now transmitted over the physical network medium. Upon receipt, the frame is verified for errors, and if it passes, the payload is delivered to the appropriate higher-layer protocol for further processing.

Meet the frame

What is a NIC?

- It stands for a Network Interface Card and is also known as a network adapter or network card, is a hardware component that allows a computer or other networked device to connect to a network and communicate with other devices over that network and share resources(web page, document etc.).

What are frames?

- Devices on a network send and receive data in discreet chunks called frames(packets)
- They are a maximum of 1500 bytes in size
- Frames are created and destroyed inside the NIC.

Explain frame handling in NIC.

- Data arrives in the form of Word documents, etc. The NIC creates the frame and sends it out through the network. Similarly, at the other end, frames are received by the NIC, and the data is then extracted, sent to the applications, and cleared from the NIC.

The MAC address

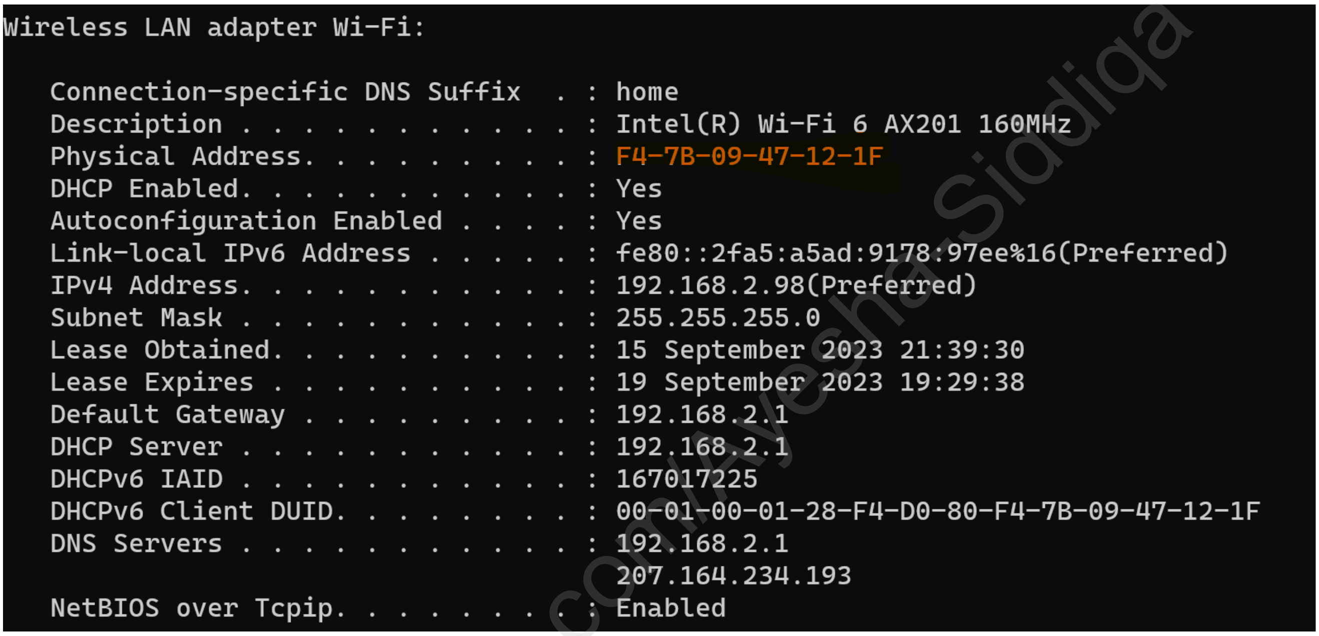
What is a MAC address?

- A MAC address is a unique 48 bit identifier for a NIC.
- Frames have a destination and a source MAC address.
- NICs use MAC addresses to decide whether or not to process a frame.

Explain how frames know how to move to the right computer?

- Consider a network that has a NIC connected to a hub(device that has multiple ports to connect other computers on the same network for resource sharing) through a cable. Now, when data is sent out from this NIC , it reaches the hub (also called as a repeater because it takes the incoming signal ,makes multiple copies and sends out on all other connected cables).
- The frame payload does not identify the destination hence a MAC address (Media Access Control address) is used to uniquely identify the network card.
- MAC address is a 48-bit (6-byte) hexadecimal number comprising of 12 numbers broken up into 6 pairs. Each hexadecimal character represents 4 binary characters(hence 48 bits).

- The first 3 numbers pairs are called the OEM numbers(Original Equipment Manufacturer) and the last 3 pairs called the Unique ID are burnt into the card at the factory and each card gets a different value.
- Hence ,it is the MAC address that are applied to the frame to make sure it is delivered to the right device.
- The frame is also included with a Cyclic Redundancy Check which is used to verify that the data is good.
- The frame is sent to all the computers connected to the hub, but only the NIC with the correct MAC address proceeds to strip off the extra bits and transfer the data to the applications.



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : F4-7B-09-47-12-1F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2fa5:a5ad:9178:97ee%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.98(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 15 September 2023 21:39:30
   Lease Expires . . . . . . . . . . : 19 September 2023 19:29:38
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . : 167017225
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-F4-D0-80-F4-7B-09-47-12-1F
   DNS Servers . . . . . . . . . . . : 192.168.2.1
                                       207.164.234.193
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

***Broadcast Vs Unicast

Communication is a process of sharing or exchanging information. There are three types of communication: one to one, one to many, and one to all. In computer networking, these types are known as unicast, multicast, and broadcast, respectively.

What is Unicast Transmission?

- It is addressed to a single device on a network

What is Broadcast Transmission?

- A broadcast transmission is sent to every device in a broadcast domain

What is a broadcast domain?

- Where all devices within the domain can receive broadcast messages sent by any other device within that same domain.

What does the broadcast address look like?

- FF-FF-FF-FF-FF-FF

FYI: A **broadcast address** belongs to all devices in the IP subnet. Any message sent to this address reaches all devices on the subnet. A broadcast is a destination-only address. It is never used in the source address field of data packets.

Introduction to IP addressing

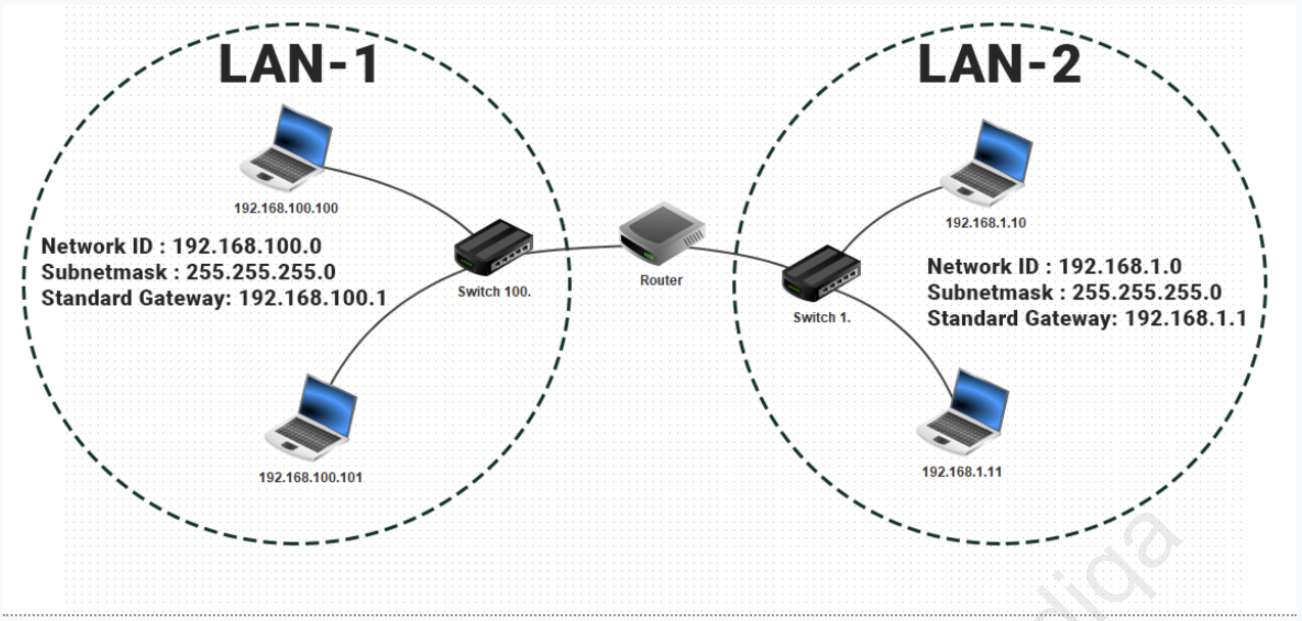
What are some limitations of MAC addresses and how does Logical addressing overcome these?

- In large networks, managing MAC address tables can become challenging, and the number of devices in a single broadcast domain may be limited due to broadcast traffic concerns.
- They do not provide routing information to allow communication between devices on different networks without additional networking infrastructure, such as routers.
- While MAC addresses provide unique identifiers for NICs within the same network segment, they do not inherently indicate that devices are part of a single network. Logical addressing helps overcome all these challenges by helping identify devices within specific networks or subnets. There are several versions but the predominant version is the IP addressing

What are IP addresses?

- An IP address is a unique identification number. Each device on an IP network needs an IP address. Devices use IP addresses to identify each other. They can have multiple IP addresses. An IP address is 32 bits in length
- An IPv4 address looks like this 31.14.17.231 or IPv6- 2001:0D8B8:FE01::

Explain how a frame travels from a computer on one end of a network to a computer on another network.


LAN-1
192.168.100.100
Network ID : 192.168.100.0
Subnetmask : 255.255.255.0
Standard Gateway: 192.168.100.1
Switch 100.
192.168.100.101
Router
LAN-2
192.168.1.10
Network ID : 192.168.1.0
Subnetmask : 255.255.255.0
Standard Gateway: 192.168.1.1
Switch 1.
192.168.1.11

Connecting two Networks with Router

- Consider two networks connected by a single router. We would want to send a frame from a computer on LAN1 to another on LAN2.
- The computer on the LAN1 has the frame that consists of the MAC addresses + CRC +payload.
- Next, the IP addresses(of the source and destination) are included to the frame. The IP addresses(source & destination) and the data together form the IP packet
- To send the IP packet, the computer on the sending end reads the IP address and understands that it does not belong to its network.
- The computer that has the IP packet puts a frame around it that consists of the destination MAC address of the default gateway in this case a router and the source MAC address (which is its own MAC address)
- The frame now travels through the network , into the switch and to the router.
- The router strips off the frame leaving behind just the IP packet.
- Every router has a routing table that knows where to send data based on the network information.
- Th router includes the MAC address of the receiving computer plus its own as the source MAC address, adds the CRC and sends out the frame.

What is a router?

- A router is a gateway that passes data between one or more local area networks (LANs) hence connecting multiple local area network

What is an IP packet?

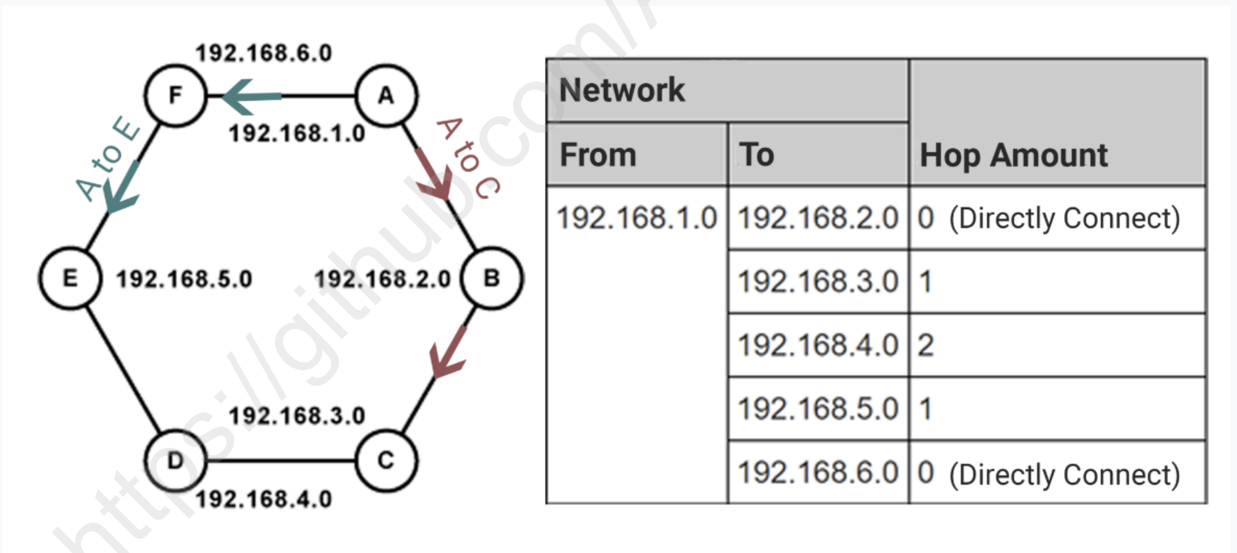
- It is a packet within the frame that includes the IP addresses(source & destination) and the data.
- The IP packet within the frame never changes.

What is a default gateway and is router same as default gateway?

- Default gateway refers to the specific network device that serves as the default route for data traffic leaving a local network or subnet. It is the entry and exit point for traffic between the local network and external networks, such as the internet.
- While the default gateway is a specific concept related to how devices within a local network reach external networks, a router is a broader networking device that handles routing functions between different networks. In many home and small business networks, the default gateway is a router, but in larger and more complex networks, routers may serve various routing roles beyond being the default gateway.

What are routing tables?

- A routing table is a critical data structure used in networking to store information about the available routes to reach various destination networks or hosts.
- It contains
  - All known network addresses
  - Connection types to other networks
  - Route information to other routers
- It is maintained by routers and networking devices to make intelligent decisions about how to forward data packets.



Network		Hop Amount
From	To	
192.168.1.0	192.168.2.0	0 (Directly Connect)
	192.168.3.0	1
	192.168.4.0	2
	192.168.5.0	1
	192.168.6.0	0 (Directly Connect)

Routing Table - Work Principle

Packets & Ports

Explain Port Number

- Port numbers help direct packet traffic between source and destination
- A port number primarily aids in the transmission of data between a network and an application. Port numbers work in collaboration with networking protocols to achieve this. For example, in an incoming message/packet, the IP address is used to identify the destination computer/node, whereas the port number further specifies the destination

application/program in that computer. Similarly, all outgoing network packets contain application port numbers in the packet header to enable the receiver to distinguish the specific application.
- The range is 0-65535

Extra Info:

Well-Known Ports (0-1023):

1. **Port 80:** HTTP (Hypertext Transfer Protocol) - Used for web browsing.
2. **Port 443:** HTTPS (Hypertext Transfer Protocol Secure) - Used for secure web browsing.
3. **Port 25:** SMTP (Simple Mail Transfer Protocol) - Used for sending email.
4. **Port 22:** SSH (Secure Shell) - Used for secure remote access and administration.
5. **Port 21:** FTP (File Transfer Protocol) - Used for file transfers.
6. **Port 53:** DNS (Domain Name System) - Used for domain name resolution.
7. **Port 110:** POP3 (Post Office Protocol version 3) - Used for retrieving email.
8. **Port 143:** IMAP (Internet Message Access Protocol) - Used for retrieving email.
9. **Port 80 and 443:** These are important for web servers, as they handle standard and secure web traffic, respectively.
10. **Port 67 and 68:** DHCP (Dynamic Host Configuration Protocol) - Used for automatic IP address assignment.
11. **Port 137-139:** NetBIOS - Used for Windows file and printer sharing.
12. **Port 161 and 162:** SNMP (Simple Network Management Protocol) - Used for network management and monitoring.
13. **Port 389 and 636:** LDAP (Lightweight Directory Access Protocol) - Used for directory services.
14. **Port 3389:** RDP (Remote Desktop Protocol) - Used for remote desktop access on Windows systems.

What is TCP?

- TCP is a connection oriented protocol.
- TCP (Transmission Control Protocol) ensures reliable and complete data delivery with teh help of Sequence and Acknowledgement.
- Sequence Numbers:
  - When data is sent over a TCP connection, it is divided into smaller units called segments. Each segment is assigned a sequence number.
  - These sequence numbers help TCP keep track of the order of segments and reassemble them at the destination.
- Acknowledgments (ACKs):
  - After receiving a segment, the recipient sends an acknowledgment (ACK) back to the sender to confirm that the segment has been received successfully.

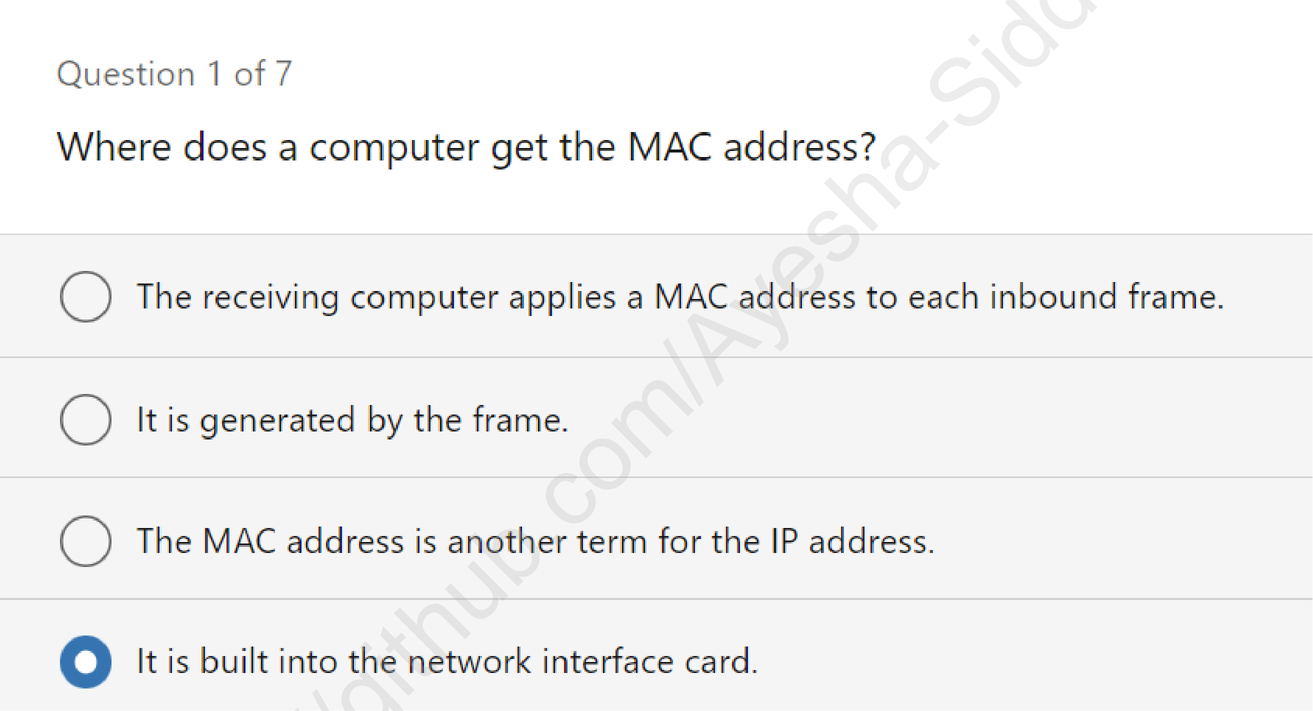
- If the sender doesn't receive an ACK for a particular segment within a reasonable time, it assumes the segment was lost and retransmits it.

Explain UDP.

- UDP is connectionless, which means it does not establish a connection before transmitting data.
- Once UDP sends a packet, it assumes the data is delivered as-is. If a packet is lost or arrives out of order, UDP does not attempt to recover or correct it.

FYI: Packets have sequence numbers so the network software can reassemble the file correctly.

Chapter Quiz



Question 1 of 7

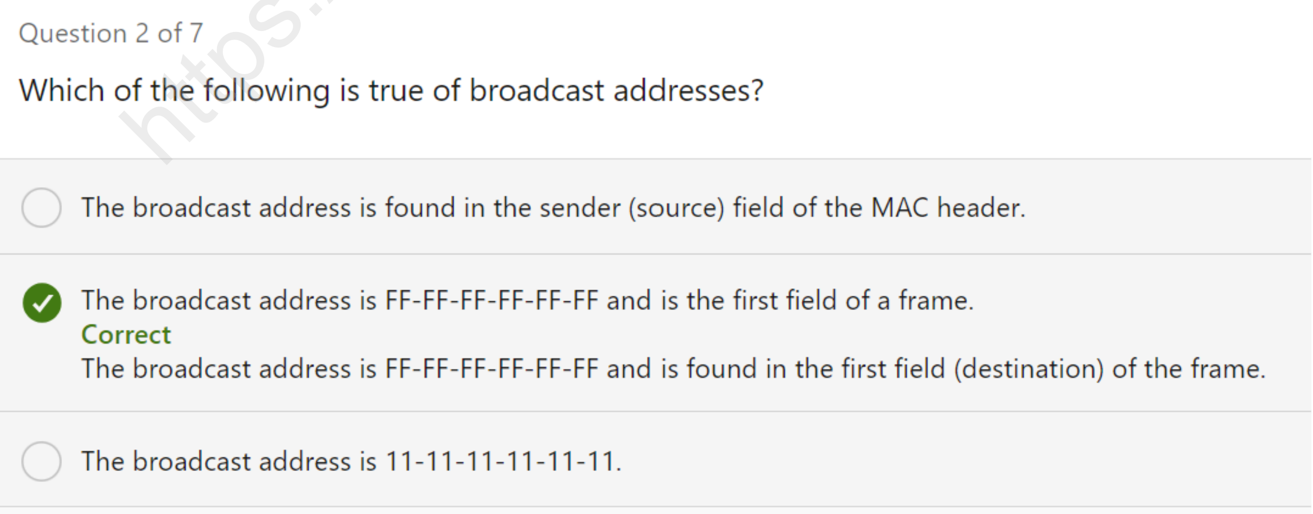
Where does a computer get the MAC address?

○ The receiving computer applies a MAC address to each inbound frame.

○ It is generated by the frame.

○ The MAC address is another term for the IP address.

● It is built into the network interface card.



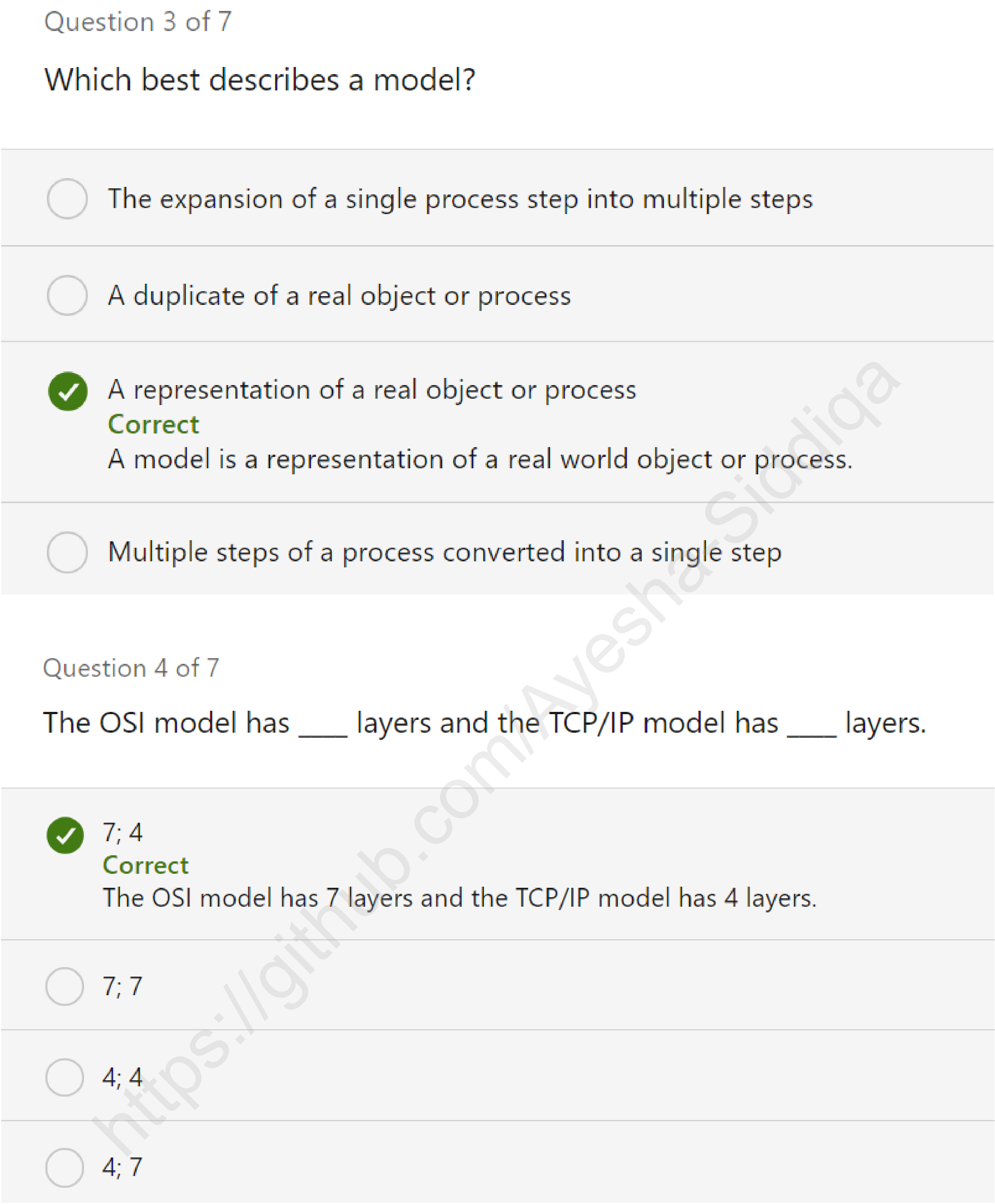
Question 2 of 7

Which of the following is true of broadcast addresses?

○ The broadcast address is found in the sender (source) field of the MAC header.

✓ The broadcast address is FF-FF-FF-FF-FF-FF and is the first field of a frame.
Correct
The broadcast address is FF-FF-FF-FF-FF-FF and is found in the first field (destination) of the frame.

○ The broadcast address is 11-11-11-11-11-11.



Question 3 of 7

Which best describes a model?

○ The expansion of a single process step into multiple steps

○ A duplicate of a real object or process

✓ A representation of a real object or process
Correct
A model is a representation of a real world object or process.

○ Multiple steps of a process converted into a single step

Question 4 of 7

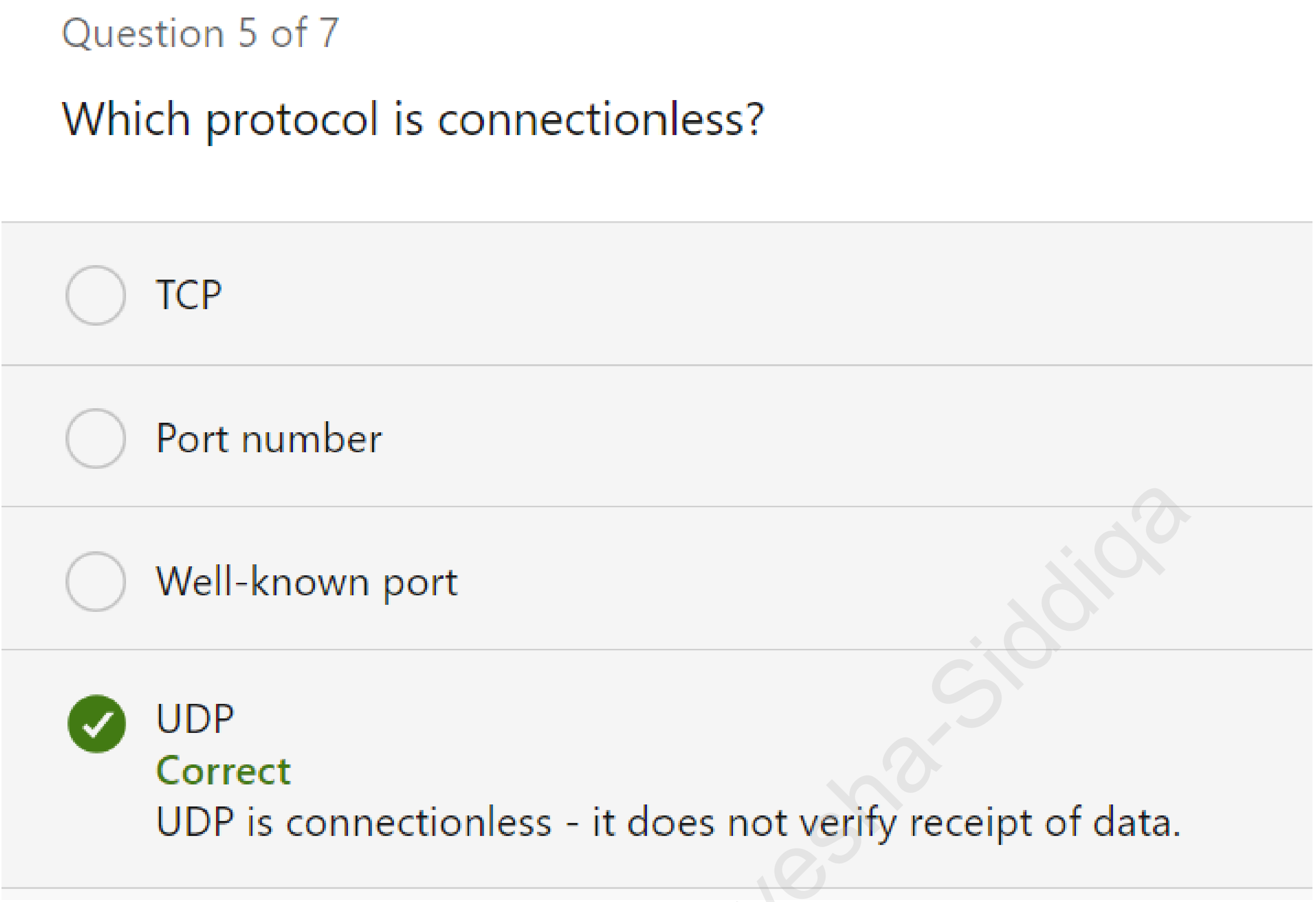
The OSI model has ___ layers and the TCP/IP model has ___ layers.

✓ 7; 4
Correct
The OSI model has 7 layers and the TCP/IP model has 4 layers.

○ 7; 7

○ 4; 4

○ 4; 7



Question 5 of 7

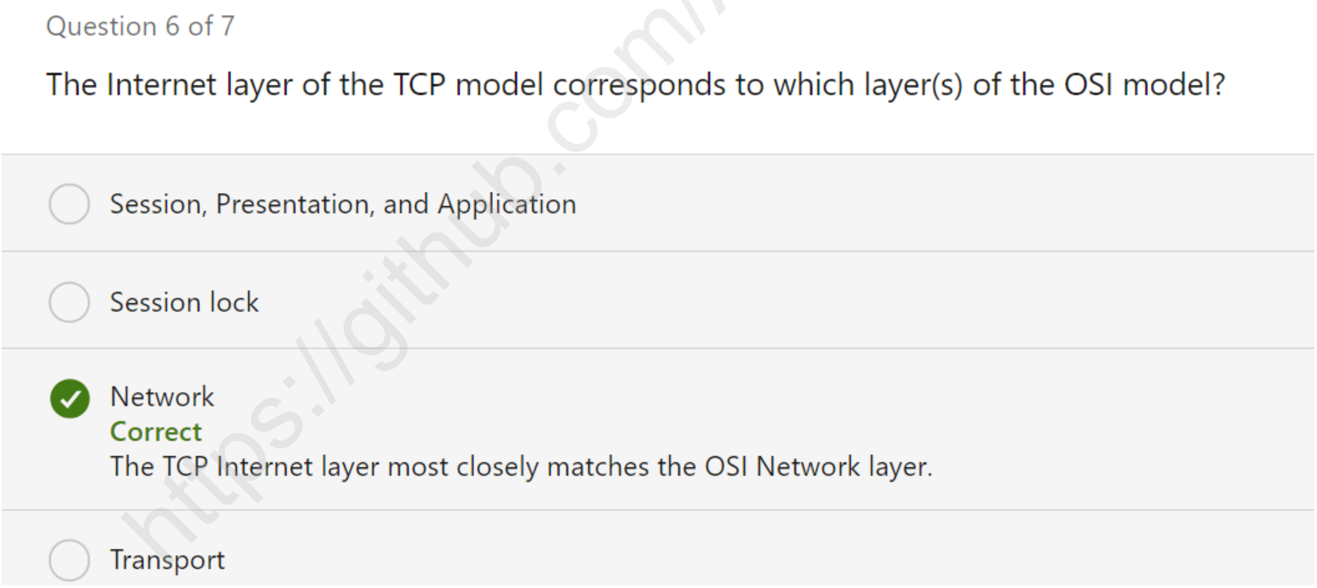
Which protocol is connectionless?

○ TCP

○ Port number

○ Well-known port

✓ UDP
Correct
UDP is connectionless - it does not verify receipt of data.



Question 6 of 7

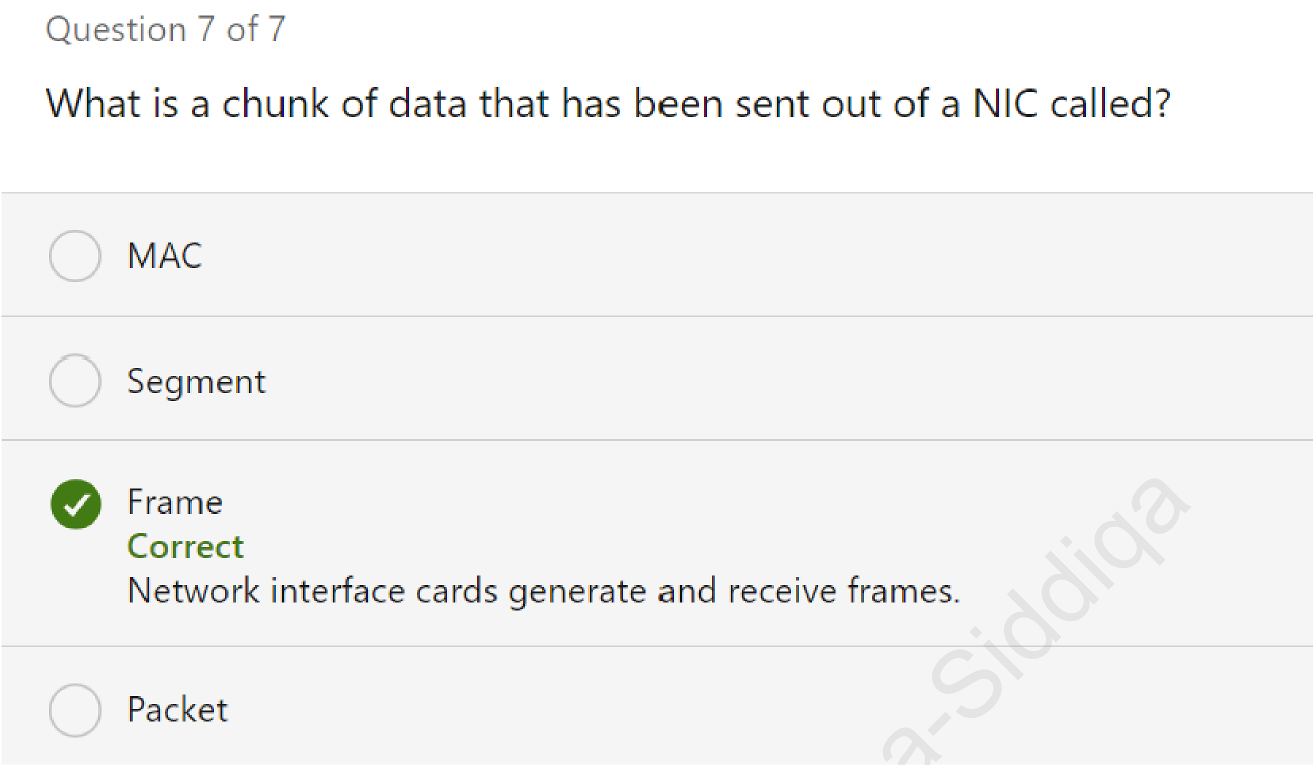
The Internet layer of the TCP model corresponds to which layer(s) of the OSI model?

○ Session, Presentation, and Application

○ Session lock

✓ Network
Correct
The TCP Internet layer most closely matches the OSI Network layer.

○ Transport



Question 7 of 7

What is a chunk of data that has been sent out of a NIC called?

○ MAC

○ Segment

✓ Frame
Correct
Network interface cards generate and receive frames.

○ Packet