Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií

Zadanie 2: Komunikácia s využitím UDP protokolu

Návrh riešenia

Peter Smreček

AIS ID: 103130

E-mail: xsmrecek@stuba.sk

Predmet: PKS

Deň a čas cvičenia: Pondelok 15:00

Semester: ZS 20/21

Ročník: 2.

Obsah

1. Zadanie úlohy

Navrhnite a implementujte program s použitím vlastného protokolu nad protokolom UDP (User Datagram Protocol) transportnej vrstvy sieťového modelu TCP/IP. Program umožní komunikáciu dvoch účastníkov v lokálnej sieti Ethernet, teda prenos textových správ a ľubovoľného súboru medzi počítačmi (uzlami).

Program bude pozostávať z dvoch častí – vysielacej a prijímacej. Vysielací uzol pošle súbor inému uzlu v sieti. Predpokladá sa, že v sieti dochádza k stratám dát. Ak je posielaný súbor väčší, ako používateľom definovaná max. veľkosť fragmentu, vysielajúca strana rozloží súbor na menšie časti - fragmenty, ktoré pošle samostatne. Maximálnu veľkosť fragmentu musí mať používateľ možnosť nastaviť takú, aby neboli znova fragmentované na linkovej vrstve.

Ak je súbor poslaný ako postupnosť fragmentov, cieľový uzol vypíše správu o prijatí fragmentu s jeho poradím a či bol prenesený bez chýb. Po prijatí celého súboru na cieľovom uzle tento zobrazí správu o jeho prijatí a absolútnu cestu, kam bol prijatý súbor uložený.

Program musí obsahovať kontrolu chýb pri komunikácii a znovuvyžiadanie chybných fragmentov, vrátane pozitívneho aj negatívneho potvrdenia. Po prenesení prvého súboru pri nečinnosti komunikátor automaticky odošle paket pre udržanie spojenia každých 10-60s pokiaľ používateľ neukončí spojenie. Odporúčame riešiť cez vlastne definované signalizačné správy.

2. Návrhu programu a komunikačného protokolu

Program je implementovaný v programovacom jazyku Python s používateľským rozhraním v konzole.

2.1 Nadviazanie a ukončenie spojenia

Po spustení programu v móde „server“ musí používateľ zadať port, na ktorom bude server prijímať komunikáciu. Je nutné zvoliť port z rozsahu 1024–49151, pretože porty menšie ako 1024 sú systémové a well-known porty a väčšie ako 49151 sú ephemeral porty.

Po spustení programu v móde „klient“ musí používateľ zadať IP adresu servera, nachádzajúceho sa v lokálnej sieti. Z dôvodu dištančnej výučby a prezentovania riešenia iba na svojom zariadení nastavujeme túto IP adresu na loopback `127.0.0.1`. Následne je nutné zadať port servera, na ktorom bude server počúvať.

Po zadaní IP a portu klient automaticky odošle signalizačnú správu pre otvorenie spojenia s príslušným flagom. Server signalizačnú správu spracuje, overí jej formát, zistí z nej port klienta a pošle signalizačnú správu klientovi pre potvrdenie otvorenia spojenia s príslušným flagom. Klient ju taktiež overí a ak je spojenie úspešne nadviazané, klient aj server

vypíšu hlásenie. Ak spojenie nie je úspešne nadviazané, program vypíše hlásenie, zatvorí socket na oboch stranách a opätovne ponúkne voľbu módu.

Ak je spojenie úspešne nadviazané, otvorí sa v programe klienta menu, kde si používateľ vyberie, či chce preniesť dáta (text alebo súbor), alebo chce zapnúť/ vypnúť udržiavanie spojenia pomocou keepalive správ, alebo uzatvoriť spojenie explicitne. Ak si používateľ vyberie prenos dát, vyberie, či chce preniesť text alebo súbor a vyberie maximálnu veľkosť fragmentu. Potom sa prenesú dáta. Po prenose dát sa klient vráti do menu. Ak klient zapne posielanie keepalive správ, začnú sa posielať keepalive správy s príslušným flagom v stanovených časových intervaloch. Ak používateľ nezvolí zapnutie keepalive správ, alebo ich po zapnutí neskôr vypne, server po troch chýbajúcich keepalive správach vyhodnotí spojenie ako spojenie bez akejkoľvek komunikácie a ukončí ho. Spojenie sa ukončí poslaním signalizačnej správy o ukončení spojenia s príslušným flagom. Ak používateľ v menu zvolí explicitné ukončenie spojenia, pošlú sa signalizačné správy s príslušným flagom o ukončení spojenia. Po akomkoľvek ukončení spojenia sa sockety zatvoria a program sa prepne do výberu módu server/ klient.

2.2 Štruktúra hlavičky

<table>
<tr><td colspan="2">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="2">Length</td><td>Checksum</td></tr>
<tr><td colspan="3">Poradové číslo</td></tr>
<tr><td colspan="3">CRC</td></tr>
<tr><td colspan="2">Veľkosť (veľkosť hlavičky + veľkosť dát)</td><td>Flag</td><td>Dáta</td></tr>
<tr><td colspan="3">Dáta (pokračovanie)</td></tr>
</table>

Source Port, Destination Port, Length a Checksum sú polia UDP hlavičky, ktoré hlavička obsahuje predvolene.

Pole Poradové číslo označuje poradie fragmentu v súbore. Vďaka nemu je možné zoradiť fragmenty do správneho poradia, aj keď prídu v rôznom poradí.

Pole CRC je kontrolný súčet hlavičky a dát. Klient ho vypočíta a zapíše do hlavičky, s tým, že počas výpočtu toto pole považuje za nulové. Server ho vypočíta samostatne a overí s tým, ktoré dostal doručené. Ak sa serverom vypočítané a doručené CRC nezhoduje, tak server označí fragment za chybný.

Pole Veľkosť (veľkosť hlavičky + veľkosť dát) určuje veľkosť v bajtoch, ktorú má mnou navrhnutá hlavička (polia, ktoré sú označené v tabuľke modrou) + veľkosť prenášaných dát.

Pole Flag obsahuje jeden bajt určujúci typ správy. Podľa flagu dokáže program očakávať, čo bude uložené v poli Dáta (názov súboru, fragment dát, číslo nesprávne doručeného fragmentu, ...). Hodnoty Flagu som navrhol nasledovne:

1. a určuje inicializáciu spojenia

2. `b` určuje posielanie fragmentu textovej správy
3. `c` určuje posielanie posledného fragmentu textovej správy
4. `d` určuje posielanie názvu súboru
5. `e` určuje posielanie fragmentov súboru
6. `f` určuje posielanie posledného fragmentu súboru
7. `g` určuje ukončenie spojenia
8. `p` určuje pozitívne potvrdenie
9. `n` určuje negatívne potvrdenie
10. `k` určuje keepalive

UDP hlavička sama o sebe má 8 bajtov. Poradové číslo a CRC sú premenné typu `unsigned int`, Veľkosť je premenná typu `short`, Flag je premenná typu `char`. Mnou navrhnutá hlavička má teda 11 bajtov. Celá UDP hlavička má teda 19 bajtov.

Pole Dáta môže prenášať 0 až 1461 bajtov. 1461 bajtov je maximum, ktoré je možné preniesť bez fragmentácie na linkovej vrstve. Táto hodnota sa počíta ako maximálna veľkosť payloadu Ethernet II rámca – veľkosť IP hlavičky – veľkosť UDP hlavičky – veľkosť vlastnej hlavičky, tj. 1500 – 20 – 8 – 11 = 1461. Pole Dáta slúži na prenos samotných dát (súboru alebo textovej správy), alebo názvu súboru, alebo na prenos čísel nesprávne doručených fragmentov. V prípade fragmentácie súboru, alebo textovej správy môže byť maximálna veľkosť fragmentu zvolená používateľom od 1B do 1461B, keďže to je maximálna veľkosť, ktorú dokáže pole dát preniesť bez fragmentácie na linkovej vrstve.

2.3 Metóda kontrolnej sumy

Pre potreby kontroly integrity informácií v hlavičke a samotných dát som vybral ako metódu kontroly CRC (Cyclic Redundancy Check), teda kontrolu cyklickým kódom. Na výpočet hodnoty CRC používam funkciu `mkCrcFun` z balíka `crcmod`.

CRC má v mnou navrhnutej hlavičke vlastné pole. CRC sa vypočítava z hlavičky a prenášaných dát. Klient hodnotu CRC vypočíta a zapíše do hlavičky, s tým, že počas výpočtu pole CRC v hlavičke považuje za nulové. Server, po prijatí paketu vypočíta vlastné CRC, kde taktiež počas výpočtu považuje pole CRC za nulové. Server vlastné vypočítané CRC overí s tým, ktoré dostal doručené v hlavičke. Ak sa serverom vypočítané a v hlavičke doručené CRC nezhodujú, tak server označí fragment za chybný a opätovne si ho vyžiada podľa pravidiel použitej ARQ metódy.

2.4 Metóda vnesenia chyby do prenosu

Do prenosu je vložená chyba takým spôsobom, že pri výpočte CRC na strane klienta je výsledok výpočtu zmenšený o 1 a až potom uložený do hlavičky. Takto odoslaný paket bude na strane servera, po opätovnom výpočte CRC, vyhodnotený ako chybný, pre nezhodujúce sa hodnoty CRC.

V programe je možnosť zapnúť vnášanie chyby do paketu. Chyba bude vnesená do prvého paketu nesúceho dáta. Teda pri textovej správe to bude úplne prvý paket, pri prenose súboru to bude druhý paket, pretože prvý paket obsahuje názov súboru a poškodzujem iba dátové pakety.

2.5 Metóda ARQ

Selective Repeat ARQ je metóda, ktorá opätovne vyžiada iba pakety, ktoré boli vyhodnotené ako poškodené, alebo nedoručené.

Server postupne potvrdzuje prijatie fragmentov od klienta tak, že klient na toto potvrdenie nečaká, ale posiela ďalšie fragmenty dovtedy, dokým nevyčerpá možnosti svojho okna. Ak klient vyčerpal možnosti svojho okna a má od servera doručené potvrdenia o doručení paketov, posúva okno a pokračuje v prenose ďalších fragmentov. Ak nejakému fragmentu vyprší čas čakania na potvrdenie doručenia, alebo príde od serveru negatívne potvrdenie značiace príjem chybného paketu, klient opätovne tento paket odošle. Týmto sa zabezpečí, že serveru budú doručené všetky pakety. V prípade, že sú pakety doručené v nesprávnom poradí, server ich usporiada do správneho poradia.

2.6 Metóda udržiavania spojenia

Server automaticky uzatvorí spojenie po tom, ako nedostane 3 keepalive správy, alebo žiadne dáta.

Klient po nadviazaní spojenia má v menu možnosť zvoliť, či chce posielať dáta (text alebo súbor), udržiavať spojenie pomocou keepalive správ, alebo explicitne ukončiť spojenie. V prípade voľby explicitného ukončenia spojenia pošle klient správu s príslušným flagom a server na ňu odpovie správou s príslušným flagom pre ukončenie spojenia. Následne server aj klient zavrú socket a program sa vráti do výberu módu.

Ak je u klienta aktívne posielanie keepalive správ, posiela keepalive správu s príslušným flagom serveru každých 10 sekúnd. Na každú keepalive správu server odpovie správou s príslušným flagom. Ak neprebieha prenos dát a posielanie keepalive správ je prerušené, server po 3 neprijatých keepalive správach spojenie ukončí vyslaním signalizačnej správy s príslušným flagom o ukončení prenosu a následne zatvorí socket a vráti sa výberu módu. Ak klient obdrží správu o ukončení spojenia od serveru, zatvorí socket a vráti sa do výberu módu programu.

Ak je u klienta aktívne posielanie keepalive správ a zároveň chce používateľ odoslať dáta, počas odosielania dát je posielanie keepalive správ prerušené a obnovené je až po úspešnom odoslaní všetkých dát.

2.7 Diagram spracovávania komunikácie

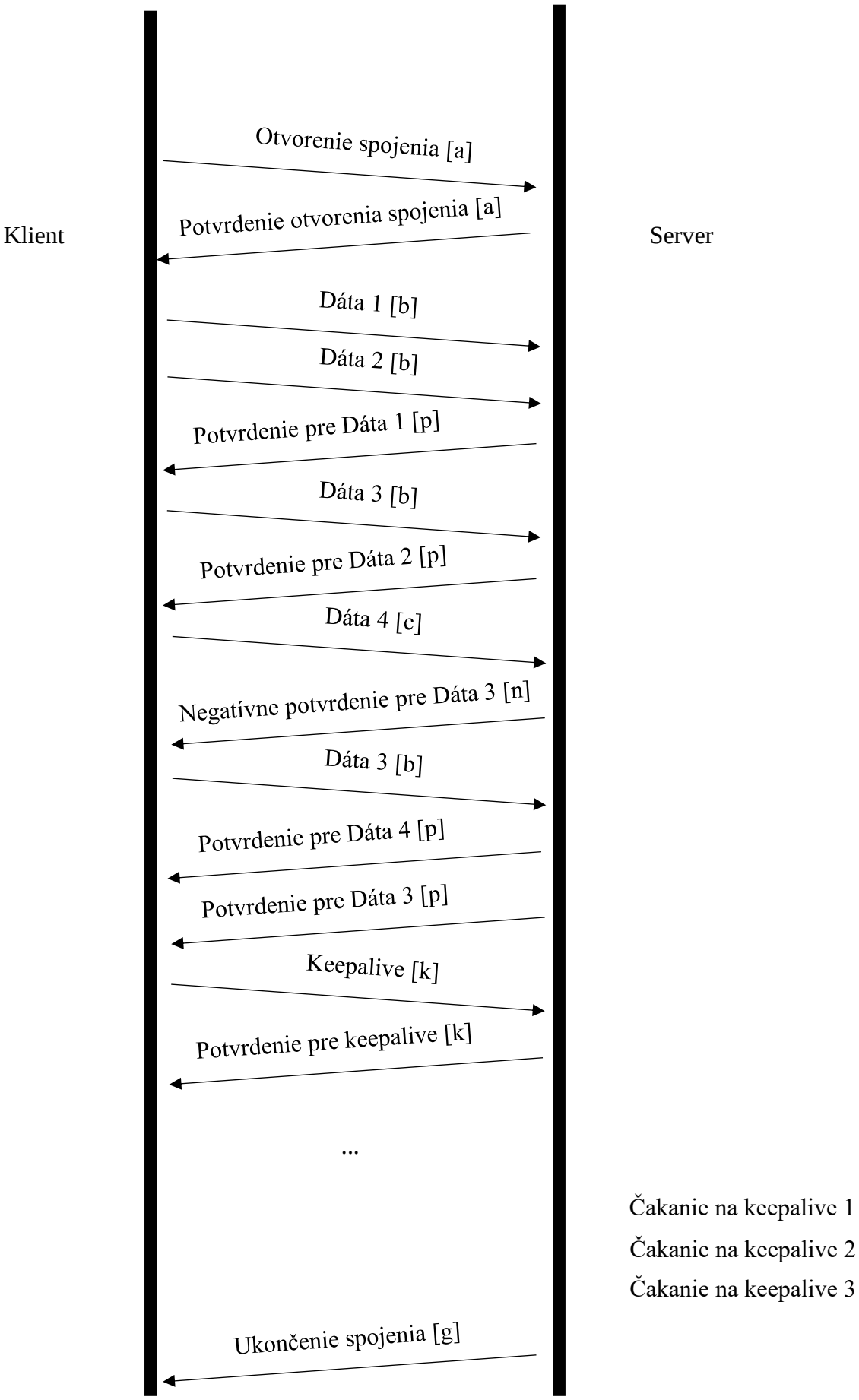
Klient
Server
Otvorenie spojenia [a]
Potvrdenie otvorenia spojenia [a]
Dáta 1 [b]
Dáta 2 [b]
Potvrdenie pre Dáta 1 [p]
Dáta 3 [b]
Potvrdenie pre Dáta 2 [p]
Dáta 4 [c]
Negatívne potvrdenie pre Dáta 3 [n]
Dáta 3 [b]
Potvrdenie pre Dáta 4 [p]
Potvrdenie pre Dáta 3 [p]
Keepalive [k]
Potvrdenie pre keepalive [k]
...
Čakanie na keepalive 1
Čakanie na keepalive 2
Čakanie na keepalive 3
Ukončenie spojenia [g]

Diagram zobrazuje nadviazanie spojenia medzi klientom a serverom. Po nadviazaní spojenia klient odosiela textovú správu zloženú zo 4 fragmentov, kde 3. fragment je poškodený a bude nutné ho odoslať znova.

Prvé tri fragmenty sú označené flagom `b`, posledný je označený flagom `c`, ktorý symbolizuje, že je to posledný fragment. Okno má pre vizuálnosť nastavenú veľkosť 2. Fragment Dáta 3 simuluje prenos chyby, server túto chybu odhalí a pomocou správy s flagom `n` si fragment 3 vyžiada znova. Fragment je opätovne poslaný, bez straty fragmentu 4, ktorý bol poslaný korektne, no ešte pred korektným doručením fragmentu 3. Každý korektne prijatý fragment server potvrdí správou s flagom `p`. Klient nečaká na tieto správy po každom fragmente, ale prichádzajú postupne a posúvajú tak okno.

Alternatívne, ak klient vyčerpá možnosti svojho okna a zároveň neprišla žiadna pozitívna alebo negatívna potvrdzujúca správa, nemôže poslať ďalší fragment, pokým nejakému fragmentu nevyprší čas na prijatie potvrdzujúcej správy od servera. Ak nejakému fragmentu vyprší čas na prijatie potvrdzujúcej správy, klient predpokladá, že fragment nebol doručený a klient pošle fragment ktorému chýba potvrdenie automaticky znova.

Spojenie sa v tomto konkrétnom diagrame ukončuje po 3 nedoručených keepalive správach. Alternatívne je možné ho ukončiť z klientovej strany odoslaním správy s flagom `g`, na ktorú by server odpovedal správou s flagom `g`.

Diagram zobrazuje prenos textových dát, alternatívne v prípade prenosu súboru najskôr klient odosiela paket s flagom `d` nesúcim meno súboru a potom posiela fragmenty súboru s flagmi `e`, pričom posledný fragment má flag `f`.

V diagrame neuvádzam šípky potvrdení a negatívnych potvrdení začínajúce v ústí šípky fragmentu dát, ako by to po správnosti malo byť. Pre prehľadnosť diagramu šípky potvrdení a negatívnych potvrdení uvádzam tak, aby sa nekrižovali. V diagrame nad šípkami uvádzam popis operácie a v [] flag, ktorý je zapísaný v hlavičke a značí typ paketu.

2.8 Popis kódu

Program som implementoval v programovacom jazyku Python. V programe som použil balík `socket` na prenos správ po sieti, balík `struct` na vytváranie štruktúr podobných jazyku C a balík `crcmod` na počítanie CRC kódu, ktorý používam ako checksum.

Keďže kód nie je dokončený a pre potreby odovzdania návrhu nie je potrebný, komentár kódu doplním pred finálnym odovzdaním.