COMPX204-20B - Network Debugging and Host IP Configuration

Due: 5th October, 2020 (v3)

1 Introduction

In this assignment, you will diagnose issues in a small network. You will be using tools such as `traceroute`, `ping`, `host`, `tcpdump`, and `wireshark` to diagnose issues with a network. In addition you will be guided through finding and fixing common network problems and using the `ip` command to add or modify routes and IPv4 addresses.

Remember you can access the manual for any tool that you are asked to use by running `man` followed by the command name. For the `ip` command, the subcommands are split out. So you would run '`man ip addr`' to find how to use the `ip` command to configure a host's IP address. Please take some time to read about the commands that you are running.

2 Academic Integrity

The files you submit must be your own work. You may discuss the assignment with others but the actual configuration you submit must be your own. You must fully also understand what you have configured and be capable of reproducing and modifying it. If there is anything that you don't understand, seek help until you do.

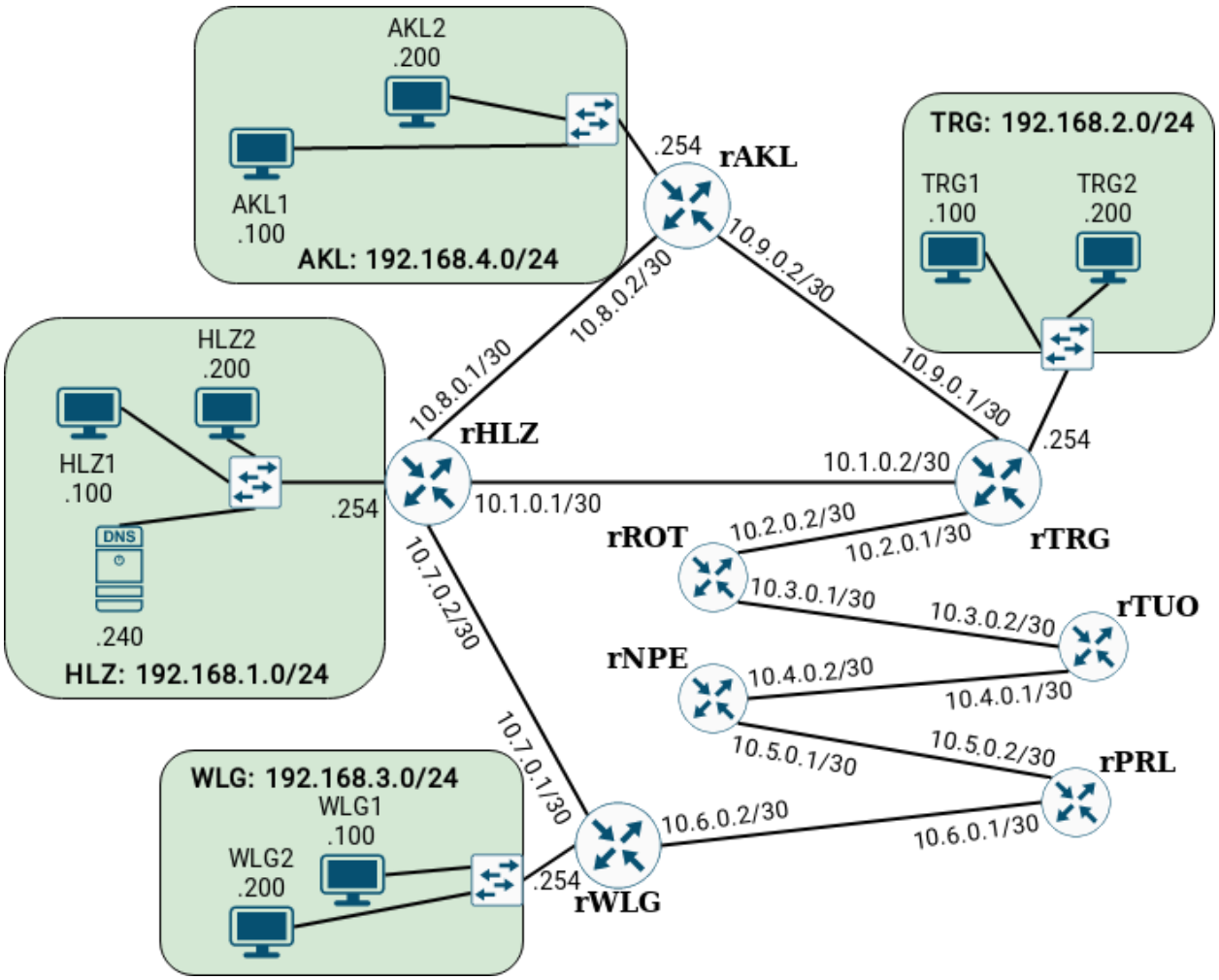
You must submit your files to Moodle in order to receive any marks recorded on your verification page.

This assignment is due **Monday 5th October by 11am** and worth 7% of your final grade.

3 Assignment Specification

The goal is to become familiar with finding issues in a network's configuration, and to do this you will be manually configuring hosts with addresses, routing and DNS. Typically, an end host learns this information automatically using the Dynamic Host Configuration Protocol (DHCP) protocol. This is the reason that you normally don't have to manually configure addresses everytime you connect to the WiFi. But having the skills to identify problems in a network is very useful, and gives you a chance to apply the theory you've learnt during the lectures.

3.1 Network addressing plan



Above is the addressing plan for the network which you will debug and configure during this assignment. There are a total of 8 routers ( ), 4 of these routers have hosts attached, while the remaining 4 do not. Between routers are links. Each link is addressed out of a /30 subnet, this contains two usable addresses, one for each end of the link. These address ranges are not global routable, but you find these addresses in ICMP responses. That means you will **not** be able to directly ping the 10.X.X.X/30 address. The routers rWLG, rTRG, rAKL, and rHLZ each have two hosts attached. For example, the WLG network has two hosts attached to a switched (

) network assigned from the 192.168.3.0/24 subnet, WLG1 with the address 192.168.3.100/24 and WLG2 with the address 192.168.3.200/24. Additionally, rWLG has an interface attached to the network with the address 192.168.3.254/24, rWLG acts as the gateway for the WLG hosts.

Attached to the HLZ network is a DNS server. This resolves both a name to an IPv4 address and IPv4 address to a friendly name. This makes interpreting traceroute output much easier. However, for DNS to work, hosts in networks other than HLZ need a route to reach the DNS server.

Your goal is to diagnose mistakes and complete the configuration to match the diagram above so that all hosts can talk to each other. For example, by the end of the assignment, WLG1 should be able to ping WLG2, HLZ1, HLZ2, TRG1, TRG2, HLZ1, HLZ2 and so on. This assignment guides you through the steps to fix the network.

Each host needs to be configured with: 1) an ip address in the correct subnet, 2) a default route pointing to the gateway (i.e. the corresponding router) (the .254 address), and 3) a DNS server. The routers, with one exception, are already fully configured for you.

3.2 Getting Started

You will use two scripts to run the assignment. You use one to start the assignment (`start_compx204_assignment5.sh`) and another (`enter_host`) to connect to hosts or routers within the assignment. These scripts are available in `/home/compx204/` on the lab machines. The scripts are also available on Moodle if you want to try at home, note you will need a modern version of Ubuntu to make this work. For this assignment, I will assume that you are running on a lab machine.

In one terminal start the assignment by running (on a lab machine):

```
cms-rg06-50:~$ /home/compx204/start_compx204_assignment5.sh ~/a5-save
No existing configuration found.
This script will initialise a fresh copy of the assignment.
Your configuration will be saved to: a5-save
Do you want to continue? [y/N] y
Assignment 5 loaded successfully
Type 'exit' when you are done
root@compx204-assignment-5#
```

This will start the assignment and save the changes that you make to a directory named a5-save in your home directory. You will need to zip and submit this via Moodle as part of your assignment submission. When you are finished working on the assignment, simply type ‘exit’ in this terminal and wait for your work to be saved. **If you close the terminal window your work will not be saved.** Try saving your configuration now:

```
root@compx204-assignment-5# exit
Please wait while your work is saved
Saving AKL1
...
Save completed to: a5-save
```

```
rsanger@cms-rg06-50:~$
```

If you look in the ‘a5-save’ directory using `ls` you will find a number of files have been saved. The next step is to connect to a host so that you can configure it. First, you need to make sure that the assignment is running. So run `start_compx204_assignment5.sh` again as before; this time it should detect the existing configuration. In another terminal, now run:

```
rsanger@cms-rg06-50:~$ /home/compx204/enter_host HLZ1
root@HLZ1:~#
```

This brings you into a terminal, notice that you can always see which machine you are by checking the hostname on the left of the machine. These hosts and routers are running in Linux namespaces, so while the network interfaces you see on these machines are unique, the filesystem is shared with the host pc. You appear as the root user within this host; however, this is mapped back to your standard user account if you make changes to the filesystem. When you ‘exit’ the main assignment script this will disconnect all hosts that are still connected.

3.3 Your tasks

This will guide you through fixing the configuration on all of the hosts, one at a time. Don’t expect to be able to ping every other host until you have completed all steps. You may wish to read ahead, to get an idea of the configuration needed, but complete the steps in order.

1. Connect to hosts AKL1 and AKL2 and verify that they can reach each other using ping. Both machines are fully configured for you. You should find that you can connect to the machines by using either their IP address or name. For example, you can ping AKL1 or 192.168.4.100.
2. Users have noticed that WLG1 and WLG2 cannot ping each other, however they can reach external hosts like AKL1. Diagnose the misconfiguration on WLG1 and WLG2 which is stopping hosts being able to talk to each other. Note, hosts should have their address configured on their `eth0` interface. Look at the addresses assigned on each machine using the ‘`ip addr show`’ command, you will find a mistake on one. Delete the incorrect address and replace it with the correct address using the ‘ip addr’ command. Use the ip command manual, or search for a tutorial to find the correct command(s) to run.

   Write down what you saw when pinging from WLG1 -> WLG2, and compare that to pinging from WLG2 to WLG1.

   Write down the command(s) that you ran to fix the problem:

   Note: once you correct the address, you will need to reinstall the default route which was removed in the process by running to get DNS and external connectivity again:
   `WGL1 (or WLG2)# ip route add default via 192.168.3.254`

3. Users have noticed that HLZ1 cannot reach any external hosts, but can reach HLZ2. From HLZ1, compare pinging to AKL1 vs HLZ2. *What error do you get when pinging to AKL1?*

   This error response is typical of what you'll see if there is no route to a destination. Find and run the correct `ip route` command to install a default route (address 0.0.0.0/0) via the gateway for the HLZ network. The gateway is the address on the router attached to the HLZ network, in this case 192.168.1.254.
   Write down the command(s) that you ran:

4. Users of HLZ2 have noticed a different issue, they can connect to IP addresses directly but cannot connect using their friendly names. ***Write down the error that you see when you try to reach HLZ1 from HLZ2 using its friendly name, for example use the*** **`ping`** ***command?***

   On most Linux systems there are two text main files which you can edit to configure DNS. 1) you can add a entry to map a specific name to a specific address in `/etc/hosts` (this will override any response from your DNS resolver), and 2) you can configure the DNS server to use in `/etc/resolv.conf` (typically, this is configured for you, but for this assignment you will need to configure it).
   Try both. First, on HLZ2, open `/etc/hosts` in a text editor of your choice and add an entry for HLZ1. Verify that you can now resolve HLZ1 by name. It is common practice to map your machine's name to the loopback address in this file and map 'loopback' to the loopback address (127.0.0.1). This file is carried over from the lab machine, but changes you make will persist on each host. ***Write down the entry that you added.***

   Second, on HLZ2, open `/etc/resolv.conf` with a text editor and configure the correct address for the nameserver (192.168.1.240). The existing file, again, is from the lab machine, you should remove the search domain and any additional nameserver entries. Verify that you can resolve AKL1 by name. It might take 10+ seconds to apply.
   Write down what you have in the /etc/resolv.conf file.

5. Hosts TRG1 and TRG2 have not yet been configured. Configure both with the correct IP address using `ip addr`, a default route via the TRG gateway router using `ip route`, and the dns resolver in `/etc/resolv.conf`. Refer back to your notes above to find the correct commands to run. Verify that TRG1 and TRG2 can reach each other and that both can reach an external host like AKL1 by name.
6. Users of TRG1 and TRG2 have noticed that they cannot reach WLG1 or WLG2. Use `traceroute` to diagnose the problem. Compare running traceroute from WLG1 to TRG1 with running traceroute from TRG1 to WLG1.

Write down the difference that you observe.

Take a packet capture using `tcpdump` of the traceroute in each direction. You can later use `wireshark` to view it; however when you are in the hosts namespace you cannot run `wireshark` directly. Open a second terminal to the host, start tcpdump:
`root@TRG1:~# tcpdump -i eth0 -w /home/<user>/trg1-tr-wlg1.pcap`
Here we run tcpdump with two options -i eth0 tells tcpdump to capture packets on the eth0 interface and -w file.pcap tells tcpdump to save the packets to that file.
Then in another terminal run the traceroute until completion. Finally, type control-c in the tcpdump terminal to end the capture.

Once you repeat for both, open these files in wireshark and identify the extra packet seen at the end of one of them. ***Write down the type of this extra packet. Does this explain the different errors you saw from traceroute?***

7. Correct the issue that you identified in step 6. To do this you will need to login to the appropriate router, this works just like logging into a host. For example:
   `rsanger@cms-rg06-50:~$ /home/compx204/enter_host rNPE`
   `root@rNPE:~#`
   The issue that you identified is a missing route on one of the routers. You will need to login to the correct router and run an `ip route` command to add this route. Unlike with the default route you add to hosts, you need to add a route for the missing subnet explicitly. Therefore, you will be adding a route for either TRG (192.168.2.0/24) or WLG (192.168.3.0/24). I recommend looking at the existing routes on the routers by running the `ip route show` command to figure out the command that you need to run.
   Write down the command that you need to run and the router you ran it on:

8. Finally, run `traceroute` to find the latency (round-trip time) of the links between the routers. At this point you should have full network connectivity. You will need to run `traceroute` between different hosts to cover all links. For this question, you can round the latencies you find to the nearest millisecond and assume that the same forward and return path is being used. *Note, if you run traceroute in quick succession Linux ICMP rate-limiting might start to limit the responses that you see, just wait a moment and try again.*
   Write down what you found (you can annotate the diagram above). Are the routes being used the most optimal in terms of latency?

VERIFICATION PAGE

Name: _____

Id: _____

Date: _____

Note: this practical must be verified by **Monday 5th of October 2020 at 11am**. It will be marked out of 7 and is worth 7% of your final grade.

You must submit your saved configuration files (first zip the folder) and both of your tcpdump captures (from step 6) to the Moodle assignment page **before** you have had the assignment verified.

1. Explain the issue you found and how you fixed it on the WLG1 and WLG2 hosts (step 2).

2. Explain the issue you found and how you fixed it (in step 3) on the host HLZ1.
3. Explain the issue you found and how you fixed it (in step 4) on the host HLZ2.
4. Demonstrate that TRG1 and TRG2 have been configured correctly, e.g. ping AKL1 (step 5).
5. Explain the extra packet that you saw (in step 6), and show the demo your wireshark capture.
6. Explain how you fixed the connectivity issue between TRG and WLG (in step 7)
7. Show the demo the latency measurements that you found in (step 8)
8. Show the demo that you have uploaded your configuration files (zip the folder) and both of your tcpdump captures to Moodle