RETI DI CALCOLATORI – Primo appello - a.a. 2010/2011

Per ottenere una valutazione sufficiente dell'intera prova è necessario ottenere una valutazione sufficiente della prima parte.

Prima parte (10 punti)

Q1. Supponiamo che un router A trasmetta un pacchetto su un collegamento con un router B, che la frequenza di trasmissione del collegamento sia 1 Mbps e che la velocità di propagazione sia $2 \cdot 10^8$ m/s. Determinare –giustificando la risposta– quanto deve essere al più la lunghezza D del collegamento affinché i primi 1.000 bit del pacchetto siano arrivati a B dopo 2 millisecondi.

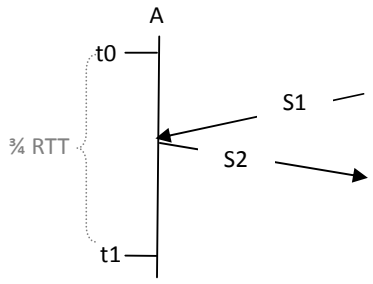
Q2. Consideriamo un host C sotto NAT che deve scaricare con FTP un file f da un server S situato in un altro paese. Indicare –giustificando la risposta– quali problemi possono essere causati da NAT dopo che S ha ricevuto da C la richiesta di download di f, e se e come tali problemi possono essere prevenuti.

Q3. Supponiamo che il servizio UDP in esecuzione su un host A debba inviare un segmento S a un suo pari in esecuzione su un host B. Indicare –giustificando la risposta– (a) i parametri (oltre S) che l'UDP di A deve specificare per richiedere al servizio IP la spedizione di S, e (b) i parametri che l'UDP di B riceverà dal suo livello di rete quando questo riceverà il datagram spedito da A.

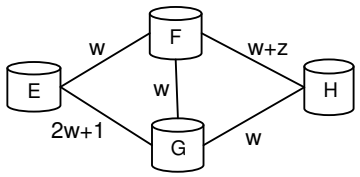
Q4. Consideriamo una rete i cui nodi utilizzano RPF per l'instradamento broadcast e supponiamo che un nodo N invii un pacchetto p in broadcast. Sia A un altro nodo della rete ($A \neq N$) e sia $\{V_1,...,V_h\}$ l'insieme dei nodi direttamente collegati ad A, con $N \notin \{V_1,...,V_h\}$ e $h \geq 3$. Indicare –giustificando la risposta– se è possibile o meno che A riceva 1 sola copia di p.

Seconda parte

E1 (6 punti). Supponiamo che al tempo t0 il TCP di un host A abbia già stabilito una connessione con un suo pari, abbia 1 segmento "in volo" contenente 1 MSS di dati, che i valori di sendBase e di CongWin siano X e 2MSS rispettivamente e che debba ancora spedire 3MSS di nuovi dati. Supponendo che nell'intervallo [t0,t1] non scatti nessun timeout, che A riceva e spedisca solo i due segmenti indicati nella figura e che il segmento S1 non contenga dati e arrivi ad A non corrotto, indicare –giustificando la risposta– i possibili valori dei campi AckNum e RcvWin di S1 e del campo SeqNum di S2 nel caso in cui: **(a)** S2 contenga 1MSS di dati, e **(b)** S2 contenga solo 3/4 MSS di dati.



E2 (5 punti). Consideriamo la rete a lato i cui nodi utilizzano il protocollo distance vector con poisoned reverse e dove z>w>1. **(a)** Indicare il contenuto del vettore delle distanze di G e dei vettori ricevuti da G dai suoi vicini una volta che la rete ha raggiunto lo stato di quiescenza. **(b)** Supponendo che, una volta raggiunto lo stato di quiescenza, il costo del collegamento GH diventi 6w, indicare il modo in cui G modifica il suo vettore delle distanze non appena rileva che il costo di tale collegamento è aumentato e indicare quale vettore G spedisce ai vicini E, F, H a seguito di tale modifica.

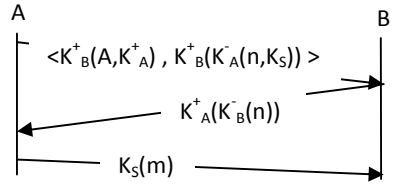


E3 (5 punti). Descrivere –con un automa a stati finiti– il comportamento del nodo "principale" (o "arbitro") di una rete che utilizza un protocollo polling ("di sondaggio") per l'accesso multiplo al canale. Nella descrizione utilizzare le operazioni:

poll(i,max) - per inviare un messaggio comunicando al nodo *i*-esimo che può trasmettere fino a *max* frame,
signal() - per rilevare la presenza di segnale, signal() restituisce 1 in caso di presenza di segnale sul canale, 0 altrimenti,
startTimer(t) - per avviare un timer di durata *t*

e l'evento *TO* che segnala lo scadere del timeout. Assumere che il nodo principale conosca sia il tempo massimo *TF* necessario per la spedizione di un frame della massima dimensione sia il tempo massimo *TL* che può intercorrere tra la spedizione del messaggio di polling e l'arrivo sul canale dei primi bit del primo frame (eventualmente) spedito dal nodo "sondato". Assumere per semplicità che i nodi della rete siano identificati dagli interi [0,N-1] dove N-1 è il nodo principale.

E4 (4 punti). Consideriamo il protocollo di autenticazione illustrato a lato, dove n è un nonce e Ks una chiave di sessione, entrambi generati da A, e m il messaggio che A desidera inviare a B. Supponendo che A possegga un certificato contenente la chiave pubblica di B, indicare –giustificando la risposta– se tale protocollo può essere o meno violato da un attacco "man-in-the-middle".



Traccia della soluzione

Q1. $\frac{10^3\ b}{10^6\ b/s} + \frac{D}{2\ 10^8 m/s} \leq 2\ \frac{1}{10^3}$ s ovvero D≤200km.

Q2. Supponiamo che la connessione di controllo sia identificata dalla quadrupla <(IP_C,P_C),(IP_S,21)> in C e dalla quadrupla <(IP_S,21),(IP_N,P_N)> in S. Se S cercasse di aprire la connessione dati con C utilizzando una porta locale diversa (per esempio da (IP_S,20) a (IP_N,P_N)) ma il router NAT di C non accettasse sessioni iniziate dall'esterno, si verificherebbe un problema in quanto il *syn* inviato da S verrebbe scartato dal router di C. Per prevenire tale problema è sufficiente che sia il cliente C ad aprire la connessione dati con S utilizzando una porta remota P_S' diversa[1] (ovvero da (IP_C,P_C) a (IP_S,P_S'), con P_S'≠21).

Q3. (a) Oltre ai dati da spedire (S), UDP dovrà specificare sia l'indirizzo IP del destinatario (l'host B in questo caso) sia il numero di protocollo di livello superiore (17 nel caso di UDP) a cui dovranno essere passati i dati che saranno trasportati nel datagram. (b) L'UDP di B riceverà l'indirizzo IP del mittente (A in questo caso) del datagram e il segmento (S in questo caso) contenuto nella parte dati del datagram.

Q4. Si, se A riceve p da V_x=nextHop(A,N) e per esempio nextHop(V_i,N)=A per ogni V_i≠V_X (dove nextHop(V,N) indica il primo hop a cui V inoltra i pacchetti destinati a N).

E1. (a) Distinguiamo tre casi possibili:

- S1 è un riscontro per tutti i dati in volo, ovvero **S1.AckNum=X+1MSS**. In questo caso, ricevuto S1, TCP non ha dati in volo e la dimensione di CongWin diventa maggiore di 2MSS. Dato che TCP spedisce solo 1MSS di nuovi dati (in S2), ciò significa che è il controllo di flusso a limitare la spedizione di nuovi dati, ovvero **S2.RcvWin=1MSS**. Ovviamente **S2.SeqNum=X+1MSS** in questo caso.
- S1 è un riscontro duplicato, ovvero **S1.AckNum=X**, ricevuto *non* per la terza volta. In questo caso, ricevuto S1, la dimensione di CongWin rimane 2MSS e TCP può quindi spedire 1MSS di nuovi dati solo nel caso in cui **S1.RcvWin≥2MSS**. Anche in questo caso **S2.SeqNum=X+1MSS**.
- S1 è un riscontro duplicato, ovvero **S1.AckNum=X**, ricevuto per la terza volta. In questo caso scatta il meccanismo di ritrasmissione rapida (indipendentemente dal valore di S1.RcvWin) e **S2.SeqNum=X**.

(b) Se S2 contiene solo ¾ MSS di dati, vi sono solo due casi possibili[2]:

- S1 è un riscontro per tutti i dati in volo, ovvero **S1.AckNum=X+1MSS**. In questo caso, ricevuto S1, TCP non ha dati in volo e la dimensione di CongWin diventa maggiore di 2MSS. Dato che TCP spedisce solo ¾ MSS di nuovi dati (in S2), ciò significa che è il controllo di flusso a limitare la spedizione di nuovi dati, ovvero **S2.RcvWin=3/4 MSS**. Ovviamente **S2.SeqNum=X+1MSS** in questo caso.
- S1 è un riscontro duplicato, ovvero **S1.AckNum=X**, ricevuto *non* per la terza volta. In questo caso, ricevuto S1, la dimensione di CongWin rimane 2MSS e TCP può spedire ¾ MSS di nuovi dati solo nel caso in cui **S1.RcvWin=7/4MSS**. Anche in questo caso **S2.SeqNum=X+1MSS**.

E2.

(a)	E	F	H
E	0	w	3w
F	w	0	∞
H	∞	∞	0
G	2w	w	w

(b) G aggiorna il suo vettore in

	E	F	H
G	2w	w	5w+1

e quindi spedisce

a E

	E	F	H
G	2w	w	∞

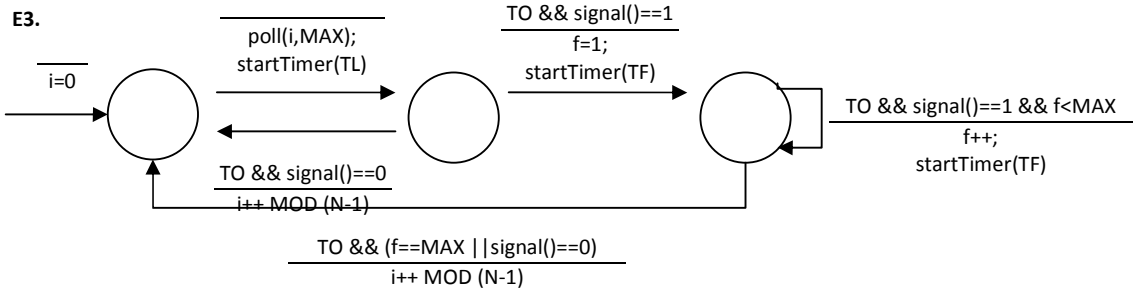
a F

	E	F	H
G	∞	∞	5w+1

a H

	E	F	H
G	2w	w	5w+1

E3.



E4. Il protocollo può essere violato solo parzialmente da un attacco "man-in-the-middle". Un intruso T può infatti intercettare il primo messaggio di A, inviare a B il messaggio <$K^+_B(A,K^+_T)$, $K^+_B(K^-_T(n',K_{S'}))$ >, intercettare la risposta $K^+_T(K^-_B(n'))$ di B e inviare a B un messaggio $K_{S'}(m')$. Notiamo tuttavia che T, non conoscendo K^-_B, non può decifrare né il nonce n né la chiave K_S generati da A, né può generare $K^-_B(n)$. L'unica risposta che T può inviare ad A è quindi $K^+_A(K^-_B(n'))$ che però A riconoscerà diversa dalla risposta che si aspettava $K^+_A(K^-_B(n))$.

[1] Precedentemente indicata da S a C sulla connessione di controllo.

[2] S2 non può infatti essere un riscontro duplicato ricevuto per la terza volta, perché in tal caso S2 dovrebbe essere una rispedizione del segmento più vecchio ancora in volo e dovrebbe quindi contenere 1MSS di dati.