DMIF, Università degli Studi di Udine — I appello A.A. 2021-22 — 1º febbraio 2022

Esame di **Reti di Calcolatori**

Scrivere le risposte su fogli a parte, NUMERANDO CHIARAMENTE le risposte in corrispondenza ad ogni domanda. Illustrare brevemente il procedimento seguito in ogni domanda, in particolare quelle "di calcolo". Scannerizzare o fotografare i fogli (massimo 4 facciate BEN LEGGIBILI) con le risposte (ad esempio con una app come "CamScanner"), ed inviarle a `marino.miculan@uniud.it`.

1. Si dica in quale livello dello stack ISO OSI è prevista ognuna delle seguenti funzionalità: (a) riordinamento dei dati; (b) rilevamento di errori di trasmissione; (c) conversione dei formati di rappresentazione; (d) multiplexing tra diversi processi.

2. Su un certo canale viene trasmesso un segnale con una potenza di 14 mW, mentre si osserva un rumore di 0.2 mW. Quanto deve essere la larghezza di banda per permettere una capacità di canale di 16 Mbps?

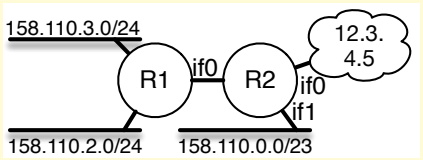
3. Un'interfaccia riceve la sequenza di bit 1011011001, che comprende anche un codice CRC generato con il polinomio generatore $x^3 + x^2 + 1$. La sequenza è corretta o no?

4. Due host A e B sono collegati ad uno switch Fast Ethernet (quindi a 100Mbps), che introduce un ritardo di 10μs. Ricordando che l'IPG corrisponde a 96 bit, quanto tempo è necessario per trasmettere da A a B un frame con 1500 byte di payload? (si trascuri il tempo di propagazione)

5. Nel Bluetooth classico, il datarate base di trasmissione è 1 Mbps, uno slot dura 625 μs e porta al massimo 483 bit. Quant'è il bitrate massimo a cui può trasmettere il nodo master, complessivamente?

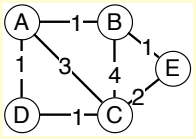
6. Si considerino i seguenti due indirizzi IP: 192.168.5.9 e 192.168.6.14. (a) Qual è la sottorete più piccola (ossia con il minor numero di indirizzi) che contiene entrambi questi indirizzi? (dare indirizzo/CIDR). (b) Qual è l'indirizzo di broadcast di tale sottorete?

7. Si dia la tabella di inoltro del router R2 della rete in figura, dove 12.3.4.5 è l'indirizzo del router gateway del provider Internet, e l'interfaccia if0 di R1 ha indirizzo 10.0.1.1.



8. L'host A con indirizzo 216.58.198.36 sta comunicando con un host B che ha indirizzo 192.168.1.100 ma che sta dietro un router che implementa NAT e che ha indirizzo pubblico 183.74.72.98. Ad un certo punto, tale indirizzo viene cambiato in 183.74.73.45. La comunicazione tra A e B viene mantenuta? Perché?

9. I router della rete a lato utilizzano un algoritmo di routing basato sullo stato dei collegamenti. (a) Si dia la tabella di routing finale di D; (b) Ad un certo punto il costo A-C cambia e diventa 1. Quanti messaggi LSP arrivano a D, e come cambia la sua tabella di routing?



10. I router della rete dell'esercizio precedente usano PIM in Sparse Mode per inoltrare il traffico multicast. Sia B il rendevouz router di un certo gruppo, a cui appartengono C e D. (a) Un pacchetto inviato a tale gruppo da un host collegato a D, quali router attraversa per raggiungere il rendevouz point? (b) E quanti altri hop deve fare per raggiungere C?

11. Si dica quale protocollo di trasporto è più adatto ad implementare ciascuno dei seguenti servizi, e perché: (a) sincronizzazione di orologi; (b) invio di una mail; (c) DHCP.

12. Un host TCP è nello stato ESTABLISHED. Invia un segmento con FIN=1. (a) Quale evento ha causato questo invio? (b) In che stato si porta dopo questo invio? (c) Che tipo di chiusura sta eseguendo?

13. Una sorgente TCP ha appena inviato in questo ordine i seguenti tre segmenti: Length=1000, SeqNum=3000; Length=1400, SeqNum=4000; Length=500, SeqNum=2000. A questo punto riceve un segmento con ACK=1, Acknowledgment=4000, AdvertisedWindow=7000. Ignorando problemi di congestione, quanti byte può ancora spedire?

14. Un host TCP utilizza l'algoritmo di congestion control con partenza lenta e ritrasmissione veloce, e inizia con cwnd=1 MSS e sshthreshold=32 MSS. (a) Dopo quanti round entra nella fase additiva? (b) Durante il decimo round di trasmissione riscontra tre ACK duplicati. Quanto diventa sshthreshold?

15. Per ognuno dei seguenti attacchi, si dica a quale aspetto di sicurezza (confidenzialità, integrità, disponibilità), e se ai dati o ai metadati.
(a) Collegarsi ad una conferenza Zoom (per esempio del Senato) con identità falsa; (b) Registrare la conversazione; (c) Condividere lo schermo e trasmettere un video... inatteso (nel caso specifico, porno).

16. Nel protocollo a lato, K è una chiave simmetrica precondivisa tra A e B, E un algoritmo di cifratura simmetrico robusto, e H una funzione di hash robusta. (a) La segretezza di K è garantita? (b) M è autenticato per B? (c) M è puntuale (ossia non soggetto ad attacchi replay)?

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

17. Si supponga che Alice, Bob e Charlie conoscano le chiavi pubbliche di tutti e tre. Alice vuole mandare una mail firmata a Bob e a Charlie, usando PGP. (a) Può inviare la stessa mail ad entrambi i destinatari, ossia mettendo sia B che C nei `To:` della stessa mail? (b) Il timestamp contenuto nel messaggio PGP è affidabile? (c) Il timestamp nell'intestazione della mail (il campo Date:) è affidabile?

18. 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. La K è la chiave condivisa costruita con Diffie-Hellman da y_A e y_B stesse. (I parametri g e p del DH siano noti e prefissati.)
Questo protocollo è soggetto ad attacchi man-in-the-middle? Perché?

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