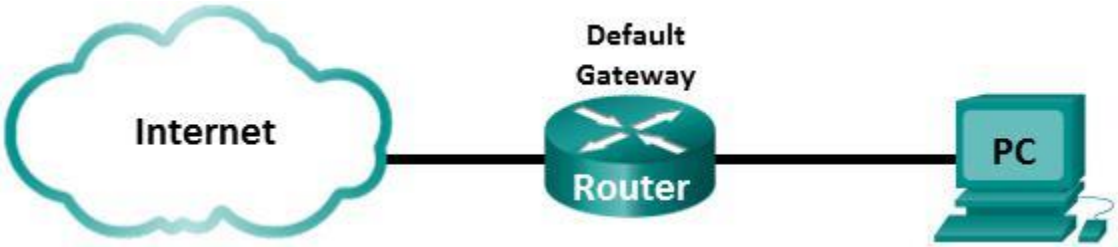
CCNA ITN Lab 1 **Instruction** **Deadline: 27.11.2020**

Name: _____Rubaiya Kabir Pranti _____

Simple Network
and
Internet Access Analysis



Tasks:

Task1 **Simple Network and Connectivity Testing**

Task2 **Capture Packets and analyze Protocols to connect to the Internet**

Task1 - Simple Network and Connectivity Testing

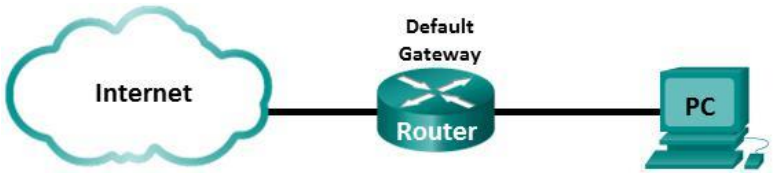
Background / Scenario

Networks are constructed of three major components: hosts, switches, and routers. Normally, in our DN.Lab you would build a simple network with two hosts (your PC and your neighbor's PC) and two switches. You will apply static IP addressing for this lab to the PCs to enable communication between these two devices. Use the **ping** (ICMP Echo Request / ICMP Echo Reply) utility to verify connectivity.

In this Corona semester you will inspect your local network @ home.

Topology

Connect your PC to your LAN, via cabled LAN or WLAN, with Default Gateway (e.g. your DSL Router).



Part 1: Set Up the Network Topology

Cable the topology according to your situation.

Part 2: Configure PC Hosts and test connectivity with ICMP Ping

Step 1: Configure static IP address information on the PCs.

a. If you run DHCP, record the IP address, network mask and Default Gateway address of your host Home PC.

- Host IP address: **IPv4 Address: 192.168.0.104 (Preferred)**
- IP network mask**: Subnet Mask: 255.255.255.0**
- Default Gateway IP address: **Default Gateway: 192.168.0.1**

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : www.tendawifi.com
   Description . . . . . . . . . . . : Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC
   Physical Address. . . . . . . . . : 30-5A-3A-8B-D8-AD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7d6a:3967:8df6:d5e4%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.104(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, November 23, 2020 3:26:40 PM
   Lease Expires . . . . . . . . . . : Tuesday, November 24, 2020 3:26:40 PM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 85767980
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-9F-3E-FD-30-5A-3A-8B-D8-AD
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

b. If you use static IP addresses, manually configure IP address, subnet mask, and default gateway, which fit to your local topology.

Step 2: Check PC settings

Use the command prompt window to verify the PC settings and connectivity.

- Host IP address: **IPv4 Address: 192.168.0.104(Preferred)**
- IP network mask: **Subnet Mask: 255.255.255.0**
- Default Gateway IP address: **Default Gateway: 192.168.0.1**
- Record your host MAC address: **Physical Address: 30-5A-3A-8B-D8-AD**

Step 3: Check connectivity

From PC-A send an ICMP ECHO REQUEST via the **ping** command to the IP address of the Default Gateway. (Linux: limit it to 5 ping requests).

- Was the ping successful?
  Answer: **Yes because packets are successfully sent and then received by router.**
- Which average Round Trip Time (RTT) did you measure?
  Answer: Average Round Trip Time (RTT) is **4ms**.

```
C:\Users\ASUS>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=8ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 8ms, Average = 4ms
```

Propagation delay

- Estimate the length of the cable path from your PC to your Default Gateway
  Answer: In my home, there is WLAN (wireless network) activated that's why I can't measure any solid cable's length from my PC to my default gateway (router).
  Therefore,
  Let, real distance between my notebook and router is, l=10m
- Calculate the propagation delay

  Answer: We know,
  Propagation delay, **tpd= l / C** where l = distance between notebook and router=10m and C= velocity of the microwave through wireless link =c= c0 = 300,000 km/s=3×10^8 m/s Therefore, tpd= l / C = 10m / (3×10^8) m/s = 3.33×10^{-8} s=**33.3 ns**
- For one RTT, how many times is a frame transmitted over this length?

  Answer: **two times**.

Transmission time

Record the data rate R of your network.
If this is not available, we assume a 100BASE-Tx network.

Answer:
Transmission time, **t_t= M / R** where M = Size of frame =32 bytes=32*8=256 bits and
R= link bit rate=100 Mbps (for 100BASE-Tx network) =10^8 bit per second
Therefore, t_t= M / R= 256 bits / 10^8 bps = 2.56×10^{-6} s=**2.56 µs**

- Let us assume your Ethernet frame carrying the ICMP message has a length of 78 Bytes. Calculate the transmission time t_t of one Ethernet frame.
- **Answer**:
Transmission time, **t_t= M / R**, where M = Size of one Ethernet frame =78 bytes=78*8=624 bits and
R= link bit rate=100 Mbps=10^8 bit per second
Therefore, t_t= M / R= 624 bits / 10^8 bps = 6.24×10^{-6} s=**6.24 µs**

- For one RTT, how many times is a frame send through an NIC interface?
Answer: **one time**.

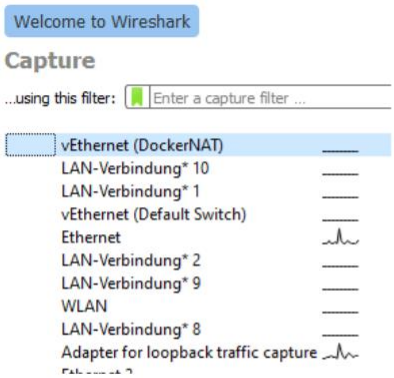
Which type of delay, transmission time or propagation delay, has the highest influence on the ping round-trip-time (RTT) in this scenario?
Answer: **Propagation delay.** It depends on the distance between source and destination.

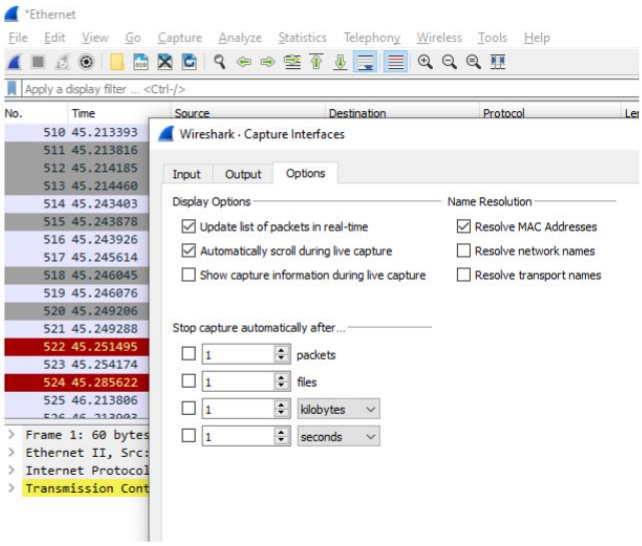
Is there any other delay which has influence on the RTT?
Answer: There are other factors those can change RTT. These are:
-processing delay
-queuing delay
-encoding delay
These delays depend on number of hops between sender and receiver

Part 3: Capture and Analyze Local ICMP Data in Wireshark

Step 1: Start Wireshark and begin capturing data.

a. Start **Wireshark** and select the **Interface**.
By selecting an interface, you **start** a capture.





Note: If multiple interfaces are listed and you are unsure which interface to check, you use **Capture ➔ Options**, where you also find information on the MAC addresses of interface

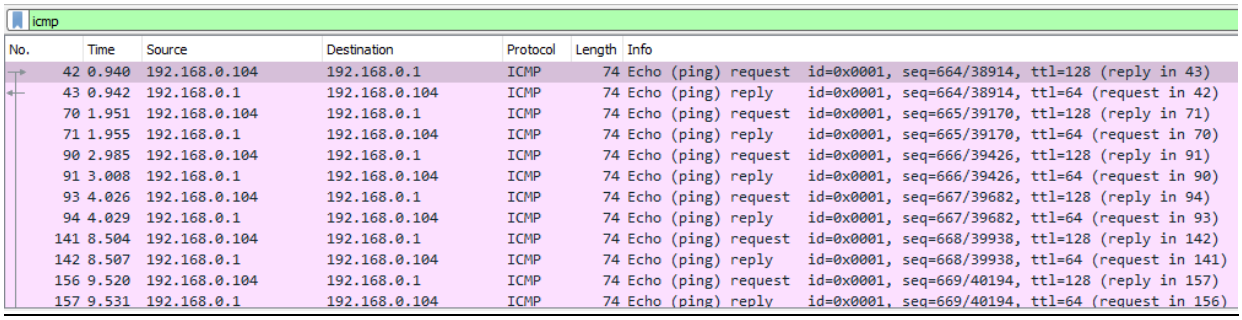
You should select **automatically scroll during live capture,** if not active**.**

b. Ping your Default Gateway (max. 5 times) and stop capturing data by clicking the **Stop Capture** icon.

Step 2: Examine the captured data

a. Filter ICMP traffic in your Wireshark capture.
Answer: After pinging default gateway for 5 times, I filtered ICMP traffic in my Wireshark capture.

```
C:\Users\ASUS>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=4ms TTL=64
Reply from 192.168.0.1: bytes=32 time=23ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 23ms, Average = 7ms

C:\Users\ASUS>
C:\Users\ASUS>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=4ms TTL=64
Reply from 192.168.0.1: bytes=32 time=11ms TTL=64
Reply from 192.168.0.1: bytes=32 time=4ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 11ms, Average = 5ms

C:\Users\ASUS>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64
Reply from 192.168.0.1: bytes=32 time=17ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 17ms, Average = 6ms

C:\Users\ASUS>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
```



icmp

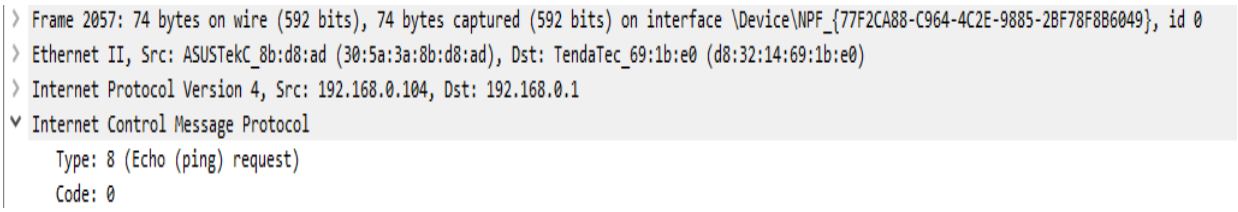
No.	Time	Source	Destination	Protocol	Length	Info
42	0.940	192.168.0.104	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=664/38914, ttl=128 (reply in 43)
43	0.942	192.168.0.1	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=664/38914, ttl=64 (request in 42)
70	1.951	192.168.0.104	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=665/39170, ttl=128 (reply in 71)
71	1.955	192.168.0.1	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=665/39170, ttl=64 (request in 70)
90	2.985	192.168.0.104	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=666/39426, ttl=128 (reply in 91)
91	3.008	192.168.0.1	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=666/39426, ttl=64 (request in 90)
93	4.026	192.168.0.104	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=667/39682, ttl=128 (reply in 94)
94	4.029	192.168.0.1	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=667/39682, ttl=64 (request in 93)
141	8.504	192.168.0.104	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=668/39938, ttl=128 (reply in 142)
142	8.507	192.168.0.1	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=668/39938, ttl=64 (request in 141)
156	9.520	192.168.0.104	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=669/40194, ttl=128 (reply in 157)
157	9.531	192.168.0.1	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=669/40194, ttl=64 (request in 156)

b. Check the 1st **ICMP Echo request** PDU frames in the top section of Wireshark. Record the following:

- Source IP address: **192.168.0.104 (notebook IP address)**
- Destination IP address: **192.168.0.1 (default gateway)**

With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the Destination and Source MAC addresses.

- Does the Source MAC address match your PC's interface?
  Answer: **Yes**
  Source MAC address in middle section**: ASUSTekC_8b: d8:ad or 30: 5a: 3a: 8b: d8: ad**
  Physical address from command prompt: **30-5A-3A-8B-D8-AD**



- Record the Destination MAC address, which is the MAC address of your Default Gateway.
  Answer:
  Destination MAC address**: TendaTec_69: 1b: e0 or d8: 32: 14: 69: 1b: e0**

Check the ICMP detailed information

- Which hex number represents message type Echo Request (ping)?
  Answer:
  An **ICMP Echo Request** represents hex number: **0×08 (type)**, Code: **0×00**

c. Select the Ethernet frame, which contains the **1st ICMP Echo reply** message

- Do the source and destination MAC addresses switch compared to Echo request?
  Answer: **No**. Compared to other following Echo requests, the source and destination MAC addresses are always same. But for Echo reply, MAC addresses switch their position.

- From the initiator PC time stamps of the first ICMP ECHO REQUEST
  and ICMP ECHO REPLY Ethernet frames, calculate the RTT in your small network.

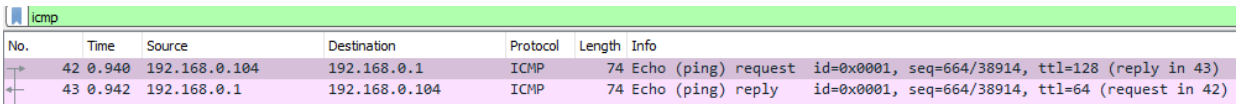
  Answer: I don't know how to calculate the exact time taken for first ICMP ECHO REQUEST.
  But, time taken for first ICMP ECHO REPLY Ethernet frame is observed as **0.002** second = 2ms.
  RTT in my network is not calculated.

d. Select the Ethernet frame, which contains the **1st ICMP Echo reply** message

- Do the source and destination MAC addresses switch compared to Echo request?
  Answer: No. Compared to other following Echo requests, the source and destination MAC addresses are always same.

- From the initiator PC time stamps of the first ICMP ECHO REQUEST and ICMP ECHO REPLY Ethernet frames, calculate the RTT in your small network.

  Answer: By using View > Time Display Format> Seconds since Beginning of capture (milliseconds)
  RTT in my network is calculated as: **RTT=0.940+0.942=1.882ms**



- Does this captured RTT match the values of Part2? Discuss your findings.
  Answer: **Command Prompt:**
  In Part2, first RTT = 2ms from command prompt.
  Also approximate round trip times are seen as below:
  Minimum RTT= 2ms, Maximum RTT= 8ms, Average RTT = 4ms

  Wireshark:
  In part3, RTT captured in Wireshark for first ICMP ECHO REQUEST and ICMP ECHO REPLY is calculated **1.882ms**. It seems like these findings are near to each other.

e. Examine **Ethernet frame** in the 1st ICMP ECHO REPLY message.

- How many Bytes have been captured in total?
  Answer: **74 Bytes** in total in one frame.

- How many Bytes are in the Ethernet 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**.

- Which Ethernet header fields are shown?
  Answer: Ethernet header all three fields are there.

  Source MAC address: TendaTec_69:1b: e0 (d8: 32: 14: 69: 1b: e0)
  Destination MAC address: ASUSTekC_8b: d8: ad (30: 5a: 3a: 8b: d8: ad),
  Frame Type: IPv4 (0x0800)

- Why is the Ethernet FCS missing in this capture?
  Answer: The Ethernet 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 detected while transferring frame, there is no FCS shown in Wireshark capture. Ethernet hardware, NIC strips it if the checksum is not correct.**

- Why is the Ethernet preamble missing in this capture?

  Answer: The Preamble contains 7 bytes and 1 byte of Start Frame Delimiter (SFD) and 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 because they are not actually part of frame. Preamble doesn't carry any useful data and is not received like others. The 8 byte of preamble is also not stored in memory.**
  After going down from data link layer to physical layer, preamble and SFD are added to frame.

Examine **IP packet** in the 1st ICMP ECHO REPLY message.

- Which size (in Bytes) does the IP packet have?
  Answer: The size of IP Packet is **21 Bytes**. Also the length of IP Packet is seen as **60 Bytes**.
- How many Bytes are in the IP header?
  Answer: **20 Bytes.**
- Which protocol is signaled in the IP header?
  - Protocol field (hex value): **0×01** Protocol field (decimal value): **1**
  - Protocol name: **ICMP**

```
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0x7647 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.0.1
Destination: 192.168.0.104
```

```
0000  30 5a 3a 8b d8 ad d8 32  14 69 1b e0 08 00 45 00   0Z:····2 ·i····E·
0010  00 3c 82 c0 00 00 40 01  76 47 c0 a8 00 01 c0 a8   ·<····@· vG······
0020  00 68 00 00 54 11 00 01  01 4a 61 62 63 64 65 66   ·h··T··· ·Jabcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

f. Examine **ICMP message** in the 1st ICMP ECHO REPLY message.

- Which hex number represents message type **Echo reply**?

  Answer: **Type: 0 and Code: 0** represents message type **Echo reply.**
  In hex number, **Type: 0×00 and Code: 0×00**

- How many Bytes of ICMP has been sent?

  Answer: **40 Bytes**.

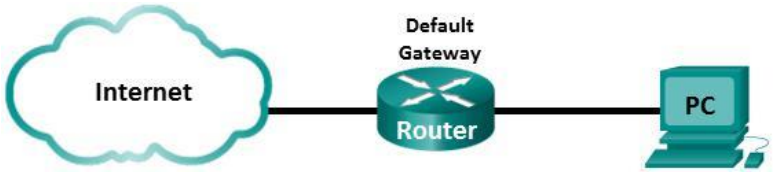
  ICMP header: **8 Bytes**. ICMP payload: **32 Bytes.**

Task 2 – Examine DHCP and Internet connection

Background / Scenario

In many cases we connect to the Internet to be online. In this lab, you will connect to the **switch on your lab workplace row**, which is connected through your Default Gateway (Router) to the Internet. You will get a dynamic IP address by DHCP.

Topology



Part 1: Use Wireshark to analyze Dynamic Address Allocation

Step 1: Connect your Home PC to the Internet

Continue with the topology of task1. If you used static IP addressing, connect your PC to a network with dynamic DHCP IP address configuration. DHCP will obtain an IP address in the background.

Step 2: Record the IP address of the default gateway on your PC.

- Host IP address: **IPv4 Address: 192.168.0.104(Preferred)**
- IP network mask: **Subnet Mask: 255.255.255.0**
- Default Gateway IP address: **Default Gateway: 192.168.0.1**
- Record your host MAC address: **Physical Address: 30-5A-3A-8B-D8-AD**

Step 3: Capture traffic on your PC's NIC.

a. Capture traffic on your active interface NIC with Wireshark. Start a Wireshark capture and generate some traffic by a ping to your Default Gateway.

b. Stop your Wireshark capture.

c. Which network protocols do you observe in your Wireshark capture?

Protocols observed: **TCP, UDP, TLSv1.2, ICMP, SSDP, ARP, DNS, QUIC**.

Step 4: Evaluation of a DHCP

a. Start a new Wireshark capture and filter the protocol **dhcp** (or bootp in former Wireshark releases). This filters traffic of the DHCP (Dynamic Host Configuration Protocol).

b. Refresh your DHCP address allocation (Windows: **ipconfig / release** and **ipconfig / renew** commands. Linux **sudo dhclient –r**, **sudo dhclient eth0** (your interface)).

c. Stop your Wireshark capture and analyze DHCP messages.

-Which device issues a **DHCP DISCOVER**? – **My notebook(host)**

-By what information can you decide that answer?

Answer: Here it is seen that my notebook IP address is the source IP address 192.168.0.104 and destination is router which is the default gateway containing IP address 192.168.0.1

When I use command ipconfig /release in command prompt, I can be no more connected with my WLAN. So as my internet connection goes off for release command, **my notebook is assigned with 0.0.0.0 IP address.**

It's observed that 0.0.0.0 is discovering or looking for a DHCP server by sending a request as broadcast request which is defined with 255.255.255.255.
From this, it is clear that, host issues DHCP DISCOVER.

dhcp

Time	Source	Destination	Protocol	Length	Info
0.000	192.168.0.104	192.168.0.1	DHCP	342	DHCP Release - Transaction ID 0x8a5106c4
6.285	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x90ffa413
0.003	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x90ffa413
1.066	192.168.0.1	255.255.255.255	DHCP	782	DHCP Offer - Transaction ID 0x90ffa413
0.001	0.0.0.0	255.255.255.255	DHCP	354	DHCP Request - Transaction ID 0x90ffa413
0.000	0.0.0.0	255.255.255.255	DHCP	354	DHCP Request - Transaction ID 0x90ffa413
0.103	192.168.0.1	255.255.255.255	DHCP	782	DHCP ACK - Transaction ID 0x90ffa413

-What is the IP address of the device, which responds with **DHCP OFFER**?
Answer: The IP address of the device which responds with DHCP OFFER is **192.168.0.1 (DHCP Server)**

-From that info, which device in your network runs the DHCP server?
Answer: **Default gateway or router is acting as DHCP server in my network.**
A DHCP server is replying to host's / my device's query to give an IP address.
DHCP server knows my device's MAC address only and so it will send offer as broadcast in the network as it does not know my notebook's IP address.

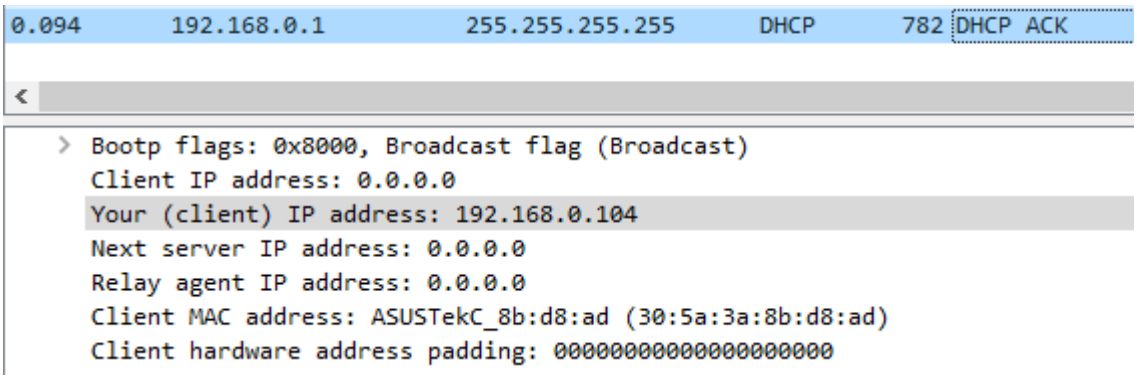
-Which IP address is preset as an option in the **DHCP REQUEST** command?
Answer: Source IP address: 0.0.0.0 and destination IP address: 255.255.255.255
192.168.0.104(host) address is now used as 0.0.0.0 for using release command.

0.000	0.0.0.0	255.255.255.255	DHCP	354 DHCP Request
0.094	192.168.0.1	255.255.255.255	DHCP	782 DHCP ACK

```
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: ASUSTekC_8b:d8:ad (30:5a:3a:8b:d8:ad)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
```

-Does the **DHCP ACK** command confirm the requested IP address?

Answer: **Yes. It is acknowledged that the last DHCP ACK command confirm the requested IP address (again 192.168.0.104) to the sender.** Along with IP address, subnet mask, default gateway and DNS server's IP address, Lease time are assigned after whole process ending with DHCP ACK.

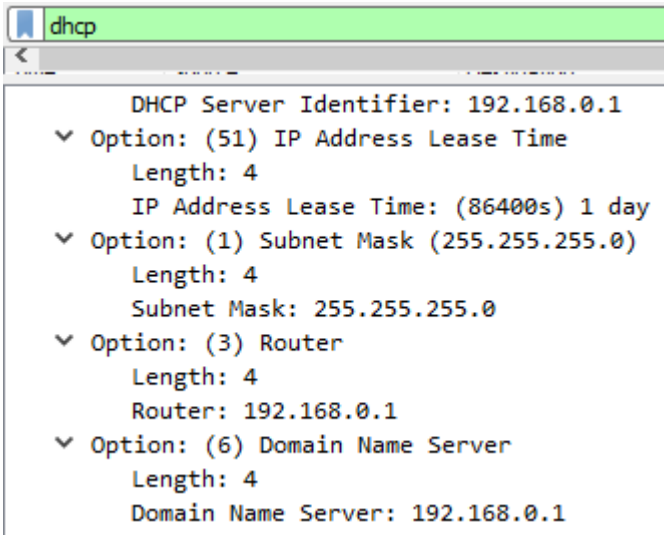


-How many seconds lease time for the IP address is given to your PC? - **86400 seconds (1 day)**

-Which subnet mask is provided by DHCP? - **255.255.255.0**

-Which default gateway IP address is provided by DHCP? – **192.168.0.1**

-Which DNS server IP address is provided by DHCP? – **192.168.0.1**



Part 2: Examine ARP

Background / Scenario

The Address Resolution Protocol (ARP) is used by the TCP/IP protocol stack to map a Layer 3 IP address to a Layer 2 MAC address. When a frame is placed on the network, it must have a destination MAC address. To discover the MAC address dynamically for the destination device, an ARP request is broadcasted on the LAN. The device that uses the destination IP address responds by ARP to this request, and the MAC address is recorded in the ARP cache. Every device on the LAN keeps its own ARP cache, or small area in RAM that holds ARP results. An ARP cache timer removes ARP entries that have not been used for a certain period of time.

Step 1: Display the ARP cache

a. Open a command window (Windows: with administrator role).

- What command option allows you to read the **ARP cache** table?
  Answer: **arp –a** command

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.0.104 --- 0xb
  Internet Address      Physical Address      Type
  192.168.0.1           d8-32-14-69-1b-e0     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 169.254.35.125 --- 0x13
  Internet Address      Physical Address      Type
  169.254.255.255       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
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

- What command would be used to delete all ARP entries (flush ARP cache)?
  Answer: **arp –d** command

b. Check the output of the **ARP** command. Display your ARP table and examine the output.

- What MAC address maps to your default gateway? – **d8-32-14-69-1b-e0**
- What MAC address maps to the IP broadcast address? – **ff-ff-ff-ff-ff-ff**

Step 2: Examine network latency caused by ARP

a. Start Wireshark to capture the active network interface.

b. Flush the ARP cache at the command prompt.

c. Verify that the ARP cache has been cleared.

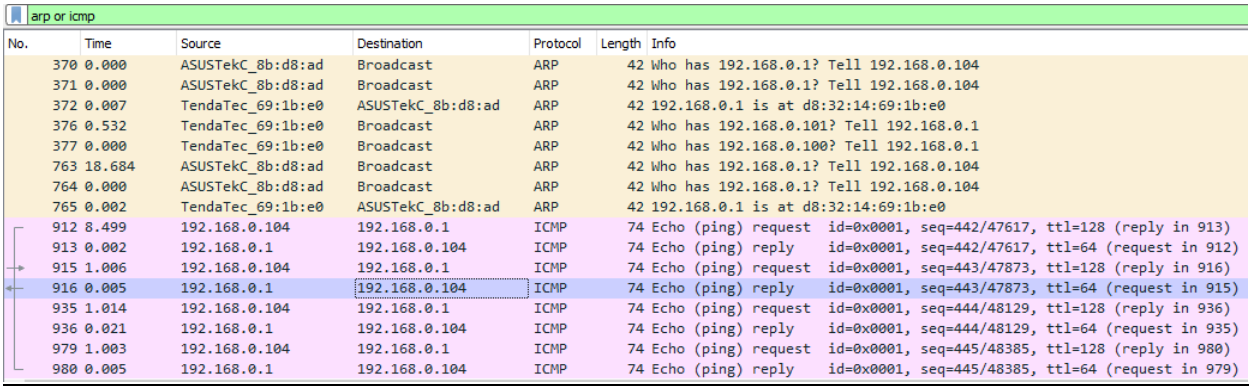
d. Flush the ARP cache again and immediately ping your default gateway IP address. Stop pinging after 4 ping in maximum

e. Stop the Wireshark capture

f. Use the Wireshark filter to display only ARP and ICMP outputs. In Wireshark filter type **“arp or icmp”.**

g. Examine the Wireshark capture. In this example.

- Which ARP messages are necessary to receive the first ICMP ECHO REPLY?
  Answer: **ARP REPLY message**. When I attempt **to ping** an IP address, an **ARP request** is sent at the same time. Then ARP REPLY is received if router is available.
- How long does it take to receive the second ICMP ECHO REPLY as response to the second ICMP ECHO REQUEST?
  Answer: It takes **0.005s=5ms** to receive the second ICMP ECHO REPLY as response to the second ICMP ECHO **REQUEST as I have used seconds since previous displayed capture.**



No.	Time	Source	Destination	Protocol	Length	Info
370	0.000	ASUSTekC_8b:d8:ad	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.104
371	0.000	ASUSTekC_8b:d8:ad	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.104
372	0.007	TendaTec_69:1b:e0	ASUSTekC_8b:d8:ad	ARP	42	192.168.0.1 is at d8:32:14:69:1b:e0
376	0.532	TendaTec_69:1b:e0	Broadcast	ARP	42	Who has 192.168.0.101? Tell 192.168.0.1
377	0.000	TendaTec_69:1b:e0	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
763	18.684	ASUSTekC_8b:d8:ad	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.104
764	0.000	ASUSTekC_8b:d8:ad	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.104
765	0.002	TendaTec_69:1b:e0	ASUSTekC_8b:d8:ad	ARP	42	192.168.0.1 is at d8:32:14:69:1b:e0
912	8.499	192.168.0.104	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=442/47617, ttl=128 (reply in 913)
913	0.002	192.168.0.1	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=442/47617, ttl=64 (request in 912)
915	1.006	192.168.0.104	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=443/47873, ttl=128 (reply in 916)
916	0.005	192.168.0.1	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=443/47873, ttl=64 (request in 915)
935	1.014	192.168.0.104	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=444/48129, ttl=128 (reply in 936)
936	0.021	192.168.0.1	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=444/48129, ttl=64 (request in 935)
979	1.003	192.168.0.104	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=445/48385, ttl=128 (reply in 980)
980	0.005	192.168.0.1	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=445/48385, ttl=64 (request in 979)

h. ARP entries in the ARP cache have a limited hold time. If ARP requests can cause network latency, why is it a bad idea to have unlimited hold times for ARP entries?
Answer: ARP entries in the ARP cache have a limited hold time. If ARP requests cause network latency, then it is a bad idea to have unlimited hold times for ARP entries. **Because network latency denotes the overall time takes for a data packet to travel from sender to receiver including delays. If network connection is bad, network latency would increase. As dynamic address keeps changing in same network. One dynamic address can be used later for another host after expired lease time. So, unlimited hold times (of dynamic address) could create problems in devices.** We may not be connected to respective network for this long hold time.

Note: As displayed in the Wireshark capture, ARP is an excellent example of performance tradeoff. With no cache, ARP must continually request address translations each time a frame is placed on the network. This adds latency to the communication and could congest the LAN.

Part 3: Examine Internet Web access

Step 1: Request a Website

a. Start your preferred Browser, but do not request any URL.
b. Start Wireshark and capture without any filter and automatic scroll during live capture.
c. Open a command window and delete DNS cache (Windows **ipconfig /flushdns** or Linux **sudo systemd-resolve --flush-caches**) and ARP cache.
d. Switch to your Browser and request the Website http://www.nt.th-koeln.de/vogt/bs.html
e. Stop your Wireshark capture.

Step 2: Examine the Wireshark capture

a. For Web-Requests you use the HTTP protocol, for Domain Name resolutions you use the DNS protocol, and for local physical communications you use the ARP protocol to map IP addresses to ARP addresses.

- In which sequence should your PC use the protocols HTTP, DNS, and ARP?
- **Answer:** **ARP, DNS, HTTP**
- Does this fit to your capture information?
  Answer: **Yes**. I captured Packets in ARP, DNS, HTTP sequence.

b. Which information is asked for in your **DNS REQUEST**?
Answer: **www.nt.th-koeln.de: type A, class IN**

- Which answer is given by the DNS RESPONSE?
  Answer: **www.nt.th-koeln.de: type CNAME, class IN, cname plesk-02-ext.cit-vip.fh-koeln.de**
- Which IP address is associated with www.nt.th-koeln.de? **Recognize**: There are CNAME alias(es) and an IP address(es).
  Answer: **139.6.10.107** and type CNAME**: cname plesk-02-ext.cit-vip.fh-koeln.de**
- To which local network device has the DNS REQUEST been sent in your LAN? Check the destination MAC address to solve this.
  Answer: **To Router (default gateway)** which has 192.168.0.1 IP address. Destination MAC address **TendaTec_69:1b: e0 (d8: 32: 14: 69: 1b: e0).** This is of router.

c. Check the HTTP request message.

- Which HTTP method has been sent in the **HTTP REQUEST**?
  Answer: Hypertext Transfer Protocol: **HEAD /vogt/bs.html HTTP/1.1\r\n]**
- Which destination IP address was used in the HTTP REQUEST?
  Answer: **139.6.10.107**
- Which remote TCP Port was used? - **80**
- Which local TCP Port was used? – **64034**
- To which local network device was the HTTP REQUEST sent? Check the destination MAC address to solve this.
  Answer: The router's destination MAC address **TendaTec_69:1b: e0 (d8: 32: 14: 69: 1b: e0)** is seen. Through this router IP address was asked to **DNS server in local network** to which the HTTP REQUEST was sent.

Step 3: Examine the network path to a Website with ping

a. Start a new Wireshark capture without saving the previous data. In the command prompt window issue **ping -4 www.cisco.com (**Windows**)** or **ping www.cisco.com (**Linux**)**

Important note: Use the "-4" option of the ping command to exclude IPv6 addresses in this step. Finally stop the Wireshark capture.

Examine the ICMP request-response pairs. Is the ping successful? – **Yes (5 pairs)**

- Which IP time-to-live (TTL) value is received in the ICMP ECHO REPLY message? – **TTL=54 Bytes**
- When an IP packet is sent, the source sets the TTL value in each IP packet. In WinOS TTL usually starts with 128, in UNIX/Linux it starts with 64. With each router hop the TTL is decremented by 1. How many router hops may be passed on the return path from cisco.com?

  Answer: Your OS assumption / no. of hops: **CISCO IOS is mainly used by CISCO.**
  As it's known, the TTL value can provide information about how many intermediary devices like switches or routers, bridges are in media, to whose, packets do reach from sender to receiver. TTL means time-to-live on the way through media before arrival to destination. However, it can be used to measure maximum number of hops, a packet can take on the way. It is acknowledged CISCO TTL or hop number is 255. And every time a packet takes other hop, its TTL is lessened by one. The TTL number that we see is the packet's final TTL when it arrives at its receiver. **To find out the number of hops a packet takes, subtraction is needed from its initial TTL (TTL of CISCO is 255) of the TTL captured. Here, my assumption is number of hops that might be taken by packets from cisco.com to my notebook is 255-54(captured)=201. Including router it would be 201+1=202 hops.**

Step 4: Examine the network path to a Website with traceroute

a. Start a new Wireshark capture without saving the previous data.

- In the command prompt window issue **tracert -4 www.cisco.co** and finally stop the Wireshark capture.
- Save this Wireshark capture locally in .**pcapng** format.
- How many hops do you get by traceroute?

  Answer: In Wireshark capture, from sender to receiver **11 hops** were traced by **tracert** command.

  Compare this result with a).
  Answer: Comparing with step 4-a) the traced routes or hops are **same**. **In command prompt, 11 hops** were detected from my notebook to www.cisco.com. Also **in Wireshark capture** there are **11 hops (TTL=11)** are captured from source to destination.

  Comparing with step 3-a) the traced routes or hops are **not same**. **In command prompt, 54 hops** were detected from www.cisco.com to my notebook as well as in **Wireshark capture** there are **54 hops (TTL=54)** from server to my notebook. But, **my assumption is number of hops that might be taken by packets from cisco.com to my notebook is 255-54=201. Including router it would be 201+1=202 hops.**

  The ICMP TTL exceeded is generated by which OS?
  Answer: The Router sends an error message as TTL exceeded to the sender or source.
  Here, Tenda router use windows operating system.

b. Examine the ICMP request-response pairs.

- In the 1st ICMP ECHO REQUEST, which TTL has been set? – **TTL= 1**
- Which ICMP response message has been received? – **(TIME-TO-LIVE EXCEEDED) Time to live exceeded in transit**
- From which IP address? – **Router's IP address 192.168.0.1**
- How many times was this test repeated with the same TTL? – **Every same TTL was repeated 3 times**

c. Look for the ICMP ECHO REQUEST with TTL+1 value (often the 5th ICMP request).

- Which TTL has been set now? - **TTL=2 was seen in ICMP 4TH ECHO REQUEST**
- Which ICMP response message has been received to this? - **TIME-TO-LIVE EXCEEDED**
- From which IP addresses? - **103.127.177.45**

d. Continue the evaluation of changing TTL values in ICMP requests

- For how many different TTL values do you get ICMP TTL EXCEEDED? –
- **Answer:** There are total TTL=11 for ICMP ECHO REQUESTS. But after 11th TTL, the echo reply was destination unreachable instead of TTL EXCEEDED. And upon 10th TTL, the reply was always as TTL EXCEEDED**. In short, up to TTL=10 values I get ICMP TTL EXCEEDED.**
- By which other ICMP response than ICMP TTL EXCEEDED does traceroute stop the search of the path? Check the last response to the tracert requests.
  Answer: **Destination unreachable ICMP response** stops the search of the path.
  The last response to the tracert command is from **ICMP ECHO REPLY** at TTL=54 from 23.7.211.81 (cisco.com).
  Also, there was simultaneous responses of **Destination unreachable (port unreachable) and Time-to-live exceeded** from other hops.

(

- Describe the mechanism which is used by traceroute to find the path from source to destination?
  Answer:
  Traceroute traces number of intermediary devices on the media from source to destination. Firstly, traceroute sends UDP packet to the destination with TTL=1. TTL means Time-to-Live which limits the life time of data packet in network. It helps to count hops. However, when first router receives first UDP packet with TTL=1, it reduces it by 1, like TTL=1-1=0 and drops the packet and then send a ICMP error message as Time Exceeded to source/sender. Through this, traceroute calculates round trip time also. After getting the error message, sender sends two more packets to the 2nd router and again 2nd router makes TTL=1-1=0 sending same ICMP error messages. Like this, this process happens for three times before source sends next packet by incrementing TTL by 1 that is TTL=2. Until the UDP packet reaches its final destination, in this same way, traceroute keeps tracking average RTT and the IP addresses of routers and other devices with names and upon reaching the destination, ICMP error message: Time exceeded is not sent anymore to source. Lastly, ICMP error message Destination unreachable is sent to source to denote that UDP packet has been reached to destination. In Wireshark, ICMP ECHO packet is sent instead of UDP packet.

Reflection

1.) When your PC wants to send a packet to a host within your network, by which protocol does your PC get the MAC address of the host?- **ARP**

2.) When your PC wants to send a packet to a host in another network, which device will forward this packet into other networks? - **Router**

3.) Wireshark does not display the preamble field of a frame header. Explain why?

Answer: **Preamble carries no useful data in it and is not received like other fields. Actually preamble and SFD work out of frame. They even does not get stored in memory.**

4.) Wireshark does not display the FCS of any Ethernet frame. This function is implemented, because only frames with correct FCS are shown. What is done with Ethernet frames with an incorrect FCS?

Answer: **Usually Ethernet hardware (NIC) drops frames with an incorrect FCS. That is why FCS is not displayed of any Ethernet frame. But if the frames are captured, most NICs will strip the FCS before passing the packets on the physical layer. So for this Wireshark is not able to see whether the FCS was correct or not.**

Checkout

When you successfully finished this Lab, save your solutions file as a PDF.

Upload this PDF and the capture file of Task2/Part3/Step 4 in Ilias Lab Solutions test.