TELEMATICA
PROVA SCRITTA
15 Luglio 2013
Tempo a disposizione 120 minuti

Prima parte 10 Punti

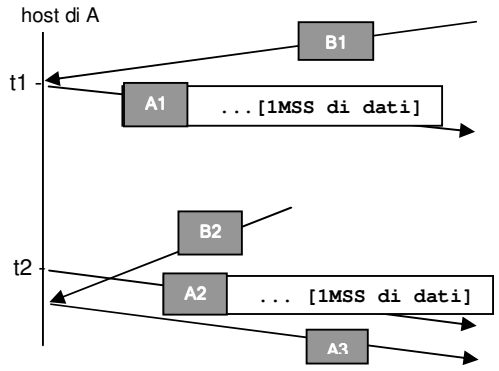
1. Consideriamo un blocco di indirizzi IP della forma a.b.c.d/n. E' possible derivare il numero di indirizzi IP del blocco, il primo indirizzo IP del blocco e l'ultimo indirizzo IP del blocco.? Motivare la risposta.
2. Spiegare il motivo per cui in Internet e' possible che vengano smarriti dei segmenti di livello di trasporto.
3. Si consideri il protocollo DNS. Quali informazioni sono presenti in un resource record della forma (Nome, Valore, MX, TTL). Si motivi la risposta.

Seconda parte 22 punti

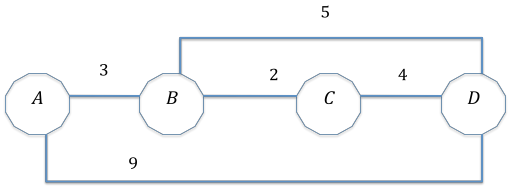
1. Consideriamo un'applicazione A che ha già stabilito una connessione TCP con un suo pari. Supponiamo che al tempo t0 il valore della finestra di congestione CongWin dell'host di A sia pari a 4MSS, gli indici sendBase e nextSeqNum valgano rispettivamente X e X+2MSS, che, sempre al tempo t0, l'host di A debba spedire 2 MSS di (nuovi) dati e che (solo) al tempo t2 scatti un timeout. Specificare, motivando la risposta:

a) il valore dei campi ACK e RcvWin dei segmenti B1 e B2;
b) il valore dei campi SEQ dei segmenti A1, A2 e A3, e
c) la quantità di dati contenuti nel segmento A3

nell'ipotesi in cui B1 sia un riscontro positivo. Supporre che tutti i segmenti contenenti dati spediti dall'host di A prima di t0 contenessero 1MSS di dati..



2. Si consideri il sistema autonomo descritto in figura.
Utilizzando l'algoritmo di routing link-state specificare la tabella di routing del nodo A.



3. Consideriamo il protocollo crittografico descritto di seguito, dove n è un nonce generato da A. Indicare –giustificando la risposta- se il protocollo permette ad A di autenticare B.

I. A invia a B: $< n >$
II. B invia a A: $< K+_A(B, K+_B),\ K+_A(K-_B(n)) >$

Traccia soluzione

Prima Parte

1. Chiamato k = 32 – n, il numero di indirizzi IP del blocco e' 2^k-1 Per individuare il primo indirizzo del blocco basta mettere a 0 gli ultimi k bit del blocco, mentre l'ultimo indirizzo si ottiene mettendo a 1 gli ultimi k bit.

2. Possono essere smarriti segmenti perche' la rete e' congestionata (code piene)

3. Serve per risolvere l'inditizzo canonico di un mailserver

Seconda Parte

Es1. Abbiamo due casi
Se B1.AckNum=X+2MSS allora in t1 il valore di CongWin è maggiore di 4MSS e l'host di A potrebbe quindi spedire tutti i 2MSS di nuovi dati. Dato che l'host di A spedisce solo 1MSS di dati abbiamo che B1.RcvWin=1MSS, A1.SeqNum=X+2MSS e, dato che in t2 scatta il timeout, anche A2.SeqNum=X+2MSS. Quando riceve B2, l'host di A spedisce nuovi dati nel segmento A31. Dato che in t2 CongWin è diventata 1MSS e l'host di A ha 1MSS "in volo", B2 deve contenere un riscontro "positivo"2, ovvero B2.AckNum=X+3MSS, e B2.RcvWin>0. Infine, A3 conterrà min(1MSS, B2.RcvWin) dati e A3.SeqNum=X+3MSS.

Con un ragionamento analogo al caso precedente, osserviamo che se B1.AckNum=X+1MSS allora B1.RcvWin=2MSS e A1.SeqNum=X+2MSS. Allo scadere del timer in t2, l'host di A rispedirà il segmento più vecchio ancora in volo, ovvero A2.SeqNum=X+1MSS. Come nel caso precedente, B2 deve contenere un riscontro positivo e abbiamo quindi due possibile sotto-casi:
(b1) Se B2.AckNum=X+3MSS allora B2.RcvWin>0 e A3 conterrà min(1MSS, B2.RcvWin) dati
(b2) Se B2.AckNum=X+2MSS allora B2.RcvWin>1MSS e A3 conterrà min(1MSS, (B2.RcvWin-1MSS)) dati In entrambi i casi A3.SeqNum=X+3MSS.

Es2. La tabella di routing del nodo **A** risulta**:**

DESTINAZIONE	NEXT HOP	COSTO
B	**B**	*3*
C	**B**	*5*
D	**B**	*8*

Es3. Il protocollo descritto non permette ad A di autenticare B. Tale protocollo è infatti suscettibile a un attacco "man-in-the-middle" in cui un intruso T intercetta il *nonce* inviato da A e invia quindi ad A il messaggio: $< K^+_A(B, K^+_T),\ K^+_A(K^-_T(n)) >$ che potrebbe indurre A a considerare K^+_T la chiave pubblica di B autenticando in questo modo erroneamente T come B.