IT Technology

Networking

Assignment 14, The ARP table and ARP process and Broadcast

University College

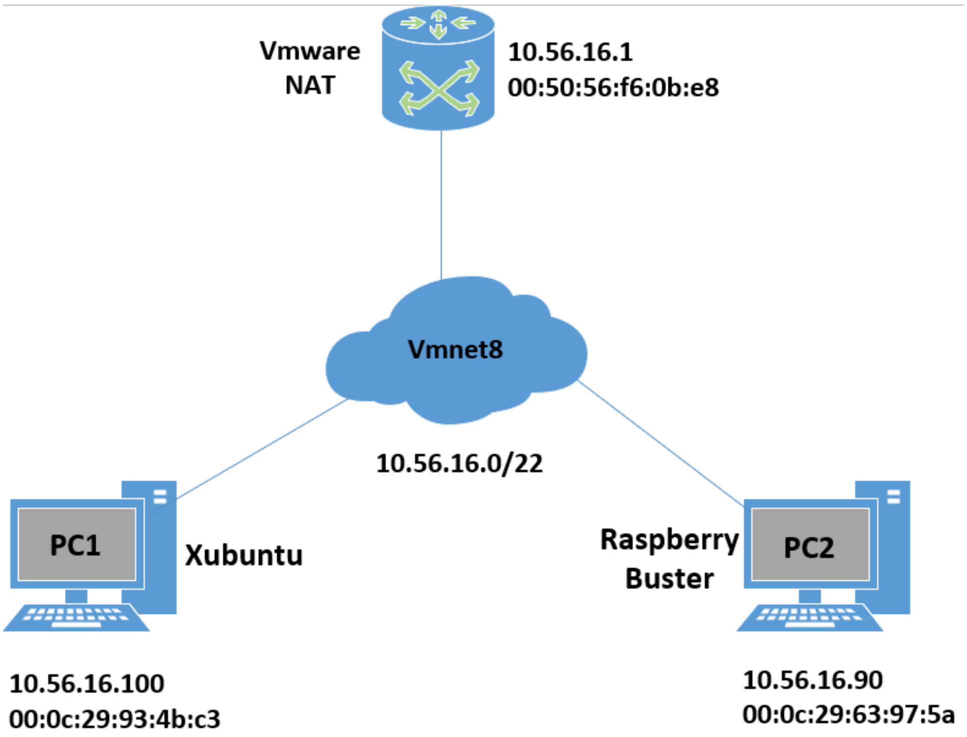
Author

Buterchi Bogdan

bdbu37436@edu.ucl.dk

ARP is a protocol and a program "silently" working "behind the scenes" on networking devices in ethernet networks. Its job is to fill the ARP table with pairs of IP and MAC addresses for the other networking devices. Knowledge about the ARP process and the ARP table can sometimes help pinpointing possible misbehaviour in a network and thus lead to a faster correction of misconfigurations.

1. A network diagram with IP addresses and MAC addresses for all devices on the 10.56.16.0/22 network.



2. Arptables on PC1 and PC2 with all neighbours in the broadcast area listed.

PC1:

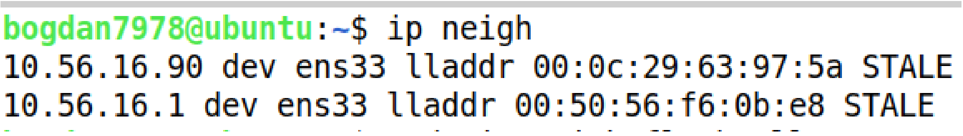
IP adress	MAC adress
10.56.16.90	00:0c:29:63:97:5a
10.56.16.1	00:50:56:f6:0b:e8

PC2:

IP adress	MAC adress
10.56.16.100	00:0c:29:93:4b:c3
10.56.16.1	00:50:56:f6:0b:e8

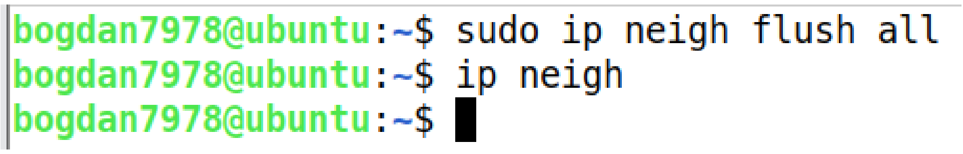
3. How to flush the ARP table.

We will use the command “sudo ip neigh flush all”. This will flush all the neighbours ip and mac adresses until you ping them again and create a new connection.



```
bogdan7978@ubuntu:~$ ip neigh
10.56.16.90 dev ens33 lladdr 00:0c:29:63:97:5a STALE
10.56.16.1 dev ens33 lladdr 00:50:56:f6:0b:e8 STALE
```

Here are all the devices connected to our PC

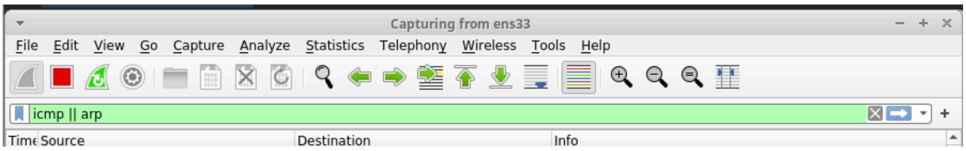


```
bogdan7978@ubuntu:~$ sudo ip neigh flush all
bogdan7978@ubuntu:~$ ip neigh
bogdan7978@ubuntu:~$ 
```

And now is empty.

4. Flush the PC1 ARP table and capture the ping from PC1 to PC2 with Wireshark.

Open Wireshark and type this filter in: “icmp || arp”

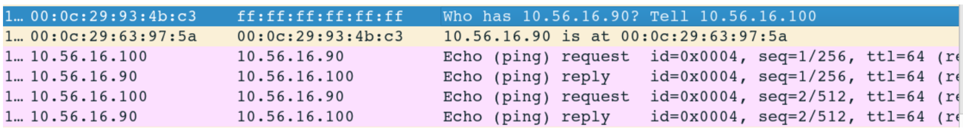


Capturing from ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Time Source Destination Info

```
icmp || arp
```

Open a new terminal and try the ping command

This will show up in the wireshark

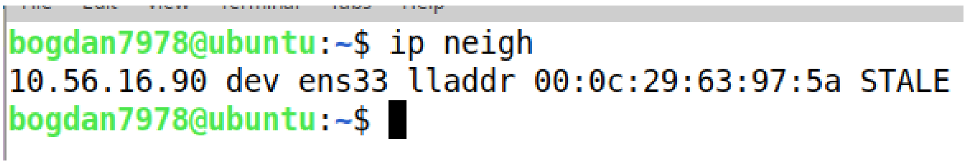


```
1… 00:0c:29:93:4b:c3   ff:ff:ff:ff:ff:ff   Who has 10.56.16.90? Tell 10.56.16.100
1… 00:0c:29:63:97:5a   00:0c:29:93:4b:c3   10.56.16.90 is at 00:0c:29:63:97:5a
1… 10.56.16.100        10.56.16.90         Echo (ping) request  id=0x0004, seq=1/256, ttl=64 (re
1… 10.56.16.90         10.56.16.100        Echo (ping) reply    id=0x0004, seq=1/256, ttl=64 (re
1… 10.56.16.100        10.56.16.90         Echo (ping) request  id=0x0004, seq=2/512, ttl=64 (re
1… 10.56.16.90         10.56.16.100        Echo (ping) reply    id=0x0004, seq=2/512, ttl=64 (re
```

Wireshark asking for the MAC adress for PC2. PC2 replying and then the ping request and reply.

5. Show that the PC1 ARP table has been populated. Comment on entries in the table.

Now if we type the “ip neigh” command we will see



```
bogdan7978@ubuntu:~$ ip neigh
10.56.16.90 dev ens33 lladdr 00:0c:29:63:97:5a STALE
bogdan7978@ubuntu:~$ 
```

6. ARP timeout is when an MAC adress is being flushed. If the adress is static it will be stored, but if it’s dynamic it will be discarded after. Also you can manually change an adress from dynamic to static

7. How ARP can be a security risk.

Nowdays there is very little chance that this will happen because almost 90% of web surfing is encrypted, BUT there is one technique called Man in The Middle where you can fool another computer that the MAC adress for the router, to communicate with the internet, is yours and you will receive the data.