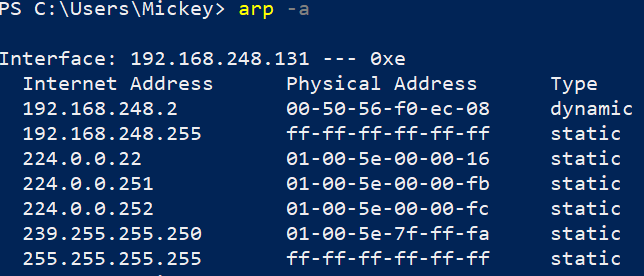
**LAB 12**

**Address Resolution Protocol ( ARP)**

1. Start both your Windows VM and your Linux VM.
2. On your Windows-VM, use the legacy ***arp*** command to retrieve the contents of the ARP cache table on your VM and paste below a screenshot of the output of your command. Use ***arp /?*** for information.

Arp -a



What 2 types of entries does this table contain? Find out what the difference between them is.

* Static: given by the OS
* Dynamic: learned by arp-requests or reply’s

Run that same command on your host. Why do you see more than 1 table here?

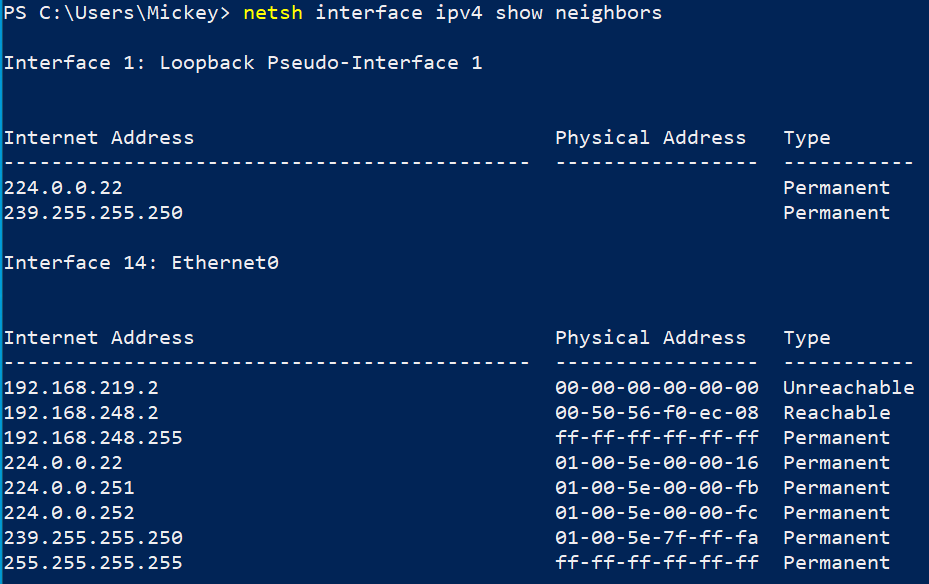
The arp command shows all tables. Since there are more NIC’s, both physical and virtual, the command shows more than one

1. Another legacy Windows command to retrieve information about the ARP cache table is the ***netsh*** command. Try to retrieve the ARP table of your Windows VM also using that command.

* Hint 1: Use the built-in help function via ***netsh /?*** to retrieve the ARP table of your Windows VM. You can use this built-in help recursively, e.g. ***netsh argument1 /?*** , ***netsh argument1 argument2 /?*** and so on
* Hint 2: ARP has to do with the IPv4 protocol.
* Hint 3: entries in the ARP table are sometimes called neighbors (because they contain MAC addresses of devices belonging to the same network as the interface)

Netsh interface ipv4 show neighbors

Paste below a screenshot of the output of your command.



1. There is also a 3rd way to get the contents of the ARP cache table in Windows, i.e. with the PowerShell cmdlet ***Get-NetNeighbor.*** Test this, too!
2. Ping from your Windows-VM to your Linux-VM and then request back the contents of the ARP cache table. Compare this with the cache table from the previous command. What do you see?

You can see that an entry was added to the list with the IP, MAC-address, the state and the PolicyStore

You can read the MAC address of your Linux-VM in the output of your command. Write down this MAC address below.

00-0C-29-EC-DA-1E

As a small recap question: what is the OUI of this MAC address? (See lecture slides about Ethernet if you’ve forgotten about that.) What manufacturer does it belong to? You can use <https://www.wireshark.org/tools/oui-lookup.html> .

00:0C:29 VMware, Inc

1. With the legacy Windows ***arp*** command, delete the contents of the ARP cache table and then request its contents. You will notice that there will soon be entries in that table again.

Arp -d

1. Ping from your Windows-VM (or from your host OS) to the computer with IP address 8.8.8.8 (or 172.21.1.111 on Howest campus, because Howest blocks outgoing pings) and then request the contents of the ARP cache table back.

Why isn't the IP address and corresponding MAC address of the server you’ve pinged in the ARP cache table? Look at the slides about ARP and communication in local versus remote networks, if you don’t know.

That is because the computer (or server) where the ICMP-packets are going to, is not in the same network.

1. Using the Linux command below, request the contents of the ARP cache table on your Linux-VM:

***ip neighbour show***

or shorter:

***ip n***

Note that the output looks a little different from Windows. In the output you see *lladdr*. What does this abbreviation stand for? You can use ***man ip-neighbour***

Link Layer Address

1. Delete the contents of the Ethernet-NIC ARP cache table on your Linux-VM using an ip command. You can use ***man ip-neighbour***

Ip neighbour flush all