Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки
Кафедра обчислювальної техніки

«Тестування та контроль якості (QA) вбудованих систем»
Лабораторна робота №5

Модель OSI. Інкапсуляція

Виконала:
студентка групи ІО-91
Тимошенко Діана

Київ
2022 р.

Мета: Розподілити стек протоколів за моделлю OSI для одного сеансу HTTP.

Посилання на репозиторій:

https://github.com/diana-tym/qa-labs

Виконання лабораторної роботи

1. Під’єднайте PC1 та PC2 через Ethernet.

В цій лр були налаштовані віртуальна машина та host-only мережа.

```
diana@diana-X510UAR:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 414  bytes 42014 (42.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 414  bytes 42014 (42.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vmnet1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.1  netmask 255.0.0.0  broadcast 10.255.255.255
        inet6 fe80::250:56ff:fec0:1  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:c0:00:01  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Запустіть DHCP-сервер на PC-1.

Спочатку змінимо у файлі /etc/default/isc-dhcp-server інтерфейс.

```
# On what interfaces s
#       Separate multi
INTERFACESv4="vmnet1"
INTERFACESv6=""
```

```
diana@diana-X510UAR:~$ sudo dhcpd
Internet Systems Consortium DHCP Server 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/vmnet1/00:50:56:c0:00:01/10.0.0.0/8
Sending on   LPF/vmnet1/00:50:56:c0:00:01/10.0.0.0/8
```

3. Налаштуйте NAT.

```
diana@diana-X510UAR:~$ sudo iptables -t nat -A POSTROUTING -o wlp2s0 -s 10.0.0.0/8 -j MASQUERADE
```

```
diana@diana-X510UAR:~$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  10.0.0.0/8           anywhere
```

4. Запустіть Wireshark на PC1.

5. Якщо ваш DHCP-сервер налаштований статично, то на PC2 введіть команду для отримання IP-адреси sudo dhclient <назва інтерфейсу>.

```
diana@ubuntu:~$ sudo dhclient ens33
diana@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.10  netmask 255.0.0.0  broadcast 10.255.255.255
        inet6 fe80::20c:29ff:fee5:e385  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e5:e3:85  txqueuelen 1000  (Ethernet)
        RX packets 12  bytes 1681 (1.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54  bytes 7803 (7.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

6. Переглянути виконання DHCP протоколу.

	Time	Source	Destination	Protocol	Length	Info
2	0.977066994	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xea1ebc19
4	1.981577362	10.0.0.1	10.0.0.10	DHCP	344	DHCP Offer - Transaction ID 0xea1ebc19
5	1.984536655	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xea1ebc19
7	1.991337087	10.0.0.1	10.0.0.10	DHCP	344	DHCP ACK - Transaction ID 0xea1ebc19

DHCP Discover

```
Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface vmnet1,
Ethernet II, Src: VMware_e5:e3:85 (00:0c:29:e5:e3:85), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
   Message type: Boot Request (1)
   Hardware type: Ethernet (0x01)
   Hardware address length: 6
   Hops: 0
   Transaction ID: 0xea1ebc19
   Seconds elapsed: 0
 > Bootp flags: 0x0000 (Unicast)
   Client IP address: 0.0.0.0
   Your (client) IP address: 0.0.0.0
   Next server IP address: 0.0.0.0
   Relay agent IP address: 0.0.0.0
   Client MAC address: VMware_e5:e3:85 (00:0c:29:e5:e3:85)
   Client hardware address padding: 00000000000000000000
   Server host name not given
   Boot file name not given
   Magic cookie: DHCP
 > Option: (53) DHCP Message Type (Discover)
 > Option: (50) Requested IP Address (192.168.132.128)
 > Option: (12) Host Name
 > Option: (55) Parameter Request List
 > Option: (255) End
   Padding: 000000000000000000000000000000000000000000000000000000000000
```

DHCP Offer

```
Frame 4: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface vmnet1, id 0
Ethernet II, Src: VMware_c0:00:01 (00:50:56:c0:00:01), Dst: VMware_e5:e3:85 (00:0c:29:e5:e3:85)
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.10
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xea1ebc19
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.0.0.10
    Next server IP address: 10.0.0.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: VMware_e5:e3:85 (00:0c:29:e5:e3:85)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (10.0.0.1)
  > Option: (51) IP Address Lease Time
  > Option: (1) Subnet Mask (255.0.0.0)
  > Option: (28) Broadcast Address (10.255.255.255)
v Option: (3) Router
      Length: 4
      Router: 10.0.0.1
v Option: (15) Domain Name
      Length: 16
      Domain Name: mydomain.example
v Option: (6) Domain Name Server
      Length: 8
      Domain Name Server: 192.168.0.1
      Domain Name Server: 8.8.8.8
> Option: (255) End
```

DHCP Request

```
Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface vmnet1,
Ethernet II, Src: VMware_e5:e3:85 (00:0c:29:e5:e3:85), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xea1ebc19
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: VMware_e5:e3:85 (00:0c:29:e5:e3:85)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (54) DHCP Server Identifier (10.0.0.1)
  > Option: (50) Requested IP Address (10.0.0.10)
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  v Option: (255) End
```

DHCP Ack

```
Frame 7: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface vmnet1, id 0
Ethernet II, Src: VMware_c0:00:01 (00:50:56:c0:00:01), Dst: VMware_e5:e3:85 (00:0c:29:e5:e3:85)
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.10
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
   Message type: Boot Reply (2)
   Hardware type: Ethernet (0x01)
   Hardware address length: 6
   Hops: 0
   Transaction ID: 0xea1ebc19
   Seconds elapsed: 0
 > Bootp flags: 0x0000 (Unicast)
   Client IP address: 0.0.0.0
   Your (client) IP address: 10.0.0.10
   Next server IP address: 10.0.0.1
   Relay agent IP address: 0.0.0.0
   Client MAC address: VMware_e5:e3:85 (00:0c:29:e5:e3:85)
   Client hardware address padding: 00000000000000000000
   Server host name not given
   Boot file name not given
   Magic cookie: DHCP
 > Option: (53) DHCP Message Type (ACK)
 > Option: (54) DHCP Server Identifier (10.0.0.1)
 > Option: (51) IP Address Lease Time
 > Option: (1) Subnet Mask (255.0.0.0)
 > Option: (28) Broadcast Address (10.255.255.255)
```

7. Після DHCP перевірити default gateway на PC2 за допомогою команди

```
diana@ubuntu:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.0.1        0.0.0.0         UG    0      0        0 ens33
10.0.0.0        0.0.0.0         255.0.0.0       U     0      0        0 ens33
```

8. Визначити IP-адресу PC2.

```
15 3.010922573   VMware_c0:00:01   Broadcast         ARP    42 Who has 10.0.0.10? Tell 10.0.0.1
16 3.011405209   VMware_e5:e3:85   VMware_c0:00:01   ARP    60 10.0.0.10 is at 00:0c:29:e5:e3:85
34 8.220384772   VMware_e5:e3:85   VMware_c0:00:01   ARP    60 Who has 10.0.0.1? Tell 10.0.0.10
35 8.220416122   VMware_c0:00:01   VMware_e5:e3:85   ARP    42 10.0.0.1 is at 00:50:56:c0:00:01
```

9. Перевірте цю IP-адресу, використавши ping на PC1.

```
diana@diana-X510UAR:~$ ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=64 time=0.656 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=64 time=0.662 ms
64 bytes from 10.0.0.10: icmp_seq=3 ttl=64 time=0.660 ms
64 bytes from 10.0.0.10: icmp_seq=4 ttl=64 time=0.661 ms
^C
--- 10.0.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3060ms
rtt min/avg/max/mdev = 0.656/0.659/0.662/0.002 ms
```

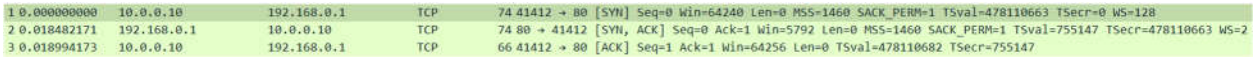
Розподілення стеку протоколів за моделлю OSI для одного сеансу HTTP

1. Відкрийте Інтернет-браузер на PC-2 і введіть в рядку пошуку IP-адресу роутера.

2. Запустіть Wireshark, щоб зареєструвати протокол HTTP з PC2.

Налаштування від DHCP-серверу та MAC-адресу PC2 вже отримав в попередніх пунктах.

Транспортний рівень – встановлення TCP з'єднання.

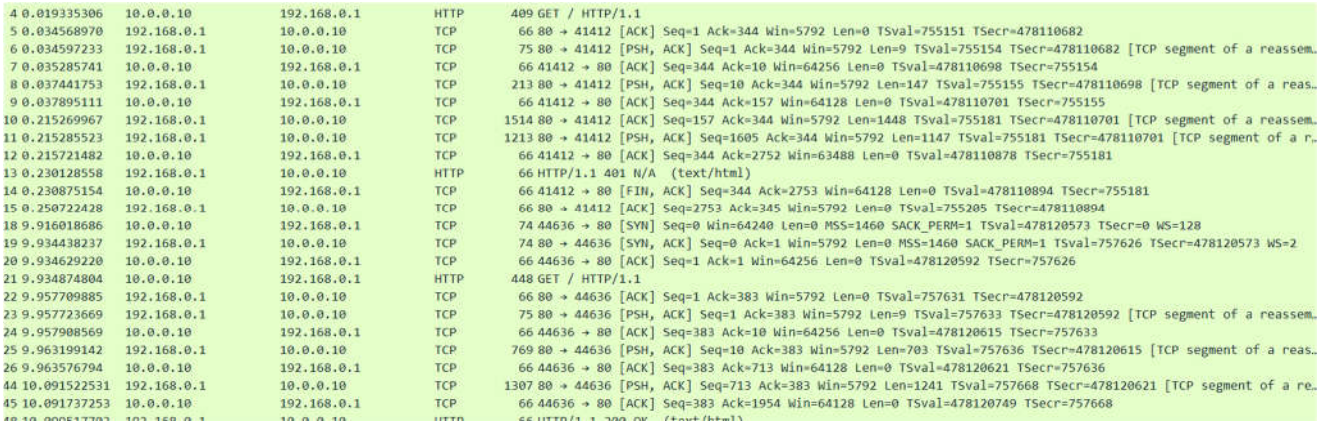


1	0.000000000	10.0.0.10	192.168.0.1	TCP	74 41412 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=478110663 TSecr=0 WS=128
2	0.018482171	192.168.0.1	10.0.0.10	TCP	74 80 → 41412 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=755147 TSecr=478110663 WS=2
3	0.018994173	10.0.0.10	192.168.0.1	TCP	66 41412 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=478110682 TSecr=755147

Сеансовий рівень – підтримання сеансу зв'язку.

Рівень представлення – перетворення протоколів та кодування/декодування даних.

Прикладний рівень – HTTP протокол.

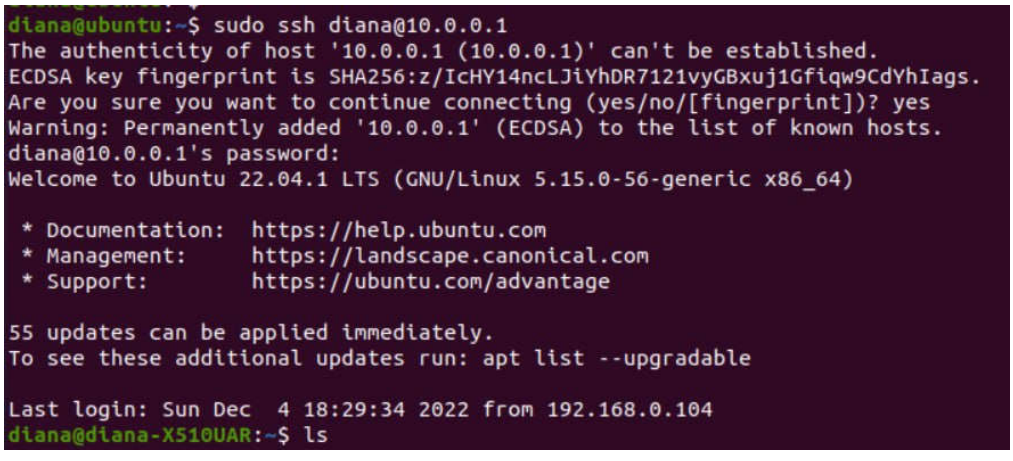


4	0.019335306	10.0.0.10	192.168.0.1	HTTP	409 GET / HTTP/1.1
5	0.034568970	192.168.0.1	10.0.0.10	TCP	66 80 → 41412 [ACK] Seq=1 Ack=344 Win=5792 Len=0 TSval=755151 TSecr=478110682
6	0.034597233	192.168.0.1	10.0.0.10	TCP	75 80 → 41412 [PSH, ACK] Seq=1 Ack=344 Win=5792 Len=9 TSval=755154 TSecr=478110682 [TCP segment of a reassem…
7	0.035285741	10.0.0.10	192.168.0.1	TCP	66 41412 → 80 [ACK] Seq=344 Ack=10 Win=64256 Len=0 TSval=478110698 TSecr=755154
8	0.037441753	192.168.0.1	10.0.0.10	TCP	213 80 → 41412 [PSH, ACK] Seq=10 Ack=344 Win=5792 Len=147 TSval=755155 TSecr=478110698 [TCP segment of a reas…
9	0.037895111	10.0.0.10	192.168.0.1	TCP	66 41412 → 80 [ACK] Seq=344 Ack=157 Win=64128 Len=0 TSval=478110701 TSecr=755155
10	0.215269967	192.168.0.1	10.0.0.10	TCP	1514 80 → 41412 [ACK] Seq=157 Ack=344 Win=5792 Len=1448 TSval=755181 TSecr=478110701 [TCP segment of a reassem…
11	0.215285523	192.168.0.1	10.0.0.10	TCP	1213 80 → 41412 [PSH, ACK] Seq=1605 Ack=344 Win=5792 Len=1147 TSval=755181 TSecr=478110701 [TCP segment of a r…
12	0.215721482	10.0.0.10	192.168.0.1	TCP	66 41412 → 80 [ACK] Seq=344 Ack=2752 Win=63488 Len=0 TSval=478110878 TSecr=755181
13	0.230128558	192.168.0.1	10.0.0.10	HTTP	66 HTTP/1.1 401 N/A (text/html)
14	0.230875154	10.0.0.10	192.168.0.1	TCP	66 41412 → 80 [FIN, ACK] Seq=344 Ack=2753 Win=64128 Len=0 TSval=478110894 TSecr=755181
15	0.250722428	192.168.0.1	10.0.0.10	TCP	66 80 → 41412 [ACK] Seq=2753 Ack=345 Win=5792 Len=0 TSval=755205 TSecr=478110894
18	9.916018686	10.0.0.10	192.168.0.1	TCP	74 44636 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=478120573 TSecr=0 WS=128
19	9.934438237	192.168.0.1	10.0.0.10	TCP	74 80 → 44636 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=757626 TSecr=478120573 WS=2
20	9.934629220	10.0.0.10	192.168.0.1	TCP	66 44636 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=478120592 TSecr=757626
21	9.934874804	10.0.0.10	192.168.0.1	HTTP	448 GET / HTTP/1.1
22	9.957709885	192.168.0.1	10.0.0.10	TCP	66 80 → 44636 [ACK] Seq=1 Ack=383 Win=5792 Len=0 TSval=757631 TSecr=478120592
23	9.957723669	192.168.0.1	10.0.0.10	TCP	75 80 → 44636 [PSH, ACK] Seq=1 Ack=383 Win=5792 Len=9 TSval=757633 TSecr=478120592 [TCP segment of a reassem…
24	9.957908569	10.0.0.10	192.168.0.1	TCP	66 44636 → 80 [ACK] Seq=383 Ack=10 Win=64256 Len=0 TSval=478120615 TSecr=757633
25	9.963199142	192.168.0.1	10.0.0.10	TCP	769 80 → 44636 [PSH, ACK] Seq=10 Ack=383 Win=5792 Len=703 TSval=757636 TSecr=478120615 [TCP segment of a reas…
26	9.963576794	10.0.0.10	192.168.0.1	TCP	66 44636 → 80 [ACK] Seq=383 Ack=713 Win=64128 Len=0 TSval=478120621 TSecr=757636
44	10.091522531	192.168.0.1	10.0.0.10	TCP	1307 80 → 44636 [PSH, ACK] Seq=713 Ack=383 Win=5792 Len=1241 TSval=757668 TSecr=478120621 [TCP segment of a re…
45	10.091737253	10.0.0.10	192.168.0.1	TCP	66 44636 → 80 [ACK] Seq=383 Ack=1954 Win=64128 Len=0 TSval=478120749 TSecr=757668

Завдання

Проаналізувати трафік для сесії на ваш вибір (Skype, SMTP, ftp та ін.).

1. Проаналізуємо трафік для сеансу SSH.

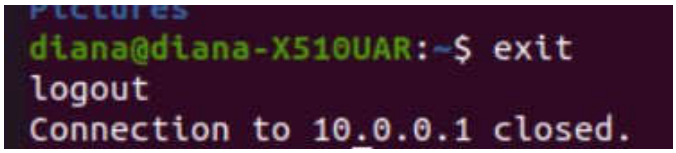


```
diana@ubuntu:~$ sudo ssh diana@10.0.0.1
The authenticity of host '10.0.0.1 (10.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:z/IcHY14ncLJiYhDR7121vyGBxuj1Gfiqw9CdYhIags.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.1' (ECDSA) to the list of known hosts.
diana@10.0.0.1's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

55 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Sun Dec  4 18:29:34 2022 from 192.168.0.104
diana@diana-X510UAR:~$ ls
```



```
Pictures
diana@diana-X510UAR:~$ exit
logout
Connection to 10.0.0.1 closed.
```

Встановлення TCP з’єднання.

1	0.000000000	10.0.0.10	10.0.0.1	TCP	74 52454 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
2	0.000059957	10.0.0.1	10.0.0.10	TCP	74 22 → 52454 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
3	0.000333431	10.0.0.10	10.0.0.1	TCP	66 52454 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval

SSH

4	0.000949252	10.0.0.10	10.0.0.1	SSHv2	107	Client: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5)
6	0.032600164	10.0.0.1	10.0.0.10	SSHv2	98	Server: Protocol (SSH-2.0-OpenSSH_8.9p1 Ubuntu-3)
9	0.033463906	10.0.0.10	10.0.0.1	SSHv2	130	Client: Key Exchange Init
10	0.037524887	10.0.0.1	10.0.0.10	SSHv2	1146	Server: Key Exchange Init
11	0.041606449	10.0.0.10	10.0.0.1	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
12	0.050816199	10.0.0.1	10.0.0.10	SSHv2	662	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=316)
14	3.236580417	10.0.0.10	10.0.0.1	SSHv2	82	Client: New Keys
16	3.283070867	10.0.0.10	10.0.0.1	SSHv2	110	Client: Encrypted packet (len=44)
18	3.283340483	10.0.0.1	10.0.0.10	SSHv2	110	Server: Encrypted packet (len=44)
20	3.284514968	10.0.0.10	10.0.0.1	SSHv2	134	Client: Encrypted packet (len=68)
21	3.290709149	10.0.0.1	10.0.0.10	SSHv2	118	Server: Encrypted packet (len=52)

Закінчення TCP з’єднання.

83	16.697243831	10.0.0.10	10.0.0.1	TCP	66 52454 → 22 [FIN, ACK] Seq=2770 Ack=5185 Win=64128 Len=0
84	16.711744519	10.0.0.1	10.0.0.10	TCP	66 22 → 52454 [FIN, ACK] Seq=5185 Ack=2771 Win=64128 Len=0
85	16.712630213	10.0.0.10	10.0.0.1	TCP	66 52454 → 22 [ACK] Seq=2771 Ack=5186 Win=64128 Len=0 TSva

2. Проаналізуємо трафік для сеансу Telnet.

```
diana@ubuntu:~$ telnet towel.blinkenlights.nl 23
```

DNS запити для отримання IPv4, IPv6 адрес telnet-серверу.

1	0.000000000	10.0.0.10	192.168.0.1	DNS	93	Standard query 0xf9cd A towel.blinkenlights.nl OPT
2	0.000183478	10.0.0.10	192.168.0.1	DNS	93	Standard query 0xbab5 AAAA towel.blinkenlights.nl OPT
3	0.223566308	192.168.0.1	10.0.0.10	DNS	121	Standard query response 0xbab5 AAAA towel.blinkenlights.nl AAAA 2001:7b8:666:ffff::1:42 OPT
4	0.223592576	192.168.0.1	10.0.0.10	DNS	109	Standard query response 0xf9cd A towel.blinkenlights.nl A 213.136.8.188 OPT

Встановлення TCP з’єднання.

5	0.225640515	10.0.0.10	213.136.8.188	TCP	74 50590 → 23 [SYN] Seq=0 Win=64240 Le
6	0.278305450	213.136.8.188	10.0.0.10	TCP	74 23 → 50590 [SYN, ACK] Seq=0 Ack=1 W
7	0.278862864	10.0.0.10	213.136.8.188	TCP	66 50590 → 23 [ACK] Seq=1 Ack=1 Win=64

Telnet

8	0.334118918	213.136.8.188	10.0.0.10	TELNET	72	Telnet Data ...
9	0.334680936	10.0.0.10	213.136.8.188	TCP	66	50590 → 23 [ACK] Seq=1 Ack=7 Win=64256 Len=0 TSval=396667648 TSecr=4181367224
10	0.374547694	213.136.8.188	10.0.0.10	TELNET	1054	Telnet Data ...
11	0.374837689	10.0.0.10	213.136.8.188	TCP	66	50590 → 23 [ACK] Seq=1 Ack=995 Win=64128 Len=0 TSval=396667688 TSecr=4181367280
12	6.784143740	10.0.0.10	213.136.8.188	TELNET	68	Telnet Data ...
13	6.836544762	213.136.8.188	10.0.0.10	TCP	66	23 → 50590 [ACK] Seq=995 Ack=3 Win=65280 Len=0 TSval=4181373730 TSecr=396674098
14	7.085774057	213.136.8.188	10.0.0.10	TELNET	1054	Telnet Data ...
15	7.086493479	10.0.0.10	213.136.8.188	TCP	66	50590 → 23 [ACK] Seq=3 Ack=1983 Win=64128 Len=0 TSval=396674401 TSecr=4181373898
16	9.886134904	10.0.0.10	213.136.8.188	TELNET	68	Telnet Data ...
17	9.942262652	213.136.8.188	10.0.0.10	TCP	66	23 → 50590 [ACK] Seq=1983 Ack=5 Win=65280 Len=0 TSval=4181376832 TSecr=396677201
18	14.582105987	10.0.0.10	213.136.8.188	TELNET	74	Telnet Data ...

Висновок

В цій лабораторній роботі ми налаштували host-only мережу, щоб з’єднати PC1 та PC2, налаштували NAT, DHCP-сервер, роздали DHCP налаштування з PC1 на PC2. Також ми проаналізували трафік для HTTP, SSH та TELNET сесій.