

LAB-01 (Wireshark)

Ex. 1 | Network card

* Καταγράψτε το τρόπο με τον οποίο βρήκατε
Με `ipconfig /all` στο comand line εμφανίζει όλες τις
απαραίτητες πληροφορίες

1.1 | Network adapter name :

Intel(R) Wireless-AC 9462

1.2 | Είδος σύνδεσης :

Wireless / Wi-fi

* Στη περίπτωση του Ethernet Adapter δείχνει "Media Disconnected"

1.3 Ταχύτητα σύνδεσης (Mbps) :

Με την εντολή `wmic NIC` Μπορούμε να δούμε την ταχύτητα για το δοσμένο
wireless adapter

Στη περίπτωσή μας είναι 48 Mbps

ProductName	ServiceName	Speed
Microsoft Kernel Debug Network Adapter	kdnic	
Realtek PCIe GBE Family Controller	rt640x64	9223372036854775807
Intel(R) Wireless-AC 9462	Netwtw08	48000000
Microsoft Wi-Fi Direct Virtual Adapter	vwifimp	9223372036854775807
Microsoft Wi-Fi Direct Virtual Adapter	vwifimp	9223372036854775807
WAN Miniport (SSTP)	RasSstp	
WAN Miniport (IKEv2)	RasAgileVpn	
WAN Miniport (L2TP)	Rasl2tp	
WAN Miniport (PPTP)	PptpMiniport	
WAN Miniport (PPPOE)	RasPppoe	
WAN Miniport (IP)	NdisWan	
WAN Miniport (IPv6)	NdisWan	
WAN Miniport (Network Monitor)	NdisWan	
Bluetooth Device (Personal Area Network)		

1.4 | Subnet MAC Address :

7C-2A-31-40-C9-AF

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : ntua.gr
Description . . . . . : Intel(R) Wireless-AC 9462
Physical Address. . . . . : 7C-2A-31-40-C9-AF
DHCP Enabled. . . . . : Yes
```

1.5 | IPv4 Address :

147.102.238.40

1.6 | IPv6 Address :

2001:648:2000:e9:197:6309:6d7b:fba0

1.7 | DNS Server Address :

147.102.224.243 (IPv4) / 2001:648:2000:2000::1 (IPv6)

1.8 | Default Gateway :

147.102.236.200 (IPv4) / fe80::aec:f5ff:fed0:d91d%11 (IPv6)

DIRECTORY

Ex. 1 | Network card

Ex. 2 | Settings & Statistics

Ex. 3 | Wireshark

DICTIONARY

Subnet Mask / Μάσκα Υποδικτύου

Δηλώνει το μέρος της
IPv4 που αντιστοιχεί
στο υποδίκτυο

CIDR (Classless InterDomain Routing)

Prefix length / Μήκος προθέματος (/xx)

Ορίζει το μήκος σε bit
του μέρους της IPv4
που αντιστοιχεί στο
υποδίκτυο (ex.
147.102.0.0/16)

netstat (command)

lets you see the
network connections
that are active between
your system and any
other systems on your
network

TCP (Transmission Control Protocol)

IPv4 (Internet Protocol version 4)

MAC (Media Access Control)

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : ntua.gr
Description . . . . . : Intel(R) Wireless-AC 9462
Physical Address. . . . . : 7C-2A-31-40-C9-AF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:648:2000:e9:197:6309:6d7b:fba0(Preferred)
Temporary IPv6 Address. . . . . : 2001:648:2000:e9:b598:46ef:7c26:65f0(Preferred)
Link-local IPv6 Address . . . . . : fe80::197:6309:6d7b:fba0%11(Preferred)
IPv4 Address. . . . . : 147.102.238.40(Preferred)
Subnet Mask . . . . . : 255.255.252.0
Lease Obtained. . . . . : Πέμπτη, 14 Οκτωβρίου 2021 11:14:20
Lease Expires . . . . . : Πέμπτη, 14 Οκτωβρίου 2021 12:28:42
Default Gateway . . . . . : fe80::aec:f5ff:fed0:d91d%11
                          147.102.236.200
DHCP Server . . . . . : 1.1.1.1
DHCPv6 IAID . . . . . : 108800561
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-BF-78-C7-54-BF-64-1B-63-67
DNS Servers . . . . . : 2001:648:2000:2000::1
                          147.102.224.243
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
ntua.gr

```

NIC (Network Interface Controller)
Κάρτα δικτύου

Ex. 2 | Settings & Statistics

* Μαζί με την απάντηση να καταγράψετε την ακριβή σύνταξη της εντολής που χρησιμοποιήσατε

Με την εντολή `ipconfig /all` βρίσκουμε τις παρακάτω πληροφορίες που μας ζητούνται

2.1 | Όνομα υπολογιστή (Host name) :

Μέσω της `hostname` στο CLI των Windows βρίσκουμε το Host Name.
BELLOS-DELL-G3 / Windows OS

2.2 | Κάρτες δικτύου (physical / virtual) :

- * Ethernet (Physical) → Realtek PCIe GBE Family Controller
- * Wireless LAN 1 (Virtual) → Microsoft Wi-Fi Direct Virtual Adapter
- * Wireless LAN 2 (Virtual) → Microsoft Wi-Fi Direct Virtual Adapter #2
- * Wireless LAN Wi-Fi (Physical) → Intel(R) Wireless-AC 9462

2.3 | MAC Address :

Physical Address. : 7C-2A-31-40-C9-AF

Με την εντολή `wmic NIC` μπορούμε να δούμε την ταχύτητα για το δοσμένο wireless adapter

2.4 | Ταχύτητα σύνδεσης :

48 Mbps / 48000000 bps

2.5 | IPv4 Address :

IPv4 Address. : 147.102.238.40

2.6 | Subnet Mask :

255.255.252.0

i) Prefix Length :

22 bits (για δίκτυο με subnet mask 255.255.255.0 είναι 24)

* Όσο λιγότερα bits υπάρχουν στο subnet mask τόσο μικρότερο είναι και το prefix length

ii) Subnet Address :

147.102.236.0 (Εφαρμόζουμε τη μάσκα δικτύου πάνω στη διεύθυνση IPv4)

2.7 | IPv6 Address :

2001:648:2000:e9:197:6309:6d7b:fba0

2.8 | Default Gateway :

147.102.236.200 (IPv4) / fe80::aec:f5ff:fed0:d91d%11 (IPv6)

2.9 | DNS :

147.102.224.243 (IPv4) / 2001:648:2000:2000::1 (IPv6)

2.10 | DHCP :

DHCP Server : 1.1.1.1



Με την εντολή `netstat -e` μπορούμε να δούμε τα sent και received πλαίσια και bytes Ethernet της κάρτας δικτύου

2.11 | Αριθμός πλαισίων Ethernet & πλήθος byte που έστειλε και έλαβε η κάρτα δικτύου :

* Bytes 125844988 (Received), 374829526 (Sent)

* Unicast packets 3576680 (Received) 1898322 (Sent)

	Received	Sent
Bytes	125844988	374829526
Unicast packets	3576680	1898322
Non-unicast packets	8016	114488
Discards	0	0
Errors	0	0
Unknown protocols	0	0



Με την εντολή `netstat -e -s` κάτω από το **IPv4 Statistics** μπορούμε να δούμε τα sent και received πακέτα IPv4 της κάρτας δικτύου

2.12 | Αριθμός πακέτων IPv4 :

* Packets Received = 19155739

* Output Requests = 8721917



Με την εντολή `netstat -n` εμφανίζονται όλα τα Active Connections. Από αυτά επιλέγουμε και μετράμε μόνο εκείνα που έχουν State **'Established'** και Local Address διαφορετική του **127.0.0.1**

2.13 | Established TCP connections :

17 Established connections (6 IPv4, 11 IPv6)

2.14 | Θύρες πηγής (source) και προορισμού (destination) :

* 1) 60671 (Source), https (destination)

* 2) 62528 (Source). 5228 (destination)

Ex. 3 | Wireshark

3.1 | Πρωτόκολλα για `edu-dy.cn.ntua.gr`

* TCP

* HTTP

3.2 | MAC Address

Address: IntelCor_40:c9:af (7c:2a:31:40:c9:af)



Στο μέρος των λεπτομεριών :
Ethernet II > Source > Address

3.3 | Κατασκευαστής κάρτας δικτύου

Intel



Τα τρία πρώτα bytes που αναγράφονται στη MAC Address

3.4 | IPv4 Address

Source Address: 192.168.1.8



Στο μέρος των λεπτομεριών :
Internet Protocol version 4 > Source Address

3.5 | Destination Address

Destination Address: 147.102.40.15



Στο μέρος των λεπτομεριών :
Internet Protocol version 4 > Destination Address

3.6 | Φίλτρο μετά από Follow → TCP Stream

tcp.stream eq 19

3.7 |

i) Τύπος εξυπηρετητή (web server) : Apache/2.2.22

ii) HTML Title Tag : <title>DY2021 CN Lab</title>

iii) Πάνω, στο label του παραθύρου

3.8 | HTTP messages

ip.addr==147.102.40.15 and http

3.9 | Received / Sent (HTTP)

* 2 Received (147.102.40.15 → 192.168.1.8)

* 2 Sent (192.168.1.8 → 147.102.40.15)

3.10 | Time until response (HTTP)

0.039425 sec

3.11 | Packets needed

[Segment count: 8] → 8 πακέτα

3.12 | Image response time

i) First response / Service Time :

first TCP Packet - HTTP GET (favicon) = 23.921490 - 23.888873 = 0.032617 sec

ii) Response spread :

last TCP Packet - first TCP Packet = 23.924674 - 23.921490 = 0.003184 sec

iii) GET to response / Application Response Time :

i) + ii) = 0.032617 + 0.003184 = 0.035801 sec

3.13 | TRANSUM RTE Data

[Service Time: 0.032617000 seconds] = 0.032617

[Rsp Spread: 0.003184000 seconds] = 0.003184

[APDU Rsp Time: 0.035801000 seconds] = 0.035801

3.14 | HTTP && Source filter

```
ip.src==192.168.1.8 and http
```