Εργαστηριακή Άσκηση 1 Αναλυτής Πρωτοκόλλων Wireshark

Θοδωρής Φρίξος Παπαρρηγόπουλος
el18040
17/10/2021
Ομάδα 4η.
Ipv6: 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a
MAC: 40-1C-83-38-F7-20
Λειτουργικό: Windows
DESKTOP-1403ER3

Άσκηση 1

Στα Settings του δικτύου λαμβάνουμε τα εξής:
SSID: COSMOTE-767182
Protocol: Wi-Fi 5 (802.11ac)
Security type: WPA2-Personal
Network band: 5 GHz
Network channel: 100
Link speed (Receive/Transmit): 234/195 (Mbps)
IPv6 address: 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a
Link-local IPv6 address: fe80::34b0:9e4a:d912:2f8a%2
IPv6 DNS servers: fe80::1%2
IPv4 address: 192.168.1.8
IPv4 DNS servers: 192.168.1.1
192.168.1.1
Manufacturer: Intel Corporation
Description: Intel(R) Wi-Fi 6 AX201 160MHz
Driver version: 22.10.0.7
Physical address (MAC): 40-1C-83-38-F7-20

1.1)
Manufacturer: Intel Corporation
Description: Intel(R) Wi-Fi 6 AX201 160MHz

1.2) Protocol: Wi-Fi 5 (802.11ac)

1.3) Link speed (Receive/Transmit): 234/195 (Mbps)

1.4) Physical address (MAC): 40-1C-83-38-F7-20

1.5) IPv4 address: 192.168.1.8

1.6) IPv6 address: 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a

1.7) IPv6 DNS servers: fe80::1%2

1.8) >netstat -r
Gateway Route: 192.168.1.1

Άσκηση 2

2.1)
>hostname
DESKTOP-1403ER3

2.2)
>ipconfig /all

Windows IP Configuration
Host Name . . . . . : DESKTOP-1403ER3
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : home

Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 40-1C-83-38-F7-21
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 42-1C-83-38-F7-20
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : home
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : 40-1C-83-38-F7-20
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a(Preferred)
Temporary IPv6 Address. . . . . : 2a02:587:4f0e:2b65:99c1:30e9:aa17:b175(Preferred)
Link-local IPv6 Address . . . . . : fe80::34b0:9e4a:d912:2f8a%2(Preferred)
IPv4 Address. . . . . : 192.168.1.8(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, October 15, 2021 5:53:31 PM
Lease Expires . . . . . : Saturday, October 16, 2021 5:58:42 PM
Default Gateway . . . . . : fe80::1%2
192.168.1.1

DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 37756035
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-7D-E1-FF-00-00-10-00-B4-66
DNS Servers . . . . . : fe80::1%2
192.168.1.1
192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 40-1C-83-38-F7-24
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

2.3) Τρέχοντας το >ipconfig /all , και κοιτώντας το

Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : home
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : 40-1C-83-38-F7-20
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a(Preferred)
Temporary IPv6 Address. . . . . : 2a02:587:4f0e:2b65:2d6b:4393:74e8:4dec(Preferred)
Link-local IPv6 Address . . . . . : fe80::34b0:9e4a:d912:2f8a%2(Preferred)
IPv4 Address. . . . . : 192.168.1.8(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, October 17, 2021 11:54:06 AM
Lease Expires . . . . . : Monday, October 18, 2021 11:56:59 AM
Default Gateway . . . . . : fe80::1%2
192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 37756035
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-7D-E1-FF-00-00-10-00-B4-66
DNS Servers . . . . . : fe80::1%2
192.168.1.1
192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

Άρα MAC Address: 40-1C-83-38-F7-20

2.4) >netsh wlan show interfaces
There is 1 interface on the system:
Name : Wi-Fi
Description : Intel(R) Wi-Fi 6 AX201 160MHz
GUID : 065e544f-fe2e-44b1-a3c5-53895f3e5671
Physical address : 40:1c:83:38:f7:20

State : connected
SSID : COSMOTE-767182
BSSID : 38:02:de:f8:09:ab
Network type : Infrastructure
Radio type : 802.11ac
Authentication : WPA2-Personal
Cipher : CCMP
Connection mode : Auto Connect
Channel : 100
Receive rate (Mbps) : 351
Transmit rate (Mbps) : 130
Signal : 43%
Profile : COSMOTE-767182
Hosted network status : Not available

2.5)

2.6) >ipconfig /release6 και κρατάμε
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : home
IPv6 Address. . . . . : 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a
Temporary IPv6 Address. . . . . : 2a02:587:4f0e:2b65:99c1:30e9:aa17:b175
Link-local IPv6 Address . . . . . : fe80::34b0:9e4a:d912:2f8a%2
IPv4 Address. . . . . : 192.168.1.8
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1%2
192.168.1.1

Επίσης γνωρίζουμε ότι,
i) Το μέγεθος του τμήματος δικτύου της διεύθυνσης IP του υπολογιστή μου είναι 8 bit
ii) η διεύθυνση του υποδικτύου είναι 24 bit.

2.7) >ipconfig /release6 και κρατάμε

Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : home
IPv6 Address. . . . . : 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a
Temporary IPv6 Address. . . . . : 2a02:587:4f0e:2b65:99c1:30e9:aa17:b175
Link-local IPv6 Address . . . . . : fe80::34b0:9e4a:d912:2f8a%2
IPv4 Address. . . . . : 192.168.1.8
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1%2
192.168.1.1

2.8) >netstat -r

Gateway Route: 192.168.1.1

2.9) >ipconfig /all

DNS Servers . . . . . : fe80::1%2
192.168.1.1
192.168.1.1

2.10) >ipcnfoig /all
DHCP Server . . . . . : 192.168.1.1

2.11)
>netstat -e
Interface Statistics

	Received	Sent
Bytes	3452447188	305062212
Unicast packets	10330962	16114944
Non-unicast packets	5190	266682
Discards	0	0
Errors	0	0
Unknown protocols	0	

2.12)
>netstat -s
IPv4 Statistics
Packets Received = 1062144
Received Header Errors = 10
Received Address Errors = 14
Datagrams Forwarded = 0
Unknown Protocols Received = 11171
Received Packets Discarded = 2877
Received Packets Delivered = 1151053
Output Requests = 729228
Routing Discards = 0
Discarded Output Packets = 30539
Output Packet No Route = 97
Reassembly Required = 0
Reassembly Successful = 0
Reassembly Failures = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created = 0

2.13)
Αρχικά έγραψα netstat -a για να δώ αναλυτικά όλα τα TCP/UDP connections, μετά έτρεξα με το | findstr "ESTABLISHED" για να μου βρεί όσα είναι εκγατεστημένα, και τέλος για να μετρήσω το αποτέλεσματα έβαλα το | find /c /v ""

>netstat -an | findstr "ESTABLISHED" | find /c /v ""
36

2.14)
>netstat -an | findstr "ESTABLISHED" βρήκα 2 συνδέσεις TCP:

```
TCP    [2a02:587:4f0e:2b65:99c1:30e9:aa17:b175]:49671  [2a03:2880:f0ff:e:face:b00c:0:2]:443  ESTABLISHED
TCP    [2a02:587:4f0e:2b65:99c1:30e9:aa17:b175]:49672  [2a03:2880:f0ff:8:face:b00c:0:2825]:443  ESTABLISHED
```

Άσκηση 3

3.1)
Τα πρωτόκολα που εμφανίζονται είναι: UDP, TCP, DNS, QUIC, APR, HTTP, TLSv1.2, ICMPv6, SSDP.

3.2)

```
Ethernet II, Src: Sercomm_f8:09:a0 (38:02:de:f8:09:a0), Dst: IntelCor_38:f7:20 (40:1c:83:38:f7:20)
    Destination: IntelCor_38:f7:20 (40:1c:83:38:f7:20)
        Address: IntelCor_38:f7:20 (40:1c:83:38:f7:20)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Sercomm_f8:09:a0 (38:02:de:f8:09:a0)
    Type: IPv4 (0x0800)
```

```
1 0.000000 Sercomm_f8:09:a0 IntelCor_38:f7:20 ARP 42 Who has 192.168.1.8? Tell 192.168.1.1
2 0.000024 IntelCor_38:f7:20 Sercomm_f8:09:a0 ARP 42 192.168.1.8 is at 40:1c:83:38:f7:20
```

Από το GET Request βλέπουμε πως η MAC addr είναι: 40:1c:83:38:f7:20

3.3) Αναγράφει πως το source (δηλαδή η MAC addr μου) είναι από την IntelCor, συνεπώς η Intel.

ip.addr == 147.102.40.15

No.	Time	Source	Destination	Protocol	Length	Info
22	0.694523	192.168.1.8	147.102.40.15	TCP	66	51717 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
23	0.694551	192.168.1.8	147.102.40.15	TCP	66	60477 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
24	0.703798	147.102.40.15	192.168.1.8	TCP	66	80 → 51717 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS=64 SACK_PERM=1
25	0.703798	147.102.40.15	192.168.1.8	TCP	66	80 → 60477 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS=64 SACK_PERM=1
26	0.703963	192.168.1.8	147.102.40.15	TCP	54	51717 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
27	0.704039	192.168.1.8	147.102.40.15	TCP	54	60477 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
28	0.704402	192.168.1.8	147.102.40.15	TCP	590	60477 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=536 [TCP segment of a reassembled PDU]
29	0.704402	192.168.1.8	147.102.40.15	HTTP	80	GET / HTTP/1.1
30	0.713690	147.102.40.15	192.168.1.8	TCP	60	80 → 60477 [ACK] Seq=1 Ack=563 Win=65344 Len=0
31	0.715193	147.102.40.15	192.168.1.8	HTTP	287	HTTP/1.1 304 Not Modified
37	0.770421	192.168.1.8	147.102.40.15	TCP	54	60477 → 80 [ACK] Seq=563 Ack=234 Win=131072 Len=0
45	1.043127	192.168.1.8	147.102.40.15	HTTP	487	GET /favicon.ico HTTP/1.1
46	1.053944	147.102.40.15	192.168.1.8	TCP	2734	80 → 60477 [ACK] Seq=234 Ack=996 Win=65920 Len=2680 [TCP segment of a reassembled PDU]
47	1.054022	192.168.1.8	147.102.40.15	TCP	54	60477 → 80 [ACK] Seq=996 Ack=2914 Win=131072 Len=0
48	1.054086	147.102.40.15	192.168.1.8	TCP	1126	80 → 60477 [ACK] Seq=2914 Ack=996 Win=65920 Len=1072 [TCP segment of a reassembled PDU]
49	1.054115	192.168.1.8	147.102.40.15	TCP	54	60477 → 80 [ACK] Seq=996 Ack=3986 Win=131072 Len=0
50	1.054140	147.102.40.15	192.168.1.8	HTTP	281	HTTP/1.1 200 OK (image/x-icon)
51	1.054151	192.168.1.8	147.102.40.15	TCP	54	60477 → 80 [ACK] Seq=996 Ack=4213 Win=131072 Len=0

3.4) Η IPv4 του υπολογιστή μου είναι: 192.168.1.8

3.5) Η Ipv4 του σιτε είναι: 147.102.40.15

3.6) tcp.stream eq 1

3.7)

```
Accept-Encoding: gzip, deflate
Accept-Language: el-GR,el;q=0.9,en;q=0.8
If-None-Match: "172914-73-5cddd92af9400"
If-Modified-Since: Fri, 08 Oct 2021 20:53:36 GMT

HTTP/1.1 304 Not Modified
Date: Sun, 17 Oct 2021 13:29:34 GMT
Server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "172914-73-5cddd92af9400"

GET /favicon.ico HTTP/1.1
Host: edu-dy.cn.ntua.gr
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/94.0.4606.81 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://edu-dy.cn.ntua.gr/
Accept-Encoding: gzip, deflate
Accept-Language: el-GR,el;q=0.9,en;q=0.8
```

i) Server: Apache/2.2.22 (FreeBSD)
ii) <head><title>DY2021 CN Lab</title></head>
iii) Αποτελεί το όνομα της καρτέλας στον browser

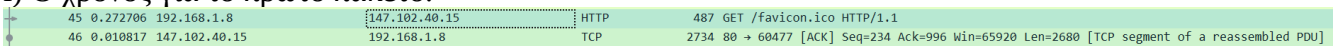
3.8) ip.addr == 147.102.40.15 and http

3.9) Στάλθηκαν 2 και λήφθηκαν 2

3.10) 0.265983 sec

3.11) Χρειάστηκαν 8 πακέτα

3.12)
i) Ο χρόνος για το πρώτο πακέτο.



0.010817 sec.

ii) Ο χρόνος από το πρώτο πακέτο για το τελευταίο είναι 0.000196 sec.

iii) Ο χρόνος για όλο το GET request είναι 0.011013 sec

3.13)
[APDU Rsp Time: 0.011013000 seconds]
[Service Time: 0.010817000 seconds]

[Req Spread: 0.000000000 seconds]
[Rsp Spread: 0.000196000 seconds]

Παρατηρώ πως είναι ίδιοι χρόνοι με αυτούς που υπολόγισα.

3.14) ip.src==192.168.1.8 and http