Traceroute

Introduktion

Uppgiften utfördes för att lära sig om hur traceroute-kommandot i linux fungerar. Detta gjordes med två anrop till `traceroute` och ett till `script` för att kunna logga det som skrevs ut i terminalen till en fil.

```
script log.txt
traceroute www.google.com
sudo traceroute www.google.com
exit
```

Materiell

En Windowsinstallation av Oracle VM VirtualBox med ett linuxbaserat operativsystem, Ubuntu.

Analys

Körning 1

Log-filen (se under log.txt-sektionen, alternativt medföljande oändrade log.txt-fil) ger oss information om hur `traceroute` fungerar. Traceroute visar hur vår request till en viss hemsida eller ip-adress hoppar mellan olika routrar, samt hur lång tid varje hopp tar.

I och med att jag använde mig av en virituell maskin, ovanpå min windowsinstallation, så gav oss de första anropet inte särskilt mycket information, vi ser att den inte får något svar och slutar med anropet efter 30 försök. Detta beror på att windows brandvägg stoppar anrop av typen UDP som traceroute-anropen från linux maskinen använder när inget annat anges.

Då vi lägger till `-I` så säger vi åt traceroute att använda sig av ”Internet Control Message Protocol (ICMP) Echo request”. Anropet i detta fallet kommer igenom windows brandvägg då det använder samma protokoll (ICMP) som windowskommandot `ping` vilket brandväggen accepterar. Detta anrop ger mycket mer information än det första. Vi kan följa det utskickade paketet från virtuella maskinens gateway till min ”hemmarouter” som sen skickar vidare paketet till telia och till sist kommer fram till googles server. Det verkar som paketet gick igenom 9 olika routrar, om man inte räknar med mina enheter, 11 med mina.

Då det är lite svårt att jämföra dessa då en av körningarna är fast i packetlosslimbo, så utförde jag istället en ny körning med lite ändrade inställningar

Körning 2

Efter lite googling och letande i Virtualbox’s inställningar så fann jag att nätverksinställningarna som standard är i NAT-mode. NAT är något som används om man har många ipadresser upptagna på sitt nätverk, och tilldelas en lokal nätverksadress från VirtualBox som i sin tur kommunicerar via värddatorns ipadress för att använda internet. Trafiken verkar då komma från

värddatorn och inte den virituella maskinen enligt omvärlden. Detta bör förklara varför den första körningen blockerades av windows brandvägg, då trafiken körs igenom dennes.

Jag ändrade inställningarna från NAT till bridged mode. Detta ger det virituella operativsystemet en egen identitet på nätverket. En egen IP-adress samt möjligheten att kopplas till andra enheter på nätverket. Den anses av nätverket som en egen fristående fysisk enhet.

Med dessa inställningar ändrade körde jag om det första testet för att se om dessa ändrade på något. Se log2.txt, alternativt medföljande log2.txt-fil.

```
script log2.txt
traceroute www.google.com
sudo traceroute www.google.com
exit
```

Här får vi ett annat resultat. Då vår virituella maskin ses som en egen enhet så får den göra UDP-anrop och vi får ut hur det skickade paketet hoppar mellan olika routrar. Vi ser också i båda anropen att den istället för att börja vid _gateway, vilket är ubuntus lokala adress given av virtualbox alternativt värddatorn, börjar den direkt vid 192.168.1.1 vilket är hemmarouterns adress. Detta signalerar att det bridged mode fungerar. Efter detta gör båda anrop samma hopp, med undantaget steg 4 då denna visar asterisker och vi inte vet hur den hoppade där, fram till steg 7. Efter detta gör vår ICMP körning 1 extrahopp för att sedan båda hamnar på samma ställe. Båda de skickade paketen gick samma väg.

Om man jämför den första ICMP körningen med den senare så ser vi dock en avvikelse i var de båda slutar. Min första tanke var att detta berodde på att den första körningen var igår och den andra idag, men detta var inte korrekt, när jag bytte tillbaka till NAT så fick jag återigen samma slut.

```
arn11s11-in-f4.1e100.net
```

Detta är spekulation då jag inte hittade något svar genom googling, men jag tror detta har något att göra med vårat operativsystemi de båda fallen. När vi skickar paketet med NAT på så tror googles server att det kommer från en windowsdator, likaså när vi skickar paketet med bridged mode så ser google att det kommer från ett linuxbaserat system och väljer en server som är avsatt för dessa typer av operativsystem.

Log-filer:

log.txt

```
script log.txt
traceroute www.google.com
sudo traceroute www.google.com
exit

Script started on 2021-08-23 15:23:54+02:00 [TERM="xterm-256color" TTY="/dev/pts/0"
COLUMNS="88" LINES="33"]
 ]0;user@user-VirtualBox: ~  [01;32muser@user-VirtualBox [00m: [01;34m~
[00m$ traceroute goo  [K  [K  [Kwww.google.com
traceroute to www.google.com (142.250.74.132), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.588 ms  0.572 ms  0.625 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
(upprepas likadant mellan 2-30)
29  * * *
30  * * *
 ]0;user@user-VirtualBox: ~  [01;32muser@user-VirtualBox [00m: [01;34m~ [00m$ sudo
traceroute -I www.google.com
[sudo] password for user:
traceroute to www.google.com (142.250.74.132), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.528 ms  0.509 ms  0.505 ms
 2  192.168.1.1 (192.168.1.1)  1.626 ms  2.283 ms  2.256 ms
 3  gw1-no243.tbcn.telia.com (217.208.61.1)  10.768 ms  11.514 ms  11.494 ms
 4  vs-b-c2-link.se.telia.net (81.228.84.40)  14.593 ms  15.935 ms  15.998 ms
 5  * hy-c1-link.se.telia.net (81.228.82.80)  15.680 ms *
 6  fre-peer4-link.se.telia.net (81.228.91.179)  16.605 ms  12.404 ms  13.057 ms
 7  s-b5-link.ip.twelve99.net (62.115.123.166)  13.405 ms  12.003 ms  13.377 ms
 8  72.14.243.64 (72.14.243.64)  13.747 ms  13.717 ms  13.683 ms
 9  142.250.213.181 (142.250.213.181)  21.353 ms  22.747 ms  23.241 ms
10  142.251.48.43 (142.251.48.43)  23.218 ms  23.193 ms  23.169 ms
11  arn11s11-in-f4.1e100.net (142.250.74.132)  12.657 ms  13.057 ms  13.541 ms
 ]0;user@user-VirtualBox: ~  [01;32muser@user-VirtualBox [00m: [01;34m~ [00m$ exit
exit

Script done on 2021-08-23 15:25:09+02:00 [COMMAND_EXIT_CODE="0"
```

log2.txt

```
Script started on 2021-08-24 13:39:35+02:00 [TERM="xterm-256color" TTY="/dev/pts/0"
COLUMNS="79" LINES="29"]
]0;user@user-VirtualBox: ~[01;32muser@user-VirtualBox[00m:[01;34m~[00m$ traceroute
www.google.com
traceroute to www.google.com (216.58.211.4), 30 hops max, 60 byte packets
 1  OpenWrt.lan (192.168.1.1)  1.196 ms  1.177 ms  1.426 ms
 2  gw1-no243.tbcn.telia.com (217.208.61.1)  10.990 ms  11.560 ms  12.439 ms
 3  vs-b-c2-link.se.telia.net (81.228.84.40)  15.146 ms u-b-c2-link.se.telia.net
(81.228.84.34)  14.074 ms  14.976 ms
```

```
 4  * * *
 5  fre-peer4-link.se.telia.net (81.228.91.179)  18.390 ms fre-peer4-
link.se.telia.net (81.228.88.203)  18.884 ms fre-peer4-link.se.telia.net
(81.228.91.179)  19.350 ms
 6  s-b5-link.ip.twelve99.net (62.115.123.166)  18.800 ms  15.438 ms  15.577 ms
 7  72.14.243.64 (72.14.243.64)  16.559 ms  12.867 ms  12.373 ms
 8  * * *
 9  172.253.72.118 (172.253.72.118)  15.461 ms 209.85.242.10 (209.85.242.10)  12.551
ms muc03s13-in-f4.1e100.net (216.58.211.4)  13.532 ms
]0;user@user-VirtualBox: ~[01;32muser@user-VirtualBox[00m:[01;34m~[00m$ t[Ksudo
traceroute -I www.google.com
[sudo] password for user:
traceroute to www.google.com (216.58.211.4), 30 hops max, 60 byte packets
 1  OpenWrt.lan (192.168.1.1)  0.681 ms  1.996 ms  1.998 ms
 2  gw1-no243.tbcn.telia.com (217.208.61.1)  10.762 ms  11.645 ms  11.888 ms
 3  vs-b-c2-link.se.telia.net (81.228.84.40)  15.425 ms  15.719 ms  16.622 ms
 4  * * *
 5  fre-peer4-link.se.telia.net (81.228.91.179)  22.263 ms  22.265 ms  22.259 ms
 6  s-b5-link.ip.twelve99.net (62.115.123.166)  19.333 ms  17.592 ms  17.520 ms
 7  72.14.243.64 (72.14.243.64)  17.509 ms  13.373 ms  13.137 ms
 8  142.250.213.179 (142.250.213.179)  14.672 ms  13.847 ms  14.553 ms
 9  209.85.241.29 (209.85.241.29)  13.861 ms  13.769 ms  12.304 ms
10  muc03s13-in-f4.1e100.net (216.58.211.4)  12.099 ms  12.096 ms  13.000 ms
]0;user@user-VirtualBox: ~[01;32muser@user-VirtualBox[00m:[01;34m~[00m$ exit
exit


Script done on 2021-08-24 13:40:02+02:00 [COMMAND_EXIT_CODE="0"]
```

Källor

https://www.fortinet.com/resources/cyberglossary/traceroutes

- Förklaring av traceroute

https://www.howtogeek.com/howto/windows-vista/allow-pings-icmp-echo-request-through-your-windows-vista-firewall/

- Förklaring av ICMP

https://linux.die.net/man/8/traceroute

- Manual för traceroute

https://www.vmware.com/support/ws55/doc/ws_net_configurations_bridged.html

- Förklaring av bridged mode

https://www.vmware.com/support/ws3/doc/ws32_network21.html

- Förklaring av NAT