CS3.301 Operating Systems and Networks

Networking - Top Down View

Karthik Vaidhyanathan

https://karthikvaidhyanathan.com

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

SERC
Software Engineering Research Centre

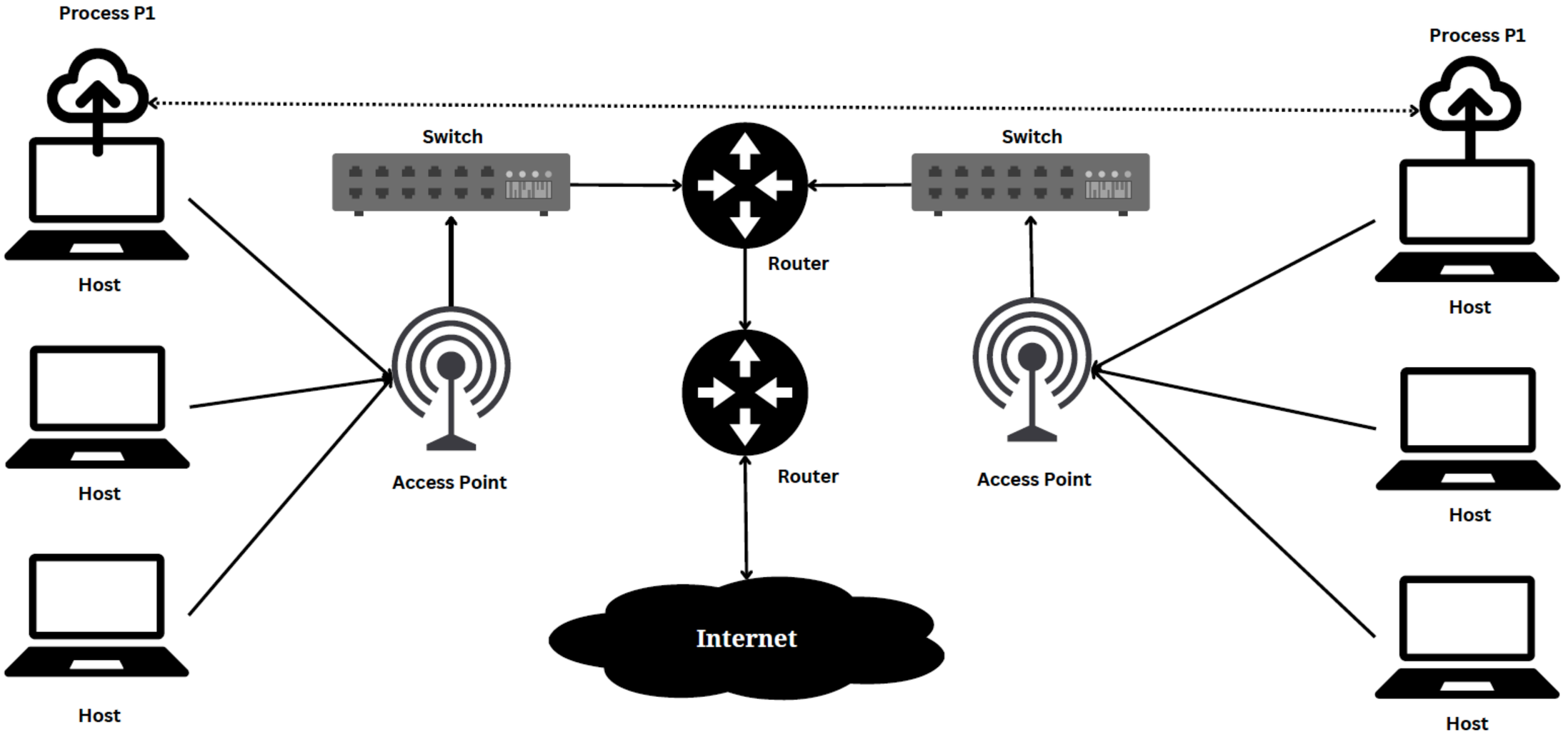
Acknowledgement

The materials used in this presentation have been gathered/adapted/generate from various sources as well as based on my own experiences and knowledge -- Karthik Vaidhyanathan

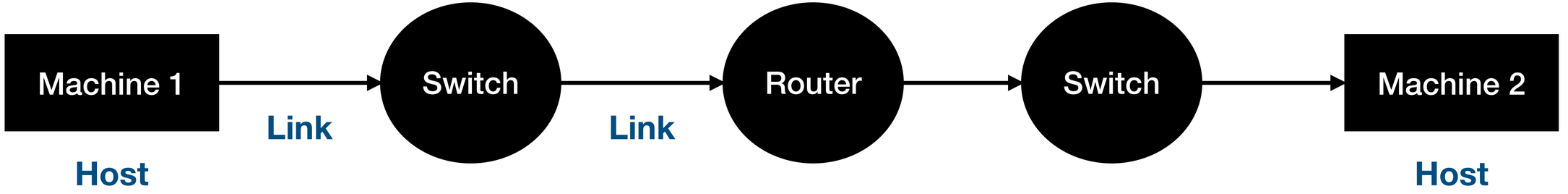
Sources:

- Computer Networks, 6e by Tanebaum, Teamster and Wetherall
- Computer Networks: A Top Down Approach by Kurose and Ross
- Computer Networking essentials, Youtube Channel
- Other online sources which are duly cited

The Bigger Picture



Components of a network



Process Communicating over network

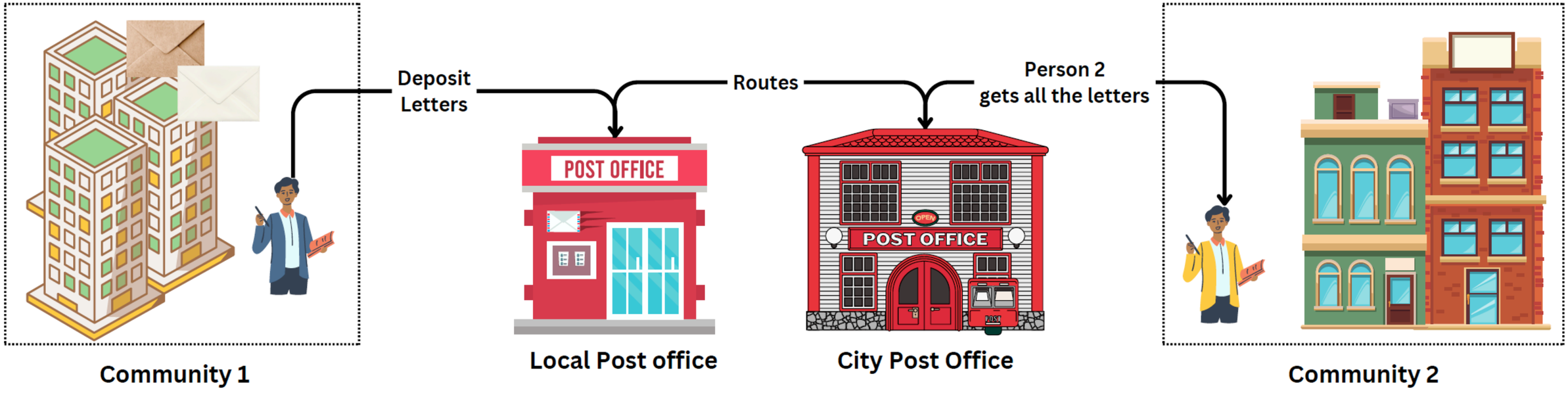
- Process A (eg: Whatsapp) is executing in Host 1
- Process B (whatsapp) executing in Host 2
- Process A wants to communicate with Process B
  - Some system call is made to access the network
    - Leads to an interrupt
    - Process A should know where process B is
    - Hardware support is needed (some network device with drivers)

An Illustrative Scenario

People in community send letters/couriers

One person is collecting all the letters/couriers

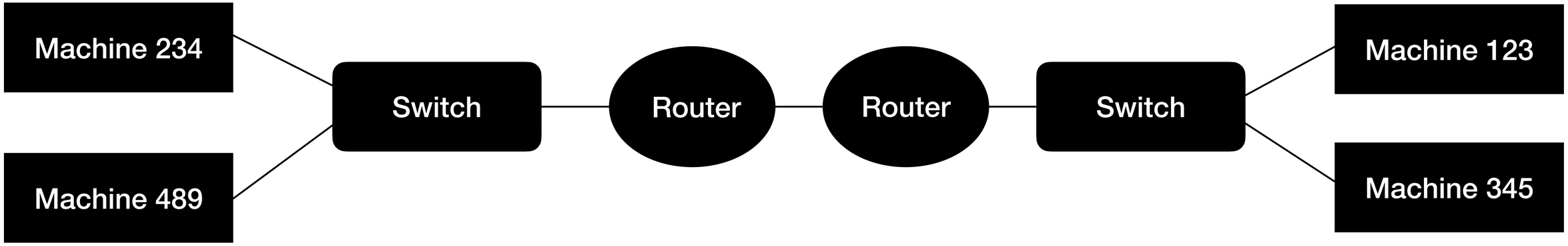
Person delivers the letter to each person



Key points: Door number, building number, Post office has an identifier, etc.

Lets put thing in perspective

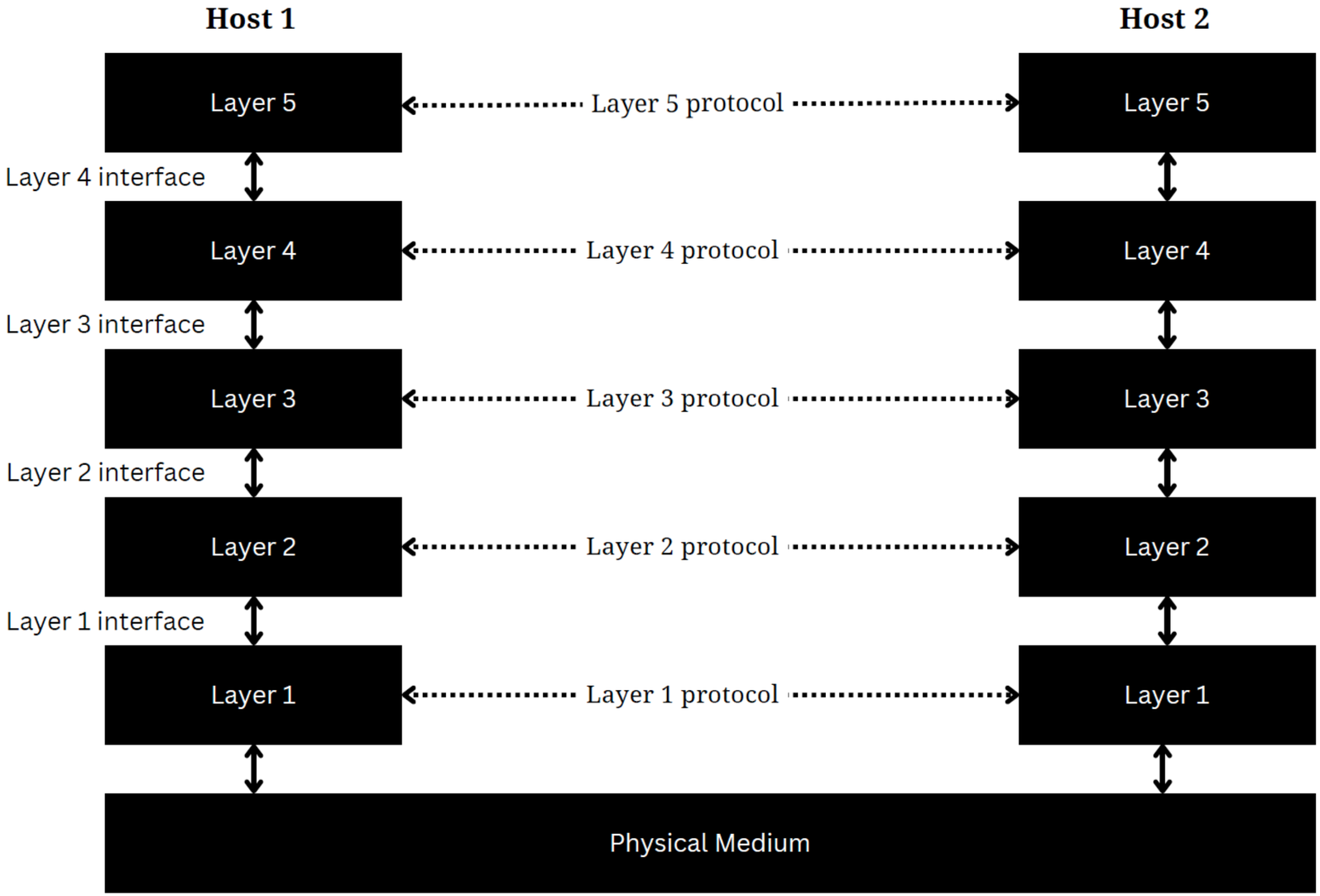
How does communication work if 234 wants to send data to 345?



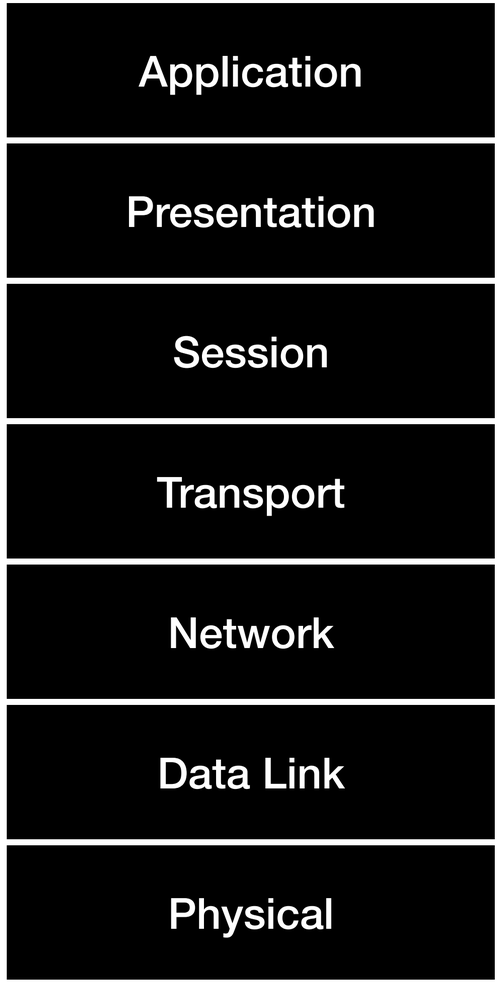
Lets take this to Process communication

- Process A (eg: Whatsapp) is executing in Host 1
  - Process B (Whatsapp) is executing in Host 2
- Host 1 will have an address, same is the case with host 2
- How to ensure the data reaches from Host 1 to Host 2?
  - What all needs to be considered?
  - Remember: There will be multiple processes that are executing in a host

Networking Layers



The OSI Model

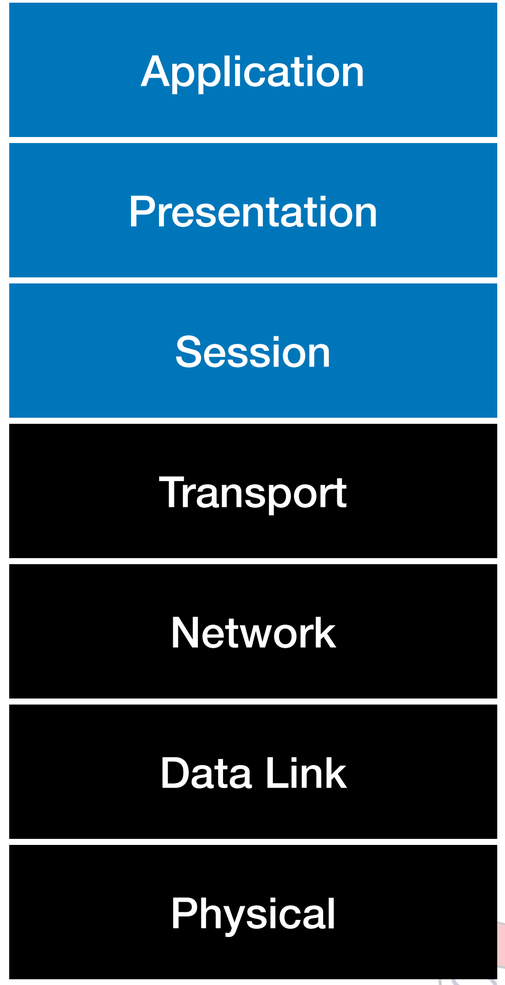


- Open System Interconnection (OSI)
- A Conceptual framework used to understand how communication works through different layers
- Divides the network communication process into seven layers
- Developed to facilitate interoperability between different technologies
- Each layer has a specific function. If they all do what they are supposed to do => sharing of data

Session, Presentation and Application

Application to Application

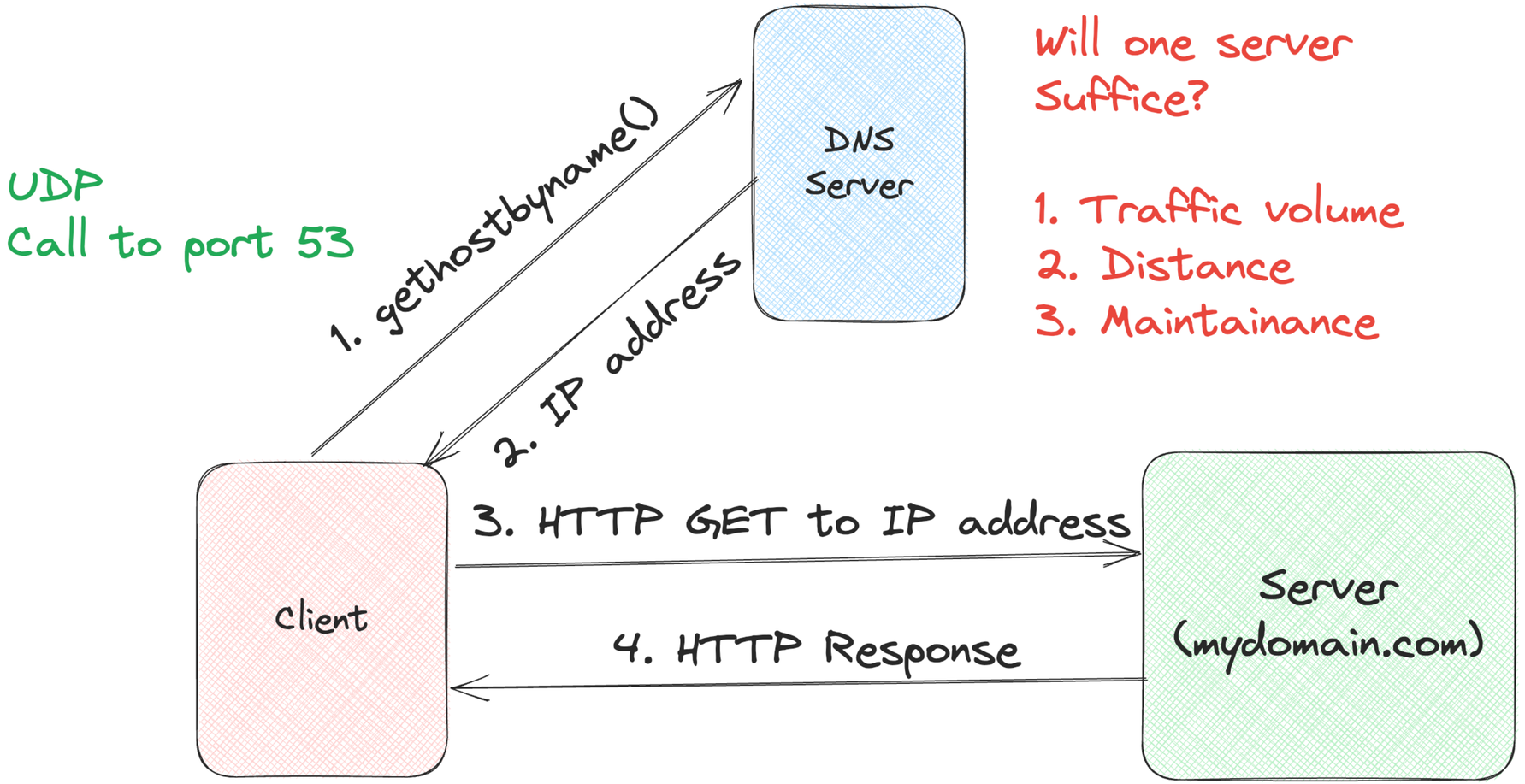
- **Session Layer (L5)**
  - Manages connection between different devices
  - Establishing, maintaining and terminating connections
- **Presentation Layer (L6)**
  - Ensures that data is in format that sender and receiver can understand
  - Manages data encryption, compression
- **Application Layer (L7)**
  - Provides network services to the application processes
  - Eg: web browser, email clients, other softwares/apps



Application Layer Protocol
What does it mean?

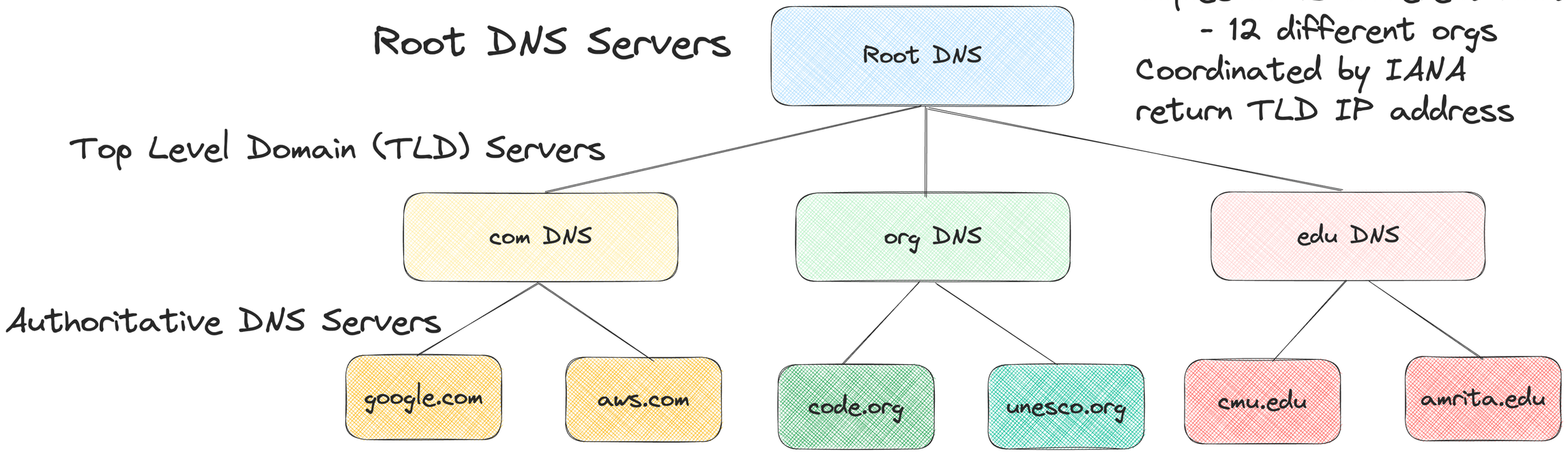
- Application layer protocol defines the following:
  - Types of message exchanges (request/response)
  - Syntax of various message types
  - Semantics of the fields
  - When and how the process sends and responds to messages
- Some protocols: HTTP, SMTP, DNS, etc.

Mapping domain name to IP: DNS



DNS: Distributed Hierarchical Database

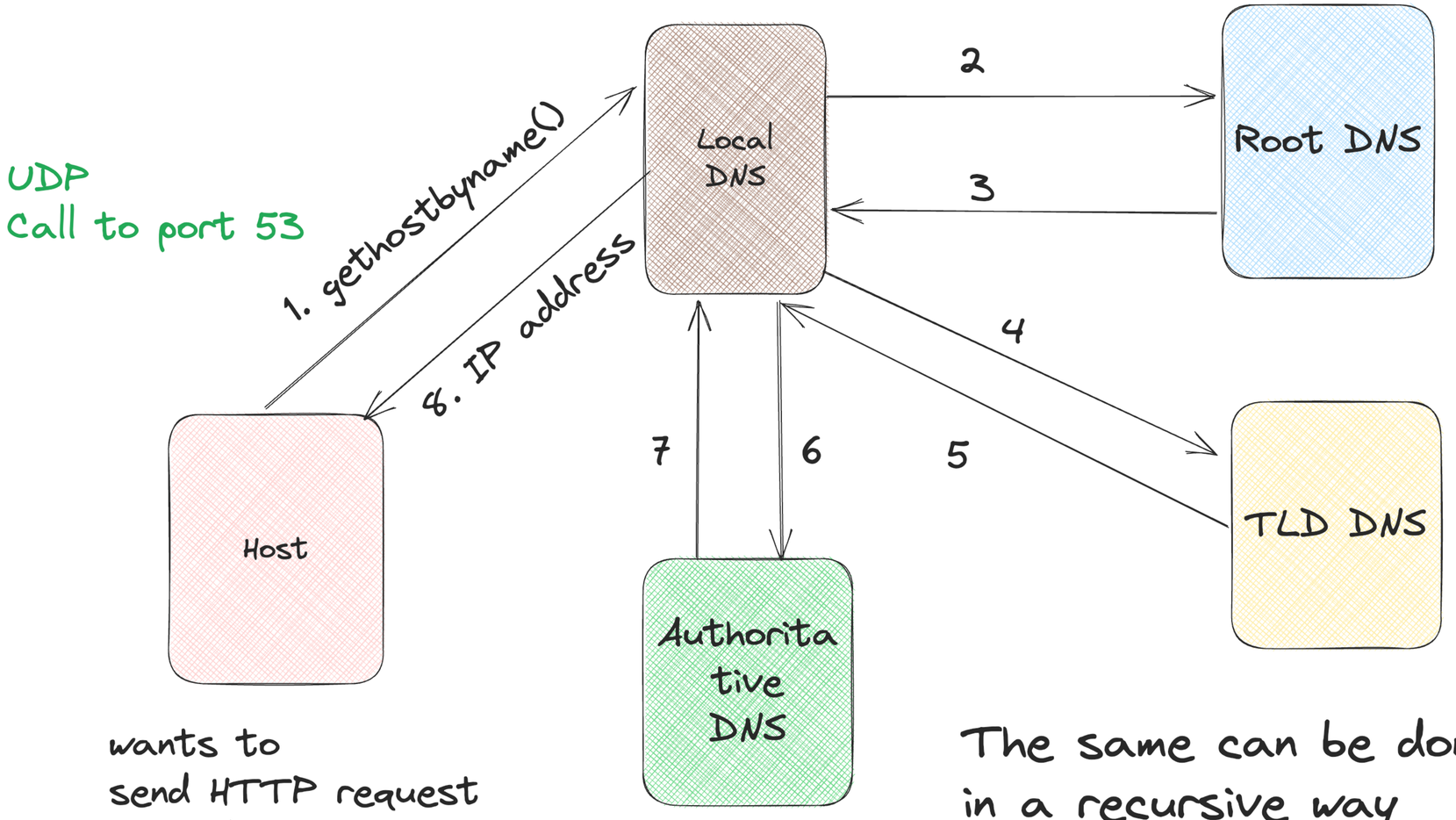
More than 1000 root servers
Copies of 13 different root servers
- 12 different orgs
Coordinated by IANA
return TLD IP address



TLD Servers - can be maintained by orgs, provide IP of authoritative DNS Servers
Authoritative DNS servers - Orgs can choose to implement their own or go for third party
All DNS records have to be made public - that maps hosts to IP address

Local DNS

Each ISP can have DNS and clients can connect to that

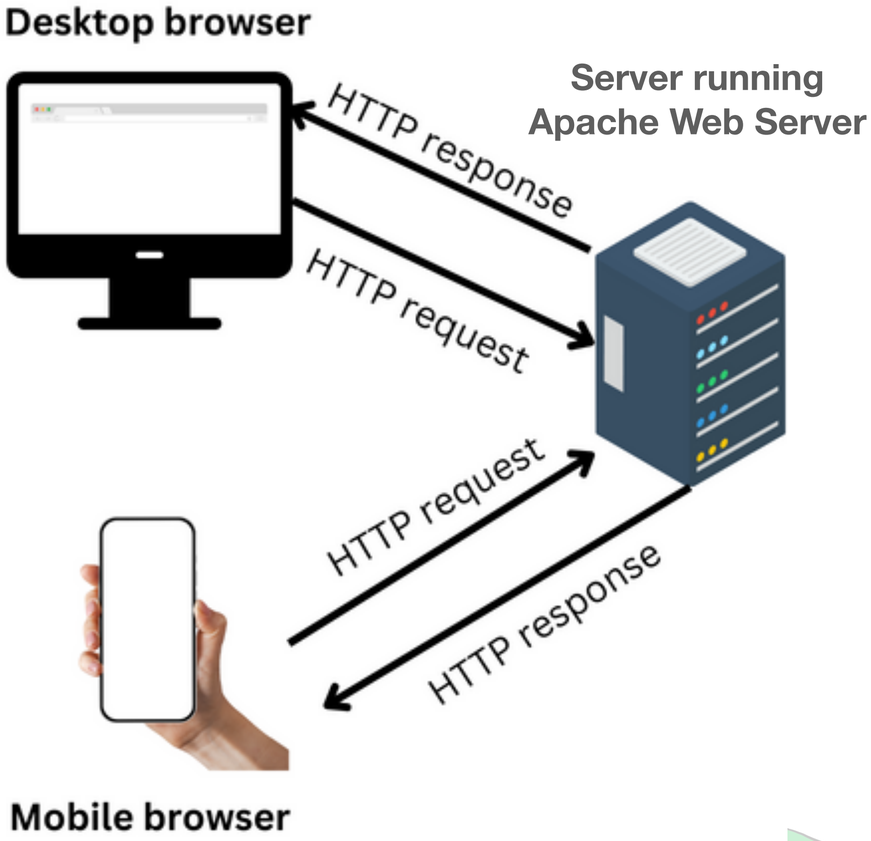


Caching can be done at the ISP Local DNS

The same can be done in a recursive way putting overhead on contacted server

HTTP: Hyper Text Transfer Protocol

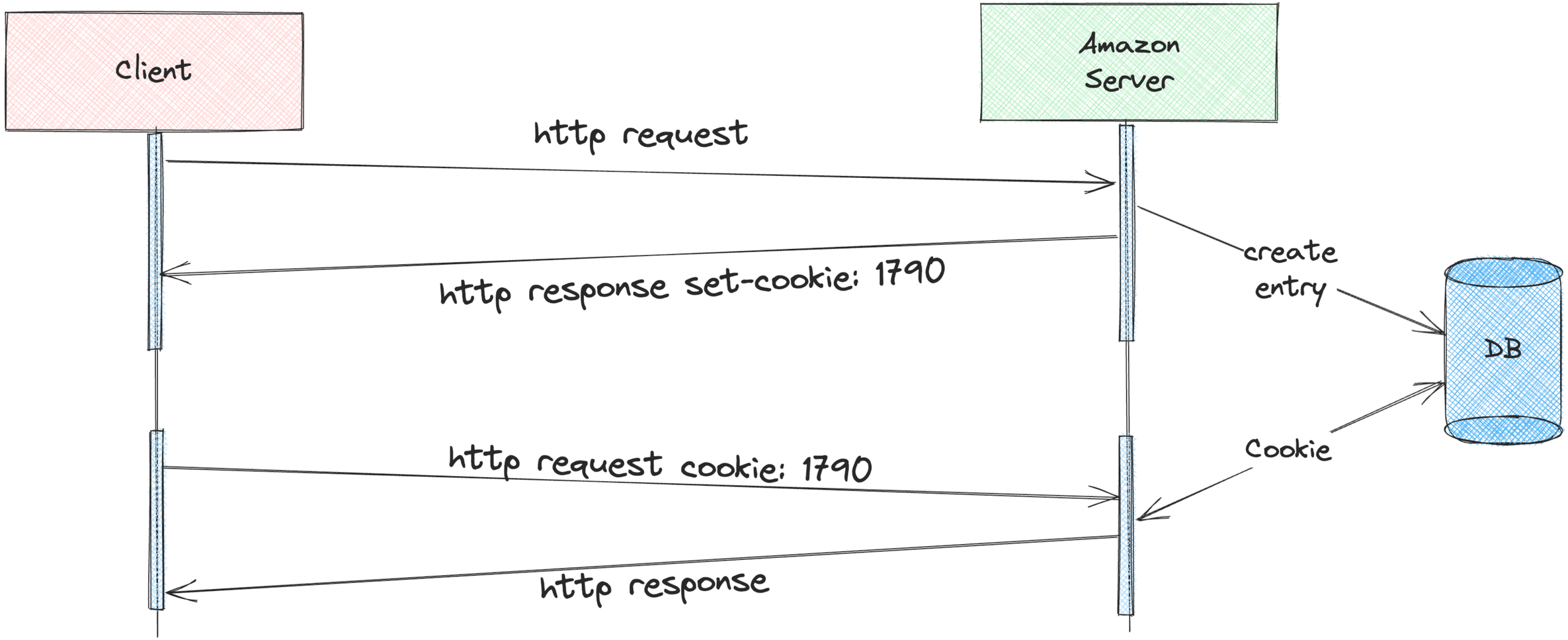
- Application layer protocol of the web
- Implemented in two programs: Client and Server
- HTTP protocol defines structure of messages
- **Client:** browser that sends requests, receives and displays web objects (using HTTP protocol)
- **Server:** Web server that sends objects in response to requests (using HTTP protocol)
- Uses **TCP** and it is stateless



https://iiit.ac.in/samplePage.html
Host name: iiii.ac.in
Object: samplePage.html

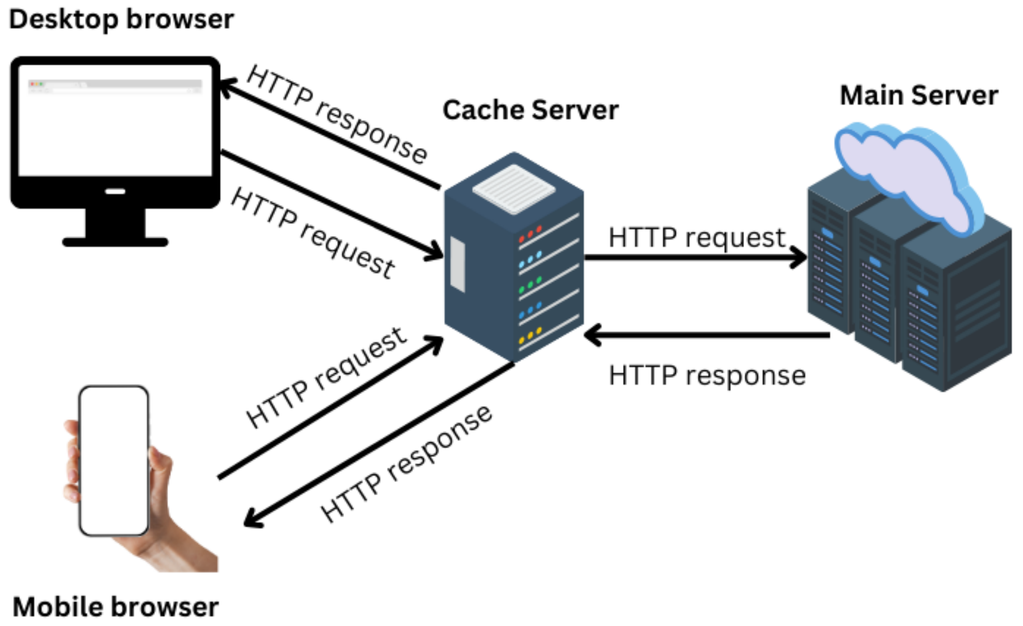
How to store information in stateless Protocol?

Using Cookies



Web Caches

- Not every time we need to access the main (original) web server
- We can have proxy server that satisfies request on behalf of main server
- Browser can be controlled to point towards a cache (mentioned in response header)
  - If cache hit: return object from cache
  - Else cache request object from main server and returns it
- Conditional GET is used to update Cache (“if-modified-since”)

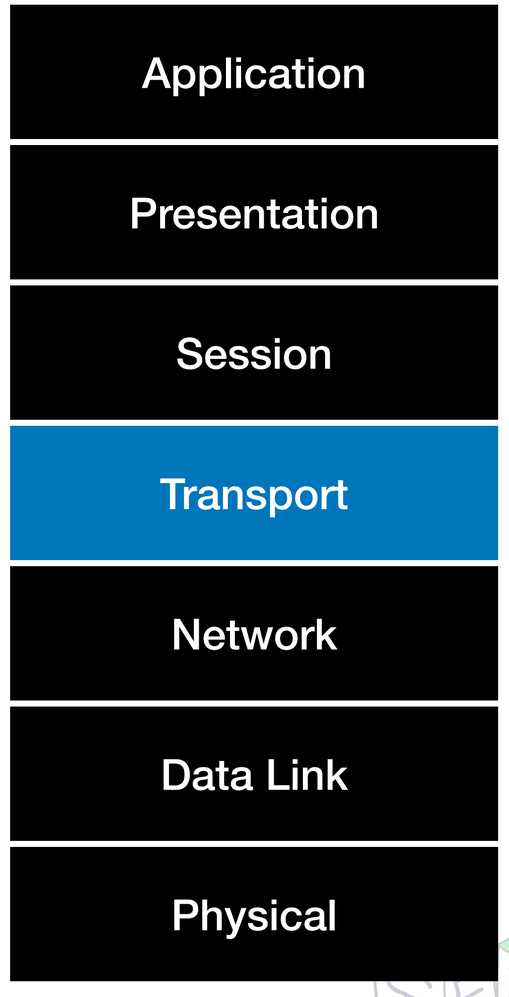



```
Cache-Control: max-age=<seconds>
```

```
Cache-Control: no-cache
```

On to Transport Layer (L4)

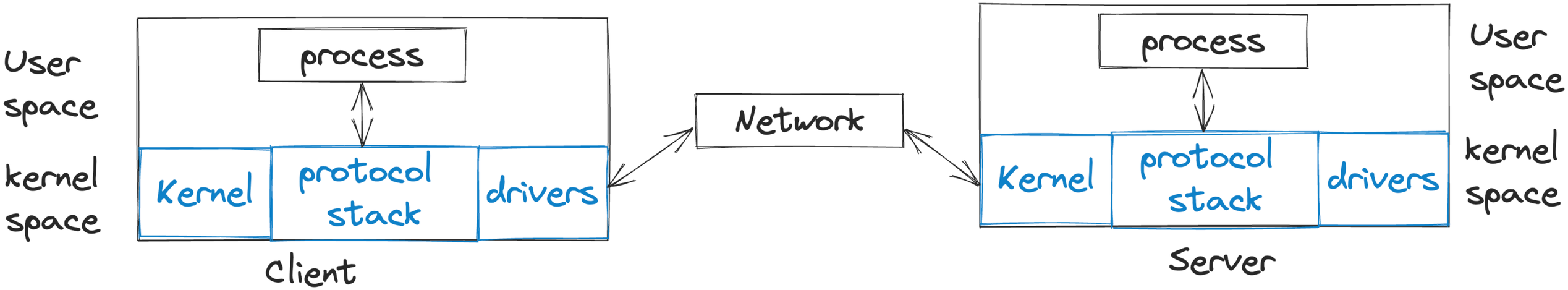
- Process gets the data delivered through support of transport layer
- Addressing scheme: Ports
- Layer 4 has an addressing scheme to guarantee message delivery
  - Ports! (0 - 65535), Privileged: 0-1023, Registered: 1024 - 49151
- Two strategies/protocols that allows this
  - **Transmission Control Protocol (TCP)** - favours reliability
  - **User Datagram Protocol (UDP)** - favours efficiency



TCP vs UDP

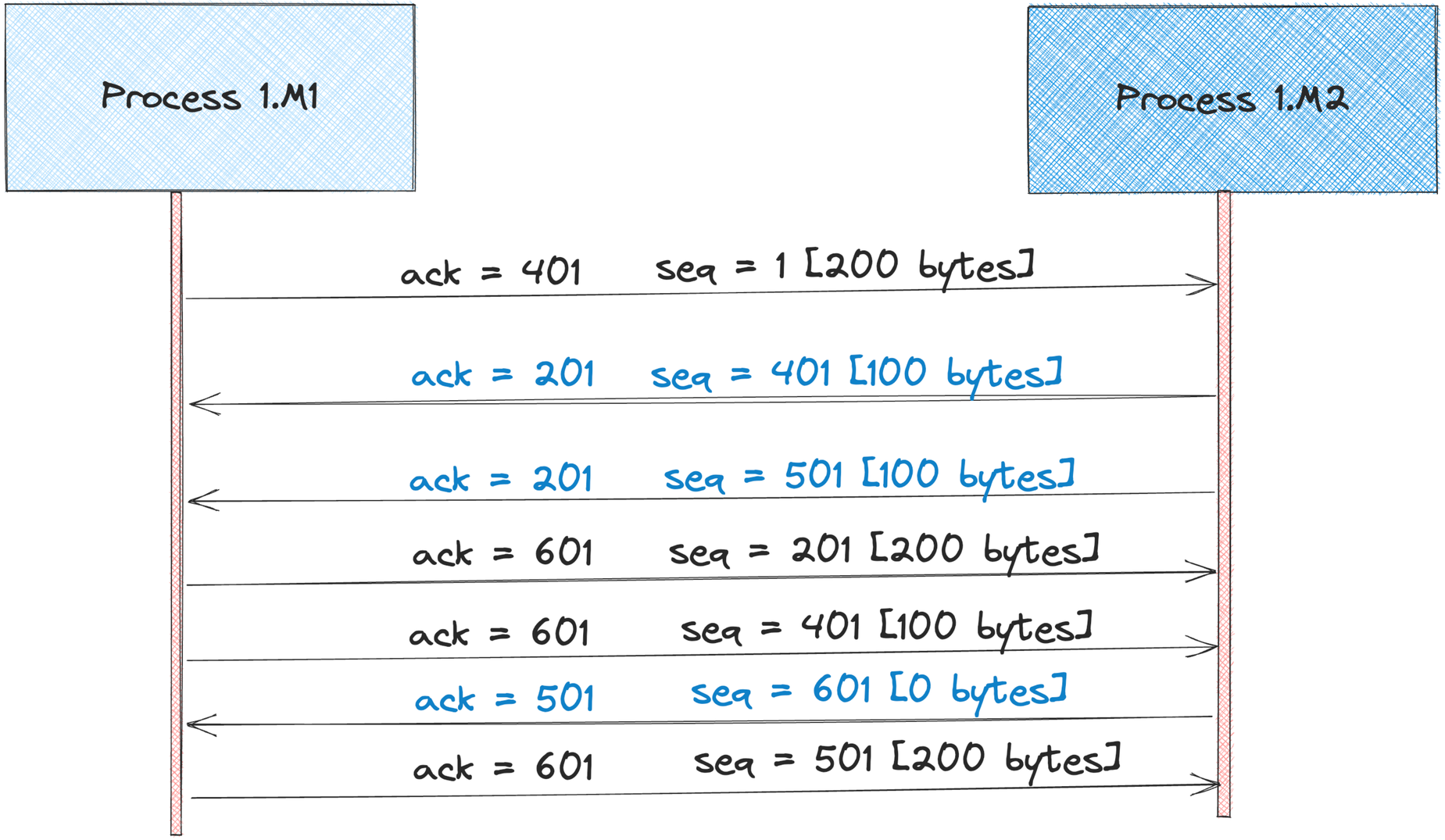
TCP	UDP
Connection Oriented	Not Connection Oriented
Reliability (order is maintained and retransmission)	Unreliable
Higher overhead - reliability, error checking, etc	Low overhead
Flow control (based on network)	No implicit flow control
Error detection - retransmit erroneous packets	Has some error checking - Erroneous packets are discarded without notification
Congestion Control	No Congestion Control
Use cases: HTTP/HTTPS, File transfer, Mail	Use cases: Streaming data, VoIP, DNS queries, ..

The role of Operating System



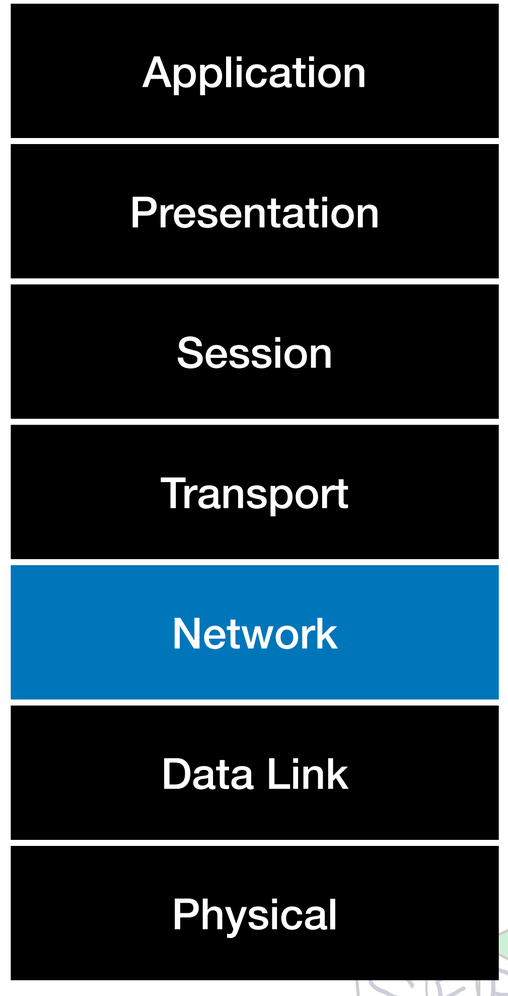
- Software component in the OS that supports network calls - **Protocol stack**
- Provides Service primitives which are nothing but system calls - **Some API?**

TCP and how it works!

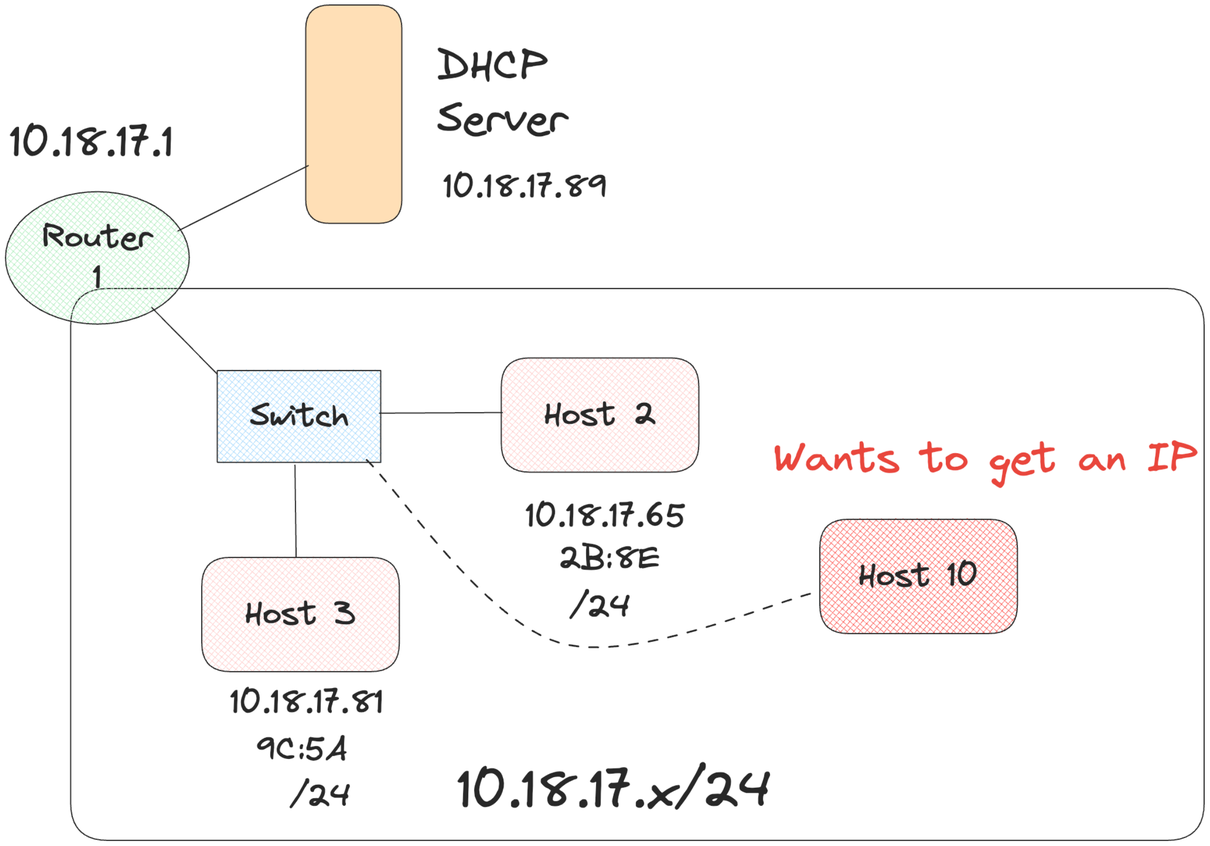


Network Layer (L3)
End-to-end Communication

- Manages routing through different routes in a large network
- Uses an addressing scheme - IP addressing
  - 32 bits represented as 4 octets (IPv4)
- Performs functionalities such as Logical addressing (IP), Path selection and packet forwarding
- L3 technologies: routers, even hosts are L3, L3 switches



Getting IP Address - DHCP

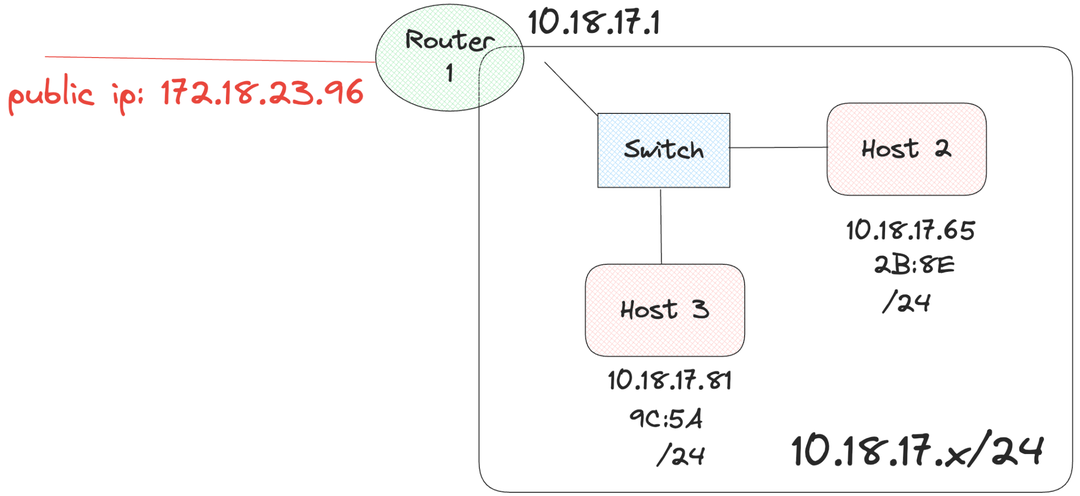


- Host 10 is the client here
- It sends out a broadcast DHCP request to every node in the network to get DHCP server
- Every device in the network will get the request
- DHCP runs over UDP
- Client uses port 68 and server port (listens on port 67)

Network Address Translation (NAT)

NAT Translation Table

WAN side address	LAN side address
172.18.23.96 5501	10.18.17.81 3801
....	.....



- All devices in the network share just one IPV4 address as far as the outside world is concerned
- NAT allows a router (similar device) to translate private IP addresses to its own public IP address
- When devices from network wants to communicate with outside network:
  - NAT modifies the source IP to make it appear that communication is from the larger public IP
  - A translation table is used for managing the translations
- **Multiple types:** Static NAT, Dynamic NAT, Port Address Translation or NAT Overload

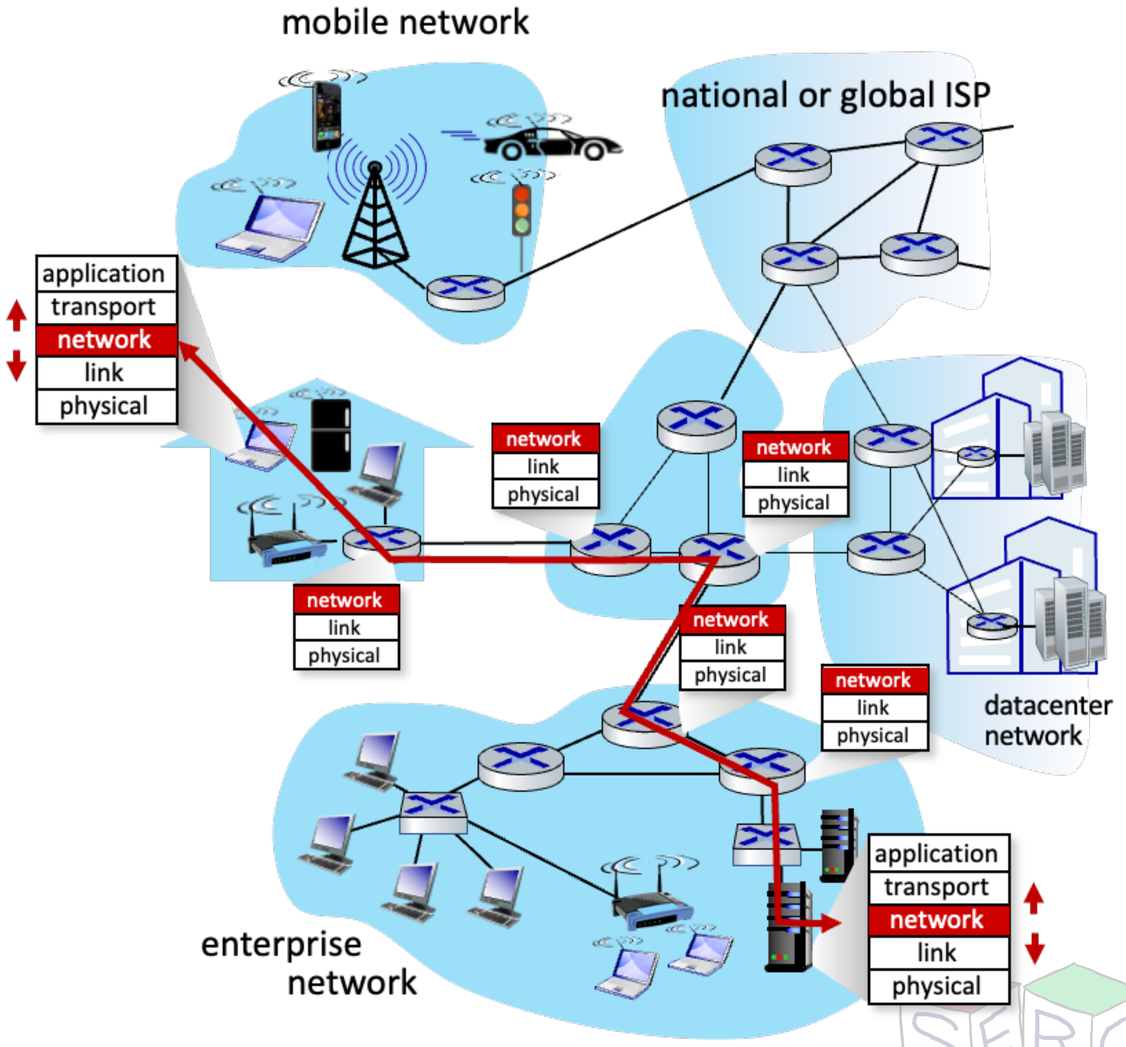
Network Layer - Functionalities

Addressing

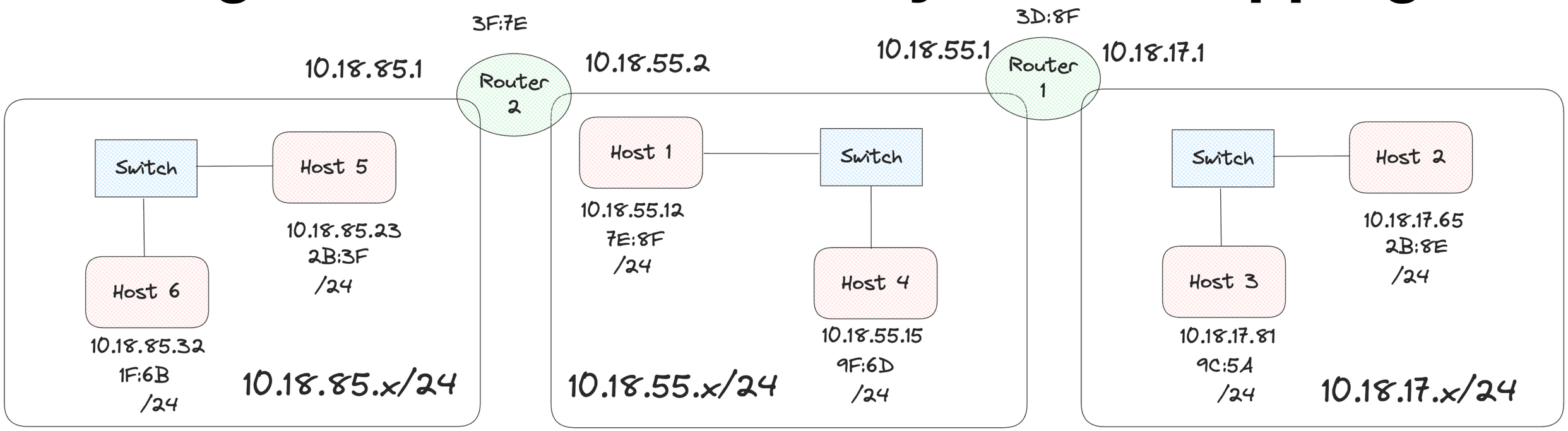
- Devices in network are assigned logical address for unique identification - IP
- Network layer uses IP to forward packets to the intended destinations

Route Determination

- Identifies best path for packets to reach to destination
- This process is dynamic and changes based on network conditions



Routing Tables - Static and Dynamic Mappings



Type	Destination	Interface
DC	**10.18.85.x/24**	Left
DC	**10.18.55.x/24**	Right
Static	**10.18.17.x/24**	10.18.55.1

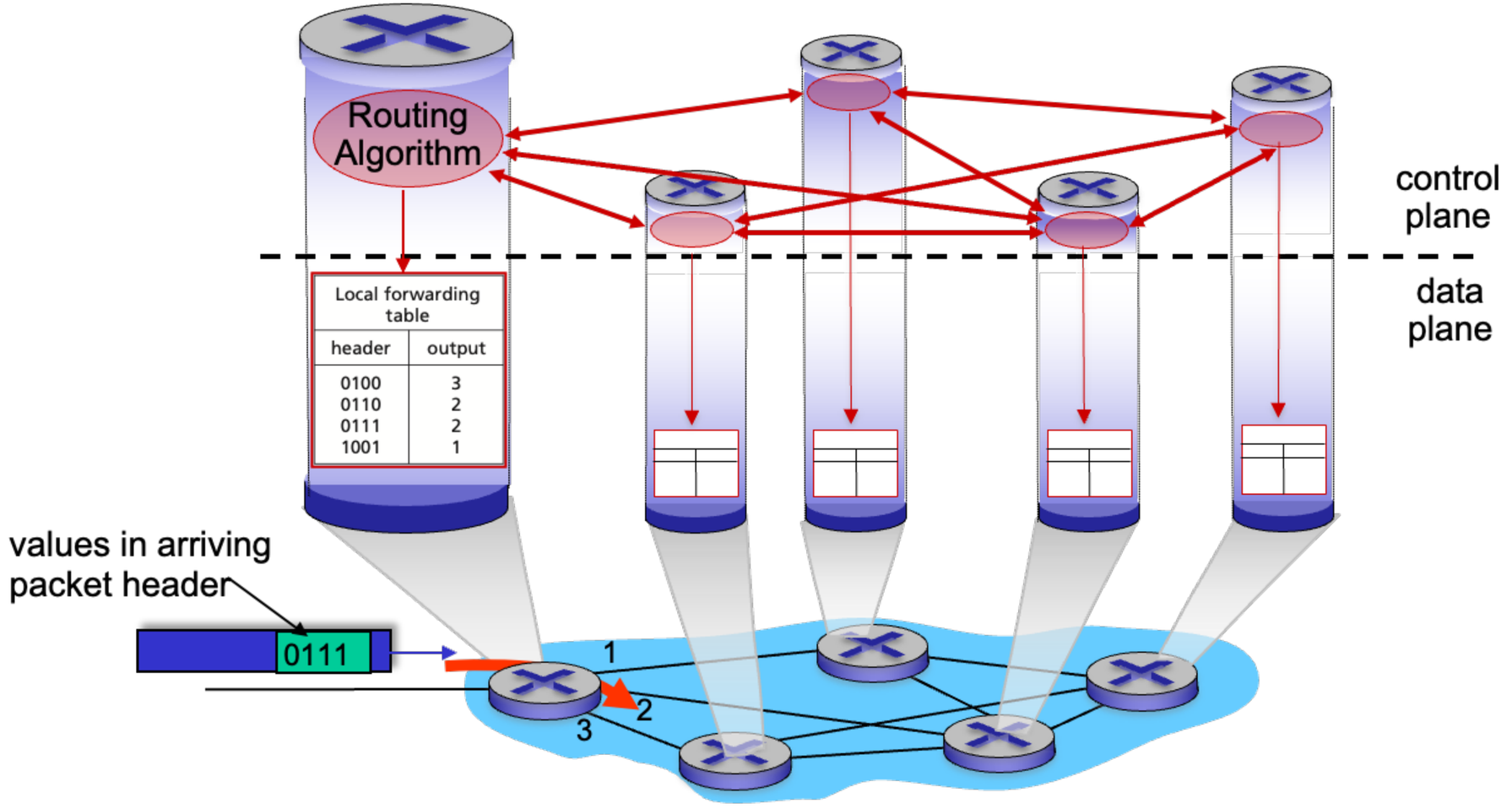
Router 2 routing table

Type	Destination	Interface
DC	**10.18.55.x/24**	Left
DC	**10.18.17.x/24**	Right
Static	**10.18.85.x/24**	10.18.55.2

Router 1 routing table

Routers can also Learn about the address

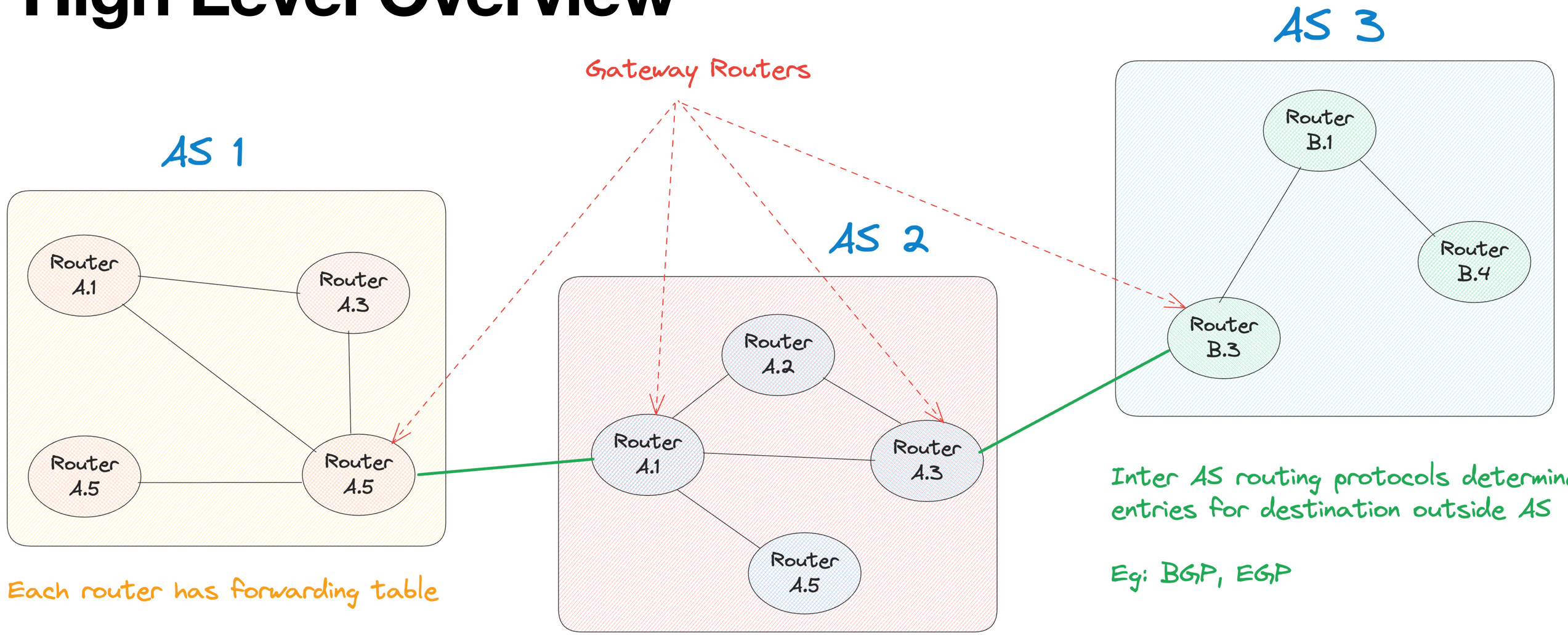
Traditional Control Plane Approach



Internet approach to scalable routing

- Aggregate routers into regions known as **“Autonomous Systems” (AS)** a.k.a “domains”
  - Total of around 70,000 AS’s have been assigned not all are active
- There are mechanisms for handling routing within the domain and across AS
- **Intra-AS or Intra-domain**
  - All routers in AS must run the same intra-domain protocol
  - There is a **gateway router** at the edge of each AS which connects with router in another AS
- **Inter-AS or Inter-domain**
  - Routing among AS’s
  - Gateways perform inter-domain as well as intra-domain within their network

High Level Overview



Each router has forwarding table

Configured by both intra and inter AS routing algorithms

Intra AS routing protocols determine entries for destination within AS

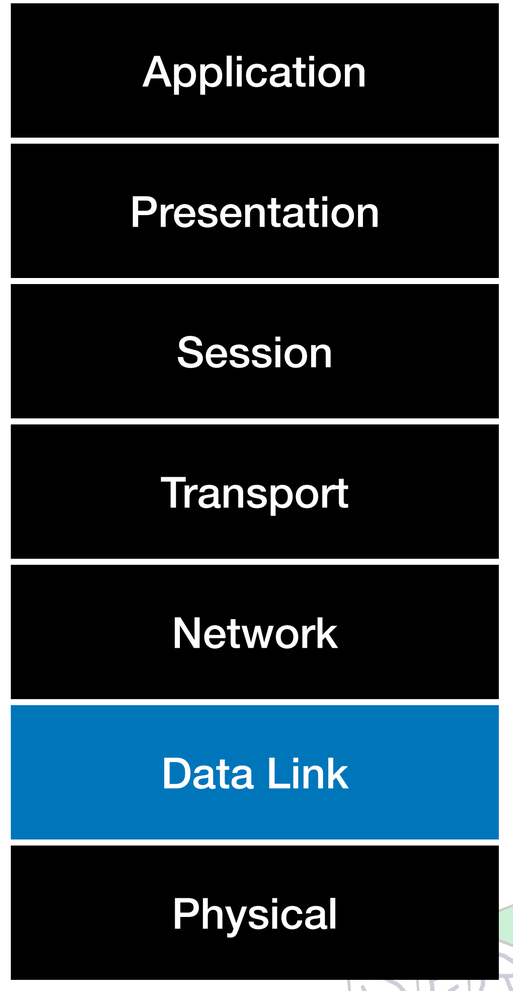
Eg: OSPF, EIGP, RIP

Inter AS routing protocols determine entries for destination outside AS

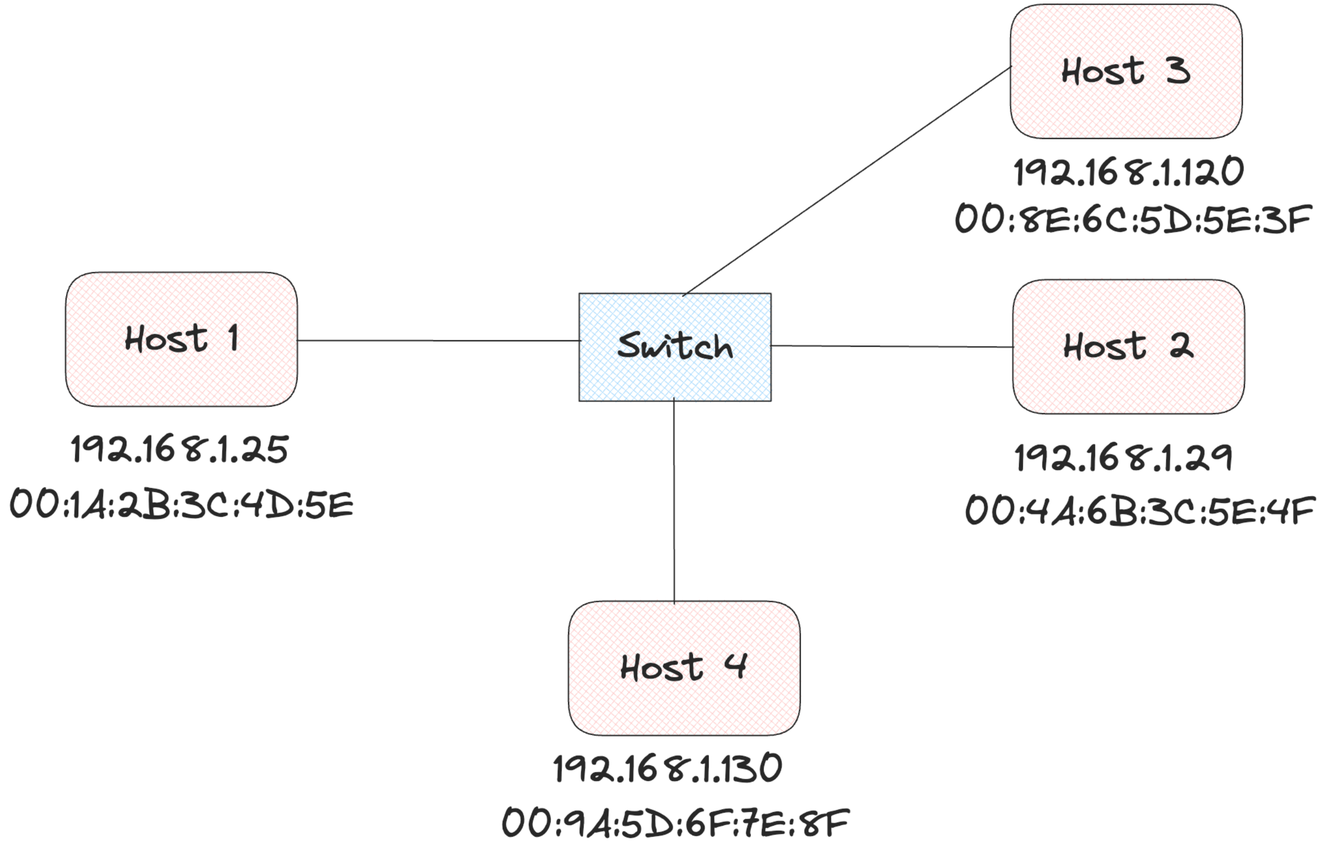
Eg: BGP, EGP

Data Link Layer (L2)

- Responsibility of transferring datagram from one node to a **physically adjacent node** over a link (no intermediate L3 routers)
- Supports **hop-to-hop** communication
- Ensures reliable connection link between two directly connected nodes (flow control, error correction and detection, etc.)
- Supported by **Media Access Control (MAC)** addressing
- Addressing scheme: MAC addressing (48 bit address, 12 hex digits, 6 bytes)
    - Eg: **00:1A:2B:3C:4D:5E**
    - First three identify manufacturer (IEEE)
    - Next three are assigned by manufacturer and should be unique



ARP - Address Resolution Protocol

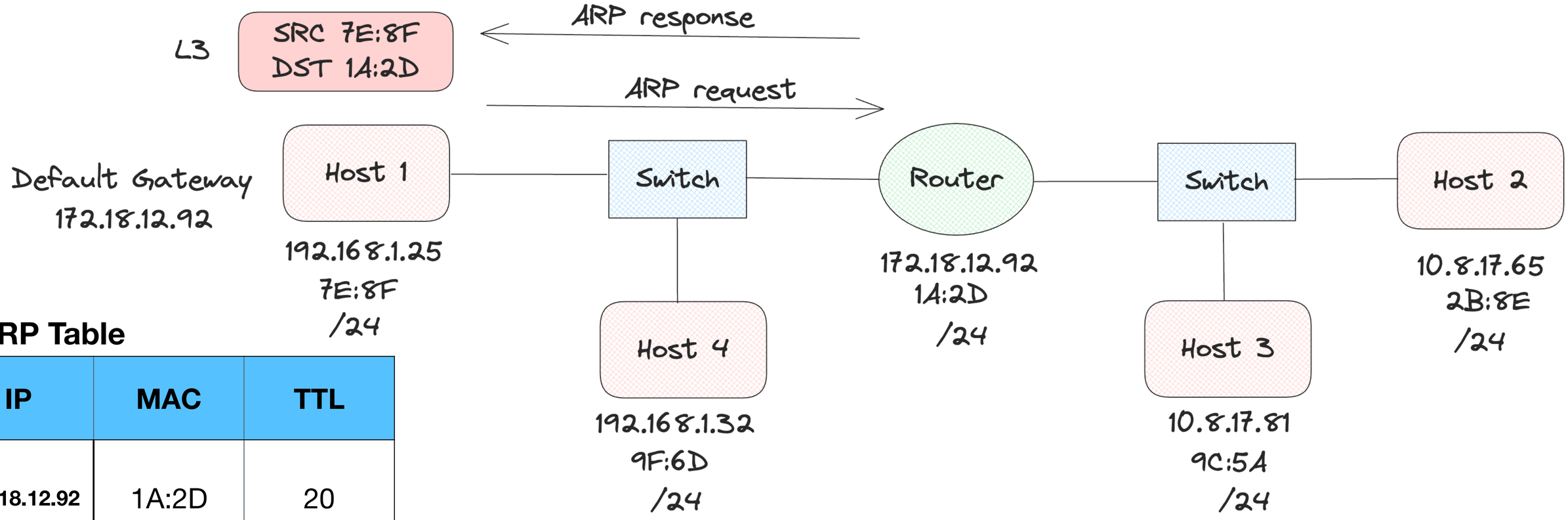


- Each IP node (router, host) on the LAN has a table - **ARP Table**
- IP/MAC address mappings for some LAN nodes
  - **<ip address, MAC address, TTL>**
- **TTL:** Time to live, time after which the mapping will be forgotten (20 mins)

ARP Query

- When ARP query is sent initially, it is broadcast to all the nodes in the network
- The request includes senders IP address and MAC address
- It also includes the target IP address
  - Destination MAC is set as **FF:FF:FF:FF:FF:FF** (Reserved to send packet to all in the network)
  - If different network then send to the IP address of the gateway router
- All the nodes will have an ARP cache or ARP table
  - It stores the mapping, when the initial request is send from one host, all other hosts stores the incoming mapping as well

ARP Working



ARP Table

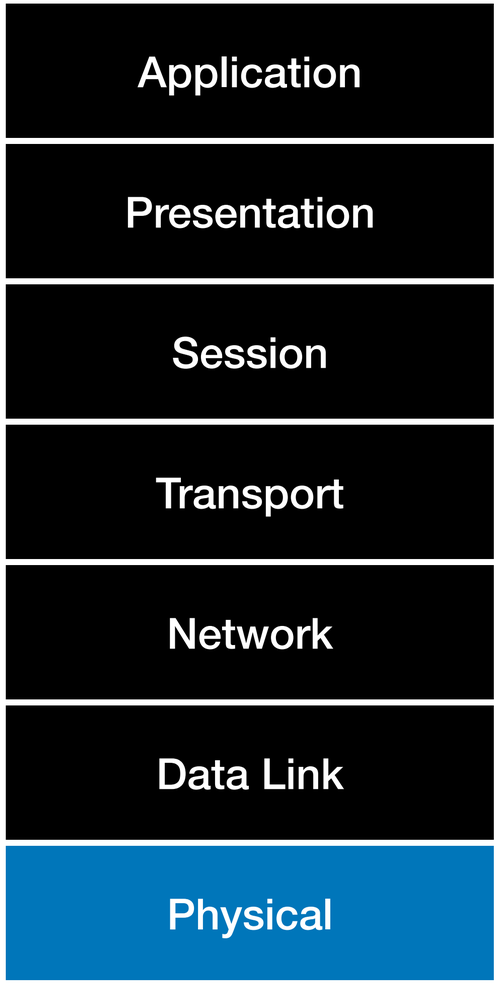
IP	MAC	TTL
172.18.12.92	1A:2D	20

- The ARP process needs to happen only once, since router is the gateway
- First step - Check if the IP of the receiver is in the same or different network
- If different network => Send ARP to gateway else, send ARP to all nodes in the network (FF:FF….:FF)

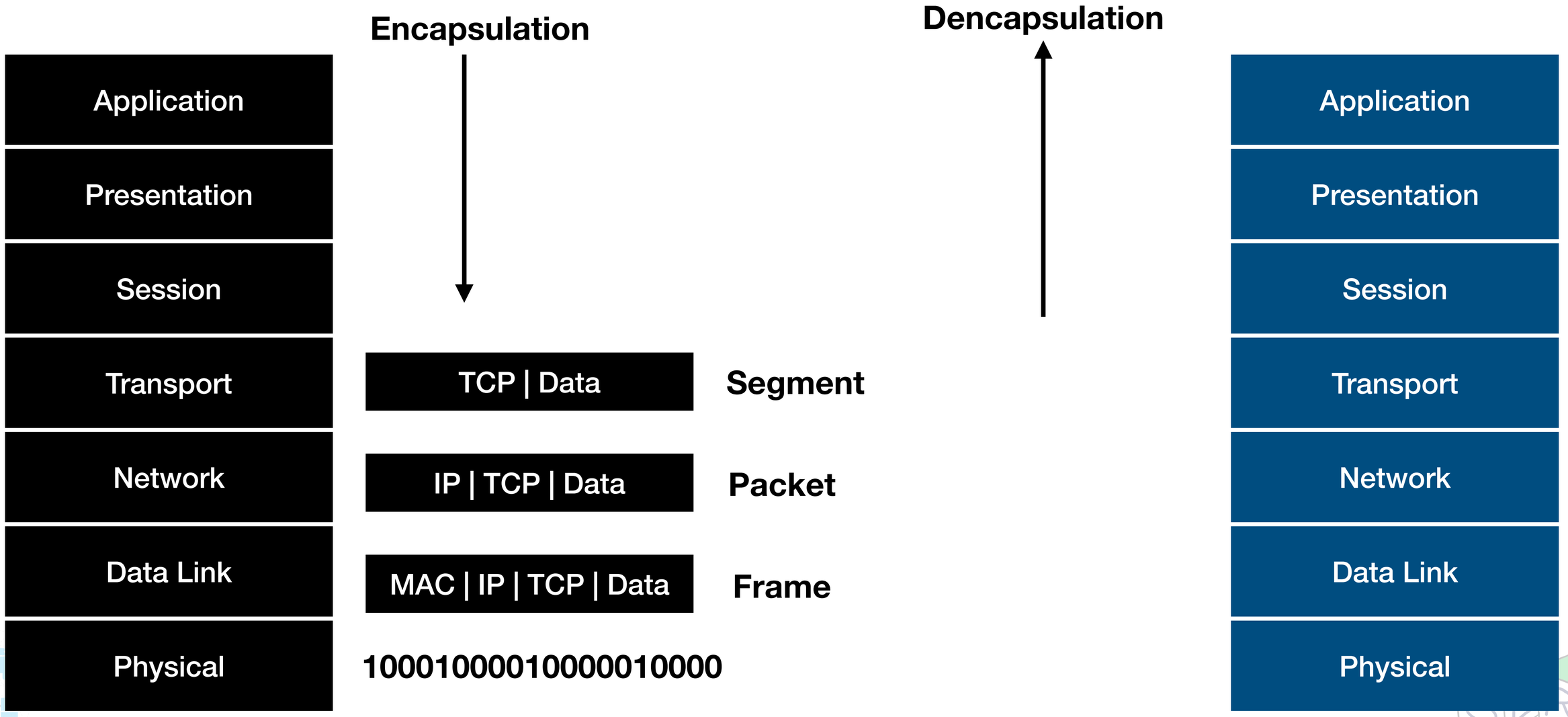
Physical Layer (L1)

Ultimately everything is 0's and 1's

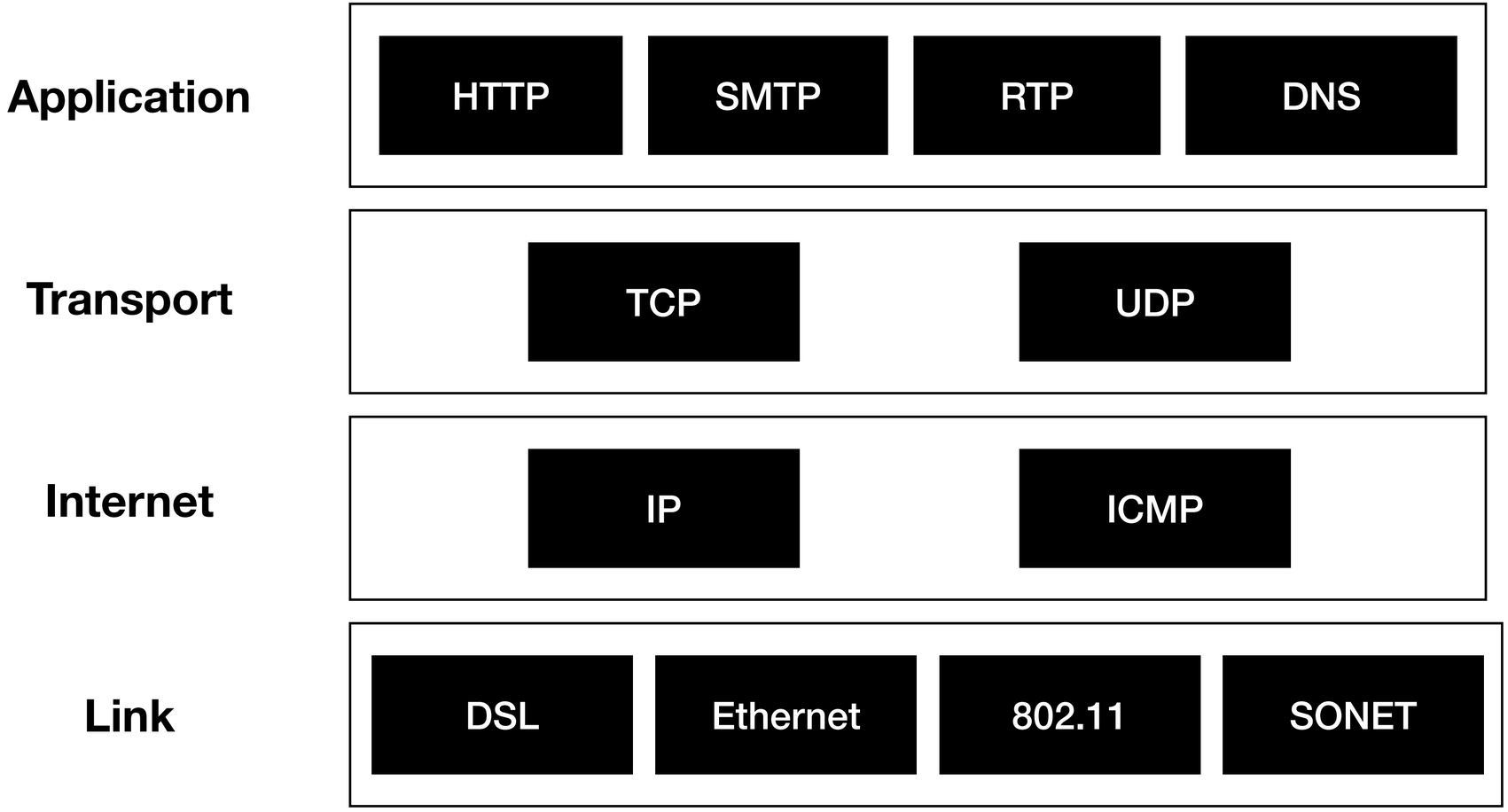
- Data is in the form of bits - 0s and 1s
- Something has to transport the bits from one machine to another - Physical layer
- Concerned with transmission of raw bits over physical medium, like a cable
- L1 technologies: Ethernet cables, Optical fiber, Coaxial cable, etc.
    - Even WiFi is L1 technology, hub, repeater, etc.



Putting It Together



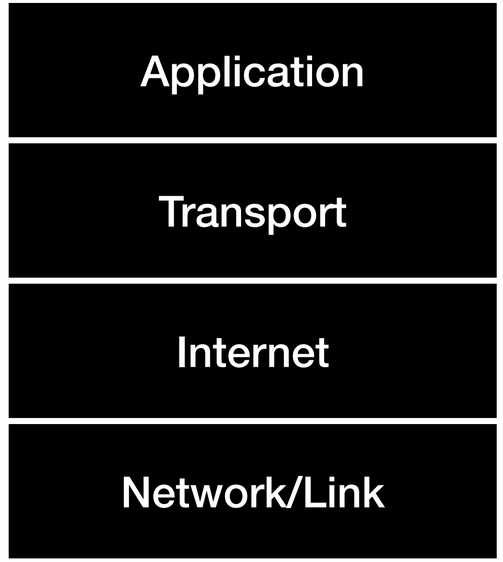
Network Protocol Stack



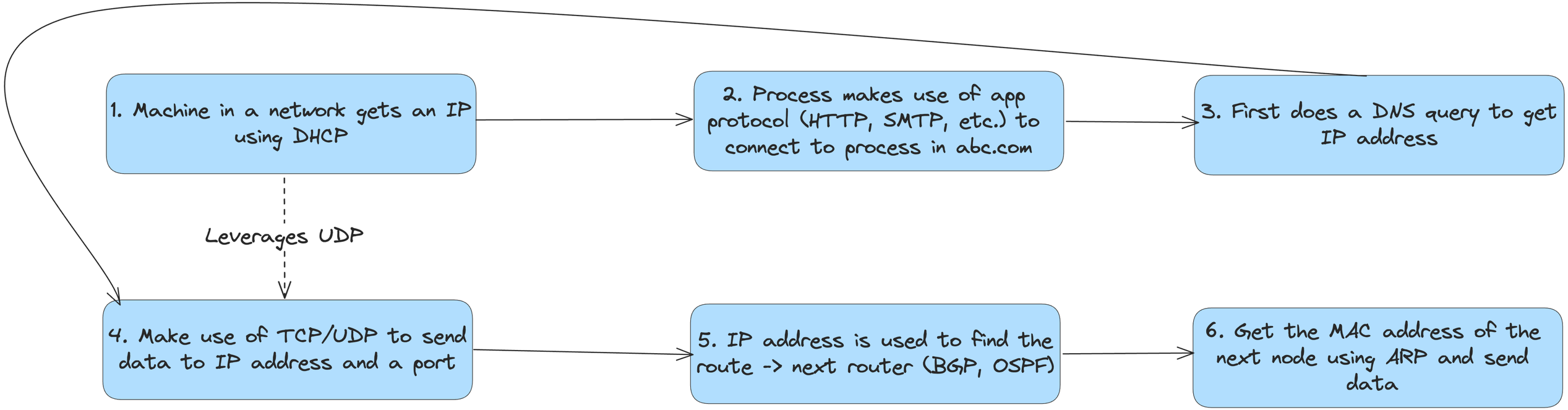
The 4 Layer Model

Internet Model or TCP/IP model,

- OSI model is more educational purpose
- 4 layer model more used in reality
- Application layer - Corresponds to application, presentation and session
- Transport layer - Transport layer of OSI
- Internet layer - Network layer of OSI
- Network - Physical and data link layers of OSI



Putting it together



Thank you

Course site: karthikv1392.github.io/cs3301_osn
Email: karthik.vaidhyanathan@iiit.ac.in
Twitter: @karthi_ishere