

KVD/PSDSB - Seminární úkol 2

Vypracovaný seminární úkol odevzdejte prostřednictvím modulu pro odevzdání. Soubor pojmenujte ve tvaru **PrijmeniCV2** a odevzdejte v některém z formátů textových editorů (.doc, .docx, .odt) či ve formátu PDF.

Poznámka: Výsledky zpracovávejte v tomto dokumentu. Vhodně vkládejte texty screenshoty obrazovky a výpočty.

1) Přiřaďte následující pojmy do tabulky ke správné vrstvě ISO/OSI modelu, na které bychom je obvykle našli nebo na které se s nimi pracuje.

Aplikační	FTP DNS HTTP SMTP
Prezentační	komprese dat šifrování dat
Relační	
Transportní	TCP UDP Segment
Síťová	IP adresa 0.0.0.0 192.16.55.8 IPv4 adresa paket
Linková	fyzická adresa ff:ff:ff:ff:ff:ff rámec
Fyzická	bit

- 2) Vyberte si libovolné 3 protokoly, které se objevovaly v komunikacích v úkolu 1. Vyhledejte, v jakém/jakých RFC dokumentu/dokumentech jsou popsány a stručně shrňte, co je obsahem RFC dokumentu pro daný protokol.

HTTP - RFC 2616

- slouží pro přenos hypertextových dokumentů
- Dokument pojednává převážně o protokolu HTTP 1.1
- Pracuje na aplikační vrstvě
- Prvotní verze 0.9 sloužila pro jednoduchý přenos dat

ICMP - RFC 792

- Je rozšíření internetového protokolu(IP) definovaného RFC 792 a protokolu hlášení chyb pro zprávy TCP / IP.
- Existují 2 verze ICMPv4 pro IPv4 a ICMPv6 pro IPv6
- ICMP zpráva obsahuje TYPE, CODE a CHECKSUM zprávu, která pomáhá identifikovat odpověď zařízení.
- základem je Internetový protokol (IP), který se používá pro datagramy host-to-host služby v systému propojených sítí nazvaných Catenet

DNS - RFC1034

- Historie doménových jmen
- Cíle návrhu DNS
- Předpoklady o použití
- Prvky DNS
- Technické pokyny pro použití

- 3) Pomocí aplikace Wireshark zjistěte, jaké protokoly se podílejí na následujících komunikacích a jaké informace jsou využívány během procesu zapouzdření na vrstvách ISO/OSI modelu (zaměřte se na linkovou, fyzickou a transportní vrstvu). Uvádějte konkrétní údaje. Zároveň uveďte, o jaký síťový provoz se jedná.

a. ping www.kvd.zcu.cz

Proběhl DNS dotaz, kde se přeložila mnou zadaná doména na IP adresu, na kterou se provedl dotaz (request) a přišla z ní nějaká odpověď (response).

Handwritten notes: "request" with a blue arrow pointing to the first packet (688) and "response" with a red arrow pointing to the second packet (690).

688	30.476746	147.228.165.160	147.228.3.3	DNS	71 Standard query 0xb827 A youtube.com
690	30.494781	147.228.3.3	147.228.165.160	DNS	342 Standard query response 0xb827 A youtube.com A 172.217.23.206 NS ns1.google.com NS ns2.google.com...

K příkazu ping probíhá ještě jeden protokol, a sice ICMP, který posílá ICMP zprávy „Echo Request“ (a očekává příjem zprávy „Echo Reply“), aby určil, zda je cílový počítač dosažitelný a jak dlouho paketům trvá, než se dostanou k cíli a zpět (tj. měří latenci)

112	5.759656	147.228.165.160	172.217.23.206	ICMP	74 Echo (ping) request id=0x0001, seq=78/19968,
113	5.761815	172.217.23.206	147.228.165.160	ICMP	74 Echo (ping) reply id=0x0001, seq=78/19968,
127	6.762296	147.228.165.160	172.217.23.206	ICMP	74 Echo (ping) request id=0x0001, seq=79/20224,
128	6.764452	172.217.23.206	147.228.165.160	ICMP	74 Echo (ping) reply id=0x0001, seq=79/20224,
141	7.770764	147.228.165.160	172.217.23.206	ICMP	74 Echo (ping) request id=0x0001, seq=80/20480,
142	7.772956	172.217.23.206	147.228.165.160	ICMP	74 Echo (ping) reply id=0x0001, seq=80/20480,
163	8.777949	147.228.165.160	172.217.23.206	ICMP	74 Echo (ping) request id=0x0001, seq=81/20736,
164	8.780131	172.217.23.206	147.228.165.160	ICMP	74 Echo (ping) reply id=0x0001, seq=81/20736,

b. ping 147.228.52.200

```
PING 147.228.52.200 (147.228.52.200): 56 data bytes
64 bytes from 147.228.52.200: icmp_seq=0 ttl=63 time=2.346 ms
64 bytes from 147.228.52.200: icmp_seq=1 ttl=63 time=3.665 ms
64 bytes from 147.228.52.200: icmp_seq=2 ttl=63 time=1.637 ms
64 bytes from 147.228.52.200: icmp_seq=3 ttl=63 time=2.657 ms
64 bytes from 147.228.52.200: icmp_seq=4 ttl=63 time=1.782 ms
```

```
--- 147.228.52.200 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.637/2.417/3.665/0.726 ms
```

No.	Time	Source	Destination	Protocol	Length	Info
249	3.237184	147.228.131.24	147.228.52.200	ICMP	98	Echo (ping) request id=0xf086, seq=0/0, ttl=64 (reply in 250)
250	3.239911	147.228.52.200	147.228.131.24	ICMP	98	Echo (ping) reply id=0xf086, seq=0/0, ttl=63 (request in 249)
326	4.237313	147.228.131.24	147.228.52.200	ICMP	98	Echo (ping) request id=0xf086, seq=1/256, ttl=64 (reply in 327)
327	4.245205	147.228.52.200	147.228.131.24	ICMP	98	Echo (ping) reply id=0xf086, seq=1/256, ttl=63 (request in 326)
409	5.239042	147.228.131.24	147.228.52.200	ICMP	98	Echo (ping) request id=0xf086, seq=2/512, ttl=64 (reply in 410)
410	5.240560	147.228.52.200	147.228.131.24	ICMP	98	Echo (ping) reply id=0xf086, seq=2/512, ttl=63 (request in 409)
539	6.242947	147.228.131.24	147.228.52.200	ICMP	98	Echo (ping) request id=0xf086, seq=3/768, ttl=64 (reply in 540)
540	6.244806	147.228.52.200	147.228.131.24	ICMP	98	Echo (ping) reply id=0xf086, seq=3/768, ttl=63 (request in 539)
639	7.243540	147.228.131.24	147.228.52.200	ICMP	98	Echo (ping) request id=0xf086, seq=4/1024, ttl=64 (reply in 640)
640	7.245953	147.228.52.200	147.228.131.24	ICMP	98	Echo (ping) reply id=0xf086, seq=4/1024, ttl=63 (request in 639)

Zde neprobíhá překlad domény pomocí DNS, protože již provádíme ping na samotnou IP adresu.

ICMP komunikace zde však probíhá. Princip popsán u úkolu výše.

c. traceroute google.com

Jedná se o příkaz, který nám ukáže cestu paketů přes veškeré uzly, které na cestě cílové adrese projde. Používá se právě na odhalení chyb v přenosu.

```
traceroute to google.com (172.217.23.206), 64 hops max, 72 byte packets
 1  ic-sp1-gw (147.228.128.1)  2.236 ms  1.453 ms  1.483 ms
 2  r140-pm (147.228.200.2)  1.900 ms  7.515 ms  2.099 ms
 3  195.113.235.109 (195.113.235.109)  5.644 ms  5.349 ms  7.351 ms
 4  r2-r93.cesnet.cz (195.113.157.70)  6.284 ms  3.504 ms  4.100 ms
 5  108.170.245.33 (108.170.245.33)  3.595 ms  3.729 ms  3.669 ms
 6  108.170.238.159 (108.170.238.159)  3.412 ms  55.056 ms  3.116 ms
 7  prg03s05-in-f14.1e100.net (172.217.23.206)  3.104 ms  3.303 ms  3.134 ms
```

Každý hop se provede třikrát, to lze dokázat podle časů u jednotlivých routů.

No.	Time	Source	Destination	Protocol	Length	Info
331	3.084000	147.228.131.24	172.217.23.206	ICMP	86	Echo (ping) request id=0x8740, seq=1/256, ttl=1 (no response found!)
332	3.085238	147.228.128.1	147.228.131.24	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
333	3.085975	147.228.131.24	172.217.23.206	ICMP	86	Echo (ping) request id=0x8740, seq=2/512, ttl=1 (no response found!)
334	3.087447	147.228.128.1	147.228.131.24	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
335	3.087534	147.228.131.24	172.217.23.206	ICMP	86	Echo (ping) request id=0x8740, seq=3/768, ttl=1 (no response found!)
336	3.089194	147.228.128.1	147.228.131.24	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
337	3.089312	147.228.131.24	172.217.23.206	ICMP	86	Echo (ping) request id=0x8740, seq=4/1024, ttl=2 (no response found!)
338	3.091151	147.228.200.2	147.228.131.24	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
339	3.091939	147.228.131.24	172.217.23.206	ICMP	86	Echo (ping) request id=0x8740, seq=5/1280, ttl=2 (no response found!)
340	3.093632	147.228.200.2	147.228.131.24	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
341	3.093800	147.228.131.24	172.217.23.206	ICMP	86	Echo (ping) request id=0x8740, seq=6/1536, ttl=2 (no response found!)
342	3.096026	147.228.200.2	147.228.131.24	ICMP	114	Time-to-live exceeded (Time to live exceeded in transit)
343	3.097198	147.228.131.24	172.217.23.206	ICMP	86	Echo (ping) request id=0x8740, seq=7/1792, ttl=3 (no response found!)
344	3.101088	195.113.235.109	147.228.131.24	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
346	3.102049	147.228.131.24	172.217.23.206	ICMP	86	Echo (ping) request id=0x8740, seq=8/2048, ttl=3 (no response found!)
347	3.109144	195.113.235.109	147.228.131.24	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
348	3.109274	147.228.131.24	172.217.23.206	ICMP	86	Echo (ping) request id=0x8740, seq=9/2304, ttl=3 (no response found!)
349	3.117194	195.113.235.109	147.228.131.24	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

d. ping 127.0.0.1

Localhost odkazuje na speciální vyhrazenou IP adresu 127.0.0.1 v protokolu IPv4 nebo IPv6

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.059 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.090 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.090 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.157 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.088 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.104 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.107 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.126 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.097 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.086 ms

--- 127.0.0.1 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.059/0.100/0.157/0.025 ms
```

Pomocí localhost (127.0.0.1) je možno prověřit stav TCP/IP stacku vlastního počítače. Pokud se provede příkaz PING na localhost a tento odpovídá, je zřejmé, že TCP/IP stack funguje jak má. Pokud tento příkaz je bez odezvy, je v systému chyba.

e. nslookup centrum.cz

Zvolil jsem adresu adobe.com, centrum.cz se mi při testování nezobrazovalo, byla již uložena v cache paměti.

Slouží pro dotazování na doménové jméno, IP adresu mapování nebo pro jiné vlastnosti DNS záznamu.

Utilita Lookup byla spuštěna...

centrum.cz -> 46.255.231.106

No.	Time	Source	Destination	Protocol	Length	Info
381	3.990589	147.228.131.24	147.228.3.3	DNS	69	Standard query 0xc349 A adobe.com
382	4.003281	147.228.3.3	147.228.131.24	DNS	486	Standard query response 0xc349 A adobe.com A 192.147.130.204 A 193.104.215.58 NS

Proběhl DNS dotaz, kde se přeložila mnou zadaná doména na IP adresu, na kterou se provedl dotaz (request) a přišla z ní nějaká odpověď (response)

f. zadání webové adresy www.cisco.com do prohlížeče

294	3.457740	147.228.131.24	147.228.3.3	DNS	73	Standard query 0xc98b A www.cisco.com
297	3.508026	147.228.3.3	147.228.131.24	DNS	551	Standard query response 0xc98b A www.cisco.com CNAME www.cisco.com.akadns.net

Znovu zde proběhl DNS dotaz na adresu www.cisco.com

▼ Answers
▼ www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
Name: www.cisco.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 811 (13 minutes, 31 seconds)
Data length: 26
CNAME: www.cisco.com.akadns.net
▼ www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
Name: www.cisco.com.akadns.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 211 (3 minutes, 31 seconds)
Data length: 26
CNAME: wwwds.cisco.com.edgekey.net
▼ wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
Name: wwwds.cisco.com.edgekey.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 8611 (2 hours, 23 minutes, 31 seconds)
Data length: 42
CNAME: wwwds.cisco.com.edgekey.net.globalredir.akadns.net
▼ wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
Name: wwwds.cisco.com.edgekey.net.globalredir.akadns.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1111 (18 minutes, 31 seconds)
Data length: 24
CNAME: e2867.dsca.akamaiedge.net

Když se podíváme do hlavičky odpovědi DNS dotazu, uvidíme, že jich je tam 5. První 4 jsou typu CNAME, kde každý alias zastupuje pravý název. Takže například v první odpovědi je alias pro www.cisco.akadns.net www.cisco.com atd.

```
▼ e2867.dsca.akamaiedge.net: type A, class IN, addr 104.127.50.83
  Name: e2867.dsca.akamaiedge.net
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 20 (20 seconds)
  Data length: 4
  Address: 104.127.50.83
```

Až 5. a tedy poslední odpověď je typu A, dotaz je tedy ze zdrojové adresy. Vidíme v ní, že e2867.dsca.akamaiedge.net je opravdová zdrojová adresa.