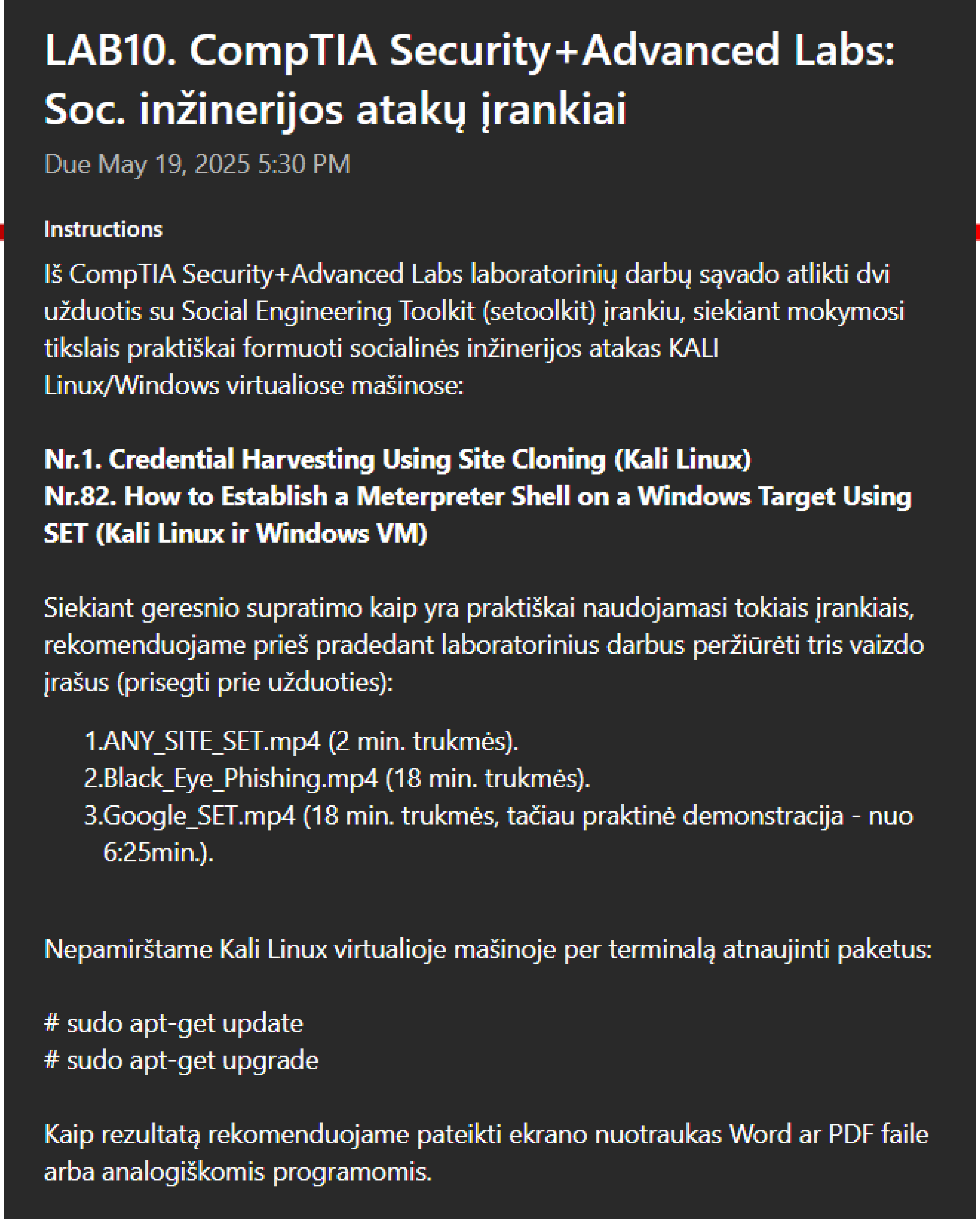
Cyber Security
Lession 22

Assignments



LAB10. CompTIA Security+Advanced Labs: Soc. inžinerijos atakų įrankiai

Due May 19, 2025 5:30 PM

Instructions

Iš CompTIA Security+Advanced Labs laboratorinių darbų sąvado atlikti dvi užduotis su Social Engineering Toolkit (setoolkit) įrankiu, siekiant mokymosi tikslais praktiškai formuoti socialinės inžinerijos atakas KALI Linux/Windows virtualiose mašinose:

Nr.1. Credential Harvesting Using Site Cloning (Kali Linux)
Nr.82. How to Establish a Meterpreter Shell on a Windows Target Using SET (Kali Linux ir Windows VM)

Siekiant geresnio supratimo kaip yra praktiškai naudojamasi tokiais įrankiais, rekomenduojame prieš pradedant laboratorinius darbus peržiūrėti tris vaizdo įrašus (prisegti prie užduoties):

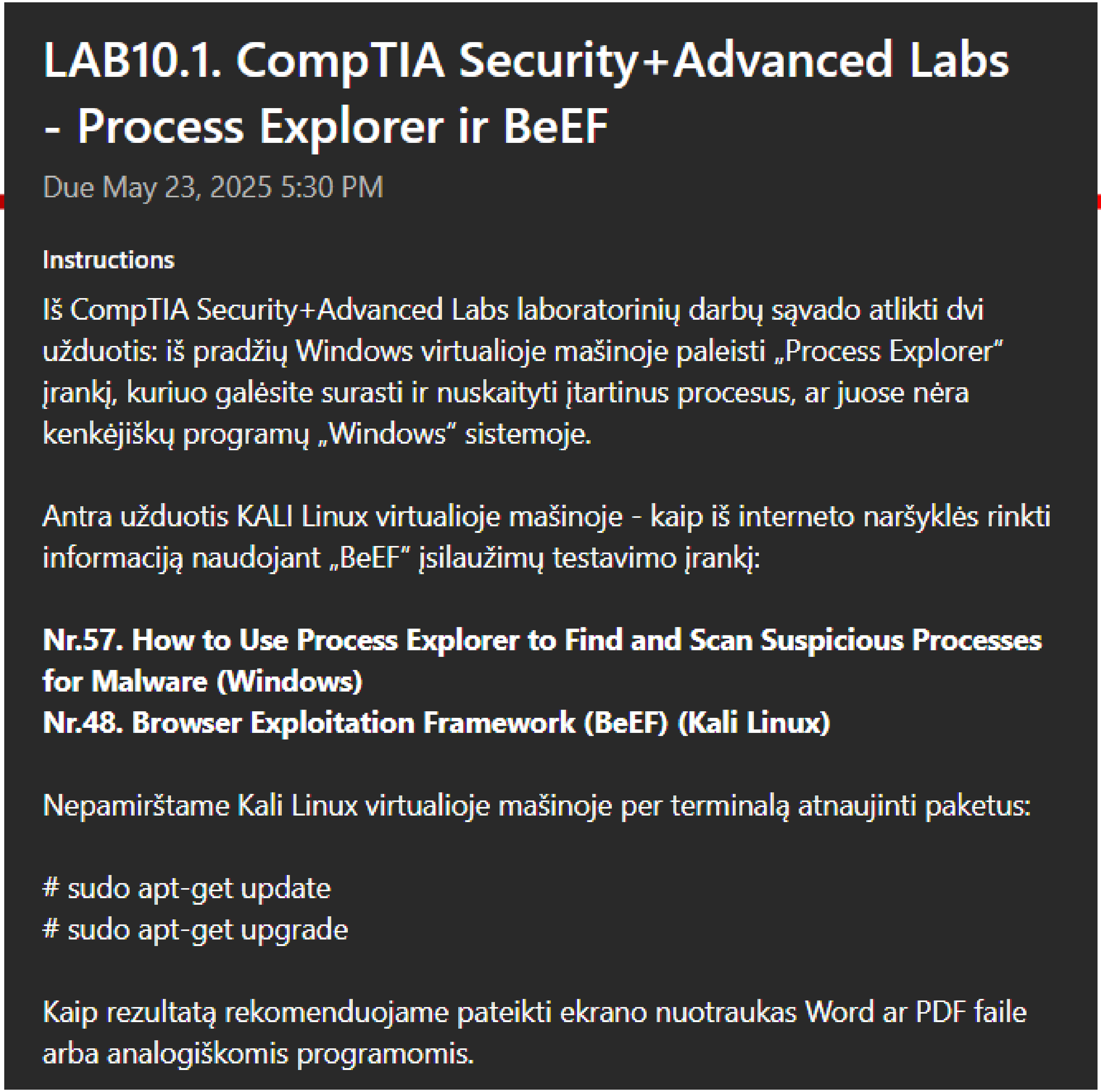
1. ANY_SITE_SET.mp4 (2 min. trukmės).
2. Black_Eye_Phishing.mp4 (18 min. trukmės).
3. Google_SET.mp4 (18 min. trukmės, tačiau praktinė demonstracija - nuo 6:25min.).

Nepamirštame Kali Linux virtualioje mašinoje per terminalą atnaujinti paketus:

```
# sudo apt-get update
# sudo apt-get upgrade
```

Kaip rezultatą rekomenduojame pateikti ekrano nuotraukas Word ar PDF faile arba analogiškomis programomis.

Assignments



LAB10.1. CompTIA Security+Advanced Labs - Process Explorer ir BeEF

Due May 23, 2025 5:30 PM

Instructions

Iš CompTIA Security+Advanced Labs laboratorinių darbų sąvado atlikti dvi užduotis: iš pradžių Windows virtualioje mašinoje paleisti „Process Explorer“ įrankį, kuriuo galėsite surasti ir nuskaityti įtartinus procesus, ar juose nėra kenkėjiškų programų „Windows“ sistemoje.

Antra užduotis KALI Linux virtualioje mašinoje - kaip iš interneto naršyklės rinkti informaciją naudojant „BeEF“ įsilaužimų testavimo įrankį:

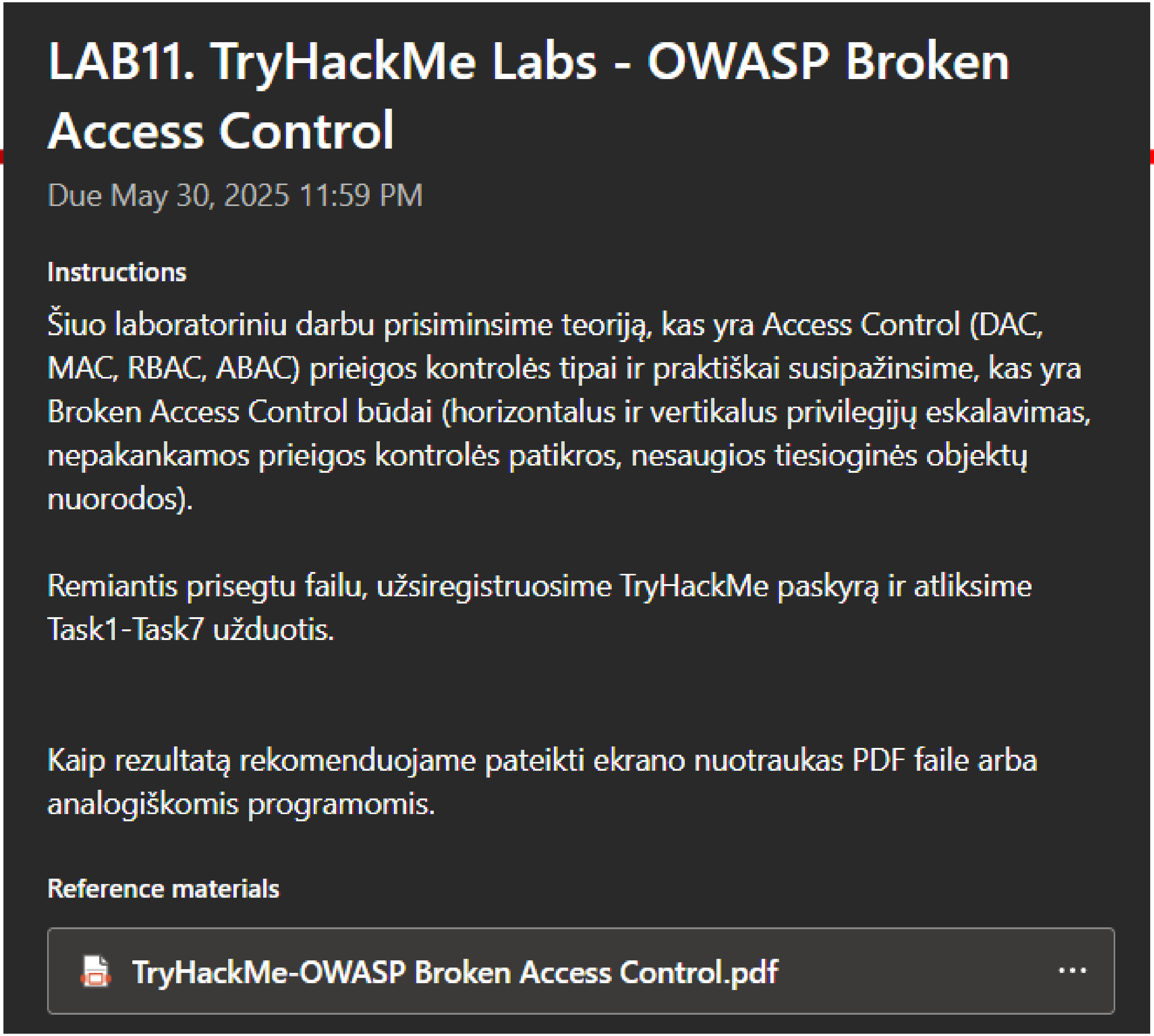
Nr.57. How to Use Process Explorer to Find and Scan Suspicious Processes for Malware (Windows)
Nr.48. Browser Exploitation Framework (BeEF) (Kali Linux)

Nepamirštame Kali Linux virtualioje mašinoje per terminalą atnaujinti paketus:

```
# sudo apt-get update
# sudo apt-get upgrade
```

Kaip rezultatą rekomenduojame pateikti ekrano nuotraukas Word ar PDF faile arba analogiškomis programomis.

Assignments



LAB11. TryHackMe Labs - OWASP Broken Access Control

Due May 30, 2025 11:59 PM

Instructions

Šiuo laboratoriniu darbu prisiminsime teoriją, kas yra Access Control (DAC, MAC, RBAC, ABAC) prieigos kontrolės tipai ir praktiškai susipažinsime, kas yra Broken Access Control būdai (horizontalus ir vertikalus privilegijų eskalavimas, nepakankamos prieigos kontrolės patikros, nesaugios tiesioginės objektų nuorodos).

Remiantis prisegtu failu, užsiregistruosime TryHackMe paskyrą ir atliksime Task1-Task7 užduotis.

Kaip rezultatą rekomenduojame pateikti ekrano nuotraukas PDF faile arba analogiškomis programomis.

Reference materials

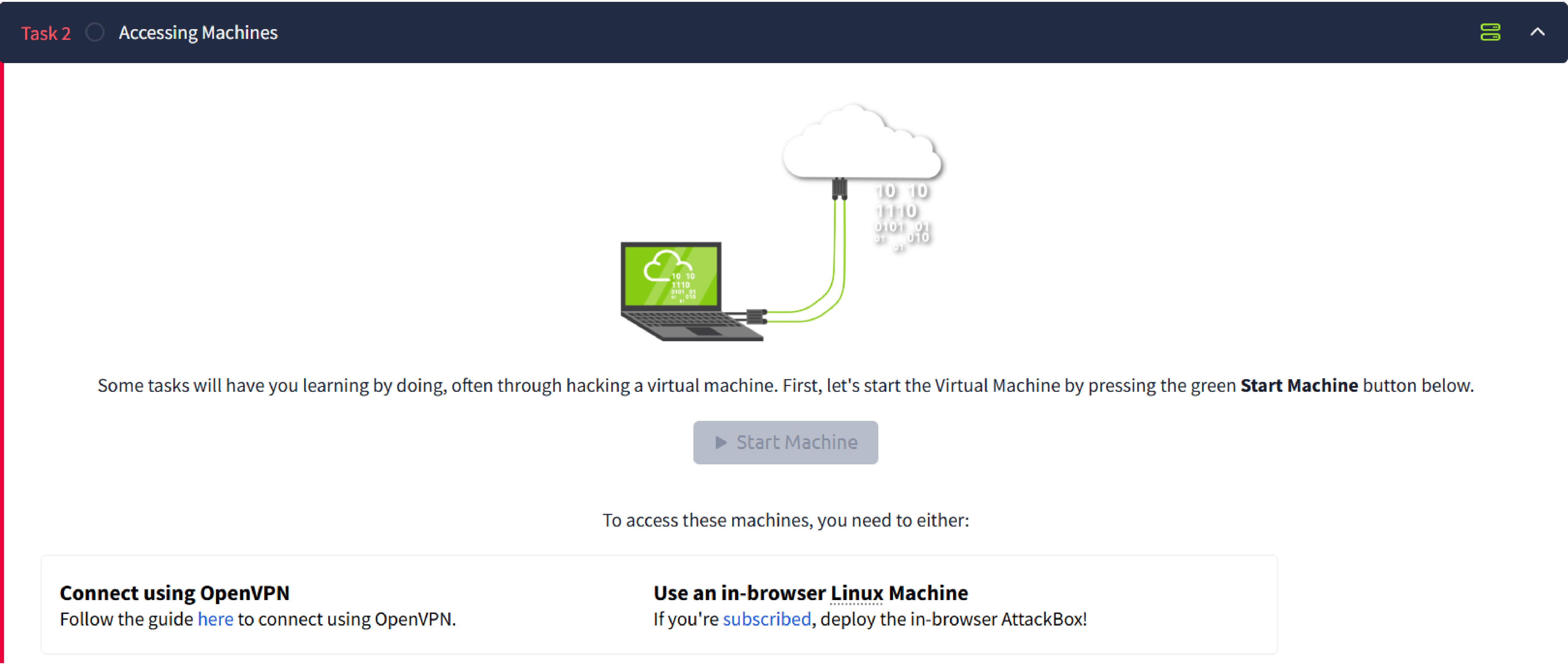
TryHackMe-OWASP Broken Access Control.pdf ···

This room breaks each OWASP topic down and includes details on the vulnerabilities, how they occur, and how you can exploit them. You will put the theory into practice by completing supporting challenges.

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging & Monitoring Failures
10. Server-Side Request Forgery (SSRF)

The room has been designed for beginners and assumes no previous security knowledge.

Labs



Task 2 ○ Accessing Machines

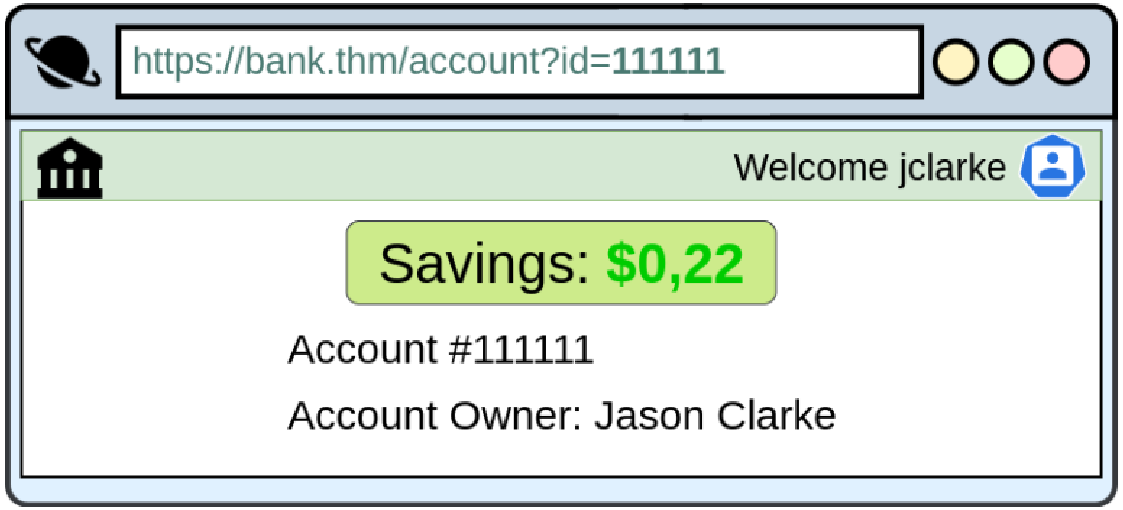
Some tasks will have you learning by doing, often through hacking a virtual machine. First, let's start the Virtual Machine by pressing the green **Start Machine** button below.

To access these machines, you need to either:

Connect using OpenVPN
Follow the guide here to connect using OpenVPN.

Use an in-browser Linux Machine
If you're subscribed, deploy the in-browser AttackBox!

Labs



https://bank.thm/account?id=111111

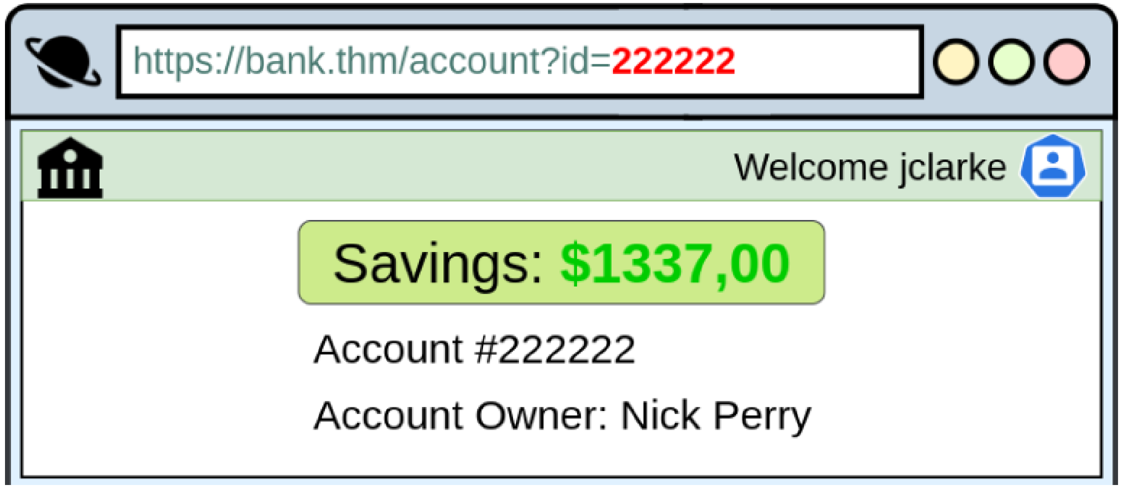
Welcome jclarke

Savings: $0,22

Account #111111

Account Owner: Jason Clarke

There is, however, a potentially huge problem here, anyone may be able to change the `id` parameter to something else like `222222`, and if the site is incorrectly configured, then he would have access to someone else's bank information.



https://bank.thm/account?id=222222

Welcome jclarke

Savings: $1337,00

Account #222222

Account Owner: Nick Perry

In the previous lession…

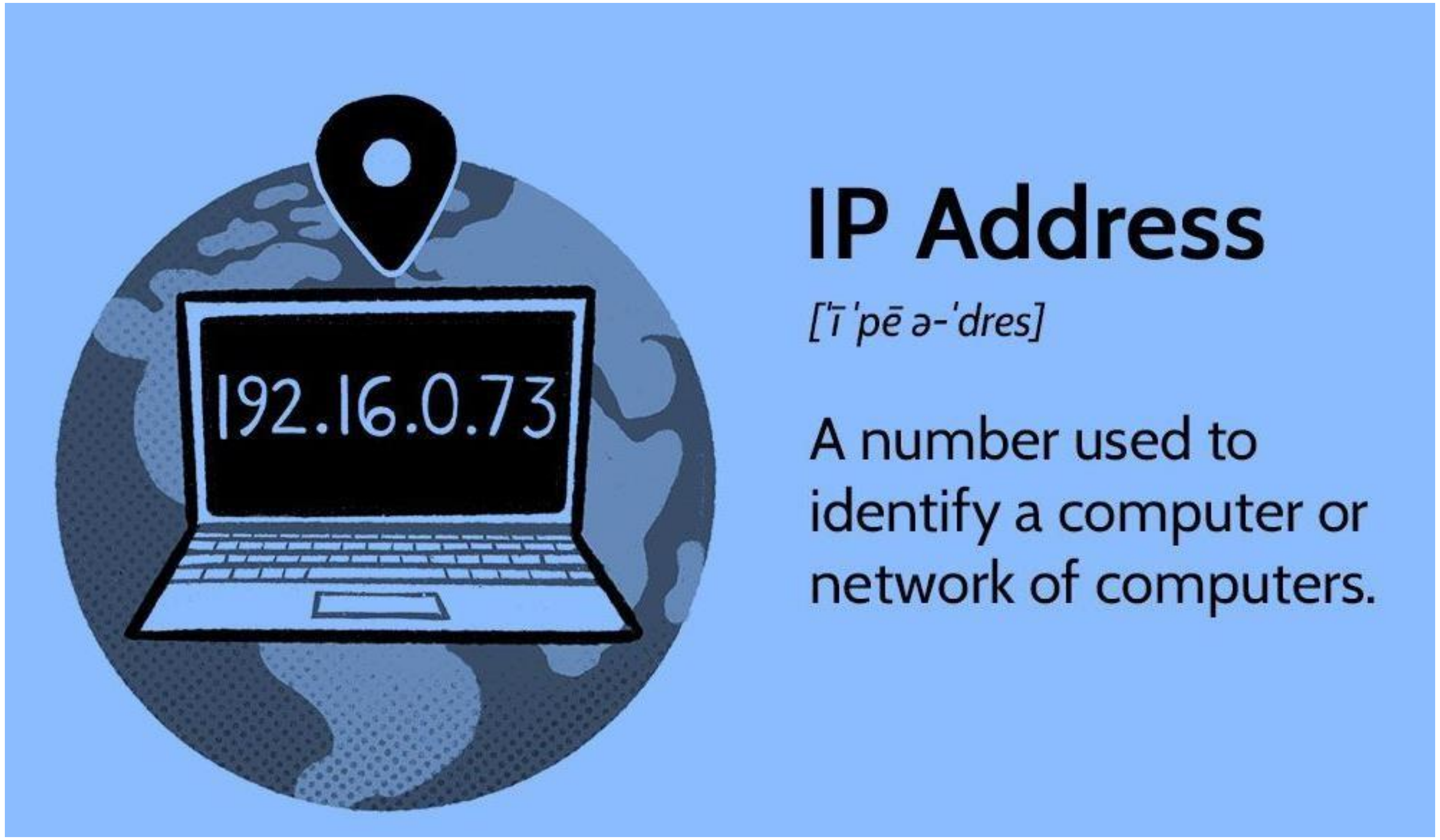
Exploring Network Technologies and Tools

(Chapter 4)

Introduction

- Reviewing Basic Networking Concepts DONE
- Basic Networking Protocols DONE
- Understanding Basic Network Devices
- Implementing Network Designs
- Routing and Switching

IP Address

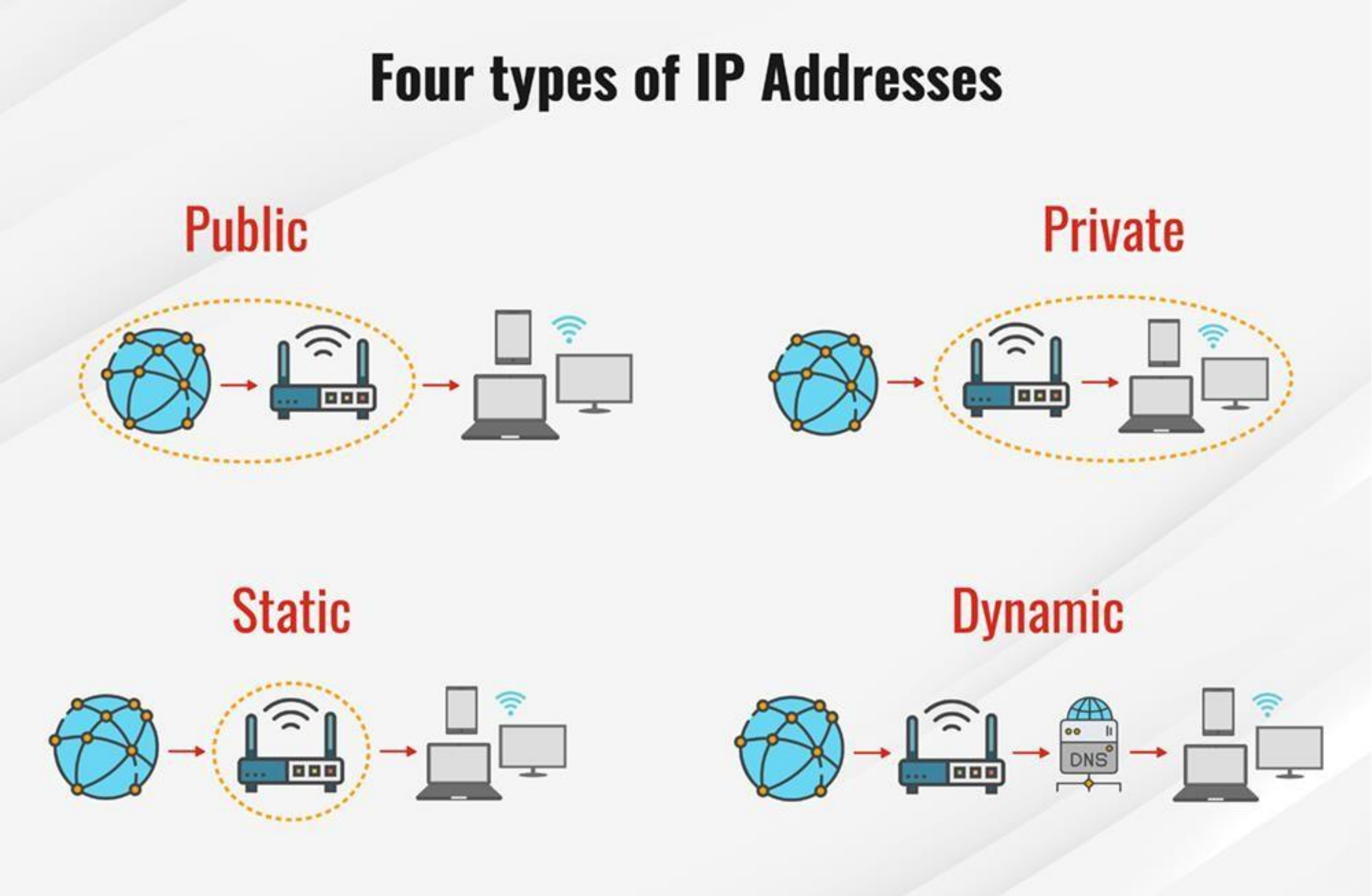


IP Address

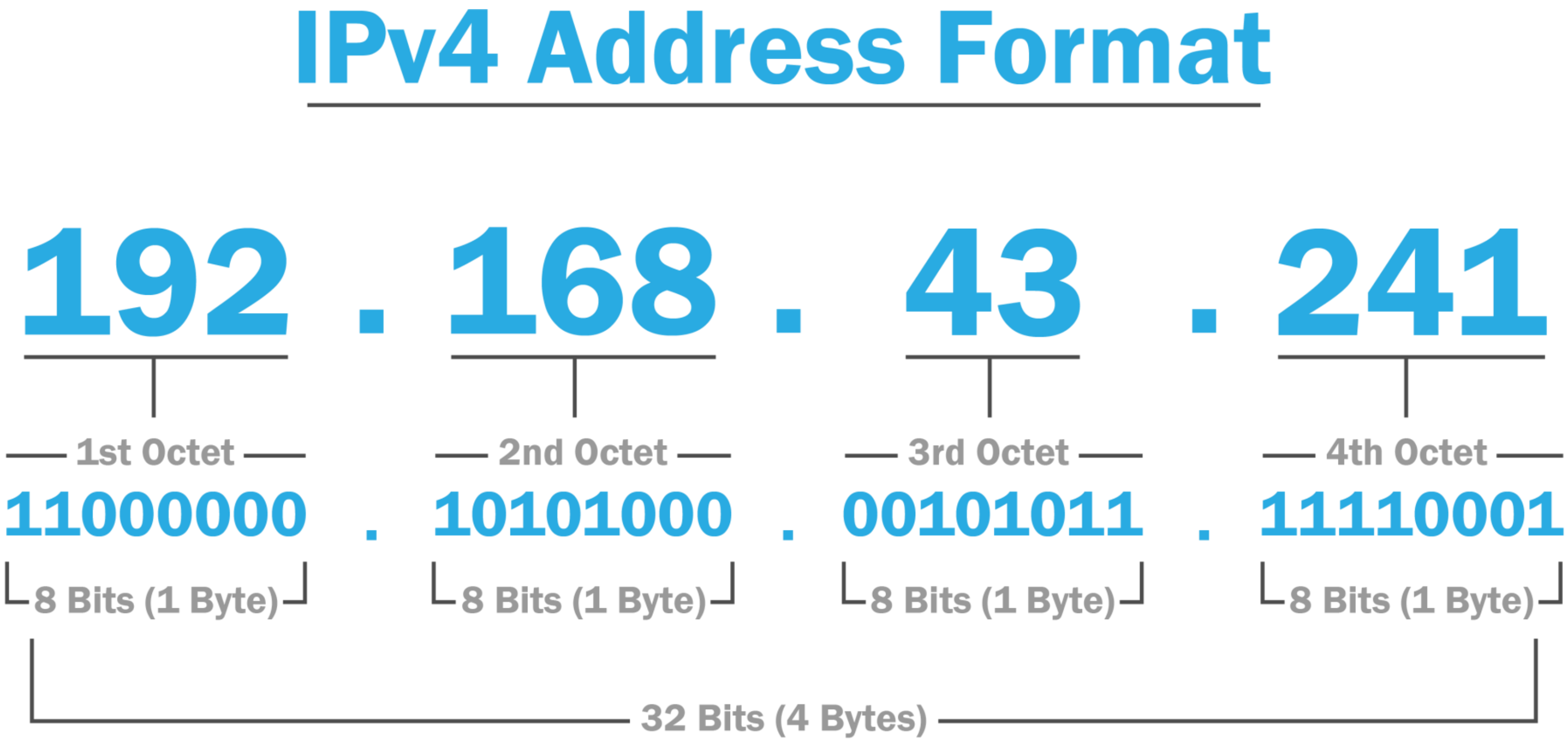
[ˈī ˈpē ə-ˈdres]

A number used to identify a computer or network of computers.

IP Address


Four types of IP Addresses
Public
Private
Static
Dynamic
DNS

IPv4



IPv4 Address Format

192 . 168 . 43 . 241

1st Octet — 11000000 — 8 Bits (1 Byte)

2nd Octet — 10101000 — 8 Bits (1 Byte)

3rd Octet — 00101011 — 8 Bits (1 Byte)

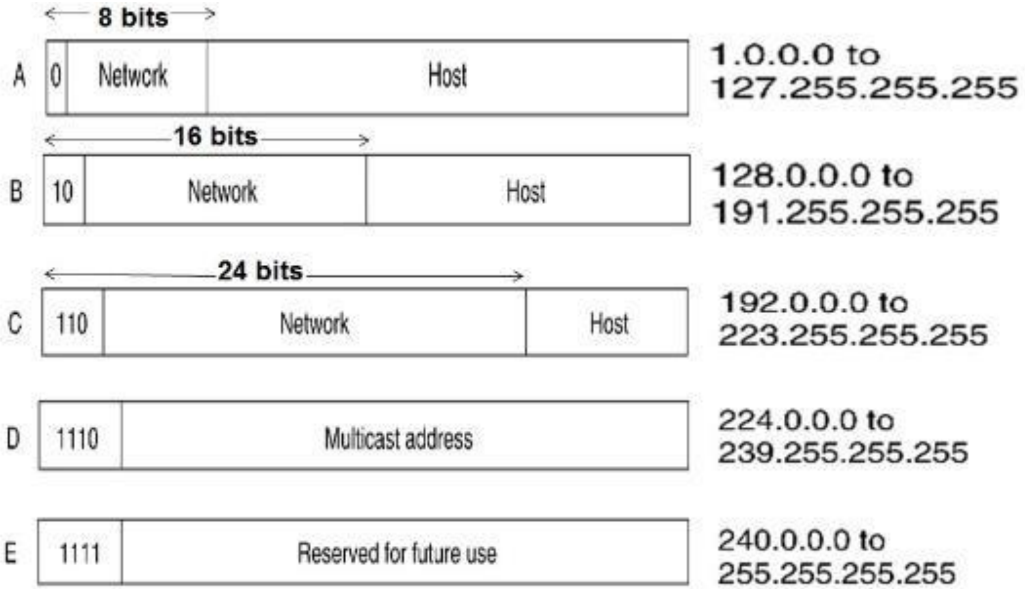
4th Octet — 11110001 — 8 Bits (1 Byte)

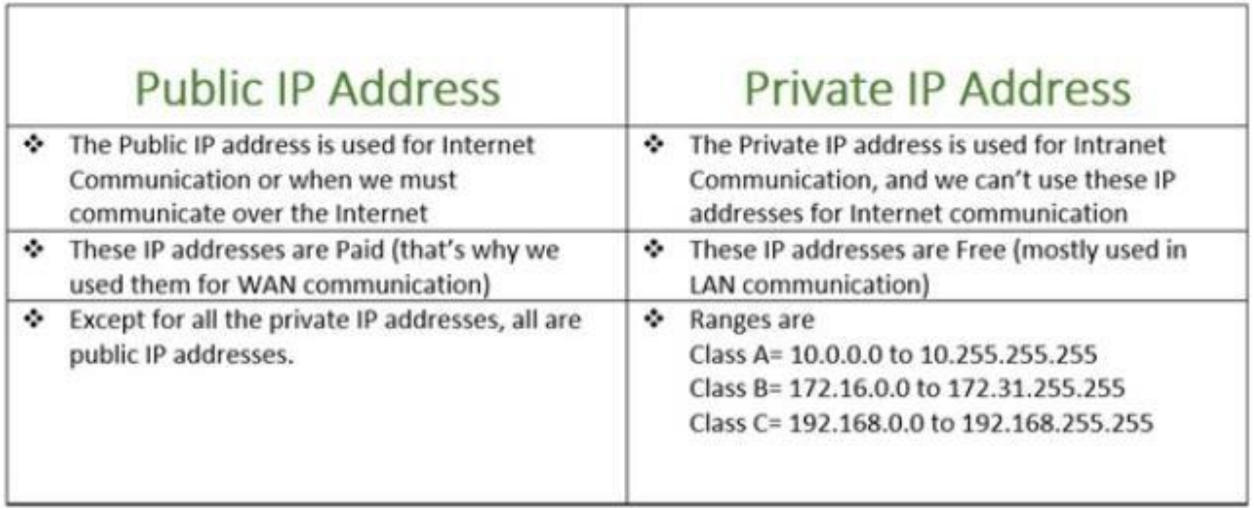
11000000 . 10101000 . 00101011 . 11110001

32 Bits (4 Bytes)

Classes

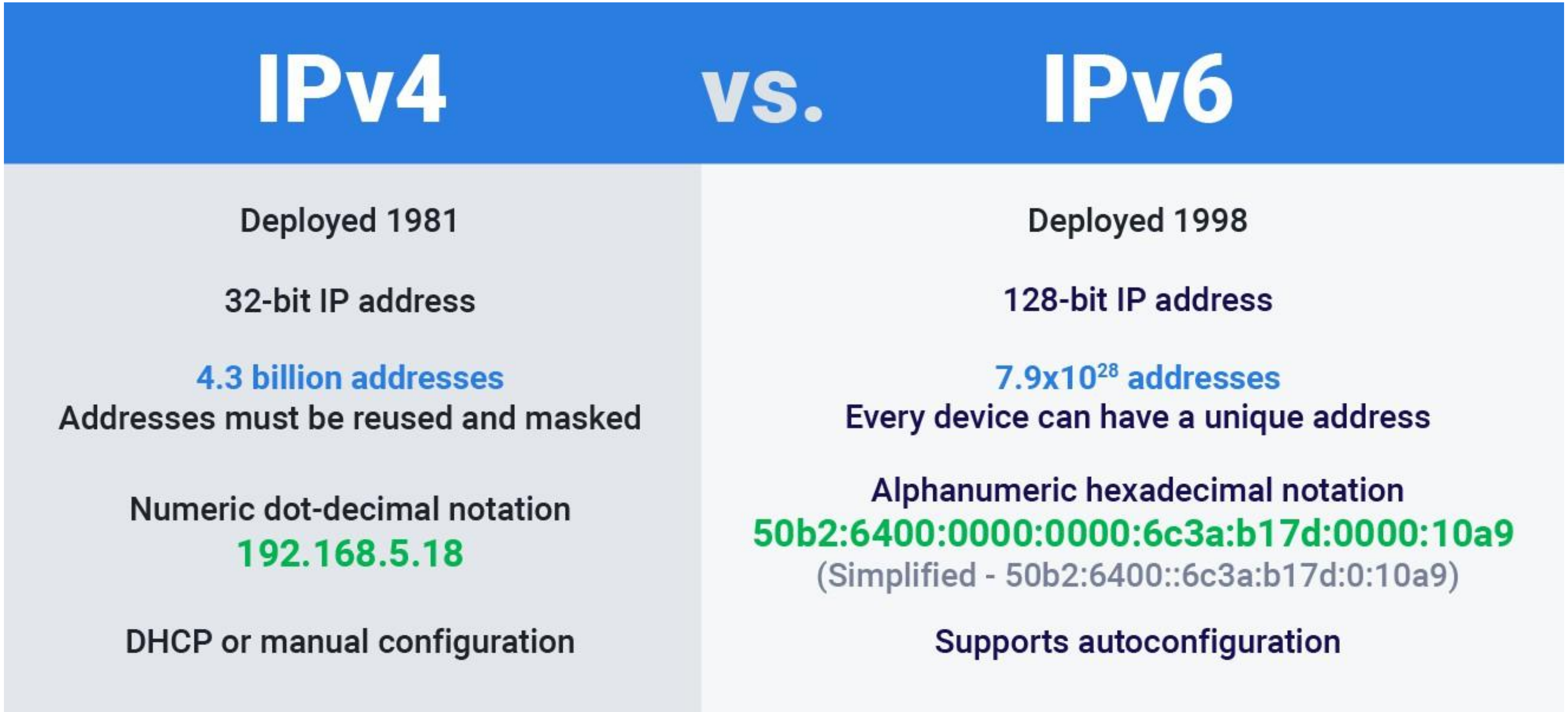
- Class A (0-127)
- Class B (128-191)
- Class C (192-223)
- Class D (224-239)
- Class E (240-255)





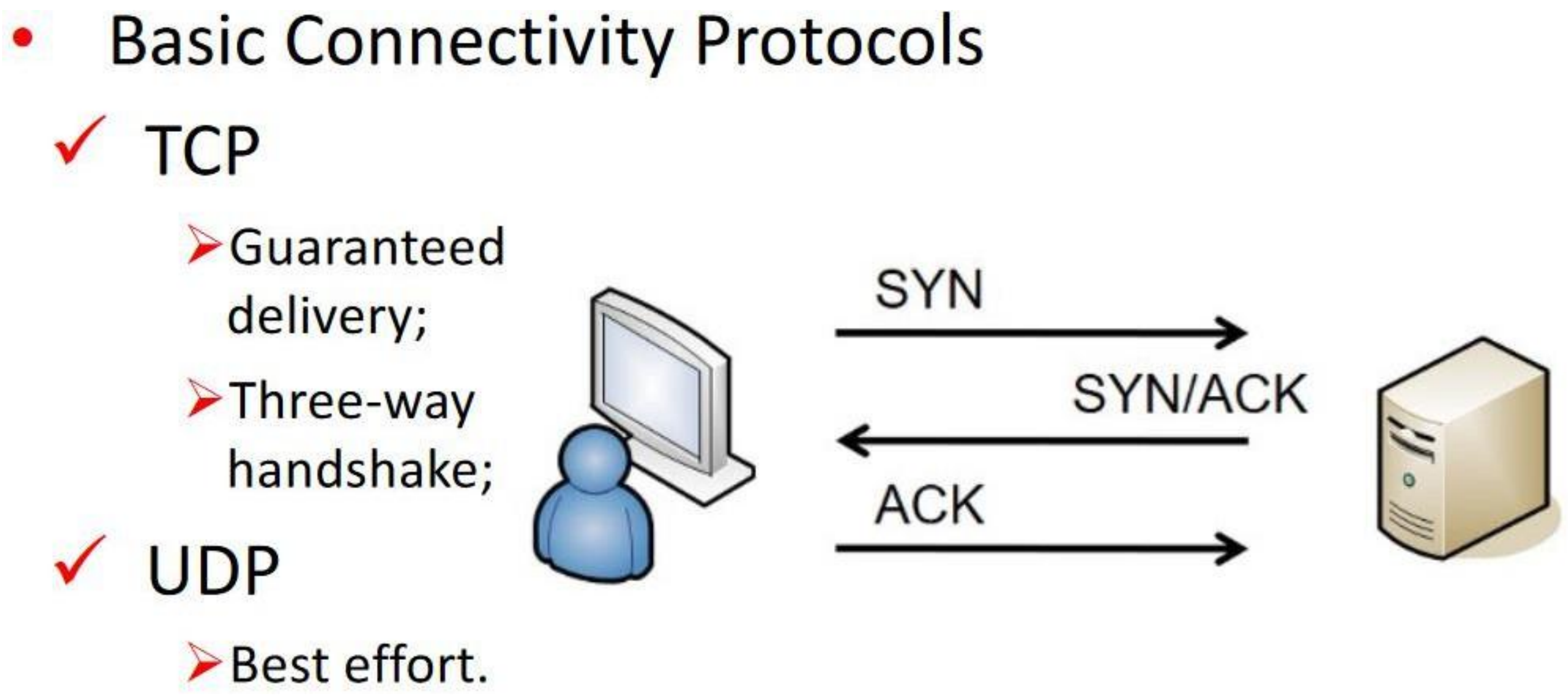
Public IP Address	Private IP Address
❖ The Public IP address is used for Internet Communication or when we must communicate over the Internet	❖ The Private IP address is used for Intranet Communication, and we can't use these IP addresses for Internet communication
❖ These IP addresses are Paid (that's why we used them for WAN communication)	❖ These IP addresses are Free (mostly used in LAN communication)
❖ Except for all the private IP addresses, all are public IP addresses.	❖ Ranges are Class A= 10.0.0.0 to 10.255.255.255 Class B= 172.16.0.0 to 172.31.255.255 Class C= 192.168.0.0 to 192.168.255.255

IPv4 vs IPv6



IPv4	vs.	IPv6
Deployed 1981		Deployed 1998
32-bit IP address		128-bit IP address
4.3 billion addresses Addresses must be reused and masked		$7.9x10^{28}$ addresses Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18		Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration		Supports autoconfiguration

Basic Networking Protocols

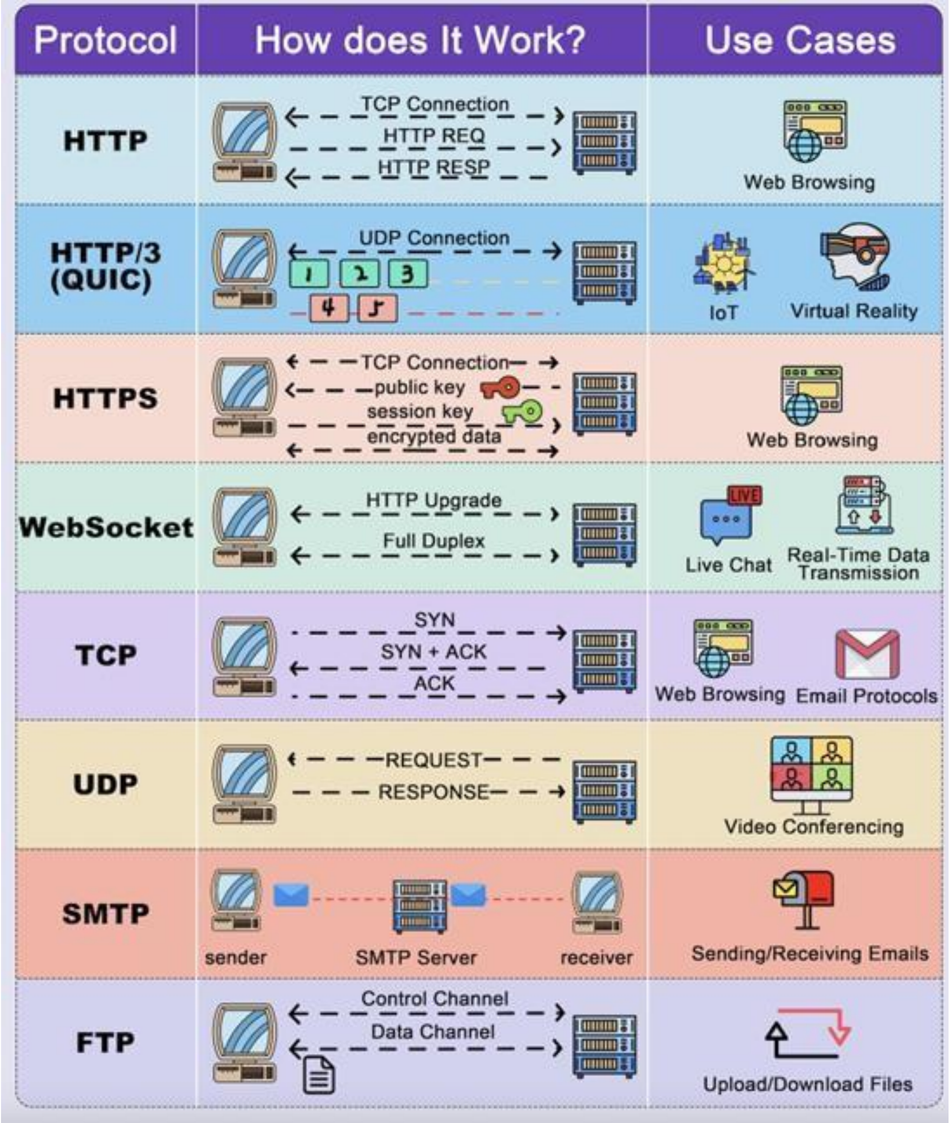


- Basic Connectivity Protocols
  - ✓ TCP
    - ➢ Guaranteed delivery;
    - ➢ Three-way handshake;
  - ✓ UDP
    - ➢ Best effort.

Basic Networking Protocols

- Reviewing Basic Connectivity Protocols
  - ✓ IPv4 and IPv6;
  - ✓ ICMP
    - ➢ Commonly blocked at firewalls;
    - ➢ If ping fails, ICMP may be blocked;
  - ✓ ARP
    - ➢ Resolves MAC addresses for IPv4.

8 most popular network protocols



Protocol	How does It Work?	Use Cases
HTTP	TCP Connection HTTP REQ HTTP RESP	Web Browsing
HTTP/3 (QUIC)	UDP Connection 1 2 3 4 5	IoT Virtual Reality
HTTPS	TCP Connection public key session key encrypted data	Web Browsing
WebSocket	HTTP Upgrade Full Duplex	LIVE Live Chat Real-Time Data Transmission
TCP	SYN SYN + ACK ACK	Web Browsing Email Protocols
UDP	REQUEST RESPONSE	Video Conferencing
SMTP	sender SMTP Server receiver	Sending/Receiving Emails
FTP	Control Channel Data Channel	Upload/Download Files

Exploring Network Technologies and Tools

(Chapter 4)

Lession 22

Introduction

- Reviewing Basic Networking Concepts DONE
- Basic Networking Protocols DONE
- Understanding Basic Network Devices
- Implementing Network Designs
- Routing and Switching

Understanding Basic Network Devices

Networks

- Networks connect computing devices together so that users can share resources, such as data, printers, and other devices;
- Any device with an IP address is a host, but you’ll often see them referred to as clients or nodes.

Addressing

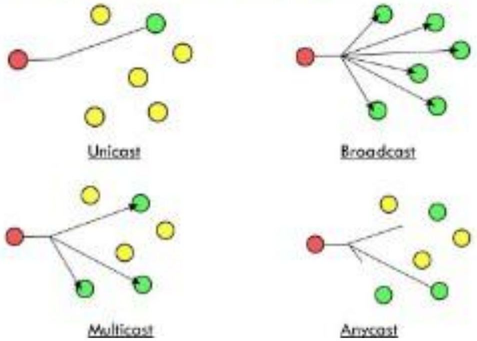
- Computer networks enabled several devices to communicate with each other across the world;
- This communication, however, is not simple and relies on various technical resources, from physical to logical, to occur;
- In particular, addressing messages with the proper method is crucial to designing and developing communication systems;
- The adequate adoption of these methods may guarantee efficient communication among connected devices;
- The incorrect use of them can result in overloaded networks and security problems;
- Addressing a message means determining to which destination a source wants to communicate;
- Each addressing method has specific characteristics (the number of receivers, reserved addresses in network protocols, routing strategies, final applications and etc.);
- The most relevant of these methods are :

✓ Unicast;

✓ Broadcast;

✓ Multicast;

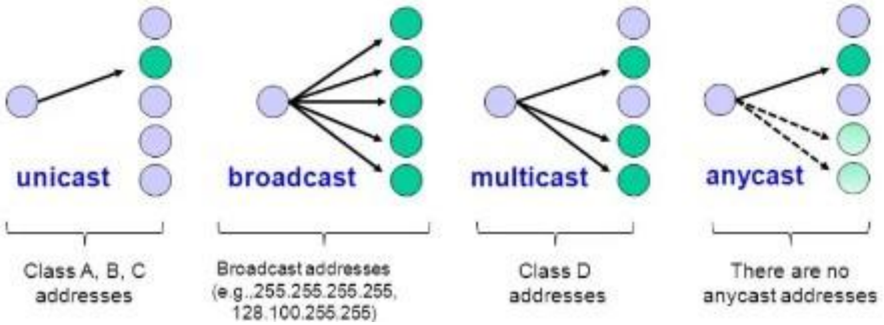
✓ Anycast.



Addressing methods

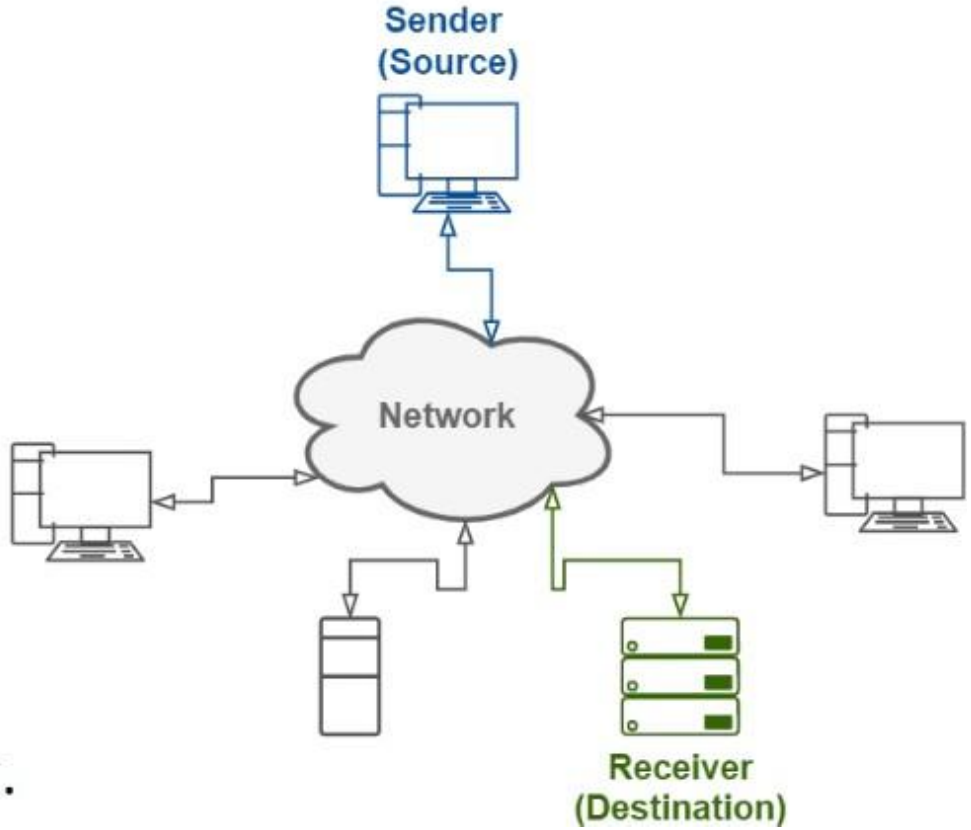
- **Unicast**
  - ✓ Is a type of communication where data is sent from one computer to another computer;
  - ✓ There is only one sender, and one receiver.
- **Broadcast**
  - ✓ Is a type of communication where data is sent from one computer once and a copy of that data will be forwarded to all the devices;
  - ✓ There is only one sender and the Broadcast data is sent only once, but the data is delivered to all connected devices.
- **Multicast**
  - ✓ Is a type of communication where multicast traffic addressed for a group of devices on the network;
  - ✓ IP multicast traffic are sent to a group and only members of that group receive and/or process the Multicast traffic;
  - ✓ Devices which are interested in a particular Multicast traffic must join to that Multicast group to receive the traffic;
  - ✓ IP Multicast Groups are identified by Multicast IP Addresses (IPv4 Class D Addresses);
  - ✓ In Multicast, the sender transmit only one copy of data and it is delivered and/or processed to many devices (Not as delivered and processed by all devices as in Broadcast) who are interested in that traffic.
- **Anycast**
  - ✓ Is a network addressing and routing methodology in which datagrams from a single sender are routed to the topologically nearest node in a group of potential receivers, though it may be sent to several nodes, all identified by the same destination address.

- Supported by IPv4
  - one-to-one (unicast)
  - one-to-all (broadcast)
  - one-to-many (multicast)
- Not supported by IPv4:
  - one-to-any (anycast)


unicast
broadcast
multicast
anycast
Class A, B, C addresses
Broadcast addresses (e.g.,255.255.255.255, 128.100.255.255)
Class D addresses
There are no anycast addresses

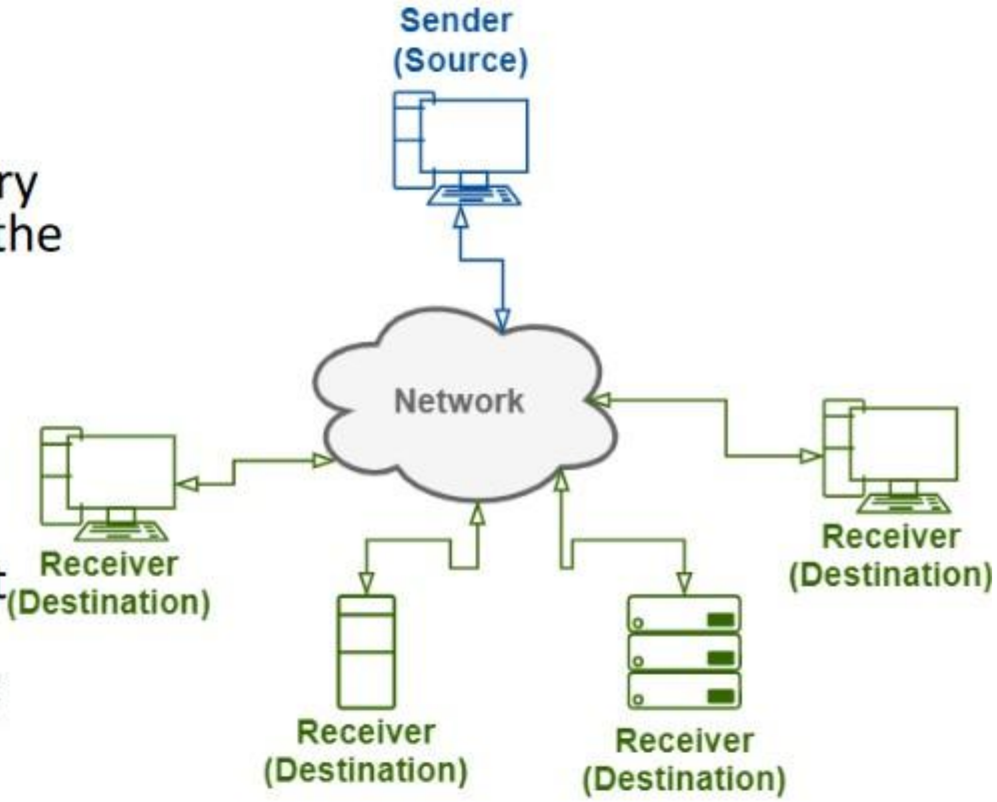
Unicast

- The unicast addressing method indicates that communication through a network involves a unique sender (source) and a single receiver (destination);
- Thus, addressing messages with the unicast method supposes private communication;
- Since other entities can intercept the messages, employing unicast addressing doesn't guarantee private communication in the network.



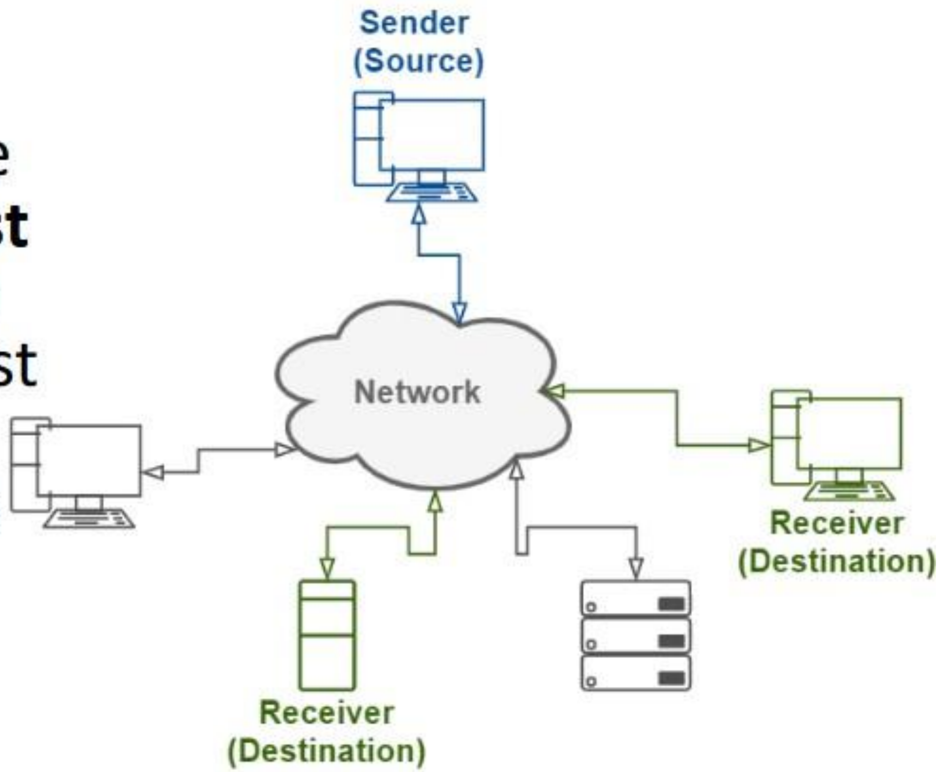
Broadcast

- Considers the communication through a network that involves a single sender (source) and multiple receivers (destinations);
- By default, the broadcast receivers are every device connected to the same network as the sender;
- Broadcasting a message doesn't imply receiving a response from every device connected to the network. It is relevant to notice that, sometimes, it can happen;
- Usually, we receive response messages just from a subgroup of connected devices, a single device, or even receive no response;
- In most cases, broadcast messages aren't routed, being restricted to a single logical network sometimes broadcast domains may be necessary.



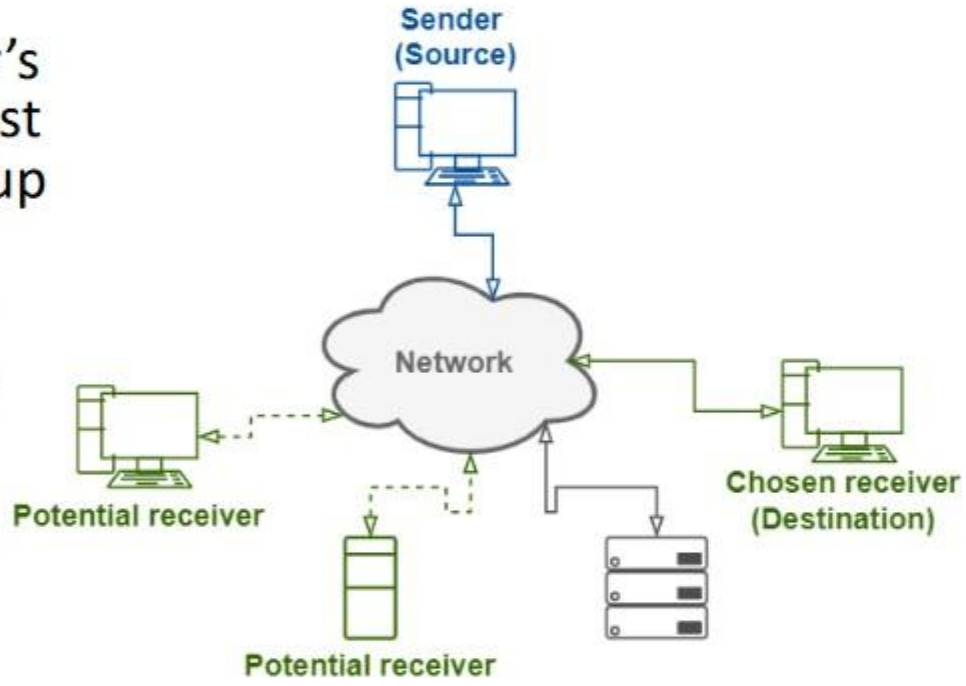
Multicast

- Addresses messages for a specific group of devices in a network;
- Even if a group contains all the devices in a network, **multicast is theoretically different from the broadcast** - in the multicast case, devices effectively subscribe to receive messages and in the broadcast case, however, devices receive messages regardless of whether or not they want to.



Anycast

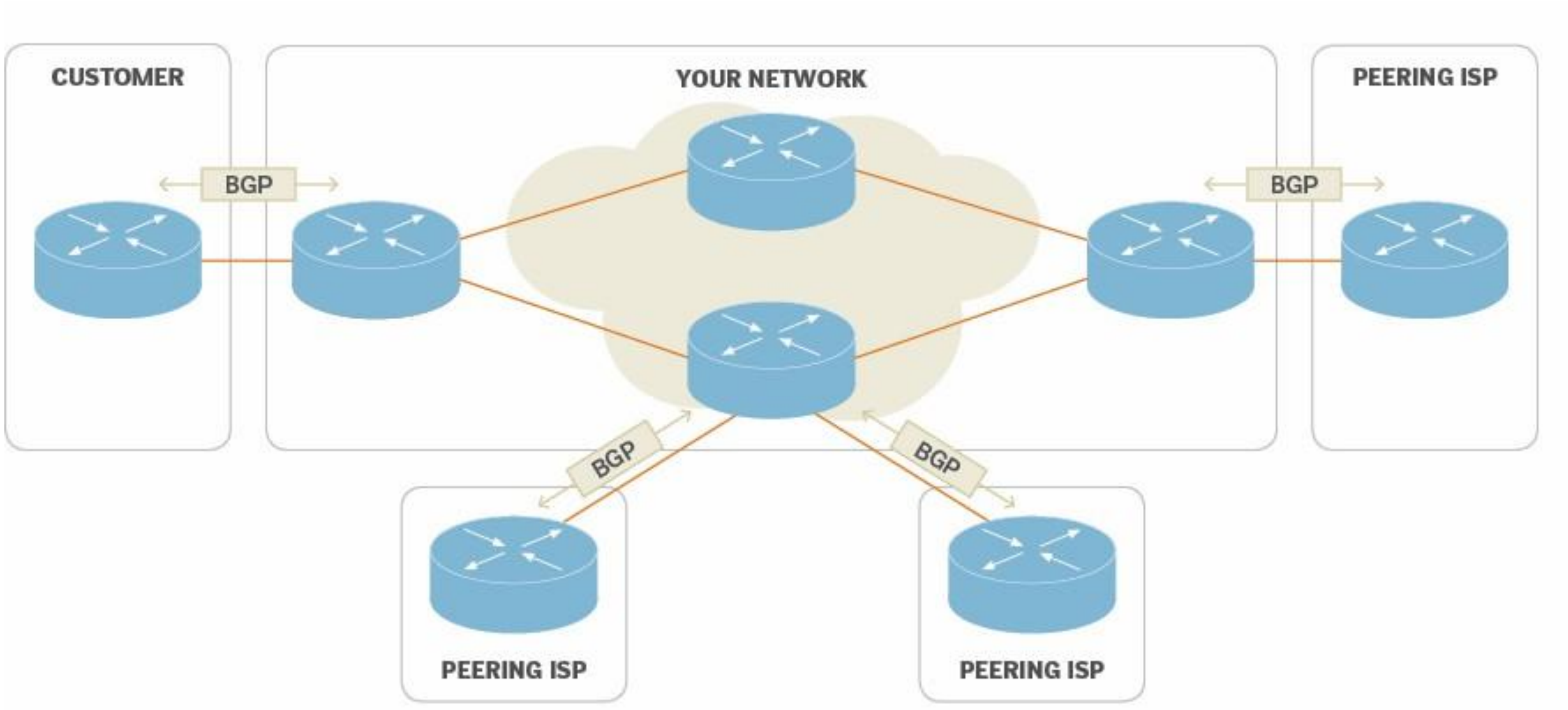
- Method forwards messages to a single device of a specific group of devices;
- Typically, considering the sender's position, the topologically nearest device of the aimed anycast group will receive the message;
- In practice, there is no exclusive address range for anycast. Thus, we form anycast groups by assigning the same unicast address to multiple devices in a network. Of course, we should configure the devices, thus making them aware of being members of an anycast group.



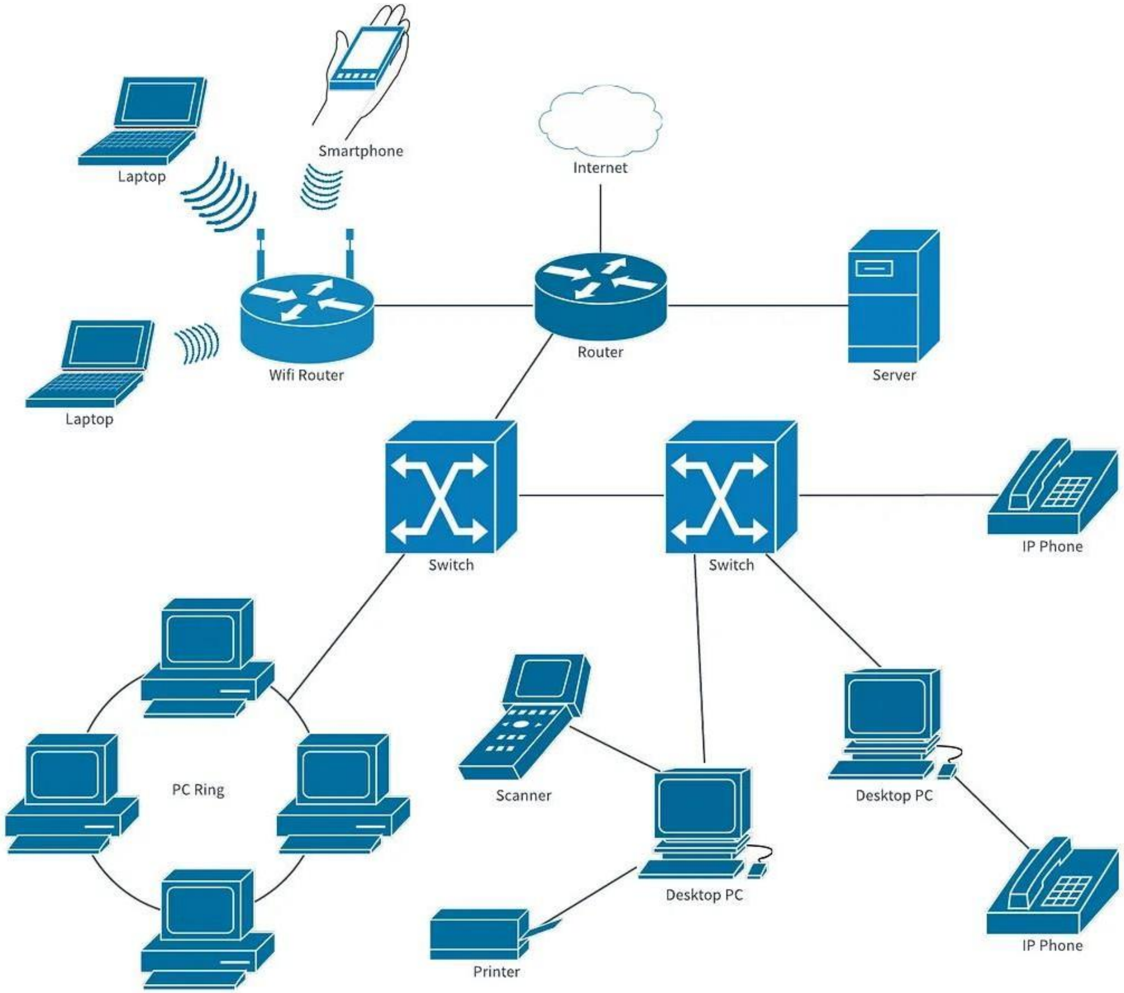
BGP

- Border Gateway Protocol (**BGP**) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (**AS**) on the Internet;
- BGP is classified as a path-vector routing protocol, and it makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator;
- Among routing protocols, BGP is unique in using TCP as its transport protocol;
- Process :
  - ✓ BGP neighbors, called peers, are established by manual configuration among routers to create a TCP session on port 179;
  - ✓ A BGP speaker sends 19-byte keep-alive messages every 30 seconds (protocol default value, tunable) to maintain the connection;
- Used for routing within an autonomous system is called Interior Border Gateway Protocol (iBGP, IBGP);
- When it runs between different autonomous systems, it is called External BGP (eBGP or Exterior Border Gateway Protocol);
- Routers on the boundary of one AS exchanging information with another AS are called border or edge routers or simply eBGP peers and are typically connected directly, while iBGP peers can be interconnected through other intermediate routers;
- Other deployment topologies are also possible, such as running eBGP peering inside a VPN tunnel, allowing two remote sites to exchange routing information in a secure and isolated manner;
- The main difference between iBGP and eBGP peering is in the way routes that were received from one peer are typically propagated by default to other peers:
  - ✓ New routes learned from an eBGP peer are re-advertised to all iBGP and eBGP peers;
  - ✓ New routes learned from an iBGP peer are re-advertised to all eBGP peers only;
- Route-propagation rules effectively require that all iBGP peers inside an AS are interconnected in a full mesh with iBGP sessions.

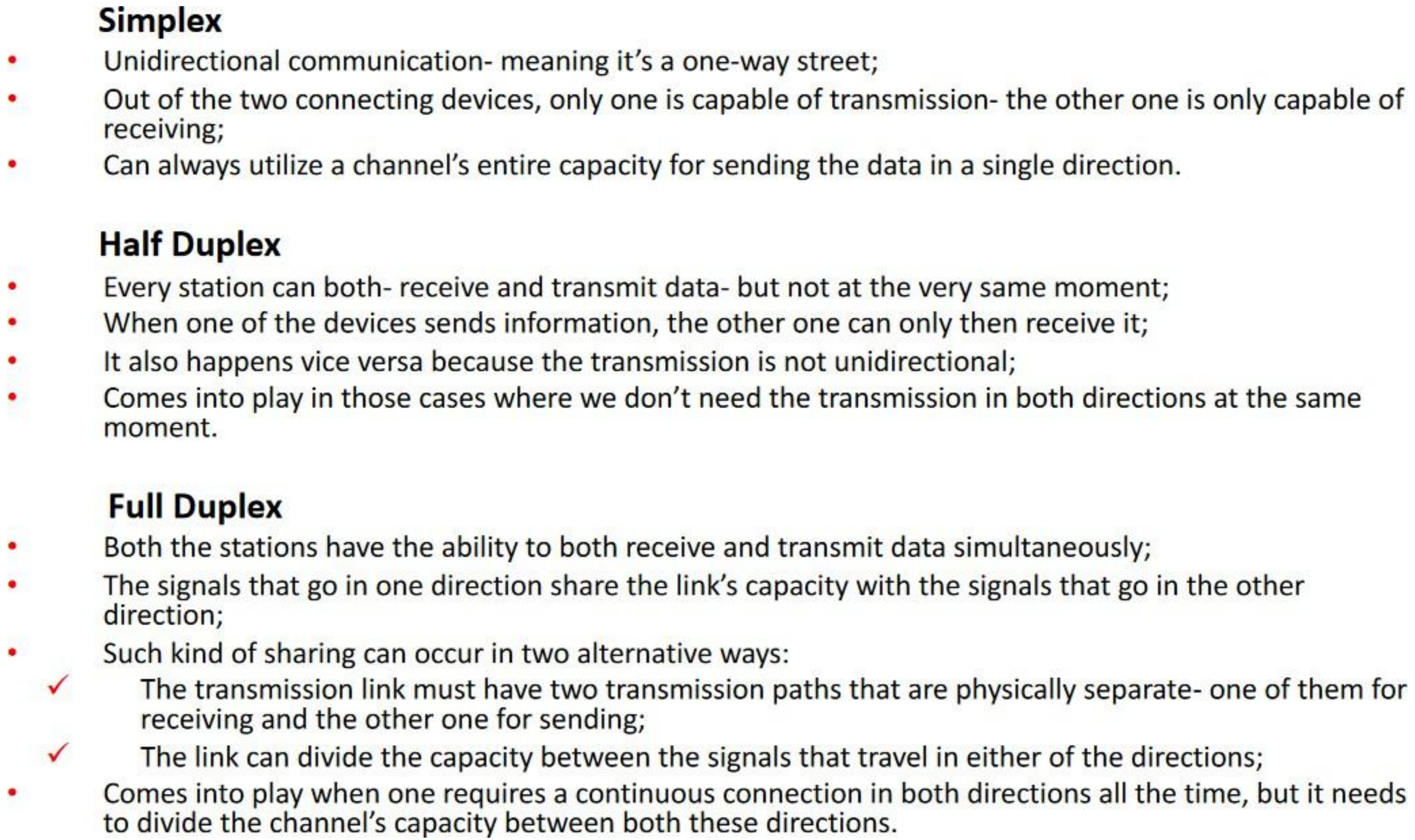
BGP Example


CUSTOMER
YOUR NETWORK
PEERING ISP
BGP
BGP
BGP
BGP
PEERING ISP
PEERING ISP

BGP Example


Smartphone
Laptop
Internet
Wifi Router
Router
Server
Laptop
Switch
Switch
IP Phone
PC Ring
Scanner
Desktop PC
Desktop PC
IP Phone
Printer

Transmission modes



Simplex

- Unidirectional communication- meaning it's a one-way street;
- Out of the two connecting devices, only one is capable of transmission- the other one is only capable of receiving;
- Can always utilize a channel's entire capacity for sending the data in a single direction.

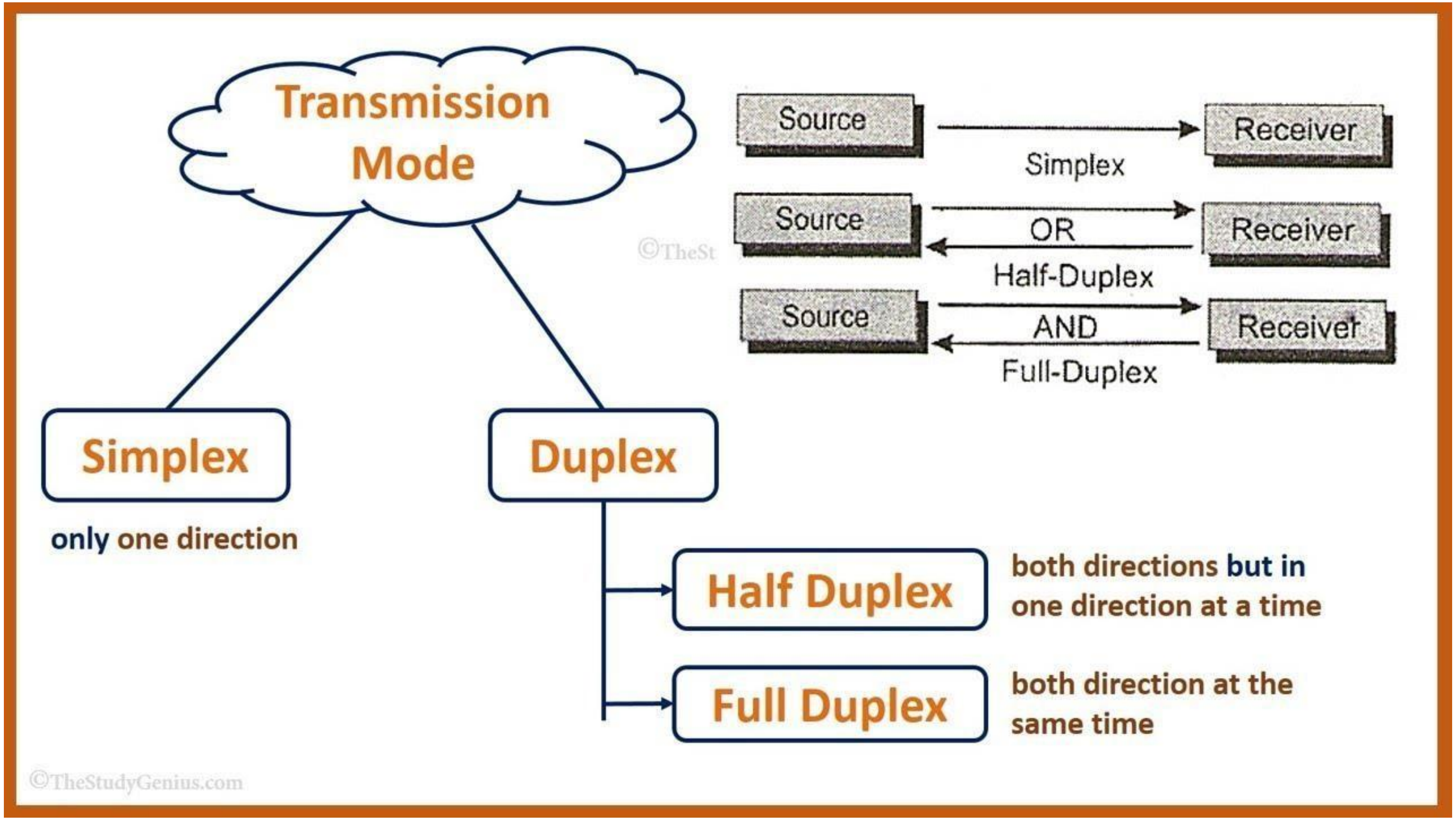
Half Duplex

- Every station can both- receive and transmit data- but not at the very same moment;
- When one of the devices sends information, the other one can only then receive it;
- It also happens vice versa because the transmission is not unidirectional;
- Comes into play in those cases where we don't need the transmission in both directions at the same moment.

Full Duplex

- Both the stations have the ability to both receive and transmit data simultaneously;
- The signals that go in one direction share the link's capacity with the signals that go in the other direction;
- Such kind of sharing can occur in two alternative ways:
  - ✓ The transmission link must have two transmission paths that are physically separate- one of them for receiving and the other one for sending;
  - ✓ The link can divide the capacity between the signals that travel in either of the directions;
- Comes into play when one requires a continuous connection in both directions all the time, but it needs to divide the channel's capacity between both these directions.

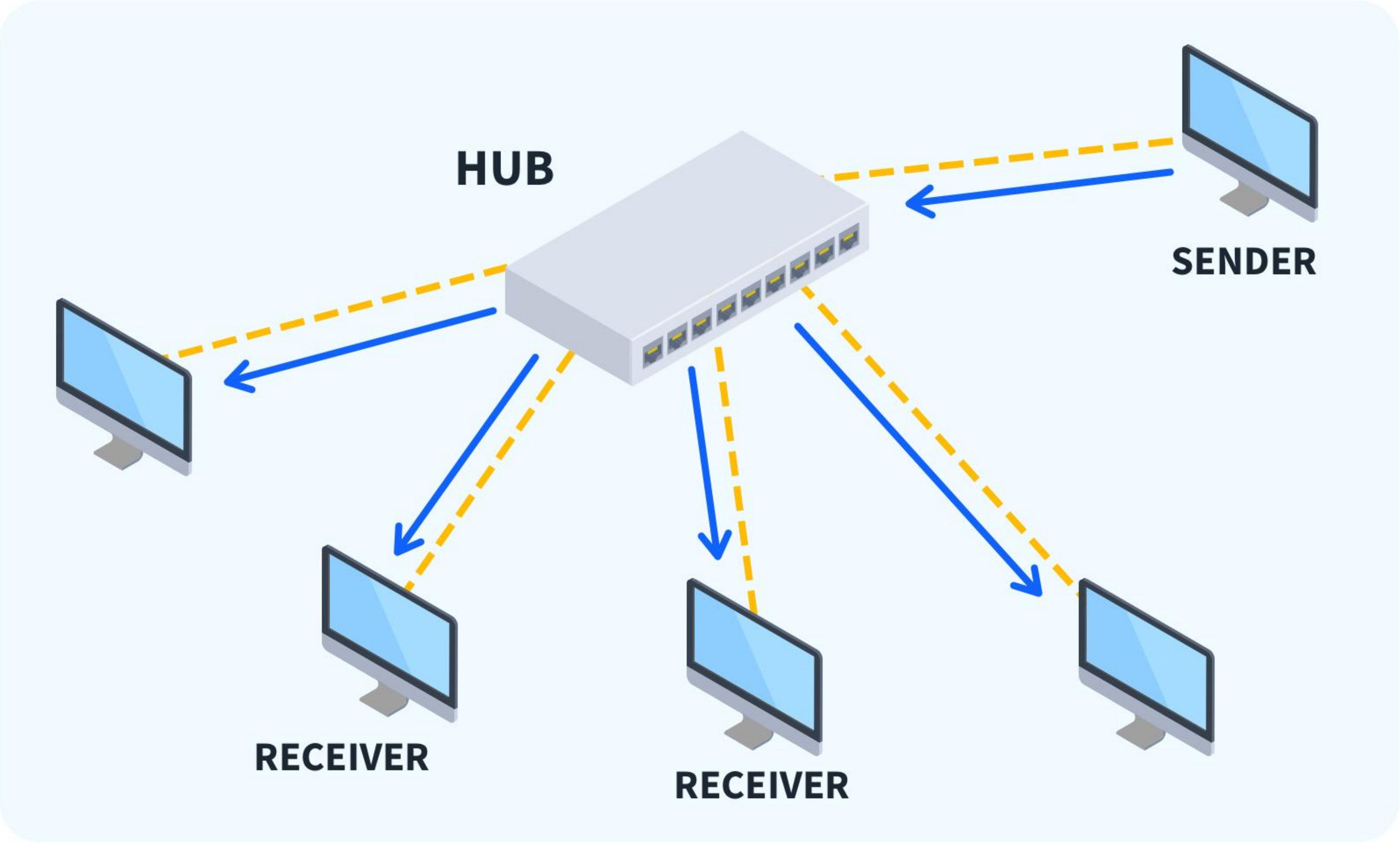
Simplex and Duplex



Hub

- Hubs are simple devices with an input Ethernet port that connects to a router and multiple output ports for devices to connect to;
- When it receives data, it transmits it to all connected devices, leaving the intended device to recognize the data;
- Hubs only operate in half-duplex, so they cannot send and receive data simultaneously, slowing down speeds;
- Hubs typically operate on layer 1—the physical layer—of the open systems interconnection (OSI) model with other hardware devices;
- Two common types of hubs are:
  - ✓ **Active hubs**: Powered devices that amplify incoming signals to connected devices, extending the distance they can travel;
  - ✓ **Passive hubs**: Bring multiple devices into one network through its Ethernet ports, it does not amplify signals or require a power supply;
- With limited capabilities, hubs only have one basic function in a modern networking environment: connecting multiple Ethernet ports into one place;
- Are a useful, inexpensive solution for small LAN environments that need to connect multiple devices together when the router doesn't have enough Ethernet ports;
- A cheap cabling option in small environments with low network traffic.

Hub

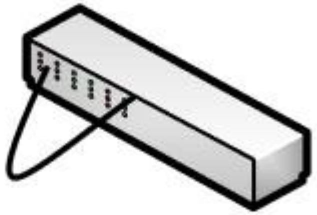


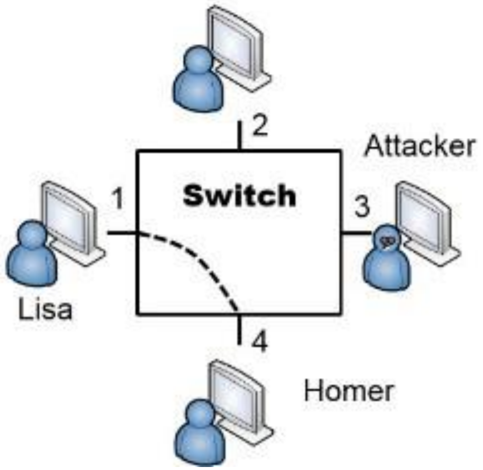
Hub

NETGEAR ProSAFE
Gigabit Switch GS108
GS108
NETGEAR
On=Link
Blink=ACT
Power
Both=1000M
100M
10M
1
2
3
4
5
6
7
8
netgear.com

Switch

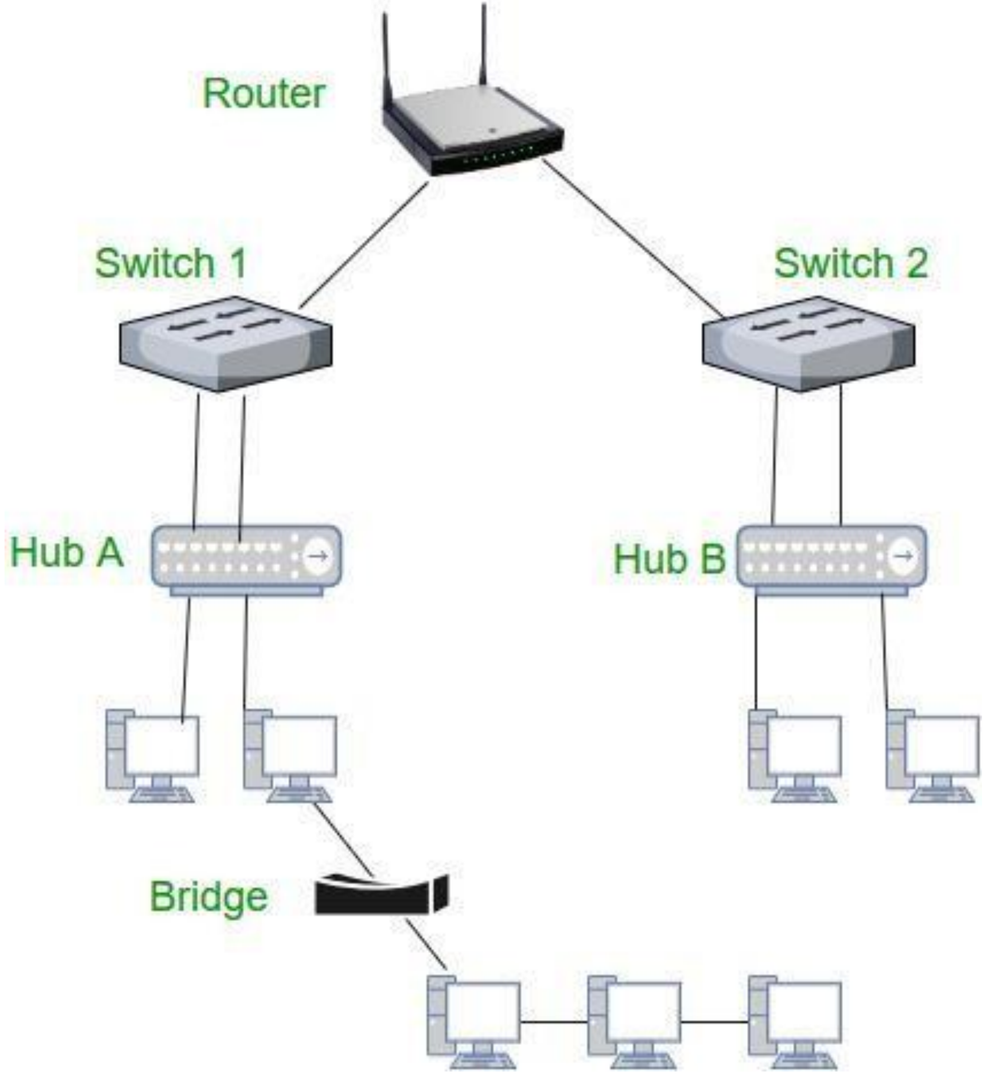
- Switches are slowly replacing hubs in many use cases;
- Network hubs broadcast the data to all connected devices, while switches identify the media access control (MAC) address in the data packet header to transmit the data only to the device that requested it;
- Once a switch knows the routes and ports, it reads data packet headers to determine which device it is supposed to transmit information to via its unique MAC address;
- Switches operate on the OSI framework's data link layer or layer 2;
- Offer a full-duplex function, meaning information being sent and received gets access to the full bandwidth of the network connection;
- Network switches have three core functions:
  - ✓ **Edge switches**: Direct network traffic flows in and out of the network from devices and access points;
  - ✓ **Distribution switches**: Found in the middle of a network topology and connect to switches closer to the edge of the network;
  - ✓ **Core switches**: The core parts of a network that connect various edge and distribution switches and user devices to a data center or enterprise network;
- Port security
  - ✓ Disable unused ports;
  - ✓ MAC address filtering;
- Broadcast Storm and Loop Prevention
  - ✓ Caused if two ports connected together;
  - ✓ STP and RSTP protect against switching loops;
- Bridge Protocol Data Unit Guard.



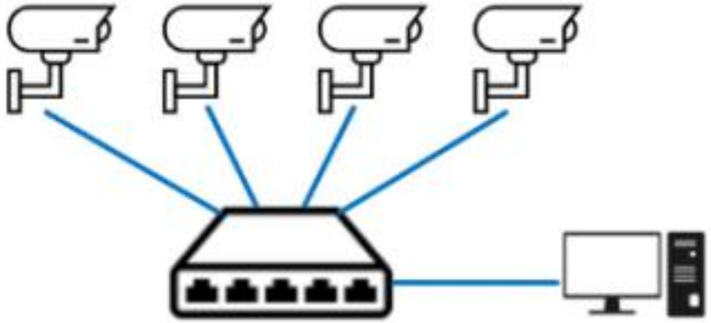


Examples

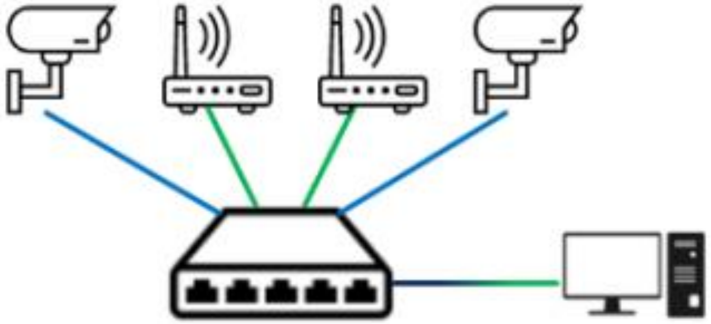
Hub vs switch vs router



Hub vs switch vs router



Hub is used to connect multiple devices together in a single network(Broadcast Domain)



Switch can segregate device via VLAN and each VLAN will have its own and separate Broadcast Domain.

Access point

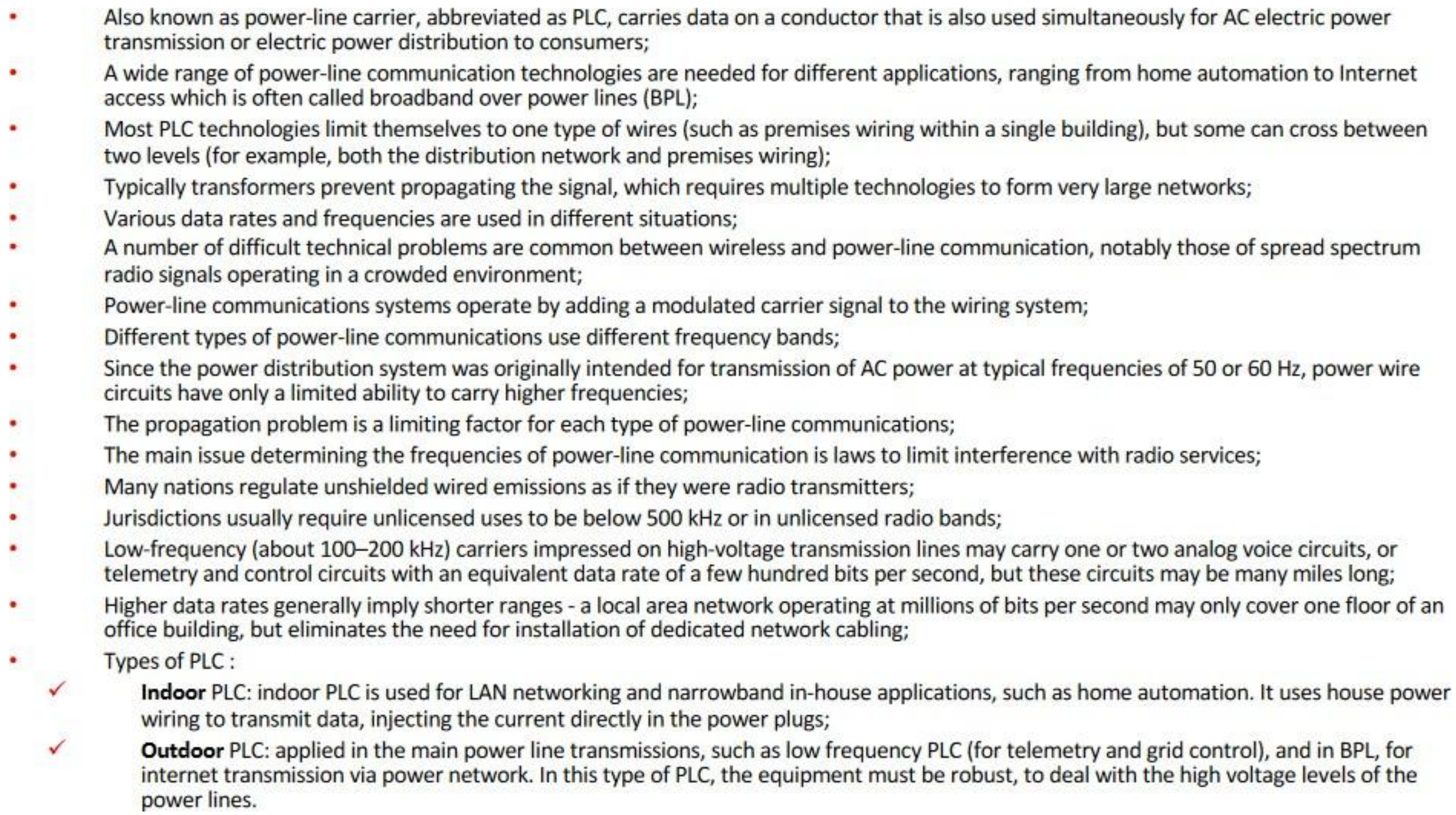
- Sometimes called **wireless access point (WAP** or **AP)**;
- Is a networking hardware device that allows other Wi-Fi devices to connect to a wired network or wireless network;
- As a standalone device, the AP may have a wired connection to a router, but, in a wireless router, it can also be an integral component of the router itself;
- Works as hub with access using antenna;
- An AP is differentiated from a hotspot, which is a physical location where Wi-Fi access is available;
- An AP connects directly to a wired local area network, typically Ethernet, and the AP then provides wireless connections using wireless LAN technology, typically Wi-Fi, for other devices to use that wired connection;
- APs support the connection of multiple wireless devices through their one wired connection;
- Ad hoc network uses a connection between two or more devices without using a wireless access point; the devices communicate directly;
- Due to its peer-to-peer layout, ad hoc Wi-Fi connections are similar to connections available using Bluetooth;
- Ad hoc connections are generally not recommended for a permanent installation;
- Internet access via ad hoc networks, using features like Windows' Internet Connection Sharing, may work well with a small number of devices that are close to each other, but ad hoc networks do not scale well;
- For internet-enabled nodes, access points have a clear advantage, with the possibility of having a wired LAN.

Examples

Repeaters

- Also called wireless range extender or Wi-Fi extender;
- Is a device that takes an existing signal from a wireless router or wireless access point and rebroadcasts it to create a second network;
- When two or more hosts have to be connected with one another over the IEEE 802.11 protocol and the distance is too long for a direct connection to be established, a wireless repeater is used to bridge the gap;
- It can be a specialized stand-alone computer networking device;
- As far as the original router or access point is concerned, only the repeater MAC is connected, making it necessary to enable safety features on the wireless repeater;
- Wireless repeaters are commonly used to improve signal range and strength within homes and small offices :
  - ✓ When there is no wireless hotspot in an area;
  - ✓ In an area with much interference;
  - ✓ Interference can be caused by many environmental factors such as microwaves (such as from a microwave oven), metal appliances or metallic coating or an impeded line of sight;
  - ✓ When the distance between the computer and the wireless access point or wireless router is too great for the internal wireless network interface card to receive the wireless signal;
  - ✓ When networking in an environment with interference and multiple computers, networks or hubs.

Power-line communication



- Also known as power-line carrier, abbreviated as PLC, carries data on a conductor that is also used simultaneously for AC electric power transmission or electric power distribution to consumers;
- A wide range of power-line communication technologies are needed for different applications, ranging from home automation to Internet access which is often called broadband over power lines (BPL);
- Most PLC technologies limit themselves to one type of wires (such as premises wiring within a single building), but some can cross between two levels (for example, both the distribution network and premises wiring);
- Typically transformers prevent propagating the signal, which requires multiple technologies to form very large networks;
- Various data rates and frequencies are used in different situations;
- A number of difficult technical problems are common between wireless and power-line communication, notably those of spread spectrum radio signals operating in a crowded environment;
- Power-line communications systems operate by adding a modulated carrier signal to the wiring system;
- Different types of power-line communications use different frequency bands;
- Since the power distribution system was originally intended for transmission of AC power at typical frequencies of 50 or 60 Hz, power wire circuits have only a limited ability to carry higher frequencies;
- The propagation problem is a limiting factor for each type of power-line communications;
- The main issue determining the frequencies of power-line communication is laws to limit interference with radio services;
- Many nations regulate unshielded wired emissions as if they were radio transmitters;
- Jurisdictions usually require unlicensed uses to be below 500 kHz or in unlicensed radio bands;
- Low-frequency (about 100–200 kHz) carriers impressed on high-voltage transmission lines may carry one or two analog voice circuits, or telemetry and control circuits with an equivalent data rate of a few hundred bits per second, but these circuits may be many miles long;
- Higher data rates generally imply shorter ranges - a local area network operating at millions of bits per second may only cover one floor of an office building, but eliminates the need for installation of dedicated network cabling;
- Types of PLC :
  - ✓ **Indoor** PLC: indoor PLC is used for LAN networking and narrowband in-house applications, such as home automation. It uses house power wiring to transmit data, injecting the current directly in the power plugs;
  - ✓ **Outdoor** PLC: applied in the main power line transmissions, such as low frequency PLC (for telemetry and grid control), and in BPL, for internet transmission via power network. In this type of PLC, the equipment must be robust, to deal with the high voltage levels of the power lines.

Examples

Modem

- A modulator-demodulator or modem is a computer hardware device that converts data from a digital format into a format suitable for an analog transmission medium such as telephone or radio;
- A modem transmits data by modulating one or more carrier wave signals to encode digital information, while the receiver demodulates the signal to recreate the original digital information;
- The goal is to produce a signal that can be transmitted easily and decoded reliably;
- Modems can be used with almost any means of transmitting analog signals, from light-emitting diodes to radio;
- Early modems were devices that used audible sounds suitable for transmission over traditional telephone systems and leased lines, These generally operated at 110 or 300 bits per second (bit/s), and the connection between devices was normally manual, using an attached telephone handset;
- By the 1970s, higher speeds of 1,200 and 2,400 bit/s for asynchronous dial connections, 4,800 bit/s for synchronous leased line connections and 35 kbit/s for synchronous conditioned leased lines were available;
- By the 1980s, less expensive 1,200 and 2,400 bit/s dialup modems were being released, and modems working on radio and other systems were available;
- As device sophistication grew rapidly in the late 1990s, telephone-based modems quickly exhausted the available bandwidth, reaching 56 kbit/s;
- The rise of public use of the internet during the late 1990s led to demands for much higher performance, leading to the move away from audio-based systems to entirely new encodings on cable television lines and short-range signals in subcarriers on telephone lines;
- The move to cellular telephones, especially in the late 1990s and the emergence of smartphones in the 2000s led to the development of ever-faster radio-based systems;
- Today, modems are ubiquitous and largely invisible, included in almost every mobile computing device in one form or another, and generally capable of speeds on the order of tens or hundreds of megabytes per second;
- Modems are frequently classified by the maximum amount of data they can send in a given unit of time, usually expressed in bits per second (symbol bit/s, sometimes abbreviated "bps") or rarely in bytes per second (symbol B/s) and modern broadband modem speeds are typically expressed in megabits per second (Mbit/s);
- Many modems are variable-rate, permitting them to be used over a medium with less than ideal characteristics, such as a telephone line that is of poor quality or is too long. This capability is often adaptive so that a modem can discover the maximum practical transmission rate during the connect phase, or during operation.

Examples

307

MODEM TECHNOLOGY
TALK AUTO 300 300 1200
DATA ANS ORG ANS 75
4ANTHER

Routers

- Route traffic between networks;
- Do not pass broadcasts.

Routers and ACLs

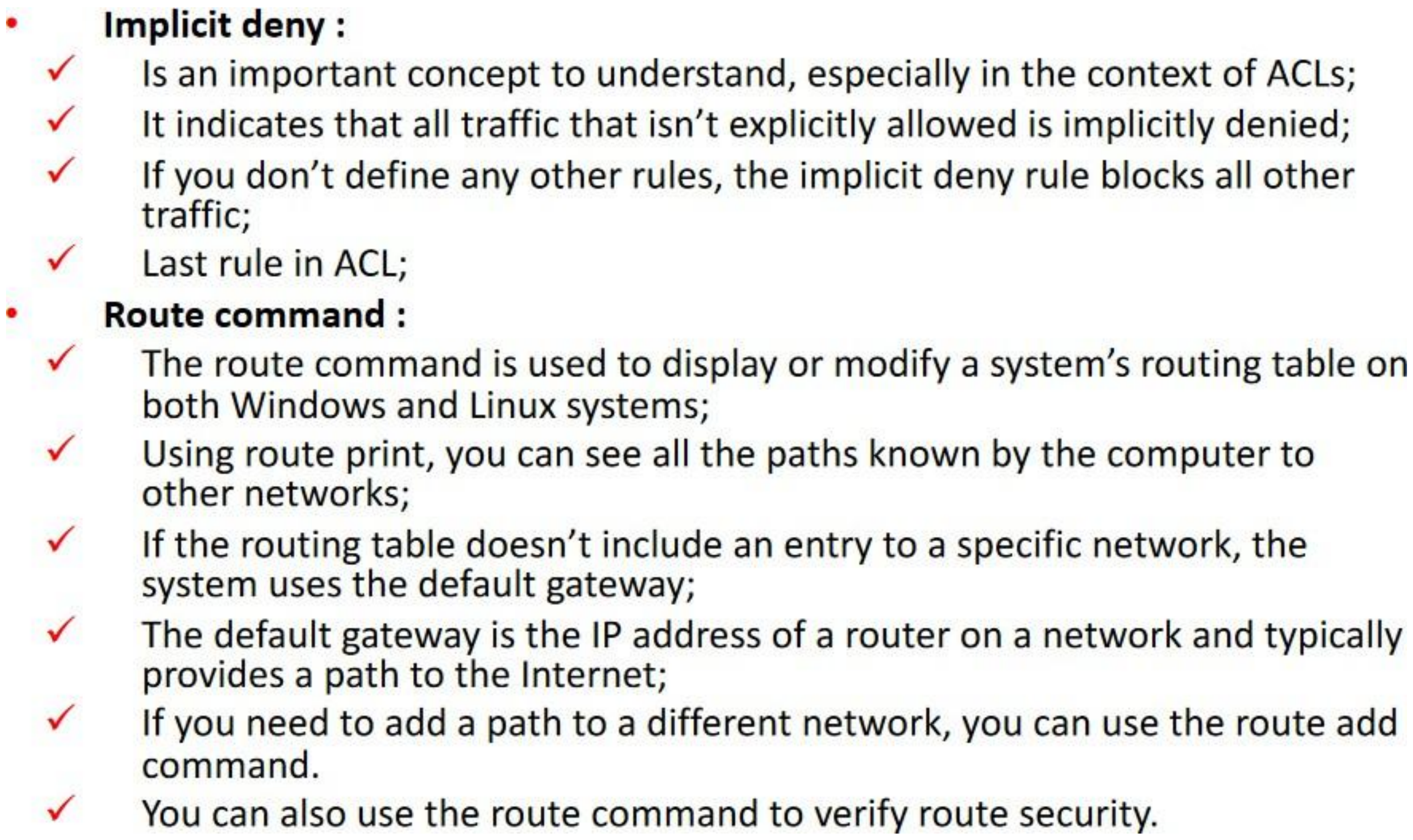
Filter based on :

✓ IP addresses and networks;

✓ Ports;

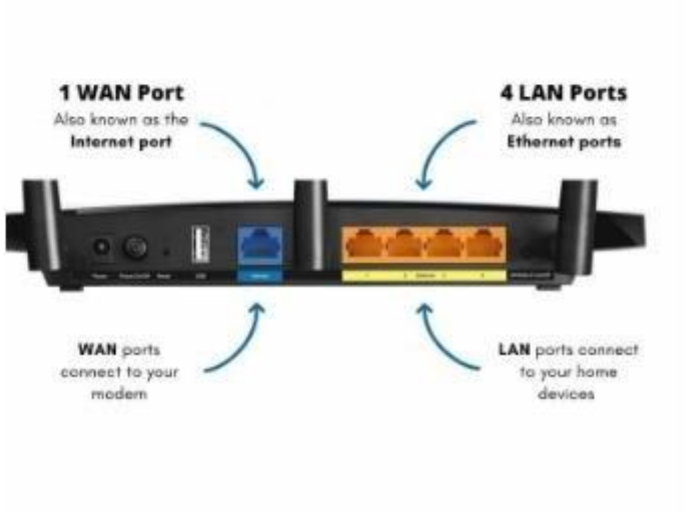
✓ Protocol numbers.

Routers inside



- **Implicit deny :**
  - ✓ Is an important concept to understand, especially in the context of ACLs;
  - ✓ It indicates that all traffic that isn’t explicitly allowed is implicitly denied;
  - ✓ If you don’t define any other rules, the implicit deny rule blocks all other traffic;
  - ✓ Last rule in ACL;
- **Route command :**
  - ✓ The route command is used to display or modify a system’s routing table on both Windows and Linux systems;
  - ✓ Using route print, you can see all the paths known by the computer to other networks;
  - ✓ If the routing table doesn’t include an entry to a specific network, the system uses the default gateway;
  - ✓ The default gateway is the IP address of a router on a network and typically provides a path to the Internet;
  - ✓ If you need to add a path to a different network, you can use the route add command.
  - ✓ You can also use the route command to verify route security.

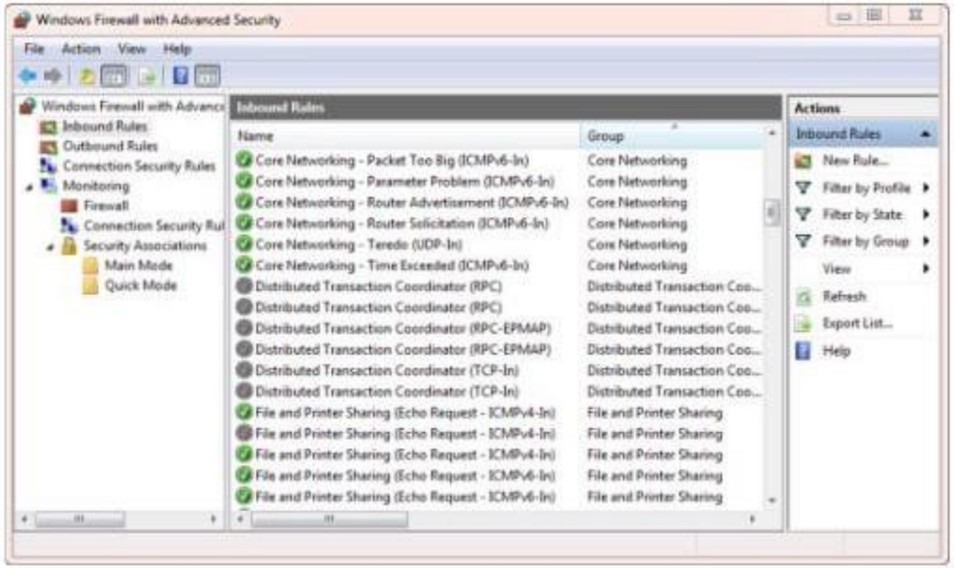
Examples


1 WAN Port
Also known as the Internet port
4 LAN Ports
Also known as Ethernet ports
WAN ports connect to your modem
LAN ports connect to your home devices

TP-LINK

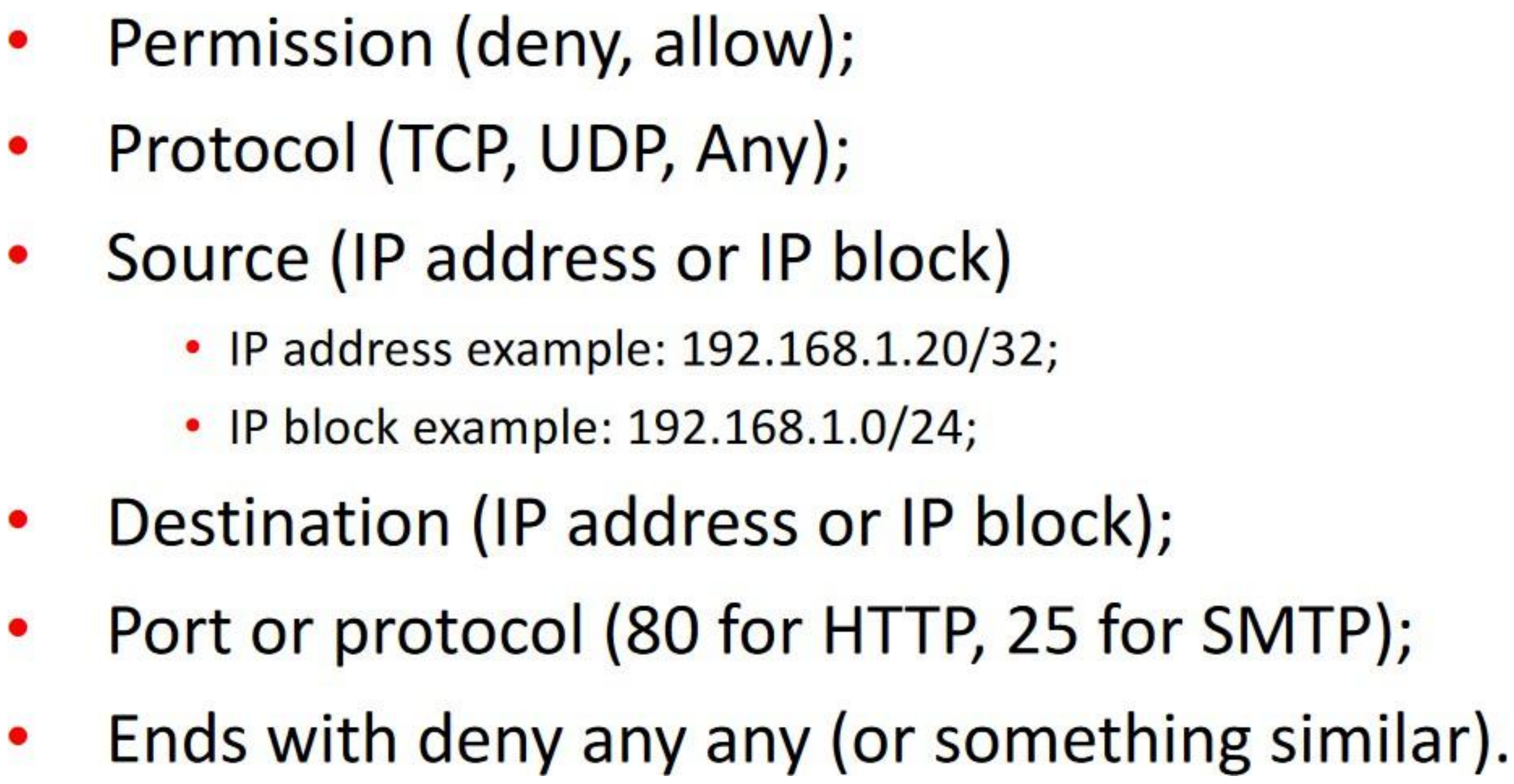
Firewalls

- Host-based;
- Software versus hardware firewalls;
- Next-generation firewall;



Name	Group
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking
Core Networking - Parameter Problem (ICMPv6-In)	Core Networking
Core Networking - Router Advertisement (ICMPv6-In)	Core Networking
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking
Core Networking - Teredo (UDP-In)	Core Networking
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing

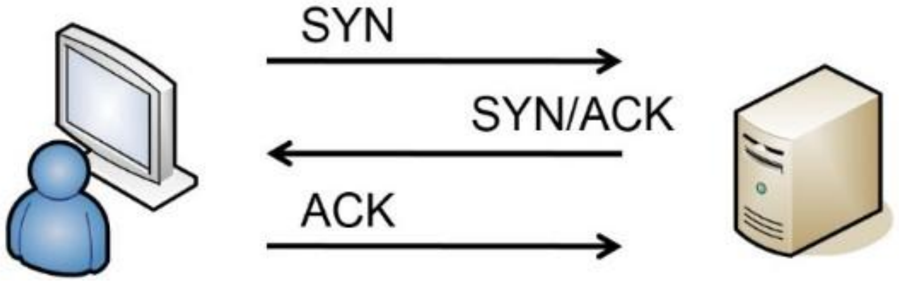
Stateless Firewalls



- Permission (deny, allow);
- Protocol (TCP, UDP, Any);
- Source (IP address or IP block)
  - IP address example: 192.168.1.20/32;
  - IP block example: 192.168.1.0/24;
- Destination (IP address or IP block);
- Port or protocol (80 for HTTP, 25 for SMTP);
- Ends with deny any any (or something similar).

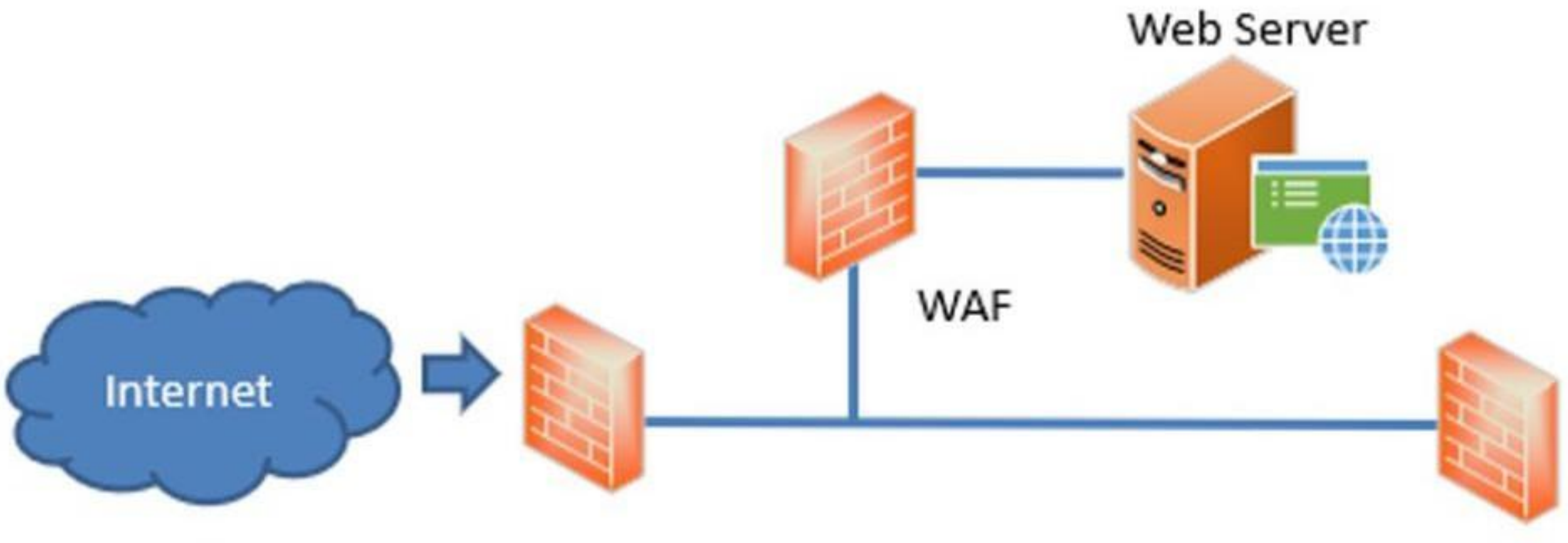
Stateful Firewalls

- Makes decisions based on context, or state, of traffic;
- Can ensure TCP traffic is part of an established TCP session - if not, traffic is blocked;



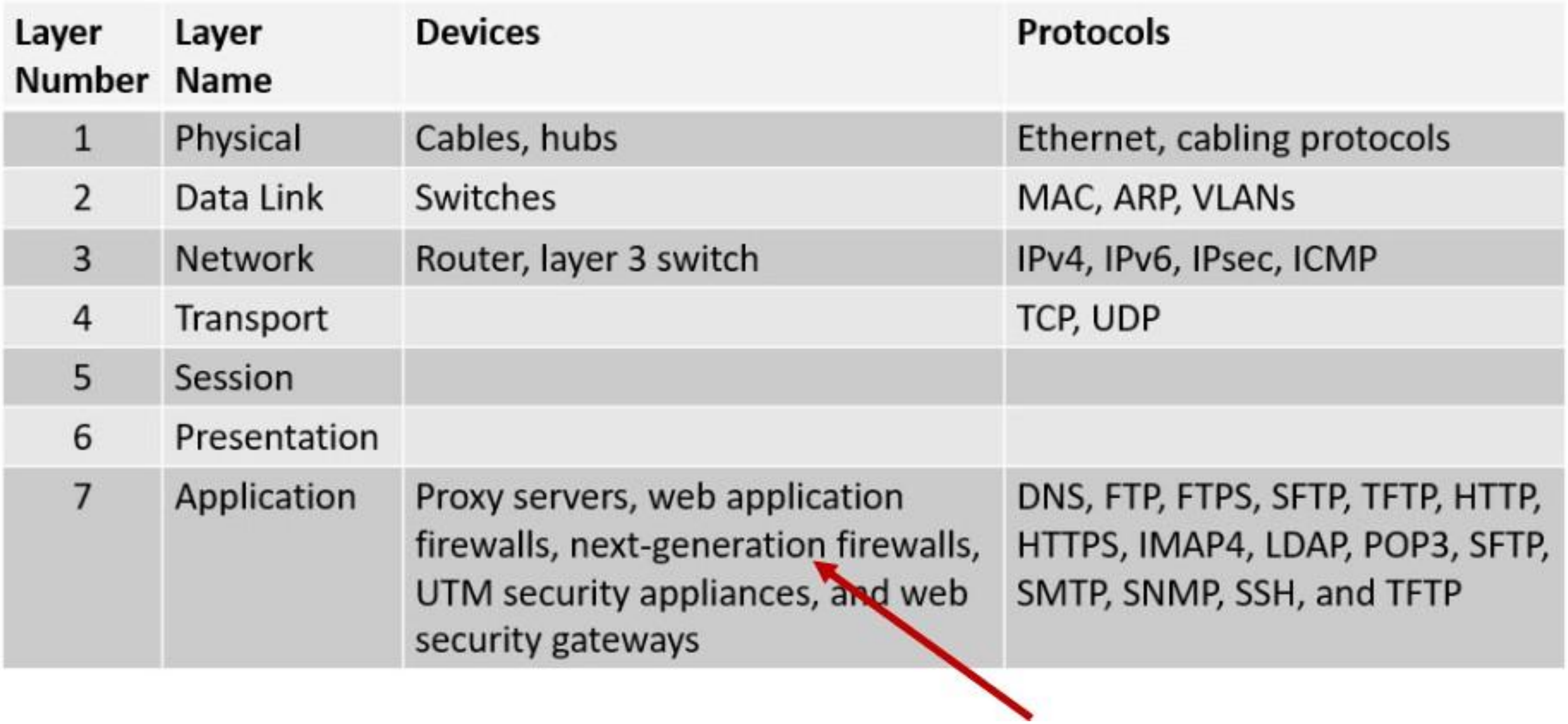
Web application firewall (WAF)

Protects a web application or web server



Next-generation firewalls

All 7 layers up to Application layer



Layer Number	Layer Name	Devices	Protocols
1	Physical	Cables, hubs	Ethernet, cabling protocols
2	Data Link	Switches	MAC, ARP, VLANs
3	Network	Router, layer 3 switch	IPv4, IPv6, IPsec, ICMP
4	Transport		TCP, UDP
5	Session		
6	Presentation		
7	Application	Proxy servers, web application firewalls, next-generation firewalls, UTM security appliances, and web security gateways	DNS, FTP, FTPS, SFTP, TFTP, HTTP, HTTPS, IMAP4, LDAP, POP3, SFTP, SMTP, SNMP, SSH, and TFTP

Examples

Multipurpose devices

- Integrates several types of network devices into one;
- Solved both hardware and software;
- Can be virtualized (like any kind of network device);
- More simply managed;
- Cheaper;
- Single point failure.

Examples

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS

› How did we make this? Learn at hivesystems.com/password