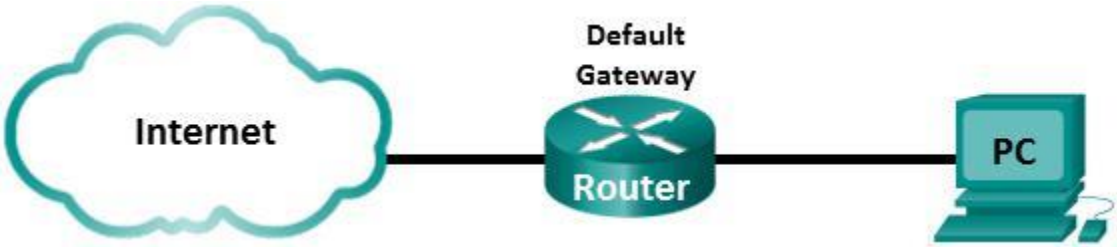
CCNA ITN Lab 1 **Instruction** **Deadline: 27.11.**

Name: Shabnaz Khanam

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

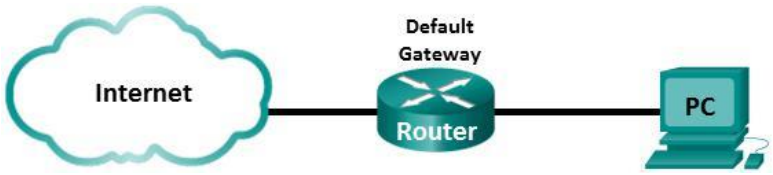
Background / Scenario

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 192.168.0.3
- IP network mask 255.255.255.0
- Default Gateway IP address 192.168.0.1

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 192.168.0.3
- IP network mask 255.255.255.0
- Default Gateway IP address 192.168.0.1
- Record your host MAC address C0-B5-D7-47-91-AB

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? yes
- Which average Round Trip Time (RTT) did you measure?
  7 Mili seconds

Propagation delay

- Estimate the length of the cable path from your PC to your Default Gateway 2100 m
- Calculate the propagation delay 2100m/(2*10^8)=42 ms
- For one RTT, how many times is a frame transmitted over this length? 4 times

Transmission time

- Record the data rate R of your network.
  If this is not available, we assume a 100BASE-Tx network.
- 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.
  (78*8)bits//(100*10^6)=6.24 ms
- For one RTT, how many times is a frame send through an NIC interface? 4 times

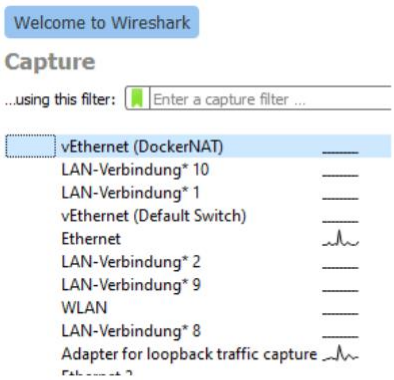
Which type of delay, transmission time or propagation delay, has the highest influence on the ping round-trip-time (RTT) in this scenario? transmission time

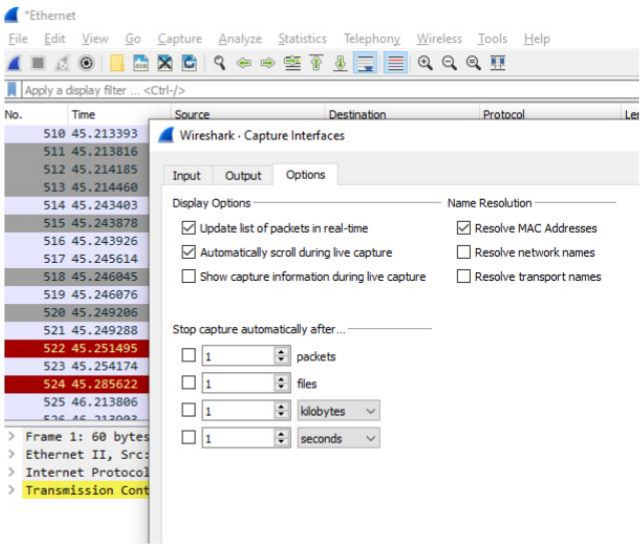
Is there any other delay which has influence on the RTT? no

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.

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

- Source IP address: 192.168.0.3
- Destination IP address 192.168.0.1

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? yes
- Record the Destination MAC address, which is the MAC address of your Default Gateway. c0:c5:22:f3:f3:f7

Check the ICMP detailed information

- Which hex number represents message type Echo Request (ping)?0x0800

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? yes
- 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
  48.64171700-48.63521700=0.00650000ms
- Does this captured RTT match the values of Part2? Discuss your findings.

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

- How many Bytes have been captured in total? 74 bytes
- How many Bytes are in the Ethernet header? 18 bytes
  - Which Ethernet header fields are shown?
    Destination: chongqin_47:91:ab,source,type
- Why is the Ethernet FCS missing in this capture?
  Frame Check Sequence, used by the NIC to identify errors during transmission. The value is computed by the sending machine, encompassing frame addresses, type, and data field. It is verified by the receiver.
- Why is the Ethernet preamble missing in this capture?

  This field contains synchronizing bits, processed by

the NIC hardware.

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

message.

- Which size (in Bytes) does the IP packet have? 32
- How many Bytes are in the IP header? 20
- Which protocol is signaled in the IP header? 14
  - Protocol field (hex value):0x0100 Protocol field (decimal value):256
  - Protocol name: internet Control Message Protocol

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

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

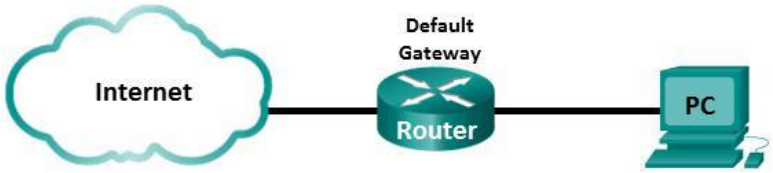
  How many Bytes of ICMP has been sent? ICMP header: 8 bytes ICMP payload:32

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 192.168.0.3
- IP network mask 255.255.255.0
- Default Gateway IP address 192.168.0.1
- Record your host MAC address C0-B5-D7-47-91-AB

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: DNS,ARP,OSPF,SSDP

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**? 0.0.0.0
    - By what information can you decide that answer?

By seeing mac address

- What is the IP address of the device, which responds with **DHCP OFFER**? 192.168.0.1
    - From that info, which device in your network runs the DHCP server? c0:c5:22:f3:f3:f7

- Which IP address is preset as an option in the **DHCP REQUEST** command? 192.168.0.3

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

- How many seconds lease time for the IP address is given to your PC? 3600 s
- 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? arp -a
- What command would be used to delete all ARP entries (flush ARP cache)? arp -d

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

- What MAC address maps to your default gateway? c0-c5-22-f3-f3-f7
- What MAC address maps to the IP broadcast address? 01-00-5e-00-00-16

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? Broadcast
- How long does it take to receive the second ICMP ECHO REPLY as response to the second ICMP ECHO REQUEST? .00054 s

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?

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. Conversely, unlimited hold times could cause errors with devices that leave the network or change the Layer 3 address.

Note: As displayed in the Wireshark capture, ARP is an excellent example of performance trade off. 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

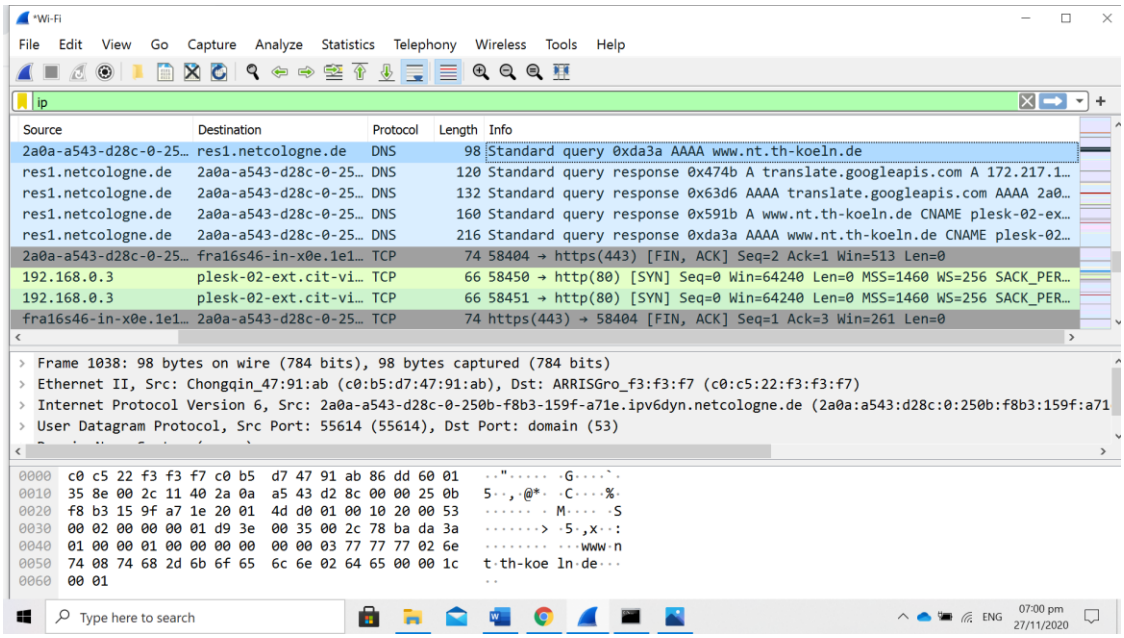
a. Start your preferred Browser, but do not request any URL.

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.

b. In which sequence should your PC use the protocols HTTP, DNS, and ARP? Does this fit to your capture information?
ARP,DNS,HT

c. Which information is asked for in your **DNS REQUEST**? Domain Name, Type,Class

- Which answer is given by the DNS RESPONSE? res1.netcologne.de
- Which IP address is associated with www.nt.th-koeln.de? **Recognize**: There are CNAME alias(es) and an IP address(es). 139.6.10.107
- To which local network device has the DNS REQUEST been sent in your LAN? Check the destination MAC address to solve this. c0:c5:22:f3:f3:f7

d. Check the HTTP request message.

- Which HTTP method has been sent in the **HTTP REQUEST**? GET
- Which destination IP address was used in the HTTP REQUEST? 139.6.10.107
- Which remote TCP Port was used? 80
- Which local TCP Port was used? 63532
- To which local network device was the HTTP REQUEST sent? Check the destination MAC address to solve this. c0:c5:22:f3:f3:f7

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

- Which IP time-to-live (TTL) value is received in the ICMP ECHO REPLY message? 58
- 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?

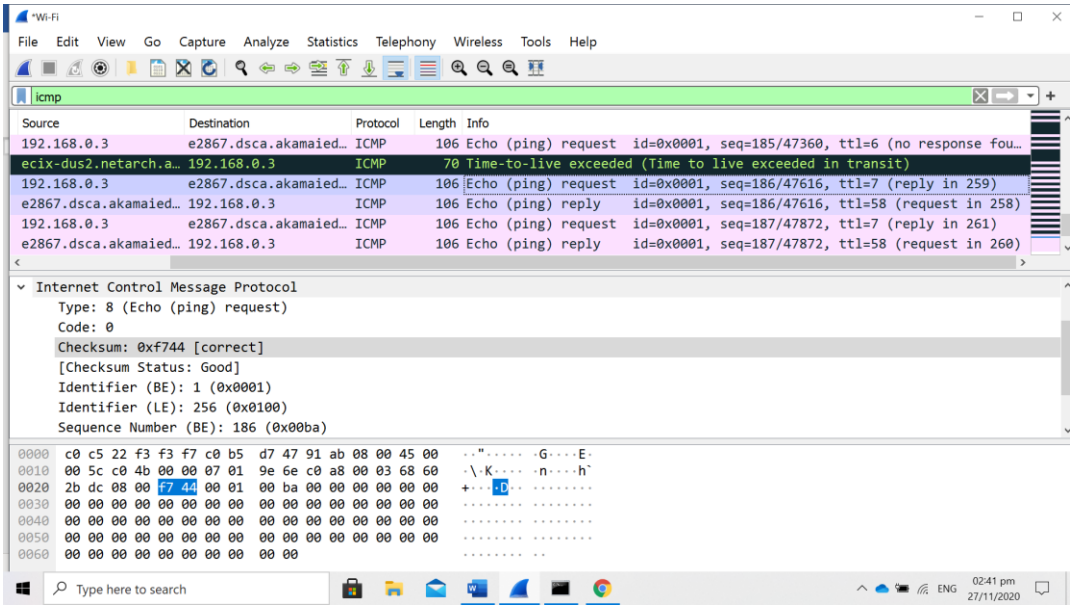
  Your OS assumption / no. of hops 7

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 and finally stop the Wireshark capture.
- Save this Wireshark capture locally in .**pcapng** format.
- How many hops do you get by traceroute? 30

  Compare this result with a). The ICMP TTL exceeded is generated by which OS? 7



b. Examine the ICMP request-response pairs.

- In the 1st ICMP ECHO REQUEST, which TTL has been set? 7
- Which ICMP response message has been received? Type: 8
- From which IP address? 192.168.0.3
- How many times was this test repeated with the same TTL? 3 times

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

- Which TTL has been set now? 2
- Which ICMP response message has been received to this? Type 8

- From which IP addresses? 192.168.0.3

d. Continue the evaluation of changing TTL values in ICMP requests
   - For how many different TTL values do you get ICMP TTL EXCEEDED? 4
   - 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. Type 0
   - Describe the mechanism which is used by traceroute to find the path from source to destination?

     Time to Live

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? Address Resolution Protocol

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?

There is no **preamble** in the fields shown in **Wireshark**. The **preamble** is a physical layer mechanism to help the NIC identify the start of a frame. It carries no useful data and is not received like other fields. There is a destination address and a source address.

4.) Wireshark display does not 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?

The **FCS** is calculated and applied by the NIC instead of by the OS. If the **Frame** Check Sequences were really **incorrect**, the **frames** would be discarded and the communication would fail.

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.