

1. $d = 60 \cdot 10^6 \text{ Km} = 60 \cdot 10^9 \text{ m}$

bitrate = 250 kb/s

$c = 3 \cdot 10^8 \text{ m/s}$

foto = $5 \text{ MB} = 40 \cdot 10^6 \text{ bit}$

a. RTT? $RTT = \frac{60 \cdot 10^6}{3 \cdot 10^8} = 200 \cdot 2 = 400 \text{ s}$

b. $t = \frac{40 \cdot 10^6}{250 \cdot 10^3} = 160 \text{ s} + 200 = 360 \text{ s}$

2. 64 simboli \Rightarrow 6 bit a simbolo

FEC (3/5)

$B = 8 \text{ MHz} = 8 \cdot 10^6 \text{ Hz}$

1m simbolo per ciclo

8% traffico di servizio

bitrate utile?

~~BR = 2B \Rightarrow BR = $8 \cdot 10^6 = 8 \cdot 10^6 \text{ simb/s}$~~

$BR = \frac{1}{1,25 \cdot 10^7 \text{ s}} \text{ simb} = 8 \cdot 10^6 \text{ simb/s}$

1 BAUD per ciclo \Rightarrow 1 ciclo = $\frac{1}{8 \cdot 10^6 \text{ Hz}} = 1,25 \cdot 10^7 \text{ s}$ e in quello ho 1 BAUD (al posto di 2)

bitrate grezzo = $BR \cdot 6 = 96 \cdot 10^6 \text{ bit/s} = 96 \text{ Mb/s}$, con la FEC diventiamo \Rightarrow perdo $\frac{3}{5} = 0,6 \Rightarrow 48 \cdot 0,6 = 28,8$

bitrate utile = bitrate grezzo $\cdot 0,08 = 23,04 \text{ Mb/s}$

3. $\text{int} = 10 \text{ B}$ (con CRC dentro)

payload = 1000 B

$p_e(1 \text{ bit}) = 10^{-5}$

file da $10 \text{ KB} \Rightarrow 10^4 \text{ B}$

per il file ci vogliono $\frac{10^4}{10^3} = 10$ pacchetti \Rightarrow ogni pacchetto ha 8080 bit

$p(\text{ALMENO UNO}) = 1 - p(\text{No error})$

$= 1 - p(\text{No error})^{10}$

$= 1 - [(1 - p_e)^{8080}]^{10} = 0,554 \Rightarrow 55,4\%$

a. prob. ALMENO UNA ritrasmissione $\rightarrow 1 - p(\text{No error})$

4. Eth. classica

A: A1, A2, ...

B: B1, B2, ...

istante 1: A1, B1 \rightarrow collisione \Rightarrow slotTime $\cdot [0,1]$

a. prob. collisione al secondo tentativo?

$\frac{(0,1) (1,0)}{(0,0) (1,1)} \Rightarrow \frac{1}{4} \text{ 1/4}$

b. se A trasmette A1 (0,1), qual è la prob.

che riesce ad inviare A2

(solo il range di B aumenta)

$\frac{(0,0)}{(0,1) (0,2) (0,3)} \Rightarrow \frac{3}{4}$

perché B1 collide con A1, quindi K di B è [0,1], poi A2 spedisce subito e B1 fa carrier sense, trova la linea occupata e lo considera come collisione \Rightarrow B è [0,1,2,3]

5. 3 slave (A,B,C)

1 master

$t_{slot} = 625 \mu\text{s} = 625 \cdot 10^{-6} \text{ s}$

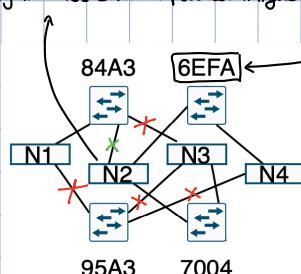
tmax di trasmissione tra due host? $(A \xrightarrow{+} M \xrightarrow{+} B \xrightarrow{+} M \xrightarrow{+} C \xrightarrow{+} M) \Rightarrow$ è al max $t_{slot} = 6 \cdot 625 \cdot 10^{-6} = 3750 \mu\text{s}$

perché per ogni router salvo il percorso migliore verso la root

6. SPANNING TREE

a. SI, 95A3

b. da N1 a N3: 84A3, 7004



7. A: 158.0.2.3

B: 158.5.3.5

C: 158.7.1.4

a. uso 3 bit \Rightarrow 158.0.0.0/21

guardo il prefisso comune \Rightarrow 158.0 \Rightarrow 158.0.0000⁸000⁵000

b. broadcast \Rightarrow 158.7.255/13

255

158.7.1111000.255

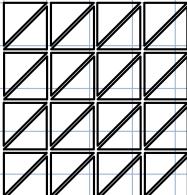
158.5 \Rightarrow 158.0.00001101⁸ \Rightarrow 158.0.0.0/13

158.7 \Rightarrow 158.0.00000111⁵ \Rightarrow 158.0.0.0/13

andava bene anche il mio ragionamento, però dovevi vedere la seconda ottava.

8. a. IP

b. il pacchetto non riesce ad arrivare a dest.



9. D-V con SPLIT-HORIZON

a.	mode	cost	m.hop
A	2	B	
B	1	B	
C	0	/	
D	1	D	
E	3	E	

b.	mode	cost	m.hop
C	0	/	
D	1	D	
E	3	E	

10. a. Si, AS3

b. AS4, AS2

c. AS1, AS5 AS4

11. a. fa il checksum su: header, payload e pseudoheader (IP degli indirizzi)

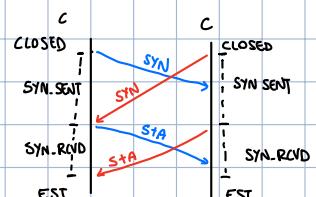
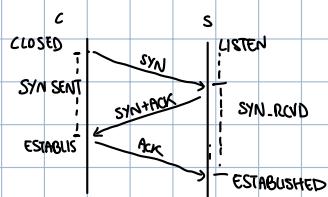
b. fallisce perché vengono modificati gli IP

12. TCP è in SYN-SENT.

a. ATTIVA

b. invia SYN=1 ACK=123456 e si porta in ESTABLISHED SYN.RCVD

c. ESTABLISHED



13. TCP

$S = 300B$ ogni $10ms$

$MSS = 1460B$

$RTT = 50ms = 50 \cdot 10^{-3}s$

$$\text{bits/second} = \frac{2400 \text{ bit}}{10 \cdot 10^{-3} \text{ s}} = 240 \text{ kb/s}$$

a. al max in un ciclo produco: $RTT \cdot \text{bits/second} = 50 \cdot 10^{-3} \cdot 240 \cdot 10^3 = 12000 \text{ bit} = 1500 \text{ B} > \text{MSS}$
perciò, per ALOHA di Negev, invio in media MSS byte

a. grandezza payload in media?

b. al max in un ciclo produco: $RTT \cdot \text{bits/second} = 30 \cdot 10^{-3} \cdot 240 \cdot 10^3 = 900 \text{ B} < \text{MSS}$, quindi

b. se RTT scende a 30ms?

spedisco 900B ogni ciclo

14. RED

MimTh: 20 KB

MaxTh: 100 KB

p = 0,05

AvgLen = ?

$$p = \frac{\text{AVGLEN} - \text{MimTh}}{\text{MaxTh} - \text{MimTh}} \Rightarrow p \cdot (\text{MaxTh} - \text{MimTh}) + \text{MimTh} = \text{AVGLEN}$$

$$\text{AVGLEN} = 24 \text{ KB}$$

15. a. masquerade, INTEGRITA', ATTIVO

b. sniffing, PASSIVO, CONFIDENZIALITA'

c. INTEGRITA', ATTIVO

16. AES con OFB

IV è 2 byte

$$\text{OFB} : C_i = P_i \oplus O_i$$

$$O_0 = IV \Rightarrow \text{mai avere } IV + K \text{ uguali}$$

$$O_i = E_K(O_{i-1})$$

KSo = IV

KSi = $E_K(K_{Si-1} \& OxFFFF)$

$L_i = P_i \oplus KSi$

a. che essendo IV = 2 byte $\Rightarrow 16$ bit, quindi si ripete ogni 2^{16} e rischi di poter decifrare i due payload

b. cambiare chiave prima di 2^{16} blocchi

18. $A \rightarrow B : M, E_{PRA}(H(M))$

a. P_{UA}

b. calcolare $h(M)$ e poi inviare $(M, E_{PRA}(h(M)))$

c. $B \rightarrow A : E_{PUA}(N)$

$A \rightarrow B : M, N, E_{PRA}(h(M), N)$

1. a. TDM, FDM
- b. TDM
- c. STDM

2. $B = 10 \text{ MHz} = 10 \cdot 10^6 \text{ Hz}$
 $\text{SNR} = -20 \text{ dB}$

a. bit rate "grezzo" max: $\text{SNR} = 10 \log_{10} (S/N) \Rightarrow S/N = 10^{\frac{\text{SNR}}{10}} = 10^{-2} = \frac{1}{10^2}$

$$C = B \cdot \log_2 (1 + \text{SNR}) \Rightarrow 10 \cdot 10^6 \cdot \log_2 (1 + 10^{-2}) = 143,6 \text{ Kbps}$$

b. ALFABETO a 8 simboli, il BR max? $\Rightarrow \text{bitrate} = \text{BR} \cdot B \Rightarrow \text{BR} = \frac{\text{bitrate}}{3} = \frac{47,9 \text{ band/s}}{\# \text{bit}}$

3. STOP & WAIT

delay A \rightarrow B = 6 ms

banda utile metta?

delay B \rightarrow A = 2 ms

$$t_{\text{TOTALE}} = \text{delay A} \rightarrow \text{B} + \text{delay B} \rightarrow \text{A} = 8 \cdot 10^{-3} \text{ s}$$

payload = 1000 Byte = 8000 bit

$$C = \frac{8000 \text{ bit}}{8 \cdot 10^{-3} \text{ s}} = 1 \text{ Mb/s} = 125 \text{ Kbps}$$

4. 100base-TX = 100 Mb/s

payload = 1600 byte = 1600 bit

banda metta massima?

per ogni frame: 1600 payload e 1760 bit com intestaz. + 4 bit CRC + 14 bit intestaz.

1 PG = 96 bit

preamble = 8 byte = 64 bit

$$\text{efficienza E} = \frac{1600}{1760 + 18} = 0,899 = \%$$

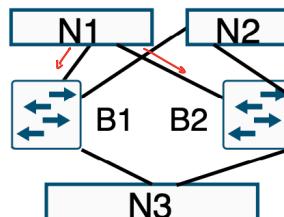
$$\text{banda utile} = 100 \text{ Mb/s} \cdot 0,899 = 90,9 \text{ Mb/s}$$

5. a. NASTO

b. no, deve aspettare di ricevere l'ACK

6. a. B2 lo consegna a N2, ma anche B1 lo fa, perciò ne arrivano 2

b. B2 deve sapere che B1 è il ROOT BRIDGE



7. A \rightarrow 40

B \rightarrow 30

a. CIDR minimi per ogni sottorete:

A \rightarrow 6 bit \Rightarrow /26

b. CIDR MINIMO: da /25 devo mappare 4 reti \Rightarrow 2 bit \Rightarrow /23

C \rightarrow 60

D \rightarrow 100

B \rightarrow 5 bit \Rightarrow /27

C \rightarrow 6 bit \Rightarrow /26

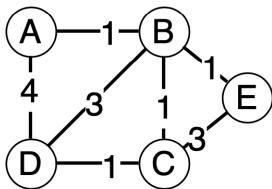
D \rightarrow 7 bit \Rightarrow /25

8. A assume lo stesso IP di B

- fa una richiesta ARP e mappa gli indirizzi
- si collega con B perché le F-table contengono IPx, B

9. DISTANCE V.

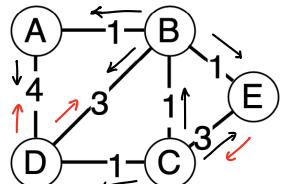
a.	dest	cost	met hop
	B	1	B
	C	3	C
	E	0	/



b.	dest	cost	met hop
	A	2	B
	B	1	B
	C	2	B
	D	3	B
	E	0	/

10. DVMPR nella rete precedente

- 10
- D



11. a. non è amministratore

- no
- no

12. MSL = 15s

- $2 \cdot MSL = 30s$
- ci sono dei pacchetti "superstiti"

13. TCP

Dim: 1200B

EFF. W.?

SegNum = 3000, 4200, 5400

ACK: 5400 → ha letto 5399 byte, mancano ultimi 1200

riceve: ACK: 3000 ADV.W: 4200

EFF. WINDOW = $1800 - 1200 = 600$ Byte

ACK: 5400 ADV.W: 1800

ACK: 4200 ADV.W: 3000

14. 10.000 pacchetti al sec

λ : 2000 pacch/s

$S: \frac{1}{10000} = 10^{-4}$ s/pacch



$$R = \frac{s}{(\lambda - \lambda s)} = 1,25 \cdot 10^{-4} \text{ s}$$

$\lambda: \frac{\text{pacch}}{\text{s}}$

$S: \frac{\text{s}}{1 \text{ pacchetto}}$

15. mittente: governo

destinatario: controllore

canale: immagine/stampa

attaccante: persona che finge il suo greenpass (firmato con chiave PR ministero e controllato, usano PU ministero)

16. a. NO

b. SI

c. NO

d. ~~SI~~ NO

17.

a. MITM? si

b. ho K_{AB} precomdiviso, come aggiusto?

1. $A \rightarrow B : A$

2. $B \rightarrow A : y_B, B, H(y_B, A, B)$

3. $A \rightarrow B : y_A, H(y_A, A, B, K_{AB})$

1. $A \rightarrow B : A$

2. $B \rightarrow A : y_B, B, H(y_B, A, B)$

3. $A \rightarrow B : y_A, H(y_A, A, B)$

1. a. scegliere un percorso alternativo
 b. si perché potrebbero arrivare (o non arrivare) pacchetti disordinati, es. usare TCP

2. 1 simbolo ha 3072 bit

$$t_{SMB} = 1,246 \text{ ms}$$

a. bitrate grezzo?

1 frame ha 76 simboli

$$t_{PAUSA_FRAME} = 1,304 \text{ ms}$$

$$\text{bitrate} = \frac{3072 \cdot 76}{(1,246 \cdot 76 + 1,304) \cdot 10^{-3}} = 2432000 \text{ bit/s} = 2,4 \text{ Mb/s}$$

$$b. B = 1536 \text{ KHz} = 1536 \cdot 10^3 \text{ Hz}$$

$$\frac{S}{N} = ? \quad C = B \cdot \log_2 (1 + \frac{S}{N}) \Rightarrow \frac{S}{N} = 2^{\frac{C}{B}} - 1 = 2^{\frac{2,4 \cdot 10^6}{1536 \cdot 10^3}} - 1 = 1,95$$

3. $p(x) = 10111 = x^4 + x^3 + x + 1$

RX: 110101101010 è corretto?

$R = 010 \Rightarrow \text{NON E' CORRETTO}$

$$\begin{array}{r}
 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \\
 \hline
 1 \ 0 \ 1 \ 1 \ 1 \\
 \hline
 0 \ 1 \ 1 \ 0 \ 1 \ 1 \\
 \hline
 1 \ 0 \ 1 \ 1 \ 1 \\
 \hline
 0 \ 1 \ 1 \ 0 \ 0 \ 1 \\
 \hline
 1 \ 0 \ 1 \ 1 \ 1 \\
 \hline
 0 \ 1 \ 1 \ 1 \ 0 \ 0 \\
 \hline
 1 \ 0 \ 1 \ 1 \ 1 \\
 \hline
 0 \ 1 \ 0 \ 1 \ 1 \ 1 \\
 \hline
 1 \ 0 \ 1 \ 1 \ 1 \\
 \hline
 0 \ 0 \ 1 \ 0
 \end{array}$$

4. S.W.

$$RWS = SWS = 8 \text{ frame} \quad 2^{m-1} = 8 \Rightarrow m-1 = 3 \Rightarrow m = 4$$

#bit del SeqNum?

5. 1 master 1 slave

multislot \rightarrow 3 slot alla volta

$$t_{bit} = 1 \mu s$$

$$t_{slot} = 625 \mu s$$

$$pausa_frame = 16 \text{ bit}$$

$$intestaz = 128 \text{ bit}$$

a. banda utile da MASTER \rightarrow SLAVE

$$\text{in uno slot max } 625 \text{ bit} \Rightarrow \begin{array}{c} 128 \\ 481 \\ 16 \end{array} |$$

$$\text{bitrate gresso} = \frac{625 \text{ bit}}{625 \cdot 10^{-6} \text{ s}} = 1 \text{ Mb/s}$$

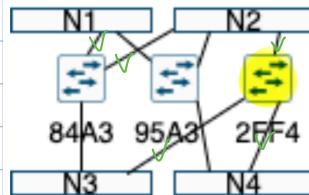
$$\text{efficienza} = \frac{481}{625} = 0,7696$$

$$\text{bitrate netto} = \frac{769,6 \text{ Kb/s}}{2} = 384,8 \text{ Kb/s}$$

\Rightarrow in realtà un frame solo in 3 slot

6. SPANNING TREE

a. S1, 95A3



b. N1, N2

7. IP

$$\text{payload} = 1000 \text{ B}$$

a. quanti pacchetti vengono trasmessi?

$$\text{MTU} = 256 \text{ B}$$

$$intestaz = 20 \text{ B} \Rightarrow \left\lfloor \frac{256 - 20}{8} \right\rfloor \cdot 8 = 232 \text{ B di payload a pacchetto}$$

$$\text{vengono inviati} \left\lceil \frac{1000}{232} \right\rceil = 5 \text{ pacchetti}$$

b. overhead aggiunto dalla frammentaz?

$$e = \frac{1000}{1000 + \frac{5 \cdot 20}{4}} = \frac{92,59\%}{98,57\%} \quad \text{e quindi overhead} = 1 - e = 7,4\%$$

8. NAT

a. quella riandomica del router che gli assegna in uscita

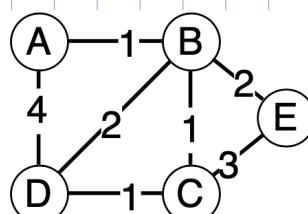
b. ma, perché dentro il router c'è la tupla $\langle \text{IP}_A, \text{p}_A, \text{IP}_B, \text{p}_B, \text{protocollo} \rangle$

9. LINK-STATE

a. il numero di vicini che ha il numero di ARCH, perché poi esegue Dijkstra e diventa = numero di nodi

b. 3

c. 2 ms



10. a. il numero di AS commessi ad esso
b. si

11. UDP: 15 UDP/s

payload = 1000B
a. bitrate IP? payload IP: 8 + 1000
intestaz IP: 20

$$\Rightarrow \text{un pacchetto IP sono 1028B} \Rightarrow \text{bitrate IP: } \frac{8 \cdot 1028 \cdot 15 \text{ bit}}{1 \text{ s}} = 123,4 \text{ Kb/s}$$

b. 2 sec. di buffer, quanti KB deve bufferizzare?

$$\text{bitrate UDP: } \frac{8 \cdot 1008 \cdot 15 \text{ bit}}{1 \text{ s}} = 120,96 \text{ Kb/s} \text{ e se } t = 2 \text{ s} \Rightarrow \text{buffer} = 120,96 \cdot 10^3 \frac{\text{b}}{\text{s}} \cdot 2 \text{ s} = 30,2 \text{ kB}$$

12. TCP

SYN = 1 SeqNum = 12345

- a. ACK = 12346 SYN = 1 e si porta in SYN-RCVD
b. ~~allora deve essere un riconseguito~~ client non ha ricevuto SYN+ACK, perciò server glielo rimanda
c. ACK

13. SeqNum Length

1000	1000
2000	500
2500	700

quanti byte può spedire A? ADW. - (1200) = 1800B

Riceve da B ADW: 3000 ACK: 2000

14. FQ sui flussi A,B,C

A : 100, 50, 80, 100

a. all'istante $50 + 80 = 130$

B : 80, 200, 80

b. ~~all'istante $50 + 80 + 100 + 150 + 220 + 280 + 300 + 320 = 1520$~~

C : 50, 250, 50

all'istante: Σ durate fino a A4 = 910

$$F(A1) = 100 \quad F(A2) = 150 \quad F(A3) = 220 \quad F(A4) = 320$$

$$F(B1) = 80 \quad F(B2) = 200 \quad F(B3) = 360$$

$$F(C1) = 50 \quad F(C2) = 300 \quad F(C3) = 350$$

15. a. a liv. trasporto (essendo librerie) (TLS è liv. 5)

b. coppia chiavi pubblica/privata per ognuno e delle NONCE

c. NO perché è libreria

16. data: YYYYMMDD $\in [1940.01.01 - 2019.12.31]$

codice di 4 cifre $\rightarrow 10^4$

data + codice

a. quanto grande è lo spazio delle chiavi (ogni 4 anni è un bisestile \rightarrow 3 mali e 1 bisestile)

365 366

$$\text{data: } (365 \cdot 80) - 1 + 20 = 29219 \Rightarrow 29219 \cdot 10^4$$

codice: 10^4

$$\text{b. } 10.000 \text{ tent/s} \Rightarrow \frac{29219 \cdot 10^4 \text{ tent}}{2 \cdot 10^4 \frac{\text{tent}}{\text{s}}} = 14609 \text{ s}$$

17. $K_A \rightarrow A, C$

$K_B \rightarrow B, C$

C è fidata

K è generata da C sul momento

1. $A \rightarrow C : A, B$

2. $C \rightarrow A : E_{K_A}(A, B, K, E_{K_B}(A, B, K))$

3. $A \rightarrow B : E_{K_B}(A, B, K), E_K(M)$

a. M segreto? sì

b. M autentico? sì perché sono sicuro da chi è stato spedito

c. M puntuale? no

1. a. APPLICATION

b. FISICO

c. TRASPORTO

d. DATA LINK

2. 45 simboli

15 frame/s

a. bitrate? $BR = 15 \text{ simb/s}$

$$\text{bitrate} = BR \cdot \log_2 (45) = 82,38 \text{ bit/s}$$

b. $\text{SNR} = 10 \text{ dB}$ $B = ?$

$$\text{SNR} = 10 \log_{10} (\text{S/N}) \Rightarrow \text{S/N} = 10^{\frac{\text{SNR}}{10}} = 10$$

$$C = B \cdot \log_2 (1 + \text{S/N}) \Rightarrow B = \frac{C}{\log_2 (1 + \text{S/N})} = \frac{82,38 \text{ bit/s}}{\log_2 (11)} = 23,81 \text{ Hz}$$

3. 1 frame ha al max. 483 bit \rightarrow su 1 slot» 1124 bit \rightarrow su 3 slot

intestazione: 126 bit

a. integrali con più trasmissioni da 1 slot:

$$\text{ho 2 trasmissioni} \Rightarrow 483 + 126 = 609 \Rightarrow 1052$$

$$317 + 126 = 443$$

$$\Rightarrow p(\text{INTEGRALI}) = (1 - p_e)^{1052} = 0,90 = 90\%$$

b. una trasmissione da 3 slot

$$800 \text{ bit} + 126 \text{ bit} = 926 \Rightarrow p(\text{INTEGRALI}) = (1 - p_e)^{926} = 31,2\%$$

4. Gigabit Ethernet = 1Gb/s

$$\text{bit time} = 1 \text{ ms} = 10^{-3} \text{ s}$$

$$\text{IPG} = 96 \text{ ms} = 96 \cdot 10^{-3} \text{ s}$$

$$\text{a. intestaz} = 26 \text{ B}$$

$$t_F = \frac{1526 \cdot 8}{10^3} + 96 \cdot 10^{-3} = 1,23 \cdot 10^{-5} \text{ s}$$

$$t_{\text{FRAME}} = ?$$

$$\text{payload frame} = 1500 \text{ B}$$

b. massimo bitrate utile?

$$\text{bit IPG} = \frac{10^3 \text{ bit}}{s} \cdot 96 \cdot 10^{-3} \text{ s} = 96 \text{ bit/s}$$

$$\text{efficienza} = \frac{1500 \cdot 8}{1526 \cdot 8 + 96} = 97,53\% \Rightarrow \text{bitrate utile} = 975,3 \text{ Mb/s}$$

5. 802.11

A riceve CTS da C \rightarrow DA \rightarrow B

a. C esposto e D maschato

b. No

6. a. A, B, C
b. 84A3, 95A3

7. 192.168.0.0/16

4 sottoreti contigui \rightarrow 800 indirizzi ciascuna

a. $A \rightarrow 192.168.0.0/22$

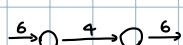
b. se ho 1022 ind. e me uso 800 $\Rightarrow 73,2\%$

$B \rightarrow 192.168.4.0/22$

$C \rightarrow 192.168.8.0/22$

$D \rightarrow 192.168.12.0/22$

8. payload IPv6 = 500B



$$\text{intestaz. IPv4} = 20B \Rightarrow \text{overhead} = 1 - e = 1 - \frac{540}{560} = 0,0357 = 3,6\%$$

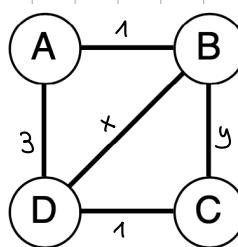
intestaz. IPv6 = 40B

overhead del tunnel?

9. DISTANCE VECTOR

- a. peso (B-D) ≥ 2
b. peso (B-C) ≥ 3

dest	d	n.h.
A	0	-
B	1	B
C	4	D
D	3	D



10. a. UDP
b. applicativo

11. UDP: bad checksum
a. il datagramma si è danneggiato
b. viene scaricato silenziosamente

12. TCP in ESTABLISHED

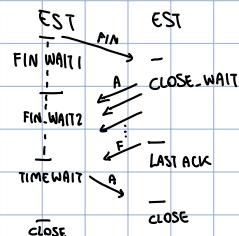
seqNum = 12000

a. CLOSE_WAIT

Length = 1000

b. no, non per forza. deve ancora essere ricevuto

c. sì



13. 500B ogni 2ms

RTT = 5ms = $5 \cdot 10^{-3}$ s

MSS = 1460B

a. byte di un segmento? $v = \frac{500}{2 \cdot 10^{-3}} = 250 \text{ KB/s}$ ogni RTT scrive = $250 \cdot 10^3 \cdot 5 \cdot 10^{-3} = 1250 \text{ B} \Rightarrow < \text{MSS}$, invia 1250B

b. MSS = 1000 \Rightarrow invia 1000

14. TCP in fase addittiva

cwnd = 7000, MSS = 1400

a. ha inviato 4 pacchetti e ricevuto 3 ACK

$$\text{increment} = \frac{\text{MSS}^2}{\text{cwnd}} \text{ (per ogni ACK)} \Rightarrow \text{sse la dim è MSS}$$

$$\text{incremento: } \frac{12200 - 10000}{7000} \cdot \text{MSS} = 440 \text{ B}$$

b. cwnd = 7440B

$$\text{SWS} = \text{cwnd} - 500 = 6940 \text{ B}$$

15. a. indirizzi

- b. Sì perché il router indirizza a liv. 3
- c. No perché il router cambia gli indirizzi

16. $A \rightarrow B : i, E_K(i, M_i)$

K è simmetrica

a. Sì

b. Sì

c. Sì

17. a. Sì

b. No

c. NO

1. $A \rightarrow B : A, E_K(A, M)$

2. $B \rightarrow A : N$

3. $A \rightarrow B : E_{PU_B}(N, K)$

18.

a. RSA (perché basta solo quello del server)

b.

c.

NET::ERR_CERT_REVOKED

Subject: www....

Issuer: QuoVadis Global SSL ICA G3

Expires on: 5 feb 2021

Current date: 28 gen 2021

1. a. RETE
- b. DATA LINK
- c. SESSION
- d. TRANSPORT

2. $B = 500 \text{ MHz} = 500 \cdot 10^6 \text{ Hz}$

1 simbolo ha 4 bit

$$BR = 2 \cdot 500 \cdot 10^6 = 10^9 \text{ baud/s}$$

$$\text{FEC con coderate} = \frac{1}{2}$$

↓
diviso per 2 il
bitrate

SNR = ?

coderate

$$\text{bitrate netto} = BR \cdot \frac{1}{2} = 2 \cdot 10^9 \text{ bit/s}$$

$$C = B \cdot \log_2 (1 + S/N) \Rightarrow S/N = 2^{\frac{C}{B}} - 1 = 2^{\frac{2 \cdot 10^9}{500 \cdot 10^6}} - 1 = 15$$

$$SNR = 10 \log_{10} (S/N) = 10 \log_{10} (15) = 11,76 \text{ dB}$$

3. $p = x^3 + 1 = 1001$

$$\begin{array}{r}
 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \\
 1 \ 0 \ 0 \ 1 \\
 \hline
 0 \ 0 \ 1 \ 0 \ 0 \ 1 \\
 1 \ 0 \ 0 \ 1 \\
 \hline
 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \\
 1 \ 0 \ 0 \ 1 \\
 0 \ 0 \ 0 \ 1
 \end{array}
 \Rightarrow \text{invio } 10110101001$$

4. Eth classica

3 host

- a. 4 tentativi $A \rightarrow$ collisione, $[0,1] \rightarrow$ on
- $B \rightarrow$ " , $[0,1] \rightarrow [0,1,2,3]$
- $C \rightarrow$ " , $[0,1] \rightarrow [0,1,2,3]$

b. p (frame al 2° tentativo) = $\frac{3}{8}$ $\begin{pmatrix} (0,1,1) \\ (1,0,1) \\ (1,1,0) \end{pmatrix}$

6. a. no, arriviamo a C

b. cambia dopo che si eliminano le entry

7. a. No, non sono corrette

b.	R1:	met	if	m.hop	R2:	met	if	m.hop
	10.1.0.0/23	if1		192.168.1.2		10.1.0.0/23	if1	-
	2.0/24	if0		-		10.1.2.0/24	if0	192.168.1.1
	10.1.3.0/24	if1		192.168.1.2		10.1.3.0/24	if2	-
	192.168.1.0/24	if1		-		192.168.1.0/24	if0	-
	/	if2		123.45.6		/	if0	192.168.1.1

8. a. quello pubblico di B
 b. ma va almeno aperto anche su B

9. LINK STATE (stato dei vicini a tutti)

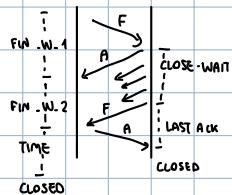
a. $LSP(B) = (A, 2), (D, 3), (C, 1) \Rightarrow A, B, C, D$
 $LSP(D) = (A, 1), (C, 1), (B, 3)$

b. B

10. a. R1, R2, RG, R5, R7
 b. R1, R3, R3, R4, R5, R6, R7

11. a. passaggio da CLOSED a LISTEN
 b. solo per il server, perché il client può usare una porta temporanea

12. a. da ESTABLISHED a CLOSE-WAIT, invia un ACK
 b. solo l'ACK finale, altri dati potrebbero essere "vecchi" ancora in circolo
 c. sì, fino a che non passa in LAST ACK



13. $v = 10 \text{ KB/s}$

$MSS = 1460 \text{ B}$

$RTT = 50 \text{ ms} = 50 \cdot 10^{-3} \text{ s}$

a. pacch: $v \cdot MSS = 10 \cdot 10^3 \cdot 50 \cdot 10^{-3} = 500 \text{ B}$ e per Neagle invia 500B di dati

b. efficienza? \Rightarrow overhead = 40B di intestaz. $\Rightarrow e = \frac{500}{540} = 92,6\%$

14.



$v_s = 1,25 \text{ MB/s}$ e 1 pacchetto (1000B) sono $\Rightarrow \frac{10^3}{1,25 \cdot 10^6} = 8 \cdot 10^{-4} \text{ s}$

$\lambda = 500 \text{ pacch/s}$
 $S = 8 \cdot 10^{-4} \text{ s/pacc}$

$$R = \frac{S}{(1 - \lambda S)} = \frac{8 \cdot 10^{-4}}{(1 - 8 \cdot 10^{-4} \cdot 500)} = 1,33 \cdot 10^{-3} \text{ s} = 1,33 \text{ ms}$$

15. a. PASSIVO, confidenzialità
 b. PASSIVO, confidenzialità
 c. ATTIVO, replay (integrità)

- blochi da 128 bit, ovvero 16B
16. AES con CBC ($C_i = (P_i \oplus C_{i-1}) \text{ C0 = IV}$).
- a. quale sezione di file va ricaricato? blocco i : da 1328 fino a 1344 \Rightarrow da 1311 a 1344
- Devo leggere il byte in posiz. 1341
- b. dal byte (1328-1344) fino all'ultimo
17. K_A : A-KDC
 K_B : B-KDC
 K : generata da A
- a. NO, è soggetta a REPLAY
- b. nel passo 3. modifica A con E (può fare solo replay)
- c. per AUT + NO REPLAY:
2. KDC \rightarrow A: $E_{K_B}(A, B, K)$
 3. A \rightarrow B: A, $E_{K_B}(A, B, K)$
18. a. ~~Si, NO~~ no era se $A \rightarrow CA: E_{PA}(idA), PIA$
- b. Si perché le cose firmate non sono modificabili
- c. $CA \rightarrow A: T, E_{PA}(A, L, H(\text{?UA}, T))$

1. $C = 3,8 \cdot 10^8 \text{ m/s}$

$d = 41 \cdot 10^3 \text{ Km} = 41 \cdot 10^6 \text{ m}$

$RTT = \frac{2 \cdot 41 \cdot 10^6}{3,8 \cdot 10^8} = 0,547 \text{ s}$

$RTT = ?$

2. $B = 1 \text{ MHz} = 10^6 \text{ Hz}$

$SNR = -30 \text{ dB}$

$SNR = 10 \log_{10} (S/N) \Rightarrow S/N = 10^{\frac{SNR}{10}} = 10^{-3}$

bitrate massimo

$C = B \cdot \log_2 (1 + S/N) = 1441,97 \text{ bit/s}$

3. Quanti simboli per bit? $\Rightarrow BR = 2B \wedge C = BR \cdot m. \text{di bit}$ $\Rightarrow \frac{BR \left[\frac{\text{band}}{\text{s}} \right]}{C \left[\frac{\text{bit}}{\text{s}} \right]} = 1387$

4. $RTS = 20B$

$CTS, ACK = 14B$

$\Rightarrow RTS + \underset{\substack{20 \\ CTS}}{10} + \underset{\substack{1500 \\ PAY}}{1500} + \underset{\substack{30 \\ HEAD}}{30} + \underset{\substack{4 \\ CRC}}{4} + \underset{\substack{4 \\ ACK}}{4} = 1582B$

 \hookrightarrow Lo manda il ricevente

$pay = 1500B$

$head = 30B$

5. turmo 1 \rightarrow collisioneturmo 2 $\rightarrow [0,1]$ A1 vince B1 becca 1turmo 3 \rightarrow invia A2

$P(A_2) = \frac{(0,0)}{\begin{pmatrix} (0,0) \\ (0,1) \\ (0,2) \\ (0,3) \end{pmatrix}} = \frac{1}{4}$

6. a. mom cambia

b. F, G

7. A: 192.168.1.190

a. 192.168.0.0/16 255.255.0.0

B: 192.168.172.5

192.168.1.190 $\Rightarrow \in A, B$

rete: 192.168.0.0

b. 192.168.0.0/24 $\Rightarrow \notin A, B$

c. 192.168.0.0/17 255.255.10000000.0

192.168.1.190 192.168.10101100.5 $\Rightarrow \in A \notin B$

rete 192.168.0.0 192.168.10...0.0

192.168.128.0

8. R2 perché mom posso arrivare alla 10.1.1.0/24

9. B - C

a. sì, magari è un rammasuglio

A

b.

10. a. SI per la tecnica del DUAL STACK
b. NO

11. PIM-SM

- a. UNICAST verso B: $2 + B-A + B-C + C-F + C-G + A-E$
b. solo UNICAST: me creo 3 da $D + D-A + A-E + B-A + B-C + C-F + C-G$

12. problema dell'INCARNAZIONE, rischio di avere vecchi pacchetti con lo stesso SeqNum.

13. NBE: 3000

--	--

 ACK = 3500
S.L.: 10000 $ADV.W = 10000 - 500 = 9500$ perché conta solo fino a NBE
4000 - 5500
3000 - 3500

14. a. indice di equità = $\frac{(\sum x_i)^2}{m \cdot \sum x_i^2} = 0,603$
b. se il flusso da 1400 termima? = 0,503, situazione è peggiorata

15. a. FALSO
b.
c. VERO

16. a. SI
b. NO
c. SI

17. a. per evitare lo scambio (e quindi le MIM)
b. P, g

18. a. HASH (pubblico) e PUs (pubblici)
b. SI
c. NO

20. a. ~~CONN SESSIONE~~
b. CONN
c. CONN
d. SESSIONE

1. a. 3
b. 12
c. 7
d. 1

2. $B = 1932 \text{ kHz}$

bitrate grezzo = 24 Mb/s

$d = 600 \text{ m}$

$$BR = 2B = 2 \cdot 1932 \cdot 10^3 \text{ baud/s}$$

$$\text{bitrate} = BR \cdot m.\text{bit} \Rightarrow m.\text{bit} = \frac{\text{bitrate}}{BR} = \frac{12 \cdot 10^3}{2 \cdot 1932 \cdot 10^3} = 6,2 \frac{\text{bit}}{\text{baud}}$$

bit per simbolo? $\left[\frac{b}{\text{simb}} \right]$

3. $S/N = ?$

$$C = B \cdot \log_2 (1 + S/N) \Rightarrow S/N = 2^{\frac{C}{B}} - 1 = 5488 \quad \text{SNR} = 10 \log_{10} (S/N) = 37,4 \text{ dB}$$

4. $p_{\text{er bit}} = 10^{-3}$

$$\begin{aligned} \text{pacchetto} &= 100 \text{ bit} \\ p(\text{err. non rilevati}) &= 1 - p(\text{err. rilevati}) \xrightarrow{\text{al max. 2}} \\ &= 1 - \left[\binom{100}{2} \cdot (p_e)^2 \cdot (1-p_e)^98 + \binom{100}{1} \cdot p_e \cdot (1-p_e)^99 + (1-p_e)^{100} \right] \\ &= 1 - 0,99998 = 1,6 \cdot 10^{-4} \end{aligned}$$

5.

RTS|SISF|CTS|SISF|HEADER + PAYLOAD + CRC|SISF|ACK|DIFS

$$100 \text{ Mb/s} \Rightarrow t_{\text{RTS}} = \frac{20 \cdot 8}{100 \cdot 10^6} = 1,6 \cdot 10^{-6} \text{ s}$$

$$t_{\text{SISF}} = 16 \cdot 10^{-6} \text{ s}$$

$$t_{\text{TOTALE}} = t_{\text{RTS}} + 3t_{\text{SISF}} + t_{\text{ACK}} + t_{\text{DIFS}} = 1,75 \cdot 10^{-4} \text{ s}$$

$$t_{\text{PAC}} = \frac{1534 \cdot 8}{100 \cdot 10^6} = 1,23 \cdot 10^{-4} \text{ s}$$

$$t_{\text{DIFS}} = 34 \cdot 10^{-6} \text{ s}$$

$$t_{\text{ACK}} = t_{\text{CTS}} = \frac{14 \cdot 8}{100 \cdot 10^6} = 1,12 \cdot 10^{-6} \text{ s}$$

6. $192.168.\underline{10101.000}.0 \Rightarrow 1/21 \text{ e ha } 2^{(32-21)-2} = 2046$

7. a. si deve essere ricalcolato passando per ogni router (visto che il checksum considera anche i router)

b. no perché i pacchetti non possono andare in loop, c'è già il circuito

8. a. si potrebbe

b. i pacchetti potrebbero perdere. Nei router intermedi o finale

9. D-V

a. A-D-E-F (4) D-E-F-C (4)

b. A-B-E-F (3) D-E-F-C (4)

10. a. AS1: AS3-AS4-N

AS2-AS4-N

b. lo rifiuta semmai creerebbe loop

11. a. UDP

b. pacchetto IGMP per fare il JOIN, che ha l'indirizzo del gruppo

12. $\alpha = 0,8$

ESTRTT = ?

$$\text{ESTRTT} = \alpha \cdot (\text{ESTRTT}) + (1-\alpha) \cdot \text{SAMPLERTT}$$

TIMEOUT = ?

$$= \alpha \cdot 50 + (1-\alpha) \cdot 80 = 56 \text{ ms}$$

$$\text{TIMEOUT} = \text{ESTRTT} \cdot 2 = 112 \text{ ms}$$

13. SeqNum = 2500 perché è il primo byte mancante. Acciato

Sono stati inviati 4 pacchetti da 1000 (partendo da 500) $\Rightarrow 500-1500-2500-3500$ e dato che non è scattato il timeout

$\Rightarrow 4500$

14. CongWi = 10000, dopo 5 ACK \Rightarrow incremento (1 ACK) = $\frac{\text{MSS}^2}{\text{cwnd}} = 196 = 196 \cdot 5 = 980$

MSS = 1400

$$\text{cwnd prima timeout} = 10980 \text{ e poi al timeout viene dimezzata} \Rightarrow \text{cwnd} = \frac{10980}{2} = 5490$$

15. a. 1, ~~5~~, 3

b. 3, ~~5~~, 6

c. 5, ~~6~~

16. OFB: a. 1bit

b. che posso ottenere due PLAINTEXT mettendo in XOR due plaintext cifrati con lo stesso Output (se uso la stessa chiave)

17. $X \cdot 509 \Rightarrow a, c$

18. a. NO b. SI c. ~~NO~~ SI

19. a. PUB b. SI e ~~NO~~ c. $B \rightarrow A : E_K(M, N)$

$A \rightarrow B : E_K(N, M)$

20. a. NO c. SI

b. NO d. NO

1. a. delay
- b. banda
- c. jitter
- d. delay, banda

2. baudrate = 1Mbaud/s

bitrate netto = 8Mb/s

bitrate grezzo = $\frac{3}{4}$ bitrate netto

$$\text{bitrate g} = \frac{\text{bitrate netto}}{\frac{\text{simb}}{3}} \cdot \frac{\text{bit simb}}{\text{simb}} \Rightarrow \frac{\text{bitrate g}}{\text{BR}} = \frac{\frac{3}{4} \cdot 8 \cdot 10^6}{2 \cdot 1 \cdot 10^6} \frac{\text{bit}}{\text{s}} = \frac{14}{2} = 7$$

↓ dato che ho due linee

m. bit per simb?

3. SNR minimo?

$$\text{BR} = 2B \Rightarrow B = \frac{\text{BR}}{2} \text{ e } \text{BR} = 2 \text{ perché ho due linee}$$

$$C = B \cdot \log_2 (1 + S/N) \Rightarrow S/N = 2^{\frac{C}{B}} - 1 = 255$$

4. pacchetti fissi : 48B pay

58 intesate

3B informaz (solo l'ultimo)

32 pacchetti (32 intesate + pay + 1 informaz)

overhead per pacchetto di 1500B

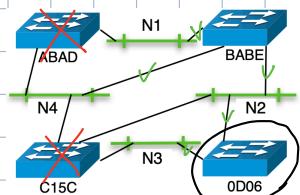
overhead = 168 B + quelli dell'ultimo 36 B non utilizzati = 204

5. $x^4 + x^2 + 1 = 10101$

$$\begin{array}{r}
 M: \quad 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 10101 \\
 \underline{1 \ 0 \ 1 \ 0 \ 1} \\
 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \\
 \underline{1 \ 0 \ 1 \ 0 \ 1} \\
 0 \ 1 \ 0 \ 1 \ 0 \ 0 \\
 \underline{1 \ 0 \ 1 \ 0 \ 1} \\
 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \\
 \underline{1 \ 0 \ 1 \ 0 \ 1} \\
 0 \ 1 \ 1 \ 0 \ 1 \ 0 \\
 \underline{1 \ 0 \ 1 \ 0 \ 1} \\
 0 \ 1 \ 1 \ 1 \ 1
 \end{array}
 \quad \Rightarrow \text{resto: } 1111$$

invio: 1011011101 **1111**

6. a. 0D06
- b. ABAD,C15C



7. 192.128.10.0/23

a. 192.128.11.0/24 \Rightarrow si perché com un bit mappa 10.0 e 11.0

b. 192.128.9.0/24 \Rightarrow No perché il bit del '2' manca (guarda se la parte network è uguale)

c. 192.128.10.0/22 \Rightarrow ~~Si~~ NO

d. 192.128.10.128/25 \Rightarrow Si

8. a. consegnato sulla rete per R2

b. ciclo tra R1 e R2

9. RIP \Rightarrow Distance V.

a. met cost next hop

A	3	E
C	4	E
D	1	D
E	1	E

b. met cost next hop

A	3	E
C	4	E
D	∞	-
E	1	E

~~D~~ \Rightarrow ~~∞~~ - riceve l'update da A $\Rightarrow 4+5=9$

10. IPv6 ha 128 bit perciò se /64 allora ho 64 bit di host, perciò per costruirli uso i 48 bit di MAC e i restanti li setto a 0

11. UDP

V consumo = 10 datagram/s

payload = 1KB

$\frac{16 \cdot 10^3 \text{ byte}}{5 \text{ s}} = 3200 \text{ B/s}$ per riempire in 5 secondi senza che consumi

buffer = 16 KB

quanto deve inviare per saturare in 5 secondi?

in 5 secondi consuma $\Rightarrow 50 \text{ KB}$, quindi $10 \text{ KB/s} + 3200 \text{ B/s} = 13,2 \text{ KB/s}$

12. a. CLOSE_WAIT

b. Si, se è l'ultimo di B, si porta in TIME_WAIT

14. FQ

A1 = 5 A2 = 7 A3 = 2

B1 = 4 B2 = 11

a. ordine: B1, A1, C1, A2, A3, B2, C2

C1 = 9 C2 = 6

b. quando termina A3: 27

Time: A1 = 5 A2 = 12 A3 = 14

B1 = 4 B2 = 15

C1 = 9 C2 = 15

15. a. ATTIVO, DISPONIBILITÀ

c. ATTIVO, INTEGRITÀ

b. ATTIVO, INTEGRITÀ

d. PASSIVO, CONFIDENZIALITÀ

16. a. simmetrica

b. confidenzialità, integrità, controllo di accesso

$$\frac{Y_A}{Y_B}$$

17. 1. $A \rightarrow B : Y_A, N_A$

2. $B \rightarrow A : Y_B, N_B, ??$

3. $A \rightarrow B : ??$

2. $B \rightarrow A : Y_B, N_B, E_K(N_A, Y_B) H(K, N_A, Y_B)$

3. $A \rightarrow B : H(K, N_B, Y_A)$

18. a. Si

b. No

c. Si

19. a. Si

b. No

c. Si

1. controllo congestione e demultiplexing a livello di applicazione

inoltre bisogna gestire l'ordine dei pacchetti e la connessione tra modi ed interfacce

2. $V = 200.000$ stati/sec

MANCHESTER \Rightarrow coderate = $\frac{1}{2}$

con 200.000 stati codifica 100.000 bit \Rightarrow bitrate = 100 kb/s

Br = ?

ci vogliono 2 stati per un cambiamento

e BAUD = BIT \Rightarrow BAUDRATE = 100 KBAUD/s

3. 15 simboli a pacchetto \Rightarrow $\frac{11 \text{ dati}}{4 \text{ parità}}$ FEC

BAUDRATE $\cdot \frac{11}{15} = 73,3$ KBAUD/s

e BITRATE = BAUDRATE \cdot n. bit \downarrow simbolo = 73,3 kb/s

bitrate metto ?

4. $pe = 10^{-6}$

FRAME = 1000 B = 8000 bit

$p(\text{frame scartato}) = ?$

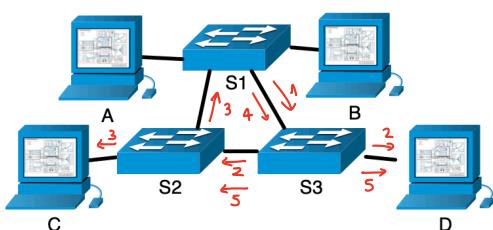
consegna fino a 2 bit errati

$$\begin{aligned} p(\text{scarto}) &= 1 - p(\text{non scarto}) \\ &= 1 - [p(0 \text{ errori}) + p(1 \text{ err}) + p(2 \text{ err})] \\ &= 1 - [(1-p)^{8000} + \binom{8000}{1} \cdot pe \cdot (1-pe)^{7999} + \binom{8000}{2} \cdot pe^2 \cdot (1-pe)^{7998}] \end{aligned}$$

5. garantisce la FAIRNESS, essendo a divisione di tempo, però uno svantaggio è che si sfrutta meno la banda.

→ attribuendo molte copie

6. si, lo riceviamo anche \Leftarrow (una sola copia)



La rete a lato è composta da switch ad autoapprendimento, S1 ha completato la fase di apprendimento mentre S2 e S3 sono appena stati resettati. L'host A invia un frame all'host D. Tale frame raggiunge D? Ci sono altri host che ricevono tale frame? In quante copie?

7. 192.168.1.0/24 ha 254 indirizzi disponibili per host

per vedere se $192.168.1.128/27 \in 192.168.1.0/25$

192.168.1.1~~0~~xxxxxx
CIDR HOST

192.168.1.100xxxxx
CIDR HOST

AND: 192.168.1.128

$\Rightarrow 192.168.1.128/25$, quindi non appartiene

sub(25) 255.255.255.10000000

quindi ho 192.168.1.0/24

192.168.1.0/25
(255.255.255.0xxxxxx)

↳ ho già usato: $2^7 - 2 = 126$

192.168.1.128/25
(255.255.255.1xxxxxx)

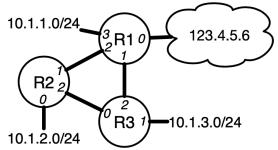
↳ di questa ho usato solo la 192.168.1.128/23
(255.255.255.100xxxxx)

e posso usare ancora
 $\hookrightarrow 2^5 - 2 = 30$

→ non considero .000 perché il primo bit (0) è .001 uguale a quella 1.0
101 $\Rightarrow 2^5 - 2 = 30$
110 $\Rightarrow 2^5 - 2 = 30$
111 $\Rightarrow 2^5 - 2 = 30$

\Rightarrow ho ancora liberi: 90
192.168.1.160/27
192.168.1.27/27
224.27

8.	met	ip	next hop
10.1.2.0/24	0	-	
10.1.3.0/24	2	192.168.1.1	
/	2	192.168.1.2	
4 ingloba anche .1.1.0			



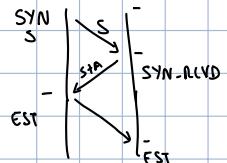
9. D-V

a.	met	cost	m. hop
B	3	B	
C	1	C	

b.	met	cost	m. hop
B	3	B	
C	1	C	
D	4	C	

10. Mi riattacco ad un altro AS di transito e non serve cambiare indirizzo

11. un Sequence Number



12. Client: ESTABLISHED
Server: SYN-RCVD

Ma, se un client invia il 1° pacchetto dati allora il server capisce che il client aveva già inviato un Ack

13. SeqNum = 5000 Ack = 4000 ADVERTISED WINDOW = $1000 + 1500 = 2500$
Length = 1500

14. RED

MIN = 10KB arriviamo 2KB, 3KB, 2KB. Quale è prob. che vengano tutti accreditati?

MAX = 20KB

$$p(2KB) = 1 \text{ perché } \text{arglem} < \text{MIN} \Rightarrow \text{ora Arglem} = 11KB$$

$$p(3KB) = \frac{\text{Arglem} - \text{MIN}}{\text{MAX} - \text{MIN}} = \frac{14 - 10}{20 - 10} = 0,4 \Rightarrow \text{ora Arglem} = 14KB$$

$$p(\text{tot}) = 0,6 \cdot 0,9 = 0,54 \Rightarrow 54\%$$

$$p(2KB) = \frac{\text{Arglem} - \text{MIN}}{\text{MAX} - \text{MIN}} = 0,4$$

15. integrità con la firma
disponibilità tengo le cose sotto chiave

16. ogni 2^m giri i si ripete, perciò posso memorizzare con la chiave k 2^m messaggi

17. No perché c'è la chiave dentro l'hash assieme alle due metà chiavi

19. 1. A → B : M

2. B → A : T

3. A → B : ~~M, T~~, E_{RA}(H(M, T))

1. a. TRANSPORT (TCP)
- b. DATA LINK
- c. PRESENTAZIONE
- d. TRANSPORT

→ segnale pulito

2. potenza = 14 mW

rumore = 0,2 mW

$$S/N = \frac{\text{potenza}}{\text{rumore}} = \frac{14}{0,2} = 70$$

C = 16 Mb/s

B = ?

$$C = B \log_2 (1 + S/N) \Rightarrow B = \frac{C}{\log_2 (1 + S/N)} = \frac{16 \cdot 10^6}{\log_2 (71)} = 2,6 \text{ MHz}$$

3. $x^3 + x^2 + 1 \Rightarrow 1101$

$$\begin{array}{r}
 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1101 \\
 1 \ 1 \ 0 \ 1 \\
 \hline
 0 \ 1 \ 1 \ 0 \ 0 \\
 1 \ 1 \ 0 \ 1 \\
 \hline
 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \\
 1 \ 1 \ 0 \ 1 \\
 \hline
 0 \ 0 \ 1 \ 1 \ 0 \ 1 \\
 1 \ 1 \ 0 \ 1 \\
 \hline
 0
 \end{array}
 \Rightarrow \text{il resto è 0, è corretto}$$

4. delay switch = 10 μs

IPG = 96 bit \rightarrow NON SERVE perché no collisioni

bitrate grezzo = 100 Mb/s

payload = 1500B

intestaz = 26B

trasmetto A \rightarrow SWITCH e SWITCH \rightarrow B e ogni volta è: FRAME: IPG + INT + PAYLOAD + CRC

$$A \rightarrow \text{SWITCH} : \frac{1526 \cdot 8 + 96}{100 \cdot 10^6} = 1,23 \cdot 10^{-4} \text{ s}$$

$$S \rightarrow A : 1,23 \cdot 10^{-4} \text{ s}$$

$$t_{\text{TOTALE}} = 2t_{A \rightarrow \text{SWITCH}} + \text{delay} = 2 \cdot 1,23 \cdot 10^{-4} + t_{\text{DELAY}} = 2,56 \cdot 10^{-4} \text{ s}$$

5. bitrate master = $\frac{483}{10^{-6} \cdot 615 \cdot 2} = 772800 \text{ bit/s} = 386400 \text{ bit/s}$

6. a. IP₁: 192.168.5.9 \Rightarrow guardo dal binario fino a dove sono uguali \Rightarrow 192.168.0.0/22

IP₂: 192.168.6.14

$$\begin{array}{r}
 8 \ 8 \\
 192.168.0.00000101.9 \\
 192.168.0.00000110.14
 \end{array}$$

7. met if m.hop

158.110.2.0/23	if2	10.0.1.1	3 \rightarrow 10.1 2 \rightarrow 10.0
158.110.0.0/23	if1	-	
158.110.0.0/23	if0	12.3.4.5	

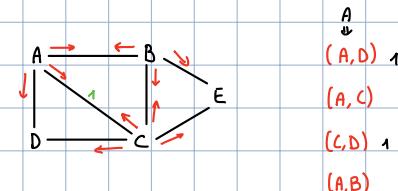
8. A \rightarrow NAT(B)

Non viene mantenuta perché il NAT mappa [IP pubblico A, porta A, IP privato B, porta B, protocollo] e se B ricontatta A si crea una nuova comunicazione.

	dest	cost	methop
A	1	A	
B	2	A	
C	1	C	
D	0	-	
E	C	3	

	dest	cost	methop
A	1	A	
B	2	A	
C	1	C	
D	0	-	
E	C	3	

me assevoamo B (da A e C) ma me accetta 4.



e simmetrico per
C

$\Rightarrow 4+4=8$ e me accetta 2

(B,C) \rightarrow B lo scatta

(C,B)

(B,E)

(E,C)

(C,D) 2

10. PIM in SPARSE MODE

- a. D,A,B
- b. B,E,C

11. a. ^{UDP} TCP è richiesto sincronismo \Rightarrow CLOCK

b. ^{TCP} UDP non è richiesto una commessione / controllo di flusso \Rightarrow MAIL

c. UDP " " , si appoggia su IP \Rightarrow DHCP

12. TCP com EST.

- a. ad esempio la chiusura della commessione
- b. FIN_WAIT_1
- c. CHIUSURA ATTIVA

13. $7000 - 1400 = 5600$

14. slow start e fast retransmit

cwnd = 1mss

a. vai avanti fino a quando arrivi a ssthresh. Perciò fai 5 round

ssthresh = 32mss \rightarrow lo setti anche all'inizio

b. al meno round \Rightarrow cwnd = $32 + 4 = 36$ e poi al decimo ssthresh = $\frac{36}{2} = 18$ mss

15. a. integrità metadati

b. confidenzialità dati e metadati

c. disponibilità dati

16. a. SI

b. SI

c. NO

17. a. SI

b. no perché potrebbe cambiare l'orologio

c. ~~SI~~ no può essere modificato

18. SI, perché non c'è autenticazione