DMIF, Università degli Studi di Udine — II appello A.A. 2019-20 — 18 febbraio 2020

Esame di **Reti di Calcolatori**

Soluzione

1. Per ognuna delle seguenti sequenze di intestazioni (lette dalla più esterna alla più interna), si dica se è possibile oppure no. (a) Ethernet-TCP-HTTP; (b) PPP-IP-UDP-DNS; (c) Ethernet-IP-IP-TCP.

   R: (a) no (manca IP); (b) sì (ad esempio è quella su un modem); (c) sì (è incapsulamento IPinIP).

2. V.92 è uno standard per i modem analogici introdotto nel 1999. (a) Supponendo che un modem V.92 operi nella banda tra 0 e 4 kHz, con un bit rate grezzo di 56 kbps, determinare il numero di bit che devono essere codificati in un simbolo. (b) Se in tale situazione il rapporto SNR del canale fisico è di 20 dB, quale è il bit rate netto della trasmissione dati?

   R: (a) Il baud rate massimo è 2 * BW = 8 kBaud e quindi il numero di bit per baud deve essere 56 kb/s / 8kBaud = 7 bit. (b) 20dB corrisponde ad un rapporto SNR in potenza pari a 100. Dal teorema SH sia ha $C = BW * \log_2(1 + SNR) = 4kHz \log_2(1 + 100) = 26.6$ kb/s.

3. Una certa rete locale utilizza il metodo di framing BISYNC. Se gli ultimi due byte del payload sono DLE e ETX, qual è la sequenza di byte da trasmettere immediatamente prima del CRC?

   R: DLE e ETX sono due caratteri speciali, che devono essere "escapati" con DLE stesso. Quindi "DLE ETX" diventa "DLE DLE DLE ETX", a cui si aggiunge un altro ETX per definire la fine del payload.

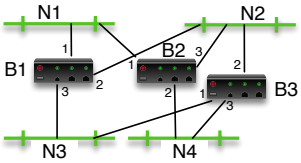
4. Un certo collegamento con un RTT di 10 ms viene utilizzato mediante il protocollo stop-and-wait. Si osserva una banda netta di 2 Mbps. Quanto è grande il payload di ogni frame, in byte?

   R: Durante un RTT viene invato 1 solo frame, e ricevuto il suo ack. Quindi la banda netta è $l * 8/(10 * 10^{-3}) = 2 * 10^6$, da cui $l = 20/8 * 10^3 = 2500$ byte.

5. In una certa area coesistono una rete 802.11 che usa un certo canale della banda ISM 2.4GHz, e una rete Bluetooth. (a) Esiste la possibilità di interferenza tra le due reti? Perché? (b) In caso di tentativo simultaneo di trasmissione, quale delle due reti ottiene la priorità?

   R: (a) Sì, perché Bluetooth, usando FHSS, prima o poi passa anche per il canale usato dalla 802.11. Se proprio in quel momento anche la 802.11 deve trasmettere, si crea il conflitto. (b) se si trovano sullo stesso canale, vince Bluetooth, perché è una TDM senza carrier sense (in origine).

6. Nella rete a lato, gli switch sono ad autoapprendimento e hanno già le tabelle completamente popolate. Ad un certo punto lo switch B2 viene resettato, e immediatamente dopo un host A su N1 trasmette un frame indirizzato ad un host B su N2. Quanti frame arrivano a B?



   R: Ne arrivano 2, perché 1 viene inoltrato da B1 (che è il root bridge), e uno da B2 che li manda in flooding. La copia che B2 manda su N4 non viene inoltrata da B3 su N2, perché B3 sa che il designed bridge di N2 è N1.

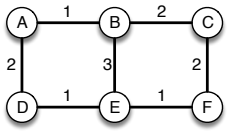
7. Un router riceve un pacchetto IP con un payload di 960 byte e `MoreFragments`=1. Deve inoltrarlo su una interfaccia che ha una MTU di 400 byte. (a) Quanto è grande il payload del primo frammento? (b) Quanto vale il flag `MoreFragments` dell'ultimo di tali frammenti?

   R: (a) Chiaramente il pacchetto da 960 (+20) byte deve essere frammentato in tanti frammenti che riescano ad entrare in 400 byte. Il primi di questi frammenti porta un payload di 376 byte, perché 376+20=396 < 400, e 376 è divisibile per 8. (b) L'ultimo di questi frammenti ha `MoreFragments`=1 perché il pacchetto da cui siamo partiti aveva già `MoreFragments`=1 (vuol dire che era già il risultato di una frammentazione precedente).

8. Supponiamo che a due host A e B sia stato assegnato (probabilmente per errore) lo stesso indirizzo IP sulla stessa LAN, in cui viene usato ARP. B inizia a funzionare dopo A. (a) Cosa accade alle connessioni di A già esistenti? (b) Cosa succederà ai pacchetti destinati a B inviati dagli host locali che avevano inviato da poco pacchetti ad A?

   R: (a) Continuano come se niente fosse, perché il router o gli host che mandavano i pacchetti a A avevano già popolato le rispettive tabelle ARP con il MAC address di A, per quell'indirizzo IP. (b) Come detto nel punto precedente, gli host che hanno già una riga relativa ad A nella ARP table continuano a consegnare correttamente i pacchetti ad A. Però consegnano ad A anche i pacchetti destinati a B, perché quando vanno a risolvere l'indirizzo IP si ritrovano il MAC address di A in cache.

9. I router della figura a lato adottano un protocollo basato sul vettore delle distanza, con *split horizon*. (a) Si mostri la tabella di instradamento di C.
   (b) Si mostri il vettore inviato da C a F.



R: (a)

dest	d	n.h.
A	3	B
B	2	B
C	0	-
D	4	F
E	3	F
F	2	F

(b)

dest	d
A	3
B	2
C	0

10. Un host invia un pacchetto IP ad un indirizzo multicast, senza però aver inviato un pacchetto IGMP in precedenza. (a) Quali host possono ricevere tale pacchetto? (b) Cosa ne fa il router-gateway dell'host?

    R: (a) Solo quelli che hanno eseguito l'iscrizione al gruppo (mediante richiesta IGMP), e sono sulla stessa LAN (b) Lo butta via, perché senza vedere un IGMP in precedenza (da quell'host o da un altro sulla stessa LAN) non riconosce l'esistenza di un gruppo multicast sulla LAN.

11. Un client sta ricevendo un flusso audio con bitrate 128 kbps, via UDP. Ogni datagramma porta 1200 byte di payload. (a) Se si perde un datagramma, quanto dura la lacuna (il "buco") che si viene a creare nell'audio? (b) Quanto è il traffico effettivamente generato in ricezione, in kbps, comprendendo anche l'overhead delle intestazioni IP e UDP?

    R: (a) 128kbps=16KB/s, quindi in un secondo ci sono 16000/1200 = 13.33 datagrammi. Ognuno copre un tempo pari a 1/13.33 = 75 ms. (b) 13.33 *(1200+8+20)=16,373 KB/s = 131 kbps.

12. In TCP: (a) quanto è il valore massimo del campo SeqNum (ovvero, di quanti bit è)? (b) è possibile che tale campo vada in overflow, ossia riparta da 0, anche dopo una trasmissione di poche decine di byte?

    R: (a) $2^{32} - 1$ (sono 32 bit) (b) sì, perché il valore iniziale è scelto a caso durante l'handshake.

13. Un'applicazione sta producendo un flusso di dati su una socket TCP, alla velocità di 200 byte ogni 10 ms. La connessione TCP ha un MSS di 1460 byte e un RTT di 80ms. Si supponga che CongestionWindow e AdvertisedWindow siano sufficientemente grandi. (a) Quanto è grande il payload di ogni segmento inviato dall'host? (b) In media, quanti pacchetti vengono inviati al secondo?

    R: (a) Il datarate è 200/0,01= 20 KB/s. Quindi in un RTT nel buffer si accumulano $20 * 80 = 1600$ byte, che è superiore al MSS. Quindi, per l'algoritmo di Nagle, appena si arriva a 1460 byte di payload viene inviato un segmento "pieno". (b) Il numero di pacchetti inviati al secondo è $20000/1460 = 13,7$.

14. Un utente si accorge che un certo router, che implementa la RED con MinThreshold=20KB e MaxThreshold=100KB, perde circa il 10% dei pacchetti. Quanto è piena la coda sul router, in kB?

    R: Per fare una probabilità di 0.1, bisogna che sia $0.1 = \frac{x-20}{100-20}$, quindi $8 = x - 20$ da cui $x = 28$ KB.

15. Per ognuna delle seguenti osservazioni si dica se è vera o falsa. (a) L'installazione di SSL è consentita solo all'amministratore del sistema; (b) IPsec è utile per mettere in sicurezza anche applicazioni di cui non si ha il codice sorgente; (c) Per utilizzare PGP o S/MIME è necessario che sia il mittente sia il destinatario possiedano una chiave privata (e corrispondente chiave pubblica).

    R: (a) no, è una libreria in user space; (b) sì: non serve modificare niente nel codice (a differenza di SSL); (c) no, basta uno dei due (ma i servizi saranno inferiori).

16. Un sensore A trasmette dei dati via UDP ad un server B al ritmo di un pacchetto al secondo. Ogni pacchetto è cifrato con AES secondo il seguente schema: $A \to B : i, E_K(i) \oplus M$, ove i è un contatore a 16 bit e K la chiave precondivisa. (a) Se un pacchetto viene perduto, il server può comunque ricevere e decifrare correttamente i pacchetti successivi? (b) È possibile effettuare un attacco replay? Perché?

    R: (a) Sì, perché ogni pacchetto viene cifrato separatamente (è la modalità CTR). (b) Dopo 2^{16} pacchetti il contatore torna a 0, e quindi un attaccante può sostituire un nuovo messaggio con quello vecchio. 2^{16} secondi sono 18 ore e 12 minuti.

17. Nel protocollo a lato, A e B possiedono ognuno una chiave simmetrica K_A, K_B precondivise con KDC; K_S è una chiave di sessione generata fresca, e H è una funzione di hash fissata. (a) K_S è confidenziale? (b) è puntuale? (c) A è autenticato per B?

    1. $A \to KDC : Id_A, Id_B, H(Id_A, Id_B, K_A)$
    2. $KDC \to A : E_{K_A}(K_S, Id_B, E_{K_B}(Id_A, Id_B, K_S))$
    3. $A \to B : E_{K_B}(Id_A, Id_B, K_S)$

    R: (a) Sì, è cifrata con le chiavi condivise K_A, K_B. (b) No, si può fare un attacco replay al passo 2. Mancano le nonce. (c) No, perché a causa di un attacco replay un attaccante può simulare una vecchia sessione.

18. Nel protocollo a lato, M è un messaggio, A possiede una chiave privata PR_A, B conosce la corrispondente chiave pubblica, N è una nonce. (a) Il messaggio M è ripudiabile da A? (a) La ricezione di M è ripudiabile da B? (c) è puntuale (ossia non è vulnerabile ad un attacco replay)?

    1. $A \to B : Id_A, M$
    2. $B \to A : N$
    3. $A \to B : E_{PR_A}(H(M, N))$

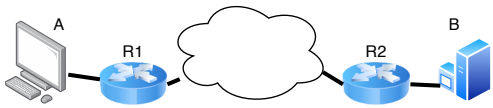
    R: (a) No, non è ripudiabile perché è firmato con la chiave privata di A (b) Sì, non c'è niente che garantisca che B abbia ricevuto proprio M (c) Sì, è puntuale perché c'è la nonce N.

19. Nel protocollo a lato y_A e y_B sono le mezze chiavi pubbliche Diffie-Hellman e K è la corrispondente chiave derivata. K_A è una chiave precondivisa tra A e la terza parte fidata C, e analogamente per K_B. (a) Il protocollo è soggetto all'attacco man-in-the-middle? (b) C potrebbe ottenere K? (c) A è autenticato per B? Perché?

    1. $A \to B : y_A$
    2. $B \to A : y_B$
    3. $A \to C : Id_A, E_{K_A}(Id_B, H(K))$
    4. $C \to B : E_{K_B}(Id_A, H(K))$

    R: (a) No, perché un attaccante prova a sostituire il messaggio con una propria mezza chiave, C se ne accorgerebbe. (b) No, non ha nessuna informazione in più degli attaccanti (tranne la hash della chiave, che non è utile). (c) Sì, al passo 4, perché solo A può generare un messaggio cifrato con K_A che possa essere accettati da C.

20. Nella situazione a lato, i router R1 e R2 implementano una VPN mediante IPsec con ESP in modalità tunnel. Attraverso tale VPN, il calcolatore A si collega al server B.
    (a) Da quale indirizzo B vede arrivare la connessione?
    (b) Sulla rete pubblica (tra R1 e R2) quali indirizzi IP si possono osservare?
    (c) A e B possono avere degli indirizzi di una rete privata (ad esempio 192.168.0.0/16)?

    R: (a) Quello di A. (b) Solo quelli dei router R1 e R2. (c) Sì, senza problemi.