



Počítačové a komunikačné siete

Relačná, prezentačná vrstva
Úvod do transportnej vrstvy

Prednáška 3

Opakovanie minulej prednášky

» HTTP

- Používa TCP,IP,Ethernet/WiFi

» DHCP

- Získanie IP adresy

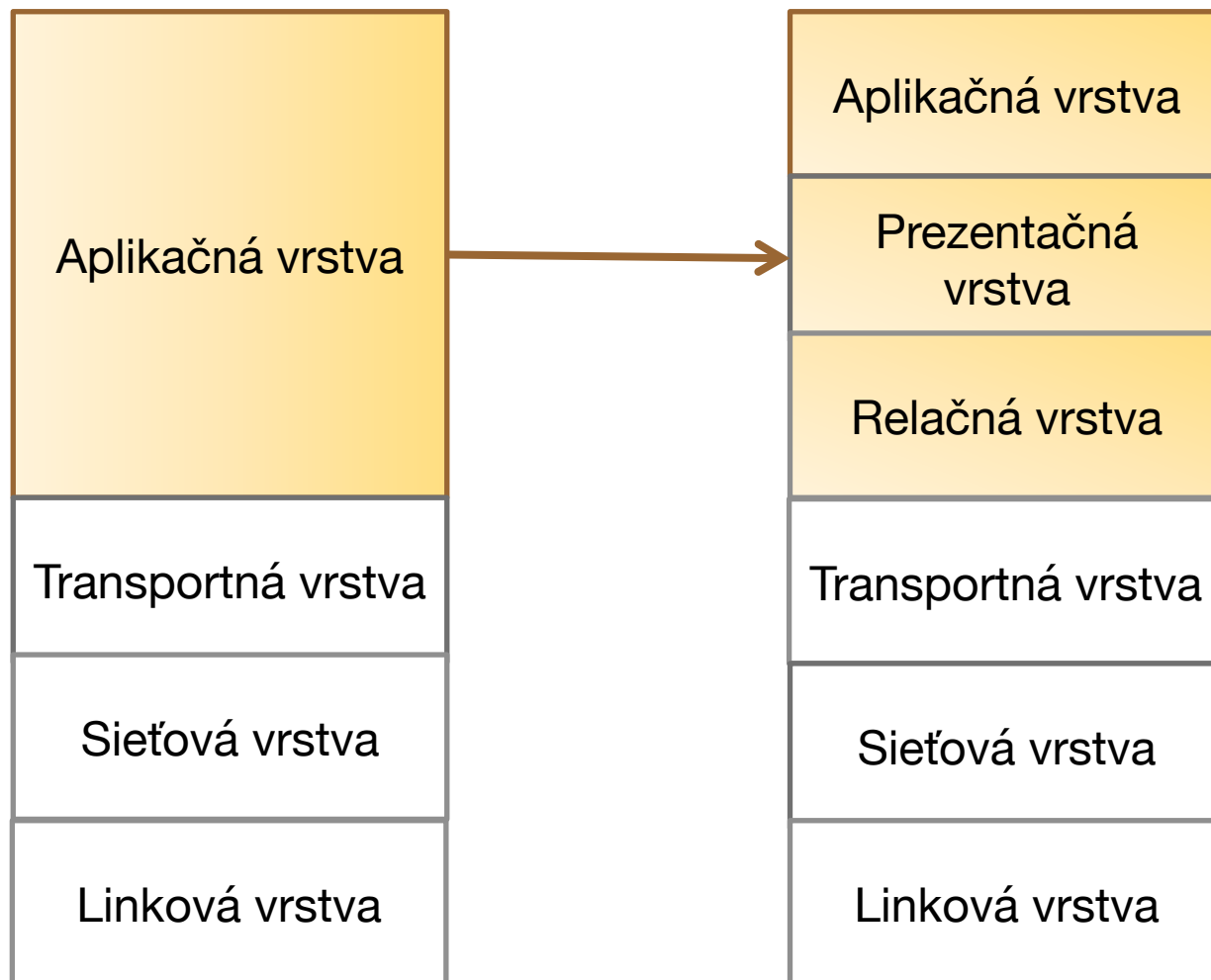
» DNS

- K menu získať IP adresu

Čo nás čaká na prednáške

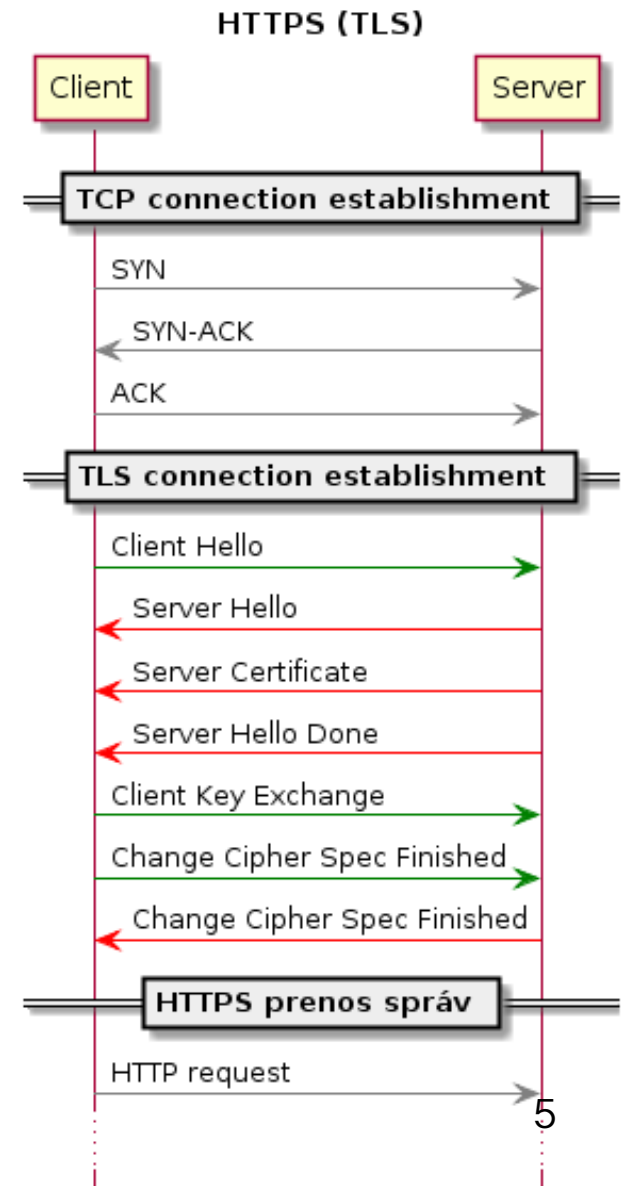
- » Relačná vrstva (HTTPS)
- » Prezentačná vrstva
- » UDP (transportná vrstva)
 - CRC (Overenie správnosti prenosu)
- » TCP (Transportná vrstva)
- » Detaily používania wiresharku

Prezentačná a Relačná vrstva



Prezentačná vrstva

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

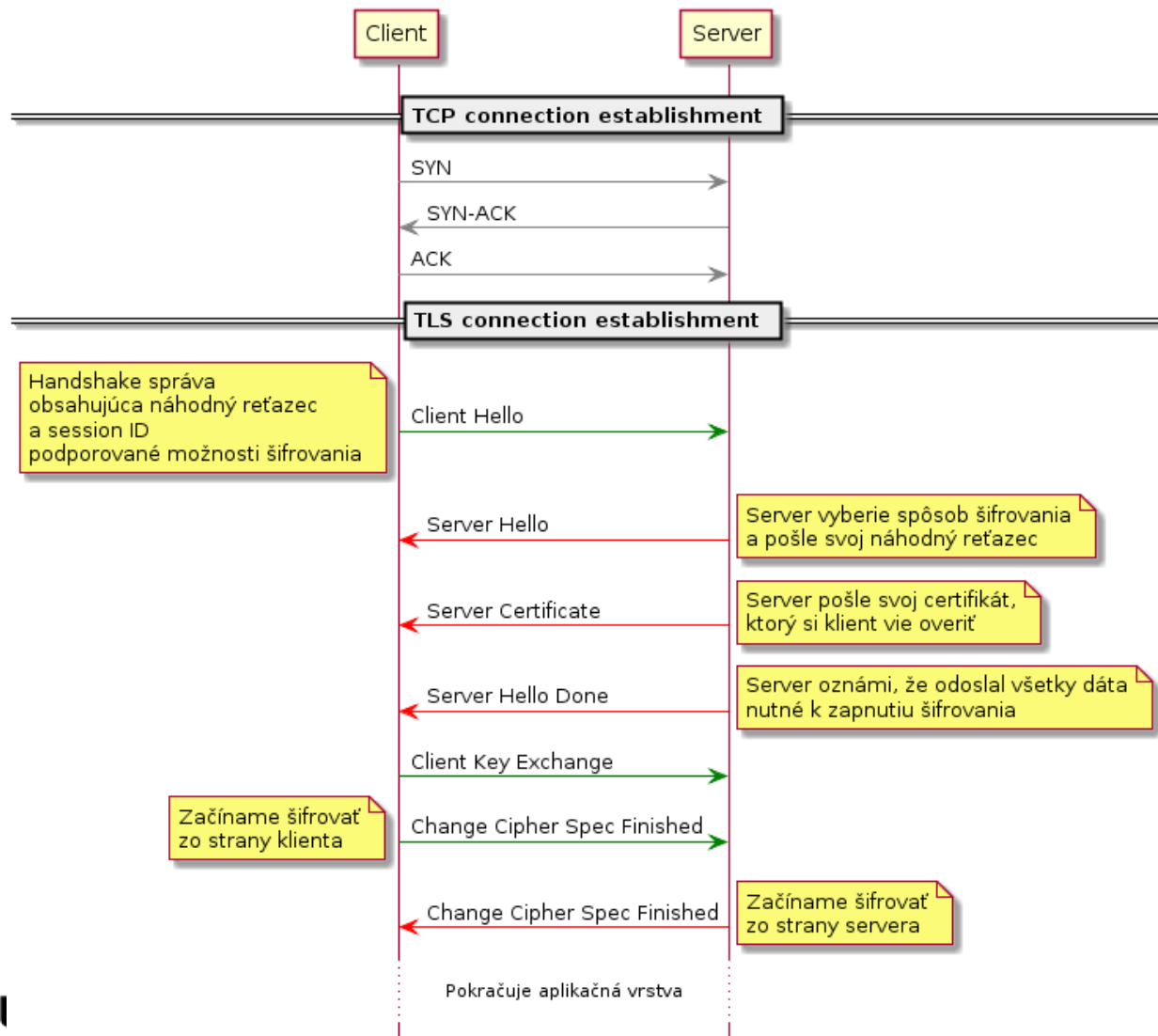


TLS

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

TLS tok správ

TLS príklad



TLS Wireshark

Wireshark interface showing a TLS handshake and data transfer. The packet list displays frames 11 through 33, all originating from 192.168.0.36 and destined for 13.107.136.9. The packet details pane shows the structure of frame 11, which is a TLSv1.2 Client Hello. The packet bytes pane shows the raw hex and ASCII data of frame 11.

No.	Time	Source	Destination	Protocol	Length	Info
11	0.651776	192.168.0.36	13.107.136.9	TLSv1...	571	Client Hello
16	0.689624	13.107.136.9	192.168.0.36	TLSv1...	1459	Server Hello, Certificate, Certificate Status, S...
20	0.697992	192.168.0.36	13.107.136.9	TLSv1...	147	Client Key Exchange, Change Cipher Spec, Encrypt...
24	0.724807	13.107.136.9	192.168.0.36	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message...
25	0.724808	13.107.136.9	192.168.0.36	TLSv1...	123	Application Data
28	0.726612	192.168.0.36	13.107.136.9	TLSv1...	107	Application Data
29	0.726613	192.168.0.36	13.107.136.9	TLSv1...	104	Application Data
30	0.726652	192.168.0.36	13.107.136.9	TLSv1...	96	Application Data
31	0.726652	192.168.0.36	13.107.136.9	TLSv1...	1142	Application Data
32	0.726832	192.168.0.36	13.107.136.9	TLSv1...	314	Application Data
33	0.726872	192.168.0.36	13.107.136.9	TLSv1...	92	Application Data

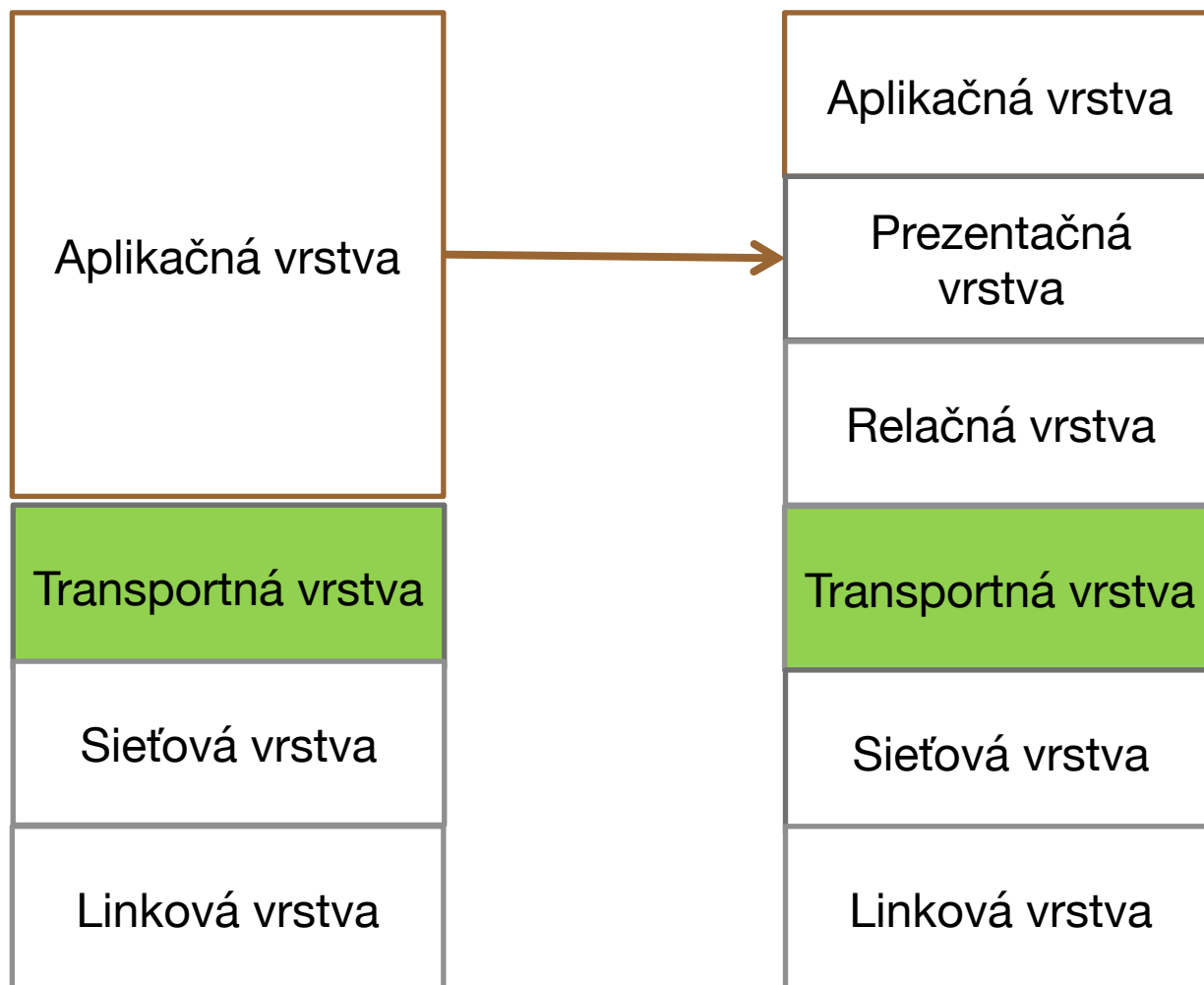
Frame 11: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0
 Ethernet II, Src: Apple_58:c4:7d (f0:18:98:58:c4:7d), Dst: CompalBr_c3:98:98 (90:5c:44:c3:98:98)
 Internet Protocol Version 4, Src: 192.168.0.36, Dst: 13.107.136.9
 Transmission Control Protocol, Src Port: 62069, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
 Transport Layer Security
 TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 512
 Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 508
 Version: TLS 1.2 (0x0303)
 Random: 15bbec4ea2ba33a466e807fd3f4bb539bece7024e9652971...
 Session ID Length: 32
 Session ID: 7adc1027693aefc4192c9a92f6207ab33024ec2804cddbdb...
 Cipher Suites Length: 52

0000 90 5c 44 c3 98 98 f0 18 98 58 c4 7d 08 00 45 00 ·\D· · · · ·X·}· ·E·
 0010 02 2d 00 00 40 00 40 06 e2 8a c0 a8 00 24 0d 6b ·-·@·@· · · · ·\$·k·
 0020 88 09 f2 75 01 bb 4b 87 a2 e8 ff 9a a5 79 50 18 · · · ·u·K· · · · ·yP·
 0030 10 00 5c 57 00 00 16 03 01 02 00 01 00 01 fc 03 · ·\W· · · · · · · · · ·
 0040 03 15 bb ec 4e a2 ba 33 a4 66 e8 07 fd 3f 4b b5 · · · ·N· ·3· ·f· ·?K·
 0050 39 be ce 70 24 e9 65 29 71 e9 fa e5 27 7e 0b 60 9· ·p\$·e) q· · · ·~·`·
 0060 65 20 7a dc 10 27 69 3a ef c4 19 2c 9a 92 f6 20 e z· ·'i: · · · · · · · ·
 0070 7a b3 30 24 ec 28 04 cd bb db b3 22 7d 04 1d 6b z·0\$·(· · · · ·}· · ·k·
 0080 a5 17 00 34 13 03 13 01 13 02 c0 2c c0 2b c0 24 · · ·4· · · · · · · · · ·+·\$·

Relačná vrstva

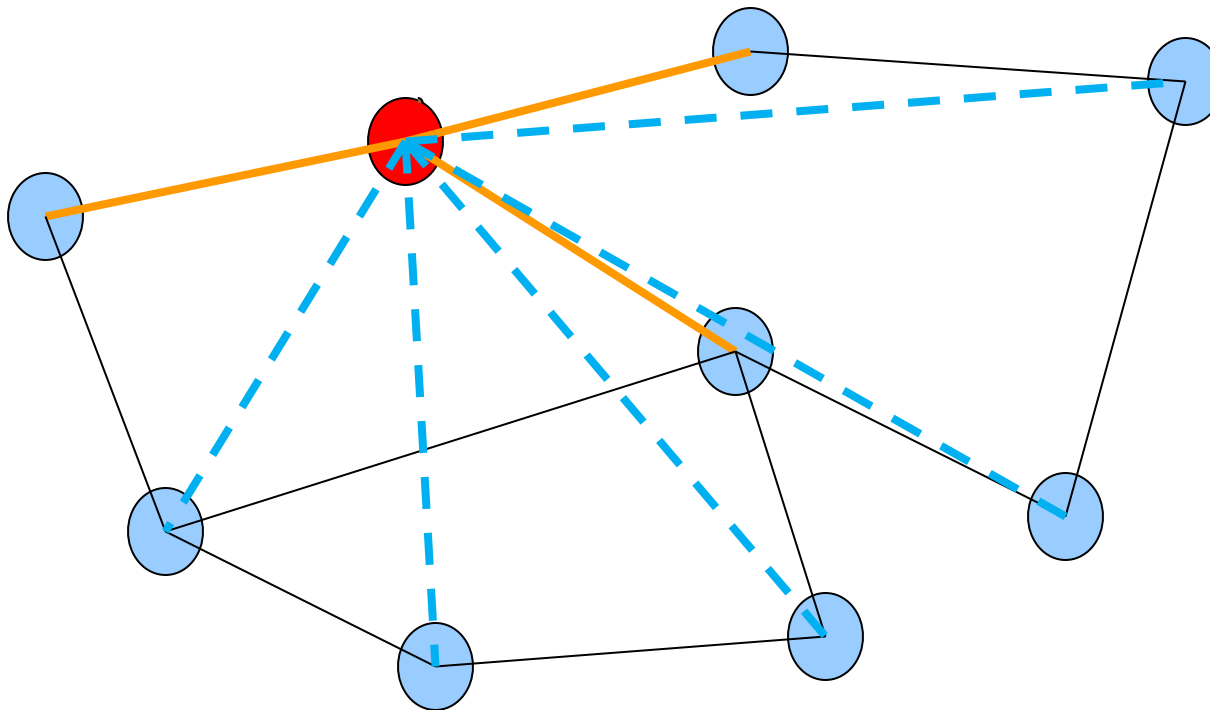
- » Riadi spojenia medzi entitami
- » Vytvára, riadi a ukončuje pripojenia (TCP v skutočnosti patrí do tejto vrstvy)
- » SDP (Session Description Protocol), RPC (Remote Procedure Call), RTCP (Real Time Transport Control Protocol)
 - Protokoly, ktoré „pomáhajú“ iným protokolom

Transportná vrstva



Pohľad vrstiev na topoloógiu siete

Transportná vrstva

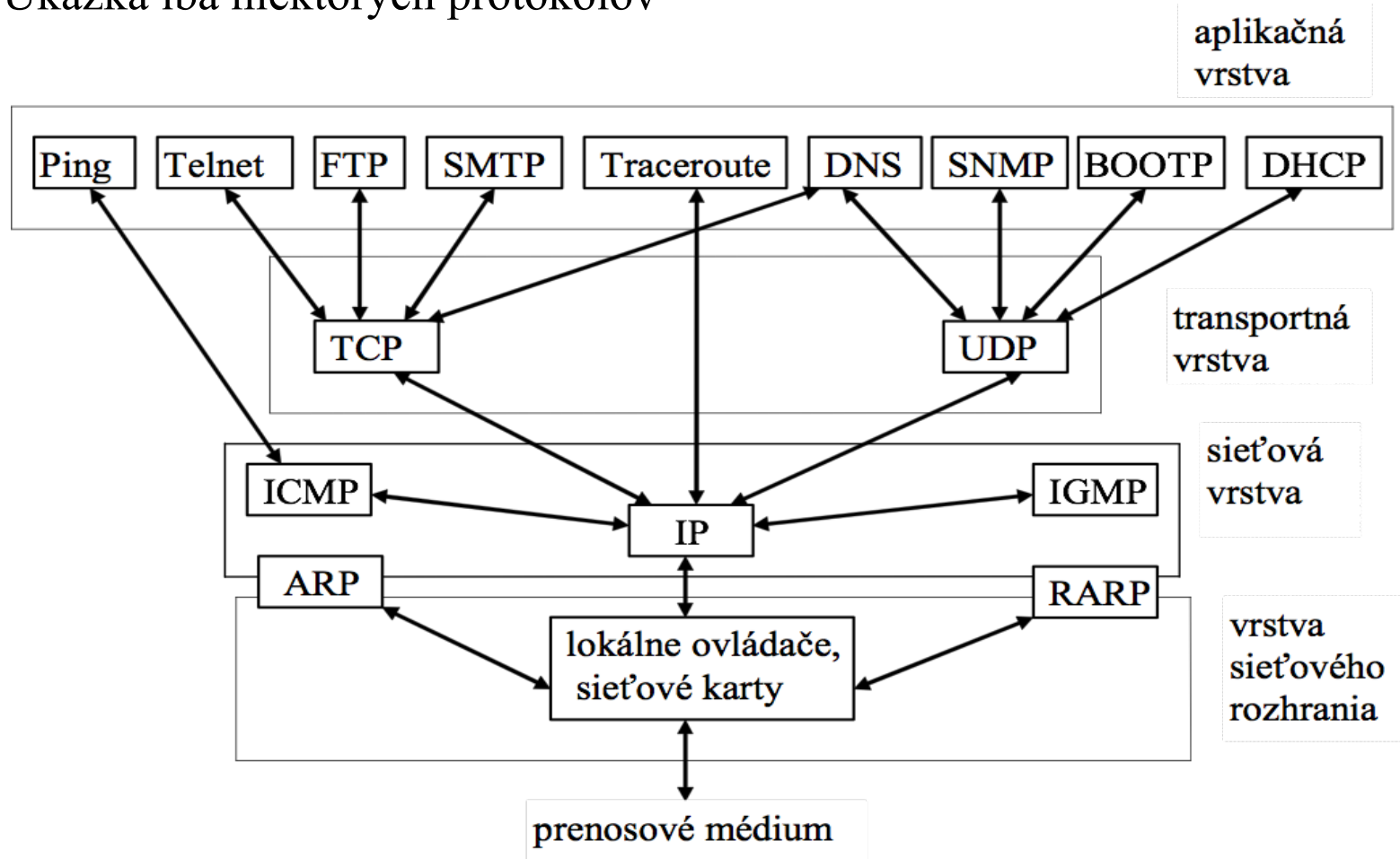


Transportná vrstva RM OSI

- » 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

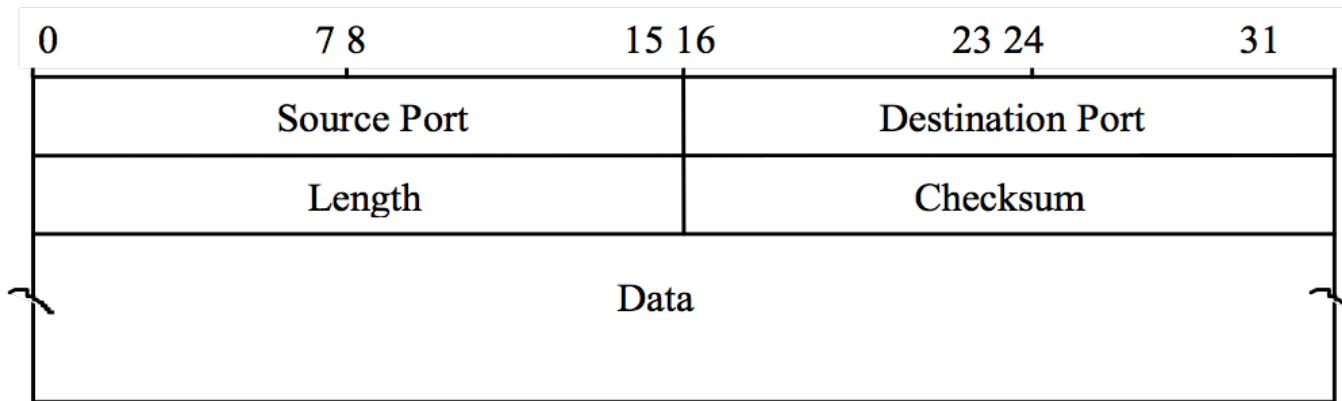
- protokol bez spojenia, bez potvrdenia, nespoľahlivý
- klient – server aplikácie
- Balí aplikačné dáta do „datagramov“
- multiplexovanie a demultiplexovanie datagramov
- podporuje broadcast, multicast

Protokol UDP

Čo nevie:

- nezriaďuje spojenie pred prenosom dát
- nepotvrďuje 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

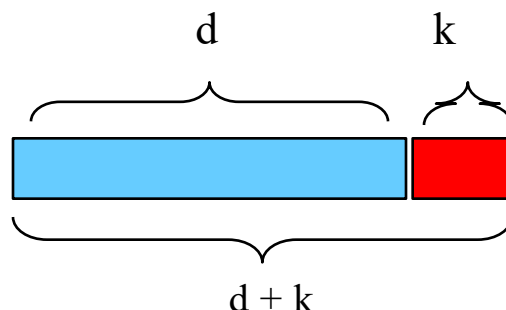
- paritný kód

kontrolná suma (Internet suma) (checksum)

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

Ethernet: $G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1$

Separovateľné kódy



4A	5B	62	1E
----	----	----	----

$$\begin{array}{r}
 621E \\
 4A5B \\
 \hline
 \emptyset \leftarrow AC79 \\
 + \quad \quad \emptyset \\
 \hline
 AC79 \\
 5386 \\
 \hline
 \text{(rozdiel do 15)}
 \end{array}$$

$$D \cdot 2^K + K = n \cdot G$$

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

zvyšok po delení $(2^K \cdot D)/G$

non-ekvivalencia

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)

$(D \cdot 2^r) : G = 1101 \ 0110 \ 11 \ \mathbf{0000} : 10011$

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

CRC príklad (2)

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

Vysielač vyšle / prijímač prijme sekvenciu:
1101 0110 11 **1110**

Kontrola prebieha ako v predchádzajúcom kroku:
1101 0110 11 **1110**: 10011

.....
 010 11 **1**
 10 01 1
 00 10 0**110**
 10 011
R= 00 0000

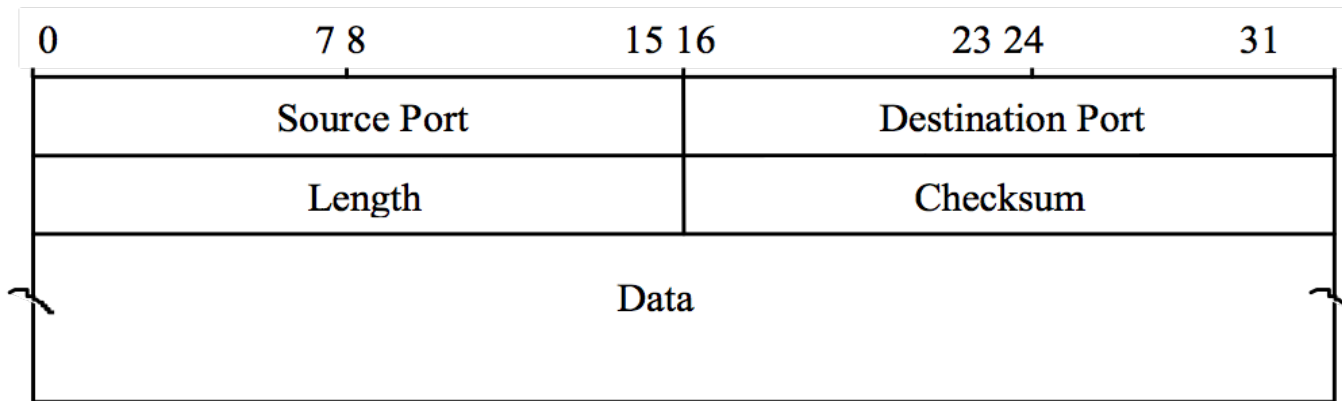
CRC príklad 2

$D = 10110011101000100101$

$G = 10111101$

$R = 111001$

UDP datagram

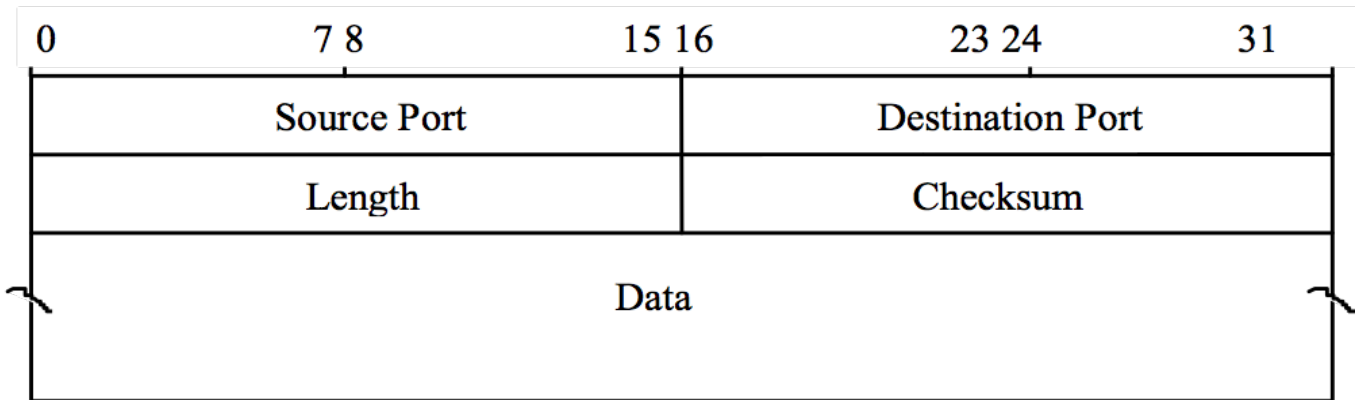


Koľko dát vložím do datagramu?

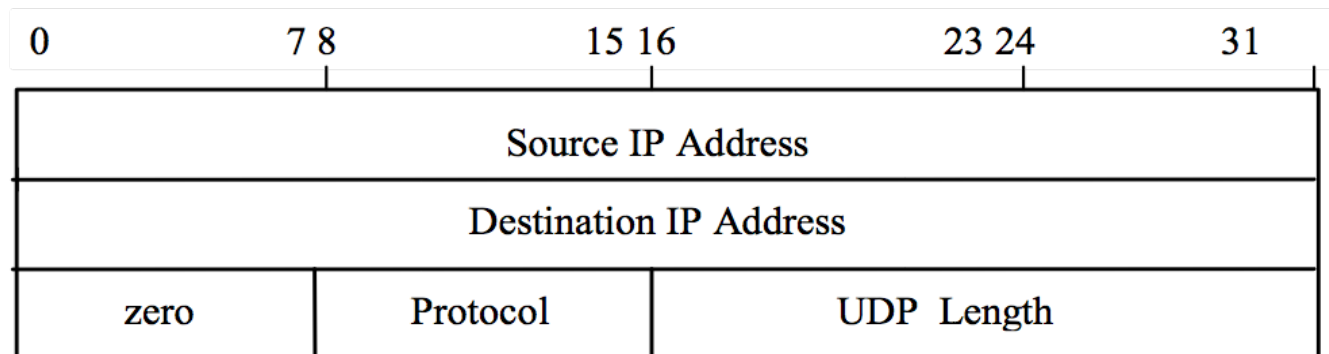
- » Obmedzenie UDP - length
- » Udáva dĺžku vrátane UDP hlavičky
 - Minimálne 8 bajtov
 - Maximálne 65535 bajtov (z toho 8 bajtov hlavička)
 - Segmentácia/znovu poskladanie dát

Protokol UDP

UDP datagram



pseudohlavička



Akú prenosovú rýchlosť potrebujem na prenos 1MB stránky?

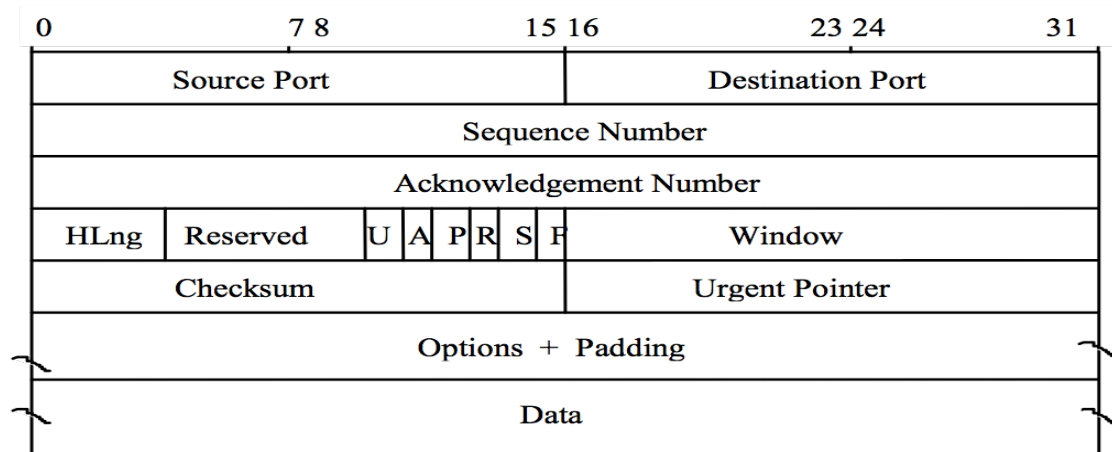
- » Keby sa HTTP prenášal v UDP?
- » Je rozdiel 1 súbor 1MB a 10súborov po 100 KB?

Stručný úvod do TCP

- protokol so spojením, s potvrdením, spoľahlivý prenos
- prenos dát – prúd bajtov, počet vyslaných bajtov aplikáciou a TCP entitou môže byť rôžny
- 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

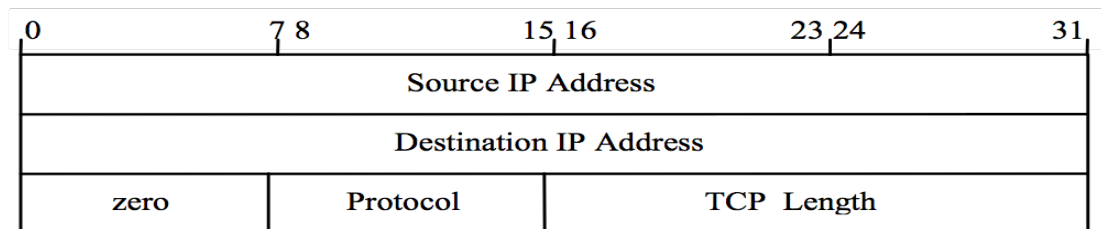
TCP segment



pseudohlavička

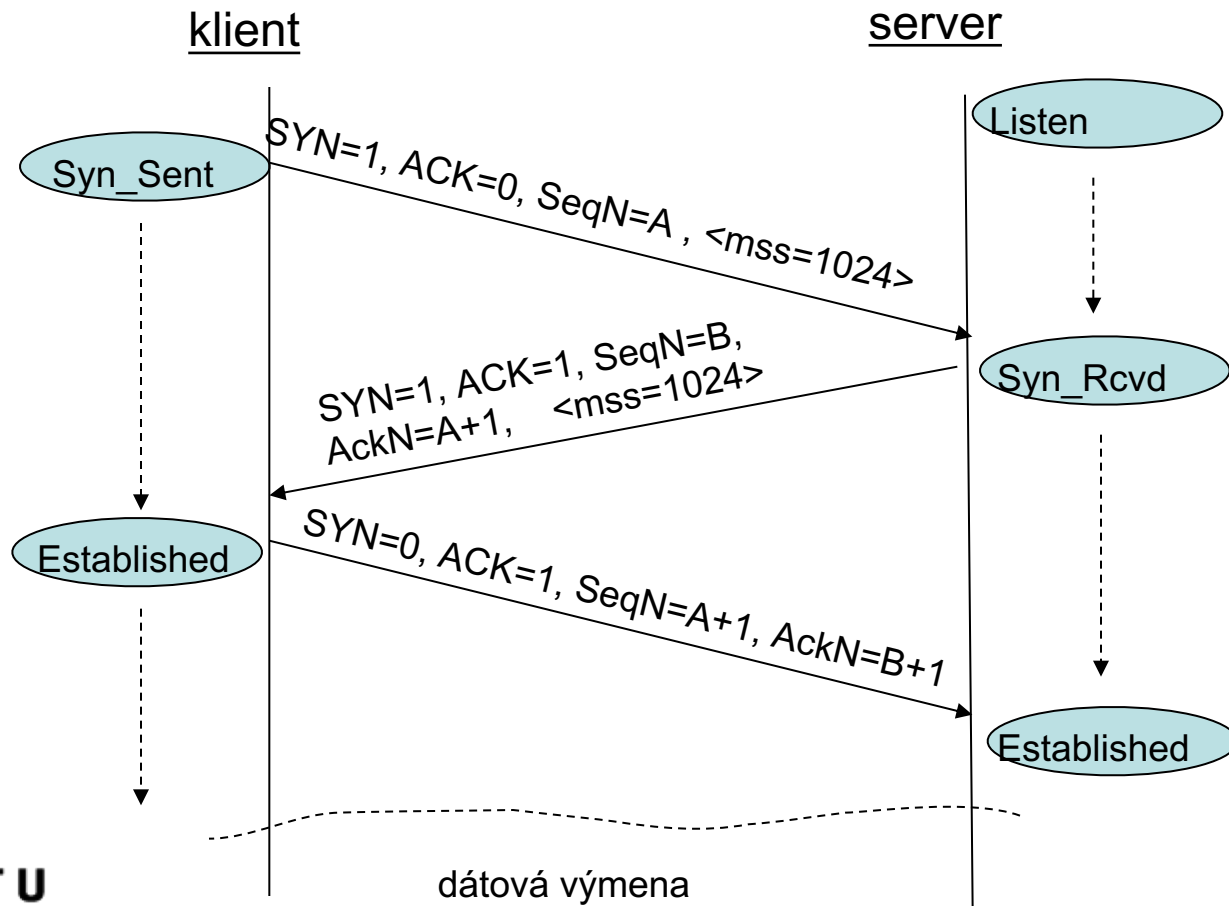
Niektoré voliteľné položky
(options):

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

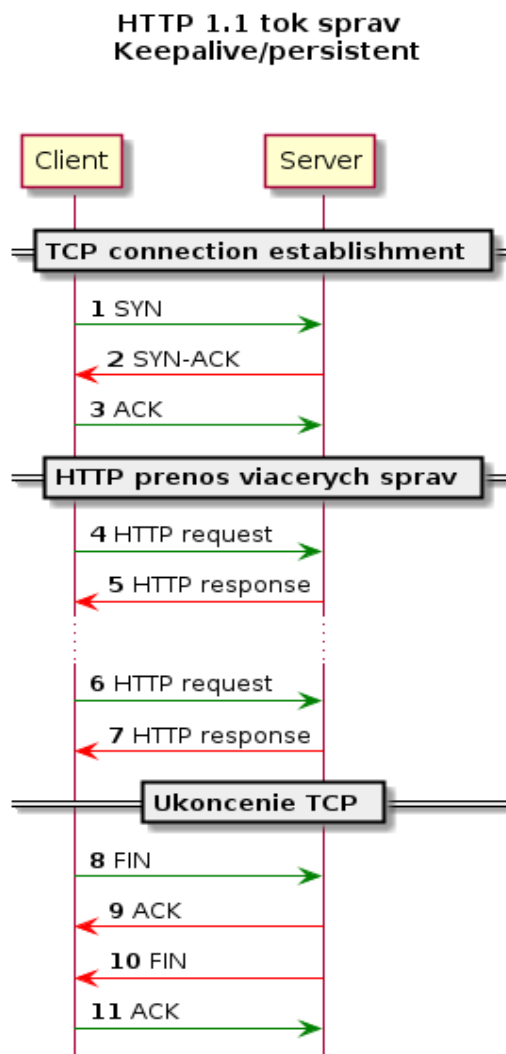


Protokol TCP – zriadenie spojenia

- výmena troch segmentov (three-way-handshake)

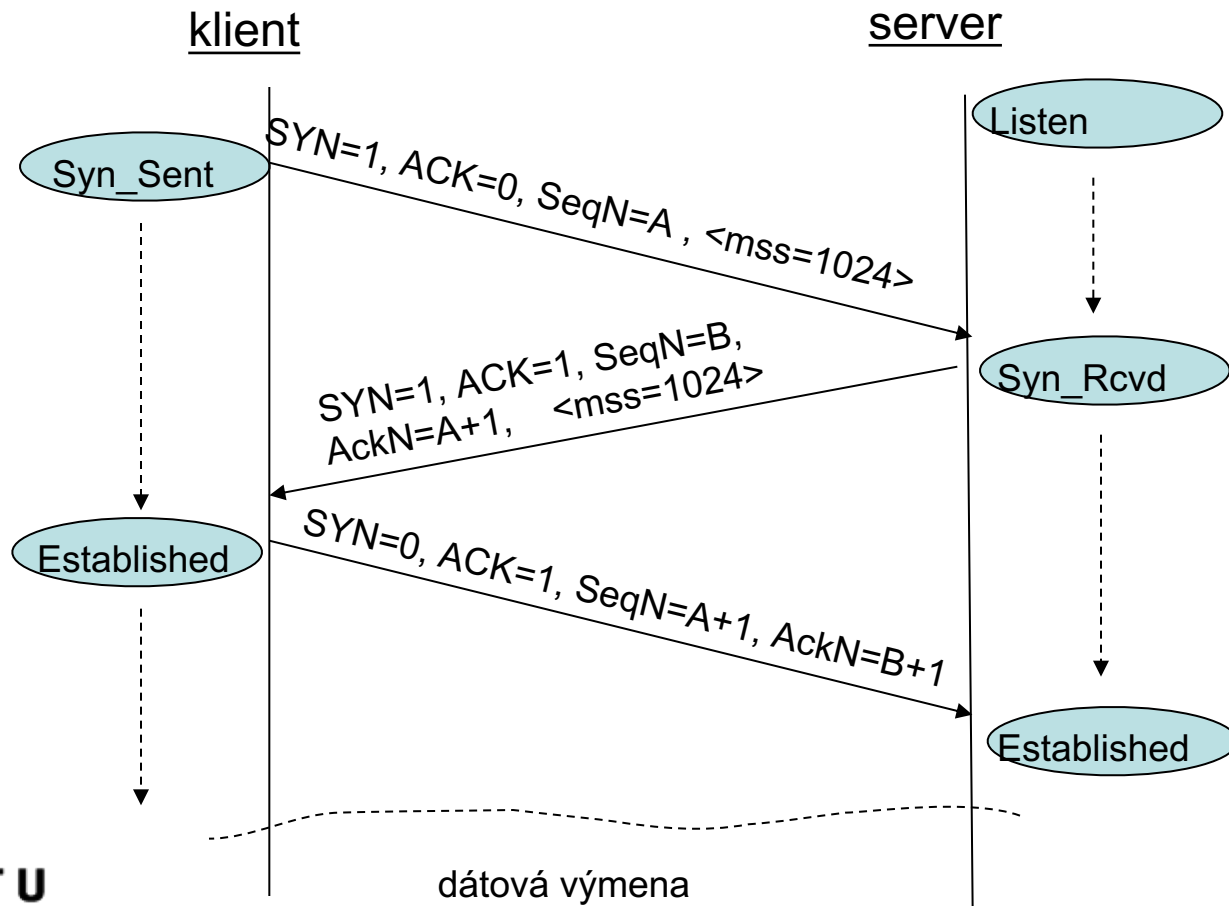


Zriadenia TCP spojenia a HTTP prenos



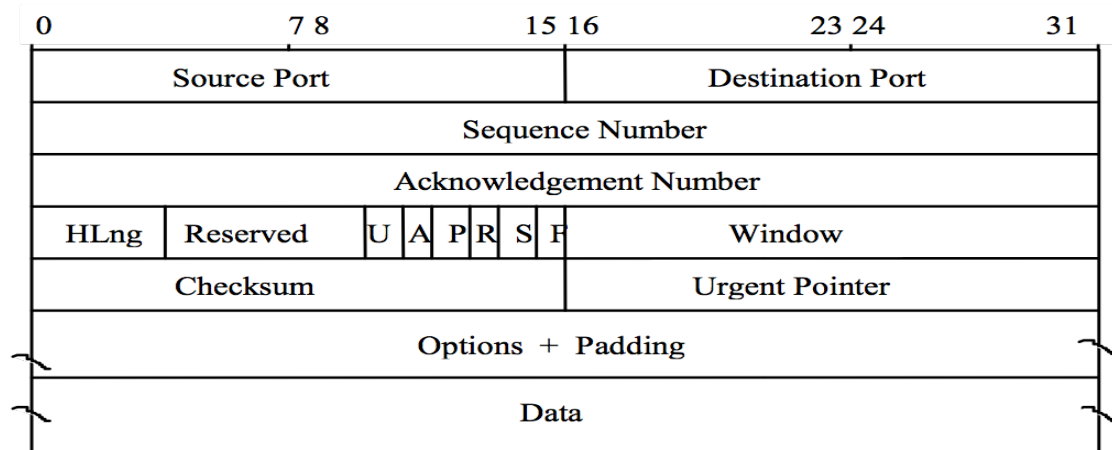
Protokol TCP – zriadenie spojenia

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



Protokol TCP

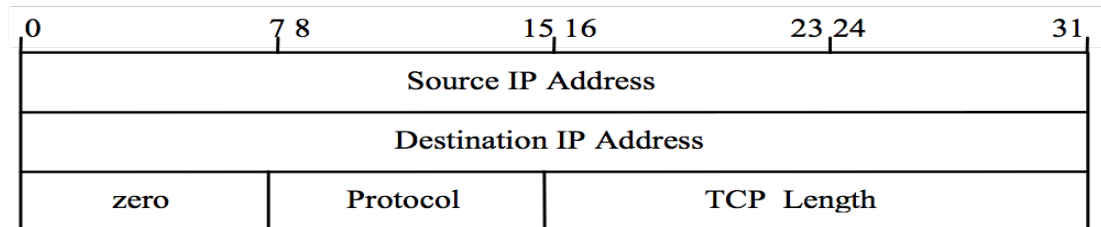
TCP segment



pseudohlavička

Niektoré voliteľné položky
(options):

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



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 linky)
- Potvrdzovanie dát (ACK, NACK)
- Ukončenie spojenia
- Znovuodoslanie dát