**Open System Interconnected(OSI) layers:**

**Layer-1:**

Physical layer-> works on physical shared medium eg: two laptops connected via copper wire and network interface cards. transmits 0s and 1s through voltage.

problems:

Only 2 laptops can work. If more than 2, hub like common device is used.

Even then, at a time only one laptop can communicate, otherwise data collision occurs.

Also, 1 laptop cannot address the specific other laptop. one sender should broadcast to all the laptops not a specific one.

If error comes, does not which laptop is throwing it.

So layer-1 isn't intelligent. Need better system.

**Layer:2:**

MAC-Media access controller -> 1e:4c:5d:7h:dg:df -> 48 bits

it is combination of company OUI (Organisation unique identifier) and Network interface card number.

Datalink layer covers the payload data (from layer3) to get transferred to other laptop by frame which also has: SFD (data series start 8 bytes), dest MAC address, source MAC address along with payload data.

This is called encapsulation. Meaning protecting data

Now data is sent to ethernet and check for carries via CSMA (carrier sense something). Meaning, if other laptop is sending signa, this CSMA would detect and wait to avoid collision.

Drawback:

At a time if 2 devices sent data to third, collision occurs but greatly reduced compare to using only layer 1.

Cannot communicate outside local networks.

**Layer-3**

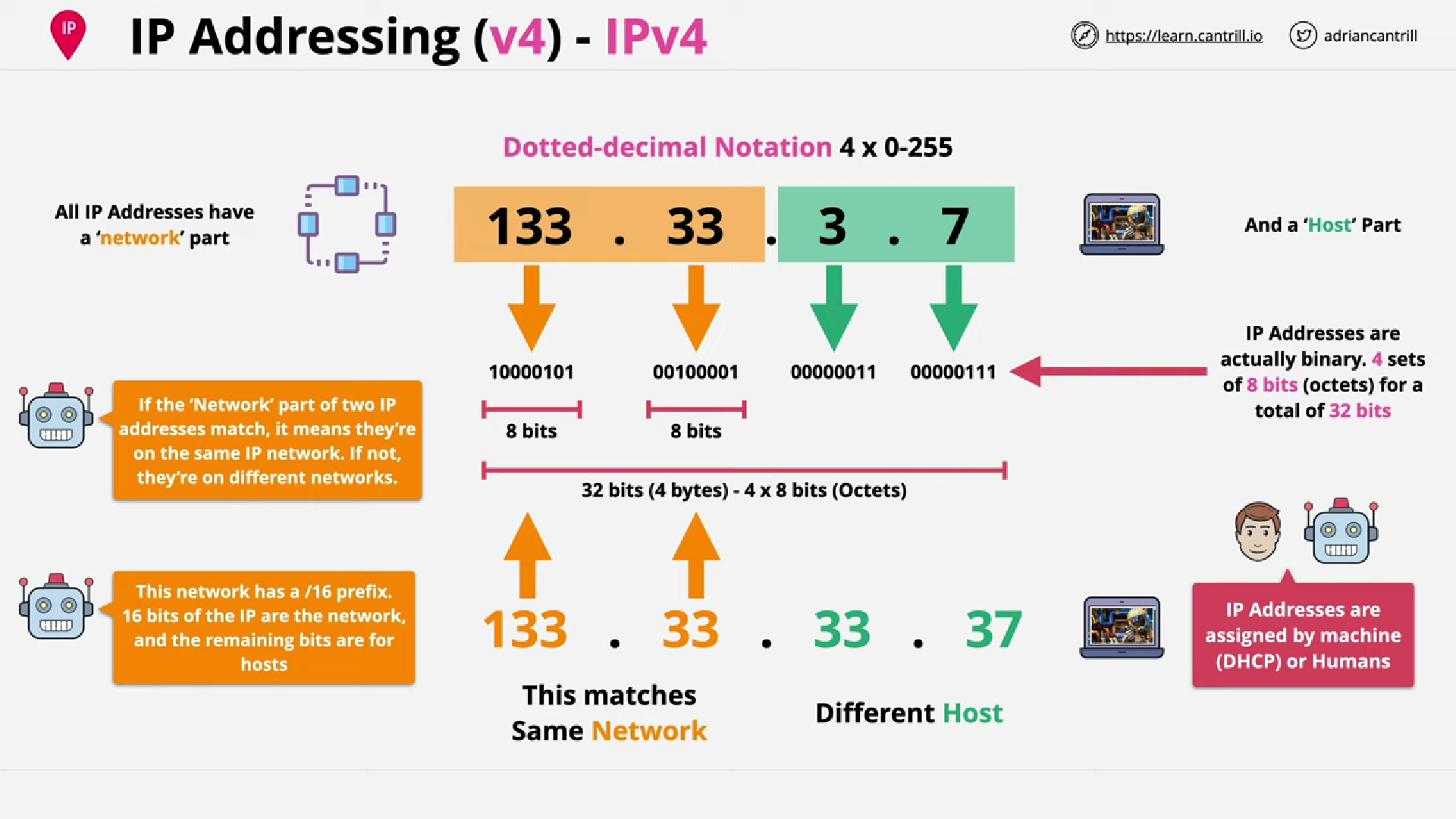
Layer-3 is built to overcome the hurdle of connecting two local area networks which is called internetworking or internet

Two types of protocol. IPv4 and IPv6.

There are many other fields other than mentioned below, but for beginners, this is enough

IPv4 -> Protocol (defines tcp or udp using number codes like 17 or 6 respectively), time-to-live(limits number of hops to reach the other network. if it keeps looping around, it may get lost, so setting limit and checking), data (usually from layer 4 protocol), source and destination IP address

IPv6 -> hop-limit(limits number of hops to reach the other network. if it keeps looping around, it may get lost, so setting limit and checking), data (usually from layer 4 protocol), lengthy source and destination IP address



Each decimal in IP address is called Octet (1 Octet = 8 bits)

Decimal to Binary and Binary to decimal see google.

133 -> 1

66-> 0

33->1

16->0

8->0

4->0

2-> 0

1-> 1 mod 2 = 1 - MSB (Most Significant Bit)

133 base 10 = 10100001 base 2

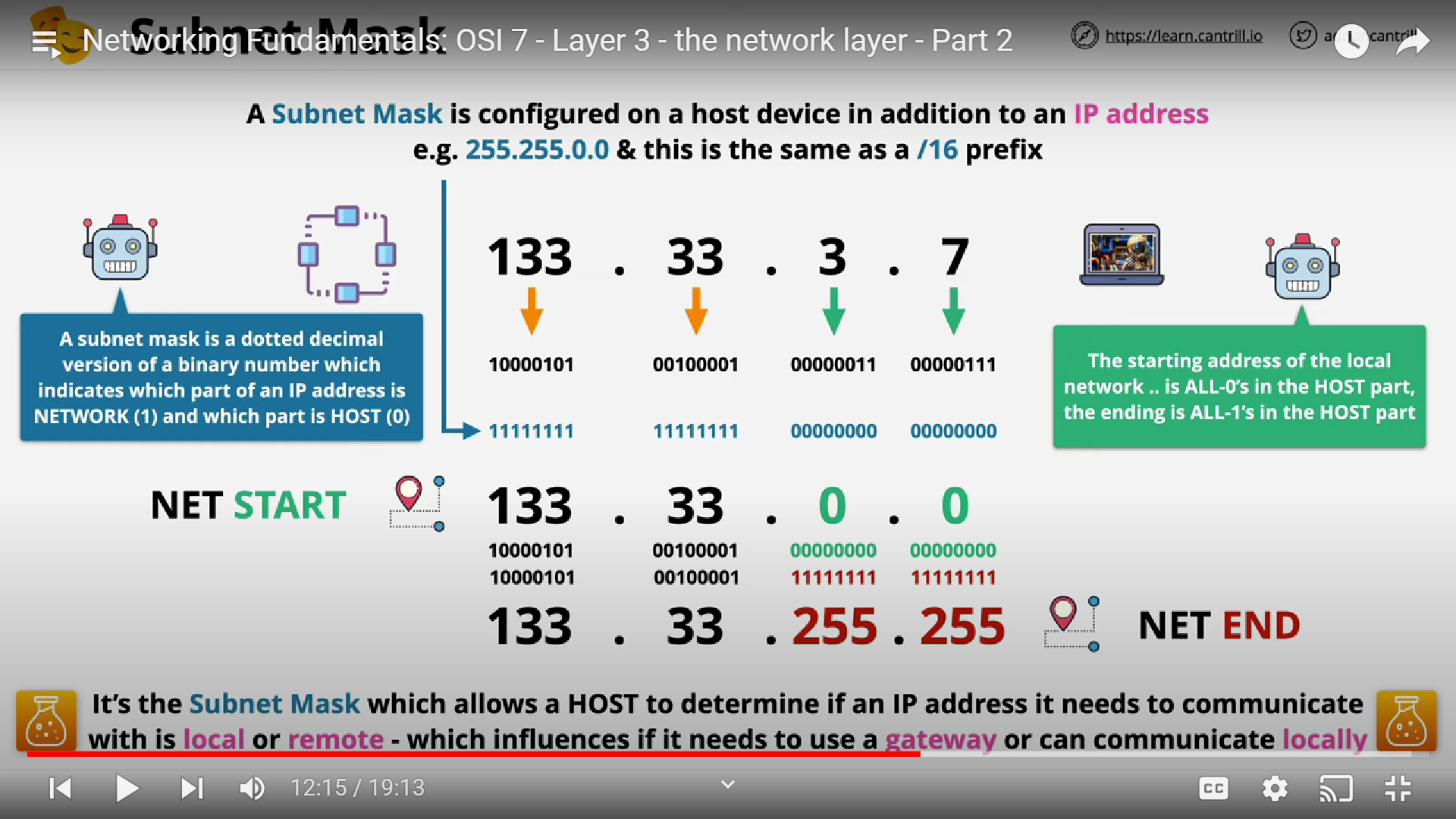
Each decimal could be any number between 0-255 coz, 255 meant for 11111111 which is the maximum signal that can be passed in a physical medium

IP address if defined by human, it is called static IP

If automatically assigned using servers on your network carrying DHCP software, it is then called dynamic IP.

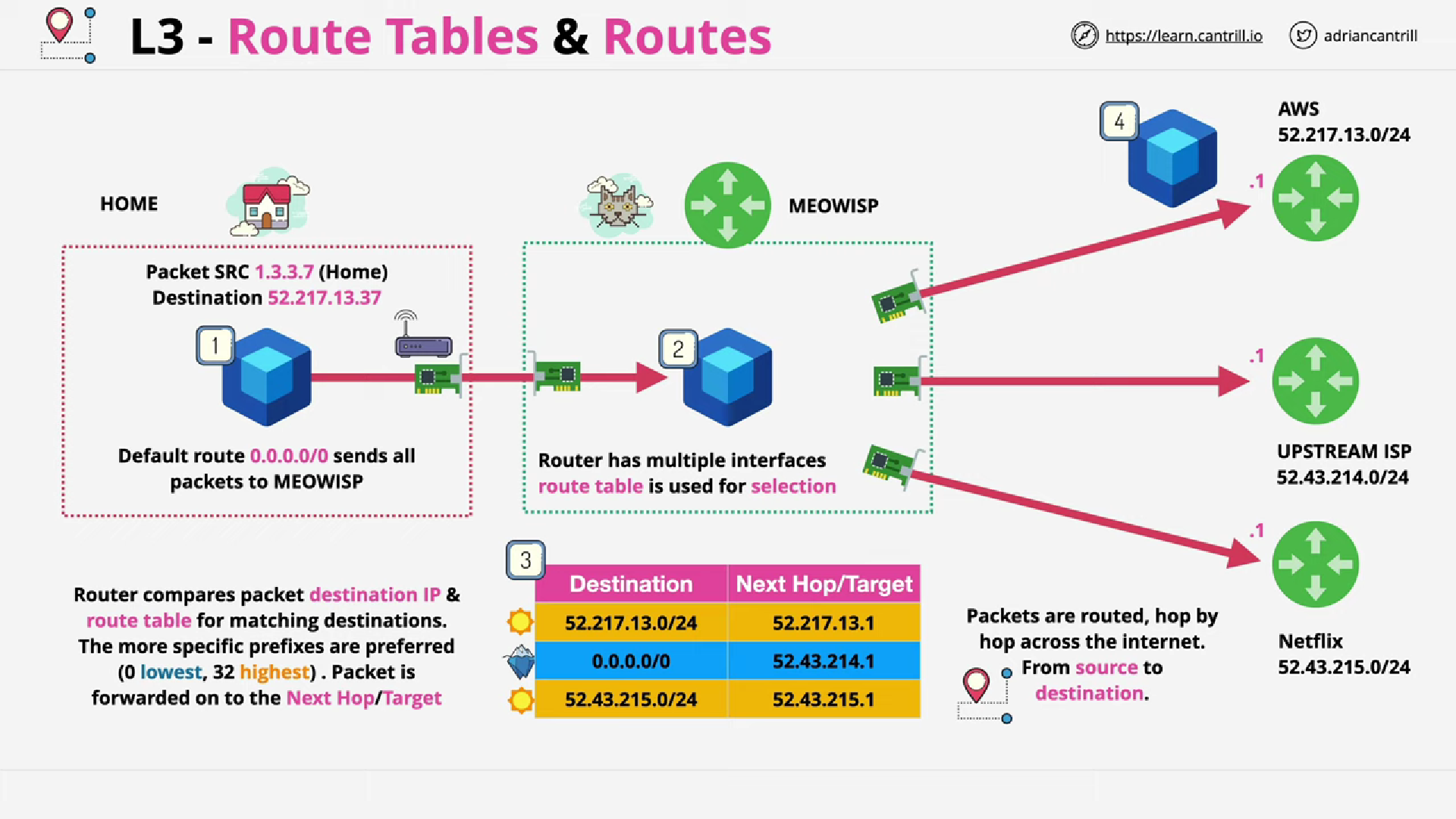
DHCP-Dynamic Host Configuration Protocol

Subnet Mask: To determine which part of ip address is network/organization/LAN address and which part is host address.



If subnet masks determine destination within network, then it goes to layer-2 and involves further encapsulation (layer-2, layer-1) and transferred to other laptop locally via cable itself, it doesn’t need router now.

Otherwise(if outside local network), the packets still go to layer-2 encapsulated and sent to router (Home wifi device) which then shares data to Internet service provider router and finally reaches the website router (like, firefox router, AWS router etc)



Layer 3 sends packets to layer 2. Layer 2 encapsulates it inside frame.

Address Resolution Protocol:

How will layer-2 determine destination MAC address? This is where ARP comes into picture.

ARP in layer 3, gets IP address from layer 3 and broadcasts the IP address asking for who owns. If other laptop in same local network has that IP address, it responds with its MAC address to my laptop’s ARP.

Now my laptop knows the MAC address of other laptop. Router isn’t required if we have layer-3 IP address.

Using IP address and physical wires, we can easily communicate with other laptops within network.

**Complete architecture of L-1,2 and 3:**

Scenario:

1. Transmitting data withing network LAN. (sometimes routers if WLAN but author mentions only LAN here)
2. Transmitting data outside the network using routers.

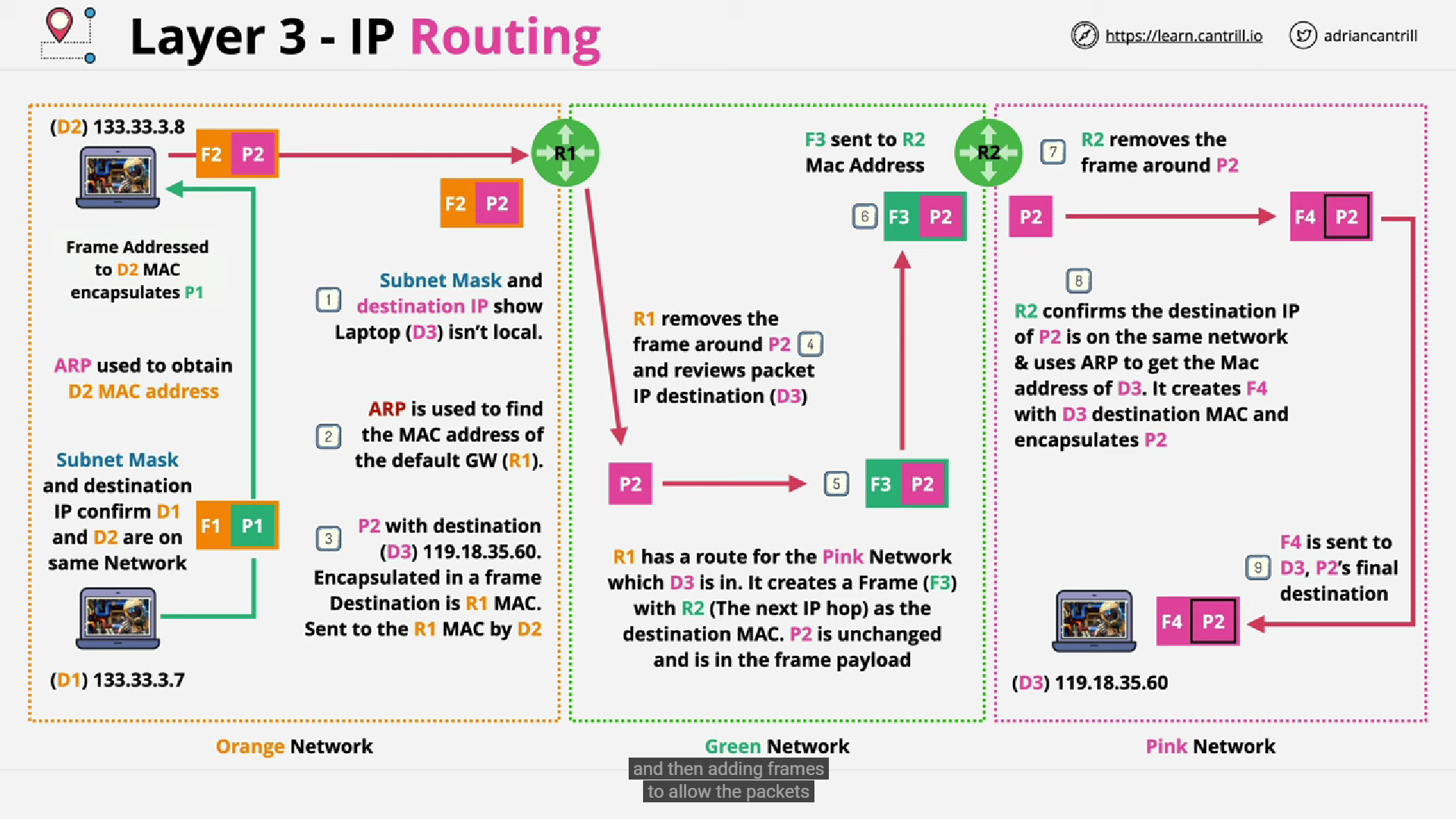
Please note that, in scenario-2, everytim

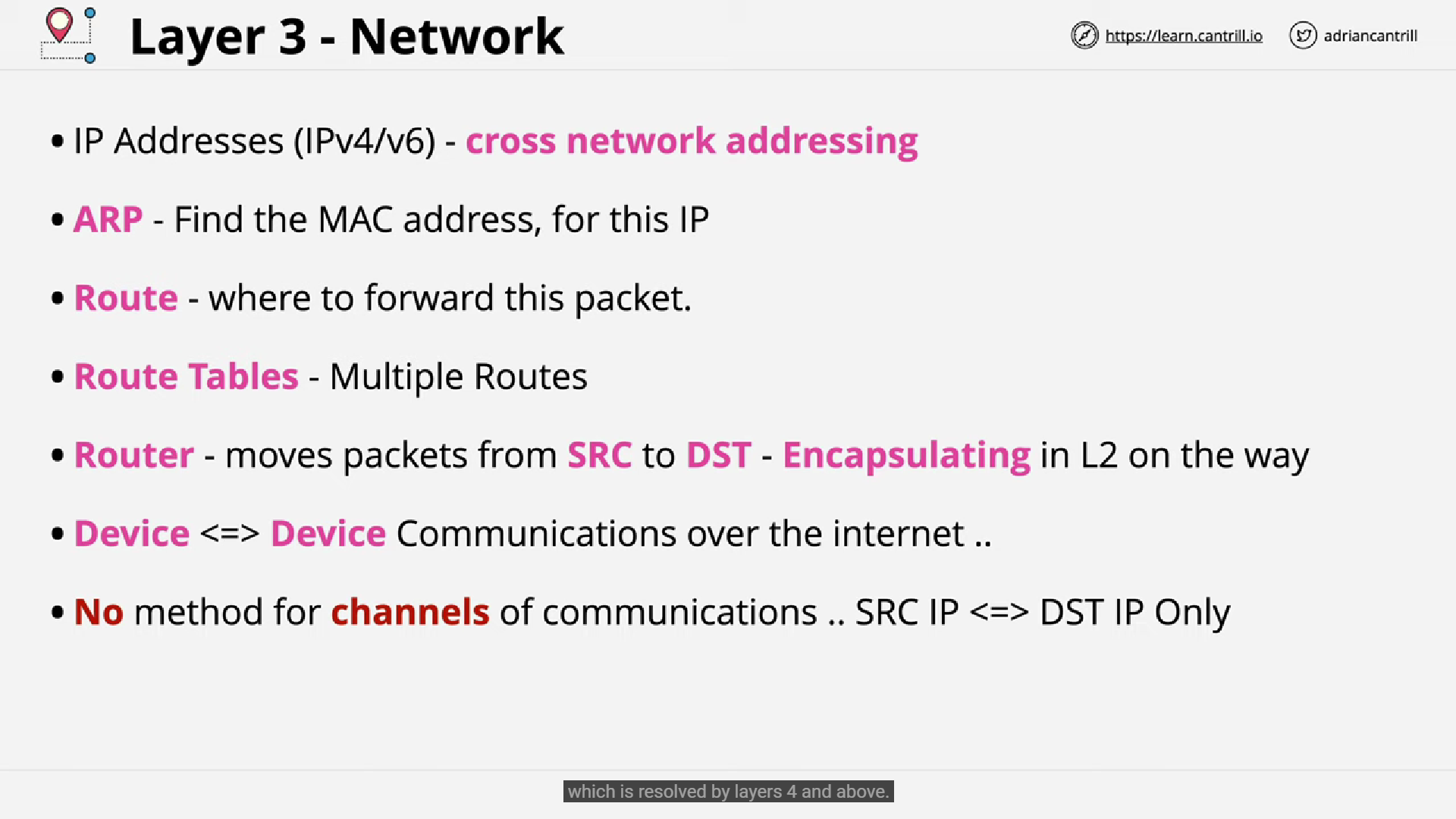
F1- FRAME

P1-PACKET

R1-ROUTER

F1,F2,F3-Frames from layer-2. It encapsulates the IP packets-lets call it as P2 (note that frames with MAC address only changes, whereas IP packets remains the same always to send right data) along with destination MAC address. Destination MAC address is identified using ARP. In routers, first routing table analyses the network. Now it found its R2. Then, using ARP, it gets R2’s MAC address then it frames the packet P2 in F3 frame attaching R2’s MAC address, and sends the packet. Rest is self explanatory





Limitations in layer-3:

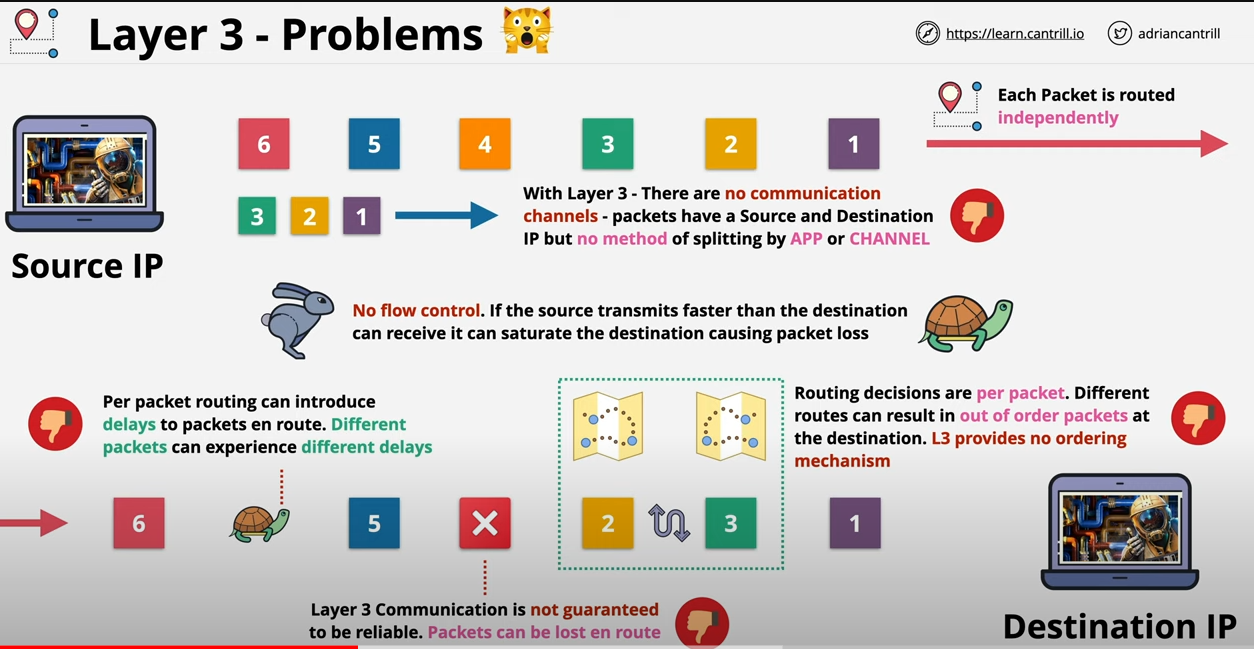
Data cannot be delivered in order. Packets take different routes and different time which is conflicting.

Delay in order

Discard in data due to multiple hops or time to live exceeded

Destined application isn’t known. It can be either: web-browser or mailbox connected to internet.

Internet speed variation.

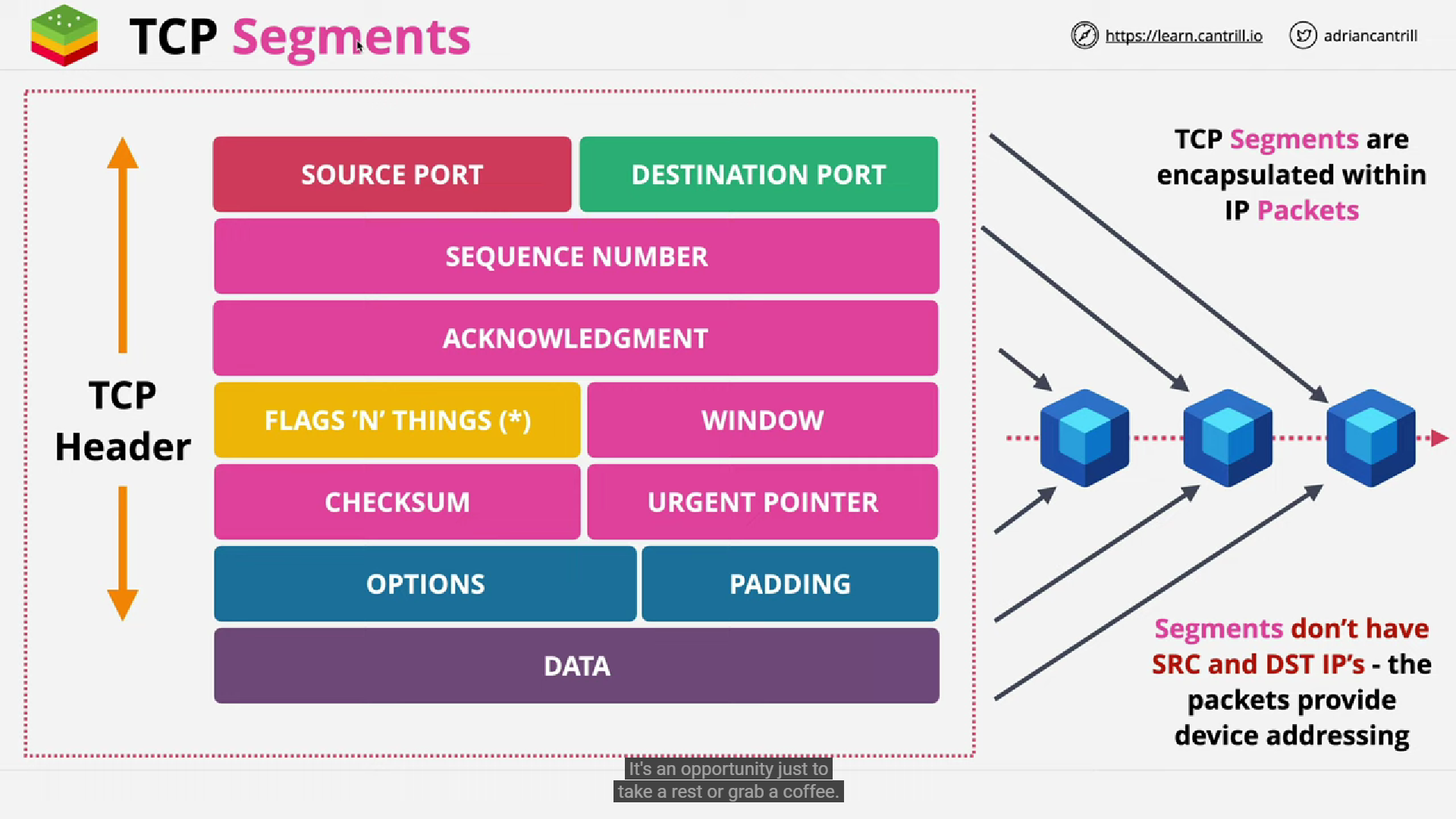
****

**Layer-4:**

**To overcome above issues, we have layer-4 TCP protocol and UDP-User Datagram Protocol.**

**TCP-Reliable and slow**

**UDP-unreliable and fast**



**Below are the segments inside TCP:**

**Sequence** **Number**: add values to each packets. It increments for each packet.

**Acknowledgement**: Once data is sent, received sends acknowledgement to sender.

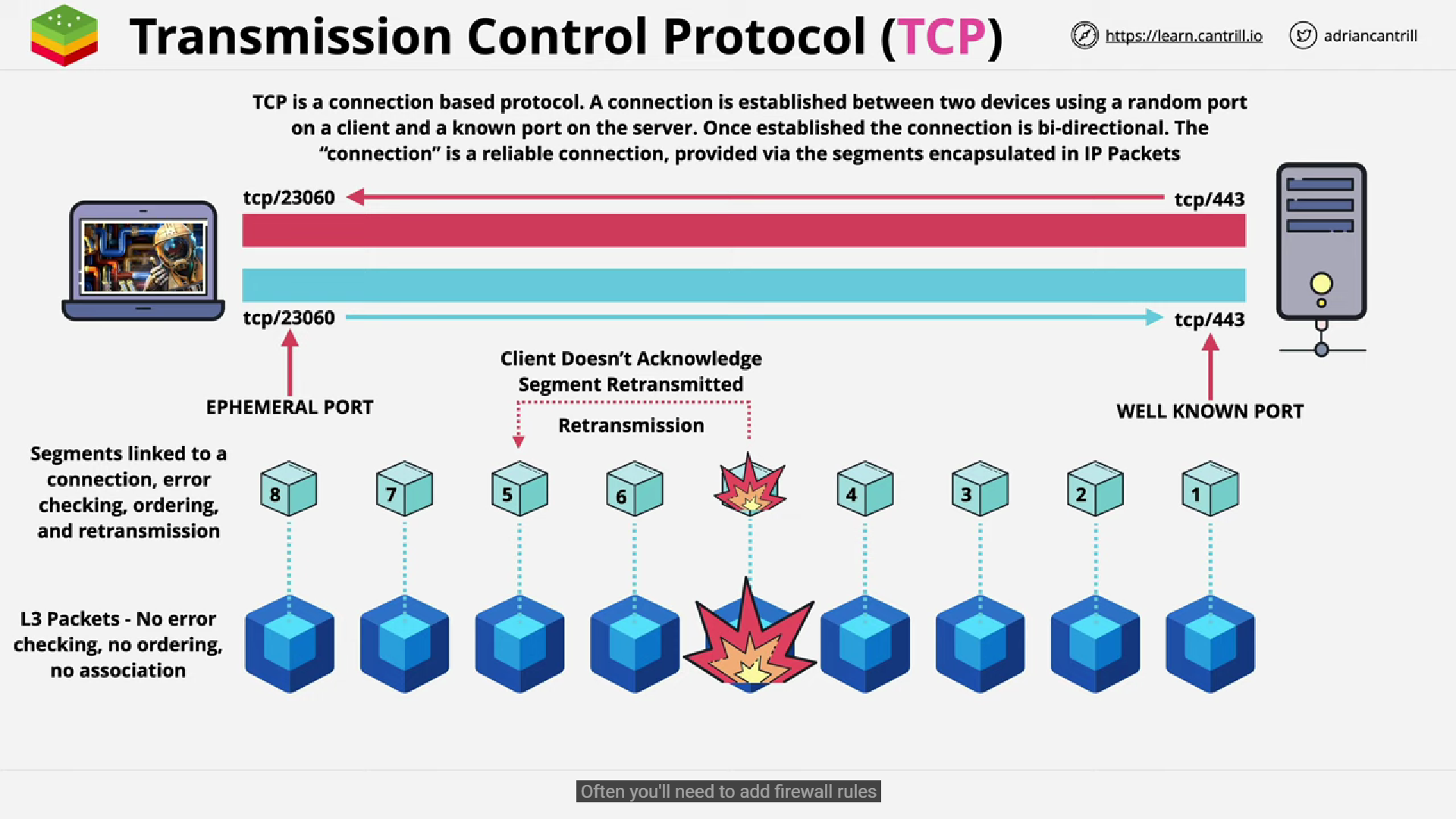
**Window**: It setups the number of acknowledgement to received in between receiving other bytes of incoming data. If limited, it will pause and other data is received. This way, controlling the segments occurs (Segments in l4 is like, Frames in l2 and packets in l3)

**Checksum**- detect error

**Urgent** **pointer** -> 99% data transferand 1% is to control transfer. Used mainly in FTP and Telnet

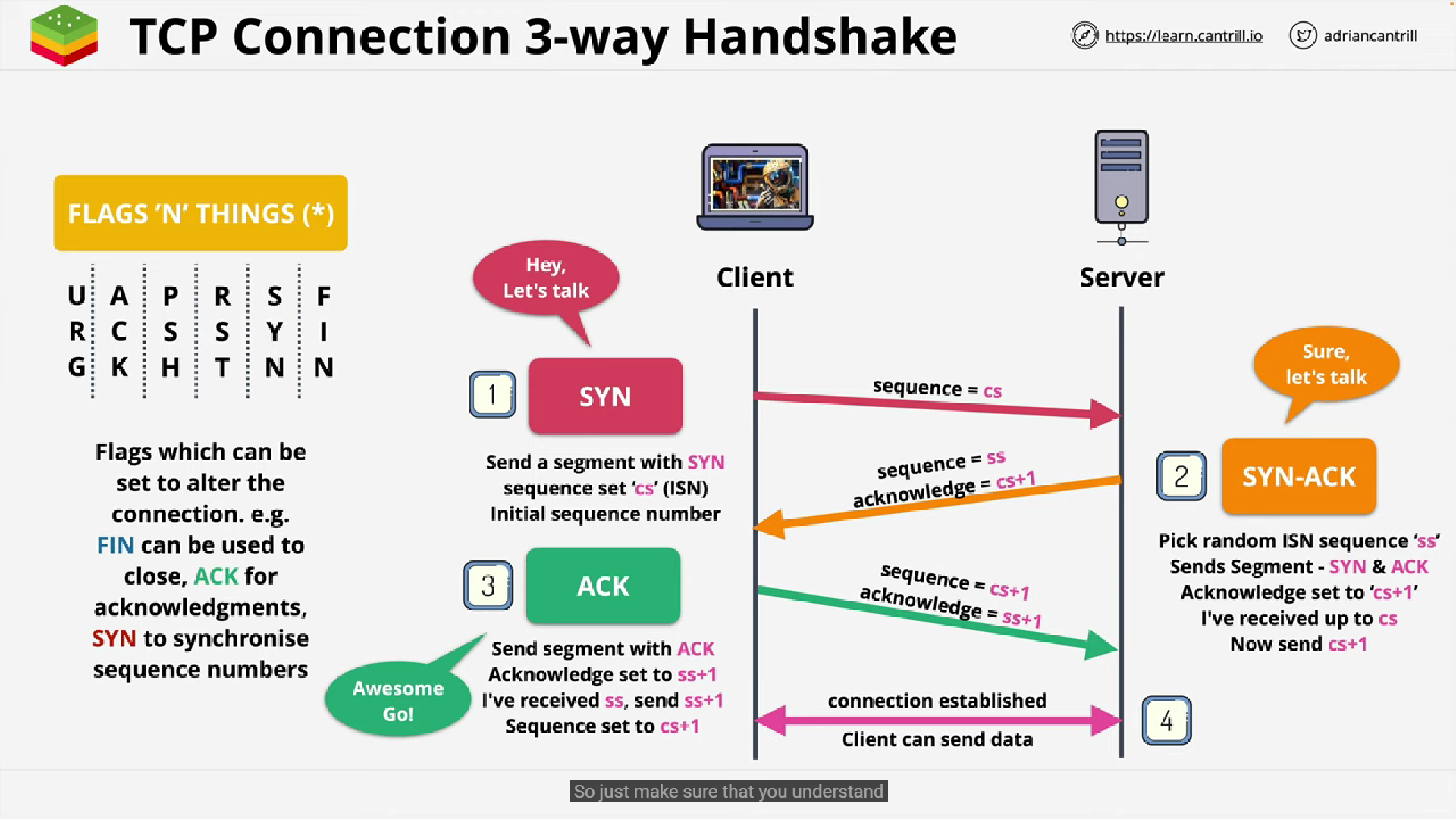
**Source Port and Destination Port:**

Destined application is known. For example, if I have mailbox and browser opened, TCP along with IP helps to reach the right destined application. That’s how we call it as TCP/IP protocol

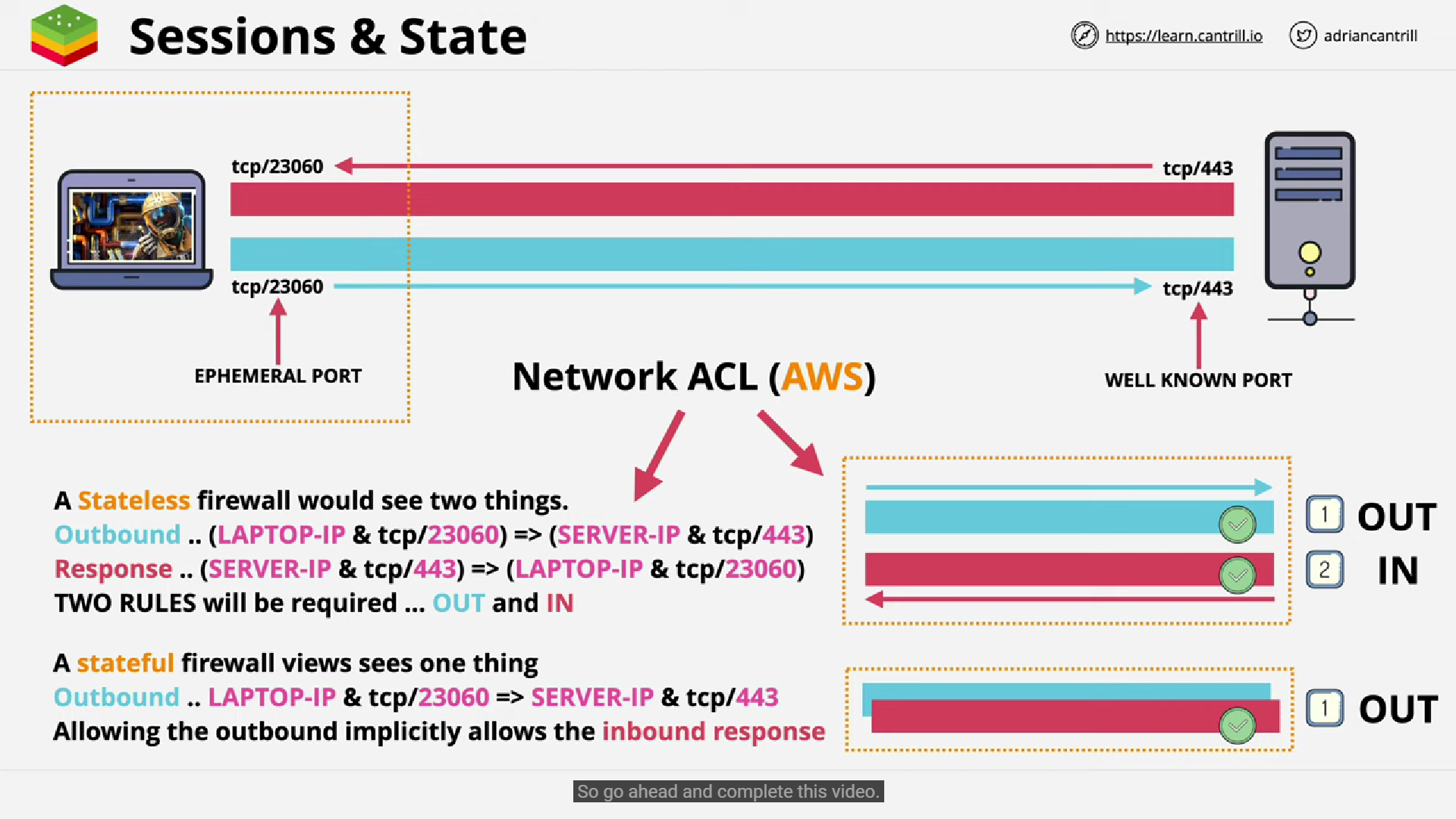


Above screenshot infers that, client is called ephemeral port and server is also called as well known port. Data is being sent as segments to L-3 where it gets encapsulated by packets then by L-2 frames and sent to server. Once sent, server will send back ack, and reverse connection happens in this way, now, server acts as a client and vice versa

Establishing connection between client and server goes like below screenshot:



Layer-5:



**Layer-6:**

**Presentation layer is for encrypting/decrypting/compressing/encoding/decoding**

**Application Layer: HTTP, FTP, DNS, SMTP**

**Zigbee:**

It is like wifi but works in very low frequency connected at home for eg: motion sensor. Smart devices are connected to ZigBee Coordinator(like router) via Zigbee router/mesh (looks like plug). It is wireless, cheap and battery dependant device which has good life. It sleeps when not in use which saves lot of power/battery unlike wifi. It helps the end users to read the energy consumption.

More details: <https://www.youtube.com/watch?v=UmpDXc3cXbU>

Raspberry PI:

PI-> Python

Raspberry PI is like a mini computer, OS can be installed, no cooling system, it has RAM and compact CPU.