DMIF, Università degli Studi di Udine IV appello A.A. 2019-20 — 20 luglio 2020

Esame di **Reti di Calcolatori**

Soluzione

1. Si dica in quale protocollo o livello dello stack TCP/IP viene implementata ognuna delle seguenti funzionalità: (a) Frammentazione; (b) Rilevamento/correzione errori di trasmissione; (d) Cifratura del payload applicativo; (c) Riordinamento messaggi fuori sequenza.

   R: (a) IP; (b) Datalink (Ethernet, ecc); (c) SSL o TLS; (d) TCP (trasporto).

2. Si vuole realizzare una linea di trasmissione utilizzando un fascio di microonde in una banda di frequenza di 500 MHz, centrata a 10 GHz. Ogni simbolo trasmesso codifica 4 bit grezzi e per la trasmissione senza errori viene utilizzato un algoritmo di correzione FEC con un code rate di 1/2. Determinare il minimo valore del rapporto segnale/rumore in dB (potenza) necessario per la trasmissione senza errori.

   R: Come conseguenza del teorema SH abbiamo $\log_2 M \leq 1/2 * \log_2(1 + SNR)$, ove $\log_2 M$ è il numero di bit per simbolo trasmessi senza errore. Poiché ogni baud codifica 4 bit e il FEC ha un code rate 1/2, $\log_2 M = 4 * 1/2 = 2$ e quindi $SNR \geq 22 * 2–1 = 15$, cioè $SNR \geq 11.8dB$.

3. Si vuole trasmettere la sequenza di bit 10110101 aggiungendo un codice CRC usando il polinomio generatore $x^3 + 1$. Come è fatto il messaggio complessivo?

   R: Il messaggio complessivo è 10110101*001*. Qui sotto il calcolo del CRC.

```
10110101 000  | 1001
1001
====
001001
  1001
  ====
  000001 000
       1 001
       = ===
       0 001
```

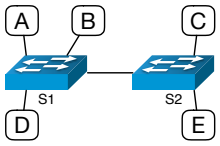
4. Tre host collegati da una Ethernet "classica" (10Mbps su cavo coassiale), provano a trasmettere contemporaneamente un frame ognuno. (a) Qual è il numero minimo di tentativi necessario affinché tutti gli host riescano a spedire i loro frame? (b) Qual è la probabilità che un host riesca a trasmettere un frame al secondo tentativo?

   R: (a) Quattro: il primo fallisce per tutti, al secondo uno trasmette e gli altri aspettano, al terzo il secondo trasmette e l'altro aspetta, al quarto anche l'ultimo riesce a spedire il messaggio. (b) Al secondo tentativo ogni host sceglie un ritardo a caso tra 0 e 1 slot. Affinché un host riesca a trasmettere, bisogna che scelga 0 mentre gli altri scelgono 1. Questo succede con probabilità $3/8 = 37.5\%$.

5. Si supponga che in una certa cella WiFi i nodi siano tutti sullo stesso piano dell'access point, e non ci siano ostacoli alla propagazione delle onde. Al massimo, quanti nodi possono essere associati all'access point, e contemporaneamente tutti nascosti l'uno all'altro?

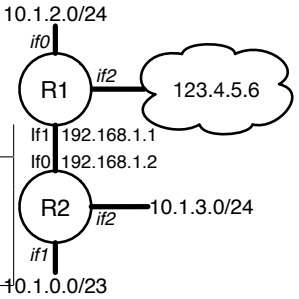
   R: Cinque. Se fossero 6, formerebbero un esagono e riuscirebbero a vedersi. Con un pentagono il lato è più lungo della distanza dal centro.

6. La rete a lato è composta da switch ad autoapprendimento, le cui tabelle di inoltro sono già popolate. Ad un certo punto, l'host A viene scollegato da S1 e collegato a S2 al posto di C, e viceversa. Si supponga che A e C non trasmettano alcun frame (per ora), stanno solo ricevendo. (a) I frame inviati verso A vengono recapitati correttamente? (b) Tale situazione è stabile, o cambia dopo un po' di tempo?



R: (a) No, perché S1 continuerebbe a mandarli sulla vecchia porta dove ora c'è C, che li scarta perché non hanno l'indirizzo giusto. (b) Bisogna aspettare il timeout delle entry nelle tabelle interne degli switch. A quel punto si ritorna in modalità flooding.

7. I router in figura hanno le tabelle qui sotto, e applicano le regole di inoltro in ordine. (a) Le tabelle sono corrette? ossia, gli host di tutte le reti sono raggiungibili? (b) Se no, si indichi la/e regola/e errata/e, e si suggerisca una possibile correzione.



R1:

Net/CIDR	if	next hop
10.1.0.0/22	if1	192.168.1.2
10.1.2.0/24	if0	-
192.168.1.0/24	if1	-
/	if2	10.1.3.1

R2:

Net/CIDR	if	next hop
10.1.0.0/23	if1	-
10.1.3.0/24	if2	10.1.3.1
192.168.1.0/24	if0	-
/	if0	192.16.1.1

R: Ci sono diversi errori. (a) No, la 10.1.2.0/24 non è raggiungibile perché la prima regola di R1 sussume anche quella rete ed è errato. (Inoltre il default gateway di R1 deve essere 123.4.5.6, e in R2 il next hop per 10.1.3.0/24 non ci deve essere perché è una consegna diretta). (b) Ecco le tabelle corrette:

R1:

Net/CIDR	if	next hop
10.1.2.0/24	if0	-
10.1.0.0/22	if1	192.168.1.2
192.168.1.0/24	if1	-
/	if2	123.4.5.6

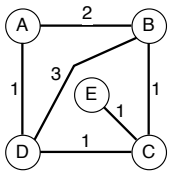
R2:

Net/CIDR	if	next hop
10.1.0.0/23	if1	-
10.1.3.0/24	if2	-
192.168.1.0/24	if0	-
/	if0	192.16.1.1

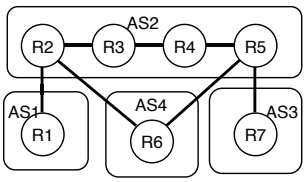
8. In una certa rete, il router di frontiera R1 è collegato al router R2 del provider. Si osserva che l'indirizzo dell'interfaccia if1 di R1 è 192.168.174.34. Il computer A ha indirizzo 10.10.2.31. (a) Qual è l'indirizzo "pubblico" con cui il traffico di A viene instradato sull'Internet? (b) Si desidera offrire un servizio web (porta 80) sull'host A. È sufficiente "aprire" la porta 80 su R1 e inoltrarla a A?

R: (a) Qui siamo davanti a due o più NAT annidati. Quindi l'indirizzo pubblico è quello dell'ultimo NAT. NON è 192.168.17.34. (b) No, bisogna forwardare anche su tutti gli altri NAT (almeno R2).

9. I router della rete a lato utilizzano un algoritmo di routing basato sullo stato dei collegamenti. (a) Poco dopo l'accensione (e quindi il reset), A riceve i pacchetti LSP originati da B e D. Si disegni l'albero di copertura che A determina a tal punto. (b) Se poi ad A arriva un pacchetto LSU (link state update) originato da D e che dice che il costo D-C è 3, quale sarà da A il next hop per raggiungere C?
R: (a) A-B, A-D-C. Il router E non è ancora raggiungibile. (b) B



10. Gli autonomous systems a lato implementano BGP. AS2 e AS4 sono di transito.
(a) Qual è il percorso più breve, in numero di hop tra router, da AS1 a AS3?
(b) Qual è il percorso che viene definito da BGP, da AS1 a AS3, e perché?
R: (a) R1-R6-R5-R7 (b) R1-R2-R3-R4-R5-R7, perché BGP non permette di tornare sullo stesso AS (sarebbe un loop, e vengono sempre evitati da BGP, e qui AS2 può raggiungere AS3 direttamente).



11. (a) L'operazione di `accept()` su una socket a flusso, a cosa corrisponde nell'automa a stati finiti di TCP?
(b) L'operazione di `bind()` è necessaria per il server? E per il client?

R: (a) al passaggio da LISTEN a ESTABLISHED, passando per SYN_RECEIVED (apertura passiva).
(b) Sì, perché altrimenti non sappiamo su che porta va ad ascoltare. Per il client non è strettamente necessario: senza la bind, si usa una porta effimera.

12. Un client TCP ha ricevuto un segmento con FIN=1. (a) In che stato si porta la sua socket? (b) Può ricevere ancora dati dalla controparte? (c) Può inviare ancora dati alla controparte?

    R: Si tratta di chiusura passiva. (a) CLOSE_WAIT; (b) Solo ritrasmissioni di dati vecchi (e non arrivati). (c) Sì, finché l'applicazione non decide di chiudere.

13. Un'applicazione produce dati alla velocità di 10kB/s, su una connessione TCP con MSS=1460 byte e RTT=50ms. (a) Qual è la dimensione dei segmenti inviati? (b) Qual è l'efficienza della trasmissione, considerando l'overhead causato dalle intestazioni TCP e IP?

    R: (a) In 50ms vengono prodotti $50 * 10^{-3} * 10 * 10^3 = 500$ byte. Essendo meno di MSS, ogni volta che arriva un ACK viene inviato quanto abbiamo nel buffer, ossia questi 500 byte. (b) L'overhead è di 20+20=40 byte, quindi l'efficienza è 500/540 = 92,6%.

14. Una certa interfaccia di uscita di un router ha una velocità di 10Mbps = 1.25 MB/s; deve servire un flusso di pacchetti di lunghezza media 1000 byte, che arrivano casualmente con una frequenza media di 500 pacchetti al secondo. Quant'è, in media, il ritardo introdotto dal router sui pacchetti in arrivo?

    R: Usiamo la teoria delle code. La frequenza di arrivo è $\lambda = 500$ p/s; Il tempo di servizio di un pacchetto è $S = 1000/1.25 * 10^6 = 0.8 * 10^{-3}$ s/p. Da cui: $R = S/(1 - \lambda S) = 0.8 * 10^{-3}/(1 - 500 * 0.8 * 10^{-3}) = 0.8 * 10^{-3}/0.6 = 1.33$ ms.

15. Per ognuna delle seguenti azioni, si dica se è attacco passivo o attivo, e a quale aspetto di sicurezza. (a) Estrarre l'hard disk da un PC, clonarlo e rimetterlo al suo posto. (b) Inserire un keylogger (dispositivo di intercettazione) sul cavo della tastiera. (c) Replicare in un secondo tempo i dati di login intercettati.

    R: (a) passivo, alla confidenzialità dei dati (perché non si interferisce con i dati stessi, che rimangono inalterati). Non è detto che sia un attacco alla disponibilità, perché magari questa operazione è effettuata quando non ci sono tentativi di accesso ai dati (ad esempio di notte). (b) passivo, alla confidenzialità dei dati (c) attivo (replay), masquerade

16. Un certo file system cifrato cifra i file usando AES in modalità CBC. Si vuole leggere il byte in posizione 1341. (a) Quale sezione di file bisogna effettivamente caricare dal disco (byte di inizio-byte di fine)? (b) E se dovessimo modificare tale byte, quale sezione dovremmo andare a riscrivere?

    R: (a) AES ha un blocco di dimensione 16 byte, quindi il byte 1341 cade nel blocco $\lfloor 1341/16 \rfloor = 83$. Per decifrare il blocco 83 bisogna caricare anche il blocco 82, che fa da IV. Quindi si deve leggere da 82*16=1312 a 83*16-1=1343 (32 byte). (b) Dal blocco 83 = posizione 1328 in poi, fino alla fine del file.

17. Nel protocollo a lato, K_A, K_B sono le chiavi master precondivise tra A, B e il KDC, e K è una chiave di sessione generata da A. (a) La chiave K è puntuale (ossia non soggetto ad attacchi replay)? (b) Come può un attaccante impersonare A? (c) Si può evitare tale attacco, con una modifica minima al protocollo?

    1. $A \to KDC : A, E_{K_A}(B, K)$
    2. $KDC \to A : E_{K_B}(B, K)$
    3. $A \to B : A, E_{K_B}(B, K)$

    R: (a) Sì, ripetendo il messaggio al passo 2. (b) Eva inizia il protocollo normalmente, poi al passo 3. invia $E \to B : A, E_{K_B}(B, K)$, e B pensa di parlare con A. (c) 2. $KDC \to A : E_{K_B}(A, B, K)$ (e magari anche una nonce per evitare l'attacco replay)

18. Il protocollo a lato simula l'emissione di un certificato di chiave pubblica da parte di una CA. PU_A è la chiave pubblica che A ha appena creato; i passi 2-3, dove N è una nonce, mirano ad autenticare A. T è il timestamp di emissione e H è una funzione di hash prefissata. (a) A è autenticato per CA? (b) Il timestamp è autentico (ossia, è inalterabile)? (c) Come si dovrebbe aggiungere l'informazione di lifespan (durata) L del certificato?

    1. $A \to CA : A, PU_A$
    2. $CA \to A : E_{PU_A}(N)$
    3. $A \to CA : N$
    4. $CA \to A : T, E_{PR_{CA}}(A, H(PU_A, T))$

    R: (a) No, chiunque può spacciarsi per A al passo 1, e rispondere correttamente al passo 3. (b) Sì, è garantito dalla hash firmata. (c) 4. $CA \to A : T, L, E_{PR_{CA}}(A, H(PU_A, T, L))$

19. Un utente deve autenticarsi presso un AS Kerberos, che rilascia token della durata di 1 ora. Prima di procedere all'autenticazione, sposta in avanti di due ore l'orologio del proprio PC. (a) Il ticket che ottiene è valido per due ore in più? (b) Riesce comunque ad autenticarsi presso i TGS?

    R: (a) No, perché nel ticket c'è il timestamp del server, non del client. (b) Sì, secondo le normali regole, ossia per una sola ora. Il TGS controlla il timestamp nel token, non timestamp del client.

20. IPSec utilizza una finestra scorrevole di larghezza 64 come misura anti-replay. Ad un certo punto, un host ha ricevuto come pacchetto più avanzato, il pacchetto numero 98. Riceve poi i seguenti pacchetti (nuovi, mai ricevuti prima) in questo ordine: 39, 100, 99, 33, 99. (a) Quali tra questi pacchetti vengono accettati? (b) Dopo questi pacchetti, qual è il minimo pacchetto accettabile?

    R: (a) 39, 100, 99 (prima copia) (b) 100-64+1 =37.