Lecture 1 Activity: Understanding OSI and TCP/IP Layers Using a Color-Coded Chart
(Slow Learner)
Case Study: Understanding OSI and TCP/IP Layers Using a Color-Coded Chart
Scenario: Objective: To help learners visualize and understand the 7 layers of the OSI model and 4 layers of the TCP/IP model, and how they map to each other using a color-coded chart.

Color-Coded Chart Description:

Color	OSI Layer	TCP/IP Layer	Function Description
⬤ Blue	Application (Layer 7)	Application	User interaction, app services (HTTP, FTP, SMTP)
▢ Green	Presentation (Layer 6)	Application	Data formatting, encryption, translation (SSL, JPEG)
▢ Purple	Session (Layer 5)	Application	Session control, connection management
▢ Yellow	Transport (Layer 4)	Transport	Reliable delivery (TCP/UDP)
⬤ Red	Network (Layer 3)	Internet	Routing, IP addressing
▢ Orange	Data Link (Layer 2)	Network Access	MAC addressing, switching, and error detection
● Black	Physical (Layer 1)	Network Access	Bits, physical transmission, cables, signals

 Case Study Questions & Answers:
1. What are the main differences between the OSI and TCP/IP models?
Answer:
- OSI has 7 layers, TCP/IP has 4 layers.
- OSI separates Presentation and Session layers; TCP/IP merges them into the Application layer.
- OSI is a theoretical model; TCP/IP is practical and widely implemented.

2. In the color-coded chart, which OSI layers are combined into a single TCP/IP layer?
Answer:
- The Application, Presentation, and Session layers (Blue, Green, Purple) of OSI are combined into the Application layer of TCP/IP.

3. Which protocols operate in the Transport layer of both models (Yellow)?
Answer:
- Common protocols include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

4. What is the primary function of the Network layer (Red) in the OSI model?
Answer:
- The Network layer is responsible for routing and IP addressing to determine how data is forwarded across networks.

5. Why is the Physical layer (Black) important in both models?
Answer:

- It deals with hardware transmission: signals, cables, and connectors. Without it, data cannot physically travel.

6. How does the color-coded chart aid in understanding these models?
Answer:
- It provides visual separation of responsibilities, shows layer relationships, and makes it easier to map OSI to TCP/IP concepts quickly.

7. In which layer would SSL/TLS encryption be found, and what is its color code?
Answer:
- Presentation Layer (Layer 6) in OSI, which is part of the Application Layer in TCP/IP. Color code: ☐ Green.

8. What layer would you troubleshoot if a user can't access a website despite a working network connection?
Answer:
- Start with the Application Layer (Blue) to check if the browser or web server is functioning. Then check Transport (Yellow) and Network (Red) layers.

9. Which layers are involved in a packet moving from a user's computer to a server across the Internet?
Answer:
- All layers:
  - OSI: from Application (7) to Physical (1).
  - TCP/IP: from Application to Network Access.
  - Each layer adds or removes information (headers, footers) as the packet travels.

Lecture 1   Activity: OSI and TCP/IP Layers
 (Slow Learner)
Case Study: Understanding the OSI and TCP/IP Layers
Scenario:
You are a network analyst intern at a mid-size company. Your manager wants you to assess your understanding of the OSI and TCP/IP networking models by answering a series of questions related to the key responsibilities of each layer and how they match up between the two models.

Question 1: Matching Layer Responsibilities
Match the OSI layer with its corresponding TCP/IP layer and a key responsibility:

OSI Layer	TCP/IP Layer	Key Responsibility
Application	A. Application	1. End-user services (e.g., HTTP, DNS)
Network	B. Internet	2. Logical addressing & routing
Transport	C. Transport	3. Reliable data transmission (TCP)
Data Link	D. Network Access	4. MAC addressing and framing

Solution:
- Application → A → 1

- Network → B → 2
- Transport → C → 3
- Data Link → D → 4

Question 2: Which OSI layer is responsible for establishing, maintaining, and terminating sessions between applications?

A.   Transport
B.   Session
C.   Presentation
D. Network

Answer: B. Session

Question 3: True or False

TCP and UDP are protocols that operate at the Transport Layer of both the OSI and TCP/IP models.

Answer: True

Question 4: Short Answer

What are the main responsibilities of the Network Layer in the OSI model?

Answer:

- Logical addressing (e.g., IP addressing)
- Routing packets across networks
- Fragmentation and reassembly of data

Question 5: Fill in the Blanks

The _____ layer in the OSI model corresponds to the Internet layer in the TCP/IP model and is primarily responsible for _____.

Answer:

- Network, Routing, and logical addressing

Question 6: Diagram Labeling

Given this simplified diagram, label each OSI layer with its TCP/IP equivalent:

OSI Model   TCP/IP Model
Application Layer   →?
Presentation Layer →?
Session Layer   → ?
Transport Layer   →?
Network Layer   → ?
Data Link Layer   →?
Physical Layer   →?

Answer:

- Application, Presentation, Session → Application (TCP/IP)
- Transport → Transport (TCP/IP)
- Network → Internet (TCP/IP)
- Data Link, Physical → Network Access (TCP/IP)

Question 7: Scenario-Based

You are troubleshooting a network where devices can ping each other using IP addresses but cannot resolve domain names like "google.com." Which layer of the OSI model is most likely involved in the issue?

A.   Data   Link
B.   Network
C.   Application
D. Transport

Answer: C. Application (specifically DNS service)

Question 8: Multiple Choice

Which of the following is a protocol that operates at the Data Link Layer?

A.   IP
B.   TCP
C.   Ethernet
D. DNS

Answer: C. Ethernet

Question 9: Short Answer

Why is the Transport Layer important for end-to-end communication?

Answer:

It ensures reliable or unreliable data delivery (via TCP or UDP), error checking, flow control, and sequencing for data integrity and order.

Lecture 1   Activity: Networking commands
(Slow Learner)

Case Study: Diagnosing Network Issues Using CMD Commands

Scenario: You are working as a support technician at an IT helpdesk. One of your users reports that they can't access a specific website and that their internet connection seems slow. You're tasked with using CMD tools to diagnose the issue.

Question 1: Basic Command Identification

Which command would you use to display the IP configuration of your local computer, including the IP address, subnet mask, and default gateway?

A.   ping
B.   tracert
C.   ipconfig
D. netstat

Answer: C. ipconfig

Question 2: Output Analysis

You run the command ipconfig /all and find the following:

yaml

CopyEdit

IP Address. . . . . : 169.254.123.45
Subnet Mask . . . . : 255.255.0.0
Default Gateway . . . . :

What does this indicate?

Answer:

The system has an APIPA (Automatic Private IP Address), which means it couldn't contact a DHCP server. This usually indicates a connectivity issue with the router or DHCP server.

Question 3: Troubleshooting with Ping

What would the command ping 8.8.8.8 help determine in a connectivity test?

Answer:

It tests whether the computer can reach Google's public DNS server, helping confirm if the Internet connection is functional at the IP level.

Question 4:Which command would you use to view the path that packets take to reach a specific destination?

A.telnet

B.route

C.tracert

D. arp

Answer: C. tracert

Question 5: Scenario-Based

You use tracert www.example.com, and it hangs at a certain hop with asterisks (***). What does this indicate?

Answer:

The router at that hop is not responding to ICMP packets, possibly due to firewall settings, or the packet is being dropped due to a network issue.

Question 6: Command Usage

A user reports intermittent access to a website. You want to check for DNS resolution issues. What command would you use, and what might you expect to see?

Answer:

Use nslookup www.example.com. It will return the IP address(s) associated with the domain name. If DNS is working, it should return the correct IP. If not, it may fail to resolve.

Question 7: Analyzing Network Connections

What does the command netstat -show?

Answer:

It displays active network connections, listening ports, and their status (e.g., ESTABLISHED, LISTENING). This helps diagnose open ports and suspicious connections.

Question 8: Command Matching

Match the command to its primary use:

Command Function

arp -a   A. Display IP-to-MAC address mappings

route print B. Show the routing table

telnet   C. Test remote access on a specific port

Solution:

- arp -a → A
- route print → B

GLA UNIVERSITY
Accredited with A+ Grade by NAAC
Mathura | Greater Noida

Summer Immersion
Placement Program
SIPP 2025

- telnet → C

Question 9: Port Testing

You want to test if a remote server is accepting connections on port 25 (SMTP). Which command do you use and how?

Answer:

Use telnet mail.example.com 25. If the port is open and accepting, you will receive a server banner or prompt. If the connection fails, the port may be blocked or the service may be down.