Ministerul Educației și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Laboratory Work:
Use Wireshark to View Network Traffic

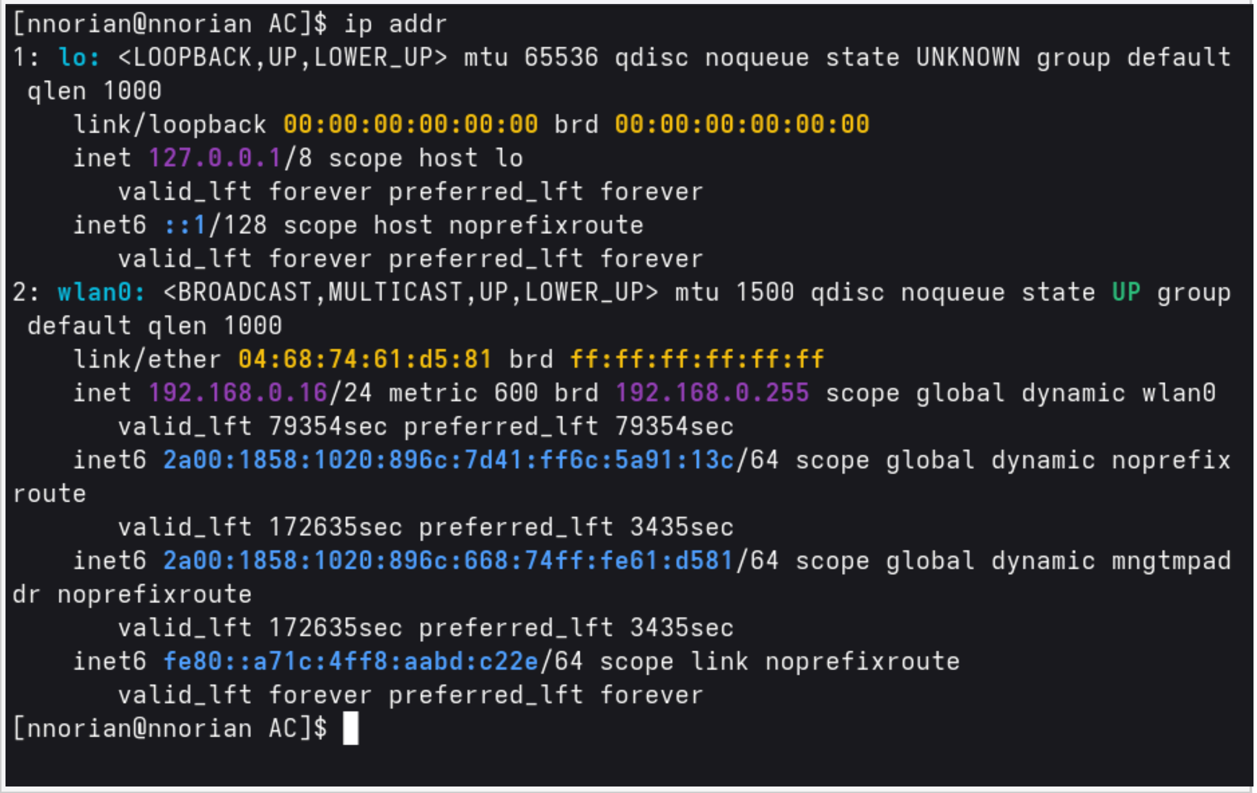
Elaborated:
st. gr. FAF-243 Kushnirenko Ecaterina

Verified:
asist. univ. Astafii Valentina

Chișinău – 2026

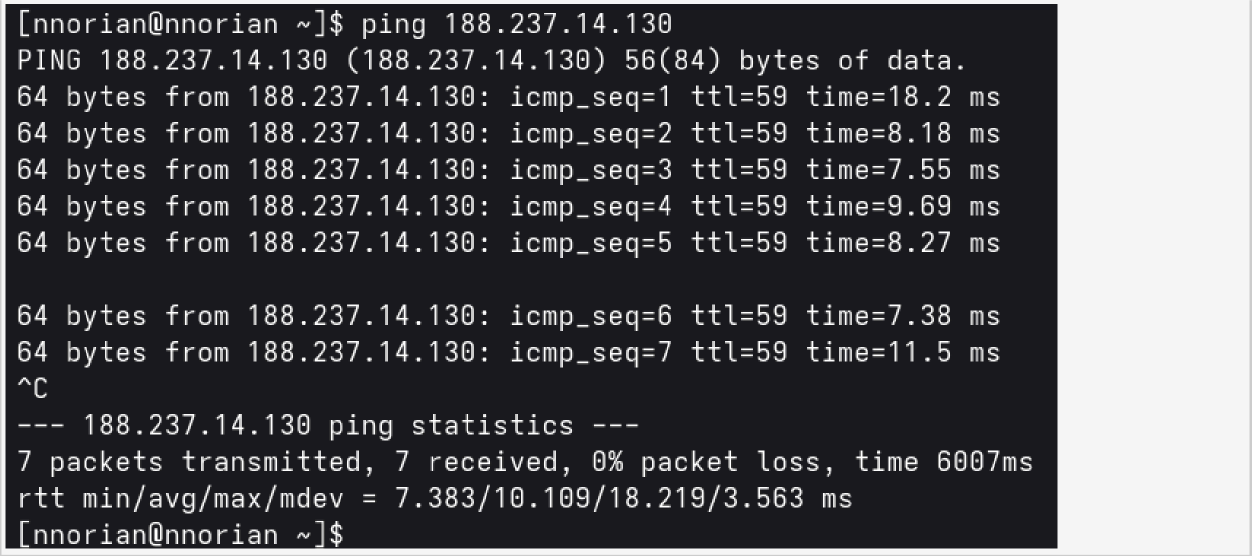
Part 1: Capture and Analyze Local ICMP Data

Step 1: PC Interface Addresses (ipconfig /all)



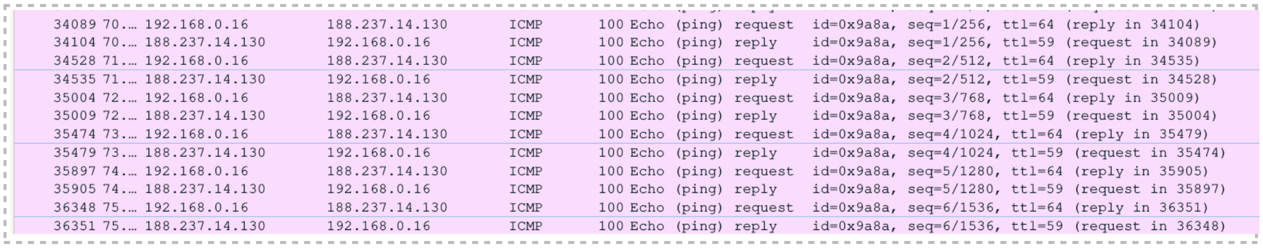
```
[nnorian@nnorian AC]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
 qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group
 default qlen 1000
    link/ether 04:68:74:61:d5:81 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.16/24 metric 600 brd 192.168.0.255 scope global dynamic wlan0
       valid_lft 79354sec preferred_lft 79354sec
    inet6 2a00:1858:1020:896c:7d41:ff6c:5a91:13c/64 scope global dynamic noprefix
route
       valid_lft 172635sec preferred_lft 3435sec
    inet6 2a00:1858:1020:896c:668:74ff:fe61:d581/64 scope global dynamic mngtmpad
dr noprefixroute
       valid_lft 172635sec preferred_lft 3435sec
    inet6 fe80::a71c:4ff8:aabd:c22e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[nnorian@nnorian AC]$ 
```

Step 2: Wireshark Capture (Local Ping)



```
[nnorian@nnorian ~]$ ping 188.237.14.130
PING 188.237.14.130 (188.237.14.130) 56(84) bytes of data.
64 bytes from 188.237.14.130: icmp_seq=1 ttl=59 time=18.2 ms
64 bytes from 188.237.14.130: icmp_seq=2 ttl=59 time=8.18 ms
64 bytes from 188.237.14.130: icmp_seq=3 ttl=59 time=7.55 ms
64 bytes from 188.237.14.130: icmp_seq=4 ttl=59 time=9.69 ms
64 bytes from 188.237.14.130: icmp_seq=5 ttl=59 time=8.27 ms

64 bytes from 188.237.14.130: icmp_seq=6 ttl=59 time=7.38 ms
64 bytes from 188.237.14.130: icmp_seq=7 ttl=59 time=11.5 ms
^C
--- 188.237.14.130 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6007ms
rtt min/avg/max/mdev = 7.383/10.109/18.219/3.563 ms
[nnorian@nnorian ~]$
```



```
34089 70.… 192.168.0.16      188.237.14.130    ICMP    100 Echo (ping) request  id=0x9a8a, seq=1/256, ttl=64 (reply in 34104)
34104 70.… 188.237.14.130    192.168.0.16      ICMP    100 Echo (ping) reply    id=0x9a8a, seq=1/256, ttl=59 (request in 34089)
34528 71.… 192.168.0.16      188.237.14.130    ICMP    100 Echo (ping) request  id=0x9a8a, seq=2/512, ttl=64 (reply in 34535)
34535 71.… 188.237.14.130    192.168.0.16      ICMP    100 Echo (ping) reply    id=0x9a8a, seq=2/512, ttl=59 (request in 34528)
35004 72.… 192.168.0.16      188.237.14.130    ICMP    100 Echo (ping) request  id=0x9a8a, seq=3/768, ttl=64 (reply in 35009)
35009 72.… 188.237.14.130    192.168.0.16      ICMP    100 Echo (ping) reply    id=0x9a8a, seq=3/768, ttl=59 (request in 35004)
35474 73.… 192.168.0.16      188.237.14.130    ICMP    100 Echo (ping) request  id=0x9a8a, seq=4/1024, ttl=64 (reply in 35479)
35479 73.… 188.237.14.130    192.168.0.16      ICMP    100 Echo (ping) reply    id=0x9a8a, seq=4/1024, ttl=59 (request in 35474)
35897 74.… 192.168.0.16      188.237.14.130    ICMP    100 Echo (ping) request  id=0x9a8a, seq=5/1280, ttl=64 (reply in 35905)
35905 74.… 188.237.14.130    192.168.0.16      ICMP    100 Echo (ping) reply    id=0x9a8a, seq=5/1280, ttl=59 (request in 35897)
36348 75.… 192.168.0.16      188.237.14.130    ICMP    100 Echo (ping) request  id=0x9a8a, seq=6/1536, ttl=64 (reply in 36351)
36351 75.… 188.237.14.130    192.168.0.16      ICMP    100 Echo (ping) reply    id=0x9a8a, seq=6/1536, ttl=59 (request in 36348)
```

Step 3: Analysis Questions

Q1: Does the source MAC address match your PC interface?

Yes, the source MAC address in Wireshark matches my PC's network interface MAC address (04:68:74:61:d5:81)

Q2: Does the destination MAC address in Wireshark match your team member’s MAC address?

Yes, when pinging a local PC, the destination MAC address shown in Wireshark matches the MAC address of the teammate's PC, because both devices are on the same LAN.

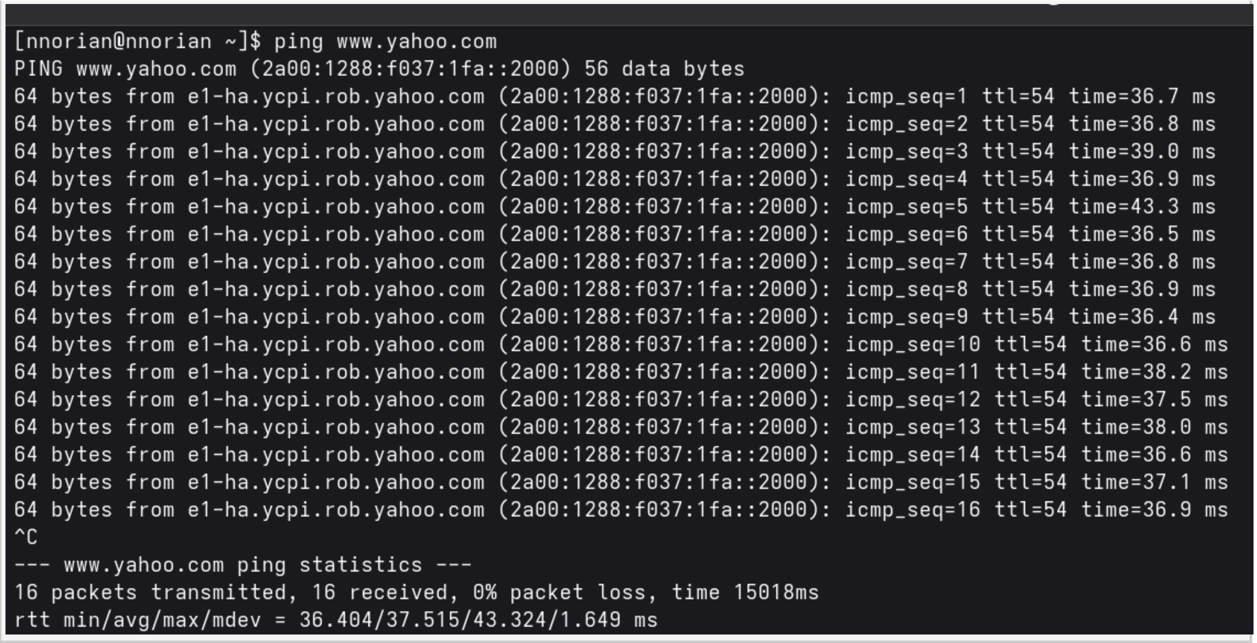
Q3: How is the MAC address of the pinged PC obtained by your PC?

The MAC address is obtained through ARP (. When my PC wants to send a packet to another device on the local network, it sends an ARP request asking "who has this IP address?" and the destination PC replies with its MAC address

Part 2: Capture and Analyze Remote ICMP Data

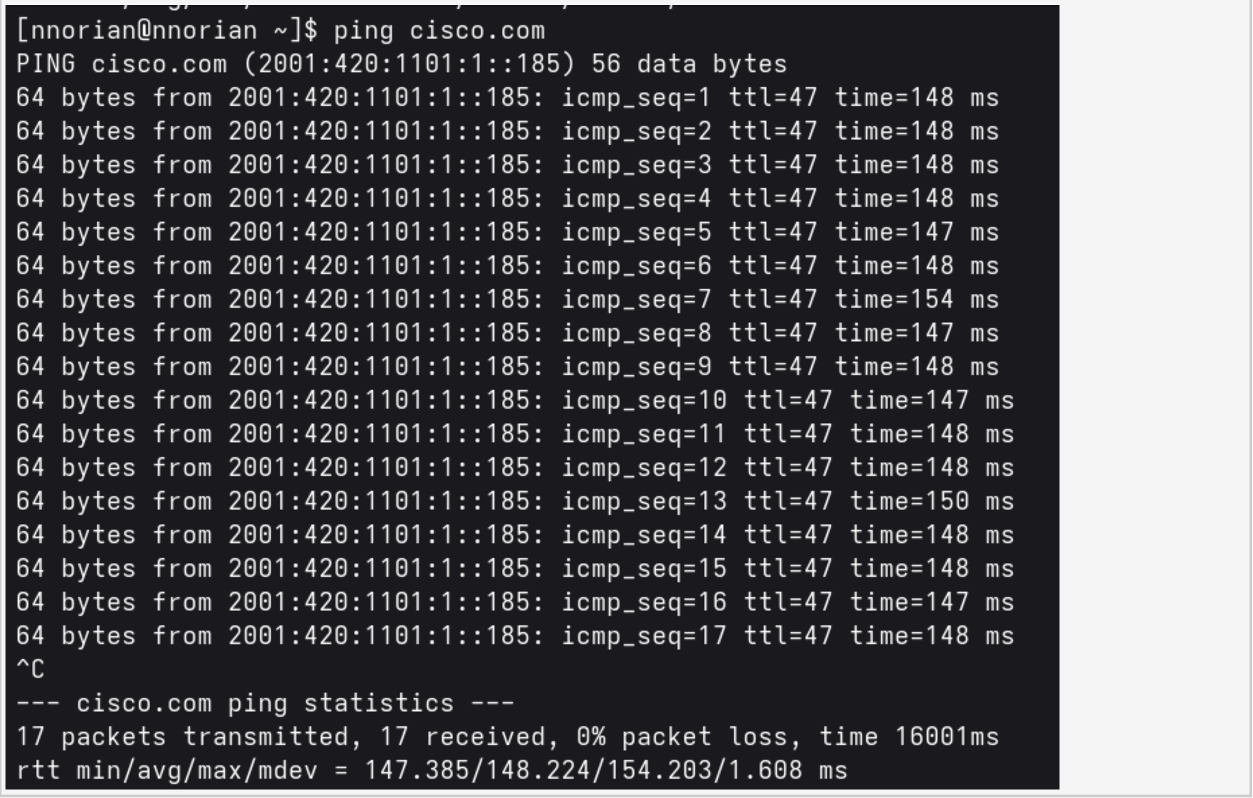
Step 1: Ping Remote Hosts

ping www.yahoo.com



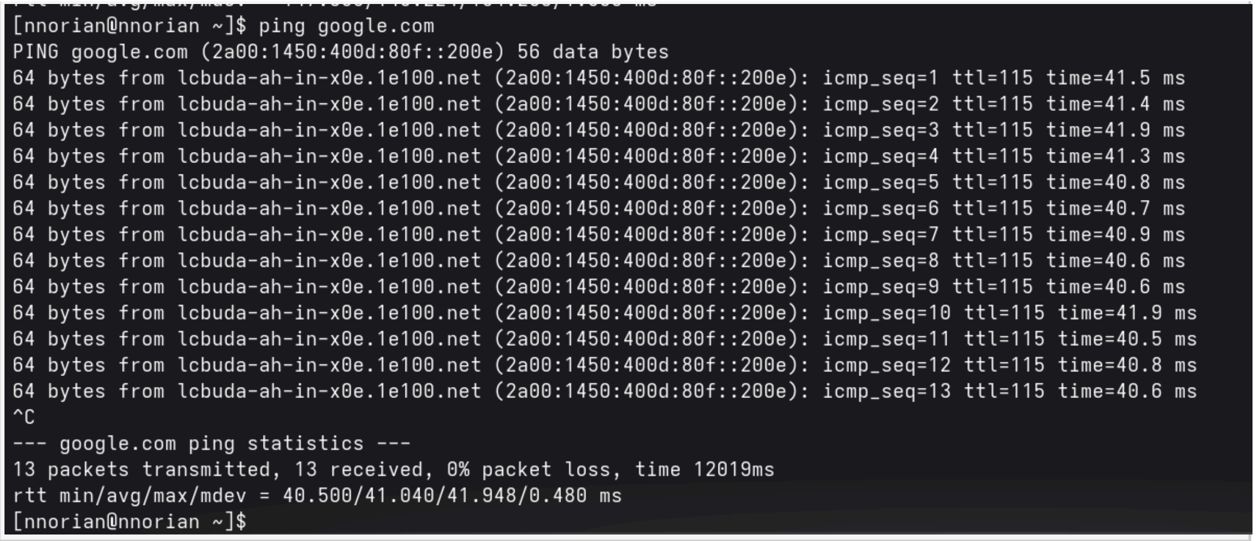
```
[nnorian@nnorian ~]$ ping www.yahoo.com
PING www.yahoo.com (2a00:1288:f037:1fa::2000) 56 data bytes
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=1 ttl=54 time=36.7 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=2 ttl=54 time=36.8 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=3 ttl=54 time=39.0 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=4 ttl=54 time=36.9 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=5 ttl=54 time=43.3 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=6 ttl=54 time=36.5 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=7 ttl=54 time=36.8 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=8 ttl=54 time=36.9 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=9 ttl=54 time=36.4 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=10 ttl=54 time=36.6 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=11 ttl=54 time=38.2 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=12 ttl=54 time=37.5 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=13 ttl=54 time=38.0 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=14 ttl=54 time=36.6 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=15 ttl=54 time=37.1 ms
64 bytes from e1-ha.ycpi.rob.yahoo.com (2a00:1288:f037:1fa::2000): icmp_seq=16 ttl=54 time=36.9 ms
^C
--- www.yahoo.com ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15018ms
rtt min/avg/max/mdev = 36.404/37.515/43.324/1.649 ms
```

ping www.cisco.com



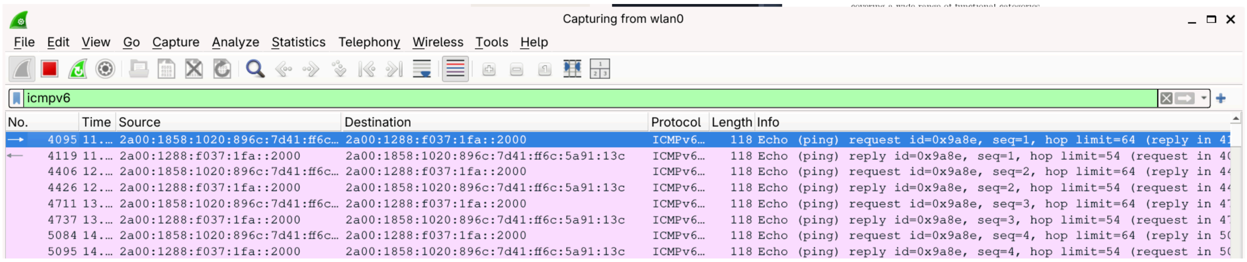
```
[nnorian@nnorian ~]$ ping cisco.com
PING cisco.com (2001:420:1101:1::185) 56 data bytes
64 bytes from 2001:420:1101:1::185: icmp_seq=1 ttl=47 time=148 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=2 ttl=47 time=148 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=3 ttl=47 time=148 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=4 ttl=47 time=148 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=5 ttl=47 time=147 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=6 ttl=47 time=148 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=7 ttl=47 time=154 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=8 ttl=47 time=147 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=9 ttl=47 time=148 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=10 ttl=47 time=147 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=11 ttl=47 time=148 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=12 ttl=47 time=148 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=13 ttl=47 time=150 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=14 ttl=47 time=148 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=15 ttl=47 time=148 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=16 ttl=47 time=147 ms
64 bytes from 2001:420:1101:1::185: icmp_seq=17 ttl=47 time=148 ms
^C
--- cisco.com ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16001ms
rtt min/avg/max/mdev = 147.385/148.224/154.203/1.608 ms
```

ping www.google.com



```
[nnorian@nnorian ~]$ ping google.com
PING google.com (2a00:1450:400d:80f::200e) 56 data bytes
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=1 ttl=115 time=41.5 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=2 ttl=115 time=41.4 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=3 ttl=115 time=41.9 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=4 ttl=115 time=41.3 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=5 ttl=115 time=40.8 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=6 ttl=115 time=40.7 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=7 ttl=115 time=40.9 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=8 ttl=115 time=40.6 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=9 ttl=115 time=40.6 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=10 ttl=115 time=41.9 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=11 ttl=115 time=40.5 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=12 ttl=115 time=40.8 ms
64 bytes from lcbuda-ah-in-x0e.1e100.net (2a00:1450:400d:80f::200e): icmp_seq=13 ttl=115 time=40.6 ms
^C
--- google.com ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12019ms
rtt min/avg/max/mdev = 40.500/41.040/41.948/0.480 ms
[nnorian@nnorian ~]$
```

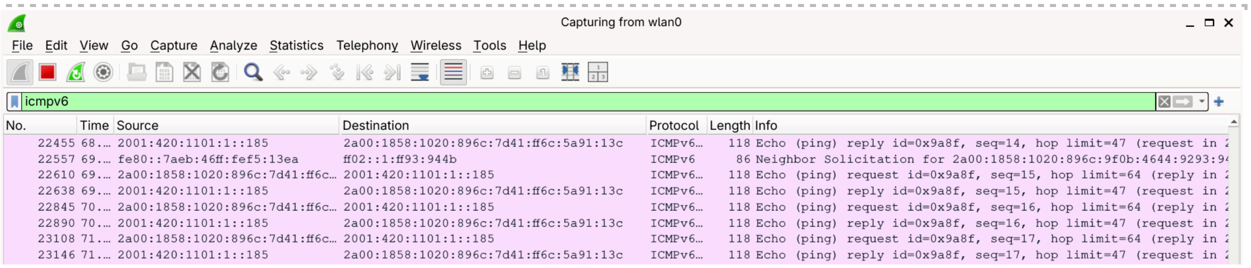
Step 2: Wireshark Screenshot (Remote Pings)



Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmpv6

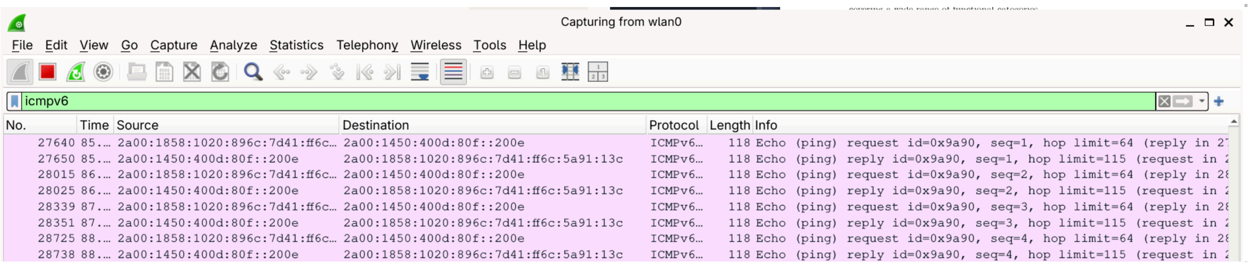
No.	Time	Source	Destination	Protocol	Length	Info
4095	11.…	2a00:1858:1020:896c:7d41:ff6c…	2a00:1288:f037:1fa::2000	ICMPv6…	118	Echo (ping) request id=0x9a8e, seq=1, hop limit=64 (reply in 41
4119	11.…	2a00:1288:f037:1fa::2000	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a8e, seq=1, hop limit=54 (request in 40
4406	12.…	2a00:1858:1020:896c:7d41:ff6c…	2a00:1288:f037:1fa::2000	ICMPv6…	118	Echo (ping) request id=0x9a8e, seq=2, hop limit=64 (reply in 44
4426	12.…	2a00:1288:f037:1fa::2000	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a8e, seq=2, hop limit=54 (request in 44
4711	13.…	2a00:1858:1020:896c:7d41:ff6c…	2a00:1288:f037:1fa::2000	ICMPv6…	118	Echo (ping) request id=0x9a8e, seq=3, hop limit=64 (reply in 47
4737	13.…	2a00:1288:f037:1fa::2000	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a8e, seq=3, hop limit=54 (request in 47
5084	14.…	2a00:1858:1020:896c:7d41:ff6c…	2a00:1288:f037:1fa::2000	ICMPv6…	118	Echo (ping) request id=0x9a8e, seq=4, hop limit=64 (reply in 50
5095	14.…	2a00:1288:f037:1fa::2000	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a8e, seq=4, hop limit=54 (request in 50



Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmpv6

No.	Time	Source	Destination	Protocol	Length	Info
22455	68.…	2001:420:1101:1::185	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a8f, seq=14, hop limit=47 (request in 2
22557	69.…	fe80::7aeb:46ff:fef5:13ea	ff02::1:ff93:944b	ICMPv6	86	Neighbor Solicitation for 2a00:1858:1020:896c:9f0b:4644:9293:94
22610	69.…	2a00:1858:1020:896c:7d41:ff6c…	2001:420:1101:1::185	ICMPv6…	118	Echo (ping) request id=0x9a8f, seq=15, hop limit=64 (reply in 2
22638	69.…	2001:420:1101:1::185	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a8f, seq=15, hop limit=47 (request in 2
22845	70.…	2a00:1858:1020:896c:7d41:ff6c…	2001:420:1101:1::185	ICMPv6…	118	Echo (ping) request id=0x9a8f, seq=16, hop limit=64 (reply in 2
22890	70.…	2001:420:1101:1::185	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a8f, seq=16, hop limit=47 (request in 2
23108	71.…	2a00:1858:1020:896c:7d41:ff6c…	2001:420:1101:1::185	ICMPv6…	118	Echo (ping) request id=0x9a8f, seq=17, hop limit=64 (reply in 2
23146	71.…	2001:420:1101:1::185	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a8f, seq=17, hop limit=47 (request in 2



Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmpv6

No.	Time	Source	Destination	Protocol	Length	Info
27640	85.…	2a00:1858:1020:896c:7d41:ff6c…	2a00:1450:400d:80f::200e	ICMPv6…	118	Echo (ping) request id=0x9a90, seq=1, hop limit=64 (reply in 27
27650	85.…	2a00:1450:400d:80f::200e	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a90, seq=1, hop limit=115 (request in 2
28015	86.…	2a00:1858:1020:896c:7d41:ff6c…	2a00:1450:400d:80f::200e	ICMPv6…	118	Echo (ping) request id=0x9a90, seq=2, hop limit=64 (reply in 28
28025	86.…	2a00:1450:400d:80f::200e	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a90, seq=2, hop limit=115 (request in 2
28339	87.…	2a00:1858:1020:896c:7d41:ff6c…	2a00:1450:400d:80f::200e	ICMPv6…	118	Echo (ping) request id=0x9a90, seq=3, hop limit=64 (reply in 28
28351	87.…	2a00:1450:400d:80f::200e	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a90, seq=3, hop limit=115 (request in 2
28725	88.…	2a00:1858:1020:896c:7d41:ff6c…	2a00:1450:400d:80f::200e	ICMPv6…	118	Echo (ping) request id=0x9a90, seq=4, hop limit=64 (reply in 28
28738	88.…	2a00:1450:400d:80f::200e	2a00:1858:1020:896c:7d41:ff6c:5a91:13c	ICMPv6…	118	Echo (ping) reply id=0x9a90, seq=4, hop limit=115 (request in 2

Step 3: Recorded IP and MAC Addresses

www.yahoo.com

IP Address: 2a00:1288:f037:1fa::2000

MAC Address: 78:eb:46:f5:13:ea

www.cisco.com
IP Address: 2001:420:1101:1::185
MAC Address: 78:eb:46:f5:13:ea

www.google.com
IP Address: 2a00:1450:400d:80f::200e
MAC Address: 78:eb:46:f5:13:ea

Step 4: Analysis Questions

Q4: What is significant about the destination MAC addresses for all three remote websites?

All three Yahoo, Cisco, and Google have the same destination MAC address (78:eb:46:f5:13:ea), even though they are completely different servers in different locations. This MAC address belongs to the default gateway router, not to the actual web servers.

Q5: How does this information differ from the local ping information you received in Part 1?

In Part 1, the destination MAC address was the actual MAC of the teammate's PC on the LAN. In Part 2, the destination MAC is always the router's MAC address regardless of which remote website we are pinging, because remote traffic has to go through the default gateway first.

Reflection

Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

MAC addresses only work within the local network. When we ping a local host, the frame goes directly to that device, so we see its real MAC. When we ping a remote host, our PC sends the frame to the default gateway router because the destination is on a different network. The router then re-encapsulates the packet with new MAC addresses for each hop along the way. That is why Wireshark only shows the router's MAC and not the remote server's MAC.

Conclusion

In this lab I learned how Wireshark captures and displays network traffic at different layers. I saw that ICMP ping packets are encapsulated inside IP packets, which are then placed inside Ethernet frames. The key takeaway is the difference between local and remote communication: on a LAN, frames are sent directly to the destination device using its real MAC address, but for remote hosts, frames are always sent to the default gateway router. This shows how Layer 2 (MAC) addressing is only relevant within the local network, while Layer 3 (IP) addressing is used for end-to-end delivery across networks.