Lab 09: IP addressing
OSL, Thu Mar 26, 2015

Objective:

1. Learn how *IP address configuration* is done in Linux.

General instructions:

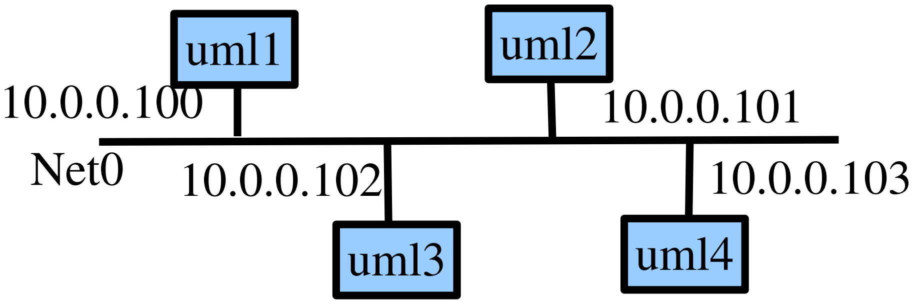
1. This lab is to be done in **groups of two students.**
2. Create a directory called <rollnumber1>_<rollnumber2>_lab09. As you proceed with the lab instructions below, note down observations or relevant output from whatever you do in a file named ”lab09.txt”.

Reference:

1. Sample VNUML configuration file (for reference)
2. Man pages of relevant commands

Lab Instructions:

Ms. Config is a mischievious network administrator and true to her name wants to misconfigure things and see what happens. However her networking background is weak. Help her understand the consequences of her mischief. The network topology under consideration is as under.



Exercise 1: IP address mis-configuration

Ms. Config decided to change the IP address of uml2 from 10.0.0.101 to 10.0.0.100. Basically she is duplicating addresses of two machines uml1 and uml2. She then wants to see what happens

1. When the two hosts with duplicate addresses contact other hosts at the same time
2. When other hosts contact a host with duplicate address at the same time

Guidance:

1. Create the simple topology as shown in the above figure using vnuml (name the file lab09-addr.xml). You can bring up the above virtual network using the command: “ vnumlparser.pl -Z -t lab09-addr.xml -v”. *In case you want to release the simulator for whatever reason, you can do so using the command “vnumlparser.pl -d lab08-addr.xml -v”.*

2. Ensure that all hosts belong to the same subnet by setting the mask of all the machines to 255.255.255.0.
3. Use “ifconfig” command to change the IP adress of uml2 from 10.0.0.101 to 10.0.0.100.
4. Also, **start any experimentation (each part below) with a clean slate**. Ensure that at all machines, there are no arp entries for any other hosts. Delete the entries if necessary using “arp” command.
5. To debug, you can run tcpdump on hosts in the background. Option '-e' can be useful here. Also check out the arp tables.

<u>Questions:</u>

Part-1: Pinging the same host from hosts with duplicate address

Ping uml3 from uml1 (use the -c option to limit the number of packets to 10). Now ping uml3 from uml2 (again use -c option to limit number of packets to 10). Start the second ping from uml2 only after some 4-5 ping packets got sent from uml1.

1. How many ping replies did uml1 and uml2 recieve? Explain all your observations in the lab report. (See how a connection can be hijacked?)

Part-2: Pinging different hosts from hosts with duplicate address

Ping uml3 from uml1 (use the -c option to limit the number of packets to 10). Now ping uml4 from uml2 (again use -c option to limit number of packets to 10). Start the second ping from uml2, only after some 4-5 ping packets got sent from uml1.

2. How many ping replies did uml1 and uml2 recieve? Explain all your observations in the lab report. Is there any difference from part-1?

Part-3: Pinging the duplicate IP address from different hosts

Ping 10.0.0.100 from uml3. After this ends, ping 10.0.0.100 from uml4. Use a small ping count like 3.

1. Explain crisply in the report what you observed in this case. In the first ping, which host replied to uml3? and in the second ping, which host replied to uml4? If uml2 is a malicious host, what does it need to do to capture the ping requests so that it can reply to them?

[Note: Some of the observations you made may not conform with theory. Different operating systems have slightly different implementations. E.g Linux ignores unsolicited replies, but acts on requests.]

Exercise 2: Sub-net mask mis-configuration

The network Ms. Config is managing has been allocated 10.0.0/24 prefix. Ms. Config playfully changed the IP address and subnet masks of the various machines as shown. The IP addresses are valid, but the masks she mis-configured.

uml1: 10.0.0.100   255.255.255.240

uml2: 10.0.0.101	255.255.255.0
uml3: 10.0.0.102	255.255.255.0
uml4: 10.0.0.120	255.255.255.240

And this has lead to weird connectivity problems when hosts with misconfigured netmasks ping others with correct net masks and vice versa. Help her understand why configuration of masks is as important as configuration of addresses.

Guidance:

1. Use ifconfig to configure the nodes according to what is specified. Note uml4 address has changed.
2. Much like before tcpdump, arp are your tools to debug

Questions:

Part-1: Pinging from hosts with incorrect address mask

From uml1 (which has incorrect address mask) ping uml2 (which has correct address mask). From uml4 (which has incorrect address mask) ping uml2 (which has correct address mask).

1. What are your observations and conclusions.

Part-2: Pinging to hosts with incorrect address mask

From uml2 which has correct address mask, ping uml1 and then uml4, both of which have incorrect mask.

1. What are your obervations and conclusions. Compare it with part-1 and highlight the differences.

Now you know the perils of misconfiguration!

After you are done playing with the simulator, do not forget to release it using the "-d" option.

Submission instructions

The directory named <rollnumber1>_<rollnumber2>_lab09 that you will submit should contain the following files:

1. lab09.txt
2. lab09-addr.xml

Tar gz the directory and submit the file <rollnumber1>_<rollnumber2>_lab09.tgz via moodle for grading.