# Cybersecurity Analyst Course: Networking Basics & Basic Nmap Scans Week 2

This document is designed for adults with little or no technical background. It introduces fundamental networking concepts and provides hands‑on instructions for using the **Nmap** port scanner. The session is structured into two parts:

* **Theory:** Understand how computers communicate using IP addresses, ports and the seven layers of the OSI model.
* **Practice:** Learn how to install Nmap and perform simple scans to discover devices and services on a network.

## 1. Networking Basics

### 1.1 What is a Network?

A **network** is a group of computers, printers or other devices that exchange data. The devices (called **nodes**) can be connected by cables or wirelessly. A node can be a laptop, smartphone, server, printer or router. Nodes send data across **links**, which may be wired (Ethernet) or wireless (Wi‑Fi). A **protocol** is a set of rules that tells nodes how to communicate. Protocols define what can be sent, how it is sent and when it is sent.

Networks come in many sizes. A local area network (LAN) covers a small area like an office or home. A wide area network (WAN) connects multiple LANs across cities or countries. The Internet is a global network of networks. Regardless of size, every network uses addresses and ports to deliver data.

### 1.2 IP Addresses

An **IP address** (Internet Protocol address) is the logical identifier for a device on a network. It works like a mailing address so that information knows where to go. It is like the street address of a device. It uniquely identifies every computer, phone or server so that data can be routed to the right destination. At the network layer, IP addresses allow packets to travel across interconnected networks. Two versions of the protocol are widely used today: **IPv4** (the original standard) and **IPv6** (the newer, expanded standard). The [Internet Assigned Numbers Authority (IANA)](https://www.iana.org/) assigns unique addresses globally. The most common format, IPv4, has four numbers separated by periods (for example, 192.168.1.10). Each IPv4 address is 32 bits long, which gives approximately 4 billion possible addresses. IPv6 uses 128‑bit addresses and provides a much larger address space for the future.

Operating systems provide tools for discovering your IP address:

* **Windows:** Open the Command Prompt and run ipconfig. Look for “IPv4 Address” in the output.
* **Linux/macOS:** Open a terminal and run ifconfig or ip addr show. Find the address assigned to your network interface.

A device may have more than one IP address—one for each network interface or virtual network.

### Public vs. private IP addresses

Think of **public IP addresses** as your street address – they are globally unique and allow anyone on the internet to find you. **Private IP addresses**, on the other hand, are like apartment numbers inside a building: they only make sense within the local network. Devices inside your home or office typically use private addresses, and a router performs **Network Address Translation (NAT)** to map those internal addresses to a single public address when accessing the internet.

Common private ranges include:

* **10.0.0.0/8** (Class A block)
* **172.16.0.0/12** (Class B block)
* **192.168.0.0/16** (Class C block)

Because private addresses are not visible on the public internet, they offer a degree of isolation and security. Public addresses are routable across the internet and must be protected by firewalls to prevent unwanted access

### 1.2 Ports and Services

A **port** is a logical communication endpoint used by software to exchange data. Ports are 16‑bit numbers ranging from 0 to 65 535. They are grouped into three ranges:

* **Well‑known ports (0–1023):** Reserved for common services like HTTP, HTTPS and SSH.
* **Registered ports (1024–49 151):** Used by vendor applications (for example, databases).
* **Dynamic/private ports (49 152–65 535):** Assigned temporarily for client connections.

The Internet Assigned Numbers Authority (IANA) lists standard port assignments for common services. Some common ports are summarised below:

|  |
| --- |
| Here are some well‑known protocols you are likely to encounter, along with their typical port numbers: |
| **HTTP (80):** Unsecured web traffic. |
| **HTTPS (443):** Secure web traffic using TLS/SSL. |
| **FTP (20/21):** File Transfer Protocol for transferring files. |
| **SSH (22):** Secure Shell for remote command‑line access. |
| **DNS (53):** Domain Name System that translates domain names to IP addresses. |
| **SMTP (25):** Simple Mail Transfer Protocol for sending email. |
| **POP3 (110):** Post Office Protocol used by clients to download mail. |
| **IMAP (143):** Internet Message Access Protocol for accessing email on a server. |
| Here are some well‑known protocols you are likely to encounter, along with their typical port numbers: |
| **HTTP (80):** Unsecured web traffic. |
| **HTTPS (443):** Secure web traffic using TLS/SSL. |
| **FTP (20/21):** File Transfer Protocol for transferring files. |
| **SSH (22):** Secure Shell for remote command‑line access. |

Understanding ports helps identify which services are running on a host. For example, if port 22 is open, it likely indicates an SSH server. Ports above 1023 are usually chosen dynamically for client connections.

### 1.3 Checking Ports on Your Computer

To see which ports are in use on your system you can use built‑in commands:

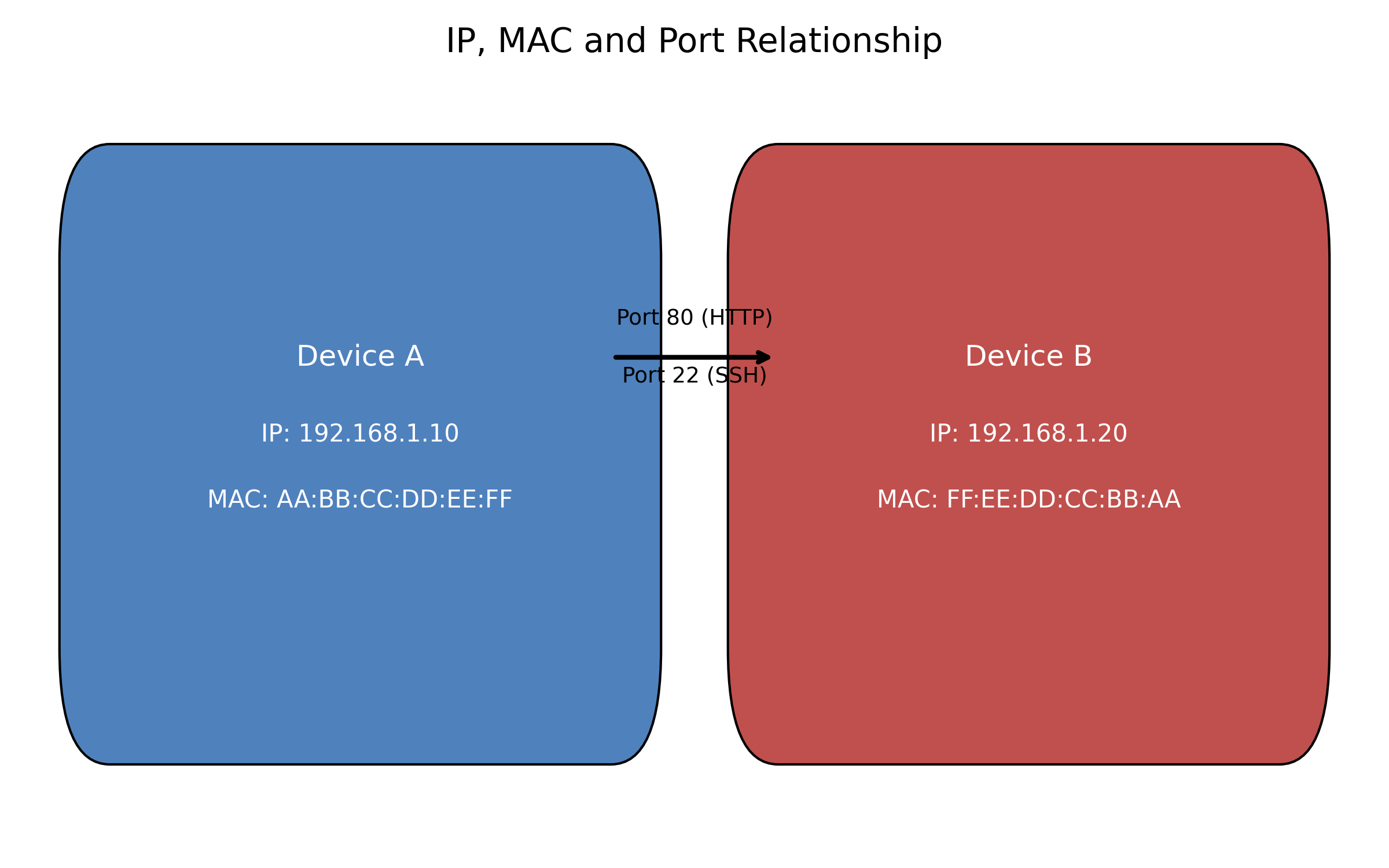
* **Windows:** run netstat -a from a Command Prompt to list all listening and open ports【666641019724348†L351-L352】.

**Linux/macOS:** use netstat -tulpn or ss -tulpn to display active ports and the processes that own them.

### 1.4 MAC Addresses

While an IP address identifies a device on a network, a **MAC address** (Media Access Control address) uniquely identifies the device’s network interface card (NIC). MAC addresses are sometimes called physical addresses and are assigned at manufacture. They are 48‑bit numbers commonly shown in hexadecimal notation, such as AA:BB:CC:DD:EE:FF. In Windows, running ipconfig /all displays the MAC address of each interface.

MAC addresses operate at the Data Link layer (layer 2) of the OSI model, while IP addresses operate at the Network layer (layer 3). The combination of an IP address and a port number is called a **socket**. The differences between IP addresses, MAC addresses and ports are illustrated below.



Devices A and B have unique MAC addresses (physical identifiers) and IP addresses (logical identifiers). Data is sent between applications using port numbers; for example, web traffic uses port 80 while remote login uses port 22.

### TCP vs. UDP (3 WAY handshake)

**TCP (Transmission Control Protocol)** is like a polite phone call: before sending data, the client and server perform a **three‑way handshake** to establish a connection. This handshake involves a SYN message from the client, a SYN‑ACK reply from the server and a final ACK from the client. Once connected, TCP ensures data arrives intact and in order by using acknowledgements and retransmissions. **UDP (User Datagram Protocol)** is more like sending postcards: it sends packets without establishing a formal connection and does not guarantee delivery, but it is faster and suitable for real‑time applications such as voice or video streaming.

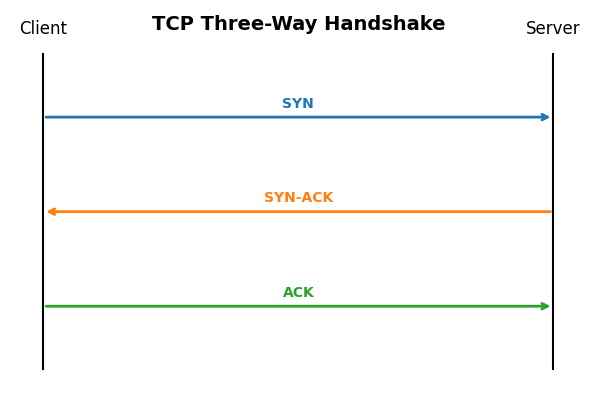


Figure 4 – TCP Three‑Way Handshake

| Attribute | TCP | UDP |
| --- | --- | --- |
| **Connection** | Yes (uses three‑way handshake) | No (connectionless) |
| **Reliability** | Guarantees delivery and order with acknowledgements | No guarantee of delivery or order |
| **Speed** | Slower due to overhead | Faster due to minimal overhead |
| **Typical uses** | Web browsing, email, file transfers | Streaming, VoIP, DNS, online gaming |

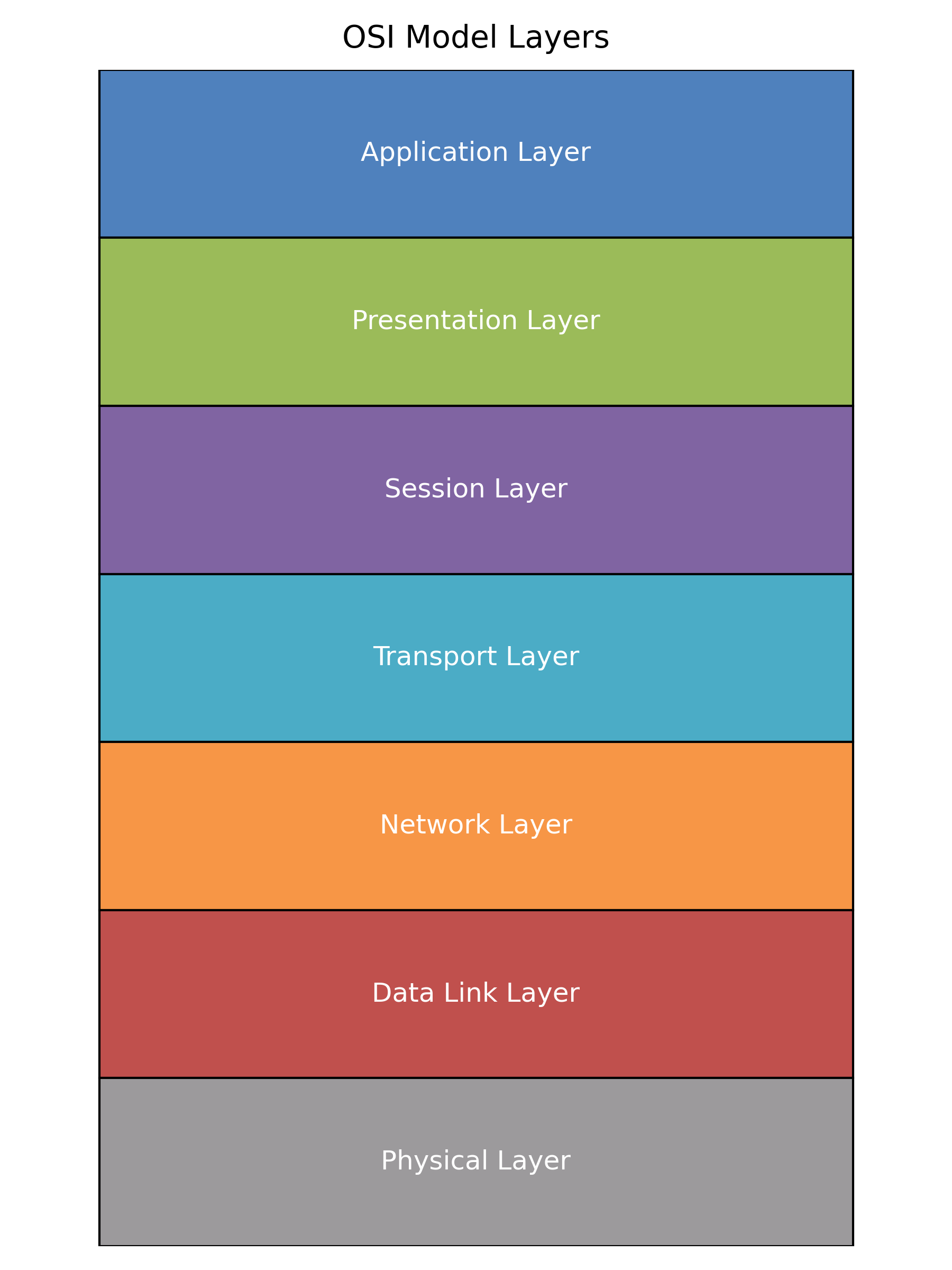
### 1.5 Domain Name System (DNS)

The **Domain Name System** translates human‑friendly domain names (like example.com) into numeric IP addresses. When you type a URL into a browser, your computer asks a DNS resolver for the corresponding IP address. The resolver checks its cache; if the address is unknown, it queries other DNS servers in a hierarchy: the root servers, top‑level domain (TLD) servers and the authoritative server for the domain. Once found, the resolver returns the IP address so your browser can connect.

DNS is essential because humans remember names better than numbers. Without DNS, you would have to memorize IP addresses for every website you visit.

## 2. The OSI Model

The **Open Systems Interconnection (OSI) model** is a conceptual framework created by the International Organization for Standardization (ISO) to describe how data moves through a network. It breaks communication into seven layers, each with specific responsibilities. Understanding the OSI model helps diagnose networking problems and design secure systems.



The seven layers of the OSI model from bottom to top: Physical, Data Link, Network, Transport, Session, Presentation and Application.

Each layer passes data up or down the stack, adding or removing information. The process works like nested envelopes: each layer adds its own header so that the receiving layer can interpret the data.

### 2.1 Layers and Their Functions

The table below summarises the purpose of each layer and provides examples of devices or protocols that operate at that level:

|  |
| --- |
| Figure 1 – OSI Model Layers |
| | Layer | What it does | Everyday analogy | | --- | --- | --- | | **Application (Layer 7)** | Provides services to user applications like web browsing and email | You write a letter using an application like Gmail | | **Presentation (Layer 6)** | Makes sure data is in a form the application understands; handles encryption and compression | The post office reads your handwriting and translates it into a standard format | | **Session (Layer 5)** | Creates and manages conversations between applications; establishes and tears down sessions | Starts and ends a phone call | | **Transport (Layer 4)** | Ensures reliable delivery from end to end; breaks data into segments and uses port numbers | Breaks a package into smaller boxes and labels them so they can be reassembled | | **Network (Layer 3)** | Finds the best path between networks; uses IP addresses | Chooses the route a delivery van takes | | **Data‑link (Layer 2)** | Handles local delivery over a link; uses MAC addresses; detects errors | Ensures the van drives down your street and stops at the right house | | **Physical (Layer 1)** | Sends raw bits over the medium; defines cables and signals | The physical road or cable the van drives on | |

A handy mnemonic for remembering the layers from bottom to top is: Please Do Not Tell Secret Passwords to Anyone. The OSI model is a guide—real‑world protocols may span multiple layers, but the model helps to understand where problems occur.

### 2.2 How Data Flows Through the OSI Layers

When you send an email or load a web page, data travels through all seven layers at the sender, then back up the layers at the receiver【222457548181883†L415-L429】:

* **Application:** The application (e.g., browser) creates the data.
* **Presentation:** Data is formatted or encrypted.
* **Session:** A session is established for communication.
* **Transport:** Data is segmented and given port numbers.
* **Network:** Segments are packaged into packets with IP addresses and routed.
* **Data Link:** Packets are framed with MAC addresses for transmission to the next device.
* **Physical:** Frames are converted to electrical or optical signals on the wire.

The process is reversed on the receiving end, where each layer strips its header and passes the remaining data to the layer above. Understanding this flow helps identify where security controls like firewalls (layers 3–4) or encryption (layer 6) operate.

## 3. Ports, Protocols and Communication

An IP address tells you which house you are visiting, but a **port number** tells you which room in the house you want. Ports are 16‑bit numbers ranging from 0 to 65 535 and are associated with the transport protocols **TCP** or **UDP**. When your browser connects to www.example.com on port 80, it knows you want the web server rather than the mail server on the same machine. Ports and protocols allow multiple services to share a single network connection. For example, a server may run a web server (HTTP on port 80) and an SSH server (SSH on port 22) simultaneously. Because each service listens on a different port, clients can connect to the correct service using the IP address plus the appropriate port number.

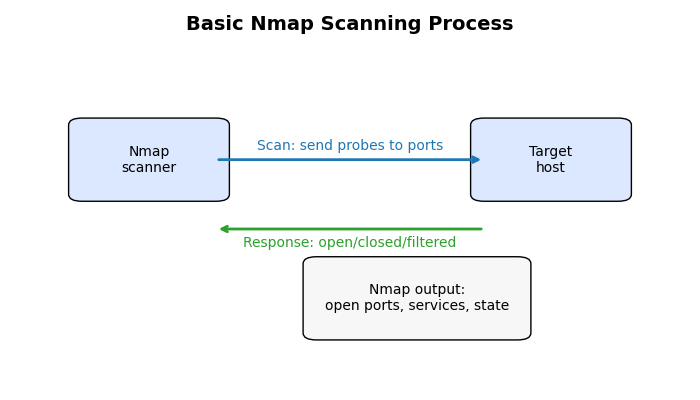
The **Transport layer** uses two main protocols:

* **Transmission Control Protocol (TCP):** Provides reliable, ordered delivery of data. It is used for web browsing, email and file transfers.
* **User Datagram Protocol (UDP):** Provides fast, connectionless communication without guaranteed delivery. It is used for streaming media, VoIP and DNS queries.

Each transport protocol identifies services using port numbers. When a client connects to a server, the client uses a random high‑numbered port and the server listens on a well‑known port. This is why the combination of IP address and port is called a socket.

## 4. Introduction to Nmap

**Nmap** (Network Mapper) is a free and open‑source tool used by network administrators and security professionals to discover devices, detect open ports and identify services on a network. According to freeCodeCamp, Nmap scans IP addresses and ports to detect installed applications. It helps administrators find which devices are running, discover open ports and detect vulnerabilities. Nmap supports both simple commands for beginners and advanced options for experienced testers.



### 4.1 Why Use Nmap?

Nmap’s popularity stems from its ease of use and powerful features:

* **Device discovery:** Quickly recognises servers, routers, switches and mobile devices on a network【713813626169885†L51-L53】.
* **Service detection:** Identifies services like web servers or DNS and can guess version numbers【713813626169885†L53-L58】.
* **Operating system detection:** Uses TCP/IP fingerprints to estimate the target’s operating system【713813626169885†L56-L58】.
* **Scripting engine:** The Nmap Scripting Engine allows automated vulnerability checks【713813626169885†L59-L60】.
* **Graphical interface:** Zenmap provides a GUI for visualising scan results【713813626169885†L61-L62】.

**Ethical note:** Scanning networks without permission is illegal and unethical. Always obtain written permission before scanning systems that you do not own.

### 4.2 Installing Nmap

#### Windows Installation

Nmap provides a Windows self‑installer (for Windows 7 and later) that includes the optional [Npcap](https://npcap.com/) packet capture library. According to the official Nmap documentation, the installer guides you through choosing an installation path and installing Npcap. After downloading nmap‑version‑setup.exe from the [Nmap download page](https://nmap.org/download.html), double‑click it and follow these steps:

1. When prompted, select the components to install (Nmap, Zenmap GUI, Ncat and Ndiff). Leave the default options enabled.
2. Allow the installer to install Npcap. Nmap requires Npcap for raw packet scanning. Choose “WinPcap API compatibility mode” if you use other capture tools.
3. Complete the installation. After finishing, you can run Nmap from the Command Prompt or Zenmap from the Start menu.

#### Linux Installation

Most Linux distributions include Nmap in their package repositories. For Red Hat/Fedora and other RPM‑based systems you can install Nmap with the yum package manager by running sudo yum install nmap【675196451623804†L114-L120】. To install the Zenmap GUI as well, run sudo yum install zenmap【675196451623804†L114-L120】.

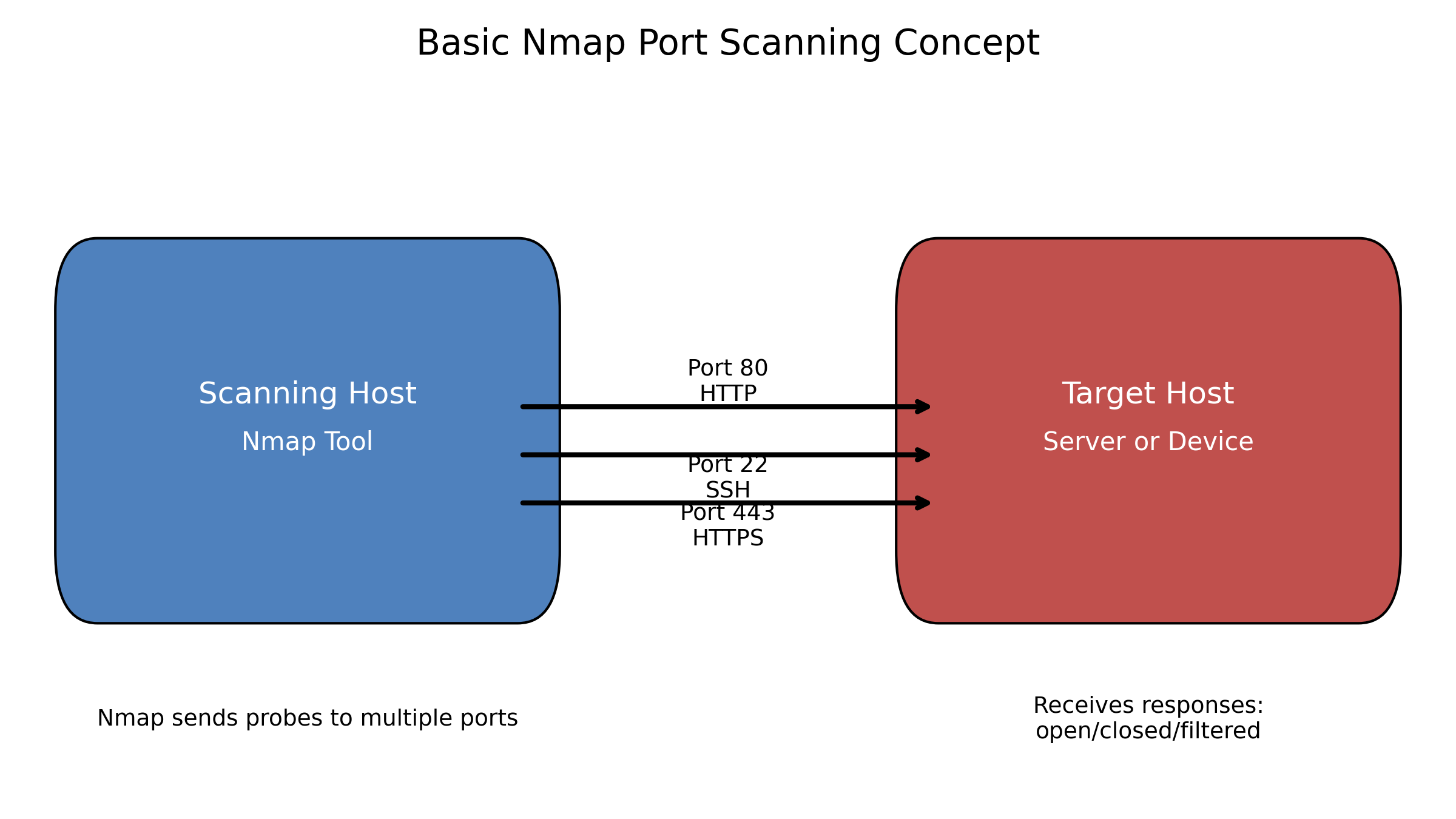
For Debian/Ubuntu and derivatives, the Nmap documentation notes that you can install the package using sudo apt‑get install nmap【675196451623804†L165-L167】. Use sudo apt‑get install zenmap for the GUI. After installation, verify the version with nmap --version.

Advanced users can compile Nmap from source or convert RPM packages to Debian format using the alien tool【675196451623804†L174-L201】, but using packages is simplest for beginners.

### 4.3 Basic Nmap Usage

Nmap’s syntax follows the pattern nmap [options] target. Below are some useful commands for beginners:

|  |
| --- |
| Command |
| nmap 192.168.1.10 |
| nmap -sn 192.168.1.0/24 |
| nmap -p 80 192.168.1.10 |
| nmap -p 1-1024 192.168.1.10 |
| nmap -sS 192.168.1.10 |
| nmap -sV 192.168.1.10 |
| nmap -A 192.168.1.10 |

 Nmap sends probes to multiple ports on the target host and classifies the responses. Ports can be open (a service responds), closed (the host replies that nothing is listening) or filtered (a firewall blocks the probe).

By default Nmap scans the top 1 000 TCP ports defined in its nmap‑services file. To scan all 65 535 ports, specify -p 0-65535 or use -p-. Options can be combined; for example, nmap -sS -p 22,80,443 192.168.1.10 performs a stealth scan of three ports. Consult the [Nmap reference guide](https://nmap.org/book/man.html) for more details.

### 4.4 Hands‑On Exercise

The following exercise guides you through running a basic scan on your own computer or a small lab network. Ensure you have permission to scan any target.

1. **Install Nmap:** Use the steps in section 4.2 to install Nmap on your operating system.
2. **Identify your IP address:** Use ipconfig (Windows) or ifconfig/ip addr (Linux/macOS) to find your device’s IP address.
3. **Discover live hosts:** Run nmap -sn your‑network/24 to see which devices respond to pings. Replace your‑network with your local network prefix (for example, 192.168.1.0).
4. **Scan your own device:** Execute nmap your‑ip to scan the most common ports. Review the list of open ports and compare them with the common port table above.
5. **Scan specific services:** Try nmap -p 22,80 your‑ip to check if SSH and HTTP ports are open.
6. **Perform a version scan:** Run nmap -sV your‑ip to see if Nmap can identify service versions. Note that this may take longer.
7. **Optional – Stealth scan:** If you are comfortable and have administrator privileges, run sudo nmap -sS your‑ip (Linux/macOS) or open an elevated Command Prompt on Windows. Observe any differences in results.
8. **Document findings:** Note which ports were open, closed or filtered. Consider why a port might be filtered (firewall) or open (service running).

Throughout the exercise, pay attention to legal boundaries. Only scan networks or devices you own or have explicit permission to test.

### Hosts and ports

A **host** is any device with an IP address on the network. **Ports** are numbered communication endpoints on that host, like doorways into different applications (web server, mail server, file transfer service, etc.). Nmap scans hosts to discover which ports are open and what services are running

## 5. Conclusion

In this session you learned foundational networking concepts such as IP addressing, MAC addresses, port numbers and the OSI model. These concepts are essential for any cybersecurity analyst because they underpin how data moves across a network and where security controls can be applied. You also installed and experimented with Nmap, a powerful tool for discovering devices and services. With a solid grasp of networking fundamentals and basic scanning techniques, you are now better prepared to explore more advanced topics in cybersecurity.

## Further Reading & References

* [OSI Model – The 7 Layers of Networking Explained](https://www.freecodecamp.org/news/osi-model-networking-layers-explained-in-plain-english/) – freeCodeCamp.
* [Basics of Computer Networking](https://www.geeksforgeeks.org/computer-networks/basics-computer-networking/) – GeeksforGeeks.
* [14 Common Network Ports You Should Know](https://opensource.com/article/18/10/common-network-ports) – opensource.com.
* [What is Nmap and How to Use It](https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/) – freeCodeCamp.
* [Nmap Installation Guide for Windows](https://nmap.org/book/inst-windows.html) – official Nmap documentation.
* [Nmap Installation Guide for Linux](https://nmap.org/book/inst-linux.html) – official Nmap documentation.
* [Quick Port Scanning Tutorial](https://nmap.org/book/port-scanning-tutorial.html) – Nmap Network Scanning book.

**Note:** All diagrams in this document were created specifically for this training. You are free to modify or reuse them for educational purposes.