

Cybersecurity Concepts

Prepared by Dr. Diaa Salama

FNT625
Network Basics

Lecture 2





مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY

Cybersecurity Concepts

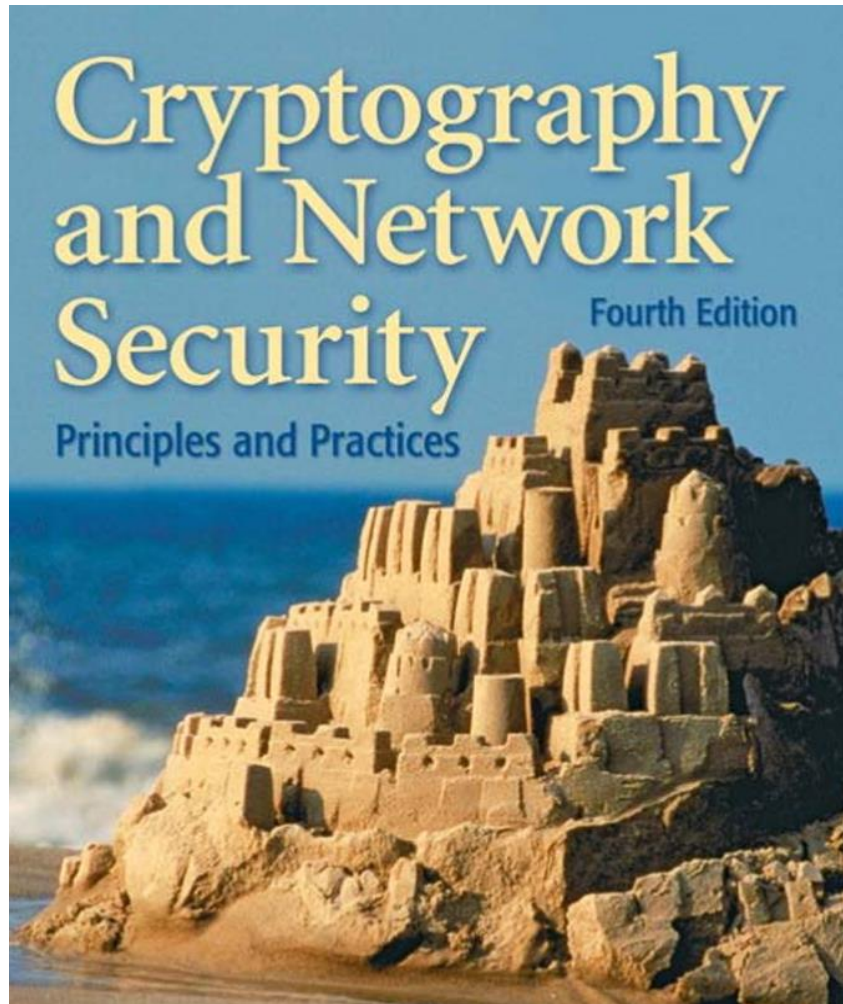
Lecture 2

FNT625

Introduction to Network and Network Security

Prepared by
Dr. Diao Salama

www.midocean.ae



Book Title:

Cryptography and Network Security

Authors:

William Stallings

Publisher:

Pearson Education, Inc.

Edition:

Seven edition

Lecture

02

Lets Start the second Lecture

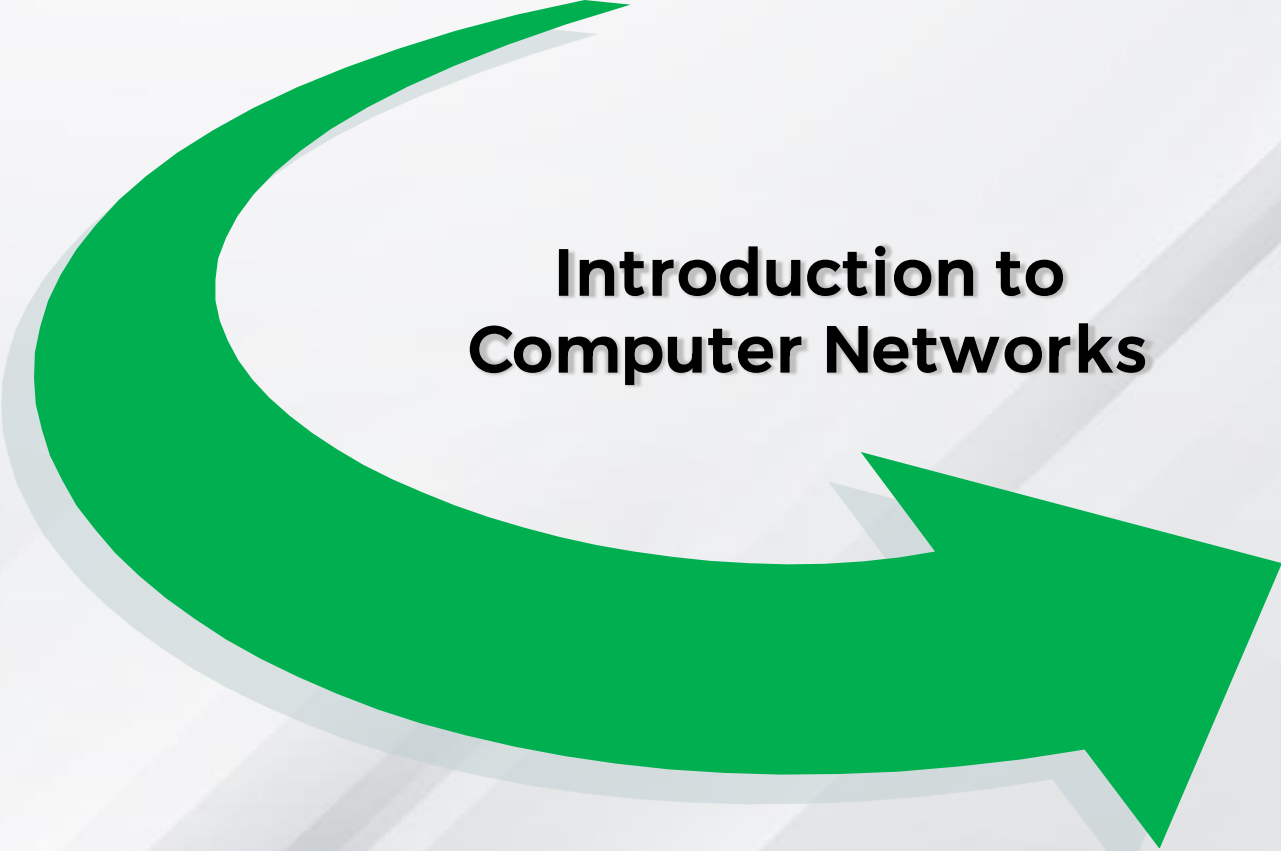


Introduction to Network and Network Security



What is Cyber Security (Network Security) !

- **A network** is simply two or more computers linked together to share data, information or resources.
- **Security** : prevention of system Crash



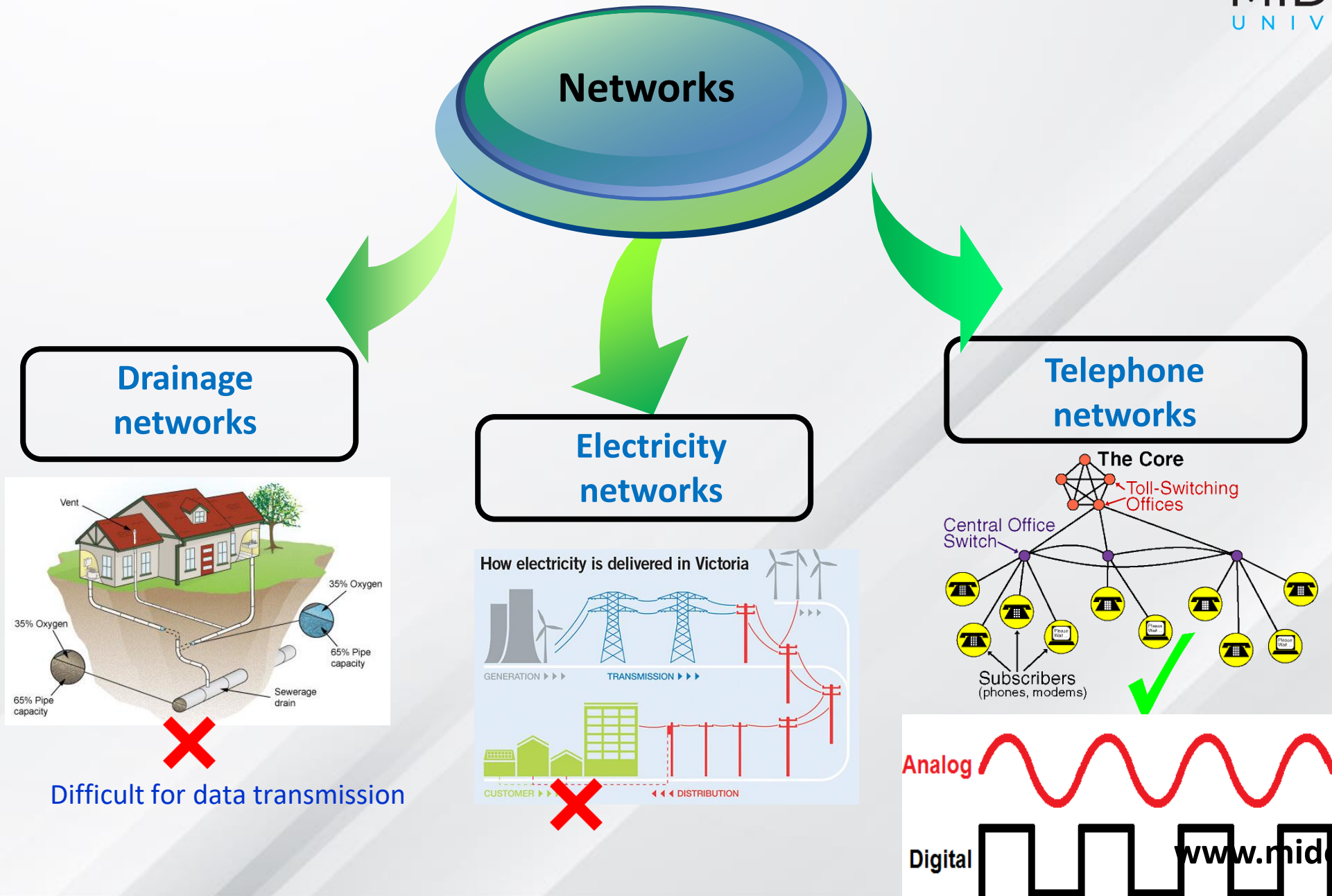
Introduction to Computer Networks

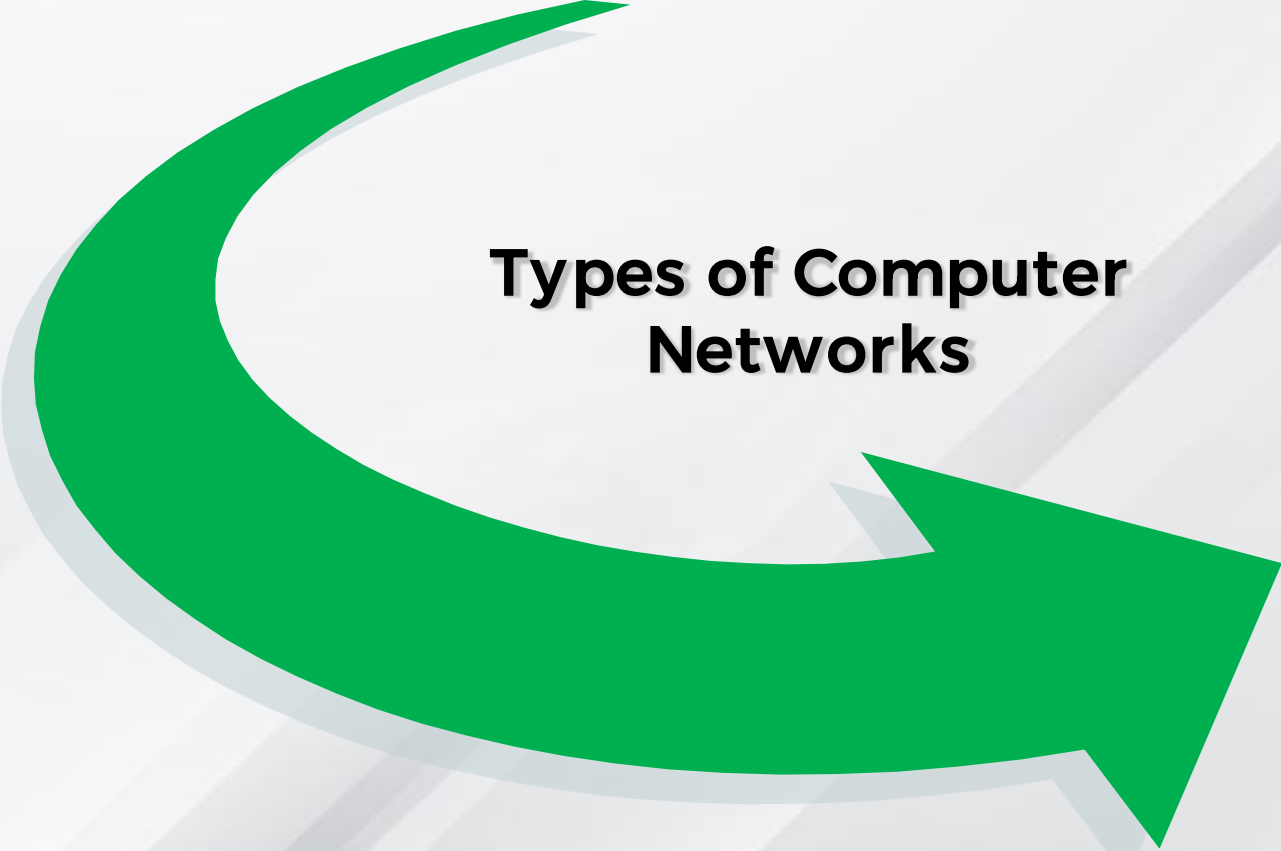
Introduction to Computer Networks

- How to communicate each point to another point or points.



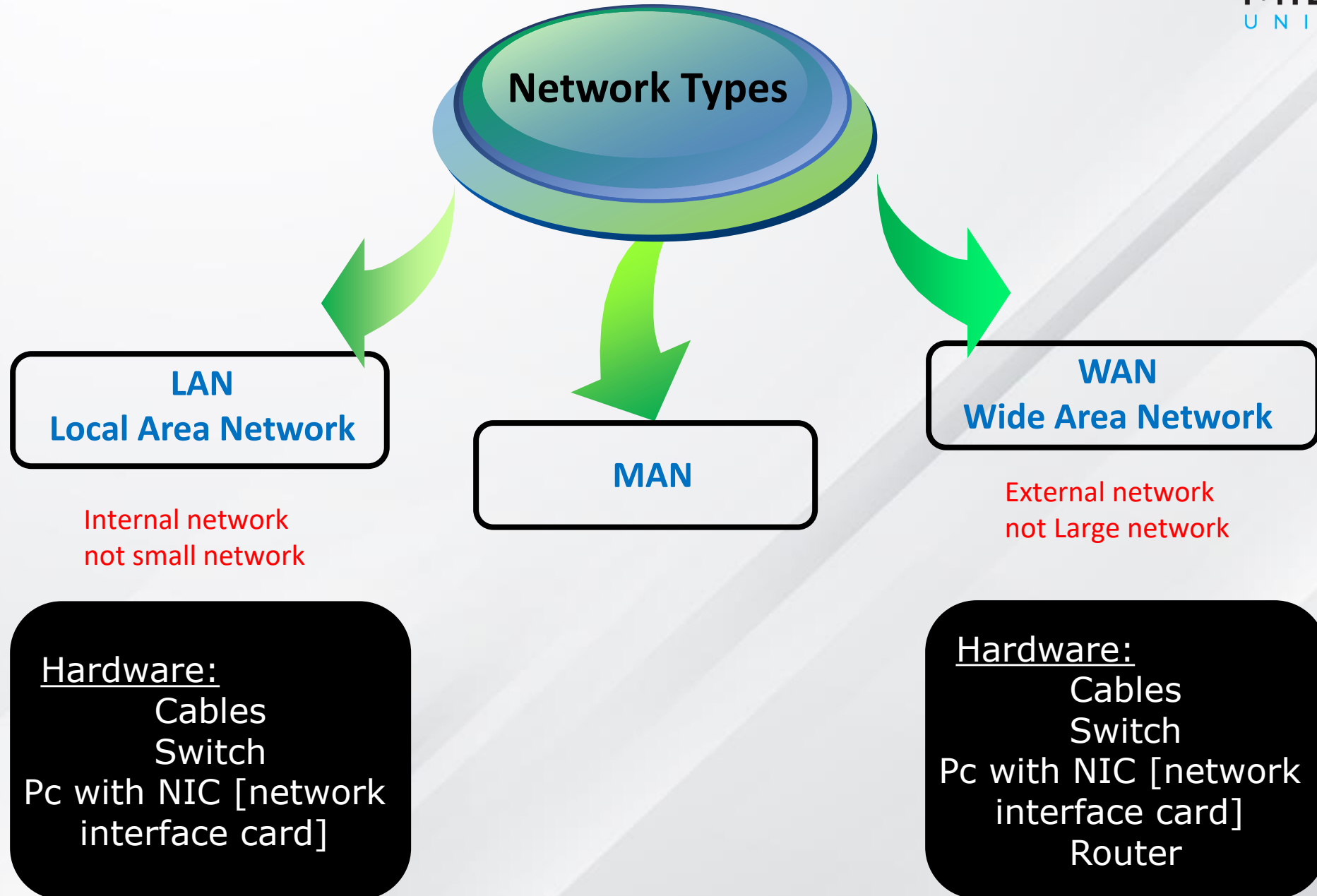
Introduction to Computer Networks





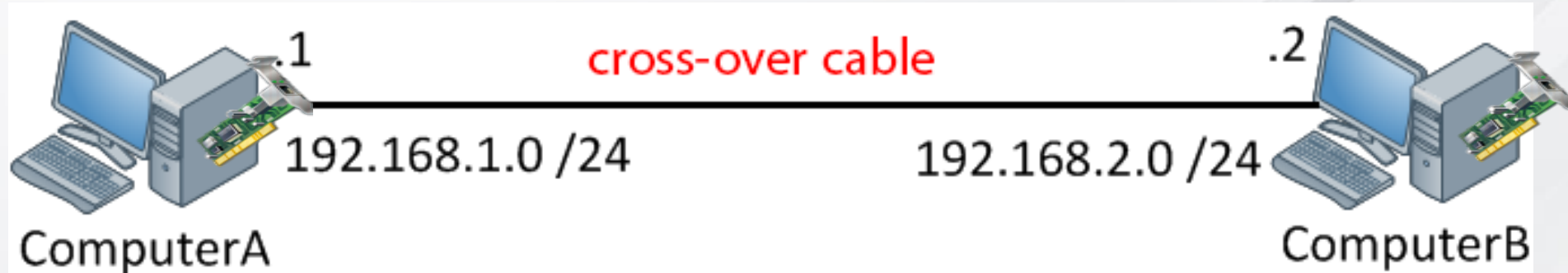
Types of Computer Networks

Types of Computer Networks

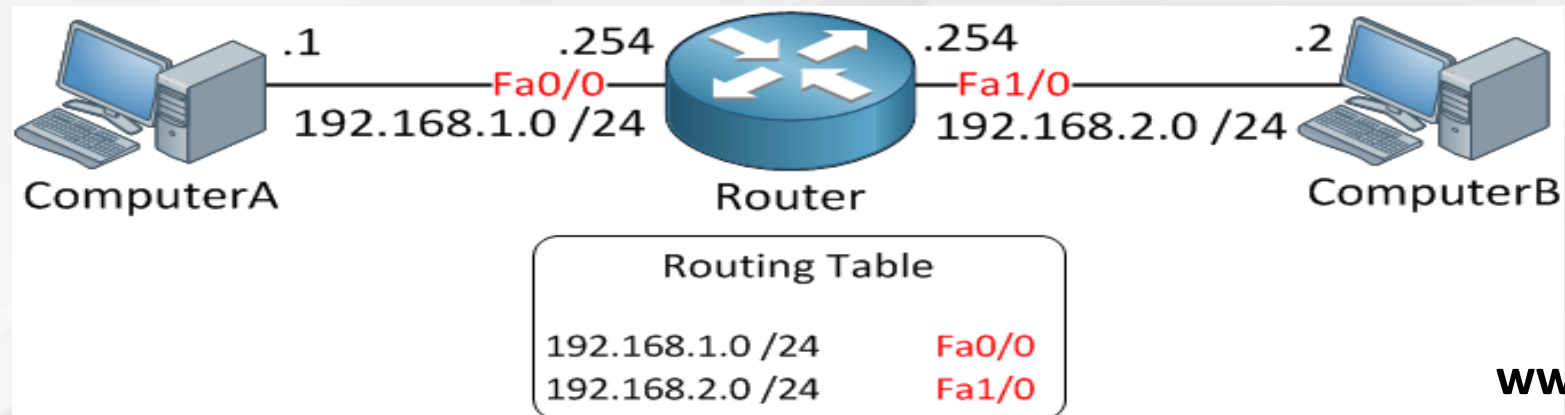


Introduction to Computer Networks

❑ Connecting two Computers on the same location



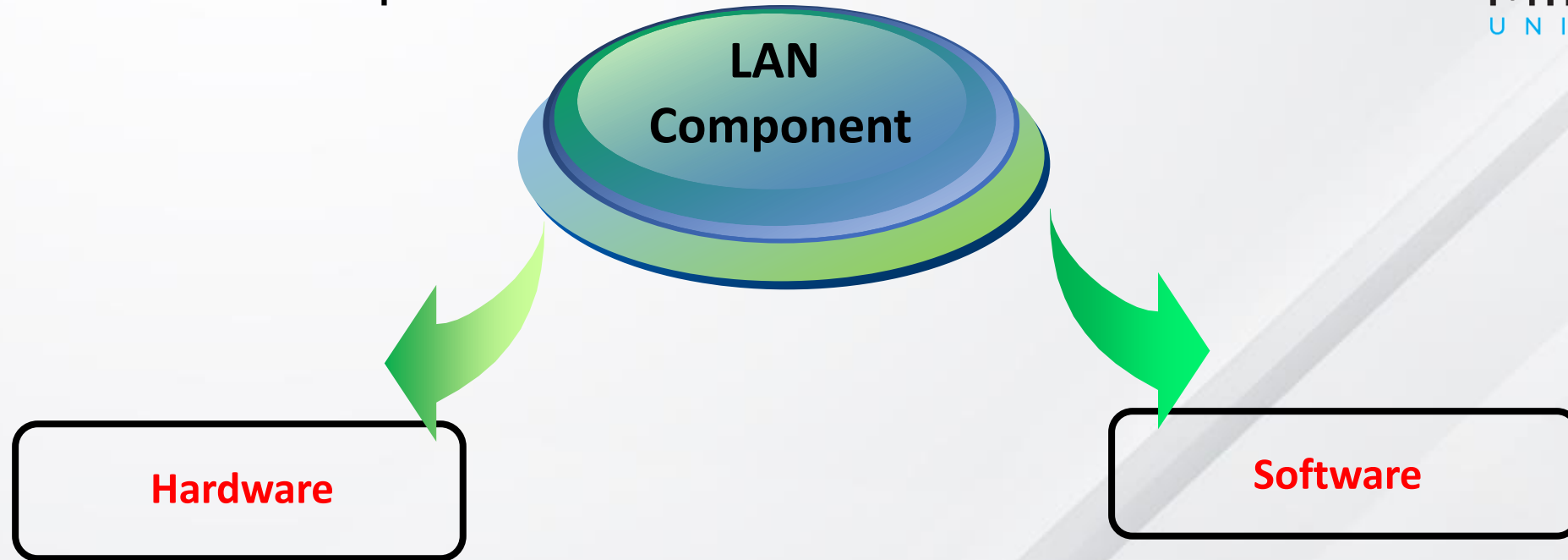
❑ Connecting two Computers on different and distant locations.





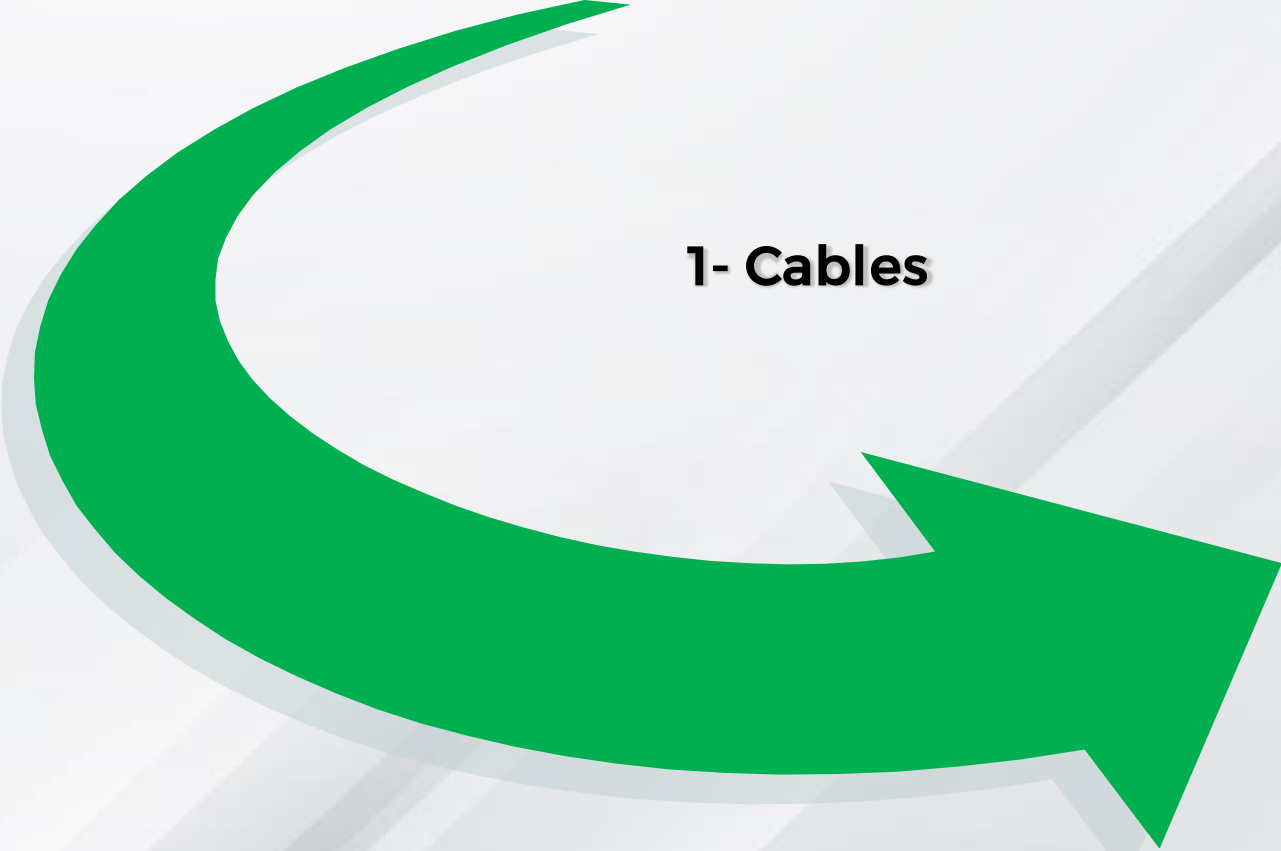
How to Setup a LAN

How to Setup a LAN



Hardware:

Cables
Switch
Pc with
NIC [network
interface card



1- Cables

Cables

Type	Scientific Name	Speed/distance Data transfer	Comments
Coaxial Cable Max Speed	Thin 10 base 2 (20 milli) (Megabit/s) Thick 10 base 5 (50 milli) (Megabit/s) Thick 100 base 5 (Megabit/s) Thick 1000 base 5 (1000 Megabit/s)	100 m (long distance need repeater). 500 m	Cable is not elastic so it is not practical for long distance. It uses BNC connector for terminals so it needs a converter to connect to a switch or router device . It is expensive
UTP unshield ed twisted pair	10 base T (Twisted Pair). In market it is famous with Cat 5 (max speed 10 Megabit/s) Cat 5 e (enhanced max) max speed 100 Megabit/s Cat 6 (max speed 1000 Megabit/s)	100 m Connector RJ45	It is not expensive It is connected directly to switch or router.

- ❑ If cable speed is 10 means 10 Mega bits/second
- ❑ Network speed is measured by bit.
- ❑ While storing data is measured by byte.

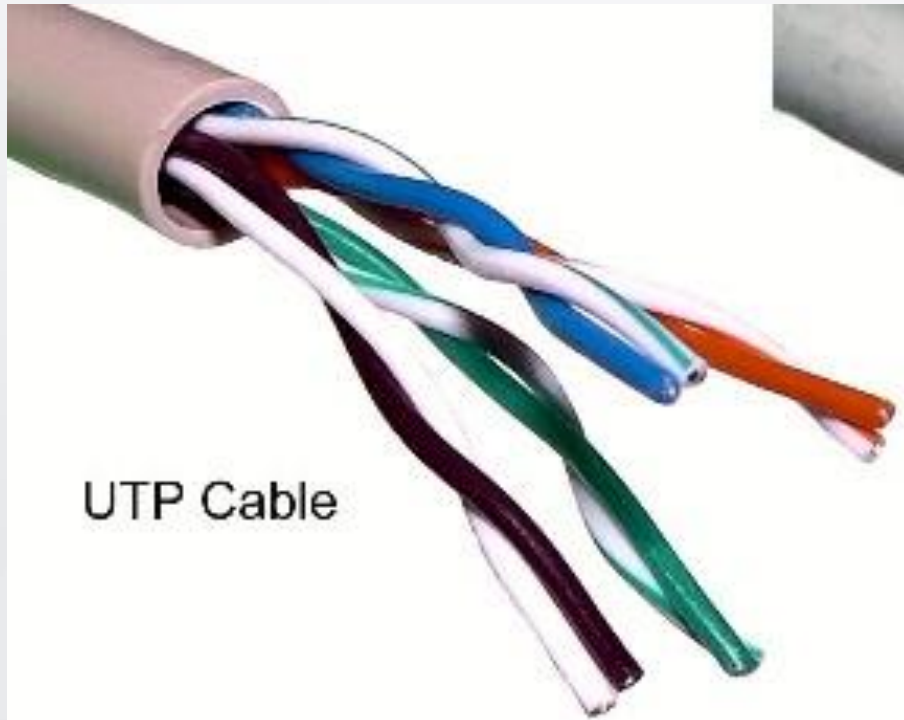
Cables

Type	Scientific Name	Speed/distance (Data transfer)	Comments
STP shielded twisted pair	10 base T (Twisted Pair). In market it is famous with Cat 5 (max speed 10 Megabit/s) Cat 5 e (enhanced max) max speed 100 Megabit/s Cat 6 (max speed 1000 Megabit/s)	100 m Connector RJ45	It is expensive It is connected directly to switch or router.
Fiber Optics	10 base F	300 km/s	

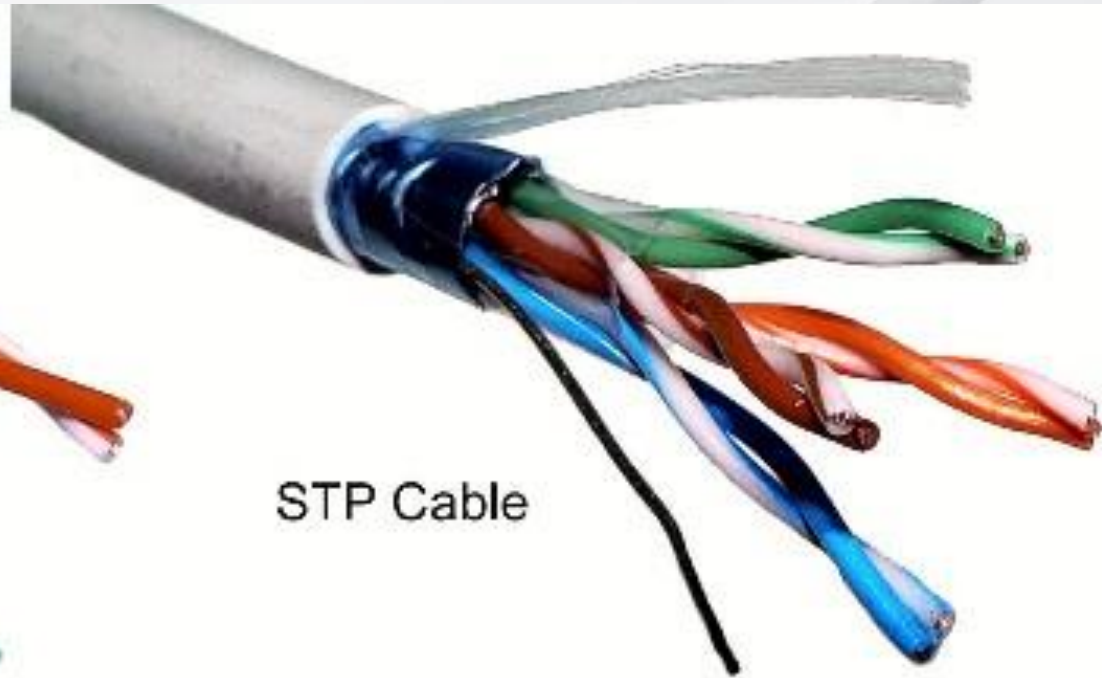
Coaxial Cable



Unshielded Twisted Pair (UTP) VS (STP)



UTP Cable



STP Cable



Fiber Optics



Standard Connector



Lucent Connector

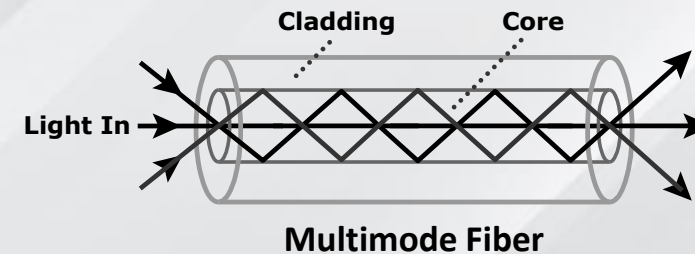
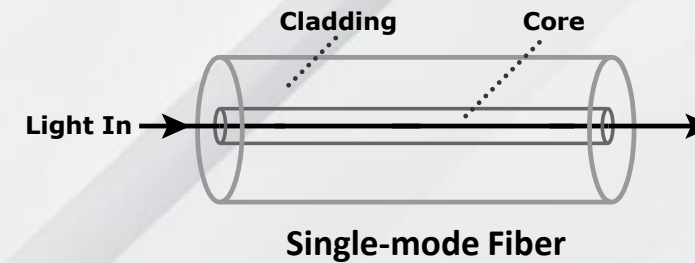


Straight Tip Connector

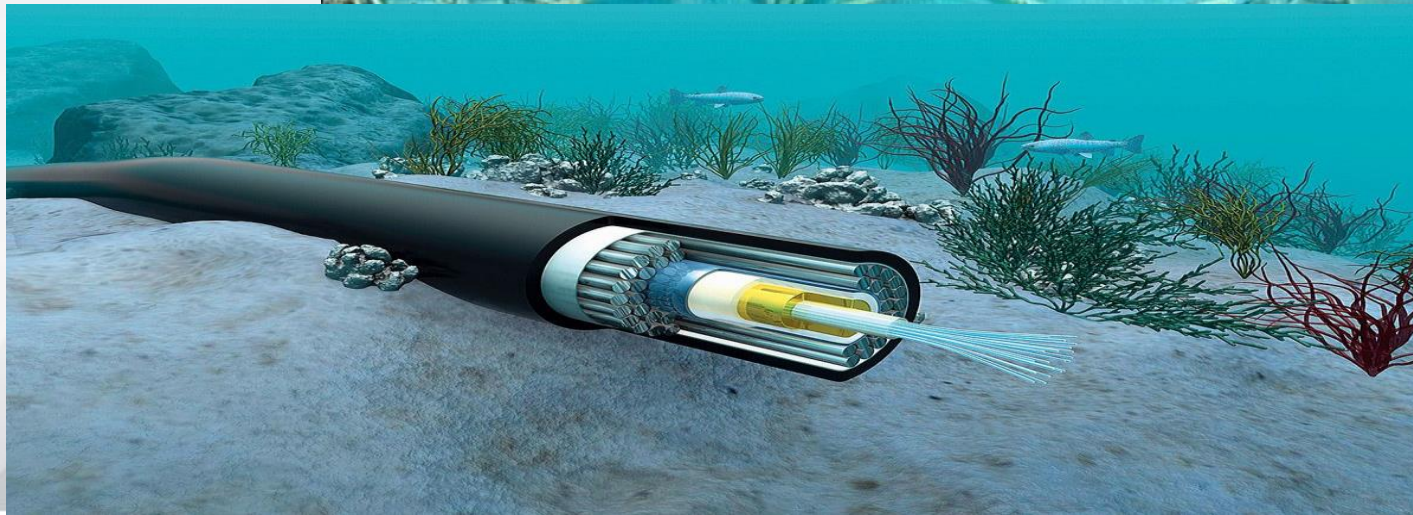
Fiber optics Cables

- Two types of optical cables: single-mode and multimode

Single-mode	Multimode
Carries single beam of light	Can carry multiple beams of light simultaneously
Distance up to 10km	Used for short distance (Modal dispersion weakens signal strength after certain distance)



Fiber Optics



Standard Connector



Lucent Connector



Straight Tip Connector



Connecting Two Devices

Week

02

Cisco Certified Network Associate (CCNA)

Standard (straight)

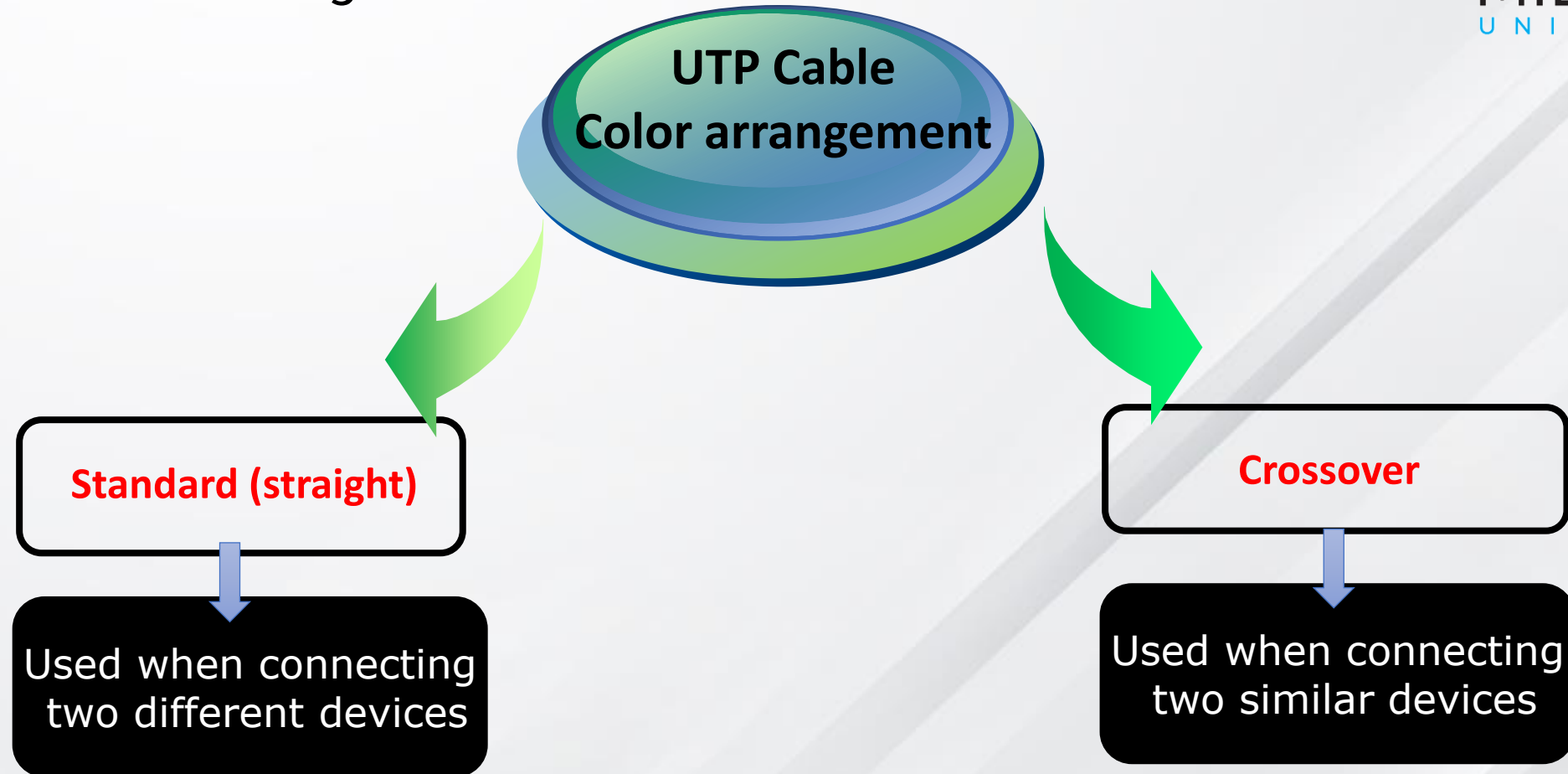
Worange orange wgreen blue wblue green wbrown brown

Crossover

Wgreen green worange blue wblue orange wbrown brown

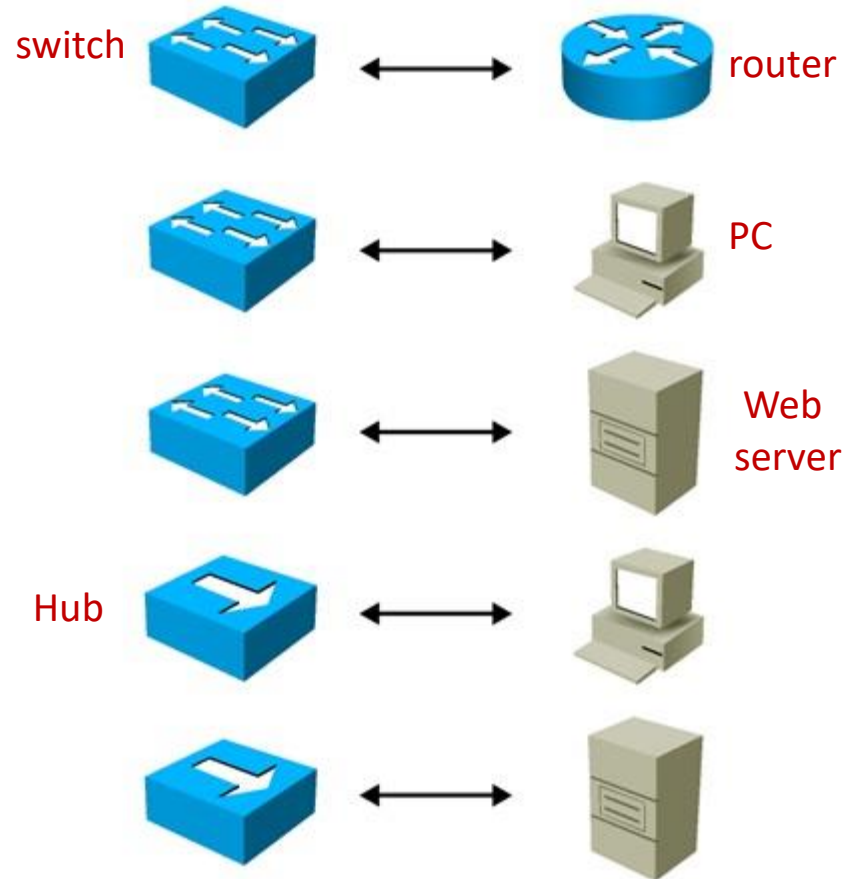
I

Connecting Two Devices



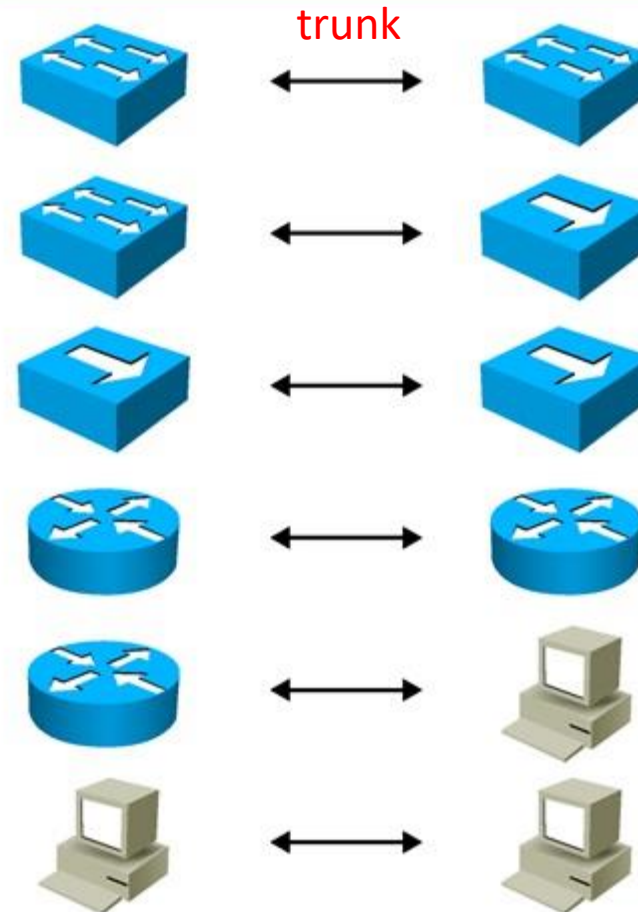
Connecting Two Devices

Straight-Through Cable



Used when connecting
two different devices

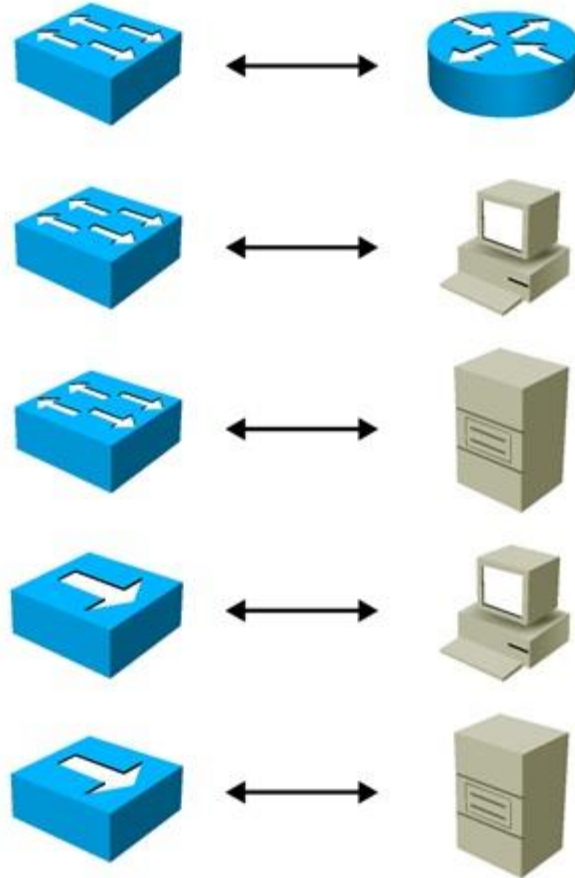
Crossover Cable



Used when connecting
two similar devices

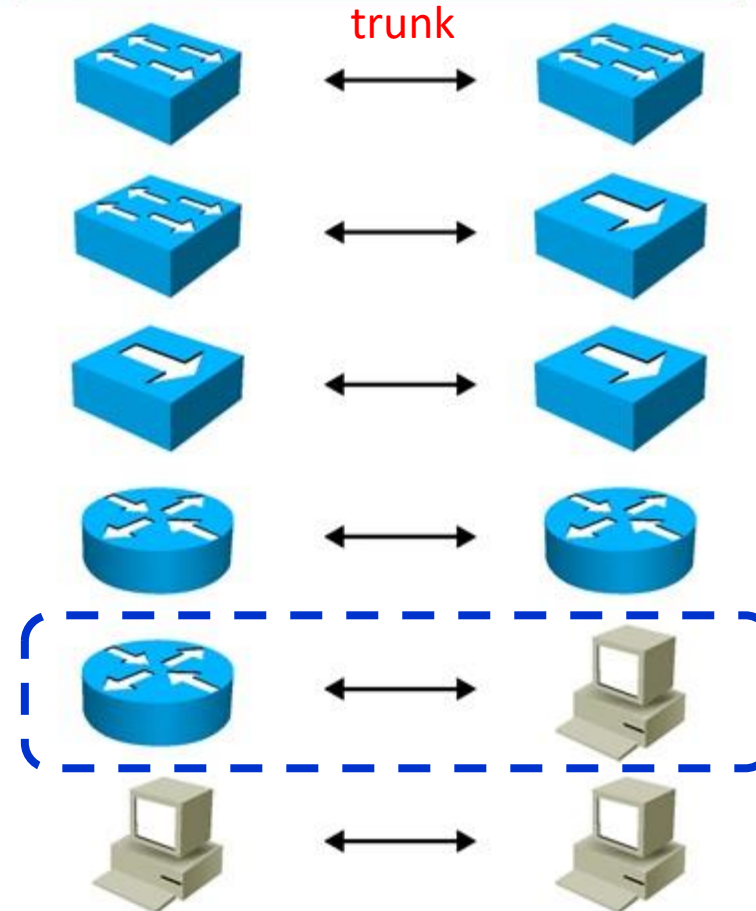
Connecting Two Devices

Straight-Through Cable



Used when connecting
two different devices

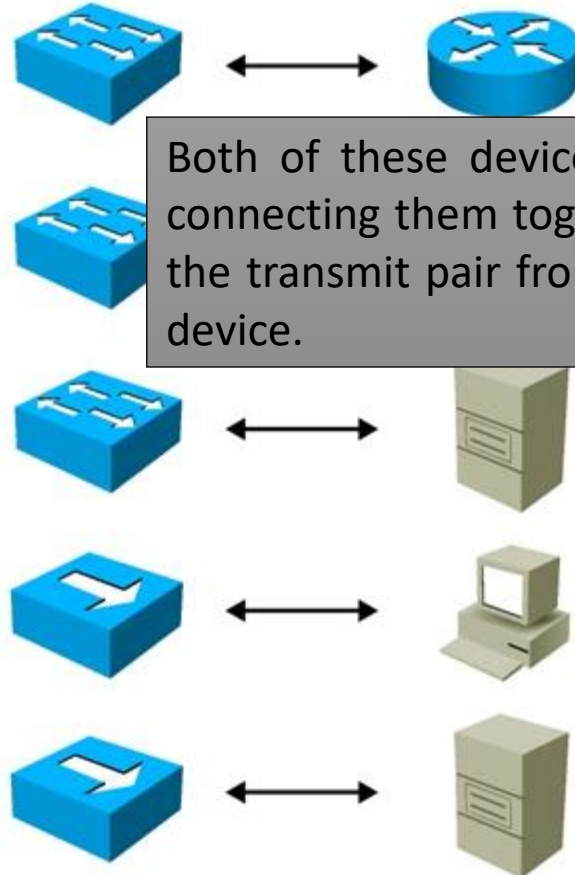
Crossover Cable



Used when connecting
similar

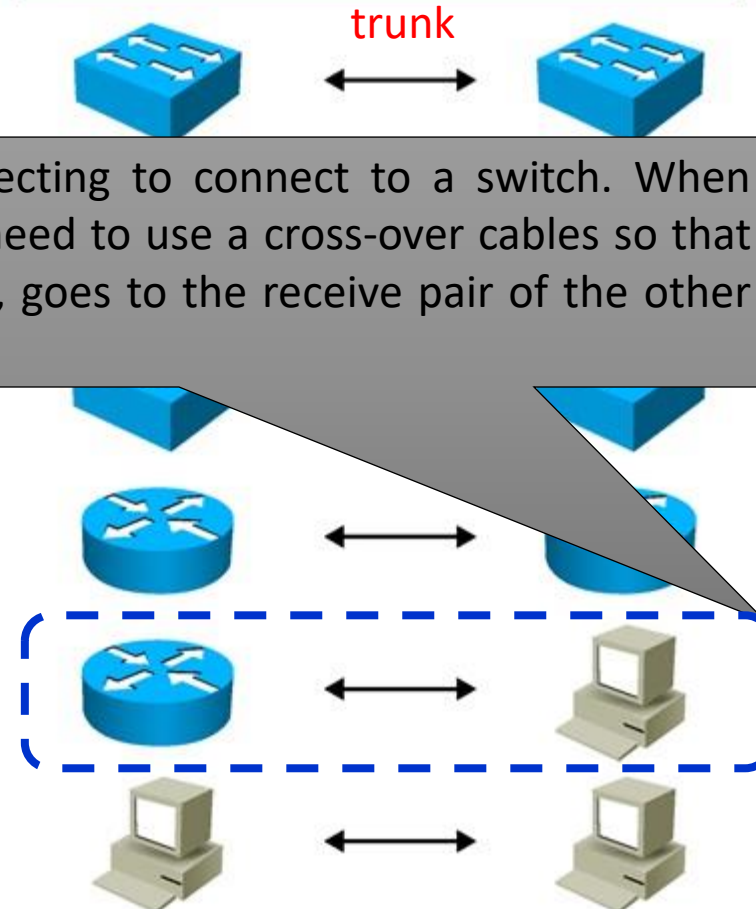
Connecting Two Devices

Straight-Through Cable



Used when connecting
two different devices

Crossover Cable

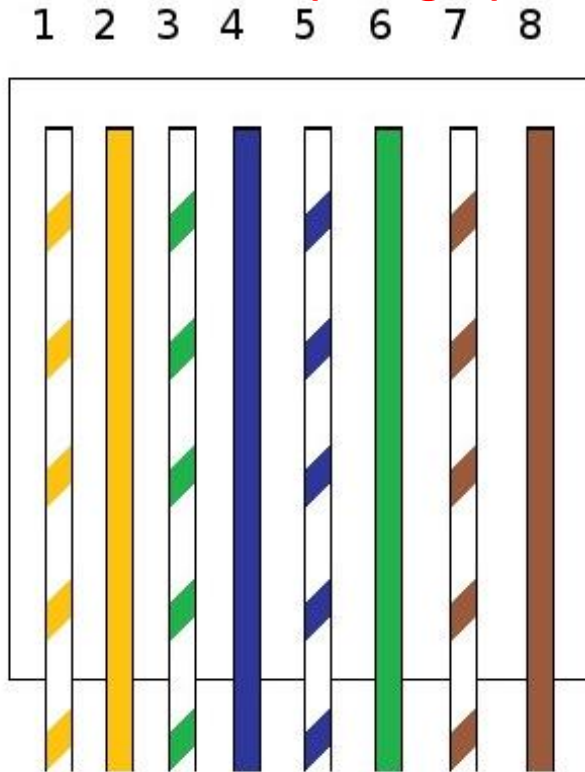


Used when connecting
two similar devices

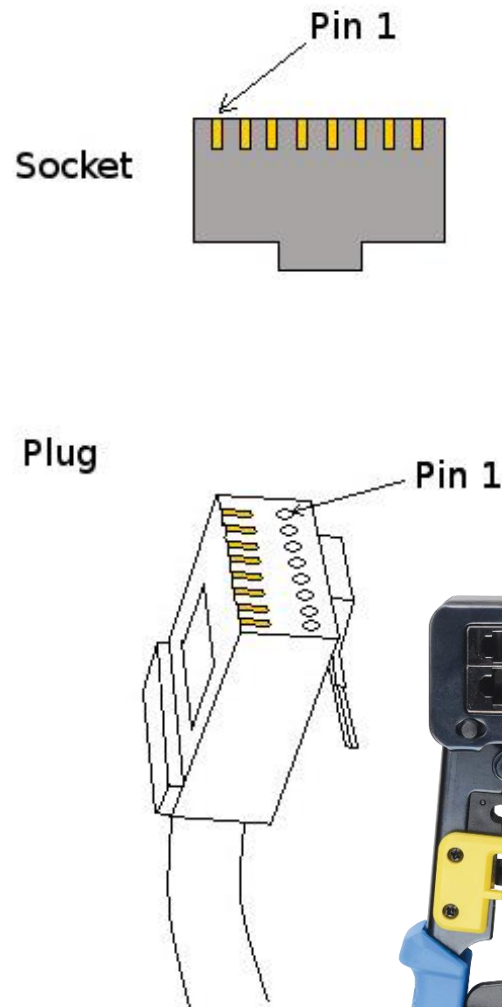
Both of these devices are expecting to connect to a switch. When connecting them together, we need to use a cross-over cables so that the transmit pair from 1 device, goes to the receive pair of the other device.

Connecting Two Devices

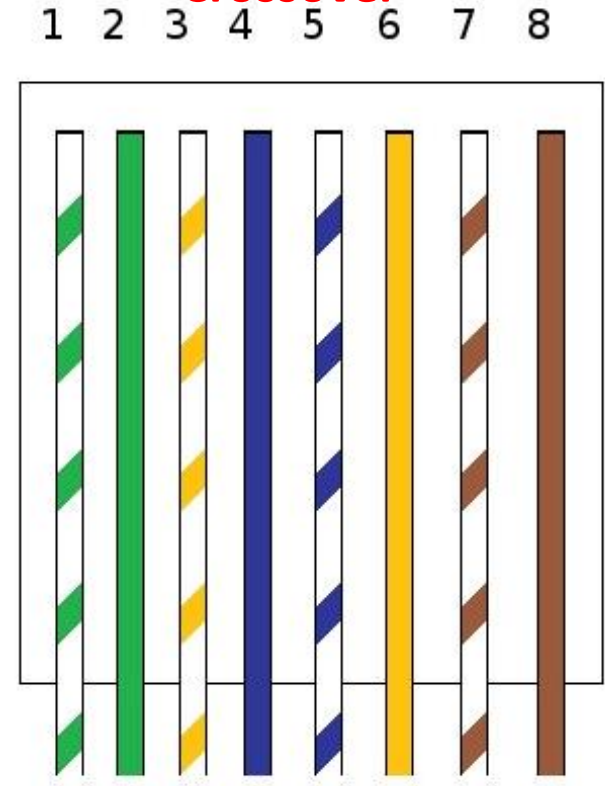
Standard (straight)



T-568B



Crossover



T-568A

Week

02

Cisco Certified Network Associate (CCNA)

Standard (straight)

Worange orange wgreen blue wblue green wbrown brown

Crossover

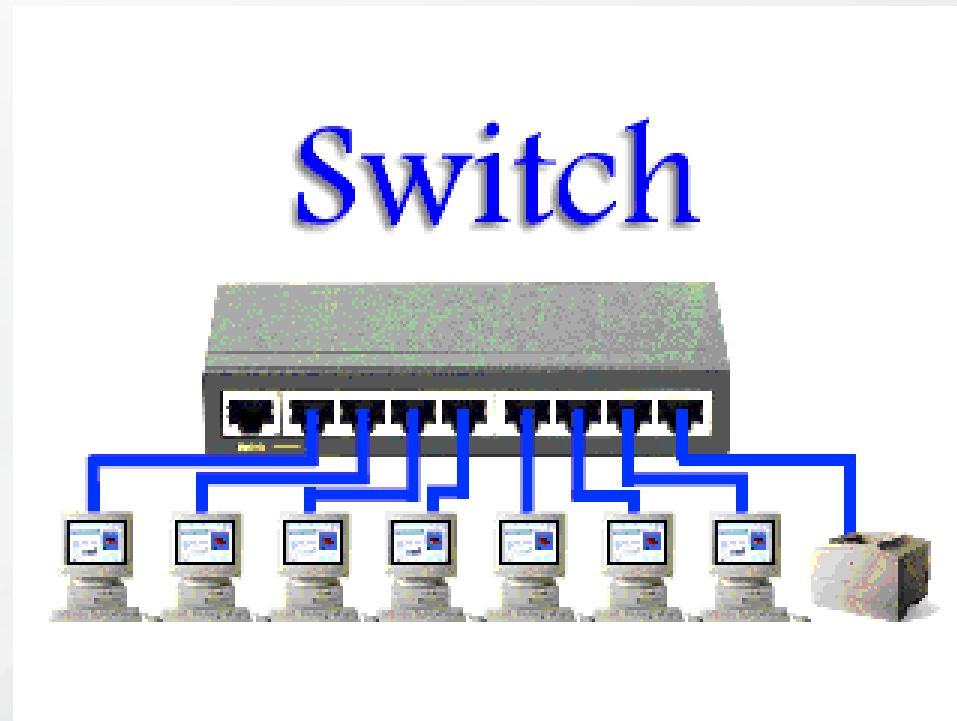
Wgreen green worange blue wblue orange wbrown brown

I

2- Switch

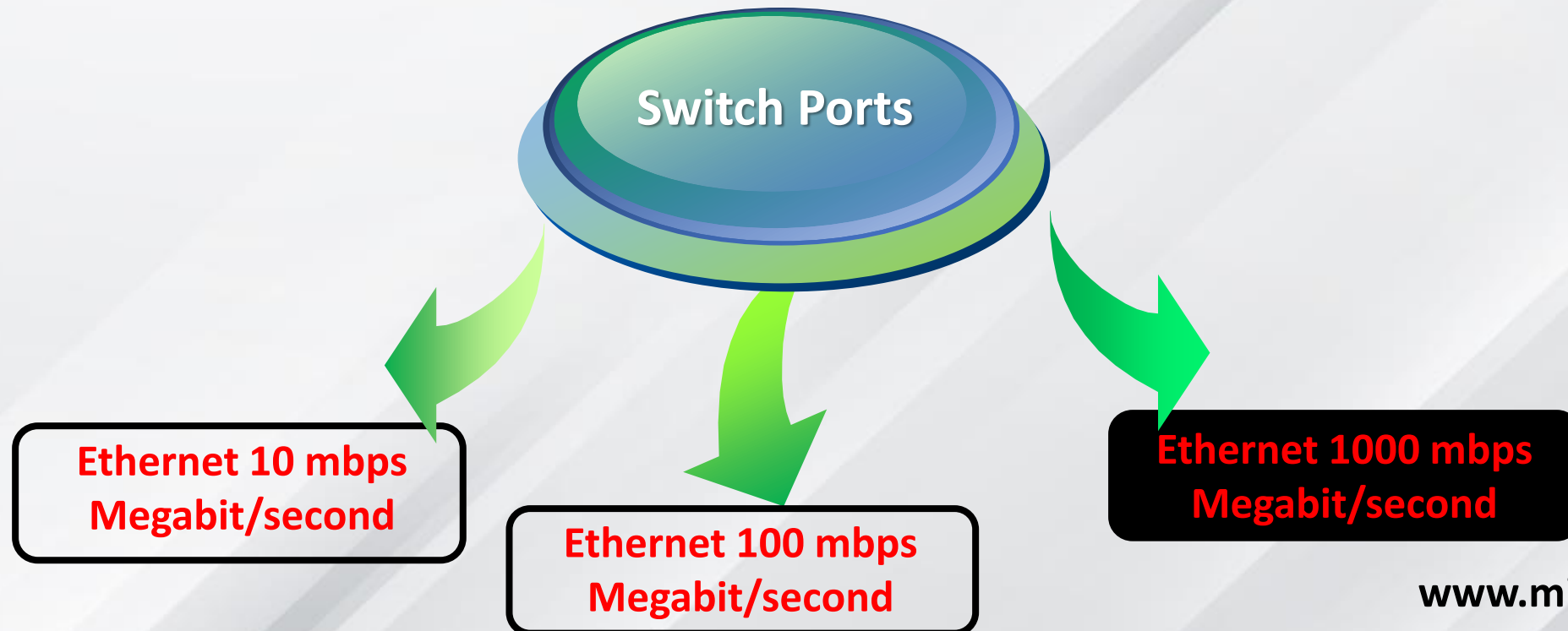


Switch



Switch

- ❑ Each **port** in the switch has a speed
- ❑ **Ports** may be **Ethernet** 10 **mbps** Megabit/second.
- ❑ **Ports** may be **Fast Ethernet** 100 **mbps** Megabit/second.
- ❑ **Ports** may be **Giga Ethernet** 1000 **mbps** Megabit/second.

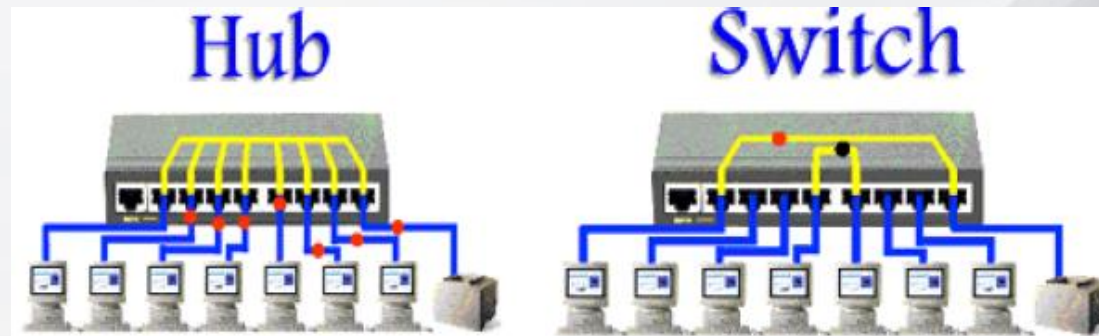


Switch

- Actually you can not differentiate between a hub and a switch once viewed.
- If PC1 to PC6 are connected to a hub. Assume that PC1 wants to send a message to PC4.
- The hub will send the message to all PC's and only PC4 will accept the message while the others will send a message to the hub "the message is not belong to me."

Switch

- Then the **hub** will **send** alert **message** to **PC1** that the **message** is **cancelled** from **PCx**. all the returned **message** will cause a **heavy** on the **network** which we call it a **loop**.



Switch

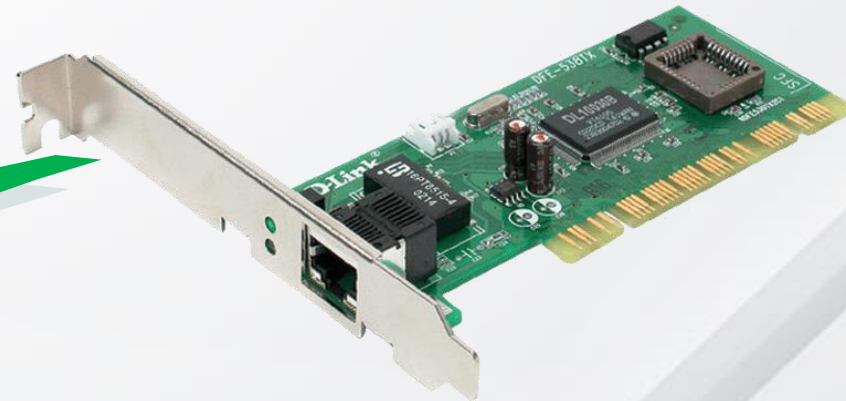
Source		Destination	
PC1	device Address	PC4	device Address

- The **switch** is **smarter** than the **hub**.
- If **PC1** to **PC6** are **connected** to a **switch**. Assume that **PC1** wants to **send** a **message** to **PC4**.
- The **switch** will act as a **hub** “it will **send** the **message** to all **PC’s** and **only PC4** will **accept** the **message** while the others will **send** a **message** to the **hub** “the **message is not** belong to **me**.”
- The **switch** has **flash memory** and a **table** that **save** all **IP address’s** of all the **connected PC’s**.

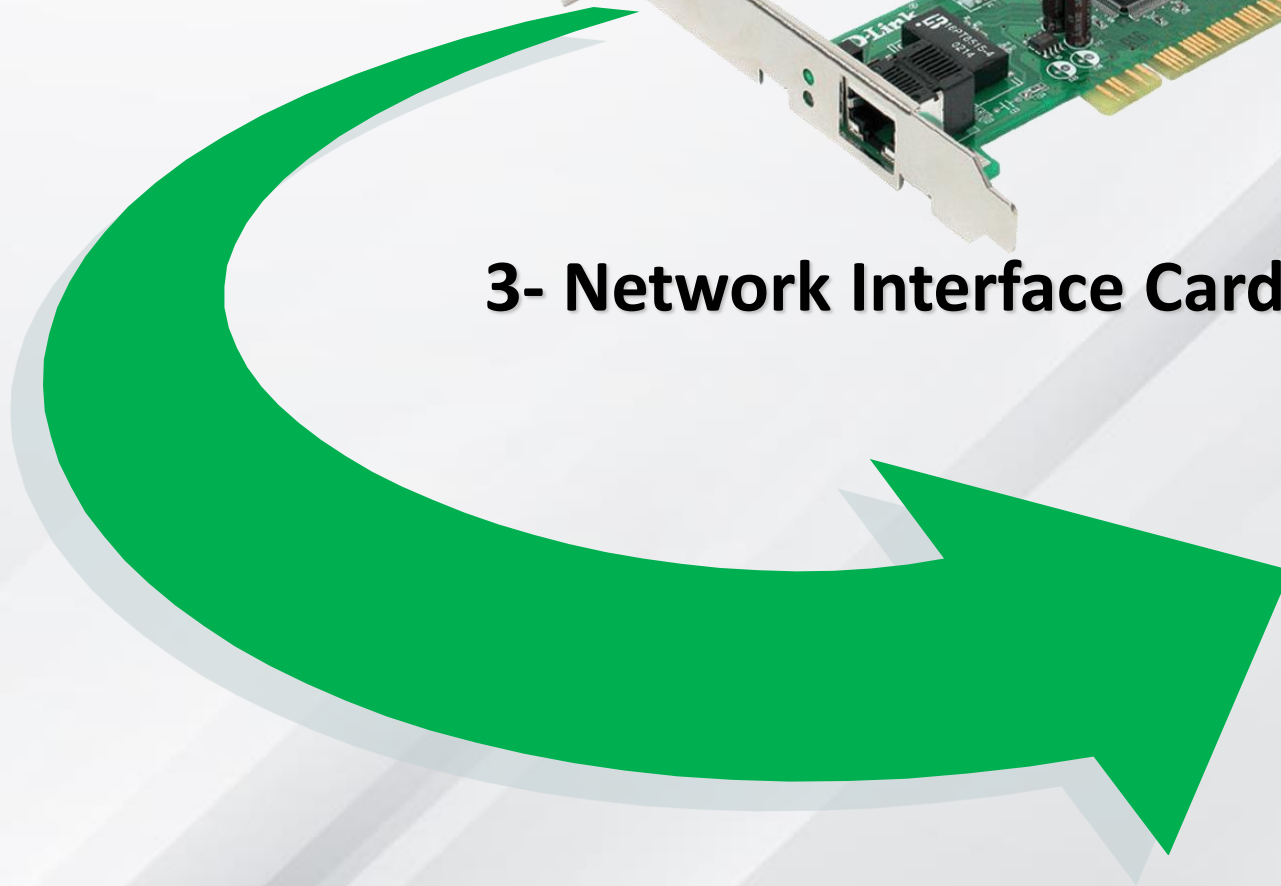
Switch

Source		Destination	
PC1	device Address	PC4	device Address

- Then the **switch** will **register PC4 address** in the **destination** when it **does not receive** any **message** from it.
- After that the **switch** will **send** all the **data** from **PC1** directly to **PC4 address without sending** it to the others.
- The **switch** will **reduce** the **loop** on the **network** but **not** prevent it.



3- Network Interface Card (NIC)

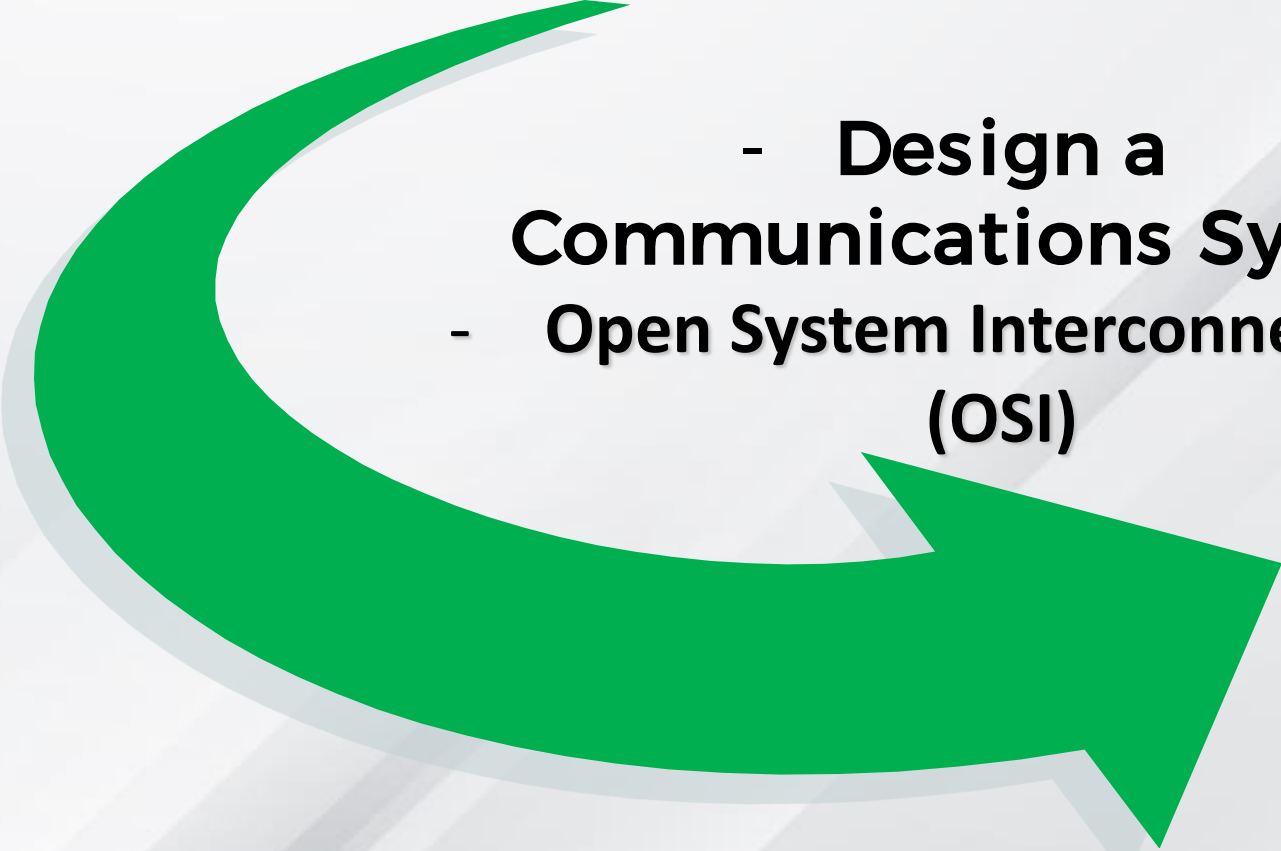


Network Interface Card

- A NIC, or LAN adapter, provides the physical connection to the network at the PC or other end device.
- The media that are connecting the PC to the networking device, plug directly into the NIC.
- Physical Port - A connector or outlet on a networking device where the media is connected to an end device or another networking device.

Network Interface Card

- **Interface** - Specialized ports on a networking device that connect to individual networks.
- Because routers are used to interconnect networks, the ports on a router are referred to as network interfaces.
- Note: Often, the terms port and interface are used interchangeably.

- 
- Design a
Communications System
 - Open System Interconnection
(OSI)

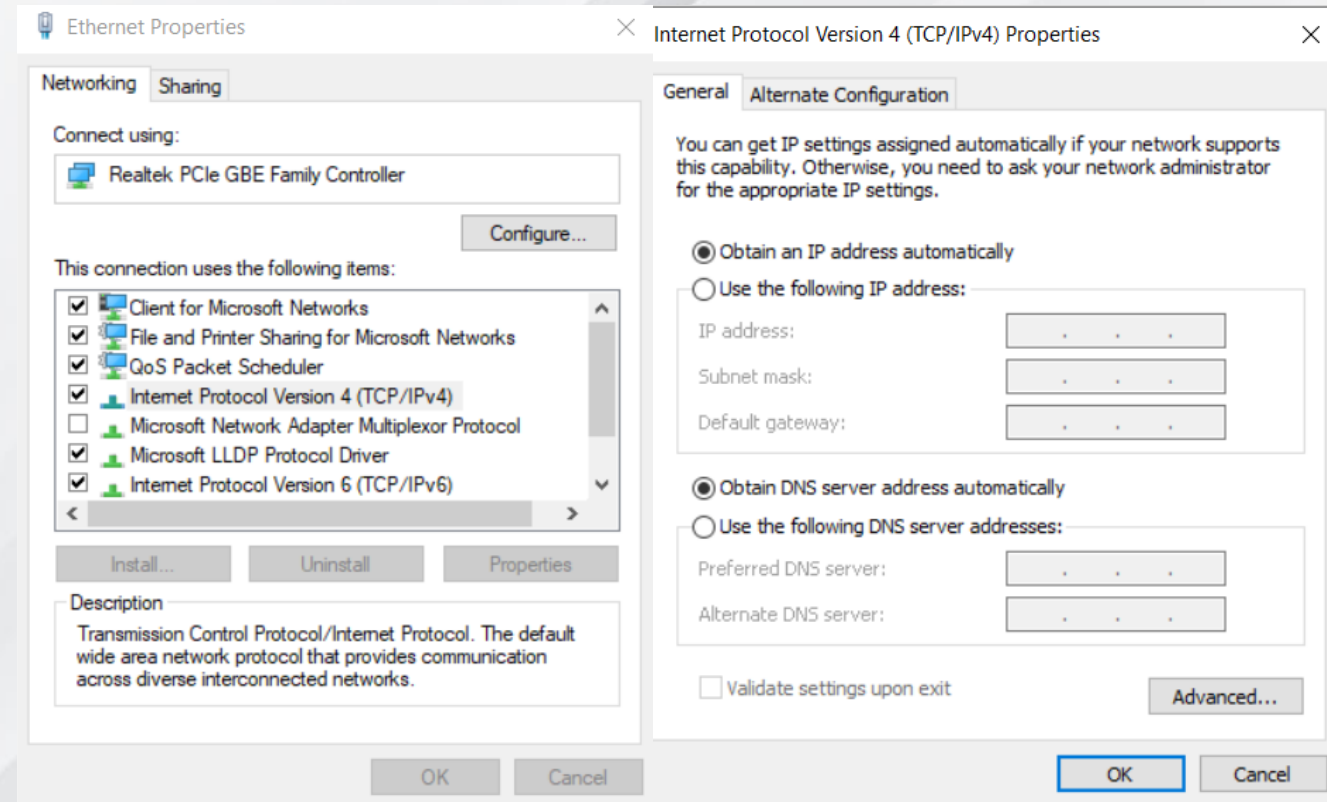
Design a Communications System

Design a Communications System

Objectives:

- Explain the role of protocols and standards organizations in facilitating interoperability in network communications.

1. IP Addressing & Subnet Mask
2. Protocol
3. Port



Week

02

IP Address and Subnet Mask Overview

- An IP (Internet Protocol) address is a numerical label assigned to each device connected to a computer network.
- Purpose: Identifying and locating devices on a network.
- Format: IPv4 addresses are typically written as four sets of numbers separated by dots (e.g., 192.168.1.1).

Subnet Mask Overview

- Definition: A subnet mask is a 32-bit number that divides an IP address into network and host portions.
- Purpose: Determines the network and host parts of an IP address.
- Format: Similar to an IP address, written in the same dotted decimal format (e.g., 255.255.255.0).

● Media Access Control (MAC) Address

A unique identifier assigned to a network interface controller for use as a network address in communications within a network segment. No two devices can have the same MAC address in the same local network; otherwise, an address conflict occurs. Example: 00-13-02-1F-58-F5

The first 3 bytes (24 bits) of the address denote the vendor

● Internet Protocol (IP) Address A unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.

An IP address is a string of numbers separated by periods (.) or colons (:)

Versions of IP Address:

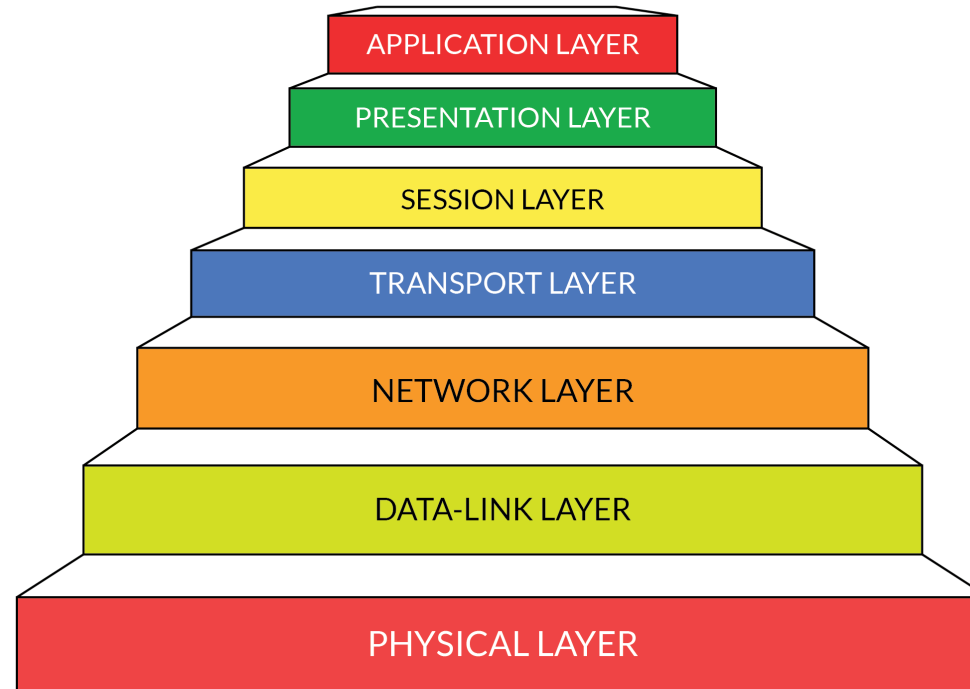
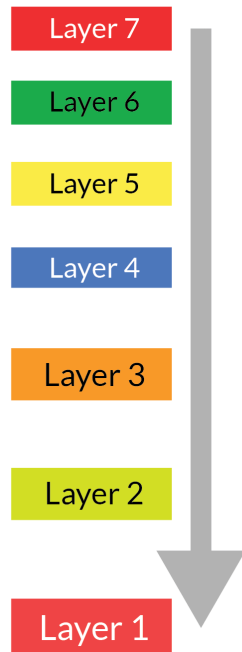
- IPV4 , ex: 192.168.1.1
- IPV6, ex: 1050:0:0:0:5:600:300c:326b

Protocols and Ports

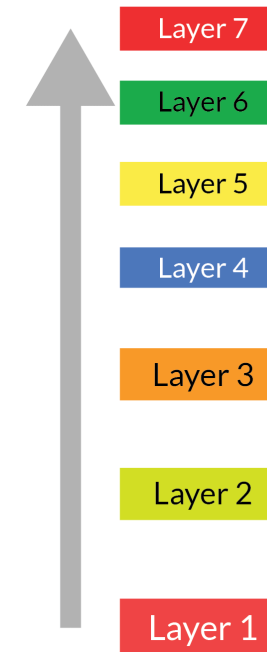
Port Number	Protocol
20, 21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet Protocol
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	HyperText Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
137	NetBIOS Name Service
143	Internet Message Access Protocol (IMAP4)
443	Secure HTTP (HTTPS)
445	Microsoft-DS (Active Directory)

OSI MODEL

Client Side



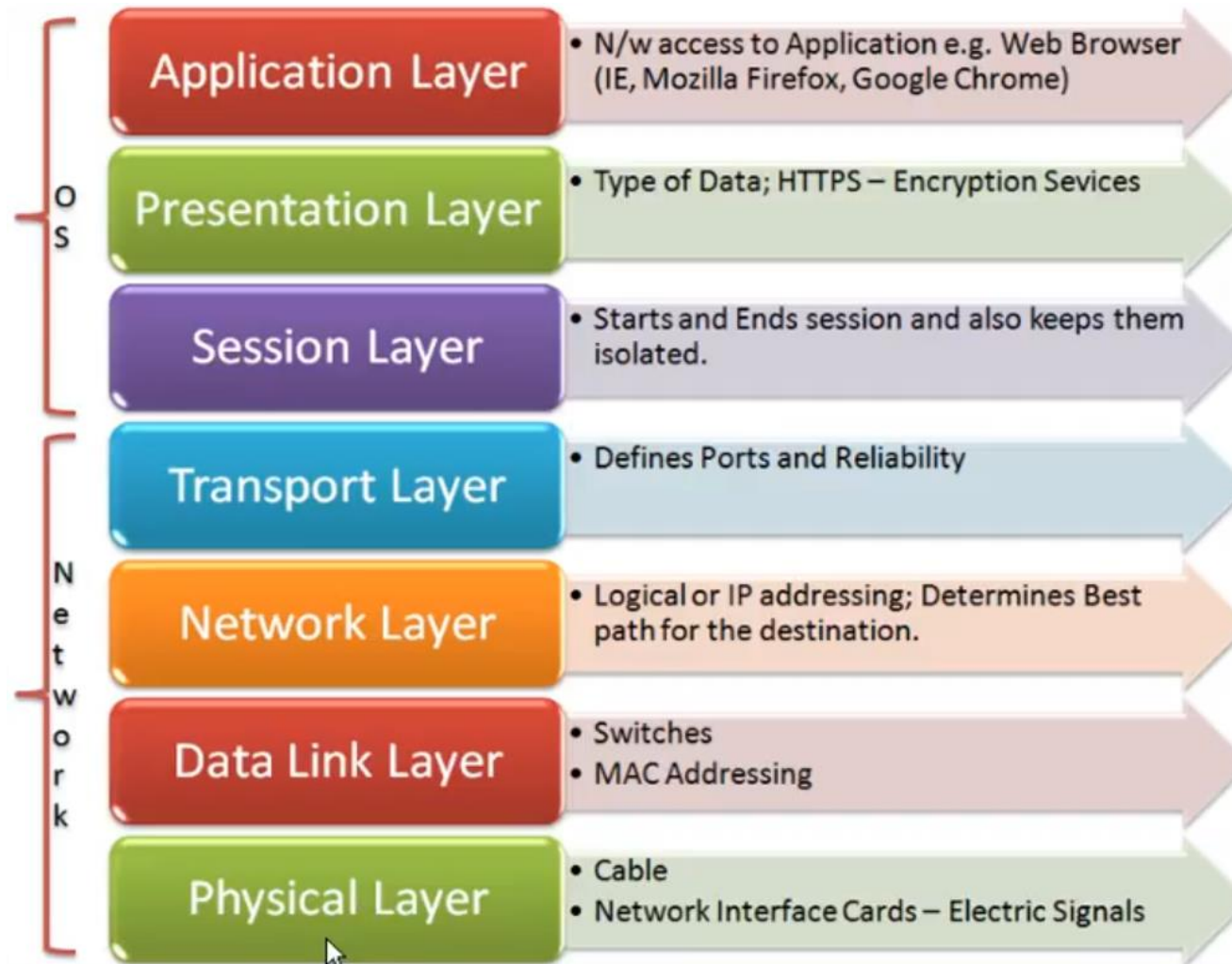
Server Side

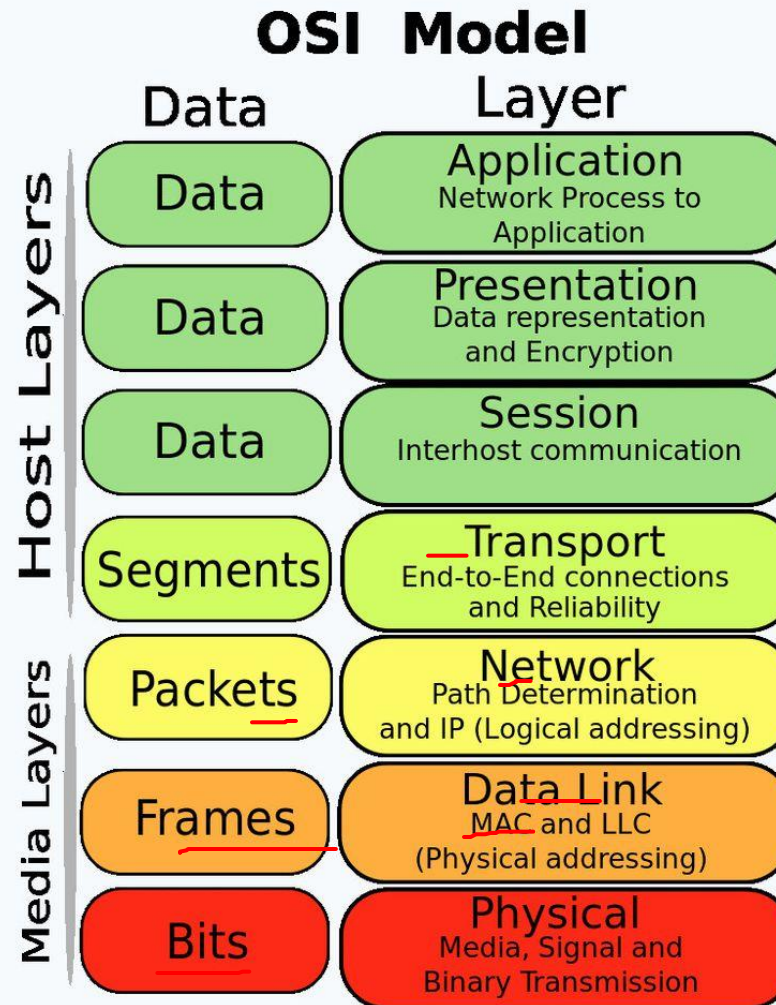


OSI Layers

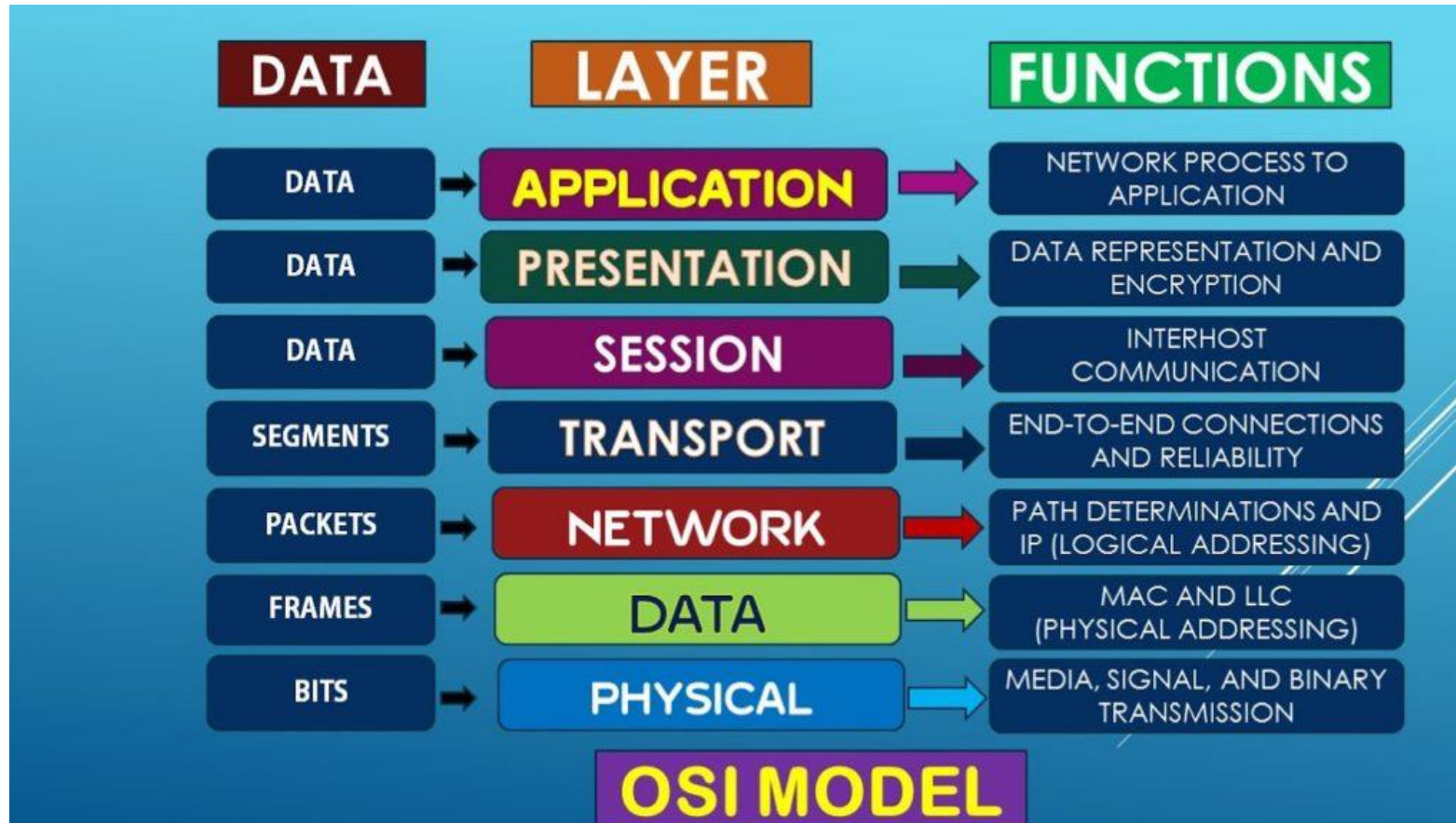
7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

OSI Layers





OSI Layers



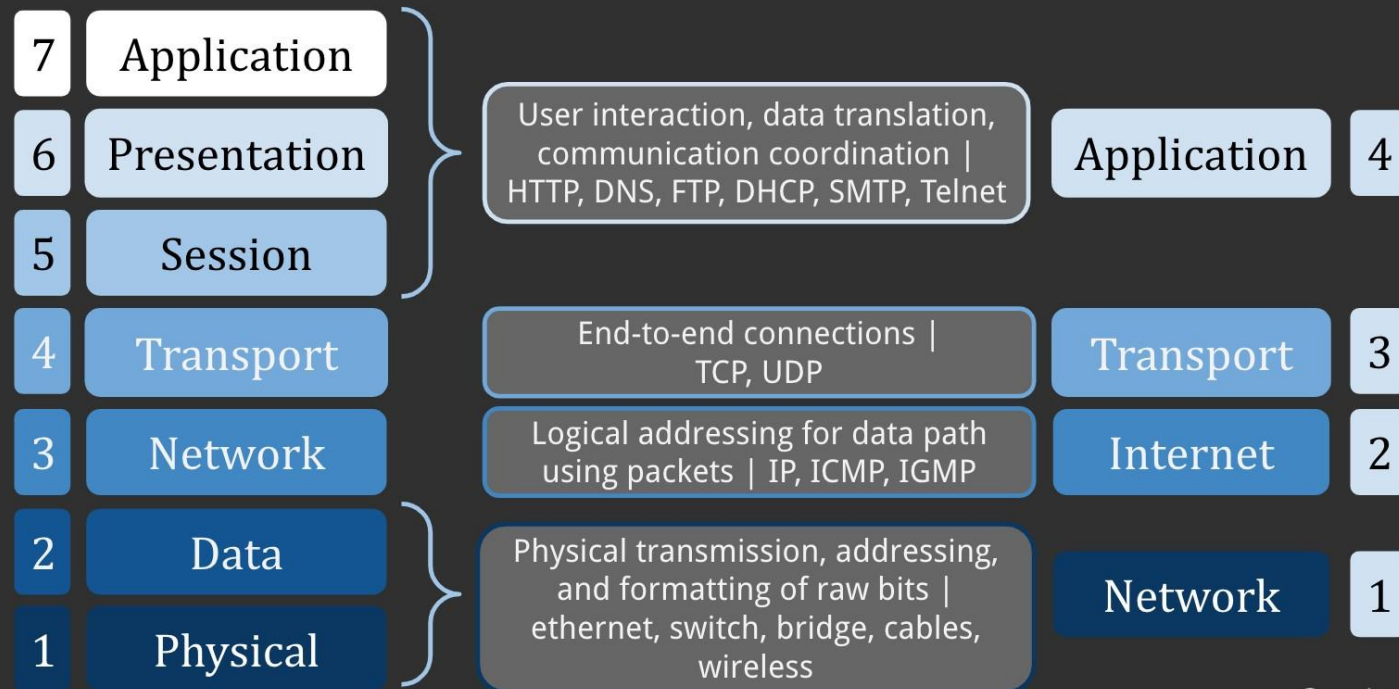
OSI Layers

<https://blueteamresources.blogspot.com/2022/01/osi-model.html>

OSI Layer	Functions	Devices	Protocols	Protocol Data Unit	Attacks	Mitigations
7. Application	Responsible for creating the data for the packets. Acts as the interface between the user and the network.	PC, Phone, Server, Host Firewall, NIPS, HIPS, WAF, Gateways	HTTP, SMTP, FTP, DNS, SNMP, Telnet, DHCP, POP3, IMAP	Data	Exploit (malware), DDoS, HTTP Floods, SQL injection, Cross-site Scripting	Use WAF and Secure Gateways (web), Application Monitoring, AV.
6. Presentation	Data is translated, compressed, encoded, encrypted (if enabled) in such a way that the receiving application can understand and can be transported over the network	-	JPEG, MP3, SSL, TLS	Data	Phishing, SSL Hijacking, Encryption Downgrade, Decryption attacks.	Keeping AV and signatures up-to-date, SSL offloading and inspection.
5. Session	Establishment, maintenance, encryption, security, and termination of sessions is handled by this layer.	Circuit Level Gateway	NetBIOS, RPC, SMB	Data	Session Hijacking, Man-in-the-Browser	Vulnerabilities should be patched.
4. Transport	Responsible for end-to-end communication (process-to-process) and for error and flow control of segments.	Gateways, Firewall, NIPS	TCP, UDP	Segments-TCP, Datagram-UDP	Reconnaissance such as Host Discovery, Port Scanning, TCP/UDP Flood, and UDP Amplification.	Use Firewall, IPS, detect based on Thresholds and block at ISP level.
3. Network	Creates a routing path for packet delivery for devices in different networks and can also select between routing paths.	Router, N/W Firewall, NIPS	IP, ICMP, RIP, OSPF, IPsec	Packets	Man-in-the-middle (MITM), IP Spoofing, ICMP Attacks, Smurf Attack, Packet Sniffing.	Use Firewall, IPS (Packet Filtering), Enable logging, Encrypt Traffic, Configure Routers.
2. Data Link	Responsible for delivery to and from hosts on local network through communication media. Also does framing, error and flow control. Consists of LLC and MAC sub-layers	Switch, Bridge, NIC.	ARP, ATM, MAC, VLAN, PPP, PPTP	Frames	ARP Spoofing, MAC Cloning, DoS, VLAN Hopping.	Configure Switches, Port locking or Port Level Security, Static ARP.
1. Physical	It acts as the communication media and responsible for the actual physical communication between devices.	Hubs, Cables, Modems, Repeaters.	802.11, Ethernet BASE	Bits	Data Sniffing, Unauthorized access, Physical Damage.	Access Control, Tracking/Securing Physical Assets.

Network Layers Models

7-layer OSI Model vs. 4-layer TCP/IP Model



@varcharr



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

