**LAB 16**

**ICMP: ping & tracert**

1. Start on your host Wireshark and start capturing on your (wireless) NIC.

Open the Windows command prompt and run the command below:

***ping -4 www.howest.be***

If you’re on Howest campus, use ***ping -4 nas.ti.howest.be*** instead if ping to the latter does not succeed. (Howest firewall is blocking some ICMP.)

Wait until the output of this command is stopped and then stop capturing.

1. Filter your capture so that you can only see the packets that were sent from the ping command from and to your wireless NIC.

Which filter do you use for this?

icmp

1. Click on an ICMP packet and fill in the table below to indicate how such a packet is built up.

Concretely: in the table, replace the question marks with protocol names and replace the question marks under the table by the size of the fields indicated.

|  |  |  |  |
| --- | --- | --- | --- |
| **Ethernet** HEADER | **IP** HEADER | **ICMP** HEADER | **ICMP** DATA |
| **14** bytes | **20** bytes | **8** bytes | **32** bytes |

1. What is the value of the Protocol field in the IP header to indicate that the IP payload is an ICMP packet?

Hexcode 01

1. What is the TTL value of the packets sent out by your host (i.e. the echo requests)?

128

Since your Windows PC is the transmitter of the echo requests, you can therefore deduce that this value is the initial value of the TTL field on a Windows PC.

1. What is the TTL value of the packets received by your host (i.e. the echo replies)?

63

Note that you can also find this value in the output of your ping command.

The device which you were pinging was a Linux server. Please refer to the link below to check the initial value of the TTL field of a Linux server and enter it below.

<http://subinsb.com/default-device-ttl-values>

Initial value TTL field for Linux = 64

You will notice that the TTL value of the echo replies is less than this initial value. From this you can deduce that the packets sent have passed a number of hops (routers) (because each hop reduces the TTL value by 1).

So how many routers are there between your laptop and the pinned server?

1 (64-63)

1. Use an legacy Windows command to track the (router) path followed by the ping packets between your laptop and www.howest.be.

tracert www.howest.be

Note that with this command you can also see how many routers are between your host and the web server.

It should also match your calculation of the deduction in TTL value (in the previous question) when you were pinging if you consider that the last line of tracert is the final destination which was sending an echo reply back to you.

1. Open the “Lab16 – Troubleshoot with ICMP” pka-file from Leho.

Note that we used the standard passwords: “cisco” for login and “class” for Privileged EXEC mode.

What is the IP address of PC3? Ping with IPv4 packets from PC1 to PC3.You'll notice there are no echo replies. This is because a wrong IP address configuration was deliberately introduced on one of the 3 routers.

The annotations about the networks that should be used on each LAN/WAN are correct, but there’s something wrong with one of the IP addresses. Solve this connectivity problem by correctly adjusting the IP address configuration of one of the routers.

(Note: the routing tables on the routers will not include all routes to the different networks, but that will automatically be fixed once you fix the IP address configuration because the routers are configured to dynamically update the routing tables.)

Hint: use a ***tracert*** command on PC1 to find out which router has the wrong configuration.

1. Save the modified pka file and upload it via Leho.