DMIF, Università degli Studi di Udine — III appello A.A. 2018-19 — 24 giugno 2019

# Esame di **Reti di Calcolatori**

Soluzione

1. Per ciascuna delle seguenti applicazioni di rete, si dica se è più sensibile all'ampiezza di banda, alla latenza (delay di trasmissione), o alla variazione della latenza (jitter):
   (a) accesso terminale remoto; (b) invio mail; (c) streaming audio; (d) videoconferenza.

   **R:** (a) latenza; (b) banda; (c) jitter; (d) latenza (e banda);

2. Si consideri una linea di trasmissione formata da 2 canali indipendenti, ognuno con un baud rate di 1 MBaud. Se la linea deve realizzare una trasmissione senza errori con un bit rate netto di 8 Mb/s con un forward error correction di Hamming [7,4,3] (3 bit di parità e 4 di dati) determinare il numero di bit codificato da un simbolo trasmesso.

   **R:** Il FEC implica che per 4 bit di dati devono essere trasmessi 7 bit grezzi: dal bitrate netto si ricava che il bitrate grezzo è 7/4 * 8 Mb/s = 14 Mb/s. Poiché ci sono 2 canali indipendenti, il Baud rate della linea è 2 MBaud e quindi il numero grezzo di bit trasmessi per simbolo è 7.

3. Per la linea dell'esercizio precedente, si determini il rapporto segnale/rumore SNR minimo necessario.

   **R:** Dal teorema di Shannon-Hartley sappiamo che $\log_2(M) = \frac{1}{2}\log_2(1+SNR)$, dove $M$ è il numero di simboli effettivi per i dati. Dato che su 7 bit trasmessi con un simbolo, 4 sono di dati, è $M = 2^4 = 16$. Risolvendo, si ha che $SNR >= M^2 - 1 = 255$

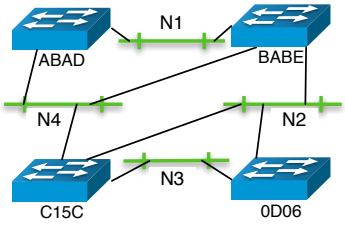
4. AAL5 è una tecnica per inviare pacchetti di livello 3 su ATM (che è di livello 2). Un pacchetto viene diviso in tanti frame di lunghezza fissa (chiamati *celle*), ognuno con 48 byte di payload e 5 di intestazione. L'ultima cella contiene, oltre alla parte finale dei dati, anche 8 byte di informazioni per la ricostruzione del pacchetto. Si calcoli l'overhead (in byte) introdotto da AAL5 per inviare un pacchetto di 1500 byte.

   **R:** I dati totali da trasmettere sono 1500+8 = 1508 byte, per cui sono necessarie 1508/48=31,41 $\mapsto$ 32 celle. Il traffico totale sarà di 32*53=1696 byte, e quindi l'overhead è di 1696-1500=196 byte.

5. Si vuole trasmettere la sequenza di bit 1011011101 aggiungendo un codice CRC usando il polinomio generatore $x^4 + x^2 + 1$. Come è fatto il messaggio complessivo?
   **R:** Il messaggio complessivo è 1011011101*1111*. Qui a lato il calcolo del CRC.

```
1011011101 0000  | 10101
10101
=====
00011111
   10101
   =====
   010100
    10101
    =====
    000011 000
        10 101
        ======
        01 1010
         1 0101
         ======
         0 1111
```

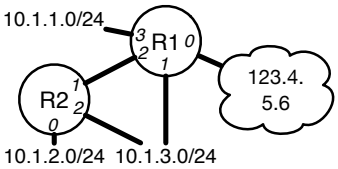
6. I bridge della rete a lato, i cui id sono scritti in esadecimale, si sono autoconfigurati con l'algoritmo di spanning tree. (a) Qual è il root bridge? (b) Ci sono bridge inattivi (e se sì, quali)?
   **R:** (a) Il root bridge è 0D06. (b) I bridge inattivi sono ABAD e C15C.



7. Per ognuna delle seguenti, si dica se è una sottorete di 192.128.10.0/23:
(a) 192.128.11.0/24; (b) 192.128.9.0/24; (c) 192.128.10.0/22; (d) 192.128.10.128/25.

**R:** (a) sì; (b) no; (c) no; (d) sì.

8. Le interfacce e le tabelle di instradamento dei router in figura sono come seguono: R1:if1=10.1.3.1, if2=192.168.2.1, if3=10.1.1.1;
R2:if0=10.1.2.1, if1=192.168.2.2, if2=10.1.3.2.




R1:

| dest | if | next hop |
|---|---|---|
| 10.1.1.0/24 | 3 | - |
| 10.1.2.0/23 | 2 | 192.168.2.2 |
| */* | 0 | 123.4.5.6 |

R2:

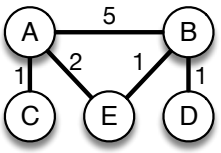
| dest | if | next hop |
|---|---|---|
| 10.1.2.0/24 | 0 | - |
| */* | 2 | 10.1.3.1 |

(a) Cosa succede ad un pacchetto inviato da 10.1.3.5 a 10.1.2.5?
(b) E al pacchetto di risposta, da 10.1.2.5 a 10.1.3.5?

**R:** (a) L'host 10.1.3.5 può utilizzare R2 come gateway, il quale inoltrerà il pacchetto a destinazione attraverso l'interfaccia 0. Oppure 10.1.3.5 invia il pacchetto a R1, il quale applica la seconda regola e lo inoltra a R2, che lo consegna. In ogni caso, il pacchetto arriva a destinazione.

(b) R2 inoltra il pacchetto al suo default gateway, ossia 10.1.3.1 (potrebbe fare una consegna diretta, ma la tabella non glielo permette). R1 inoltra il pacchetto a R2 in base alla seconda regola, e quindi il pacchetto inizia a ciclare tra R1 e R2, finché il TTL non scende a 0 e viene scartato.

9. I router della rete a lato utilizzano RIP e hanno raggiunto la configurazione stabile. (a) Si dia la tabella di instradamento di B. (b) Ad un certo punto, il collegamento B-D si interrompe, e subito dopo B riceve il vettore delle distanze di A. Come diventa la tabella di instradamento di B?




**R:** (a)

| dest | d | n.h. |
|---|---|---|
| A | 3 | E |
| B | 0 | - |
| C | 4 | E |
| D | 1 | D |
| E | 1 | E |

(b)

| dest | d | n.h. |
|---|---|---|
| A | 3 | E |
| B | 0 | - |
| C | 4 | E |
| D | 9 | A |
| E | 1 | E |

10. I provider di connettività IPv6 assegnano ad ogni utente (anche singoli privati) una rete pubblica /64 (se non addirittura una /48). Supponendo di aver ricevuto un prefisso /64 per una certa rete Ethernet/WiFi, come può ogni host della rete assegnare alla propria interfaccia un indirizzo IPv6 univoco globalmente, senza server DHCP e senza configurazione manuale?

**R:** Dato che un indirizzo IPv6 è di 128 bit, se il prefisso è di 64 bit rimangono 64 bit liberi per la parte di host. Questi 64 bit possono essere costruiti in modo univoco appendendo i 48 bit del MAC address (l'indirizzo Ethernet) e 16 bit a 0 per riempimento. (Questa è la tecnica di autoconfigurazione di IPv6.)

11. Un server sta trasmettendo un flusso di datagrammi UDP ad un client, che li consuma ad una velocità di dieci datagrammi al secondo. Ogni datagramma ha un payload di 1KB. A quale velocità (in KB/s) deve inviare dati il server per saturare in 5 secondi il buffer di input, se questo è da 16KB?

**R:** Siano rispettivamente $I, O$ i datarate di input e output (in KB/s) del buffer di lunghezza $L$ (in KB). Per saturare il buffer in un tempo $t$, deve essere $(I - O) * t = L$, da cui $I = O + L/t$. Sostituendo, abbiamo $I = 10 + 16/5 = 13,2$ KB/s.

12. Durante una connessione TCP tra $A$ e $B$, $A$ ha appena inviato un frame con FIN=1.
(a) Se $A$ riceve un segmento con ACK=1 e FIN=0, in che stato si è portato $B$?
(b) $A$ potrebbe ricevere un segmento con ACK=1 e FIN=1? In che stato si porterebbe?

**R:** (a) Vuol dire che $B$ ha ricevuto il FIN ma non ha ancora deciso di chiudere la comunicazione, quindi si è portato in CLOSE_WAIT (deve aspettare il close da parte della sua applicazione).

(b) Vuol dire che $B$ ha ricevuto il FIN e praticamente nello stesso momento la sua applicazione ha deciso di chiudere; quindi nel segmento di risposta $B$ manda sia l'ACK del FIN che ha ricevuto, sia il FIN della sua chiusura. In tale situazione $A$ si porta in TIME_WAIT.

13. Durante una connessione TCP, una delle due parti ha ricevuto `AdvertisedWindow`=0. In quali modi può sapere se la finestra si riapre?

    **R:** In tre modi: 1. se la parte ha inviato dei dati di cui non ha ricevuto l'ACK, aspetta tali ACK perché potrebbero avere `AdvertisedWindow` $> 0$; 2. Altrimenti, se ha dei dati da inviare, la parte invia periodicamente un piccolo segmento (di 1 byte) per stimolare la controparte a comunicare la sua `AdvertisedWindow`. 3. Infine la controparte potrebbe mandare spontaneamente un segmento di dati, e nella cui intestazione c'è la nuova `AdvertisedWindow` (in piggyback).

14. Un router sta servendo tre flussi A, B, C secondo la politica di accodamento equo (Fair Queueing). I pacchetti in coda, con il tempo necessario per trasmetterli (in $ms$), sono i seguenti: A1=5, A2=7, A3=2, B1=4, B2=11, C1=9, C2=6. (a) In che ordine vengono trasmessi i pacchetti? (b) A che istante termina la trasmissione del pacchetto A3?

    **R:** Secondo FQ, l'ordine di conclusione di invio dei pacchetti è: A1=5, A2=12, A3=14; B1=4, B2=15; C1=9; C2=15. Quindi (a) L'ordine di trasmissione è B1, A1, C1, A2, A3, B2, C2. (A parità di tempo, si trasmette B2 prima di C2 per round robin). (b) Sommando i tempi, A3 termina a 27ms.

15. Per ognuna delle seguenti azioni, si dica se è un attacco attivo o passivo, e a quale aspetto di sicurezza (confidenzialità, integrità, disponibilità): (a) rubare dal frigo le birre del compagno di appartamento; (b) sostituire le Leffe Blonde con delle Budweiser; (c) allungare il rum con l'acqua per nascondere di aver bevuto mezza bottiglia; (d) osservare con attenzione la camminata del compagno di appartamento.

    **R:** (a) attivo, disponibilità; (b) attivo, integrità; (c) attivo, integrità (e disponibilità); (d) passivo, confidenzialità.

16. Nei vari sistemi di sicurezza per 802.11 (ossia WEP, WPA, WPA2): (a) viene utilizzata cifratura simmetrica o asimmetrica? (b) Quali servizi di sicurezza si vuole implementare?

    **R:** (a) Simmetrica; (b) Confidenzialità (relativa), integrità, controllo di accesso al mezzo.

17. Il protocollo a lato è uno scambio chiavi di tipo Diffie-Hellman, in cui $Y_A$ e $Y_B$ sono le mezze chiavi pubbliche di $A$ e $B$ rispettivamente, $N_A, N_B$ sono due nonce. Avendo a disposizione una funzione di hash $H$, e un segreto precondiviso $K$, completare il protocollo (ossia, riempire al posto dei "??") in modo da impedire attacchi MITM e garantire la puntualità della chiave derivata.

    1. $A \to B : Y_A, N_A$
    2. $B \to A : Y_B, N_B, ??$
    3. $A \to B : ??$

    **R:** Una soluzione è la seguente (ma ce ne sono altre):

    1. $A \to B : Y_A, N_A$
    2. $B \to A : Y_B, N_B, H(Y_B, N_A, K)$
    3. $A \to B : H(Y_A, N_B, K)$

18. Nel protocollo a lato la terza parte fidata $C$ conosce le chiavi pubbliche di $A$ e $B$, mentre $A$ non conosce la chiave pubblica di $B$ e $B$ non conosce la chiave pubblica di $A$. $K$ è una chiave simmetrica generata casualmente da $B$. (a) $A$ è autenticato per $B$? (b) $B$ è autenticato per $A$? (c) $M$ è puntuale (ossia non soggetto ad attacchi reply)? Motivare le risposte.

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

    **R:** (a) Sì, perché solo chi è in possesso di $PR_A$ può entrare in possesso di $K$ (oltre a $C$ e $B$ stessi). Quindi l'ultimo messaggio deve venire da $A$. (b) No. L'unica azione che fa $B$ è al passo 2, e può essere eseguita da chiunque. (c) Sì. La cifratura con una chiave fresca vale come l'uso di una nonce.

19. Nel protocollo a lato $S$ è un server fidato, la cui chiave pubblica è nota ad $A, B$, e $T$ è un timestamp generato da $S$. Si dica se il messaggio $M$ è (a) integro; (b) non ripudiabile; (c) puntuale.

    1. $A \to S : H(M)$
    2. $S \to A : E_{PR_S}(T, H(M))$
    3. $A \to B : M, E_{PR_S}(T, H(M))$

    **R:** (a) sì, grazie alla firma messa da $S$ (b) no, nessuno sa l'identità del mittente (c) sì, grazie al timestamp.

20. Due applicazioni remote comunicano con un canale TCP su IPsec con ESP.
    (a) Cosa è necessario stabilire tra le due parti prima che vengano inviati i primi dati?
    (b) È necessario ripetere tale operazione per ogni connessione TCP?

    **R:** (a) due Security Association, una per direzione. A mano, o automaticamente con ISAKMP. (b) No, non è necessario finché la SA rimane valida.