```
kpacu@Krasi-HP:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
Krasi-HP.mshome.net      ether   00:15:5d:c1:84:9b   C                     eth0

kpacu@Krasi-HP:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         Krasi-HP.mshome 0.0.0.0         UG    0      0        0 eth0
172.18.176.0    0.0.0.0         255.255.240.0   U     0      0        0 eth0

kpacu@Krasi-HP:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  Krasi-HP.mshome.net (172.18.176.1)  0.519 ms  0.482 ms  0.461 ms
 2  192.168.0.1 (192.168.0.1)  37.839 ms  34.720 ms  39.302 ms
 3  193.238.174.7 (193.238.174.7)  15.605 ms  19.038 ms  21.940 ms
 4  border1.ssi.bg (193.238.174.1)  26.715 ms  30.427 ms  25.114 ms
 5  185.178.4.129 (185.178.4.129)  44.118 ms  45.934 ms  48.622 ms
 6  google.bix.bg (193.169.198.80)  49.822 ms  48.420 ms  49.897 ms
 7  108.170.250.177 (108.170.250.177)  50.789 ms 108.170.250.161 (108.170.250.161)
16.183 ms 142.251.92.65 (142.251.92.65)  36.508 ms
 8  142.250.60.187 (142.250.60.187)  43.198 ms 142.250.212.21 (142.250.212.21)  42.978
ms 142.251.246.235 (142.251.246.235)  41.450 ms
 9  dns.google (8.8.8.8)  27.623 ms  28.238 ms  26.679 ms
```

Why would you need to use the ping command?
Testing network connectivity: The ping command is often used to test if a networked device, such as a server or router, is reachable on the network. This can help **diagnose connectivity** issues and determine if there are any network-related **problems**.

Troubleshooting network problems: If you are experiencing network connectivity problems, using the ping command can help you identify where the issue might be occurring. If you are unable to ping a device on the network, it indicates that the issue might be with the device or service you are trying to access.
Checking **latency**: The ping command can be used to measure the time it takes for a packet to travel from your device to another device on the network and back again. This can help identify latency or performance issues on the network.

Testing DNS resolution: The ping command can also be used to test if DNS resolution is working correctly. By pinging a domain name, you can verify if the domain name is resolving to the correct IP address.

Checking for **packet loss**: The ping command can be used to check for packet loss on the network. If packets are lost when pinging a device, it may indicate that there is an issue with the network connection or the device being pinged.

Overall, the ping command is a versatile tool for troubleshooting and diagnosing network issues. It provides quick and easy feedback about network connectivity, latency, and packet loss, making it an essential tool for network administrators and IT professionals.

Write down the TCP/UDP ports of the most commonly used services bellow.
HTTP - TCP80
SNMP - UDP161
HTTPS - TCP443
DNS client - UDP53/TCP53
DNS zone transfer - TCP53
SMTP - TCP25
SSH - TCP22
FTP - TCP21
Telnet - TCP23
MSSQL - TCP1433/UDP1434
MySQL - TCP3306
PostgreSQL - TCP5432
RDP (Remote Desktop Protocol) - TCP3389
NTP - UDP123
NFS - TCP2049/UDP2049

For each of the packet locations shown, 1 to 4 write down the source and destination MAC addresses of the packet as it travels across the network interfaces.
1. The laptop initiates communication with the web server and prepares a packet. What would the packet look like at this stage?
SRC IP: 100.20.30.10/24
DST IP: 80.70.60.100/24
SRC MAC: AA:AA:AA:33:33:33
DST MAC: BB.BB.BB.11.11.01
2. RTR1 receives the packet on its IF-LAN interface, prepares it accordingly and forwards it out its IFWAN. What would the packet look like at this stage?
SRC IP: 100.20.30.10/24
DST IP: 80.70.60.100/24
SRC MAC: BB.BB.BB.11.11.01
DST MAC: CC.CC.CC.22.22.01
3. RTR2 receives the packet on its IF-WAN interface, prepares it accordingly and forwards it out via IFLAN. What would the packet look like at this stage?
SRC IP: 100.20.30.10/24
DST IP: 80.70.60.100/24
SRC MAC: CC.CC.CC.22.22.01
DST MAC: DD.DD.DD.77.77.77
4. The web server receives the packet and prepares a response packet back. What would the packet look like at this stage?
SRC IP: 80.70.60.100/24
DST IP: 100.20.30.10/24
SRC MAC: DD.DD.DD.77.77.77
DST MAC: CC.CC.CC.22.22.01

Since we are talking about web traffic (www) in the example, which transport layer protocol will most probably be used?
TCP

If we do a traffic analysis with a network packet monitoring tool like WireShark, what can we expect to see for the source and destination ports when the laptop sends the packet?
SRC PORT: A random port number assigned by the laptop's operating system from the range of available ephemeral ports (typically 49152 to 65535).
DST PORT: Port number 80, which is the default port used by HTTP for communication with web servers. If the web server is using HTTPS (HTTP Secure), the destination port will be 443 instead.

Similarly, and vice versa, what can we expect to see as destination ports when the Web server sends a response packet back?
SRC PORT: Port number 80 (or 443 for HTTPS), which is the port used by the web server to communicate with the client.
DST PORT: The same port number used as the source port in the original request, which will be a random ephemeral port number assigned by the laptop's operating system.

How many broadcast domains are there in the exhibit shown?
6

Analyze the TCP's three-way handshake and using screenshots from the Wireshark window answer the questions bellow:
1. What is the source IP (of the initiating host): 192.168.0.110
2. What is the destination IP? (target website): 91.215.216.43

Identify the Network Interface (Layer 1 & 2) section of the SYN packet and paste a screenshot from it:
Layer 1:
Frame Length: 66 bytes (528 bits)
Capture Length: 66 bytes (528 bits)
Layer 2:
Encapsulation type: Ethernet (1)
Source MAC address: HewlettP_59:df:6c (ac:e2:d3:59:df:6c)
Destination MAC address: Cisco_bd:be:fe (e0:2f:6d:bd:be:fe)

Identify the Network Layer 3 section of the SYN/ACK packet and paste a screenshot from it:
Layer 3:
Protocol: Internet Protocol Version 4
Source IP address: 192.168.0.110
Destination IP address: 91.215.216.43

Identify the Transport Layer 4 section of the ACK packet and paste a screenshot from it bellow:
Transmission Control Protocol, Src Port: 4664, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
Source Port: 4664
Destination Port: 443
Sequence Number: 1 (relative sequence number)
Acknowledgment Number: 1 (relative ack number)

Flags: 0x010 (ACK)
....1 .... = Acknowledgment: Set

Who is the owner of the destination MAC address of the SYN packet?
Cisco_bd:be:fe (e0:2f:6d:bd:be:fe)