DMIF, Università degli Studi di Udine I appello A.A. 2020-21 — 28 gennaio 2021

Esame di **Reti di Calcolatori**

Soluzione

1. Per ognuna delle seguenti funzionalità si dica in quale strato dello stack TCP/IP viene implementata: (a) Conversione formato dei dati; (b) Codifica/decodifica bit su mezzo fisico; (c) demultiplexing alle applicazioni; (d) Correzione errori di trasmissione.

   R: (a) Applicazione; (b) Fisico/datalink; (c) Trasporto; (d) Datalink.

2. La lingua italiana conta 45 simboli sonori, chiamati *fonemi*, e in un normale eloquio vengano pronunciati circa 15 fonemi al secondo. (a) A quanto equivale il bitrate di tale trasmissione? (b) Se il canale usato per la trasmissione ha un SNR di 10dB, quale ampiezza di banda è necessaria?

   R: (a) Ogni simbolo porta $\log_2(45) = 5.49$ bit, quindi il bitrate è $5.49 * 15 = 82.3$ bps. (b) Ricordiamo che per SH è $C = B\log_2(1 + S/R)$. Nel nostro caso è $S/R = 10^{10/10} = 10$ e $C = 82.3$ bps, quindi $82.3 = B\log_2(11)$ da cui $B = 82.3/3.459 = 23.8Hz$

3. In Bluetooth un frame può contenere al massimo 483 bit se occupa uno slot e 1124 bit su tre slot, a cui va aggiunta l'intestazione di 126 bit. Si vuole trasmettere 100 byte di dati. Sapendo che la probabilità di errore per bit è $p = 10^{-4}$, si calcoli la probabilità che arrivino integri usando (a) più trasmissioni da 1 slot; (b) con una sola da tre slot.

   R: 100 byte = 800 bit. (a) Usando uno slot alla volta servono 2 comunicazioni, quindi in totale i bit da trasmettere sono $800 + 126 * 2 = 1052$ bit. La probabilità che arrivino tutti giusti è $(1 - 10^{-4})^{1052} = 0.9001 = 90\%$. (b) Con le comunicazioni multislot basta una comunicazione, quindi in totale i bit sono $800 + 126 = 926$ bit. La probabilità che arrivino tutti giusti è $(1 - 10^{-4})^{926} = 0.9115 = 91,15\%$.

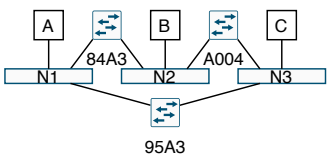
4. Nello standard Gigabit Ethernet, il bit time è di 1ns e l'interpacket gap è di 96 ns. (a) Quanto tempo è necessario per trasmettere un frame con 1500 byte di payload? (b) Di conseguenza, qual è il massimo bitrate utile teorico, al netto degli overhead introdotti dalla tramatura?

   R: (a) Il preambolo è di 8 byte, l'intestazione è di 14 byte, il CRC di 4 byte, e l'IPG è equivalente a 12 byte. Quindi complessivamente un frame occupa $12 + 8 + 14 + 1500 + 4 = 1538byte = 12304bit = 12.3\mu s$ (b) Per trasmettere 1500 byte servono 12.3 μs, quindi il bitrate è 1500*8/12.3 = 975,6 Mbps.

5. In una certa cella 802.11, un nodo A vorrebbe trasmettere un frame a B. Si mette in ascolto, e riceve un frame CTS da un altro host con MAC C indirizzato a D. (a) Cosa deduce A riguardo C e D? (b) Può A trasmettere il frame a B immediatamente?

   R: (a) A capisce di essere un nodo nascosto per una comunicazione da D ad C (di cui ha perso il RTS). (b) No, potrebbe disturbare la trasmissione. Deve aspettare il prossimo turno.

6. La rete a lato è composta da switch ad autoapprendimento. All'inizio, gli switch 84A3 e A004 sono appena accesi (e quindi resettati), mentre 95A3 è ancora spento. (a) L'host A invia un frame indirizzato a B. Da quali host viene ricevuto? (b) Viene acceso lo switch 95A3. Dopo che si sono stabilizzati, quali switch rimangono attivi?



   R: (a) Anche da C, perché A004 fa flooding. (b) 84A3 e 95A3. A004 si disattiva.

7. All'interno della rete 192.168.0.0/16 si vogliono definire quattro sottoreti contigue, ognuna con almeno 800 indirizzi utili. (a) Si diano gli indirizzi di rete di tali quattro sottoreti. (b) Usando 800 indirizzi per sottorete, qual è l'utilizzo complessivo di tali sottoreti, in percentuale?

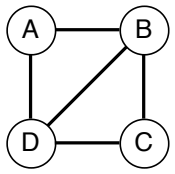
   R: (a) 192.168.0.0/22, 192.168.4.0/22, 192.168.8.0/22, 192.168.12.0/22. (b) È sufficiente calcolarla per una sola sottorete: 800/1024 = 78%.

8. Due reti IPv6 comunicano attraverso un tunnel "6-to-4" (cioè IPv6 in IPv4) realizzato dai due router di frontiera. Se la dimensione media dei payload di IPv6 è di 500 byte, quant'è l'overhead (in percentuale) causato dal tunnel, rispetto ad avere una rete puramente IPv6?

   R: Se non ci fosse il tunnel, i pacchetti sarebbero lunghi 500+40=540 byte. Il tunnel aggiunge un'intestazione IPv4 di 20 byte. Quindi l'overhead è 20/540=3,7%.

9. I router della rete a lato utilizzano un algoritmo di routing basato sul vettore delle distanze. Non si conosce il peso di ogni arco, ma la tabella di A è quella riportata a lato. (a) Quant'è il peso del collegamento B–D? (b) E di quello B–C?
   R: (a) A–B vale 1, e se da A a D vale 3, B–D deve essere 2 o più. (b) Almeno 3, dato che per andare a C il n.h. è D, con distanza 4. Se B-C fosse 2, il n.h. di C sarebbe B con distanza 3.

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



10. Nel multicast implementato nello stack TCP/IP, (a) Quali protocolli di trasporto possono essere usati per inviare dati ad un indirizzo multicast? (b) In tale situazione, a quale livello dello stack vengono eventualmente gestite la perdita o l'arrivo fuori ordine dei pacchetti?

    R: (a) solo UDP o altri protocolli connectionless, perché non si possono fare connessioni multicast. (b) A livello applicazione. Ossia, se la deve vedere il programmatore.

11. L'amministratore di un certo sistema riceve il seguente messaggio dal kernel:
    `UDP: bad checksum. From 220.110.189.98:19 to 94.31.136.187:51243 ulen 1234`
    (a) Quale problema si è verificato? (b) Come viene gestito quel datagramma?

    R: (a) A quanto pare è arrivato un pacchetto UDP che non ha superato il controllo del checksum. Forse il payload è errato o c'è un problema nello pseudoheader. (b) Viene scartato da UDP (potrebbe anche essere il risultato di un attacco).

12. Una socket TCP si trova in stato ESTABLISHED. L'ultimo segmento che ha inviato ha `SeqNum`=12000, `Length`=1000. Riceve un segmento con `Acknowledgment`=12000, FIN=1. (a) In che stato si porta? (b) Il segmento con SeqNum=12000 è andato perduto? (c) La socket può inviare ancora dati nuovi oltre a quelli già inviati?

    R: (a) CLOSE_WAIT (chiusura passiva). (b) No, deve ancora arrivare il suo ACK. (c) Sì, senza problemi, se la sua applicazione continua a scrivere sulla socket.

13. Un'applicazione scrive 500 byte su una socket TCP ogni 2ms. Il RTT è 5ms, e MSS=1460. (a) Quanti byte contiene ogni segmento inviato dall'host? (b) E se fosse MSS=1000?

    R: (a) In un RTT vengono prodotti (500/2)*5=1250 byte. Siccome è inferiore a MSS, viene invata tale quantità di dati ogni 5ms. (b) In questo caso il buffer si riempie di 1000 byte ogni 4ms, quindi prima che arrivi l'ACK del precedente, quindi si invia un MSS bello pieno.

14. Un host TCP è in fase additiva, con `cwnd`=7000, e MSS=1400. Invia i seguenti segmenti: `SeqNum`=10000, `Length`=500; `SeqNum`=10500, `Length`=1400; `SeqNum`=11900, `Length`=300; `SeqNum`=12200, `Length`=500. Poi riceve due segmenti, uno con `Acknowledgment`=11900 e uno con `Acknowledgment`=12200.
    (a) Quanto vale l'incremento complessivo della `cwnd`, a questo punto? (b) Quanti byte può ancora inviare (supponendo che la advertised window sia sufficientemente larga)?

    R: (a) incremento=(12200-10000)*MSS/cwnd = 2200*1400/7000 = 440 byte. Può essere calcolato anche in due passi: (11900-10000)*MSS/cwnd + (12200-11900)*MSS/cwnd. (b) Dobbiamo calcolare la EffectiveWindow = MaxWindow – (LastByteSent – LastByteAcked). In questo caso, MaxWindow=7000, LastByteSent=12699, LastByteAcked=12199. Quindi EffectiveWindow = 7000 – (12699 – 12199) = 7000 – 500 = 6500.

15. Un certo host A si collega al router B usando una tecnologia di rete custom (simile a 802.11) che vuole realizzare autenticità ed integrità a livello di collegamento. (a) Quali informazioni dell'intestazione di livello 2 devono essere coperte da tale meccanismo per garantire l'autenticità? (b) Questa soluzione permette l'esecuzione delle funzioni di instradamento nel router? (c) Viene garantita l'integrità dei dati anche nel caso in cui il router (o un altro router) sono non fidati?

R: (a) Tutto il frame, compreso il MAC della scheda mittente, con un HMAC o una firma digitale. Non si deve cifrare il frame. (b) Sì, è tutto in chiaro (e poi non c'è più alcuna protezione) (c) no, dopo il primo router è tutto insicuro.

16. Un host A invia a B una serie di messaggi $M_1, M_2, \ldots$ cifrandoli in questo modo: $A \to B : i, E_K(i, M_i)$, dove K è una chiave simmetrica precondivisa e l'algoritmo di cifratura è robusto (ad esempio AES-CBC). (a) I messaggi sono autenticati per B? (b) È possibile effettuare un attacco replay? (c) Se un messaggio si perde, è possibile decifrare i successivi?

    R: (a) sì, perché solo A conosce K; (b) Solo se i va in overflow, e ricomincia. (c) Senza problemi, ogni messaggio è autocontenuto.

17. Si consideri il protocollo a lato, dove: K è una chiave random generata da A sul momento, N è una nonce, e PU_B è la chiave pubblica di B. (a) Il messaggio M è segreto? (b) M è autentico, ossia B è sicuro della sua provenienza? (c) A è autenticato per B?

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

    R: (a) sì, un attaccante non riesce a rubare la chiave K. (b) No: chiunque può spacciarsi per A ed eseguire tutto il protocollo, e quindi dare un qualsiasi M a B. (c) No, non c'è niente che garantisca l'identità di A.

18. Durante la connessione ad un certo sito web HTTPS, il browser mostra il seguente errore:

    ```
    NET::ERR_CERT_REVOKED
    Subject: www....
    Issuer: QuoVadis Global SSL ICA G3
    Expires on: 5 feb 2021
    Current date: 28 gen 2021
    ```

    (a) Quale tipo di scambio chiave è stato tentato da TLS? (b) Come fa il browser ad accorgersi dell'errore? (c) Cosa deve fare l'amministratore del sistema per rimediare?

    R: (a) RSA, con certificato del server. (b) Dato che non è scaduto, deve aver controllato in una CRL o usando OSCP (c) Farsi rilasciare un nuovo certificato e installarlo sul server al posto di quello revocato.