BY NADIA SCHUTZ

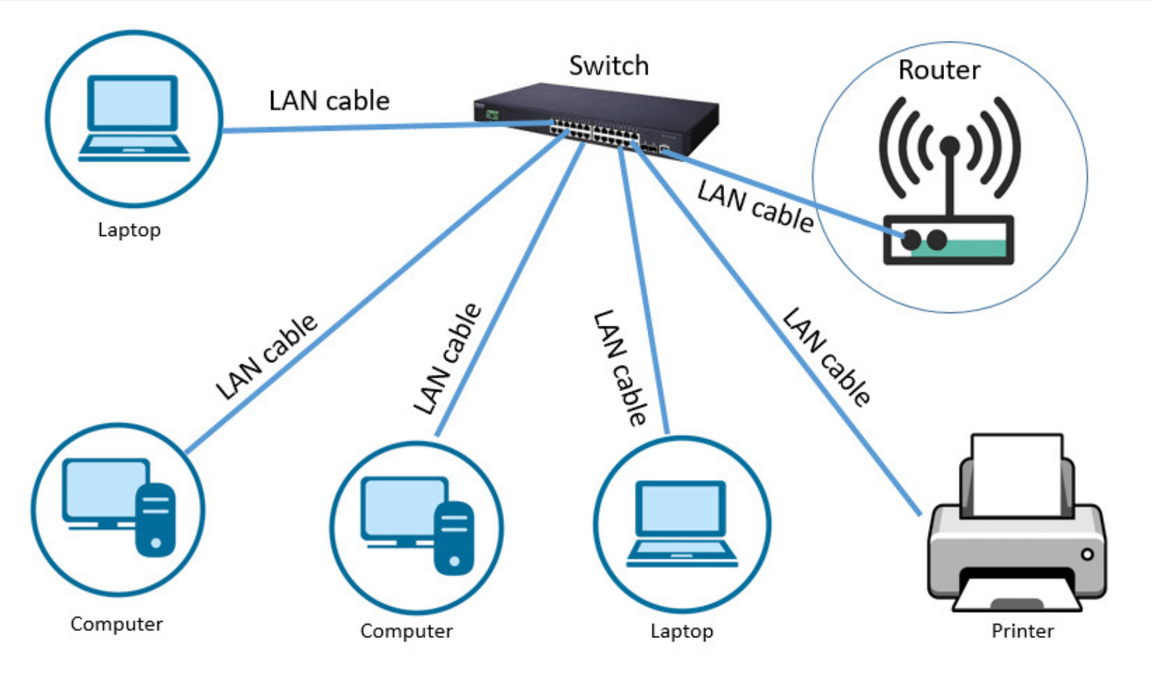
PENETRATION TESTING

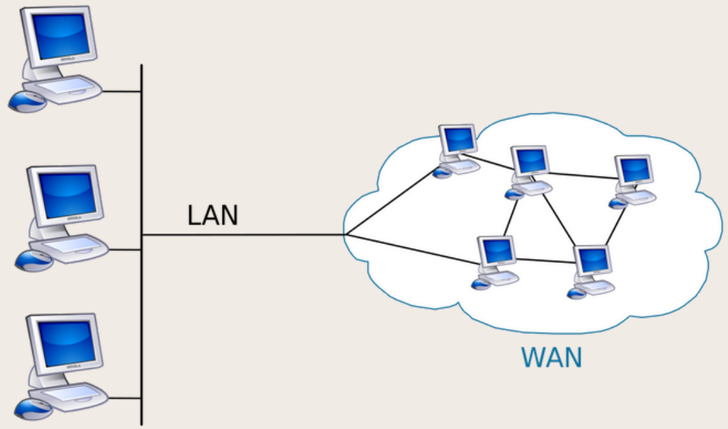
BEGINNER

NETWORKING

LAN/WAN

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building. By contrast, a wide area network (WAN) not only covers a larger geographic distance but also generally involves leased telecommunication circuits.
Ethernet (LAN) and Wi-Fi (WLAN) are the two most common technologies in use for local area networks.





What happens when we type a URL in a browser bar

DNS Resolution.

validates the URL and resolves the IP addr

3-way handshake:

SYN/SYN-ACK/ACK/FIN

Server Response: The server responds with status codes:

1xx: Information Message

2xx: Success

3xx: Redirects

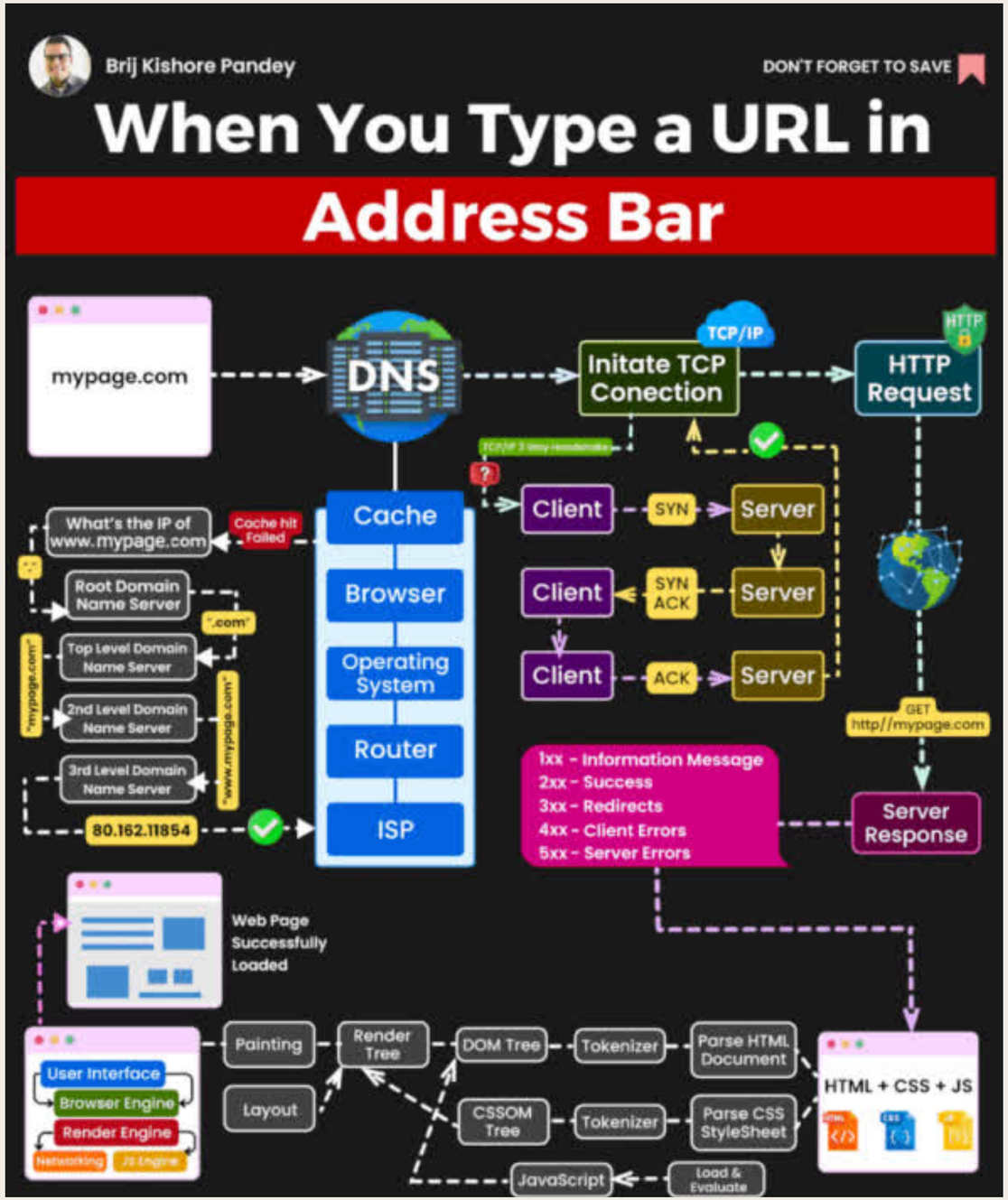
4xx: Client Errors

5xx: Server Errors

The server sends files back to the client

HTML+CSS+JS

The browser parses the files and loads the web page



twitter.com/brijpandeyji

OSI model
(Please Do Not Throw Sausage Pizza Away)

1. P - Physical:

BIT

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for the transmission of the raw data.

Cables (cat6/cat8, more twist, more copper=>cleaner signal);

Hubs (send data to all ports except its own, flooding not broadcasting);

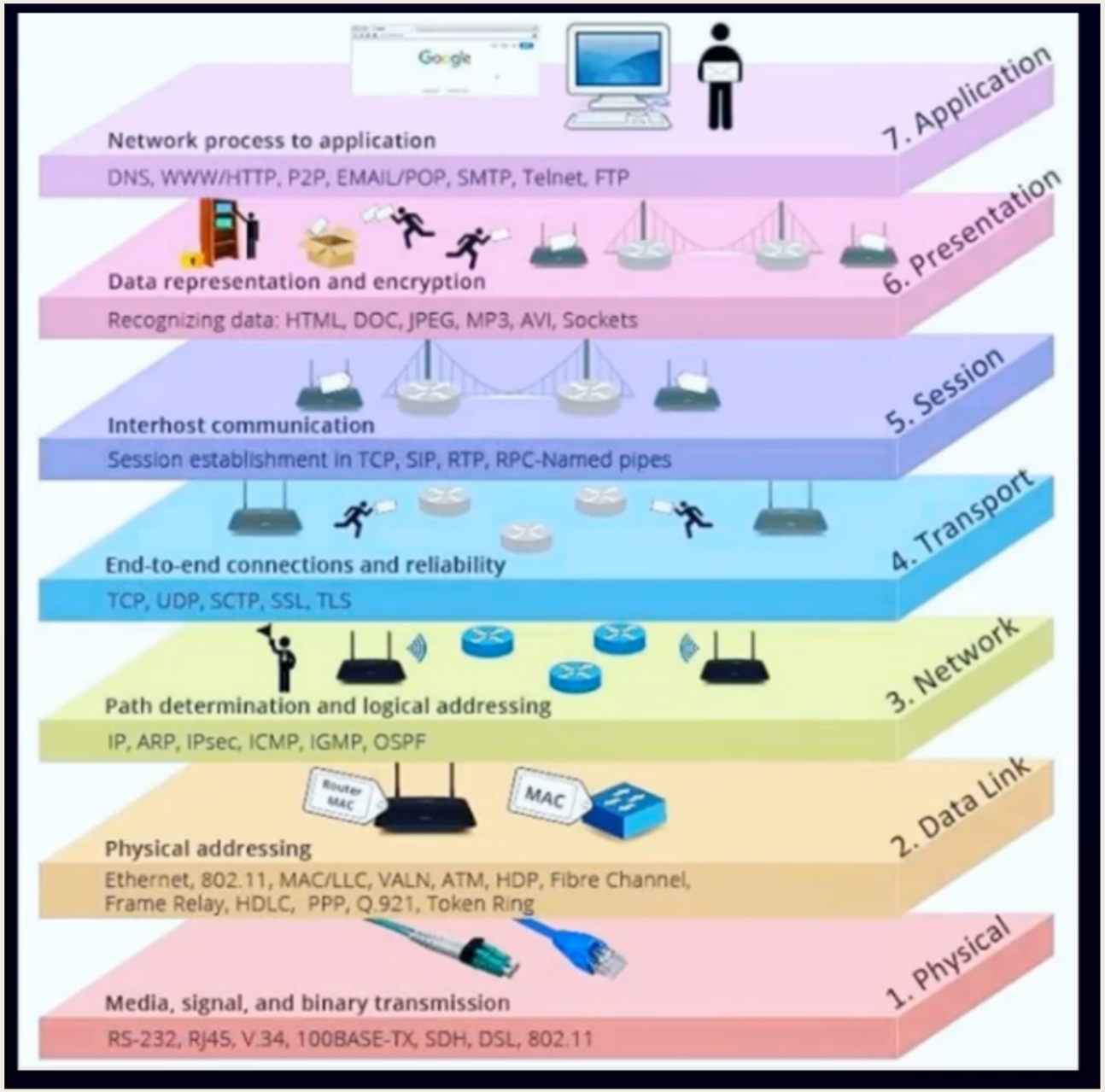
Repeaters (amplify and retransmit the signals of incoming packets to the other side of the network segments. Repeater helps to increase or extend the distance of the network)

2. D - Data:

FRAME

The data link layer establishes and terminates a connection between two physically connected nodes on a network. It breaks up packets into frames and sends them from source to destination.

Switch uses MAC address to transmit data over the network.



OSI model
(Please Do Not Throw Sausage Pizza Away)

3. N - Network:

PACKET

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network.

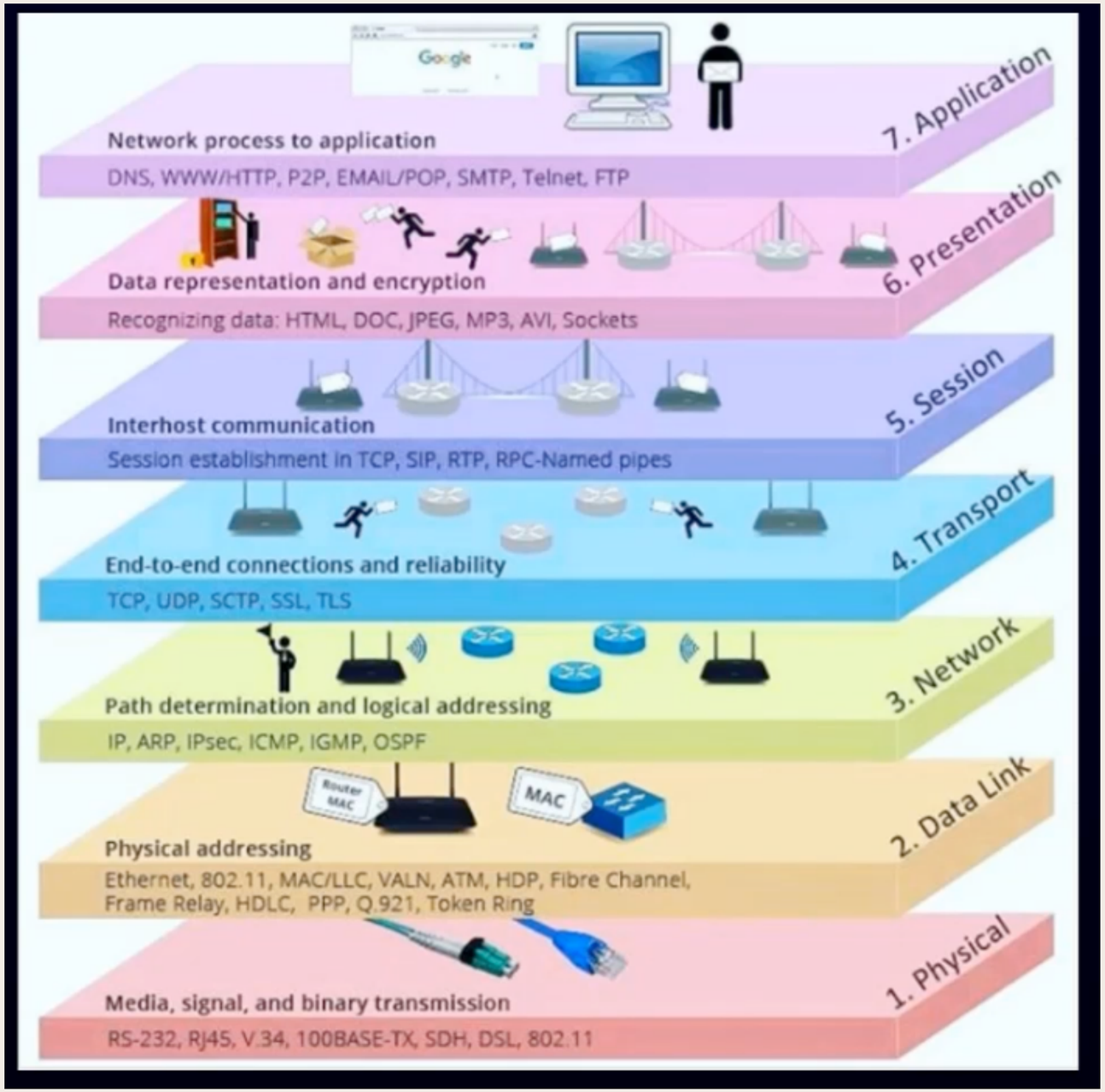
IP address, routing, IPX, ICMP

4. T - Transport:

SEGMENT

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end and turning them back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

TCP and UDP



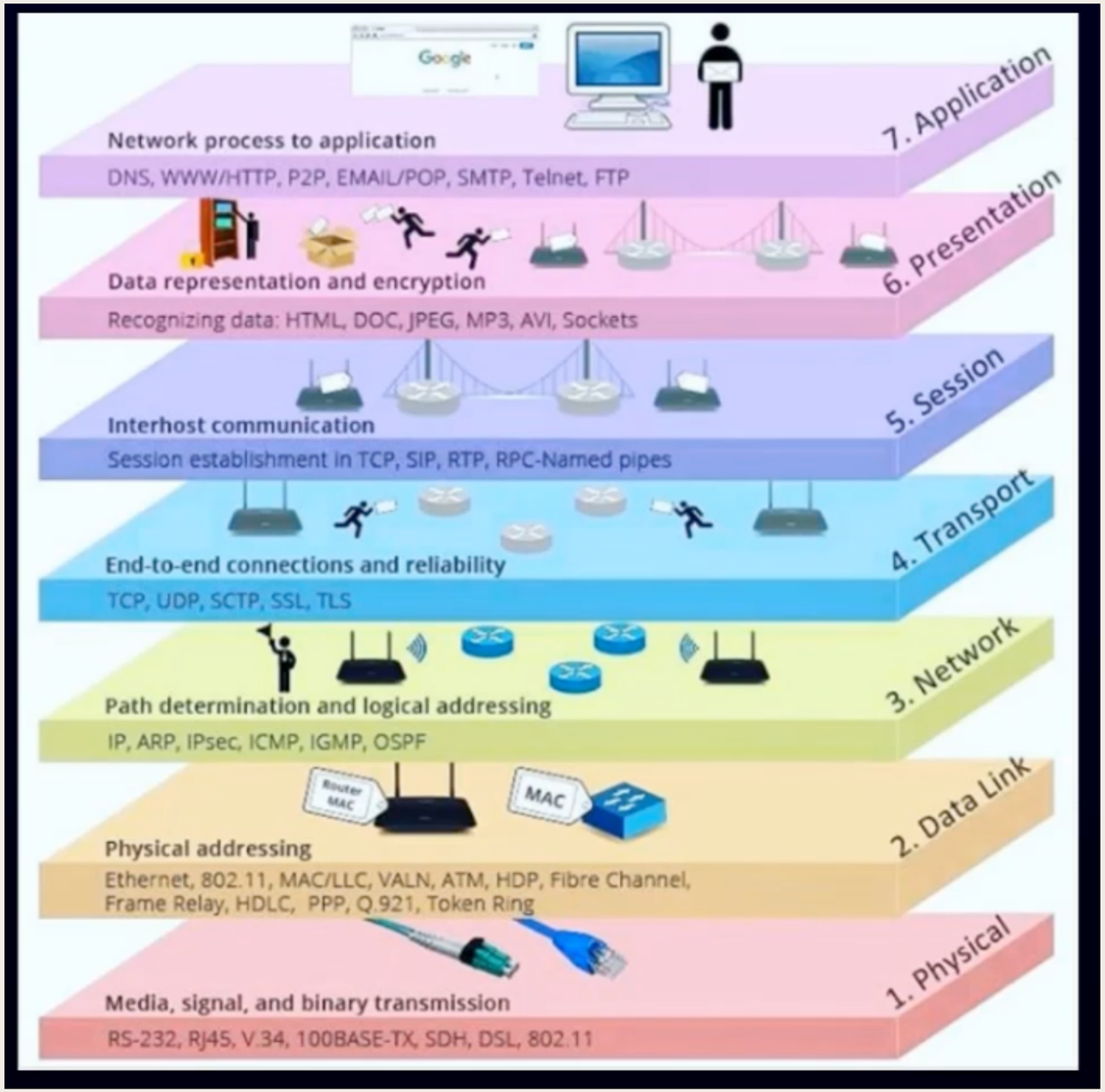
OSI model
(Please Do Not Throw Sausage Pizza Away)

5. S - Session:

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends.
session management, Apple Talk, interhost communication
NETBIOS, PPTP(tunnelling protocol)

6. P - Presentation:

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end.
WMV, JPEG, MOV, Gif
example: JPEG file can’t be opened in Note pad



OSI model
(Please Do Not Throw Sausage Pizza Away)

7. A - Application:

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users.

Application protocols like HTTP, FTP, SMTP,

Used for Firefox, Safari, and telnet apps like Patty

Microsoft Outlook uses IMAP, POP3

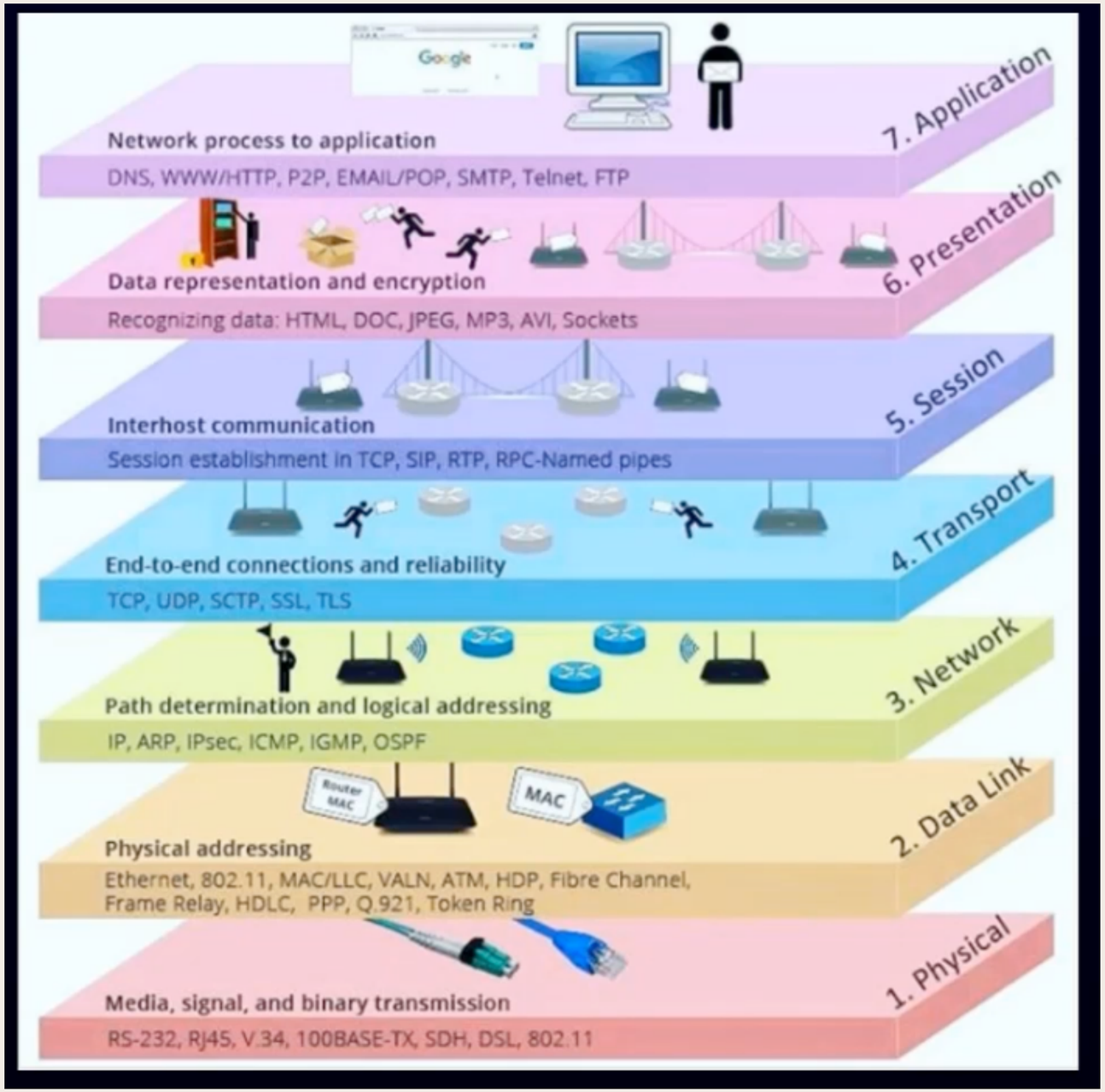
Remote file access, remote printer access

Each layer only communicates with the same layer of the other device

Receive data going from 1 to 7

Transmit data going from 7 to 1

Troubleshooting -start from physical 1 to 7

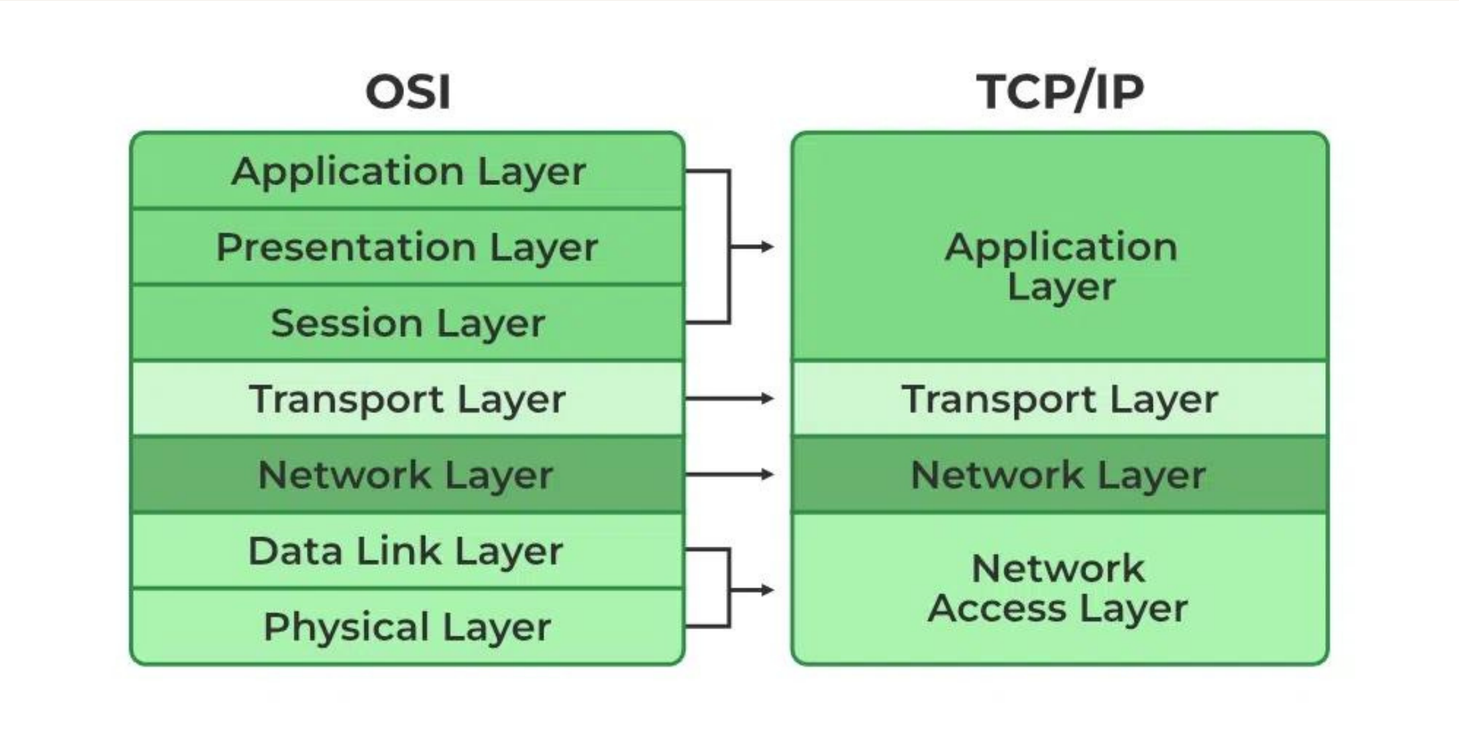


TCP/IP model

TCP/IP model was developed at the same time as OSI model.

OSI model is a comprehensive theoretical framework.

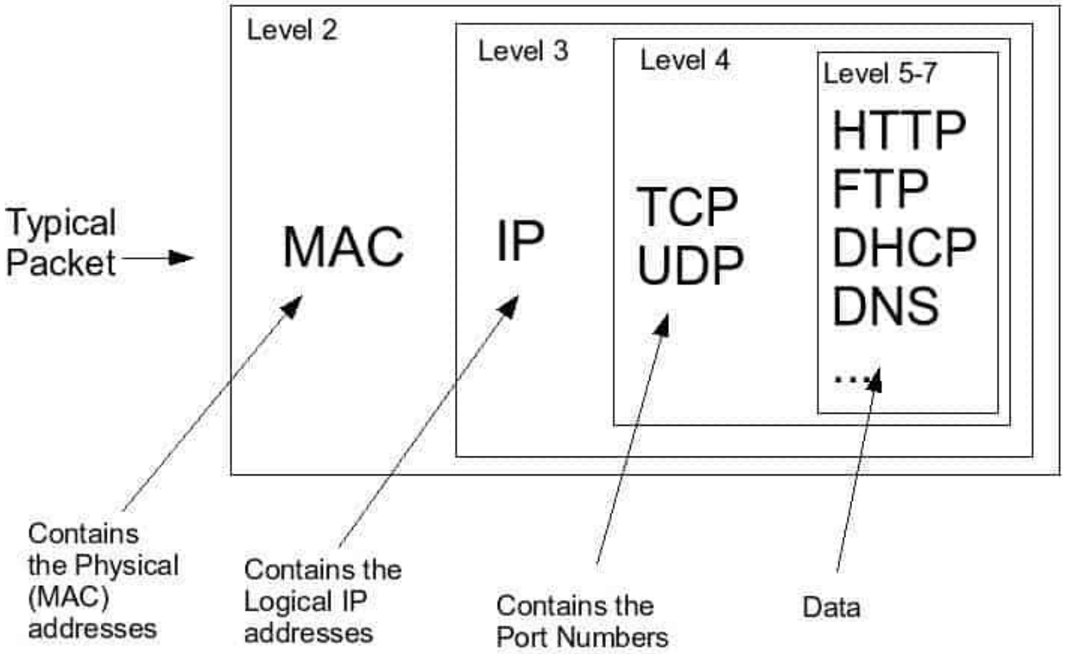
TCP/IP is a practical model that addresses specific communication challenges and relies on standardized protocols.



Encapsulation

Most modern computer networks use protocols based on packet-mode transmission. A network packet is a formatted unit of data carried by a packet-switched network.
Packets consist of two types of data: control information and user data (payload).

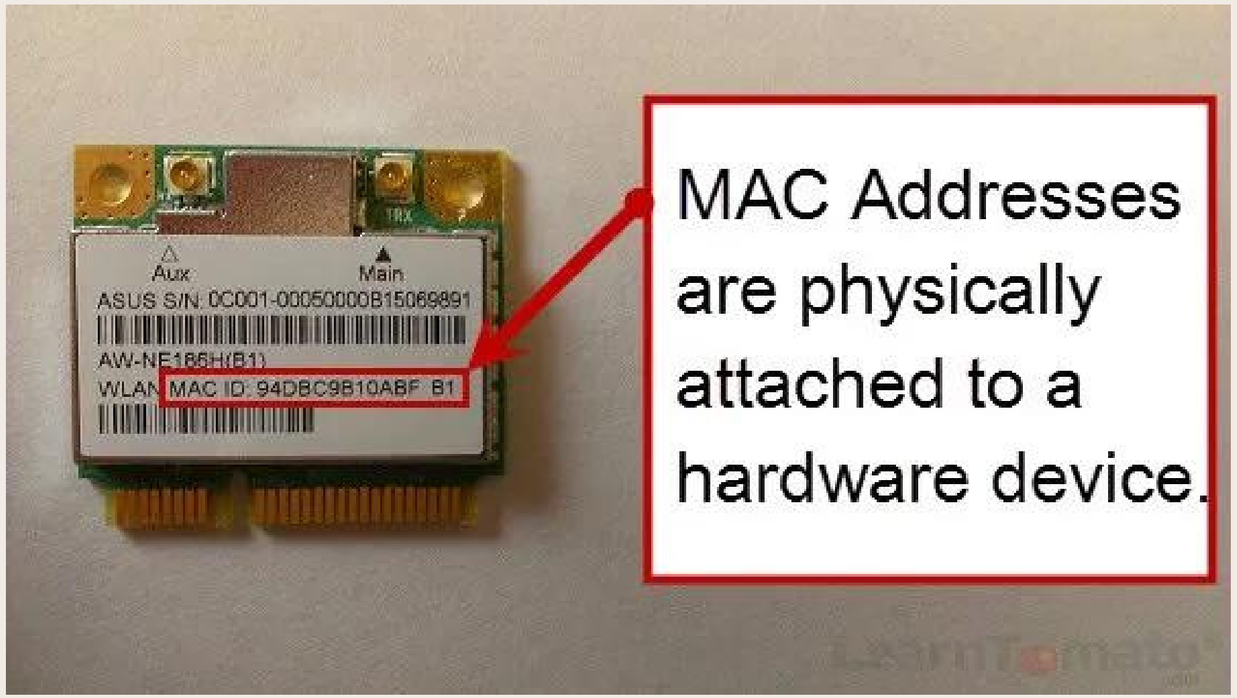
Encapsulation adds information to a packet as it travels to its destination.
Decapsulation reverses the process by removing the info, so a destination device can read the original data.

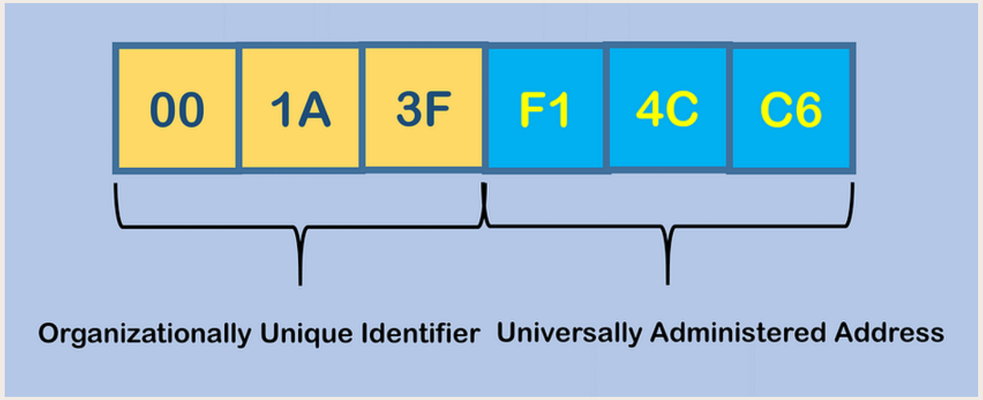


LAYER 2 (Data): MAC

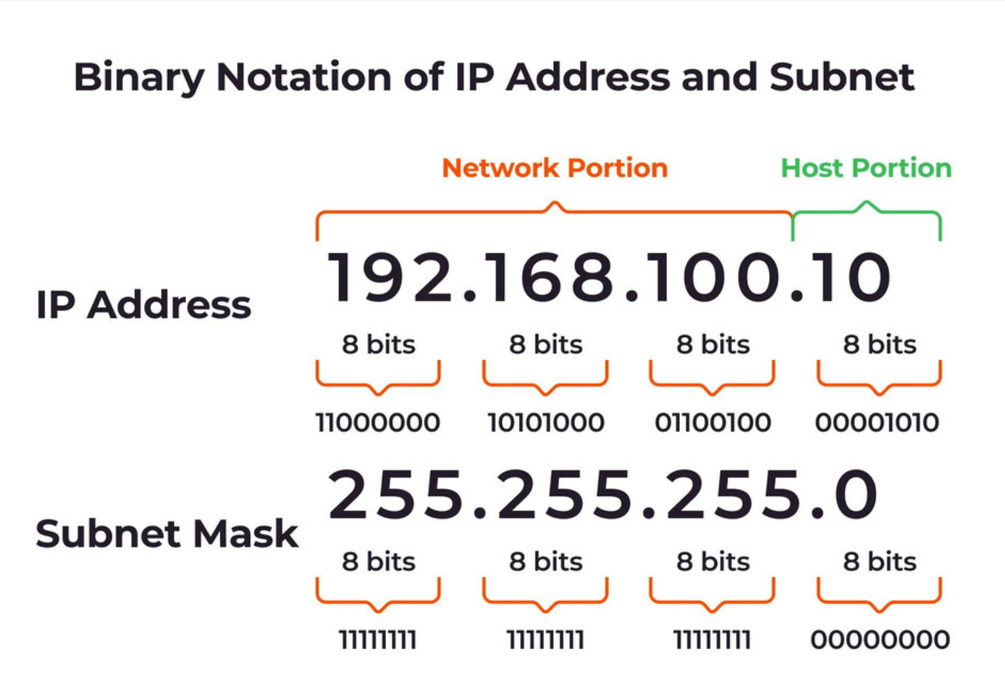
A MAC (Media Access Control) address, sometimes referred to as a hardware or physical address, is **a unique, 12-character alphanumeric attribute that is used to identify individual electronic devices on a network**. An example of a MAC address is: 00-B0-D0-63-C2-26.

To check vendor
https://www.wireshark.org/tools/oui-lookup.html





LAYER 3 (Network): Internet Protocol



Private IP addresses are reserved for LANs and can not be seen by other devices on the Internet.

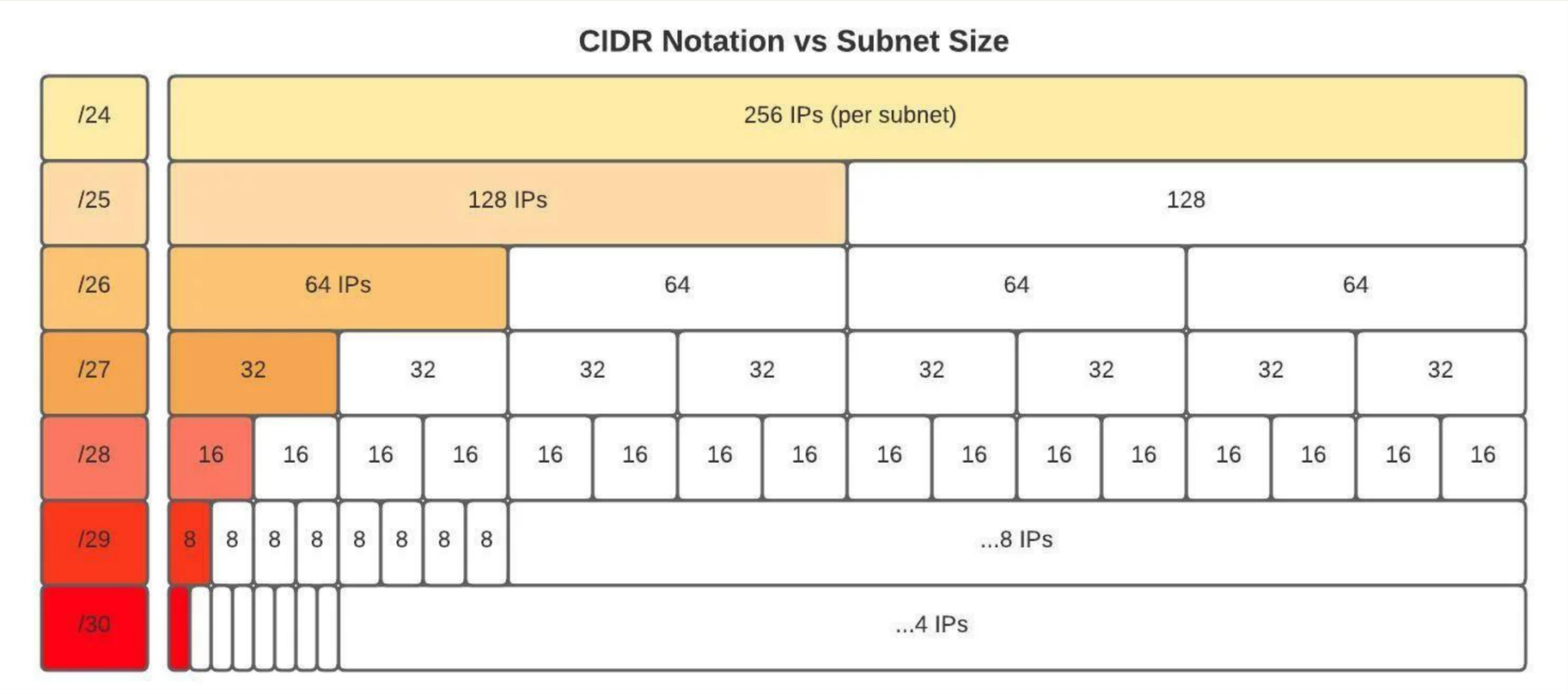
Network Class	Network Numbers	Network Mask	No. of Networks	No. of Hosts per Network
CLASS A	10.0.0.0	255.0.0.0	126	16,646,144
CLASS B	172.16.0.0 to 172.31.0.0	255.255.0.0	16,383	65,024
CLASS C	192.168.0.0 to 192.168.255.255	255.255.255.0	2,097,151	254
LOOPBACK (localhost)	127.0.0.0 to 127.0.0.7	255.255.255.0	-	-

LAYER 3 (Network): Internet Protocol

CIDR Notation - Classless Inter-Domain Routing is a method for allocating IP addresses and for IP routing. The Internet Engineering Task Force introduced CIDR to replace the previous classful network addressing architecture on the Internet.

192.168.50.30 / 32

IP Address CIDR



LAYER 3 (Network): Internet Protocol

Classful IP Addressing

Class A addresses are for networks with large number of total hosts. Class A allows for 126 networks by using the first octet for the network ID. Class A network number values begin at 1 and end at 127.

Every IP Addresses in the Internet		Class	Classful IP Ranges	Subnet Mask for each Block	Number of Blocks	IP addresses per Block
0.0.0.0 /0	Unicast	A	**0**.0.0.0 - **127**.255.255.255 0.0.0.0 /1	**255.0.0.0** **/8**	128	16,777,216
		B	**128**.0.0.0 - **191**.255.255.255 128.0.0.0 /2	**255.255.0.0** **/16**	16,384	65,536
		C	**192**.0.0.0 - **223**.255.255.255 192.0.0.0 /3	**255.255.255.0** **/24**	2,097,152	256
	Multicast	D	**224**.0.0.0 - **239**.255.255.255	*n/a*	*n/a*	*n/a*
	Reserved	E	**240**.0.0.0 - **255**.255.255.255	*n/a*	*n/a*	*n/a*

LAYER 3 (Network): Internet Protocol

Classful IP Addressing

Class B addresses are for medium to large-sized networks. Class B allows for 16,384 networks by using the first two octets for the network ID. Class B network number values begin at 128 and end at 191.

Every IP Addresses in the Internet		Class	Classful IP Ranges	Subnet Mask for each Block	Number of Blocks	IP addresses per Block
0.0.0.0 /0	Unicast	A	**0**.0.0.0 - **127**.255.255.255 0.0.0.0 /1	**255.0.0.0** **/8**	128	16,777,216
		B	**128**.0.0.0 - **191**.255.255.255 128.0.0.0 /2	**255.255.0.0** **/16**	16,384	65,536
		C	**192**.0.0.0 - **223**.255.255.255 192.0.0.0 /3	**255.255.255.0** **/24**	2,097,152	256
	Multicast	D	**224**.0.0.0 - **239**.255.255.255	*n/a*	*n/a*	*n/a*
	Reserved	E	**240**.0.0.0 - **255**.255.255.255	*n/a*	*n/a*	*n/a*

LAYER 3 (Network): Internet Protocol

Classful IP Addressing

Class C addresses are used in small local area networks (LANs). Class C allows for approximately 2 million networks by using the first three octets for the network ID. The last octet (8 bits) represents the host ID and allows for 254 hosts per network. Class C network number values begin at 192 and end at 223.

Every IP Addresses in the Internet		Class	Classful IP Ranges	Subnet Mask for each Block	Number of Blocks	IP addresses per Block
0.0.0.0 /0	Unicast	A	**0**.0.0.0 - **127**.255.255.255 0.0.0.0 /1	**255.0.0.0** **/8**	128	16,777,216
		B	**128**.0.0.0 - **191**.255.255.255 128.0.0.0 /2	**255.255.0.0** **/16**	16,384	65,536
		C	**192**.0.0.0 - **223**.255.255.255 192.0.0.0 /3	**255.255.255.0** **/24**	2,097,152	256
	Multicast	D	**224**.0.0.0 - **239**.255.255.255	*n/a*	*n/a*	*n/a*
	Reserved	E	**240**.0.0.0 - **255**.255.255.255	*n/a*	*n/a*	*n/a*

LAYER 3 (Network): Internet Protocol

Classful IP Addressing

Class D IP addresses are not allocated to hosts and are used for multicasting. Multicasting allows a single host to send a single stream of data to thousands of hosts across the Internet at the same time. It is often used for audio and video streaming, such as IP-based cable TV networks. Another example is the delivery of real-time stock market data from one source to many brokerage companies.
Class E IP addresses are not allocated to hosts and are not available for general use. These are reserved for research purposes.

Every IP Addresses in the Internet		Class	Classful IP Ranges	Subnet Mask for each Block	Number of Blocks	IP addresses per Block
0.0.0.0 /0	Unicast	A	**0**.0.0.0 - **127**.255.255.255 0.0.0.0 /1	**255.0.0.0** **/8**	128	16,777,216
		B	**128**.0.0.0 - **191**.255.255.255 128.0.0.0 /2	**255.255.0.0** **/16**	16,384	65,536
		C	**192**.0.0.0 - **223**.255.255.255 192.0.0.0 /3	**255.255.255.0** **/24**	2,097,152	256
	Multicast	D	**224**.0.0.0 - **239**.255.255.255	*n/a*	*n/a*	*n/a*
	Reserved	E	**240**.0.0.0 - **255**.255.255.255	*n/a*	*n/a*	*n/a*

LAYER 3 (Network): Internet Protocol

Classless addressing

To reduce the wastage of IP addresses in a block, we use sub-netting. We use host bits as net bits of a classful IP address.

At a high level, classless addressing works by allowing IP addresses to be assigned arbitrary network masks without respect to “class.” That means /8 (255.0. 0.0), /16 (255.255. 0.0), and /24 (255.255. 255.0) network masks can be assigned to any address that would have traditionally been in the Class A, B, or C range.

192.168.0.0/30

Network 192.168.0.0

Gateway 192.168.0.1

Broadcast 192.168.0.3

First 192.168.0.2

Last 192.168.0.2

www.calculator.net

CIDR Notation:	Total number of addresses:	Network Mask:	Description:
/0	4,294,967,296	0.0.0.0	Every Address
/1	2,147,483,648	128.0.0.0	128 /8 nets
/2	1,073,741,824	192.0.0.0	64 /8 nets
/3	536,870,912	224.0.0.0	32 /8 nets
/4	268,435,456	240.0.0.0	16 /8 nets
/5	134,217,728	248.0.0.0	8 /8 nets
/6	67,108,864	252.0.0.0	4 /8 nets
/7	33,554,432	254.0.0.0	2 /8 nets
/8	16,777,214	255.0.0.0	1 /8 net
/9	8,388,608	255.128.0.0	128 /16 nets
/10	4,194,304	255.192.0.0	64 /16 nets
/11	2,097,152	255.224.0.0	32 /16 nets
/12	1,048,576	255.240.0.0	16 /16 nets
/13	524,288	255.248.0.0	8 /16 nets
/14	262,144	255.252.0.0	4 /16 nets
/15	131.072	255.254.0.0	2 /16 nets
/16	65,536	255.255.0.0	1 /16
/17	32,768	255.255.128.0	128 /24 nets
/19	16,384	255.255.192.0	64 /24 nets
/19	8,192	255.255.224.0	32 /24 nets
/20	4,096	255.255.240.0	16 /24 nets
/21	2,048	255.255.248.0	8 /24 nets
/22	1,024	255.255.252.0	4 /24 nets
/23	512	255.255.254.0	2 /24 nets
/24	256	255.255.255.0	1 /24
/25	128	255.255.255.128	Half of a /24
/26	64	255.255.255.192	Fourth of a /24
/27	32	255.255.255.224	Eighth of a /24
/28	16	255.255.255.240	1/16th of a /24
/29	8	255.255.255.248	5 Usable addresses
/30	4	255.255.255.252	1 Usable address
/31	2	255.255.255.254	Unusable
/32	1	255.255.255.255	Single host

LAYER 3 (Network): Internet Protocol

IPv6 is turned on by default. It’s recommended to turn off IPv6 if it’s not used for security purposes.

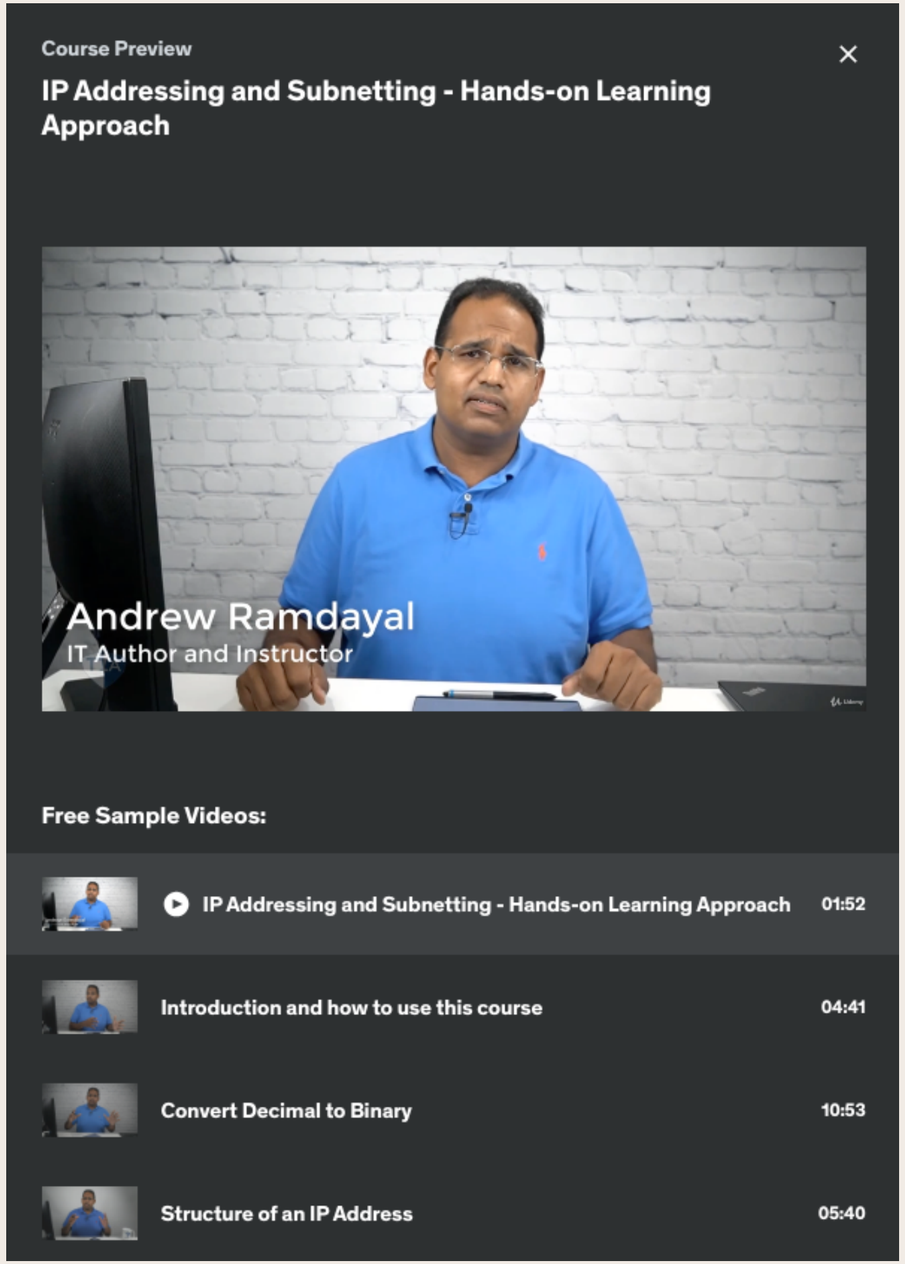
IPv4	vs.	IPv6
Deployed 1981		Deployed 1998
32-bit IP address		128-bit IP address
4.3 billion addresses Addresses must be reused and masked		7.9×10^{28} addresses Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18		Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration		Supports autoconfiguration

LAYER 3 (Network): Internet Protocol

If you would like to learn more about subnetting, here is my favourite course on Udemy

IP Addressing and Subnetting - Hands-on Learning Approach by Andrew Ramdayal

https://www.udemy.com/course/ip-addressing-and-subnetting-course/



LAYER 4 (Transport): Ports

When you add a port into a packet it’s called SEGMENT

Well-known Ports	**0-1023**
Registred Ports	**1024-49151**
Dynamic Ports	**49152-65565**

Well-known ports are used by system processes that provide widely used types of network services.

Dynamic or private ports are the ports that cannot be registered with IANA. This range is used for private, or customized services or temporary purposes and for automatic allocation of ephemeral ports.

The range of port numbers from 1024 to 49151 are the **registered ports**. They are assigned by IANA for a specific service upon application by a requesting entity. On most systems, registered ports can be used without superuser privileges.

You may find the full list here
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

LAYER 4 (Transport): Ports

The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. TCP provides **reliable, ordered, and error-checked** delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network.

The Acknowledgment Number contains the next expected Sequence Number.
Sequence Number is used to sort the received packets into the same order as they were sent.

Real-life examples: HTTP, FTP file transfer, text messages

TCP segment header

Offsets		0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0 0				CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
16	128	Checksum																Urgent pointer (if URG set)														
20	160	Options (if *data offset* > 5. Padded at the end with "0" bits if necessary.)																															
⋮	⋮																																
56	448																																

LAYER 4 (Transport): Ports

TCP flags

SYN - Ask for a new connection

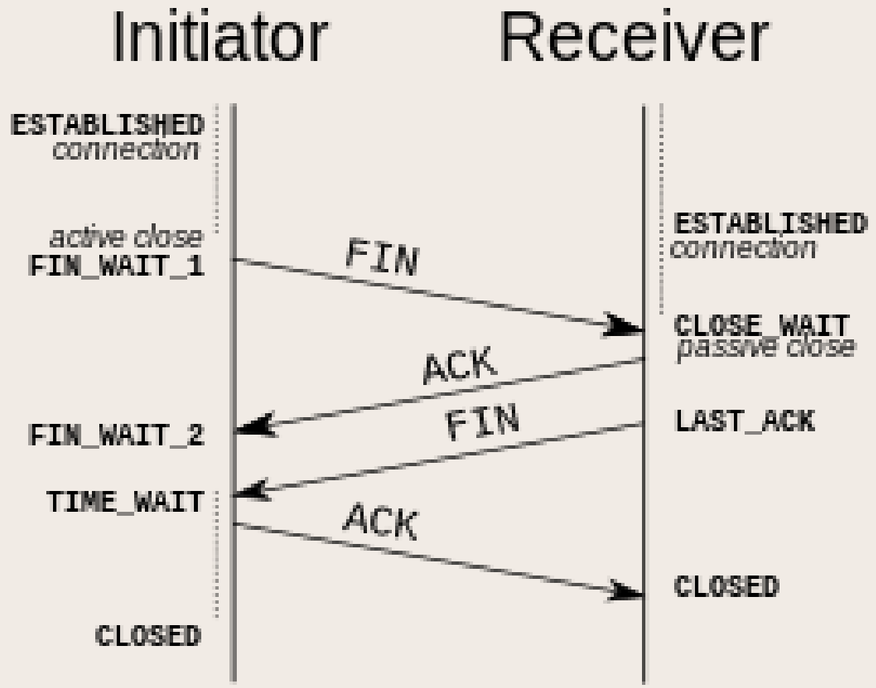
ACK - Acknowledge the receipt of a packet

RST - cancel a connection attempt, when a host connects to a closed port

FIN - Cleanly close an established connection

URG - Mark packet as urgent

PSH - Handle packet with higher priority



LAYER 4 (Transport): Ports

UDP (User Datagram Protocol) uses a simple connectionless communication model with a minimum of protocol mechanisms. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. It has **no handshaking** dialogues and thus exposes the user's program to any unreliability of the underlying network; there is **no guarantee of delivery, ordering, or duplicate protection**.

Real-life examples: video streaming, Zoom meetings, online games, DNS

UDP datagram header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Length																Checksum															

LAYER 4 (Transport): Ports

Protocol	Description	TCP Port	UDP Port
FTP	File Transfer Protocol: Transfers files with a remote host (typically requires authentication of user credentials)	20 and 21	
SSH	Secure Shell: Securely connect to a remote host over an unsecured network	22	
SFTP	Secure FTP: Provides FTP file-transfer service over an SSH connection	22	
FTPS	FTP Secure: Provides FTP file-transfer service over Secure Sockets Layer (SSL) or the more secure Transport Layer Security (TLS)	989 and 990	989 and 990
Telnet	Telnet: Used to connect to a remote host (typically via a terminal emulator)	23	
SMTP	Simple Mail Transfer Protocol: Used for sending e-mail	25	
SMTP over SSL/TLS	Simple Mail Transfer Protocol over Secure Sockets Layer or Transport Layer Security: Sends e-mail securely using SSL or the more secure TLS	587	
DNS	Domain Name System: Resolves domain names to corresponding IP addresses	53	53
TFTP	Trivial File Transfer Protocol: Transfers files with a remote host (does not require authentication of user credentials)		69

LAYER 4 (Transport): Ports

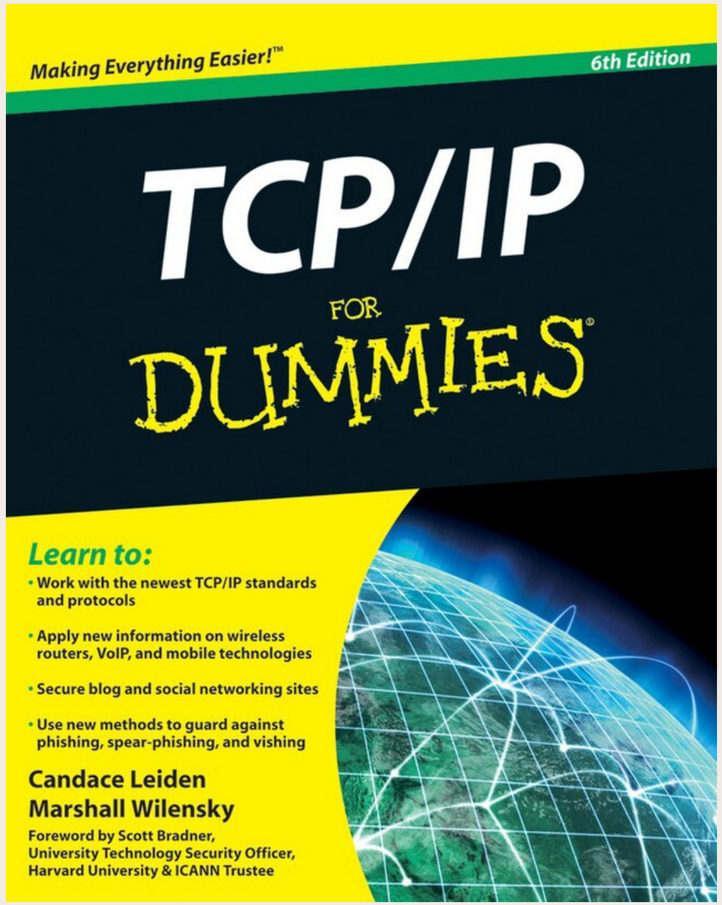
Protocol	Description	TCP Port	UDP Port
DHCP	Dynamic Host Configuration Protocol: Dynamically assigns IP address information (for example, IP address, subnet mask, DNS server's IP address, and default gateway's IP address) to a network device		67
HTTP	Hypertext Transfer Protocol: Retrieves content from a web server	80	
HTTPS	Hypertext Transfer Protocol Secure: Secures HTTP transmission over an unsecured network using Secure Sockets Layer (SSL) or the more secure option of Transport Layer Security (TLS)	443	
POP3	Post Office Protocol version 3: Retrieves e-mail from an e-mail server	110	
POP3 over SSL/TLS	Post Office Protocol version 3 over Secure Sockets Layer or Transport Layer Security: Retrieves e-mail from an e-mail server while encrypting the e-mail in transmit using SSL or the more secure option of TLS	995	995
NTP	Network Time Protocol: Used by a network device to synchronize its clock with a time server (NTP server)		123
IMAP	Internet Message Access Protocol version 4: Allows the viewing of e-mail on an e-mail server	143	
IMAP over SSL/TLS	Internet Message Access Protocol version 4 over Secure Sockets Layer or Transport Layer Security: Allows the viewing of e-mail on an e-mail server while encrypting the e-mail in transit using SSL or the more secure option of TLS	993	

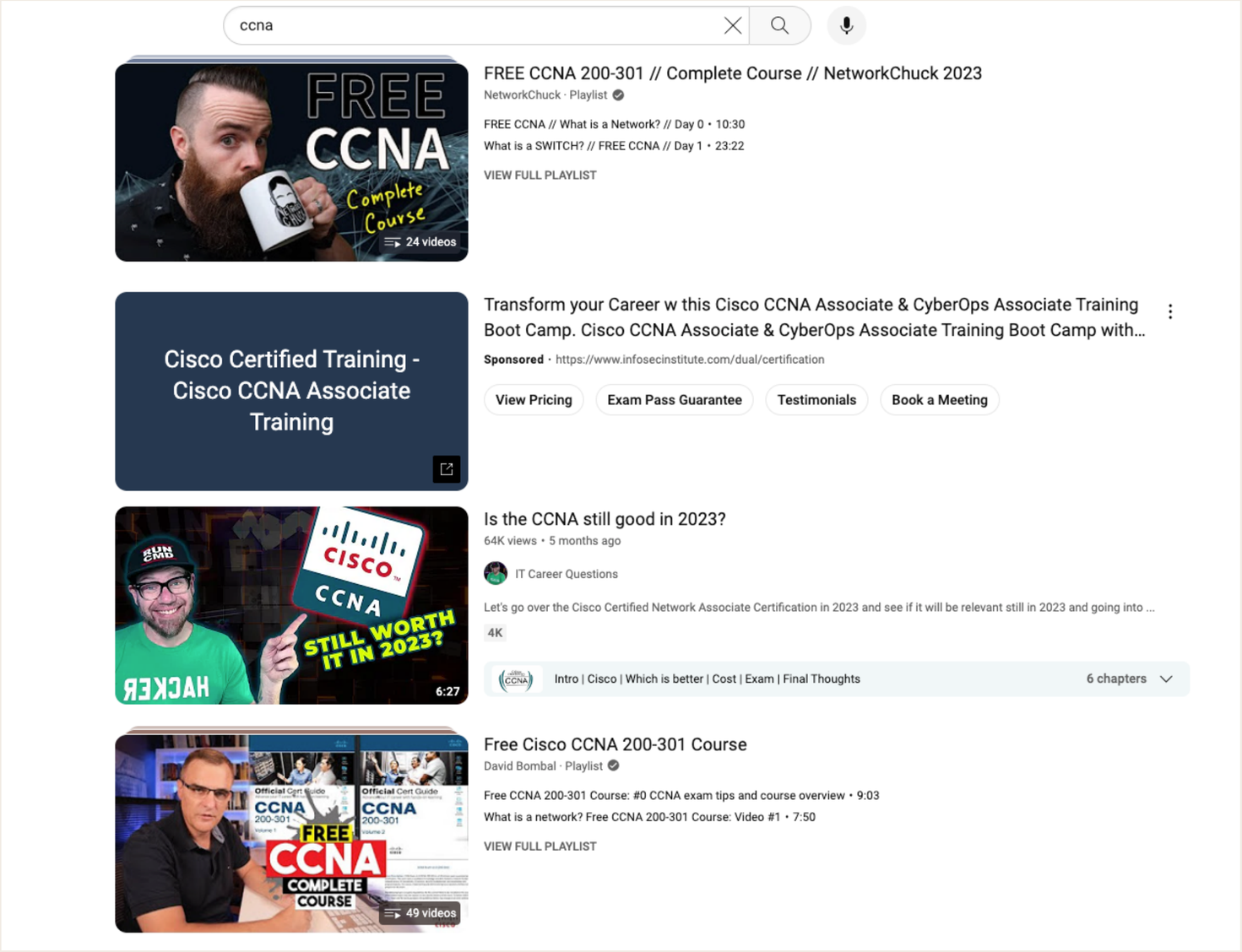
LAYER 4 (Transport): Ports

Protocol	Description	TCP Port	UDP Port
SNMP	Simple Network Management Protocol: Used to monitor, manage, and configure network devices. An SNMP agent receives requests on port 161, and an SNMP agent sends traps on port 162	161 and 162	161 and 162
RDP	Remote Desktop Protocol: A Microsoft protocol that allows a user to view and control the desktop of a remote computer	3389	
SIP	Session Initiation Protocol: A signaling protocol used to setup, monitor, and teardown multimedia calls (e.g. voice and video calls). Port 5060 is commonly used for unencrypteypted calls, and port 5061 is commonly used to setup encrypted calls	5060 and 5061	5060 and 5061
H.323	An ITU-T recommendation that can setup and teardown multimedia calls (e.g. voice and video calls)	1720	
SMB	Server Message Block: Used primarily in Microsoft networks for sharing resources (e.g. file resources) between devices		445

For more information:

1) TCP/IP for dummies book
2) Any CCNA course on Udemy or YouTube





HOMEWORK

Turn off IPv6 on your home router for all devices both on WLAN and LAN