Networking Essentials

Learned:

- DHCP automatically assigns an IP address to a client after the steps of discover offer, request, and Acknowledgment.

- An ARP request is used to find the MAC address linked to a IP address. It includes the source MAC address and asks who has the destination IP, so the device that owns it can reply with its MAC address. This allows data to be sent between the two devices.

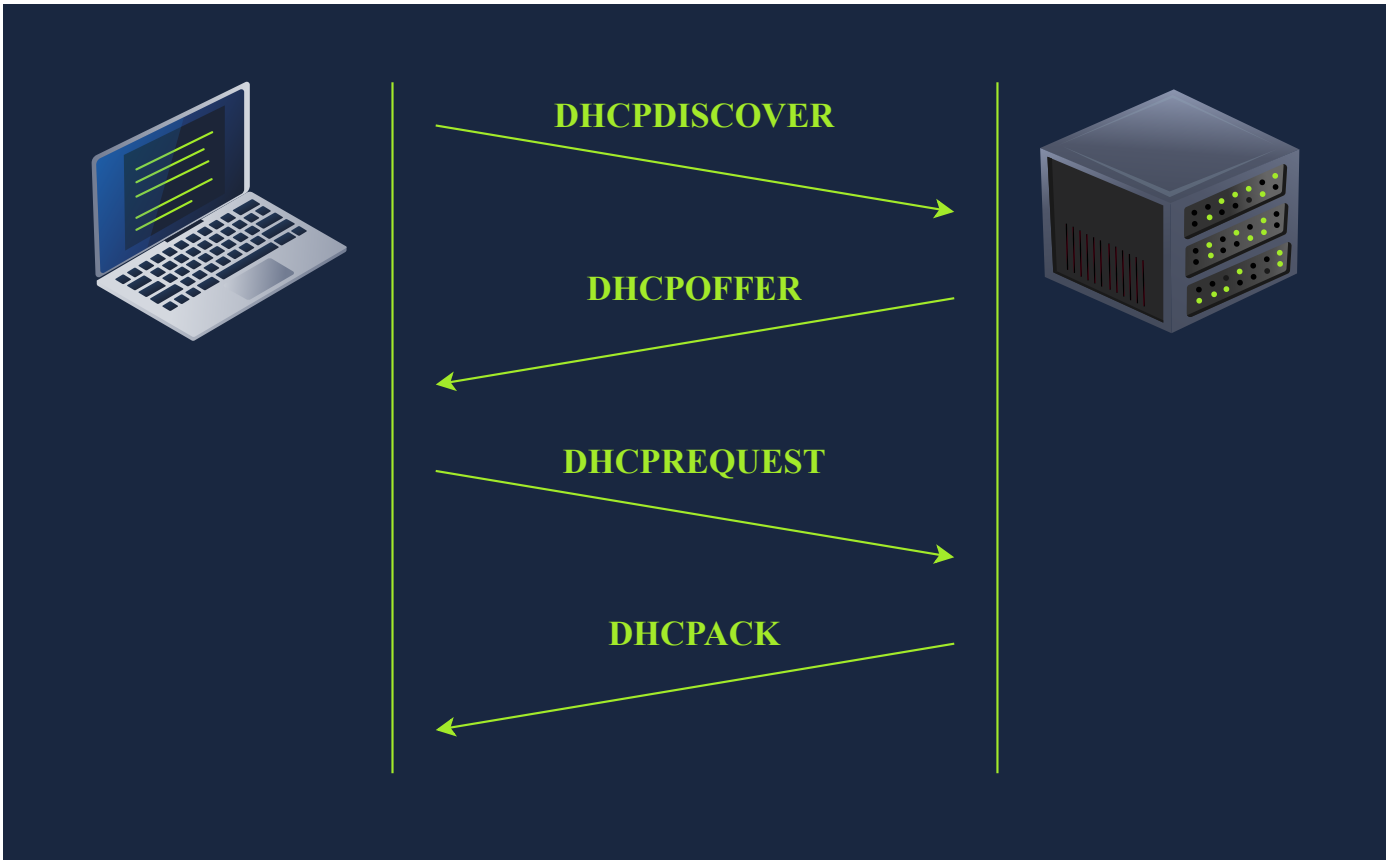
- ICMP is used to check the status of devices on a network. Commands like `ping` and `traceroute` use ICMP to measure how long packets take to travel and to see if any packets are lost along the way.

- NAT converts private IP addresses into a public IP address, allowing multiple devices on a local network to access the internet using a public IP.

DHCP

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.



The following packet capture shows the four steps explained above. In this example, the client gets the IP address `192.168.66.133`.

Terminal

```
user@TryHackMe$ tshark -r DHCP-G5000.pcap -n
    1   0.000000      0.0.0.0 → 255.255.255.255 DHCP 342 DHCP Discover -
Transaction ID 0xfb92d53f
    2   0.013904 192.168.66.1 → 192.168.66.133 DHCP 376 DHCP Offer    - Transaction
ID 0xfb92d53f
    3   4.115318      0.0.0.0 → 255.255.255.255 DHCP 342 DHCP Request  -
Transaction ID 0xfb92d53f
    4   4.228117 192.168.66.1 → 192.168.66.133 DHCP 376 DHCP ACK      - Transaction
ID 0xfb92d53f
```

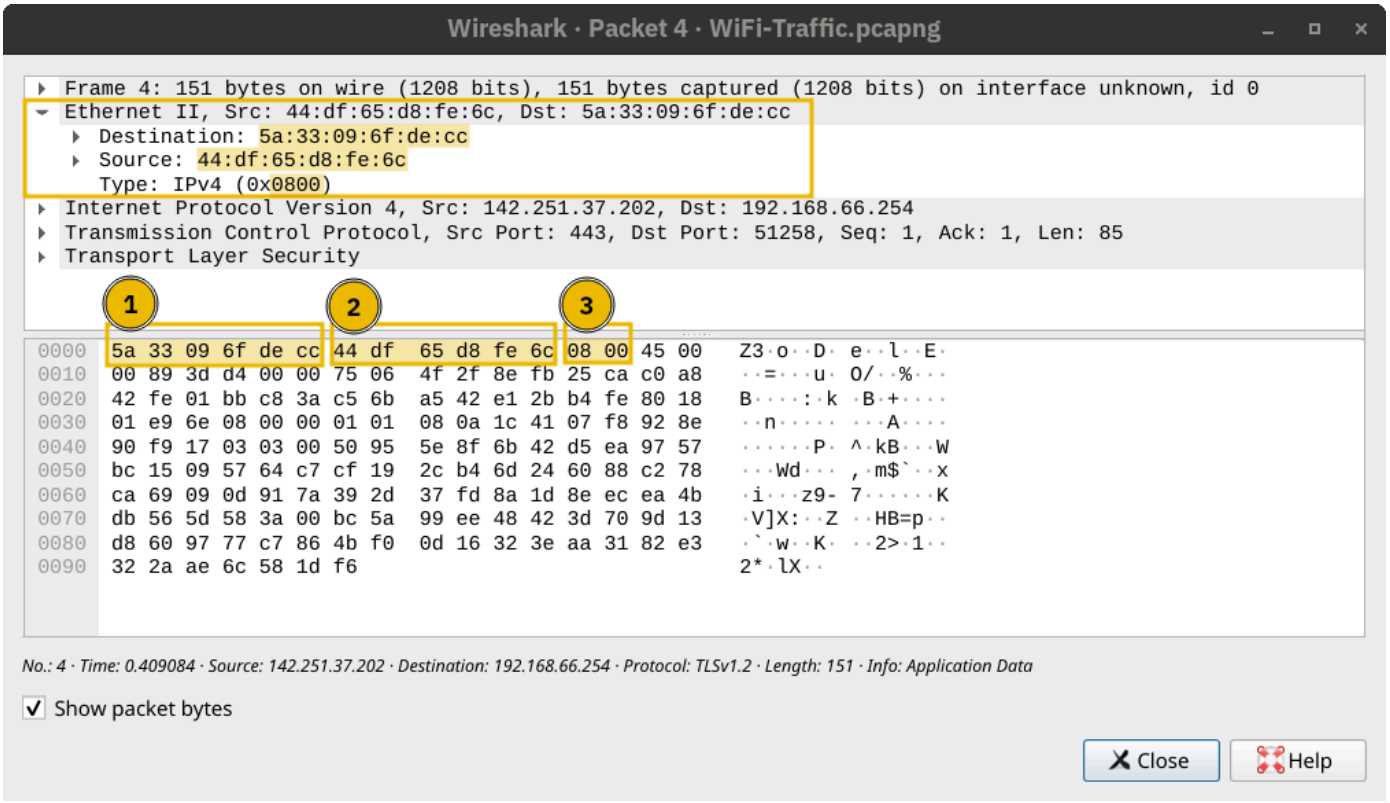
- The client starts without any IP network configuration. It only has a MAC address. In the first and third packets, DHCP Discover and DHCP Request, the client searching for a DHCP server still has no IP network configuration and has not yet used the DHCP server's offered IP address. Therefore, it sends packets from the IP address `0.0.0.0` to the broadcast IP address `255.255.255.255`.
- As for the link layer, in the first and third packets, the client sends to the broadcast MAC address, `ff:ff:ff:ff:ff:ff` (not shown in the output above). The DHCP server offers an available IP address along with the network configuration in the DHCP offer. It uses the client's destination MAC address. (It used the proposed IP address in this example system.)

At the end of the DHCP process, our device would have received all the configuration needed to access the network or even the Internet.

ARP

In the screenshot below, we see an IP packet within an Ethernet frame. The Ethernet frame header contains:

- Destination MAC address
- Source MAC address
- Type (IPv4 in this case)



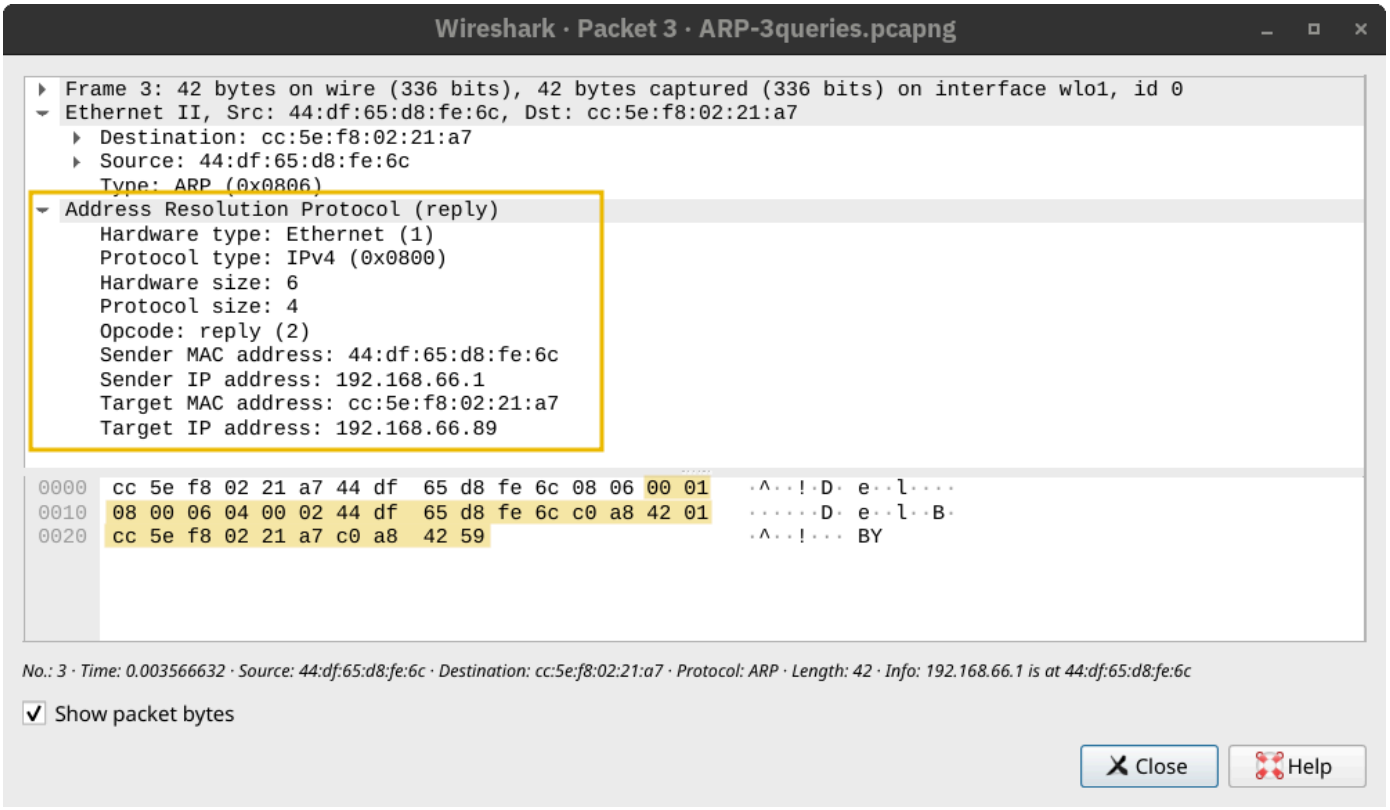
Address Resolution Protocol (ARP) makes it possible to find the MAC address of another device on the Ethernet. In the example below, a host with the IP address `192.168.66.89` wants to communicate with another system with the IP address `192.168.66.1`. It sends an ARP Request asking the host with the IP address `192.168.66.1` to respond. The ARP Request is sent from the MAC address of the requester to the broadcast MAC address, `ff:ff:ff:ff:ff:ff` as shown in the first packet. The ARP Reply arrived shortly afterwards, and the host with the IP address `192.168.66.1` responded with its MAC address. From this point, the two hosts can exchange data link layer frames.

Terminal

```
user@TryHackMe$ tshark -r arp.pcapng -Nn
    1 0.000000000 cc:5e:f8:02:21:a7 → ff:ff:ff:ff:ff:ff ARP 42 Who has
192.168.66.1? Tell 192.168.66.89
```

```
    2 0.003566632 44:df:65:d8:fe:6c → cc:5e:f8:02:21:a7 ARP 42 192.168.66.1 is at
44:df:65:d8:fe:6c
```

An ARP Request or ARP Reply is not encapsulated within a UDP or even IP packet; it is encapsulated directly within an Ethernet frame.

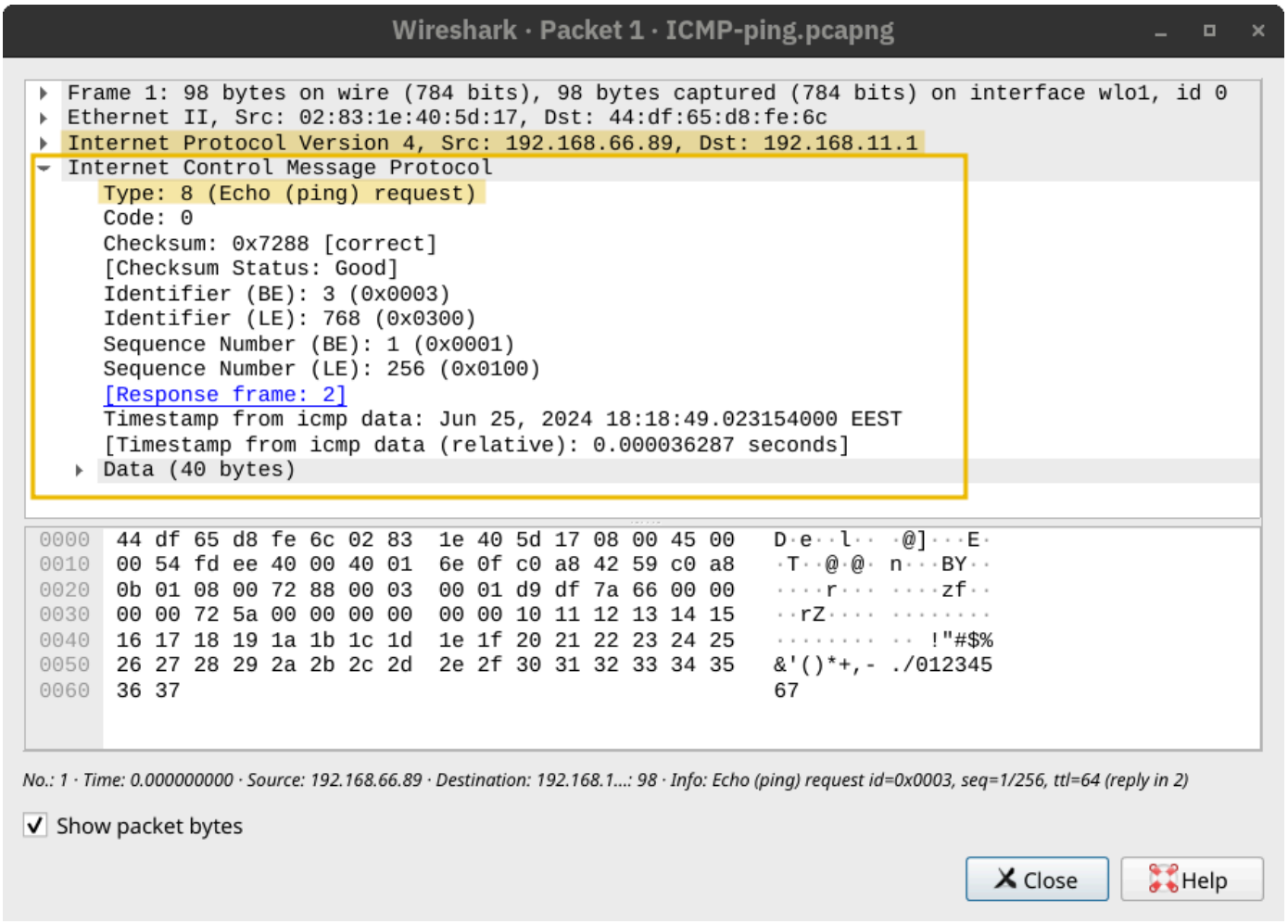


ICMP

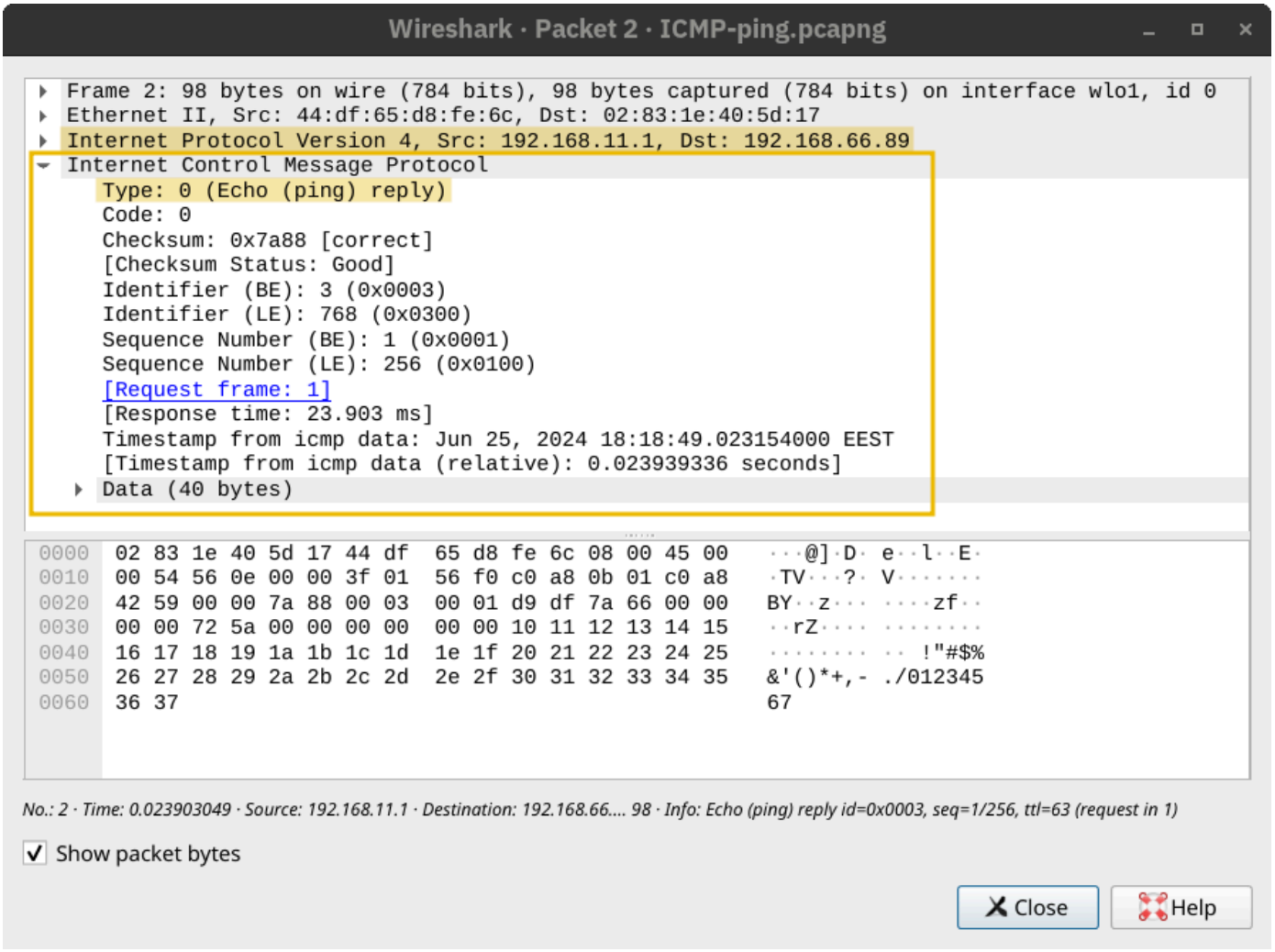
Internet Control Message Protocol (ICMP) is mainly used for network diagnostics and error reporting. Two popular commands rely on ICMP, and they are instrumental in network troubleshooting and network security. The commands are:

- `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.

Ping



The computer on the receiving end responds with an ICMP Echo Reply (ICMP Type `0`).



Many things might prevent us from getting a reply. In addition to the possibility of the target system being offline or shut down, a firewall along the path might block the necessary packets for `ping` to work. In the example below, we used `-c 4` to tell the `ping` command to stop after sending four packets.

Terminal

```
user@TryHackMe$ ping 192.168.11.1 -c 4
PING 192.168.11.1 (192.168.11.1) 56(84) bytes of data.
64 bytes from 192.168.11.1: icmp_seq=1 ttl=63 time=11.2 ms
64 bytes from 192.168.11.1: icmp_seq=2 ttl=63 time=3.81 ms
64 bytes from 192.168.11.1: icmp_seq=3 ttl=63 time=3.99 ms
64 bytes from 192.168.11.1: icmp_seq=4 ttl=63 time=23.4 ms

--- 192.168.11.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 3.805/10.596/23.366/7.956 ms
```

The output shows no packet loss; moreover, it calculates the minimum, average, maximum, and standard deviation (mdev) of the round-trip time (RTT).

Traceroute

The Internet protocol has a field called Time-to-Live (TTL) that indicates the maximum number of routers a packet can travel through before it is dropped. The router decrements the packet's TTL by one before it sends it across. When the TTL reaches zero, the router drops the packet and sends an ICMP Time Exceeded message (ICMP Type `11`). (In this context, "time" is measured in the number of routers, not seconds.)

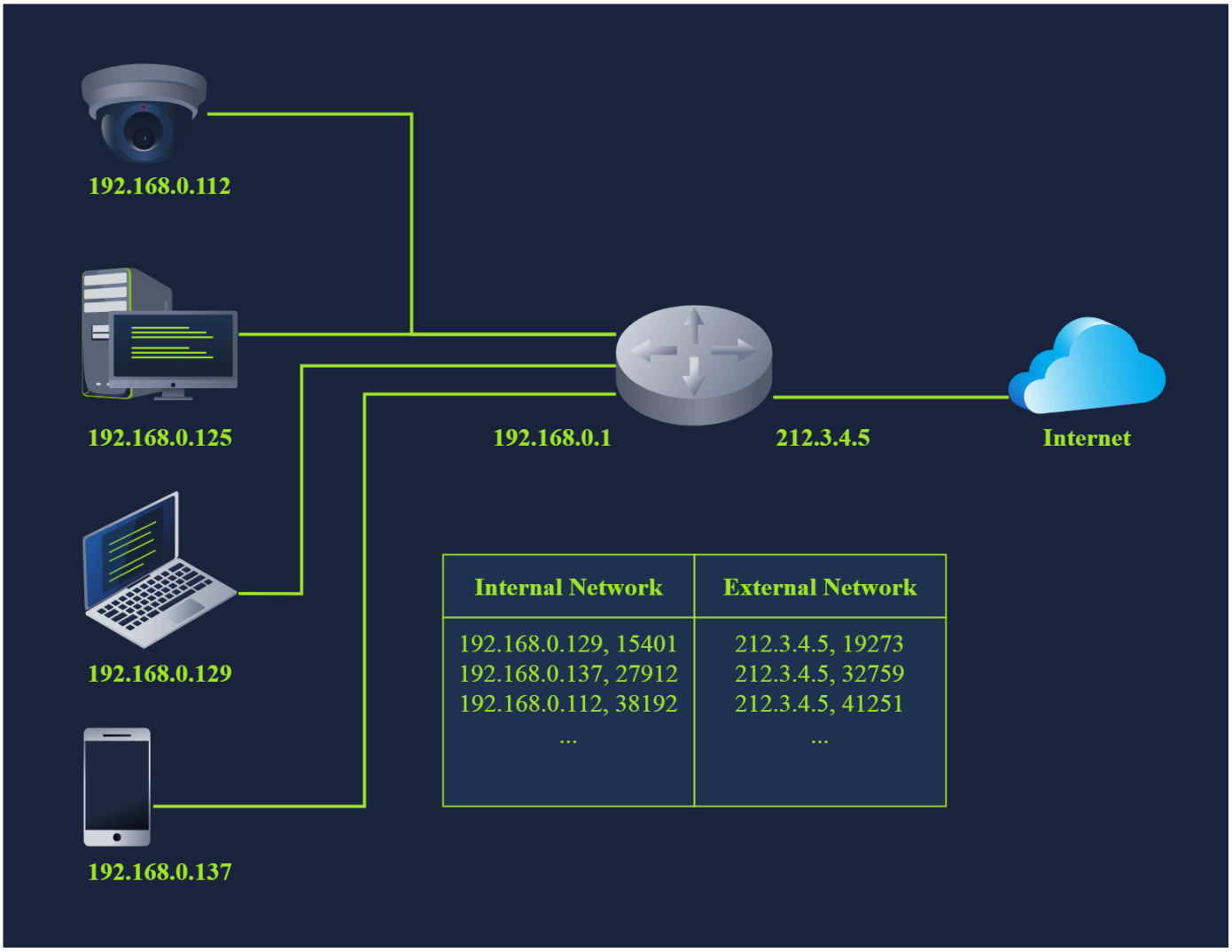
The terminal output below shows the result of running `traceroute` to discover the routers between our system and `example.com`.

Routing

- **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

The idea behind NAT lies in using **one public IP address** to provide Internet access to **many private IP addresses**. In other words, if you are 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.


192.168.0.112
192.168.0.125
192.168.0.129
192.168.0.137
192.168.0.1
212.3.4.5
Internet
Internal Network
External Network
192.168.0.129, 15401
192.168.0.137, 27912
192.168.0.112, 38192
...
212.3.4.5, 19273
212.3.4.5, 32759
212.3.4.5, 41251
...