Eng/ Ahmed El-khatib

CCNA Course

Part One - CCNA Lectures from lecture 1 - 14

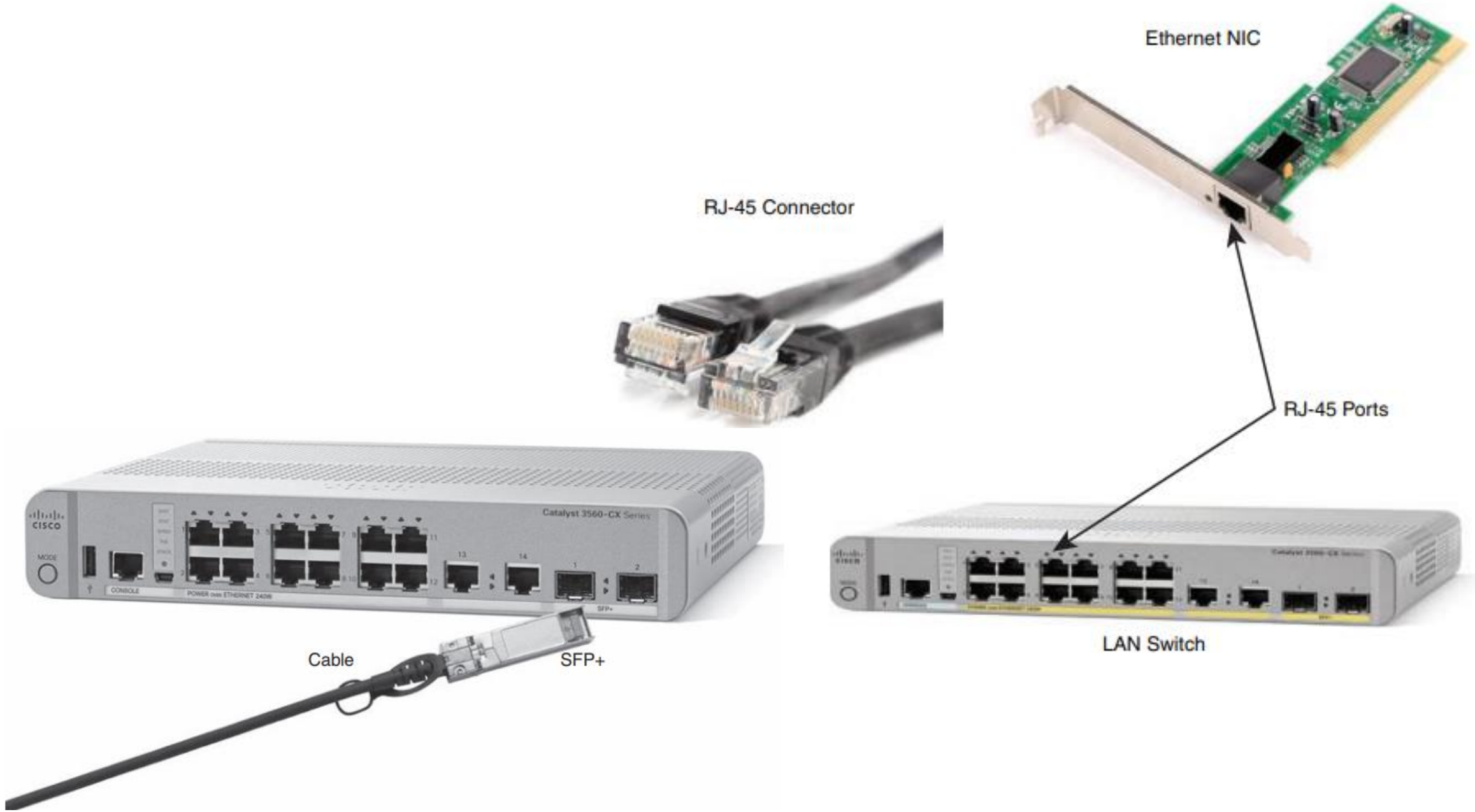
Eng/ Ahmed El-khatib

What is the network anyway …?

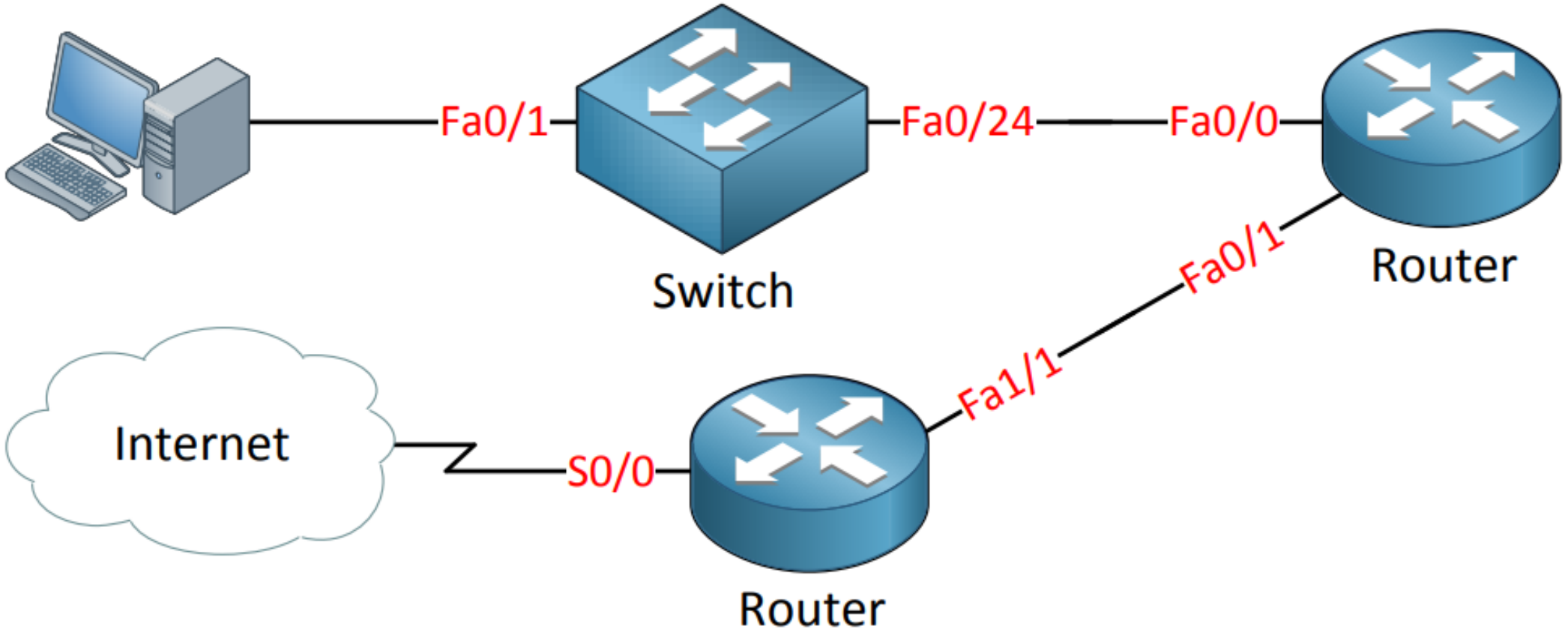
A network is just a collection of devices and end systems connected to each other and able to communicate with each other . This devices could be computers , servers , smartphones ,routers , etc. … . A network could be as large as internet or as small as your two computers at home sharing files and printers .

Some of components that make up the network

- **Personal Computers (PC)** :- These are the end point of your Network , Sending and Receiving data .
- **Interconnections** :- These are the components that's make sure data can travel from one device to another , Like , Network interface card (NIC) , Media (Cables – Wireless) , and connectors .
- **Switches** :- This boxes are network devices which provide a network connection for your end devices .
- **Routers** :- that's interconnect networks and choose the best path to each network destination


Ethernet NIC
RJ-45 Connector
RJ-45 Ports
Cable
SFP+
LAN Switch

An Examples (A Network Diagram)



Why do we use networks …?

I Think this one obvious since your are using networks on a daily basis but let's sum up what we use network for :-

- **Applications** :- Sending data between computers , Sharing files .
- **Recourses** :- Networks Printers , Network Cameras
- **Storage** :- Using NAS (Network Attached Storage) will make your storage available on the network , many people use one at home to share files ,videos , and picture between computers .
- **Backups** :- using central backup server where all computers send their data to for backup .
- **VOIP** : Voice Over IP is becoming more important day and replacing analog telephone

Types Of Applications

We are all using applications on a daily basis but if we look at them with a network-minded view we can divide them in 3 different categories :-

- Batch Applications
- Interactive Application
- Real-Time Applications

A Batch Applications is something you just let run and you don't care if it takes a minute more or less since nobody is "Waiting" for a response .

This applications have No direct human Interaction, Like (FTP , TFTP , HTTP downloads , could be a backup job overnight ….)

Interactive Applications is a Human-to-Human Interaction but it someone is waiting for response ,so there is response time (delay) is important .

With interaction application you need to think about someone who is working on a database server and sending commands. Once your press enter you want it to responds fast but a second more or less is perhaps .

Real-Time applications also Human-To-Human Interaction but there aren't a delay like , VOIP (Voice Over IP) , or Live Conferencing) .

Network Topologies

When We look at a Networks we have different types of "Topologies" and we have two different type of topologies :

- **Logical Topology :-** Is what the network looks like and how all cables and devices are connected to each other

- **Physical Topology :-** Is the Path our data signals takes through the physical topology .

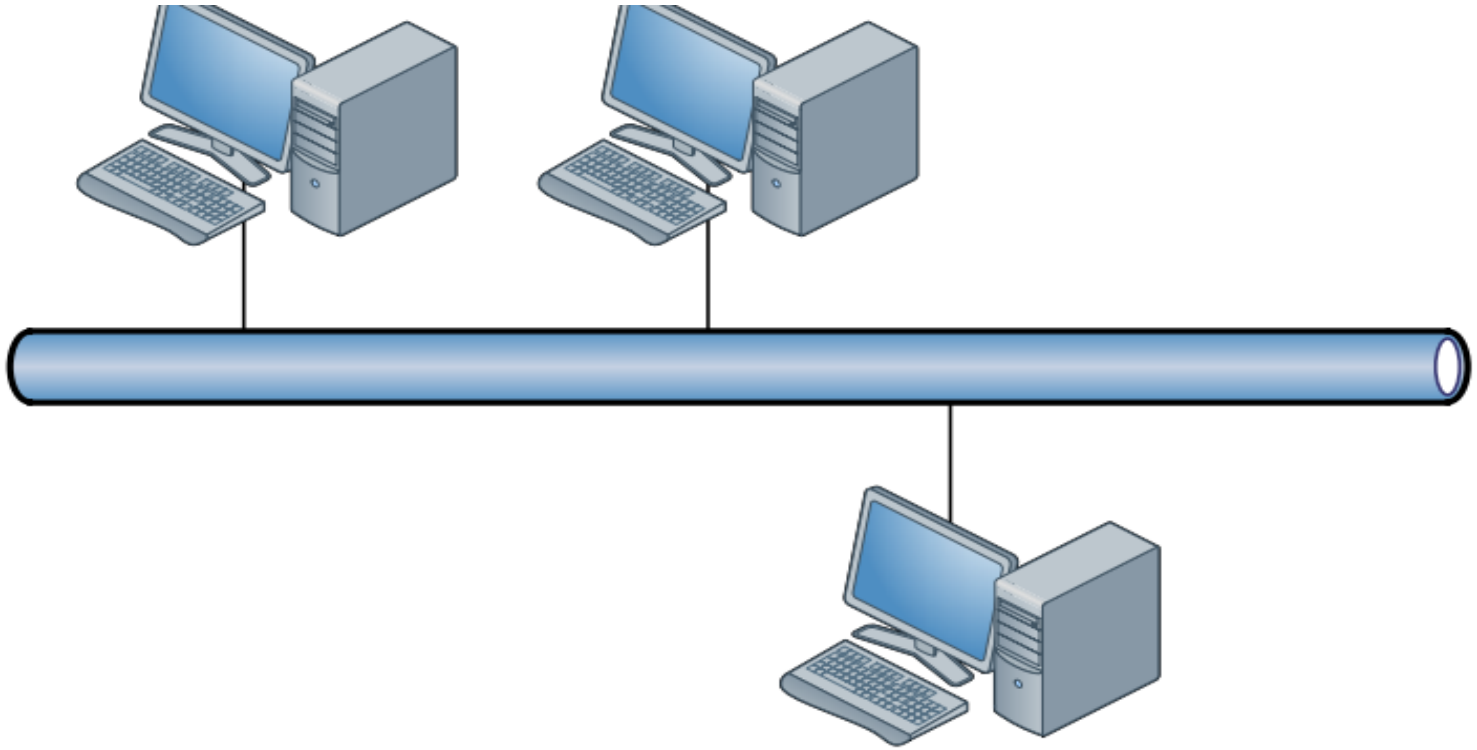
Physical Network Topologies

There are Multiple Types Of Physical Topologies :-

- Bus Topology
- Ring Topology
- Star Topology
- Mesh topology

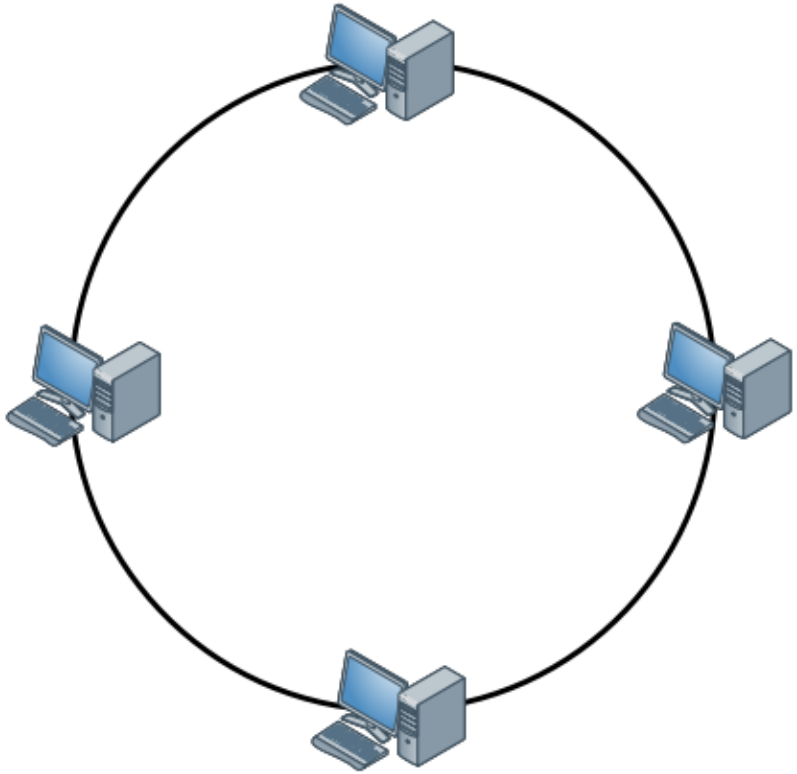
Bus Topology

One of the first networks was based on Coaxial- Cables. This was basically just a one long cable and every device was connected to it . At the end of the cable you had to place a terminator .If the cable breaks then your Network is Down



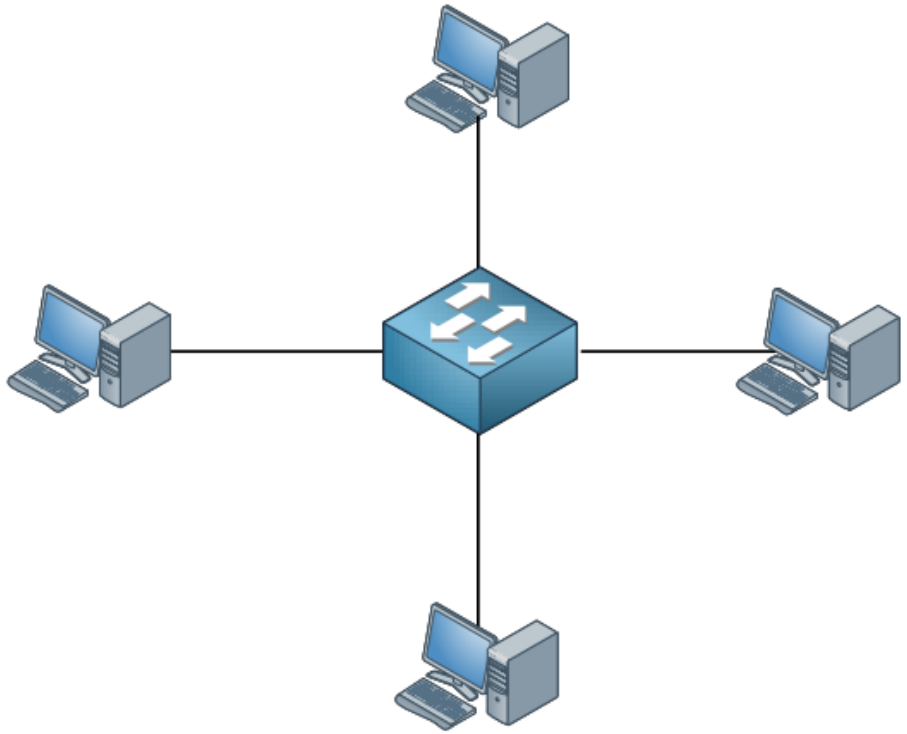
Ring Topology

In Ring Topology all computers and network devices are connected on a cable and that last two devices are connected to each other to form a "Ring" . **If the cables breaks your network is down** . There is also **"Dule-Ring" setup** for redundancy ,This just another cable to make sure if one cable breaks your networks isn't going down.



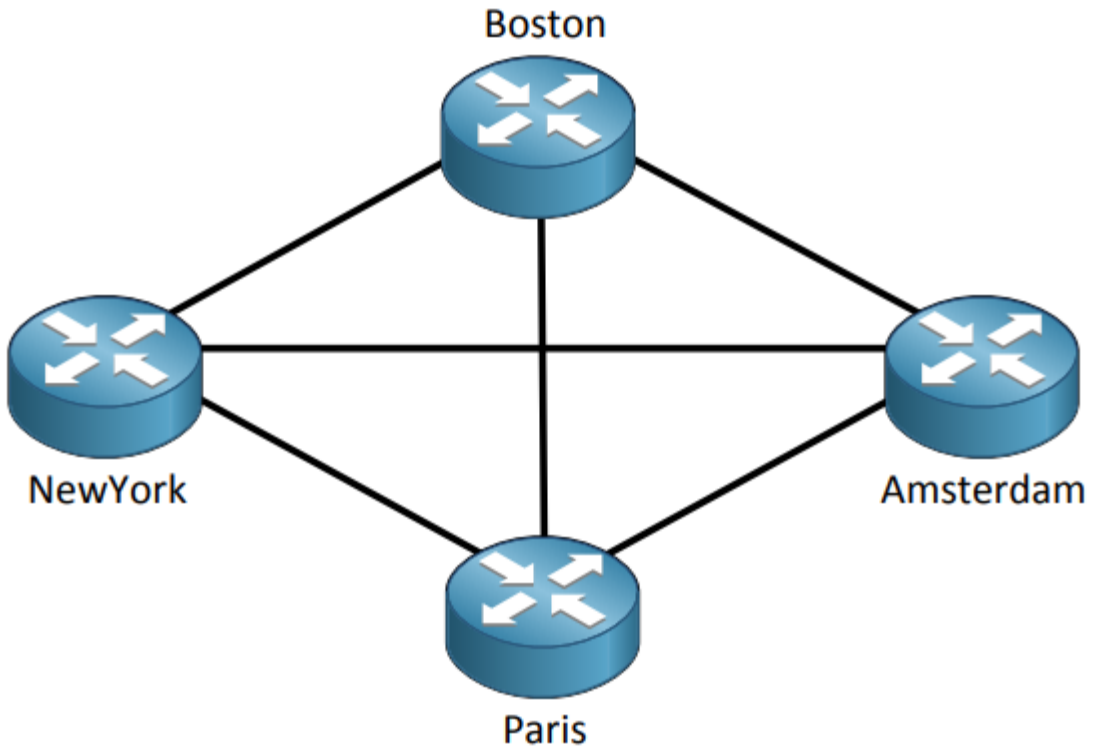
Star Topology

In Star topology All our end devices (Computers) connected to a central devise creating a "Star" model .This is what use nowadays on Local Area Network (LAN) with a Switch in the middle . When your switch goes down your network is down as well .



Mesh Topology

In Mesh Topology each device connecting directly to the other device . If we have a company that has a multiple sites and each sit as a "Router" so we link all sites Via a Mesh Topology



Networks Types

Networks types can be divided into 3 basic classifications :

1. Types of network according to geographical area
2. Types of network according to access methods
3. Types of network according to the Functionality

By Geographic Area

1- LAN (Local Area Network): Connects devices in a small space like your home, office, or lab

Example: Connecting your laptop to a printer in your office

2- MAN (Metropolitan Area Network) : Covers a larger area like a city or a group of campuses

Example: A university network linking all its faculties in one city

3- WAN (Wide Area Network) : Covers huge distances — connects cities or even countries

Example: Sending an email from Egypt to the USA = WAN at work!

By Access Type

1- Internet : The global open network we all use daily

Example: Browsing Facebook, YouTube, or Google.

2- Intranet : A private internal network for companies or organizations

Example: Employees accessing the HR system to request vacations

3- Extranet: Similar to an intranet but gives limited access to outsiders

Example: A supplier accessing a company's system to check inventory.

By Functionality

1-Client-Server : A main server provides services to other devices (clients) Example: Visiting a website – your browser is the client, the site is on a server. In Windows, this setup is usually part of a "Domain".

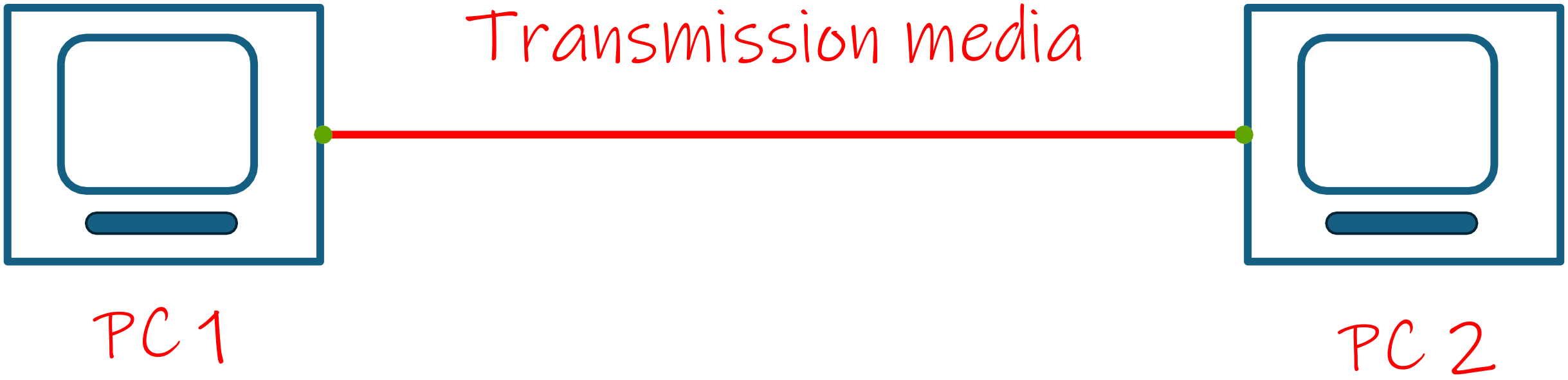
2- Peer-to-Peer (P2P) : All devices are equal, sharing resources directly

Example: Using BitTorrent – your PC is both client and server. In Windows, this is known as a "Workgroup".

Cabling

Introduction

In The network , to connect to devices to each other we need a Transmission media



Transmission media

Cables

Network cabling is the backbone of any computer network, providing the physical medium for data transmission. Without proper cabling, devices wouldn't be able to communicate, and the network would simply not function. It's a critical component often overlooked, yet its quality directly impacts network performance, reliability, and scalability.

Types of Network Cables

There are several types of cables used in networking, each with its own characteristics and ideal applications:

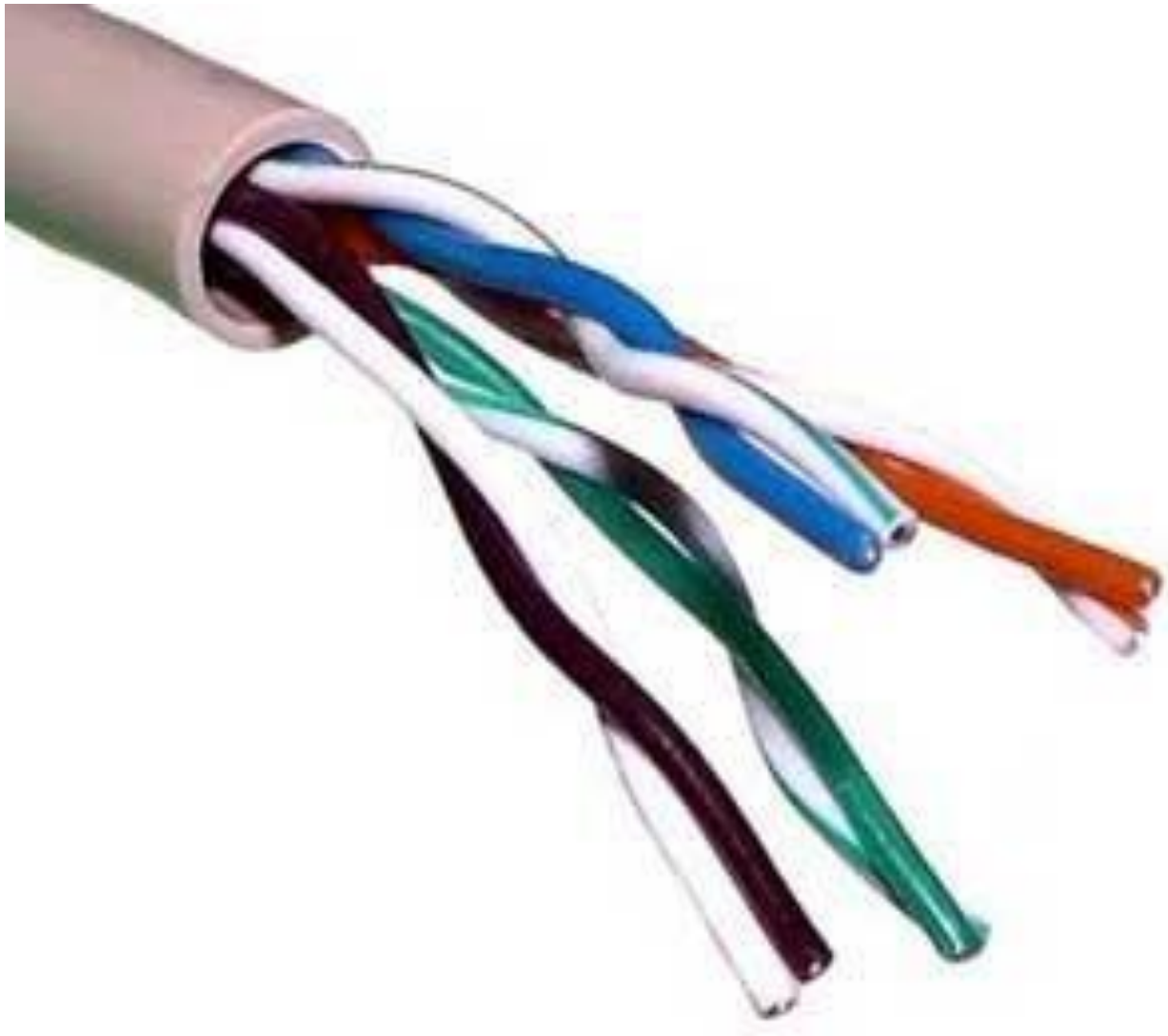
- **Ethernet Cables (Twisted Pair):** These are the most common type of cables used in Local Area Networks (LANs). They consist of insulated copper wires twisted into pairs to reduce electromagnetic interference (EMI).

- **Fiber Optic Cables:** These cables transmit data using light pulses through glass or plastic strands. They offer significantly higher bandwidth, longer transmission distances, and are immune to electromagnetic interference.

- **Coaxial Cables:** Less common in modern LANs but still used for cable television and some older network technologies. They have a central copper conductor surrounded by an insulating layer, a metallic shield, and an outer insulating jacket.

Ethernet Cables (Twisted Pair)

UTP



Unshielded
Twisted
Pair

10 BASE - T

100 BASE - T

= 2 pairs (4 wire)

1000 BASE - T

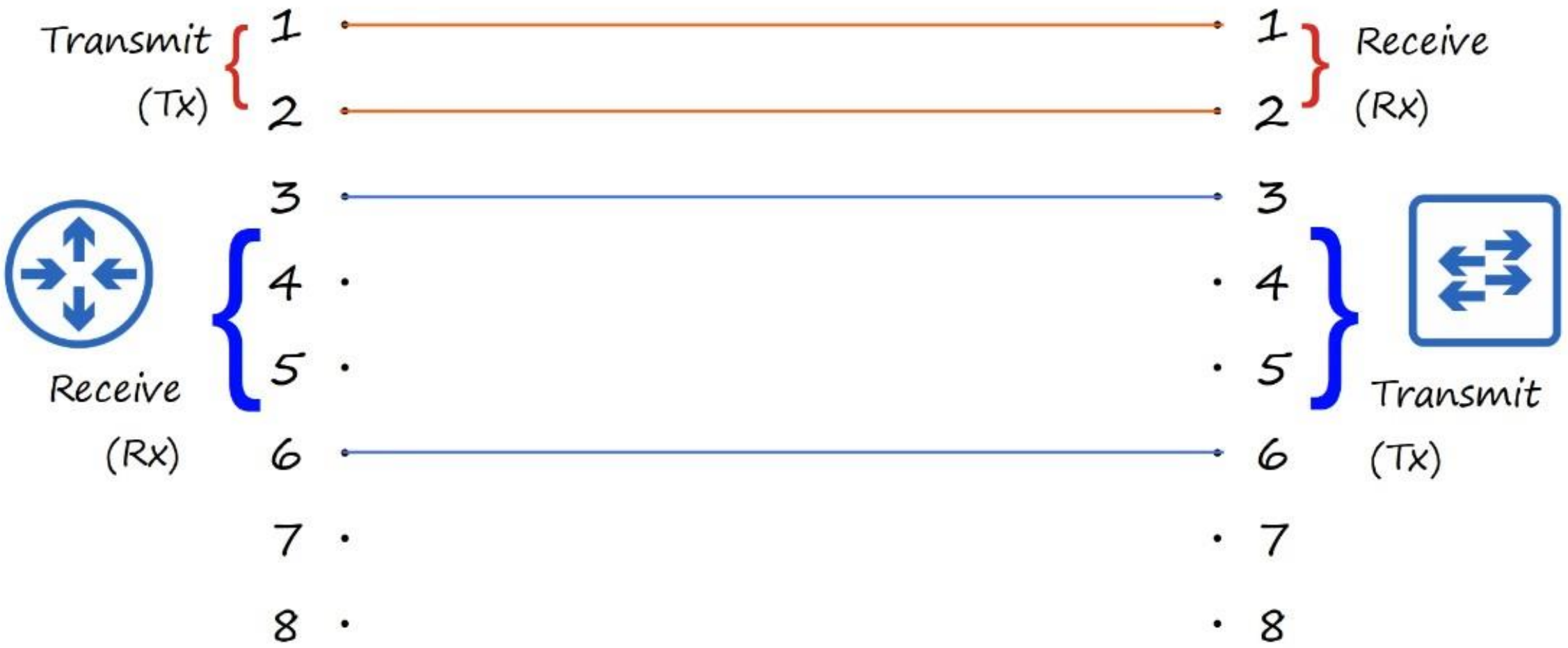
10G BASE - T

= 4 pair (8 wire)


Transmit
(Tx)
1
2
3
4
5
6
7
8
1
2
3
4
5
6
7
8
Receive
(Rx)
Receive
(Rx)
Transmit
(Tx)

Straight-through cable: Used to connect an MDI device to an MDI-X device (e.g., a computer to a switch). The transmit pins on one end connect to the receive pins on the other, and vice-versa.

Straight-through cable

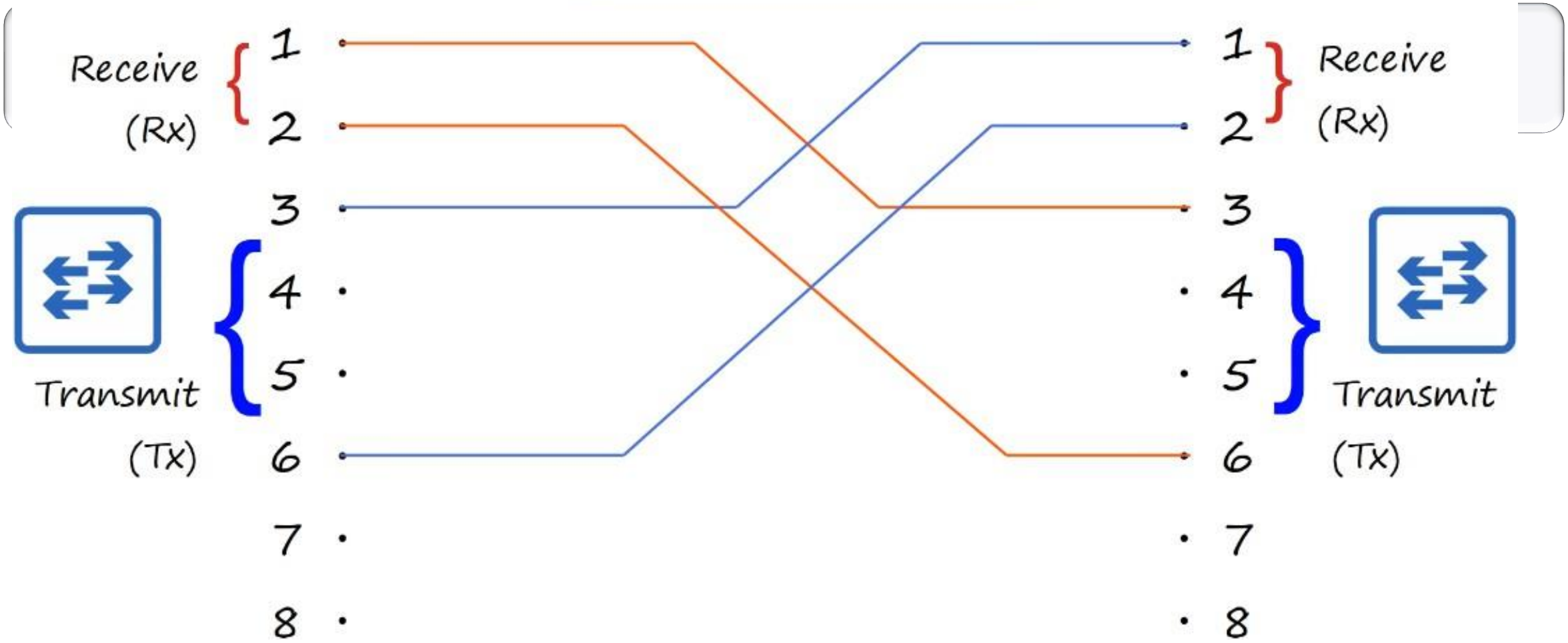


Straight-through cable

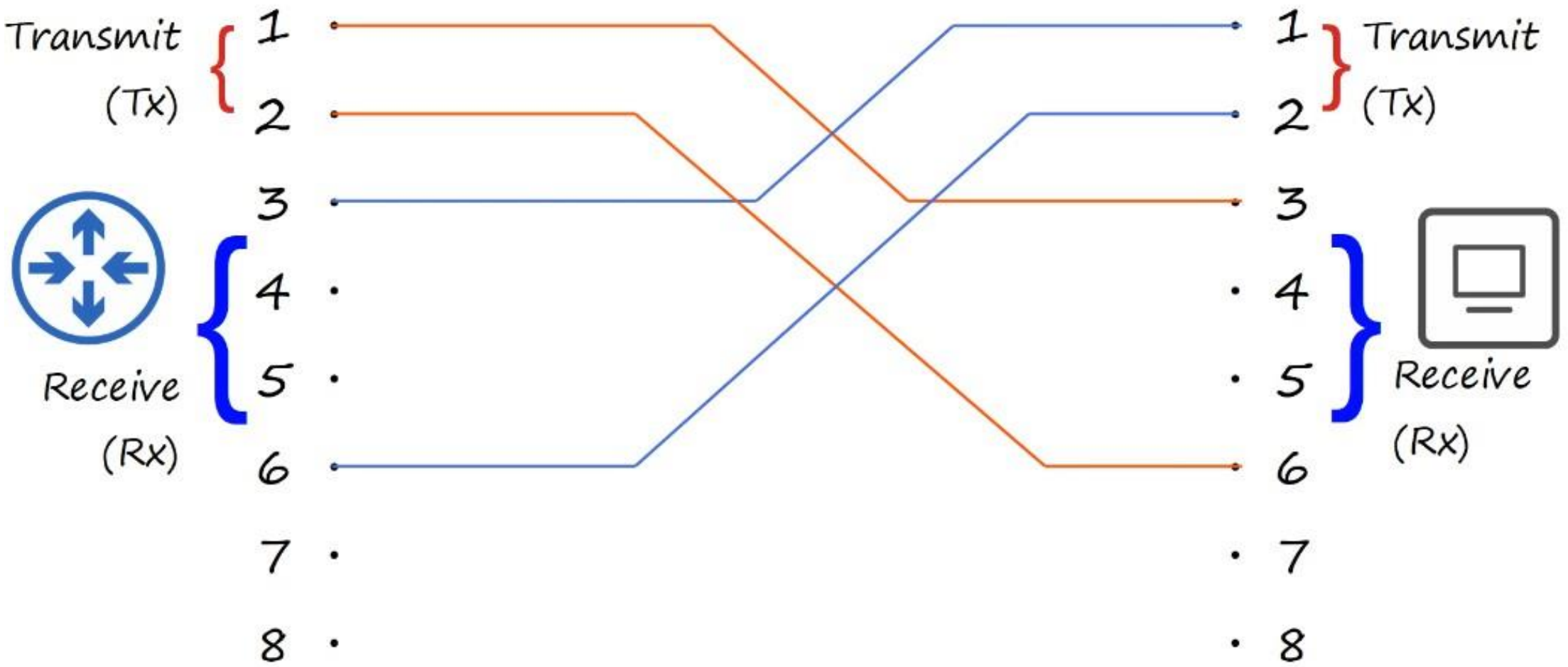
Straight-through cable

Crossover cable: Used to connect two devices of the *same* type (e.g., a computer to another computer, or a switch to another switch). This cable has some internal wiring that "crosses over" the transmit and receive pairs, so that the transmit pins on one device connect to the receive pins on the other.

Crossover cable



Crossover cable



Device Type	Transmit (TX) Pins	Receive (Rx) Pins
Router 	1 and 2	3 and 6
Firewall 	1 and 2	3 and 6
PC 	1 and 2	3 and 6
Switch 	3 and 6	1 and 2

Auto MDI-X (Automatic Medium-Dependent Interface Crossover) is a very handy feature found in modern network devices like switches, routers, and even some computers. To understand what it does, let's first look at the problem it solves:

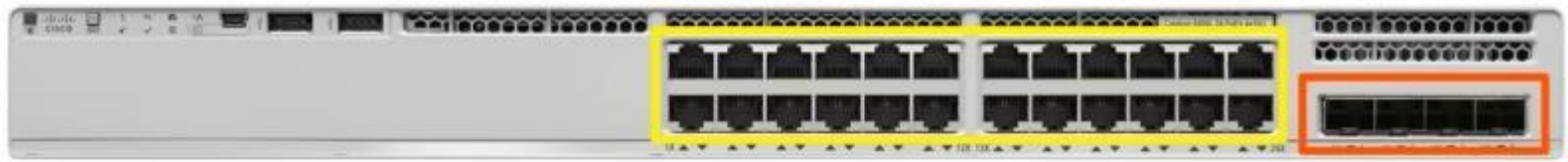
Auto MDI-X

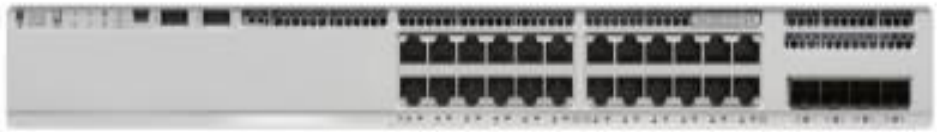

Receive
(Rx)
1
2
3
4
5
6
7
8
Transmit
(Tx)
1
2
3
4
5
6
7
8
Receive
(Rx)
Transmit
(Tx)

Auto MDI-X


Receive
(Rx)
1
2
3
4
5
6
7
8
Transmit
(Tx)
1
2
3
4
5
6
7
8
Transmit
(Tx)
Receive
(Rx)

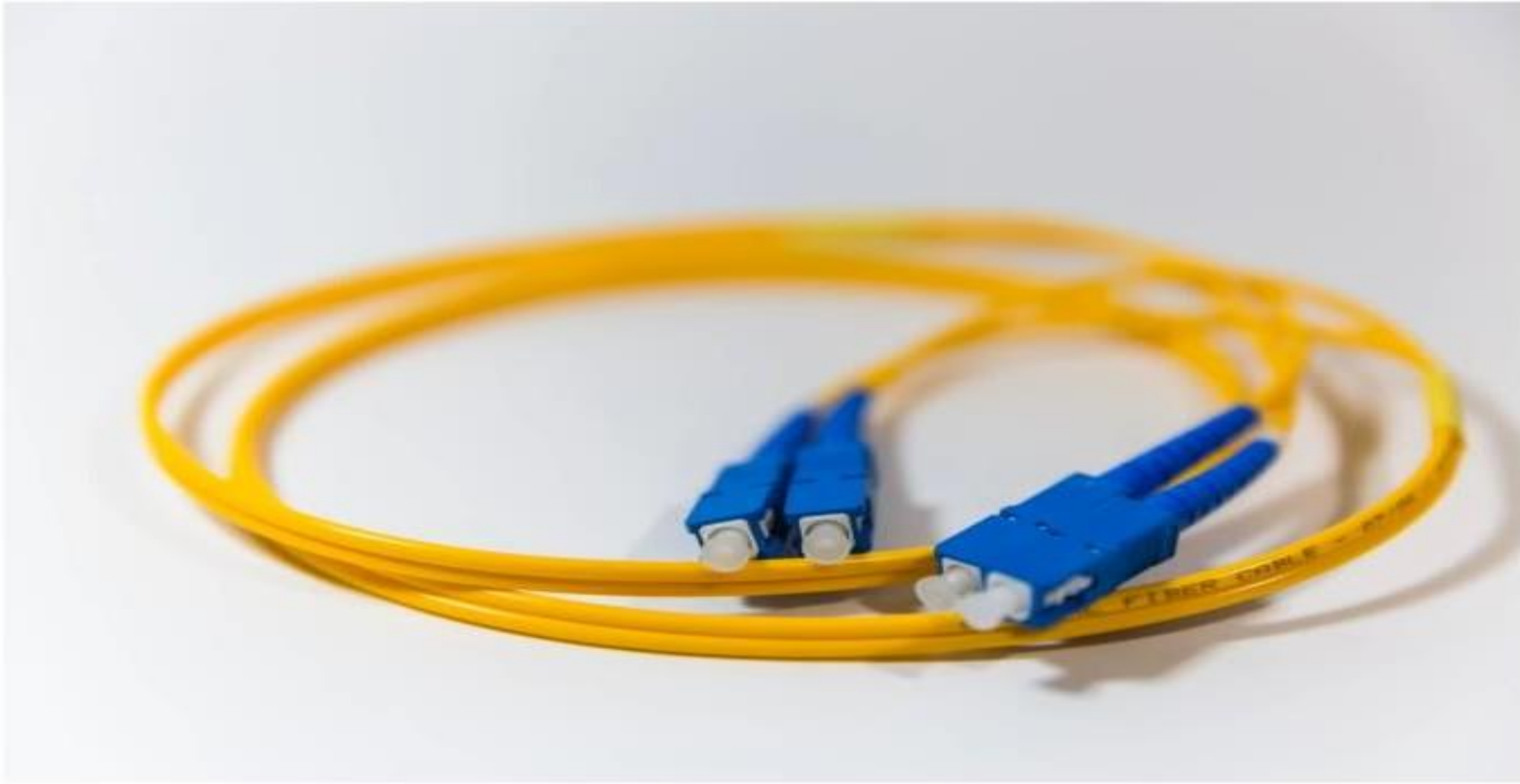
Fiber Optic Cables





SFP Transceiver

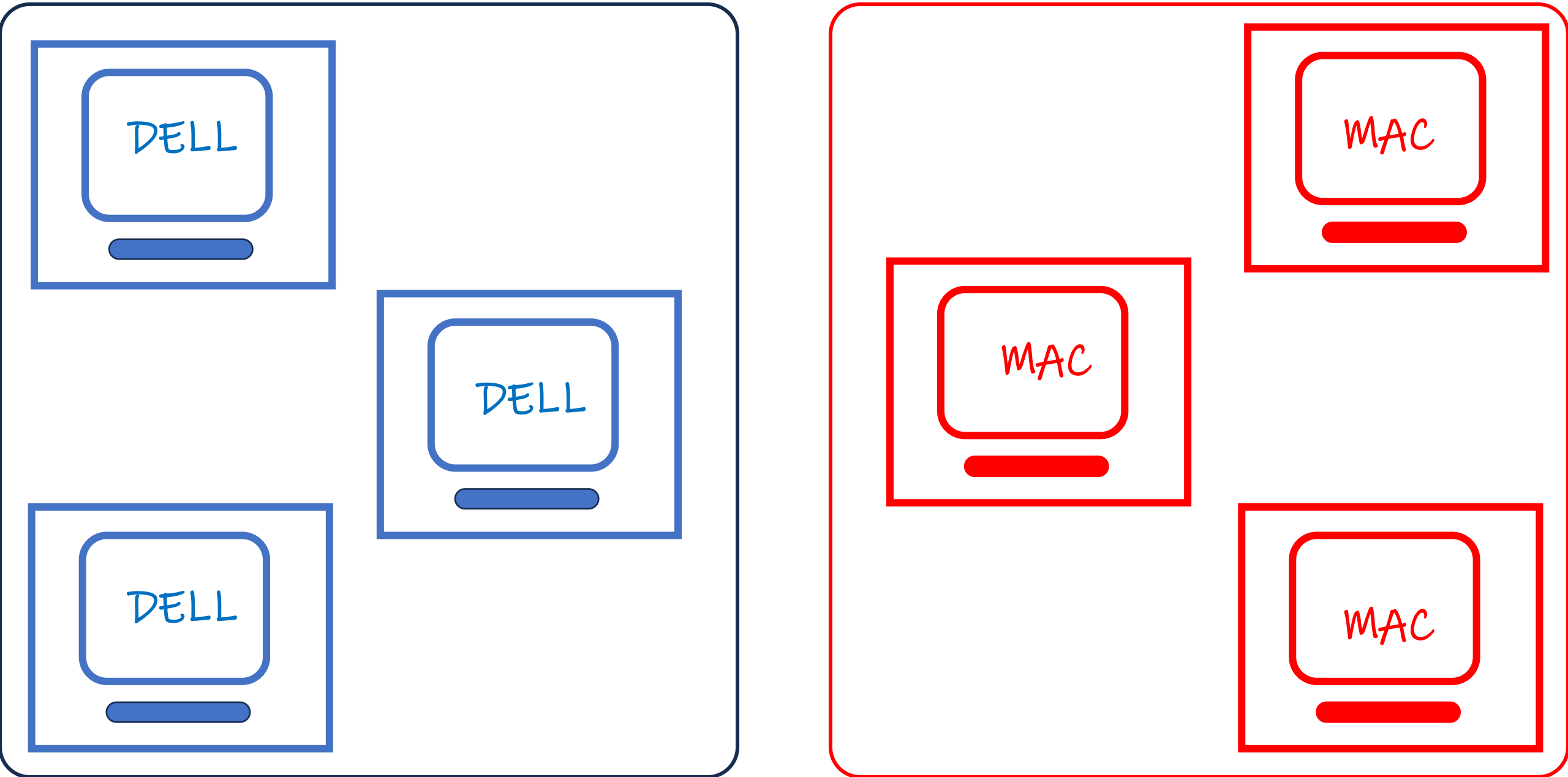
(Small Form-Factor Pluggable)

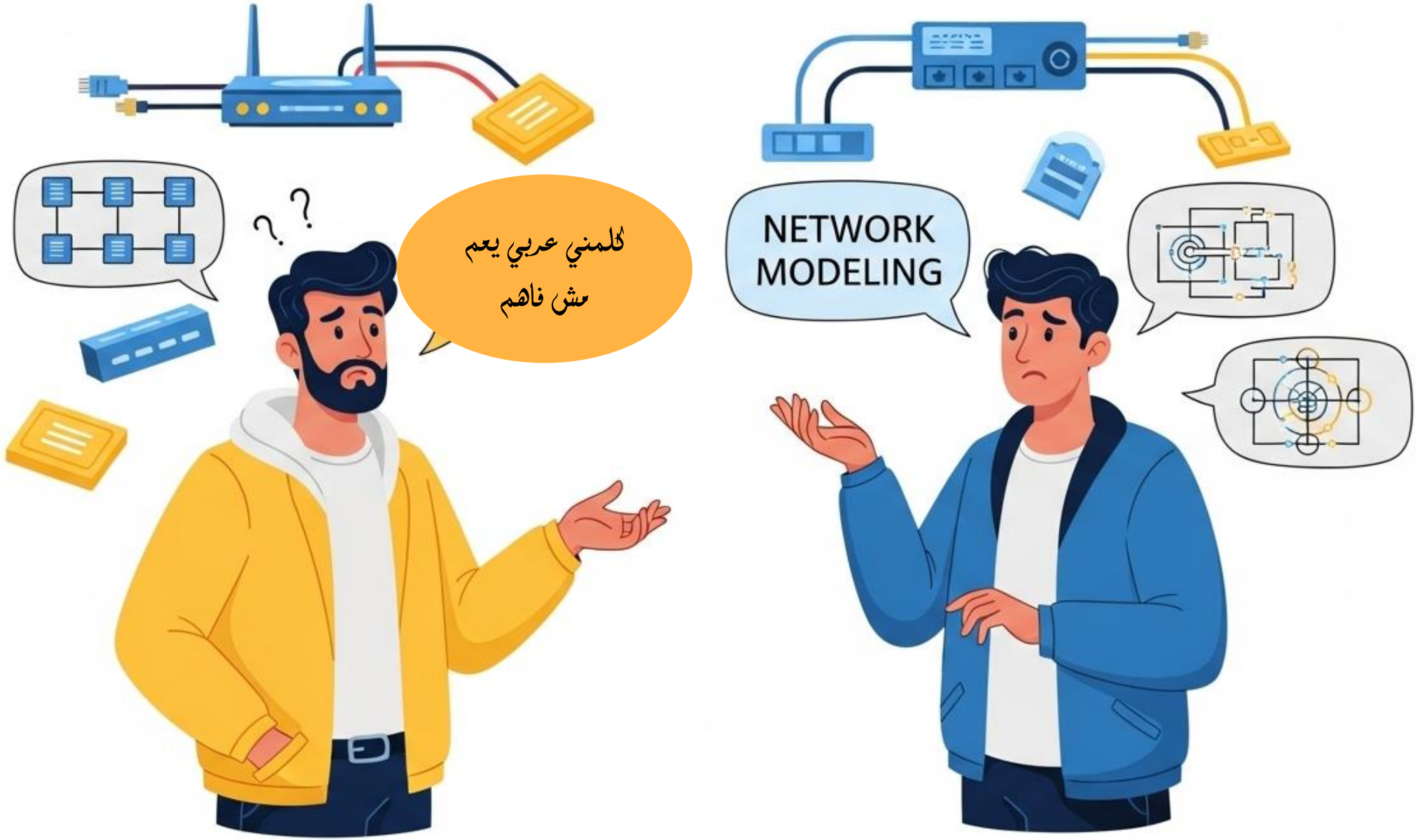



Tx
Rx
Rx
Tx

Network Models

Introduction




كلمني عربي يعم
مش فاهم
NETWORK
MODELING

Introduction

Networking Models : it is categories and provide a structure for Network Protocols and Standards

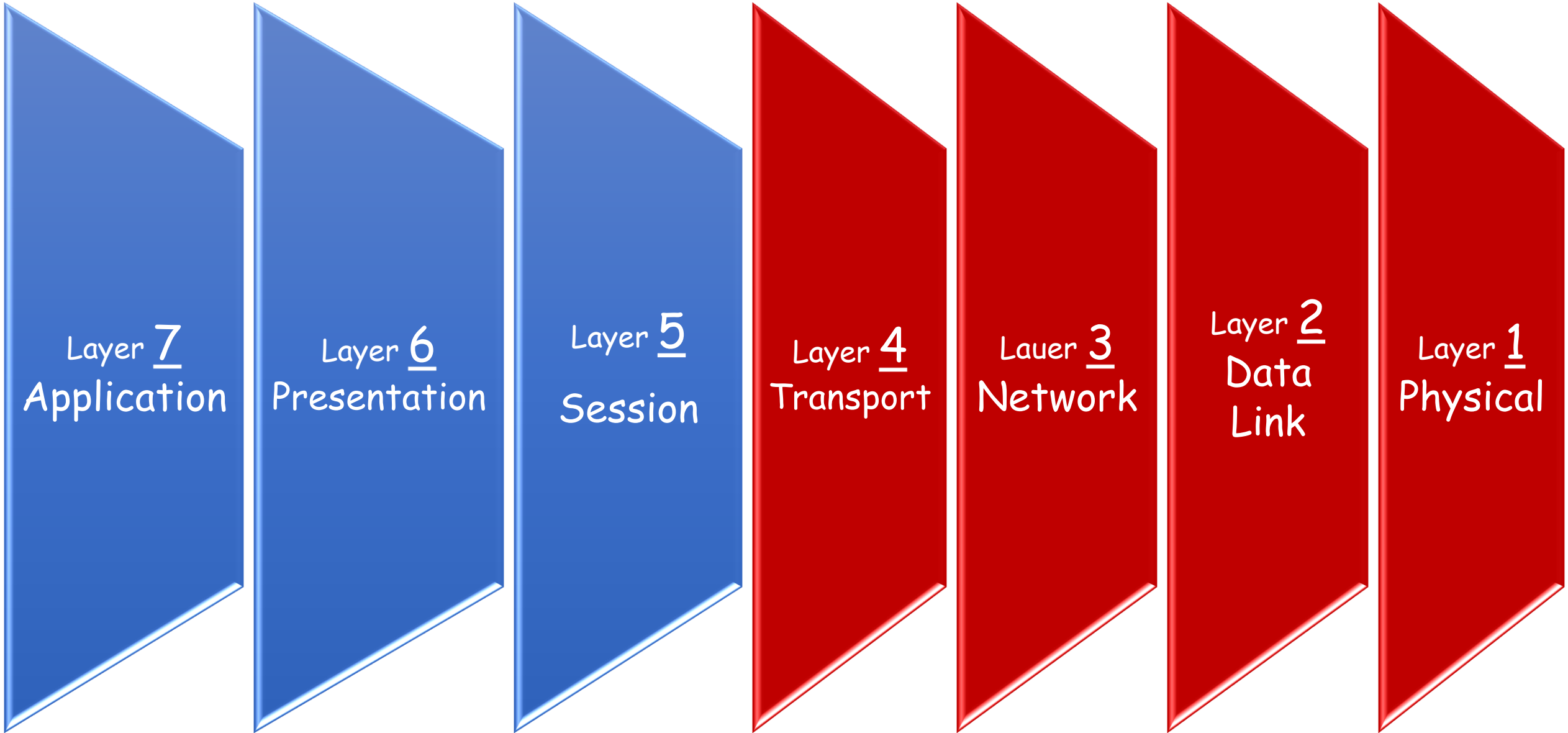
Network Protocols : is a set of rules defining how network devices and software should work

In the beginning the development of networks was chaotic.

- Each vendor had its own proprietary solution.
- The bad part was that one vendor's solution was not compatible with another vendor's solution.
- This is where the idea for the OSI-model was born, having a layered approach to networks our hardware vendors would design hardware for the network, and others could develop software for the application layer.
- Using an open model which everyone agrees on means we can build networks that are compatible with each other.

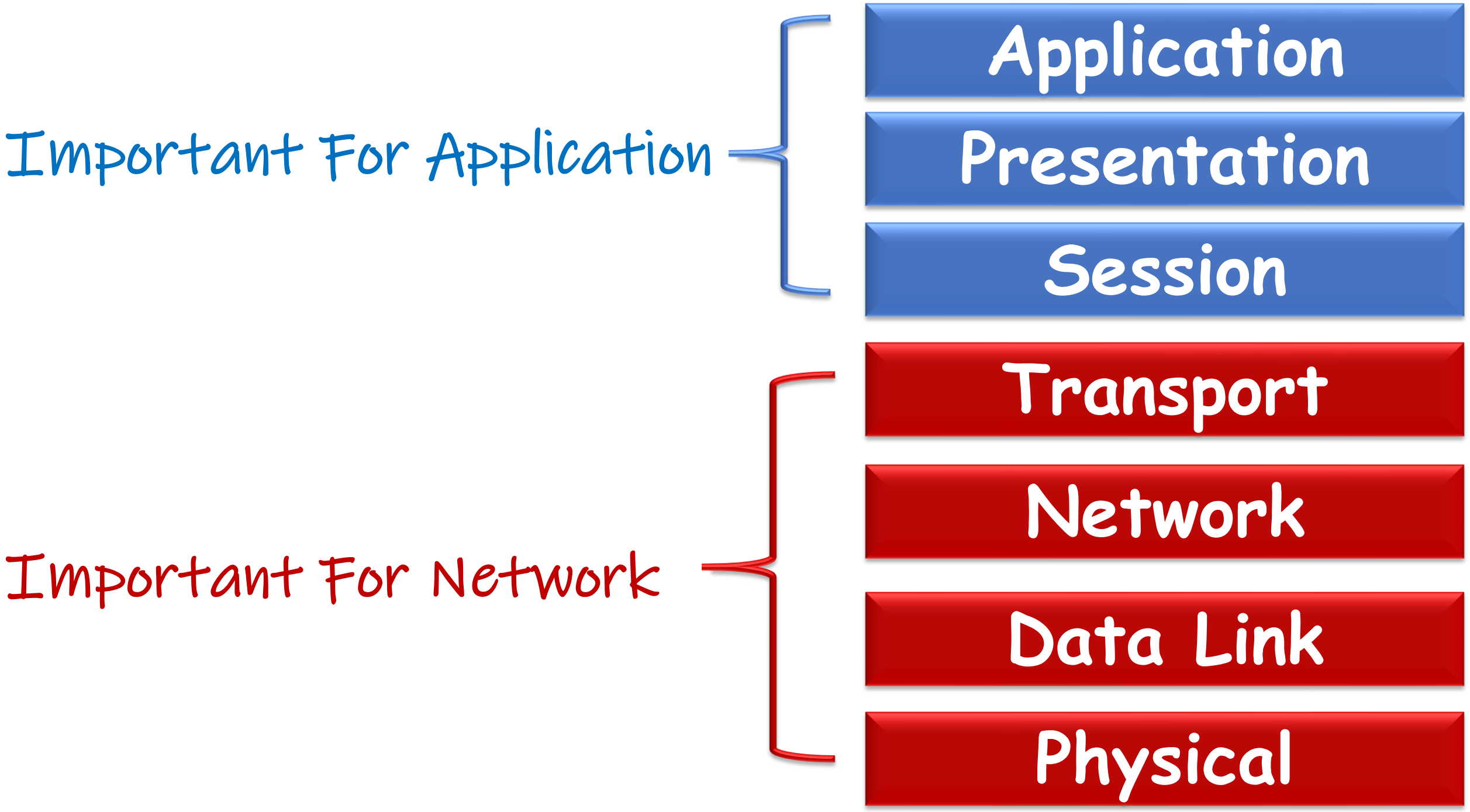
The OSI-model isn't just a model to make networks compatible; it's also one of the BEST ways to teach people about networks. Keep this in mind since I'll be referring a lot to the OSI-model, it's very useful!

OSI Layers Approach



Note!!

- The first four layers are important for networking.
- The upper three layers are important for applications.


Important For Application
Application
Presentation
Session
Important For Network
Transport
Network
Data Link
Physical

- **Physical Layer:** This layer describes stuff like voltage levels, timing, physical data rates, physical connectors and so on. Everything you can "touch" since it's physical.

- **Data Link:** This layer makes sure data is formatted the correct way, takes care of error detection and makes sure data is delivered reliably. This might sound a bit vague now, for now try to remember this is where "Ethernet" lives. MAC Addresses and Ethernet frames are on the Data Link layer.

- **Network:** This layer takes care of connectivity and path selection (routing). This is where IPv4 and IPv6 live. Every network device needs a unique address on the network.

- **Transport:** The transport layer takes care of transport, when you downloaded this book from the Internet the file was sent in segments and transported to your computer.
  - TCP lives here; it's a protocol which send data in a reliable way.
  - UDP lives here; it's a protocol which sends data in an unreliable way

- **Session:** The session layer takes care of establishing, managing and termination of sessions between two hosts. When you are browsing a website on the internet you are probably not the only user of the webserver hosting that website. This webserver needs to keep track of all the different "sessions".

- **Presentation:** This one will make sure that information is readable for the application layer by formatting and structuring the data. Most computers use the ASCII table for characters. If another computer would use another character like EBCDIC than the presentation layer needs to "reformat" the data so both computers agree on the same characters.

- **Application:** Here are your applications. E-mail, browsing the web (HTTP), FTP and many more.

Note!!

you can't skip any layers in the OSI-model, it's impossible to jump from the Application layer directly to the Network layer. You always need to go through all the layers to send data over the network.

Let's take a look at a real life example of data transmission.

1. You are sitting behind your computer and want to download some files of a local web server.
   - ❑ You start up your web browser and type in the URL of your favourite website.
   - ❑ Your computer will send a message to the web server requesting a certain web page.
   - ❑ You are now using the HTTP protocol which lives on the application layer.

2. The presentation layer will structure the information of the application in a certain format.

3. The session layer will make sure to separate all the different sessions.

4. Depending on the application you want a reliable (TCP) or unreliable (UDP) protocol to transfer data towards the web server in transport layer , in this case it'll choose TCP since you want to make sure the webpage makes it to your computer. We'll discuss TCP and UDP later.

5. Your computer has a unique IP address (for example 192.168.1.1) and it will build an IP packet. This IP packet will contain all the data of the application, presentation and session layer. It also specifies which transport protocol it's using (TCP in this case) and the source IP address (your computer 192.168.1.1) and the destination (the web server's IP address). The IP Address lives in Network Layer

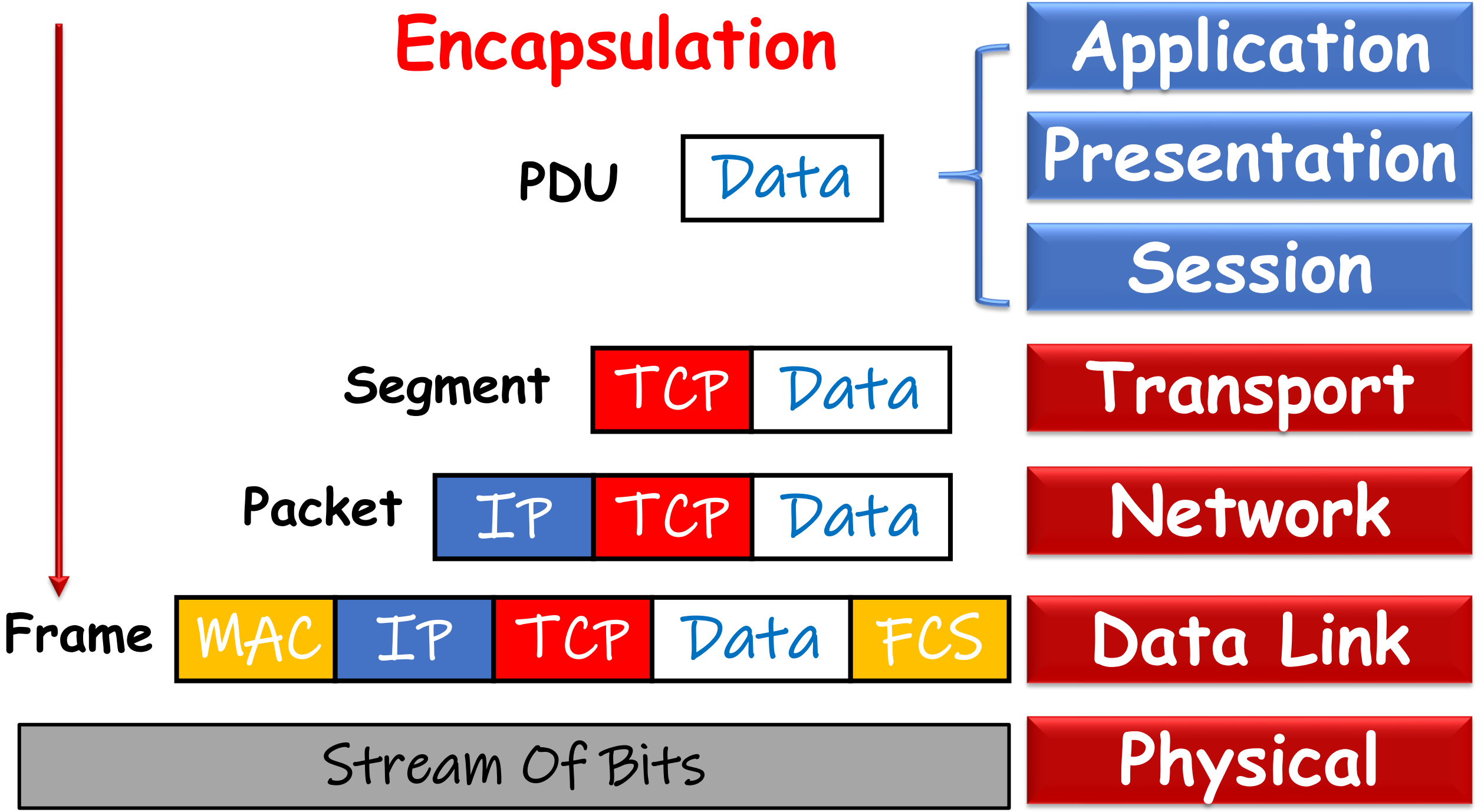
6. The IP packet will be put into an Ethernet Frame. The Ethernet frame has a source MAC address (your computer) and the destination MAC address (web server). The MAC Address lives in Data Link Layer. More about Ethernet and MAC addresses later.

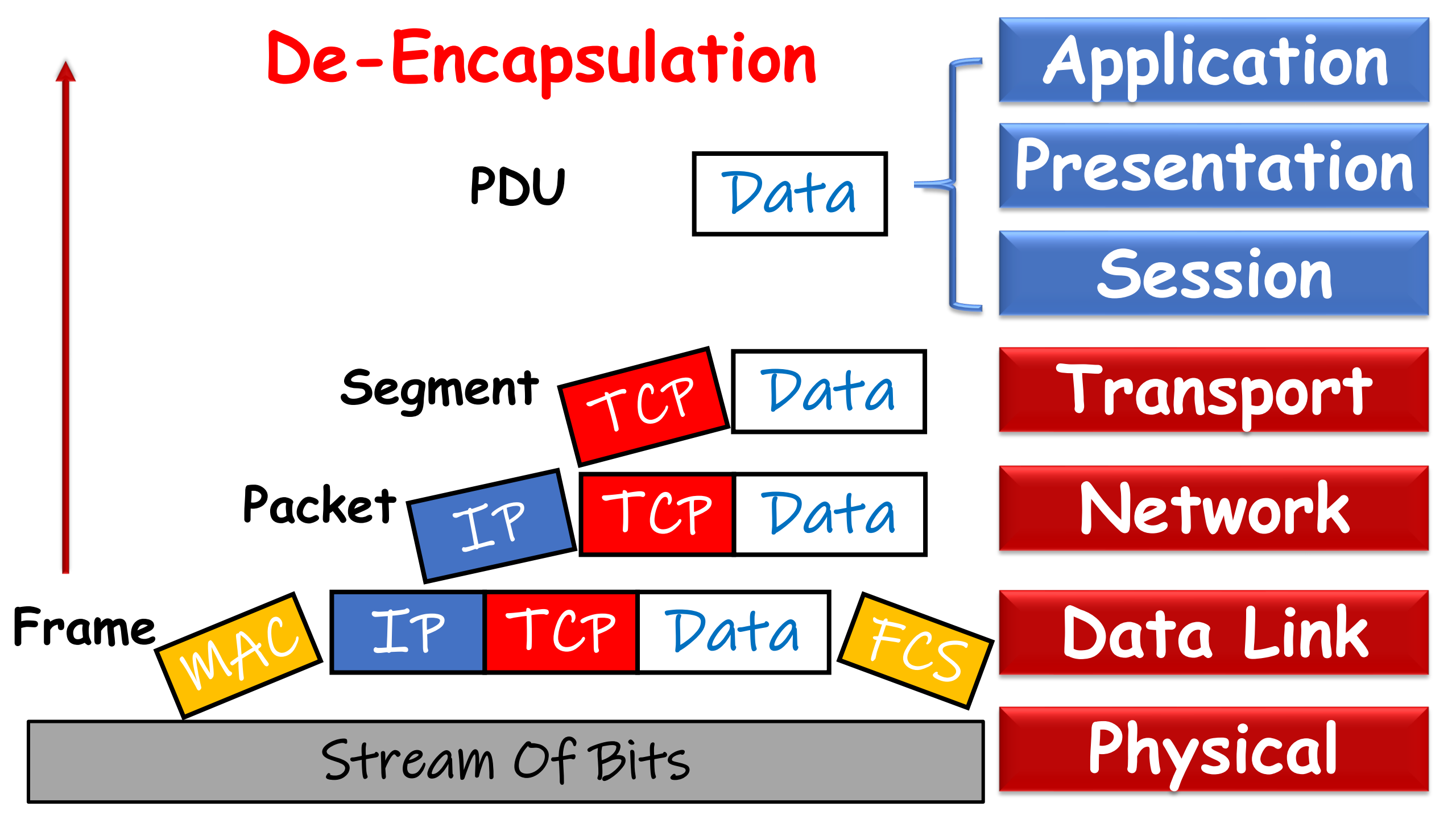
7. Finally everything is converted into bits and sent down the cable using electric signals. In Physical Layer

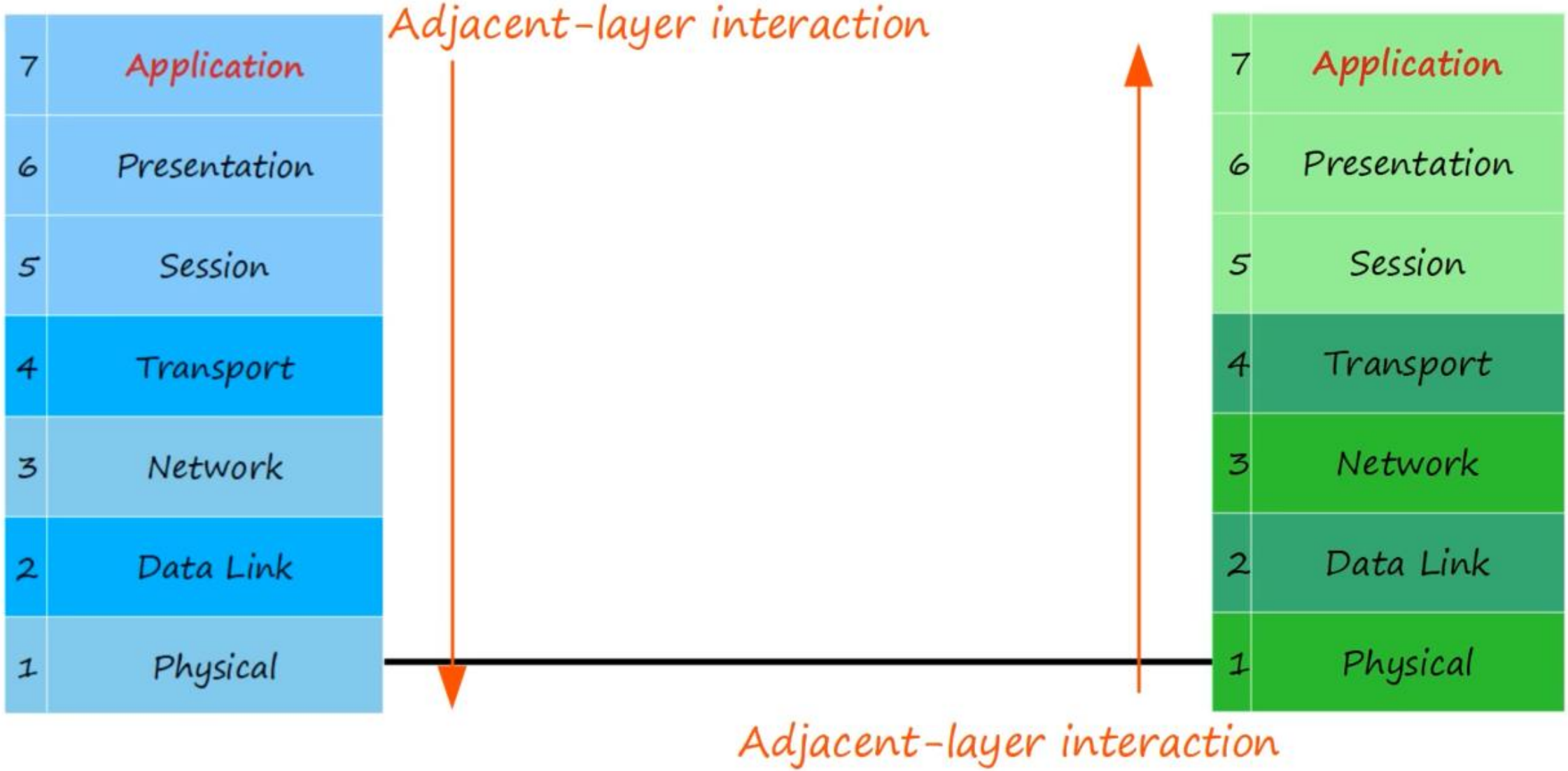
Encapsulation and De-Encapsulation

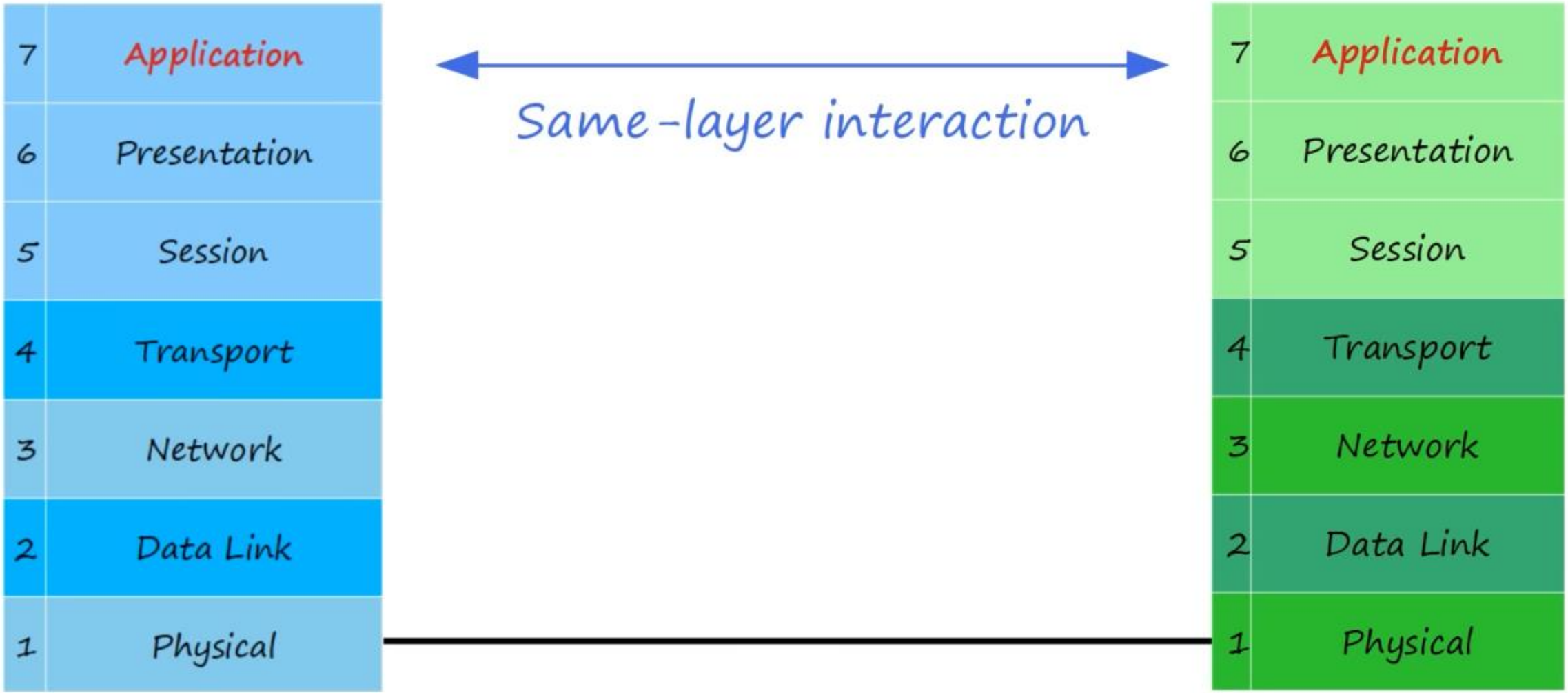
- Going from the application layer all the way down to the physical layer is what we call **encapsulation.**
- Going from the physical layer and working your way up to the application layer is called **de-encapsulation.**

Encapsulation




De-Encapsulation
PDU
Data
Application
Presentation
Session
Segment
TCP
Data
Transport
Packet
IP
TCP
Data
Network
Frame
MAC
IP
TCP
Data
FCS
Data Link
Stream Of Bits
Physical


Adjacent-layer interaction
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Adjacent-layer interaction

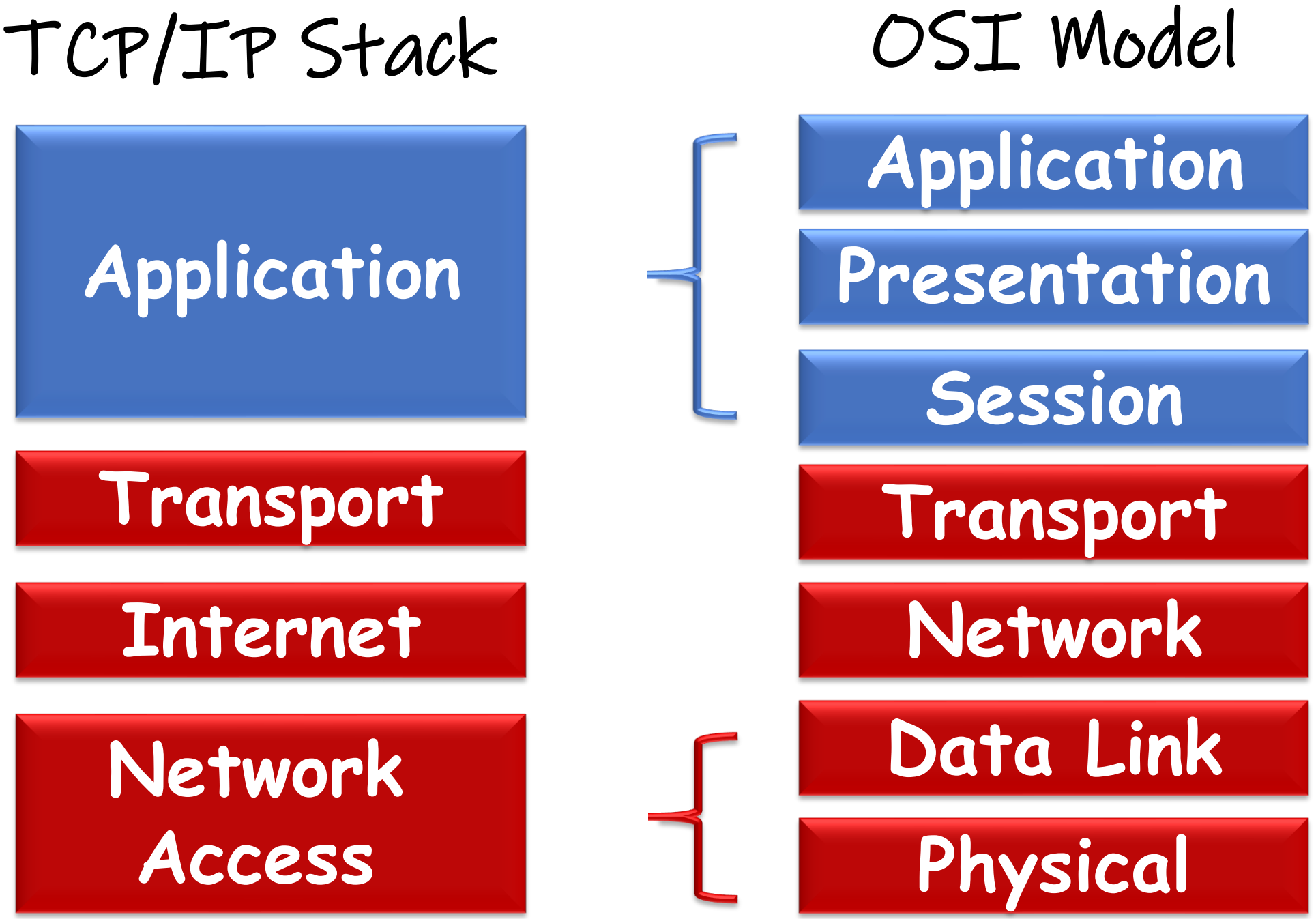

7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Same-layer interaction
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

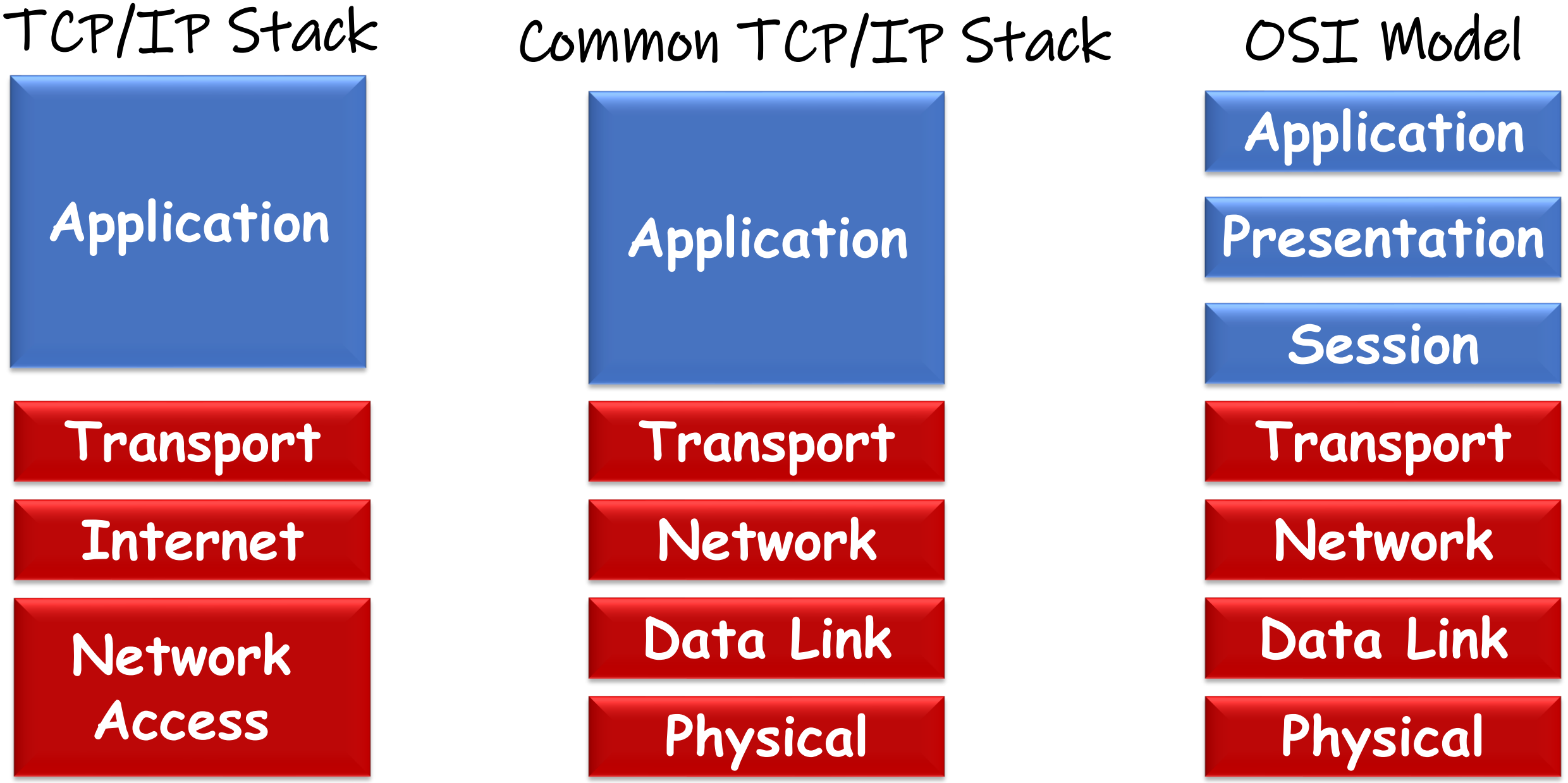
Now you know about the OSI-model, the different layers and the function of each layer. During peer-to-peer communication each layer has "packets of information". We call these protocol data units (PDU). Now every unit has a different name on the different layers:

- Transport layer: Segments; For example we talk about TCP segments.
- Network layer: Packets; For example we talk about IP packets here.
- Data link layer: Frames; For example we talk about Ethernet frames here.

TCP/IP Stack

Besides the OSI-model there was another organization that created a similar model which never became quite as popular. However for your CCNA you'll need to know what it looks like. It's called the TCP/IP stack and it's similar except some of the layers are combined and have different names.


TCP/IP Stack
OSI Model
Application
Transport
Internet
Network Access
Application
Presentation
Session
Transport
Network
Data Link
Physical


TCP/IP Stack
Application
Transport
Internet
Network Access
Common TCP/IP Stack
Application
Transport
Network
Data Link
Physical
OSI Model
Application
Presentation
Session
Transport
Network
Data Link
Physical

RFC 1122, Internet STD 3 (1989)	Cisco Academy[31]	Kurose,[32] Forouzan[33]	Comer,[34] Kozierok[35]	Stallings[36]	Tanenbaum[37]	Arpanet Reference Model (RFC 871)	OSI model
Four layers	*Four layers*	*Five layers*	*Four+one layers*	*Five layers*	*Five layers*	*Three layers*	*Seven layers*
"Internet model"	"Internet model"	"Five-layer Internet model" or "TCP/IP protocol suite"	"TCP/IP 5-layer reference model"	"TCP/IP model"	"TCP/IP 5-layer reference model"	"Arpanet reference model"	OSI model
Application	Application	Application	Application	Application	Application	Application/Process	Application
							Presentation
							Session
Transport	Transport	Transport	Transport	Host-to-host or transport	Transport	Host-to-host	Transport
Internet	Internetwork	Network	Internet	Internet	Internet		Network
Link	Network interface	Data link	Data link (Network interface)	Network access	Data link	Network interface	Data link
		Physical	(Hardware)	Physical	Physical		Physical

Internet Protocol version 4 (IPv4)

Let's talk about IP!

- IP (Internet Protocol) determines where we are going to send packets to by looking at the destination IP address. How we determine where to send them is up to the routing protocol, we'll talk more about routing later.

- IP uses Packets called IP packets to carry information.

- Every IP packet is a single unit of information and besides data it carries information to determine where to send the packet.

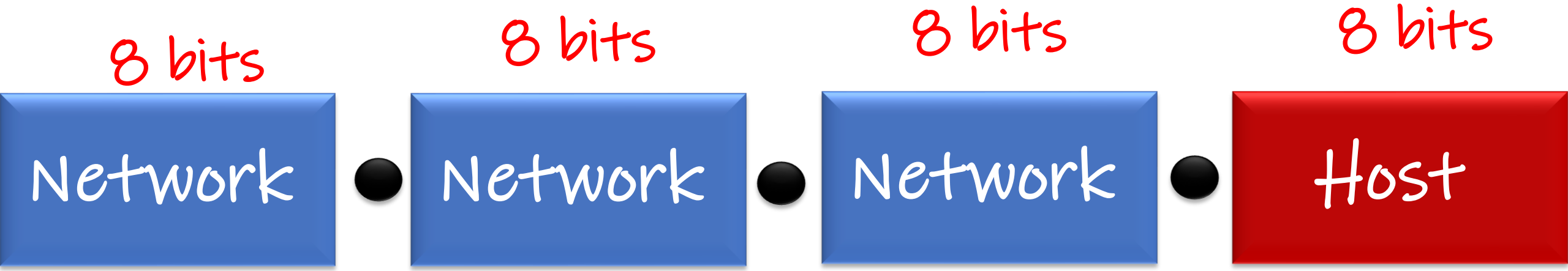
- Operates at the network layer of the OSI model.
- Connectionless protocol: IP itself does not setup a connection, in order to transport data you need the "transport" layer and use TCP or UDP
- Every packet is treated independently; there is no order in which the packets are arriving at their destination
- Hierarchical: IP addresses have a hierarchy; we'll discuss this a bit more in depth when we talk about subnetting and subnet masks.

We need an IP address to uniquely identify each network device on the network. An IP address is just like a phone number (I'm talking about regular phone numbers, no cell phones). Everyone in a city who has a phone at home has a unique phone number where you can reach them.

An IP address is 32-bit and consists of 2 parts,

the network part and the host part

The IP address is 32-bit but we write it down in 4 blocks of 8 bits. 8 bits is what we call a "byte" or "Octet". So the IP address will look like this . How many Network octet and How many hosts octet we Learn That's later !! Now Just an Example !!



The network part will tell us to which "network" the IP address will belong, you can compare this to the city or area code of a phone number. The "host" part uniquely identifies the network device; these are like the last digits of your phone number.

- The following computers will be in the same network: As you can see their "network" part is the same

192.168.1.1
192.168.1.2
192.168.1.3

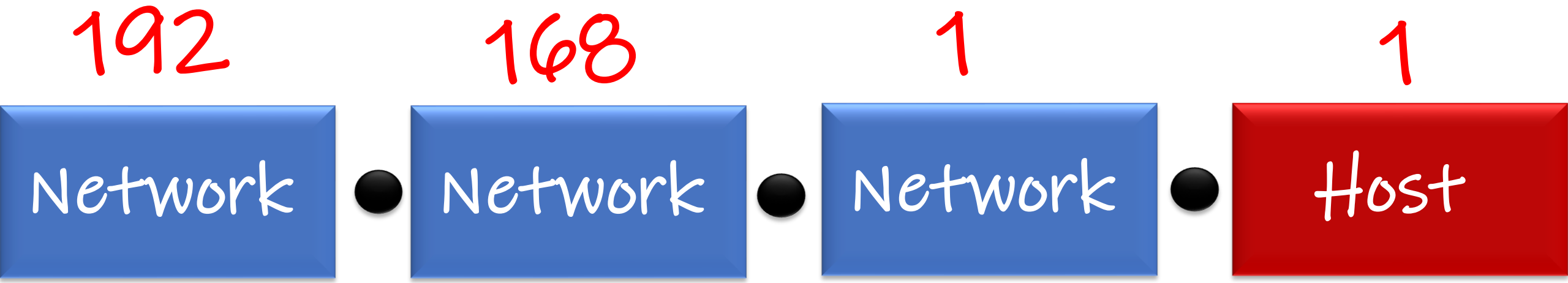
- A computer with "192.168.2.1" is not in the same network since it's "network" part is different, it's 192.168.2.X compared to 192.168.1.X

- What do you think your computer will do when it wants to send an IP packet to another network ??!

Take a look at this IP address which you might have seen before since it's a common IP address on local area networks:

192.168.1.1

For this IP address the first 3 bytes are the "network" address and the last byte is the "host"

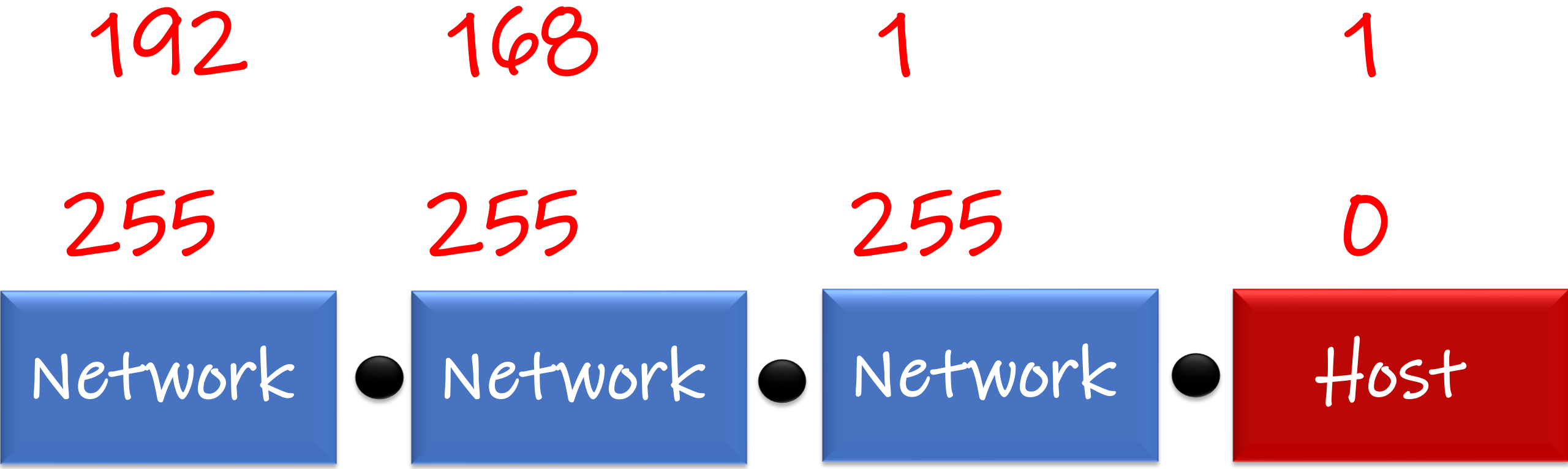


Ok awesome…but why are the first 3 bytes the "network" part and why is the last byte the "host" part?

Good question! I only gave you the IP address but you might remember that if you configure an IP address you also have to specify the subnet mask. Our IP address 192.168.1.1 would come along with the subnet mask 255.255.255.0.

The subnet mask tells your computer which part is the "network" part and which part is the "host" part.

Despite the name it does not "hide" or "mask" anything. We'll talk about binary and subnetting calculations later on, for now just hold the thought that your subnet mask tells us which part of the IP address is the "network" part and which part is for "hosts".

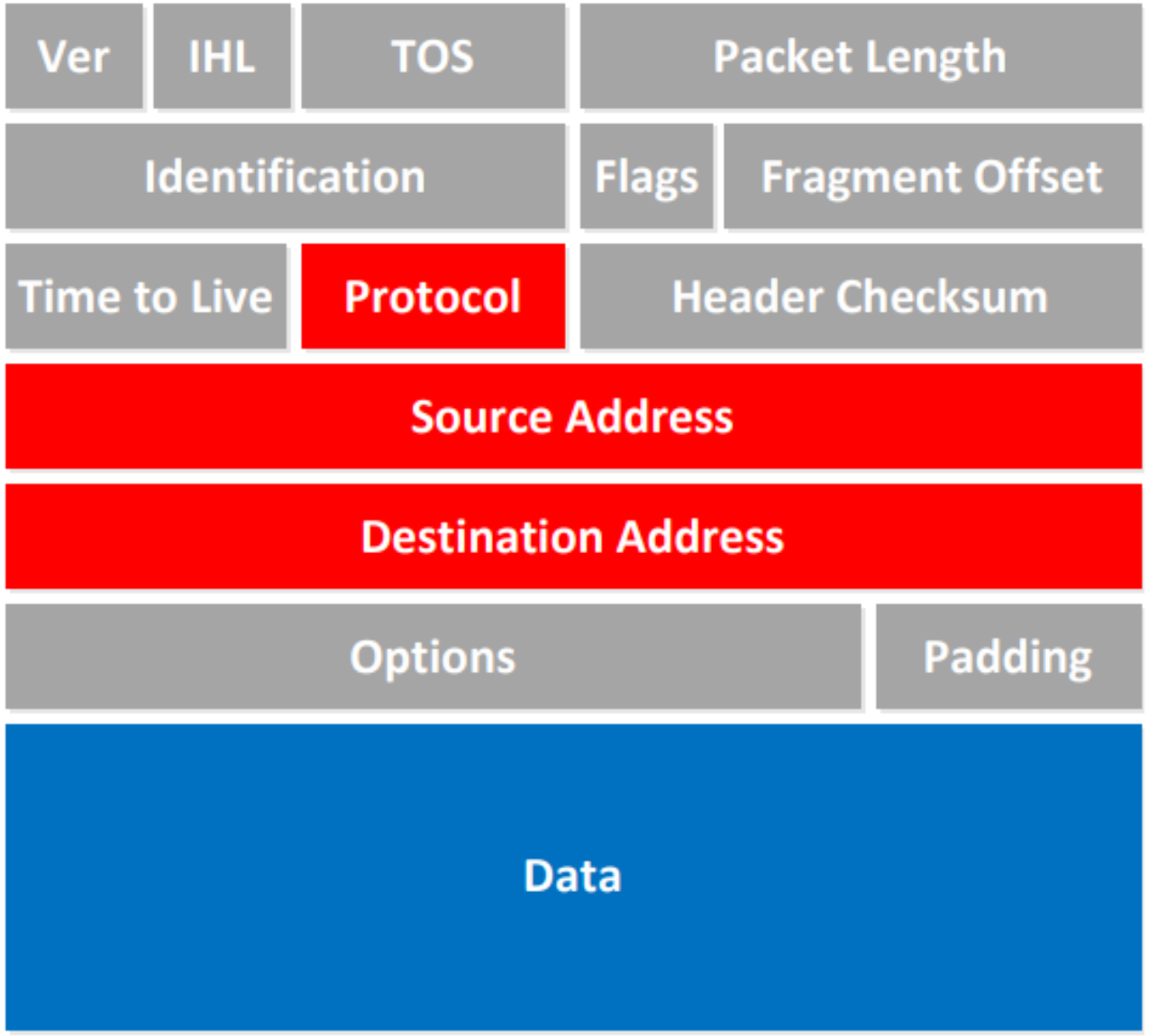


255 means That the part of IP is Network Part

0 means That the part of IP is Host Part

Let's take a look at an actual IP packet:

There are a lot of fields there! Now don't go look over them and feel puzzled that you have no idea what they are about. For now there are only a few fields that are interesting to us. The fields we don't care about are in Gray, I want to focus on the red and blue fields.



- **Protocol**: Here you will find which protocol we are using on top of IP, this is how we specify which transport layer protocol we are using. So you'll find TCP, UDP or perhaps something else in here.

- **Source Address**: Here you will find the IP address of the device that created this IP packet.

- **Destination Address**: This is the IP address of the device that should receive the IP packet

- **Data**: this is the actual data that we are trying to get to the other side.

Let's take another look at an IP address

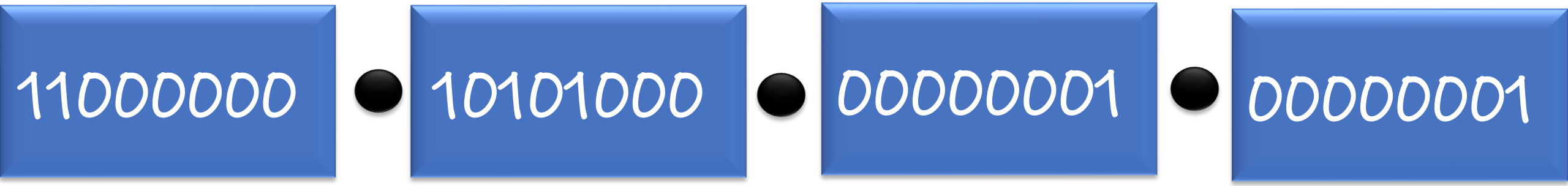
We Will Take this IP address for Example :- **192.168.1.1**

What do we know about this IP address?

- First of all we know it's a 32-bit value, so in binary it will look like this:

11000000101010000000000100000001

Now this is a number that is not very human-friendly so to make our life easier we can at least put this number into "blocks" of 8 bits separated with dot notation. 8 bits is also called a byte or an octet.



Now we can convert each byte into decimal, let's take each block and convert it from binary to decimal using the following table:

Bits	128	64	32	16	8	4	2	1
	0	0	0	0	0	0	0	0

First block:

11000000

Bits	128	64	32	16	8	4	2	1
	1	1	0	0	0	0	0	0

First Octet = 128 + 64 = 192

Second block:

10101000

Bits	128	64	32	16	8	4	2	1
	1	0	1	0	1	0	0	0

Second Octet = 128 + 32 + 8 = 168

Third block:

00000001

Bits	128	64	32	16	8	4	2	1
	0	0	0	0	0	0	0	1

Third Octet = 1

Fourth block:

00000001

Bits	128	64	32	16	8	4	2	1
	0	0	0	0	0	0	0	1

Fourth Octet = 1

Excellent so now you know why IP addresses look like this and why we write them down like this, we even did some basic binary to decimal calculations. One last thing to look at and that's the different classes that we have for networks. Maybe you have heard of class A,B or C networks before. Our IP address that we just used (192.168.1.1) is an example of a class C network.

We have 5 different classes but we work with first :

- ✓ Class A
- ✓ Class B
- ✓ Class C
- X Class D
- X Class E

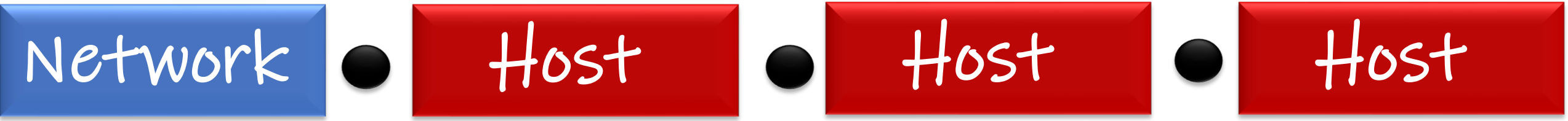
So what's the difference between them?

The difference between them is how many hosts you can fit in each network.

let me start off by showing you the difference between the classes

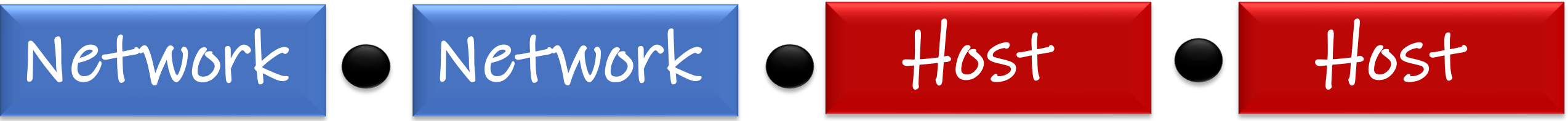
Class A

If you use a class A network you can have a LOT of hosts in each network that you create.



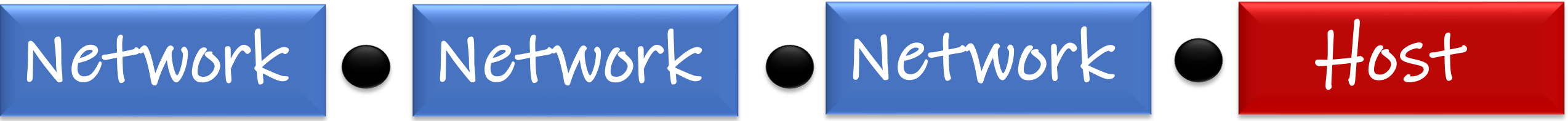
Class B

If you use a class B you can build more networks, but fewer hosts per network.



Class C

and with class C you can build a LOT of networks but only with a few hosts in each network.

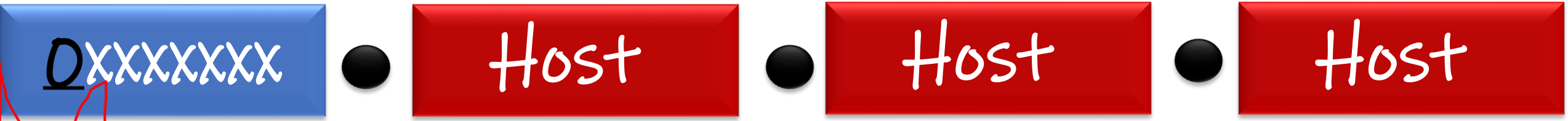


Now If I told you this IP "192.168.1.1" is a class "C" Network

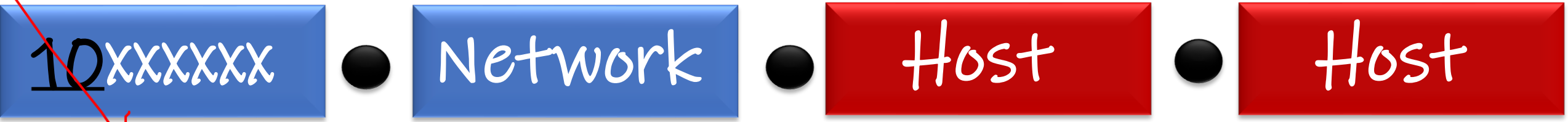
How do I know this?

It's because the first bits are "fixed" for the different classes, let me show you this:

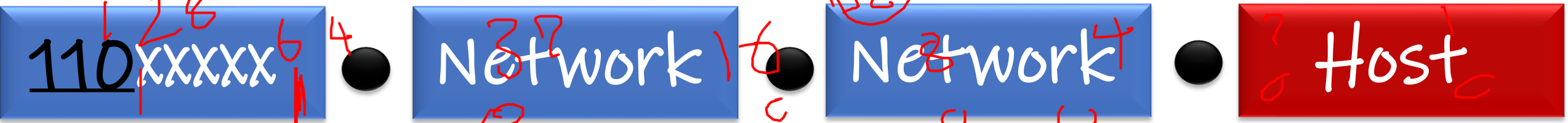
Class A The first bit always has to be 0



Class B The first 2 bits always have to be 10



Class C The first 3 bits always have to be 110



So if you calculate this from binary to decimal you'll get the following ranges:

- ✓ Class A starts at 0.0.0.0
- ✓ Class B starts at 128.0.0.0
- ✓ Class C starts at 192.0.0.0

So what are the exact ranges that we have?

- ✓ Class A: 0.0.0.0 – 126.255.255.255
- ✓ Class B: 128.0.0.0 – 191.255.255.255
- ✓ Class C: 192.0.0.0 – 223.255.255.255

Hmm now this raises 2 questions:

- If you look closely, do you see a 127.0.0.0 subnet? It's not in the class A range so what happened to it?
- Why does Class C stop at 223.255.255.255?

To answer the first question:- Go to your command prompt of your computer and type in "ping 127.0.0.1" and you'll get a response. This network range is being used as "loopback". Your loopback interface is something to check if your IP stack is OK.

To answer the second question:- I have to tell you that there's actually a class D range, we don't use those IP addresses to assign to computers but it's being used for "multicast". We'll get back to multicast later in the course; it starts with the 224.0.0.0 range.

The last thing I need to tell you about classes is the difference between "private" and "public" IP addresses.

- Public IP addresses are used on the Internet.
- Private IP addresses are used on your local area network and should not be used on the Internet.

These are the Private IP address ranges:

- ✓ Class A: 10.0.0.0 – 10.255.255.255
- ✓ Class B: 172.16.0.0 – 172.31.255.255
- ✓ Class C: 192.168.0.0 – 192.168.255.255

Is there anything else we need to know about IP addresses?!

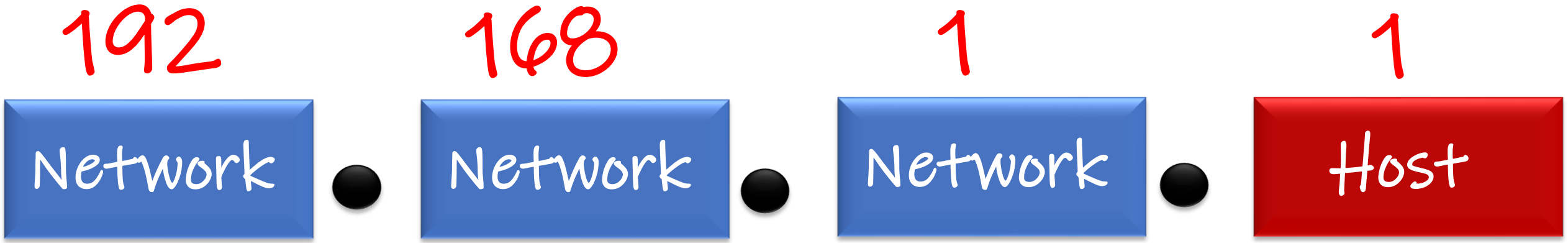
Well yes, one last thing! There are 2 IP addresses we cannot use on our network.

- ✓ Network Address
- ✓ Broadcast Address

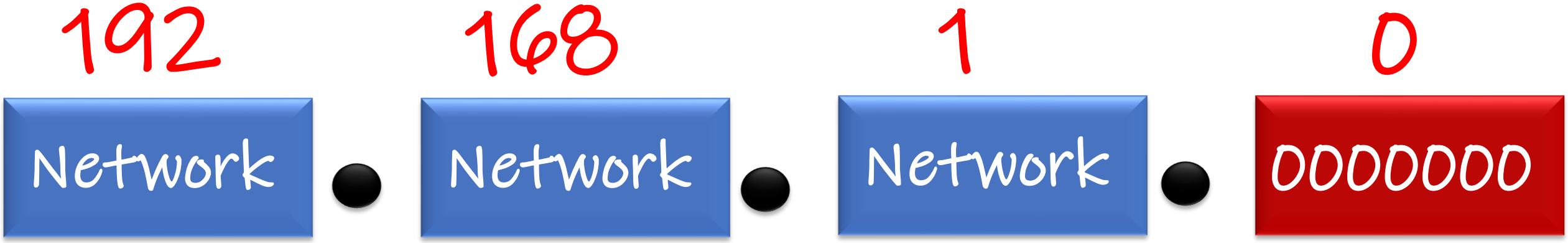
- The network address cannot be used on a computer as an IP address because it's being used to "define" the network. Routers will use the network address as you will discover later in the book.

- The broadcast address cannot be used on a computer as an IP address because it's used by broadcast applications. A broadcast is an IP packet that will be received by all devices in your network.

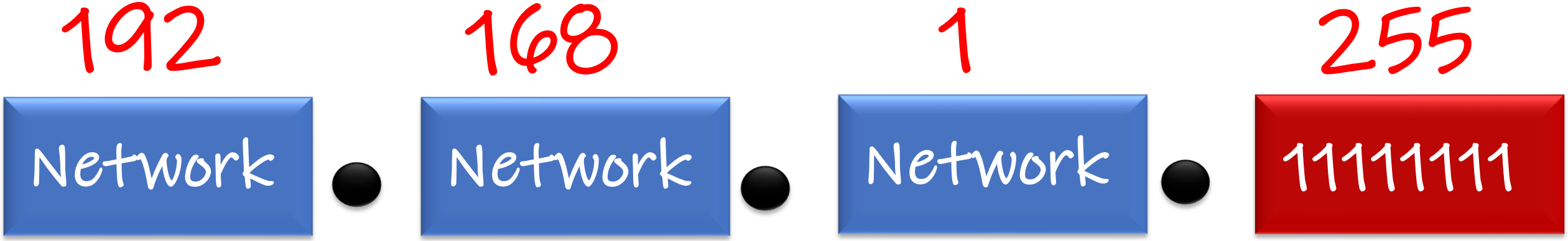
So how do we recognize these two IP addresses that we cannot use? Let me give you an example for this: Let's use the Class C range and our IP address 192.168.1.1.



We need to look at the last octet which is being used for hosts. If we set all the bits to 0 in our "host" part then we have the network address:



If we set all the bits to 1 we'll have a broadcast IP address and we also cannot use this for computers.



So in summary:

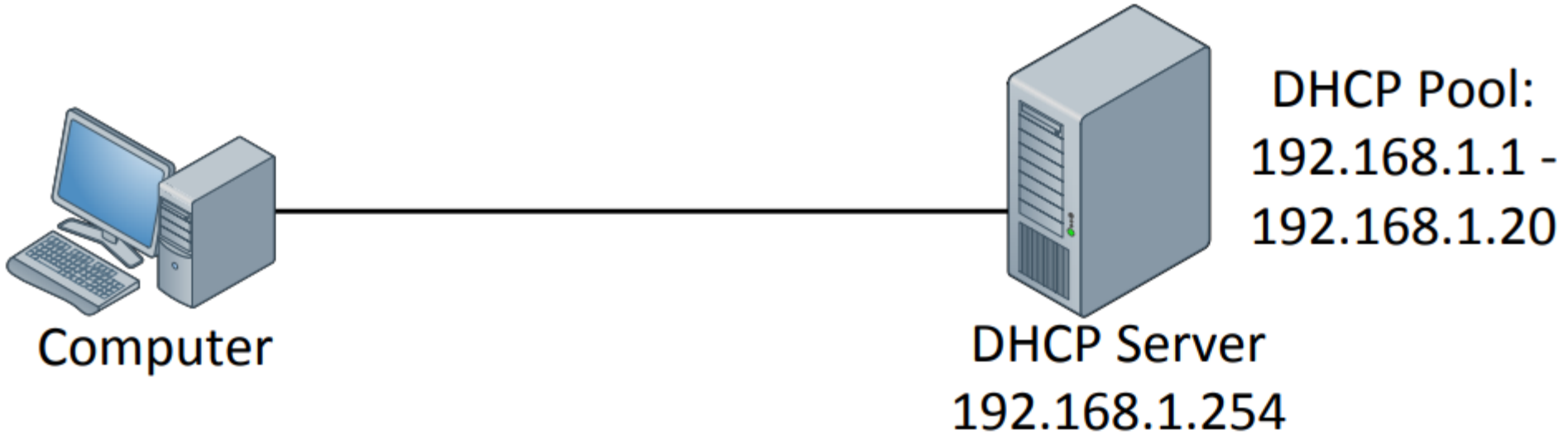
- Set all the host bits to 0 gives you the network address.
- Set all the host bits to 1 gives you the broadcast address.
- These 2 IP addresses we cannot use for computers.

How I can configure The IP address in my device ?

IP addresses can be configured **statically** or **dynamically**.

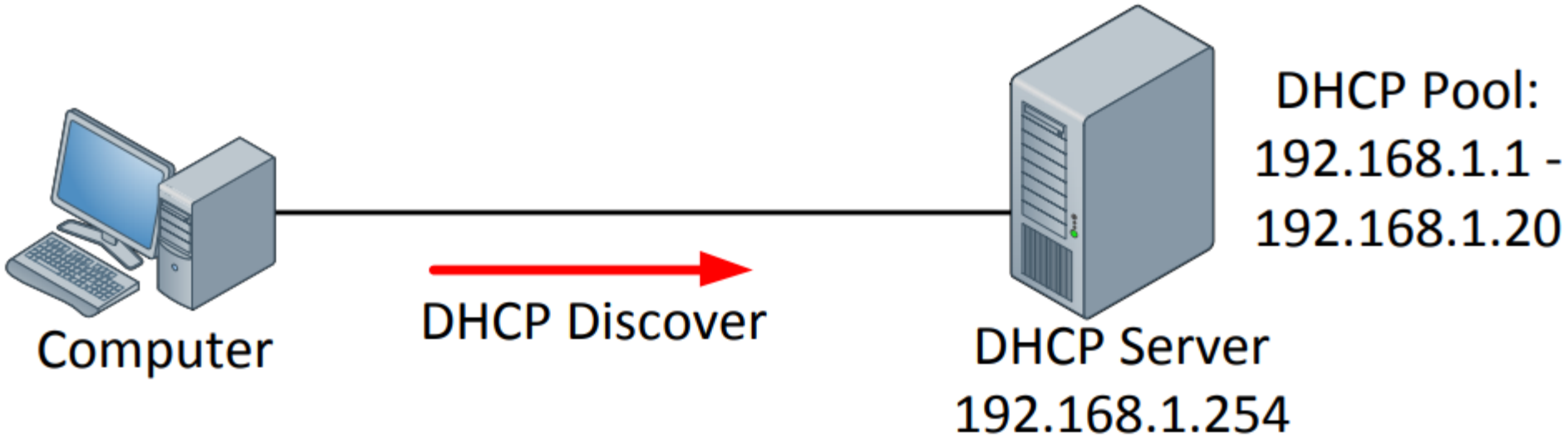
- If you go the static way you have to **configure the IP address yourself** on your computer, router or switch.
- Dynamic means **we use DHCP (Dynamic Host Configuration Protocol).**
- **DHCP is a server process** that assigns IP addresses from a "pool" to network devices
- A cisco router can be used as a DHCP server but you will also see this often on Microsoft or Linux servers.

How DHCP Works?



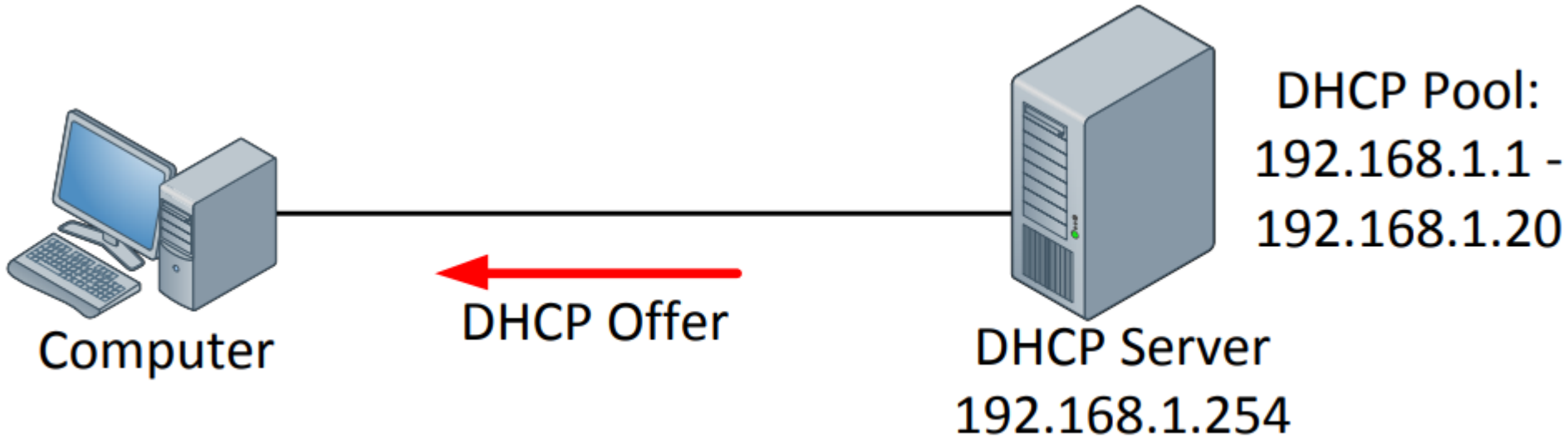
- On the left side we see a computer without an IP address
- On the right side is a DHCP server with IP address 192.168.1.254.
- "A DHCP pool" has been configured with IP address 192.168.1.1 – 192.168.1.20.

- Once the computer boots it will request an IP address by broadcasting a "DHCP discover message"

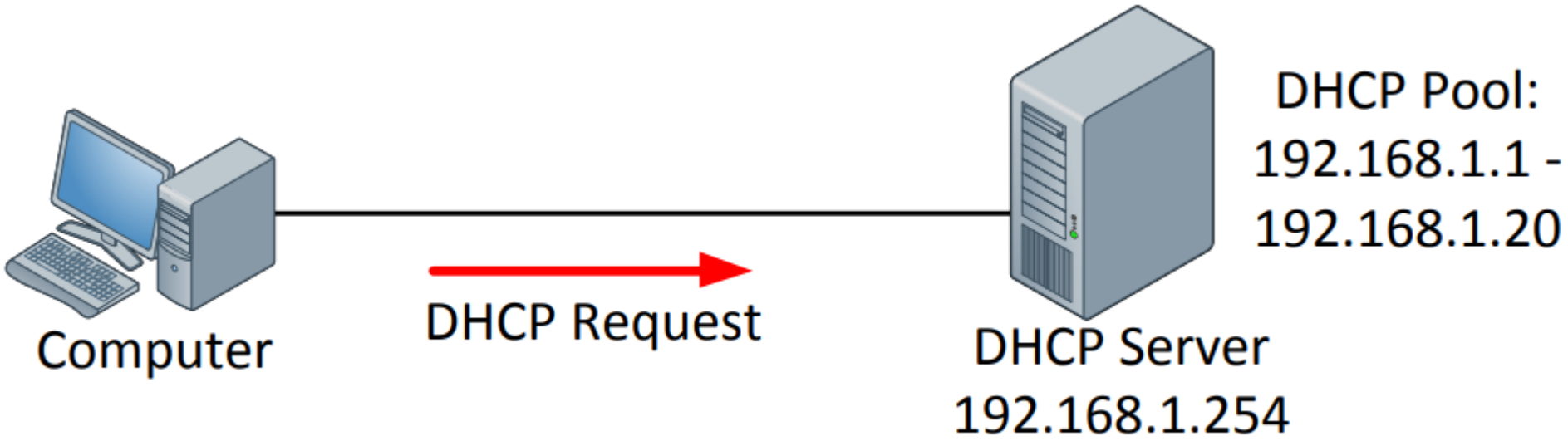


- The DHCP server will send a "DHCP offer message" which contains the IP address that the computer can use.

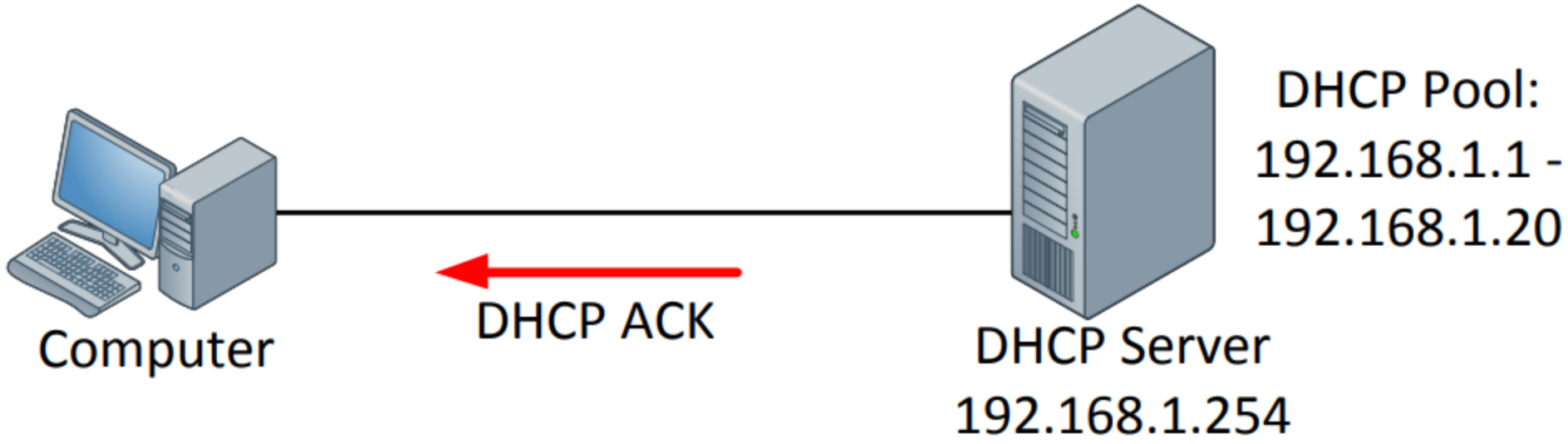
- Besides giving an IP address we can also supply a default gateway, a DNS server IP address and some other options.



- After receiving the DHCP offer our computer will send a "DHCP request" to ask if it's OK to use this information…



- And the final step in this process will be a "DHCP ACK" from the DHCP server to "acknowledge" the request from the computer.



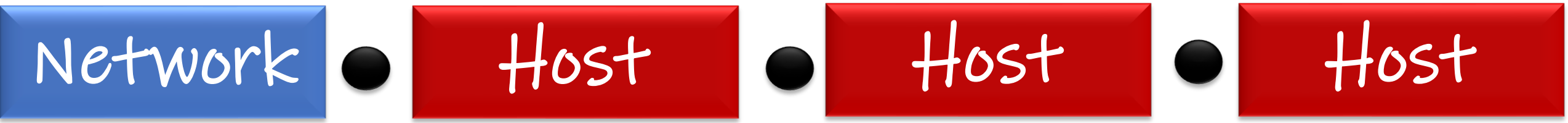
CIDR & Prefix Length (IPv4)

The Old Way: Classful Addressing

- In the beginning, the line between network and host was rigidly defined by **"classes."**
- Based on the very first number in the IP address,
- you immediately knew the size of the network.
- This was simple but incredibly **inflexible**.

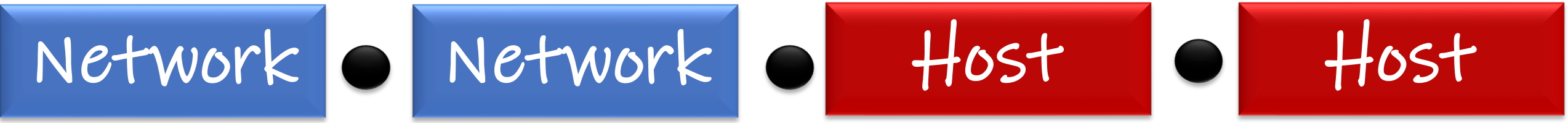
Class A

If you use a class A network you can have a LOT of hosts in each network that you create.



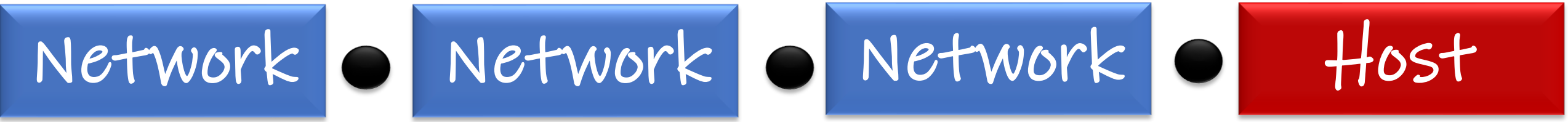
Class B

If you use a class B you can build more networks, but fewer hosts per network.



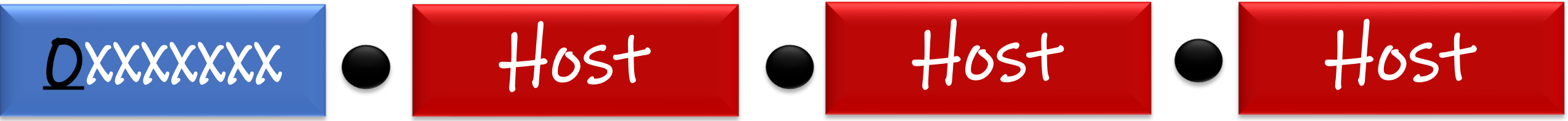
Class C

and with class C you can build a LOT of networks but only with a few hosts in each network.

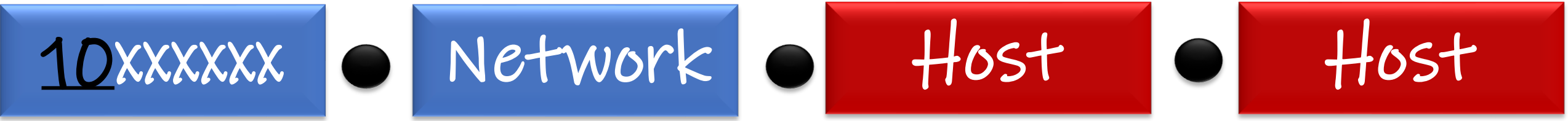


the first bits are "fixed" for the different classes, let me show you this:

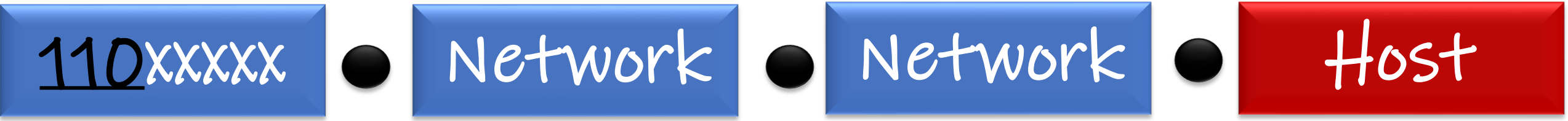
Class A The first bit always has to be 0



Class B The first 2 bits always have to be 10



Class C The first 3 bits always have to be 110



So if you calculate this from binary to decimal you'll get the following ranges:

- ✓ Class A starts at 1.0.0.0
- ✓ Class B starts at 128.0.0.0
- ✓ Class C starts at 192.0.0.0

So what are the exact ranges that we have?

- ✓ Class A: 1.0.0.0 – 126.255.255.255
- ✓ Class B: 128.0.0.0 – 191.255.255.255
- ✓ Class C: 192.0.0.0 – 223.255.255.255

The Problem of Waste

- The rigid nature of classful addressing led to immense IP address waste.

- Imagine you need a network for 500 devices. What would you do?

1. Try Class C: It provides 254 usable host addresses. Not enough.

2. You're forced to use Class B: It provides 65,534 usable host addresses. You use 500 and waste over 65,000 addresses.

3. This inefficiency was unsustainable for the growing internet and a new, more flexible system was needed.

The New Way: CIDR & Prefix Length

- Classless Inter-Domain Routing (CIDR) replaced rigid classes with a simple concept: "Prefix Length".
- It's a number after a slash (e.g., /24) that tells you exactly how many bits are for the network.
- This allows you to create networks of any size you need.

Remember that

An IP address is 32-bit and consists of 2 parts,

the network part and the host part

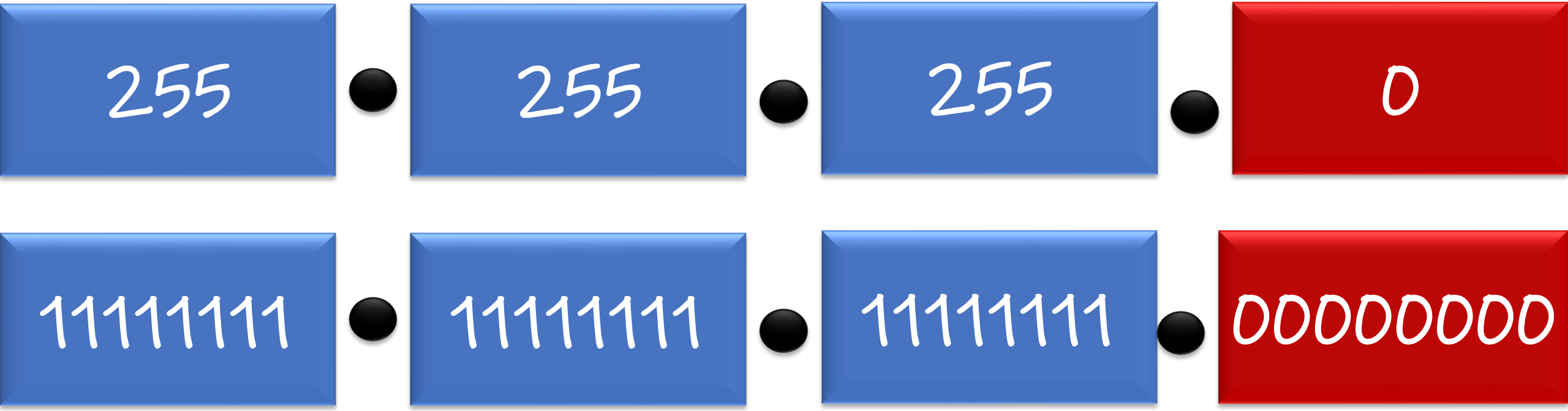
The subnet mask show you what is the network part an what is the host part

192	168	1	1
255	255	255	0
Network	Network	Network	Host

255 means That the part of IP is Network Part

0 means That the part of IP is Host Part

Let's Talk The subnet mask in Binary View



1 bit means this a network bit so her we have 24 networks bits

0 means this a host bit so her we have 8 hosts bits

Prefix Length

The **Prefix Length** is the number of bits used to represent the **network portion** of an IP address.

IP Format in Prefix Length

For example,

192.168.10.5/24

This is means we have a 24 bits in a network portion = in subnet mask the first 24 bits is 1s = we have an 8 bits in host portion (32 bits – 24 bits = 8 bits)

Calculations we can do using IP Format in Prefix Length

- ✓The number of bits in IP host portion (N) (N =Prefix Length)
- ✓The number of bits in IP host portion (H) (H =32 – Prefix Length)
- ✓Subnet mask in decimal format
- ✓The number of hosts we can get in a given IP ($2^H - 2$)

When calculating usable IPs, we subtract 2: one for the Network ID and one for the Broadcast address.

Practice Problems

Problem 1

How many usable hosts are available in the network 192.168.50.0/26?

Solution

- ✓ Total bits in IPv4 is 32 bits.
- ✓ Given prefix length is 26 .
- ✓ Number of host bits (H) = 32 - 26 = 6 bits
- ✓ Number of usable hosts = 2^6 - 2 = 64 - 2 = 62 hosts

Practice Problems

Problem 2

If you have a network 10.0.0.0/10, how many hosts are available?

Solution

- ✓ Total bits in IPv4 is 32 bits.
- ✓ Given prefix length is 10 .
- ✓ Number of host bits (H) = 32 - 10 = 22 bits
- ✓ Number of usable hosts = 2^{22} - 2 = 4,194,304 - 2 = 4,194,302 hosts

Practice Problems

Problem 3

How many usable hosts are available in a subnet with a mask of 255.255.255.240?

Solution

- ✓ To convert the subnet mask to a prefix length, convert each octet to binary and count the consecutive 1s.
- ✓ 255.255.255.240 in binary is: 11111111.11111111.11111111.11110000.
- ✓ The number of consecutive 1s (prefix length) is 28.
- ✓ Number of host bits (H) = 32 - 28 = 4 bits.
- ✓ Number of usable hosts = 2^4 - 2 = 16 - 2 = 14 hosts

Practice Problems

In The Last Problem

How many usable hosts are available in a subnet with a mask of 255.255.255.240?

Solution

- ✓ To convert the subnet mask to a prefix length, convert each octet to binary and count the consecutive 0s.
- ✓ 255.255.255.240 in binary is: 11111111.11111111.11111111.11110000.
- ✓ The number of consecutive 0s (Hosts bits) is 4.
- ✓ Number of host bits (H) = . The number of consecutive 0s = 4
- ✓ Number of usable hosts = $2^4 - 2 = 16 - 2 = 14$ hosts

Tray To Solve

Problem 4

How many usable hosts are available in the network 172.16.0.0/20?

Problem 5

How many usable hosts are available in a subnet with a mask of 255.255.254.0?

IP Subnetting Part 1 (IPv4)

What we will Learn in this Part ?

In this section, I will provide you with an IP address, and based on that, you will be asked to identify the following:

- ✓ What is the **Network ID** (Subnet Address)?
- ✓ What is the **Subnet Mask / CIDR Notation?**
- ✓ What is the **Broadcast Address?**
- ✓ What is the **First Usable IP Address?**
- ✓ What is the **Last Usable IP Address?**
- ✓ What is the **Number of Usable IPs in this Subnet?**
- ✓ What is the **Hop Count (Block size)** in this Subnet? (optional, since it's similar to usable IPs)
- ✓ What is the **Next Network Address?**

How we can get it

If you're given an IP address in CIDR notation (e.g. /26), follow these steps to calculate all subnet-related information:

- ✓ Convert the CIDR (Prefix Length) into a Subnet Mask
- ✓ Determine the Number of Host Bits (H) (H = 32 – Prefix Length)
- ✓ To Get the Hop count (Block size) :Hop Count = 2^H
- ✓ To Get the Number of Usable IPs: $2^H - 2$
- ✓ Convert the Subnet Mask into Binary Format (💡 *Trick:* Only convert the octet(s) that are less than 255.)
- ✓ Convert the IP into Binary Format (💡 *Trick:* You only need to convert the octet(s) that contain both network and host bits (i.e. not fully 255 or 0 in the subnet mask).
- ✓ Identify the Network Part and Host Part in the given IP (in mask , 1s = Networks , 0s = Hosts)
- ✓ To Get the Network ID (Subnet Address): Replace all host bits in the IP with zeros.
- ✓ To Get the Broadcast Address: Replace all host bits in the IP with ones.
- ✓ To Get the First Valid IP Address: Replace all host bits with zeros except the first bit = 1, (💡 Or simply: Network ID + 1)
- ✓ To Get the Last Valid IP Address: Replace all host bits with ones except the last bit = 0, (💡 Or simply: Broadcast Address – 1)
- ✓ To Get the Next Network Address: Network ID + Hop count (💡 Broadcast Address + 1)

Practice Problems

Problem 1

Given: 192.168.1.100/26

Find →

- Subnet Mask
- Network ID
- Broadcast Address
- First Usable IP
- Last Usable IP
- Number of Usable IPs
- Next Network
- Hop Count

Solution Problem 1

1. Prefix = 26 that's means we have 26 ones in sub netmask
2. The the Number of Host Bits (H) = 32-26 = 6 bits
3. To Get the Hop count (Block size) : $2^H = 2^6 = 64$
4. Number of Usable IPs: $2^6 - 2 = 64 - 2 = 62$
5. The subnet mask :

11111111	11111111	11111111	11000000

in decimal Format

255	255	255	192

Solution Problem 1 … cont.

6. Identify the Network Part and Host Part in the given IP

192	168	1	01100100
255	255	255	11000000

Network Part | Host Part

Solution Problem 1 … cont.

7. To Get the **Network ID** (Subnet Address): Replace all host bits in the IP with zerosa

192	168	1	01000000

in decimal Format

192	168	1	64

Solution Problem 1 … cont.

8. To Get the **Broadcast Address**: Replace all host bits in the IP with ones.

192	168	1	01111111

in decimal Format

192	168	1	127

Solution Problem 1 … cont.

9. To Get the **First Valid IP Address**: Replace all host bits with zeros except the first bit = 1, (💡 Or simply: Network ID + 1)

192	168	1	01000001

in decimal Format

192	168	1	65

Solution Problem 1 … cont.

10. To Get the **Last Valid IP Address**: Replace all host bits with ones except the last bit = 0, (💡 Or simply: Broadcast Address – 1)

192	168	1	01111110

in decimal Format

192	168	1	126

Solution Problem 1 … cont.

11. To Get the **Next Network Address**: Network ID + Hop count

(💡 Broadcast Address + 1)

192	168	1	64+64

OR

192	168	1	127+1

=

192	168	1	128

Solution Problem 1 … cont.

Solution: Problem 1

- ✅ Subnet Mask: 255.255.255.192
- ✅ Host bits: 6
- ✅ Network ID = 192.168.1.64
- ✅ Broadcast = 192.168.1.127
- ✅ First Usable IP = 192.168.1.65
- ✅ Last Usable IP = 192.168.1.126
- ✅ Number of all Usable IPs = 62
- ✅ Next Network = 192.168.1.128
- ✅ Hop Count = 64

Practice Problems

Problem 2

Given: 10.0.0.25/30

Find →

- Subnet Mask
- Network ID
- Broadcast Address
- First Usable IP
- Last Usable IP
- Number of Usable IPs
- Next Network
- Hop Count

Solution Problem 2

1. Prefix = 30 that's means we have 30 ones in sub netmask
2. The the Number of Host Bits (H) = 32-30 = 2 bits
3. To Get the Hop count (Block size) : $2^H = 2^2 = 4$
4. Number of Usable IPs: $2^2 - 2 = 4 - 2 = 2$
5. The subnet mask :

11111111	11111111	11111111	11111100

in decimal Format

255	255	255	252

Solution Problem 2 … cont.

6. Identify the Network Part and Host Part in the given IP

10	0	0	000110 | 01
255	255	255	111111 | 00
Network Part			Host Part

Solution Problem 2 … cont.

7. To Get the **Network ID** (Subnet Address): Replace all host bits in the IP with zeros

10	0	0	00011000

in decimal Format

10	0	0	24

Solution Problem 2 … cont.

8. To Get the **Broadcast Address**: Replace all host bits in the IP with ones.

10	0	0	00011011

in decimal Format

10	0	0	27

Solution Problem 2 … cont.

9. To Get the **First Valid IP Address**: Replace all host bits with zeros except the first bit = 1, (💡 Or simply: Network ID + 1)

10	0	0	00011001

in decimal Format

10	0	0	25

Solution Problem 2 … cont.

10. To Get the **Last Valid IP Address**: Replace all host bits with ones except the last bit = 0, (💡 Or simply: Broadcast Address – 1)

10	0	0	00011010

in decimal Format

10	0	0	26

Solution Problem 2 … cont.

11. To Get the **Next Network Address**: Network ID + Hop count

(💡 Broadcast Address + 1)

10	0	0	24+4

OR

10	0	0	27+1

=

10	0	0	28

Solution Problem 2 … cont.

Solution: Problem 2

- ✅ Subnet Mask: 255.255.255.252
- ✅ Host bits: 2
- ✅ Network ID = 10.0.0.24
- ✅ Broadcast = 10.0.0.27
- ✅ First Usable IP = 10.0.0.25
- ✅ Last Usable IP = 10.0.0.26
- ✅ Number of all Usable IPs = 2
- ✅ Next Network = 10.0.0.28
- ✅ Hop Count = 4

Practice Problems

Problem 3

Given: 172.16.5.200/27

Find →

- Subnet Mask
- Network ID
- Broadcast Address
- First Usable IP
- Last Usable IP
- Number of Usable IPs
- Next Network
- Hop Count

Solution Problem 3

1. Prefix = 27 that's means we have 27 ones in sub netmask
2. The the Number of Host Bits (H) = 32-27 = 5 bits
3. To Get the Hop count (Block size) : $2^H = 2^5 = 32$
4. Number of Usable IPs: $2^5 - 2 = 32 - 2 = 30$
5. The subnet mask :

11111111	11111111	11111111	11100000

in decimal Format

255	255	255	224

Solution Problem 3 … cont.

6. Identify the Network Part and Host Part in the given IP

172	16	5	110 01000
255	255	255	111 00000

Network Part

Host Part

Solution Problem 3 … cont.

7. To Get the **Network ID** (Subnet Address): Replace all host bits in the IP with zeros

172	16	5	11000000

in decimal Format

172	16	5	192

Solution Problem 3 … cont.

8. To Get the **Broadcast Address**: Replace all host bits in the IP with ones.

172	16	5	110**11111**

in decimal Format

172	16	5	223

Solution Problem 3 … cont.

9. To Get the **First Valid IP Address**: Replace all host bits with zeros except the first bit = 1, (💡 Or simply: Network ID + 1)

172	16	5	11000001

in decimal Format

172	16	5	193

Solution Problem 3 … cont.

10. To Get the **Last Valid IP Address**: Replace all host bits with ones except the last bit = 0, (💡 Or simply: Broadcast Address – 1)

172	16	5	110111110

in decimal Format

172	16	5	222

Solution Problem 3 … cont.

11. To Get the **Next Network Address**: Network ID + Hop count
(💡 Broadcast Address + 1)

172	16	5	192+32

OR

172	16	5	223+1

=

172	16	5	224

Solution Problem 3 … cont.

Solution: Problem 3

- ✅ Subnet Mask: 255.255.255.224
- ✅ Host bits: 32
- ✅ Network ID = 172.16.5.192
- ✅ Broadcast = 172.16.5.223
- ✅ First Usable IP = 172.16.5.193
- ✅ Last Usable IP = 172.16.5.222
- ✅ Number of all Usable IPs = 30
- ✅ Next Network = 172.16.5.224
- ✅ Hop Count = 32

Practice Problems

Problem 4

Given: 192.168.10.200/17

Find →

- Subnet Mask
- Network ID
- Broadcast Address
- First Usable IP
- Last Usable IP
- Number of Usable IPs
- Next Network
- Hop Count

Solution Problem 4

1. Prefix =17that's means we have 17 ones in sub netmask
2. The the Number of Host Bits (H) = 32-17 = 15 bits
3. To Get the Hop count (Block size) : $2^{15} = 32768$
4. Number of Usable IPs: $2^{15} - 2 = 32768 - 2 = 32766$
5. The subnet mask :

11111111	11111111	10000000	00000000

in decimal Format

255	255	128	0

Solution Problem 4 … cont.

6. Identify the Network Part and Host Part in the given IP

192	168	0	0001010	11001000
255	255	1	0000000	00000000

Network Part

Host Part

Solution Problem 4 … cont.

7. To Get the **Network ID** (Subnet Address): Replace all host bits in the IP with zeros

192	168	00000000	00000000

in decimal Format

192	168	0	0

Solution Problem 4 … cont.

8. To Get the **Broadcast Address**: Replace all host bits in the IP with ones.

192	168	01111111	11111111

in decimal Format

192	168	127	255

Solution Problem 4 … cont.

9. To Get the **First Valid IP Address**: Replace all host bits with zeros except the first bit = 1, (💡 Or simply: Network ID + 1)

192	168	00000000	00000001

in decimal Format

192	168	0	1

Solution Problem 4 … cont.

10. To Get the **Last Valid IP Address**: Replace all host bits with ones except the last bit = 0, (💡 Or simply: Broadcast Address – 1)

192	168	01111111	11111110

in decimal Format

192	168	127	254

Solution Problem 4 … cont.

11. To Get the **Next Network Address**: Network ID + Hop count

(💡 Broadcast Address + 1)

192	168	127	255+1

=

192	168	128	0

Solution Problem 4 … cont.

Solution: Problem 4

- ✅ Subnet Mask: 255.255.128.0
- ✅ Host bits: 15
- ✅ Network ID = 192.168.0.0
- ✅ Broadcast = 192.168.127.255
- ✅ First Usable IP = 192.168.0.1
- ✅ Last Usable IP = 192.168.127.254
- ✅ Number of all Usable IPs = 32,766
- ✅ Next Network = 192.168.128.0
- ✅ Hop Count = 32,768

Practice Problems

Problem 5

Given: 10.0.0.5/9

Find →

- Subnet Mask
- Network ID
- Broadcast Address
- First Usable IP
- Last Usable IP
- Number of Usable IPs
- Next Network
- Hop Count

Solution Problem 5

1. Prefix =9 that's means we have 9 ones in sub netmask
2. The the Number of Host Bits (H) = 32 - 9 = 23 bits
3. To Get the Hop count (Block size) : $2^{23} = 8388608$
4. Number of Usable IPs: $2^{23} - 2 = 8388608 - 2 = 8388606$
5. The subnet mask :

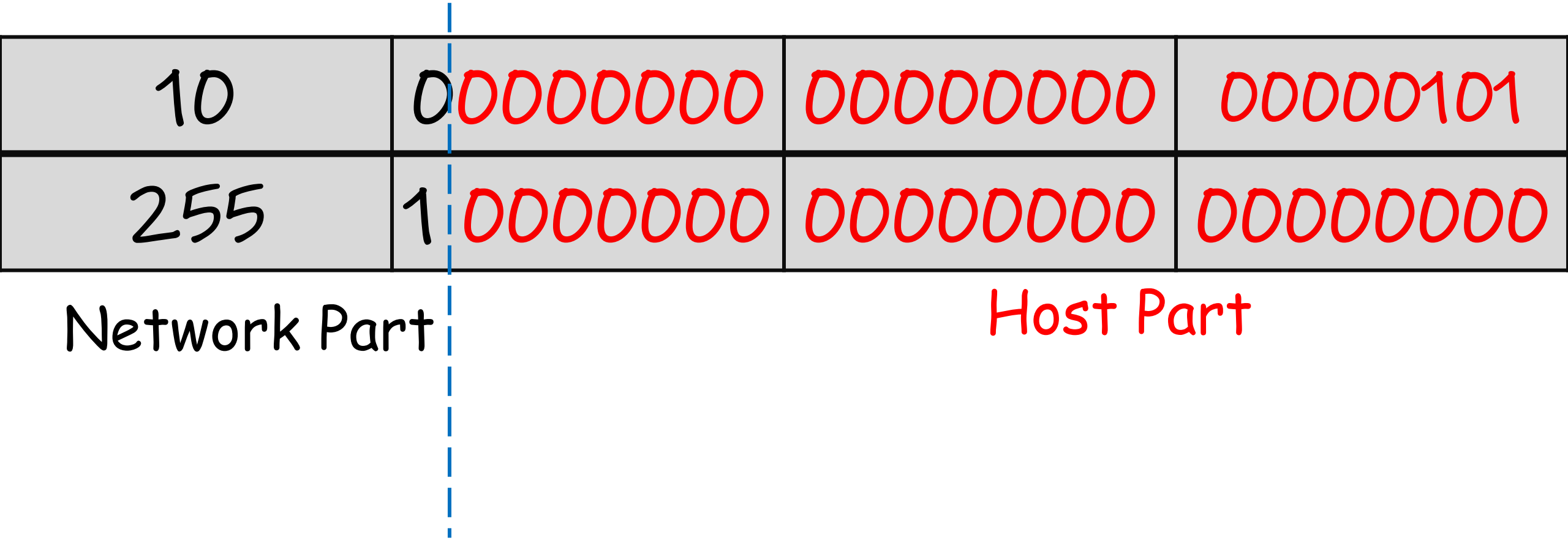
11111111	10000000	00000000	00000000

in decimal Format

255	128	0	0

Solution Problem 5 … cont.

6. Identify the Network Part and Host Part in the given IP



Solution Problem 5 … cont.

7. To Get the **Network ID** (Subnet Address): Replace all host bits in the IP with zeros

10	0000000	00000000	00000000

in decimal Format

10	0	0	0

Solution Problem 5 … cont.

8. To Get the **Broadcast Address**: Replace all host bits in the IP with ones.

10	01111111	11111111	11111111

in decimal Format

10	127	255	255

Solution Problem 5 … cont.

9. To Get the **First Valid IP Address**: Replace all host bits with zeros except the first bit = 1, (💡 Or simply: Network ID + 1)

10	0DDDDDDD	DDDDDDDD	DDDDDDD1

in decimal Format

10	0	0	1

Solution Problem 4 … cont.

10. To Get the **Last Valid IP Address**: Replace all host bits with ones except the last bit = 0, (💡 Or simply: Broadcast Address – 1)

10	01111111	11111111	11111110

in decimal Format

10	127	255	254

Solution Problem 5 … cont.

11. To Get the **Next Network Address**: Network ID + Hop count
(💡 Broadcast Address + 1)

10	127	255	255+1

=

10	128	0	0

Solution Problem 5 … cont.

Solution: Problem 4

- ✅ Subnet Mask: 255.128.0.0
- ✅ Host bits: 23
- ✅ Network ID = 10.0.0.0
- ✅ Broadcast = 10.127.255.255
- ✅ First Usable IP = 10.0.0.1
- ✅ Last Usable IP = 10.127.255.254
- ✅ Number of all Usable IPs = 8,388,606
- ✅ Next Network = 10.128.0.0
- ✅ Hop Count = 8,388,608

Tray To Solve

Problem 1

Given: 192.168.200.55/19

Find →

- Subnet Mask
- Network ID
- Broadcast Address
- First Usable IP
- Last Usable IP
- Number of Usable IPs
- Next Network
- Hop Count

Tray To Solve… cont.

- Problem 2

Given: 10.20.15.100/12

Find →

- Subnet Mask
- Network ID
- Broadcast Address
- First Usable IP
- Last Usable IP
- Number of Usable IPs
- Next Network
- Hop Count

Solution Problem 1

- ✅ Subnet Mask: 255.255.224.0
- ✅ Host bits: 13
- ✅ Network ID = 192.168.192.0
- ✅ Broadcast = 192.168.223.255
- ✅ First Usable IP = 192.168.192.1
- ✅ Last Usable IP = 192.168.223.254
- ✅ Number of all Usable IPs = 8190
- ✅ Next Network = 192.168.224.0
- ✅ Hop Count = 8192

Solution Problem 2.

- ✅ Subnet Mask: 255.240.0.0
- ✅ Host bits: 20
- ✅ Network ID = 10.16.0.0
- ✅ Broadcast = 10.31.255.255
- ✅ First Usable IP = 10.16.0.1
- ✅ Last Usable IP = 10.31.255.254
- ✅ Number of all Usable IPs = 1,048,574
- ✅ Next Network = 10.32.0.0
- ✅ Hop Count = 1,048,576

Quiz

Given this Ips :

- 192.168.80.150/23
- 172.20.45.33/21
- 192.0.2.70/29
- 198.51.100.220/25
- 172.30.100.5/18

Find →

- Subnet Mask
- Network ID
- Broadcast Address
- First Usable IP
- Last Usable IP
- Number of Usable IPs
- Next Network
- Hop Count

IP Subnetting Part 2 (IPv4)

What we will Learn in this Part ?

- you'll learn how to Calculate the required subnet mask based on
  - The number of hosts needed
  - The number of subnets (Networks) required
- Solve 15 realistic subnetting Use Case Scenarios step-by-step
- By the end of this part, you'll be able to confidently design a subnetting plan based on different business needs.

What is the Demo Usage?

To understand subnetting practically, we will follow a structured calculation process and apply it to real-world demo scenarios.

🛠 Demo Usage:

In each scenario, **you'll be given:**

- 📌 A network address with a prefix (e.g. 192.168.1.0/24)
- 📌 A specific requirement:
  - ✅ Either number of Hosts needed
  - ✅ Or number of Subnets required

Then **You'll ask** for calculating :

- 📌 New Prefix Length
- 📌 Subnet Mask
- 📌 Number of Usable Hosts per Subnet
- 📌 Subnet Ranges (Network ID, First IP, Last IP, Broadcast)

What is the Calculation Steps

✅ **If the requirement is "Number of Hosts":**

- 📌 The Number of hosts before subntteing (H): 32 – prefix length
- 📌 Use formula: $2^n - 2 \geq Number\ of\ Hosts$
- 📌 Calculate n $(Number\ of\ bit\ Hosts)$
- 📌 Calculating the number of network bits we were borrow (N) = $H - n$
- 📌 The number of Subnets = 2^N
- 📌 New Prefix = $32 - n$
- 📌 Hope count (Block Size) : 2^n

✅ **If the requirement is "Number of Subnets":**

- 📌 Use formula: $2^N \geq Number\ of\ Subnets$
- 📌 Calculate N $(number\ of\ network\ bits\ to\ borrow)$
- 📌 New Prefix = $Original\ Prefix + N$
- 📌 Calculate n $(Number\ of\ Hosts\ after\ subnneting)$ = 32 - New Prefix
- 📌 Determine Subnet Mask and Subnet Ranges
- 📌 Hope count (Block Size) : 2^n

Practice Use cases

📌 Problem 1

💼 Tech Company Office Network

You're hired as a network engineer for a growing tech company. They just rented a new office space and want to split their network into 4 isolated departments :

- ✅ Development
- ✅ HR
- ✅ Sales
- ✅ Management

The company provides you with the network: 192.168.10.0/24They don't care how many hosts are in each; they just want 4 separate subnets.

Solution Problem 1

📌 A network address with a prefix : 192.168.10.0/24

📌 A requirement is :split the network into 4 isolated departments

📌 I will use this formula $2^N \geq Number\ of\ Subnets$: $2^N \geq 4$

📌 So N (number of network bits to borrow) = 2 because $2^2 = 4$ (4 is the number of subnets)

📌 New Prefix = $Original\ Prefix + N$: $24 + 2 = 26$

📌 Determine the Hosts bits after subnetting (n) = $32 - 26 = 6$

📌 Network Subnet mask : 255.255.255.192

📌 Hope count (Block Size) : $2^n = 2^6 = 64$

So

✅ Development Department ID is : 192.168.10.0/26
✅ Development HR ID is : 192.168.10.64/26
✅ Development Sales ID is : 192.168.10.128/26
✅ Development Management ID is : 192.168.10.192/26

Practice Use cases

📌 Problem 2

🏥 Clinic Floor Design

A private clinic has 3 floors. Each floor needs a subnet that can support at least 14 medical devices.

You are given the network: 192.168.20.0/24

Solution Problem 2

- A network address with a prefix : 192.168.20.0/24
- The Number of hosts before subntteing (H) $= 32 - \text{prefix length} = 32 - 24 = 8$
- A requirement is : Each subnet that can support at least 14 devices
- I will use this formula $2^n - 2 \geq Number\ of\ Hosts$: $2^n - 2 \geq 14$
- So $n\ (Number\ of\ bit\ Hosts)$ = 4 because $2^4 - 2 = 14$ (14 is the number of hosts in each subnet)
- Calculating the number of network bits we were borrow (N) = $H - n = 8 - 4 = 4$
- The number of Subnets = $2^N = 2^4 = 16$
- New Prefix = $32 - n$: $32 - 4 = 28$
- Network Subnet mask : 255.255.255.240
- Hope count (Block Size) : $2^n = 2^4 = 16$

So The subnets IPs are :

- ✅ 192.168.20.0 /28
- ✅ 192.168.20.16 /28
- ✅ 192.168.20.32 /28
- ✅ 192.168.20.48 /28
- ✅ 192.168.20.64 /28
- ✅ 192.168.20.80 /28
- ✅ 192.168.20.96 /28
- ✅ 192.168.20.112 /28
- ✅ 192.168.20.128 /28
- ✅ 192.168.20.144 /28
- ✅ 192.168.20.160 /28
- ✅ 192.168.20.176 /28
- ✅ 192.168.20.192 /28
- ✅ 192.168.20.208 /28
- ✅ 192.168.20.224 /28
- ✅ 192.168.20.240 /28

I have Just 3 floors so I need only 3 subnet to use

- ✅ 192.168.20.0 /28
- ✅ 192.168.20.16 /28
- ✅ 192.168.20.32 /28

Practice Use cases

📌 Problem 3

🏫 School Network Departments

A small school has 6 departments. The network team wants to isolate each into its own subnet.

You're given the block 10.0.0.0/24.

Solution Problem 3

📌 A network address with a prefix : 10.0.0.0/24

📌 A requirement is :split the network into 6 isolated departments

📌 I will use this formula $2^N \geq Number\ of\ Subnets$: $2^N \geq 6$

📌 So N (number of network bits to borrow) = 3 because $2^3 = 8$ (8 is the number of subnets)

📌 New Prefix = $Original\ Prefix + N$: $24 + 3 = 27$

📌 Determine the Hosts bits after subnetting (n) = $32 - 27 = 5$

📌 Network Subnet mask : 255.255.255.224

📌 Hope count (Block Size) : $2^n = 2^5 = 32$

- ✅ Development 1 ID is : 10.0.0.0 /27
- ✅ Development 2 ID is : 10.0.0.32 /27
- ✅ Development 3 ID is : 10.0.0.64 /27
- ✅ Development 4 ID is : 10.0.0.96 /27
- ✅ Development 5 ID is : 10.0.0.128 /27
- ✅ Development 6 ID is : 10.0.0.160 /27
- ✅ Extra Subnet ID is : 10.0.0.192 /27
- ✅ Extra Subnet ID is : 10.0.0.224 /27

Practice Use cases

📌 Problem 4

🏨 Hotel Wi-Fi Design

A hotel has a separate Wi-Fi subnet for each of its 5 guest floors. Each floor has 50 rooms, and each room needs 1 IP for a smart TV and 1 IP for Wi-Fi – so 100 devices per floor. You're given: 10.1.0.0/21.

Solution Problem 4

- A network address with a prefix : 10.1.0.0/21.
- The Number of hosts before subntteing (H) $= 32 - \text{prefix length} = 32 - 21 = 11$
- A requirement is : Each subnet that can support at least 100 devices
- I will use this formula $2^n - 2 \geq Number\ of\ Hosts$: $2^n - 2 \geq 100$
- So $n\ (Number\ of\ bit\ Hosts)$ = 7 because $2^7 - 2 = 126$ (126 is the number of hosts in each subnet)
- Calculating the number of network bits we were borrow (N) = $H - n = 11 - 7 = 4$
- The number of Subnets = $2^N = 2^4 = 16$
- New Prefix = $32 - n$: $32 - 7 = 25$
- Network Subnet mask : 255.255.255.128
- Hope count (Block Size) : $2^n = 2^7 = 128$

So The subnets IPs are :

- ✅ 10.1.0.0 / 25
- ✅ 10.1.0.128 / 25
- ✅ 10.1.1.0 / 25
- ✅ 10.1.1.128 /25
- ✅ 10.1.2.0 / 25
- ✅ 10.1.2.128 / 25
- ✅ 10.1.3.0 / 25
- ✅ 10.1.3.128 /25
- ✅ 10.1.4.0 / 25
- ✅ 10.1.4.128 / 25
- ✅ 10.1.5.0 / 25
- ✅ 10.1.5.128 /25
- ✅ 10.1.6.0 / 25
- ✅ 10.1.6.128 / 25
- ✅ 10.1.7.0 / 25
- ✅ 10.1.7.128 /25

I have Just 5 guest floors so I need only 5 subnet to use

- ✅ 10.1.0.0 / 25
- ✅ 10.1.0.128 / 25
- ✅ 10.1.1.0 / 25
- ✅ 10.1.1.128 /25
- ✅ 10.1.2.0 / 25

Practice Use cases

📌 Problem 5

🚗 Car Showroom Chain

A car company owns 8 showrooms across Egypt. They're connected via VPN tunnels, and each location should be on its own subnet. You're given the block: 172.16.0.0/23

Solution Problem 5

📌 A network address with a prefix : 172.16.0.0/23

📌 A requirement is :split the network into 8 isolated showrooms

📌 I will use this formula $2^N \geq Number\ of\ Subnets$: $2^N \geq 8$

📌 So N (number of network bits to borrow) = 3 because $2^3 = 8$ (8 is the number of subnets)

📌 New Prefix = $Original\ Prefix + N$: $23 + 3 = 26$

📌 Determine the Hosts bits after subnetting (n) = $32 - 26 = 6$

📌 Network Subnet mask : 255.255.255.192

📌 Hope count (Block Size) : $2^n = 2^6 = 64$

- ✅ showroom 1 ID is : 172.16.0.0 /26
- ✅ showroom 2 ID is : 172.16.0.64 /26
- ✅ showroom 3 ID is : 172.16.0.128 /26
- ✅ showroom 4 ID is : 172.16.0.192 /26
- ✅ showroom 5 ID is : 172.16.1.0 /26
- ✅ showroom 6 ID is : 172.16.1.64 /26
- ✅ showroom 7 ID is : 172.16.1.128 /26
- ✅ showroom 8 ID is : 172.16.1.192 /26

Tray To Solve

📌 Problem 1

🧪 School Labs Network

A school has 4 computer labs. Each lab has 20 computers + 2 printers. You are assigned: 192.168.5.0/24

📌 Problem 2

☕ Coffee Shop Chain

A coffee chain with 4 branches wants each branch to have its own subnet to isolate POS (Point of Sale) devices. The ISP gave them: 192.168.30.0/25

Tray To Solve

📌 Problem 3

📞 VoIP Office

A call center has a VoIP system with 70 phones. Each phone needs an IP, and they gave you the range 192.168.50.0/24.You need to isolate the phones in their own subnet.

📌 Problem 4

🚀 Startup with Growing Teams

A startup company has 3 existing teams but plans to expand to 8 in total. They give you 192.168.0.0/26 and want to know if that's enough for 8 separate teams.

Tray To Solve

📌 Problem 5

🛍️ Store with Separate Devices

A store wants to isolate its 10 security cameras, 5 point of sale systems, and 4 printers into one subnet. 192.168.77.0/24

📌 Problem 6

🌍 NGO Office Division

An NGO with a single office needs to divide its LAN into 3 segments: Admin, Volunteers, Finance. Each must be isolated. Given: 192.168.40.0/24

IP Subnetting Part 3 (IPv4)

(VLSM)

What we will Learn in this Part ?

💼 In this lecture, we will dive into Variable Length Subnet Masking (VLSM) and learn:

- What is VLSM and why it's a powerful technique for efficient IP addressing
- How to apply VLSM step-by-step in real-world scenarios
- How to calculate the required subnet mask for different segments
- How to avoid IP waste by allocating address spaces based on host requirements
- How to identify Network ID, First Host, Last Host, and Broadcast Address for each subnet

💼 By the end of this session, you'll be able to design scalable, optimized networks using VLSM.

🔧 VLSM in Action: What is the Process?

💼 VLSM (Variable Length Subnet Masking) allows us to subnet a subnet. It enables you to assign subnet masks of variable lengths to different subnets based on actual host needs, rather than using a fixed-length subnet mask for all.

💼 Key Benefits:

- 🔷 Reduces IP address waste
- 🔷 Supports hierarchical and scalable network design
- 🔷 Matches subnets precisely to department or device group needs

✅ Step-by-Step VLSM Strategy

- ✅ List all network segments and the number of required hosts
- ✅ Sort the list in descending order (largest to smallest)
- ✅ For each segment:
  - Calculate required host bits using the formula: $2^n - 2 \geq$ Required Hosts
  - Determine subnet mask and CIDR (Prefix) Prefix = 32 - n
  - Calculate block size: 2^n
  - Assign the first available IP range
  - Move to the next subnet, starting at the next available IP

Practice Use cases

📌 Problem 1

💼Scenario: ISP Branch Allocation :

You are given the network 192.168.10.0/24. Your task is to allocate the IP space using VLSM for the following branches:

Branch	Devices Needed
Head Office	100
Branch 1	50
Branch 2	25
Branch 3	10

Solution Problem 1

✅ Head Office – Needs 100 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 100 \rightarrow$ n = 7 $\rightarrow$ because $2^7 - 2 = 126$
- Step 2 (CIDR Prefix): Prefix = 32 - 7 = 25 $\rightarrow$ /25
- Step 3 (Block Size): $2^7 = 128$
- Step 4 (Subnet Assignment): Start at 192.168.10.0
- Step 5 (Address Range):
  - Network ID: 192.168.10.0
  - First Host: 192.168.10.1
  - Last Host: 192.168.10.126
  - Broadcast: 192.168.10.127

Solution Problem 1… cont.

✅ Branch 1 – Needs 50 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 50 \rightarrow$ n = 6 → because $2^6 - 2 = 62$
- Step 2 (CIDR Prefix): Prefix = 32 - 6 = 26 → /26
- Step 3 (Block Size): $2^6 = 64$
- Step 4 (Subnet Assignment): Start at 192.168.10.128
- Step 5 (Address Range):
  - Network ID: 192.168.10.128
  - First Host: 192.168.10.129
  - Last Host: 192.168.10.190
  - Broadcast: 192.168.10.191

Solution Problem 1… cont.

✅ Branch 2 – Needs 25 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 25 \rightarrow$ n = 5 → because $2^5 - 2 = 30$
- Step 2 (CIDR Prefix): Prefix = 32 - 5 = 27 → /27
- Step 3 (Block Size): $2^5 = 32$
- Step 4 (Subnet Assignment): Start at 192.168.10.192
- Step 5 (Address Range):
  - Network ID: 192.168.10.192
  - First Host: 192.168.10.193
  - Last Host: 192.168.10.222
  - Broadcast: 192.168.10.223

Solution Problem 1… cont.

✅ Branch 3 – Needs 10 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 10 \rightarrow$ n = 4 → because $2^4 - 2 = 14$
- Step 2 (CIDR Prefix): Prefix = 32 - 4 = 28 → /28
- Step 3 (Block Size): $2^4 = 16$
- Step 4 (Subnet Assignment): Start at 192.168.10.224
- Step 5 (Address Range):
  - Network ID: 192.168.10.224
  - First Host: 192.168.10.225
  - Last Host: 192.168.10.238
  - Broadcast: 192.168.10.239

🗓 Summary Table

Branch	Subnet	Mask	Hosts Range	Broadcast
Head Office	192.168.10.0/25	255.255.255.128	192.168.10.1 - 126	192.168.10.127
Branch 1	192.168.10.128/26	255.255.255.192	192.168.10.129 - 190	192.168.10.191
Branch 2	192.168.10.192/27	255.255.255.224	192.168.10.193 - 222	192.168.10.223
Branch 3	192.168.10.224/28	255.255.255.240	192.168.10.225 - 238	192.168.10.239

Practice Use cases

📌 Problem 2

💼University Building Wi-Fi Design:

You are given the network 10.10.10.0/24 Your task is to allocate the IP space using VLSM for the following branches:

Area	Devices Needed
Lecture Halls	60
Library	30
Administration	12
Security Office	6

Solution Problem 2

✅ Head Lecture Halls – Needs 60 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 60 \rightarrow$ n = 6 → because $2^6 - 2 = 62$
- Step 2 (CIDR Prefix): Prefix = 32 - 6 = 26 → /26
- Step 3 (Block Size): $2^6 = 64$
- Step 4 (Subnet Assignment): Start at 10.10.10.0/26
- Step 5 (Address Range):
  - Network ID: 10.10.10.0
  - First Host: 10.10.10.1
  - Last Host: 10.10.10.62
  - Broadcast: 10.10.10.63

Solution Problem 2… cont.

✅ Library – Needs 30 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 30 \rightarrow n = 5 \rightarrow$ because $2^5 - 2 = 30$
- Step 2 (CIDR Prefix): Prefix = 32 - 5 = 27 → /27
- Step 3 (Block Size): $2^5 = 32$
- Step 4 (Subnet Assignment): Start at 10.10.10.64/27
- Step 5 (Address Range):
  - Network ID: 10.10.10.64
  - First Host: 10.10.10.65
  - Last Host: 10.10.10.94
  - Broadcast: 10.10.10.95

Solution Problem 2… cont.

- ✅ Administration – Needs 12 Hosts
- Step 1 (Determine n): $2^n - 2 \geq 12 \rightarrow$ n = 4 → because $2^4 - 2 = 14$
- Step 2 (CIDR Prefix): Prefix = 32 - 4 = 28 → /28
- Step 3 (Block Size): $2^4 = 16$
- Step 4 (Subnet Assignment): Start at 10.10.10.96/28
- Step 5 (Address Range):
  - Network ID: 10.10.10.96
  - First Host: 10.10.10.97
  - Last Host: 10.10.10.110
  - Broadcast: 10.10.10.111

Solution Problem 2… cont.

✅ Security Office – Needs 6 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 8 \rightarrow$ n = 3 $\rightarrow$ because $2^3 - 2 = 6$
- Step 2 (CIDR Prefix): Prefix = 32 - 3 = 29 $\rightarrow$ /29
- Step 3 (Block Size): $2^3 = 8$
- Step 4 (Subnet Assignment): Start at 10.10.10.112/29
- Step 5 (Address Range):
  - Network ID: 10.10.10.112
  - First Host: 10.10.10.113
  - Last Host: 10.10.10.118
  - Broadcast: 10.10.10.119

📅 Summary Table

Area	Subnet	Mask	Hosts Range	Broadcast
Lecture Halls	10.10.10.0/26	255.255.255.192	10.10.10.1 - 10.10.10.62	10.10.10.63
Library	10.10.10.64/27	255.255.255.224	10.10.10.65 - 10.10.10.94	10.10.10.95
Administration	10.10.10.96/28	255.255.255.240	10.10.10.97 - 10.10.10.110	10.10.10.111
Security Office	10.10.10.112/29	255.255.255.248	10.10.10.113 - 10.10.10.118	10.10.10.119

Practice Use cases

📌 Problem 3

💼 Software Company Network:

You are given the network 10.10.10.0/24 Your task is to allocate the IP space using VLSM for the following branches:

Department	Devices Needed
Developers	70
QA Team	35
IT Support	15
HR + Finance	10

Solution Problem 3

✅ Developers – Needs 70 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 70 \rightarrow$ n = 7 $\rightarrow$ because $2^7 - 2 = 126$
- Step 2 (CIDR Prefix): Prefix = 32 - 7 = 25 $\rightarrow$ /25
- Step 3 (Block Size): $2^7 = 128$
- Step 4 (Subnet Assignment): Start at 172.16.0.0/25
- Step 5 (Address Range):
  - Network ID: 172.16.0.0
  - First Host: 172.16.0.1
  - Last Host: 172.16.0.126
  - Broadcast: 172.16.0.127

Solution Problem 3… cont.

✅ QA Team – Needs 35 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 35 \rightarrow$ n = 6 $\rightarrow$ because $2^6 - 2 = 62$
- Step 2 (CIDR Prefix): Prefix = 32 - 6 = 26 $\rightarrow$ /26
- Step 3 (Block Size): $2^6 = 64$
- Step 4 (Subnet Assignment): Start at 172.16.0.128/26
- Step 5 (Address Range):
  - Network ID: 172.16.0.128
  - First Host: 172.16.0.129
  - Last Host: 172.16.0.129
  - Broadcast: 172.16.0.191

Solution Problem 3… cont.

- ✅ IT Support – Needs 15 Hosts
- Step 1 (Determine n): $2^n - 2 \geq 15 \rightarrow$ n = 5 → because $2^5 - 2 = 30$
- Step 2 (CIDR Prefix): Prefix = 32 - 5 = 27 → /27
- Step 3 (Block Size): $2^5 = 32$
- Step 4 (Subnet Assignment): Start at 172.16.0.192/27
- Step 5 (Address Range):
  - Network ID: 172.16.0.192
  - First Host: 172.16.0.193
  - Last Host: 172.16.0.222
  - Broadcast: 172.16.0.223

Solution Problem 3… cont.

✅ HR + Finance – Needs 10 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 10 \rightarrow$ n = 4 → because $2^4 - 2 = 14$
- Step 2 (CIDR Prefix): Prefix = 32 - 4 = 28 → /28
- Step 3 (Block Size): $2^4 = 16$
- Step 4 (Subnet Assignment): Start at 172.16.0.224/28
- Step 5 (Address Range):
  - Network ID: 172.16.0.224
  - First Host: 172.16.0.225
  - Last Host: 172.16.0.238
  - Broadcast: 172.16.0.239

📅 Summary Table

Department	Subnet	Mask	Hosts Range	Broadcast
Developers	172.16.0.0/25	255.255.255.128	172.16.0.1 - 172.16.0.126	172.16.0.127
QA Team	172.16.0.128/26	255.255.255.192	172.16.0.129 - 172.16.0.190	172.16.0.191
IT Support	172.16.0.192/27	255.255.255.224	172.16.0.193 - 172.16.0.222	172.16.0.223
HR + Finance	172.16.0.224/28	255.255.255.240	172.16.0.225 - 172.16.0.238	172.16.0.239

Practice Use cases

📌 Problem 4

💼Retail Chain Store Network:

You are given the network 192.168.50.0/25 Your task is to allocate the IP space using VLSM for the following branches:

Location	Devices Needed
POS Systems	25
Cameras	20
Staff Phones	15
Management	8

Solution Problem 4

✅ POS Systems – Needs 25 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 25 \rightarrow$ n = 5 → because $2^5 - 2 = 30$
- Step 2 (CIDR Prefix): Prefix = 32 - 5 = 27 → /27
- Step 3 (Block Size): $2^5 = 32$
- Step 4 (Subnet Assignment): Start at 192.168.50.0/27
- Step 5 (Address Range):
  - Network ID: 192.168.50.0
  - First Host: 192.168.50.1
  - Last Host: 192.168.50.30
  - Broadcast: 192.168.50.31

Solution Problem 4… cont.

✅ Cameras – Needs 20 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 20 \rightarrow$ n = 5 → because $2^5 - 2 = 30$
- Step 2 (CIDR Prefix): Prefix = 32 - 5 = 27 → /27
- Step 3 (Block Size): $2^5 = 32$
- Step 4 (Subnet Assignment): Start at 192.168.50.32/27
- Step 5 (Address Range):
  - Network ID: 192.168.50.32
  - First Host: 192.168.50.33
  - Last Host: 192.168.50.62
  - Broadcast: 192.168.50.63

Solution Problem 4… cont.

✅ Staff Phones – Needs 15 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 15 \rightarrow$ n = 5 → because $2^5 - 2 = 30$
- Step 2 (CIDR Prefix): Prefix = 32 - 5 = 27 → /27
- Step 3 (Block Size): $2^5 = 32$
- Step 4 (Subnet Assignment): Start at 192.168.50.64/27
- Step 5 (Address Range):
  - Network ID: 192.168.50.64
  - First Host: 192.168.50.65
  - Last Host: 192.168.50.94
  - Broadcast: 192.168.50.95

Solution Problem 4… cont.

✅ Management – Needs 8 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 10$ → n = 4 → because $2^4 - 2 = 14$
- Step 2 (CIDR Prefix): Prefix = 32 - 4 = 28 → /28
- Step 3 (Block Size): $2^4 = 16$
- Step 4 (Subnet Assignment): Start at 192.168.50.96/28
- Step 5 (Address Range):
  - Network ID: 192.168.50.96
  - First Host: 192.168.50.97
  - Last Host: 192.168.50.110
  - Broadcast: 192.168.50.111

📅 Summary Table

Location	Subnet	Mask	Hosts Range	Broadcast
POS Systems	192.168.50.0/27	255.255.255.224	192.168.50.1 - 192.168.50.30	192.168.50.31
Cameras	192.168.50.32/27	255.255.255.224	192.168.50.33 - 192.168.50.62	192.168.50.63
Staff Phones	192.168.50.64/27	255.255.255.224	192.168.50.65 - 192.168.50.94	192.168.50.95
Management	192.168.50.96/28	255.255.255.240	192.168.50.97 - 192.168.50.110	192.168.50.111

Practice Use cases

📌 Problem 5

💼Healthcare Network:

You are given the network 10.0.1.0/24 Your task is to allocate the IP space using VLSM for the following branches:

Department	Devices Needed
ICU	40
Outpatient Clinic	20
Radiology	12
Reception & Admin	6

Solution Problem 5

- ✅ ICU – Needs 40 Hosts
- Step 1 (Determine n): $2^n - 2 \geq 40 \rightarrow$ n = 6 $\rightarrow$ because $2^6 - 2 = 62$
- Step 2 (CIDR Prefix): Prefix = 32 - 6 = 26 $\rightarrow$ /26
- Step 3 (Block Size): $2^6 = 64$
- Step 4 (Subnet Assignment): Start at 10.0.1.0/26
- Step 5 (Address Range):
  - Network ID: 10.0.1.0
  - First Host: 10.0.1.1
  - Last Host: 10.0.1.62
  - Broadcast: 10.0.1.63

Solution Problem 5… cont.

✅ Outpatient Clinic – Needs 20 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 20 \rightarrow$ n = 5 → because $2^5 - 2 = 30$
- Step 2 (CIDR Prefix): Prefix = 32 - 5 = 27 → /27
- Step 3 (Block Size): $2^5 = 32$
- Step 4 (Subnet Assignment): Start at 10.0.1.64/27
- Step 5 (Address Range):
  - Network ID: 10.0.1.64
  - First Host: 10.0.1.65
  - Last Host: 10.0.1.94
  - Broadcast: 10.0.1.95

Solution Problem 5… cont.

✅ Radiology – Needs 12 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 12 \rightarrow$ n = 4 → because $2^4 - 2 = 14$
- Step 2 (CIDR Prefix): Prefix = 32 - 4 = 28 → /28
- Step 3 (Block Size): $2^4 = 16$
- Step 4 (Subnet Assignment): Start at 10.0.1.96/28
- Step 5 (Address Range):
  - Network ID: 10.0.1.96
  - First Host: 10.0.1.97
  - Last Host: 10.0.1.110
  - Broadcast: 10.0.1.111

Solution Problem 5… cont.

✅ Reception & Admin – Needs 6 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 6 \rightarrow$ n = 3 → because $2^3 - 2 = 6$
- Step 2 (CIDR Prefix): Prefix = 32 - 3 = 29 → /29
- Step 3 (Block Size): $2^3 = 8$
- Step 4 (Subnet Assignment): Start at 10.0.1.112/29
- Step 5 (Address Range):
  - Network ID: 10.0.1.112
  - First Host: 10.0.1.113
  - Last Host: 10.0.1.118
  - Broadcast: 10.0.1.119

🗓️ Summary Table

Department	Subnet	Mask	Hosts Range	Broadcast
ICU	10.0.1.0/26	255.255.255.192	10.0.1.1 - 10.0.1.62	10.0.1.63
Outpatient Clinic	10.0.1.64/27	255.255.255.224	10.0.1.65 - 10.0.1.94	10.0.1.95
Radiology	10.0.1.96/28	255.255.255.240	10.0.1.97 - 10.0.1.110	10.0.1.111
Reception & Admin	10.0.1.112/29	255.255.255.248	10.0.1.113 - 10.0.1.118	10.0.1.119

Practice Use cases

📌 Problem 6

💼 Training Center Network:

You are given the network 192.168.60.0/24 Your task is to allocate the IP space using VLSM for the following branches:

Room Type	Devices Needed
Lab A	60
Lab B	30
Conference Hall	25
Admin Office	14

Solution Problem 6

✅ Lab A – Needs 60 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 40 \rightarrow$ n = 6 → because $2^6 - 2 = 62$
- Step 2 (CIDR Prefix): Prefix = 32 - 6 = 26 → /26
- Step 3 (Block Size): $2^6 = 64$
- Step 4 (Subnet Assignment): Start at 192.168.60.0/26
- Step 5 (Address Range):
  - Network ID: 192.168.60.0
  - First Host: 192.168.60.1
  - Last Host: 192.168.60.62
  - Broadcast: 192.168.60.63

Solution Problem 6… cont.

✅ Lab B – Needs 30 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 20 \rightarrow$ n = 5 → because $2^5 - 2 = 30$
- Step 2 (CIDR Prefix): Prefix = 32 - 5 = 27 → /27
- Step 3 (Block Size): $2^5 = 32$
- Step 4 (Subnet Assignment): Start at 192.168.60.64/27
- Step 5 (Address Range):
  - Network ID: 192.168.60.64
  - First Host: 192.168.60.64
  - Last Host: 192.168.60.94
  - Broadcast: 192.168.60.95

Solution Problem 6… cont.

✅ Conference Hall – Needs 25 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 25 \rightarrow$ n = 5 → because $2^5 - 2 = 30$
- Step 2 (CIDR Prefix): Prefix = 32 - 5 = 27 → /27
- Step 3 (Block Size): $2^5 = 32$
- Step 4 (Subnet Assignment): Start at 192.168.60.96/27
- Step 5 (Address Range):
  - Network ID: 192.168.60.96
  - First Host: 192.168.60.97
  - Last Host: 192.168.60.126
  - Broadcast: 192.168.60.127

Solution Problem 6… cont.

✅ Admin Office – Needs 14 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 14 \rightarrow$ n = 4 → because $2^4 - 2 = 14$
- Step 2 (CIDR Prefix): Prefix = 32 - 4 = 28 → /28
- Step 3 (Block Size): $2^4 = 16$
- Step 4 (Subnet Assignment): Start at 192.168.60.128/28
- Step 5 (Address Range):
  - Network ID: 192.168.60.128
  - First Host: 192.168.60.129
  - Last Host: 192.168.60.142
  - Broadcast: 192.168.60.143

📅 Summary Table

Room Type	Subnet	Mask	Hosts Range	Broadcast
Lab A	192.168.60.0/26	255.255.255.192	192.168.60.1 - 62	192.168.60.63
Lab B	192.168.60.64/27	255.255.255.224	192.168.60.65 - 94	192.168.60.95
Conference Hall	192.168.60.96/27	255.255.255.224	192.168.60.97 - 126	192.168.60.127
Admin Office	192.168.60.128/28	255.255.255.240	192.168.60.129 - 142	192.168.60.143

Practice Use cases

📌 Problem 7

💼 Smart Building Sensors

You are given the network 172.20.0.0/24 Your task is to allocate the IP space using VLSM for the following branches:

System	Devices Needed
HVAC	50
Surveillance	35
Elevators System	10
Fire Detection	8

Solution Problem 7

✅ HVAC – Needs 50 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 40 \rightarrow$ n = 6 $\rightarrow$ because $2^6 - 2 = 62$
- Step 2 (CIDR Prefix): Prefix = 32 - 6 = 26 $\rightarrow$ /26
- Step 3 (Block Size): $2^6 = 64$
- Step 4 (Subnet Assignment): Start at 172.20.0.0/26
- Step 5 (Address Range):
  - Network ID: 172.20.0.0
  - First Host: 172.20.0.1
  - Last Host: 172.20.0.62
  - Broadcast: 172.20.0.63

Solution Problem 7… cont.

✅ Surveillance – Needs 35 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 35 \rightarrow$ n = 6 → because $2^6 - 2 = 62$
- Step 2 (CIDR Prefix): Prefix = 32 - 6 = 26 → /26
- Step 3 (Block Size): $2^6 = 64$
- Step 4 (Subnet Assignment): Start at 172.20.0.64/26
- Step 5 (Address Range):
  - Network ID: 172.20.0.64
  - First Host: 172.20.0.65
  - Last Host: 172.20.0.126
  - Broadcast: 172.20.0.127

Solution Problem 7… cont.

✅ Elevators System – Needs 10 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 10 \rightarrow$ n = 4 → because $2^4 - 2 = 14$
- Step 2 (CIDR Prefix): Prefix = 32 - 4 = 28 → /28
- Step 3 (Block Size): $2^5 = 32$
- Step 4 (Subnet Assignment): Start at 172.20.0.128/28
- Step 5 (Address Range):
  - Network ID: 172.20.0.128
  - First Host: 172.20.0.129
  - Last Host: 172.20.0.142
  - Broadcast: 172.20.0.143

Solution Problem 7… cont.

✅ Fire Detection – Needs 8 Hosts

- Step 1 (Determine n): $2^n - 2 \geq 14 \rightarrow$ n = 4 → because $2^4 - 2 = 14$
- Step 2 (CIDR Prefix): Prefix = 32 - 4 = 28 → /28
- Step 3 (Block Size): $2^4 = 16$
- Step 4 (Subnet Assignment): Start at 192.168.60.144/28
- Step 5 (Address Range):
  - Network ID: 192.168.60.144
  - First Host: 192.168.60.145
  - Last Host: 192.168.60.158
  - Broadcast: 192.168.60.159

📅 Summary Table

System	Subnet	Mask	Hosts Range	Broadcast
HVAC	172.20.0.0/26	255.255.255.192	172.20.0.1 - 62	172.20.0.63
Surveillance	172.20.0.64/26	255.255.255.192	172.20.0.65 - 126	172.20.0.127
Elevators	172.20.0.128/28	255.255.255.240	172.20.0.129 - 142	172.20.0.143
Fire Detection	172.20.0.144/28	255.255.255.240	172.20.0.145 - 158	172.20.0.159

TCP & UDP Protocols

Introduction

Let's work our way up the OSI-model, we just covered IP and now it's time to pick a "transport" protocol. Keep in mind IP is "nothing more" but a number (ok that's very simplistic) but I want to make sure you understand we need a transport protocol for actually setting up the connection and sending data between our computers.

In this Lecture I want to focus on the transport protocols that are used most of the time:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

why do we have 2 different transport protocols here?

why do we care and when do we need one over another?

The short answer is:

- TCP is a reliable protocol.
- UDP is a unreliable or best-effort protocol.

Unreliable you might think? Why do I want data transport which is unreliable? Does that make any sense? Let me tell you a little story to explain the difference between the two protocols

First Story

You are sitting behind your computer and downloading the latest greatest movie in 1080P HD with 7.1 surround super sound directly from Universal studio's brand new "download on demand" service (hey you never know…it might happen one day…). This file is 20GB and after downloading 10GB there's something going wrong and a couple of IP packets don't make it to your computer, as soon as the entire download is done you try to play the movie and you get all kind of errors. Unable to watch the movie you are frustrated and head for the local DVD rental place to watch some low-quality movie…

So the idea , you want to make sure the transport of your download to your computer is reliable which is why we use TCP. In case some of the IP packets don't make it to your computer you want to make sure this data will be retransmitted to your computer!

Second Story

In our second story you are the network engineer for a major company and you just told your boss how awesome this brand new open source Voice over IP solution is. You decide to implement this new VoIP solution and to get rid of all the analogy phones but your users are now complaining big time that their phone call quality is horrible. You contact the open source VoIP solution provider and you find out that they thought it would be a good idea to use a reliable transport protocol like TCP since well, we want phone calls to be reliable right?!

Wrong thinking! TCP does error correction which means that data that didn't make it to your computer will be retransmitted. How weird will your phone call sound if you are talking to someone and you hear something that they said a few seconds ago? It's real-time so we don't want retransmission. It's better to send VoIP packets and lose a few than retransmitting them afterwards, your VoIP codec can also fix packet loss up to a certain degree. In this example we'll want to use a best effort or unreliable protocol which is UDP.

	TCP	UDP
Connection Type	Connection-Oriented	Connectionless
Sequencing	YES	NO
Usage	Downloads- File Sharing – Printing …	VOIP Video (Streaming)

What do we have in the table above?

First of all you see "connection type".

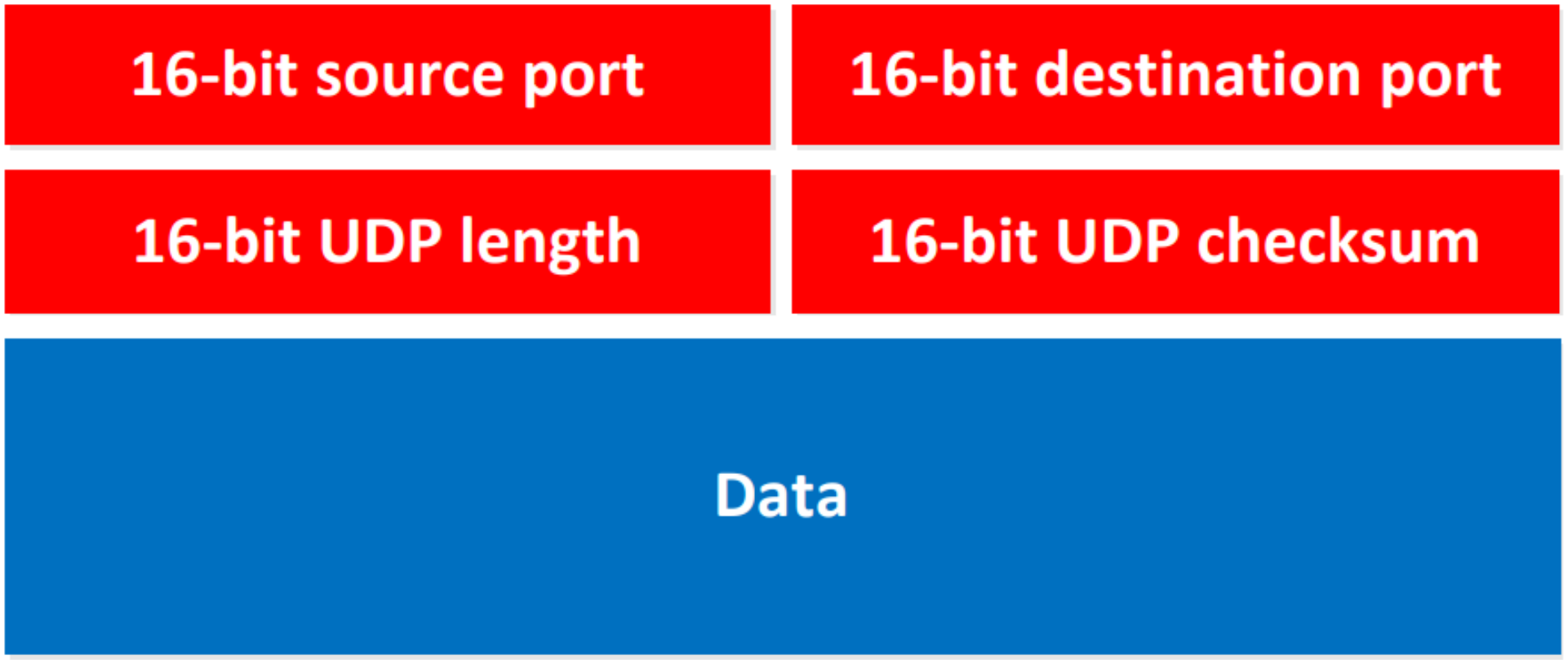
- TCP is connection-oriented which means it will "setup" a connection and then start transferring data.
- UDP is connectionless which means it will just start sending and doesn't care if it arrives yes or not.
- The connection that TCP will setup is called the "3 way handshake" which I will show you in a minute.

Second of all you see “Sequencing”.

- Sequencing means that we use a sequence number
- if you download a big file you need to make sure that you can put all those packets back in the right order.
- As you can see UDP does not offer this feature, there's no sequence number there.

So what about VoIP? Don't we need to put those packets back in order at the receiver side? Well actually yes we do otherwise we get some strange conversations. UDP does not offer this "sequencing" feature though…let me tell you a little secret: for VoIP it's not just UDP that we use but we also use RTP which does offer sequencing! (And some other cool features we need for VoIP).

Let's take a look at an UDP header



You can see how simple it is, it has the source and destination port number (this is how we know for which application the data is meant), there's a checksum and the length.

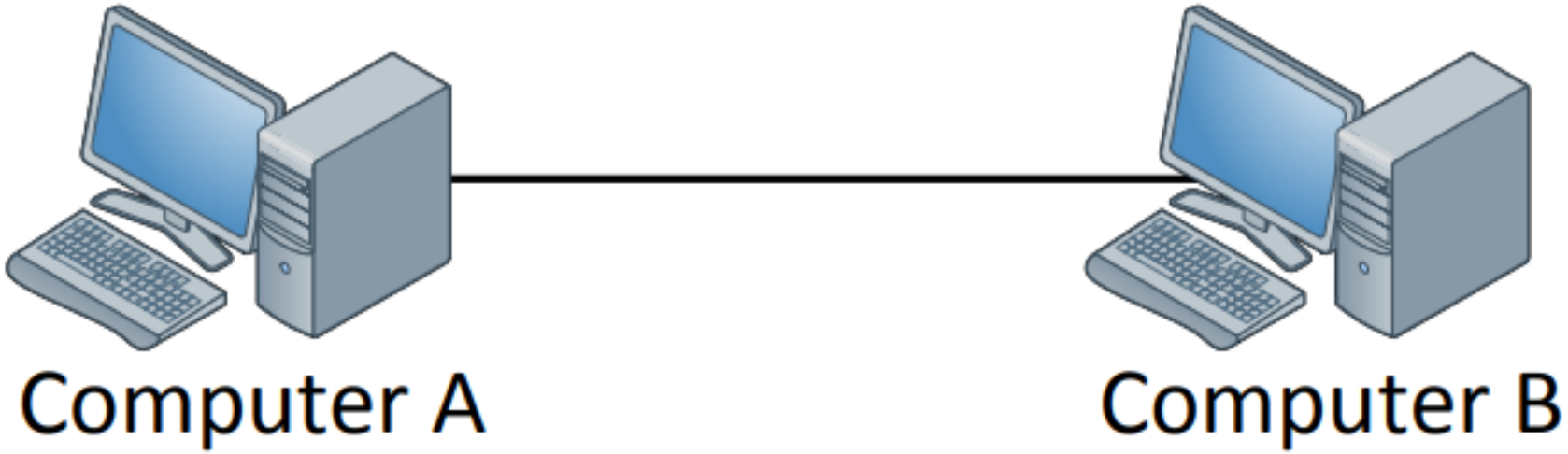
Let's sum up what we now know about UDP

- It operates on the transport layer of the OSI model.
- Is a connectionless protocol, does not setup a connection…just sends data.
- Limited error correction because we have a checksum
- Best-effort or unreliable protocol.
- No data-recovery features.

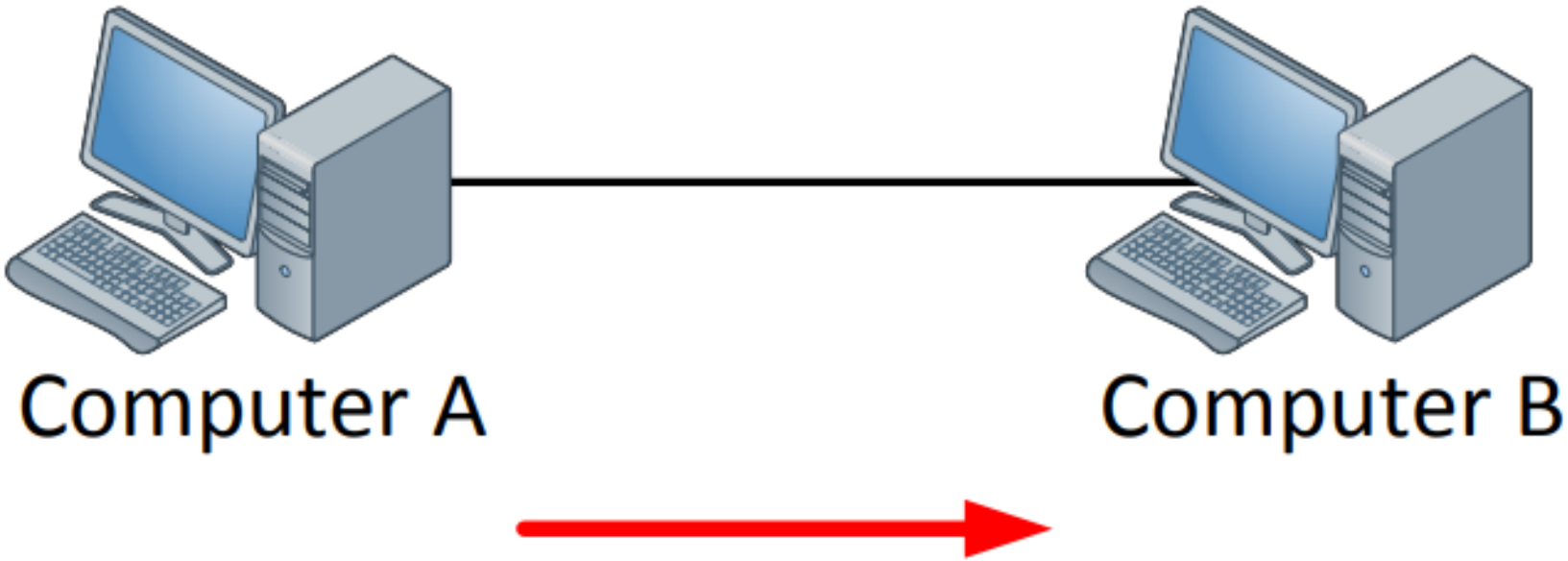
Now let's see what TCP can offer us.

- First of all since TCP is a reliable protocol it will "setup" a connection before we start sending any data.
- This connection is called the "3 way handshake".

"Computer A" wants to send data to "computer B" in a reliable way, so we are going to use TCP to accomplish this. First we will setup the connection by using a 3-way handshake, let me walk you through the process

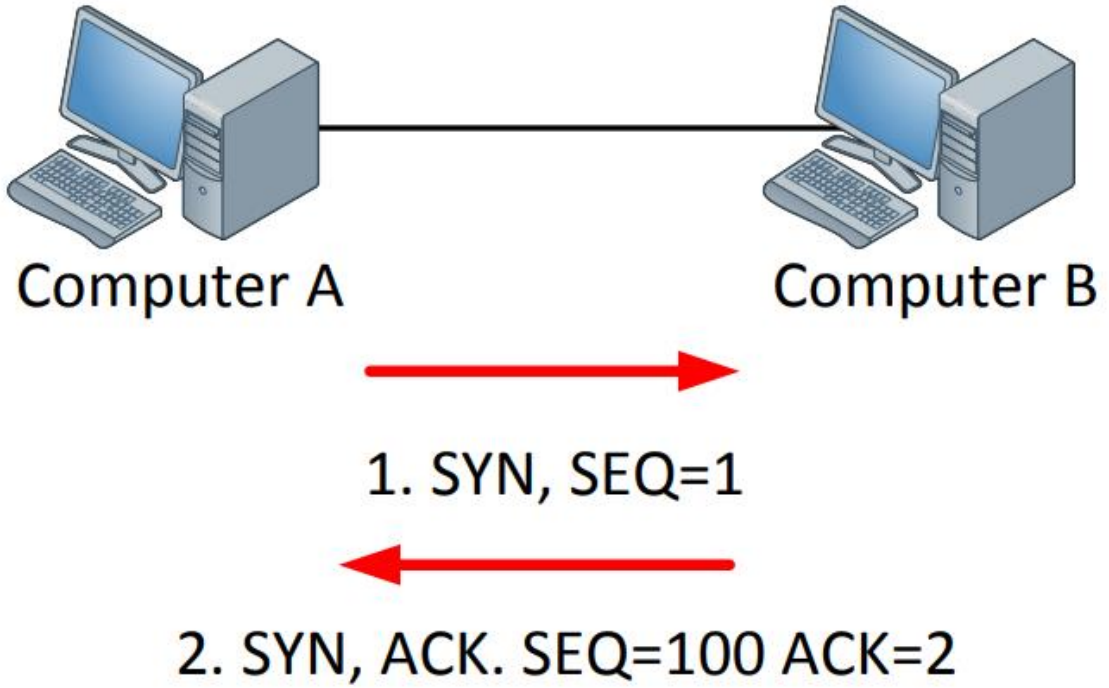


First our "computer A" will send a TCP SYN, telling "computer B" that it wants to setup a connection. There's also a sequence number and to keep things simple I picked number 1.

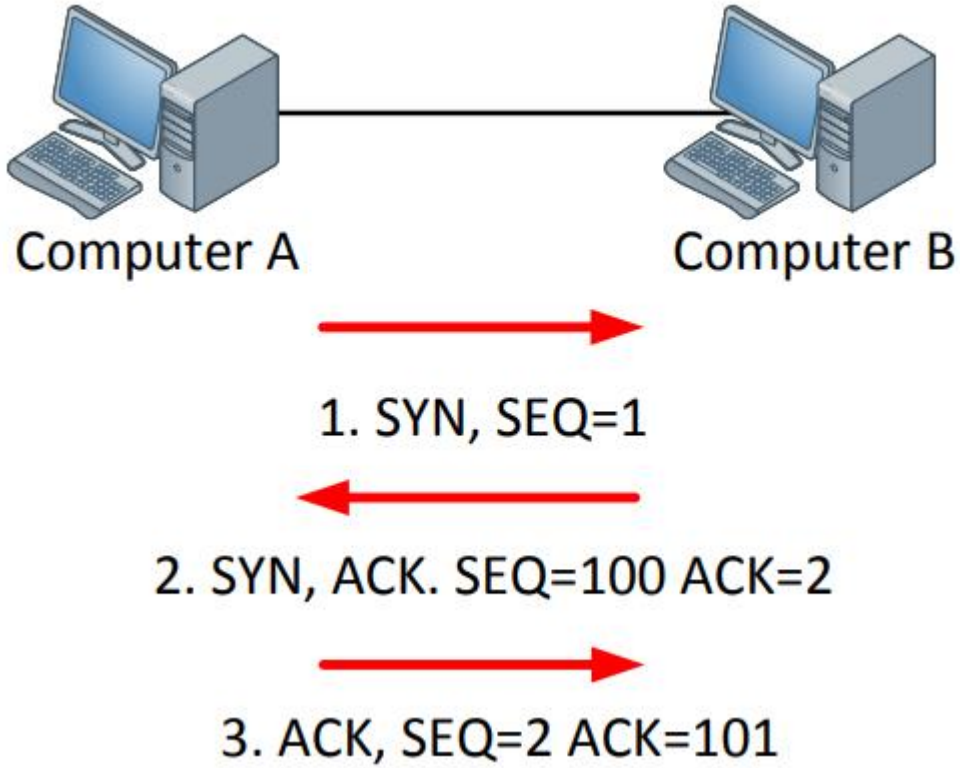


"Computer B" will respond to "computer A" by sending a SYN,ACK message back. You can see it picks its own sequence number 100 (I just picked a random number) and it sends ACK=2.

ACK=2 means that it acknowledges that it has received the TCP SYN from "computer A" which had sequence number 1 and that it is ready for the next message with sequence number 2.



The last step is that "computer A" will send an acknowledgement towards "computer B" in response of the SYN that computer B sent towards computer A. You can see it sends ACK=101 which means it acknowledges the SEQ=100 from "computer B". Since "computer B" sent a ACK=2 towards computer A, "computer A" now knows it can send the next message with sequence number 2



To simplify things

- Computer A sends a TCP SYN. (I want to talk to you)
- Computer B sends a TCP SYN,ACK. (I accept that you want to talk to me, and I want to talk to you as well)
- Computer A sends a TCP ACK. (I accept that you want to talk to me)

Phew so we have setup a connection using the 3 way handshake!

Now we can start sending data…

what else does TCP offer us?!

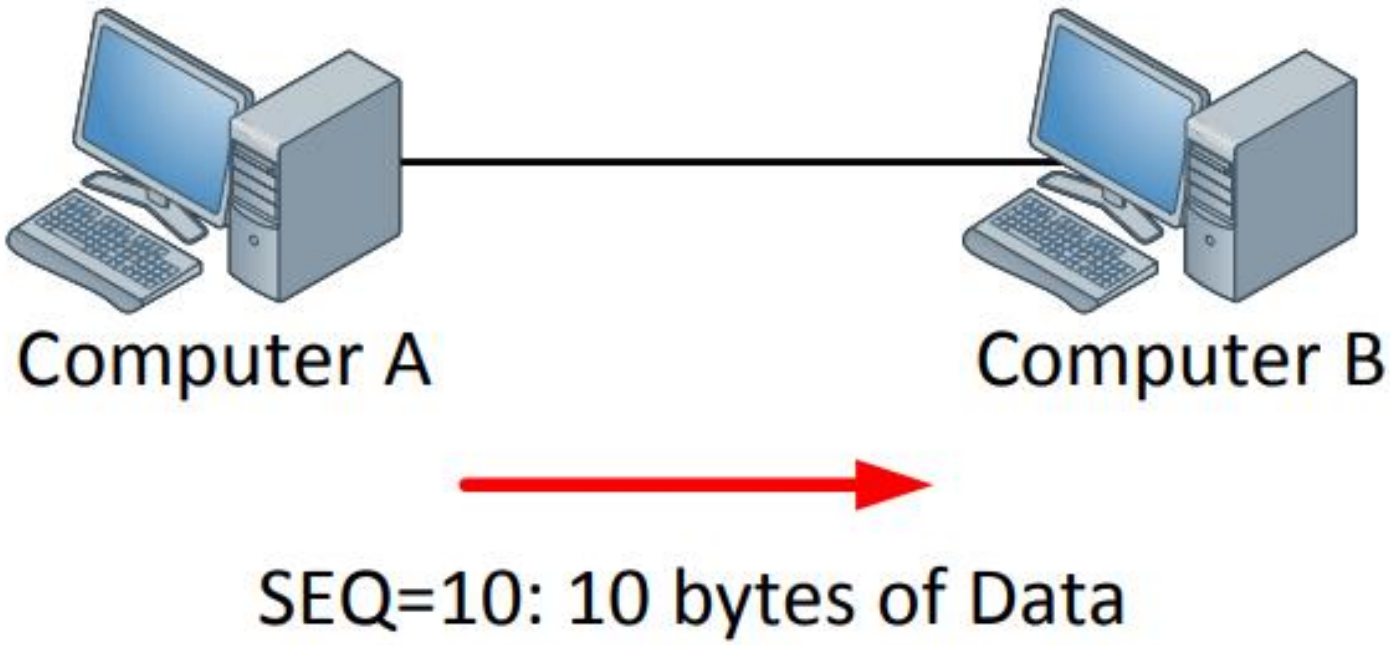
One of the things is "flow control".

Imagine you have a fast computer transmitting data to a smartphone, obviously the computer could overburden the smartphone with traffic which is why we have flow control. In each TCP segment the receiver can specify in the "receive window" field how much data in bytes it wants to receive.

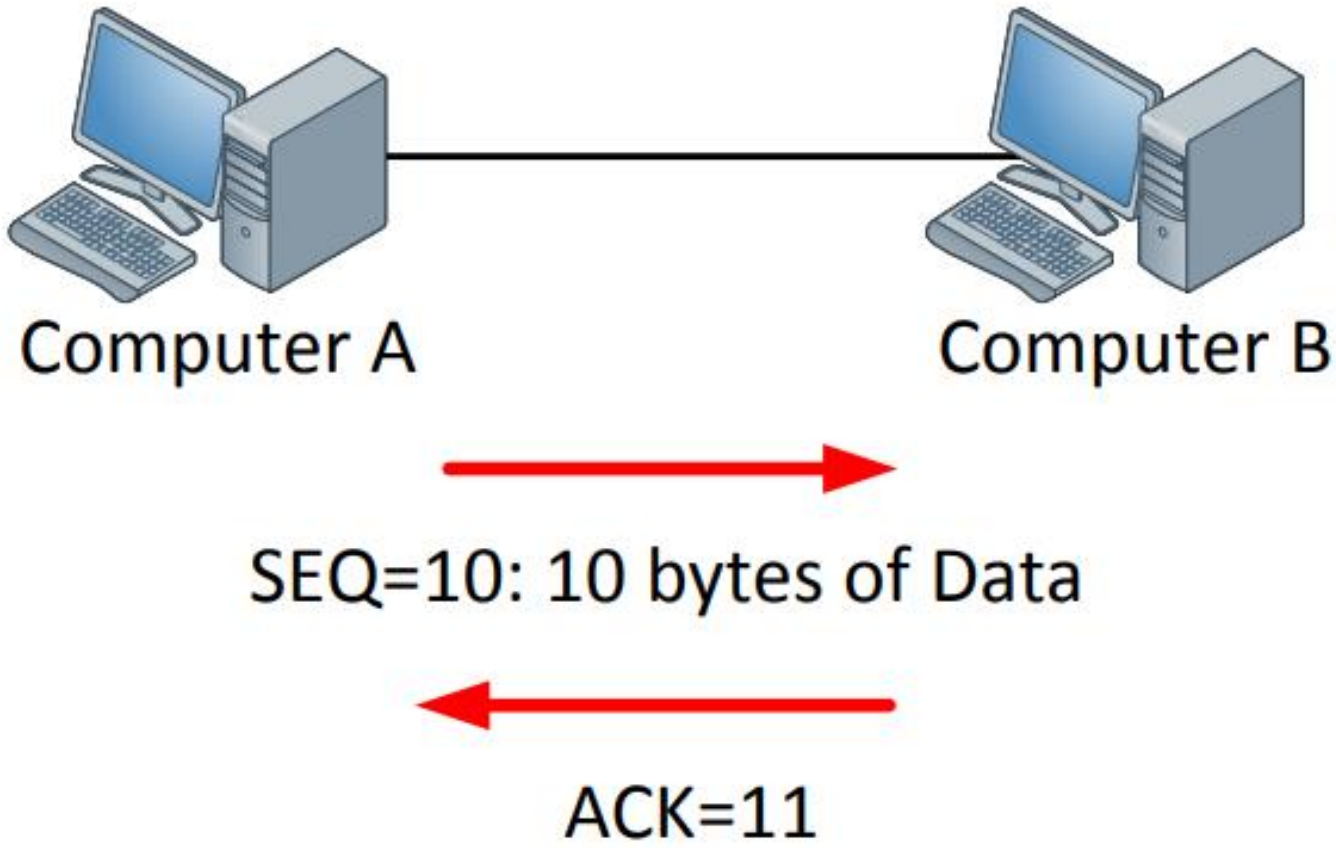
Our sending computer can only send data up to this size so the smartphone doesn't get overburdened. The more data you can send each time the higher your throughput will be. Let's look at an example of how this all fits together

- "Computer A" has setup a connection with "Computer B" by using the 3 way handshake.

- We are sending 10 bytes of Data which means our "window size" is 10 bytes. The sequence number is 10.



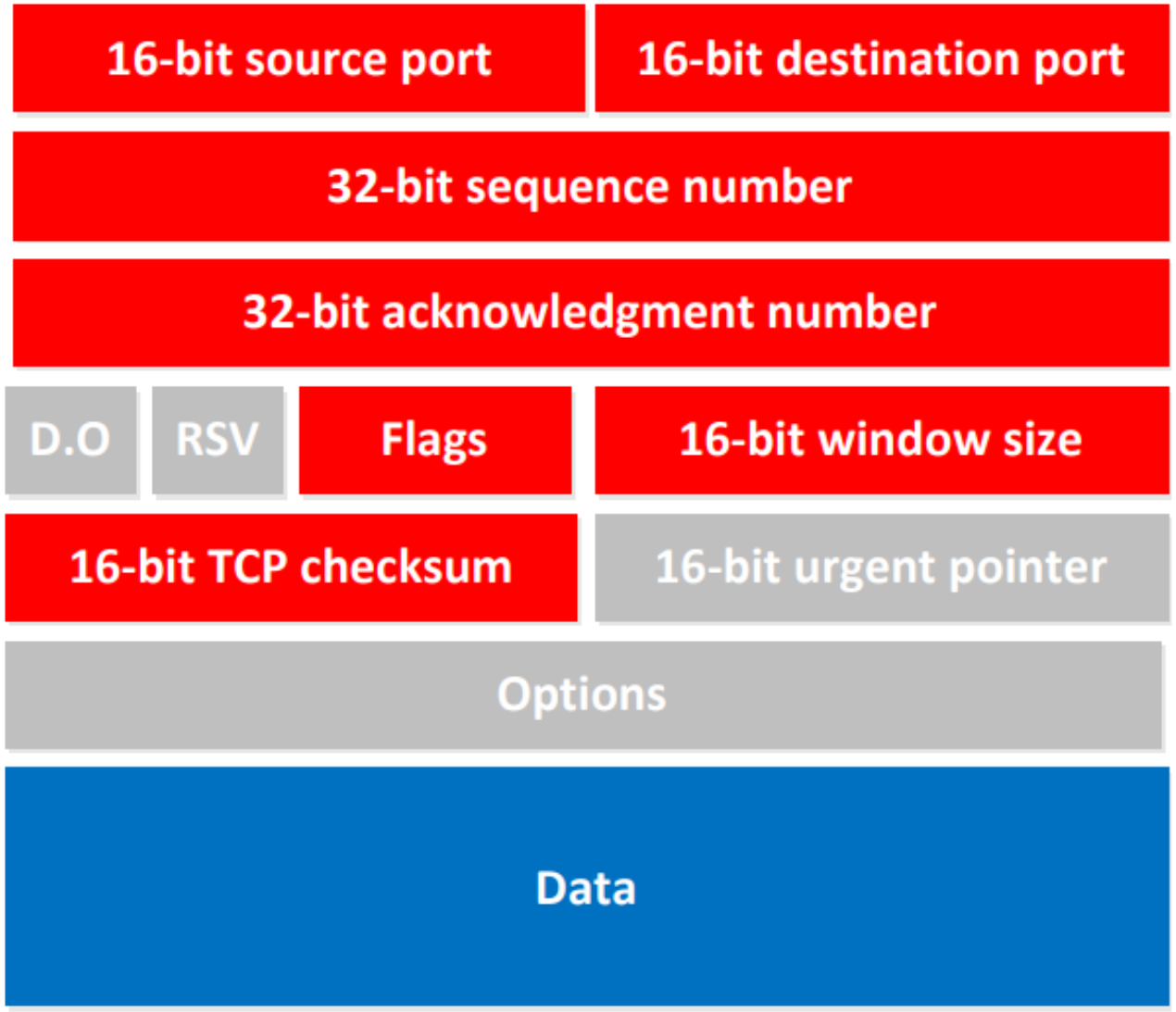
"Computer B" is going to respond by sending "ACK=11" which means "thanks I received your 10 bytes, now send me #11 and the rest". TCP is a reliable protocol which is why we have to acknowledge everything we are receiving.



The larger your window size, the higher your throughput will be. This makes sense because you are sending fewer ACK"s compared to the data you are sending.

TCP is a fairly complex protocol and if we look at the header you'll see it has a lot more fields than UDP has:

The fields in "Gray" are not important for us; everything in red is what I would like to tell you about.



- As you can see there's a 16-bit source and destination port
  - Port numbers are used to determine for which application this data is meant (This is how we go from the transport layer up to the higher layers in the OSI-model).
- You can see we have 32-bits that are used for our sequence numbers, and there's also 32-bits for the acknowledgment (ACK) reserved.
- The "Flags" field is where TCP sets the different message types like "SYN" or "ACK".
- Window size has a 16-bit field which specifies how many bytes of data you will send before you want an acknowledgment from the other side.
- Finally there's a checksum and of course our data, the stuff we are actually trying to send to the other side.

Let's sum up what we have learned about TCP

- It"s a reliable protocol.
- Before you send data you will setup the connection by using "the 3 way handshake."
- After sending X amount of bytes you will receive an "acknowledgment (ACK)" from the other side.
- How many bytes you send before you get an ACK is controlled by using the "window size".
- TCP can do retransmissions.

Part One Ends Here

More parts coming soon!

Eng/ Ahmed Elkhatib