Immagine che contiene testo, screenshot, clipart

Descrizione generata automaticamente

Ingegneria di Internet e Web

Progetto A.A. 2019/2020

UDP-GBN

Massimo Mazzetti

0253467

**INDICE**

[1. Traccia del Progetto 2](#_Toc119632712)

[2. Architettura e scelte progettuali 4](#_Toc119632713)

[3. Implementazione 5](#_Toc119632714)

[4. Limitazioni 6](#_Toc119632715)

[5. Piattaforma utilizzata per sviluppo e testing 7](#_Toc119632716)

[6. Esempi 8](#_Toc119632717)

[7. Valutazione Prestazioni 9](#_Toc119632718)

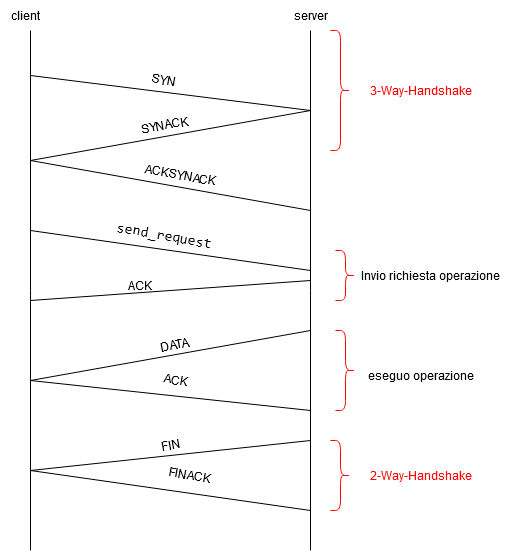
[8. Configurazione, Installazione eD Esecuzione 10](#_Toc119632719)

# Traccia del Progetto

|  |  |
| --- | --- |
|  | **Reti di Calcolatori ed Ingegneria del Web - A.A. 2019/20**  **Progetto B1: Trasferimento file su UDP**  Lo scopo de progetto è quello di progettare ed implementare in linguaggio C usando l’API del socket di Berkeley un’applicazione client-server per il trasferimento di file che impieghi il servizio di rete senza connessione (socket tipo SOCK\_DGRAM, ovvero UDP come protocollo di strato di trasporto). Il software deve permettere:  • Connessione client-server senza autenticazione;  • La visualizzazione sul client dei file disponibili sul server (comando list);  • Il download di un file dal server (comando get);  • L’upload di un file sul server (comando put);  • Il trasferimento file in modo affidabile.  La comunicazione tra client e server deve avvenire tramite un opportuno protocollo. Il protocollo di comunicazione deve prevedere lo scambio di due tipi di messaggi: messaggi di comando: vengono inviati dal client al server per richiedere l’esecuzione delle diverse operazioni; messaggi di risposta: vengono inviati dal server al client in risposta ad un comando con l’esito dell’operazione.  **Funzionalità del server**  Il server, di tipo concorrente, deve fornire le seguenti funzionalità:  • L’invio del messaggio di risposta al comando list al client richiedente; il messaggio di risposta contiene la filelist, ovvero la lista dei nomi dei file disponibili per la condivisione;  • L’invio del messaggio di risposta al comando get contenente il file richiesto, se presente, od un opportuno messaggio di errore;  • La ricezione di un messaggio put contenente il file da caricare sul server e l’invio di un messaggio di risposta con l’esito dell’operazione.  **Funzionalità del client**  I client, di tipo concorrente, deve fornire le seguenti funzionalità:  • L’invio del messaggio list per richiedere la lista dei nomi dei file disponibili;  • L’invio del messaggio get per ottenere un file  • La ricezione di un file richiesta tramite il messaggio di get o la gestione dell’eventuale errore  • L’invio del messaggio put per effettuare l’upload di un file sul server e la ricezione del messaggio di risposta con l’esito dell’operazione.  **Trasmissione affidabile**  Lo scambio di messaggi avviene usando un servizio di comunicazione non affidabile. Al fine di garantire la corretta spedizione/ricezione dei messaggi e dei file sia i client che il server implementano a livello applicativo il protocollo Go-Back N (cfr. Kurose & Ross “Reti di Calcolatori e Internet”, 7° Edizione). Per simulare la perdita dei messaggi in rete (evento alquanto improbabile in una rete locale per non parlare di quando client e server sono eseguiti sullo stesso host), si assume che ogni messaggio sia scartato dal mittente con probabilità p. La dimensione della finestra di spedizione N, la probabilità di perdita dei messaggi p, e la durata del timeout T, sono tre costanti configurabili ed uguali per tutti i processi. Oltre all’uso di un timeout fisso, deve essere possibile scegliere l’uso di un valore per il timeout adattativo calcolato dinamicamente in base alla evoluzione dei ritardi di rete osservati. I client ed il server devono essere eseguiti nello spazio utente senza richiedere privilegi di root. Il server deve essere in ascolto su una porta di default (configurabile). |

# Architettura e scelte progettuali

L'applicazione presenta un'architettura di tipo Client-Server.

Il client e il server utilizzano il protocollo di livello 4 UDP.

La fruizione del servizio avviene in quattro fasi:

* Instaurazione della connessione tramite 3-Way-Handshake.
* Il client richiede che operazione fare (GET, PUT, LIST).
* Il server esegue la richiesta da parte del client in modo affidabile tramite il protocollo Go-Back N.
* Chiusura della connessione tramite il 2-Way-Handshake al termine dell’operazione.

I messaggi scambiati sono di 3 tipi:

* Comandi;
* Dati;
* Risposta.

Si è scelto un server concorrenziale a processi per semplicità sviluppo e manutenibilità in quanto difficilmente si incorrerà nella saturazione delle risorse di sistema; tuttavia, rimane il fatto che essa risulterà più lenta rispetto ad altre soluzioni a causa del cambio di contesto.

A fine di permettere la rilevazione di connessioni morte è stato realizzato un sistema che consente un numero massimo di ritrasmissioni e un tempo massimo per inviare una richiesta da parte del client.

L’Instaurazione avviene, come già detto, tramite 3-Way-Handshake, cioè vengono scambiati 3 messaggi:

* SYN: Inviato dal client al server per richiedere di connettersi;
* ACKSYN: Inviato dal server al client come riscontro del SYN e manda al client un numero di porta che sarà associata alla socket del figlio che servirà il client;
* ACKSYNACK, inviato dal client al server, riscontra il SYNACK e serve al server per avere conferma che il client è ancora presente ed ha ricevuto le informazioni necessarie per l’instaurazione della connessione, così se ciò non è vero il server può deallocare le risorse dedicate a quello specifico client e renderle di nuovo disponibili per altre eventuali richieste di connessione.

La richiesta dell’operazione avviene con 2 messaggi:

* Il client invia un dato contenente quale operazione svolgere:
* Il server invia un ACK per riscontrare quell’operazione e inizia a eseguire l’operazione.

La chiusura della connessione, come già detto, tramite 2-Way-Handshake, cioè vengono scambiati 2 messaggi:

* FIN: inviato da chi invia dati quando finisce l’operazione e conseguente chiusura della connessione;
* ACKFIN: riscontro del FIN.

# Implementazione

**Struttura pacchi**

I messaggi scambiati tra server e client come visto nella sezione precedente sono di tre tipi (comandi, dati e risposta) e sono stati implementati tramite una struct data\_packet.

|  |
| --- |
| struct data\_packet {      int type;      long seq\_no;      int length;      char data[MTU];  }; |

Essa viene utilizzata per lo scambio di dati, messaggi di comando, messaggi di sincronizzazione e messaggi di riscontro, per lo svolgimento di tale compito possiede quattro attributi:

* type (int), indica il tipo di messaggio; che può essere un comando (PUT, LIST, GET), un dato (NORMAL) oppure un messaggio di sincronizzazione (SYN, FIN).
* seq\_no (long), il quale indica il numero di sequenza del pacchetto, in caso di SYN indica un codice identificativo della richiesta.
* length (int), il quale indica la lunghezza in byte del dato nel campo “data”.
* data (char [MTU], dove MTU vale 1024), il quale contiene il dato che viene scambiato( NORMAL nel caso contiene un dato relativo al tipo di servizio richiesto dal client (chunk di file oppure un nome di file su server che può essere scaricato/caricato dal client).

**Perdita simulata**

Per simulare la perdita di messaggi è stata creata la funzione:

|  |
| --- |
| bool simulate\_loss(float loss\_rate)  {    double value;    struct timespec tms;    if (clock\_gettime(CLOCK\_REALTIME, &tms))    {      srand(time(NULL));    }    else    {      int64\_t micros = tms.tv\_sec \* 1000000;      micros += tms.tv\_nsec / 1000;      if (tms.tv\_nsec % 1000 >= 500)      {        ++micros;      }      srand(micros);    }    int r1 = rand() % 100;    int r2 = rand() % 100;    int r3 = rand() % 100;    unsigned short vec[3] = {r1, r2, r3};    seed48(vec);    value = drand48();    if (value < loss\_rate){      return true;    }    return false;  } |

La funzione prende in ingresso un parametro float relativo alla probabilità di perdita inserita dall'utente, ed in base ad esso, attraverso un procedimento di generazione di valori randomici per l'impostazione del seed della funzione drand48() della libreria stdlib.h, produce un valore float pseudorandomico nell'intervallo [0, 1). In base al valore ottenuto la funzione ritornerà un booleano per indicare se debba essere applicato o meno l'evento di perdita.

**Server**

L’implementazione del server si divide in quattro parti:

1. **Inizializzazione:** 
   1. si prendono i parametri inseriti dall’utente e tramite questi si crea la socket (UDP) di ascolto utilizzando il numero di porta passato dall’utente e ne fa la bind.
2. **Instaurazione della connessione:** 
   1. si entra in un loop infinito dove la prima operazione è una “**recvfrom**” bloccante dove si attende richieste di connessione da parte del client. Quando arriva una richiesta di connessione si prende il dato nel campo seq\_no ricevuto e lo salva, infine si crea una socket per il figlio associata al processo e si fa la bind.
   2. Poi, si entra in un nuovo loop infinito dove per prima cosa si controlla il numero di tentativi (meccanismo per evitare connessioni morte), in caso il numero di tentativi sia maggiore di 20 la socket ad esso assegnata viene chiusa e il numero di porta ridiventa disponibile.
   3. Invio un data\_packet al client, che rappresenta il SYNACK, di tipo SYN e con il seq\_no uguale all’id della richiesta ricevuta e contenente nel campo data il numero di porta associato al nuovo socket. Successivamente viene lanciato il timer.
   4. Viene poi controllato il timeout verificando che l’interallo di tempo trascorso dal lancio del timer supera il valore del timer inserito dall’utente (((clock() - timer\_sample) \*1000)/ CLOCKS\_PER\_SEC > timer) in caso ritorni vero (quindi si verifichi il timeout) si incrementa il trial\_counter e si rinvia il SYNACK.
   5. Infine, vi è il blocco di ricezione dell’ACKSYNACK con una “recvfrom” non bloccante che attende un data\_packet dal client e se è di tipo SYN e il seq\_no è uguale all’id della richiesta si esce dal while.
   6. Quando si esce dal while l’instaurazione della connessione con il client è avvenuta con successo, viene fatta la fork del processo figlio dedicato al client.

Il chiude il riferimento alla socket associata al client con il quale si è instaurata la connessione, in modo che alla terminazione del processo figlio la socket venga effettivamente chiusa, mentre se ci si trova nel figlio ci si mette in attesa del comando del client.

1. **Attesa del comando:**
   1. Si entra in un loop infinito nel quale viene lanciato un timer tramite la funzione “alarm” che chiude la connessione se il client non invia un’operazione in un determinato lasso di tempo.
   2. Si mette in attesa tramite una “recvfrom” bloccante. Una volta ricevuto il comando invia un ACK della corretta ricezione del comando indicato nel campo type.
   3. Tramite uno switch a seconda del tipo del data\_packet (GET, PUT, LIST) si eseguirà l’operazione scelta utilizzando le impostazioni inserite dall’utente al lancio del server.
2. **Esecuzione dell’operazione:**
   1. **GET** si dichiara il data\_packet, nel campo type si dichiara che è di tipo GET e nel campo data si inserisce il nome del file da inviare infine viene chiamata la funzione **Upload\*.**
   2. **PUT** si dichiara il data\_packet, nel campo type si dichiara che è di tipo PUT e nel campo data si inserisce il nome del file da ricevere infine viene chiamata la funzione **Download\*.**
   3. **LIST** si dichiara il data\_packet e nel campo type si dichiara che è di tipo LIST e viene chiamata la funzione **Upload\***.

**Client**

L’implementazione del client si divide in quattro parti:

1. **Inizializzazione:**
   1. si prendono i parametri inseriti dall’utente e tramite questi si crea la socket (UDP) che utilizzerà per comunicare con il server e fa la connect per fissare i componenti del server, infine viene installato il gestore della SIGALARM che segnalerà all’utente quando avverrà il timeout per la scelta dell’operazione.
2. **Richiesta connessione:**
   1. Si entra in un loop infinito dove per prima cosa si verifica il numero di tentativi
   2. Poi viene inviato il SYN che è un data\_packet di tipo SYN in cui il campo seq\_no viene generato randomicamente
   3. Viene fatto partire il timer
   4. Viene poi controllato il timeout verificando che l’interallo di tempo trascorso dal lancio del timer supera il valore del timer inserito dall’utente (((clock() - timer\_sample) \*1000)/ CLOCKS\_PER\_SEC > timer) in caso ritorni vero (quindi si verifichi il timeout) si incrementa il trial\_counter e si rinvia il SYN.
   5. Poi vi è il blocco di ricezione dell’SYNACK con una “recvfrom” che attende un data\_packet dal client e se è di tipo SYN e il seq\_no è uguale all’id della richiesta si esce dal while.
   6. Ricevuto il SYNACK ne viene estrapolato il contenuto, cioè il nuovo numero di porta che sarà associato al processo server che servirà il client
   7. Successivamente viene inviato l’ACKSYNACK di tipo SYN e seq\_no pari all’id della richiesta
   8. Vengono aggiornate le informazioni remote del server, cioè viene settata una nuova “struct sockaddr” che è stata chiamata “child\_addr” con il numero di porta ricevuto
   9. Viene fatta di nuovo la connect per fissare queste informazioni.
   10. Si entra in un loop dove viene lanciato il timer (tempo massimo per selezionare un’operazione)
   11. Si prende il valore inserito dall’utente e tramite uno switch si eseguirà l’operazione scelta utilizzando le impostazioni inserite dall’utente al lancio del client.
3. **Invio del comando:**
   1. Si entra in un loop infinito
   2. Si verifica il numerod ei tentativi
   3. Invia il comando che è un data\_packet in cui nel campo type viene inserito il tipo di operazione che si vuole svolgere e si fa partire un timer
   4. Viene poi controllato il timeout verificando che l’interallo di tempo trascorso dal lancio del timer supera il valore del timer inserito dall’utente (((clock() - timer\_sample) \*1000)/ CLOCKS\_PER\_SEC > timer) in caso ritorni vero (quindi si verifichi il timeout) si incrementa il trial\_counter e si rinvia il comando.
   5. Si mette in attesa di ricevere l’ACK e se è dello stesso tipo del comando inviato si esce dal ciclo
4. **Scambi di dati:**
   1. **GET** si dichiara il data\_packet, nel campo type si dichiara che è di tipo GET e nel campo data si inserisce il nome del file da ricevere infine viene chiamata la funzione **Download\*.**
   2. **PUT** si dichiara il data\_packet, nel campo type si dichiara che è di tipo PUT e nel campo data si inserisce il nome del file da inviare infine viene chiamata la funzione **Upload\*.**
   3. **LIST** si dichiara il data\_packet e nel campo type si dichiara che è di tipo LIST e viene chiamata la funzione **Download\***.

**Timer Dinamico**

Così come previsto dalla specifica, è stata inserita la possibilità di utilizzare un timer statico, il cui valore espresso in millisecondi viene configurato in fase di avvio e rimane invariato per tutta la durata dell'esecuzione dell'applicazione. È stata inserita anche la possibilità di utilizzare un timer dinamico, il cui valore, anch'esso espresso in millisecondi, tende a adattarsi in base allo stato del canale. Viene inizializzato al valore di default di 1 secondo, in modo da consentire una immissione 'prudente' nel canale seguendo l'approccio 'fair' di TCP.

Il timer dinamico viene ricalcolato in 2 diversi momenti:

* **Quando avviene un Timeout:** Il Timer viene settato al doppio dell’ultimo valore utilizzato, se il valore è superiore a 10 secondi il timer viene reimpostato al suo valore di default (1 secondo), questo viene fatto per “sbloccare” il canale e limitare l’attesa.
* **Quando, in fase di invio dei file, ricevo un ACK**:

|  |
| --- |
| sample\_RTT = (clock() - start\_sample\_RTT) \* 1000 / CLOCKS\_PER\_SEC;              estimated\_RTT = (double)(0.875 \* estimated\_RTT) + (0.125 \* sample\_RTT);              dev\_RTT = (double)(0.75 \* dev\_RTT) + (0.25 \* fabs(sample\_RTT - estimated\_RTT));              timer = (double)estimated\_RTT + (4 \* dev\_RTT); |

**Upload**

**Download**

La funzione Download viene eseguita quando si vuole ricevere un file o quando si vuole avere la lista dei file presenti sul server.

1. Se il tipo dell’operazione (passato dal data\_packet) è GET o PUT
2. Si entra in un loop infinito
3. Si controlla il numero dei tentativi
4. Si mette in attesa di una “recvfrom” bloccante che attende dei segment\_packet i quali conterranno i chunk di file provenienti dal client (NORMAL) oppure il FIN, il pacchetto può essere scartato per simulare la perdita tramite la funzione “simulate\_loss” in caso non venga scartato, ci possono essere tre opzioni:
   1. Se l’operazione non è LIST e se il data\_packet ricevuto sono dati (NORMAL) quello che viene fatto è scrivere su file con la funzione “write” lenght byte del campo data del messaggio ricevuto (se per qualche motivo non vengono scritti tutti, ci si riposiziona indietro nel file di un numero di byte pari a quelli effettivamente scritti e non si riscontra il pacchetto) si genera poi un data\_packet di tipo NORMAL e con seq\_no pari al seq\_no del data\_packet ricevuto, infine si incrementa il contatore “expected\_sequence\_no” il quale come intuibile dal nome indica il prossimo pacchetto che il server si aspetta.
   2. Se l’operazione è LIST i dati ricevuti non sono chunk di file ma stringhe contenenti il nome dei file scaricabili da server, quest’ultime vengono solamente stampate a schermo.
   3. In caso si riceva un FIN, se il FIN è di errore (si riconosce perché il campo lenght è diverso da 0) si rimuove il file che si era creato utilizzando la rm\_string, si estrapola la stringa di errore contenuta nel FIN, lo si stampa a schermo ed infine si genera un data\_packet di tipo FIN con seq\_no pari al seq\_no del data\_packet ricevuto e si esce dal while.
5. Dopo la fase di ricezione, viene inviato il data\_packet generato in precedenza tramite la “sendto” e si continua il while. Se si è usciti dal while significa necessariamente che è stato ricevuto un FIN, non avendolo fatto prima viene inviato con la “sendto” il data\_packet di FIN che era stato solamente generato, viene chiuso il file (se l’operazione non era LIST) e la socket del figlio.

# Limitazioni

# Piattaforma utilizzata per sviluppo e testing

Lo sviluppo è avvenuto in ambiente Unix in particolare si è utilizzata una **WSL2** (Windows Subsystem for Linux) su cui è installata la distribuzione “**Ubuntu 20.04.4 LTS**”.

La versione del Kernel è “**5.10.60.1-microsoft-standard-WSL2**”.

Per la compilazione è stato utilizzato “**gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0**”.

Per la scrittura del codice è stato utilizzato il text editor “**Visual Studio Code**”.

# Esempi

# Valutazione Prestazioni

|  |  |  |  |
| --- | --- | --- | --- |
| Perdita | Finestra | Timer [ms] | Tempo esecuzione [ms] |
| 0 |  |  |  |
| 0.2 |  |  |  |
| 0.5 |  |  |  |
| 0.8 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Configurazione, Installazione ed Esecuzione