

Analýza komunikace na Tcp/Ip sítích

by Timushev Fedor, Meister Stepan

1. Analýza protokolů

1.1. Dynamic host configuration protocol (DHCP)

- Postup přidělení IP adresy:
Discover → Offer → Request → ACK (Acknowledgement);
- Zdrojové a cílové L2 a L3 adresy rámců / paketů s DHCP datagramy:
d8:3b:bf:b7:49:68, 192.168.0.1;
- Doba zapůjčení IP adresy:
2 hodiny;
- Název sledovaného PC:
Scarlet;
- Zapůjčená IP adresa:
192.168.0.106;
- Masku podsítě:
255.255.255.0;
- IP adresa výchozí brány:
192.168.0.1;
- IP adresa DHCP serveru:
192.168.0.1;

1.2. Address resolution protocol

- Postup získání MAC adresy výchozí brány:
Zeptej se kdo má adresu, odešli této adrese → Adresu je na této mac adrese;
- Zdrojové a cílové L2 adresy ARP rámců:
d8:3b:bf:b7:49:68;
- Poznamenejte si obsah ARP rámců:
Sender: ip, mac; target: ip, mac; hardware: type, size; protocol: size type;

1.3. Internet Control Message Protocol

- Na PC zadejte do příkazové řádky příkaz „ping 147.32.192.2“. – jedná se o DNS server na ČVUT FEL, můžete použít i jiný vhodný server:

```
C:\Users\overlord>ping 147.32.192.2

Pinging 147.32.192.2 with 32 bytes of data:
Reply from 147.32.192.2: bytes=32 time=15ms TTL=55
Reply from 147.32.192.2: bytes=32 time=6ms TTL=55
Reply from 147.32.192.2: bytes=32 time=8ms TTL=55
Reply from 147.32.192.2: bytes=32 time=15ms TTL=55

Ping statistics for 147.32.192.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 15ms, Average = 11ms
```

Img 1. Ping serveru

- Poznamenejte si obsahy zpráv požadavku (Echo Request) a příslušné odpovědi (Echo Reply):
Request - 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
Reply - 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
- Zjistěte prostřednictvím příkazové řádky a příkazu „tracert“ počet síťových mezilehlých zařízení mezi sledovaným PC a libovolným serverem:

```
C:\Users\overlord>tracert 147.32.192.2

Tracing route to crns1.feld.cvut.cz [147.32.192.2]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    192.168.0.1
  2  *         *         *         Request timed out.
  3  2 ms     2 ms     2 ms     10.132.0.1
  4  1 ms     2 ms     1 ms     ip-185-136-198-65.sta.ji.cz [185.136.198.65]
  5  2 ms     2 ms     2 ms     ip-229-230.sta.ji.cz [213.226.229.230]
  6  7 ms     7 ms     7 ms     nix1-100ge.cesnet.cz [91.210.16.191]
  7  9 ms     7 ms     7 ms     195.113.235.109
  8  6 ms     6 ms     6 ms     cvut-r92.cesnet.cz [195.113.144.173]
  9  5 ms     6 ms     6 ms     feld-de.net.cvut.cz [147.32.252.74]
 10 14 ms     7 ms     6 ms     crns1.feld.cvut.cz [147.32.192.2]

Trace complete.
```

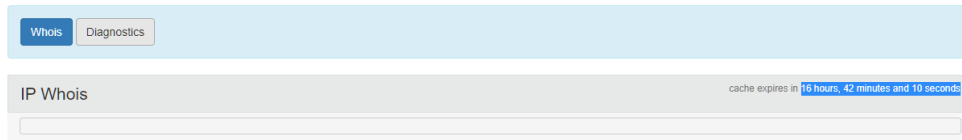
Img 2. Počet síťových mezilehlých zařízení

1.4. Domain Name System

- Zdrojové a cílové L2 a L3 adresy rámců / paketů s DNS datagramy:
d8:3b:bf:b7:49:68, 192.168.0.1;
- Dotazované doménové jméno:
www.seznam.cz;

- IP adresa dotazované stanice (tedy serveru www.seznam.cz):
77.75.74.172, 77.75.74.176;
- Z volně dostupných databází doménových jmen (tzv. „whois“ služeb) zjistěte datum vypršení pronájmu doménového jména libovolného serveru:

8.8.8.8 address profile



Img 3. Datum vypršení pronájmu doménového jména

1.5. Hypertext Transfer Protocol:

- Obsah požadavku zasláného webovým prohlížečem:
Jmeno serveru, typ připojení, encoding, jazyk, cookies

```

164_ 27.345480 192.168.0.106 216.58.201.78 HTTP 783 GET / HTTP/1.1
> Frame 16467: 783 bytes on wire (6264 bits), 783 bytes captured (6264 bits) on interface \Device\NPF_{E
> Ethernet II, Src: IntelCor_b7:49:68 (d8:3b:bf:b7:49:68), Dst: Tp-LinkT_8e:4a:86 (74:da:88:8e:4a:86)
> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 216.58.201.78
> Transmission Control Protocol, Src Port: 60289, Dst Port: 80, Seq: 1, Ack: 1, Len: 729
< Hypertext Transfer Protocol
  < GET / HTTP/1.1\r\n
    Host: google.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,cs;q=0.7\r\n
  < [truncated]Cookie: SID=8gfd3uEeDyadBbMhqbJGqV2Z66dHuob0enJwLGPEx72aqRyvW8r3urcXP7KXRufwcVMjSw.; HS
    Cookie pair: SID=8gfd3uEeDyadBbMhqbJGqV2Z66dHuob0enJwLGPEx72aqRyvW8r3urcXP7KXRufwcVMjSw.
    Cookie pair: HSID=ARzJ95Rohh1DnFhX
    Cookie pair: APISID=iqJbITYxmUQSGKC/AVS-P-tqhrtF-u4AS
    Cookie pair: OGPc=19022519-1:
    Cookie pair: SEARCH_SAMESITE=CgQIU5IB
    Cookie pair: SIDCC=AJi4Qfjlu_xx53VF4Yh51aw51d4AMzJapJIGolZKtNGAfs3ZbwzNu5-y2iMoB4Q3FVgF_88mn9i
  \r\n
  [Full request URI: http://google.com/]
  [HTTP request 1/1]
  [Response in frame: 16491]

```

Img 4. Obsah požadavku

- Obsah odpovědi zasláné serverem:
Kod statusu, znění odpovědi, typ obsahu, datum, tzp připojení, doba od požadavku

```

345_ 88.775292 34.234.80.176 192.168.0.106 HTTP 194 HTTP/1.1 200 OK
> Frame 34566: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface \Dev
> Ethernet II, Src: Tp-LinkT_8e:4a:86 (74:da:88:8e:4a:86), Dst: IntelCor_b7:49:68 (d8:3b:bf:b7
> Internet Protocol Version 4, Src: 34.234.80.176, Dst: 192.168.0.106
> Transmission Control Protocol, Src Port: 80, Dst Port: 50522, Seq: 141, Ack: 745, Len: 140
< Hypertext Transfer Protocol
  < HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    [HTTP/1.1 200 OK\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Content-Type: text/plain\r\n
    Date: Mon, 03 May 2021 18:04:14 GMT\r\n
    Server: nginx\r\n
  < Content-Length: 0\r\n
  Connection: keep-alive\r\n
  \r\n
  [HTTP response 2/2]
  [Time since request: 0.129234000 seconds]
  [Prev request in frame: 13256]
  [Prev response in frame: 13309]
  [Request in frame: 34512]
  [Request URI: http://heartbeat.dm.origin.com/pulse?authn&user=4C8BC2FF1C660403BA2FC403A8

```

Img 5. Obsah odpovědi

- Z kolika webových serverů se celkem načítala data pro zvolenou webovou stránku: ze dvou;

1.6. File Transfer Protocol:

- Pokuste se najít zachycené přihlašovací údaje:

425...	89.303419	147.32.200.238	192.168.0.106	FTP	92 Response: 530 Please login with USER and PASS.
425...	89.304661	192.168.0.106	147.32.200.238	FTP	68 Request: USER student
425...	89.310336	147.32.200.238	192.168.0.106	TCP	54 21 → 52146 [ACK] Seq=97 Ack=35 Win=64256 Len=0
425...	89.310532	147.32.200.238	192.168.0.106	FTP	88 Response: 331 Please specify the password.
425...	89.310625	192.168.0.106	147.32.200.238	FTP	69 Request: PASS B3B38KDS
425...	89.341500	147.32.200.238	192.168.0.106	FTP	77 Response: 230 Login successful.
425...	89.343721	192.168.0.106	147.32.200.238	FTP	73 Request: CWD /home/student

Img 6. Zachycené přihlašovací údaje

- Analyzujte mechanismus navázání TCP spojení:

Pro navázání spojení se používá třicestný handshake (potřesení ruky). V průběhu navazování spojení se obě strany dohodnou na čísla sekvence (sequence number).

Číslo sekvence a odpovědi (sequence, acknowledgement number) jsou 32bitové hodnoty uváděné v TCP hlavičce.

Pro navázání spojení se posílá TCP segment, který má nastaveny příznaky (flags) v TCP hlavičce. Navázání spojení probíhá ve třech krocích.

- Mechanismus pomalého startu:

Tento mechanismus se používá při zahájení přenosu mezi stanicemi nebo když dojde k zahlcení sítě.

Po sestavení spojení může vysílací stanice zvolit poměrně velkou počáteční velikost Klouzavého okna. Správnou velikost pak odvodí samočasovací algoritmus na základě doby návratu potvrzení.

Je zde však velké riziko zahlcení sítě příliš velkým počtem segmentů. Nebudou se vracet potvrzení a vysílač včas nezaregistruje, že překročil kapacitu sítě.

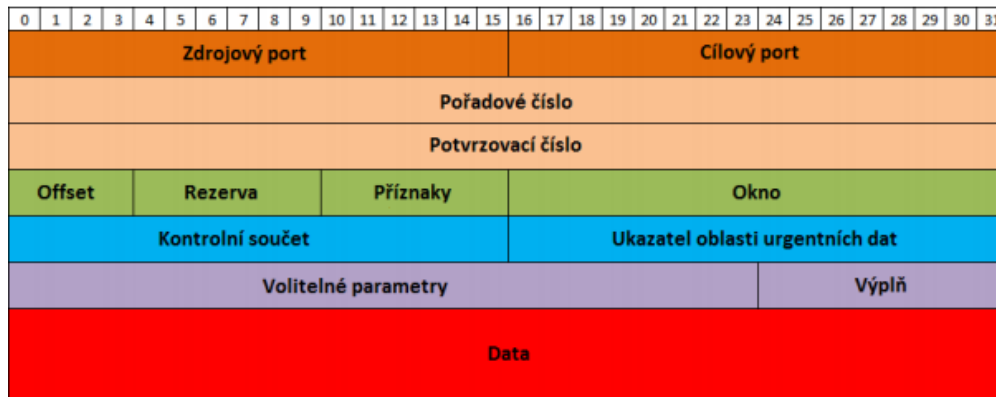
Princip spočívá v přidání dalšího okna, tzv. okna zahlcení, které se nastaví na velikost jednoho segmentu. Vysílací stanice odešle jeden segment a pak čeká na potvrzení zprávou ACK. Jakmile přijde potvrzovací zpráva ACK jednoho segmentu, vysílací stanice zvětší hodnotu okna o jedna, tedy na 2 segmenty, a tyto segmenty odešle atd.

39	2.808348	192.168.0.191	147.32.200.238	FTP-D..	14654 FTP Data: 14600 bytes (PORT) (STOR test.txt)
40	2.821435	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=1461 Win=62780 Len=0
41	2.821436	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=2921 Win=62780 Len=0
42	2.821436	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=14601 Win=55480 Len=0
43	2.821507	192.168.0.191	147.32.200.238	FTP-D..	29254 FTP Data: 29200 bytes (PORT) (STOR test.txt)
44	2.834382	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=16061 Win=62780 Len=0
45	2.834383	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=17521 Win=62780 Len=0
46	2.834383	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=18981 Win=61320 Len=0
47	2.834383	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=20441 Win=61320 Len=0
48	2.834384	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=32121 Win=54020 Len=0
49	2.834450	192.168.0.191	147.32.200.238	FTP-D..	35094 FTP Data: 35040 bytes (PORT) (STOR test.txt)
50	2.834654	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=33581 Win=52560 Len=0
51	2.834655	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=35041 Win=51100 Len=0
52	2.834655	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=36501 Win=51100 Len=0
53	2.834655	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=37961 Win=49640 Len=0
54	2.834655	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=39421 Win=49640 Len=0
55	2.834656	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=40881 Win=62780 Len=0

Img 7. Vysílací stanice zvětší hodnotu okna o n-segmentu

- Mechanismus řízení datového toku pomocí pole Window Size v hlavičkách TCP segmentů:

TCP využívá k řízení toku dat Klouzavé okno. Od ostatních protokolů pro řízení se však liší oddělením funkce potvrzování přijatých dat od přidělování kreditů pro vysílání. V hlavičce TCP segmentu jsou důležitá pole, která slouží pro řízení toku dat. Jsou to pole Sekvenčního čísla SN, pole Potvrzovacího čísla AN, a pole Klouzavého okna W.

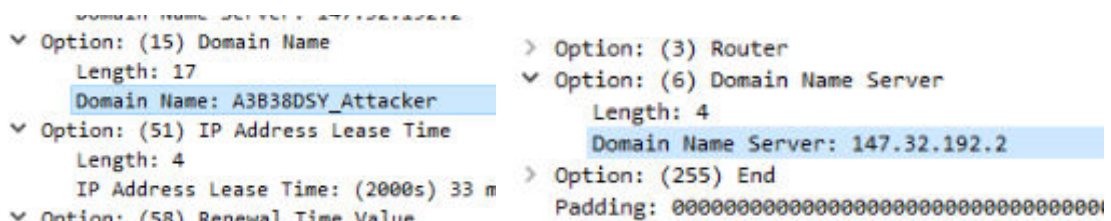


Img 8. Hlavička TCP segmentu

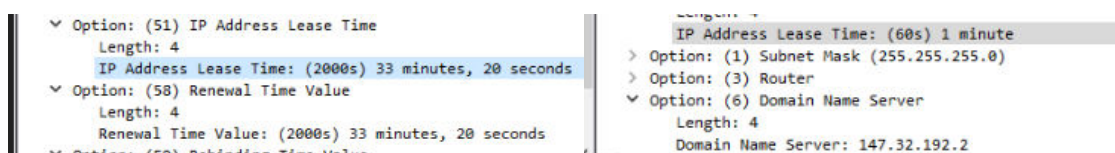
Přijímací stanice přijaté TCP segmenty potvrdí jednotlivě či kumulativně vysláním potvrzovacího segmentu, případně využitím datového segmentu zasílaného v opačném směru. Vysílací stanice obdrží tento potvrzovací segment a z pole AN přečte SN očekávaného TCP segmentu. V potvrzovacím segmentu se také nastavuje velikost Klouzavého okna W, ve kterém přijímací stanice přiděluje vysílací stanici další kredity. Přijímací stanice má možnost potvrdit přijaté segmenty, ale vysílací stanici nové kredity nepřidělit

1.7. DHCP Útok:

- Pro online výuku pouze analyzujte trace dostupný z Moodle. Místo přednastavených filtrů aplikujte klíčové slovo dhcp ekvivalentní přednastavenému filtru „DHCP“ a *filtr dns && dns.qry.name==www.seznam.cz && !(eth.src == 00:0c:42:ef:e0:f2)*, který odpovídá filtru „DNS (Attack)“:



Img 9. Attacker domain jmeno místo standartní adresy



Img 10. Čas připojení při útoku

1.8. DHCP Útok:

- Pro online výuku pouze analyzujte trace dostupný z moodle. Místo přednastavených filtrů aplikujte klíčové slovo arp ekvivalentní přednastavenému filtru „ARP“ a filtr *dns && dns.qry.name==www.seznam.cz && !(eth.src == 00:0c:42:ef:e0:f2)*, který odpovídá filtru „DNS (Attack)“:

25	0.558127	Shenzhen_24:a6:3a	Broadcast	ARP	42 Who has 192.168.88.1? Tell 192.168.88.251
26	0.558212	Routerbo_ef:e0:f2	Shenzhen_24:a6:3a	ARP	60 192.168.88.1 is at 00:0c:42:ef:e0:f2
30	0.735992	Shenzhen_24:a6:3a	Broadcast	ARP	42 Who has 192.168.88.251? (ARP Probe)
33	0.799811	Shenzhen_24:a6:3a	Broadcast	ARP	42 Who has 192.168.88.1? Tell 192.168.88.251
34	0.799918	Routerbo_ef:e0:f2	Shenzhen_24:a6:3a	ARP	60 192.168.88.1 is at 00:0c:42:ef:e0:f2
88	1.729342	Shenzhen_24:a6:3a	Broadcast	ARP	42 Who has 192.168.88.251? (ARP Probe)
95	2.739460	Shenzhen_24:a6:3a	Broadcast	ARP	42 Who has 192.168.88.251? (ARP Probe)
406	3.738379	Shenzhen_24:a6:3a	Broadcast	ARP	42 ARP Announcement for 192.168.88.251
4782	8.765683	Routerbo_ef:e0:f2	Shenzhen_24:a6:3a	ARP	60 Who has 192.168.88.251? Tell 192.168.88.1
4783	8.765697	Shenzhen_24:a6:3a	Routerbo_ef:e0:f2	ARP	42 192.168.88.251 is at 50:af:73:24:a6:3a

< >

> Frame 26: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{48104DA0-975A-4446-A32C-2D92C0983E2D},
> Ethernet II, Src: Routerbo_ef:e0:f2 (00:0c:42:ef:e0:f2), Dst: Shenzhen_24:a6:3a (50:af:73:24:a6:3a)
> Address Resolution Protocol (reply)

Img 11. Běžné připojení

123	3.853749	Giga-Byt_5b:25:80	Broadcast	ARP	60 Gratuitous ARP for 192.168.88.1 (Reply) (duplica...
733	4.842131	Giga-Byt_5b:25:80	Broadcast	ARP	60 Gratuitous ARP for 192.168.88.1 (Reply) (duplica...
735	5.356740	Giga-Byt_5b:25:80	Broadcast	ARP	60 Gratuitous ARP for 192.168.88.1 (Reply) (duplica...
744	6.194168	Giga-Byt_5b:25:80	Broadcast	ARP	60 Gratuitous ARP for 192.168.88.1 (Reply) (duplica...
748	6.702374	Giga-Byt_5b:25:80	Broadcast	ARP	60 Gratuitous ARP for 192.168.88.1 (Reply) (duplica...
1302	7.225971	Giga-Byt_5b:25:80	Broadcast	ARP	60 Gratuitous ARP for 192.168.88.1 (Reply) (duplica...
1359	7.737881	Giga-Byt_5b:25:80	Broadcast	ARP	60 Gratuitous ARP for 192.168.88.1 (Reply) (duplica...
1372	8.273323	Giga-Byt_5b:25:80	Broadcast	ARP	60 Gratuitous ARP for 192.168.88.1 (Reply) (duplica...
1416	8.860529	Routerbo_ef:e0:f2	Shenzhen_24:a6:3a	ARP	60 Who has 192.168.88.251? Tell 192.168.88.1
1417	8.860563	Shenzhen_24:a6:3a	Routerbo_ef:e0:f2	ARP	42 192.168.88.251 is at 50:af:73:24:a6:3a

> Frame 123: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{48104DA0-975A-4446-A32C-2D92C0983E2D},
> Ethernet II, Src: Giga-Byt_5b:25:80 (e0:d5:5e:5b:25:80), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (reply/gratuitous ARP)
v [Duplicate IP address detected for 192.168.88.1 (e0:d5:5e:5b:25:80) - also in use by 00:0c:42:ef:e0:f2 (frame 26)]
v [Frame showing earlier use of IP address: 26]
v [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.88.1)]
[Seconds since earlier frame seen: 3]

Img 12. Falešná IP adresa útočníka