RETI DI CALCOLATORI – prova scritta del 10/02/2016

Per essere ammessi alla prova orale è necessario ottenere una valutazione sufficiente sia della prima parte che dell'intera prova scritta.

Prima parte (12 punti)

Q1. Una azienda ha installato una nuova rete locale con topologia a bus, lunga 300 metri, la cui velocità di propagazione è di $2x10^8$ m/sec. Per verificare l'effettiva frequenza R di trasmissione della rete, l'amministratore invia un pacchetto di 90 byte da un host situato all'estremo della rete e misura il tempo necessario affinché un host situato all'altro estremo della rete completi la ricezione di tale pacchetto. Indicare – giustificando la risposta – quale è il valore effettivo di R se il tempo rilevato dalla misurazione sopra descritta è di 76,5 microsecondi.

Q2. Indicare – giustificando la risposta – quanti *nuovi* segmenti può inviare un sender Selective Repeat che ha dimensione della finestra N e che ha N/2 segmenti spediti e non ancora riscontrati.

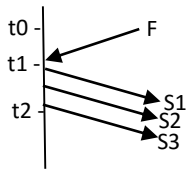
Q3. Un router IPv4 R deve inoltrare su un collegamento con MTU di 500 byte un datagram IP che ha ricevuto, la cui intestazione contiene 20 byte di opzioni e che contiene un segmento UDP di 960 byte. Indicare –giustificando la risposta– i valori dei campi *offset* ("scostamento") e *length* ("lunghezza totale") dei frammenti inviati da R.

Q4. Barbara riceve da Alice un messaggio *m* unitamente a un digest *d(m)* di *m* firmato da Alice con la propria chiave privata K_A^-. Indicare –giustificando la risposta– in che modo Barbara potrà dimostrare che il messaggio *m* è stato effettivamente firmato da Alice.

Seconda parte

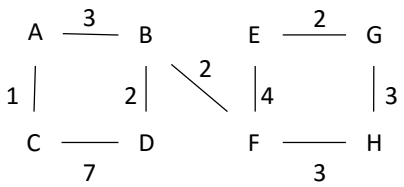
E1 (6 punti). Al tempo t0 il TCP di un server A ha una connessione già stabilita, per la quale:

- ha 2 segmenti *full-sized in volo*, con S_f=X,
- ha 3 MSS di *nuovi* dati da spedire,
- ha come valori delle variabili *cwnd* e *rwnd* 3 MSS e 2 MSS, rispettivamente, e
- si trova nello stato di *slow start*.



Al tempo t1 il TCP di A riceve un segmento F con flag FIN a 1 e quindi spedisce in sequenza 3 segmenti S1, S2, S3, l'ultimo dei quali subito prima del tempo t2. Supponendo che nell'intervallo [t0,t2] non scatti alcun timeout indicare –giustificando la risposta– i valori delle variabili *cwnd* e *rwnd* e lo stato del TCP di A al tempo t2.

E2 (6 punti). Consideriamo la rete a lato, i cui nodi utilizzano l'algoritmo distance vector con poisoned reverse.



(a) Indicare il contenuto del vettore delle distanze calcolato dal nodo B e (delle ultime copie) dei vettori che B ha ricevuto dagli altri nodi quando la rete ha raggiunto lo stato di quiescenza.

(b) Supponiamo che, subito dopo aver raggiunto lo stato di quiescenza, B rilevi che il collegamento BF è caduto.
(b1) Indicare il contenuto del vettore delle distanze calcolato da B a seguito di tale evento.
(b2) Indicare –giustificando la risposta– se la rete raggiunge di nuovo lo stato di quiescenza nel caso in cui lo stato dei collegamenti non subisca altre variazioni.

E3 (6 punti). Consideriamo una rete locale che utilizza il protocollo MAC Slotted Aloha 1-persistente e supponiamo che quattro host di tale rete cerchino di trasmettere un frame durante lo slot S, due di essi per la prima volta e due di essi per la seconda volta. Indicare – giustificando la risposta – quale è la probabilità che i quattro nodi NON riescano tutti a trasmettere con successo entro la fine dello slot S+4.

Traccia della soluzione

Q1. Sappiamo che $\frac{720\ b}{R} + \frac{300}{2 \cdot 10^8} s = \frac{76{,}5}{10^6} s$ quindi $R = \frac{720 \cdot 10^6}{75}$ bps = 9,6 Mbps.

Q2. Il sender può inviare (N-X) nuovi segmenti, dove X è il numero di segmenti compresi tra send_base e nextseqnum-1. Più precisamente: $\mathrm{X} = \begin{cases} \text{nextseqnum} - \text{send\_base} \ \ se \ \text{send\_base} < \text{nextseqnum} \\ \text{buffer.size}() - (\text{sendbase} - \text{nextseqnum}) \ \ altrimenti. \end{cases}$

Q3. Per inoltrare il datagram di 1000 byte ricevuto (composto da 960 byte di dati e 40 byte di intestazione), R dovrà inviare 3 frammenti:

- il primo, contenente 456 byte di dati, con offset=0 e length=496,
- il secondo, contenente 456 byte di dati, con offset=456/8=57 e length=496,
- il terzo, contenente 48 byte di dati, con offset=912/8=114 e length=88.

Q4. Barbara potrebbe conservare il messaggio ricevuto *<m,c>* per mostrare che applicando la chiave pubblica K_A^+ di Alice al crittogramma *c* si ottiene il digest di *m*, ovvero che $d(m)=K_A^+(c)$. Ciò tuttavia non sarebbe sufficiente per dimostrare che m è stato firmato da Alice se Alice cambiasse le proprie chiavi. Per poter dimostrare che il messaggio *m* è stato effettivamente firmato da Alice, Alice avrebbe dovuto inviare $<m,K_A^-(d(m))>$, unitamente alla propria identità e a quella di Barbara, a una terza parte "fidata", la quale avrebbe dovuto conservare una copia di $<m,K_A^-(d(m))>$ (dopo averne verificato l'autenticità) associandola all'identità di mittente, all'indentità del destinatario e a un timestamp.

E1. Dato che il TCP di S invia 3 segmenti dopo avere ricevuto il segmento F, quest'ultimo deve contenere un riscontro non duplicato. A seguito della ricezione di F il TCP di S aggiorna *cwnd* a 4 MSS e quindi:

- se F.*ackNum*=X+1 MSS allora F.*rwnd*≥4 MSS, dato che il TCP di S invia 3 MSS[1] di nuovi dati;
- analogamente, se F.*ackNum*=X+2 MSS allora F.*rwnd*≥3 MSS.

Al tempo t2 il valore di *cwnd* sarà quindi 4 MSS, il valore di *rwnd* sarà il valore che era contenuto in F.*rwnd* e il TCP di S si troverà nello stato *slow start* se *ssthresh*>4 MSS e nello stato *congestion avoidance* altrimenti.

E2.

(a)	**B**	A	D	F
A	3	-	∞	∞
C	4	1	∞	∞
D	2	∞	-	∞
E	6	∞	∞	4
F	2	∞	∞	-
G	8	∞	∞	6
H	5	∞	∞	3

(b1)	**B**
A	3
C	4
D	2
E	∞
F	∞
G	∞
H	∞

(b2) Se lo stato dei collegamenti non subisce altre variazioni la rete non raggiunge lo stato di quiescenza in quanto per esempio:

1. B invia $D_B(F)= \infty$ a D
2. D aggiorna la sua distanza $D_D(F)$ a $7+D_C(F)=13$ e invia $D_D(F)=13$ a B
3. B aggiorna la sua distanza $D_B(F)$ a $2+D_D(F)=15$ e invia $D_B(F)=15$ a A
4. A aggiorna la sua distanza $D_A(F)$ a $3+D_B(F)=18$ e invia $D_A(F)=18$ a C
5. C aggiorna la sua distanza $D_C(F)$ a $1+D_A(F)=19$ e invia $D_C(F)=19$ a D

2'. D aggiorna la sua distanza $D_D(F)$ a $7+D_C(F)=26$ e invia $D_D(F)=26$ a B

e il ciclo di aggiornamenti continua.

E3. Osserviamo che affinché tutti e quattro i nodi riescano a trasmettere con successo entro la fine dello slot S+4 non deve verificarsi alcuna collisione negli slot [S+1,S+4]. Affinché ciò avvenga, i due nodi che cercano di trasmettere per la prima volta devono scegliere uno di non attendere e uno di attendere 1 slot prima di ritentare la trasmissione. Analogamente, i due nodi che cercano di trasmettere per la seconda volta devono scegliere uno di attendere 2 slot e uno di attendere 3 slot prima di ritentare la trasmissione. Ciò avverrà con probabilità $\frac{4}{2 \cdot 2 \cdot 4 \cdot 4} = \frac{1}{16}$ e quindi la probabilità che i quattro nodi NON riescano tutti a trasmettere con successo entro la fine dello slot S+4 è pari a $1 - \frac{1}{16} = \frac{15}{16}$.

[1] Assumendo che S1, S2 e S3 siano tutti full-sized. Altrimenti F.*rwnd*≥1 MSS + D se se F.*ackNum*=X+1 MSS e F.*rwnd*≥D se F.*ackNum*=X+2 MSS, dove D è la somma della quantità di dati trasportati da S1, S2 e S3.