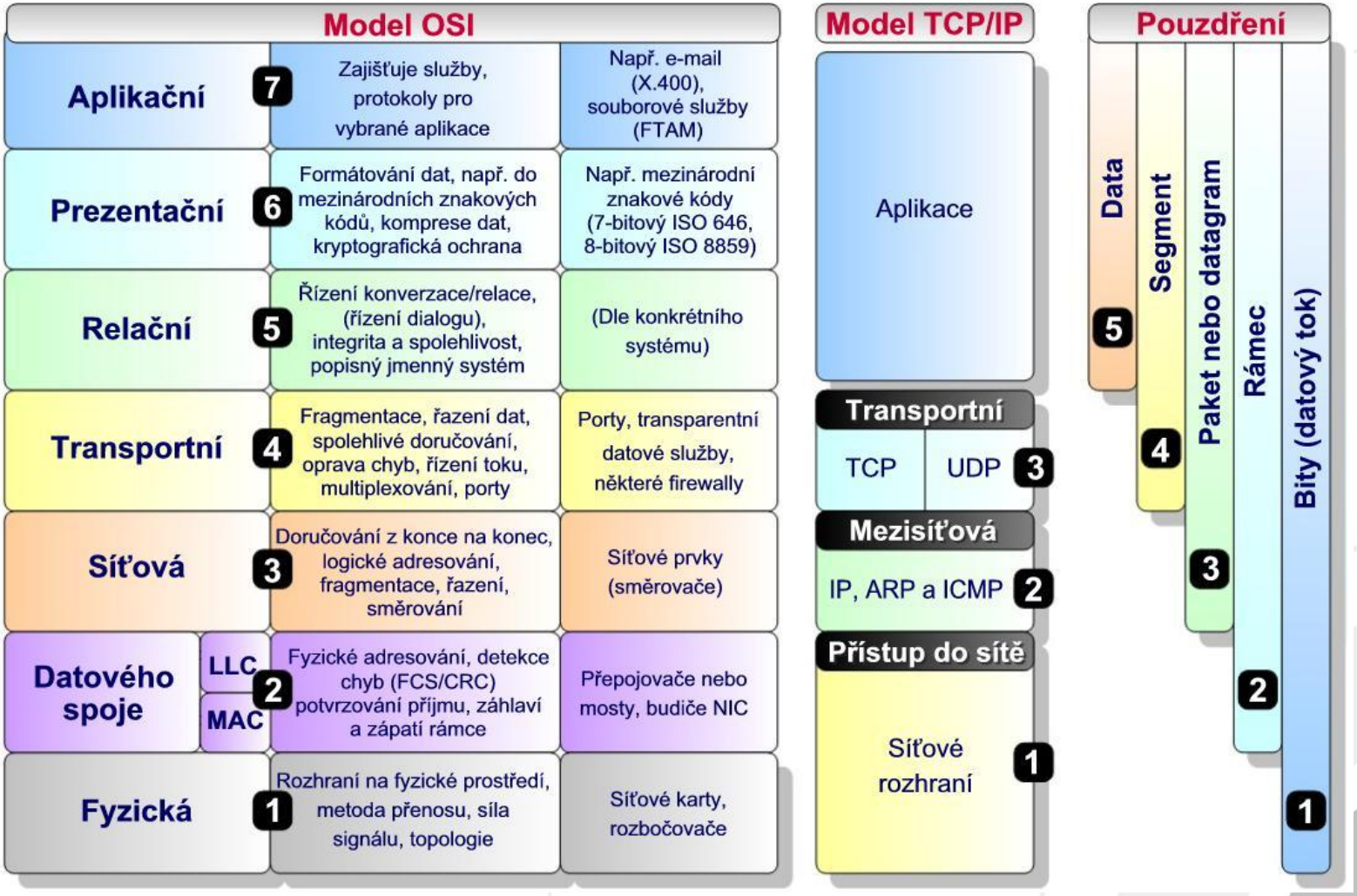
Cvičení 6

4IZ110 - Informační a komunikační technologie

Obsah

- Transportní protokoly
- TCP
- TCP útoky
- UDP
- Domácí úkol na příště

Transportní protokoly



Síťové porty

- Slouží k rozlišení jednotlivých služeb v rámci jedné IP adresy

  FTP[:20-21]
  DNS[:53]
  HTTPS[:443]
  SSH[:22]
  LoL[:5000 – 5500]

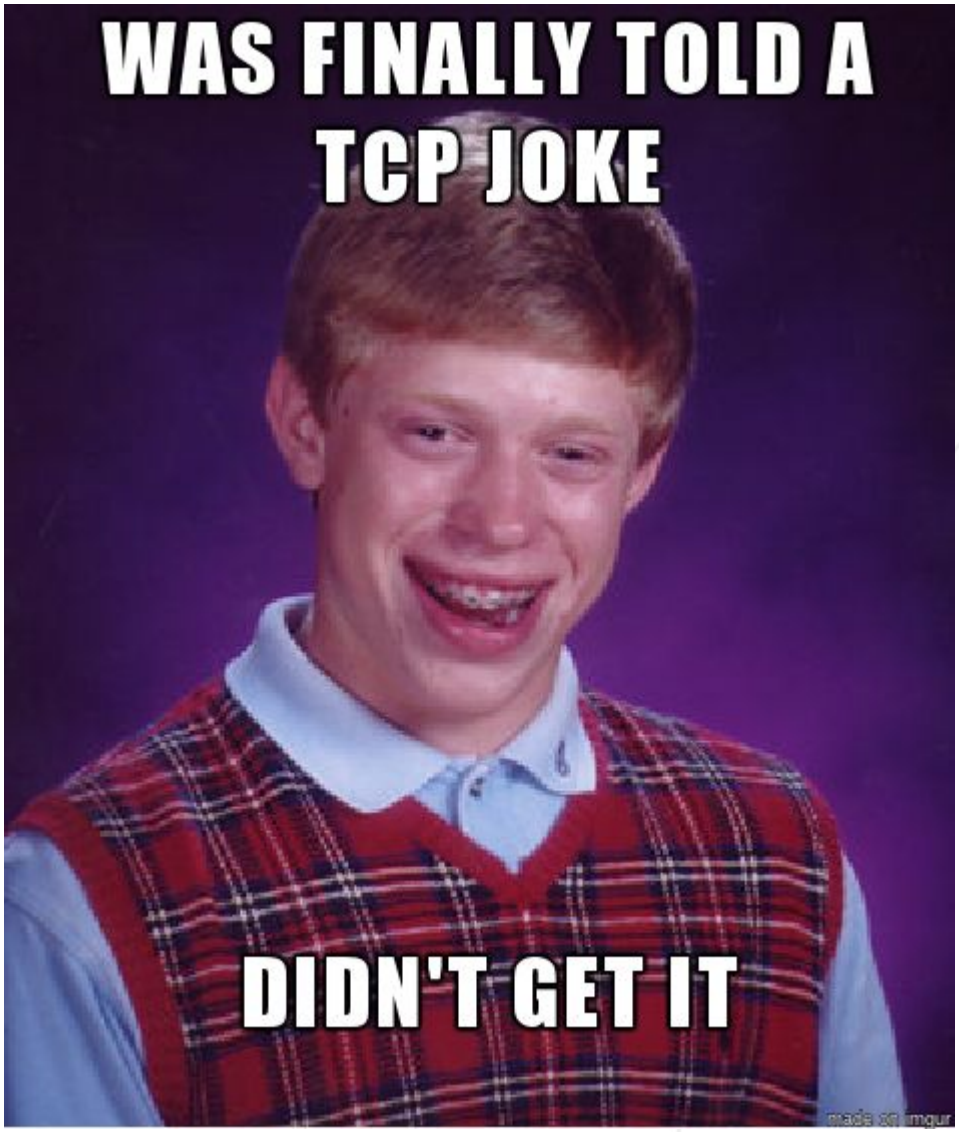
- Typicky seznam.cz:443

- Dělí se do skupin (16bitů):
  - Známé porty (0 – 1023) – vyhrazeno pro nejběžnější služby
  - Registrované porty (1024 – 49151) – je doporučena registrace u společnosti ICANN
  - Dynamické a soukromé porty (49152 – 65535)

Síťové sokety

- Nadstavba nad transportními protokoly
- Reprezentují jedno síťové spojení
- Mají různé stavy:
  - LISTEN
  - ESTABLISHED
  - TIME_WAIT
  - CLOSE_WAIT

TCP – Transmission Control Protocol



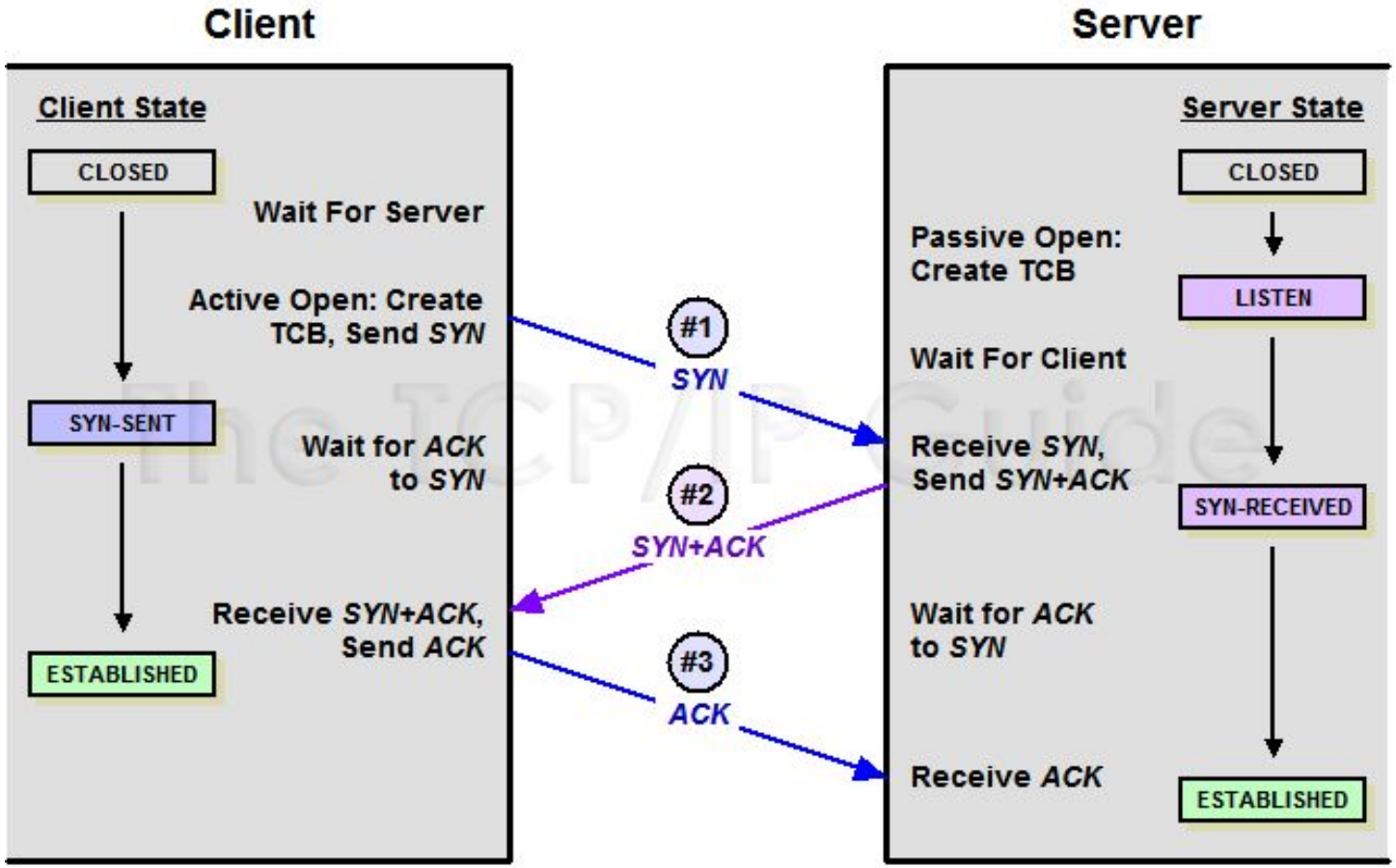
TCP – Transmission Control Protocol

- **Přenosový protokol s ochranou proti ztrátě dat při přenosu**

- Protože TCP je spojovaná transportní služba, musí se před odesíláním dat navázat spojení mezi klientem a serverem. K tomu slouží **trojcestný handshaking** (three-way handshake). V průběhu navazování spojení se obě strany dohodnou na **číslu sekvence** a **potvrzovacím čísle**. Pro navázání spojení se odesílají datagramy s nastavenými příznaky SYN a ACK.

- Toto spojení se následně musí i ukončit pakety FIN a ACK, aby se uvolnila čísla portů
- Užití http, ftp, ssh…

TCP - handshake



TCP - handshake

tcp.stream eq 13

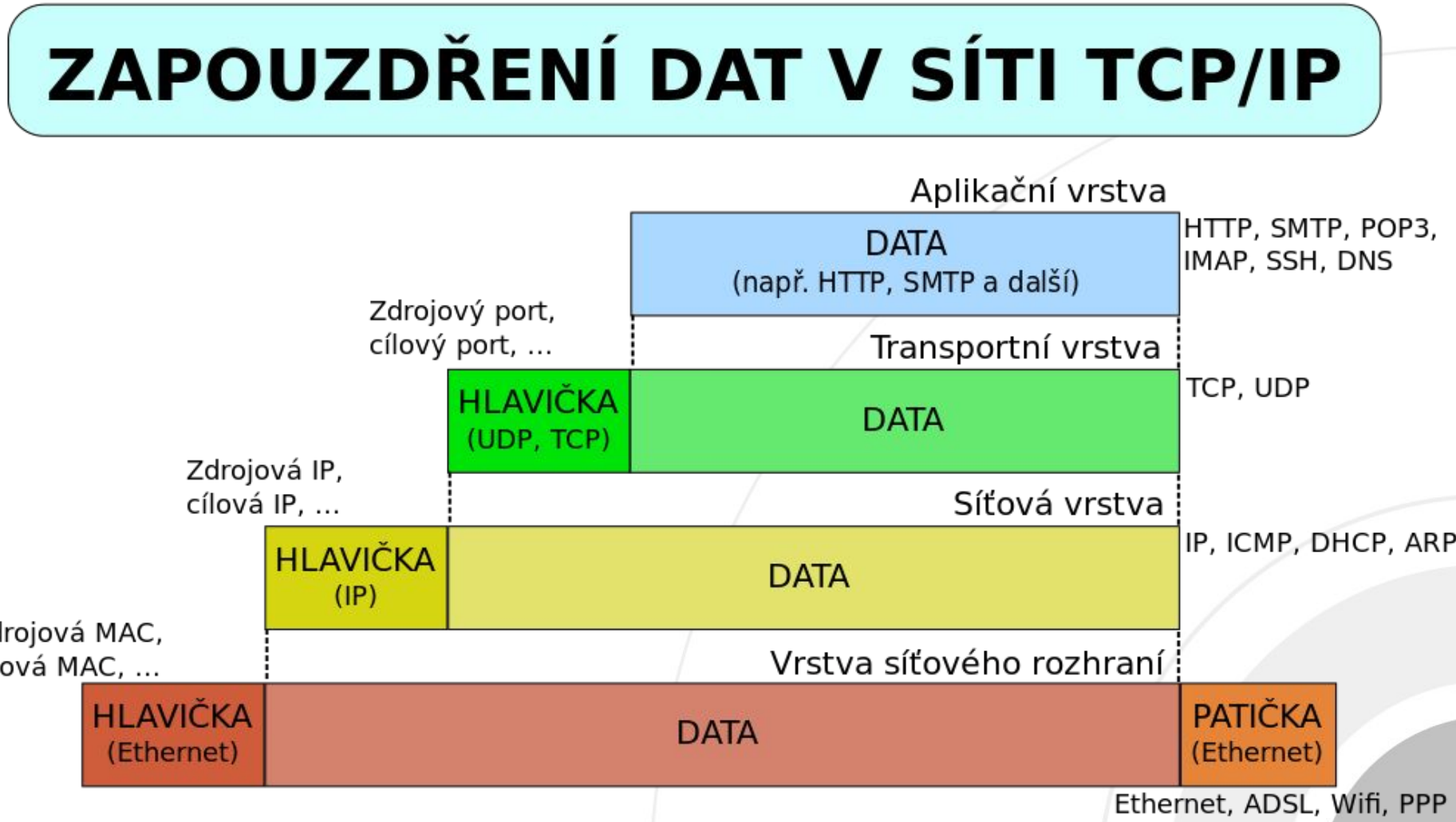
No.	Time	Source	Destination	Protocol	Length	Info
280	2.325440	146.102.147.177	77.75.76.72	TCP	66	18227 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
294	2.329678	77.75.76.72	146.102.147.177	TCP	66	443 → 18227 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1386 SACK_PERM=1 WS=128
300	2.330233	146.102.147.177	77.75.76.72	TCP	54	18227 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
301	2.330975	146.102.147.177	77.75.76.72	TLSv1.2	253	Client Hello
319	2.338807	77.75.76.72	146.102.147.177	TCP	60	443 → 18227 [ACK] Seq=1 Ack=200 Win=30336 Len=0
331	2.340101	77.75.76.72	146.102.147.177	TLSv1.2	1440	Server Hello
332	2.340102	77.75.76.72	146.102.147.177	TCP	1440	443 → 18227 [ACK] Seq=1387 Ack=200 Win=30336 Len=1386 [TCP segment of a reassembled PDU]
333	2.340102	77.75.76.72	146.102.147.177	TLSv1.2	413	Certificate, Server Key Exchange, Server Hello Done
336	2.340332	146.102.147.177	77.75.76.72	TCP	54	18227 → 443 [ACK] Seq=200 Ack=3132 Win=66304 Len=0
360	2.352390	146.102.147.177	77.75.76.72	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
367	2.355572	77.75.76.72	146.102.147.177	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
368	2.355573	77.75.76.72	146.102.147.177	TLSv1.2	123	Application Data
371	2.355697	146.102.147.177	77.75.76.72	TCP	54	18227 → 443 [ACK] Seq=326 Ack=3459 Win=66048 Len=0

```
> Frame 280: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: IntelCor_26:ec:06 (f8:59:71:26:ec:06), Dst: Cisco_ff:fc:10 (00:08:e3:ff:fc:10)
> Internet Protocol Version 4, Src: 146.102.147.177, Dst: 77.75.76.72
> Transmission Control Protocol, Src Port: 18227, Dst Port: 443, Seq: 0, Len: 0
```

TCP – handshake (netstat –n)

```
TCP    146.102.147.177:18223  77.75.78.146:443       ESTABLISHED
TCP    146.102.147.177:18224  77.75.78.146:443       ESTABLISHED
TCP    146.102.147.177:18225  149.202.200.33:443     ESTABLISHED
TCP    146.102.147.177:18227  77.75.76.72:443        ESTABLISHED
TCP    146.102.147.177:18242  146.102.18.84:6690     SYN_SENT
TCP    146.102.147.177:18243  146.102.18.84:6690     SYN_SENT
TCP    146.102.147.177:18245  81.0.212.200:443       ESTABLISHED
TCP    146.102.147.177:31848  0.0.0.0:0              LISTENING
```

TCP – zapouzdření dat



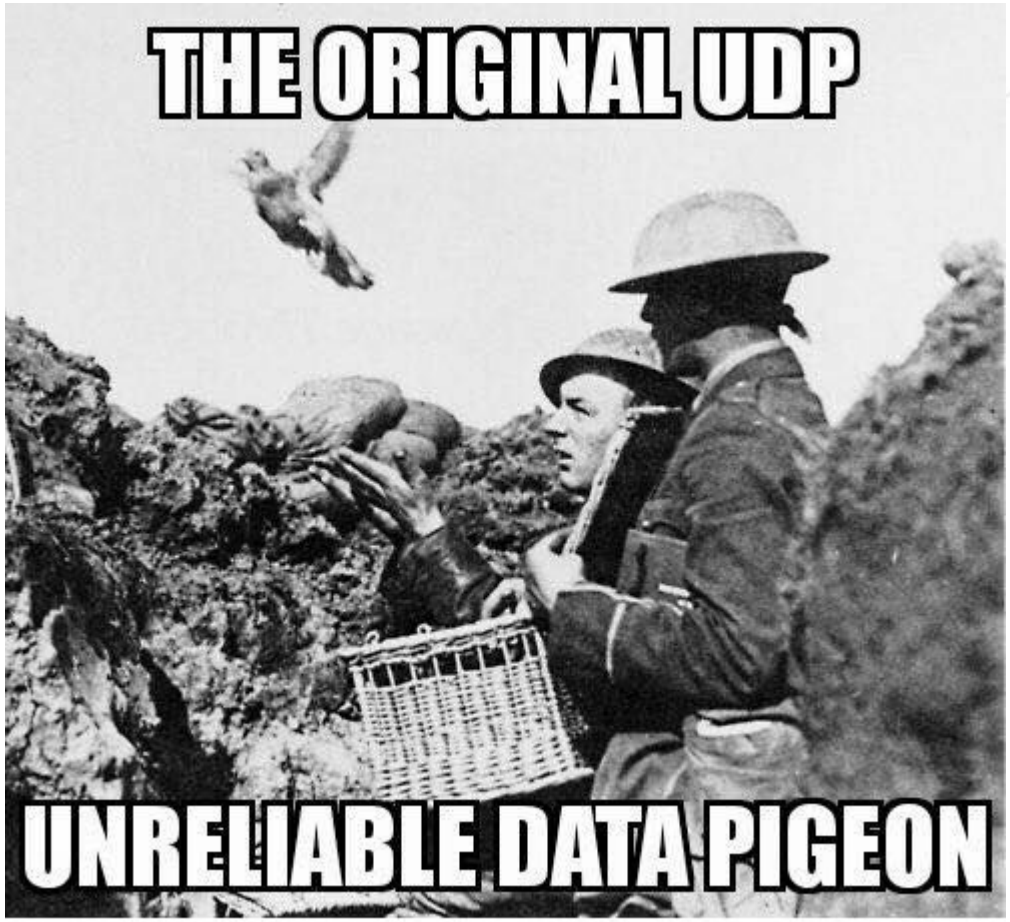
TCP - retransmission

265	2.320051	146.102.147.177	77.75.78.146	TCP	66 18223 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
274	2.324781	77.75.78.146	146.102.147.177	TCP	66 443 → 18223 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1386 SACK_PERM=1 WS=512
277	2.325041	146.102.147.177	77.75.78.146	TCP	54 18223 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
287	2.327290	146.102.147.177	77.75.78.146	TLSv1.2	255 Client Hello
307	2.334215	77.75.78.146	146.102.147.177	TCP	60 443 → 18223 [ACK] Seq=1 Ack=202 Win=30720 Len=0
328	2.340100	77.75.78.146	146.102.147.177	TLSv1.2	1440 Server Hello
329	2.340100	77.75.78.146	146.102.147.177	TCP	1440 443 → 18223 [ACK] Seq=1387 Ack=202 Win=30720 Len=1386 [TCP segment of a reassembled PDU]
330	2.340101	77.75.78.146	146.102.147.177	TLSv1.2	407 Certificate, Server Key Exchange, Server Hello Done
335	2.340287	146.102.147.177	77.75.78.146	TCP	54 18223 → 443 [ACK] Seq=202 Ack=3126 Win=66304 Len=0
344	2.343549	77.75.78.146	146.102.147.177	TCP	407 [TCP Spurious Retransmission] 443 → 18223 [PSH, ACK] Seq=2773 Ack=202 Win=30720 Len=353[Reassembly error, protocol TCP: New fragment overlaps old data (retransmission?)]
354	2.344529	146.102.147.177	77.75.78.146	TCP	66 [TCP Dup ACK 335#1] 18223 → 443 [ACK] Seq=202 Ack=3126 Win=66304 Len=0 SLE=2773 SRE=3126
359	2.350335	146.102.147.177	77.75.78.146	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
364	2.354884	77.75.78.146	146.102.147.177	TLSv1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
444	2.395562	146.102.147.177	77.75.78.146	TCP	54 18223 → 443 [ACK] Seq=328 Ack=3384 Win=66048 Len=0

TCP - Útoky

- TCP sequence prediction attack
  - Útočník uhodne číslo sequence a přidá do přenosu svůj škodlivý kód
- Synflood
  - Útok typu DoS
  - Útočník podvrhne source ip adresu a otevírá tolik soketů pomocí SYN paketu na straně serveru, až server spadne

UDP – User Datagram Protocol



UDP – User Datagram Protocol

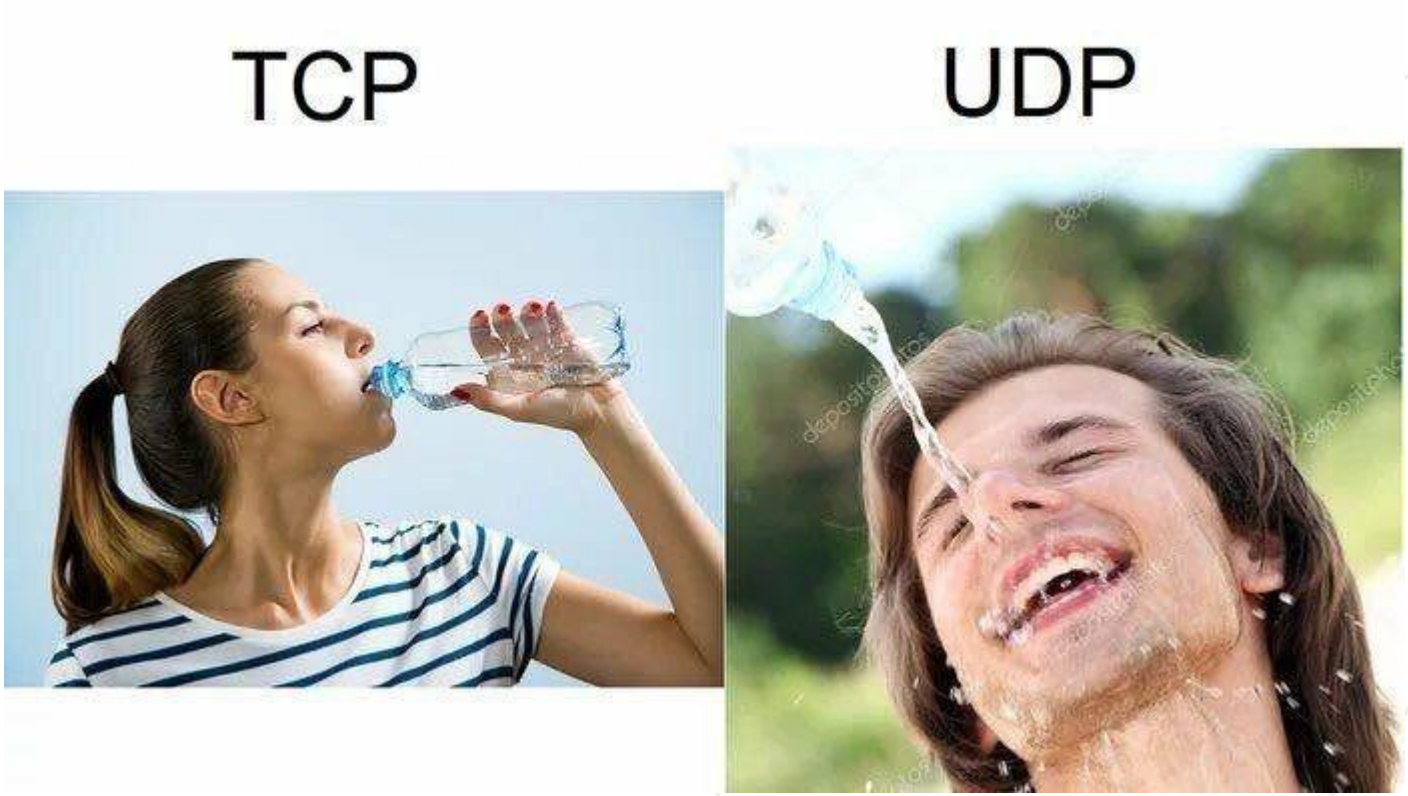
- Nezaručuje, zda se přenášený datagram neztratí, zda se nezmění pořadí doručených datagramů, nebo zda některý datagram nebude doručen vícekrát.
- Nevytváří spojení

- Protokol UDP je vhodný pro nasazení, které vyžaduje jednoduchost nebo pro aplikace pracující systémem otázka-odpověď (např. DNSProtokol UDP je vhodný pro nasazení, které vyžaduje jednoduchost nebo pro aplikace pracující systémem otázka-odpověď (např. DNS, sdílení souborů v LANProtokol UDP je vhodný pro nasazení, které vyžaduje jednoduchost nebo pro aplikace pracující systémem otázka-odpověď (např. DNS, sdílení souborů v LAN). Jeho bezstavovost je užitečná pro servery, které obsluhují mnoho klientů nebo pro nasazení, kde se počítá se ztrátami datagramů a není vhodné, aby se ztrácel čas novým odesíláním (starých)

UDP – User Datagram Protocol

2688	64.267210	fe80::8047:48fa:3ae6:6b7c	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
2689	64.439327	146.102.76.125	239.1.2.2	IGMPv2	46	Membership Report group 239.1.2.2
2690	64.493879	SamsungE_71:ff:d5	Broadcast	ARP	60	Who has 146.102.79.253? Tell 146.102.76.253
2691	64.493999	146.102.76.125	146.102.161.10	TCP	237	34914 → 50112 [PSH, ACK] Seq=18608 Ack=56446 Win=525312 Len=183
2692	64.494473	146.102.161.10	146.102.76.125	TCP	60	50112 → 34914 [ACK] Seq=56446 Ack=18791 Win=44800 Len=0
2693	64.502821	83.240.1.50	239.1.2.2	MPEG TS	1358	33333 → 33333 Len=1316
2694	64.504521	83.240.1.50	239.1.2.2	MPEG TS	1358	33333 → 33333 Len=1316
2695	64.505767	SamsungE_71:ff:63	Broadcast	ARP	60	Who has 146.102.79.253? Tell 146.102.77.25
2696	64.505768	SamsungE_2f:57:96	Broadcast	ARP	60	Who has 146.102.79.253? Tell 146.102.77.22
2697	64.506396	83.240.1.50	239.1.2.2	MPEG TS	1358	33333 → 33333 Len=1316 [MP2T fragment of a reassembled packet]
2698	64.508439	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2699	64.510182	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2700	64.511855	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2701	64.513744	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2702	64.515749	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2703	64.517555	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2704	64.519098	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2705	64.520890	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2706	64.522744	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet] [MP2T fragment of a reassembled packet]
2707	64.524724	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2708	64.526582	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2709	64.528392	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2710	64.530251	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2711	64.532115	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]
2712	64.533835	83.240.1.50	239.1.2.2	MPEG TS	1358	[MP2T fragment of a reassembled packet]

Rozdíl TCP a UDP



Rozdíl TCP a UDP

- TCP :
  - spolehlivost – TCP používá potvrzování o přijetí, opětovné posílání a překročení časového limitu. Pokud se jakákoliv data ztratí po cestě, server si je opětovně vyžádá. U TCP nejsou žádná ztracená data, jen pokud několikrát po sobě vyprší časový limit, tak je celé spojení ukončeno.
  - zachování pořadí – Pokud pakety dorazí ve špatném pořadí, TCP vrstva příjemce se postará o to, aby se některá data pozdržela a finálně je předala správně seřazená.
  - vyšší režie – TCP protokol potřebuje např. tři pakety pro otevření spojení, umožňuje to však zaručit spolehlivost celého spojení.

- UDP :
  - bez záruky – Protokol neumožňuje ověřit, jestli data došla zamýšlenému příjemci. Datagram se může po cestě ztratit. UDP nemá žádné potvrzování, přeposílání ani časové limity. V případě potřeby musí uvedené problémy řešit vyšší vrstva.
  - nezachovává pořadí – Při odeslání dvou zpráv jednomu příjemci nelze předvídat, v jakém pořadí budou doručeny.
  - jednoduchost – Nižší režie než u TCP (není zde řazení, žádné sledování spojení atd.).

Netstat

- Sledování otevřených stavů spojení na windows
- Netstat –a (Všechna spojení)
- Netstat –n (Spojení podle IP adresace)
- Netstat –s (Statistiky spojení)

Domácí úkol na příště

- Odchytejte a popište síťový provoz, který probíhá při startu libovolného operačního systému.
- Analýzu provozu (Známé protokoly – alespoň 5 příkladů) odevzdejte do připravené odevzdávárny ve studijním systému.
- 5 bodů

Děkuji za pozornost