Week 1: Network Fundamentals

Ayman El Hajjar

Email: a.elhajjar@westminster.ac.uk
Twitter: @azelhajjar

6COSC002W - Security and Forensics

18 January 2021

University of Westminster

Session Overview

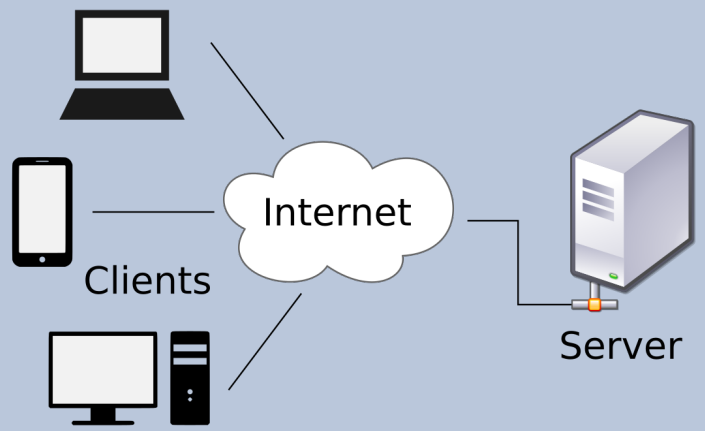
1. **Networking Foundations**
   - Networking Fundamentals
   - Communication protocols
   - Layering models
2. **Addressing**
   - Addressing Requirements
   - Internet Protocol and addressing

Introduction to Networking

- What is a Network?
  - Set of technologies that connects computers
  - Allows communication and collaboration between users
  - Collection of computers and devices connected together
- The uses of a network
  - Simultaneous access to data
  - Shared Resources
  - Personal communication
  - Easier data backup
- Common Network types
  - Personal Area Network (PAN)
  - Local Area Network (LAN)
  - Metropolitan Area Network (MAN)
  - Wide Area Network (WAN)

Network architecture: Centralized Architecture

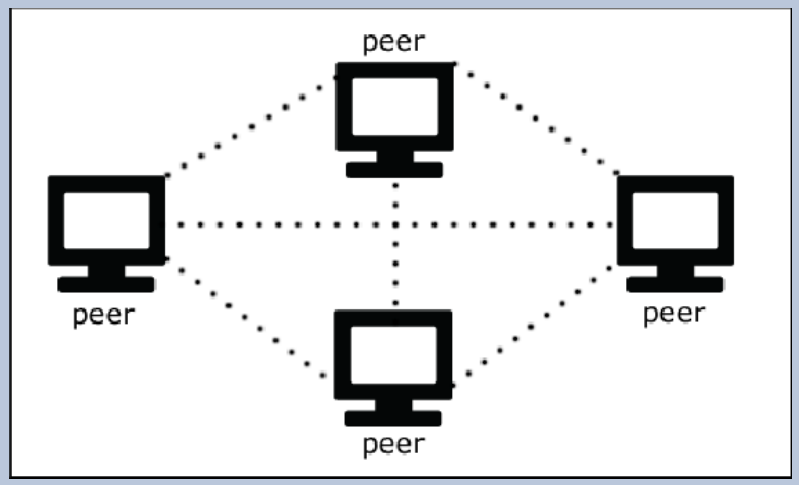
- Client/server architecture is a **centralized architecture**.
- A client/Server architecture exist is when one main device in order to get a service.
- In this instance, a server is the device providing a service
- All devices connected to it are clients.
- Most of the internet is of Client/Server architecture.
- A website is an example of a client/server architecture



Centralized Archicture: Client/Server

Network architecture: De-Centralized Architecture

- Peer to peer architecture (Ad Hoc): Devices are connected directly to each other.
- This is a **decentralized architecture**
- Each device can be server or client depending on whether it is sending or receiving



De-Centralized Archicture: Peer to Peer

The Internet

What is the Internet

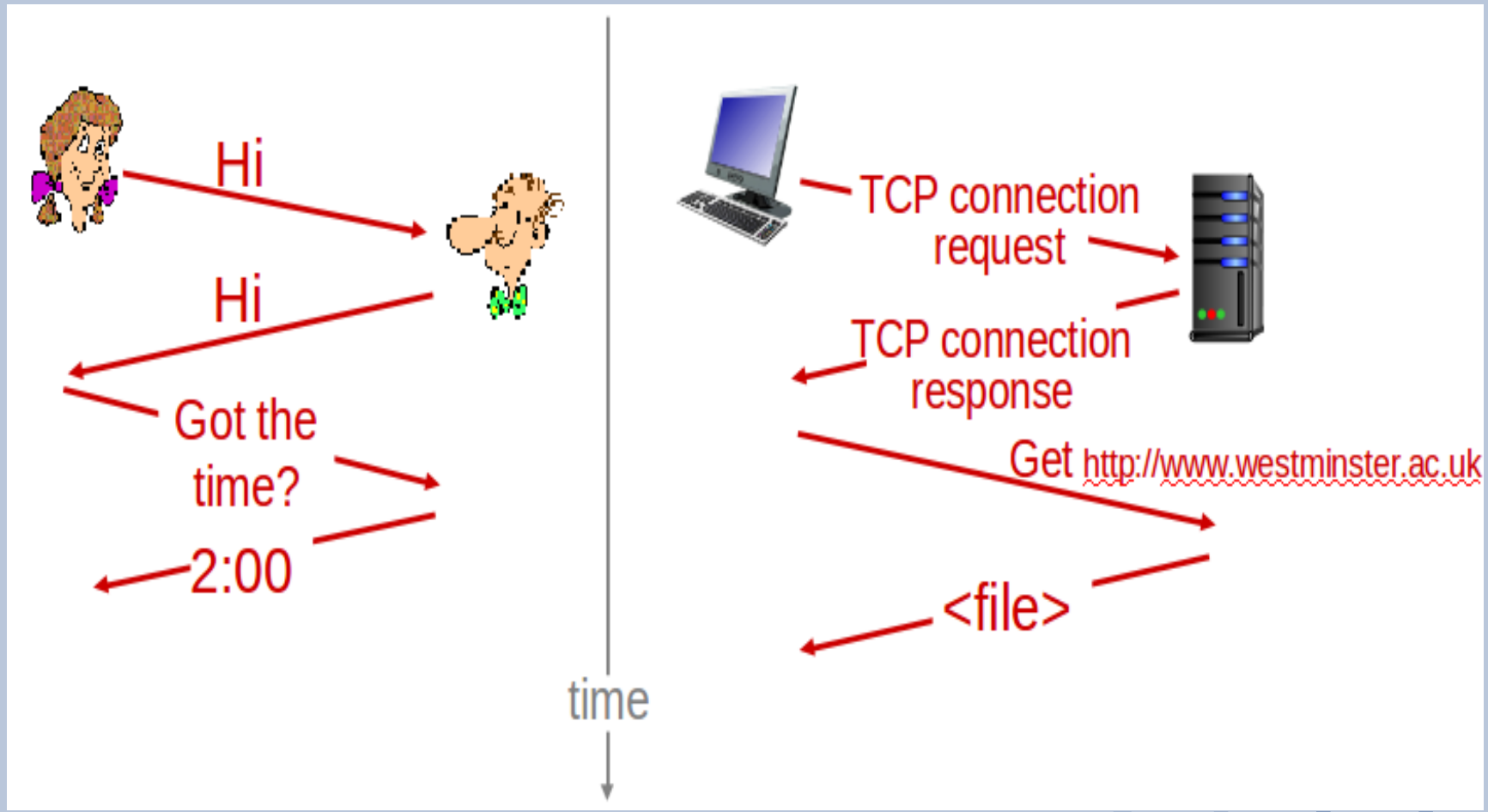
The simplest definition of the Internet is that it's a network of computer networks

What is a protocol?

- A protocol is a set of rules or conventions that dictate communication.
  - Without communication protocols, I might ask a question and you might respond by closing your eyes.
  - Communication in this instance did not actually happen, or it was meaningless.
  - In another word, the communication failed because it did not follow the rule.
  - The rule is- If and when we ask a question, we expect a response.
    - Regardless of what the response is!

What is a protocol?

A human protocol and a computer network protocol:



What is a protocol?

Human protocols:

- Class starts at 09 AM sharp
- Switch off your phones
- If you have a question, Wait for your turn!

Network protocols:

- Machines rather than humans
- All communication activity in Internet governed by protocols

Protocol

A protocol is a set of rules and formats that govern the communication between communicating peers.

- set of valid messages
- meaning of each message

What is a layer?

- Person delivery of parcel
- Post office counter handling
- Ground transfer: loading on trucks
- Airport transfer: loading on airplane
- Airplane routing from source to destination

Advantages of Layering

- Simplify our understanding of a complex system
- All communication activity in Internet governed by protocols

Open System Interconnection (OSI) model

- The OSI model consists of seven separate and distinct layers, each describing a particular set of functions and behaviors.
- Although every protocol used for communication will fit into one of these seven layers, not all communication streams will make use of all seven layers.
- Order is essential- Remember:
  - **P**lease **D**o Not **T**ell **S**ecret **P**asswords **A**nymore

OSI model: Application (Layer 7)

- The Application layer is the one closest to the end user.
- It is **NOT** the application itself.
- Application layer protocols manage the communication needs of the application.
- They may identify resources and manage interacting with those resources.
- For example, when you visit a website, the **HyperText Transfer Protocol (HTTP)** (an Application layer protocol), takes care of negotiating for resources (pages, etc.) between the client and the server.

OSI model: Presentation (Layer 6)

- The Presentation layer is responsible for preparing data for the Application layer.
- It makes sure that the data that is handed up to the application is in the right format so it can be consumed.
- Systems cannot communication if they are using different format.
- JPEG, ASCII code are two examples of Presentation layer protocols

OSI model: Session (Layer 5)

- Manages the communication between the endpoints (e.g. client/server).
- Remote procedure calls (RPCs) are an example of a function at the Session layer.
- There are components of file sharing that also live at the Session layer, since negotiation of communication between the endpoints needs to take place.

OSI model: Transport (Layer 4)

- The Transport layer takes care of segmenting messages for transmission.
- The Transport layer also takes care of multiplexing of the communication.
- Both the **TCP** and the **UDP** are transport protocols.
- These protocols use ports for addressing so receiving systems know which application to pass the traffic to.

OSI model: Network (Layer 3)

- Responsible for Addressing and Routing packets from one endpoint to another.
- The IP is one protocol that exists at this layer.

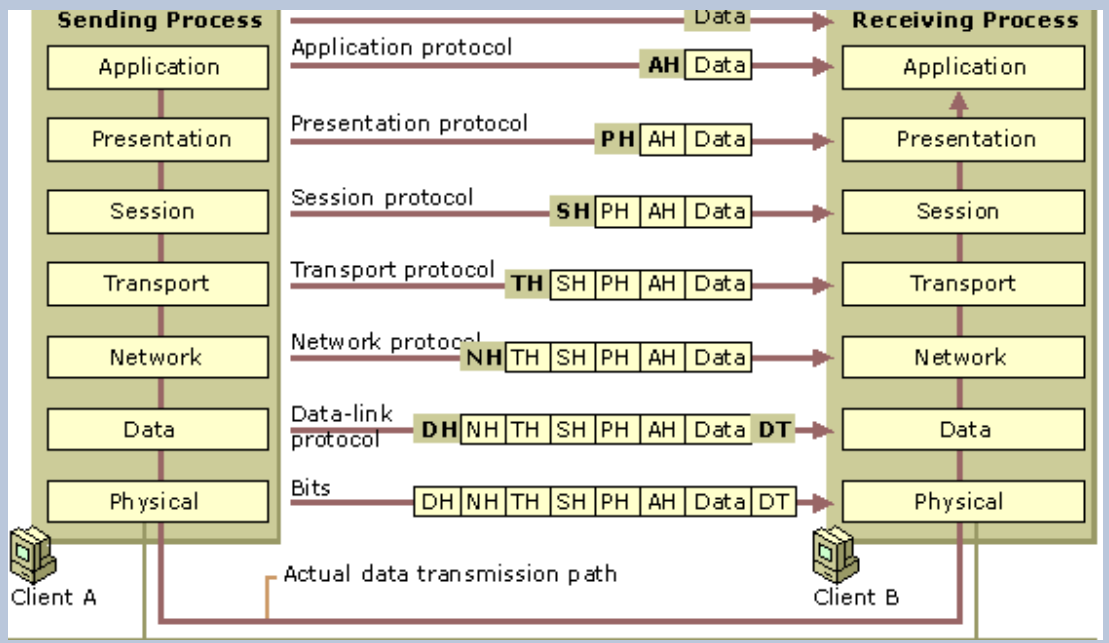
OSI model: Data Link (Layer 2)

- Uses Layer 2 address (the media access control (MAC) address) to identifying the network interface on the network so communications can get from one system to another on the local network.
- The Address Resolution Protocol (ARP), virtual local area networks (VLANs), Ethernet, and Frame Relay are Data Link layer protocols.
- They take care of formatting the data to be sent out on the transmission medium.

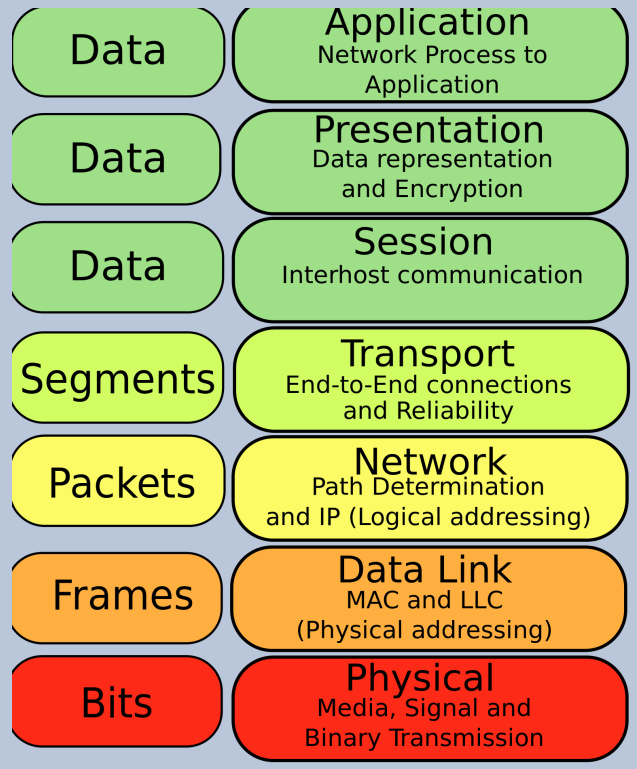
OSI model: Physical (Layer 1)

- In this layer, bits leave one end using the physical medium (wired or wireless) to reach another endpoint.
- This is all the protocols that manage the physical communications. 10BaseT, 10Base2, 100BaseTX, and 1000BaseT are all examples of Physical layer protocols.
- They dictate how the pulses are handled.

OSI Data format structure: Encapsulation



Encapuslation

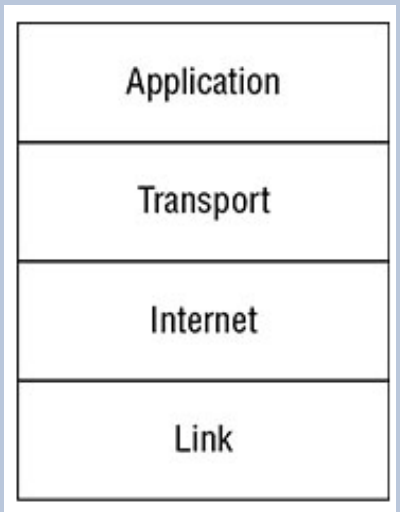


Data form

Data format

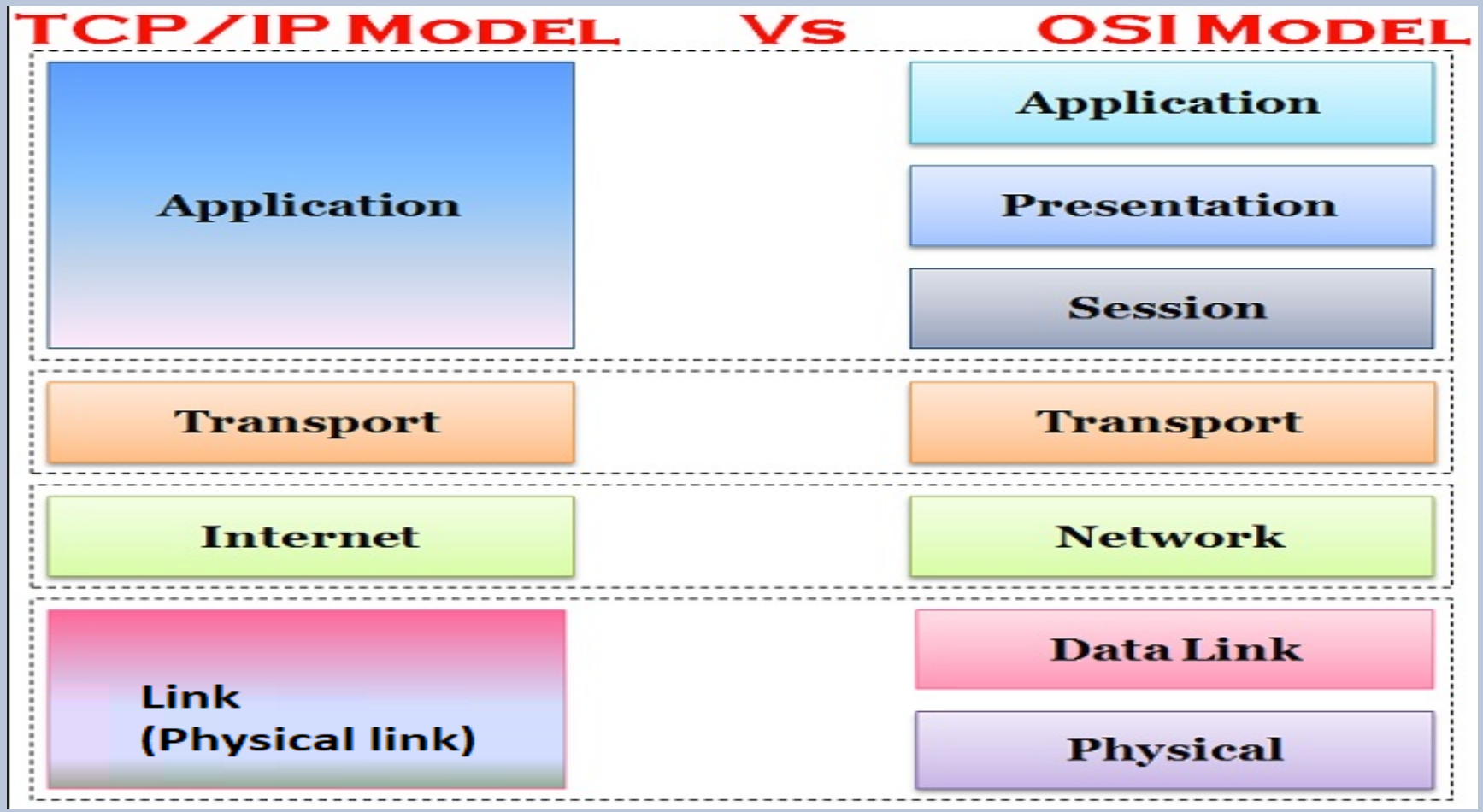
Four Layers of the TCP/IP model

- OSI had to be abstract and flexible in order to accommodate a wide variety of protocols and designs.
- TCP/IP, on the other hand, as an as-built definition, is only four layers.
- The TCP/IP architecture is a much simpler design than the OSI model.



- Session, Presentation, and Application layers from the OSI model are collapsed into the **Application layer**.
- **Transport layer** is the same in both models.
- The **Internet** and Network layers are named and function very similarly
- Physical and Data Link layers from the OSI model are collapsed into the **Link layer** in the TCP/IP model

TCP/IP Vs OSI Model

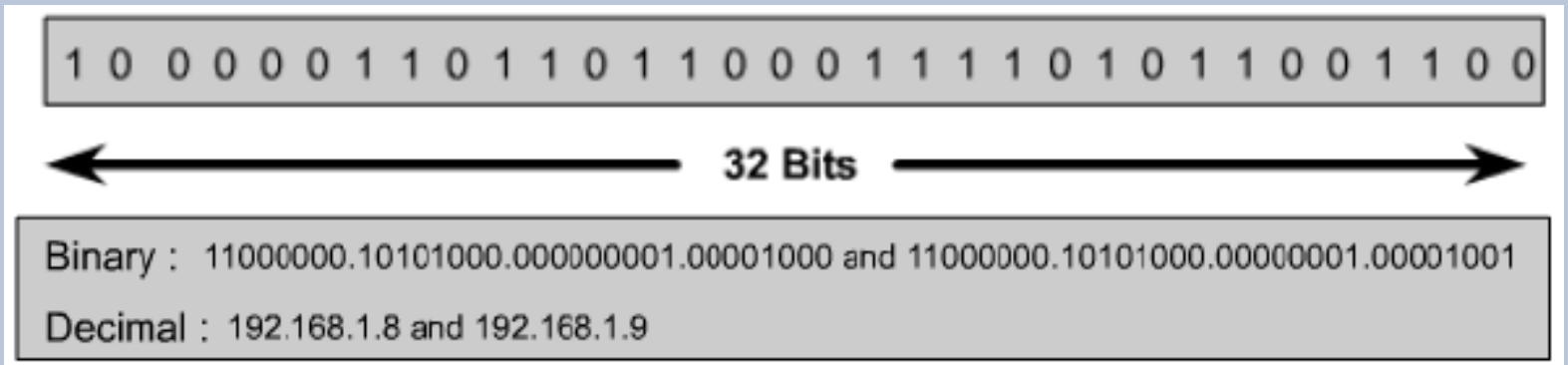


Addressing Requirements

- Two levels of addressing required
  1. each host on a subnet needs a unique global network address
     - This is its **Internet protocol address (IP)**
  2. each application on a (multi-tasking) host needs a unique address port within the host
     - This is known as a **port**
  3. For each communication to succeed it uses the two addresses together:
     - The IP address is needed to reach a specific host
     - The port number if needed for the device to identify what type of communication is this (what services it needs to run)
     - For example an email received using POP3 protocol will use port 110

IP addressing version 4 (IPv4)

- An IP address is a 32-bit sequence of 1s and 0s.
- To make the IP address easier to use, the address is usually written as four decimal numbers separated by periods.
- This way of writing the address is called the dotted decimal format.



IP classes

Address Class	Number of Networks	Number of Host per Network
A	126 *	16,777,216
B	16, 384	65,535
C	2,097,152	254
D (Multicast)	N/A	N/A

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

* The 127.x.x.x address range is reserved as a loopback address, used for testing and diagnostic purposes.

Default IP Addresses format for classes

- A network address: is an IP address that is used to locate a specific network. The network usually contains several devices, all belonging to it.
- A broadcast address: It is used when we want to either send datagram to all devices on the network or when we want the message to be processed only by a single specific device - but we do not know the address of that device, so the only solution is to send the message to everyone and hope that the specific device receives the broadcast as well.
- A Subnet address: Sometimes we need to divide a network into several sub networks. For this, each network will have a subnet address that specifies which subnet it belongs to. If we use the default subnet address, it means we did not divide the network into different subnets.

Default IP Addresses format for classes

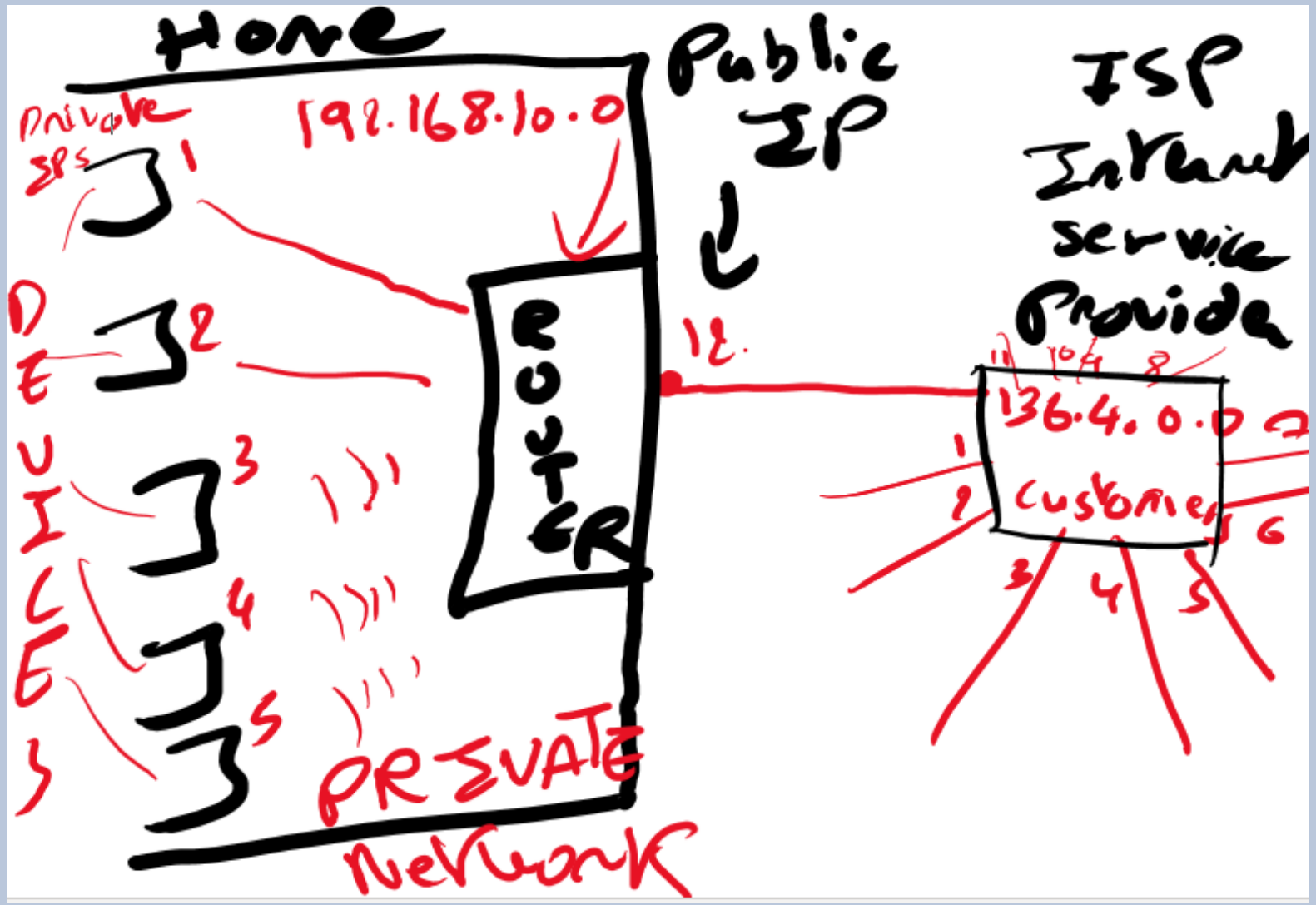
- In a network , a default network IP address is when:
  - All **host bits** are **0**
- In a network , a default broadcast IP address is when:
  - All **host bits** are **1**
- In a network , a default subnet address is when:
  - All **network bits** are **1**
  - All **host bits** are **0**

Public and Private IP Addresses

- No two machines that connect to a public network can have the same IP address because public IP addresses are global and standardized.
- However, private networks may use any host addresses, as long as each host within the private network is unique.
- RFC 1918 sets aside three blocks of IP addresses for private, internal use.
- Connecting a network using private addresses to the Internet requires translation of the private addresses to public addresses using Network Address Translation (NAT).
-

Class	RFC 1918 Internal Address Range
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

Public and Private IP Addresses Example



Network addressing requirements

- For devices to be able to communicate within a network they need to have:
  - Each needs to be allocated a unique IP address within the network range.
  - The same network address
  - The same broadcast address
  - The same subnet address

Example of addressing for a network

- Consider a device with an IP address 192.168.10.4
  1. What class is this IP address?
     - We look at the first part of the IP.
     - 192 $\Rightarrow$: This is class C
  2. What is the default network address for this device?
     - Class C $\Rightarrow$ N.N.N.H
     - Network address $\Rightarrow$ All host bits are 0: $\Rightarrow$ 192.168.10.0
  3. What is the default network address for this device?
     - Class C $\Rightarrow$ N.N.N.H
     - Broadcast address $\Rightarrow$ All host bits are 1: $\Rightarrow$ 192.168.10.255
  4. What is the default subnet address for this device?
     - Class C $\Rightarrow$ N.N.N.H
     - Subnet address $\Rightarrow$ All Network bits are 1 and all host bits are 0: $\Rightarrow$ 255.255.255.0
- More examples in tutorial

References

- Resources used:
  - Chapter 1 of the book CEHv10 Certified Ethical Hacker study guide Networks by Ric Messier, published by Sybex 2019. Click here for the online book Library link
- Recommended Readings
  - I suggest you look in the library for a computer networks book and read about the network infrastructure.