Crash Course: Network Fundamentals

Objectives to cover:

- **ISO OSI network model**
- **IP addresses, subnets, and routing**
- **TCP, UDP, and port numbers**
- **How to connect to an open TCP port from the command line**
- **Dynamic Host Configuration Protocol (DHCP)**
- **Address Resolution Protocol (ARP)**
- **Network Address Translation (NAT)**
- **Internet Control Message Protocol (ICMP)**
    - **Ping**
    - **Traceroute**
- **DNS**
- **HTTP and FTP**
- **SMTP, POP3, and IMAP**
- **SSL/TLS**

OSI network model

Layer Number	Layer Name	Main Function	Example Protocols and Standards
Layer 7	Application layer	Providing services and interfaces to applications	HTTP, FTP, DNS, POP3, SMTP, IMAP
Layer 6	Presentation layer	Data encoding, encryption, and compression	Unicode, MIME, JPEG, PNG, MPEG
Layer 5	Session layer	Establishing, maintaining, and synchronising sessions	NFS, RPC
Layer 4	Transport layer	End-to-end communication and data segmentation	UDP, TCP
Layer 3	Network layer	Logical addressing and routing between networks	IP, ICMP, IPSec
Layer 2	Data link layer	Reliable data transfer between adjacent nodes	Ethernet (802.3), WiFi (802.11)
Layer 1	Physical layer	Physical data transmission media	Electrical, optical, and wireless signals

- **Layer 1**
  - **The physical layer, also referred to as layer 1, deals with the physical connection between devices; this includes the medium, such as a wire, and the definition of the binary digits 0 and 1.**
- **Layer 2**
  - **The data link layer, i.e., layer 2, represents the protocol that enables data transfer between nodes on the same network segment.**
  - **Examples of layer 2 include Ethernet, i.e., 802.3, and WiFi, i.e., 802.11. Ethernet and WiFi addresses are six bytes. Their address is called a MAC address, where MAC stands for Media Access Control.**
- **Layer 3**
  - **The network layer, i.e., layer 3, is concerned with sending data between different networks.**

    - Examples of the network layer include Internet Protocol (IP), Internet Control Message Protocol (ICMP), and Virtual Private Network (VPN) protocols such as IPSec and SSL/TLS VPN.
- Layer 4
    - Layer 4, the transport layer, enables end-to-end communication between running applications on different hosts.
    - Examples of layer 4 are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- Layer 5
    - The session layer is responsible for establishing, maintaining, and synchronizing communication between applications running on different hosts. Establishing a session means initiating communication between applications and negotiating the necessary parameters for the session.
    - Examples of the session layer are Network File System (NFS) and Remote Procedure Call (RPC).
- Layer 6
    - The presentation layer ensures the data is delivered in a form the application layer can understand. Layer 6 handles data encoding, compression, and encryption. An example of encoding is character encoding, such as ASCII or Unicode.
    - Unicode, MIME (Multipurpose Internet Mail Extensions), JPEG, PNG, MPEG
- Layer 7
    - The application layer provides network services directly to end-user applications. Your web browser would use the HTTP protocol to request a file, submit a form, or upload a file.
    - Examples of Layer 7 protocols are HTTP, FTP, DNS, POP3, SMTP, and IMAP. Don't worry if you are not familiar with all of them.

IP addresses, subnets, and routing

- What is an IP Address
    - Every host on the network needs a unique identifier for other hosts to communicate with it. Without a unique identifier, the host cannot be found without ambiguity. When using the TCP/IP protocol suite, we need to assign an IP address for each device connected to the network.
    - We will be talking about IPv4 as it remains the most widely used.

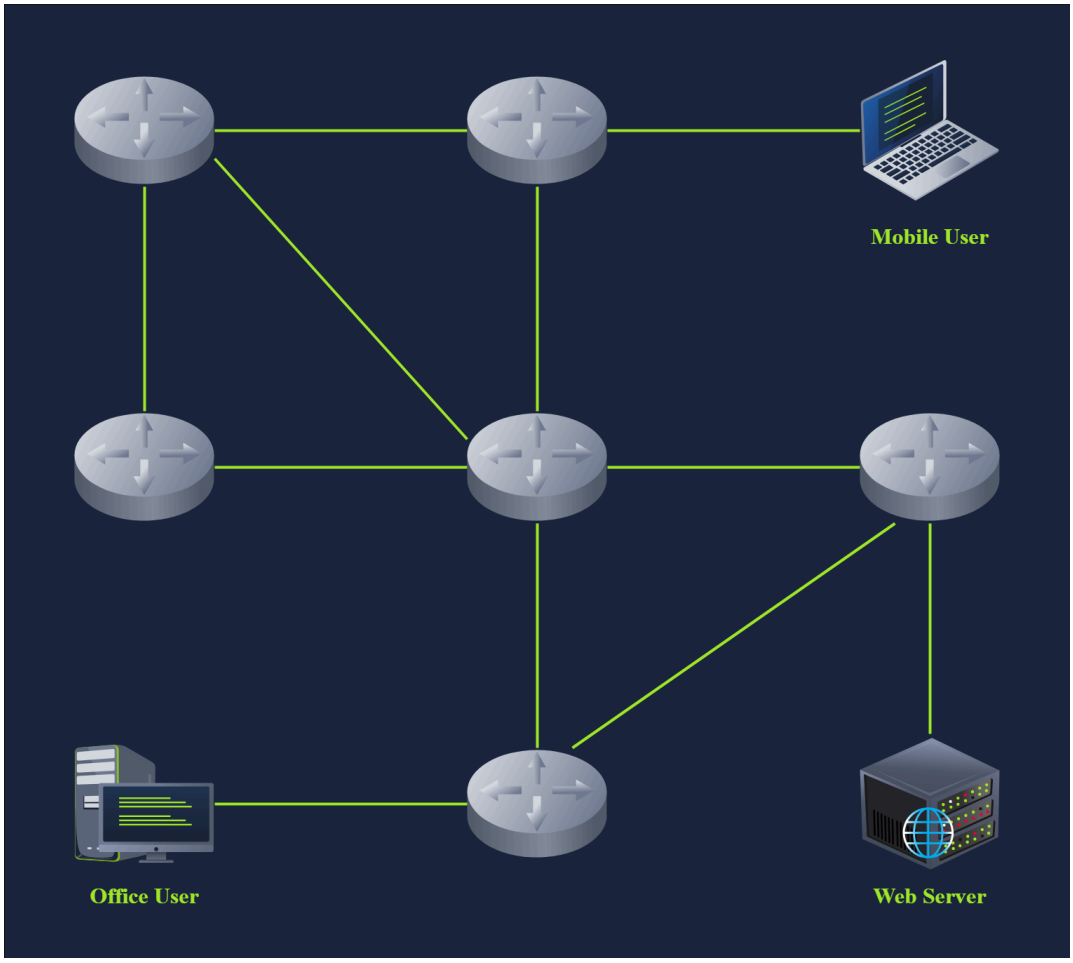
- What makes up an IP
    - An IP address comprises four octets, i.e., 32 bits. Being 8 bits, an octet allows us to represent a decimal number between 0 and 255.

- Private vs Public IP Addresses
    - Private IP's are defined by RFC 1918, see the ranges below:
        - 10.0.0.0 - 10.255.255.255 (10/8)
        - 172.16.0.0 - 172.31.255.255 (172.16/12)
        - 192.168.0.0 - 192.168.255.255 (192.168/16)
    - Public is anything outside of RFC 1918
    - public IP address is like your home postal address
    - A private IP address is like an isolated city or a compound, where all houses and apartments are numbered systematically and can easily exchange mail with each other, but not with the outside world.
- Subnets
    - Subnetting is the term given to splitting up a network into smaller, miniature networks within itself.
    - Subnets use IP addresses in three different ways:
        - Identify the network address
        - Identify the host address
        - Identify the default gateway

Type	Purpose	Explanation	Example
Network Address	This address identifies the start of the actual network and is used to identify a network's existence.	For example, a device with the IP address of 192.168.1.100 will be on the network identified by 192.168.1.0	192.168.1.0
Host Address	An IP address here is used to identify a device on the subnet	For example, a device will have the network address of 192.168.1.1	192.168.1.100
Default Gateway	The default gateway address is a special address assigned to a device on the network that is capable of sending information to another network	Any data that needs to go to a device that isn't on the same network (i.e. isn't on 192.168.1.0) will be sent to this device. These devices can use any host address but usually use either the first or last host address in a network (.1 or .254)	192.168.1.254

- **Subnetting provides a range of benefits, including:**
  - **Efficiency**
  - **Security**
  - **Full control**
- **Routing**
  - **Analogy for a Router**
    - **A router is like your local post office**

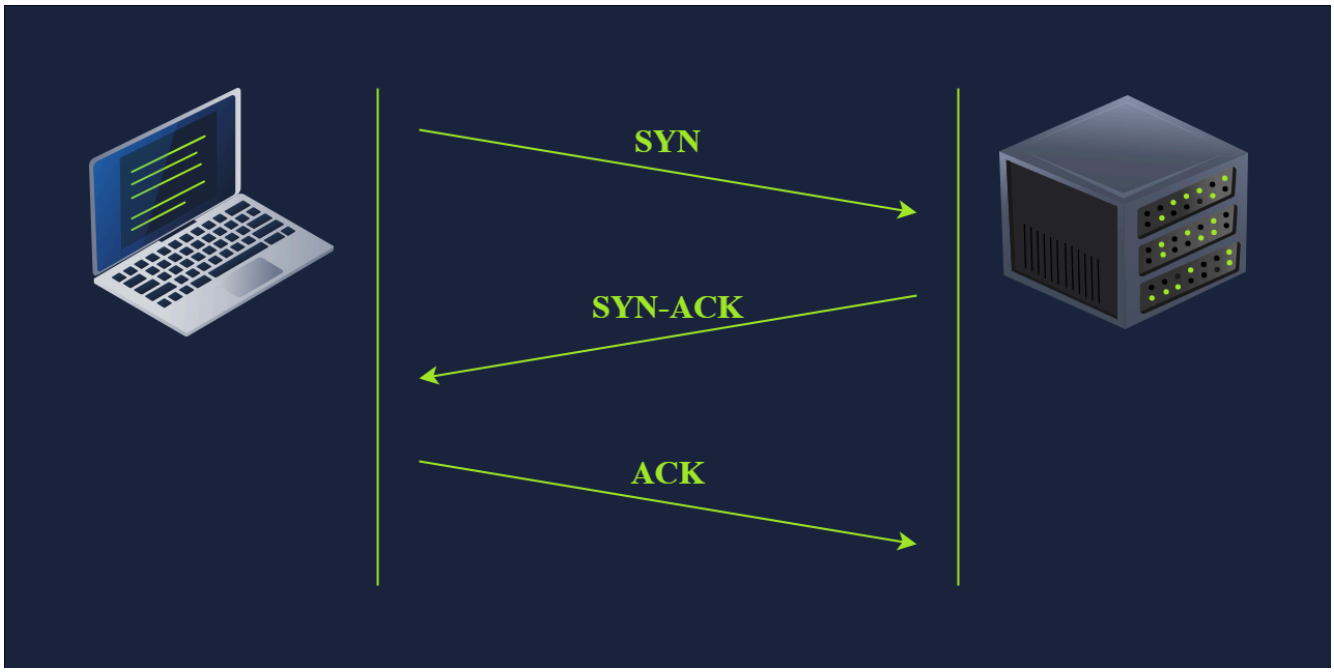
Usually, a data packet passes through multiple routers before it reaches its final destination. The router functions at layer 3, inspecting the IP address and forwarding the packet to the best network (router) so the packet gets closer to its destination.



TCP, UDP, and port numbers

- UDP
  - UDP (User Datagram Protocol) allows us to reach a specific process on this target host.
  - UDP is a simple connectionless protocol that operates at the transport layer, i.e., layer 4.
    - Being connectionless means that it does not need to establish a connection.
    - UDP does not even provide a mechanism to know that the packet has been delivered.
- Ports
  - An IP address identifies the host; we need a mechanism to determine the sending and receiving process. This can be achieved by using port numbers.
  - A port number uses two octets; consequently, it ranges between 1 and 65535; port 0 is reserved.

- TCP
  - TCP (Transmission Control Protocol) is a connection-oriented transport protocol.
  - Like UDP, it is a layer 4 protocol. Being connection-oriented, it requires the establishment of a TCP connection before any data can be sent.
  - In TCP, each data octet has a sequence number; this makes it easy for the receiver to identify lost or duplicated packets.



- A TCP connection is established using what's called a three-way handshake. Two flags are used: SYN (Synchronize) and ACK (Acknowledgment). The packets are sent as follows:
  - SYN Packet: The client initiates the connection by sending a SYN packet to the server. This packet contains the client's randomly chosen initial sequence number.
  - SYN-ACK Packet: The server responds to the SYN packet with a SYN-ACK packet, which adds the initial sequence number randomly chosen by the server.
  - ACK Packet: The three-way handshake is completed as the client sends an ACK packet to acknowledge the reception of the SYN-ACK packet.

Dynamic Host Configuration Protocol (DHCP)

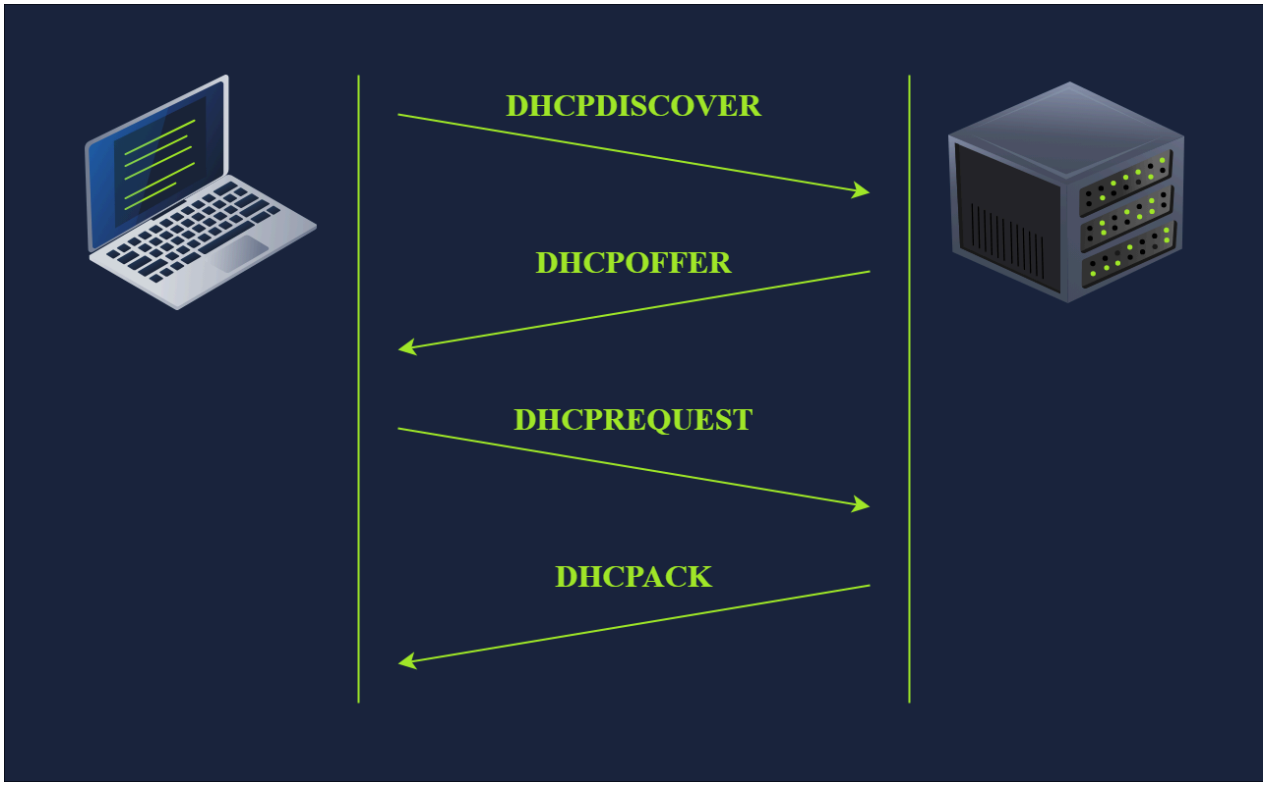
- What is DHCP?
  - DHCP (Dynamic Host Configuration Protocol) is an application-level protocol that relies on UDP; the server

listens on UDP port 67, and the client sends from UDP port 68. Your smartphone and laptop are configured to use DHCP by default.

- How Does DHCP Work?

- DHCP follows four steps: Discover, Offer, Request, and Acknowledge (DORA):

- DHCP Discover: The client broadcasts a DHCPDISCOVER message seeking the local DHCP server if one exists.
- DHCP Offer: The server responds with a DHCPOFFER message with an IP address available for the client to accept.
- DHCP Request: The client responds with a DHCPREQUEST message to indicate that it has accepted the offered IP.
- DHCP Acknowledge: The server responds with a DHCPACK message to confirm that the offered IP address is now assigned to this client.



- Example DHCP Packet Capture

```
Terminal

user@TryHackMe$ tshark -r DHCP-G5000.pcap -n
    1   0.000000      0.0.0.0 → 255.255.255.255 DHCP 342 DHCP Discover
    2   0.013904 192.168.66.1 → 192.168.66.133 DHCP 376 DHCP Offer
    3   4.115318      0.0.0.0 → 255.255.255.255 DHCP 342 DHCP Request
    4   4.228117 192.168.66.1 → 192.168.66.133 DHCP 376 DHCP ACK
```

Address Resolution Protocol (ARP)

- Background info on why ARP
  - Whenever one host needs to communicate with another host on the same Ethernet or WiFi, it must send the IP packet within a data link layer frame. Although it knows the IP address of the target host, it needs to look up the target's MAC address so the proper data link header can be created.

- What is ARP and What does it do?
  - Address Resolution Protocol (ARP) makes it possible to find the MAC address of another device on the Ethernet.

Network Address Translation (NAT)

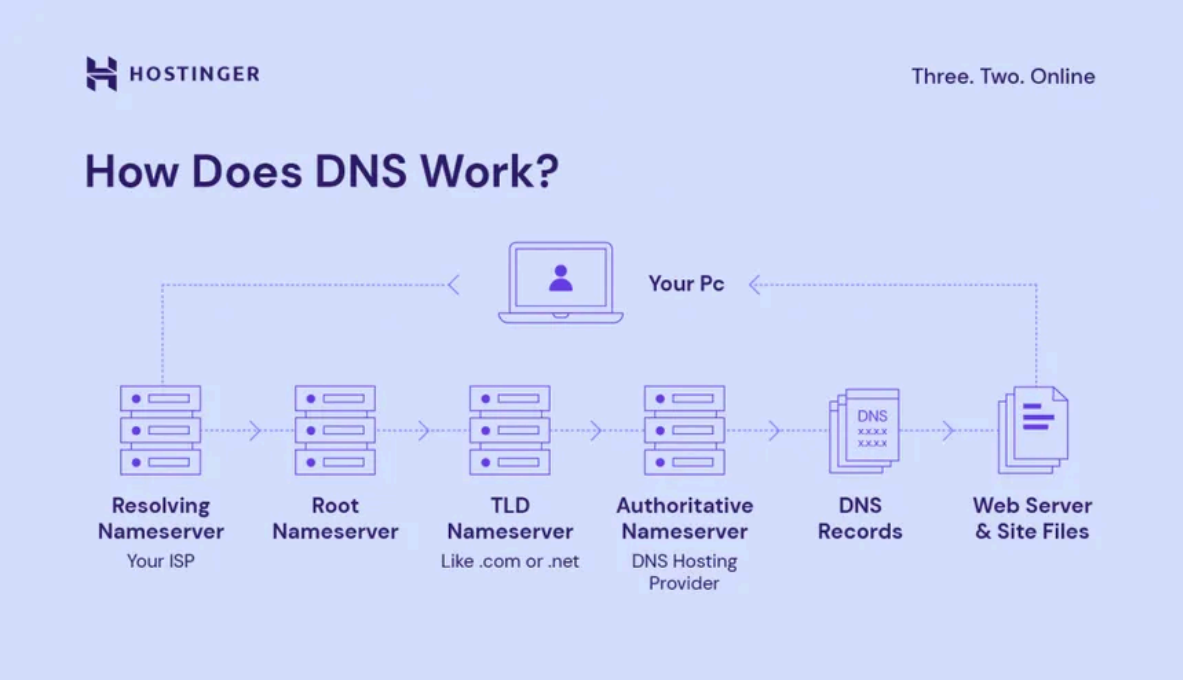
- Translates private (RFC 1918) IP addresses to a public IP on egress (out-going), conserving global address space.
- Two common types:
- Source NAT (SNAT) for outbound traffic (many → one).
- Destination NAT (DNAT) for inbound/load-balanced traffic (one→many).
- Keeps internal topology hidden and helps with basic firewalling.

Internet Control Message Protocol (ICMP)

- A "companion" to IP used for diagnostics and error reporting.
- Ping sends ICMP Echo Request/Reply to test reachability and measure round-trip time.
- Traceroute exploits TTL-expired ICMP Time - Exceeded replies to map the path (hop-by-hop) to a destination.

Domain Name System (DNS)

- A hierarchical, distributed database that maps human-readable names (www.example.com) to IP addresses.
- Queries travel from your PC → Resolving Name Server → Root Nameserver → TLD (Top Level Domain) → Authoritative Nameserver → DNS Records → Web Server & Site Files.



- Caching at each step accelerates lookups and reduces load.

SSL/TLS

- TLS (Transport Layer Security) is the modern protocol (successor to SSL) operating at the transport layer to provide:
- Confidentiality (encryption), integrity (MAC), and optional authentication (certificates).
- Handshake negotiates a cipher suite, exchanges keys (often via RSA or ECDHE), then secures application data.
- SSL is the deprecated predecessor (SSL 2.0/3.0), now replaced entirely by TLS 1.2/1.3.

SSH

- SSH (Secure Shell) is a protocol for secure remote login and other network services over an insecure network.
- It operates on port 22 by default.

- It provides encryption, integrity, and strong authentication using algorithms like AES, HMAC, and Diffie-Hellman key exchange.
- It supports password and public-key authentication (RSA, ECDSA, Ed25519).
- It enables secure remote command execution and interactive shell sessions.
- It provides port forwarding (local, remote, dynamic) and X11 forwarding.
- It includes SFTP for secure file transfer over the same encrypted channel.

HTTP/HTTPS and SFTP/FTP

- HTTP (port 80) is the stateless, text-based protocol for web traffic.
- HTTPS (port 443) wraps HTTP in TLS to secure web sessions.
- FTP (ports 20/21) provides separate control/data channels, no built-in encryption.
- SFTP (port 22) is SSH-based file transfer: single encrypted channel, integrated with SSH authentication.

SMTP/S, POP3/S, and IMAP/S (Email protocols)

- SMTP (port 25/587) is used by mail clients/servers to send and relay outgoing mail.
- POP3 (port 110/995) lets a client download mail from the server, typically removing it from the server.
- IMAP (port 143/993) lets a client view/manipulate mail folders on the server, keeping mail synchronized across devices.