RETI DI CALCOLATORI – Seconda verifica *in itinere* a.a. 2008/09

E1 (4 punti). Consideriamo un'applicazione A che ha una connessione TCP attiva con un suo pari B. Assumiamo che il valore di entrambi le variabili di stato *sendBase* e *NextSeqNum* del TCP di A sia *X* e che A debba inviare due messaggi rispettivamente di dimensione 1 MSS e ½ MSS.

(a) Supponiamo che A invii entrambi i messaggi sulla connessione e che il primo messaggio giunga a destinazione dopo l'arrivo del secondo. Indicare i valori contenuti nel campo contenente il numero di riscontro dei segmenti di riscontro inviati da B.

(b) Supponiamo ora che i due messaggi inviati da A arrivino a destinazione nell'ordine corretto. Supponiamo inoltre che il segmento di riscontro inviato da B alla ricezione del primo segmento di A vada perso e che il secondo riscontro inviato da B arrivi ad A solo dopo che è scattato il time-out del primo segmento. Specificare la sequenza di segmenti scambiati tra A e B dopo lo scadere del time-out, assumendo che nessun altro pacchetto vada perso.

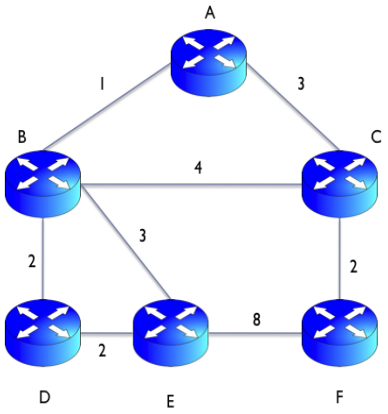
E2 (6 punti). Progettare una modifica del meccanismo di controllo di congestione di TCP in modo tale che la dimensione della finestra di congestione venga modificata in funzione delle variazioni del *round trip time* misurato in modo che *CongWin* aumenti di 2 MSS a ogni RTT se i valori delle misurazioni di RTT continuano a decrescere. Descrivere come può essere definita tale modifica e illustrare un esempio in cui la ricezione nello stato di *congestion avoidance* di tre riscontri per segmenti ancora "in volo" porti a ottenere valori diversi di *CongWin* nei due casi.

E3 (6 punti). Consideriamo la rete illustrata di lato e assumiamo che i router utilizzino un algoritmo di routing *distance vector* senza *poisoned reverse* e che il router C sia soggetto a una politica di instradamento che lo obbliga a privilegiare il router A in caso di cammini con costo identico.

(a) Illustrare la tabella della distanze del router F nel momento in cui tutti i nodi hanno raggiunto lo stato di quiescenza.

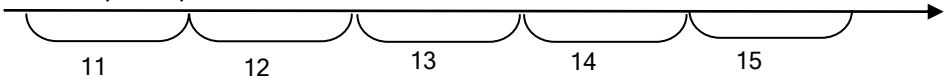
(b) Supponiamo di usare un meccanismo di *reverse path forwarding* per inviare in broadcast un messaggio da F a tutti gli altri router. Indicare da quali vicini B riceverà una copia del messaggio e quali azioni eseguirà alla ricezione di tali copie.

(c) Si consideri uno scenario in cui possono variare i costi dei collegamenti A-B e B-C. In quali caso una variazione del costo del collegamento A-B non comporta una variazione della tabella di F? In quale caso una variazione del costo del collegamento B-C comporta una variazione della tabella di F? Motivare la risposta.



E4 (4 punti). Supponiamo che un host H di una rete NAT invii un comando "LIST" a un server FTP remoto. Indicare le informazioni relative all'indirizzamento contenute in tutti i preamboli del frame contenente tale richiesta ricevuto dal router di H e del frame corrispondentemente ritrasmesso dal router di H.

E5 (4 punti). Supponiamo che due nodi A e B cerchino di spedire con CSMA/CD, entrambi per la seconda volta, un frame nello slot 11 della figura sottostante. Supponiamo inoltre di sapere già che il nodo C cercherà di spedire un frame per la prima volta nello slot 13.



Assumendo per semplicità che non vi siano altri nodi che cercano di spedire e che ogni trasmissione inizi all'inizio di uno slot, indicare - motivando la risposta – con quale probabilità tutti e tre i frame potranno essere stati trasmessi con successo: (a) prima dell'inizio dello slot 14, e (b) prima dell'inizio dello slot 15.

E6 (6 punti). Supponiamo che A, per inviare il messaggio *m* a B, invii a B la tripla

$$<A, m, encr(K_A^-, encr(K_B^+, H(m)))>$$

dove *encr(K,x)* indica il testo *x* cifrato con la chiave *K* e dove K_A^- e K_B^+ indicano rispettivamente la chiave privata di A e la chiave pubblica di B. Indicare, motivando la risposta, se tale tripla garantisce riservatezza e integrità di m e autenticazione di A.

Traccia della soluzione

E1. (a) X nel primo segmento di riscontro inviato da B e X+1,5MSS nel secondo. (b) L'host di A rispedirà il primo segmento (ovvero quello con SeqNum=X contenente 1 MSS di dati). Quando l'host di B riceverà (per la seconda volta) tale segmento, invierà un riscontro cumulativo con numero di riscontro X+1,5 MSS.

E2. Dato che SampleRTT viene di solito misurato da TCP per uno solo dei segmenti "in volo", otteniamo approssimativamente un nuovo valore di SampleRTT a ogni RTT. Possiamo quindi prevedere che quando viene ricevuto un riscontro per un segmento in volo e tale ricezione causa la misurazione di un nuovo valore di SampleRTT, se tale valore è minore dell'ultimo valore precedentemente misurato (o della media EstimatedRTT, nel caso in cui non venga conservato il valore della precedente misurazione) il valore di CongWin venga direttamente incrementato di 2 MSS.

È facile vedere che tale modifica porta a ottenere valori diversi di CongWin rispetto al normale incremento di CongWin operato da TCP nello stato di congestion avoidance. Se ad esempio CongWin=3MSS, dopo avere ricevuto tre riscontri per segmenti ancora in volo, il valore di CongWin sarà aumentato in TCP di 1 MSS. Nel caso invece del meccanismo modificato sopra descritto il valore di CongWin sarà aumentato di 2 MSS oppure sarà rimasto invariato.

[Se si prevede che venga modificata anche la frequenza con cui viene misurato SampleRTT, effettuando una nuova misurazione per ogni riscontro positivo, dovremo incrementare CongWin di una frazione (per esempio MSS/CongWin) di 2 MSS ogni volta che viene ricevuto un riscontro positivo.]

E3.

(a)	A	B	C	D	E
C	3	4	0	6	7
E	4	3	7	2	0
F	5	6	2	8	8

(b) Il router B riceverà una copia del messaggio da tutti i suoi vicini tranne D. Dato che B inoltra a $\Delta \in$ {A,C} i pacchetti destinati a F, B inoltrerà a tutti i suoi vicini ad eccezione di Δ la copia del messaggio che ha ricevuto da Δ, e scarterà invece tutte le altre copie ricevute.
(c) Se il costo del collegamento A-B aumenta:

- C inizierà a inoltrare a B i pacchetti destinati a B,D,E ma nessuno dei valori delle distanze calcolate da C varierà, e
- B aggiornerà il valore della sua distanza da A e tale aggiornamento porterà E ad aggiornare il valore della sua distanza da A.

I valori delle distanze calcolate da F comunque non varieranno, dato che F continuerà a inoltrare a C i pacchetti destinatati ad A:
Se invece il costo del collegamento B-C diminuisce per esempio di 1 unità, C aggiornerà a 3 il valore della sua distanza per B e di conseguenza F aggiornerà a 5 il valore della sua distanza per B.

E4. Supponendo che l'host H sia direttamente collegato al router R, il frame ricevuto da R conterrà nei vari preamboli le seguenti informazioni relative all'indirizzamento:

```
//preambolo DL
 SRC: INDIRIZZO MAC DI H
DEST: INDIRIZZO MAC DELL'INTERFACCIA DI R SULLA RETE LOCALE DI H

//preambolo IP
 SRC: INDIRIZZO IP DI H (NELLA RETE NAT)
DEST: INDIRIZZO IP DEL SERVER FTP
UpperLayerProtocol: 6

//preambolo TCP
 SRC: PORTA TCP DEL PROCESSO CLIENT FTP IN H
DEST: PORTA TCP DEL SERVER FTP
```

Il frame inviato dal router R al successivo router R' conterrà nei vari preamboli le seguenti informazioni relative all'indirizzamento:

```
//preambolo DL
 SRC: INDIRIZZO MAC DELL'INTERFACCIA DI R SULLA RETE DI R'
DEST: INDIRIZZO MAC DELL'INTERFACCIA DI R' SULLA RETE DI R

//preambolo IP
 SRC: INDIRIZZO IP DELL'INTERFACCIA DI R SULLA RETE DI R'
DEST: INDIRIZZO IP DEL SERVER FTP
UpperLayerProtocol: 6

//preambolo TCP
 SRC: PORTA TCP ASSOCIATA DA NAT ALLA PORTA DEL PROCESSO CLIENT FTP IN H
DEST: PORTA TCP DEL SERVER FTP
```

E5. (a) Dato che nello slot 11 si verifica una collisione tra A e B, non è possibile che i tre frame vengano trasmessi con successo nei due slot successivi. (b) Affinché tutti e tre i frame possano essere trasmessi con successo negli slot 12, 13 e 14, A e B dovrebbero riuscire a trasmettere con successo uno nello slot 12 e l'altro nello slot 14. A e B, dopo avere rilevato di avere sofferto una seconda collisione nello slot 11, attenderanno ciascuno un numero (casuale) di slot compreso tra 0 e 3 e riusciranno quindi a trasmettere entrambi con successo uno nello slot 12 e l'altro nello slot 14 con probabilità 1/8.

E6. Non viene ovviamente garantita la riservatezza di *m*, dato che m viene trasmesso in chiaro come secondo elemento della tripla. Quando riceve ricevuta una tripla <A,m,c>, B può verificare se $decr(K_B^-, decr(K_A^+, c))$ coincide o meno con $H(m)$. Osserviamo tuttavia che un intruso T potrebbe avere sostituito la tripla $<A, m, encr(K_A^-, encr(K_B^+, H(m)))>$ spedita da A con $<A, m, encr(K_T^-, encr(K_B^+, H(m)))>$. L'affidabilità del controllo effettuato di B sull'integrità del messaggio è quindi pari all'affidabilità del meccanismo utilizzato per la distribuzione della chiave pubblica di A. Osserviamo infine che la ricezione di un'unica tripla <A,m,c> non può garantire l'autenticazione di A, dato che potrebbe trattarsi di una riproduzione di un messaggio registrato e ritrasmesso da un intruso.

(AB)