

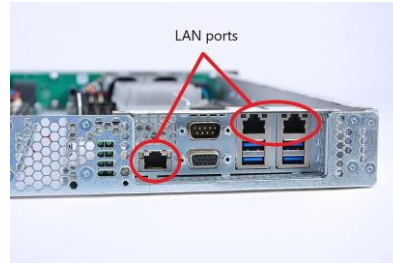
# Welcome to Section 6

## Networking

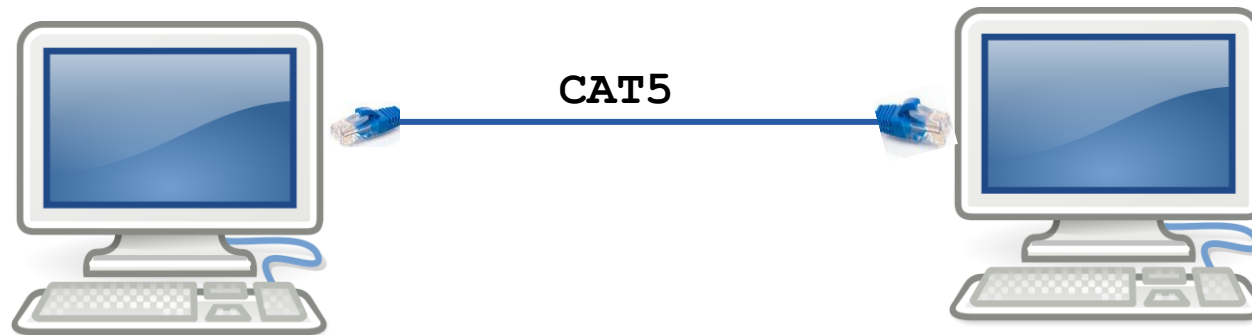
# How Computers Communicate

1/2

- To connect to the Internet and other computers on a network, a computer must have a NIC (network interface card) installed and a network cable plugged into the NIC on one end and plugged into another computer's NIC port



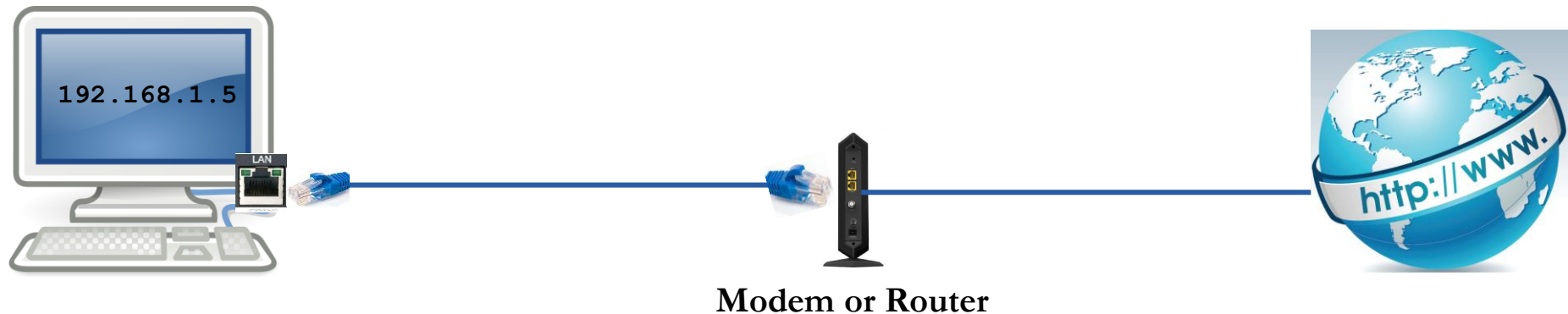
- Computers need to be connected to one another through Ethernet cable, or "Category 5" wiring



# How Computers Communicate

2/2

- Like a phone line, Ethernet cables can have four to eight wires, as much as double the amount found in a phone line
- To connect to other computers on the internet, CAT5 cable must be connected to a computer port and then to a cable modem, DSL modem, router, or switch



# IP address

1/4

- IP stands for Internet Protocol
- An Internet Protocol address is a **numerical label** assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing
- Compare IP address with our home address. We need our home address to send and receive mail and provides the location information

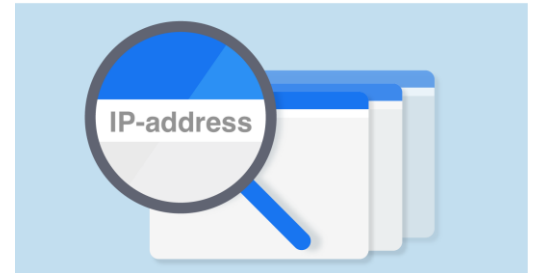


- When you're at home, an IP address is assigned to your computer by your Internet service provider aka ISP (e.g., Time Warner Cable, Optimum, AT&T or Verizon). Since they are the ones giving you access to the Internet, it's their role to assign an IP address to your computer. Your Internet activity goes through them, and they route it back to you, using your IP address

# IP address

2/4

- IPv4 addresses are usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., **192.168.123.13**. Each part represents a group of 8 bits (an octet) of the address with a total of 32 bits
- For example, the dotted-decimal IP address **192.168.123.132** is (in binary notation) the 32-bit number **110000000101000111101110000100**. This number may be hard to make sense of, so divide it into four parts of eight binary digits.
- These 8-bit sections are known as octets. The example IP address, then, becomes **11000000.10101000.01111011.10000100**. This number makes a little more sense now, so to make it even simpler convert it into dotted-decimal format (**192.168.123.132**).



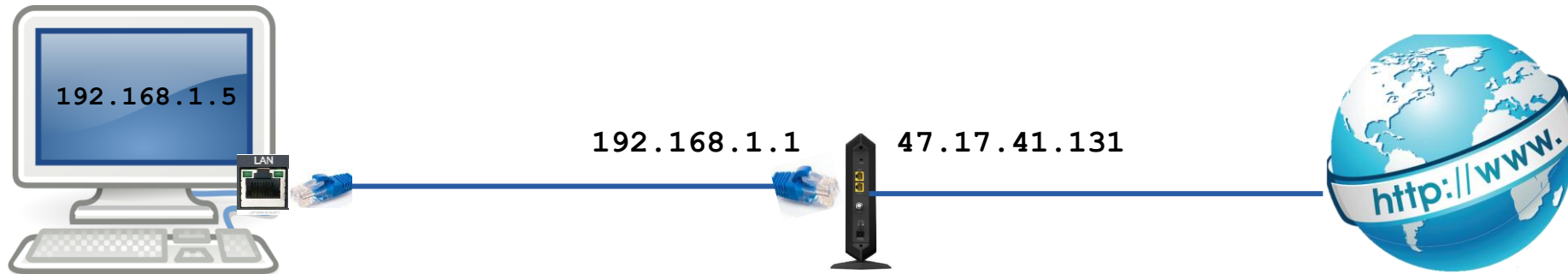
# IP address

3/4

- There are two IP versions: IPv4 and IPv6. IPv4 is the older version which has a space of over 4 billion IP addresses. However, the new IPv6 version can provide up to trillions of IP addresses to fulfill the need of all internet users and devices
- Example of IPv4 = **192.168.1.30**
- Example of IPv6 = **4ggr:1925:5656:7:600:t4tt:tc54:98vt**
- IP address can be private or public



Let's look at how to find IP of your computer?

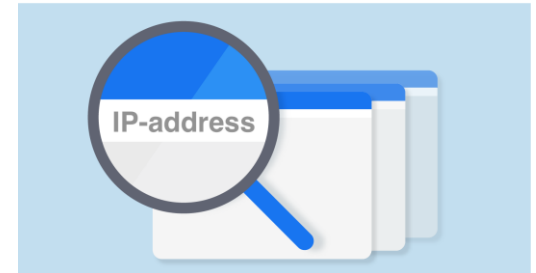


- There are 2 types of IPs
  - Static
  - DHCP (Dynamic Host Configuration Protocol)

# IP address

4/4

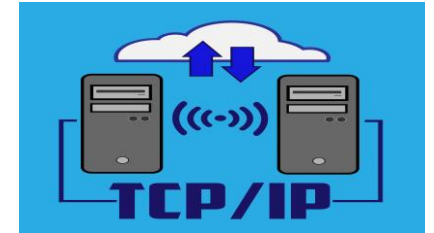
- Every website has and IP address
- E.g. when we input the URL [www.google.com](http://www.google.com) it gets translated to an IP address by DNS



- Internet addresses are allocated by the **InterNIC**, the organization that administers the Internet
- **InterNIC** is a registered service mark of the U.S. Department of Commerce. It is licensed to the Internet Corporation for Assigned Names and Numbers.

# TCP/IP

- TCP stands for Transmission Control Protocol and IP stands for Internet Protocol
- Bob Kahn at ARPA, and Vint Cerf, at Stanford University, published research in 1974 that evolved into the Transmission Control Protocol (TCP) and Internet Protocol (IP), the two protocols of the Internet protocol suite
- TCP and IP are two separate computer network protocols. IP is the part that obtains the address to which data is sent. TCP is responsible for data delivery once that IP address has been found
- This protocol is responsible for managing the connection between a client and a server, making sure that the data which needs to be transferred is split into several packets which will all eventually reach their destination. If they don't, or if one of them is corrupt, TCP defines how the missing data will be retransmitted
- When you configure the TCP/IP protocol on a Windows computer, the TCP/IP configuration settings require:
  - An IP address
  - A default gateway
  - A subnet mask





# Gateway

- A gateway is a hardware device that acts as a "gate" between two networks. It may be a router, firewall, server, or other device that enables traffic to flow in and out of the network. It allows computers within the local network to send and receive data over the Internet
- For basic Internet connections at home, the gateway is the Internet Service Provider that gives you access to the entire Internet
- Gateway can provide hard-wired network or Wifi network (Wireless Fidelity)
- A gateway has an IP address just like any computer and most of the it's IP address ends with 1.  
e.g. **192.168.1.1**
- A home ISP gateway serves the DHCP server purpose as well to lease out IP addresses to requested devices

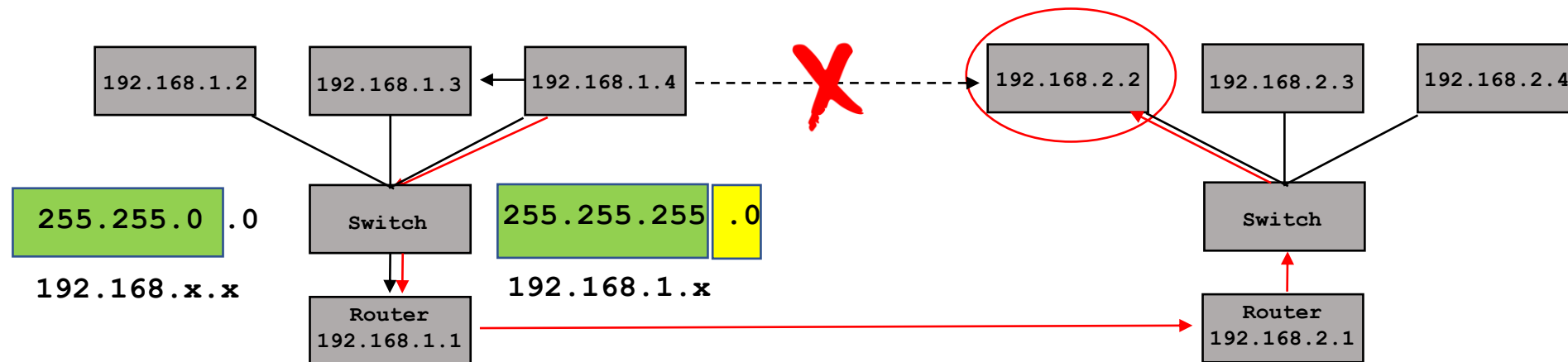


Let's look at how to find Gateway of your computer?

# Subnet Mask

1/2

- A subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses. (*Wikipedia*)
- A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs
- The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network



# Subnet Mask

2/2

- There are 3 major classes of IP address subnets:

Class	Address range	Supports
<b>Class A</b>	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
<b>Class B</b>	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
<b>Class C</b>	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
<b>Class D</b>	224.0.0.0 to 239.255.255.255	Reserved for <a href="#">multicast</a> groups.
<b>Class E</b>	240.0.0.0 to 254.255.255.254	Reserved for future use, or research and development purposes.

Let's look at how to find Subnet mask of your computer?

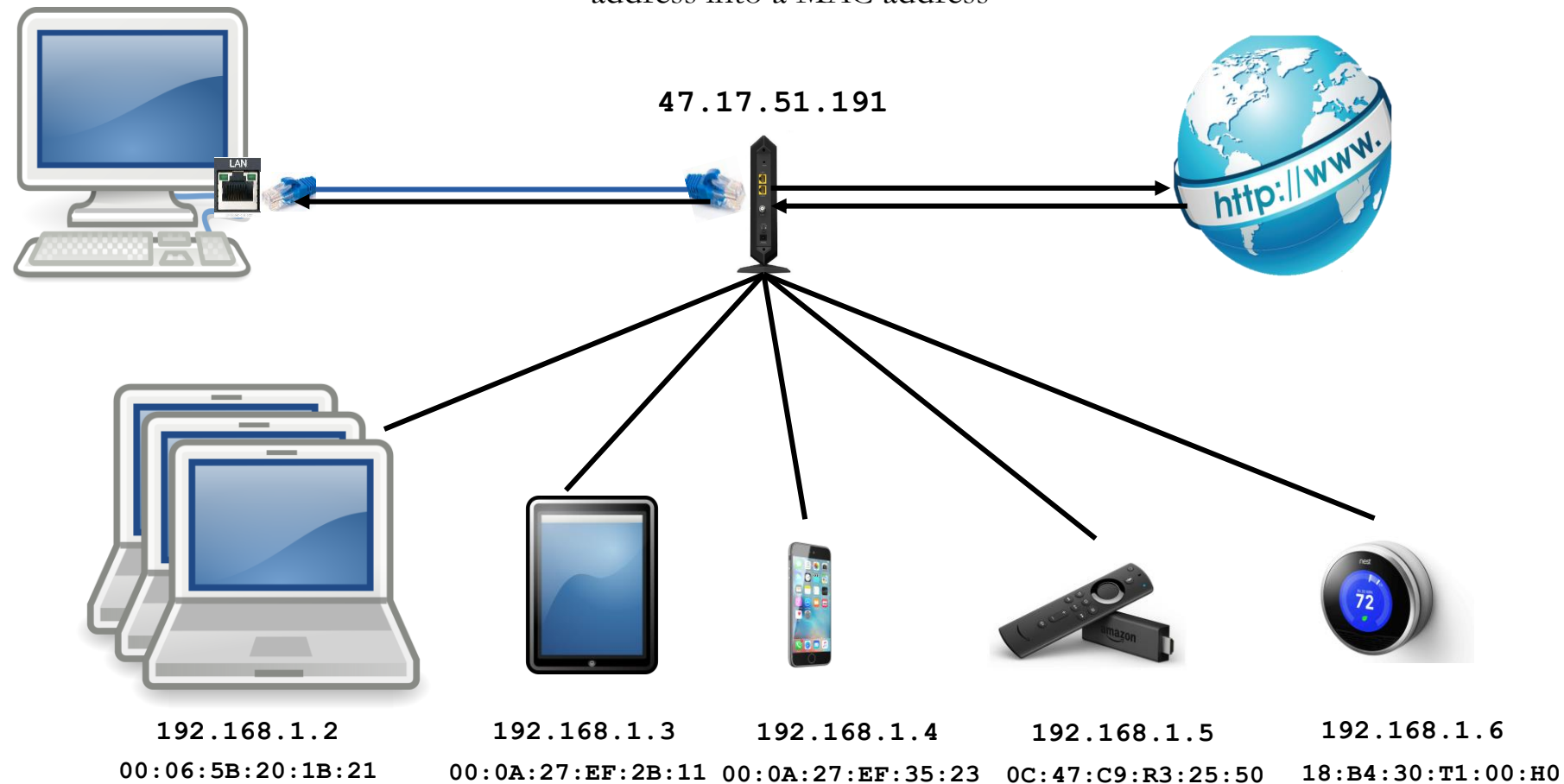
# MAC Address

- MAC stands for Media Access Control; it is given to a network adapter when it is manufactured. It is hardwired or hard-coded onto your computer's network interface card (NIC) and is unique to it
- The MAC address is sometimes referred to as a networking hardware address, the burned-in address (BIA), or the physical address
- The MAC address is a string of usually six sets of two-digits or characters, separated by colons. Here's an example of a MAC address: **00:14:22:DA:77:71**
- Each manufacturer put an Organizationally Unique Identifier or OUI in the MAC address.  
For example:

- **Dell:** 00:14:22
- **Nortel:** 00:04:DC
- **Cisco:** 00:40:96
- **Belkin:** 00:30:BD

# MAC Address

Something called the ARP (Address Resolution Protocol) translates an IP address into a MAC address



# MAC Address

- MAC addresses are assigned by the manufacturers of the device

Who assigns MAC addresses to manufacturers

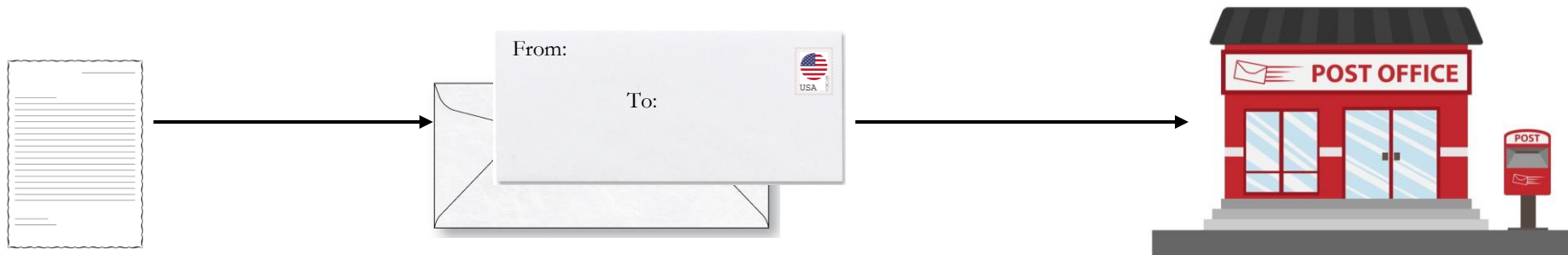
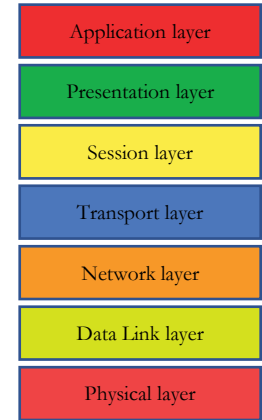


- The IEEE (Institute of Electrical and Electronics Engineers) assigns manufacturers the numbers, called organizationally unique identifiers
- The Institute of Electrical and Electronics Engineers is a professional association for electronic engineering and electrical engineering with its corporate office in New York City and its operations center in Piscataway, New Jersey

Let's look at how to find MAC address of your computer?

# OSI Layer

- OSI stands for Open Systems Interconnection and it is a theoretical or reference model that computer system uses to communicate over a network
- The main purpose of the OSI model was to standardize the communication between different hardware vendors
- OSI was introduced in 1983 by the major computer and telecom companies
- There are 7 layers in the OSI model
  - Physical, Data link, Network, Transport, Session, Presentation and Application

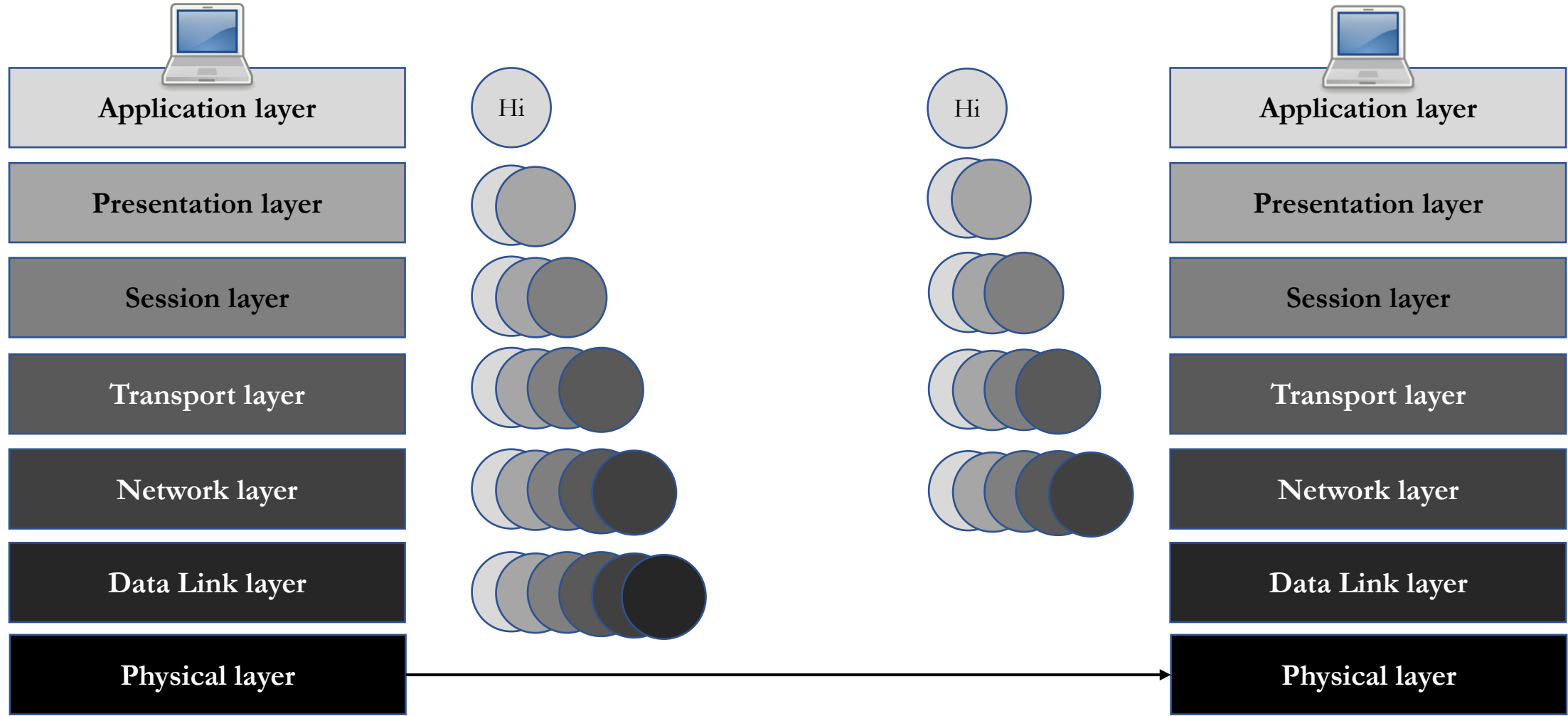


# OSI Layer

7	Application layer → FTP, SMTP, Telnet
6	Presentation layer → Format data, Encryption
5	Session layer → Start and Stop Session
4	Transport layer → TCP, UCP, Port numbers
3	Network layer → IP address, routers
2	Data Link layer → MAC addresses Switches
1	Physical layer → Cables, NIC, Hubs etc.



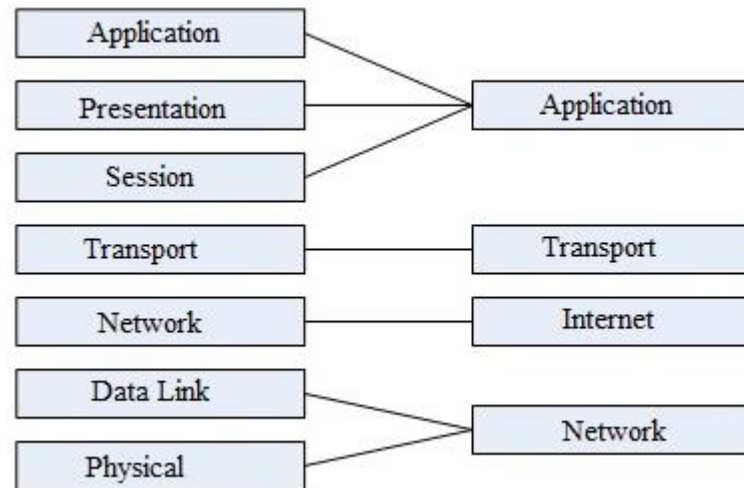
# OSI Layer



# OSI vs. TCP/IP

- OSI is a reference model around which the networks are built and generally, it is used as a guidance tool. On the other hand TCP/IP model is, in a way implementation of the OSI model

- OSI has 7 layers and TCP/IP has 4



- OSI model is developed by ISO (International Standard Organization), whereas TCP Model is developed by ARPANET (Advanced Research Project Agency Network)

# LAN, MAN and WAN

- **LAN - Local Area Network**

- A Local Area Network (LAN) is a private network that connects computers and devices within a limited area like a residence, an office, a building or a campus. On a small scale, LANs are used to connect personal computers to printers. However, LANs can also extend to a few kilometers when used by companies, where many computers share a variety of resources like hardware (e.g., printers, scanners, audiovisual devices etc.), software (e.g., application programs) and data.

- **MAN - Metropolitan Area Network**

- A Metropolitan Area Network (MAN) is a larger network than LAN. It often covers multiple cities or towns. It is quite expensive and not a lot of organization own it. Example of companies using MAN is cable TV network, ISP or companies running their businesses across country . MAN provides higher speed, from 1 gigabit per second to 100 Gbps

- **WAN - Wide Area Network**

- A Wide Area Network (WAN) is a much larger network than LAN and MAN. It often covers multiple countries or continents. Satellite is used to manage WAN. Internet is a big example of WAN

# Protocols and Ports

## Protocol:

- Network Protocols are a set of rules governing exchange of information in an easy, reliable and secure way
- A **protocol** is just the language that the two applications on either end of a conversation agree to speak in. If an application “A” is sending streams of bytes to application “B” then application “B” needs to know how to translate those bytes
- Most common protocols used in computer networks and the internet are TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and IP (Internet Protocol)

## Port:

- As the IP address identifies the computer, The network port identifies the application or service running on the computer. The use of ports allow computers/devices to run multiple services/applications
- You can think of a **port** as a phone extension, with the computer's IP address being like its phone number. You can call the number (IP address) to talk to the computer, then dial the extension (port) to talk to a specific application. An application needs to be listening on a port in order to communicate
- Most common ports used are **SSH (22)** , **HTTP (80)** , **HTTPS (443)** , **FTP (20)** , **DNS (53)** etc.

# Types of Network Devices

(Hub, Switch, Modem, Router, Gateway, Access point)

1/4

- Network devices are called hardware devices that link computers, printers, faxes and other electronic devices to the network. Such devices easily and safely transfer data from one network to another
- Back in the days, each network device referred to a single device that performed a single function. That is no longer the case these days. Your “modem” from your ISP is probably a modem, router, switch and access point all-in-one

## Hub:



- Hub has several Ethernet ports that allows multiple computers to communicate with each other over a network. It is an obsolete device that you would never want to buy these days. It looks just like a switch but works differently on the inside
- Hubs are like switches but are not as "smart." Switches send incoming data to a specific port whereas hubs broadcast all incoming data to all active ports
- Hub shares the bandwidth across all the ports
- Hubs are considered the OSI layer 1 (Physical) devices.

# Types of Network Devices

(Hub, Switch, Modem, Router, Gateway, Access point)

2 / 4

## Switch:



- Switches have a smarter job than hubs in general. A switch improves the capacity of the network
- A switch also has several ports that allows multiple computers to communicate with each other over a network
- Switches read incoming packets “hardware addresses” to transfer them to their respective destinations that is why incoming data is sent to a specific port whereas hubs broadcast all incoming data to all active ports
- Switches are considered the OSI layer 2 (Data link)
- Switch provides dedicated speed on each port unlike hub.



## Modem:

- A modem is a small box that connects your household to the Internet using cables. It acts as a digital translator, taking an information signal (Internet data) from your cable or phone lines and making it accessible to your computer
- Mostly modem has one port for Coaxial cable and 2<sup>nd</sup> for Ethernet which can either go directly to your computer or a switch/hub.

# Types of Network Devices

(Hub, Switch, Modem, Router, Gateway, Access point)

3/4

## Router:



- Routers work at Layer 3 (Network) of the OSI model, which deals with IP addresses
- A router is a device that joins networks together and routes traffic between them. At home, this typically means the router connects your local network to your ISP's network
- Now a days a router serves as a hub, switch, modem, gateway and router functionality (All in one)
- A gateway and a router are essentially the same. The term "default gateway" is used to mean the router on your LAN which has the responsibility of being the first point of contact for traffic to computers outside the LAN.



# Types of Network Devices

(Hub, Switch, Modem, Router, Gateway, Access point)

4 / 4

## Access Point:

- Access points are used for extending the wireless coverage of an existing network and for increasing the number of users that can connect to it
- A high-speed Ethernet cable runs from a router to an access point, which transforms the wired signal into a wireless one.



# How Internet Works?

## List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project