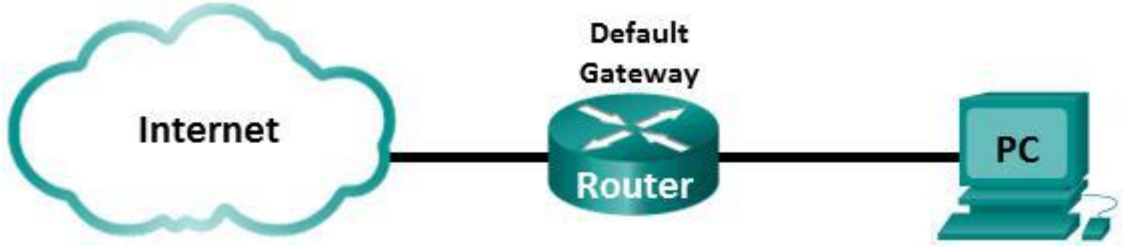
CCNA ITN Lab 1 **Homework** **Deadline: 23.11.2020**

Name: **Rubaiya Kabir Pranti (MatrNum: 11146364)**

Simple Network
and
Internet Access Analysis



PrepExam: **ITN Module Group Exams 1-3**

ITN Module Group Exams 4-7

Tasks: **Ideas about some delays in networks**

IP addressing of a host computer

Wireshark packet capture

Examine ICMP Message Types

Examine DHCP

Homework / Preparation

Ideas about some delays in networks

Read the NP lecture chapter 1 (1. Grundlagen), and calculate the following delays.

a) Propagation delay

In our DN.Lab we have Cat5e twisted pair cabling (signal transmission speed c = 2/3 c_0) with 100BASE-Tx Ethernet technology using a data rate of R = 100 Mbps. Calculate the propagation delay t_{pd} of an Ethernet link with a length of 55m.

Answer: We know,
Propagation delay, $t_{pd=}$ l ⁄ C
where l = length of the link =55m and
C= velocity of the signal through twisted pair cabling =2 ⁄ 3 c_0 = 2 ⁄ 3 × 300.000 km ⁄s=200,000 km ⁄s=$2×10^8$ m ⁄s
Therefore, t_{pd}= l ⁄ C = 55m ⁄ ($2×10^8$) m ⁄s = $2.75×10^{-7}$ s=275 ns

Calculate the propagation delay t_{pd} of a similar link, which would run from TH Köln IWZ to Berlin (~ 600 km).

Answer: From TH Köln IWZ to Berlin (~ 600 km), fiber optic cable is used. Therefore, the C will be same as before.
C= velocity of the signal through fiber optic cabling =2 ⁄ 3 c_0 = 2 ⁄ 3 × 300.000 km ⁄s=200,000 km ⁄s=$2×10^8$ m ⁄s
l = length of the link =600 km (given)
We know,
Propagation delay, $t_{pd=}$ l ⁄ C = ($6×10^5$ m) ⁄ ($2×10^8$) m ⁄s = $3×10^{-3}$ s= 3 ms = 300,0000 ns

b) Transmission time

Transmission time is the time for serial (Bit by Bit) transmission of a data frame. Calculate the transmission time t_t of a 100BASE-Tx NIC transmitting a minimum sized Ethernet frame with a length of 64 Bytes and a maximum sized Ethernet frame with a length of 1518 Bytes.

64 Byte Ethernet frame:
Answer: Transmission time , $t_{t=}$ M⁄R
where M = Size of the frame =64 bytes=64*8=512 bits and
R= Bit rate=100 Mbps=10^8 bit per second
Therefore, t_t= M ⁄ R= 512 bits ⁄ 10^8 bps = $5.12×10^{-6}$ s=5.12 µs

1518 Byte Ethernet frame :
Transmission time , $t_{t=}$ M⁄R
where M = Size of the frame =1518 bytes=1518*8=12144 bits and
R= Bit rate=100 Mbps=10^8 bit per second
Therefore, t_t= M ⁄ R= 12144 bits ⁄ 10^8 bps = $1.2144×10^{-4}$ s=121.44 µs

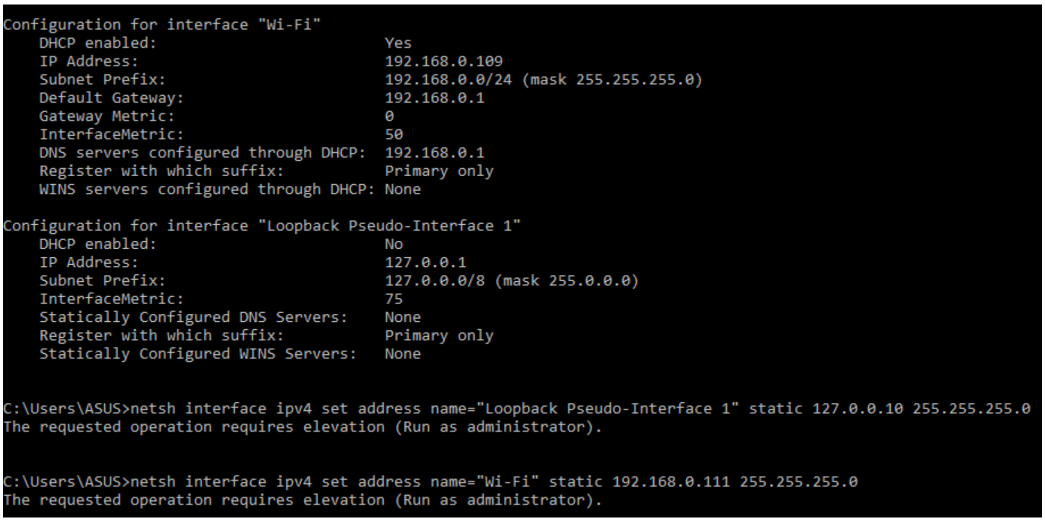
IP addressing of a host computer

There are different ways to configure IP connectivity in Windows or Linux-based PCs from a shell / terminal window / console window.
Research how to configure IP connectivity in PCs.

a) Windows PC

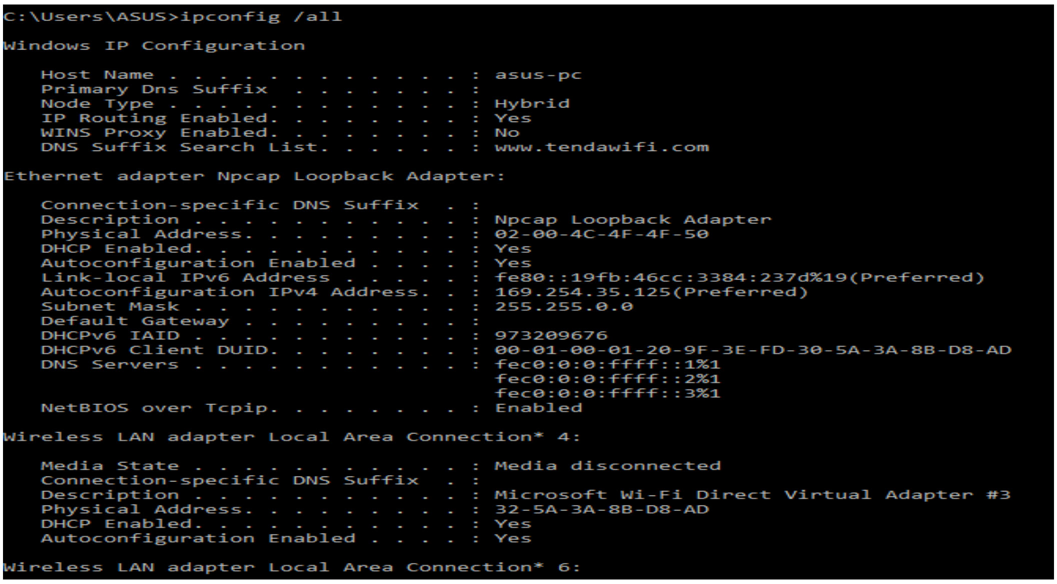
Which command is used to set an IP address and subnet mask?

Answer: In command prompt, the following command is used to set IP address and subnet mask.
For example: ***netsh interface ipv4 set address name="Wi-Fi" static 192.168.0.111 255.255.255.0***

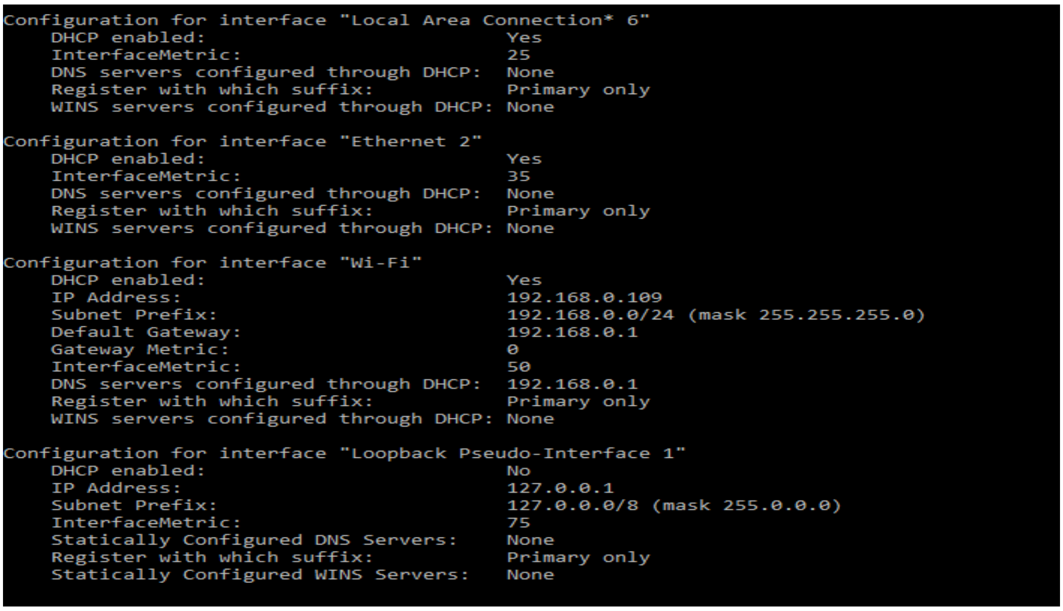


```
Configuration for interface "Wi-Fi"
    DHCP enabled:                         Yes
    IP Address:                           192.168.0.109
    Subnet Prefix:                        192.168.0.0/24 (mask 255.255.255.0)
    Default Gateway:                      192.168.0.1
    Gateway Metric:                       0
    InterfaceMetric:                      50
    DNS servers configured through DHCP:  192.168.0.1
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Loopback Pseudo-Interface 1"
    DHCP enabled:                         No
    IP Address:                           127.0.0.1
    Subnet Prefix:                        127.0.0.0/8 (mask 255.0.0.0)
    InterfaceMetric:                      75
    Statically Configured DNS Servers:    None
    Register with which suffix:           Primary only
    Statically Configured WINS Servers:   None


C:\Users\ASUS>netsh interface ipv4 set address name="Loopback Pseudo-Interface 1" static 127.0.0.10 255.255.255.0
The requested operation requires elevation (Run as administrator).


C:\Users\ASUS>netsh interface ipv4 set address name="Wi-Fi" static 192.168.0.111 255.255.255.0
The requested operation requires elevation (Run as administrator).
```

Which command displays all IP settings?
Answer: In command prompt***, ipconfig /all*** command displays all IP settings.



```
C:\Users\ASUS>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : asus-pc
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : Yes
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : www.tendawifi.com

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Npcap Loopback Adapter
   Physical Address. . . . . . . . . : 02-00-4C-4F-4F-50
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::19fb:46cc:3384:237d%19(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.35.125(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 973209676
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-9F-3E-FD-30-5A-3A-8B-D8-AD
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : 32-5A-3A-8B-D8-AD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 6:
```



```
Configuration for interface "Local Area Connection* 6"
    DHCP enabled:                         Yes
    InterfaceMetric:                      25
    DNS servers configured through DHCP:  None
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Ethernet 2"
    DHCP enabled:                         Yes
    InterfaceMetric:                      35
    DNS servers configured through DHCP:  None
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Wi-Fi"
    DHCP enabled:                         Yes
    IP Address:                           192.168.0.109
    Subnet Prefix:                        192.168.0.0/24 (mask 255.255.255.0)
    Default Gateway:                      192.168.0.1
    Gateway Metric:                       0
    InterfaceMetric:                      50
    DNS servers configured through DHCP:  192.168.0.1
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Loopback Pseudo-Interface 1"
    DHCP enabled:                         No
    IP Address:                           127.0.0.1
    Subnet Prefix:                        127.0.0.0/8 (mask 255.0.0.0)
    InterfaceMetric:                      75
    Statically Configured DNS Servers:    None
    Register with which suffix:           Primary only
    Statically Configured WINS Servers:   None
```

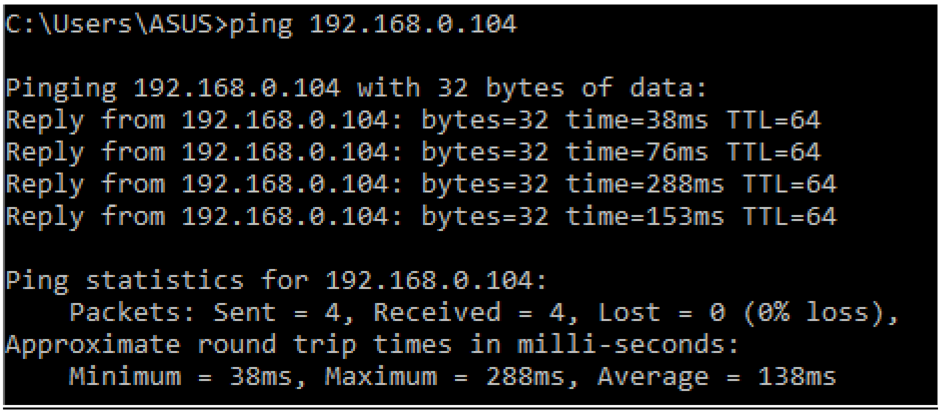
When you open the network configuration tab in your control panel GUI, which options must be configured or are available when configuring IPv4 of an Interface?

Answer: When I open the network configuration tab in my control panel GUI, through following steps I can get two options available for configuring IPv4 address of an interface. And one must be selected for configuration.
Control Panel>Network and Sharing Centre> Change adapter settings>Network connections window>Wi-Fi (or any other active options)>click Properties>click IPv4 version protocol (TCP/IPv4)> IPv4 version protocol (TCP/IPv4) Properties window. There we will get two options:

1. Obtain IP address automatically (which is assigned by DHCP, called Dynamic IP addressing)
2. Use the following IP address (which is done manually, called Static IP addressing)
   -Here, we have to fill up IP address, subnet mask and default gateway by our own.

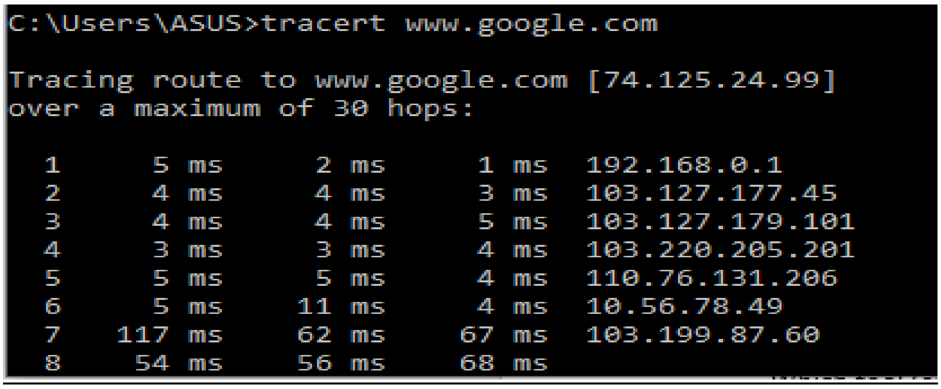
c) Networking tools

Which tool (command) shows, whether a host reachable or not?
Answer: ***ping*** command in command prompt is used to watch if a host is reachable or not.



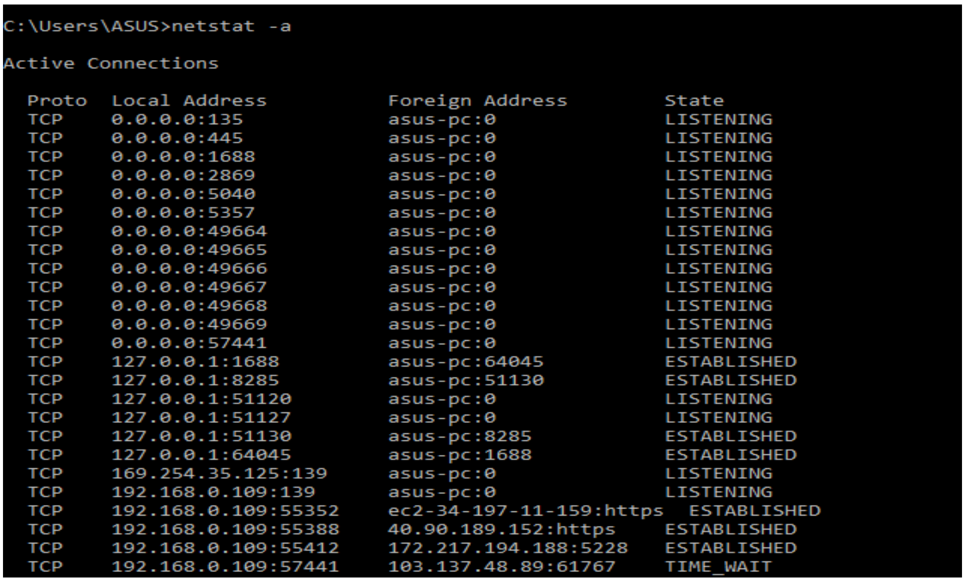
```
C:\Users\ASUS>ping 192.168.0.104

Pinging 192.168.0.104 with 32 bytes of data:
Reply from 192.168.0.104: bytes=32 time=38ms TTL=64
Reply from 192.168.0.104: bytes=32 time=76ms TTL=64
Reply from 192.168.0.104: bytes=32 time=288ms TTL=64
Reply from 192.168.0.104: bytes=32 time=153ms TTL=64

Ping statistics for 192.168.0.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 38ms, Maximum = 288ms, Average = 138ms
```

Which tool (command) lists all routers in the path from your host to a destination?
Answer: To list all routers, we need a source (my pc) and a specific website from where I want to fetch information or IP address of a destination device. Then by using ***tracert*** command with desired destination IP address or website , we can all routers present in the path as following:



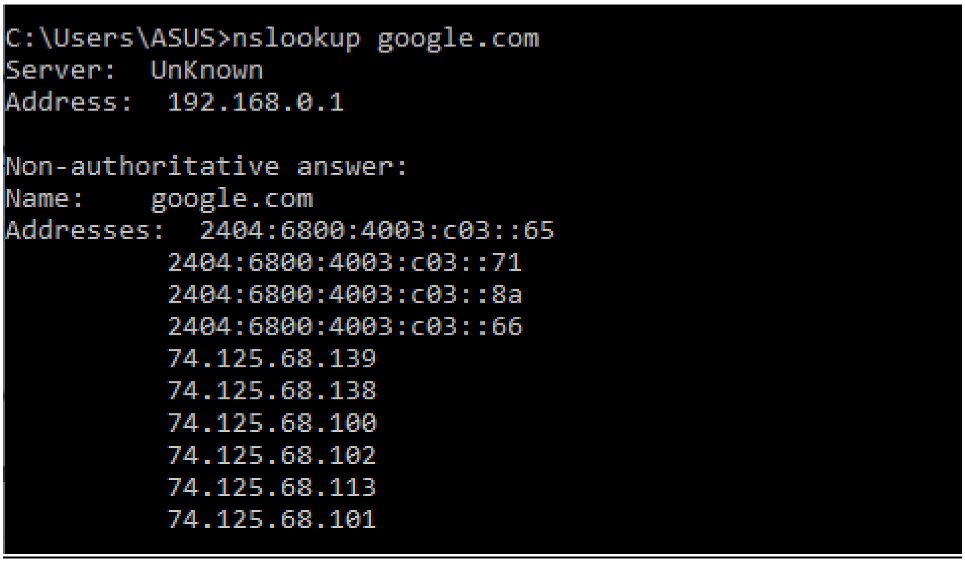
```
C:\Users\ASUS>tracert www.google.com

Tracing route to www.google.com [74.125.24.99]
over a maximum of 30 hops:

  1     5 ms     2 ms     1 ms  192.168.0.1
  2     4 ms     4 ms     3 ms  103.127.177.45
  3     4 ms     4 ms     5 ms  103.127.179.101
  4     3 ms     3 ms     4 ms  103.220.205.201
  5     5 ms     5 ms     4 ms  110.76.131.206
  6     5 ms    11 ms     4 ms  10.56.78.49
  7   117 ms    62 ms    67 ms  103.199.87.60
  8    54 ms    56 ms    68 ms
```

Which tool (command) displays all sockets used on your computer (Windows and Linux)?
Answer: By using ***netstat –a*** command in command prompt, we can see all active or used port numbers to which sockets are bound to and we can also acknowledge the state of the connections.



```
C:\Users\ASUS>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            asus-pc:0              LISTENING
  TCP    0.0.0.0:445            asus-pc:0              LISTENING
  TCP    0.0.0.0:1688           asus-pc:0              LISTENING
  TCP    0.0.0.0:2869           asus-pc:0              LISTENING
  TCP    0.0.0.0:5040           asus-pc:0              LISTENING
  TCP    0.0.0.0:5357           asus-pc:0              LISTENING
  TCP    0.0.0.0:49664          asus-pc:0              LISTENING
  TCP    0.0.0.0:49665          asus-pc:0              LISTENING
  TCP    0.0.0.0:49666          asus-pc:0              LISTENING
  TCP    0.0.0.0:49667          asus-pc:0              LISTENING
  TCP    0.0.0.0:49668          asus-pc:0              LISTENING
  TCP    0.0.0.0:49669          asus-pc:0              LISTENING
  TCP    0.0.0.0:57441          asus-pc:0              LISTENING
  TCP    127.0.0.1:1688         asus-pc:64045          ESTABLISHED
  TCP    127.0.0.1:8285         asus-pc:51130          ESTABLISHED
  TCP    127.0.0.1:51120        asus-pc:0              LISTENING
  TCP    127.0.0.1:51127        asus-pc:0              LISTENING
  TCP    127.0.0.1:51130        asus-pc:8285           ESTABLISHED
  TCP    127.0.0.1:64045        asus-pc:1688           ESTABLISHED
  TCP    169.254.35.125:139     asus-pc:0              LISTENING
  TCP    192.168.0.109:139      asus-pc:0              LISTENING
  TCP    192.168.0.109:55352    ec2-34-197-11-159:https  ESTABLISHED
  TCP    192.168.0.109:55388    40.90.189.152:https    ESTABLISHED
  TCP    192.168.0.109:55412    172.217.194.188:5228   ESTABLISHED
  TCP    192.168.0.109:57441    103.137.48.89:61767    TIME_WAIT
```

Which tool (command) displays the mapping a domain name to an IP address?
Answer: ***nslookup*** named command displays the mapping of a domain name to their IP address. For example:



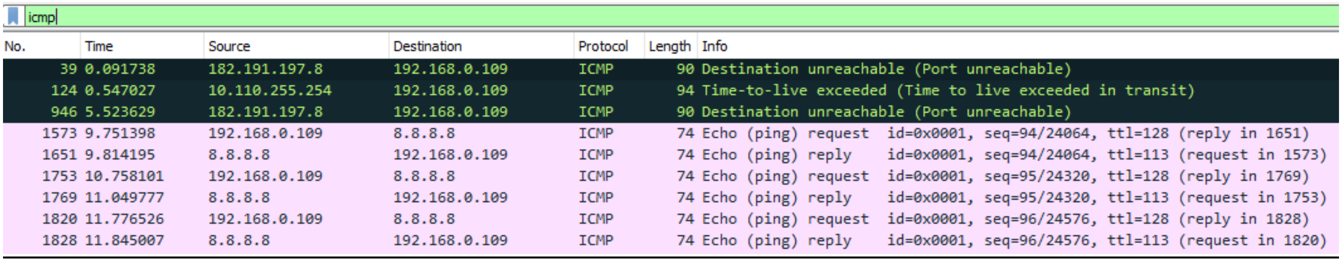
```
C:\Users\ASUS>nslookup google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4003:c03::65
          2404:6800:4003:c03::71
          2404:6800:4003:c03::8a
          2404:6800:4003:c03::66
          74.125.68.139
          74.125.68.138
          74.125.68.100
          74.125.68.102
          74.125.68.113
          74.125.68.101
```

Wireshark packet capture

a) Read the Wireshark manual and answer the following question

If you want to filter PING traffic in your capture, what must done after you captured all packets, sent and received by your host?

Answer: After capturing all packets, I can filter a particular protocol related packets for example using DNS, HTTP, TCP, UDP, ICMP in filter section will filter only particular packets. Here, ICMP ping is used to check the reachability of servers or to learn some failure code from ICMP messages (*collected from Wireshark manual*). We can also examine details from a specific packet that has been captured among a huge traffic.



icmp

No.	Time	Source	Destination	Protocol	Length	Info
39	0.091738	182.191.197.8	192.168.0.109	ICMP	90	Destination unreachable (Port unreachable)
124	0.547027	10.110.255.254	192.168.0.109	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
946	5.523629	182.191.197.8	192.168.0.109	ICMP	90	Destination unreachable (Port unreachable)
1573	9.751398	192.168.0.109	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=94/24064, ttl=128 (reply in 1651)
1651	9.814195	8.8.8.8	192.168.0.109	ICMP	74	Echo (ping) reply id=0x0001, seq=94/24064, ttl=113 (request in 1573)
1753	10.758101	192.168.0.109	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=95/24320, ttl=128 (reply in 1769)
1769	11.049777	8.8.8.8	192.168.0.109	ICMP	74	Echo (ping) reply id=0x0001, seq=95/24320, ttl=113 (request in 1753)
1820	11.776526	192.168.0.109	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=96/24576, ttl=128 (reply in 1828)
1828	11.845007	8.8.8.8	192.168.0.109	ICMP	74	Echo (ping) reply id=0x0001, seq=96/24576, ttl=113 (request in 1820)

b) Review the Ethernet II header field descriptions and lengths.

Background / Scenario

When upper layer protocols communicate with each other, data flows down the Open Systems Interconnection (OSI) layers and is encapsulated into a Layer 2 frame. The frame composition is dependent on the media access type. For example, if the upper layer protocols are TCP and IP and the media access is Ethernet, then the Layer 2 frame encapsulation will be Ethernet II. This is typical for a LAN environment.

1. Looking at the Ethernet II frame format, answer the questions.

Preamble	Destination Address	Source Address	Frame Type	Data	FCS
(8 Bytes)	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

The preamble represents **no bits and provides no header information**!!!

Answer: The Preamble contains 7 bytes and 1 byte - Start Frame Delimiter (SFD) altogether do synchronization process between the sender and receiver. If a new frame is sent from source, the receiver gets sign to get ready to receive a new frame by the help of preamble and SFD. If in Wireshark, there is no preamble shown, it means that both of them are working out of frame. The 8 byte is also not stored in memory. They only work for their respective duty.

It is only used for physical signal transmission of Ethernet frames over LAN cables. Which function does the Ethernet preamble have?

Answer: Ethernet preamble is used to let know the receiver of upcoming arrival of a frame from source.

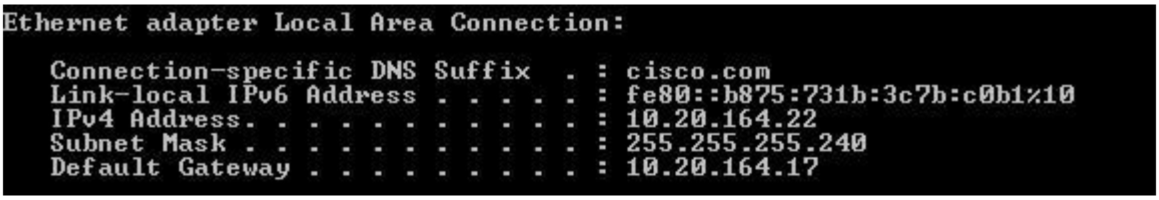
How many Bytes do we have in the Ethernet II header?

Answer: Ethernet II header has destination address (6 Bytes), source address (6 Bytes) and frame type (2 Bytes). In total, it’s header has 6+6+2=14 Bytes.

How many Bytes do we have in the Ethernet II trailer?

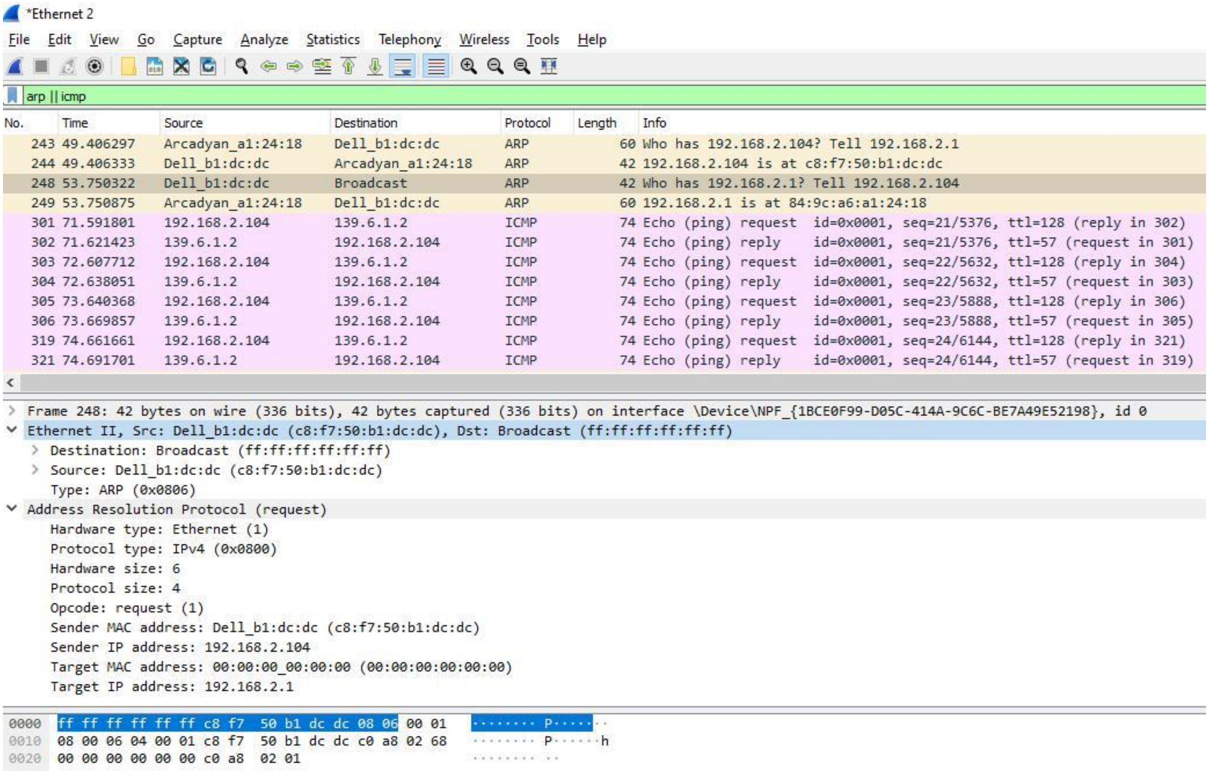
Answer: Ethernet II trailer has frame check sequence- FCS (4 Bytes) which is used for error detection.

b) Examine Ethernet frames in a Wireshark capture. The following information is known from a PC:



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : cisco.com
   Link-local IPv6 Address . . . . . : fe80::b875:731b:3c7b:c0b1%10
   IPv4 Address. . . . . . . . . . . : 10.20.164.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 10.20.164.17
```

The Wireshark capture below shows the packets generated by a ping being issued from a PC host to its default gateway. A filter has been applied to Wireshark to view the ARP and ICMP protocols only. The session begins with an ARP query for the MAC address of the gateway router, followed by four ping requests and replies.


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp || icmp

```
No.   Time       Source              Destination         Protocol  Length  Info
  243 49.406297  Arcadyan_a1:24:18   Dell_b1:dc:dc       ARP           60  Who has 192.168.2.104? Tell 192.168.2.1
  244 49.406333  Dell_b1:dc:dc       Arcadyan_a1:24:18   ARP           42  192.168.2.104 is at c8:f7:50:b1:dc:dc
  248 53.750322  Dell_b1:dc:dc       Broadcast           ARP           42  Who has 192.168.2.1? Tell 192.168.2.104
  249 53.750875  Arcadyan_a1:24:18   Dell_b1:dc:dc       ARP           60  192.168.2.1 is at 84:9c:a6:a1:24:18
  301 71.591801  192.168.2.104       139.6.1.2           ICMP          74  Echo (ping) request  id=0x0001, seq=21/5376, ttl=128 (reply in 302)
  302 71.621423  139.6.1.2           192.168.2.104       ICMP          74  Echo (ping) reply    id=0x0001, seq=21/5376, ttl=57 (request in 301)
  303 72.607712  192.168.2.104       139.6.1.2           ICMP          74  Echo (ping) request  id=0x0001, seq=22/5632, ttl=128 (reply in 304)
  304 72.638051  139.6.1.2           192.168.2.104       ICMP          74  Echo (ping) reply    id=0x0001, seq=22/5632, ttl=57 (request in 303)
  305 73.640368  192.168.2.104       139.6.1.2           ICMP          74  Echo (ping) request  id=0x0001, seq=23/5888, ttl=128 (reply in 306)
  306 73.669857  139.6.1.2           192.168.2.104       ICMP          74  Echo (ping) reply    id=0x0001, seq=23/5888, ttl=57 (request in 305)
  319 74.661661  192.168.2.104       139.6.1.2           ICMP          74  Echo (ping) request  id=0x0001, seq=24/6144, ttl=128 (reply in 321)
  321 74.691701  139.6.1.2           192.168.2.104       ICMP          74  Echo (ping) reply    id=0x0001, seq=24/6144, ttl=57 (request in 319)
```

```
> Frame 248: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{1BCE0F99-D05C-414A-9C6C-BE7A49E52198}, id 0
v Ethernet II, Src: Dell_b1:dc:dc (c8:f7:50:b1:dc:dc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   > Source: Dell_b1:dc:dc (c8:f7:50:b1:dc:dc)
     Type: ARP (0x0806)
v Address Resolution Protocol (request)
     Hardware type: Ethernet (1)
     Protocol type: IPv4 (0x0800)
     Hardware size: 6
     Protocol size: 4
     Opcode: request (1)
     Sender MAC address: Dell_b1:dc:dc (c8:f7:50:b1:dc:dc)
     Sender IP address: 192.168.2.104
     Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
     Target IP address: 192.168.2.1
```

```
0000  ff ff ff ff ff ff c8 f7  50 b1 dc dc 08 06 00 01   ········ P·······
0010  08 00 06 04 00 01 c8 f7  50 b1 dc dc c0 a8 02 68   ········ P······h
0020  00 00 00 00 00 00 c0 a8  02 01                     ········ ··
```

a) **Check frame #248.** In the shown hex dump at the bottom of the Wireshark window you see all bytes displayed by Wireshark. Is the Ethernet II trailer shown in the Wireshark capture? Explain your answer.

Answer: No. The Ethernet II trailer ***FCS*** is not shown in Wireshark capture. FCS stands for Frame check Sequence to detect errors in frames while transferring frames to the receiver. FCS is added to the frame at the end as a trailer containing 4 bytes in data link layer. If there is no significant error capture or bad checksum while transferring frame, there might be no FCS shown in Wireshark capture.

b) ARP – Address Resolution Protocol. **Check frames #248 and #249.**

b.1) Which IP source address is used in the **ARP request**?
Answer: 192.168.2.104

b.2) Which type (unicast, multicast, broadcast) of MAC address is used as the MAC destination address in the **ARP request**?

Answer: Broadcast MAC address **ff: ff: ff: ff: ff: ff** is used as the MAC destination address in the **ARP request**.

b.3.) The MAC address of which network device is given back by the **ARP response**?

Answer: The MAC address **84: 9c: a6: a1: 24: 18** is given back by the **ARP response.**

c) What is the Vendor ID (OUI) of the Source's NIC?

Answer: ***Dell***

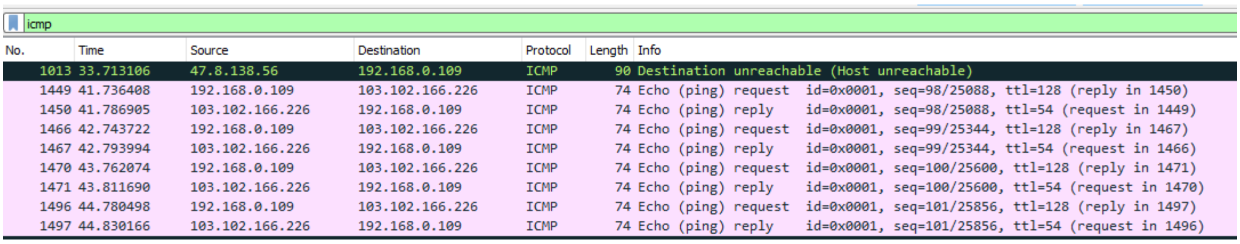
d) What is the Source's NIC serial number?

Answer: **b1: dc: dc**

P.T.O

Examine ICMP Message Types

Check information about the ICMP protocol, e.g. using www.wikipedia.com. Which function is provided by the following ICMP message?

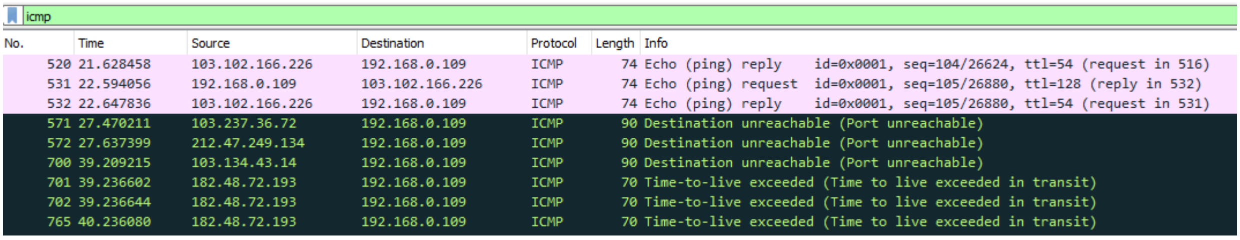


```
icmp
No.    Time       Source           Destination      Protocol  Length Info
  1013 33.713106  47.8.138.56      192.168.0.109    ICMP      90 Destination unreachable (Host unreachable)
  1449 41.736408  192.168.0.109    103.102.166.226  ICMP      74 Echo (ping) request  id=0x0001, seq=98/25088, ttl=128 (reply in 1450)
  1450 41.786905  103.102.166.226  192.168.0.109    ICMP      74 Echo (ping) reply    id=0x0001, seq=98/25088, ttl=54 (request in 1449)
  1466 42.743722  192.168.0.109    103.102.166.226  ICMP      74 Echo (ping) request  id=0x0001, seq=99/25344, ttl=128 (reply in 1467)
  1467 42.793994  103.102.166.226  192.168.0.109    ICMP      74 Echo (ping) reply    id=0x0001, seq=99/25344, ttl=54 (request in 1466)
  1470 43.762074  192.168.0.109    103.102.166.226  ICMP      74 Echo (ping) request  id=0x0001, seq=100/25600, ttl=128 (reply in 1471)
  1471 43.811690  103.102.166.226  192.168.0.109    ICMP      74 Echo (ping) reply    id=0x0001, seq=100/25600, ttl=54 (request in 1470)
  1496 44.780498  192.168.0.109    103.102.166.226  ICMP      74 Echo (ping) request  id=0x0001, seq=101/25856, ttl=128 (reply in 1497)
  1497 44.830166  103.102.166.226  192.168.0.109    ICMP      74 Echo (ping) reply    id=0x0001, seq=101/25856, ttl=54 (request in 1496)
```

ICMP Type 8: **Echo request**

ICMP Type 0: **Echo reply**

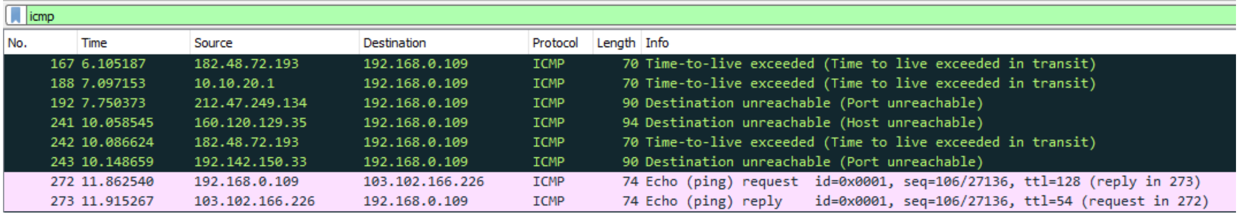
ICMP Type 11: **Time exceeded (Time to live exceeded in transit)**



```
icmp
No.    Time       Source           Destination      Protocol  Length Info
   520 21.628458  103.102.166.226  192.168.0.109    ICMP      74 Echo (ping) reply    id=0x0001, seq=104/26624, ttl=54 (request in 516)
   531 22.594056  192.168.0.109    103.102.166.226  ICMP      74 Echo (ping) request  id=0x0001, seq=105/26880, ttl=128 (reply in 532)
   532 22.647836  103.102.166.226  192.168.0.109    ICMP      74 Echo (ping) reply    id=0x0001, seq=105/26880, ttl=54 (request in 531)
   571 27.470211  103.237.36.72    192.168.0.109    ICMP      90 Destination unreachable (Port unreachable)
   572 27.637399  212.47.249.134   192.168.0.109    ICMP      90 Destination unreachable (Port unreachable)
   700 39.209215  103.134.43.14    192.168.0.109    ICMP      90 Destination unreachable (Port unreachable)
   701 39.236602  182.48.72.193    192.168.0.109    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   702 39.236644  182.48.72.193    192.168.0.109    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   765 40.236080  182.48.72.193    192.168.0.109    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
```

ICMP Type 3 Code 0: **Destination unreachable (Net Unreachable)**
In capture, there was not observed such type of ICMP message.

ICMP Type 3 Code 1: **Destination unreachable (Host Unreachable)**



```
icmp
No.    Time       Source           Destination      Protocol  Length Info
   167 6.105187   182.48.72.193    192.168.0.109    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   188 7.097153   10.10.20.1       192.168.0.109    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   192 7.750373   212.47.249.134   192.168.0.109    ICMP      90 Destination unreachable (Port unreachable)
   241 10.058545  160.120.129.35   192.168.0.109    ICMP      94 Destination unreachable (Host unreachable)
   242 10.086624  182.48.72.193    192.168.0.109    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   243 10.148659  192.142.150.33   192.168.0.109    ICMP      90 Destination unreachable (Port unreachable)
   272 11.862540  192.168.0.109    103.102.166.226  ICMP      74 Echo (ping) request  id=0x0001, seq=106/27136, ttl=128 (reply in 273)
   273 11.915267  103.102.166.226  192.168.0.109    ICMP      74 Echo (ping) reply    id=0x0001, seq=106/27136, ttl=54 (request in 272)
```

ICMP Type 3 Code 3: **Destination unreachable (Port Unreachable)**

ICMP Type 3 Code 4: **Fragment Needed or Don't Fragment was Set**
This type of ICMP message also was not captured.

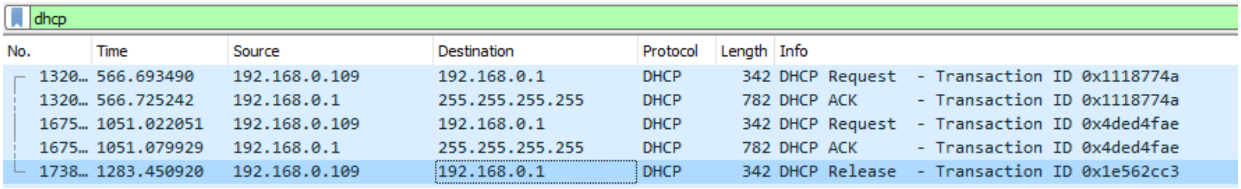
Any idea why the PC sends out a broadcast ARP prior to sending the first ping request?
Answer: The ARP request sends out as a broadcast request because host wants to get specific MAC address of a particular destination device by sending only destination IP address in the local area network. Then the existing all devices start matching with the given IP address and finally when IP address get matched with destined host, it sends out ARP response to the first host with it's MAC address.

Examine DHCP

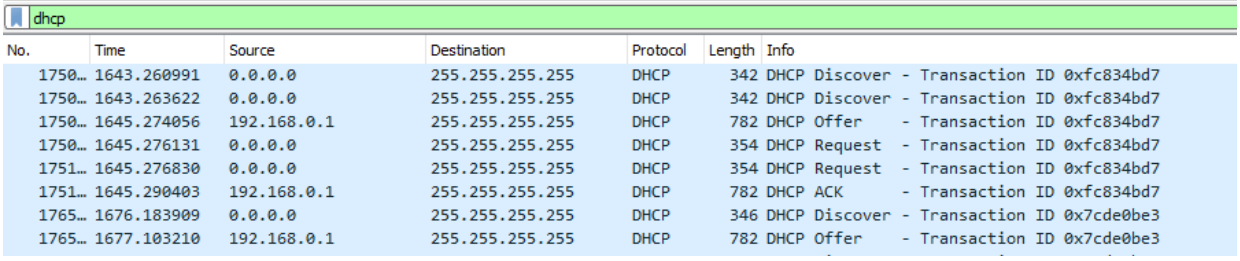
Check information about the DHCP protocol, e.g. using www.wikipedia.com. Describe briefly the task of DHCP (Dynamic Host Configuration Protocol).

Answer: DHCP (Dynamic Host Configuration Protocol) is a protocol which has significant task to assign IP address, subnet mask, default gateway and DNS server address automatically on a leased basis.
If we do not want to let DHCP assign automatically, then we have to fill up manually which is called static IP addressing. It can both perform as a client and as a server. It has four principles to follow.
For instance: DHCP Discover, DHCP offer, DHCP Request and DHCP Ack.
DHCP Discover: Here host looks for DHCP server.
DHCP Offer: Then DHCP server offers an address.
DHCP Request: Here, the host request to lease the address.
DHCP ACK: Finally, the DHCP server sends the IP address to the host on a lease.

Which eight DHCP messages are available in this protocol?
Answer: I did not get eight DHCP messages. Rather I have got DHCP Request and DHCP ACK messages first for two times. Then I used Release command to have a new IP address on a lease. Then DHCP Discover, DHCP Offer, DHCP request and DHCP ACK gradually took places. In total, I observed five types of DHCP messages.



```
dhcp
No.      Time         Source          Destination      Protocol  Length Info
  1320… 566.693490    192.168.0.109   192.168.0.1      DHCP       342 DHCP Request  - Transaction ID 0x1118774a
  1320… 566.725242    192.168.0.1     255.255.255.255  DHCP       782 DHCP ACK      - Transaction ID 0x1118774a
  1675… 1051.022051   192.168.0.109   192.168.0.1      DHCP       342 DHCP Request  - Transaction ID 0x4ded4fae
  1675… 1051.079929   192.168.0.1     255.255.255.255  DHCP       782 DHCP ACK      - Transaction ID 0x4ded4fae
  1738… 1283.450920   192.168.0.109   192.168.0.1      DHCP       342 DHCP Release  - Transaction ID 0x1e562cc3
```



```
dhcp
No.      Time         Source          Destination      Protocol  Length Info
  1750… 1643.260991   0.0.0.0         255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0xfc834bd7
  1750… 1643.263622   0.0.0.0         255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0xfc834bd7
  1750… 1645.274056   192.168.0.1     255.255.255.255  DHCP       782 DHCP Offer    - Transaction ID 0xfc834bd7
  1750… 1645.276131   0.0.0.0         255.255.255.255  DHCP       354 DHCP Request  - Transaction ID 0xfc834bd7
  1751… 1645.276830   0.0.0.0         255.255.255.255  DHCP       354 DHCP Request  - Transaction ID 0xfc834bd7
  1751… 1645.290403   192.168.0.1     255.255.255.255  DHCP       782 DHCP ACK      - Transaction ID 0xfc834bd7
  1765… 1676.183909   0.0.0.0         255.255.255.255  DHCP       346 DHCP Discover - Transaction ID 0x7cde0be3
  1765… 1677.103210   192.168.0.1     255.255.255.255  DHCP       782 DHCP Offer    - Transaction ID 0x7cde0be3
```

Which DHCP messages are used to acquire an IP address from DHCP server?

Answer: ***DHCP offer*** message is used to acquire IP address from DHCP server. It can also provide subnet mask, default gateway of sender, DNS server address and so on.