DMIF, Università degli Studi di Udine — III appello A.A. 2020-21 — 22 giugno 2021

Esame di **Reti di Calcolatori**

Soluzione

1. Le strategie di accesso condiviso al mezzo si dividono in TDM, FDM e STDM. Si dica quali di queste NON sono indicate, nelle seguenti situazioni: (a) Stazioni che trasmettono pochi dati e raramente. (b) Stazioni che non hanno modo di tenere un clock sincronizzato. (c) Comunicazioni con vincoli real time.

   R: (a) No TDM, FDM, perché occupano banda inutilmente (b) No TDM, perché devono sincronizzarsi (c) No STDM perché non garantisce tempi massimi di consegna.

2. Un canale di trasmissione ha una larghezza di banda di 10 MHz e un rapporto segnale/rumore in potenza di -20 dB. (a) Determinare il massimo bit rate "grezzo" di tale canale. (b) Se si usa una codifica con un alfabeto di 8 simboli, qual è il baudrate massimo corrispondente?

   R: (a) Un rapporto SNR in potenza di -20 dB equivale a $S/R = 10^{-2}$, perché $SNR = 10 * \log(S/R)$. Dal teorema di Shannon-Hartley, $C \leq B \log_2(1 + S/R)$ quindi $C \leq 10MHz \log_2(1 + 10^{-2}) = 143$ kbps. (b) Ogni simbolo porta 3 bit, quindi per fare 143 kbps servono 143/3 = 47 kbaud.

3. Due host A e B stanno comunicando con un protocollo stop-and-wait su un canale che ha un delay di 6ms da A a B e 2ms da B ad A. Ogni frame ha un payload di 1000 byte. Quant'è la banda utile netta?

   R: Il RTT è pari a 6+2=8ms. In ogni RTT si trasferiscono 1000 byte, quindi 1000/8 = 125 kbyte/s.

4. Un host è collegato ad uno switch Fast Ethernet (100Base-TX), e trasmette frame con un payload medio di 200 byte. Ricordando che l'IPG equivale a 96 bit e il preambolo è sempre di 8 byte, qual è la banda netta massima (in Mbps) ottenibile in queste condizioni?

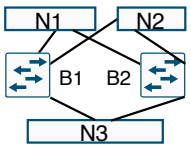
   R: Un frame Ethernet prende 8 byte di preambolo + 14 di intestazione + 4 di CRC + 200 di payload = 226 byte = 1808 bit, a cui si aggiungono i 96 dell'IPG, per un totale di 1904 bit. A 100 Mb/s, servono 19,04 μs per trasmettere un frame, quindi la banda utile è 200/19,04 = 10,5 Mbyte/s = 84 Mbps.

   Una calcolo più veloce è il seguente: l'overhead è 8+14+4+96/8 = 38 byte, quindi l'efficienza è 200/(200+38) = 84%. Quindi la banda utile è 100*0,84 = 84Mbps.

5. In una cella 802.11, una certa stazione con MAC address A ha appena trasmesso un RTS alla stazione con indirizzo B. Poi riceve un CTS con mittente B, ma l'indirizzo di destinazione è quello di un altro host C, che A non conosce. (a) L'host C potrebbe essere un nodo nascosto o esposto? (b) A può riprovare immediatamente a trasmettere il RTS? Se no, cosa deve aspettare di ricevere?

   R: (a) Un nodo nascosto: A non ha ricevuto l'RTS di C per B, forse perché fuori range. (b) Non può riprovare subito, perché c'è in corso una comunicazione tra C e B. Deve aspettare di vedere passare l'ACK da B a C (e la fine del NAV che ha determinato dal CTS che ha ricevuto).

6. Si consideri la rete a lato con switch ad autoapprendimento; B1 è il root bridge e ha le tabelle interne completamente aggiornate, mentre B2 è stato resettato, e conosce solo la posizione di un host B collegato alla rete N2. (a) Se un host A sulla rete N1 trasmette un frame indirizzato ad un host B, cosa succede a tale frame? Quante copie arrivano a B? (b) Cosa è necessario affinché si torni ad una situazione "corretta"?



   R: (a) Il frame viene ricevuto da B1 e da B2. B1 lo manda su N2 (è il root), ma anche B2 lo inoltra perché non sa ancora che B1 è il root. Quindi arrivano due copie del frame. (b) Che B2 riconosca B1 come root, attraverso il protocollo di spanning tree, e quindi che si disattivi.

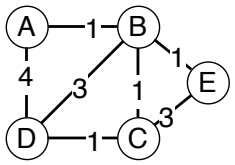
7. Una certa organizzazione ha quattro reparti, A, B, C, D, di rispettivamente 40, 30, 60 e 100 postazioni di lavoro. Si vuole assegnare una sottorete separata ad ogni reparto. (a) Si diano i CIDR minimi per ogni sottorete. (b) Si dia il CIDR minimo per la rete che possa essere suddivisa nelle quattro sottoreti.

   R: (a) A: /26; B: /27; C: /26; D: /25. (b) Se fosse una rete unica e non quattro sottoreti, sarebbero 230 indirizzi, e quindi un /24 sarebbe sufficiente. Ma non si riesce a dividere in quattro sottoreti come sopra, per cui è necessario un /23.

8. Un host A si collega ad una rete ma (forse per errore di configurazione) assume lo stesso indirizzo IP X di un altro host B già collegato. (a) Come potrebbe A accorgersi dell'esistenza di B? (b) Un altro host C vuole aprire una connessione TCP con tale indirizzo X, con cui non aveva avuto alcun contatto finora. Con quale host si collega?

   R: (a) Con una richiesta "auto-ARP": chiede chi ha quell'indirizzo ARP, e se qualcuno risponde, è un problema (b) A caso, tra A e B, a seconda di quale risponde prima all'ARP.

9. I router della rete a lato utilizzano un algoritmo di routing basato sul vettore delle distanze. (a) Si dia la tabella di routing iniziale di E. (b) Si dia la tabella di routing finale di E (ossia dopo la stabilizzazione).



   R: (a)

dest	d	n.h.
B	1	B
C	3	C
E	0	-

   (b)

dest	d	n.h.
A	2	B
B	1	B
C	2	B
D	3	B
E	0	-

10. Nella rete dell'esercizio precedente, viene usato DVMRP per instradare il traffico multicast. Un host collegato a C invia un pacchetto multicast ad un certo gruppo G (p.e., 224.1.2.3). (a) Se non c'è stato ancora"pruning", quanti pacchetti vengono generati, in tutta la rete, in totale? (b) Supponiamo che solo i router A,C,E siano interessati a tale gruppo. Dopo il "pruning", quali router non vengono interessati dal traffico del gruppo G?

    R: (a) 10; (b) B deve rimanere nell'albero per servire A e E, quindi si isola solo D e i suoi collegamenti.

11. Un server UDP è in ascolto sulla porta 1234. (a) Cosa si può dire dell'utente che ha lanciato tale processo? (b) Se riceve due datagrammi uno di seguito all'altro, provengono sicuramente dallo stesso client? (c) Se viene spento e riavviato, il client deve riaprire la connessione?

    R: (a) niente, perché 1234 non è una porta privilegiata. (b) Non è detto (c) No, UDP è senza connessione!

12. Un certo sistema ha fissato il Maximum Segment Lifetime a 15 secondi. (a) Se un processo chiude una connessione su una data porta, dopo quanto tempo può aprire una nuova connessione usando la stessa porta? (b) Cosa potrebbe succedere se il RTT con un certo client è superiore a tale tempo?

    R: (a) In chiusura passiva, si può tornare subito in stato CLOSED. In chiusura attiva, si deve aspettare il doppio di MSL, ossia 30 secondi. (b) Potrebbe succedere che segmenti vecchi, di una incarnazione precedente, arrivino nel mezzo di quella nuova causando disordine, ed eventualmente l'abort della comunicazione.

13. Una sorgente TCP ha inviato tre segmenti da 1200 byte l'uno, con SequenceNum pari a 3000, 4200, 5400 rispettivamente, e ha ricevuto i seguenti segmenti in questo ordine: ACK=3000, AdvertisedWindow=4200; ACK=5400, AdvertisedWindow=1800; ACK=4200, AdvertisedWindow=3000. Quanti byte può ancora spedire?

    R: Il terzo ACK è arrivato in ritardo, ed è reso obsoleto dal primo, che è quello che fa testo. Quindi EffectiveWindow=AdvertisedWindow -(LastByteSent-LastByteAcked) = 1800 - (6599 - 5399) = 600.

14. Un certo router può trasmettere su una interfaccia al massimo 10.000 pacchetti al secondo. I pacchetti arrivano casualmente, al ritmo di 2000 al secondo. Quant'è, in media, il ritardo complessivo dato dall'attraversamento dal router?

R: Usiamo la teoria delle code. Il tempo di servizio di un pacchetto è $S = 10^{-5}$ s/p. La frequenza di arrivo è $\lambda = 2000$ p/s; Da cui: $R = S/(1 - \lambda S) = 10^{-5}/(1 - 2000 * 10^{-5}) = 10^{-5}/0.8 = 12.5\mu s$.

15. In questi giorni il Ministero della Salute sta distribuendo i certificati di vaccinazione ("Green Pass"). In pratica si tratta di un QR code contenente informazioni come identità della persona, tipo di vaccino ricevuto e data di vaccinazione. Questa immagine viene salvata sul cellulare dell'utente, o perfino stampata su carta, e esibita al momento opportuno (p.e., imbarco in aereo, accesso a concerti, ecc.).
Rappresentate la situazione indicata secondo il modello del canale insicuro, e precisamente: chi è il mittente del messaggio? Chi è il destinatario? Cosa è il canale? Chi potrebbe essere l'attaccante?

    R: Mittente: Ministero. Destinatario: chi controlla l'accesso (hostess, buttafuori, ecc.). Canale: cellulare o altro supporto (anche un pezzo di carta). Attaccante: l'utente stesso, che potrebbe tentare di modificare il certificato o crearne uno falso.

16. Quali delle seguenti informazioni sono contenute in un certificato X.509: (a) Chiave privata del soggetto; (b) Identità dell'emittente (issuer); (c) Chiave pubblica dell'emittente; (d) Hash dei vari campi firmati con la chiave privata del soggetto.

    R: (a) no (b) sì (c) no (d) no

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, e H una funzione di hash. (Si supponga che i parametri g e p del DH siano noti e prefissati.)

    1. $A \to B : A$
    2. $B \to A : y_B, B, H(y_B, A, B)$
    3. $A \to B : y_A, H(y_A, A, B)$

    (a) Questo protocollo è soggetto ad attacchi MITM? (b) Se sì, si suggerisca come ripararlo, avendo a disposizione un segreto precondiviso K_{AB}, ma senza usare altre funzioni crittografiche.

    R: (a) sì perché non c'è niente che autentichi i messaggi. (b) è sufficiente mettere K_{AB} dentro le hash:
    1. $A \to B : A$
    2. $B \to A : y_B, N_B, H(y_B, A, B, K_{AB})$
    3. $A \to B : y_A, H(y_A, A, B, K_{AB})$

18. Durante l'handshake TLS, un server seleziona lo scambio RSA, e successivamente invia al client il suo certificato X.509 con la chiave pubblica. Il client controlla il certificato e nota che, rispetto al suo orologio, il periodo di inizio di validità è nel futuro. (a) Da cosa potrebbe essere causato questo problema? (b) Cosa deve fare il client? (c) E il server può fare qualcosa?

    R: (a) L'orologio del client è indietro. Oppure il certificato è veramente post-datato. (b) Controllare il proprio orologio. Se è giusto, allora deve rifiutare il collegamento (c) Se il problema è nel certificato, deve usare un altro certificato: non può modificare le date di quello non ancora valido, perché non è stato emesso da lui.