PRACTICUM V MODULE

PING AND ROUTE

COMPETENCE:

- ❖ Students can use PING utility to detect connection problems in the network
- ❖ Students are able to understand the function of route tables.

TOOLS AND MATERIALS:

- Software Simulator GNS3
- Stable Internet Connection
- Connection to IT Department VPN Server

THEORY REVIEW:

1. PING (Packet Internet Gopher)

```
Sofyans-MBP:~ sofyanarief$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=3.609 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=5.912 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.727 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=3.589 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.589/4.209/5.912/0.984 ms
Sofyans-MBP:~ sofyanarief$
```

Figure 1. Examples of USING PING Utilities

It is a method of checking network connectivity based on Transmission Control Protocol /Internet Protocol (TCP/IP) technology from one host to another sending a packet. Packets delivered in PING activities are ICMP packets. The packet is sent from one host to another host to see the status of the reply. There are three types of reply messages in PING activities, including:

a. Reply

If the PING activity that we do to a host generates this reply message, then it can be concluded that connectivity can be formed from your host to your destination host and vice versa. Or it could be said that the package you send from your host can be received at the destination host and the destination host can send a reply package to your host. An example of connectivity checking output using PING (Reply) can be seen in Figure 1.

In the image above in addition to the status of the packet that was successfully delivered, there are several other parameters, including **time** that shows the time required by the packet when running on the network from the

source host to the destination host. The shorter **the time** displayed, the better the quality of connectivity between the source host and the destination host. But it is important to know that, better connection does not always depend on the faster speed or larger bandwidth, it could also be due to the density of data / traffic that is not too heavy on the network between the source host to the destination host. In addition, there is also **a packet loss** calculation, where **the packet loss** here shows the amount of packets lost / did not received by the destination in percentage.

b. Request Time Out

If the PING activity we do to a host generates this reply message, then it can be concluded that connectivity can be formed from your host to your destination host, but your destination host does not return the packet you sent. The cause could be that the destination host does not understand which path to use to send back the packet you sent because the router does not provide path information from your destination host to your host to your host. Or also your destination host is too busy serving other hosts in the network so that its network resources are no longer available to serve you.

If your PING activity generates this message, it's a good idea to double-check your router's configuration if you are certain that the destination host is not busy serving other network activities.

c. Destination Host Unreacheable

If the PING activity we do to a host generates this message, then it can be concluded that connectivity cannot be formed from your host to your destination host and vice versa. Or it could be said that the packets you send from your host are not received on the destination host and the destination host can not send a reply packet to your host. Let alone be accepted by the destination host, the sending host may not know the destination host. This can happen for several reasons, including no path information from the router that can be used to send packets from the source host to the destination host. It could also be because our destination host is not connected to the network. Or there may be a configuration in our source host that is incorrect (usually incorrectly entering the ip gateway which causes us to be unable to communicate between networks).

To use the **PING** utility, you can open your terminal (on linux) or command prompt (in windows) and type "ping<space>destination_hostname/address "

In addition, you can use some of the options available in the PING utility by opening the manual ("man ping" in the linux terminal or "ping /?" in the windows command prompt).

2. ROUTE

Route is a CLI command for displaying/manipulating routing. Usually route is used to define static routing to a host/network through a network interface. To display a list of routes that are already known a computer you can open the terminal and run the "route" command. Then it will look like the image below.

```
root@engine-deb:/home/engine# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         router.asus.com 0.0.0.0         UG    1024   0        0 eth0
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
```

Figure 2. Route List

In the image above it can be seen that the network with a range of 192.168.1.0 – 192.168.1.255, with a gateway that is * which means 0.0.0.0. The meaning of this route line is when a packet is destined to host whose address in those IP range, when the MAC address of its destination is found in the ARP protocol then the packet will be sent to the destination MAC address. And if the packet is sent to a destination outside that IP range, then the packet will be forwarded to the default gateway where it will determine the next routing for the packet.

In general, in the route table the host will be displayed in its hostname form only. To display ip address details in the route table, you can add the "-n" option behind the "route" command.

```
root@engine-deb:/home/engine# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    1024   0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Figure 3. IP details in route table

In the route table seen in figures 2 and 3, we can tell that our computer already has a default gateway. With the default gateway, our computer can communicate with hosts outside the IP range in the network 192.168.1.0/24. This can be checked by sending packets through the PING utility that we have learned previously to an address such **as detik.com**. A reply message will appear in the PING utility. This happens because packets from our computer are passed by the default gateway to **detik.com**. To be sure you can try to remove the default gateway by using the command "route del default gw <ip_gateway>". Then you look back at the route list, and try running PING ultility to send the package to **the detik.com**. Then the result will look like the image below.

```
root@engine-deb:/home/engine# route del default gw 192.168.1.1
root@engine-deb:/home/engine# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
root@engine-deb:/home/engine# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
root@engine-deb:/home/engine# ping detik.com
connect: Network is unreachable
```

Figure 4. Gateway Default Penghapusan Results

It can be seen from the image above that we can no longer connect to **the detik.com** because no one forwards packets from our computer to **the detik.com** where **the detik.com** is outside the ip range of the network 192.168.1.0/24. To restore it as before, we must add the default gateway in its route table using the "route add default gw <ip_gateway>" command. After we add we first make sure that the default gateway is already in the route table, and we try to send the packet back to **the detik.com** using the PING utility. Then it will look like the result as below screenshot shown.

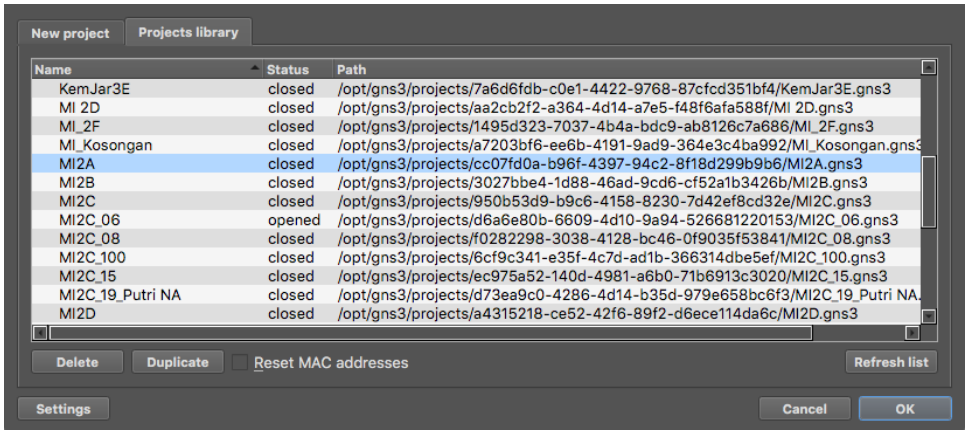
```
root@engine-deb:/home/engine# route add default gw 192.168.1.1
root@engine-deb:/home/engine# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         router.asus.com 0.0.0.0         UG    0      0        0 eth0
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
root@engine-deb:/home/engine# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
root@engine-deb:/home/engine# ping detik.com
PING detik.com (203.190.242.69) 56(84) bytes of data.
64 bytes from 203.190.242.69: icmp_seq=1 ttl=54 time=22.3 ms
64 bytes from 203.190.242.69: icmp_seq=1 ttl=53 time=22.3 ms (DUP!)
^C
--- detik.com ping statistics ---
1 packets transmitted, 1 received, +1 duplicates, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 22.317/22.329/22.341/0.012 ms
```

Figure 5. Gateway Default Reassembling Results

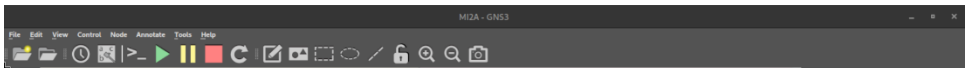
The use of **route** is not only limited to the example above, the use of **route** can also be used to block access to your computer from other computers. Whether the blocking is in one network, or different networks. And it can also apply to one computer or several computers in a range. To do so you can use the "route add –host <ip_address_host_tobeblocked> reject" command to block only 1 host, and use the "route add –net <network_address> netmask <its_netmask> reject" command to block a network with a certain IP range.

PRACTICUM PREPARATION

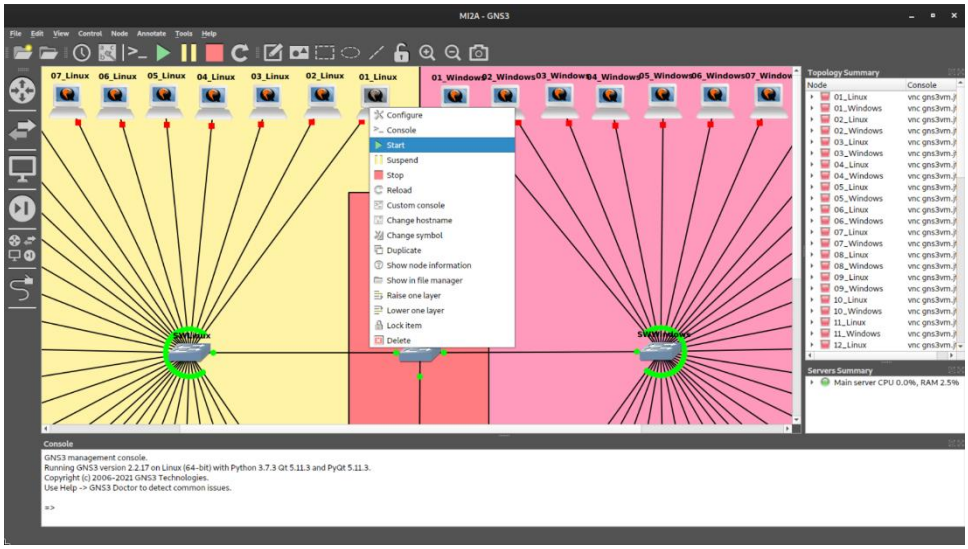
1. Connect your computer to the internet network.
2. Connect your computer to an Information Technology Department VPN server using the OpenVPN Connect app. Use the profile, username and password you have obtained at previous meetings.
3. Once connected to an OpenVPN server, open the GNS3 app on your computer.
4. In the initial view of the GNS3 application window, select the Project library tab. Then select the project that has been set up for your class (e.g. TI2I). Then remove the check mark on the Reset MAC Address option. Then press the OK button.



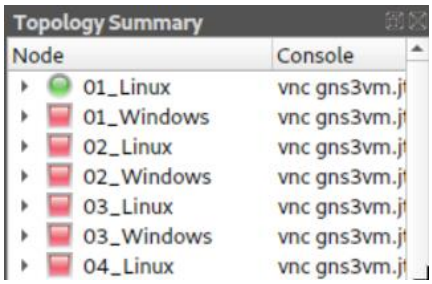
5. Then after the project opens in the main window of the GNS3 application, you can adjust the zoom on the appearance of the project as you wish by pressing the positive magnifying glass button (to enlarge) or the negatif magnifying glass button (to minimize) on the toolbar at the top of the window.



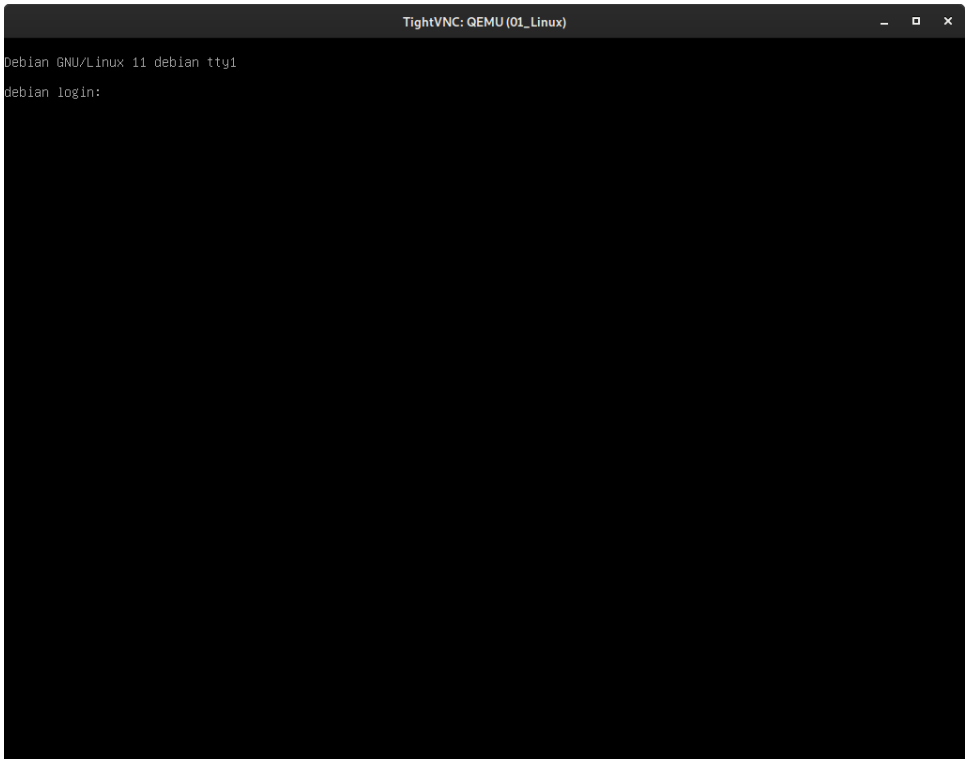
6. Then you can turn on the computer you are going to use. To do this, right-click on the logo of the computer you are going to use, and then select the Start option.



7. Wait a while and you can check the status of whether or not your computer is on in the Topology Summary sidebar to the right of the window.



8. Once your computer is on, access your computer by double-clicking (2x) on your computer logo. Then a new window will appear, which is the appearance of your computer as shown below.



9. You can use the computer for practicum according to the next steps.

PRACTICUM STEPS:

1. **PING (Packet Internet Gopher)**
   a. Open the terminal on your **linux**.
   b. Check your connectivity to the local network by sending **the ICMP Ping** packet to 10.10. 10. 1, stop the Ping utility manually after 5 packets are sent by pressing the Control+C button, observe the result.
   c. Check your connectivity to the internet network by sending **ICMP Ping** packets to **detik.com** as many as **10 packets**, and make the Ping utility **stop automatically** (use the correct parameter) after the 10 packets are delivered. Observe and conclude the results.
   d. Check your connectivity to the internet network by sending **ICMP Ping** packets to **kompas.com** as many as **5 packages** with a package delivery **delay time every 3 seconds**, and after that the ping tool will **stop automatically**. Observe the results.
   e. Check your connectivity to the internet network by sending **ICMP Ping** packets to **mikrotik.com** as many as **5 packages** with a packet **timeout of 0.3 seconds**, and after that the ping tool will **stop automatically**. Observe and conclude the results.
   f. For points c, d, and e please refer to the Ping utility manual to find out which options/parameters to add in the Ping command.

2. **ROUTE**
   a. Open the terminal on your **Linux** computer.
   b. Look at the route table of your computer.
   c. Remove the default gateway from your computer's route table.
   d. Look back at your route table and ping it to 192.168.60.142 and also to **detik.com**. Record (Screenshot) and analyze the results.
   e. Reconfigure to Add the default gateway on your computer's route table.
   f. Look back at your route table and ping it to 192.168.60.142 and also to **detik.com**. Record and analyze the results.
   g. Pair up with 3 of your friends.
   h. Try accessing your 1st friend's computer from your computer using the PING utility. Record and analyze the results.
   i. Ask your 1st friend to block access to his computer by adding it to the route table.
   j. Try to re-access your friend's 1st computer from your computer using the PING utility. Record the results.
   k. Try to ask your 2nd friend to access your 1st friend's computer from his computer using the PING utility. Record the results.
   l. Ask your 1st friend to remove the access blocking setting to his computer by deleting it in the route table.
   m. Try to re-access your friend's 1st computer from your computer using the PING utility. Record the results.
   n. Analyze the results you get from the step h to step m.
   o. Do step h to step m but switch your positions. If you were blocked by your friend before, now you block your friend. Do it until all the friends in your group do the step h to step m.
   p. Block your computer's access from the network with an IP range of 10.10.10.0/24.
   q. Ping from 2 other friends' computers, and record the results.

r. Compare and analyze the results of j-k points with the results obtained in step o.

ASSIGNMENT

1. Perform a practicum step and document each step in a report.