

Išablona pro odevzdávání výstupů z distančních cvičení předmětu MPC-PKT určená k editaci a odevzdání po vytvoření PDF verze

Vaše jméno	Alex Sporni
VUT ID	204633
Vypracovaný lab (označení)	Lab5 (Úvod do programu Wireshark s pomocí utility ping ICMP protokolu, DNS resolveru a DHCP protokolu)

---

#### 1. číslovaný úkol z návodu

Zadání úkolu: **Zjistěte, kolik bajtů má celá ICMP část kteréhokoliv ze zachycených paketů.**

Řešení: Celá ICMP část má **40B** a datová část má **32B**

Source: 192.168.17.138

Destination: 77.75.74.176

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x4d52 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 9 (0x0009)

Sequence number (LE): 2304 (0x0900)

[Response frame: 4]

▼ Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f707172737475767761...

[Length: 32]

---

2. číslovaný úkol z návodu

Zadání úkolu: **Ve svém hlavním operačním systému si nainstalujte Wireshark a opakujte z něj úkony výše. Zjistěte z Wiresharku, jakou konkrétní hodnotu TTL využívá váš hlavní operační systém u ICMP echo request paketu a jaká hodnota je u ICMP echo reply. V tomto i dalších relevantních úkolech nezapomeňte, že u printscreenu příkazové řádky musí být vidět název složky dle vašeho VUT loginu.**

Řešení: Hodnota TTL na VM představuje TTL = 128 pre request aj reply a hodnota na PC představuje TTL = 54 pre reply a TTL = 128 pre request.

```

C:\Users\student\Desktop\xsporn01>ping -4 seznam.cz

Pinging seznam.cz [77.75.74.176] with 32 bytes of data:
Reply from 77.75.74.176: bytes=32 time=4ms TTL=128
Reply from 77.75.74.176: bytes=32 time=4ms TTL=128
Reply from 77.75.74.176: bytes=32 time=12ms TTL=128
Reply from 77.75.74.176: bytes=32 time=4ms TTL=128

Ping statistics for 77.75.74.176:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 12ms, Average = 6ms

C:\Users\student\Desktop\xsporn01>

```

```

C:\Users\alexs\Desktop\xsporn01>ping -4 seznam.cz

Pinging seznam.cz [77.75.75.176] with 32 bytes of data:
Reply from 77.75.75.176: bytes=32 time=3ms TTL=54
Reply from 77.75.75.176: bytes=32 time=3ms TTL=54
Reply from 77.75.75.176: bytes=32 time=3ms TTL=54
Reply from 77.75.75.176: bytes=32 time=4ms TTL=54

Ping statistics for 77.75.75.176:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Users\alexs\Desktop\xsporn01>

```

166	3.669267	147.229.192.11	77.75.75.176	ICMP	74 Echo (ping) request	id=0x0001, seq=18/4608	ttl=128 (reply in 167)
167	3.672941	77.75.75.176	147.229.192.11	ICMP	74 Echo (ping) reply	id=0x0001, seq=18/4608	ttl=54 (request in 166)
221	4.673371	147.229.192.11	77.75.75.176	ICMP	74 Echo (ping) request	id=0x0001, seq=19/4864	ttl=128 (reply in 222)
222	4.677059	77.75.75.176	147.229.192.11	ICMP	74 Echo (ping) reply	id=0x0001, seq=19/4864	ttl=54 (request in 221)
264	5.678795	147.229.192.11	77.75.75.176	ICMP	74 Echo (ping) request	id=0x0001, seq=20/5120	ttl=128 (reply in 265)
265	5.682559	77.75.75.176	147.229.192.11	ICMP	74 Echo (ping) reply	id=0x0001, seq=20/5120	ttl=54 (request in 264)
313	6.682612	147.229.192.11	77.75.75.176	ICMP	74 Echo (ping) request	id=0x0001, seq=21/5376	ttl=128 (reply in 314)
314	6.686525	77.75.75.176	147.229.192.11	ICMP	74 Echo (ping) reply	id=0x0001, seq=21/5376	ttl=54 (request in 313)

Destination	Protocol	Length	Info
8.8.8.8	DNS	69	Standard query 0xac08 A seznam.cz
192.168.17.138	DNS	133	Standard query response 0xac08 A seznam.cz A 77.75.74
77.75.74.176	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128
192.168.17.138	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=128
77.75.74.176	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128
192.168.17.138	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=128
77.75.74.176	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128
192.168.17.138	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=128
77.75.74.176	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128
192.168.17.138	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=128

### 3. číslování úkol z návodu

Zadání úkolu: **Vyzkoušejte si filtr (ip.src==192.168.0.1) and (icmp or dns).** IP adresu ve filtru však upravte, tak aby byla relevantní pro váš virtuální operační systém.  
**Řádně dokumentujte do protokolu, stejně jako všechny ostatní úkoly.**

Řešení: Na obrázku níže vidíte, že zadaný filter filtruje jako icmp tak aj dns.

The screenshot displays a Wireshark packet capture window with a filter set to `(ip.src==192.168.17.138) and (icmp or dns)`. The packet list shows several ICMP Echo (ping) requests and one DNS Standard query. The packet details pane for the selected packet (No. 42) shows the following structure:

- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.17.138, Dst: 77.75.75.176
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 60
  - Identification: 0xa5d7 (42455)
  - > Flags: 0x0000
  - Fragment offset: 0
  - Time to live: 128
  - Protocol: ICMP (1)
  - Header checksum: 0x0000 [validation disabled]
  - [Header checksum status: Unverified]
  - Source: 192.168.17.138
  - Destination: 77.75.75.176
- Internet Control Message Protocol
  - Type: 8 (Echo (ping) request)

Overlaid on the Wireshark window is a Windows Command Prompt window showing the results of two ping commands:

```
C:\Users\student\Desktop\xsporn01>ping -4 seznam.cz

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Users\student\Desktop\xsporn01>ping google.com

Pinging google.com [77.75.75.176] with 32 bytes of data:
Reply from 77.75.75.176: bytes=32 time=4ms TTL=128
Reply from 77.75.75.176: bytes=32 time=5ms TTL=128
Reply from 77.75.75.176: bytes=32 time=4ms TTL=128
Reply from 77.75.75.176: bytes=32 time=4ms TTL=128

Ping statistics for 77.75.75.176:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms

C:\Users\student\Desktop\xsporn01>ping google.com

Pinging google.com [172.217.23.238] with 32 bytes of data:
Reply from 172.217.23.238: bytes=32 time=3ms TTL=128
Reply from 172.217.23.238: bytes=32 time=4ms TTL=128
Reply from 172.217.23.238: bytes=32 time=4ms TTL=128
Reply from 172.217.23.238: bytes=32 time=3ms TTL=128

Ping statistics for 172.217.23.238:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Users\student\Desktop\xsporn01>
```

#### 4. číslovaný úkol z návodu

Zadání úkolu: **Výše uvedený příkaz vyzkoušejte i v hlavním OS a to ve variantě s tečkou na konci i bez ní. Jak se liší komunikace zachycená ve Wiresharku v těchto dvou případech?**

Řešení: Příkaz s bodkou hledá DNS záznamy přímo na root serveri. Příkaz bez bodky zisťuje DNS najprv v lokálnej tabuľke.

- Screenshot nižšie je z **VM**:

The screenshot displays two windows. The top window is Wireshark, showing a packet capture filter '(p.src==192.168.17.138) and (icmp or dns)'. The packet list shows several DNS queries from 192.168.17.138 to 8.8.8.8. The selected packet (No. 9) is a DNS query for AAAA mapy.cz. The bottom window is a Windows command prompt titled 'Příkazový řádek', showing the command 'C:\Users\student\Desktop\xsporn01>nslookup mapy.cz'. The output shows the DNS server as dns.google and the IP address as 8.8.8.8. Below the command prompt, the packet details for the selected packet are visible, showing the Ethernet II header, Internet Protocol Version 4 header, and the DNS query details.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.17.138	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
3	0.005974	192.168.17.138	8.8.8.8	DNS	79	Standard query 0x0002 A mapy.cz.localdomain
5	0.023982	192.168.17.138	8.8.8.8	DNS	79	Standard query 0x0003 AAAA mapy.cz.localdomain
7	0.037635	192.168.17.138	8.8.8.8	DNS	67	Standard query 0x0004 A mapy.cz
9	0.045744	192.168.17.138	8.8.8.8	DNS	67	Standard query 0x0005 AAAA mapy.cz
18	18.062584	192.168.17.138	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
20	18.071443	192.168.17.138	8.8.8.8	DNS	67	Standard query 0x0002 A mapy.cz
22	18.079269	192.168.17.138	8.8.8.8	DNS	67	Standard query 0x0003 AAAA mapy.cz
27	34.864747	192.168.17.138	8.8.8.8	DNS	76	Standard query 0x3a97 A wpad.localdomain

```
C:\Users\student\Desktop\xsporn01>nslookup mapy.cz
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: mapy.cz
Addresses: 2a02:598:a::79:138
           2a02:598:2::1138
           77.75.79.138
           77.75.77.138

C:\Users\student\Desktop\xsporn01>nslookup mapy.cz.
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: mapy.cz
Addresses: 2a02:598:a::79:138
           2a02:598:2::1138
           77.75.79.138
           77.75.77.138

C:\Users\student\Desktop\xsporn01>
```

Packet details for selected packet (No. 9):

- Ethernet II, Src: VMware\_28:f7:4b (00:0c:29:28:f7:4b), Destination: VMware\_fb:de:3c (00:50:56:fb:de:3c), Address: VMware\_fb:de:3c (00:50:56:fb:de:3c), Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.17.138, Destination: 8.8.8.8, Type: IPv4 (0x0800)
- DNS Standard query query 0x0005 AAAA mapy.cz

Screenshot nižšie je z hostovského PC

Capturing from Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.src==147.229.192.11) and (icmp or dns)

No.	Time	Source	Destination	Protocol	Length	Info
204	4.538547	147.229.192.11	147.229.191.143	DNS	88	Standard query 0x0001 PTR 143.191.229.147.in-addr.arpa
206	4.540305	147.229.192.11	147.229.191.143	DNS	79	Standard query 0x0002 A mapy.cz.kn.vutbr.cz
208	4.540697	147.229.192.11	147.229.191.143	DNS	79	Standard query 0x0003 AAAA mapy.cz.kn.vutbr.cz
210	4.541069	147.229.192.11	147.229.191.143	DNS	76	Standard query 0x0004 A mapy.cz.vutbr.cz
212	4.541436	147.229.192.11	147.229.191.143	DNS	76	Standard query 0x0005 AAAA mapy.cz.vutbr.cz
214	4.541833	147.229.192.11	147.229.191.143	DNS	67	Standard query 0x0006 A mapy.cz
216	4.544999	147.229.192.11	147.229.191.143	DNS	67	Standard query 0x0007 AAAA mapy.cz
625	8.792845	147.229.192.11	147.229.191.143	DNS	88	Standard query 0x0001 PTR 143.191.229.147.in-addr.arpa
627	8.794580	147.229.192.11	147.229.191.143	DNS	67	Standard query 0x0002 A mapy.cz
629	8.797439	147.229.192.11	147.229.191.143	DNS	67	Standard query 0x0003 AAAA mapy.cz
2369	32.928393	147.229.192.11	147.229.191.143	DNS	74	Standard query 0x16ce A www.google.com
2370	32.928666	147.229.192.11	147.229.191.143	DNS	74	Standard query 0x1335 AAAA www.google.com

> Frame 204: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0  
> Ethernet II, Src: Dell\_33:f9:29 (54:bf:64:33:f9:29), Dst: He...  
> Internet Protocol Version 4, Src: 147.229.192.11, Dst: 147.229.191.143  
> User Datagram Protocol, Src Port: 56992, Dst Port: 53  
> Domain Name System (query)

```
0000  94 3f c2 07 ca 14 54 bf 64 33 f9 29 08 00 45 00  .?...  
0010  00 4a af 6c 00 00 80 11 00 00 93 e5 c0 0b 93 e5  .J.l.  
0020  bf 8f de a0 00 35 00 36 a7 ad 00 01 01 00 00 01  ....5  
0030  00 00 00 00 00 00 03 31 34 33 03 31 39 31 03 32  ....  
0040  32 39 03 31 34 37 07 69 6e 2d 61 64 64 72 04 61  29.147  
0050  72 70 61 00 00 0c 00 01  rpa...
```

Command Prompt

```
C:\Users\alexs\Desktop\xsporn01>nslookup mapy.cz  
Server: arepur.kn.vutbr.cz  
Address: 147.229.191.143  
  
Non-authoritative answer:  
Name: mapy.cz  
Addresses: 2a02:598:2::1138  
2a02:598:a::79:138  
77.75.79.138  
77.75.77.138  
  
C:\Users\alexs\Desktop\xsporn01>nslookup mapy.cz.  
Server: arepur.kn.vutbr.cz  
Address: 147.229.191.143  
  
Non-authoritative answer:  
Name: mapy.cz  
Addresses: 2a02:598:a::79:138  
2a02:598:2::1138  
77.75.79.138  
77.75.77.138  
  
C:\Users\alexs\Desktop\xsporn01>
```

UpravyZobrazitHistorieZáložkyNástrojeNápověda

seznam - najdu tam, co neznám


→↻🏠🔒🛡️https://www.seznam.cz

InternetFirmyMapyZbožíObrázkySlovník

... najdu tam, co neznám

Právě se hledá: Kaufland antigenní testyVakcína ModernaFormu

SZ | Seznam Zprávy • Středa 10. března. Svátek má Viktorie.



**Neslýchané, devadesátky skončily. Opozice kritizuje Zemana za jeho výroky**  
Opozice nesouhlasí s výrokem prezidenta Miloše Zemana, který si přeje konec ministra zdravotnictví Jana Blatného,...

**Koronavirus**  
Potvrzené případy  
**+15 196**  
1 351 195


**Očkování**  
Kapacity

Nechápu, proč Babiš řeší maturitu. Je to diletantismus, říká expert

Expert na ...


Malý stát n...

**Novinky**




ČSA jsou v ...  
Kupé ze Š ...  
Královna c ...  
Australané ...  
Budou se r ...  
Zeman cho ...  
Muž zaútoč ...

**Super**



Tři týdny po porodu prožívá Veronika Kašáková nejtěžší chvíle v životě: Jejímu miminku diagnostikovali vážnou nemoc  
Modelka z Playboye ví, jak zaujmout. V sexy plavkách vystavila na odiv skvělé křivky

**Sport**



**Sbohem! Česká biatlonová legenda se loučí**  
V neděli v Novém Městě na Moravě sestřelí své poslední terče, přijede do cíle a uzavře se kariéra medailově...

Spiknutí? Zeman rázně hájí Slováky před našťavanou Američankou

SouborÚpravyFormátZobrazeníNápověda

www.seznam.cz

Record Name . . . . . : www.seznam.cz  
Record Type . . . . . : 28  
Time To Live . . . . . : 94  
Data Length . . . . . : 16  
Section . . . . . : Answer  
AAAA Record . . . . . : 2a02:598:4444:1::1

Record Name . . . . . : www.seznam.cz  
Record Type . . . . . : 28  
Time To Live . . . . . : 94  
Data Length . . . . . : 16  
Section . . . . . : Answer  
AAAA Record . . . . . : 2a02:598:4444:1::2

Record Name . . . . . : www.seznam.cz  
Record Type . . . . . : 28  
Time To Live . . . . . : 94  
Data Length . . . . . : 16  
Section . . . . . : Answer  
AAAA Record . . . . . : 2a02:598:3333:1::1

Record Name . . . . . : www.seznam.cz  
Record Type . . . . . : 28  
Time To Live . . . . . : 94  
Data Length . . . . . : 16  
Section . . . . . : Answer  
AAAA Record . . . . . : 2a02:598:3333:1::2

www.seznam.cz

Record Name . . . . . : www.seznam.cz  
Record Type . . . . . : 1  
Time To Live . . . . . : 67  
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . . : 77.75.74.172

Record Name . . . . . : www.seznam.cz  
Record Type . . . . . : 1  
Time To Live . . . . . : 67  
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . . : 77.75.74.176

Record Name . . . . . : www.seznam.cz  
Record Type . . . . . : 1  
Time To Live . . . . . : 67  
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . . : 77.75.75.172

Record Name . . . . . : www.seznam.cz  
Record Type . . . . . : 1  
Time To Live . . . . . : 67  
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . . : 77.75.75.172

Record Name . . . . . : www.seznam.cz  
Record Type . . . . . : 1  
Time To Live . . . . . : 67  
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . . : 77.75.75.172

Príkazový řádek

C:\Users\student\Desktop\vsporn01>ipconfig -flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\student\Desktop\vsporn01>ipconfig -displaydns > vsporn01.txt

C:\Users\student\Desktop\vsporn01>

Služby

Akce / Letáky  
Auto / Moto  
Bazar  
Deníky  
Dovolená

Počasí - Če

4 °C  
Odp

## 5. číslovaný úkol z návodu

Zadání úkolu: Jak se liší hodnota doby odezvy udávaná v příkazové řádce od té zobrazené ve Wiresharku?

Řešení: Hodnota je v oboch případech takmer rovnaká, jediný rozdiel je v zobrazení na počet desatinných miest.

1	0.000000	192.168.17.138	77.75.74.172	ICMP	74 Echo (ping) request	id=0x0001, seq=40/10240, ttl=128
2	0.004168	77.75.74.172	192.168.17.138	ICMP	74 Echo (ping) reply	id=0x0001, seq=40/10240, ttl=128

The image shows a side-by-side comparison of ping results from a Windows Command Prompt and Wireshark. On the left, the Wireshark packet list shows two ICMP Echo (ping) packets. The first packet (No. 1) is a request from 192.168.17.138 to 77.75.74.172. The second packet (No. 2) is a reply from 77.75.74.172 to 192.168.17.138. The packet details for the second packet are expanded, showing the Internet Control Message Protocol (ICMP) section with a Type of 0 (Echo (ping) reply) and a Response time of 4,168 ms. The packet bytes panel shows the raw data in hexadecimal and ASCII. On the right, the Windows Command Prompt shows the command 'C:\Users\student\Desktop\xsporn01>ping -4 -n 1 seznam.cz'. The output shows the ping statistics for 77.75.74.172, including the approximate round trip times in milliseconds: Minimum = 4ms, Maximum = 4ms, Average = 4ms.

Wireshark packet details for packet 2:

- Differentiated Services Field: 0x00 (DSCP: Default)
- Total Length: 60
- Identification: 0x823c (33340)
- Flags: 0x0000
- Fragment offset: 0
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0x4e5b [validation disabled] [Header checksum status: Unverified]
- Source: 77.75.74.172
- Destination: 192.168.17.138
- Internet Control Message Protocol
  - Type: 0 (Echo (ping) reply)
  - Code: 0
  - Checksum: 0x5533 [correct] [Checksum Status: Good]
  - Identifier (BE): 1 (0x0001)
  - Identifier (LE): 256 (0x0100)
  - Sequence number (BE): 40 (0x0028)
  - Sequence number (LE): 10240 (0x2800)
  - [Request frame: 1]
  - [Response time: 4,168 ms]
- Data (32 bytes)
  - Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
  - [Length: 32]

Windows Command Prompt output:

```
C:\Users\student\Desktop\xsporn01>ping -4 -n 1 seznam.cz
Pinging seznam.cz [77.75.74.172] with 32 bytes of data:
Reply from 77.75.74.172: bytes=32 time=4ms TTL=128

Ping statistics for 77.75.74.172:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms
```



## 6. číslovaný úkol z návodu

Zadání úkolu: **Postupně zvyšujte hodnotu parametru -l a zjistěte tak maximální hodnotu objemu dat, které je možné odeslat ICMP pingem bez fragmentace z vašeho virtuálního operačního systému.**

Řešení: Maximální hodnota, kterou je možné nastavit tak, aby sa paket nefragmentoval je **1472 B**.

1	0.000000	192.168.17.138	147.229.2.90	ICMP	1514 Echo (ping) request	id=0x0001, seq=75/19200, ttl=128 (rep
2	0.000922	147.229.2.90	192.168.17.138	ICMP	1514 Echo (ping) reply	id=0x0001, seq=75/19200, ttl=128 (req

The image shows a network packet capture analysis on the left and a command prompt window on the right.

**Packet Capture Analysis (Left):**

- Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
- Ethernet II, Src: VMware\_28:f7:4b (00:0c:29:28:f7:4b), Dst: VMware\_fb:de:3c (00:50:56:fb:de:3c)
- Destination: VMware\_fb:de:3c (00:50:56:fb:de:3c)
- Address: VMware\_fb:de:3c (00:50:56:fb:de:3c)
- ... ..0. .... = LG bit: Globally unique address
- ... ..0. .... = IG bit: Individual unicast address
- Source: VMware\_28:f7:4b (00:0c:29:28:f7:4b)
- Address: VMware\_28:f7:4b (00:0c:29:28:f7:4b)
- ... ..0. .... = LG bit: Globally unique address
- ... ..0. .... = IG bit: Individual unicast address
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.17.138, Dst: 147.229.2.90
- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not Set)
- Total Length: 1500
- Identification: 0x6c91 (27793)
- Flags: 0x4000, Don't fragment
- 0. .... = Reserved bit: Not set
- .1.. .... = Don't fragment: Set
- ..0. .... = More fragments: NOT set
- Fragment offset: 0
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0x0000 [validation disabled]

**Command Prompt (Right):**

```
C:\Users\student\Desktop\xsporn01>ping -4 -n 1 -f -l 1472 vutbr.cz
```

Pinging vutbr.cz [147.229.2.90] with 1472 bytes of data:  
Reply from 147.229.2.90: bytes=1472 time=1ms TTL=128

Ping statistics for 147.229.2.90:  
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 1ms, Maximum = 1ms, Average = 1ms

```
C:\Users\student\Desktop\xsporn01>ping -4 -n 1 -f -l 1473 vutbr.cz
```

Pinging vutbr.cz [147.229.2.90] with 1473 bytes of data:  
Packet needs to be fragmented but DF set.

Ping statistics for 147.229.2.90:  
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

```
C:\Users\student\Desktop\xsporn01>
```



## 7. číslovaný úkol z návodu

Zadání úkolu: **Druhý případ** zachyťte ve Wiresharku a vyhledejte typ a kód chyby ICMP protokolu, který souvisí se zprávou „TTL expired in transit“. Pozn.: Jedná se o případ neúspěšného pingu.

Řešení:

- Typ 11 představuje, že time to live je překročený
- Code 0 představuje že sa time to live překročil pri prenose

No.	Time	Source	Destination	Protocol	Length	Info
4	4.229213	192.168.17.138	77.75.75.176	ICMP	74	Echo (ping) request id=0x0001, seq=81/20736, ttl=1 (no response found)
5	4.229425	192.168.17.2	192.168.17.138	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
6	5.248798	192.168.17.138	77.75.75.176	ICMP	74	Echo (ping) request id=0x0001, seq=82/20992, ttl=1 (no response found)
7	5.249059	192.168.17.2	192.168.17.138	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
8	6.264421	192.168.17.138	77.75.75.176	ICMP	74	Echo (ping) request id=0x0001, seq=83/21248, ttl=1 (no response found)
9	6.264597	192.168.17.2	192.168.17.138	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
10	7.280284	192.168.17.138	77.75.75.176	ICMP	74	Echo (ping) request id=0x0001, seq=84/21504, ttl=1 (no response found)
11	7.280537	192.168.17.2	192.168.17.138	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: ...)

Total Length: 88

Identification: 0x86b6 (34486)

> Flags: 0x0000

Fragment offset: 0

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0x1012 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.17.2

Destination: 192.168.17.138

▼ Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

Checksum: 0xf4ff [correct]

[Checksum Status: Good]

Unused: 00000000

▼ Internet Protocol Version 4, Src: 192.168.17.138, Dst: 77.75.75.176

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0x0c65 (3173)

...

Príkazový riádek

C:\Users\student\Desktop\xsporn01>ping -4 -i 1 seznam.cz

Pinging seznam.cz [77.75.75.176] with 32 bytes of data:

Reply from 192.168.17.2: TTL expired in transit.

Reply from 192.168.17.2: TTL expired in transit.

Reply from 192.168.17.2: TTL expired in transit.

Reply from 192.168.17.2: TTL expired in transit.

Ping statistics for 77.75.75.176:

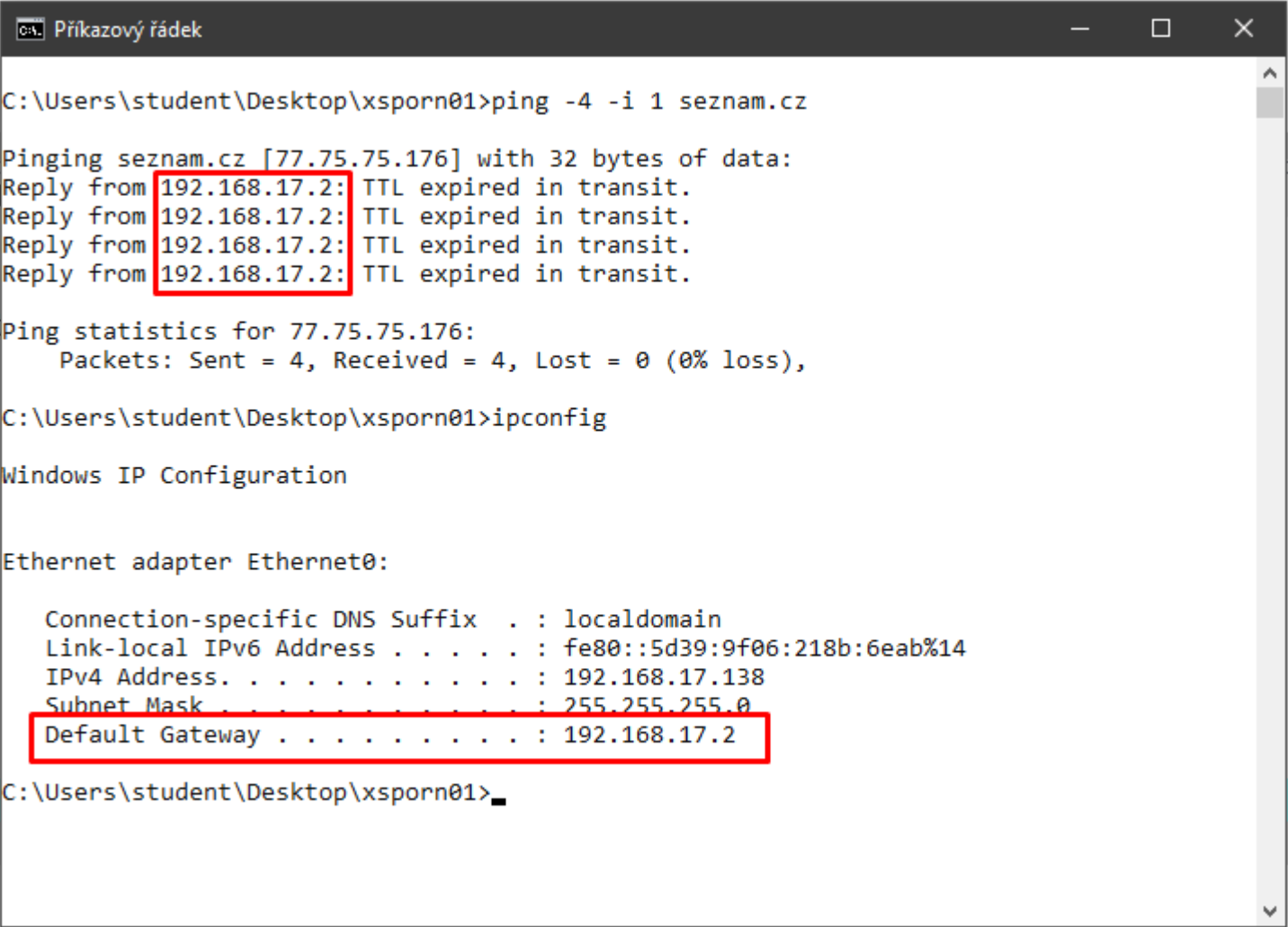
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\student\Desktop\xsporn01>

## 8. číslovaný úkol z návodu

Zadání úkolu: **Ve výpisu paketů ve Wiresharku vidíme chybové zprávy protokolu ICMP (v základním nastavení podbarveny černě), které v informační části mají popisek Time-to-Live exceeded. Kdo je odesilatelem těchto paketů z hlediska síťové vrstvy (IP adresy)?**

Řešení: Jedná se o **Default Gateway** (východzia brána, router), ktorý má IP adresu **192.168.17.2**



```
C:\Users\student\Desktop\xsporn01>ping -4 -i 1 seznam.cz

Pinging seznam.cz [77.75.75.176] with 32 bytes of data:
Reply from 192.168.17.2: TTL expired in transit.
Reply from 192.168.17.2: TTL expired in transit.
Reply from 192.168.17.2: TTL expired in transit.
Reply from 192.168.17.2: TTL expired in transit.

Ping statistics for 77.75.75.176:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\student\Desktop\xsporn01>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::5d39:9f06:218b:6eab%14
    IPv4 Address. . . . . : 192.168.17.138
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.17.2

C:\Users\student\Desktop\xsporn01>
```

## 9. číslovaný úkol z návodu

Zadání úkolu: **Vyzkoušejte stejný pokus se třemi pingy odeslanými unicastem, broadcastem a multicastem ve svém hlavním OS. IP adresy upravte odpovídajícím způsobem. V případě, že některý z pingů ve Wiresharku nevidíte, byl pro jeho odeslání použit špatný interface. Pro použití správného rozhraní je nutné příkaz doplnit o parametr -S se zdrojovou IP adresou, která je nakonfigurovaná na daném rozhraní.**

Řešení:

The image shows a Wireshark packet capture and a Windows Command Prompt window. The Wireshark packet list shows several ICMP Echo (ping) requests and replies. The Command Prompt shows the execution of three ping commands: a successful unicast ping to 147.229.192.1, a failed broadcast ping to 147.229.195.255, and a failed multicast ping to 224.0.0.1.

No.	Time	Source	Destination	Protocol	Length	Info
540	9.718635	147.229.192.11	147.229.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=95/24320, ttl=128 (reply in 541)
541	9.720348	147.229.192.1	147.229.192.11	ICMP	74	Echo (ping) reply id=0x0001, seq=95/24320, ttl=255 (request in 540)
1212	21.395997	147.229.192.11	147.229.195.255	ICMP	74	Echo (ping) request id=0x0001, seq=96/24576, ttl=128 (no response found!)
1213	21.396373	147.229.192.14	147.229.192.11	ICMP	74	Echo (ping) reply id=0x0001, seq=96/24576, ttl=64
1889	34.018561	147.229.192.11	224.0.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=97/24832, ttl=128 (multicast)
1890	34.018860	147.229.192.14	147.229.192.11	ICMP	74	Echo (ping) reply id=0x0001, seq=97/24832, ttl=64

```
C:\Users\alexs\Desktop\xsporn01>ping -4 -n 1 -S 147.229.192.11 147.229.192.1

Pinging 147.229.192.1 from 147.229.192.11 with 32 bytes of data:
Reply from 147.229.192.1: bytes=32 time=1ms TTL=255

Ping statistics for 147.229.192.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\alexs\Desktop\xsporn01>ping -4 -n 1 -S 147.229.192.11 147.229.195.255

Pinging 147.229.195.255 from 147.229.192.11 with 32 bytes of data:
Request timed out.

Ping statistics for 147.229.195.255:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Users\alexs\Desktop\xsporn01>ping -4 -n 1 -S 147.229.192.11 224.0.0.1

Pinging 224.0.0.1 from 147.229.192.11 with 32 bytes of data:
Request timed out.

Ping statistics for 224.0.0.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Users\alexs\Desktop\xsporn01>
```

Frame 540: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface  
Ethernet II, Src: Dell\_33:f9:29 (54:bf:64:33:f9:29), Dst: HewlettP\_07:ca:14 (08:00:07:00:00:07)  
Internet Protocol Version 4, Src: 147.229.192.11, Dst: 147.229.192.1  
Internet Control Message Protocol  
Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0x4cfc [correct]  
[Checksum Status: Good]  
Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence Number (BE): 95 (0x005f)  
Sequence Number (LE): 24320 (0x5f00)  
[Response frame: 541]  
Data (32 bytes)

```
0000  94 3f c2 07 ca 14 54 bf 64 33 f9 29 08 00 45 00  .?....T. d3)...E.  
0010  00 3c f8 74 00 00 80 01 00 00 93 e5 c0 0b 93 e5  .<.t....  
0020  c0 01 08 00 4c fc 00 01 00 5f 61 62 63 64 65 66  ....L... _abcdef  
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv  
0040  77 61 62 63 64 65 66 67 68 69                  wabcdefg hi
```

## 10. číslovaný úkol z návodu

Zadání úkolu: Pomocí vámi navrženého filtru zobrazení paketů ve Wiresharku vyfiltrujte ze zobrazených pingů pomocí ICMP sekvenčních čísel pouze poslední dva zobrazené pingy (v obou případech zprávu echo request i echo reply).

Řešení: icmp and icmp.seq > 101

No.	Time	Source	Destination	Sekvenční číslo	Protocol	Length	Info
21	13.030217	192.168.17.138	147.229.2.90	102 (0x0066)	ICMP	74	Echo (ping) request id=0x0001, seq=102/26112, ttl=128 (reply in 22)
22	13.031020	147.229.2.90	192.168.17.138	102 (0x0066)	ICMP	74	Echo (ping) reply id=0x0001, seq=102/26112, ttl=128 (request in 21)
23	13.654912	192.168.17.138	77.75.74.176	103 (0x0067)	ICMP	74	Echo (ping) request id=0x0001, seq=103/26368, ttl=128 (reply in 24)
24	13.659188	77.75.74.176	192.168.17.138	103 (0x0067)	ICMP	74	Echo (ping) reply id=0x0001, seq=103/26368, ttl=128 (request in 23)

## 11. číslovaný úkol z návodu

Zadání úkolu: Jakým vhodným filtrem bychom zobrazili ve Wiresharku pouze pingy na vutbr.cz a odfiltrovali pingy na seznam.cz?

Řešení: icmp and ip.addr == 147.229.2.90

No.	Time	Source	Destination	Sekvenční číslo	Protocol	Length	Info
7	9.989996	192.168.17.138	147.229.2.90	96 (0x0060)	ICMP	74	Echo (ping) request id=0x0001, seq=96/24576, ttl=128 (reply in 8)
8	9.990576	147.229.2.90	192.168.17.138	96 (0x0060)	ICMP	74	Echo (ping) reply id=0x0001, seq=96/24576, ttl=128 (request in 7)
13	10.999234	192.168.17.138	147.229.2.90	98 (0x0062)	ICMP	74	Echo (ping) request id=0x0001, seq=98/25088, ttl=128 (reply in 14)
14	11.000056	147.229.2.90	192.168.17.138	98 (0x0062)	ICMP	74	Echo (ping) reply id=0x0001, seq=98/25088, ttl=128 (request in 13)
17	12.014443	192.168.17.138	147.229.2.90	100 (0x0064)	ICMP	74	Echo (ping) request id=0x0001, seq=100/25600, ttl=128 (reply in 18)
18	12.015741	147.229.2.90	192.168.17.138	100 (0x0064)	ICMP	74	Echo (ping) reply id=0x0001, seq=100/25600, ttl=128 (request in 17)
21	13.030217	192.168.17.138	147.229.2.90	102 (0x0066)	ICMP	74	Echo (ping) request id=0x0001, seq=102/26112, ttl=128 (reply in 22)
22	13.031020	147.229.2.90	192.168.17.138	102 (0x0066)	ICMP	74	Echo (ping) reply id=0x0001, seq=102/26112, ttl=128 (request in 21)

Príkazový řádek

C:\Users\student\Desktop\xporn01>ping -4 seznam.cz

> Frame 21: 74 by  
> Ethernet II, Sr  
> Internet Protoc  
v Internet Contro  
Type: 8 (Echo)  
Code: 0  
Checksum: 0x4  
Identifier (E  
Identifier (U  
Sequence num  
Sequence num  
[Response frame, xx]  
Data (32 bytes)

Pinging seznam.cz [77.75.74.176] with 32 bytes of data:  
Reply from 77.75.74.176: bytes=32 time=4ms TTL=128  
Reply from 77.75.74.176: bytes=32 time=4ms TTL=128  
Reply from 77.75.74.176: bytes=32 time=4ms TTL=128  
Reply from 77.75.74.176: bytes=32 time=4ms TTL=128  
Ping statistics for 77.75.74.176:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 4ms, Maximum = 4ms, Average = 4ms

Príkazový řádek

C:\Users\student\Desktop\xporn01>ping -4 vutbr.cz

te  
Pinging vutbr.cz [147.229.2.90] with 32 bytes of data:  
Reply from 147.229.2.90: bytes=32 time<1ms TTL=128  
Reply from 147.229.2.90: bytes=32 time<1ms TTL=128  
Reply from 147.229.2.90: bytes=32 time<1ms TTL=128  
Reply from 147.229.2.90: bytes=32 time<1ms TTL=128  
Ping statistics for 147.229.2.90:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 1ms, Average = 0ms

## 12. číslovaný úkol z návodu

Zadání úkolu: **Jakou IP adresu používá stanice jako zdrojovou v situaci, kdy odesílá DHCP Discover paket?**

Řešení: Zdrojová stanice používá IP adresu **0.0.0.0** z důvodu, že jej ešte nebola pridelená žiadna IP adresa.

dhcp							
No.	Time	Source	Destination	Sekvenčné číslo	Protocol	Length	Info
1	0.000000	192.168.17.138	192.168.17.254		DHCP	342	DHCP Release - Transaction ID 0x870d6993
59	177.120359	0.0.0.0	255.255.255.255		DHCP	344	DHCP Discover - Transaction ID 0xa3a57650
63	178.121211	192.168.17.254	192.168.17.138		DHCP	342	DHCP Offer - Transaction ID 0xa3a57650
64	178.121890	0.0.0.0	255.255.255.255		DHCP	370	DHCP Request - Transaction ID 0xa3a57650
65	178.122158	192.168.17.254	192.168.17.138		DHCP	342	DHCP ACK - Transaction ID 0xa3a57650

> Frame 59: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{F54A6428-385F-4667-8D33-4C9ADC633F43}, id 0	
> Ethernet II, Src: VMware_28:f7:4b (00:0c:29:28:f7:4b), 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: 0xa3a57650	
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_28:f7:4b (00:0c:29:28:f7:4b)	
Client hardware address padding: 00000000000000000000	
Server host name not given	
Boot file name not given	
Magic cookie: DHCP	
▼ Option: (53) DHCP Message Type (Discover)	
Length: 1	
DHCP: Discover (1)	
> Option: (61) Client identifier	

### 13. číslovaný úkol z návodu

Zadání úkolu: **Na jakou cílovou IP adresu stanice odesílá DHCP Discover paket a z jakého důvodu?**

Řešení: Stanica odosiela požiadavku typu **Broadcast 255.255.255.255** všetkým dostupným zariadeniam na danej **LAN**. Zisťuje, či sa na LAN nachádza DHCP server, ktorý by potom unicastovou odpoveďou poslal požadovanú DHCP konfiguráciu. V nasledujúcej správe DHCP server s IP adresou **192.168.17.138** odpovedá klientovi.

No.	Time	Source	Destination	Sekvenčné číslo	Protocol	Length	Info
1	0.000000	192.168.17.138	192.168.17.254		DHCP	342	DHCP Release - Transaction ID 0x870d6993
59	177.120359	0.0.0.0	255.255.255.255		DHCP	344	DHCP Discover - Transaction ID 0xa3a57650
63	178.121211	192.168.17.254	192.168.17.138		DHCP	342	DHCP Offer - Transaction ID 0xa3a57650
64	178.121890	0.0.0.0	255.255.255.255		DHCP	370	DHCP Request - Transaction ID 0xa3a57650
65	178.122158	192.168.17.254	192.168.17.138		DHCP	342	DHCP ACK - Transaction ID 0xa3a57650

> Frame 59: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF\_{F54A6428-385F-4667-8D33-4C9ADC633F43}, id 0

> Ethernet II, Src: VMware\_28:f7:4b (00:0c:29:28:f7:4b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 330  
Identification: 0x62b6 (25270)  
> Flags: 0x0000  
Fragment offset: 0  
Time to live: 128  
Protocol: UDP (17)  
Header checksum: 0x0000 [validation disabled]  
[Header checksum status: Unverified]  
Source: 0.0.0.0  
Destination: 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: 0xa3a57650  
Seconds elapsed: 0  
> Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0  
Your (client) IP address: 0.0.0.0

## 14. číslovaný úkol z návodu

Zadání úkolu: **Ve zprávě DHCP ACK naleznete hodnotu Lease Time a porovnejte ji s údaji v nově provedeném výpisu ipconfig /all.**

Řešení: Ako je možné vidieť na ukážke nižšie, tak sa obe hodnoty zhodujú. Jedná sa o **30 minútový lease time**.

1	0.000000	192.168.17.138	192.168.17.254	DHCP	342 DHCP Release	- Transaction ID 0x870d6993
59	177.120359	0.0.0.0	255.255.255.255	DHCP	344 DHCP Discover	- Transaction ID 0xa3a57650
63	178.121211	192.168.17.254	192.168.17.138	DHCP	342 DHCP Offer	- Transaction ID 0xa3a57650
64	178.121890	0.0.0.0	255.255.255.255	DHCP	370 DHCP Request	- Transaction ID 0xa3a57650
65	178.122158	192.168.17.254	192.168.17.138	DHCP	342 DHCP ACK	- Transaction ID 0xa3a57650

```
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xa3a57650
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.17.138
Next server IP address: 192.168.17.254
Relay agent IP address: 0.0.0.0
Client MAC address: VMware_28:f7:4b (00:0c:29:28:f7:4b)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
< Option: (53) DHCP Message Type (ACK)
  Length: 1
  DHCP: ACK (5)
< Option: (54) DHCP Server Identifier (192.168.17.254)
  Length: 4
  DHCP Server Identifier: 192.168.17.254
< Option: (51) IP Address Lease Time
  Length: 4
  IP Address Lease Time: (1800s) 30 minutes
< Option: (1) Subnet Mask (255.255.255.0)
  Length: 4
  Subnet Mask: 255.255.255.0
```

```
Wybrat Příkazový řádek

Host Name . . . . . : DESKTOP-HVSVAFP
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-28-F7-4B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::5d39:9f06:218b:6eab%14(Preferred)
IPv4 Address. . . . . : 192.168.17.138(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, 11 March 2021 16:56:53
Lease Expires . . . . . : Thursday, 11 March 2021 17:26:52
Default Gateway . . . . . : 192.168.17.2
DHCP Server . . . . . : 192.168.17.254
DHCIPv6 IAID . . . . . : 100666409
DHCIPv6 Client DUID. . . . . : 00-01-00-01-27-D7-F3-51-00-0C-29-28-F7-4B
DNS Servers . . . . . : 8.8.8.8
                        8.8.4.4
Primary WINS Server . . . . . : 192.168.17.2
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\student\Desktop\vsporn01>
```

```
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0110 00 00 00 00 00 00 63 82 53 63 35 01 05 36 04 c0 .....C..Sc5..6..
0120 a8 11 fe 33 04 00 00 07 08 01 04 ff ff ff 00 03 ...3.....
0130 04 c0 a8 11 02 06 04 c0 a8 11 02 0f 0b 6c 6f 63 .....loc
0140 61 6c 64 6f 6d 61 69 6e 2c 04 c0 a8 11 02 ff 00 aldomain ,.....
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```