Počítačové siete
Transmission Control Protocol (TCP)
Explicit Congestion Notification (ECN)
SYN cookies

TCP

- spoľahlivý prúd byte-ov
- potvrdzovanie prijatých segmentov
- sliding window
  - okno sa posúva (a prípadne mení veľkosť) prijatím potvrdenia
  - odosielateľ môže poslať akýkoľvek segment dát, ktorý sa zmestí do okna
  - umožňuje príjemcovi regulovať rýchlosť odosielania dát

TCP

- ako dlho čakať na potvrdenie
  - čas (retransmit time-out, RTO) sa určuje dynamicky
    - zohľadňuje sa čas medzi odoslaním segmentu a prijatím potvrdenia (round-trip time, RTT)
  - reaguje na meniace sa podmienky na sieti
    - keď sa spomalí príchod potvrdení, predĺži sa RTO
    - keď sa zrýchli príchod potvrdení, skráti sa RTO

TCP – výpočet RTO

- na začiatku min. 1s
- po prvom zmeranom RTT:
  - SRTT = RTT
  - RTTVAR = RTT / 2
  - RTO = SRTT + 4 * RTTVAR
- po ďalšom zmeranom RTT
  - RTTVAR = 0.75 * RTTVAR + 0.25 * |SRTT – RTT|
  - SRTT = 0.875 * SRTT + 0.125 * RTT
  - RTO = SRTT + 4 * RTTVAR
- po vypršaní
  - RTO = 2 * RTO
- limit
  - min. 1s, max. 60s

TCP

- problémy s pomalou (alebo zahltenou) linkou na ceste
  - ak odosielateľ pošle priveľa segmentov, časť z nich sa zdrží alebo bude zahodená
  - vyprší RTO
  - odosielateľ ich pošle znovu
  - ak pôvodné segmenty neboli zahodené, dôjde k duplicitnému odoslaniu, čím sa situácia ešte zhorší
  - cieľom je, aby odosielateľ neposlal veľa naraz

TCP

- odosielateľ udržiava *congestion window*
  - koľko segmentov môže poslať (ak sa vojdú do normálneho TCP okna)
- slow start
  - cwnd na začiatku malé
  - zväčšuje sa o 1 segment každým prijatým potvrdením
    - až po určitú hranicu
- congestion avoidance
  - po dosiahnutí hranice pre slow start
  - cwnd sa zväčšuje o 1 segment za RTT

TCP

- pri vypršaní RTO
  - cwnd sa zmenší na 1 segment
  - hranica sa zmenší na polovicu počtu segmentov na ceste
- fast retransmit & fast recovery
  - po prijatí 3 duplicitných potvrdení po sebe
    - pravdepodobne sa stratil segment a prišli 3 neskoršie
  - nebude čakať na vypršanie RTO
  - zníži hranicu pre slow start na polovicu počtu segmentov na ceste
  - zníži cwnd na hranicu + 3
  - znovu pošle chýbajúci segment

Random Early Detection (RED)

- klasický prístup
  - kým sa pakety zmestia do frontu, pridávam
  - keď sa nezmestia, zahodím
- RED
  - podľa dĺžky frontu určujem pravdepodobnosť zahodenia
    - kým je málo zaplnená, pravdepodobnosť je 0
    - ako rastie, pravdepodobnosť stúpa
  - pakety zahadzujem s určenou pravdepodonosťou
    - teda aj skôr, než naozaj zaplním front na maximum

Explicit Congestion Notification

- umožňuje informovať odosielateľa o zahltení skôr, než dôjde k zahadzovaniu paketov
  - umožní reagovať na zahltenie bez straty
- vyžaduje podporu
  - na oboch koncoch spojenia
  - na router-och, ktoré chcú signalizovať zahltenie

ECN

- IP
  - 2 bity v hlavičke (ECN, spodné 2 bity v TOS/DSCP políčku)
    - 00 – ECN nie je podporované
    - 01, 10 – ECN je podporované
    - 11 – router signalizuje zahltenie
- TCP
  - 2 nové príznaky
    - ECE – signalizuje druhej strane prijatie informácie o zahltení
    - CWR – signalizuje druhej strane redukciu cwnd v reakcii na prijatie ECE

ECN

- dohodnutie (pri vytváraní spojenia)
  - SYN+ECE+CWR
    - indikuje, že iniciátor spojenia chce používať ECN
  - SYN+ACK+ECE
    - indikuje, že príjemca spojenia súhlasí s použitím ECN
- použitie
  - odosielateľ nastaví ECN v IP hlavičke na 10
  - router pri zahltení zmení ECN na 11
  - príjemca nastaví ECE v ACK pakete
  - odosielateľ zareaguje zmenšením cwnd a nastavením CWR v ďalšom segmente

RED + ECN

- RED
  - umožňuje včas identifikovať blížiace sa upchatie
- ECN
  - umožňuje na blížiace sa upchatie reagovať spomalením
- výhoda
  - spomalenie sa dosiahne skôr ako sa bude musieť zahodiť paket
  - efektívnejšie využitie linky

SYN cookies

- SYN flood
  - Denial of Service (DOS) útok na TCP
  - veľké množstvo falošných SYN paketov
    - vyčerpá zdroje obete
    - znefunkční legitímne spojenia
- SYN cookies
  - po vyčerpaní zdrojov na uloženie stavu nových spojení
  - umožní vytvoriť ďalšie legitímne spojenia bez potreby ďalších zdrojov pre nepotvrdené spojenia

SYN cookies

- špeciálna voľba počiatočného sekvenčného čísla na strane TCP servera
  - t – čas v 64 sekundových krokoch
  - m – MSS (maximum segment size)
  - s – 24 bit kryptografický hash IP adresy a portu servera, IP adresy a portu klienta a t
  - počiatočné sekvenčné číslo:
    - 5 bitov = (t mod 32)
    - 3 bity = reprezentácia MSS
    - 24 bitov = s

SYN cookies

- keď sa vyčerpajú zdroje pre uloženie kompletnej informácie zo SYN paketu klienta
  - zvolí sa jedna z 8 podporovaných hodnôt MSS
  - pošle sa SYN+ACK so špeciálnym sekv. číslom
  - nič sa neuloží
- keď sa následne príjme ACK
  - z potvrdzovacieho čísla sa určí počiatočné sekv. číslo
  - určí sa t, overí sa kryptografický hash
  - dekóduje sa MSS
  - vytvorí sa záznam, ktorý by sa normálne bol vytvoril po prijatí SYN paketu

SYN cookies

- nevýhody
  - neumožňuje použitie TCP options
    - napr. window scaling
  - obmedzuje použiteľné hodnoty MSS
- uvedené nevýhody sa však týkajú len spojení, ktoré by inak vôbec nevznikli
- užitočná metóda na zvládanie SYN flood útokov bez straty funkčnosti