

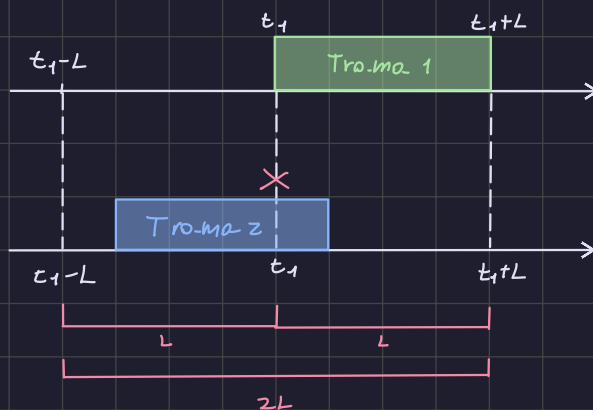
Esercizio 27/09/23

### Domande sulla teoria (4 punti ciascuna)

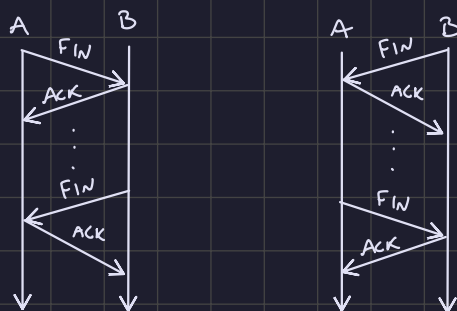
Lo studente risponda in maniera concisa, ma precisa, alle seguenti domande riguardanti la parte teorica. E' necessario che lo studente ottenga almeno 7 punti (su un totale di 12 punti a disposizione). In caso contrario, gli esercizi non verranno considerati e il voto finale sarà insufficiente.

1. Si dia una definizione di periodo di vulnerabilità per una rete ad accesso multiplo con mezzo condiviso e si mostri come esso possa essere ricavato nel caso di protocollo ALOHA, supponendo che nella rete le stazioni generino trame della stessa lunghezza pari a  $L$  (byte).
2. Non tutti gli indirizzi IP possono essere assegnati agli host: ve ne sono alcuni, definiti "indirizzi speciali", che hanno un particolare utilizzo. Tra questi, vi sono: l'indirizzo composto da tutti "1", l'indirizzo composto da tutti "0", l'indirizzo in cui l'host ID e' composto da tutti "1", l'indirizzo in cui l'host ID e' composto da tutti "0". Per ciascuno dei 4 indirizzi si spieghi il loro utilizzo.
3. Si descriva la fase di chiusura della connessione nel TCP, indicando i messaggi scambiati e i principali campi dell'header utilizzati durante tale fase. Si specifichino le diverse sequenze di messaggi in base a chi inizia la chiusura.

1. Il periodo di vulnerabilità è quell'intervallo di tempo in cui una trama può subire collisioni e dipende dal protocollo. Per ricavarlo dal protocollo ALOHA supponiamo che tutte le trame sono generate della stessa lunghezza  $L$  e che la prima stazione ne generi una al tempo  $t_1$ . Il protocollo ALOHA dice che se una stazione ha una trama da trasmettere lo fa subito e mentre trasmette ascolta per controllare se c'è una collisione. Da questo sappiamo che una trama non può essere generata nell'intervallo  $[t_1, t_1 + L)$  perché ci sarebbe una collisione, però non può neanche essere generata prima di questo intervallo perché altrimenti la fine della seconda trama sarebbe contenuta nell'intervallo della prima, di conseguenza si creerebbe una collisione anche se la seconda trama venisse generata nell'intervallo  $(t_1 - L, t_1]$ . Unendo questi due intervalli abbiamo che il periodo di vulnerabilità di ALOHA è la lunghezza dell'intervallo  $(t_1 - L, t_1 + L)$ , cioè  $2L$ .



2. Ci sono alcuni indirizzi IP che sono riservati e hanno un significato speciale. Gli indirizzi riservati sono:
  - 0.0.0.0: È l'indirizzo IP che un host assume quando non gli è stato assegnato alcun indirizzo IP.
  - 255.255.255.255: È l'indirizzo IP di local broadcast, cioè permette di inviare un messaggio a tutti gli host di una rete locale.
  - Host ID a 0: È l'indirizzo che identifica una rete e nessun host può avere questo indirizzo.
  - Host ID a 1: È l'indirizzo IP di directed broadcast, cioè permette di inviare un messaggio a tutti gli host di una rete locale specifica identificata dai bit di prefisso.
3. Per chiudere una connessione TCP bisogna dichiararlo attraverso uno scambio di messaggi che dovrà essere effettuato da entrambe le direzioni della comunicazione. I principali campi utilizzati sono:  
Flag: Per interrompere la connessione viene settato a 1 il flag FIN, mentre il flag ACK viene messo a 1 per inviare il riscontro.  
La connessione si può interrompere in 2 modi:  
Da un lato alla volta: La connessione viene chiusa soltanto da una direzione perché ha finito di trasmettere, ma rimane comunque in ascolto perché l'altra direzione può comunque continuare a comunicare finché non interrompe la trasmissione.

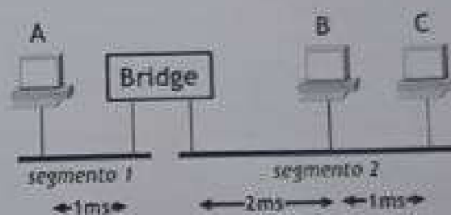


Da entrambi i lati: La connessione può essere direttamente interrotta da entrambi i lati contemporaneamente e questo viene fatto settando entrambi i flag FIN e ACK a 1.



### Esercizio 1 (7 punti)

Si consideri la configurazione in figura, dove due segmenti di rete sono collegati da un Bridge; sul segmento 1 vi è una stazione (A), mentre sul segmento 2 vi sono 2 stazioni (B e C). Il Bridge è un particolare tipo di stazione che memorizza ciascuna trama che arriva da un segmento di rete e, una volta ricevuta completamente, la ritrasmette sull'altro segmento di rete (tale comportamento è valido, in modo indipendente l'uno dall'altro, in entrambi i sensi); le trame restano in memoria del Bridge fino a quando la trasmissione sull'altro segmento non è andata a buon fine.



Le stazioni e il Bridge utilizzano un protocollo **CSMA persistent**. Le caratteristiche del sistema sono:

- velocità dei segmenti: 800 kbit/s;
- lunghezza delle trame generate dalle stazioni: 1200 byte;
- ritardo di propagazione pari ad 1 ms tra la stazione A e il bridge, pari a 2 ms tra il bridge e la stazione B, e pari a 1 ms tra la stazione B e la stazione C;

Le stazioni generano le seguenti trame:

- stazione A: due trame (A1 e A2) agli istanti  $t_{A1}=310$  e  $t_{A2}=336$  msec, la prima diretta ad C, la seconda diretta a B;
- stazione B: una trama (B1) all'istante  $t_{B1}=316$  diretta ad A;
- stazione C: una trama (C1) all'istante  $t_{C1}=322$  diretta ad A;

In caso di collisione, si supponga che le stazioni decidono di ritrasmettere Z millisecondi dopo la fine della trasmissione della trama corrotta; il numero Z viene deciso secondo il seguente metodo:

- si attende un tempo pari a  $Z = S_c \cdot N + T$ , dove
  - $S_c$  = somma delle cifre che compongono l'istante di inizio trasmissione
  - $N$  = numero di collisioni subite da quella trama
  - $T$  tempo di trama

ad esempio, se l'istante di inizio trasmissione è 418 msec,  $Z = (4+1+8) \cdot N + T$

Determinare:

1. graficamente le trasmissioni delle diverse trame, indicando se avviene collisione, in quali istanti essa viene eventualmente avvertita e da quali apparati;
2. il periodo di vulnerabilità del sistema preso in considerazione.

$$V = 800 \text{ Kbit/s}$$

$$L = 1200 \text{ byte}$$

$$\tau_1 = 1 \text{ ms}$$

$$\tau_2 = 2 \text{ ms}$$

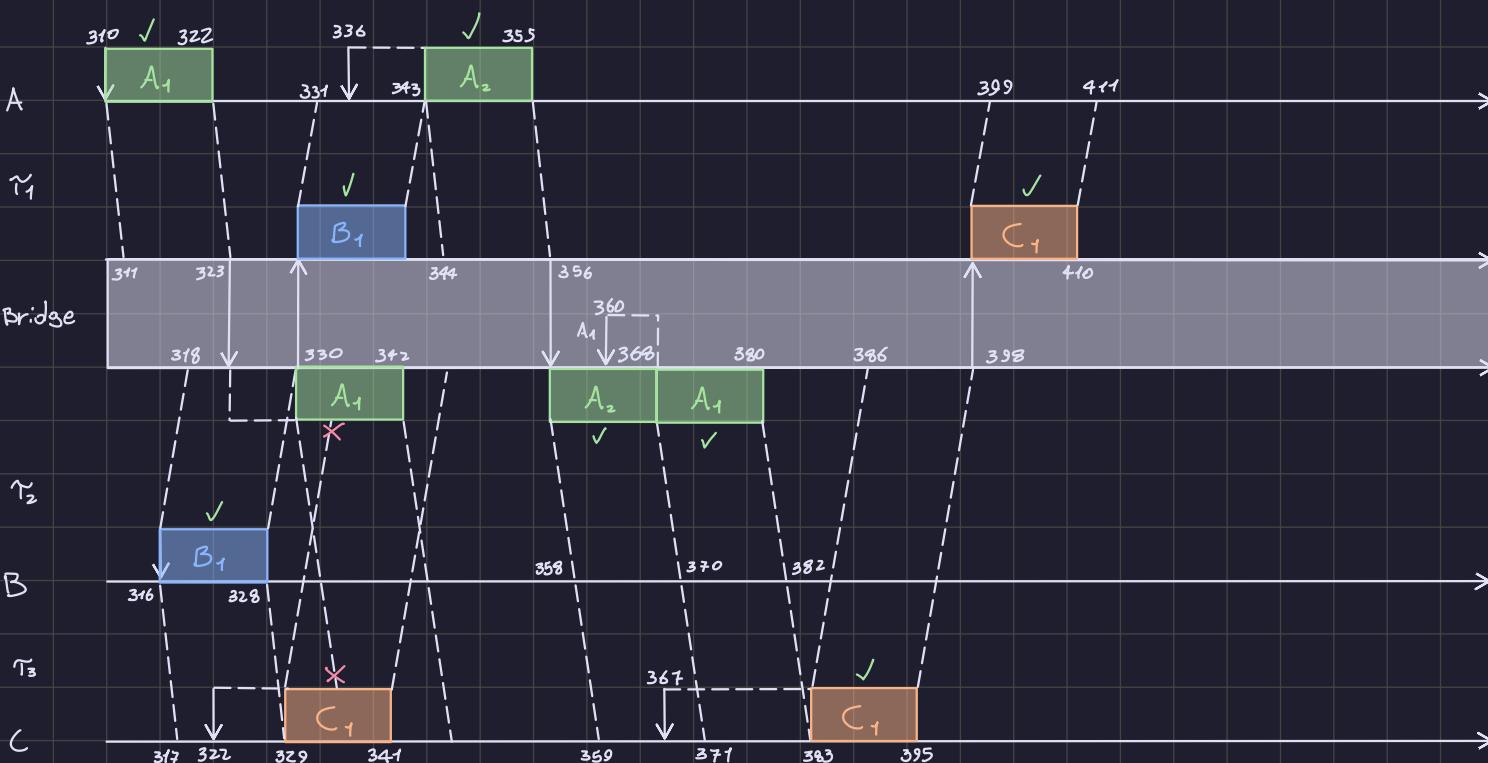
$$\tau_3 = 1 \text{ ms}$$

$$A: \begin{cases} t_{A1} = 310 \text{ ms} \rightarrow C \\ t_{A2} = 336 \text{ ms} \rightarrow B \end{cases}$$

$$B: t_{B1} = 316 \rightarrow A$$

$$C: t_{C1} = 322 \rightarrow A$$

$$T = \frac{L}{V} = \frac{1200 \cdot 8}{800 \cdot 10^3} = 12 \text{ ms}$$



Alla collisione tra A1 e C1:

$$Z_{A1} = (3+3+0) \cdot 1 + 12 = 18 \text{ ms} \rightarrow 342 + 18 = 360 \text{ ms} \quad A_1 \text{ ritrasmette per primo}$$

$$Z_{C1} = (3+2+9) \cdot 1 + 12 = 26 \text{ ms} \rightarrow 341 + 26 = 367 \text{ ms}$$

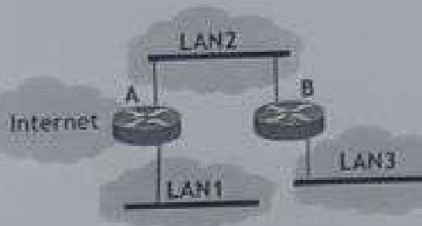
## Esercizio 2 (7 punti)

Si consideri la rete rappresentata in Figura, collegata ad Internet attraverso il router A (router di default per la rete). Si hanno i seguenti vincoli:

- la LAN 1 contiene un host con indirizzo 59.84.213.12;
- Le LAN 1, 2, e 3 devono poter contenere rispettivamente almeno 300, 1200 e 520 host.

In base ai suddetti vincoli:

1. Si specifichi il blocco CIDR più piccolo da assegnare alla rete;
2. Si assegnino gli indirizzi di rete e di broadcast alle LAN 1, 2, e 3, utilizzando il blocco CIDR individuato nel punto precedente;
3. Si scriva la tabella di routing del router B, considerando come metrica il numero di hop e assumendo che qualsiasi host su Internet possa essere raggiunto in 4 hop.



$$\text{LAN 1: } 300 \rightarrow 512 = 2^9 \text{ host}$$

$$\text{LAN 2: } 1200 \rightarrow 2048 = 2^{11} \text{ host}$$

$$\text{LAN 3: } 520 \rightarrow 1024 = 2^{10} \text{ host}$$

1. Il blocco CIDR totale è dato dal blocco in base 2 più piccolo che riesce a contenere la somma tra tutti i blocchi di ogni lan in base 2

$$\text{Blocco CIDR} = 512 + 2048 + 1024 = 3584 \rightarrow 4096 = 2^{12}$$

Possiamo derivare l'indirizzo di rete partendo dall'indirizzo appartenente alla lan 1 che ci viene fornito:

59 . 84 . 213 . 12

↓

59 . 84 . 1 1 0 1 0 1 0 1 . 0 0 0 0 1 1 0 0

Il blocco CIDR totale ha bisogno di 12 bit di suffisso, quindi 20 bit di prefisso:

59 . 84 . 1 1 0 1 0 1 0 1 . 0 0 0 0 1 1 0 0

Prefisso

L'indirizzo di rete è caratterizzato da tutti i bit di suffisso posti a 0, mentre l'indirizzo di broadcast è caratterizzato da tutti i bit di suffisso posti a 1:

Ret: 59 . 84 . 1 1 0 1 0 1 0 1 . 0 0 0 0 0 0 0 0

Prefisso

↓

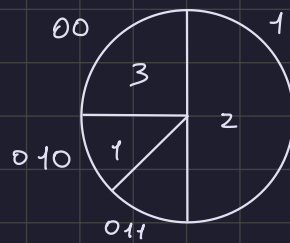
59 . 84 . 208 . 0 / 20

Broadcast: 59 . 84 . 1 1 0 1 1 1 1 1 . 1 1 1 1 1 1 1 1

Prefisso

↓

59 . 84 . 223 . 255 / 20



## 2. Lan 1:

Ci viene fornito un indirizzo appartenente alla lan 1 da cui possiamo ricavare a quale sottorete appartiene perchè sappiamo che la lan 1 ha bisogno di 9 bit di suffisso, quindi 23 saranno dedicati al prefisso, di cui 3 sono dedicati alla sottorete:

Rete: 59 . 84 . 1 1 0 1 0 1 0 0 . 0 0 0 0 0 0 0 0

Prefisso Sottorete

↓

59 . 84 . 212 . 0 /23

Broadcast 59 . 84 . 1 1 0 1 0 1 0 1 . 1 1 1 1 1 1 1 1

Prefisso Sottorete

↓

59 . 84 . 213 . 255 /23

## Lan 2:

La lan 2 ha bisogno di 11 bit di suffisso, quindi 21 saranno dedicati al prefisso, di cui 1 è dedicato alla sottorete:

Rete: 59 . 84 . 1 1 0 1 1 0 0 0 . 0 0 0 0 0 0 0 0

Prefisso Sottorete

↓

59 . 84 . 216 . 0 /21

Broadcast: 59 . 84 . 1 1 0 1 1 1 1 1 . 1 1 1 1 1 1 1 1

Prefisso Sottorete

↓

59 . 84 . 223 . 255 /21

## Lan 3:

La lan 3 ha bisogno di 10 bit di suffisso, quindi 22 saranno dedicati al prefisso, di cui 2 sono dedicati alla sottorete:

Rete: 59 . 84 . 1 1 0 1 0 0 0 0 . 0 0 0 0 0 0 0 0

Prefisso Sottorete

↓

59 . 84 . 208 . 0 /22

Broadcast: 59 . 84 . 1 1 0 1 0 0 1 1 . 1 1 1 1 1 1 1 1

Prefisso
Sottorete

↓

59 . 84 . 211 . 255 / 22

### 3. Tabella di routing di B:

dst	next hop	cost
LAN1	A	2
LAN2	B	1
LAN3	B	1
Internet	A	5
A	A	1
B	B	0

### Esercizio 3 (7 punti)

Un'applicazione A deve trasferire 67200 byte all'applicazione B utilizzando il protocollo TCP. Si supponga che la connessione tra A e B sia già stata instaurata. La trasmissione dei segmenti inizia al tempo  $t=0$ . Sono noti i seguenti parametri:

- MSS concordata pari a 800 byte;
- RCVWND annunciata da B ad A durante l'instaurazione della connessione pari a 12800 byte; a partire dal tempo  $t > 6$  sec la destinazione annuncia una RCVWND pari a 6400 byte; a partire dal tempo  $t > 8$  sec la destinazione annuncia una RCVWND pari a 12800 byte;
- SSTHRESH iniziale = RCVWND;
- CWND = 1 segmento a  $t=0$ ;
- RTT pari a 1 secondo, costante per tutto il tempo di trasferimento;
- RTO base =  $2 \cdot \text{RTT}$ ; nel caso di perdite consecutive dello stesso segmento, i timeout seguenti raddoppiano fino ad un massimo di 4 volte il RTO base, dopodiché la connessione viene abbattuta;
- il tempo di trasmissione dei segmenti è trascurabile rispetto RTT;
- il ricevitore riscontra immediatamente i segmenti.

Inoltre si supponga che la rete vada fuori servizio nei seguenti intervalli di tempo:

- da  $t_1 = 6.5s$  a  $t_2 = 7.5s$ ;
- da  $t_3 = 14.5s$  a  $t_4 = 15.5s$ .

Si tracci l'andamento della CWND nel tempo e si determini in particolare:

- il valore finale di CWND (sia graficamente, sia esplicitandolo);
- i valori assunti dalla SSTHRESH durante il trasferimento (graficamente);
- il tempo necessario per il trasferimento dei dati (sia graficamente, sia esplicitandolo);
- il numero di segmenti trasmessi ad ogni intervallo, specificando se ne vengono ricevuti i riscontri o meno (sia graficamente, sia esplicitando i valori).

$$L = 67200 \text{ byte} = \frac{67200}{800} = 84 \text{ segmenti}$$

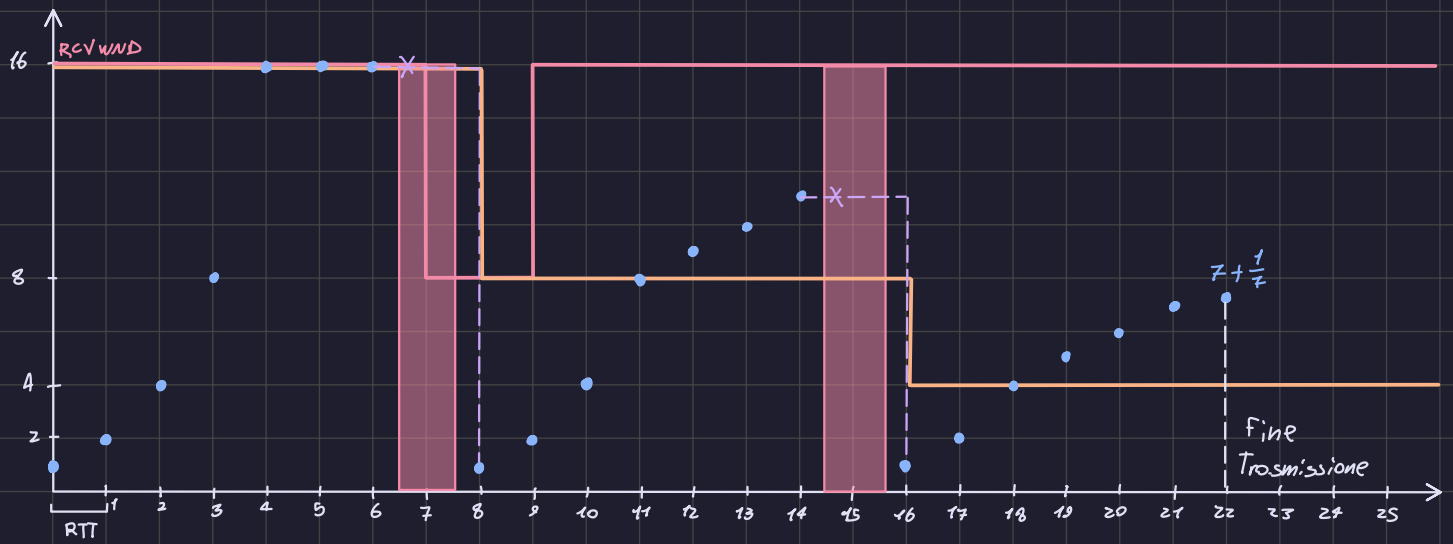
$$\text{MSS} = 800 \text{ byte}$$

$$\text{RCVWND} = \begin{cases} 12800 \text{ byte} & t \leq 6 = 16 \\ 6400 \text{ byte} & 6 < t \leq 8 = 8 \text{ segmenti} \\ 12800 \text{ byte} & t > 8 = 16 \end{cases}$$

$$\text{SSTHRESH} = \text{RCVWND}$$

$$\text{RTT} = 1s \text{ costante}$$

$$\text{DOWN} = \begin{cases} (6.5, 7.5) \\ (14.5, 15.5) \end{cases}$$



# segmenti trasmessi:  $1 + 2 + 4 + 8 + 16 + \cancel{16} + 1 + 2 + 4 + 8 + 9 + 10 + 11 + 1 + 2 + 4 + 5 + 6 + \overset{1}{7} = 84$   
 1 3 7 15 31 ~~47~~ 32 34 38 46 55 65 ~~76~~ 66 68 72 77 83 84

Il tempo necessario a trasmettere tutti i segmenti è di 22 secondi e la cwnd finale vale  $7 + \frac{1}{7}$