Università degli Studi di Udine

DIMA — Dipartimento di Scienze Matematiche, Informatiche e Fisiche

Esame di **Reti di Calcolatori**

Soluzione

A.A. 2016-17 — II appello — 13 febbraio 2017

N.B.: il punteggio associato ad ogni domanda è solo una misura della difficoltà, e peso, di ogni domanda. Per calcolare il voto complessivo bisogna normalizzare a 30 (circa).

1. (3pt) Al tempo $t_0 = 0$ un'antenna inizia a inviare a velocità $c = 2.5 \cdot 10^8$ m/s un segnale sinusoidale $s(t) = A\sin(2\pi ft)$ di frequenza $f = 10$ MHz verso una seconda antenna, posta a distanza $d = 10$ km dalla prima. Si calcoli il primo istante t_1 successivo a t_0 in cui il segnale si annulla nel minor numero di punti appartenenti allo spazio tra le due antenne (incluse). Si conti anche il numero di punti in cui, nel medesimo istante t_1, il segnale $s(t)$ è nullo.

   R: Dopo avere coperto lo spazio in questione in un tempo $t_S = d/c = 10^4/(2.5 \cdot 10^8) = 4 \cdot 10^{-5}$ s, il segnale si ripete periodicamente nello spazio per $d/\lambda = d \cdot f/c = 10^4 \cdot 10^7/(2.5 \cdot 10^8) = 400$ volte. Dunque in corrispondenza delle due antenne i valori del segnale sono sempre identici. In più nello stesso tempo t_S il segnale ha ovviamente ciclato esattamente per $t_S/T = t_S \cdot f = d \cdot f/c = 400$ volte, quindi il suo valore è nullo in corrispondenza delle due antenne. Il numero minimo di zeri nello spesso spazio si ha dunque quando questo tempo è appena trascorso: $t_1 > t_S$. A questo punto gli zeri sono $2 \cdot 400 = 800$.

2. (3pt) Un cavo per la trasmissione di segnali possiede un fattore di attenuazione $\beta = 0.5$ e contemporaneamente introduce un rumore medio di potenza N_0, 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 uguale a $\alpha = 4$. Detto SNR_i il rapporto segnale/disturbo all'uscita dell'i-esimo cavo (prima dell'amplificatore), quanto vale il rapporto SNR_1/SNR_4?

   R: Indicando ogni amplificatore con `=>`, le potenze del segnale e del rumore sono le seguenti:

```
P        P/2  2P        P   4P       2P   8P        4P
----------=>----------=>----------=>----------
           N  4N     2N+N   12N    6N+N   28N    14N+N
```

   e quindi

   $$\frac{SNR_1}{SNR_4} = \frac{\frac{P_0}{2N_0}}{\frac{4P_0}{15N_0}} = \frac{15}{8}.$$

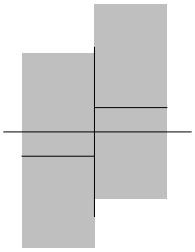
3. (3pt) Nel caso particolare in cui nel canale precedente entri un segnale di potenza P_0 tale che $P_0 = N_0$, detta C_i la capacità del canale all'uscita dell'i-esimo cavo (prima dell'amplificatore), si calcolino i rapporti C_2/C_1, C_3/C_1 e C_4/C_1, motivando sinteticamente l'andamento della successione di valori trovati.

   R: $C_1 = B\log_2(1 + \frac{P_0}{2N_0})$, $C_2 = B\log_2(1 + \frac{P_0}{3N_0})$, $C_3 = B\log_2(1 + \frac{2P_0}{7N_0})$, $C_4 = B\log_2(1 + \frac{4P_0}{15N_0})$,
   da cui immediatamente i tre rapporti con $P_0/N_0 = 1$. Gli stessi rapporti riflettono la diminuzione della capacità di canale al crescere della potenza del rumore rispetto a quella del segnale.

4. (2pt) Nel canale precedente, in presenza delle potenze di segnale e di rumore proposte si può realizzare una codifica NRZ senza problemi? Si motivi la risposta.

   R: All'uscita del canale il rapporto segnale-disturbo è uguale a 4/15. Una codifica NRZ vedrebbe dunque il segnale di tensione positiva e quello di tensione negativa severamente affetti da rumore, con i problemi che ne conseguono.

5. (4pt) Si provi a stimare la probabilità d'errore p su ogni bit ricevuto nel canale precedente, in cui sia stata realizzata la codifica NRZ.



R: L'ampiezza del segnale NRZ, la cui ampiezza è normalizzata al valore 4, e del rumore che lo altera sono rappresentate in figura. Il segnale è decodificato scorrettamente se il suo segno cambia durante la trasmissione. Questo accade se il rumore ha segno opposto al segnale ed è in modulo maggiore di 4. Poichè con la normalizzazione scelta i valori assunti dal rumore sono distribuiti uniformemente tra -15 e 15, la probabilità che ciò accada è uguale a $(30-19)/30 = 11/30$.

6. (3pt) Si calcolino risultato e resto di $(x^9+x^2+1)/(x^3+x^2+1)$ in aritmetica modulo 2.

   R:

```
1000000101|1101
1101      |------
----      |111010
01010     |
 1101     |
 ----     |
 01110    |
  1101    |
  ----    |
  00110   |
   0000   |
   ----   |
   01101  |
    1101  |
    ----  |
    00000 |
     0000 |
     ---- |
      0001|
```

   da cui $(x^9+x^2+1) = (x^6+x^5+x^4+x^2)(x^3+x^2+1)+1$.

7. (3pt) Qual è la minima lunghezza che può avere un frame nel protocollo ethernet?

   R: $64+32 = 96$ bit, il che accade quando un nodo rileva la collisione immediatamente dopo avere iniziato a inviare i primi 64 bit del preambolo, a cui segue una *jamming sequence* lunga 32 bit.

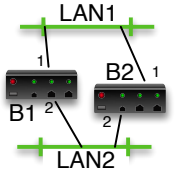
8. (3pt) Perché il campionamento che JPEG opera sui blocchi Y,U,V di dimensione 32x32 produce un blocco U 8x8 e un blocco V 8x8 invece di 4 blocchi 8x8, come accade per la componente Y?

   R: Perchè l'occhio è più accurato nel discriminare la componente di luminanza Y di un'immagine rispetto al suo colore.

9. (3pt) Un ente gestisce la rete 129.23.94.0/24, che viene suddivisa in 4 sottoreti: una "grande", una "media" e due "piccole" ed uguali. Si diano gli indirizzi (completi di CIDR) per ciascuna di queste reti.

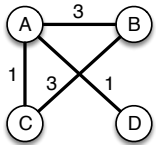
   R: Ci sono diverse soluzioni; una è la seguente: 129.23.94.0/25, 129.23.94.128/26, 129.23.94.192/27, 129.23.94.224/27.

10. (3pt) Si consideri la rete a lato con due switch ad autoapprendimento. B1 è il root bridge e ha le tabelle interne completamente aggiornate, mentre B2 è appena stato resettato e non ha ancora iniziato l'apprendimento né l'algoritmo di spanning tree. Cosa succede se un host A sulla LAN1 invia un frame indirizzato ad un host B collegato alla rete LAN2, prima che B invii un qualsiasi frame? E se A invia tale frame dopo che B ha inviato un frame?



R: Finché B2 non impara la posizione degli host sulla rete, inoltra tutti i pacchetti che vede da una parte all'altra. Quindi il frame inviato da A viene inoltrato sia da B1 sia da B2. Ora, quando B1 inoltra il frame sulla LAN2, questo viene ricevuto anche da B2 (siamo su un mezzo condiviso, come Ethernet), che non sa dove si trovi B; quindi, a rigore, deve inoltrare tale frame da LAN2 a LAN1. A questo punto lo riceve anche B1, che lo rimanda su LAN2, e così via. Questo loop si interrompe non appena B fa notare la propria presenza, trasmettendo un frame (e quindi informando B2 della sua posizione), oppure parte l'algoritmo di spanning tree e B2 si disattiva.

11. (3pt) Nella rete a lato i nodi utilizzano un algoritmo di routing basato sul vettore delle distanze. Si dia la tabella di instradamento del nodo B. Come diventa tale tabella se si aggiunge un collegamento tra B e D di peso 1?



R:

Destinazione	Hop	Next
A	3	A
B	0	-
C	3	C
D	4	A

Destinazione	Hop	Next
A	2	D
B	0	-
C	3	C
D	1	D

12. (3pt) A cosa serve il meccanismo NAT? Perché è utile per contrastare la carenza di indirizzi IPv4?

R: Il NAT serve per tradurre gli indirizzi IP da una rete ad un'altra, specialmente per uscire/entrare da una rete "cieca" come 10/8 o 192.168/16. Aiuta a contrastare la carenza di indirizzi IPv4 perché, associato alla traduzione di porte (PAT), permette di utilizzare un numero ridotto di indirizzi IPv4 pubblici (anche uno solo) per un insieme più ampio di host.

13. (3pt) Un server sta inviando dati ad un client via UDP con datagrammi di 1kB di payload, ad una velocità di 12 datagrammi al secondo, su una rete che perde il 5% dei pacchetti. Nel contempo, il client consuma i dati ad una velocità di 10 datagrammi al secondo. Se il buffer di ingresso del client è di 128kB, in quanto tempo si riempie?

R: I dati che arrivano al client sono 12*0,95 = 11,4 datagrammi al secondo. Quindi la differenza tra dati arrivati e dati consumati è 11,4-10=1,4 datagrammi al secondo = 1,4 kB/s. Il buffer si riempie in 128/1,4=91,4 secondi.

14. (3pt) Durante la fase di handshake TCP, un host ha inviato `SequenceNum` = 2000 con SYN=1, e ha ricevuto un segmento con `SequenceNum`=3000, SYN=1, ACK=1, `Acknowledge`=2001. Come sono i flag SYN, ACK e i campi `SequenceNum` e `Acknowledge` del prossimo segmento che invierà l'host?

R: L'host in questione sta eseguendo l'apertura attiva, e il prossimo segmento sarà il terzo della sequenza. Quindi, avrà SYN=0, ACK=1 `SequenceNum`=2001, `Acknowledge`=3001.

15. (3pt) In una connessione TCP, l'host A ha inviato all'host B un segmento di 1000 byte con `SequenceNum` = 10000, e riceve da B un segmento con `AdvertisedWindow` = 5000, `Acknowledge` = 8000. Quanti dati può ancora inviare A?

R: La finestra effettiva è 5000 - (10000+1000-8000) = 2000.

16. (3pt) Un router sta servendo tre flussi di pacchetti. Il primo flusso è composto da pacchetti con payload medi di 100 byte; il secondo ha payload di 200 byte; il terzo ha payload da 300 byte. Volendo assegnare la stessa quantità di banda ad ogni flusso, quale deve essere il rapporto tra il numero di pacchetti selezionati da ogni coda?

R: Deve essere $100 * n_1 = 200 * n_2 = 300 * n_3$; la soluzione più semplice è $n_1 = 6, n_2 = 3, n_3 = 2$, ossia ogni 6 pacchetti del primo flusso si inviano 3 del secondo e 2 del terzo.

17. (3pt) Un router adotta la strategia RED con MinThresh=50%, MaxThresh=80% su una coda che attualmente è piena al 60%. Qual è la probabilità che il prossimo pacchetto venga scartato?

R: Basta applicare la formula: $p = (Len - Min)/(Max - Min) = (60 - 50)/(80 - 50) = 10/30 = 33\%$

18. (3pt) Per ognuna delle seguenti affermazioni, si dica se è vera o falsa. (a) Implementare servizi di sicurezza negli strati bassi dello stack garantisce una maggiore sicurezza dei dati applicativi. (b) I protocolli di sicurezza a livello di rete sono trasparenti (=invisibili) ai programmatori. (c) I protocolli di sicurezza a livello di rete impediscono l'analisi del traffico.

    R: (a) falso; (b) vero; (c) falso.

19. (3pt) Un programma utilizza AES con una chiave di 256 bit, che è ottenuta dalla hash di una password di otto caratteri alfanumerici (ossia le 26 lettere minuscole, le 26 maiuscole e 10 cifre). In media, quanto tempo serve per trovare la chiave con un attacco brute force, potendo eseguire 10^6 tentativi al secondo?

    R: Il reale spazio delle chiavi è $62^8 = 2.18 * 10^{14}$; i 256 bit sono ininfluenti. Di conseguenza, in media bastano $2.18 * 10^{14}/(2 * 10^6) = 1,1 * 10^8$ secondi, ossia 1263 giorni, ossia 3,5 anni.

20. (2pt) Alice riceve da Bob un certificato X.509 rilasciato da una CA a lei ignota. Cosa deve fare Alice per verificare l'autenticità di tale certificato?

    R: Deve innanzi tutto risalire la gerarchia delle CA, ossia reperire la catena di certificati da quello di Bob fino ad una (root) CA nota. Ogni certificato deve essere verificato controllando la firma digitale in esso contenuto.

21. (3pt) Nel protocollo a lato, B conosce la chiave pubblica PU_A di A (che ha la corrispondente chiave privata PR_A), K è una chiave di sessione generata da A e N è una nonce generata da B. Il messaggio M è confidenziale? È autentico e puntuale? È ripudiabile da A?

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

    R: Non è confidenziale: chiunque può decifrare il messaggio al passo 3, ed ottenere la chiave K, con cui decifrare il messaggi del passo 1.

    È autentico e puntuale: la nonce garantisce la puntualità di K, e questa la puntualità di M.

    È ripudiabile da A: in teoria B può generarsi e cifrarsi un altro messaggio M', usando la K e la N di una sessione precedente, quindi B non può dimostrare che un messaggio M è stato inviato da A.

22. (3pt) In Kerberos, a cosa serve il ticket rilasciato dal server AS? Come viene impedito che questo ticket venga alterato o manomesso dal client?

    R: È il ticket che si usa per autenticarsi presso il TGS, nel momento in cui bisogna ottenere un ticket per accedere ad un servizio. È inalterabile dal client perché è cifrato con una chiave precondivisa tra AS e TGS.

23. (3pt) Quali servizi principali vengono offerto dalla *Posta Elettronica Certificata* (PEC)? È possibile implementare questi servizi senza una terza parte fidata?

    R: La PEC implementa l'autenticazione del mittente, il timestamp certificato, e il non ripudio del destinatario. Non è possibile implementarli senza una terza parte, perché il timestamp e il certificato di consegna non deve dipendere da nessuna delle due parti.

24. (3pt) Quali dei seguenti metadati di una comunicazione HTTP sono resi confidenziali da SSL? (a) Indirizzi IP del mittente e destinatario; (b) Porte del mittente e destinatario; (c) quantità di dati trasferita; (d) Intestazioni della risposta HTTP del server.

    R: (a) no (b) no (c) sì, parzialmente (c'è frammentazione e compressione dei dati) (d) sì (sono payload).