Networking Essentials

DHCP

Whenever we want to access a network, at the very least, we need to configure the following:

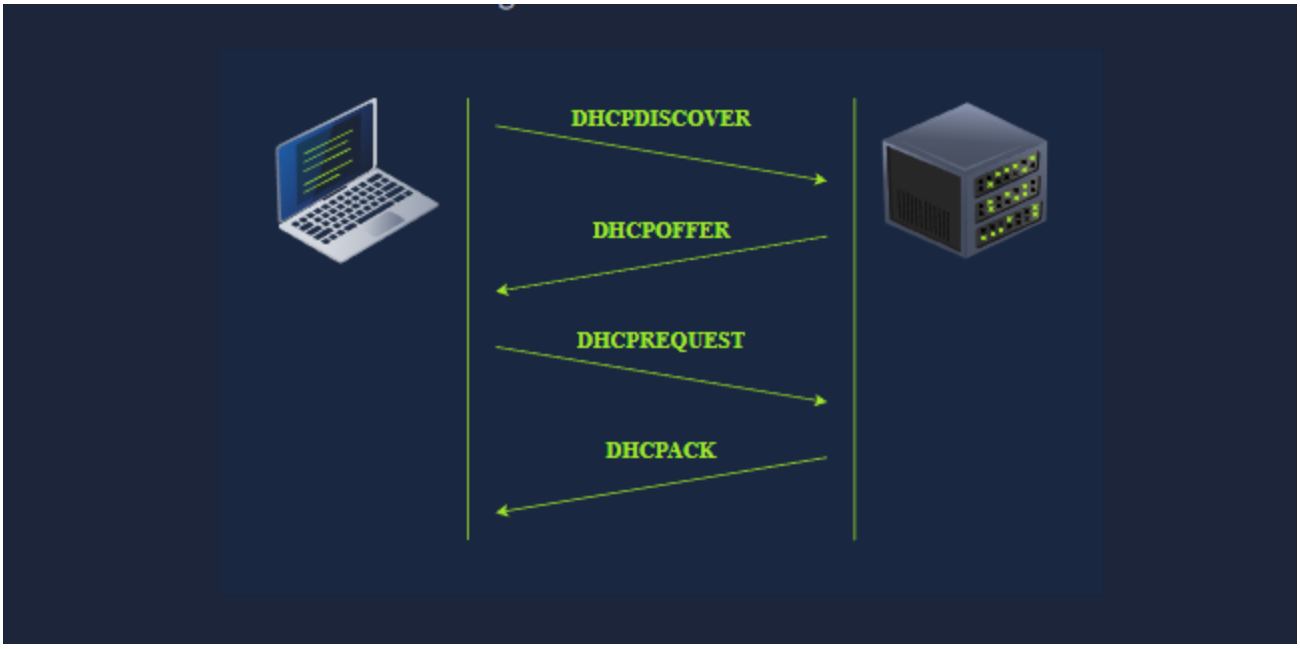
- IP address along with subnet mask
- Router (or gateway)
- DNS server

DHCP application level protocol that relies on UDP the server listens on **UDP port 67** and the client sends from **UDP port 68**

it provides a way to automatically configures to a new network without having to configure IP, router and DNS sever manually.

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

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



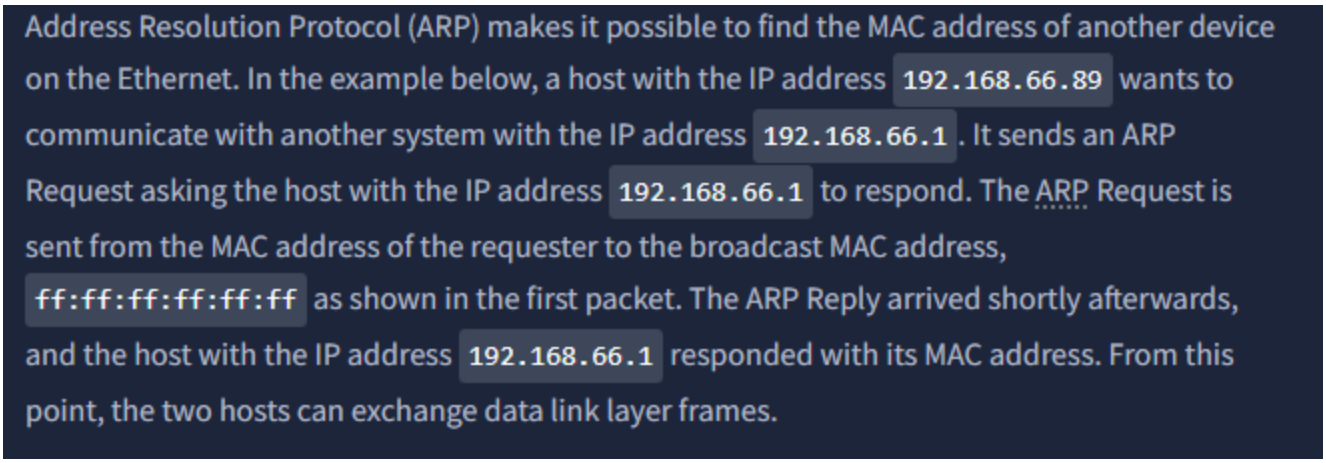
we expect that the DHCP server has provided us with the following:

- The leased IP address to access network resources
- The gateway to route our packets outside the local network
- A DNS server to resolve domain names

Destination IP address that a client uses when it sends a DHCP Discover packet is 255.255.255.255

he source IP address a client uses when trying to get IP network configuration over DHCP is 0.0.0.0

ARP



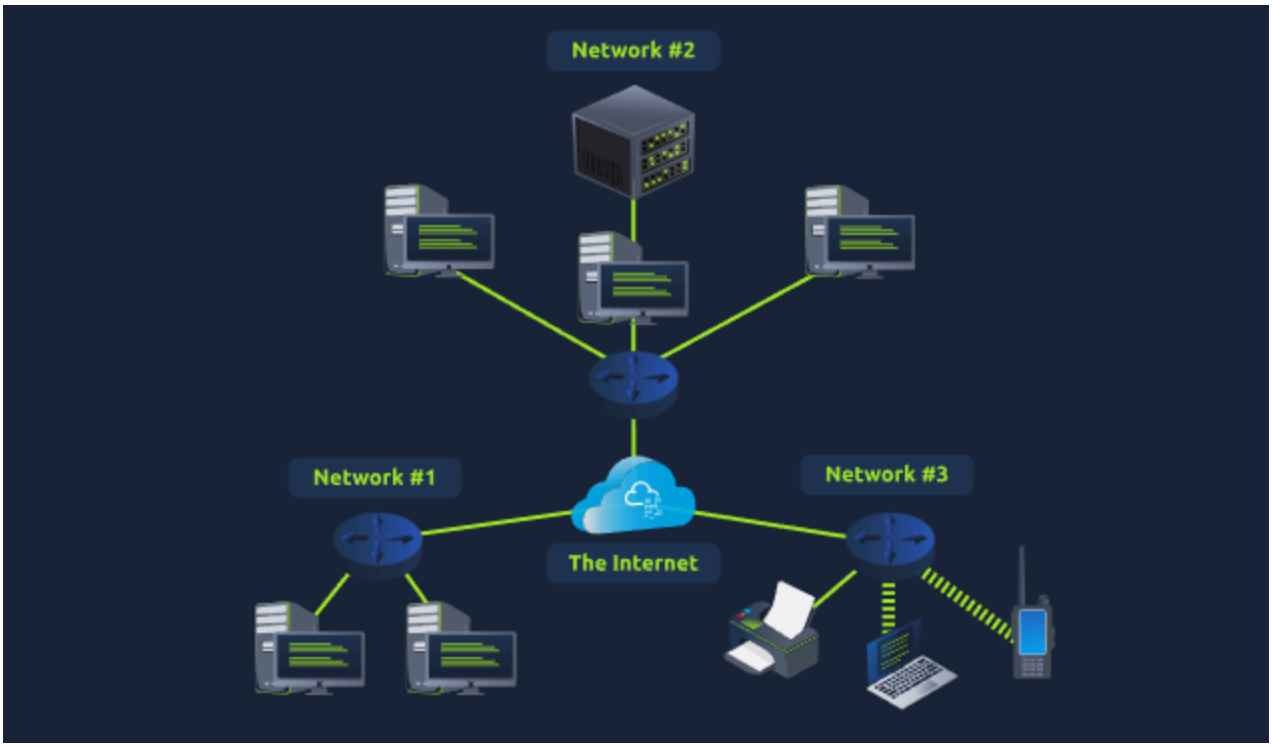
ICMP

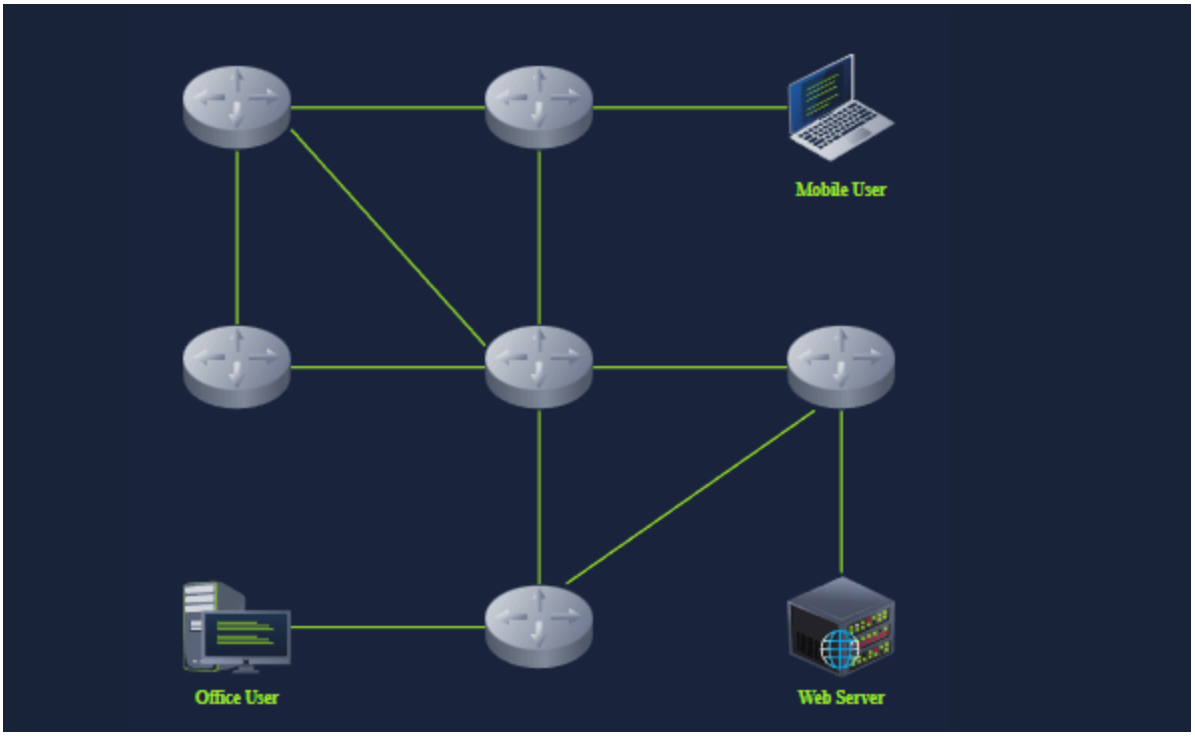
Internet Control Message Protocol (ICMP) is mainly used for network diagnostics and error reporting

Two popular commands rely on ICMP, and they are instrumental in network troubleshooting and network security. The commands are:

- `ping` : This command uses ICMP to test connectivity to a target system and measures the round-trip time (RTT). In other words, it can be used to learn that the target is alive and that its reply can reach our system.
- `traceroute` : This command is called `traceroute` on Linux and UNIX-like systems and `tracert` on MS Windows systems. It uses ICMP to discover the route from your host to the target.

Routing





few routing protocols so that you become familiar with their names:

- **OSPF (Open Shortest Path First)**: OSPF is a routing protocol that allows routers to share information about the network topology and calculate the most efficient paths for data transmission. It does this by having routers exchange updates about the state of their connected links and networks. This way, each router has a complete map of the network and can determine the best routes to reach any destination.
- **EIGRP (Enhanced Interior Gateway Routing Protocol)**: EIGRP is a Cisco proprietary routing protocol that combines aspects of different routing algorithms. It allows routers to

share information about the networks they can reach and the cost (like bandwidth or delay) associated with those routes. Routers then use this information to choose the most efficient paths for data transmission.

- **BGP (Border Gateway Protocol)**: BGP is the primary routing protocol used on the Internet. It allows different networks (like those of Internet Service Providers) to exchange routing information and establish paths for data to travel between these networks. BGP helps ensure data can be routed efficiently across the Internet, even when traversing multiple networks.
- **RIP (Routing Information Protocol)**: RIP is a simple routing protocol often used in small networks. Routers running RIP share information about the networks they can reach and the number of hops (routers) required to get there. As a result, each router builds a routing table based on this information, choosing the routes with the fewest hops to reach each destination.

NAT (Network Address Translation)

NAT is a solution to address depletion

the idea behind NAT lies in using **one public IP address** to provide Internet access to **many private IP addresses**

connecting a company with twenty computers, you can provide Internet access to all twenty computers by using a single public IP address instead of twenty public IP addresses.