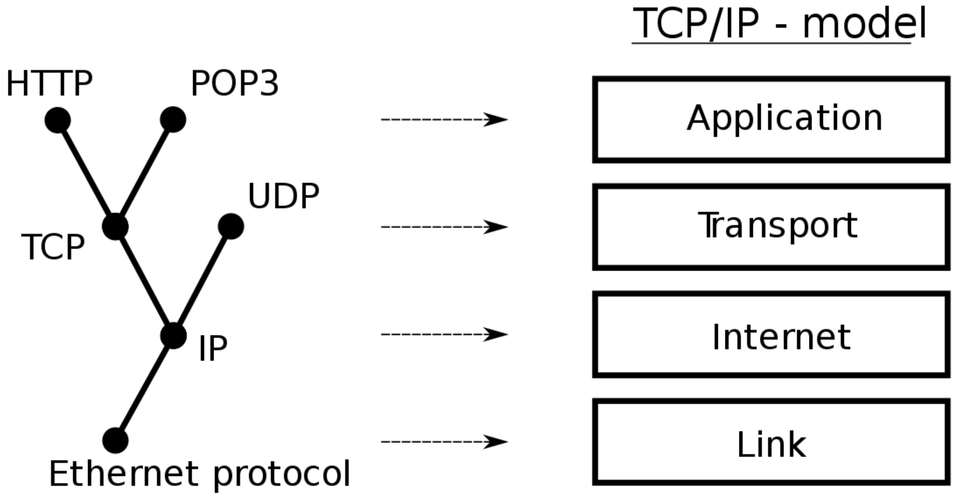
Data Encapsulation & TCP/IP model

Frank Walsh

Recap - Protocols

- An agreed convention for communication
- Formally Defined and unambiguous
- Network Protocols define:
  - Format
  - Message order
  - Actions on transmission/receipt

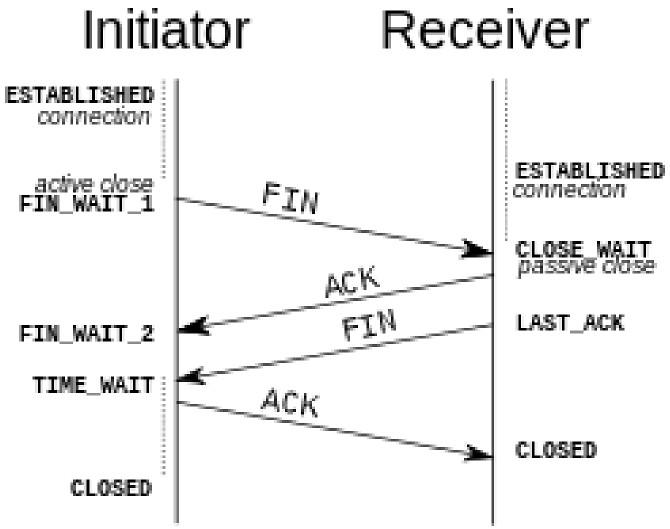


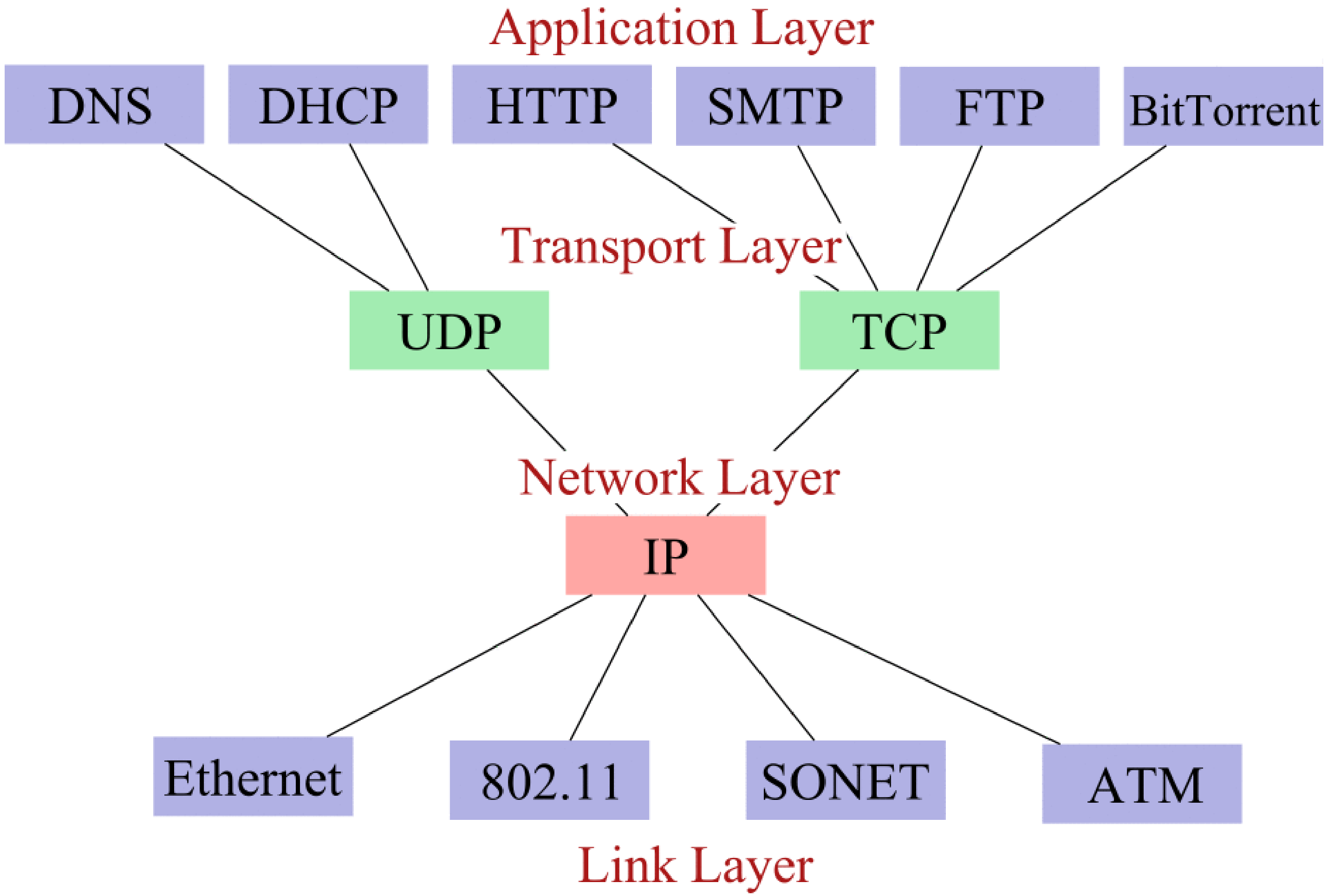
Protocol Suites & Standards

- A Protocol Suite is a group of protocols designed to work together
- Typically use open, widely used protocols.
  - Example: Wifi, HTTP, FTP, TCP, IP...
- Protocol Standards established by Institute of Electrical and Electronics Engineers (IEEE) or the Internet Engineering Task Force (IETF)
- Protocol suites based on open standards ensures that products from different manufacturers can work together for efficient communications

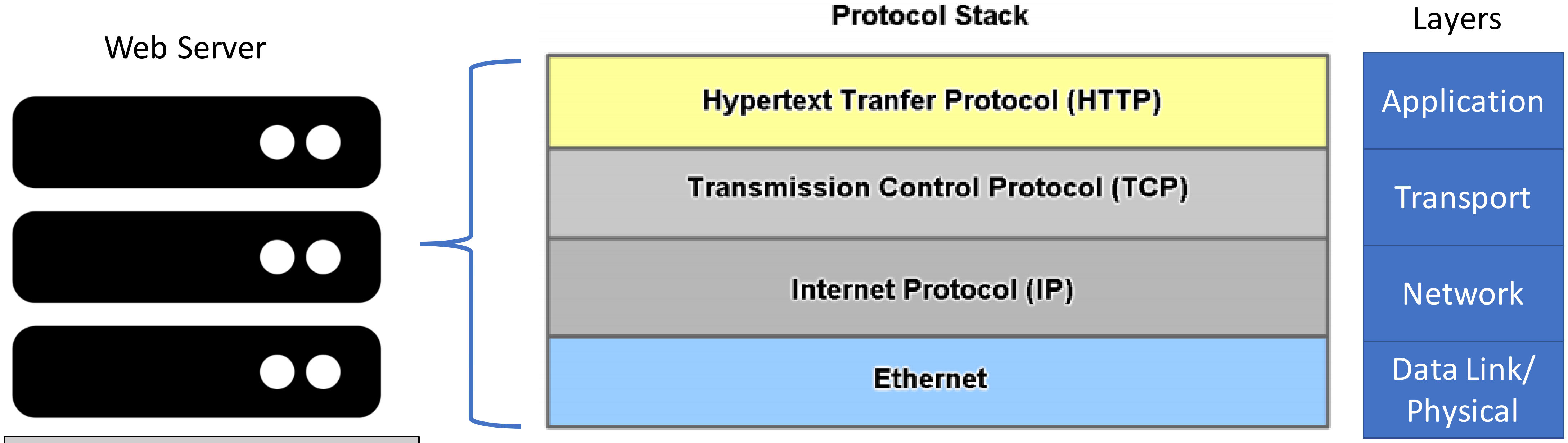
TCP/IP Protocol Suite

- Often referred to as TCP/IP, TCPIP, or just IP
- A whole suite of protocols, including TCP, IP, UDP, ARP, DNS, HTTP, ICMP and many more acronyms!
- TCP originally developed by the US Department of Defense for wartime comms.
  - Remember ARPA
- TCP/IP is now the “standard” protocol suite for the internet




Application Layer
DNS
DHCP
HTTP
SMTP
FTP
BitTorrent
Transport Layer
UDP
TCP
Network Layer
IP
Ethernet
802.11
SONET
ATM
Link Layer

Example: Layered Model Network Comms



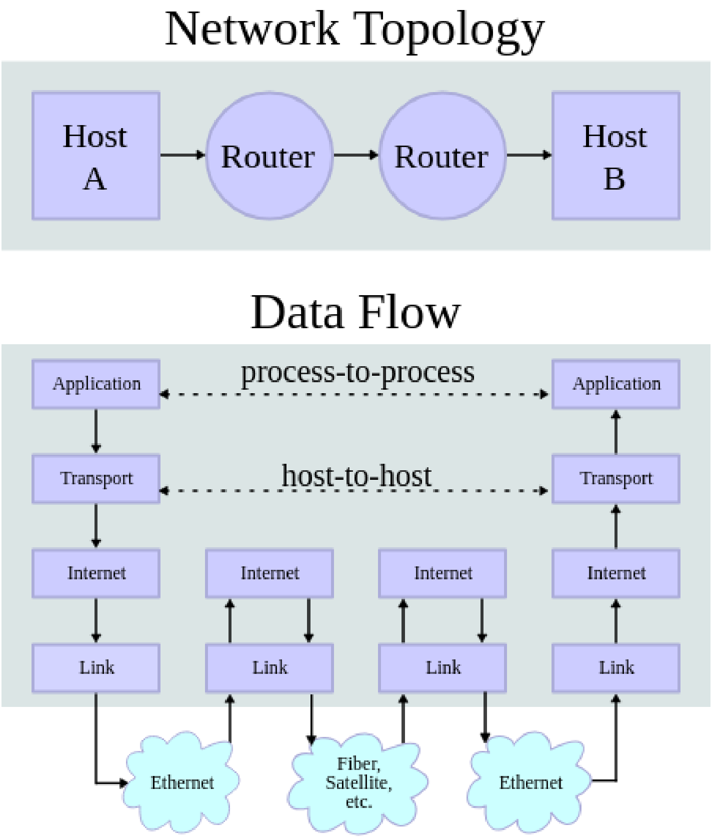
Web Server

Protocol Stack	Layers
Hypertext Tranfer Protocol (HTTP)	Application
Transmission Control Protocol (TCP)	Transport
Internet Protocol (IP)	Network
Ethernet	Data Link/ Physical

Benefits of Layered Model:

- assists in protocol design
- fosters competition
- changes in one layer do not affect other layers
- provides a common language

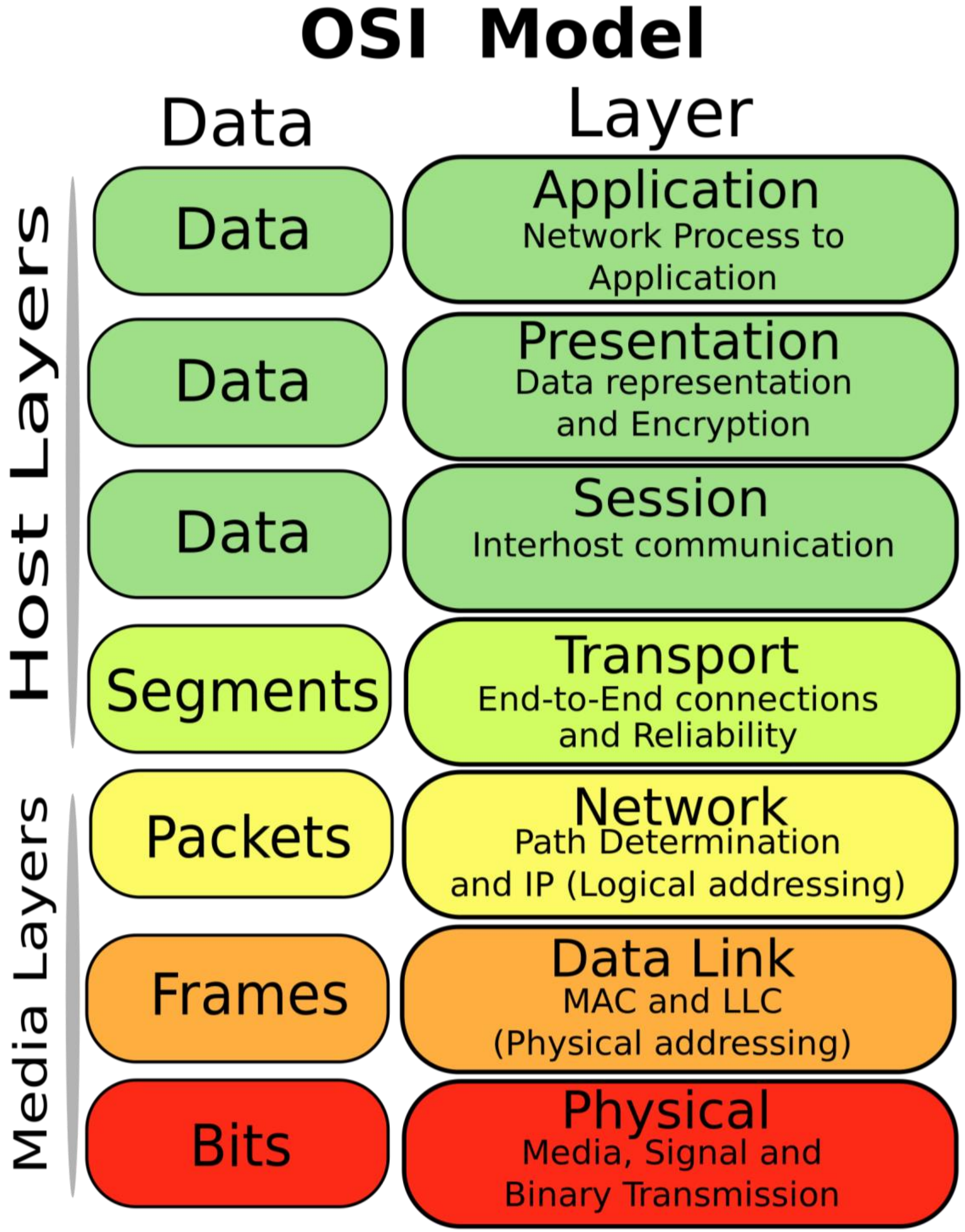
Layered Model: From A to B across the internet



https://commons.wikimedia.org/wiki/File:TCP-IP_Model_-_en.png

OSI Model

- Open Systems Interconnection(OSI) introduced by the International Organization for Standardization (ISO) in 1984
- Provide a reference model to make sure products of different vendors would interoperate in networks.
- A layer in the OSI model communicates with three other layers:
  - the layer above it, the layer below it, and the same layer at its communication partner.



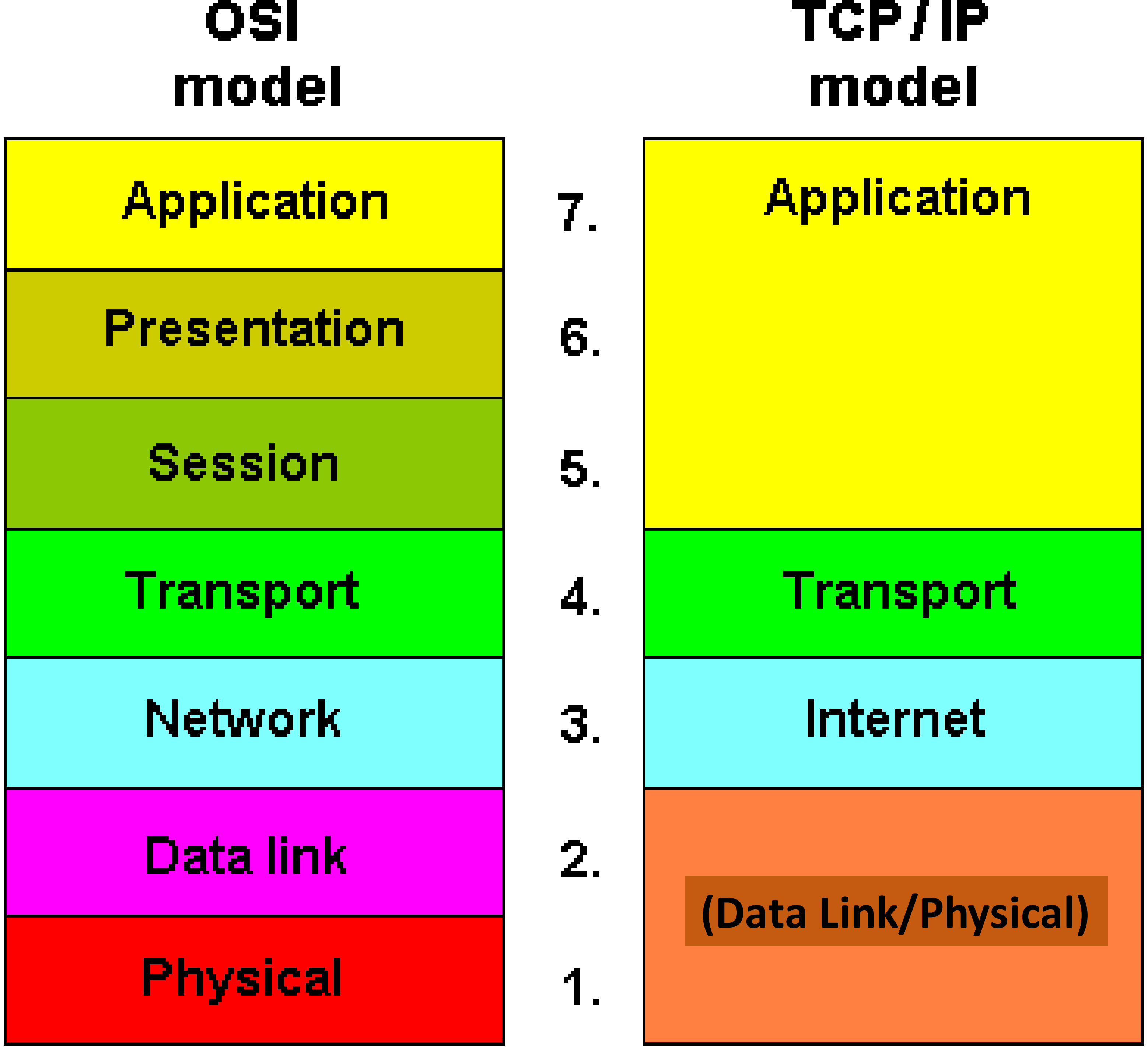
OSI Model

	Data	Layer
Host Layers	Data	Application Network Process to Application
	Data	Presentation Data representation and Encryption
	Data	Session Interhost communication
	Segments	Transport End-to-End connections and Reliability
Media Layers	Packets	Network Path Determination and IP (Logical addressing)
	Frames	Data Link MAC and LLC (Physical addressing)
	Bits	Physical Media, Signal and Binary Transmission

Image Source: https://upload.wikimedia.org/wikipedia/commons/thumb/4/47/Osi-model-jb.svg/2000px-Osi-model-jb.svg.png

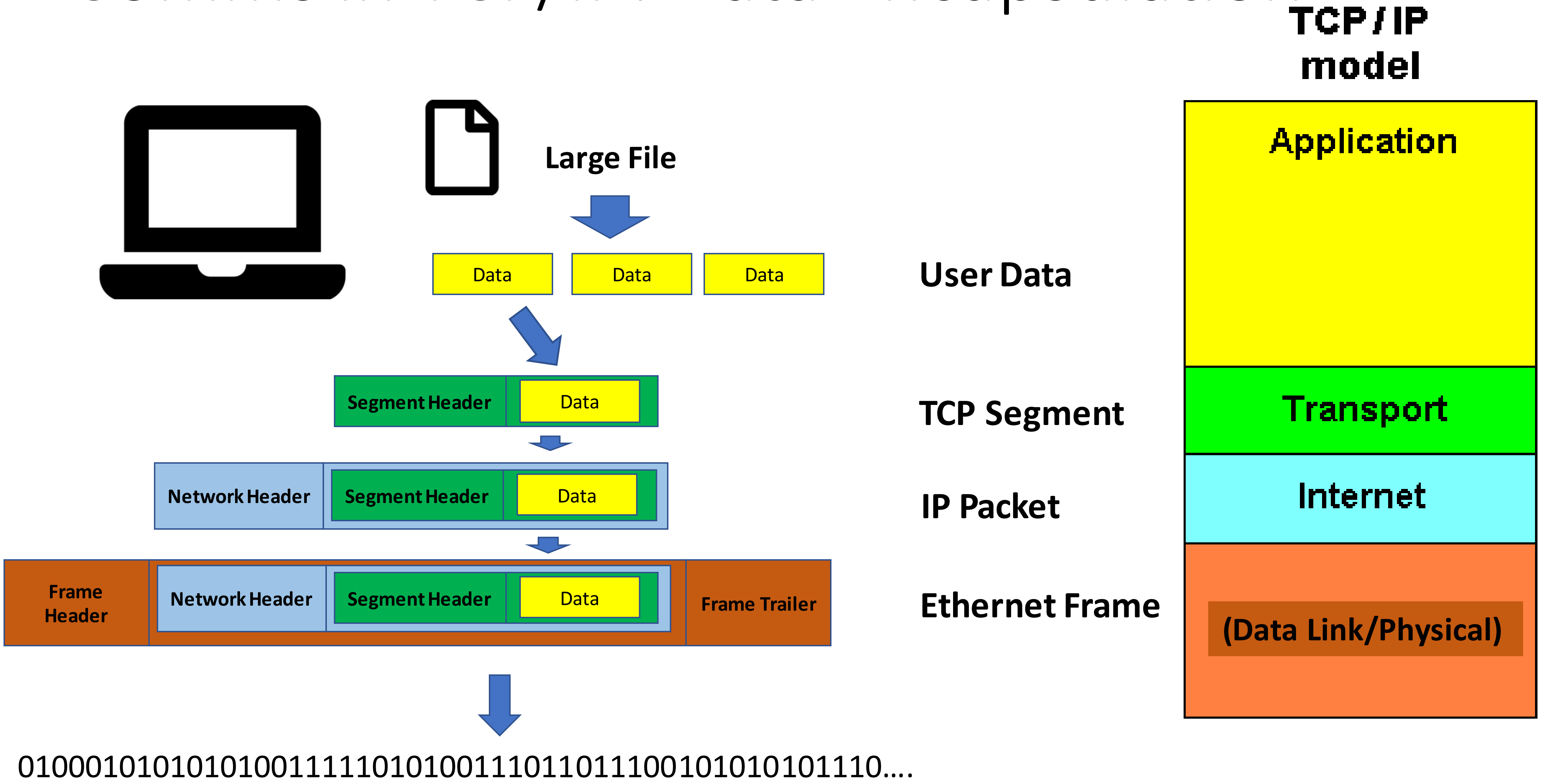
OSI vs TCP/IP

- TCP/IP model combines the presentation and session layer into its application layer.
- TCP/IP combines the OSI data link and physical layers into the host-to-network/network access layer
- Internet developed on around TCP/IP protocols.
  - Thus very popular.... Networks are not usually built on the OSI model, even though the OSI model is used as a guide.



OSI model		TCP/IP model
Application	7.	Application
Presentation	6.	
Session	5.	
Transport	4.	Transport
Network	3.	Internet
Data link	2.	(Data Link/Physical)
Physical	1.	

Comms in TCP/IP: Data Encapsulation



Data Encapsulation: Protocol Data Units (PDUs)

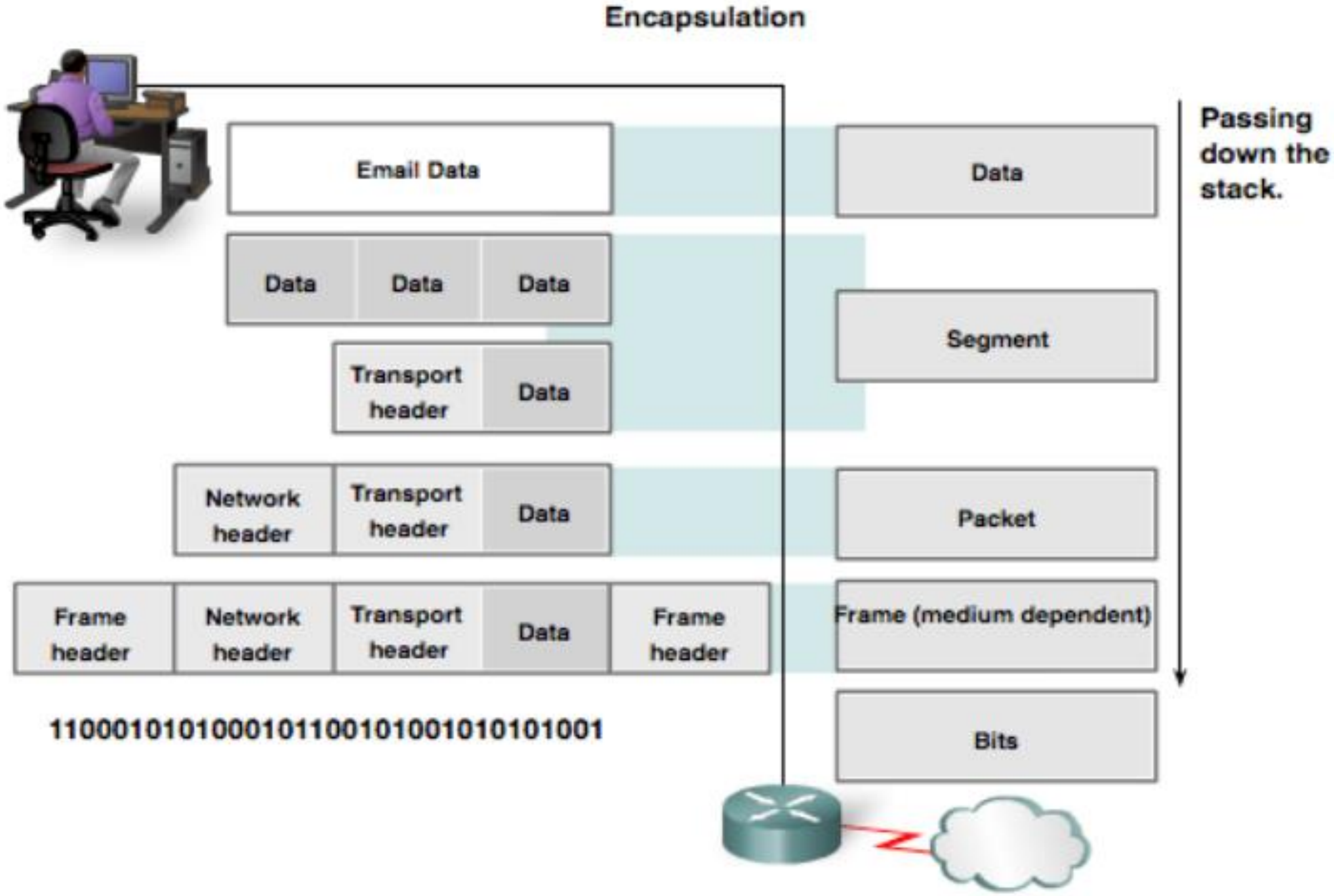
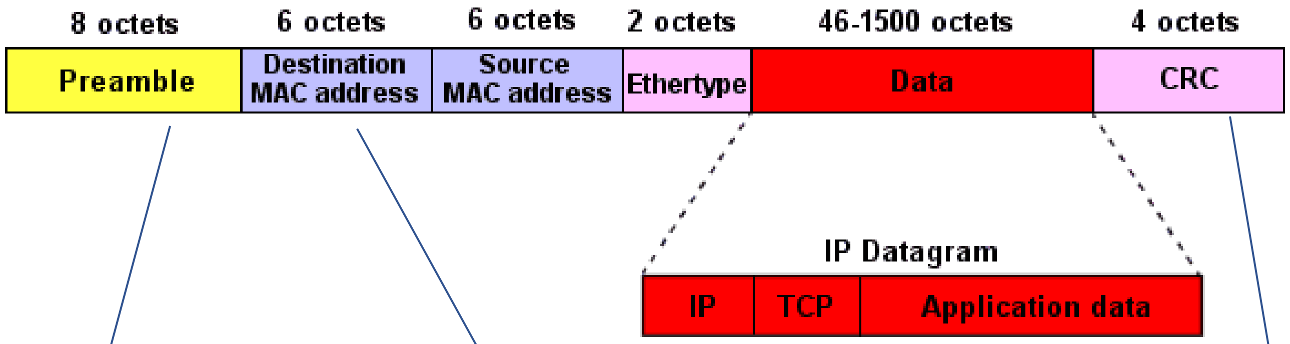


Image: cisco.com

Link Layer(Layer 2) Communication - Ethernet

- Data Link Layer protocol
- Supported by many physical layer implementations
  - Wireless/wired
- PDU is the **frame**



Sequence of alternating 1s and 0s for synchronisation

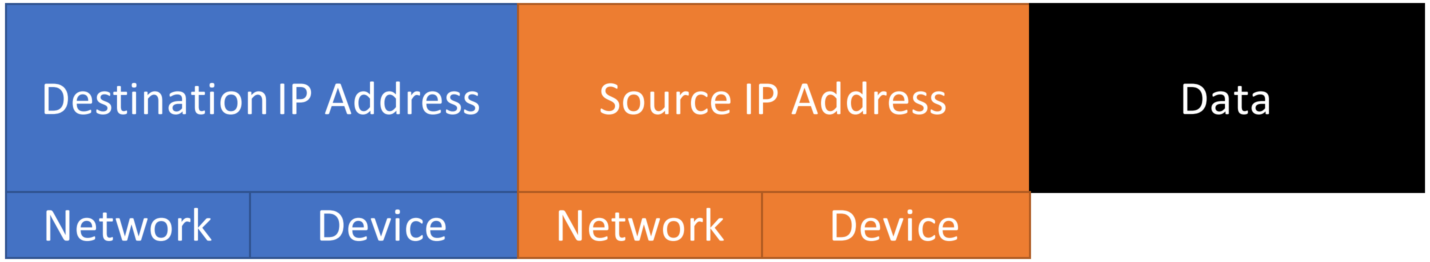
Unique 6 octet (48 bit) address. “hardware” or “physical” address

Value used to check accidental changes to raw data. Calculated at both ends using data. Received value should match calculated value…

Network Layer Communication

- Network layer protocols primary function is to move data from one network to another network
- Network addresses(IP Addresses) must have a mechanism to locate hosts on different networks
- Intermediary network devices such as routers, decapsulate frames to read destination host address contained in the packet header.
- Routers use the network portion of this address to determine which path to use to reach its destination.

IP/Network Packet



Destination IP Address

Source IP Address

Data

Network

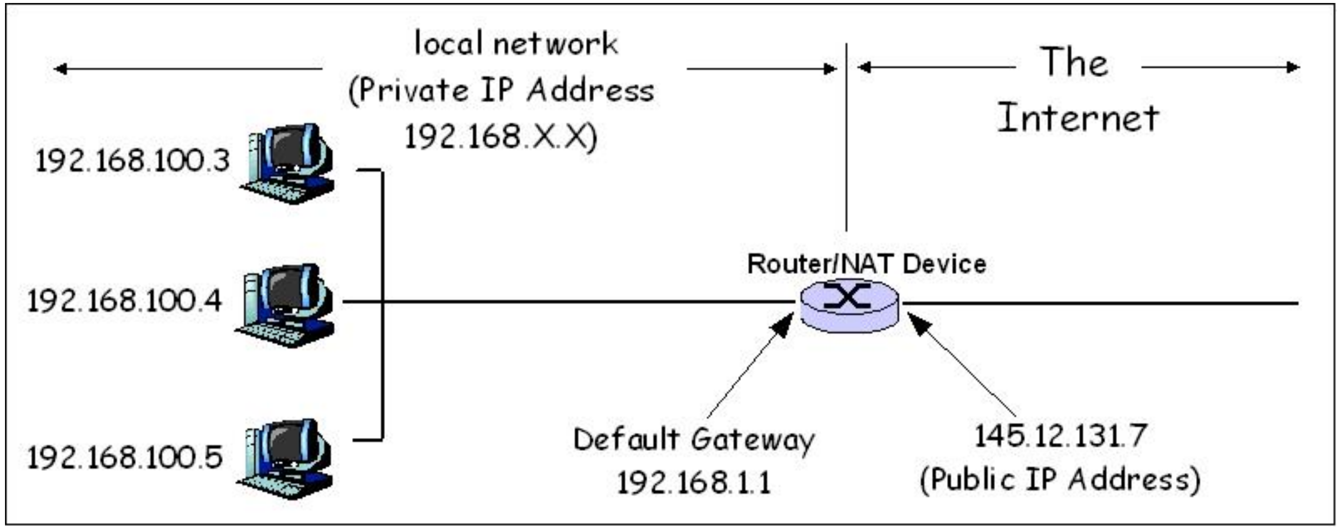
Device

Network

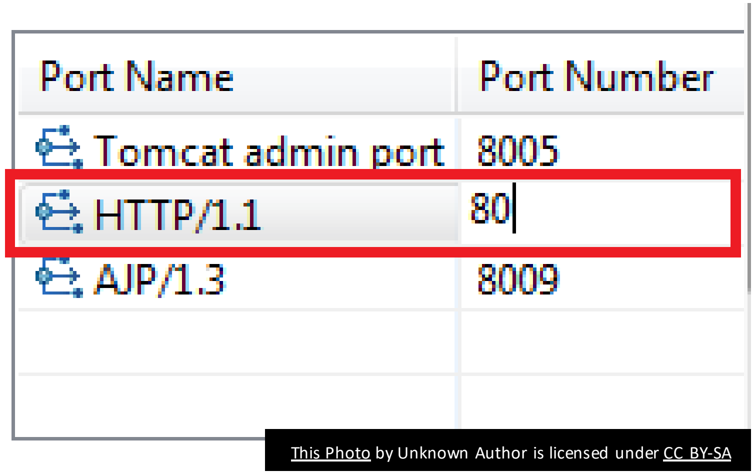
Device

Network Layer Communication

- IP addresses are “logical”
  - Can be assigned to a device
- Includes network identification and Host identification
- Each device on a network must have a unique IP address
- Public IP addresses for the internet assigned by a central authority (IANA)
- Private IP addresses are reserve for internal use behind routers/Network address translation(NAT) devices.



This Photo by Unknown Author is licensed under CC BY-SA



Port Name	Port Number
Tomcat admin port	8005
HTTP/1.1	80
AJP/1.3	8009

This Photo by Unknown Author is licensed under CC BY-SA

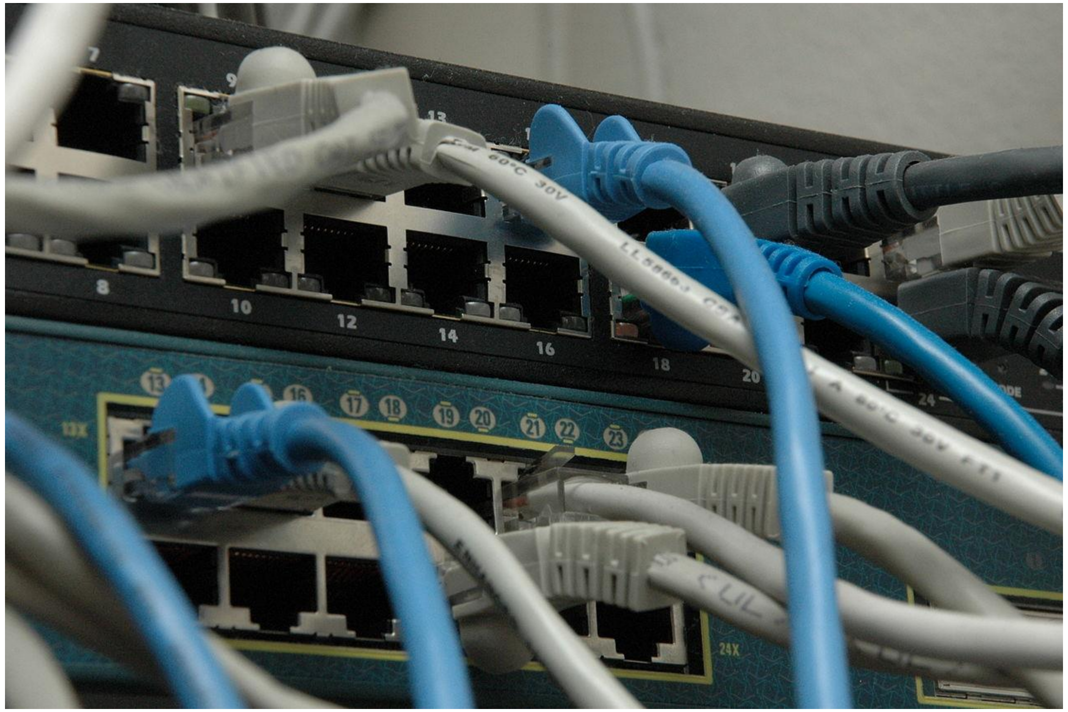
Transport Layer Communication

- How does a computer with one network interface differentiate between different data types?
- Port Numbers are used in the transport layer to represent applications or services
- When a device receives data, the port number is used to determine which app or process is the correct destination
- There are generally accepted port numbers:
  - What’s the port for SSH service?
  - HTTP service?

Ethernet

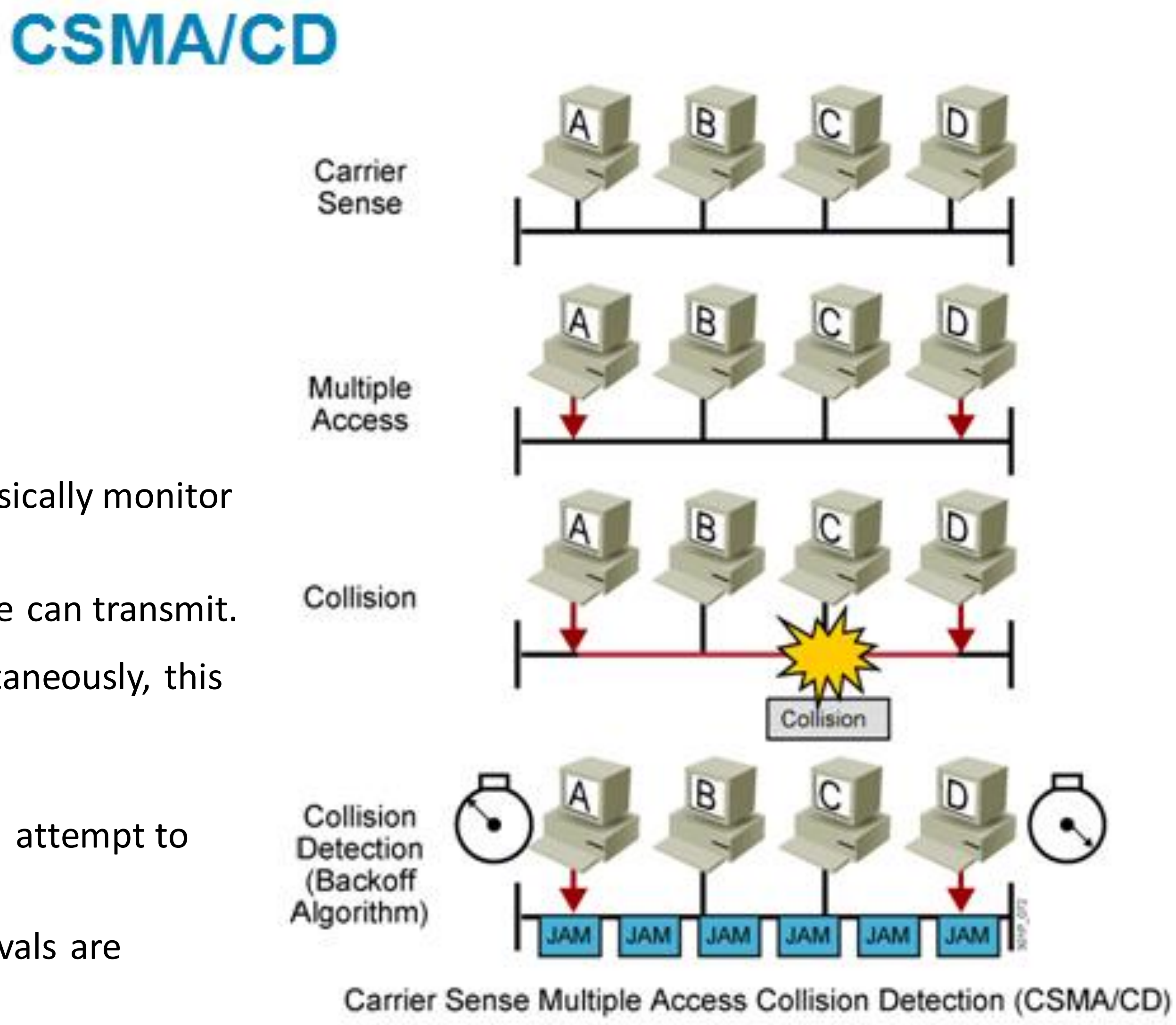
Ethernet

- Operates across Link/physical layer
- Provides the following that pure physical layers do not:
  - Connects to upper layers (i.e. network)
  - Provides mechanism to recognise devices
  - Organises bits into frames
- Provides encapsulation into “Frames”
- Ethernet Provides Media Access Control
  - Placement and removal of frames onto media
  - Media access control for ethernet is CSMA/CD
    - All devices on network segment share media
    - All devices receive all frames transmitted on network



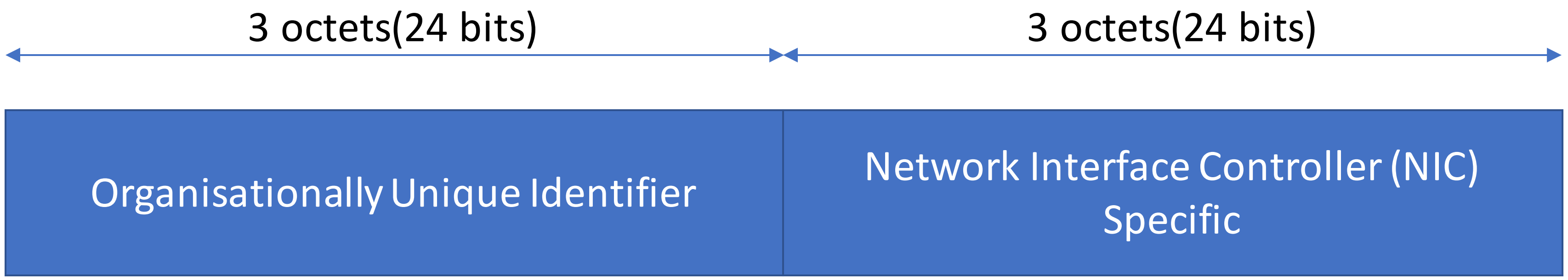
Ethernet CSMA/CD

- Ethernet networks use CSMA/CD to physically monitor network channel
- If no transmission is taking place ,a device can transmit.
- If two devices attempt to transmit simultaneously, this causes a collision
  - Jam signal detected by all devices.
- After a random time interval, the devices attempt to transmit again.
- If another collision occurs, the time intervals are increased step by step.
  - known as **exponential back off.**


CSMA/CD
Carrier Sense
A
B
C
D
Multiple Access
Collision
Collision
Collision Detection (Backoff Algorithm)
JAM
JAM
JAM
JAM
JAM
JAM
Carrier Sense Multiple Access Collision Detection (CSMA/CD)

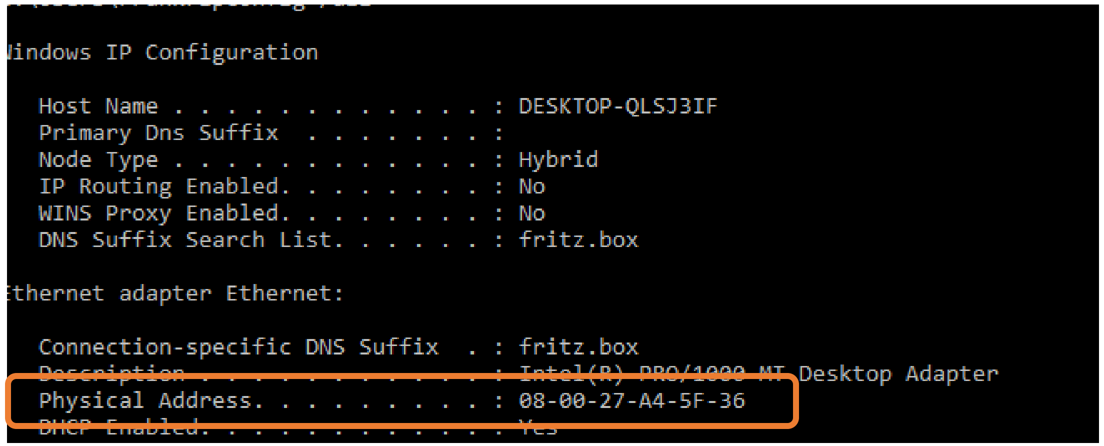
Ethernet - MAC Address

- Every Ethernet interface must have 6 byte MAC address
- Addresses assigned to physical interface by manufacturer/vendor


3 octets(24 bits)
3 octets(24 bits)
Organisationally Unique Identifier
Network Interface Controller (NIC) Specific

- Example: 80:19:34:95:D1:02

Usually expressed as HEX



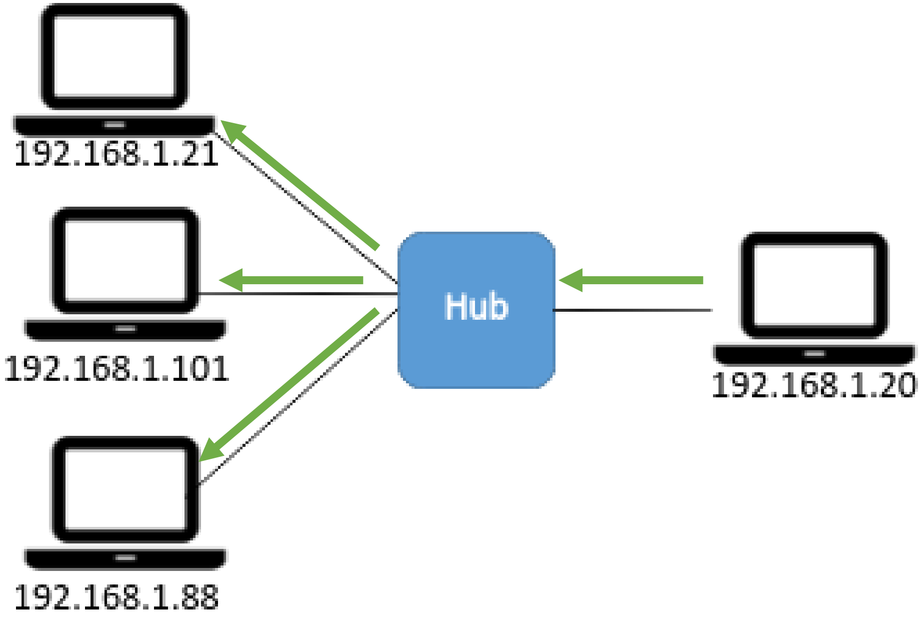
```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-QLSJ3IF
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : fritz.box

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : fritz.box
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-A4-5F-36
   DHCP Enabled. . . . . . . . . . . : Yes
```

Link Layer Communication - Delivery

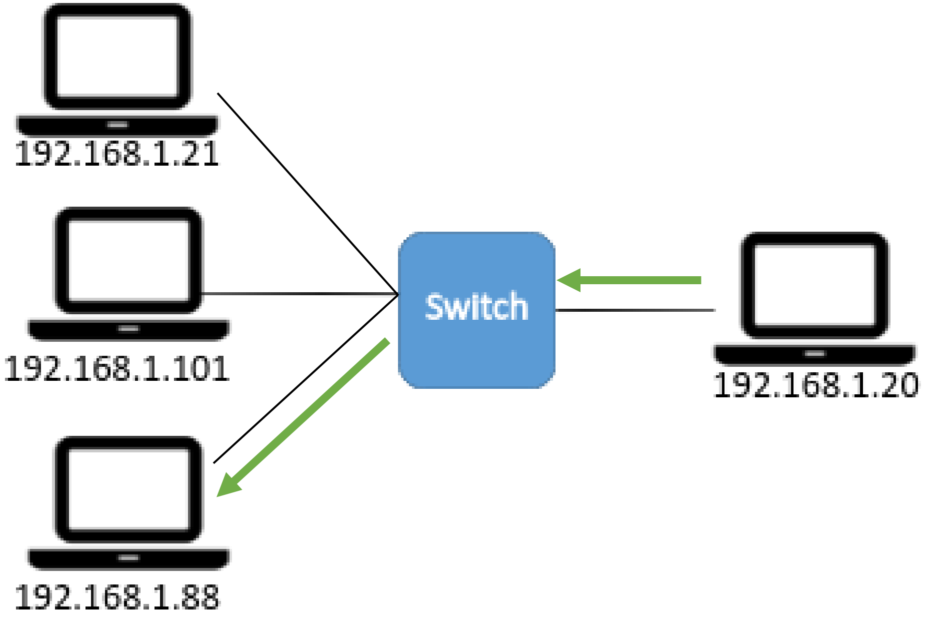
- Concerned with getting data to end device.
    - Delivery of messages on a single local network
- Layer 2 addresses are unique on the local network.
    - Represents "physical" address
- In an LAN, using Ethernet, referred to as the Media Access Control (MAC) address
- Each network interface inspects destination address of every frame. If it does not match hardware address(or broadcast address), the frame is discarded
- Once a frame is successfully received at destination, Layer 2 info is removed as the data is decapsulated and moved up the protocol stack to Network layer(layer 3).

Physical/Link Layer (layer 2) intermediate devices

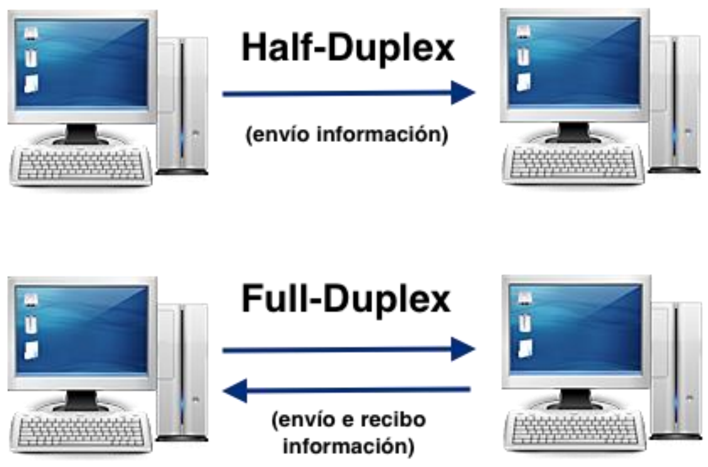
- Hub
  - Used to connect devices
  - Frames sent out on all ports.
  - Shared Media (only one device can transmit)



- Switch
  - Replaces hubs on Ethernet networks
  - Ports isolated. Frame is sent just to its proper destination(if known).



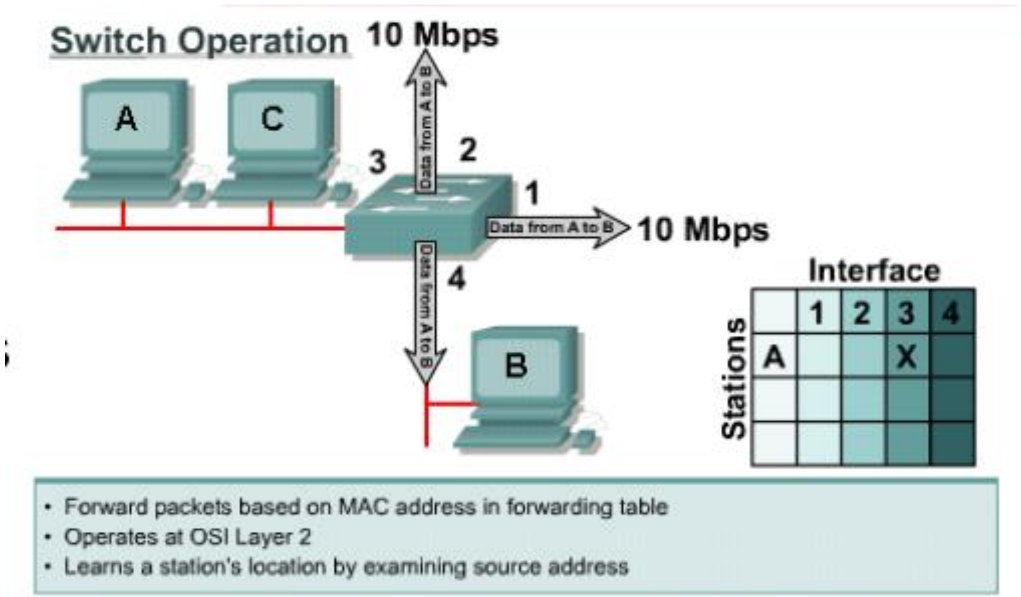
Ethernet Collision Detection



- In shared media, only one device can transmit
- More devices on network => more collisions
- Switches reduce collisions
- Switches isolate each port and can send a frame to its destination (if known) rather than every device
- Remember twisted pair cabling from week 1
  - Allows for one pair for transmission, one for receiving.
- The capability to do both simultaneously is called full duplex
  - No contention for media => no collision domain.

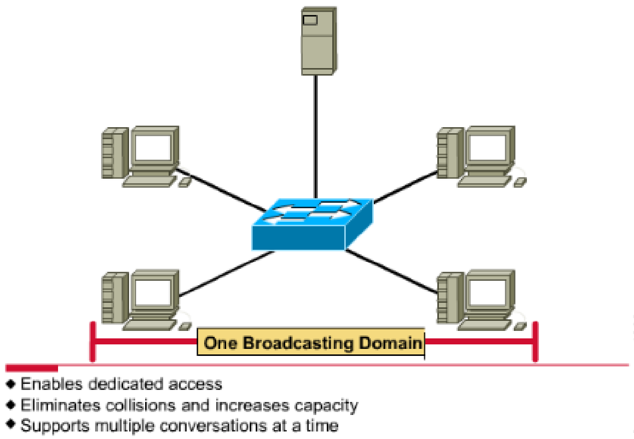
Switch Operation

- Microsegments
  - If only one device connected to switch port, collision domain contains just two nodes
  - Small physical segment is called a microsegment
- Switch maintains **forwarding table**
- **Constantly learns a devices location by examining source address**

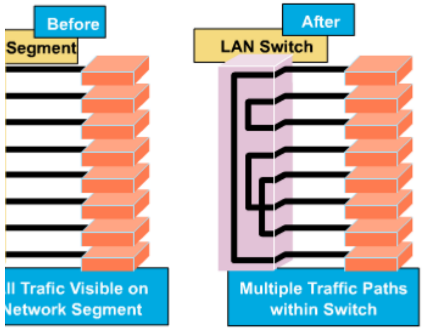


	1	2	3	4
A			X	

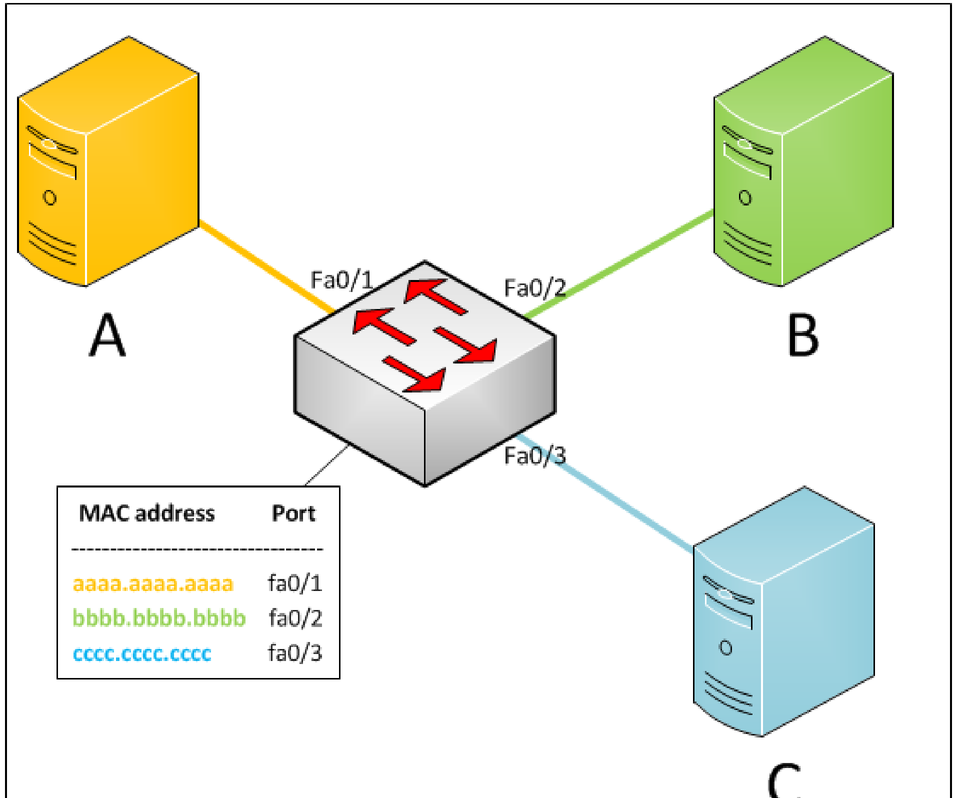
- Forward packets based on MAC address in forwarding table
- Operates at OSI Layer 2
- Learns a station's location by examining source address



- Enables dedicated access
- Eliminates collisions and increases capacity
- Supports multiple conversations at a time

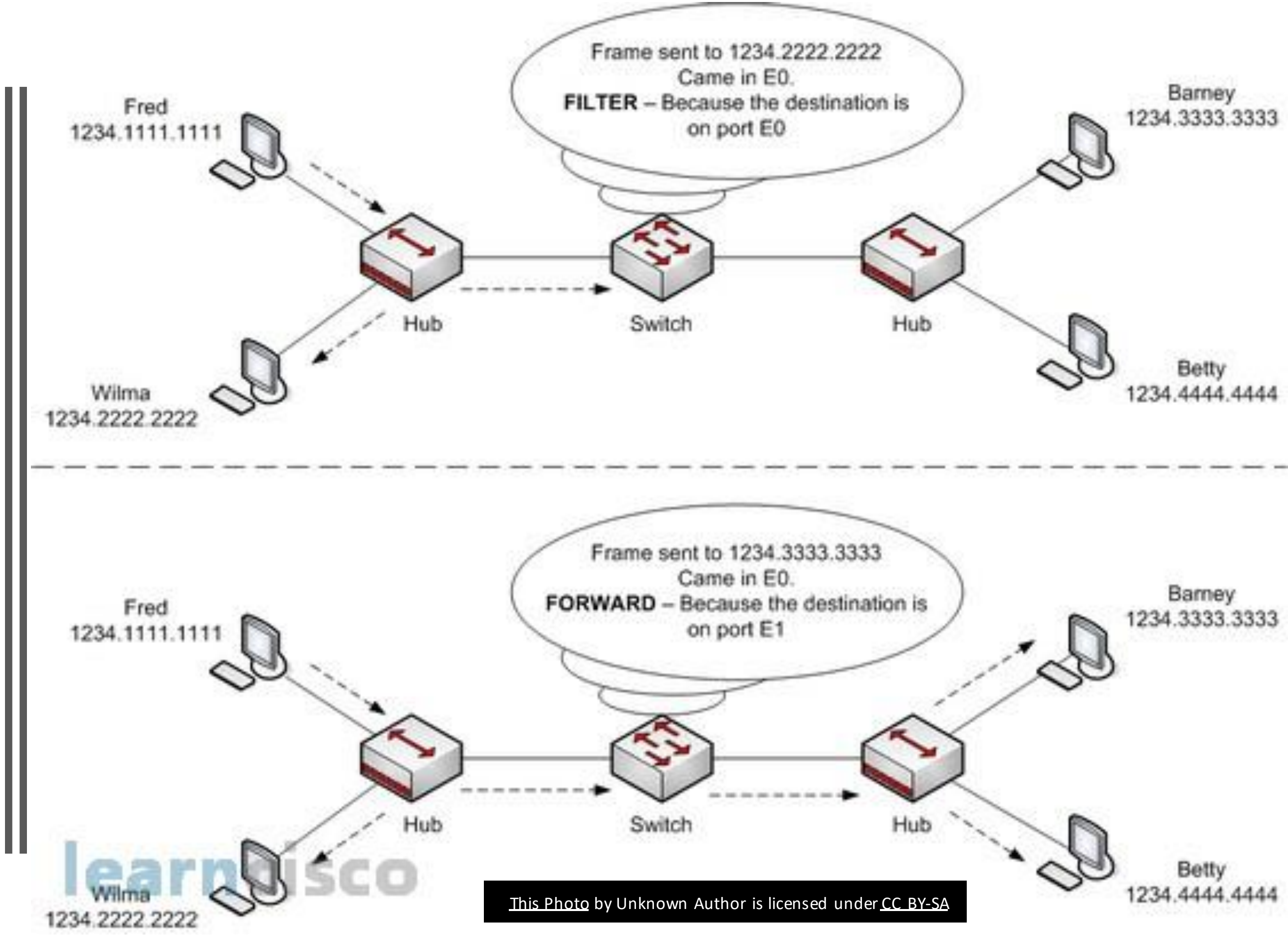


Switching



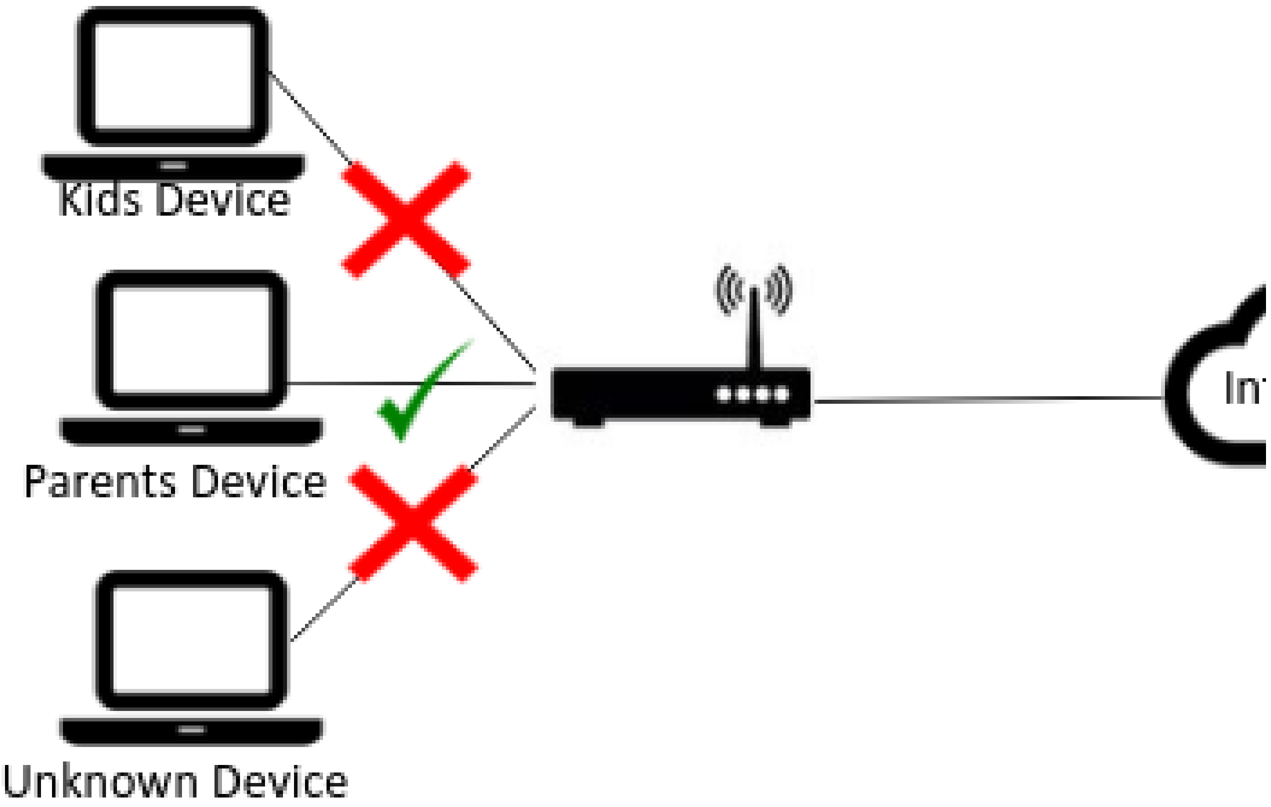
MAC address	Port
aaaa.aaaa.aaaa	fa0/1
bbbb.bbbb.bbbb	fa0/2
cccc.cccc.cccc	fa0/3

Complete MAC address table



Switching Operation

- Learning
  - MAC table populated by examining traffic across ports
- Aging
  - MAC table entries are timestamped
  - Removed after a period of time
- Flooding
  - If destination MAC not in address, frame transmitted on all ports on switch
- Selective Forwarding
  - Sending frame on one port based on MAC address
- Filtering
  - Performs CRC and drops corrupted frames
  - Block frames to/from selected MAC addresses

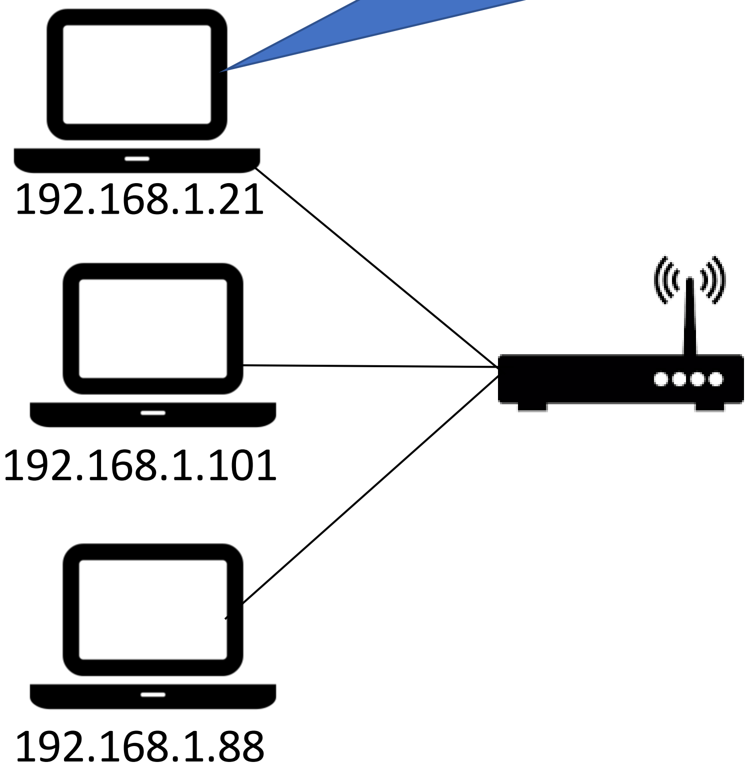


Key Points

- MAC
- What’s the OUI part of the MAC address
- CSMA/CD
- Switched Ethernet
- Hubs vs Swtiches
- Simplex/Half Duplex/Duplex

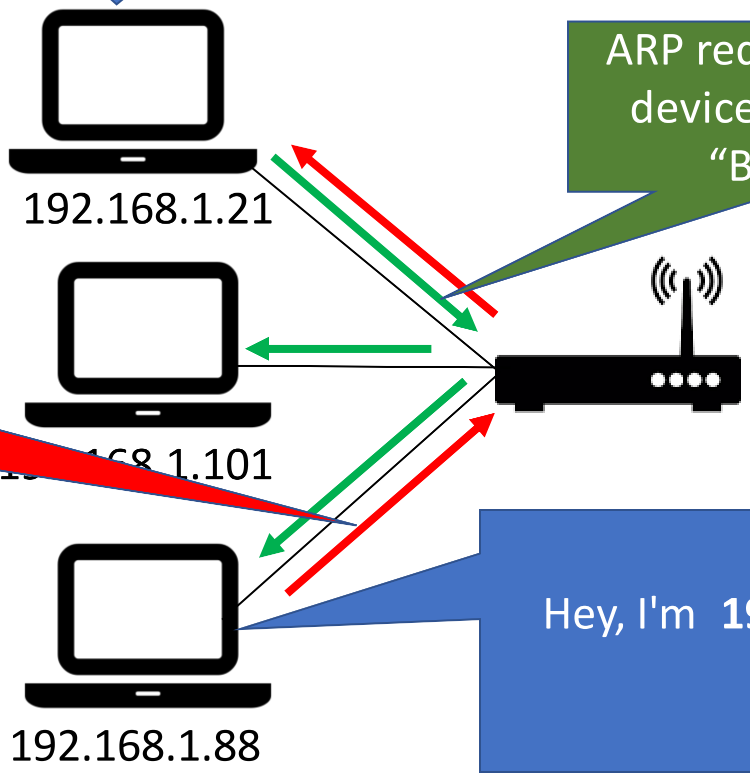
Introduction to ARP

I need to send a message to **192.168.1.88** but I don’t have a MAC address of the device that has that has that IP.



ARP Conversation

Hey everyone! I need to send a message to **192.168.1.88** but I don’t have a MAC address. Is there anybody out there with an IP of **192.168.1.88**



ARP request sent to all devices on network: “Broadcast”

ARP response sent only to requesting device: “Unicast”

Hey, I'm **192.168.1.88** and my MAC address is **00:cd:12:4d:3a:08**

Address Resolution Protocol

- The *Address Resolution Protocol (ARP)* is used by a sending device when it knows the IP address of the destination but needs the Ethernet address.
- ARP is a broadcast protocol - every host on the network receives the request.
- Each host checks the request against it’s IP address - the right one responds.
- Hosts *remember* the hardware addresses of each other.

The ARP Process – Mapping IP to MAC Address

- Ethernet frames must have a destination MAC address
- Devices will maintain a table in memory that maps IP addresses to MAC addresses: the **ARP Table**
- The ARP table is populated using 2 mechanisms:
  - Monitor traffic on the local network
  - Broadcast an ARP request
- ARP request is broadcast to all devices on the Ethernet network.
  - Node receiving an ARP request that identifies the IP address as it sends a single response (I.e. unicast) back to the sender. Senter uses this to update the ARP table

ARP Request for device on another network

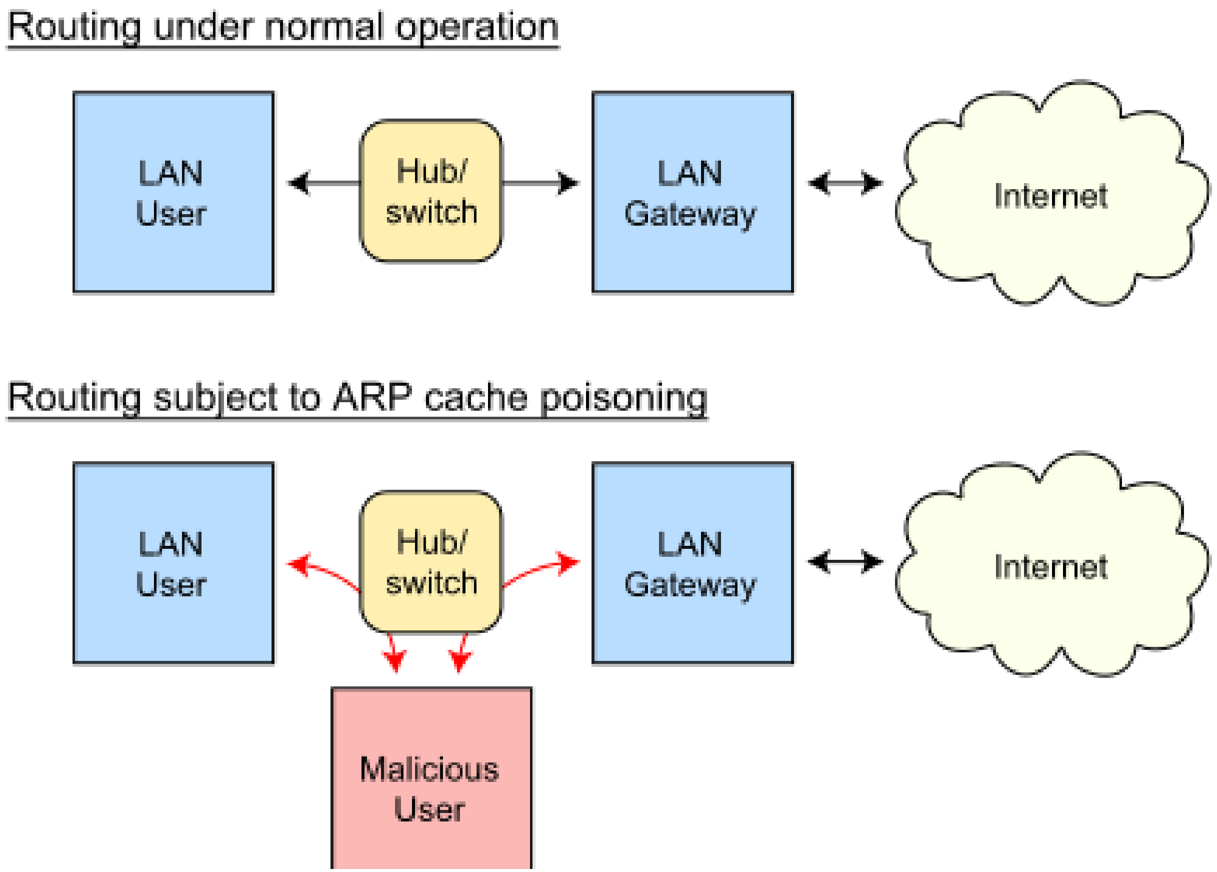
- Sending device needs to send a message to a device on another/external network. What's the destination MAC address???
- Sending device will use the MAC address of the "default gateway" - usually the MAC address of the router interface that routes to that network
- What if the ARP table doesn't contain an entry for the default gateway???
  - Device will perform ARP request for MAC

Maintaining ARP tables

- Devices remove ARP table entries that have not been used in a specified period.
  - Period differs across devices. Typically 2 minutes for Windows.
- Example use: Device removed from network/switched off

ARP Issues...

- Media Overhead
  - A lot of traffic generated by ARP request (broadcast). Minimal impact in typical business setting
- Security
  - ARP Spoofing/Poisoning: Attacker forges MAC address – frames sent to wrong device...



Key Points -ARP

- Ethernet uses ARP to determine MAC addresses
- Each device has an IP address and a MAC address.
- ARP resolves IP addresses to MAC addresses