NETWORKS AND COMMUNICATIONS LEC

MIDTERM EXAM REVIEWER

UCOS 3-2

GROUP 1 - SANGALANG

MEMBERS:
ANDRES, KHRYSSHA MARIE
CORTEZ, KRISTIAN BERNARD
ESCUREL, JOHN ROBERT
NAVELGAS, QUENZZY
SARMIENTO, CARL ANDREI
SOLIS, JOHN MARK
TALABOC, YERIK YVES GAVRIE

SUBMITTED TO:
ENGR. SO, JOHN CARLO

DATE SUBMITTED:
10/23/2024

TABLE OF CONTENTS

Lecture 1: Network Topologies

1.1 Key Concepts

Network topologies define the layout of devices in a network. Common types include star, bus, ring, and mesh, each with unique structures and data flow methods. Topologies impact performance, scalability, and fault tolerance.

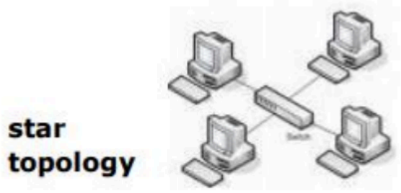
1.2 Physical Topology

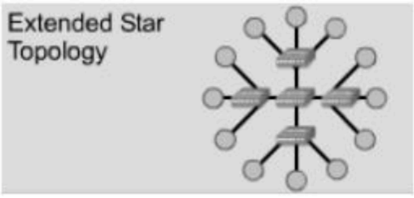
Bus Topology

- Bus topology connects all the devices to a common, shared cable that proceeds from one computer to the next.
- Commonly called a linear bus.

Star And Extended Star Topology

- Star topology is the most common in Ethernet LANs. It consists of a central device (hub, switch, or router) where all cables connect. Each host has its own cable to the central device, making it more expensive than bus topology.
- Star topology's advantage is that a single cable issue only affects the connected host, keeping the rest of the network operational. However, if the central device fails, the entire network disconnects. Expanding the network with another device creates an extended-star topology.



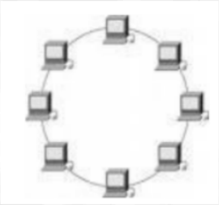


Ring Topology

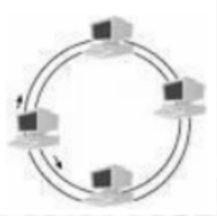
- In ring topology, hosts are connected in a circle without needing termination. A frame travels around the ring, and nodes can add data and a destination address to it. The frame moves until it reaches the destination. The key advantage is that there are no data collisions.

Types of Ring

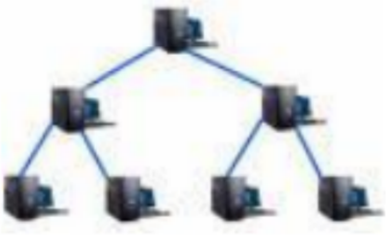
- **Single Ring**
  - All devices on the network share a single cable, and the data travels in one direction only.
  - Each device in single ring topology waits its turn to send data over the network.



- **Dual Ring**
  - In dual ring topology, two rings allow data to be sent in both directions.
  - Dual ring setup creates redundancy which means that if one ring fails, data can be transmitted on the other ring. If both rings fail, a “wrap” at the fault can heal the topology back into a ring.



Hierarchical Topology



- This topology is similar to extended-star topology; the only difference is that it does not use a central node.
- Hierarchical topology uses a trunk node from which it branches to other nodes.

Full-Mesh Topology

- In full-mesh topology, all devices are connected to each other for redundancy and fault tolerance.
- The advantage of full-mesh topology is that every node is connected physically to every other node, thus creating a redundant connection. If one of the links fails, information can flow through many other links to reach its destination.

Partial-Mesh Topology

- In this topology, at least one device maintains multiple connections to others without being fully meshed.
- Provides redundancy by having several alternative routes.

1.3 Logical Topology

- Describes the logical pathway a signal follows as it passes among the network nodes.
- It defines how the medium is accessed by the hosts for sending data.
- The two most common types of logical topology are broadcast, and token passing

Broadcast Topology

- In broadcast topology, each host addresses its data to a particular NIC, to a
- Multicast address, or to a broadcast address on the network medium.
- The stations do not follow specific order in using the network; instead, it is first come, first serve basis.

Token Passing

- In token passing, network access is controlled by using an electronic token which is passed to each host in the network.
- The advantage of token passing is that collisions are eliminated and bandwidth can be fully utilized without idle time when

Lecture 2: Data Center Technology

1.1 Key Concept

❖ Data center technology encompasses a range of systems and protocols that manage, store, and transmit data efficiently. It includes the physical infrastructure, networking, and software services that ensure high availability and reliability for businesses. Core elements such as servers, storage devices, networking equipment, and security systems are integral to data centers' operation.

1.2 Network Types

1.2.1 Intranets

- are private networks used within an organization to share information securely among employees.

1.2.2 Extranets

- extend intranet functionality to select external partners, enabling secure collaboration between organizations.

1.2.3 Virtual Private Networks (VPN)

- create secure connections over public networks, ensuring data privacy and protection when accessing remote systems.

1.2.3.1 Advantages

- VPNs include cost-effectiveness, enhanced security, and the ability to support remote work by encrypting data traffic.

1.3 Bandwidth

1.3.1 Key Concepts

- Bandwidth refers to the maximum rate at which data can be transferred over a network connection.

1.3.2 Importance of Bandwidth

- It is critical to determine how much information can be sent or received in a given time, influencing the speed and quality of data services.

1.3.3 Analogies that Describe Digital Bandwidth

- Bandwidth can be compared to the width of a highway: the broader the highway, the more vehicles (or data) can travel simultaneously, improving efficiency and reducing congestion.

1.4 Data Throughput

1.4.1 Key Concept

- Data throughput measures the actual amount of data successfully transmitted over a network in a specific period.

1.4.2 Factors that Determine Data Throughput

- Several factors impact throughput, including network congestion, hardware limitations, and protocol inefficiencies. Throughput is a critical metric in evaluating the performance of a data center network.

Lecture 3: Networking Models

1.1 Key Concepts

Networking models offer an organized framework for comprehending the flow of data between networks. They make it easier to debug and design networks by helping to deconstruct the intricate networking process into digestible stages.

1.2 Networking Comparison

Several networking models, including the Transmission Control Protocol/Internet Protocol (TCP/IP) model and the Open Systems Interconnection (OSI) model, provide different ways to standardize network communication. These models make it possible for many devices and technologies to work together.

1.3 The OSI Reference Model

1.3.1 Definitions

The OSI (Open Systems Interconnection) model defines a framework for how different network functions are separated into **seven layers**. These layers work together to ensure communication across networks by breaking down the process into manageable parts.

1.3.2 OSI Layers and Functions

1. **Physical Layer (Layer 1)**:
   - Deals with the physical connection of devices to the network, including cables, switches, and transmission of raw bitstreams over a physical medium.
   - Attributes: Voltage levels, physical data rates, connectors, etc.
2. **Data Link Layer (Layer 2)**:
   - Ensures reliable data transfer across a single link or network segment.
   - Handles error detection, physical addressing, and flow control.
3. **Network Layer (Layer 3)**:
   - Manages logical addressing and path selection between different networks (e.g., IP addressing).
   - Provides routing and forwarding services.
4. **Transport Layer (Layer 4)**:
   - Ensures reliable transmission of data across the network, handling segmentation, flow control, and error correction.
   - Protocols: TCP (reliable), UDP (unreliable).
5. **Session Layer (Layer 5)**:
   - Establishes, manages, and terminates sessions between two communicating devices.
   - Synchronizes data exchanges and manages dialog control.
6. **Presentation Layer (Layer 6)**:
   - Translates, encrypts, and compresses data so that it can be properly interpreted between the application layer of different systems.
   - Examples: JPEG for images, MPEG for videos.
7. **Application Layer (Layer 7)**:
   - Closest to the end user, this layer interacts with software applications to implement networking services like email, file transfer, etc.
   - Examples: HTTP, Telnet.

1.3.3 Advantages Of Dividing the Network into Seven Layers

- **Simplification**: Each layer performs a specific function, simplifying network design and troubleshooting.

- **Standardization**: Vendors can create hardware and software that interoperate, promoting compatibility across devices.
- **Modularity**: Changes to one layer do not affect others, making updates or upgrades easier.
- **Layer Isolation**: Problems in one layer can be solved without impacting other layers, streamlining debugging and error resolution.
- **Learning**: Breaking down communication into smaller parts helps learners understand complex networking concepts.

1.3.4 Layer 7 To 1 (Top-Down)

A top-down approach describes data flow starting from the Application layer (Layer 7) and moving down to the Physical layer (Layer 1) during transmission. The reverse happens when receiving data.

1. **Layer 7 (Application Layer)**: User interacts with network applications (e.g., email, web browsing).
2. **Layer 6 (Presentation Layer)**: Data is formatted and encrypted.
3. **Layer 5 (Session Layer)**: Sessions between devices are established.
4. **Layer 4 (Transport Layer)**: Data is segmented and sent reliably (TCP) or unreliably (UDP).
5. **Layer 3 (Network Layer)**: Data packets are routed across networks using IP addresses.
6. **Layer 2 (Data Link Layer)**: Data frames are transmitted over the physical network.
7. **Layer 1 (Physical Layer)**: Data is sent as raw bits over the network medium (e.g., cables).

1.4 Peer-To-Peer Communication

In peer-to-peer communication, each layer on one device communicates with its corresponding layer on another device (e.g., Layer 4 on Device A communicates with Layer 4 on Device B).

- **How it works**: Each OSI layer on the sending device communicates with its peer layer on the receiving device through standardized protocols (e.g., IP for Network Layer, TCP for Transport Layer).
- **Purpose**: Ensures that data is properly transmitted, understood, and interpreted across different systems, even if the devices use different hardware or software.

This communication model enables seamless data transfer between systems with different architectures, ensuring interoperability in a network environment.

Lecture 4: Networking Concepts: IP Configuration, VLANs, and Packet Tracer

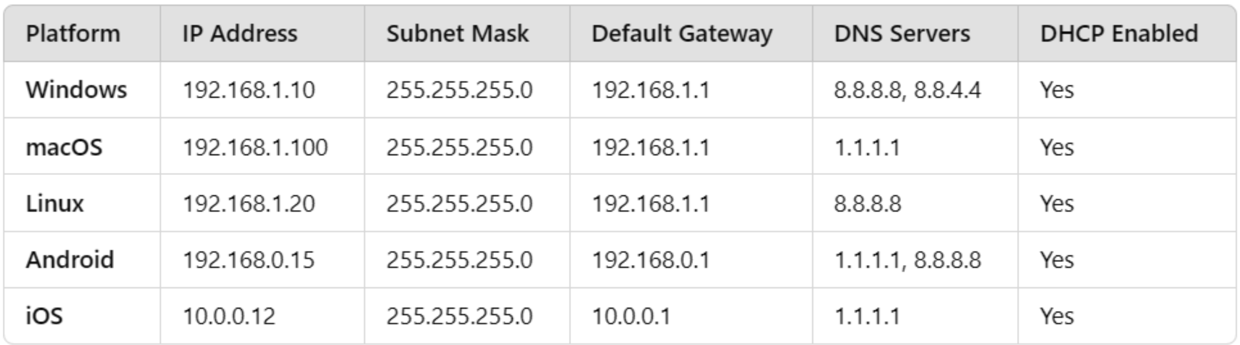
1.1 IP Configuration

IP configuration refers to the process of assigning and managing an IP address on a network device such as a computer, router, or server.

Key Components

- **IP Address:** Unique identifier for a device.
- **Subnet Mask:** Defines the network and host portion of an IP address.
- **Default Gateway:** Routes traffic to external networks.
- **DHCP:** Dynamic IP address assignment.
- **DNS Server:** Resolves domain names to IP addresses.

Here are some examples of each key components



Platform	IP Address	Subnet Mask	Default Gateway	DNS Servers	DHCP Enabled
Windows	192.168.1.10	255.255.255.0	192.168.1.1	8.8.8.8, 8.8.4.4	Yes
macOS	192.168.1.100	255.255.255.0	192.168.1.1	1.1.1.1	Yes
Linux	192.168.1.20	255.255.255.0	192.168.1.1	8.8.8.8	Yes
Android	192.168.0.15	255.255.255.0	192.168.0.1	1.1.1.1, 8.8.8.8	Yes
iOS	10.0.0.12	255.255.255.0	10.0.0.1	1.1.1.1	Yes

1.1.1 Static vs. Dynamic IP Configuration

IP Configuration Types

- **Static IP:** Manually assigned and does not change.
  - Example: Servers, printers, or network devices (routers, switches).
- **Dynamic IP:** Assigned dynamically by a DHCP server; changes periodically.
  - Example: Client PCs, mobile devices.

1.2 Introduction to Cisco Packet Tracer

Cisco Packet Tracer is a powerful network simulation tool developed by Cisco. It allows users to create network topologies, configure devices, and simulate network behavior without needing physical networking equipment.

Cisco Packet Tracer is used for network simulation and network design. Its primary functions and use cases include:

- Network simulation tool for learning and practice.
- Used for training and planning network configurations.
- Simulates routers, switches, PCs, and more.
- Packet-level simulation to test and analyze network traffic.

1.2.1 Creation of a LAN

Steps to Create a LAN:

1. **Open Cisco Packet Tracer**
   a. Launch Cisco Packet Tracer to create a new project.
2. **Add network devices**
   a. Like PCs, switches, and routers.
3. **Connect devices using appropriate cables.**
   a. Copper Straight-Through cable (for connecting different devices like PC-to-switch)
   b. Then connect it to the switch using the **FastEthernet** port.
4. **Assign IP addresses to devices.**
   a. Click on the first PC and go to the **Desktop** tab.
   b. Click on **IP Configuration** and manually assign an IP address.

c. Repeat this for all other PCs to connect them to the switch using their **FastEthernet** ports.

5. **Test connectivity using the ping command.**
   a. After assigning IP addresses, test the connection between the devices.
   b. Click on **PC1**, go to the **Desktop** tab, and select **Command Prompt**.
   c. Type “ping <IP address of PC2 or the PC you want to check the connection>
   d. Then, You should see replies from the PC you are checking, indicating that the two devices are connected.

1.2.2 VLAN Creation

- Virtual Local Area Networks (VLANs) logically segment a network.
- Use VLANs to improve security and manage traffic.
- Create VLANs and assign switch ports to VLANs in Cisco Packet Tracer.
- VLANs isolate devices; inter-VLAN routing required for communication.

VLAN Creation in Packet Tracer

- **Open Cisco Packet Tracer**
  a. Launch Cisco Packet Tracer and create a new project.
- **Add Network Devices**
  a. Add a Switch.
  b. Add PCs
- **Connect PCs to the Switch**
  a. Use **Copper Straight-Through cables** to connect each PC to different FastEthernet ports on the switch
- **Configure VLANs on the Switch**
  a. Click on the switch to access its configuration.
  b. Go to the CLI (Command Line Interface) tab.
    - Enter Global Configuration Mode
      - Switch> enable
      - Switch# configure terminal
    - **Create VLAN 10 (HR Department)**:
      - Switch(config)# vlan 10
      - Switch(config-vlan)# name (HR Department)
      - Switch(config-vlan)# exit
    - **Create VLAN 20 (IT Department))**:
      - Switch(config)# vlan 20
      - Switch(config-vlan)# name (IT Department)
      - Switch(config-vlan)# exit
    - **Assign Switch Ports to VLANs**
      - Switch(config)# int fa 0/1 - 2
      - Switch(config-if-range)# switchport mode access
      - Switch(config-if-range)# switchport access vlan 10
      - Switch(config-if-range)# exit
    - **Verify VLAN Configuration**
      - Switch# show vlan brief
    - **Assign IP Addresses to PCs**
    - Test VLAN Connectivity (Ping)

1.2.4 VLAN Trunking

1. **Open Cisco Packet Tracer**
   a. Launch Cisco Packet Tracer and set up your network with at least two switches and some PCs.

2. **Add and Connect Devices**
   a. Add Two Switches
   b. Add PCs
   c. Connect Switches

3. Configure VLANs on Both Switches
   a. For each switch, create the same VLANs to ensure consistency.
   b. Access the CLI of each switch and enter the following commands:

Switch1 Configuration	Assign Ports to VLANs	Switch2 Configuration	Assign Ports to VLANs
Switch1> enable Switch1# configure terminal Switch1(config)# vlan 10 Switch1(config-vlan)# name HR Department Switch1(config-vlan)# exit Switch1(config)# vlan 20 Switch1(config-vlan)# name IT Department Switch1(config-vlan)# exit	Switch1(config)# interface range FastEthernet 0/1 - 2 Switch1(config-if-range)# switchport mode access Switch1(config-if-range)# switchport access vlan 10 Switch1(config-if-range)# exit Switch1(config)# interface range FastEthernet 0/3 - 4 Switch1(config-if-range)# switchport mode access Switch1(config-if-range)# switchport access vlan 20 Switch1(config-if-range)# exit	Switch1> enable Switch1# configure terminal Switch1(config)# vlan 10 Switch1(config-vlan)# name HR Department Switch1(config-vlan)# exit Switch1(config)# vlan 20 Switch1(config-vlan)# name IT Department Switch1(config-vlan)# exit	Switch1(config)# interface range FastEthernet 0/1 - 2 Switch1(config-if-range)# switchport mode access Switch1(config-if-range)# switchport access vlan 10 Switch1(config-if-range)# exit Switch1(config)# interface range FastEthernet 0/3 - 4 Switch1(config-if-range)# switchport mode access Switch1(config-if-range)# switchport access vlan 20 Switch1(config-if-range)# exit

4. **Configure the Trunk Link**

Switch 1 Trunk Configuration:	Switch 2 Trunk Configuration:
Switch1(config)# interface FastEthernet 0/5 # *Assuming Fa0/5 is the trunk link* Switch1(config-if)# switchport mode trunk Switch1(config-if)# switchport trunk allowed vlan	Switch2(config)# interface FastEthernet 0/5 # *Assuming Fa0/5 is the trunk link* Switch2(config-if)# switchport mode trunk Switch2(config-if)# switchport trunk allowed vlan

10,20 Switch1(config-if)# exit	10,20 Switch2(config-if)# exit

5. **Testing Connectivity Across VLANs**
   a. Assign IP addresses to PCs in VLAN 10 and VLAN 20.
   b. Test connectivity within the same VLAN

Lecture 5: Data Encapsulation and De-Encapsulation

1.1 Key Concepts

- Encapsulation: Adding protocol information as data moves down OSI layers
- De-encapsulation: Removing protocol information as data moves up OSI layers
- Each layer adds/removes its own specific header
- Data can only be exchanged between peer layers

Purpose

- Prepare data for network transmission
- Add necessary addressing information
- Ensure proper data delivery
- Enable communication between different networks

1.3 Encapsulation Process (Top-Down)

1. Application → Original user data
2. Presentation → Encrypts data
3. Session → Adds Session ID
4. Transport → Adds TCP/UDP header
5. Network → Adds IP header
6. Data Link → Adds MAC header
7. Physical → Converts to bits

1.4 De-encapsulation Process (Bottom-Up, Physical Layer to Application Layer)

- Reverse of encapsulation
- Each layer removes its corresponding header
- Final result: original data at application layer

1.5 Data Units at Each Layer

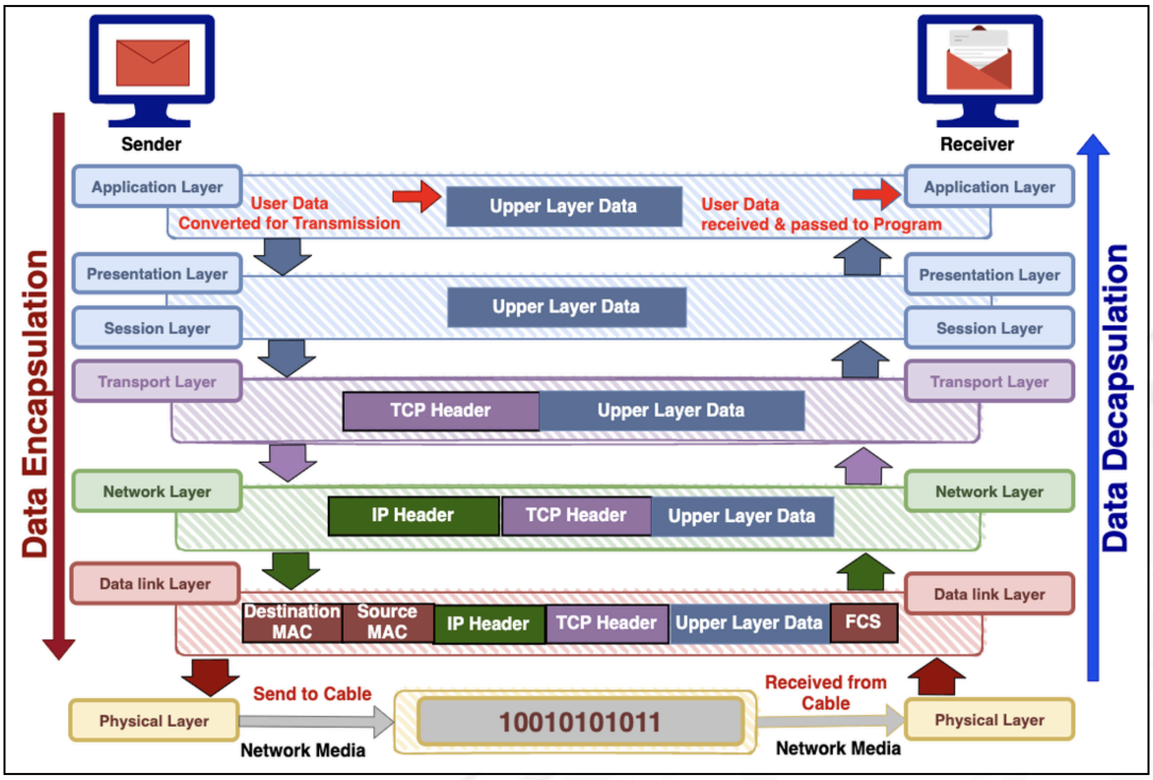
1. Application → Data
2. Presentation → Data
3. Session → Data
4. Transport → Segments/Datagrams
5. Network → Packets
6. Data Link → Frames
7. Physical → Bits

Key Points to Remember

- Headers are added going down layers
- Headers are removed going up layers
- Each layer performs specific functions

❖ Process works in both directions across networks
❖ Data format changes at each layer

Here’s a diagram of how devices talk to each other using Data Encapsulation and Data Decapsulation:


Sender
Receiver
Data Encapsulation
Data Decapsulation
Application Layer
User Data
Converted for Transmission
Upper Layer Data
User Data
received & passed to Program
Application Layer
Presentation Layer
Presentation Layer
Upper Layer Data
Session Layer
Session Layer
Transport Layer
TCP Header
Upper Layer Data
Transport Layer
Network Layer
IP Header
TCP Header
Upper Layer Data
Network Layer
Data link Layer
Destination MAC
Source MAC
IP Header
TCP Header
Upper Layer Data
FCS
Data link Layer
Send to Cable
Received from Cable
Physical Layer
10010101011
Physical Layer
Network Media
Network Media