**Exercise 1 – Basic network stuff Difficulty: Easy**

***Use the arp command and paste the output from the arp table on your system:***

**Interface: 192.168.1.106 --- 0x14**

**Internet Address Physical Address Type**

**192.168.1.1 50-0f-f5-e6-17-08 dynamic**

**192.168.1.255 ff-ff-ff-ff-ff-ff static**

**224.0.0.22 01-00-5e-00-00-16 static**

**224.0.0.251 01-00-5e-00-00-fb static**

**224.0.0.252 01-00-5e-00-00-fc static**

**239.255.255.250 01-00-5e-7f-ff-fa static**

**255.255.255.255 ff-ff-ff-ff-ff-ff static**

**Interface: 172.17.176.1 --- 0x34**

**Internet Address Physical Address Type**

**172.17.191.255 ff-ff-ff-ff-ff-ff static**

**224.0.0.22 01-00-5e-00-00-16 static**

**224.0.0.251 01-00-5e-00-00-fb static**

**224.0.0.252 01-00-5e-00-00-fc static**

**239.255.255.250 01-00-5e-7f-ff-fa static**

**Use the route command and paste the output from the routing table on your system:**

**===========================================================================**

**Interface List**

**18...18 67 b0 32 e6 68 ......Realtek PCIe GbE Family Controller**

**11...c8 f7 33 f5 37 d3 ......Microsoft Wi-Fi Direct Virtual Adapter**

**13...ca f7 33 f5 37 d2 ......Microsoft Wi-Fi Direct Virtual Adapter #2**

**20...c8 f7 33 f5 37 d2 ......Intel(R) Centrino(R) Advanced-N 6235**

**7...c8 f7 33 f5 37 d6 ......Bluetooth Device (Personal Area Network)**

**1...........................Software Loopback Interface 1**

**52...00 15 5d 88 fa cb ......Hyper-V Virtual Ethernet Adapter**

**===========================================================================**

**IPv4 Route Table**

**===========================================================================**

**Active Routes:**

**Network Destination Netmask Gateway Interface Metric**

**0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.106 50**

**127.0.0.0 255.0.0.0 On-link 127.0.0.1 331**

**127.0.0.1 255.255.255.255 On-link 127.0.0.1 331**

**127.255.255.255 255.255.255.255 On-link 127.0.0.1 331**

**172.17.176.0 255.255.240.0 On-link 172.17.176.1 5256**

**172.17.176.1 255.255.255.255 On-link 172.17.176.1 5256**

**172.17.191.255 255.255.255.255 On-link 172.17.176.1 5256**

**192.168.1.0 255.255.255.0 On-link 192.168.1.106 306**

**192.168.1.106 255.255.255.255 On-link 192.168.1.106 306**

**192.168.1.255 255.255.255.255 On-link 192.168.1.106 306**

**224.0.0.0 240.0.0.0 On-link 127.0.0.1 331**

**224.0.0.0 240.0.0.0 On-link 192.168.1.106 306**

**224.0.0.0 240.0.0.0 On-link 172.17.176.1 5256**

**255.255.255.255 255.255.255.255 On-link 127.0.0.1 331**

**255.255.255.255 255.255.255.255 On-link 192.168.1.106 306**

**255.255.255.255 255.255.255.255 On-link 172.17.176.1 5256**

**===========================================================================**

**Persistent Routes:**

**None**

**IPv6 Route Table**

**===========================================================================**

**Active Routes:**

**If Metric Network Destination Gateway**

**1 331 ::1/128 On-link**

**20 306 fe80::/64 On-link**

**52 5256 fe80::/64 On-link**

**52 5256 fe80::f75:1f51:3d93:db68/128**

**On-link**

**20 306 fe80::d2fa:27e1:d177:866a/128**

**On-link**

**1 331 ff00::/8 On-link**

**20 306 ff00::/8 On-link**

**52 5256 ff00::/8 On-link**

**===========================================================================**

**Use the traceroute command on your system and observe the hops to Google’s DNS, 8.8.8.8. Paste the full output from the command bellow showing all the hops from your system to 8.8.8.8.**

**C:\Users\Kochalevski>tracert 8.8.8.8**

**Tracing route to dns.google [8.8.8.8]**

**over a maximum of 30 hops:**

**1 1 ms 1 ms 1 ms 192.168.1.1**

**2 2 ms 1 ms 2 ms 192.168.0.1**

**3 12 ms 8 ms 10 ms 10.183.128.1**

**4 \* \* \* Request timed out.**

**5 \* \* \* Request timed out.**

**6 \* \* \* Request timed out.**

**7 \* \* \* Request timed out.**

**8 13 ms 12 ms 18 ms ctel-78-157-16-209.cabletel.com.mk [78.157.16.209]**

**9 30 ms 32 ms 32 ms 195.3.114.153**

**10 \* 28 ms 30 ms lg22-9070.as8447.a1.net [195.3.64.57]**

**11 \* \* \* Request timed out.**

**12 34 ms 36 ms 36 ms lg59-9071.as8447.a1.net [80.120.167.46]**

**13 38 ms 36 ms 39 ms 209.85.245.45**

**14 35 ms 34 ms 35 ms 209.85.244.145**

**15 36 ms 35 ms 34 ms dns.google [8.8.8.8]**

**Trace complete.**

**Why would you need to use the ping command?**

The command has basic function to confirm network between two hosts also ping command is commonly used for troubleshooting network issues. The ping command also measures the time needed for the package of data to travel.

During live games, ping helps gamers understand how fast their computer is communicating with a gaming server.

In cybersecurity, hackers also use this ping method to check whether they are getting a response back from the host or not.

**Most common TCP/UDP ports**

* HTTP - TCP80
* SNMP - UDP161
* HTTPS - TCP443
* DNS client - UDP53
* DNS zone transfer - TCP53
* SMTP - TCP25
* SSH - TCP22
* FTP - TCP21
* Telnet - TCP23
* MSSQL - TCP1433
* MySQL - TCP3306
* PostgreSQL - TCP5432
* RDP (Remote Desktop Protocol) - TCP3389
* NTP - UDP123
* NFS - UDP2049 (TCP2049 for TCP)

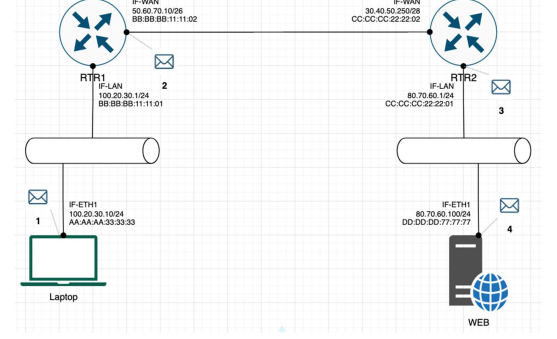
**Exercise 2 – TCP/IP Basics**

**Difficulty: Medium**

Refer to the exhibit and answer the questions below.

The letter symbol ✉, represents the IP packet as it travels across the network.

In the example shown, the laptop attempts to communicate with the web server in question. During its travel the packet will be forwarded across the network nodes and will eventually end up across six network interfaces before it reaches the web server. Each packet as part of the TCP/IP Stack contains fields for the source and destination MAC Address, IP Address and the TCP/UDP Port.



**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:11:11:02
* DST MAC CC:CC:CC:22:22:02

**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: random port with range (49152-65535)
* DST PORT: The destination port could be 443(HTTPS), 80(HTTP), 22(SSH), 25(FMTP) etc.

**Similarly, and vice versa, what can we expect to see as destination ports when the Web server sends a response packet back?**

* SRC PORT: As a source port for the response, we will have the port of the web server used for the communication
* DST PORT: The destination port will be the same port used as a source port when the laptop sent the packet.

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

* There are 3 broadcast domains