DMIF, Università degli Studi di Udine  III appello A.A. 2019-20 — 22 giugno 2020

Esame di **Reti di Calcolatori**

Soluzione

1. Per ognuno dei seguenti metodi di connessione si dica se è half o full duplex: (a) Ethernet classica (quella su cavo coassiale); (b) Ethernet commutata (quella con switch); (c) WiFi (802.11n); (d) Colombigramma (ossia, piccioni viaggiatori).

   R: (a) half duplex (b) full duplex (c) half duplex (d) full duplex

2. Un canale fisico analogico per la fonia ha una larghezza di banda tipica di 3 kHz. Supponendo che il segnale in arrivo ad un ricevitore abbia un rapporto segnale/rumore di 30 dB, determinare il massimo bit rate senza errore possibile (trascurando eventuali framing).

   R: Dal teorema di S-H, la capacità del canale è $C = BW * \log_2(1 + SNR)$. Con i dati della domanda si ha $C = 3kHz \log_2(1 + 10^{30dB/10}) = 29.9kb/s$.

3. Nella situazione della domanda precedente, viene usata una modulazione 256-QAM, in cui il simbolo corrispondente ad un baud è composto da 8 bit. Quale è il code rate (rapporto dati utili/dati grezzi) dell'algoritmo di correzione utilizzato?

   R: Con una larghezza di banda di 3kHz, dal teorema di Nyquist-Shannon la frequenza di campionamento del segnale analogico massima è $f_{sample} = 2BW = 6kBaud$. Il rate grezzo risulta di $6kBaud * 8bit = 48kb/s$, quindi il code rate è $29.9kb/s / 48kb/s = 0.62$.

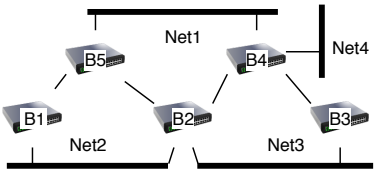
4. Un host è collegato ad uno switch Fast Ethernet (100Base-TX). Ricordando che l'interpacket gap è pari al tempo di 96 bit, quanti frame con un payload di 1000 byte possono essere inviati in un secondo?

   R: Un frame Ethernet prende 8 byte di preambolo + 14 di intestazione + 4 di CRC + 1000 di payload = 1026 byte = 8208 bit, a cui si aggiungono i 96 dell'IGP, per un totale di 8304 bit. A 100 Mb/s, ci sono 10^8 bit in un secondo, quindi ci stanno $10^8/8304 = 12042$ pacchetti.

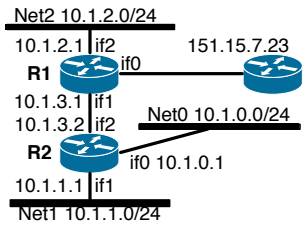
5. In Bluetooth LE (Low Energy) il bitrate di trasmissione è 1 Mb/s ma, diversamente dal Bluetooth normale, ogni frame viene inviato come segue: host A manda un frame dati (max 41 byte, di cui 27 payload) e B risponde con un frame di ack da 10 byte. Dopo ogni frame (dati o ack) bisogna aspettare 150 μs. Quant'è la banda utile massima (in kbyte/s) che si può ottenere in queste condizioni?

   R: Una comunicazione contiene $(41 + 10) * 8 = 408$ bit, che prendono 408 μs, a cui bisogna aggiungere $150 * 2 = 300\mu$s per i spazi tra i frame. In totale sono necessari 708 μs per trasmettere 27 byte, quindi la banda è $27/(708 * 10^{-6}) = 38$ kB/s = 305 kbps.

6. Gli switch della rete a lato implementano l'algoritmo di spanning tree. (a) Ci sono switch che si disattivano? (b) Quali switch deve attraversare un frame per andare dalla Net1 alla Net4?
   R: (a) Sì, B3. (b) B5-B1-B2-B4



7. Si dia la tabella di inoltro del router R2 della rete in figura.



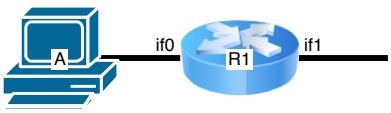
R:

Net/CIDR	if	next hop
10.1.0.0/24	if0	-
10.1.1.0/24	if1	-
10.1.2.0/24	if2	10.1.3.1
10.1.3.0/24	if2	-
/	if2	10.1.3.1

ma si può omettere una entry:

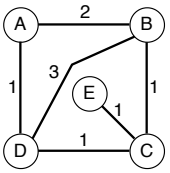
Network/CIDR	if	next hop
10.1.0.0/24	if0	-
10.1.1.0/24	if1	-
10.1.3.0/24	if2	-
/	if2	10.1.3.1

8. Il PC A ha ricevuto l'indirizzo 192.168.7.32 dal server DHCP, e il router a cui è collegato ha l'indirizzo 192.168.0.74 sull'interfaccia if1. Qual è la netmask minima (ossia, quella che blocca il minimo numero di bit) delle due sottoreti a cui si affaccia R1, supponendo che le due sottoreti abbiano la stessa netmask?



R: Affinché il router possa distinguere tra gli indirizzi delle due sottoreti, la maschera deve coprire almeno fino al primo bit differente tra i due indirizzi. In questo caso è il sesto bit più significativo del terzo byte, quind il CIDR minimo è 22 ossia la netmask minima è 255.255.252.0.

9. I router della rete a lato utilizzano un algoritmo di routing basato sul vettore delle distanze. (a) Si dia la tabella di routing finale di D; (b) Potrebbe succedere che la rete diventi instabile? Se sì, perché?



R: (a)

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

(b) L'evento è l'interruzione del collegamento tra E e C, e in contemporanea l'invio del vettore da B a C o da D a C; in tale situazione, C crede di poter raggiungere E attraverso B o D, ecc.

10. (a) Quali informazioni contiene l'intestazione di un pacchetto IPv6 per supportare funzionalità come la Quality of Service? (b) Un pacchetto IPv6 viene incapsulato in un IPv4 per consentirne l'instradamento su una rete IPv4. I router di tale rete possono tenere conto delle informazioni dell'intestazione IPv6?

R: (a) Il TrafficClass per la priorità e la FlowLabel per identificare i flussi all'interno dei router. (b) no, strettamente parlando, ma al limite potrebbero sbirciare il contenuto del payload, se si accorgono che è IPv6 incapsulato..

11. Si dica quale protocollo di trasporto è più adatto ad implementare ciascuno dei seguenti servizi:
(a) richieste a DNS (b) query (anche INSERT) a database (c) stampa remota (d) segnalazione allarme urgente (ad esempio, mancanza di corrente o incendio)

R: (a) UDP (b) TCP (perché non sono operazioni idempotenti) (c) TCP (d) UDP, con eventuale ritrasmissione

12. Una comunicazione TCP sta trasmettendo alla velocità di 1 Gbps = 10^9 b/s attraverso una rete che può consegnare i pacchetti con un ritardo fino a 60 secondi. È possibile che un pacchetto vecchio venga accettato al posto di uno nuovo a causa di un "wraparound"?

R: Per evitare che un pacchetto in ritardo possa prendere il posto di uno nuovo, con lo stesso numero di sequenza, bisogna evitare che il tempo di wraparound sia inferiore a 60 secondi. Ma questo tempo è $2^{32} byte/((10^9/8) byte/s) = 34.36$ secondi, quindi il wraparound è possibile.

13. Un host TCP ha appena trasmesso alcuni segmenti, tutti della lunghezza di 1000 byte, con i seguenti numeri di sequenza (e in questo ordine): 5000; 6000; 4000; 7000. Ha ricevuto due segmenti: il primo ha `Acknowledge`=6000 e `AdvWindow`=12000; il secondo ha `Acknowledge`=4000 e `AdvWindow`=8000. Quanti byte può ancora inviare?

R: Dato che in TCP l'Acknowledge è cumulativo, il segmento con `Acknowledge`=6000 è stato inviato dopo quello con `Acknowledge`=4000 (quello con ACK=4000 viene inviato quando viene ricevuto il segmento con SeqNum=3000, quello con ACK=6000 viene inviato quando viene ricevuto il segmento con SeqNum=5000). Evidentemente poi i due segmenti di ACK sono arrivati all'host in ordine invertito, per cui quando arriva quello con `Acknowledge`=4000 viene ignorato. Quindi la `AdvWindow` da considerare è quella associata all'`Acknowledge` più grande. Per cui, 12000 − (8000 − 6000) = 10000.

14. Un certo host TCP, che usa un algoritmo di congestion control con partenza lenta e ritrasmissione veloce, apre una nuova connessione, con MSS=1400. Esegue 3 round completi in partenza lenta, partendo da `CongestionWindow` = 2 MSS=2800. Se non vengono ricevuti gli ACK per due segmenti inviati nel terzo round, quanto vale `CongestionWindow` all'inizio del quarto round?

R: Partendo con `CongestionWindow`=2 MSS, dopo il primo round `CongestionWindow`=4 MSS; dopo il secondo round `CongestionWindow`=8 MSS; dopo il terzo round `CongestionWindow`=16 MSS meno 2 = 14 MSS = 19600.

15. Secondo il modello Dolev-Yao del canale insicuro, le due parti A e B possono appoggiarsi ad una "terza parte fidata" C (se presente). (a) Come si assumono le comunicazioni tra le controparti (A e B) e C? (b) In generale, potrebbe essere usata C come intermediario per lo scambio dei messaggi tra A e B? (ad esempio: $1.A \to C : A, B, M; 2.C \to B : A, B, M$)?

    R: (a) Sicure, non attaccabili dall'attaccante. (b) Si potrebbe in teoria, ma solitamente questi canali sicuri sono lenti, costosi, o fuori tempo (non esistono nel momento in cui A e B devono comunicare).

16. Una certa azienda impone che le password siano lunghe almeno 8 caratteri, con almeno 1 lettera maiuscola, 1 cifra e 1 segno "speciale". Le lettere dell'alfabeto sono 26 e i simboli speciali ammessi sono 12. Molti utenti, per soddisfare questo vincolo, scelgono password con una sola maiuscola all'inizio della parola e la cifra e il simbolo alla fine, in qualche ordine (ad esempio "Ciccio2!", "Milano-4"). (a) In questa situazione, quante sono le password di 8 caratteri? (b) Potendo tentare 100.000 password al secondo, in media dopo quanto tempo una password siffatta viene indovinata?

    R: (a) $26 * (26)^5 * 12 * 10 * 2 = 74139786240$.

    (b) In media servono $74139786240/(2 * 100000) = 370699$ secondi, pari a 103 ore, ossia 4.29 giorni.

17. Nel protocollo a lato, N è una nonce, K è una chiave simmetrica precondivisa tra A e B, e H è una funzione di hash prefissata. (a) Il messaggio M è integro per B? (b) È puntuale (ossia non soggetto ad attacchi replay)? (c) A può ripudiare il messaggio M?

    1. $A \to B : M$
    2. $B \to A : N$
    3. $A \to B : H(K, M), H(K, N)$

    R: (a) Sì, perché c'è un HMAC, in pratica. (b) No, si può fare un attacco replay al passo 2-3, sostituendo la prima parte del messaggio al passo 3. (c) Sì, non c'è niente che B possa utilizzare per dimostrare la paternità del messaggio.

18. Alice vuole mandare la stessa mail a Bob e a Charlie, confidenziale e all'insaputa l'uno dell'altro. Costruisce un messaggio PGP cifrato che vada bene per entrambi, e poi lo manda in due mail separate, una per destinatario. (a) Il timestamp che Bob e Charlie vedono è lo stesso? (b) Bob può scoprire se anche Charlie ha ricevuto lo stesso messaggio? (c) È necessario che Bob e Charlie conoscano la chiave privata di Alice?

    R: (a) Sì, è nel messaggio PGP. Quello della mail non conta. (b) Sì, perché si può scoprire nella parte del messaggio in cui è cifrata la chiave di sessione. (c) no, mai e poi mai qualcuno deve scoprire la chiave privata di Alice!

19. Nel protocollo a lato N è una nonce, PU_C è la chiave pubblica della terza parte fidata C, K_A è una chiave simmetrica precondivisa tra A e C, K è una chiave di sessione generata da B. (a) A è autenticato per B? (b) B è autenticato per A? (c) La chiave K è puntuale? Motivare le risposte.

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

    R: (a) Sì, perché solo A può ottenere la chiave al passo 3. (b) No, non c'è niente che dimostri a A l'identità di B. (c) Sì, perché in caso di attacco replay al passo 2 o 3, A se ne accorge grazie alla nonce.

20. Durante una connessione HTTPS, il client ha il sospetto che il server non sia quello che dice di essere. (a) Quali modi di handshake SSL potrebbero dare adito a questo sospetto? (b) Avendo a disposizione un altro canale sicuro (ad esempio, telefono), quale informazione di sessione potrebbero confrontare le due controparti, per garantire l'assenza di MITM?

    R: (a) DH anonimo, oppure RSA con controllo dei certificati disabilitato (b) potrebbero confrontare il Master Secret, che deve essere lo stesso per entrambi.