Università degli Studi di Udine

DIMA — Dipartimento di Scienze Matematiche, Informatiche e Fisiche

Esame di **Reti di Calcolatori**

Soluzione

A.A. 2016-17 — III appello — 19 giugno 2017

N.B.: ove non specificato diversamente, ogni esercizio vale 3 punti. Per calcolare il voto effettivo bisogna sommare tutti i punti conseguiti e normalizzare a 33.

1. Al tempo $t_0 = 0$ un'antenna inizia a inviare con velocità $c = 2.5 \cdot 10^8$ m/s un segnale cosinusoidale $s(t) = A\cos(2\pi ft)$ a frequenza $f = 10$ MHz verso una seconda antenna, posta a distanza $d = 10$ km dalla prima. Si calcoli l'istante t_1 successivo a t_0 in cui la seconda antenna capta il decimo picco negativo del segnale ricevuto s_R: $s_R(t_1) = -A$.

   R: Il segnale raggiunge l'antenna ricevente dopo un tempo

   $\tilde{t} = d/c = \dfrac{10^4}{2.5 \cdot 10^8} = \dfrac{10 \cdot 10^3}{2.5 \cdot 10^8} = 4 \cdot 10^{-5}$ s.

   Data la conformazione della funzione coseno, in cui il picco negativo occorre trascorso mezzo periodo T, il decimo picco negativo viene captato trascorsi 9.5 periodi di segnale: $t^* = 9.5T = 9.5/f = 9.5 \cdot 10^{-7}$ s. E quindi si ha

   $t_1 = \tilde{t} + t^* = 4000 \cdot 10^{-8} + 95 \cdot 10^{-8} = 4095 \cdot 10^{-8}$ s.

2. Un cavo per la trasmissione di segnali, senza attenuazione, introduce un rumore medio di potenza $N_0 = 1$ mW misurata all'uscita del cavo. Si crea un canale giuntando 4 cavi di questo tipo attraverso tre amplificatori ideali (uno per giunzione), ciascuno avente un fattore di amplificazione $\alpha = 2$. Detto SNR_i il rapporto segnale/disturbo all'uscita dell'i-esimo cavo (prima dell'amplificatore), quale dev'essere la potenza P_0 del segnale immesso nel canale nell'ipotesi di richiedere $SNR_4 = 0$ dB al termine del canale?

   R: Dette `P` e `N` rispettivamente le potenze del segnale e del rumore, ricordando che 0 dB equivale a dire $SNR_4 = 1$ è sufficiente: i) calcolare la potenza del rumore uscente, ii) eguagliare le potenze all'uscita del canale, e iii) calcolare la potenza del segnale entrante andando a ritroso nel canale:

```
P              1.875               3.75               7.5                15  mW
   ----------------- > ----------------- > ----------------- > -----------------
N                  1   2               3    6              7   14             15  mW
```

   In conclusione, $P_0 = 1.875$ mW.

3. Con riferimento al canale dell'esercizio precedente, detta C_i la capacità misurata all'uscita dell'i-esimo cavo (prima dell'amplificatore), si calcolino i rapporti tra le capacità all'uscita di ogni cavo e la capacità all'uscita del canale: C_1/C_4, C_2/C_4, C_3/C_4, C_4/C_4. Il risultato cambia se le stesse capacità sono misurate dopo il rispettivo amplificatore?

   R: Essendo le tratte di canale composte usando cavi identici, la banda è costante su tutto il canale. Quindi, osservando che da $SNR_4 = 1$ si ha $C_4/B = \log_2(1 + SNR_4) = 1$, è sufficiente calcolare

   $C_1/B = \log_2\left(1 + \dfrac{1.875}{1}\right) \approx 1.5236$

   $C_2/B = \log_2\left(1 + \dfrac{3.75}{3}\right) \approx 1.17$

   $C_3/B = \log_2\left(1 + \dfrac{7.5}{7}\right) \approx 1.05$

   per trovare i rapporti richiesti. Gli stessi rapporti non variano se misurati prima o dopo il rispettivo amplificatore ideale, il quale per sua natura non cambia il rapporto segnale/disturbo.

4. In un canale con periodo di clock T in cui si adopera la codifica di bit Manchester, il decodificatore al ricevitore si guasta. Restano disponibili un decodificatore NRZ e un decodificatore NRZI. Nell'ipotesi di poter scegliere l'istante esatto all'interno del periodo di clock in cui il decodificatore decide qual è il bit ricevuto, c'è un modo per riuscire a decodificare ugualmente i bit codificati Manchester?

   R: Poichè il livello del segnale nella codifica Manchester è identico a quello nella codifica NRZ in ogni istante all'interno della prima metà del periodo di clock, è sufficiente che un decodificatore NRZ decida il bit scegliendo ogni volta un istante all'interno appunto del primo semiperiodo di clock. Viceversa, il segnale codificato mediante NRZI in generale non è in relazione con quello codificato mediante Manchester.

5. Un nodo in una rete di commutazione a pacchetto invia a un singolo destinatario 4 pacchetti etichettati ciascuno con il rispettivo numero d'ordine d'invio: 1,2,3,4. A causa di un guasto i pacchetti sono casualmente instradati nella rete. In assenza di ulteriori informazioni, a quanto ammonta la probabilità che gli stessi pacchetti giungano a destinazione nello stesso ordine in cui sono stati inviati?

   R: Le combinazioni possibili con cui i pacchetti possono essere ordinati sono $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ (per 4 possibili scelte del primo pacchetto ne rimangono tre per il secondo, due per il terzo e infine una per il quarto). La probabilità di ricevere casualmente i pacchetti in sequenza ordinata è quindi $p = 1/24$.

6. Nel protocollo di framing orientato ai bit denominato HDLC si applica lo *stuffing* dopo il quinto bit, e in più si adotta l'ottetto `01111110` come sequenza di controllo sia d'inizio che di fine frame. Come si comporta l'algoritmo di estrazione del messaggio se per errore il frame ricevuto contiene l'ottetto `01111111`?

   R: In presenza di un simile ottetto è avvenuto un errore o sul sesto bit di *stuffing* oppure sulla sequenza di controllo. In questa situazione il sistema scarta l'intero frame e attende l'arrivo di una nuova sequenza di controllo.

7. In un'aritmetica di polinomi in complemento a 2 associata a una codifica a correzione d'errore CRC, sia $P(x)$ il polinomio caratteristico del messaggio trasmesso, $P'(x)$ quello del messaggio ricevuto, $C(x)$ il polinomio generatore ed $E(x)$ il polinomio caratteristico rappresentativo dell'eventuale errore di trasmissione. Adoperando questi polinomi, si spieghi come un decodificatore CRC decide se il messaggio ricevuto è affetto da errore.

   R: Il decodificatore CRC calcola il resto $E(x)$ della divisione $P'(x)/C(x)$. Se $E(x) \neq 0$ allora decide per la presenza di un errore nel messaggio ricevuto.

8. Si consideri la compressione ideale di un testo effettuata mediante l'invio di un dizionario di n parole assieme al testo compresso. L'invio è ottimizzato in modo che ogni parola del testo da comprimere è anche nel dizionario, e ogni parola del dizionario compare almeno una volta nel testo. Se ogni parola è mediamente lunga 16 bit e ogni parola dopo la compressione è mediamente lunga 8 bit, quante parole devono essere mediamente presenti nel testo da comprimere affinché la compressione risulti vantaggiosa?

   R: Si ha una situazione vantaggiosa quando l'invio del dizionario (n parole ciascuna lunga mediamente 16 bit) piú il testo compresso (k parole ciascuna lunga mediamente 8 bit) ha un peso globalmente minore dell'invio dello stesso testo privo di compressione (k parole ciascuna lunga mediamente 16 bit):

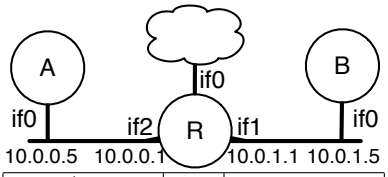
   $n \cdot 16 + k \cdot 8 < k \cdot 16 \Rightarrow n \cdot 16 < k \cdot 8 \Rightarrow k > 2 \cdot n.$

   In altre parole il testo da comprimere deve avere lunghezza almeno mediamente doppia rispetto a quella del dizionario.

9. La rete di un certo ente è composto da quattro sottoreti: tre con 20 host ciascuna e una da 50 host. Quanto deve essere il CIDR minimo che l'ente deve farsi assegnare dal suo provider?

   R: Ogni sottorete piccola richiede 5 bit per gli host, e la quarta ne richiede 6. Purtroppo non bastano 7 bit, perché poi non si riesce a suddividere una da 64 indirizzi in tre sottoreti da 20. Pertanto ne servono 8 bit, e quindi il CIDR è 24 (ossia una rete in classe C).

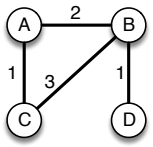
10. Si consideri la rete a lato, il cui router ha la tabella di instradamento riportata. Cosa succede se: (a) A invia un pacchetto a B; (b) B invia un pacchetto ad A; (c) A prova ad aprire un collegamento TCP con 174.23.54.76.



Net/CIDR	if	next hop
10.0.0.0/23	if2	-
10.0.1.0/23	if1	-
/	if0	150.13.12.3

R: In pratica 10.0.1.0/23 è equivalente a 10.0.0.0/23, perché quel bit di differenza non viene considerato (i CIDR delle due reti dovrebbero essere /24). Quindi:
(a) il pacchetto non arriva a destinazione, perché il router applica la prima regola e prova a reinviarlo attraverso if2.
(b) il pacchetto arriva a destinazione, perché si applica la prima regola e quindi viene consegnato ad A.
(c) la connessione si realizza correttamente, perché il router instrada correttamente i pacchetti da e per A.

11. I router della rete a lato utilizzano un algoritmo di routing basato sul vettore delle distanze. (a) Si dia la tabella di routing finale di B; (b) Quale evento potrebbe portare all'instabilità della rete?



R:

dest	d	next hop
A	2	A
B	0	-
C	3	C
D	1	D

L'evento è l'interruzione del collegamento tra B e D, e in contemporanea l'invio del vettore da C a B o da A a B; in tale situazione, B crede di poter raggiungere D attraverso A o C, ecc.

12. Un host con indirizzo 192.168.1.123 ha stabilito una connessione TCP con l'host 172.217.23.132, attraversando un router che implementa NAT. Ad un certo punto, l'indirizzo esterno del router viene cambiato. Cosa succede alla connessione in corso? E se la comunicazione fosse su UDP?

R: La comunicazione TCP viene resettata, perché i pacchetti dal server verrebbero inviati ad un indirizzo pubblico errato. Mentre in una comunicazione UDP si perderebbero un numero limitato di pacchetti (cosa peraltro legittima in UDP), e poi continuerebbe con il nuovo indirizzo.

13. Si consideri un host con due indirizzi IP, I_1 e I_2. Una applicazione è in ascolto su una socket UDP con indirizzo I_1 : 8000. Lo strato IP riceve dalla rete un pacchetto indirizzato a I_2, contenente un datagramma UDP per la porta 8000. Questo datagramma viene consegnato all'applicazione? Perché?

R: Se c'è un checksum, non viene consegnato all'applicazione, perché il checksum è stato generato con lo pseudoheader che contiene I_2, mentre viene controllato con I_1 e quindi non passa il controllo.

14. Su un certo sistema il Maximum Segment Lifetime è impostato a 15 secondi, ma si osserva che una connessione con un certo client ha dei RTT anche superiori ai 40 secondi. Cosa può succedere alla chiusura/riapertura della socket?

R: Potrebbe succedere che un FIN di una incarnazione precedente arriva nel mezzo di quella nuova causando l'immediato abort della comunicazione.

15. Una sorgente TCP invia tre segmenti da 1000 byte l'uno, con SequenceNum pari a 14000, 15000, 16000 rispettivamente. Riceve due segmenti: il primo ha ACK=15000 e AdvertisedWindow=4500, il secondo ha ACK=14000 e AdvertisedWindow=1400. A quanto ammonta la EffectiveWindow?

R: Il secondo ACK è arrivato in ritardo, ed è stato reso obsoleto dal primo, che è quello che fa veramente testo. Quindi EffectiveWindow=AdvertisedWindow -(LastByteSent-LastByteAcked) = 4500 - (16999-14999) = 4500 - 2000 = 2500.

16. Durante una certa connessione TCP, si ha CongestionWindow=4000, MSS=1000, RTT=10ms. La sorgente inizia un round di trasmissione, inviando un segmento ogni 50ms. Per i primi tre segmenti la sorgente riceve l'ACK nei tempi previsti, mentre l'ACK del quarto segmento non arriva. Dopo quanto tempo dall'inizio del round scade il timeout? Quanto vale la CongestionWindow dopo tale istante?

R: Il timeout per ogni segmento è il doppio di RTT, quindi 20ms. I quattro segmenti sono inviati rispettivamente agli istanti 0, 50, 100, 150ms, quindi i rispettivi timeout sono 20, 70, 120, 170ms. Quindi

il timout scade a 170ms. Fino a quel momento, la CW è stata incrementata di 3*MSS/4= 750 byte; quindi vale 4750 byte, ma viene dimezzata per il timeout, e quindi diventa 2375 byte.

17. Perché nelle reti a circuito virtuale è facile riservare le risorse necessarie ad ogni comunicazione, prima di iniziare a trasmettere i dati? Perché allora non si usano al posto di quelle a commutazione di pacchetto?

    R: Nelle reti a circuito virtuale si può allocare le risorse necessarie al momento della creazione del circuito: il protocollo di segnalazione indica qual è il servizio richiesto, e i router allocano le risorse necessarie. Non si usano perché non sono efficienti.

18. Un vostro amico vi dice che sul suo PC usa un'applicazione via web browser che comunica con il server in modo segreto. Voi notate che il PC è connesso via WiFi e sulla barra di navigazione del browser non appare il lucchetto verde che indica l'uso di HTTPS. È possibile che il vostro amico abbia ragione? Motivate la risposta.

    R: Sì, è possibile se i dati sono cifrati a qualche altro livello dello stack. Ci sonoi tre possibilità: 1) a livello applicazione: i dati vengono cifrati da qualche programma all'interno della pagina web (ad esempio JavaScript o applet Java); 2) a livello di rete: la comunicazione tra client e server avviene via IPsec, che è trasparente ai livelli superiori 3) a livello datalink: la connessione WiFi è cifrata con WPA o WPA2, e il server è sulla stessa cella, quindi un altro host collegato allo stesso AP, o lo stesso host dove c'è il client, o l'AP stesso.

19. Un sito web richiede che le password siano di 8 caratteri, con lettere maiuscole, minuscole e cifre, ma in cui ci deve essere almeno una lettera maiuscola. Quante sono le password possibili?

    R: L'alfabeto totale sono 26+26+10=62 caratteri, ma le maiuscole sono 26 e le cifre 10. Se non ci fosse il vincolo della lettera maiuscola, ci sarebbero 62^8 combinazioni. Da queste bisogna togliere quelle che non contengono nessuna maiuscola, ossia che sono composte solo di minuscole e cifre, e che sono 36^8. Quindi le password che contengono almeno una maiuscola sono $62^8 - 36^8 = 2,155 * 10^{14}$.

20. Il protocollo a lato è un semplice scambio Diffie-Hellman, dove y_A e y_B sono le due mezze chiavi. Supponendo che le due parti abbiano condiviso un segreto K e possano usare una funzione di hash H, si completino le parti lasciate in bianco in modo da impedire l'attacco man-in-the-middle.

    1. $A \to B : y_A, \ldots$
    2. $B \to A : y_B, \ldots$

    R: 1. $A \to B : y_A, H(K, y_A)$; 2. $B \to A : y_B, H(K, y_B)$

21. Nel protocollo a lato, K è una chiave segreta precondivisa tra A e B, N è una nonce, e K' è una chiave di sessione generata sul momento da B. Il messaggio M è confidenziale? È puntuale? È non ripudiabile?

    1. $A \to B : N$
    2. $B \to A : E_K(N, K')$
    3. $A \to B : E_{K'}(M)$

    R: È confidenziale, è puntuale (perché cifrato con la chiave generata sul momento da B), ma è ripudiabile da A perché A può sostenere che il messaggio è stato creato da B stesso.

22. Con riferimento al protocollo dell'esercizio precedente: A è autenticato per B? B è autenticato per A? Si motivi la risposta.

    R: B è autenticato per A perché risponde ad una challenge al passo 2: cifra con la chiave K la nonce che ha inviato A, e solo A e B ne sono in grado. A è autenticato per B perché risponde ad una challenge al passo 3: cifra con la chiave K' un messaggio, quindi ha ottenuto la chiave K' dal precedente passo, e quindi deve conoscere K, e quindi deve essere A.

23. (2pt) In SSL e TLS, quali delle seguenti informazioni sono di sessione e quali di connessione? (a) Numero di sequenza; (b) Master secret; (c) Algoritmo di cifratura; (d) IV per la cifratura.

    R: Di sessione: Master secret e algoritmo di cifatura; le altre due sono di connessione.

24. Solitamente IPsec viene impiegato per trattare tutto il traffico tra due host o tra due reti, ma è possibile utilizzarlo per mettere in sicurezza solo le connessioni TCP tra due socket specifiche? Se sì, come?

    R: Sì, impostando adeguatamente il Security Policy Database: basta inserire una entry per la specifica connessione (indirizzo mittente, indirizzo destinazione, porta mittente, porta destinazione, protocollo) che attivi l'uso del protocollo di sicurezza richiesto, e lasciare il default come "bypass".