**LABO 16**

**PING & TRACERT**

1. Start op je host Wireshark op en start het capteren op je wireless NIC.

Open de Windows command prompt en voer onderstaand commando uit:

***ping -4 op-nas.howest.be***

*Opm: deze opdracht dien je wel op school uit te voeren*

Wacht tot de output van dit commando gestopt is en stop dan ook het capteren.

1. Filter je capture zodat je enkel nog de pakketten te zien krijgt die in opdracht van het ping-commando verstuurd werden vanaf en naar je wireless NIC.

Welke filter gebruik je hiervoor?

icmp

1. Klik op een ICMP-pakket en vul onderstaande tabel in om aan te duiden hoe zo’n pakket opgebouwd is.

Concreet: vervang in de tabel de vraagtekens door protocolnamen en vervang onder de tabel de vraagtekens door de grootte van de aangeduide velden.

|  |  |  |  |
| --- | --- | --- | --- |
| ????? HEADER | ???? HEADER | ???? HEADER | ???? DATA |

?? B ?? B ?? B ?? B

|  |  |  |  |
| --- | --- | --- | --- |
| ETHERNET HEADER | IP HEADER | ICMP HEADER | ICMP DATA |

14 B 20 B 8 B 32 B

1. Welke hexadecimale code wordt door het IP-protocol gebruikt om aan te duiden dat de IP-payload voor het ICMP-protocol bedoeld is?

In middelste window op Protocol: ICMP (1) klikken 🡪 overeenkomstige hexacode staat in onderste window aangeduid in blauw 🡪 hexacode = 01

1. Wat is de TTL-waarde van de door jouw host uitgestuurde pakketten (dus de echo requests)?

128

Aangezien jouw Windows-PC de zender is van de echo requests, kan je hieruit dus afleiden dat deze waarde de initiële waarde is van het TTL-veld bij een Windows-PC.

1. Wat is de TTL-waarde van de door jouw host ontvangen pakketten (dus de echo reply’s)?

63

Merk op dat je deze waarde ook in de output van je ping-commando kan vinden.

Raadpleeg onderstaande link om de initiële waarde van het TTL-veld van een Linux-server na te gaan en vul deze hieronder in.

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

Initiële waarde TTL-veld bij Linux = 64

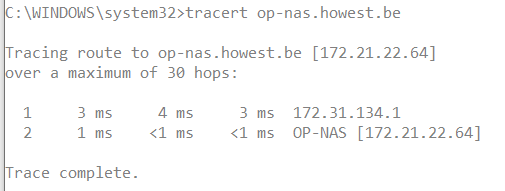
Je zal merken dat de TTL-waarde van de echo reply’s minder is dan deze initiële waarde. Hieruit kan je afleiden dat de verstuurde pakketten een aantal hops (routers) gepasseerd zijn (want elke hop doet de TTL-waarde met 1 verminderen).

Hoeveel routers bevinden er zich dus tussen je laptop en de gepingde server?

64 - 63 = 1

1. Maak van een een legacy Windows-commando gebruik om het (router)pad te traceren die door de ping-pakketten gevolgd worden tussen je laptop en de webserver met als naam op-nas.howest.be.

tracert op-nas.howest.be



Merk op dat je ook met dit commando kan zien hoeveel routers er tussen je host en de webserver zitten.

1. Op dezelfde manier kan je ook nagaan hoeveel routers er gepasseerd worden bij het surfen vanaf je host naar bv [www.facebook.com](http://www.facebook.com). Waarom kan je dit niet op school, maar wel thuis doen?

Firewall in Howest blokkeert ICMP-messages

1. Open de PKA-file uit <https://contenthub.netacad.com/itn/13.2.7>

Ping met IPv4-pakketten vanaf PC1 naar PC3. Je zal merken dat er geen echo reply’s terugkeren. Er werd immers met opzet een verkeerde IP-adresconfiguratie ingevoerd op één van de 3 routers.

Los dit connectiviteitsprobleem op door de IP-adresconfiguratie van één van de routers correct aan te passen.

Tip: maak gebruik van een tracert-commando op PC1 om na te gaan bij welke router de configuratie verkeerd is.

Tracert-commando blijft steken bij R1

* Configuratie op R2 is wellicht verkeerd
* Linkerinterface van R2 = S0/0/0 moet tot het netwerk 10.10.1.4 /30 behoren volgens de info op de figuur
* /30 betekent dat er maar 32-30 = 2 bits zijn voor de hosts 🡪 22 = 4 mogelijke adressen, zijde:
  + 10.10.1.4 = netwerkadres
  + 10.10.1.5 = eerste host
  + 10.10.1.6 = tweede host
  + 10.10.1.7 = broadcast

Aangezien de rechterinterface van R1 = S0/0/1 dat ook tot dit netwerk behoort al het adres 10.10.1.6 heeft en de linker interface van R2 als verkeerd IP-adres 10.10.1.9 heeft, moet dit IP-adres vervangen worden door 10.10.1.5

Commando’s op R2:

int s0/0/0  
ip addr 10.10.1.5 255.255.255.252

na deze aanpassing kan er gepingd worden vanaf PC1 naar PC3 met het commando ping 10.10.1.18

1. Bewaar de aangepaste Packet Tracer file onder de naam **familienaam-voornaam-lab16.pka** (waarbij je familienaam en voornaam door je eigen familienaam en voornaam vervangt) en upload deze via Leho.