Počítačové a komunikačné siete

Relačná, prezentačná vrstva
Úvod do transportnej vrstvy

Prednáška 3

STU FIIT

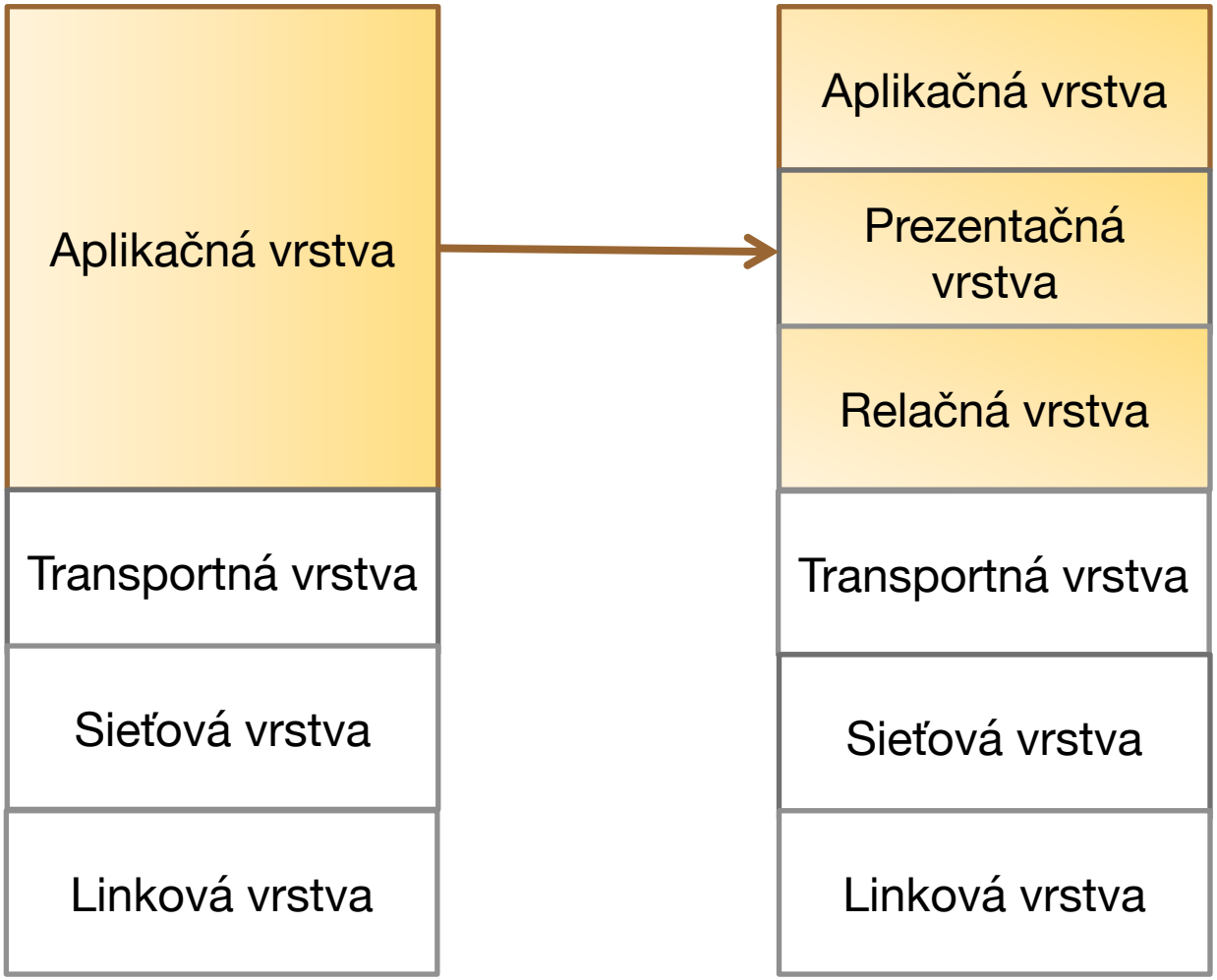
Opakovanie minulej prednášky

- HTTP
  - Používa TCP,IP,Ethernet/WiFi
- DHCP
  - Získanie IP adresy
- DNS
  - K menu získať IP adresu

Čo nás čaká na prednáške

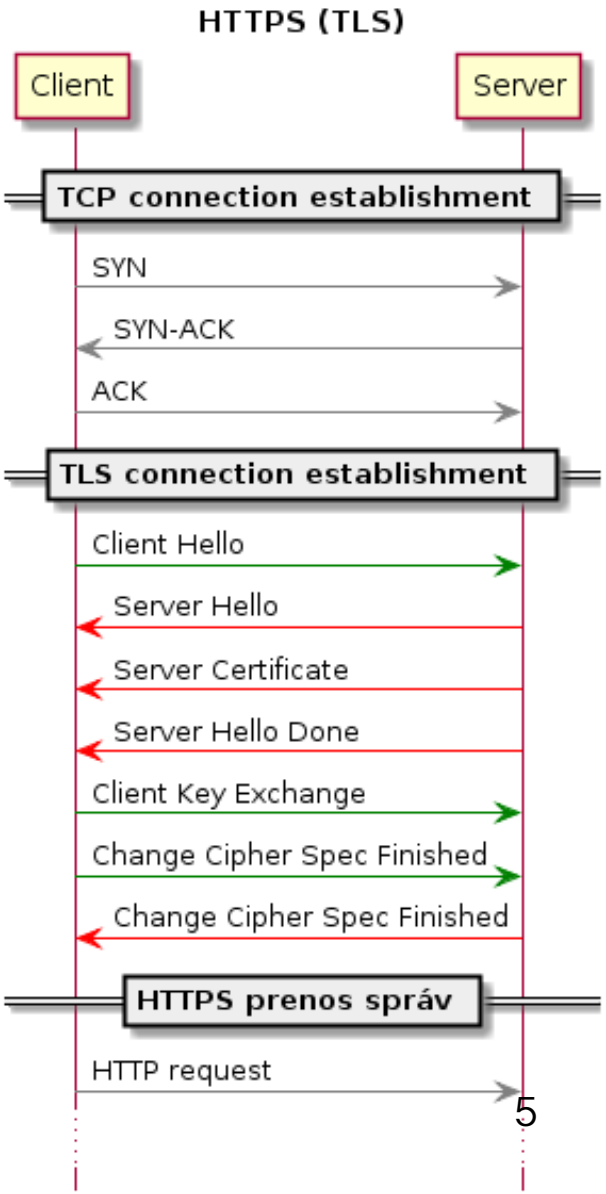
- Relačná vrstva (HTTPS)
- Prezentačná vrstva
- UDP (transportná vrstva)
  - CRC (Overenie správnosti prenosu)
- TCP (Transportná vrstva)
- Detaily používania wiresharku

Prezentačná a Relačná vrstva



Prezentačná vrstva

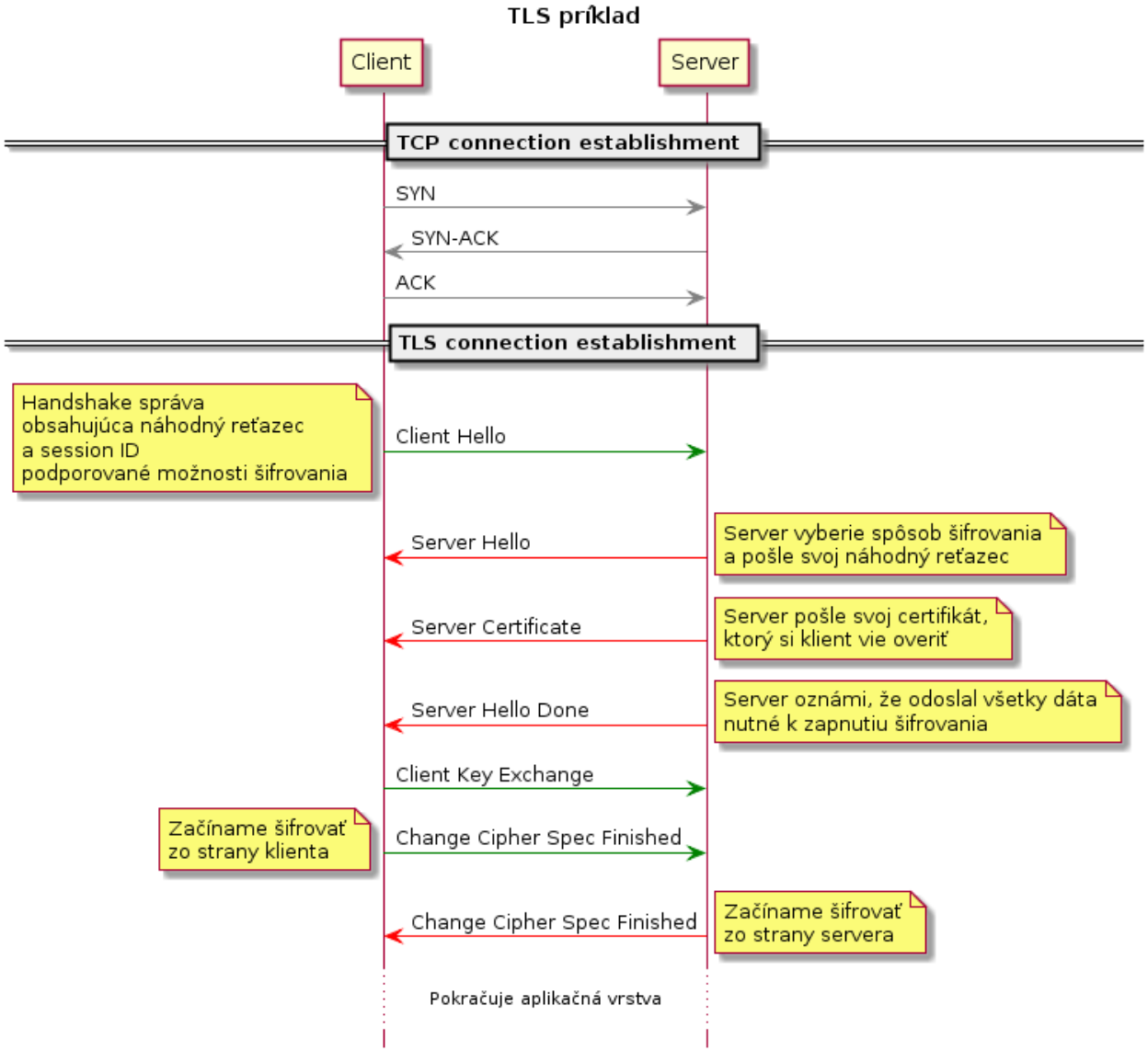
- Vytvára kontext na prenos dát medzi entitami aplikačnej vrstvy
- Príkladom je TLS, SSL
- Nie je aplikačný protokol



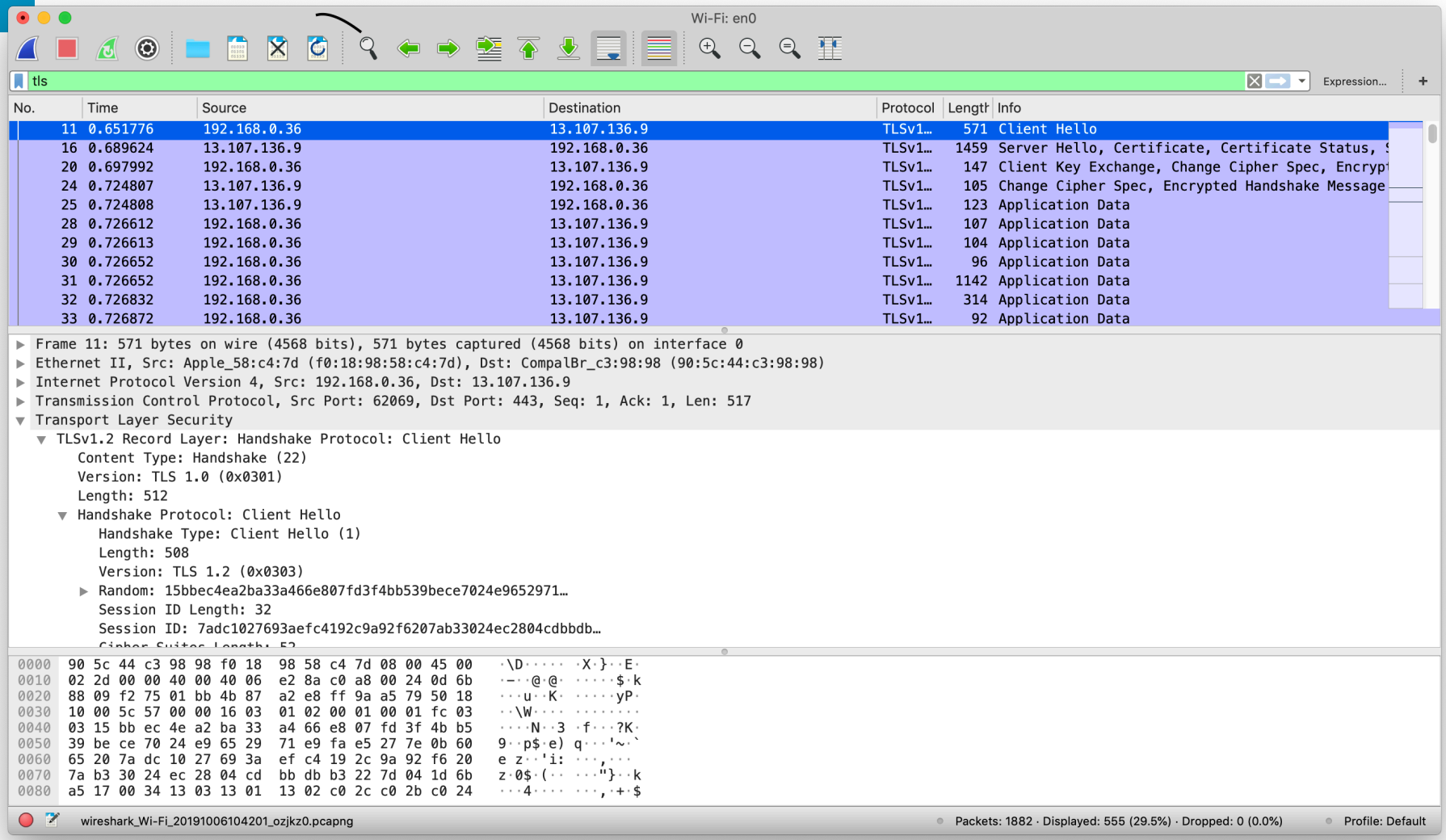
TLS

- Transport Layer Security
- Zabezpečuje komunikáciu (šifruje) pre vyššie vrstvy
  - HTTP → HTTPS

TLS tok správ



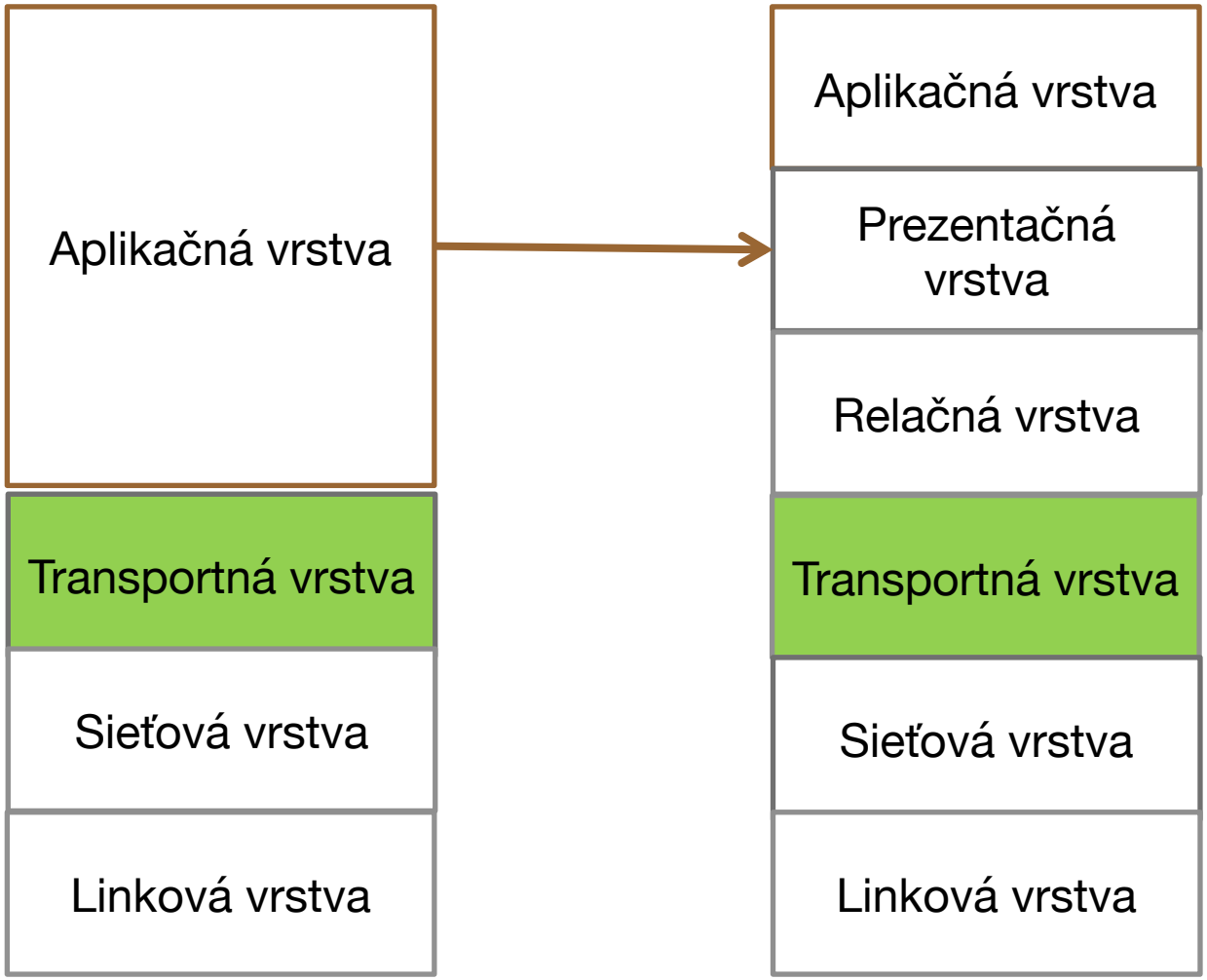
TLS Wireshark



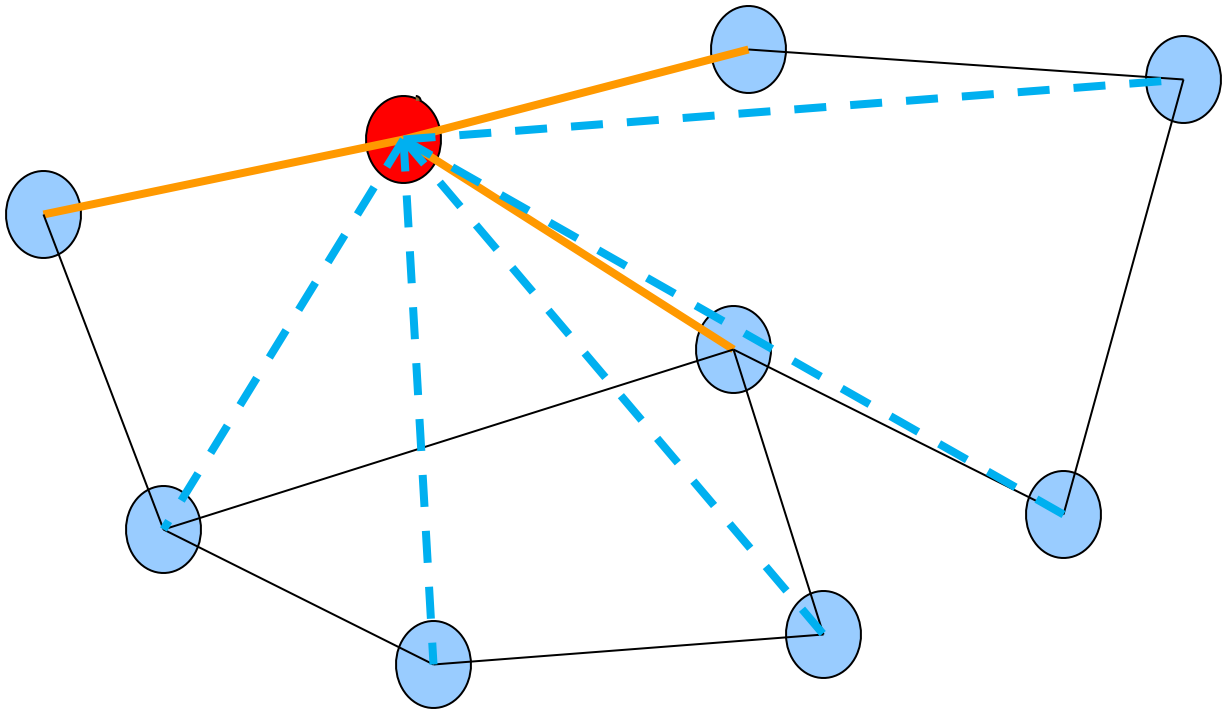
Relačná vrstva

- Riadi spojenia medzi entitami
- Vytvára, riadi a ukončuje pripojenia (TCP v skutočnosti patrí do tejto vrstvy)
- SDP (Session Description Protocol), RPC (Remote Procedure Call), RTCP (Real Time Transport Control Protocol)
  - Protokoly, ktoré „pomáhajú“ iným protokolom

Transportná vrstva



Pohľad vrstiev na topoloógiu siete
Transportná vrstva

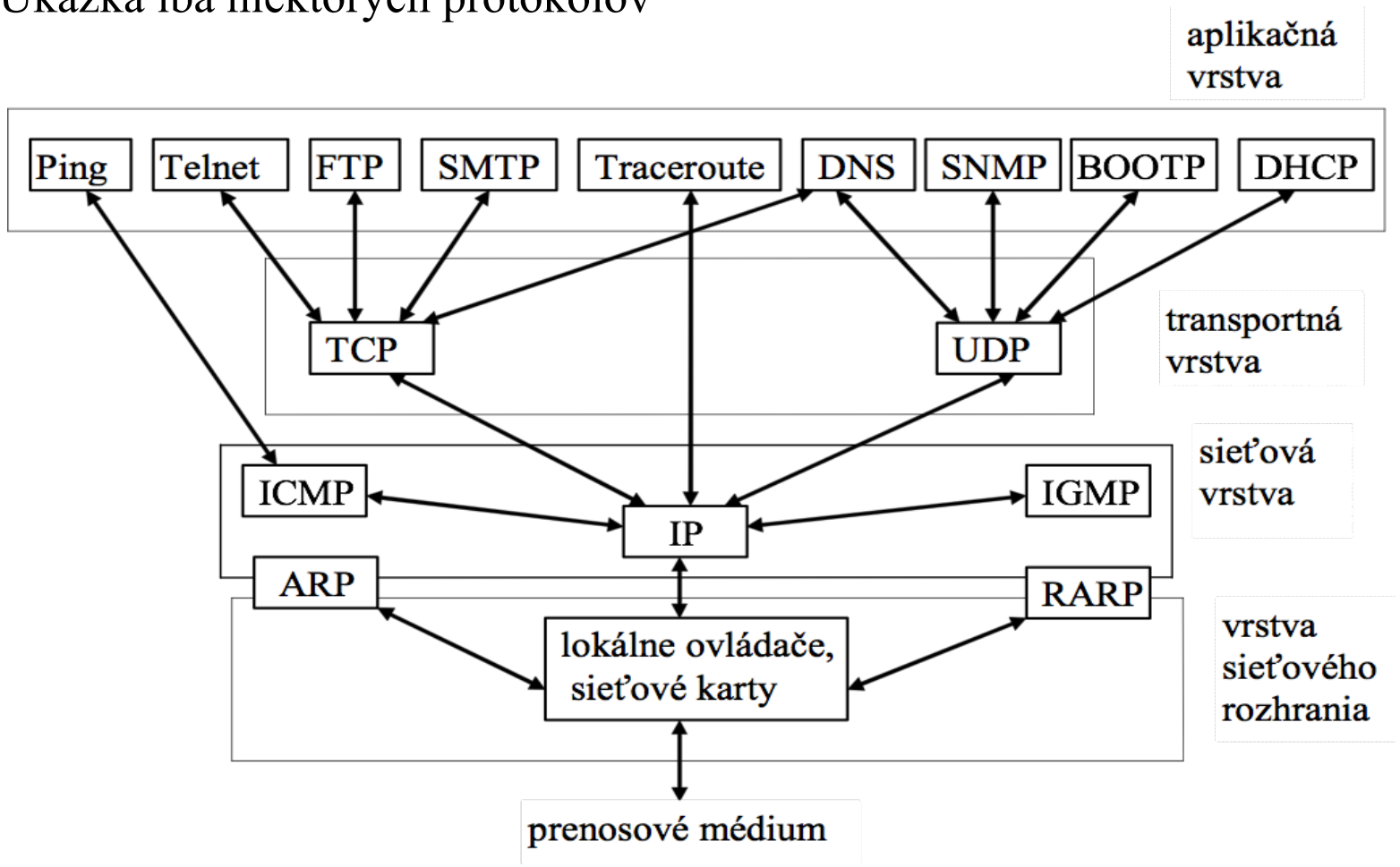


Transportná vrstva RM OSI

- poskytovateľ (relačnej vrstve) a žiadateľ služby (od sieťovej vrstvy)
- služby so spojením a bez spojenia, s potvrdením a bez potvrdenia
- multiplexovanie spojov

Protokolový zásobník TCP/IP

Ukážka iba niektorých protokolov



Transportná vrstva TCP/IP

TCP (Transmission Control Protocol)

- služby so spojením, s potvrdením
- TCP ~ protokol triedy TP4
- prenos dát = prenos prúdu bajtov - segmenty
- multiplexovanie a demultiplexovanie

UDP (User Datagram Protocol)

- služby bez spojenia, bez potvrdenia
- blokový prenos dát - datagramy
- multiplexovanie a demultiplexovanie

~~*DCCP (Datagram Congestion Control Protocol)*~~

Protokol UDP

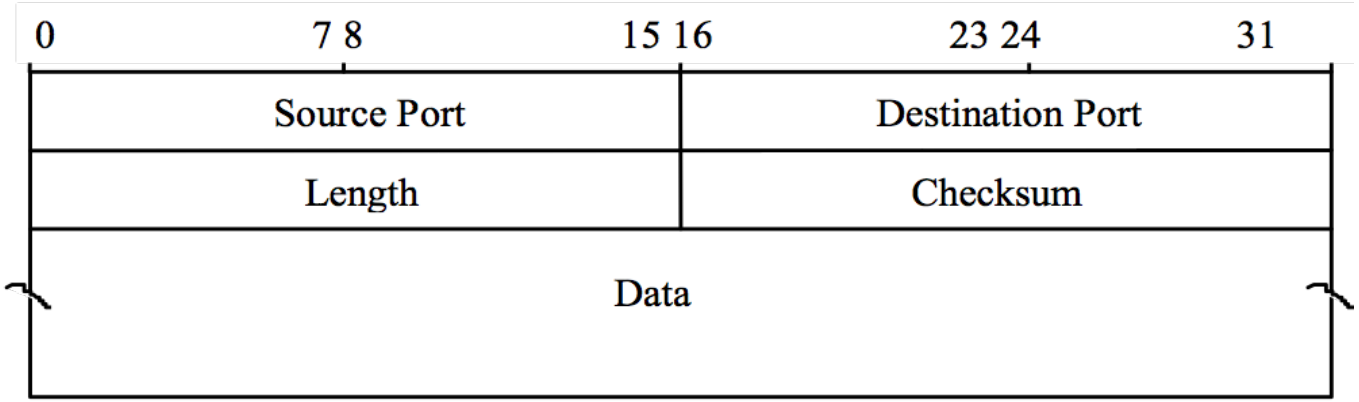
- protokol bez spojenia, bez potvrdenia, nespoľahlivý
- klient – server aplikácie
- Balí aplikačné dáta do „datagramov“
- multiplexovanie a demultiplexovanie datagramov
- podporuje broadcast, multicast

Protokol UDP

Čo nevie:

- nezriaďuje spojenie pred prenosom dát
- nepotvrdzuje prijaté dáta
- nedeteguje straty
- nie je možnosť požadovať opakovanie prenosu dát
- negarantuje doručenie dát
- nezaručuje, že dáta sú prijímané v rovnakom poradí ako boli vyslané
- nemá mechanizmus na riadenie toku dát medzi koncovými uzlami resp. na riadenie zahltenia

UDP datagram



Čo je checksum?

Detekčné kódy

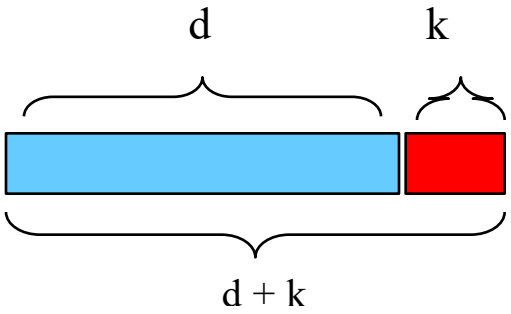
- paritný kód

kontrolná suma (Internet suma) (checksum)

CRC (Cyclic Redundancy Check Code) kód (FCS (Frame Check Sequence))

Ethernet: G (x)= x32 + x26 + x23 + x22 + x16 + x12 x11 + x10 + x8 + x7 + x5 + x4 + x2 + x1

Separovateľné kódy



4A	5B	62	1E

6 2 1 E
4 A 5 B
Ø ← A C 7 9
\+ Ø
A C 7 9
5 3 8 6
(rozdiel do 15)

$D * 2^K + K = n * G$

- generujúci polynóm (štandardizovaný)
- dĺžka (k+1) bitov, v najvyššom bite je *1*

non-ekvivalencia

zvyšok po delení $(2^K * D)/G$

STU FIIT

Cyclic Redundancy Code

- (**r+1**) dlhý generátor **G**, ktorý je známy ako vysielajúcej tak prijímajúcej strane
- Dátové bity **D**
- Cieľ je nájsť také **R**, že **(D, R)** sú deliteľné **G**
- Inými slovami:

$$R = \text{zvyšok}\ (D \times 2^r / G)$$

CRC príklad (1)

D = 1101 0110 11

G = 100 11 (r=4)

$(D*2^r):G$ = 1101 0110 11 **0000**: 10011

1001 1

0100 11

100 11

010 11 **0**

10 01 1

00 10 1**000**

1 00 11

R= 0 0**1** **110**

Používa sa XOR operácia

STU FIIT

CRC príklad (2)

```
D = 1101 0110 11
G = 100 11 (r=4)
```

Vysielač vyšle / prijímač príme sekvenciu:
`1101 0110 11 1110`

Kontrola prebieha ako v predchádzajucom kroku:
`1101 0110 11 1110: 10011`

```
.....................................
             010 11 1
              10 01 1
              00 10 0110
                 10 011
             R=  00 0000
```

STU FIIT

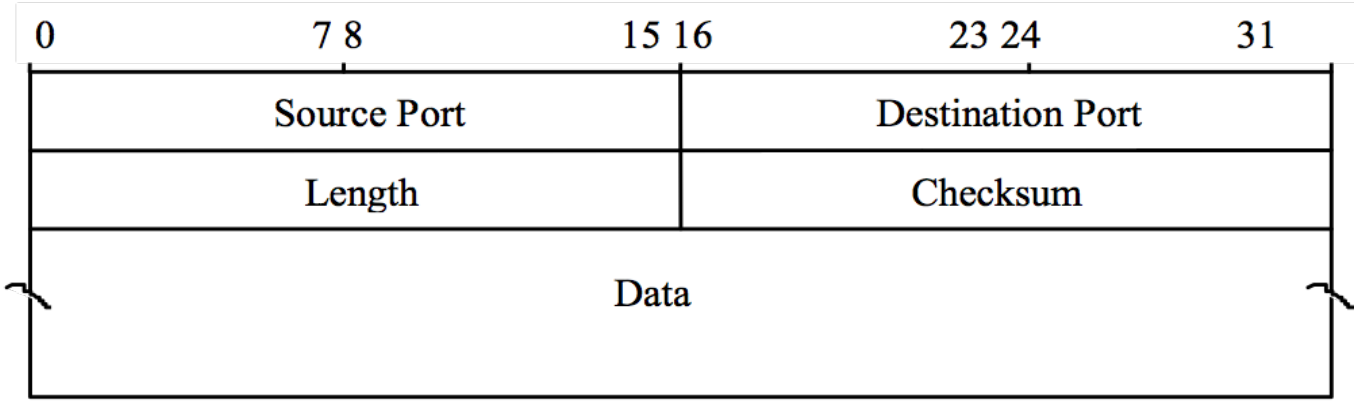
CRC príklad 2

D = 10110011101000100101

G = 10111101

R= 111001

UDP datagram

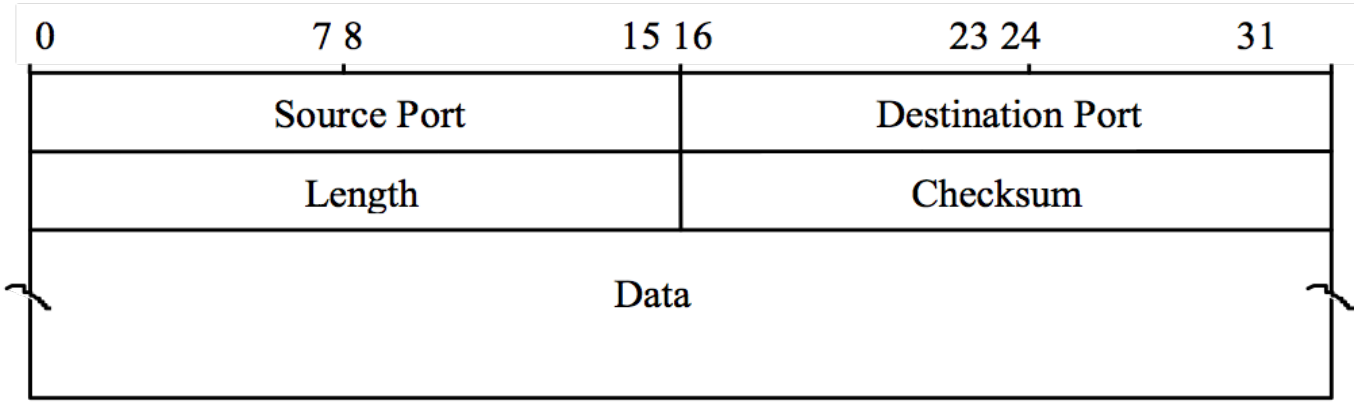


Koľko dát vložím do datagramu?

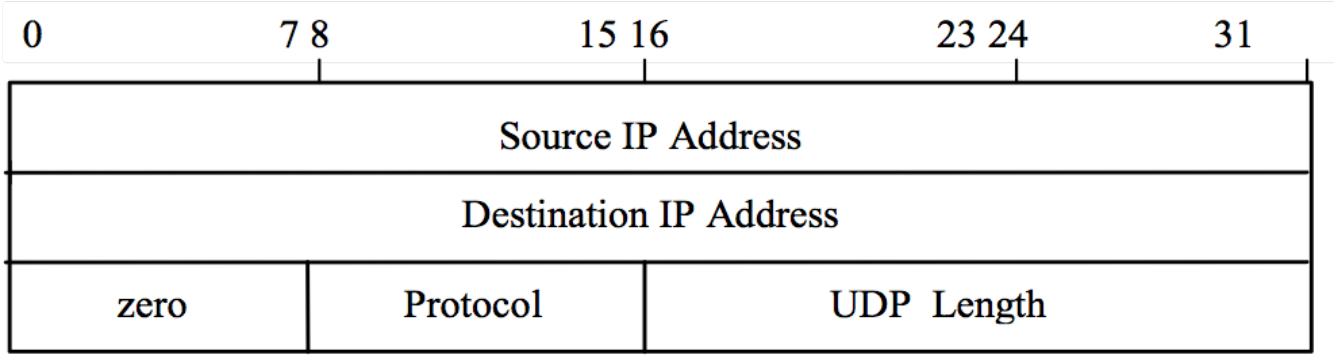
- Obmedzenie UDP - length
- Udáva dĺžku vrátane UDP hlavičky
  - Minimálne 8 bajtov
  - Maximálne 65535 bajtov (z toho 8 bajtov hlavička)
  - Segmentácia/znovu poskladanie dát

Protokol UDP

UDP datagram



pseudohlavička



Akú prenosovú rýchlosť potrebujem na prenos 1MB stránky?

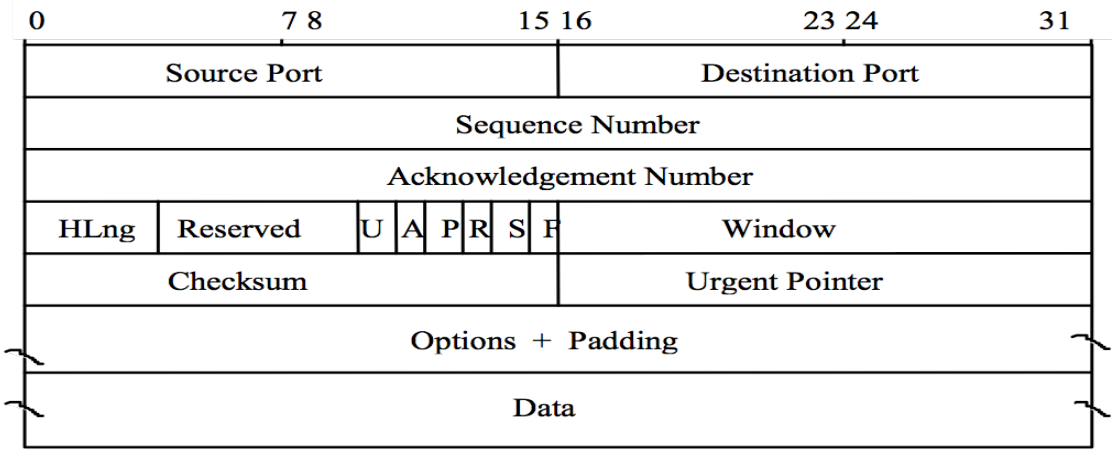
- Keby sa HTTP prenášal v UDP?
- Je rozdiel 1 súbor 1MB a 10súborov po 100 KB?

Stručný úvod do TCP

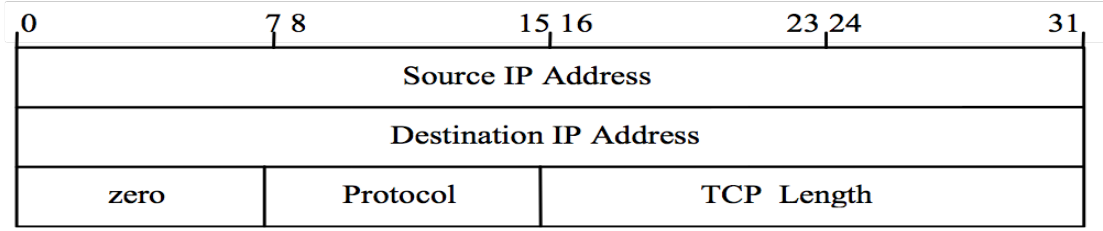
- protokol so spojením, s potvrdením, spoľahlivý prenos
- prenos dát – prúd bajtov, počet vyslaných bajtov aplikáciou a TCP entitou môže byť rôzny
- vyrovnávacie pamäte – segmentácia prúdu bajtov
- interaktívny a neinteraktívny prenos dát (typ aplikácie)
- TCP spojenie – plný duplex, dvojbodové
- urgentné dáta
- príjem dát aplikáciou – príznak PUSH

Protokol TCP

TCP segment



pseudohlavička



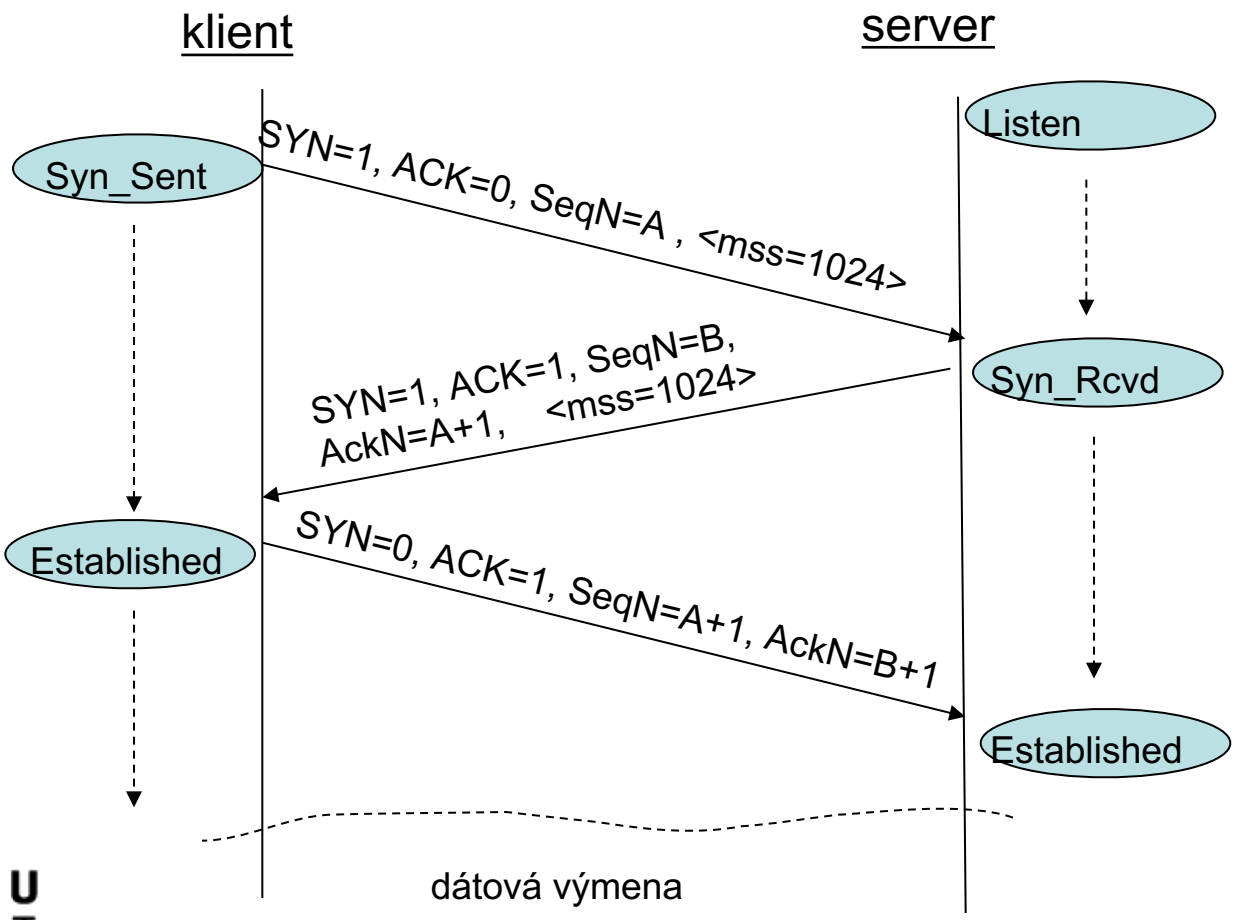
Niektoré voliteľné položky (options):

kind	length	význam
2	4	MSS
3	3	zväčšenie okna
4	2	povolenie SACK
5	prem.	SACK

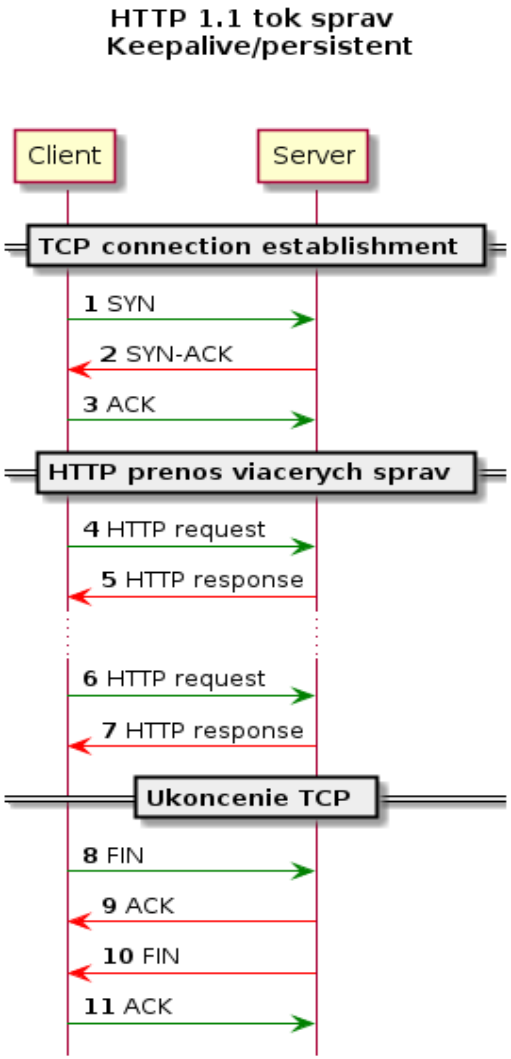
STU FIIT

Protokol TCP – zriadenie spojenia

- výmena troch segmentov (three-way-handshake)

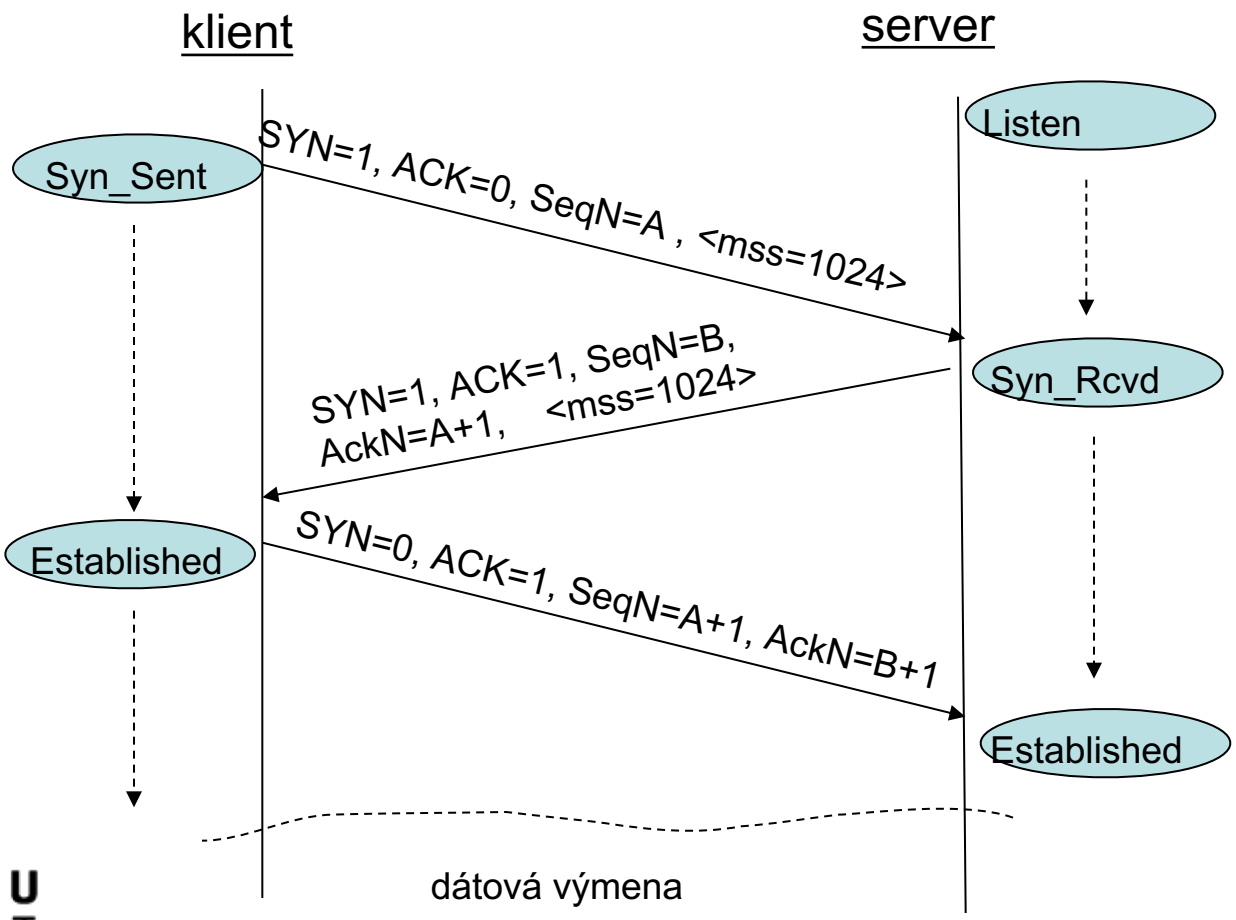


Zriadenia TCP spojenia a HTTP prenos



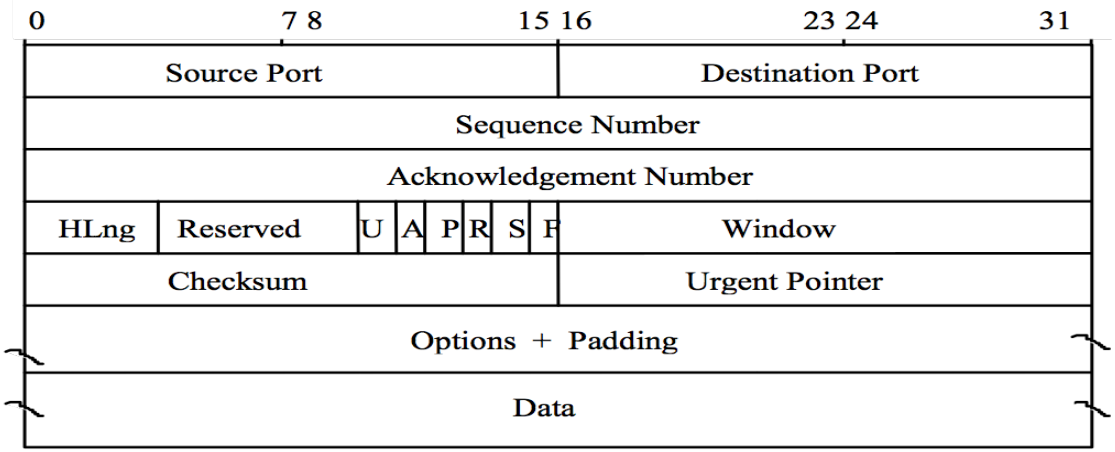
Protokol TCP – zriadenie spojenia

- Kde sa SYN a ACK vlastne nechádzajú a načo mi sú?

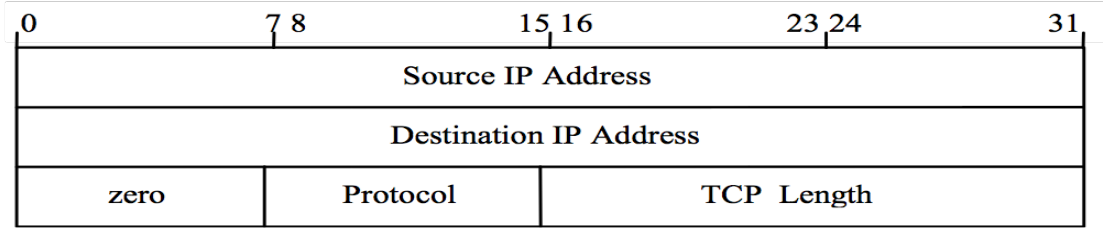


Protokol TCP

TCP segment



pseudohlavička



Niektoré voliteľné položky (options):

kind	length	význam
2	4	MSS
3	3	zväčšenie okna
4	2	povolenie SACK
5	prem.	SACK

STU FIIT

Akú prenosovú rýchlosť potrebujem na prenos 1MB stránky?

» Je rozdiel 1 súbor 1MB a 10súborov po 100 KB?

» Koľko má TCP hlavička?

Zhrnutie prednášky

- Prezentačná vrstva
  - TLS
- Relačná vrstva
  - SDP – nebolo na prednáške
- Transportná vrstva – prenos cez sieť
  - UDP – využíva sa na zadaní
  - TCP (Je využívané hlavne HTTP)

Čo nás čaká na budúcej prednáške

» TCP dokončenie
  – Riadenie toku (pomalé / rýchle linmky)
  – Potvrdzovanie dát (ACK, NACK)
  – Ukončenie spojenia
  – Znovuodoslanie dát