NT Assignment Repetition

A Day in the Life: Brief Repetition of Network Technologies

Task 1: Start Linux Environment with Kathara

Download the virtual guest OS Kathara image from <https://www.fhict.nl/docent/downloads/TI/S3/>.

You are going to repeat the basic Internet protocols that you have already learned and simulate a typical home network.

You are going to do that with help of a Kathara network simulation tool (<https://www.kathara.org>) that is included in the provided Linux image.

Kathara is a newer and much more efficient version of Netkit, based on Docker.

You can find manual pages of Kathara on the above mentioned site.

The provided lab simulates “A Day in the Life Scenario” from the presentation.

To execute the assignment, unzip the provided zip file.

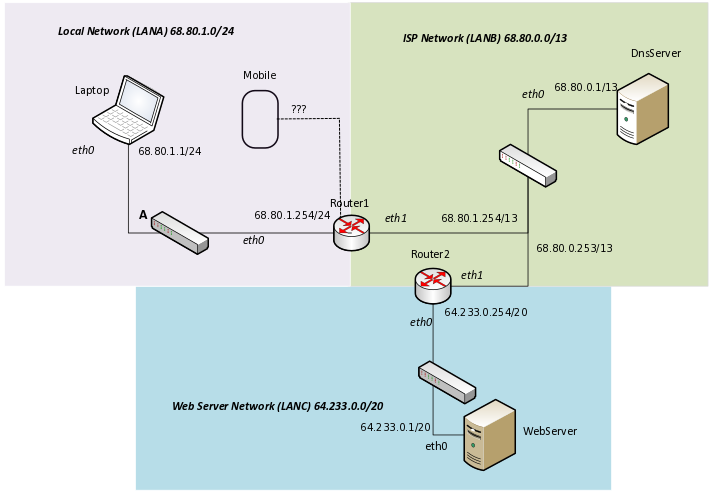
You can start your lab by issuing the following command in the root directory of the lab:

kathara lstart

After you’ve finished with the lab, you can shut the lab down by issuing:

kathara lclean

Now you have running network as shown during the lesson presentation:



*Laptop*, *Router1*, *Router2*, *WebServer* and *DnsServer* have static addresses and are connected to each other through routing. *Mobile* is a node that enters the network and will get an address through DHCP. Study the provided lab and network picture. Try out connectivity of the network nodes by using ping command.

Task 2: DHCP Protocol

The local network (LANA) uses both static and dynamic IP addresses. Dynamic IP addresses are in the range 68.80.1.11/24 – 68.80.1.100/24. All other addresses are static and are not to be used by DHCP.

Please study the DHCP protocol from the provided materials or from Internet.

The *Router1* is already configured and running DHCP Server (isc-dhcp-server). You can find its DHCP configuration file by looking to the subdirectory router1/etc/dhcp. Study this configuration file and configure this DHCP server to distribute all possible dynamic addresses.

What did you change? Provide your configuration below:

Text

Description automatically generated

After configuration, go to the *Mobile* node, which does not have address yet,

Issue these commands to start and trace the DHCP procedure.

tcpdump –w /hosthome/<file>.pcap –s 0 &

dhclient eth0[[1]](#footnote-1)

The first command should create a Wireshark trace of the traffic you’re going to generate and store it in your Linux home directory in a <file>.pcap file.

The second command should start the DHCP process and generate the DHCP traffic.

Once the DHCP process is finished, the IP address of Mobile should be configured.

Provide screenshot of a Linux command that shows the new configured address.

Text

Description automatically generated

If your IP address is configured properly, you can stop the tcpdump program.

You do it by issuing these commands:

fg %1

CONTROL C

The first command brings tcpdump command to foreground (it was put to background with & at the end of command).

The second command stops tcpdump and closes your file <file>.pcap

Now you should be able to use Wireshark to read your <file>.pcap trace from the home directory.

You do it like this:

wireshark <file>.pcap

Provide a screenshot from Wireshark showing the 4 packets of DHCP DORA process.

Graphical user interface, table

Description automatically generated

*Tip :*

*Note that in the Kathara lab environment you can use the directory structure under <node> directory to specify the files in your virtual <node> environment.*

*<node> has to start with small (so not capital) letter.*

*So, e.g. if you want to change /etc/dhcp/dhcpd.conf file of your virtual Router1 node, you can do this in the lab directory:*

*/home/student/kathara\_labs/aditl/router1/etc/dhcp, in the file dhcpd.conf.*

*Also, next to adjusting existing configuration file you can also add configuration files as far as they have expected name and location. After a change to configuration you should restart your Kathara lab again.*

Study DHCP protocol. Explain why there are 4 packets exchanged (DHCP DORA). Why is Discovery and Offer not enough?

Look at the Wireshark trace again and show the field in the Offer packet where the IP address is offered. Provide screenshot.

The 4 packets of the DHCP protocol are Discover, Offer, Request and Acknowledge. When the client connects to the server, it has no idea of anything of the network it just entered, so a discovery broadcast is sent to all devices connected. The server then also doesn’t have how to directly speak to the new client so it broadcastes back an ip offer. Those two steps aren’t enough because the server also needs to know if the new client will accept the ip. This is done in the next two steps, where the client request to use the given ip address and then the server acknowledges back the request so the ip is set and the connection is established inside the network.

Text

Description automatically generated

Task 3: DNS

Part 1:

Study the DNS protocol from the provided material and/or Internet. You are going to do a simple configuration of the DNS server (*DnsServer* node). When you look at the subdirectories of the *DNSServer* node in the lab, you’ll find an example configuration for a domain *mygoogle.com*. Make up your own domain name and configure it in exact the same way as *mygoogle.com*. Find out some name for your host (it will map to the IP address of the *WebServer*) and add an A record for it. Just look at the way *mygoogle.com* and *host1.mygoogle.com*  is configured and create your configuration in an analogue way.

Test your configuration by issuing ping from the Laptop to your configured host address. Provide screenshot of the successful ping and described what you configured.

Text

Description automatically generated

Is the DNS server at your *DNSServer* node authoritative or recursive? Explain your answer.

The DNS server is recursive because we only ping it and then it is tasked to find the ip address of the provided name. If the ip address isn’t cached in it, then it will ask for help from an authoritative dns that contains the “.com” section or many others that may contain the name provided.

Part 2:

Choose your own web address (e.g. [www.fontys.nl](http://www.fontys.nl)) and use *dig* command from the Linux command line to find out its IP address.

What is the output of this dig command? Can you explain what you see in the output of the dig command?

Text

Description automatically generated­­­

The output of the dig command shows the information of the web address such as:

• flags

• class of the query (IN stands for internet)

• name of the web address

• the type of query (A stands for address)

• ip address associated with the domain name

What IP Address belongs to your chosen host?

The ip address is 68.80.0.1/53

Try also DNS delegation for your chosen host. Go to <http://simpledns.com/lookup-dg> page and find out how the DNS resolution is being done.

Provide a screenshot of the output. Which root server is used?

“l.root-servers.net” is used for the root server.

Graphical user interface, application

Description automatically generated

Task 4: Adress Resolution Protocol - ARP (Optional)

Study the working of ARP protocol from the provided materials/Internet.

Restart your lab, so you have clean environment and all ARP entries are empty.

Otherwise clean the ARP cache of all nodes by hand (you can issue “ip –s –s neigh flush all” to clean up ARP cache).

Check whether your ARP cache is clean by issuing “arp” command.

Make a ping between *Laptop* and *WebServer*. Now check the ARP entries of all nodes again.

What have changed? And why? Provide the screenshots of the changed ARP tables.

Note: keep your lab, we will further configure it in next lessons!

1. Please ignore the error: mv: cannot move '/etc/resolv.conf.dhclient-new.46' to '/etc/resolv.conf': Device or resource busy [↑](#footnote-ref-1)