Cvicenie10

OBSAH

Protokoly transportnej vrstvy

Úloha 1: Experimenty s metódou **sliding window** [editovať]

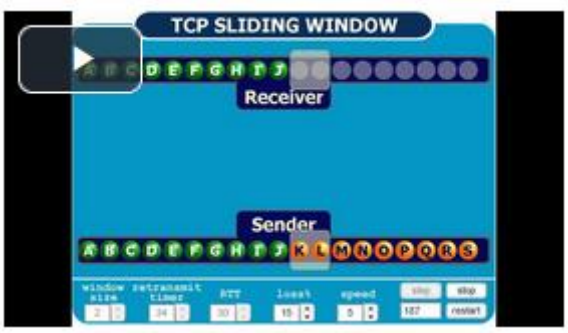
Preskúmajte ako pracuje metóda plávajúceho okna, na týchto ukážkach:

WS = 4, RTO (Retransmission Timeout) = 34, RTT (Round Trip Time) = 30, straty paketov = 10%, rýchlosť animácie=5

(www.youtube.com/watch?v=lk27yiITOvU)

- Čo je to RTT a RTO?
- Ako reaguje príjemca na príchod paketov mimo poradia? (napr. keď prvý segment nepríde, ale ďalšie 3 z okna veľkosti 4 áno)
    - aké/ako/koľko ACK posiela?

WS = 2, RTO = 34, RTT = 30, straty = 15%, rýchlosť animácie=5

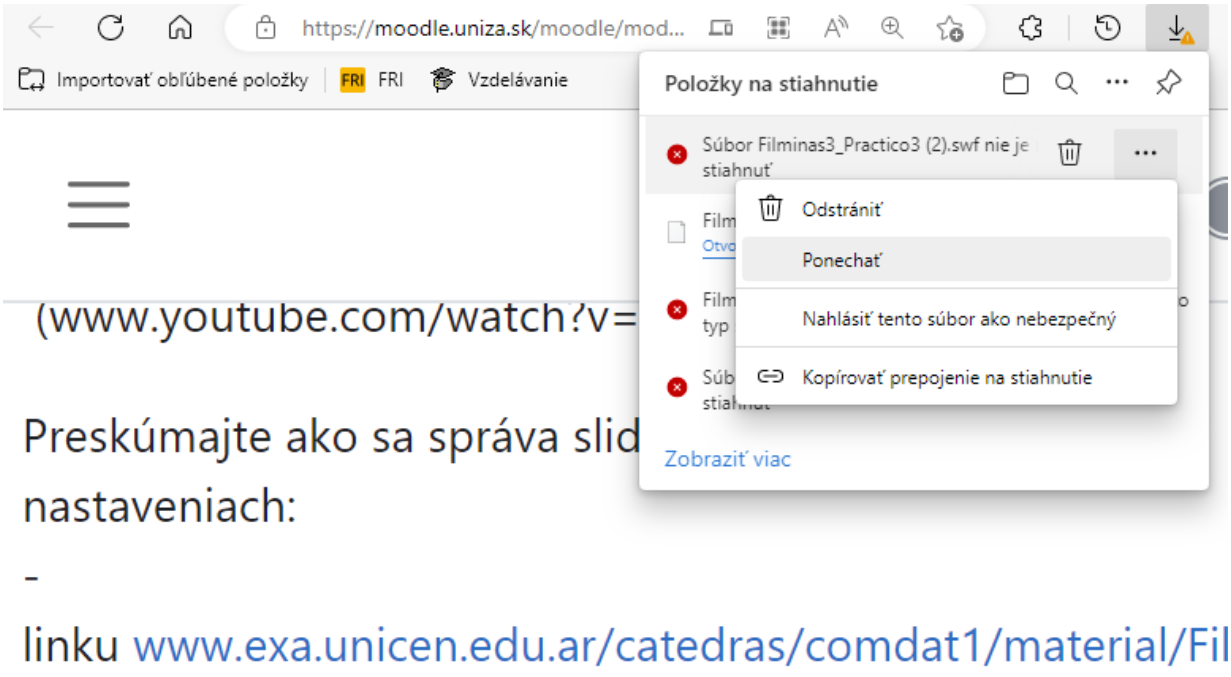


(www.youtube.com/watch?v=zY2pwPF6pl8)

Preskúmajte ako sa správa sliding window pri rôznych nastaveniach:

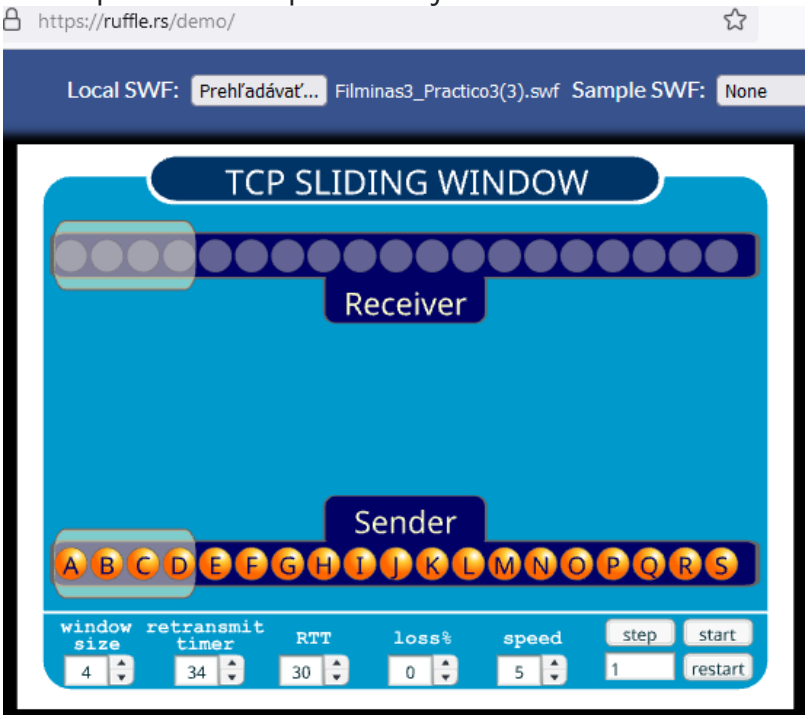
-

linku www.exa.unicen.edu.ar/catedras/comdat1/material/Filminas3_Practico3.swf vložte do webového prehliadača a súbor uložte.



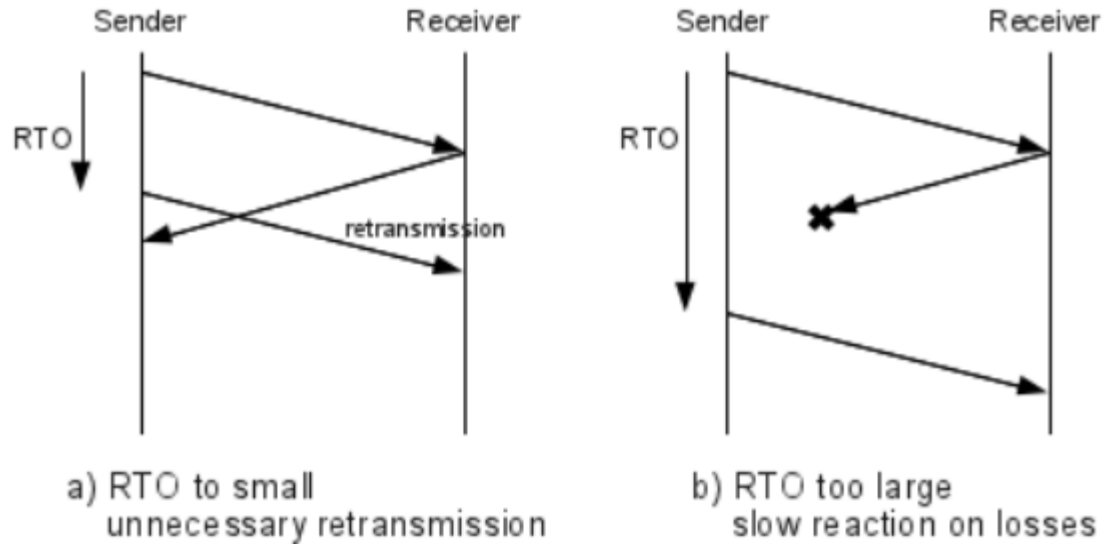
Potom tento súbor pesuňte na stránku https://ruffle.rs/demo/. Zobrazí sa animácia, ktorú môžete odštartovať alebo krokovať. Môžete tiež meniť veľkosť kĺzavého okna a

ďalšie parametre. Experimentujte s interaktívnou animáciou.



- Aký problém vidíte pri nenulových stratách a týchto nastaveniach:
  - RTT = 40, RTO = 20 ?
  - RTT = 20, RTO = 40 ?

http://sgros.blogspot.sk/2012/02/calculating-tcp-rto.html



Úloha 2: Preskúmajte polia **hlavičky TCP a UDP** segmentu vo **Wiresharku**

[editovať]

(bude potrebné používať filter, podľa IPsource a IPdestination, resp. **tcp.stream**==X, ..., **ip.addr** == ...)

- odchyťte komunikáciu so serverom **vzdelavanie.uniza.sk**:
    - aký trasnportný protokol sa využil?
    - preskúmajte **3-way-handshake**
        - aké sekvenčné čísla sa použili?
            - tu pozor, Wireshark zobrazuje realtívne sekvenčné čísla, t.j. prvé skutočné sekvenčné číslo prevedie na 0 a otatné potom zobrazí ako relatívne čísla, ktoré čísluje od 0
            - túto funkciu možno v programe vypnúť: Edit > Preferences > Protocols > TCP > Relative Sequence Number
                - keď si overíte že je to tak, vráťte nastavenia naspäť, lepšie sa čítajú relatívne ako absolútne čísla (plalí tak pre sekvenčné ako aj pre potvrdzovacie čísla)
        - ako narastajú čísla potvrdení (acknowledgement number, AN)? Odsledujte dva, alebo niekoľko za sebou idúcich AN, ktoré odosielate vy (source) na daný server
    - preskúmajte slušné ukončenie spojenia (2x 2-way-handsake: FIN, ACK)
        - akými a koľkými segmentami klient zo serverom rozviazal spojenie?
    - veľkosť okna
        - aké okno si nastavila vaša strana a aké príjemca?
        - použil sa Windows Scale (hľadajte iba v SYN segmentoch v časti naspodu v Options)

- čo je možné vidieť pri "Folow TCP stream?"

- pri komunikácii s **DHCP serverom** (vypnite a zapnite sieťovú kartu, resp. **ipconfig /renew**; Wireshark - Filter: **dhcp**, alebo bootp)
    -
        - aký trasnportný protokol sa využil?
        - aké/koľko má polí?
- Nájdite v odchytenej prevádzke (akejkoľvek, nemusí byť len HTTP komunikácia so serverom vzdelavanie.uniza.sk):
    - reset spojenia
        - preskúmajte Flags, ...
    - **MSS**, Windows Scale a podporu pre SACK v Options:
        - pozerajte a hľadajte iba v SYN segmentoch
        - windows scale je výška/hodnota mocniny (**scaling factor** je potom 2^**windows scale**)
        - v ostatných segmentoch, teda mimo tých čo nesú SYN je tiež viditeľný scaling factor, ale to len preto, že to Wireshark pre používateľov programu tak dekóduje a zobrazuje... a prepočíta pre nás Calculated Windows Size.

        - doplňujúce info k položkám KIND a LENGTH v TCP options si pozrite v nsledovnom linku a nájdite tam hodnoty pre MSS, Windows Scale a **SACK**: zdroj info
    - segment s príznakov PUSH a segment nesúci urgentné dáta
        - doplňujúce info na tomto zdroji

Úloha 3: Sledovanie štatistík pomocou utility **netstat** [editovať]

- aké prepínače má tento príkaz?
- aký výstup dávajú?
- aké máte otvorené **TCP spojenia**?
    - v akom sú stave? vidíte aj iné ako ESTALISHED?
    - čo by sa stalo keby sme tam videli aj iné stavy?
    - ktoré z nich indikujú nejakú chybu spojenia?
    - pozrite stavový diagram z prednášky, a pokúste sa na cvičení analyzovať

Úloha 4: Prieskum **TCP procesu** v programe **Packet Tracer** [editovať]

Táto úloha je **hodnotená**, pracuje sa v pripravenej topológii v programe PT (podobnú topológiu sme používali na cvičení 6, tu sme ju však dopracovali pre potreby tohto cvičenia 10).

Odovzdáva sa **pka** súbor, v ktorom **názov súboru**, ktorý si stiahnete z odkazu nižšie nijako nebudete meniť, iba na jeho koniec pridáte: **_Priezvisko_Meno** (t.j. za pôvodný názov súboru, a príponu pka samozrejme ponecháte, nepoužívajte v Priezvisko_Meno diakritiku).

Po otvorení pka súboru zadajte do **User profile:**

-
    - Name zadajte svoje: **Priezvisko_Meno** (bez diakritiky, pričom študenti s viac menami uvedú prvé meno, a tí s viacerými priezviskami, uvedú posledné priezvisko
    - E-mail: **login@stud.uniza.sk** (zadajte váš študentský e-mail)
    - Additional info: **2023** (zadajte aktuálny rok)

inak vám riešenie neuznáme.

Vypracované riešenie je potrebné odovzdať do nedele pol noci v týždni, kedy je úloha zadaná.

Stručný nákres topológie: PC1 - SW1 - R1 - R2 - SW2 - PC2
Stručný popis úlohy (konkrétne inštrukcie nájdete v odkaze nižšie vo Word dokumente):

- použite **simulačný** mód a na počítači Web Client v prehliadači si vyžiadajte stránku (192.168.10.254) zo servera Web server a sledujte, **či sa zdrojové a cieľové porty menia** alebo nemenia od zdroja k cieľu - sledujeme hlavičku na každom zariadení, ktorým segment prechádza od zdroja k cieľu
    - vo Wiresharku toto nemáme možnosť vidieť (vidíme iba segmenty idúce z/na náš počítač)
- sledujte (použite simulačný mód a nahliadnite do hlavičiek) ako sa prenášajú dáta pri spojení na smerovač cez TELNET aplikačný protokol
    - v programe PT nastavte Filter: **tcp** aj **telnet** (na karte Misc - vpravo dole)
    - na smerovači R2 nakonfigurujte prístup pre TELNET (password a login) a heslo do privilegovaného módu
    - odsledujte hlavičky (heslo vkladajte po znakoch a po každom znaku odkrokujte Capture/Foreword) a zistite:
        - ako sa segmentujú dáta prenášané aplikačným protokolom telnet? čo sa posiela v jednom segmente? aké to má výhody pre danú aplikáciu? aké nevýhody pre priepustnosť danej siete?
        - je vidieť v prenášaných segmentoch aj heslo, ktoré ste zadávali pri prihlasovaní sa na konzolu smerovača cez TELNET? prečo?

- **Inštrukcie:**
    - v slovenčine: PIKS_LAB_10.4_TCP_process_investigation_in_PT_instructions_SK_2023_04_25
    - v angličtine: PIKS_LAB_10.4_TCP_process_investigation_in_PT_instructions_EN_2023_04_25
- **Topológia:** PIKS_LAB_10.4_TCP_process_investigation_in_PT_topology_2022_04_25.pka