Università degli Studi di Udine

DMIF — Dipartimento di Scienze Matematiche, Informatiche e Fisiche

Esame di **Reti di Calcolatori**

Soluzione

A.A. 2016-17 — V appello — 25 settembre 2017

1. Al tempo $t_0 = 0$ un'antenna inizia a inviare con velocità $c_0 = 2.5 \cdot 10^8$ m/s un segnale cosinusoidale $s(t) = A\cos(2\pi f_0 t)$ a frequenza $f_0 = 1.25$ MHz verso una seconda antenna, posta a una distanza $d = 1.25$ km dalla prima. Si calcoli dopo quanto tempo la seconda antenna riceve il secondo picco negativo del segnale trasmesso dalla prima.

   R: Il tempo t_1 che il segnale impiega per raggiungere la seconda antenna è uguale a

   $t_1 = d/c_0 = 1250/(2500 \cdot 10^5) = 0.5 \cdot 10^{-5} = 5 \cdot 10^{-6}$ s.

   A esso dobbiamo aggiungere il tempo t_2 necessario per rilevare il secondo picco negativo, il quale giunge dopo un periodo e mezzo da quando il segnale cosinusoidale arriva alla seconda antenna:

   $t_2 = 1.5\,T = 1.5/f = 1.5/(1.25 \cdot 10^6) = 1.5 \cdot 0.8 \cdot 10^{-6} = 1.2 \cdot 10^{-6}$ s.

   In definitiva: $t = t_1 + t_2 = 5 \cdot 10^{-6} + 1.2 \cdot 10^{-6} = 6.2 \cdot 10^{-6}$ s.

2. Si crea un canale giuntando cavi identici attraverso amplificatori non ideali, progettati per restaurare la potenza del segnale informativo al valore che aveva in ingresso al cavo. Ogni cavo dimezza la potenza del segnale in ingresso, e aggiunge un rumore di potenza $N_c = 1$ mW misurato all'uscita del cavo. Ogni amplificatore restaura come detto la potenza del segnale informativo, aggiungendo contemporaneamente un rumore di potenza $N_a = 1$ mW all'uscita dell'amplificatore. Dopo quante coppie cavo/amplificatore il rumore presente all'uscita del canale raggiunge 15 mW?

   R: Indicando con `----` il cavo e con `>` l'amplificatore si ha:

```
P           0            0            0           0            0  mW
   ---------- > ---------- > ---------- > ---------- > ---------- >
N          0+1 2+1    1.5+1 5+1      3+1 8+1    4.5+1 11+1     6+1 14+1=15 mW
```

   e quindi il rumore ammonta a $N = 15$ mW dopo 5 coppie cavo/amplificatore.

3. In corrispondenza del punto del canale calcolato all'esercizio precedente, la capacità di canale vale $C = 1$ kbit/s. Se la banda dello stesso canale in ogni punto vale $B = 1$ kHz, quanto vale la potenza P_0 del segnale informativo in ingresso nel canale in questione?

   R: Nel punto in questione la capacità $C = B\log_2(1 + P/N)$ osserva la relazione

   $1000 = 1000\log_2\big(1 + \dfrac{P}{15 \cdot 10^{-3}}\big)$ bit/s, da cui immediatamente $P = N = 15 \cdot 10^{-3}$ W. Poichè ogni amplificatore restaura la potenza che il segnale informativo aveva all'ingresso del rispettivo cavo, la potenza P_0 del segnale in ingresso nel canale è la medesima: $P_0 = P = 15$ mW.

4. Un codificatore NRZ in stato di quiete trasmette una sequenza indefinitamente lunga di simboli `0`, fino a quando a seguito di una richiesta proveniente dagli strati superiori invia la sequenza `1010011` a cui segue un nuovo stato di quiete indefinitamente lungo. Per errore, il decodificatore al ricevitore è del tipo NRZI. Che sequenza viene decodificata in ricezione?

   R: Il decodificatore NRZI è a sua volta nello stato di quiete fino a quando non rileva la prima commutazione, e ritorna in quiete dopo l'ultima commutazione ricevuta. Al di fuori dello stato di quiete dunque decodifica la sequenza `11110101`.

5. Una linea di trasmissione di pacchetti di lunghezza $L = 3$ bit ha una probabilità di errore per bit $p = 10^{-6}$. Si assume per semplicità l'indipendenza dell'errore su ciascun bit. In tal caso, si calcoli la probabilità che su 4 pacchetti consecutivi ve ne sia solamente uno scorretto.

   R: La probabilità che un pacchetto sia corretto è $p_c = (1-p)^3$. Di conseguenza, la probabilità che un pacchetto sia scorretto è $p_s = 1 - p_c = 1 - (1-p)^3$. Il pacchetto scorretto può essere posizionato ovunque nella quartina, e dunque la probabilità richiesta è uguale a

   $p_t = 4\, p_s\, p_c^3 = 4(1-10^{-6})^9\,\{1-(1-10^{-6})^3\}$.

6. In un protocollo *sliding window* ci sono 2 bit disponibili per etichettare ogni pacchetto. Qual è la dimensione massima che possono avere le finestre RWS e SWS nell'ipotesi in cui abbiano la stessa dimensione?

   R: La dimensione massima di entrambe le finestre dev'essere strettamente minore della metà del massimo numero assegnabile alle etichette, più 1, quindi:

   $\dim(\text{RWS}) = \dim(\text{SWS}) \leq (2^2)/2 = 2$, e quindi $\dim(\text{RWS}) = \dim(\text{SWS}) = 2$.

7. Quali azioni intraprendeva un nodo che voleva trasmettere un pacchetto in una rete *token ring*?

   R: Il nodo in questione attendeva in ascolto l'arrivo del *token*, lo sostituiva col pacchetto da trasmettere e infine, riascoltato il suo stesso pacchetto, lo rimpiazzava nuovamente con il *token* che quindi iniziava a ricircolare nella rete.

8. Qual è il rapporto di compressione r minimo che giustifica l'invio di dati compressi invece che non compressi, nell'ipotesi in cui la banda di trasmissione B_n della rete sia di 1 kbit e la banda equivalente B_c con cui la CPU comprime i dati sia di 4 kbit?

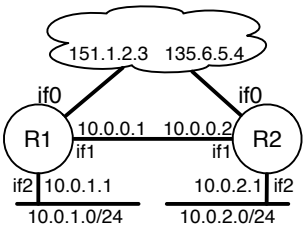
   R: Dalla relazione $B_c > B_n\, r/(r-1)$ si ha, al limite dell'uguaglianza,

   $\dfrac{B_c}{B_n} = \dfrac{r}{r-1} \Rightarrow \dfrac{r}{r-1} = 4 \Rightarrow r = \dfrac{4}{3}$.

9. Un'azienda ha due reparti; il reparto A ha una rete A1 di 25 postazioni; il reparto B ha due reti, B1 con 43 postazioni e B2 con 28 postazioni. Se l'azienda ha a disposizione la rete 158.110.0.0/16, come può assegnare gli indirizzi delle tre reti, minimizzando gli indirizzi inutilizzati?

   R: Per le due reti piccole bastano 5 bit ciascuna, per quella grande servono 6. Più 1 bit per distinguere tra grande e le 2 piccole. Quindi una possibile allocazione è la seguente: B1=158.110.0.0/26, B1=158.110.0.64/27, B2=158.110.0.96/27. Un'altra soluzione è A1=158.110.0.0/27, B1=158.110.0.64/26, B2=158.110.0.32/27.

10. a) Si dia la tabella di instradamento del router R2 (trascurando le problematiche relative alla traduzione NAT).
    b) Se i router R1 e R2 appartengono allo stesso Autonomous System, questo può essere di tipo stub?

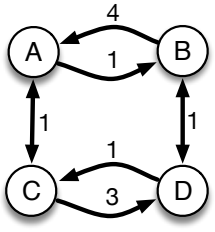


   R: a)

dest	next hop	if
10.0.0.0/24	–	if1
10.0.1.0/24	10.0.0.1	if1
10.0.2.0/24	–	if2
*	135.6.5.4	if0

   b) no

11. La rete a lato ha dei collegamenti asimmetrici, ossia il cui costo non è lo stesso nelle due direzioni. I router usano un algoritmo di routing basato sullo stato delle linee.
    a) Si mostri il contenuto (essenziale) dei pacchetti LSP generati da C.
    b) Si dia la tabella di routing di B.



   R: a) (C:(A,1),(D,3),n. di ordine) ; b)

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

12. Nel PIM Sparse Mode: a) si usa un instradamento ad albero condiviso o basato sulla sorgente? b) Se un host invia un pacchetto al gruppo multicast, come viene trattato dal suo router-gateway?

    R: a) ad albero condiviso; b) viene incapsulato in un altro pacchetto IP unicast e inviato al nodo rendez-vous (la radice dell'albero condiviso).

13. Un server sta inviando ad un client un flusso di 10 datagrammi UDP al secondo, ognuno con un payload di 1000 byte. Il client può rallentare la lettura dei dati per un tempo massimo di 10 secondi, fino ad un minimo di 5 datagrammi al secondo. Quanto deve essere grande il buffer di input per evitare di perdere pacchetti (tenendo conto dell'intestazione UDP e della pseudointestazione IP)?

    R: Alla peggio il buffer deve accomodare (10-5)*10 = 50 pacchetti. Se ognuno è di 1000 byte, più 8 byte di intestazione UDP, più 12 di pseudointestazione IP, in totale sono (1000+8+12) = 51000 byte. (Se uno conta 20 byte di intestazione IP, per un totale di 51400, va quasi bene).

14. a) Quando riceve un segmento con il flag FIN=1, in che stato si porta una socket TCP e cosa invia? b) In tale stato, dove si porta e cosa trasmette se riceve nuovamente un segmento con FIN=1?

    R: Da ESTABLISHED si porta in CLOSE-WAIT, e invia ACK. Rimane in CLOSE-WAIT, e rimanda ACK (può essere dovuto al fatto che l'ACK precedente è andato perduto).

15. Un'applicazione sta trasmettendo dati attraverso una socket TCP, il cui MSS è 1460 byte e con un RTT di 80ms. (a) Quanto è grande il payload di ogni segmento inviato, se l'applicazione scrive un blocco di 1000 byte ogni 100ms? (b) E se invece scrive 100 byte ogni 10ms?

    R: (a) Appena si scrive un buffer di 1000 byte, questo viene inviato immediatamente; il suo ACK arriva dopo 80ms, ma bisogna aspettare 20ms per avere i successivi dati da inviare. Quindi vengono inviati segmenti da 1000byte ogni 100ms. (b) In questa situazione, il buffer di output si riempie durante l'attesa dell'ACK per 800 byte. Così quando arriva l'ACK, può essere inviato immediatamente un nuovo segmento di 800 byte.

16. Un certo router gestisce i flussi con politica round robin. La suddivisione delle risorse è più equa se ci sono tre flussi di pacchetti di 100, 200 e 400 byte, oppure due flussi di 100 e 300 byte?

    R: Il modo più corretto per valutare l'equità è usare l'indice di Jain. Nel primo caso l'indice di Jain è $F_1 = (100 + 200 + 400)^2/(3 * (100^2 + 200^2 + 400^2)) = 7/9 = 0.77$. Nel secondo caso è $F_2 = (100 + 300)^2/(2 * (100^2 + 300^2)) = 4/5 = 0.8$. Quindi è più equa la seconda.

17. In una sorgente TCP, in cui CongestionWindow=32kB e MSS=1kB, è appena scaduto un timeout per la ricezione dell'ACK dell'ultimo segmento inviato. Se non si adotta il Fast Recovery, quanti round di "slow start" sono necessari per rientrare nella fase additiva?

    R: A causa del timeout, CongestionThreshold=16kB e si parte con CongestionWindow=MSS=1kB. La fase additiva si ha quando CongestionWindow=CongestionThreshold=16kB, per cui servono 4 round (1 + 2 + 4 + 8 = 16).

18. Si dia un protocollo di sicurezza per ognuno dei seguenti livelli OSI. (a) Data link (b) Rete (c) Trasporto (d) Applicazione.

    R: (2 pt) (a) WEP, WPA, WPA2 (b) IPsec (c) TLS, SSL (d) PGP, S/MIME, PEC, SSH, EMV, ...

19. Quale vulnerabilità ci sarebbe se si hanno due file cifrati con AES in modo CTR con la stessa chiave e partendo dallo stesso contatore iniziale? Come si potrebbe evitare?

    R: CTR è un modo a flusso, quindi si possono mettere in XOR i due file cifrati e ottenere lo XOR dei file in chiaro. Per sventare questo problema, bisogna usare contatori iniziali diversi, ad esempio casuali. Inoltre è importante che siano molto diversi, perché altrimenti si rischia che si sovrappongano porzioni diverse di file.

20. Si consideri uno scambio chiave Diffie-Hellman come a lato, dove y_A e y_B sono le due mezze chiavi e PR_B è la chiave privata per cifratura asimmetrica di B. Ci potrebbe essere l'attacco man-in-the-middle?

    1. $A \to B : y_A$
    2. $B \to A : E_{PR_B}(y_B)$

    R: Un attaccante potrebbe sostituirsi solo ad A per B, ma non a B per A. Questo gli permette di negoziare una chiave falsa con B, ma non con A. Quindi eventuali comunicazioni da B vengono intercettate, ma non quelle da A.

21. Nel protocollo a lato PU_B e PU_C sono le solite chiavi pubbliche per cifratura asimmetrica, mentre K è una chiave di sessione per cifratura simmetrica generata sul momento da A. Il messaggio M è confidenziale? È puntuale? Perché?

    1. $A \to C : E_{PU_C}(A, B, K)$
    2. $C \to B : E_{PU_B}(A, K)$
    3. $B \to A : E_K(M)$

    R: Un attaccante può facilmente sostituirsi a C ed inviare a B al passo 2 un messaggio contraffatto contenente una K' di sua invenzione, quindi intercettare il messaggio al passo 3 e leggere il contenuto. Però se arriva ad A cifrato correttamente, è puntuale: la cifratura con la K generata sul momento funge come da nonce.

22. Con riferimento al protocollo dell'esercizio precedente, si dica se (a) A è autenticato per C; (b) C è autenticato per B; (c) B è autenticato per A (se C è fidato).

    R: (a) no, A non risponde a nessuna challenge di C; (b) no, chiunque può inviare un messaggio a B cifrato con la sua chiave pubblica) (c) sì, perché risponde alla sfida di decifrare la K.

23. (a) Qual è un servizio di sicurezza offerto da S/MIME ma non da PEC? (b) E da PEC ma non da S/MIME? (c) E da entrambi?

    R: (a) Firma digitale (non ripudio del mittente) (b) Non ripudio del destinatario (c) integrità del messaggio (ma non segretezza, perché i server vedono i messaggi in chiaro)

24. Un client apre una sessione SSL con un server, usando il metodo RSA per lo scambio chiave. Durante tale sessione (e quindi dopo la fase di handshake), il certificato X.509 del server scade. Cosa succede alle connessioni già aperte? È possibile possibile aprire nuove connessioni all'interno di tale sessione?

    R: Non succede niente: la validità del certificato viene verificata solo durante l'handshake, quindi poi la sessione, e tutte le connessioni aperte e che si apriranno, rimangono valide. Naturalmente la sessione ha una scadenza, alla quale bisogna rinegoziare le chiavi, e a quel punto si ricontrolla la validità del certificato.