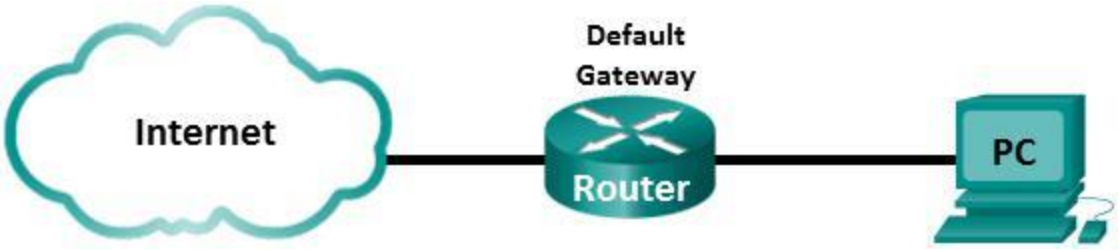
CCNA **ITN Lab 1**

Team-No.: 04 **Names: Sanjida Shamin, Febin Chollapra, Rubaiya Kabir Pranti**

ITN Assessments: Modules 1 - 3: Basic Network Connectivity and Communications Exam

Simple Network and Internet Access Analysis



Lab Preparations

Lab Instructions

Task1	Simple Network and Connectivity Testing
Task2	Capture Packets and analyze Protocols to connect to the Internet

Deliverables and List of Due Date

Lab Preparation

Part 1: Lab Instructions

a. Read the **Lab Instructions** of this Lab before you continue.

Part 2: Ideas about some delays in networks

a. Read the NP lecture chapter 1 (1. Grundlagen) or the ITN 1 Info for Master Students, and calculate the following delays.

b. 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.
We know,

Propagation delay, tpd= l / C = length of link/transmission speed

where l = length of the link =55m and

C= velocity of the signal through twisted pair cabling =2 / 3 c0 = 2 / 3 × 300.000 km / s
=200,000 km / s
=2×108 m / s
Therefore, tpd= l / C = 55m / (2×108) 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).

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 c0 = 2 / 3 × 300.000 km / s
=200,000 km / s=2×108 m / s
l = length of the link =600 km (given)
We know,
Propagation delay, tpd= l / C
= (6×105 m) / (2×108) m / s = 3×10-3 s= 3 ms = 300,0000 ns

c. 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:
We know,
Transmission time , t_t= M/R = Size of data/ bit rate
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

Part 3: 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? Which command displays all IP settings?

In command prompt, the following command is used to set IP address and subnet mask.
For example: netsh interface ipv4 set address name

Which command displays all IP settings?

ipconfig /all

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?

static or dynamic(DHCP): ipv4 address, subnet mask, gateway

b. Linux PC

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

ifconfig IP address subnet-mask up

Which command displays all IP settings?

ifconfig –a

Networking tools

Which tool (command) shows, whether a host reachable or not? **ping**

Which tool (command) lists all routers in the path from your host to a destination?

tracert(windows) or
traceroute(linux)
tracert www.google.com

Which tool (command) displays all sockets used on your computer (Windows and Linux)?
netstat 192.168.0.4(host ip address) > windows

Which tool (command) displays the mapping a domain name to an IP address?
nslookup google.com

Part 4: 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 be done after you captured all packets, sent and received by your host?

By using ICMPv6 in filter option of wireshark, we can filter traffic.
Additionally, DNS, HTTP, TCP, UDP can also be filtered.

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!!!**

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

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 Ethernet frame. The 8 byte is also not stored in memory. They only work for their respective duty.

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

Destination address+ source address +frame type= (6+6+2) bytes=14 Bytes

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

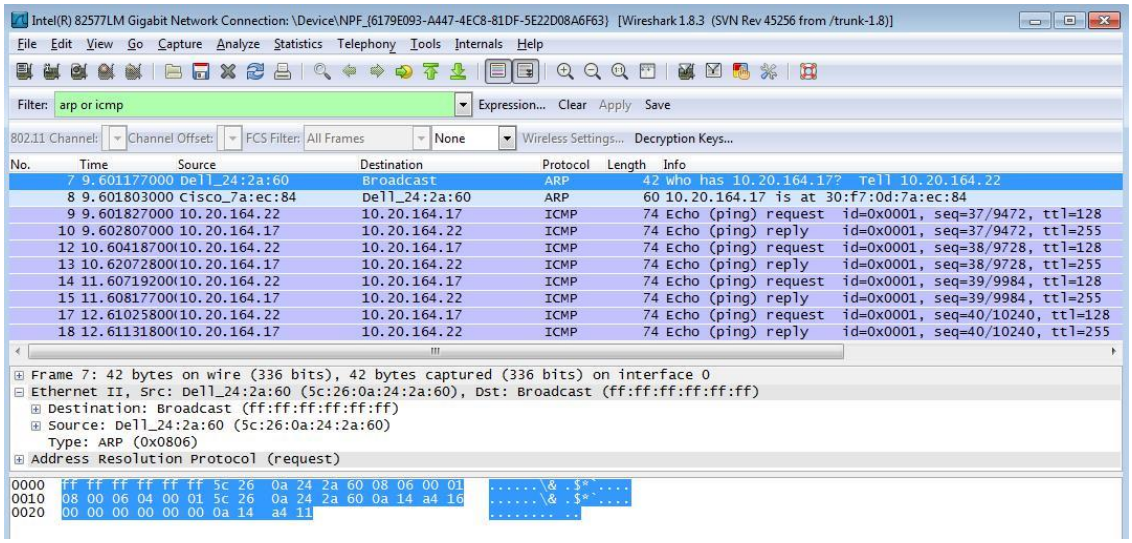
FCS=4 byte

c. Examine Ethernet frames in a Wireshark capture. The

```
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.



1. **Check frame #7.** 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.
   If there is no significant error capture or bad checksum while transferring frame, there might be no FCS shown in Wireshark capture.

2. ARP – Address Resolution Protocol. **Check frames #7 and #8.**

   b.1) Which IP source address is used in the **ARP request**?
   No IP source address is used in ARP request. MAC address is used by ARP only.

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

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

   The Ethernet frames generated from host device already get the MAC address of the local destination.

   b.4) What is the Vendor ID (OUI) of the Source's NIC?
   5c:26:0a or Dell

Part 5: 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 Type 8: **Echo request**

ICMP Type 0: **Echo reply**

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

ICMP Type 3 Code 0: **Destination unreachable (Net Unreachable)**

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

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

ICMP Type 3 Code 4: **Fragment Needed or Don't Fragment was Set**

Any idea why the PC sends out a broadcast ARP prior to sending the first ping request?

Prior to sending the first ping request to a destination device, PC needs to know the MAC address of the default gateway/router. Then after knowing the MAC address of gateway, PC can finally send request to remote area. And the ARP request is sent as a broadcast request from PC because PC wants to get specific MAC address of a particular device such as of default gateway 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 router's, router (default gateway) sends out ARP response to the first host with its MAC address.

Part 6: Examine DHCP

Check information about the DHCP protocol, e.g. using www.wikipedia.com.

a. Describe briefly the task of DHCP (Dynamic Host Configuration Protocol).

DHCP server (Dynamic Host Configuration Protocol) 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 etc.
DHCP Discover: Here host looks for DHCP server.
DHCP Offer: Then DHCP server offers an IP 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.

b. Which eight DHCP messages are available in this protocol?

Discover, Offer, Request, ACK, NCK, Decline, Release, Inform

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

Discover, Offer, Request, ACK

Task1 - Simple Network and Connectivity Testing

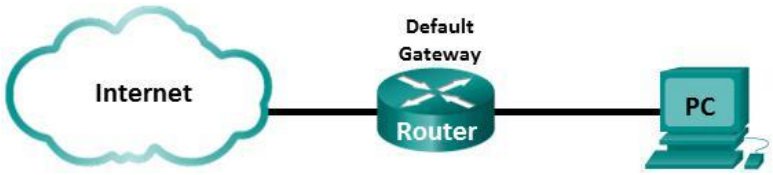
Background / Scenario

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 HomePC.

- Host IP address: **192.168.0.4**
- 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: **192.168.0.4**
- IP network mask: **255.255.255.0**
- Default Gateway IP address: **192.168.0.1**
- Record your host MAC 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? **yes**
- Which average Round Trip Time (RTT) did you measure?
  RTT from command prompt= 4ms

  RTT from wire shark= 441us

Propagation delay

- Estimate the length of the cable path from your PC to your Default Gateway

  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

  We know,
  Propagation delay, t_{pd}= 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, t_{pd}= 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? **2 times**

Transmission time

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

  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=624 ns

- For one RTT, how many times is a frame send through an NIC interface?

  4 times

Part 3: Capture and Analyze Local ICMP Data in Wireshark

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

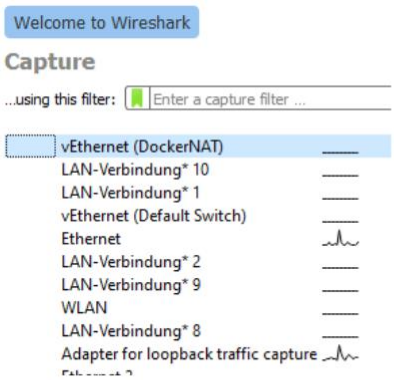
Total propagation delay for 2 times: 2* t_{pd}=2*33.3ns=66.6ns
Total transmission time for 4 times: 4* t_t=4*624 ns= 2496 ns
So, $t_{pd} > t_t$
Propagation delay influence RTT most.

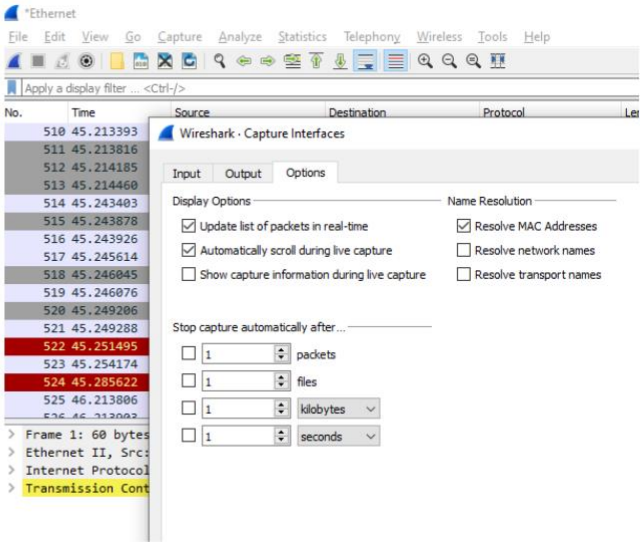
Is there any other delay which has influence on the RTT?

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
Devices: Intermediate routers or servers
These delays depend on number of hops between sender and receiver.
Overall, distance and transmission media between server and host along with number of network hops, traffic in media, interference present in circuit, the speed of intermediary devices and server response time effects RTT.

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: **192.168.0.4(laptop)**
- Destination IP address: **192.168.0.1(router/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? **yes**
- Record the Destination MAC address, which is the MAC address of your Default Gateway.
  MAC address of your Default Gateway/Router/Destination:
  c0: c5: 22: eb: 0f: 6f or ARRISGRO_eb:0f:6f

Check the ICMP detailed information

- Which hex number represents message type Echo Request (ping)?
  0×08 (type), Code: 0×00 which denotes ICMP Type 8, Code 0

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 **548 µs**
- Does this captured RTT match the values of Part2? Discuss your findings.
  Yes. Previously RTT was varying around 441us, now it varies around 548us

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

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

How many Bytes are in the Ethernet header?
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? **3 fields such as**
  Source MAC address: ASUSTekC_8b:d8:ad
  Destination MAC address: ARRISGRO_eb:0f:6f
  Frame Type: **IPv4 (0x0800)**

- Why is the Ethernet FCS missing in this capture?

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?

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.

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

- Which size (in Bytes) does the IP packet have? The length of IP Packet is seen as **60 Bytes**.
- How many Bytes are in the IP header? **20 Bytes.**
- Which protocol is signaled in the IP header?
    - Protocol field (hex value): **0x01** Protocol field (decimal value): **01**
    - Protocol name: **ICMP**

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

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

- How many Bytes of ICMP has been sent? **40 Bytes**

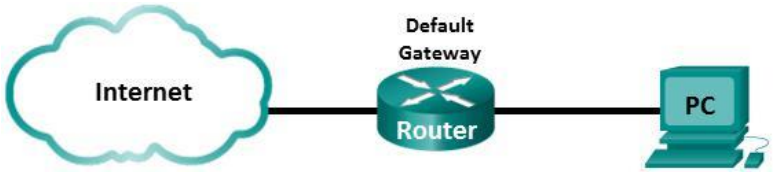
ICMP header: **8 Bytes** ICMP payload: **32 Bytes**

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 **192.168.0.4**
- IP network mask **255.255.255.0**
- Default Gateway IP address **192.168.0.1**
- Record your host MAC address **ASUSTekC_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: **DNS, ARP, MDNS, SSDP, TCP, UDP, TLSv1.2, ICMP, ICMPv6, NBNS**

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 Asus laptop**
- By what information can you decide that answer? **MAC address of laptop**
- 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? **(router)/gateway**
- Which IP address is preset as an option in the **DHCP REQUEST** command? **laptop's=192.168.0.4**
- Does the **DHCP ACK** command confirm the requested IP address? **Yes. It is acknowledged that the last DHCP ACK command confirm the requested IP address (again 192.168.0.4) 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? **3600 s or 1 hour**
- 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** command
- What command would be used to delete all ARP entries (flush ARP cache)? **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? **c0-c5-22-eb-0f-6f dynamic**
- What MAC address maps to the IP broadcast address? **192.168.0.255 ff-ff-ff-ff-ff-ff static**

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?

  an ARP request is to Broadcast.
  an ARP reply is to host laptop.

- How long does it take to receive the second ICMP ECHO REPLY as response to the second ICMP ECHO REQUEST? **429 µs**

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?

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?
  ARP, DNS, HTTP
- Does this fit to your capture information? **yes same as before as**
  ARP> DNS >HTTP

Which information is asked for in your **DNS REQUEST**?
As DNS request, IP address of www.nt.th-koeln.de is asked.

- Which answer is given by the DNS RESPONSE?
  DNS first response to query www.nt.th-koeln.de:
- **www.nt.th-koeln.de: type CNAME, class IN, cname plesk-02-ext.cit-vip.fh-**
- **koeln.de**
  DNS second response to query www.nt.th-koeln.de:
- **www.nt.th-koeln.de: type A, class IN, addr 139.6.10.107**
  another DNS Response:
  plesk-02-ext.cit-vip.fh-koeln.de: type A, class IN, addr 139.6.10.107 and etc.
- 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.
  To Router (default gateway) which has 192.168.0.1 IP address

b. Check the HTTP request message.

Which HTTP method has been sent in the **HTTP REQUEST**? **GET request**

GET method (GET /vogt/bs.html HTTP/1.1)

- 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? **61405,61406**
- To which local network device was the HTTP REQUEST sent? Check the destination MAC address to solve this.

The MAC address is of router's/default gateway's. so it's the gateway/router.
Router's MAC address: c0: c5: 22: eb: 0f: 6f or ARRISGRO_eb:0f:6f

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? **TTL=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?
  As CISCO uses Linux operating system also. For this OS, we know, TTL=64
  64-58=6 hops maybe passed by from cisco.com to host on return path.

  Your OS assumption / no. of hops: **Linux server with 6 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.com** and finally stop the Wireshark capture.
   - Save this Wireshark capture locally in .**pcapng** format.
   - How many hops do you get by traceroute? **7 hops**

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

     7 hops (**from my notebook to cisco server**).
     To find out the number of hops a packet takes, subtraction is needed from its initial TTL (which is TTL of linux is 64) to the TTL captured(TTL=58 from a).
     hops taken from cisco.com server to my laptop is 64-58(captured)=6 hops. Including router, it would be 6+1=7 hops.

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**
   - From which IP address? **192.168.0.1**
   - 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? **TTL=2**
   - Which ICMP response message has been received to this? **Time-to-live Exceeded**
   - From which IP addresses? **172.31.0.1**

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

- For how many different TTL values do you get ICMP TTL EXCEEDED? **for 6 different TTL values**
- 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. **ICMP echo reply**
- Describe the mechanism which is used by traceroute to find the path from source to destination?

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?

Preamble & 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 Ethernet frame. Preamble carries no useful data in it and is not received like other fields. 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?

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.

Deliverables

Lab Teams

This lab may be solved in teams of max. 3 students. All teams have to upload their deliverables in time.

Teams are grouped into 2 groups, which have different due dates and presentation dates.

Module Group Exams

Each team member must solve the requested **Module Group Exams** before delivery date.

Deliverables

Each teams uploads the following files:

- One **PDF-File (.pdf)** with the completed **Lab Preparations and Lab Instructions**. All tasks and questions must be answered.
- One **Wireshark capture file** of Task2/Part3/Step 4

Due Dates

Group 1	Teams 1-10	Due Date
	Module 1-3 Group Exam	25.10. - EOB
	Upload Deliverables	25.10. - EOB
	CCNA ZOOM Presentation	27.10. - 16:45 ff.

Group 2	Teams 11-20	Due Date
	Module 1-3 Group Exam	01.11. - EOB
	Upload Deliverables	01.11. - EOB
	CCNA ZOOM Presentation	03.11. - 16:45 ff.