RETI DI CALCOLATORI – secondo 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 in modo continuato dati su un collegamento lungo 200 km 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– il numero massimo di bit che possono essere simultaneamente presenti nel collegamento.

Q2. Supponiamo che un server DNS in esecuzione su un host A debba inviare una query Q a un suo pari in esecuzione su un host B. Indicare –giustificando la risposta– i parametri (oltre a Q) che il name server in A deve specificare per richiedere al servizio UDP la spedizione di Q.

Q3. Sia R un router che utilizza il protocollo distance vector con poisoned reverse e siano V1 e V2 gli unici due router con cui R ha un collegamento diretto. Supponiamo che:

- al tempo t_1 V1 determini che la sua distanza per Z è x e che invii il suo vettore delle distanze ai suoi vicini;
- al tempo $t_2 > t_1$ V2 determini che la sua distanza per Z è 2x+y e che invii anch'esso il suo vettore delle distanze ai suoi vicini;
- al tempo $t_3 > t_2$ il vettore delle distanze determinato da R (dopo avere ricevuto gli advertisement spediti da V1 e V2 al tempo t_1 e t_2 rispettivamente) contenga $D_R(V1)=y$, $D_R(V2)=x$ e $D_R(Z)=x+y$;
- al tempo $t_4 > t_3$ R rilevi che il collegamento R-V1 è caduto.

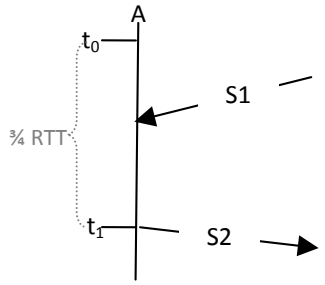
Indicare –giustificando la risposta– quale è la nuova distanza per Z che R determina non appena rileva che R-V1 è caduto.

Q4. Consideriamo un anello Chord, i cui identificatori sono rappresentati con 6 bit, formato dai nodi con identificatori 2, 12, 28, 30, 32, 41, 43, 51, e 56. Determinare quali sono i finger del nodo 28.

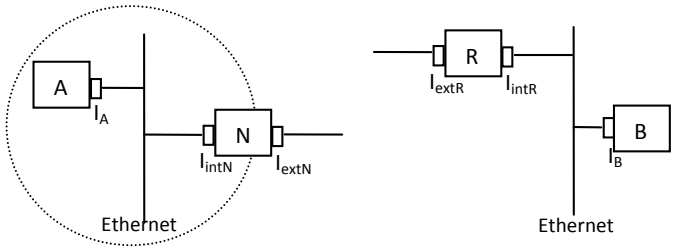
Seconda parte

E1 (6 punti). Supponiamo che al tempo t_0 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 il valore di sendBase sia X e che debba spedire 1MSS di nuovi dati "urgenti". Supponendo che il segmento S1 non contenga dati e arrivi ad A non corrotto, che nell'intervallo $[t_0,t_1)$ A riceva solo il segmento S1 e non scatti nessun timeout, e che al tempo t_1 scatti il timeout, indicare –giustificando la risposta– i possibili valori del campo AckNum di S1, del campo SeqNum di S2 e la quantità di dati contenuti in S2 nel caso in cui

(a) il valore di RcvWin in S1 sia 0, e (b) il valore di RcvWin in S1 sia 1MSS.



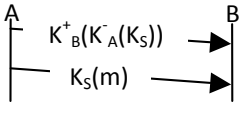
E2 (4 punti). Supponiamo che un cliente SMTP in esecuzione su un host A sotto NAT cerchi di trasferire un messaggio di email a un server in esecuzione su un host B, e consideriamo il segmento S inviato da B in risposta al primo segmento che A ha spedito a B. Indicare i valori dei campi contenenti informazioni di addressing in <u>tutti</u> i preamboli contenuti nel frame che trasporta S spedito da B e nel frame che trasporta "S" ricevuto da A.



(dove I_A, I_{intN}, I_{extN}, I_{extR}, I_{intR}, I_B, sono interfacce)

E3 (6 punti)**.** Supponiamo che solo due nodi di una rete Ethernet debbano trasmettere dati e che al tempo t0, dopo avere entrambi riscontrato che il canale è inattivo, essi inizino simultaneamente a trasmettere ciascuno per la prima volta un frame di 64 byte. Supponendo che la frequenza di trasmissione sia 10Mbps e che il ritardo di propagazione tra i due nodi sia 0,7 microsecondi, indicare –giustificando la risposta– quale è la probabilità che almeno uno dei due nodi riesca a trasmettere con successo un frame prima che siano trascorsi 120 microsecondi da t0.

E4 (4 punti). Supponiamo che A invii a B una chiave di sessione K_S dopo averla cifrata prima con la sua chiave privata e quindi con la chiave pubblica di B, e che quindi A invii a B un messaggio m cifrato con tale chiave di sessione. Indicare –giustificando la risposta– se ciò garantisce o meno riservatezza, integrità e non ripudiabilità di m, assumendo che B possegga un certificato affidabile di A.



Traccia della soluzione

Q1. I bit che possono essere simultaneamente presenti nel collegamento sono quelli che il router riesce a trasmettere mentre il segnale si propaga nel canale, ovvero $R \cdot d_{prop} = 10^6$ b/s $\cdot$ *200 · 103⁻2· 108⁻/⁻* = 1.000 b.
Q2. Oltre ai dati da spedire (Q), il name server dovrà specificare sia il numero della porta locale UDP (53 in questo caso) che l'indirizzo IP e la porta remota del destinatario (indirizzo IP di B e 53, rispettivamente).
Q3. Vi sono due casi possibili:

(a) se V2 aveva "avvelenato" la sua distanza per Z nell'advertisement inviato a R, allora R considererà Z non piú raggiungibile;
(b) altrimenti la distanza per Z determinata da R sarà $D_R(Z)=C(R,V2)+2x+y$, dove C(R,V2) indica il costo del collegamento R-V2.

Q4. I finger i finger del nodo 28 sono successor(28+1)= successor(28+2)=30, successor(28+4)=32, successor(28+8)=41, successor(28+16)=51 e successor(28+32)=2.

E1. (a) Se il valore di RcvWIn in S1 è 0, possono verificarsi due casi.

- S1 è un riscontro per tutti i dati in volo, ovvero **S1.AckNum=X+1MSS**. In questo caso, ricevuto S1, TCP attende lo scadere del timeout per inviare un segmento di zero-window probing con **S2.SeqNum=X+1MSS** contenente **1 byte** di dati
- S1 è un riscontro duplicato, ovvero **S1.AckNum=X**, ricevuto *non* per la terza volta[1]. In questo caso, allo scadere del timoeout in t_1, TCP rispedisce il segmento più vecchio ancora in volo, quindi **S2.SeqNum=X** e S2 contiene **1 MSS** di dati.

(b) Se invece il valore di RcvWIn in S1 è 1 MSS, S1 può solo essere un riscontro duplicato, ovvero **S1.AckNum=X**, ricevuto *non* per la terza volta[2]. In questo caso, allo scadere del timoeout in t_1, TCP rispedisce il segmento più vecchio ancora in volo, quindi **S2.SeqNum=X** e S2 contiene **1 MSS** di dati.

E2.

Frame inviato da B
//preambolo DL
sourceAddress = indirizzo MAC di I_B
destAddress = indirizzo MAC di I_{intR}
type = k
//preambolo IP
sourceAddress = indirizzo IP di I_B
destAddress = indirizzo IP di I_{extN}
upperLayerProtocol = 6
//preambolo TCP
sourcePort = 25
destPort = P_N

Frame ricevuto da A
//preambolo DL
sourceAddress = indirizzo MAC di I_{intN}
destAddress = indirizzo MAC di I_A
type = k
//preambolo IP
sourceAddress = indirizzo IP di I_B
destAddress = indirizzo IP di I_A
upperLayerProtocol = 6
//preambolo TCP
sourcePort = 25
destPort = P_A

dove P_A è il numero di porta utilizzato dal cliente SMTP in esecuzione su A, P_N è il numero di porta associato a P_A dal router NAT N[3], e k è il numero di protocollo di livello di rete.

E3. Inizialmente entrambi i nodi inizieranno a trasmettere, rileveranno l'avvenuta collisione e trasmetteranno quindi il jam di disturbo di 48 bit, impiegando complessivamente (0,7+4,8) μs. A questo punto:

(1) Se entrambi i nodi attendono 512 tempo di bit, entrambi cercheranno di nuovo di trasmettere dopo ulteriori (51,2+9,6) μs e rileveranno quindi entrambi la nuova collisione al tempo t0+(0,7+4,8+51,2+9,6+0,7) μs =t0 + 67 μs. Dato che prima di poter tentare di nuovo di trasmettere ciascun nodo dovrà attendere ulteriori (4,8+9,6) μs e quindi impiegare 51,2 μs per trasmettere il frame, è facile vedere che nessuno dei due nodi può riuscire a completare una trasmissione con successo prima che siano trascorsi 120 μs da t0.
(2) Se invece solo uno dei due nodi attende 512 tempo di bit mentre l'altro ritenta subito la trasmissione, il secondo riuscirà a completare la trasmissione con successo di un frame dopo (0,7+4,8+9,6+51,2) μs ovvero dopo 66,3 μs da t0.
(3) Infine, se entrambi ritentano subito la trasmissione, entrambi rileveranno la nuova collisione e trasmetteranno il jam arrivando così al tempo t0+20,6 μs. A questo punto solo uno dei due nodi potrà riuscire a completare una trasmissione con successo prima che siano trascorsi 120 μs da t0, ma ciò potrà avvenire solo nel caso in cui l'altro decida di attendere K·512 tempo di bit, con $K \in [1,3]$.

La probabilità che almeno uno dei due nodi sia già riuscito a trasmettere con successo un frame prima che siano trascorsi 120 microsecondi da t0 è quindi *14+14+14×716=3964* .

E4. La riservatezza del messaggio è garantita dal fatto che la chiave di sessione K_S dovrebbe essere nota solo ad A e a B e che un intruso non dovrebbe essere in grado di decifrare $K_S(m)$ senza conoscere K_S. L'integrità del messaggio non è invece garantita dato che B non ha modo di verificare se il crittogramma ricevuto è solo una parte di quello che A ha inviato. Un intruso potrebbe infatti avere rimosso ad esempio la parte finale di tale crittogramma. La non ripudiabilità del messaggio non è garantita dato che sia A che B conoscono K_S e non è quindi possibile stabilire se il messaggio $K_S(m)$ sia stato generato da A oppure da B.

---

[1] Se infatti si trattasse di un riscontro duplicato ricevuto per la terza volta dovrebbe scattare il meccanismo della ritrasmissione veloce.
[2] S1 non può infatti essere né un riscontro duplicato ricevuto per la terza volta (altrimenti dovrebbe scattare il meccanismo della ritrasmissione veloce) né un riscontro non duplicato (altrimenti TCP spedirebbe nuovi dati subito dopo avere ricevuto S1 dato che non vi sarebbero più dati in volo e che la dimensione di CongWin non è mai inferiore a 1 MSS).
[3] Ovvero la tabella di traduzione NAT conterrà la riga $<(I_A,P_A),(I_{extN},P_N)>$.