

BERITECK

# COMPUTER NETWORKS



# NETWORK DEVICES

BERITECK

They are physical devices that allow hardware on a computer network to communicate and interact with one another.

# REPEATER

BERITECK

– A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network.



# HUB

BERITECK

A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches



# SWITCH

BERITECK

A switch is a data link layer device with multiple ports to connect other network devices. It operates with MAC Addresses

MAC address lookup → <https://maclookup.app/>



# ROUTERS

BERITECK

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device.



BERITECK

# TYPES OF NETWORK



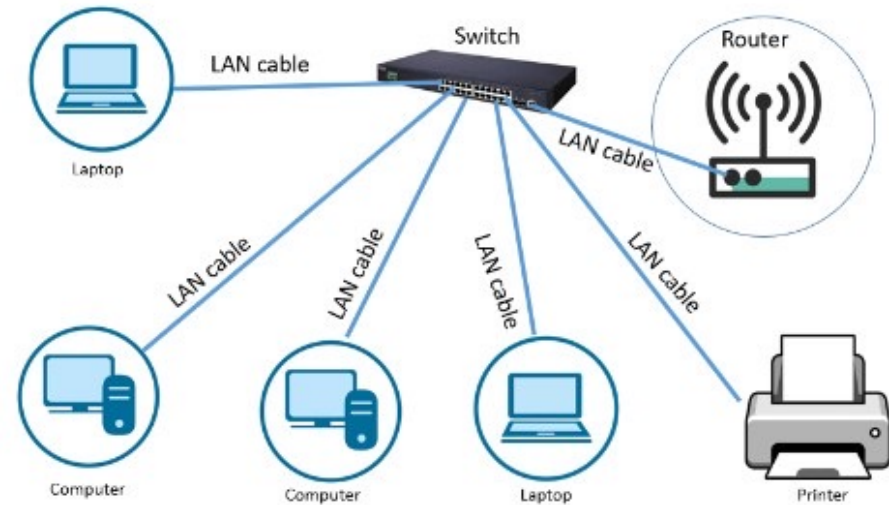


# LAN – LOCAL AREA NETWORK

BERITECK

## LAN (local area network):

A LAN connects computers over a relatively short distance, allowing them to share data, files, and resources. For example, a LAN may connect all the computers in an office building, school, or hospital. Typically, LANs are privately owned and managed.



Local Area Network

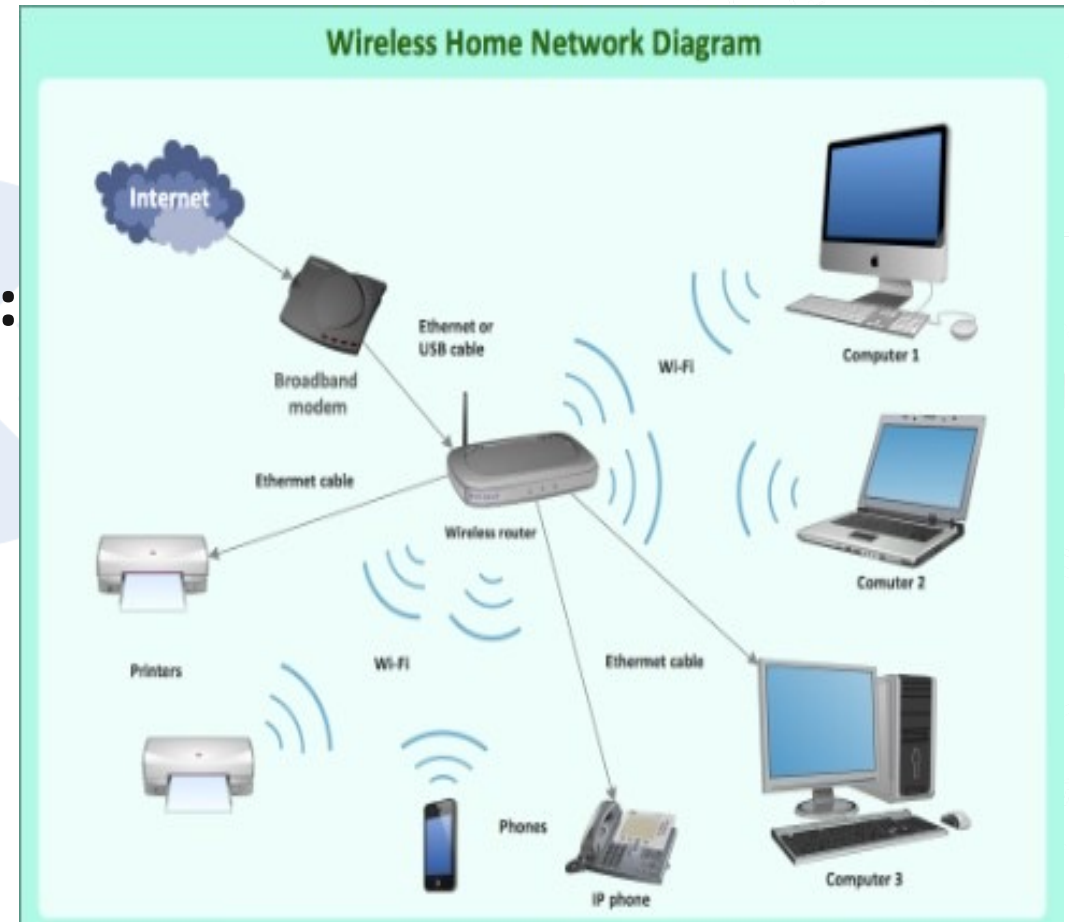


# WLAN – WIRELESS LOCAL AREA NETWORK

BERITECK

## WLAN (wireless local area network):

A WLAN is just like a LAN but connections between devices on the network are made wirelessly.

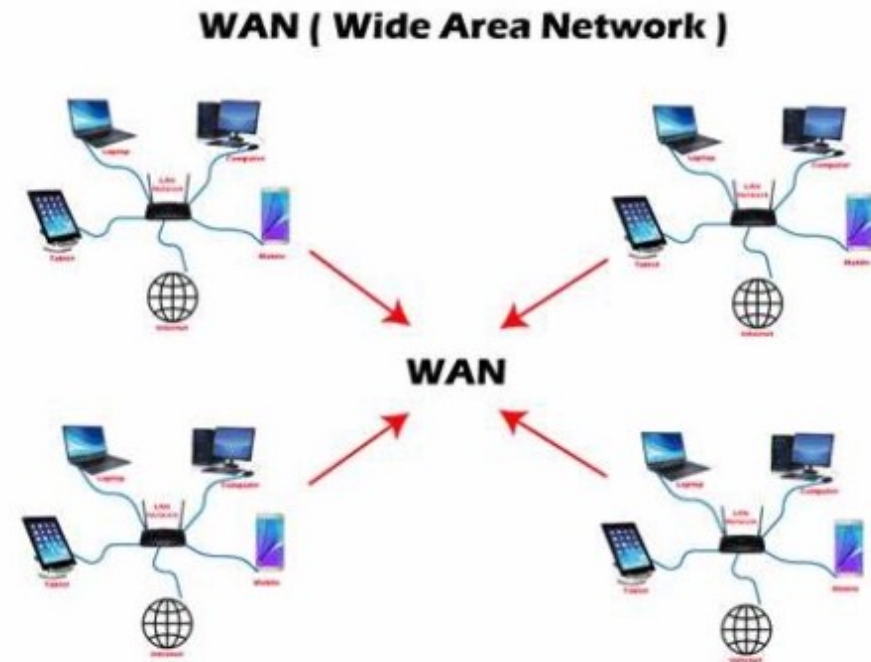


# WAN – WIDE AREA NETWORK

BERITECK

## WAN (wide area network):

As the name implies, a WAN connects computers over a wide area, such as from region to region or even continent to continent. The internet is the largest WAN, connecting billions of computers worldwide. You will typically see collective or distributed ownership models for WAN management.

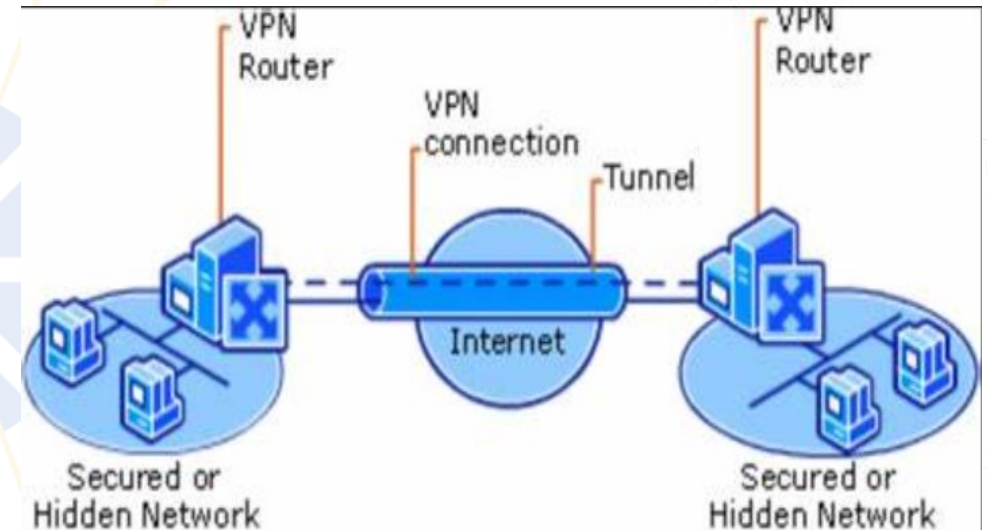


# VPN – VIRTUAL PRIVATE NETWORK

BERITECK

## VPN (virtual private network):

A VPN is a secure, point-to-point connection between two network end points (see 'Nodes' below). A VPN establishes an encrypted channel that keeps a user's identity and access credentials, as well as any data transferred, inaccessible to hackers.



# NETWORK PROTOCOLS

BERITECK

A network protocol is a **set of rules** and conventions that govern how data is transmitted, received, and processed across a computer network.



BERITECK

Network protocols ensure that devices can **communicate** with each other **effectively**, even if they are manufactured by different vendors or run on different operating systems.



BERITECK

Each protocol serves a **specific purpose**, such as data transmission, addressing, error detection and correction, security, and more.

# EXAMPLES OF PROTOCOLS

BERITECK

Transmission Control Protocol (**TCP**): A reliable, connection-oriented protocol that ensures data packets are delivered in the correct order and without errors. It is commonly used for applications like web browsing, email, and file transfer.



# IP

BERITECK

Internet Protocol (**IP**): A fundamental protocol that provides the addressing and routing mechanisms required for data packets to be sent and received across networks. IP is used in conjunction with other protocols like TCP or UDP.

# UDP

BERITECK

User Datagram Protocol (**UDP**): A connectionless, lightweight protocol that provides a faster but less reliable way to transmit data packets. It is commonly used for applications like **real-time streaming, online gaming, and VoIP.**

# HTTP

BERITECK

Hypertext Transfer Protocol (**HTTP**): The protocol used for transferring web pages and other resources on the World Wide Web. It governs how web browsers and web servers communicate.

# SMTP

BERITECK

Simple Mail Transfer Protocol (**SMTP**): The protocol used for sending and receiving email messages between mail servers.

# FTP

BERITECK

File Transfer Protocol (**FTP**): A protocol used for transferring files between a client and a server on a network.

# HTT

# P

BERITECK

The **Hypertext Transfer Protocol (HTTP)** is the foundation of the World Wide Web and is used to load webpages using hypertext links.

# REMOTE ACCESS PROTOCOL

BERITECK

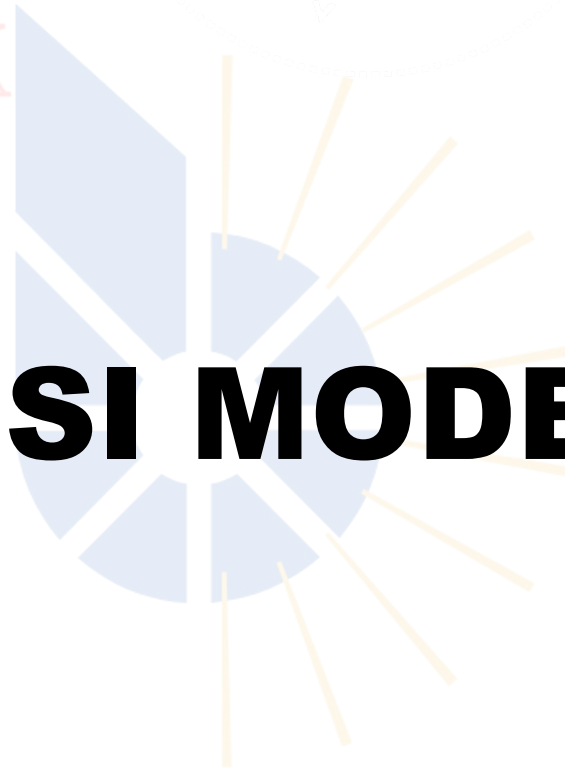
**Telnet** → NOT reliable and in cleartext

**SSH** → Reliable and encrypted



BERITECK

# THE OSI MODEL



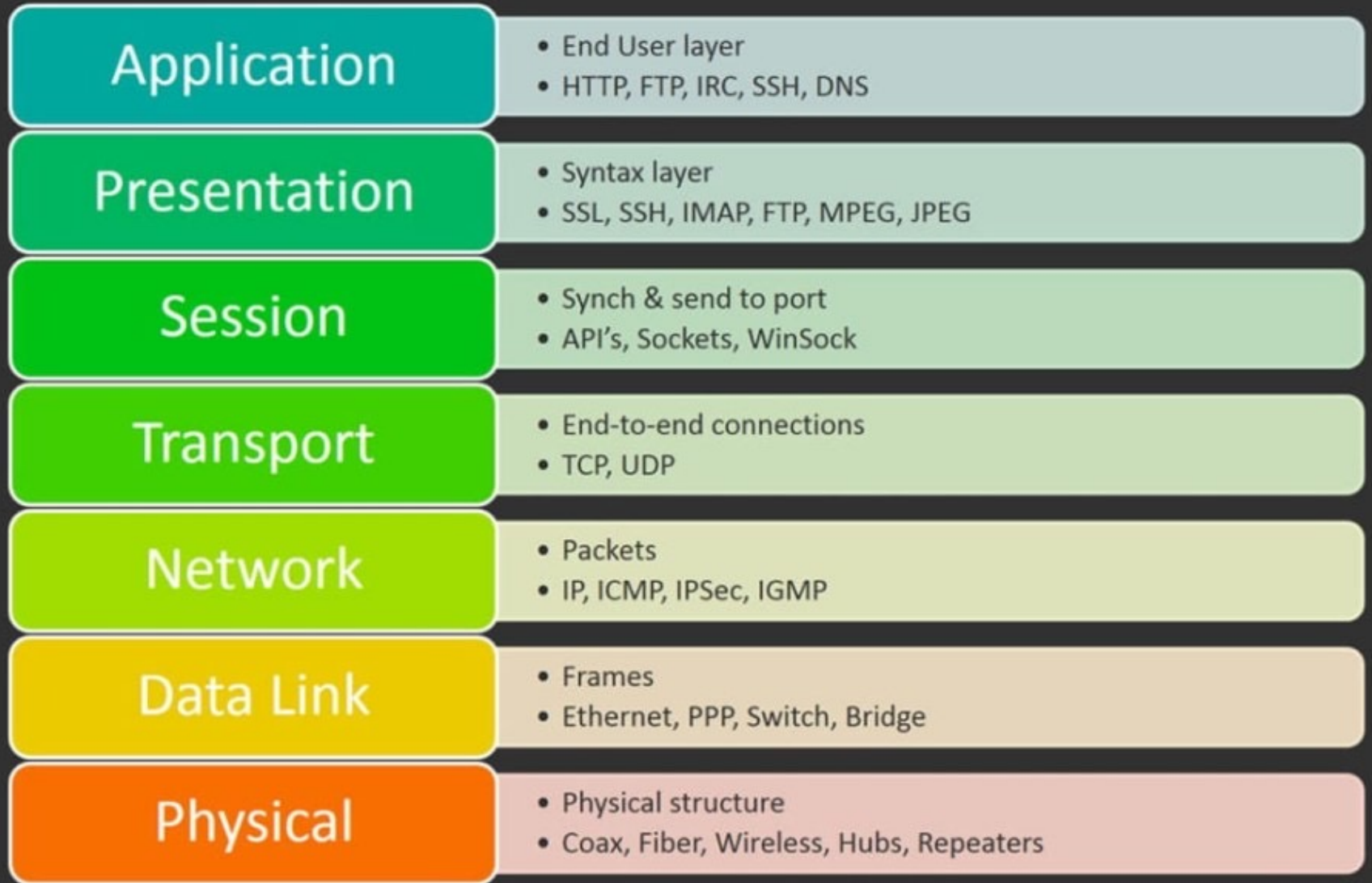
# THE OSI MODEL

## OPEN SYSTEMS INTERCONNECTION MODEL

The **OSI model** describes **7 layers** that computer systems use to communicate over a network.



# 7 Layers of the OSI Model



ALL

AWAY

PEOPLE

PIZZA

SEEM

SAUSAGE

TO

THROW

NEED

NOT

DATA

DO

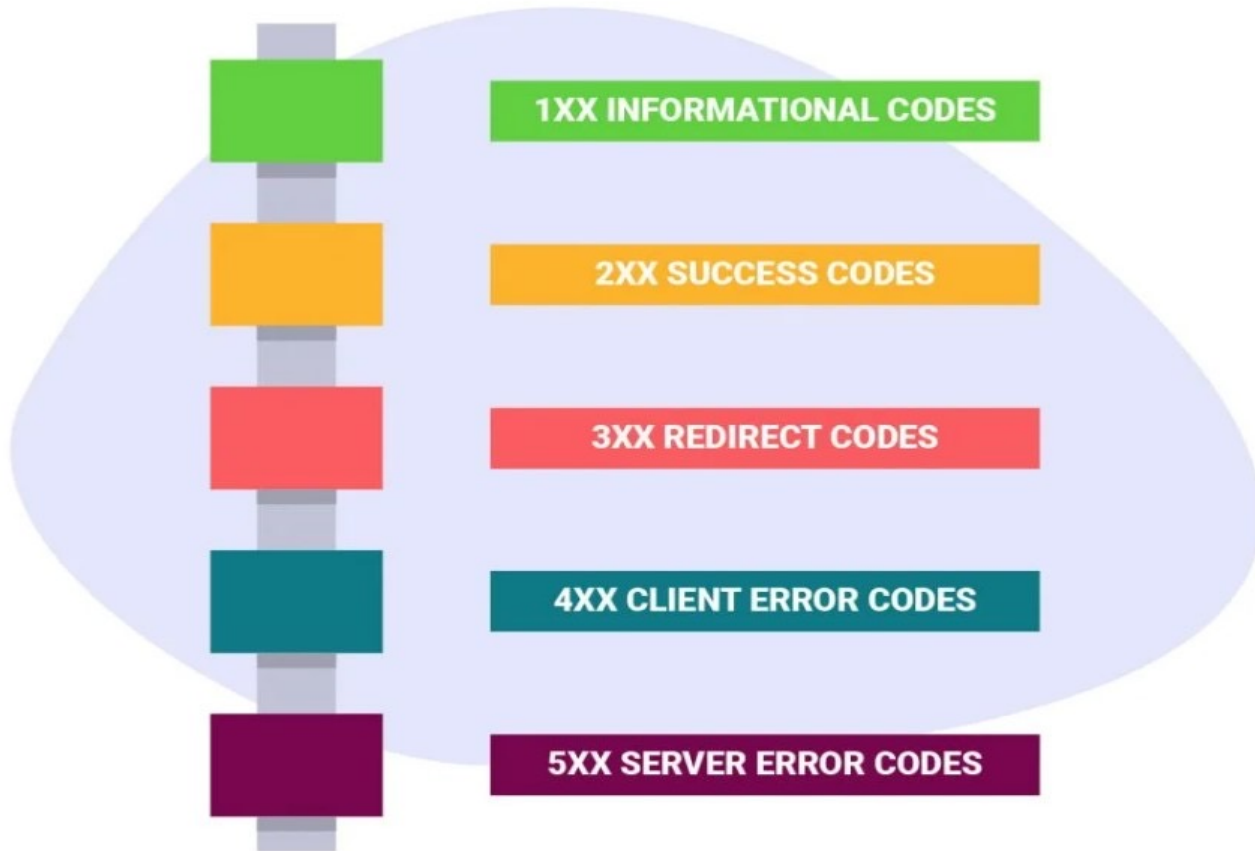
PROCESSING

PLEASE

BE

# HTTP STATUS CODE

## HTTP Status Codes



## HTTP Status Codes

### Level 200

200: OK  
201: Created  
202: Accepted  
203: Non-Authoritative Information  
204: No content

### Level 400

400: Bad Request  
401: Unauthorized  
403: Forbidden  
404: Not Found  
409: Conflict

### Level 500

500: Internal Server Error  
501: Not Implemented  
502: Bad Gateway  
503: Service Unavailable  
504: Gateway Timeout  
599: Network Timeout

## **NOTE**

BERITECK

The combination of various protocols in a network architecture ensures efficient and secure communication between devices and systems across the internet and other networks.