TRANSPORTNÍ VRSTVA

RNDr. Ing. Vladimir Smotlacha, Ph.D.

Katedra počítačových systémů
Fakulta informačních technologií
České vysoké učení technické v Praze

Počítačové sítě BI-PSI

LS 2018/19, Přednáška 6

https://courses.fit.cvut.cz/BI-PSI

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

OPPA PRAHA PRAGUE PRAGA PRAG EVROPSKÁ UNIE

OBSAH

Transportní vrstva

- druhy služeb
- protokoly
- vytvoření a uzavření spojení
- řízení toku

TCP

UDP

RTP, RTCP

SLUŽBY

Transportní vrstva – hranice mezi

- aplikací (software)

  a

- sítí (technologie)

Transparentní přenos dat mezi koncovými uživateli

- spolehlivost
- řízení datového toku
- segmentace dat
- oprava chyb

ADRESACE

Služba musí mít adresu

- TSAP – Transport Service Access Point

- předdefinované TSAP („well-known ports“)
  - např. port 80 pro http
- dynamicky přidělované
  - portmapper
  - registruje TSAP pro služby

NAVÁZÁNÍ SPOJENÍ

Základní dohoda o navázání spojení:

CONNECTION REQUEST --->

<--- *CONNECTION ACCEPTED*

- problémy: duplikace paketu *Request* nebo ztráta *Accepted*

- potřebné vylepšení
  - unikátní identifikátor každé relace
  - omezená životnost požadavku
  - nutný 3. paket („potvrzení potvrzení“)

NAVÁZÁNÍ SPOJENÍ

Správné řešení

- 3 pakety („three-way handshake“)
- identifikátor/čítač přenesených dat

CONECTION REQUEST --->

(seq = *x*)

<--- *ACKNOWLEDGE*

(seq = *y*, ack = *x*)

DATA --->

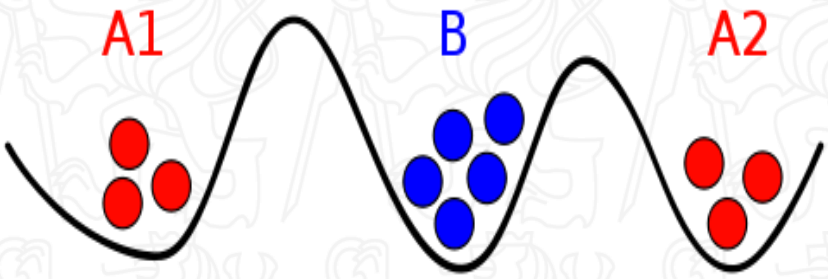
(seq = *x+1*, ack = *y*)

UKONČENÍ SPOJENÍ

- Asymetrické ukončení
  - jeden účastník ukončí spojení
    - příklad: telefonní hovor
  - možná ztráta dat
    - účastník mohl odeslal data před přijetím zprávy o ukončení
- Symetrické ukončení
  - obě strany se musí dohodnout
  - neexistuje zcela spolehlivé řešení, pokud komunikace není bezpečná
    - Problém dvou armád (Two Armies Problem / Coordinated Attack Problem / Two Generals' Problem)

UKONČENÍ SPOJENÍ

Premisa: A zvítězí, pokud A1 i A2 zaútočí najednou



- A1 pošle zprávu
  - není jisté že projde
- A2 odešle potvrzení
  - co když se ztratí zpráva nebo potvrzení?
    - A1 odpoví potvrzením přijatého potvrzení
- stále není jisté, že A1 i A2 se dohodli
    - další potvrzení ???

Důkaz neexistence řešení sporem:

Nechť *n* je délka nejkratšího protokolu. Je poslední, *n*-tý paket nezbytný?

ZAJIŠTĚNÍ SPOLEHLIVOSTI

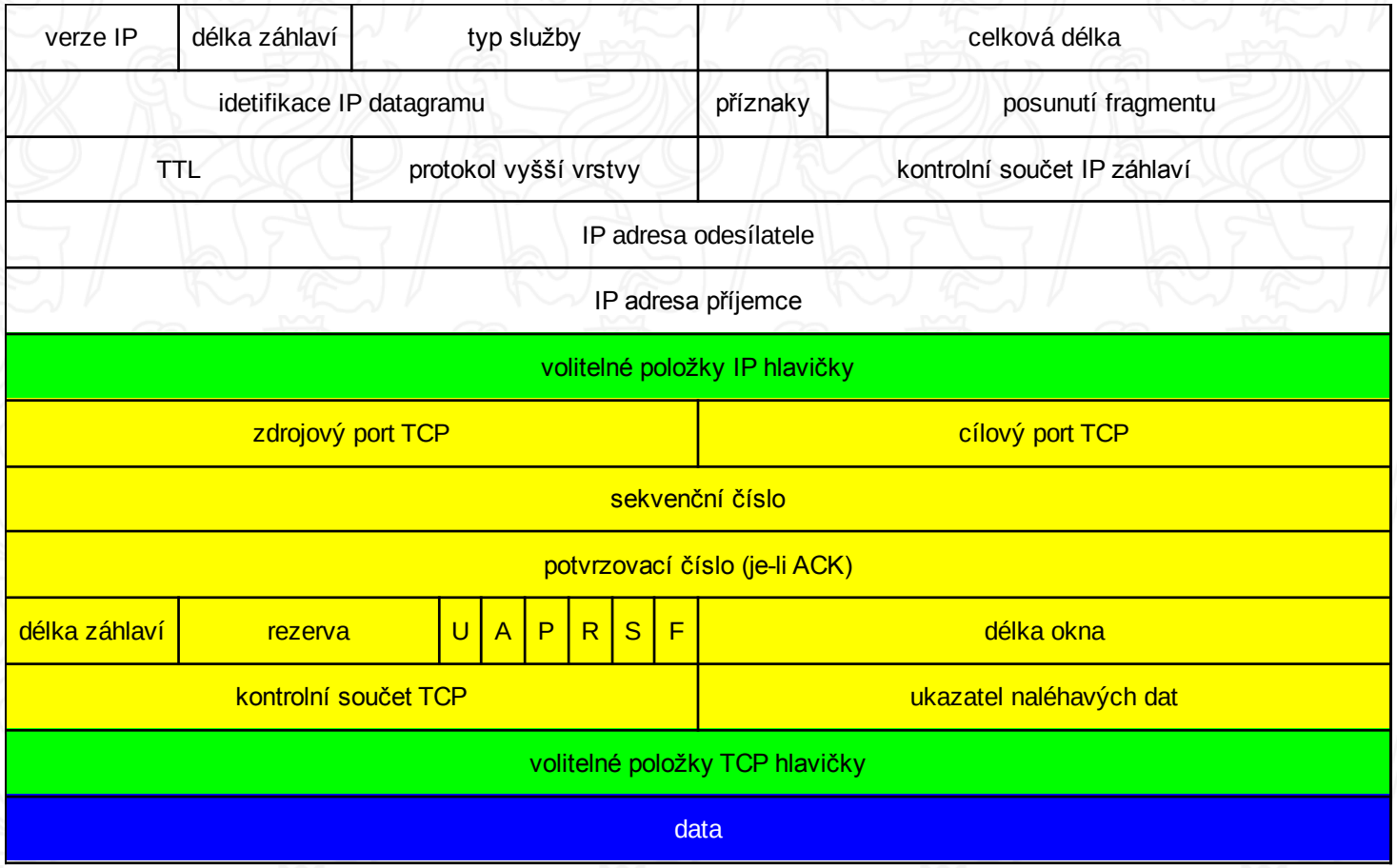
Princip obdobný jako v linkové vrstvě

- detekce chybných paketů
- eliminace duplikovaných paketů
  - sekvenční číslo
- omezený počet nepotvrzených paketů
  - „plovoucí okénko“ (sliding window)
- zamezení zahlcení (congestion control)
  - vynucené omezení/přerušení přenosu

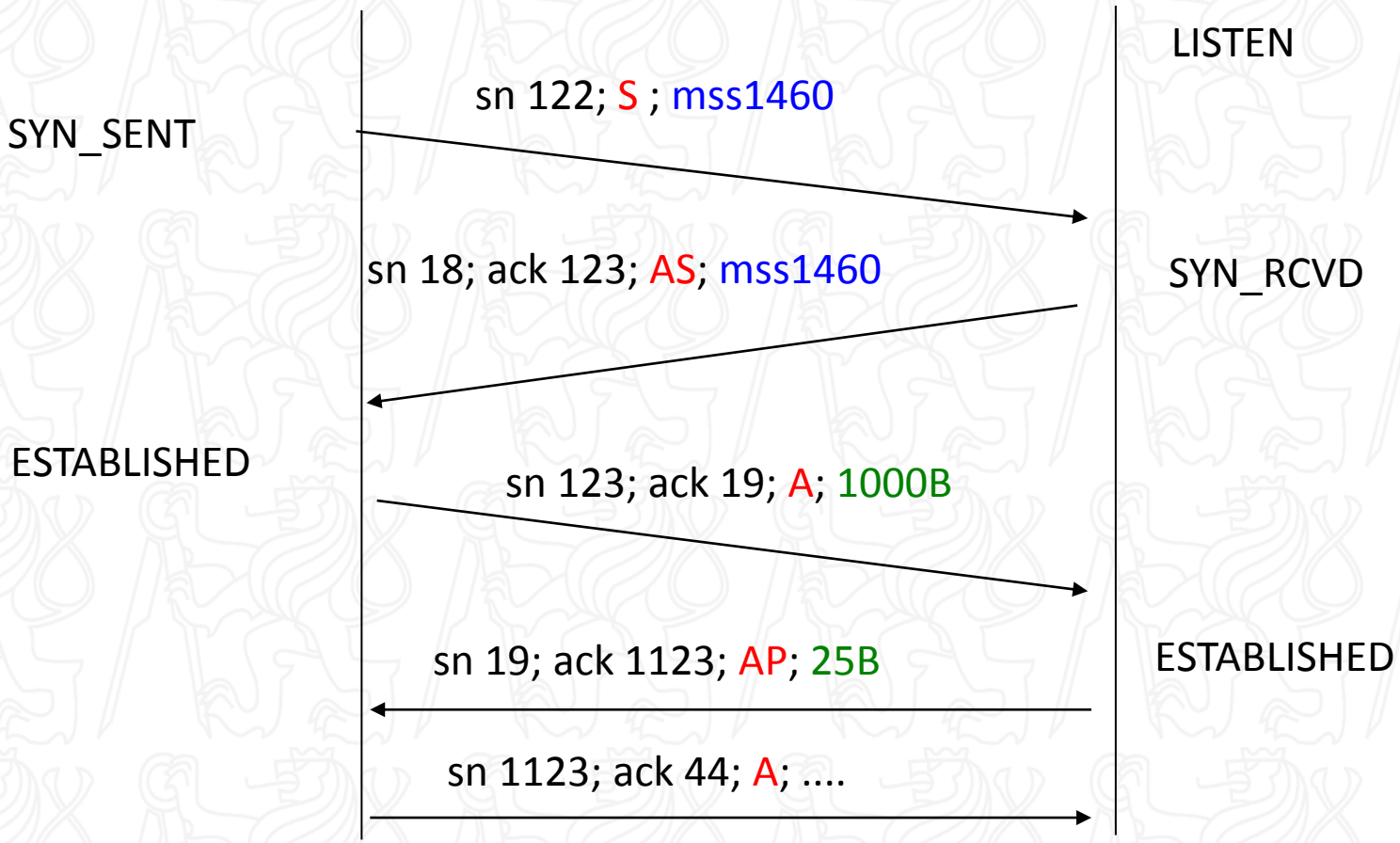
Transmission Control Protocol

- služba v L4
  - spojově orientovaná
  - zabezpečená
  - duplexní
  - v jedné relaci lze přenášet neomezený počet dat
- mnoho implementací
  - různá vylepšení (např. předcházení zahlcení, ...)
    - Reno
    - Tahoe
    - Vegas

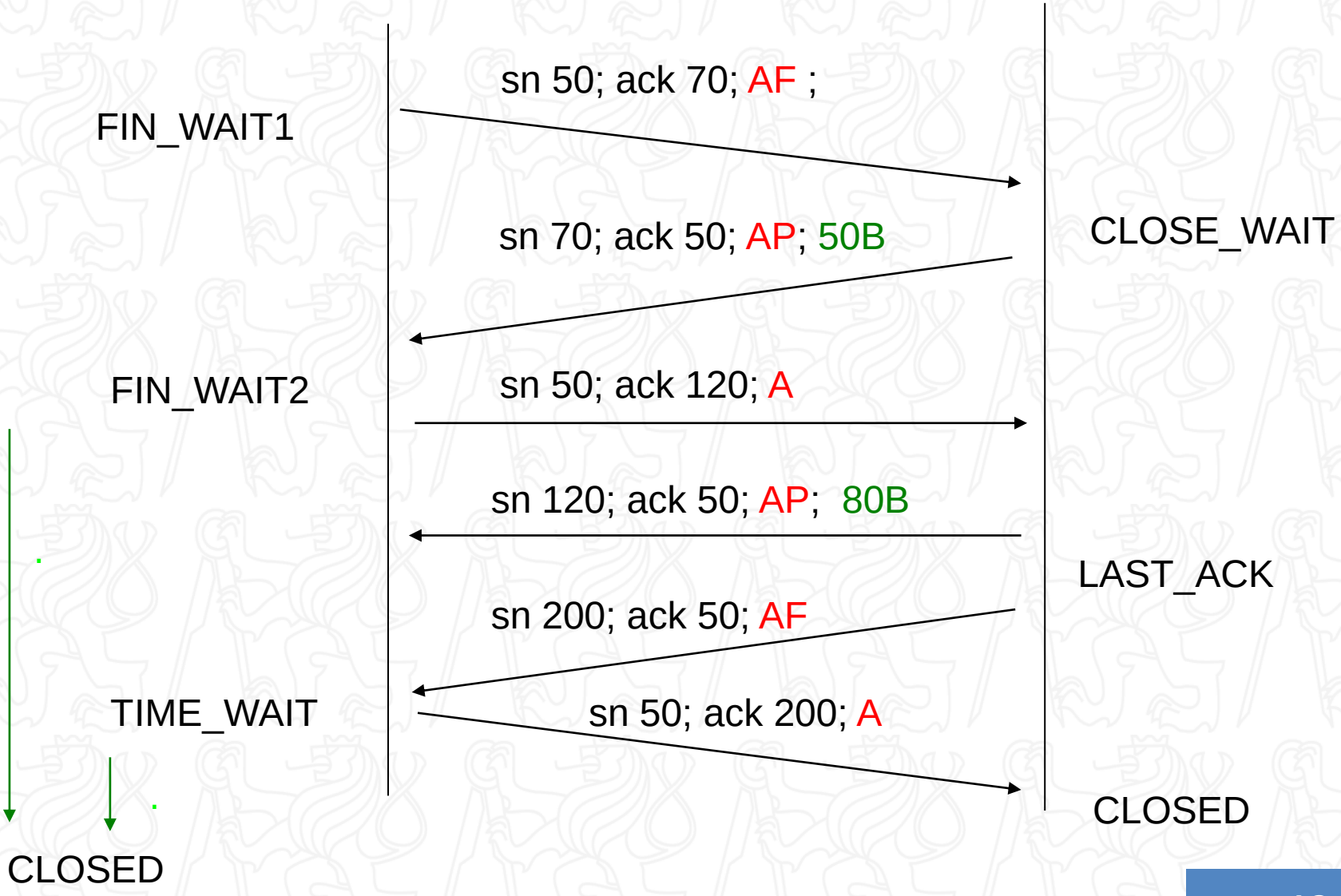
HLAVIČKA TCP



TCP – NAVÁZÁNÍ SPOJENÍ



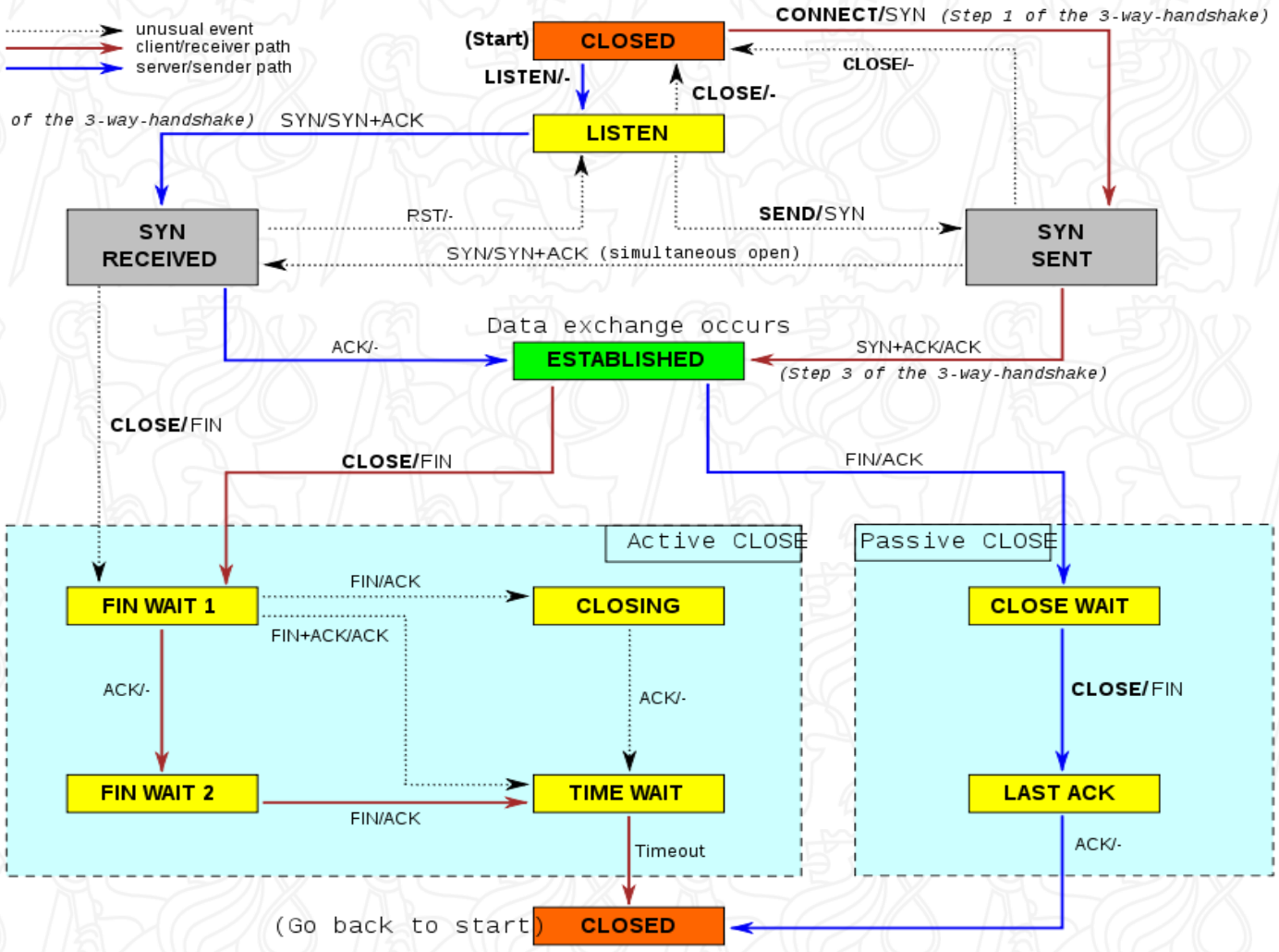
TCP - UKONČENÍ SPOJENÍ



VLASTNOSTI TCP

- zabezpečení
  - kontrolní součty
  - detekce duplicitních paketů
  - opakované odeslání
  - správné seřazení
  - timeout
- odesílání dat bez potvrzení předešlých
  - „sliding window“
- detekce zahlcení

TCP – STAVOVÝ DIAGRAM



POTVRZOVÁNÍ

- příjemce odesílá ACK
  - uvede pořadové číslo byte, který se očekává
  - tím potvrdí, že všechny předešlé byte byly přijaty
    - není nutné všechny potvrzovat pakety jednotlivě
- timeout (u odesílatele)
  - vysílání se vrátí k prvnímu nepotvrzenému paketu pokud nepřišlo potvrzení do očekávané doby

POTVRZOVÁNÍ II

- duplicitní ACK
  - pokud některý paket nepřijde, ale následující ano, příjemce zopakuje poslední ACK
  - slouží jako indikace, že se paket možná ztratil
- timeout (u příjemce)
  - do očekávaného okamžiku nepřišel nový paket
    - odešle se znovu poslední ACK
      - max. 3x opakovat

OKÉNKO ODESÍLATELE

Posuvné okénko (sliding window)

- položka *Délka okénka* je 16 bitů => max. 64 kB
- snižuje efektivitu pro velké rychlosti nebo zpoždění
  - bandwidth * delay
  - příklad: linka 1 Gbps
    - odeslání 64 kB trvá cca 0.5 ms
    - pro „delay“ 50 ms je linka využita jen z 1%
- řešení: option „Window scale“
  - posun o max. 14 bitů => 30 bitů pro velikost okénka

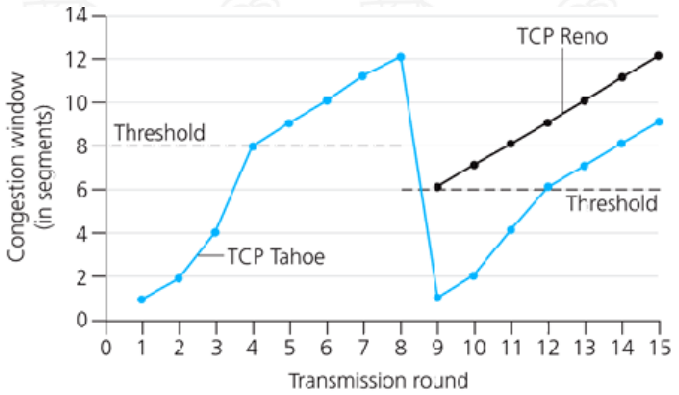
ZAMEZENÍ ZAHLCENÍ

Nelze odeslat více dat nepotvrzených než udává hodnota (Congestion Window)

- Proměnné využité „congestion control“:
  - MSS (Maximum Segment Size) – max. velikost posílaného paketu
    - definuje příjemce
  - SSTHRESH (Slow-start Threshold) – hranice pravděpodobného zahlcení
    - odhad, kolik nepotvrzených dat lze odeslat
    - v násobcích MSS
  - CWND (Congestion Window) – okénko odesílatele
    - kolik dosud nepotvrzených dat odesílatel vyšle
    - je nezávislé na „sliding window“

ZAMEZENÍ ZAHLCENÍ - ALGORITMUS

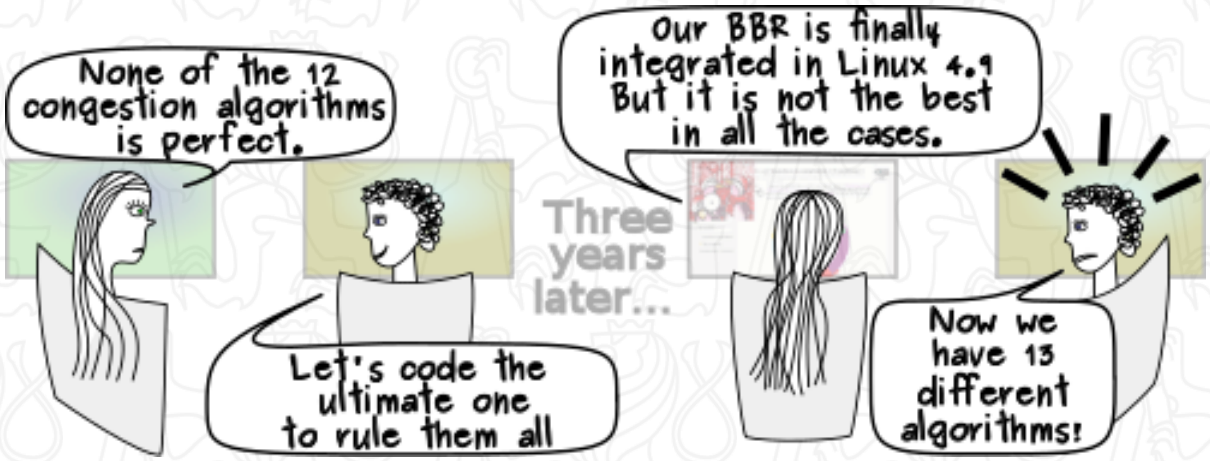
- pomalý start („slow start“)
  - počáteční hodnota CWND je 1
  - zpočátku se okénko odesílatele (CWND) zvětšuje 2x
    - velikost okénka roste exponenciálně !
- po dosažení SSTHRESH se CWND zvětšuje lineárně
- ztracený paket nebo jeho ACK se chápe jako příznak zahlcení (congestion)
  - opakuje se vysílání od posledního potvrzeného paketu
  - opakuje se slow start (verze Tahoo)
    - SSTHRESH se nastaví na polovinu CWND
  - CWND se zmenší na polovinu (verze Reno)



zdroj: http://black.goucher.edu/~kelliher/s2011

Stále jsou vyvíjeny nové algoritmy congestion control

Never ending story:



VYUŽITÍ TCP

TCP je nezbytné všude, kde je nutný zabezpečený datový kanál

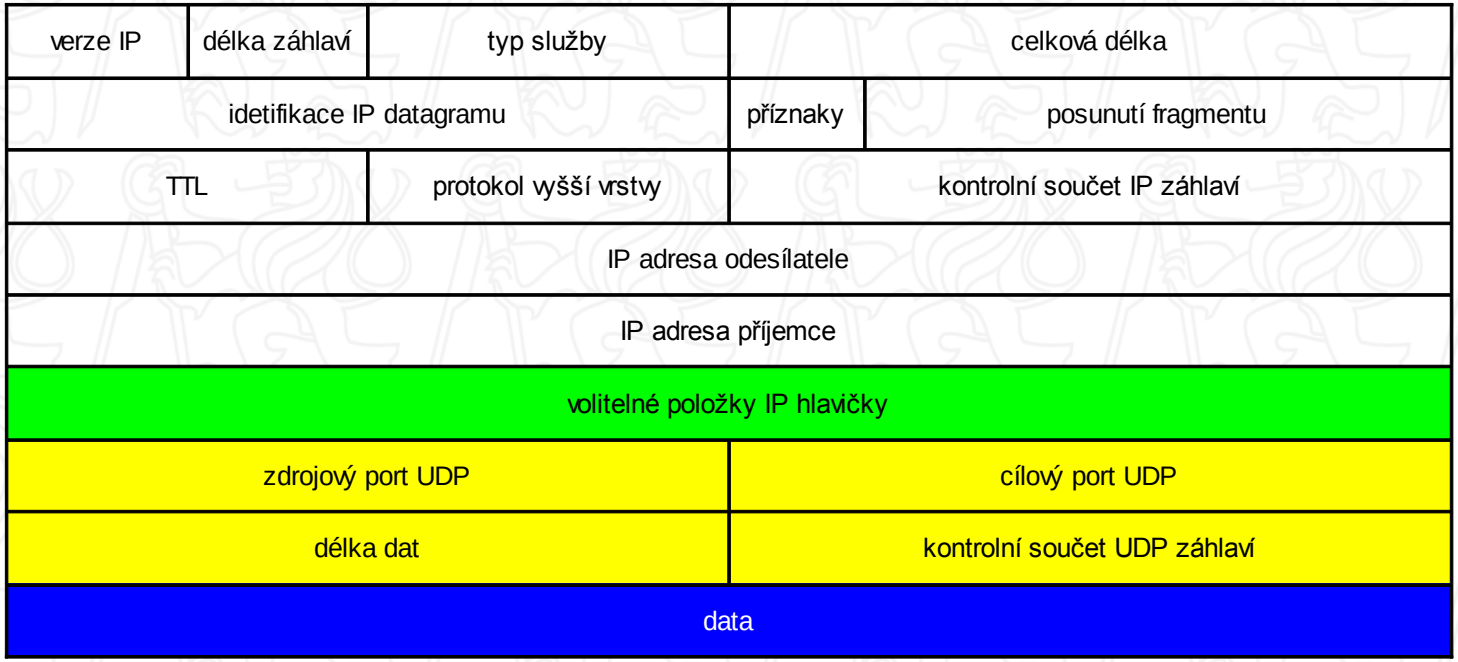
- není nutné pro
  - malé bloky dat
    - má velkou režii (čas i data)
- nevhodné pro
  - real-time aplikace: VOIP, streaming
    - paket je doručen za každou cenu – nežádoucí zpoždění
  - vestavné systémy (embedded-systems)
    - příliš komplexní

UDP

User Datagram Protocol

- služba v L4
  - nespojovaná
  - nezabezpečená
- porty
- max. 64 kB dat
  - většinou menší bloky dat
    - fragmentace ve vrstvě IP je nežádoucí

HLAVIČKA UDP



VYUŽITÍ UDP

Všude, kde není nutné zabezpečení nebo vadí režie TCP

- pro malé bloky dat
- nevadí případná ztráta
  - např. DNS
- je nežádoucí režie TCP
    - např NTP
- real-time aplikace
  - je lepší ztratit část dat než čekat

RTP

Real-time Transport Protocol

- přenos proudu (stream) dat mezi koncovými body v reálném čase
- hlavička obsahuje „timestamp“
  - čas od začátku streamu
  - jednotka závisí na aplikaci
  - umožní interpretovat přijatý blok
- implementováno většinou nad UDP

VYUŽITÍ RTP

- multimediální formáty
  - H.264, MPEG-4, MJPEG, MPEG, ...

- videokonference
- data streaming
- IP telefonie

Děkuji za pozornost