1. Un certo canale viene acceduto da tre stazioni con modalità TDM; ogni slot ha una durata fissa di $200\mu s$ e il bitrate è di 1 Mbps. Le tre stazioni trasmettono in media 10, 15, 20 byte per slot, rispettivamente. Quant'è l'efficienza di questa situazione, in termini di utilizzo percentuale del canale?

3 slot = $600\mu s$ e $(10 + 15 + 20) \cdot 8 = 360$ bit

Teoricamente potrebbe trasmettere $600 \cdot 10^{-6}\,s \cdot 1 \cdot 10^{6}$ bps = 600 bit

Efficienza = $\frac{360}{600} = 60\,\%$

2. Un certo canale ha $SNR = -8$ dB, con una larghezza di banda pari a $20MHz$. (a) Qual è la massima capacità ottenibile (in Mbps)? (b) Se il baudrate è di 3 Mbaud, quanti bit devono essere codificati in ogni simbolo per avere tale capacità di canale?

a) $C = B \log_2(1 + SNR)$

$= 20\,MHz \log_2(1 + 10^{-8/10})$

$= 4.24$ Mbps

b) 3 MBaud/s = 4.24 Mbps

$\rightarrow$ 1 Baud = $\frac{4.24}{3} = 1.41$ bit

3. Su una certa linea che presenta una probabilità di errore per bit (nota anche come BER) pari a $p = 10^{-4}$, vengono inviati dei frame di 1000 byte (comprensivi di intestazione e CRC). Per aumentare l'affidabilità, ogni frame viene inviato due volte. Qual è la probabilità che almeno una delle due copie arrivi integra?

p = 1 - (PROBABILITÀ ENTRAMBI ERRATI)

$= 1 - (1 - (1-p)^{8000})^2$

$= 69.67\,\%$

oppure

$p = (1-p)^{16000} + 2 \cdot (1-p)^{8000} \cdot (1 - (1-p)^{8000})$

4. (a) Qual è la dimensione minima di un frame Ethernet? (b) In teoria, quanti frame (di dimensione minima) possono essere trasmessi al massimo in un secondo su una Fast Ethernet (100 Mbps), ricordando che l'IPG è di 96 bit?

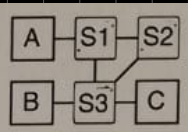
a) 8 byte preambolo + 32 bit jamming sequence = 96 bit

b) $\frac{100\ Mbps \cdot 1s}{96\ bit + 96\ bit} = 520833$

5. Due stazioni 802.11, A, B, sono associate allo stesso Access Point AP. (a) È possibile che A e B siano nascoste l'una all'altra? (b) Come si accorgono di questo? (c) In tal caso, A e B possono comunicare?

a) Sì
b) Vedono solo il CTS dell'AP
c) Possono comunicare attraverso l'Access Point

6. Nella rete a lato, gli switch S1, S2, S3 sono ad autoapprendimento, e sono appena stati resettati. A invia un frame indirizzato a B. (a) Quante copie di tale frame arrivano a B (se arrivano)? (b) Tale frame arriva anche a C? (c) Se poi C invia un frame a A, arriva anche a B?



a) Tante
b) Sì
c) No

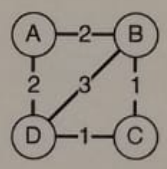
7. Nella rete 192.168.0.0/16 si vogliono definire tre sottoreti contigue, a partire dall'indirizzo 192.168.0.0. Le tre sottoreti devono essere le più piccole necessarie per contenere rispettivamente 50, 60, 70 indirizzi. Si diano gli indirizzi di tali sottoreti, completi di CIDR.

192.168.0.0/26
192.168.0.64/26
192.168.0.128/25

8. Un server DHCP assegna indirizzi nella sottorete 10.0.1.0/26. (a) Quanti client possono essere collegati alla rete, contemporaneamente? (b) Ad un certo punto il server DHCP viene resettato (ad esempio per una mancanza di corrente), mentre i client rimangono attivi. Cosa può succedere se un nuovo client chiede un indirizzo al DHCP?

a) $2^6 - 2 = 62$ indirizzi per gli host
b) Clash di indirizzi

9. I router della rete a lato utilizzano un algoritmo di routing basato sul vettore delle distanze, con *split horizon with poison reverse*. Dopo che la rete si è stabilizzata: (a) Si dia la tabella di instradamento di D. (b) Si mostri il vettore delle distanze che D invia a A.



a)

DESTINATION	COST	NEXTHOP
A	2	A
B	2	C
C	1	C
D	0	-

b)

A	∞
B	2
C	1
D	0

10. In IPv6: (a) Quanti bit occupa un indirizzo? (b) A cosa serve l'*etichetta di flusso*? (c) Quali di queste informazioni viene riutilizzata a livello IPv4, se si incapsula IPv6 in IPv4?

a) 128 bit
b) Per permettere ai router di identificare a che flusso appartengono i pacchetti
c) Nessuna

11. Un processo server S, sull'host A, sta ricevendo datagrammi UDP sulla porta P da due client remoti C_1, C_2. (a) Se C_1 invia D_1 prima che C_2 invii D_2, il processo S riceve D_1 prima di D_2? (b) È possibile che un datagramma che arriva alla porta P dell'host A, non venga poi consegnato a S?

a) Dipende
b) Sì, ad esempio se il buffer di ricezione è pieno

12. L'host A ha appena inviato ad un host B un segmento con SYN=1, ACK=1, SeqNum=12345, Acknowledgement=34123. (a) In che stato si porta se riceve da B un segmento con SYN=0, ACK=1, Acknowledgement=12346? (b) E se riceve da B un segmento con SYN=1, ACK=0, SeqNum=34122?

a) ESTABLISHED
b) Rimane in SYN_RECEIVED

13. Un certo processo sta inviando dati ad un altro, attraverso una connessione TCP con MSS=1460 byte e RTT=20ms. (a) Se il processo scrive nella socket 100 byte ogni 5 ms, a regime qual è la dimensione del payload segmenti inviati? (b) E se invece scrive nella socket 1000 byte ogni 50 ms?

a) 400 B
b) 400 B se continuo, 1000 B se discreto

14. Un router serve tre flussi secondo la politica di accodamento equo (Fair Queueing); attualmente i pacchetti in coda (con le loro lunghezze) sono i seguenti: A1=100, A2=300, A3=200; B1=200, B2=100; C1=50, C2=100; C3=300. In che ordine vengono trasmessi i pacchetti?

C1, A1, C2, B1, B2, A2, C3, A3

15. Alice ha precondiviso con Bob una chiave master K_M a 128 bit. Ogni volta che A deve inviare a B un messaggio M, prima calcola $K = H(M)$, dove H è una funzione di hash prefissata a 64 bit; poi invia a B il messaggio $C = E_{K_M}(K), E_{KK}(M)$, dove E è un cifrario simmetrico robusto che usa chiavi a 128 bit e KK è la concatenazione di K con se stessa. Bob, quando riceve C, prima estrare K usando la chiave master, e poi con KK decifra il messaggio M; per verificare se la decifratura è corretta, controlla che sia $H(M) = K$. Quanto è il costo di un attacco brute force alla segretezza di M?

2^{64} tentativi, 2^{63} nel caso medio

16. Una serie di blocchi in chiaro $P_1, P_2, \ldots P_n$ viene cifrata con un cifrario a blocchi e modalità CBC, ottenendo $C_1, C_2, \ldots C_n$. (a) Se viene alterato 1 bit del blocco P_i prima della cifratura, quali blocchi cifrati vengono alterati? (b) E che effetto ha tale modifica, sui dati dopo la decifratura?

a) $P_i, P_{i+1}, \ldots, P_n$
b) ?

17. Nel protocollo a lato, C è una terza parte fidata, K_A, K_B sono chiavi master precondivise tra A e C, e B e C, rispettivamente. K è una chiave di sessione generata casualmente da A, e N una nonce generata da B. (a) A è autenticato per B? (b) B è autenticato per A? Perché?

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