

**LINK STATE**: info dei vicini a tutti

→ **RELIABLE FLOODING**: inviato a tutti i vicini tranne quelli da cui ricevo e ogni LSP ha un SeqNum (ID router che lo genera, SeqNum), così forward solo verso i pacchetti nuovi. Il SeqNum lo incrementa solo la sorgente quando genera un nuovo pacchetto. Scarta i pacchetti vecchi e quelli già forwardati.

→ **DIJKSTRA**: una volta che tutti i nodi hanno tutti i collegamenti salvati, calcolo con Dijkstra i cammini minimi

mon viene mai cambiato dai router intermedi

stessa coppia. (idA, seq1) (idA, seq1)

**DISTANCE VECTOR**: info di tutti ai vicini

→ ogni vicino mi invia  $v$  (Dest, Cost, N.hop) → non serve il next hop perché inizialmente invia solo i vicini se io passo già per il vicino per arrivare a  $x$  → aggiorno il costo se il costo passando per il vicino " è minore di quello attuale (next hop ≠ vicino) → cambio next hop

→ problema dell'infinito count: se si rompe un collegamento tra due nodi ed uno dei due non è più raggiungibile

$A \xrightarrow{1} B \xrightarrow{2} C$

$B \rightarrow C : A +\infty A$

$C \rightarrow B : A 3 B$

allora  $B$  aggiorna  $A 3+2 C$  e invia a  $C \Rightarrow$  risolto con **FINITE-INFINITE** (max. 15 hop)  
allora  $C$  aggiorna  $A (3+2)+2 B \dots B$

**PIM SPARSO**: approccio GROUP-SHARED con Rendezvous Router, NON VINCOLATO all'algo UNICAST

→ Ogni host che vuole aggiungersi al gruppo manda una join verso RP seguendo il cammino minimo se un router riceve il pacchetto, lo gira all'RP e aggiunge nella sua tabella l'indirizzo del router chi vuole trasmettere invia un UNICAST al router RP (=incapsulamento) e poi lui invia sull'albero multicast

**DVMRP**: deve avere DISTANCE-VECTOR come unicast

→ tecnica REVERSE PATH FLOODING: inviato i pacchetti multicast a tutti i miei vicini (escluso chi me lo manda) e accetto SOLO dal NEXT HOP verso la sorgente.

**SWITCHING**: if (MAC.dest ∈ TABLE)

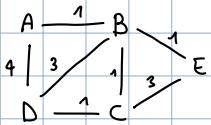
    imoltro su interfaccia if output

else

    flooding (tramme sulla porta su cui ricevo)

if (MAC.mittente ∈ TABLE)

    salvo che su if input c'è MAC.mittente

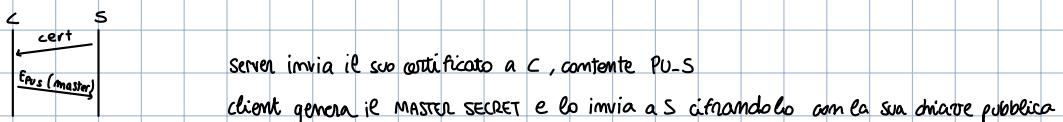


L.S.:  $D \rightarrow A$   $C \rightarrow B$   $B \rightarrow E$   
 $D \rightarrow B$   $C \rightarrow E$   $B \rightarrow D$   
 $D \rightarrow C$   $B \rightarrow A$

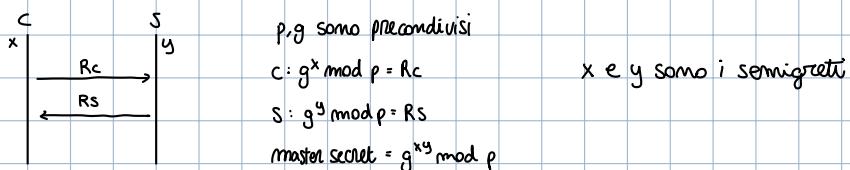
DVMRP:  $D \rightarrow A$   $C \rightarrow B$   $B \rightarrow E$   $A \rightarrow D$   
 $D \rightarrow B$   $C \rightarrow E$   $B \rightarrow D$   
 $D \rightarrow C$   $B \rightarrow A$   $E \rightarrow C$

**RSA**  
AUTENTICAZIONE in SSL  
D.H. ANONIMO  
D.H. FISSATO  
D.H. EFFIMERO

**RSA**: client non autenticato, server è autenticato (con x.509)

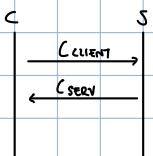


**D-H ANONIMO**: nessuno dei due è autenticato



**D-H fissato**: sia il server che il client hanno un certificato

si inviano i loro certificati, e ogni certificato contiene  $R$   $\Rightarrow C_c = (id_c, id_{ca}, h, \dots, R_c)$   
 $C_s = (id_s, id_{ca}, h, \dots, R_s)$

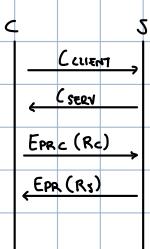


uso i certificati per decidere le chiavi.

nei certificati ho sempre lo stesso numero, è autenticato da me, ma è sempre lo stesso  
 $\hookrightarrow$  valgono per più sessioni.

**D-H effimero**: sia il server che il client hanno un certificato

simile al D-H statico, ma più sicuro in quanto il numero usato per generare il master secret cambia ogni volta  $\Rightarrow$  non è fisso



e  $R_c, R_s$  vengono generati ad ogni sessione, non sono associati ai certificati (che sono fissi)

## ESERCIZI ESAMI

28.01.2019

2. Si vuole realizzare una linea di trasmissione della capacità di 1 Mb/s di bitrate di dati senza errori, utilizzando un fascio di microonde in una banda di frequenza centrata a 10 GHz e di larghezza 500 kHz. Determinare il rapporto segnale/rumore (in dB) della linea in tali condizioni.

$$\text{uso Shannon: } C = B \log_2 \left( 1 + \frac{S}{N} \right)$$

$$\Rightarrow 10^6 = 500 \cdot 10^3 \log_2 \left( 1 + \frac{S}{N} \right) \Rightarrow \frac{10^3}{500} = \log_2 \left( 1 + \frac{S}{N} \right) \Rightarrow 2^{\frac{10^3}{500}} - 1 = \frac{S}{N} \Rightarrow \frac{S}{N} = 2^{\frac{1000}{500}} - 1 = 3$$

e poi  $\frac{S}{N}$  lo converto in decibel  $SNR = 10 \log_{10} (3) = 4,7 \text{ dB}$

3. Sulla linea di trasmissione dell'esercizio precedente, viene utilizzato un Forward Error Coding che codifica 12 bit in pacchetti di 24 bit. Determinare il numero minimo di bit che deve venir codificato da un simbolo per baud, per avere un bitrate netto di 1 Mb/s.

quindi 2 Mb/s dato che 50% dei dati è sprecato (su 24 bit solo 12 sono di dati)

per Nyquist-Shannon abbiamo che  $R = 2B$  banda [Hz], quindi  $R = 500 \cdot 10^3 \cdot 2 = 10^6 = 1 \text{ Mbaud}$  simboli al sec [sym/s]

e quindi se voglio avere un bitrate effettivo di 1 Mb/s  $\Rightarrow \frac{2 \text{ Mbit/s}}{1 \text{ Mbaud}} = \frac{2 \text{ Mb}}{8 \text{ sym}} = 2 \text{ bit per simbolo}$

4. Una certa linea ha una probabilità di errore  $p = 10^{-3}$  per ogni bit. Prima della trasmissione ogni 3 bit viene aggiunto un bit di parità. Qual è la probabilità che in un pacchetto di 4 bit così formato avvengano degli errori non rilevati?

gli errori NON RILEVABILI sono se ci sono errori in numero pari  $\rightarrow 0, 2, 4$

$$p(2 \text{ errori}) = \underbrace{p^2 \cdot \binom{4}{2}}_{\text{2 errati}} \cdot (1-p)^2 = 10^{-6} \cdot \binom{4}{2} \cdot (1-10^{-3})^2$$

$$p(4 \text{ errori}) = p^4$$

$$p(\text{TOTALE}) = p(2 \text{ errori}) + p(4 \text{ errori}) = p^2 \binom{4}{2} (1-p^2) + p^4 = 5,99 \cdot 10^{-6}$$

5. Due stazioni Ethernet A e B hanno già tentato di trasmettere una volta, rilevando collisione. Al secondo tentativo, anche una terza stazione C prova a trasmettere (per la prima volta). Qual è la probabilità che la trasmissione avvenga senza collisioni?

in generale dopo  $m$  collisioni l'algoritmo sceglie  $K$  ( $K$  slottime è il tempo che aspetta ciascuno che riceva collisioni) in un range che varia da  $0 \dots 2^m - 1$

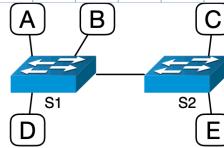
$$m = 0, 1; \text{ quindi } 2 \text{ tentativi}$$

$\Rightarrow$  range:  $0 \dots 1$  perciò C, dato che è appena arrivato non attende e gli altri non devono aspettare 0.

$$\frac{1}{2} \text{ perché o becca 0 o becca 1}$$

$$p(A=1) \cdot p(B=1) = \frac{1}{4}$$

6. Nella rete a lato, gli switch S1 e S2 sono ad autoapprendimento. S2 ha le tabelle completamente popolate, mentre S1 è appena stato resettato. L'host A invia un frame indirizzato a C. (a) A quali host viene recapitato tale frame? (b) Se C risponde ad A, il suo frame a chi viene recapitato?



non E perché lo switch 2 direziona a C

- (a) B, C, D ↑ perché lo switch 1 ha la sua tabella vuota e anche se A ha le MAC di C, lo switch S1 non ha la "mappa di rete"  
 (b) solo ad A perché S1 sa dove ora A quando A ha mandato un messaggio

7. Un'azienda ha tre reti A, B, C con 100, 300 e 200 postazioni rispettivamente. Per ognuna di queste reti si dia una sottorete (minima) all'interno della rete 192.168.0.0/16.

16 bit di parte Host e 16 bit di parte Network

$2^{16}$  host in totale = 64k host

100 host $\rightarrow$ 7 bit	$32 - 7 = 25$ bit NETWORK	$\rightarrow 192.168.0.0/25 \rightarrow 192.168.0.0 - 192.168.0.128$	raff. della rete	ind. broadcast
300 host $\rightarrow$ 9 bit	$\Rightarrow 32 - 9 = 23$ "	$\rightarrow 192.168.0.129/23 \rightarrow 192.168.0.129 - 192.168.0.255 + 192.168.1.0 - 192.168.1.255 + 192.168.2.0 - 192.168.2.129$	raff. della rete	
200 host $\rightarrow$ 8 bit	$32 - 8 = 24$ "	$\rightarrow$		è un host

No, prendi reti separate !!

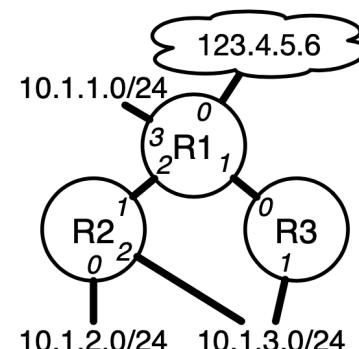
100 host $\rightarrow$ 7 bit	$32 - 7 = 25$ bit NETWORK	$\rightarrow 192.168.0.0/25 \rightarrow 192.168.0.0 - 192.168.0.128$	raff. della rete	ind. broadcast
300 host $\rightarrow$ 9 bit	$\Rightarrow 32 - 9 = 23$ "	$\rightarrow 192.168.2.0/23 \rightarrow 192.168.2.0 - 192.168.2.255 + 192.168.3.0 \dots 192.168.3.255$	raff. della rete	host
200 host $\rightarrow$ 8 bit	$32 - 8 = 24$ "	$\rightarrow 192.168.1.0/24 \rightarrow 192.168.1.0 - 192.168.1.255$		

11111111.11111111.11111110.00000000  $\Rightarrow$  255.255.254.0 e poi faccio AND con IP per vedere la rete

8. Si dia la tabella di inoltro del router R3 della rete a lato, sapendo che le interfacce dei router hanno i seguenti indirizzi:

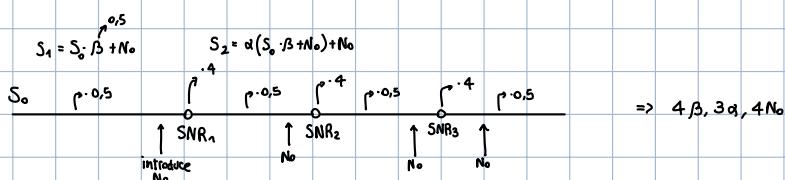
R1:if1=192.168.1.1 R2:if0=10.1.2.1 R3:if0=192.168.1.2  
 R1:if2=192.168.2.1 R2:if1=192.168.2.2 R3:if1=10.1.3.2  
 R1:if3=10.1.1.1 R2:if2=10.1.3.1

R3	DEST	IF	NEXT HOP
	10.1.3.0/24	1	/
	10.1.2.0/24	1	10.1.3.1
	*/*	0	192.168.1.1



1. (3pt) Al tempo  $t_0 = 0$  un'antenna inizia a inviare a velocità  $c = 2.5 \cdot 10^8$  m/s un segnale sinusoidale  $s(t) = A \sin(2\pi f t)$  di frequenza  $f = 10$  MHz verso una seconda antenna, posta a distanza  $d = 10$  km dalla prima. Si calcoli il primo istante  $t_1$  successivo a  $t_0$  in cui il segnale si annulla nel minor numero di punti appartenenti allo spazio tra le due antenne (incluse). Si conti anche il numero di punti in cui, nel medesimo istante  $t_1$ , il segnale  $s(t)$  è nullo.

2. (3pt) Un cavo per la trasmissione di segnali possiede un fattore di attenuazione  $\beta = 0.5$  e contemporaneamente introduce un rumore medio di potenza  $N_0$ , misurata all'uscita del cavo. Si crea un canale giungendo 4 cavi di questo tipo attraverso tre amplificatori ideali (uno per giunzione), ciascuno avente un fattore di amplificazione uguale a  $\alpha = 4$ . Detto  $SNR_i$  il rapporto segnale/disturbo all'uscita dell' $i$ -esimo cavo (prima dell'amplificatore), quanto vale il rapporto  $SNR_1/SNR_4$ ?



$$SNR = \frac{S}{N} \Rightarrow SNR_1 = \frac{S_0 \cdot \beta}{N_0} \quad SNR_2 = \frac{S_0 \cdot \alpha \cdot \beta^2}{\alpha \beta N_0 + N_0} \quad SNR_3 = \frac{S_0 \cdot \alpha^2 \cdot \beta^3}{\alpha \beta (\alpha \beta N_0 + N_0) + N_0} \quad SNR_4 = \frac{S_0 \cdot \alpha^3 \cdot \beta^4}{\alpha \beta (\alpha \beta (\alpha \beta N_0 + N_0) + N_0) + N_0}$$

$$\frac{S_0 \cdot \beta}{N_0} \cdot \frac{\alpha \beta (\alpha \beta (\alpha \beta N_0 + N_0) + N_0) + N_0}{S_0 \cdot \alpha^3 \cdot \beta^3} = \frac{15}{8}$$

3. (3pt) Nel caso particolare in cui nel canale precedente entri un segnale di potenza  $P_0$  tale che  $P_0 = N_0$ , detta  $C_i$  la capacità del canale all'uscita dell' $i$ -esimo cavo (prima dell'amplificatore), si calcolino i rapporti  $C_2/C_1$ ,  $C_3/C_1$  e  $C_4/C_1$ , motivando sinteticamente l'andamento della successione di valori trovati.

$$C_i = B \cdot \log_2 (1 + SNR_i)$$

$$\frac{C_2}{C_1} = \frac{B \cdot \log_2 \left( 1 + \frac{S_0 \cdot \alpha \cdot \beta^2}{\alpha \beta N_0 + N_0} \right)}{B \cdot \log_2 \left( 1 + \frac{S_0 \cdot \beta}{N_0} \right)} = \frac{\log_2 \left( 1 + \frac{S_0 \cdot \alpha \cdot \beta^2}{N_0 (\alpha \beta + 1)} \right)}{\log_2 (1 + \beta)} = \frac{\log_2 \left( 1 + \frac{\frac{1}{4} \cdot \frac{1}{4}}{\left( \frac{1}{2} \cdot \frac{1}{2} + 1 \right)} \right)}{\log_2 \left( \frac{3}{2} \right)} = \frac{\log_2 \left( \frac{4}{3} \right)}{\log_2 \left( \frac{3}{2} \right)}$$

$$\frac{C_3}{C_1} = \frac{B \cdot \log_2 \left( 1 + \frac{S_0 \cdot \alpha^2 \cdot \beta^3}{\alpha \beta (\alpha \beta N_0 + N_0) + N_0} \right)}{B \cdot \log_2 \left( 1 + \frac{S_0 \cdot \beta}{N_0} \right)} = \frac{\log_2 \left( 1 + \frac{\frac{1}{16} \cdot \frac{1}{16}}{\left( \frac{1}{4} \cdot \frac{1}{4} + 1 \right)} \right)}{\log_2 \left( \frac{3}{2} \right)}$$

1. a. LORA MODULATION = PHY

LORAWAN MAC = D.L., NETWORK

b. nel lora MODULATION

2.  $B = 10 \text{ kHz} = 10^4 \text{ Hz}$ a. Determina SNR minimo per bitrate =  $100 \text{ Kb/s} = 10^5 \text{ bits/s}$  senza errori

$$C = B \cdot \log_2 \left( 1 + \frac{S}{N} \right) \Rightarrow \frac{C}{B} = 2^{\frac{S}{B}} - 1 = 2^{\frac{10^5}{10^4}} - 1 = 1023 \quad \text{SNR} = 30 \text{ dB}$$

b. Si usa una FEC con code rate = 0,5. Determina il num. minimo di bit codificati in un BAUD

io so che  $C = BR \cdot \log_2 (N \text{ simboli})$  e dato che al max  $BR = 2B = 2 \cdot 10^4 \text{ Hz}$ 

$$\text{allora } N \text{ simboli} = 2^{\frac{C}{BR}} = 2^{\frac{10^5}{2 \cdot 10^4}} = 32 \quad \text{No}$$

3. linea aggiunge 1 bit di parità ogni 4 bit  $\Rightarrow 5 \text{ bit e 4 utili}$ 

$$p(e_{\text{bit}}) = 10^{-3}$$

 $\begin{array}{c} \vdash \vdash \vdash \vdash \\ \uparrow \\ \text{XOR} \end{array}$ 

a. prob che un pacchetto con almeno 1 errore venga accettato corretto? (su 5bit NON 4)

$$p(2 \text{ errori}) + p(4 \text{ errori}) \rightarrow p(2 \text{ errori}) = \frac{4}{6} \cdot (p_e)^2 \cdot (1-p_e)^2 \quad p(2 \text{ errori}) = \frac{5}{6} \cdot (p_e)^2 \cdot (1-p_e)^3$$

~~$\frac{1}{6} \cdot (p_e)^2 \cdot (1-p_e)^2$~~

$$p(4 \text{ errori}) = 5 \cdot (p_e)^4 \cdot (1-p_e)$$

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

$$C = 100 \text{ Mb/s} = 100 \cdot 10^6 \text{ bit/s}$$

a. Quanto grande il buffer trasmettente (SWS) per sfruttare il canale completamente?

SL.WINDOW

per sfruttare a pieno, SWS: throughput  $\cdot$  RTT =  $10 \cdot 10^6 \text{ bit/s} \cdot 10 \cdot 10^{-3} \text{ s} \cdot 100 \cdot 10^6 \text{ bit} = 100 \cdot 10^4 \text{ bit}$ 

5. frame BLUETOOTH

$$1 \text{ slot} = 483 \text{ bit}$$

a. bitrate massimo del flusso audio?

$$t_{\text{slot}} = 625 \text{ ms} = 625 \cdot 10^{-3} \text{ s}$$

$$\frac{483}{625 \cdot 10^{-3}} = \frac{x}{1s} \Rightarrow x = \frac{483}{625 \cdot 10^{-3}} = 772800 \text{ bit/s} \quad \text{ma essendo che trasmette in slot pari}$$

$$\text{bitrate} = \frac{x}{2} = 386400 \text{ bit/s}$$

6. a. costruisci il circuito, garanzia di arrivo, memo overhead

b. la commutaz. di pacchetto

7. A: 184.85.16.0/22

B: 184.85.16.0/24

C: 184.85.16.0/26

a. chi ha più indirizzi?  $\rightarrow$  A perché ha  $2^{10} - 2$  ind. host

b. a quale appartiene 184.85.19.15

$$A: \text{Subnet: } \overbrace{1 \dots 1}^8 \overbrace{1 \dots 1}^8.11111100.00000000$$

|P: 184.85.00010011. 15 => EA

Prete: 184.85.00010000. 0  
↓  
16

|P: 184.85.00010011. 15

.000 10011.  
↓  
19

$$C: \text{Subnet: } \underbrace{1\dots 1}_{8}, \underbrace{1\dots 1}_{8}, 11111111.11000000 \Rightarrow \text{q.c.}$$

IP: 184.85.00010011.00010001

.000 10011. 0  
    ↓  
    19

c. E l'indirizzo 184.85.16.200

A: Subnet:  $\overbrace{1...1}^8 \overbrace{.1...1}^8.11111100.00000000$

IP: 184.85.00010000. 200 => EA

Prete: 184.85.00010000. 0  
↓  
16

$$B: \text{ Subnet: } \frac{8}{1.1.1.1.1.1.1.1.0.00000000} \Rightarrow \in B$$

|P: 184. 85.00010000. 200

.000 1 0000. 0  
↓  
16

$$C: \text{Subnet: } \overbrace{1 \dots 1}^8. \overbrace{1 \dots 1}^8.11111111.11000000 \Rightarrow \notin C$$

|P: 184.85.00010000.11 001000

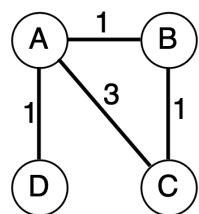
.000 1 0000. 11 000000  
    ↓    ↓  
    16    197

8. host: 185.84.31.8 → ARP req. a 185.84.31.5

Sottocrete: 185.84.31.0/29

- a) IP dest: BROADCAST
  - b) MAC dest
  - c) l'host man è raggiungibile

9. DISTANCE VECTOR → inf. di tutti ai vicini  
con split-h.p.reverse



a) tabella forw. di A

mode cost next hop

A	0	/
B	1	B
C	2	B
D	1	D

b) che vettore dist. invia B ad A

mode cost next hop

A	$\infty$	A
B	0	/
C	1	C
D	$\infty$	A

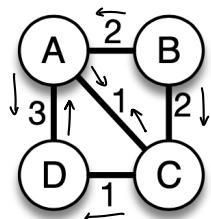
10.

router usano DVMRP

B è il CORE ROUTER

a) quanti pacchetti arrivano in flooding a D?

1. arriva da C che è il next hop verso B  
2 arriva da C e da A

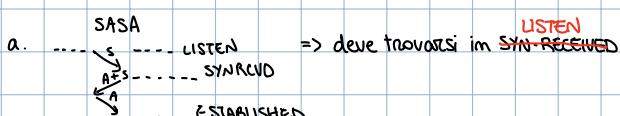


b) quello da C viene imoltrato ad A

11. app C su host A invia dati con UDP ad app S su host B

- NON è detto che arrivino in ordine
- l'ordine può essere variabile, dipende dal percorso → non c'è riordinamento!
- si, nel caso in cui la coda è piena viene scaricato

12. host TCP riceve SYN=1, SeqNum=1343



Un host TCP riceve su una certa porta un segmento con SYN=1, SeqNum=1343. (a) In che stato deve trovarsi la socket affinché venga inviato un segmento con SYN=1, in risposta al precedente? (b) Cosa viene inviato in risposta, se la socket associata a quella porta è nello stato CLOSED? (c) E se non c'è nessuna socket associata a quella porta?

- SYN=1 ACK=1344 o RST segment
- RST segment

### 13. socket TCP

MAXSENDBUFFER = 10000Byte

in un certo istante: LASTBYTWRITTEN = 8000

LAST BYTE ACKED = 2000

LAST BYTE SENT = 7000

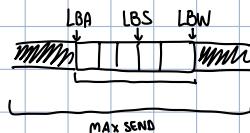
a. quanti byte può spedire ancora alla contraparte?

ADV.WIND. = MAXSENDBUFFER

EFFECTIVE WIND. = ADV.WIND. - (LBS - LBA) = 5000

b. se ADV.WIND. = 0, quanti byte può ancora produrre l'applicaz. che usa la socket, senza bloccarsi?

↳ non consuma, quindi lo spazio è MAXSENDBUFFER - (LBS - LBA) = 4000



### 14. RED sui router

MINTH = 20KB

MAXTH = 60KB

$p(\text{PACCHETTO 1}) = 1$  perché coda < MINTH  $\Rightarrow$  ora la coda contiene 21KB

all'istante  $i$ , la coda contiene 18KB. arrivano 3 pacchetti di 3KB.

prob. che tutti e 3 vengano accodati?

$\bar{p}(\text{PACCHETTO 2}) = \frac{21-20}{60-20} = \frac{1}{40}$  che venga scaricato  $\Rightarrow p(\text{pacch2}) = \frac{1}{40} \Rightarrow$  ora la coda contiene 24

$\bar{p}(\text{PACCHETTO 3}) = \frac{24-20}{60-20} = \frac{1}{10}$  che venga scaricato  $\Rightarrow p(\text{pacch3}) = \frac{1}{10}$

$p(3 \text{ pacchetti}) = \frac{39}{40} \cdot \frac{1}{10} = 87.8\%$

15. a. sì, in quanto soltanto l'header di trasporto rimane in chiaro

b. no, quella è in chiaro

c. Sì in quanto l'indirizzamento è in chiaro ed i router indirizzano a liv. 3

16. flusso  $M_1, M_2, \dots$  cifrato con AES:  $C_i = (i, \underline{\text{AESK}(i)} \oplus M_i)$  AES è crittografia a BLOCCHI

K chiave precondivisa

Se  $M_i$  è più lungo di 128 bit, si ripete lo XOR  $\text{AESK}(i)$  lungo tutto  $M_i$

a.  $C_i = i, \underline{\text{E}}_K(i) \oplus M_i$ , considero  $C_i = i, R$  con  $R = \underline{\text{E}}_K(i) \oplus M_i$

prendo  $i$ , calcolo  $\text{E}_K(i)$  e poi faccio  $\text{E}_K(i) \oplus R = M_i$

b. ~~no~~ perché con la crittografia garantisce l'integrità

R: (a) se  $C = i, R$ , allora  $M_i = E_K(i) \oplus R$ . (b) Sì, perché posso spostare/togliere/duplicare blocchi di 128 bit all'interno dello stesso messaggio e la decifratura ha successo lo stesso. In pratica è come se usassimo AES in modo ECB.

1. a. HALF DUPLEX (Eth classica) → due persone non posso inviare contemporaneamente.  
 b. FULL DUPLEX (Eth switch)  
 c. ~~POX~~ DUPLEX (WiFi) → due persone non posso inviare contemporaneamente.  
 d. FULL DUPLEX (piccioni)

2.  $B = 3 \text{ kHz} = 3 \cdot 10^3 \text{ Hz}$

SNR = 30 dB

$$C = B \cdot \log_2 \left( 1 + \frac{S}{N} \right)$$

bitrate massimo = ?

$$\text{SNR} = 10 \log_{10} (S/N) \Rightarrow S/N = 10^{\frac{\text{SNR}}{10}} = 1000$$

$$C = B \cdot \log_2 (1000) = 29901,7 \text{ bit/s} = 29,9 \text{ kbit/s}$$

### 3. 256-QAM

1 baud = 8 bit

il BR massimo =  $2B = 6 \cdot 10^3 \text{ simb/s}$

code rate (dati utili / dati grezzi)

quindi il bitrate grezzo =  $\frac{BR \cdot \text{simb}}{\text{simb}} = \frac{6 \cdot 10^3}{8} \text{ bit/s} = 48 \text{ kbit/s}$

$$\text{codrate} = \frac{29,9}{48} = 0,623 = 62,3\%$$

### 4. Fast Ethernet (100 base Tx) = 100 Mbit/s

ITP = 96 bit = 12 byte

sequenza:  $18 + 1000 + 8 + 12 = 1038 \text{ Byte per un frame}$

quanti frame con payload = 1000 byte invio in

un secondo?

$$\frac{100 \cdot 10^6}{1038} = 12042 \text{ pacchetti}$$

INTESTAZ:  $18 \text{ B} + 8 \text{ B} =$

### 5. Bluetooth LE

bitrate = 1 Mbit/s =  $10^6 \text{ bit/s}$

A t ACK t

A manda frame dati (max. 41 byte, 27 byte payload)

$$\text{int. ho } \frac{10^6 \text{ [bit]}}{2} \cdot 150 \cdot 10^{-6} \text{ s} = 150 \text{ bit}$$

B risponde ACK da 10 byte

dopo ogni frame aspetto  $t = 150 \mu\text{s} = 150 \cdot 10^{-6} \text{ s}$

$$\text{eff.} = \frac{27 \cdot 5}{41 \cdot 8 + 150 + 10 \cdot 8 + 150} \frac{\text{bit utili}}{\text{bit netti}} = 0,305$$

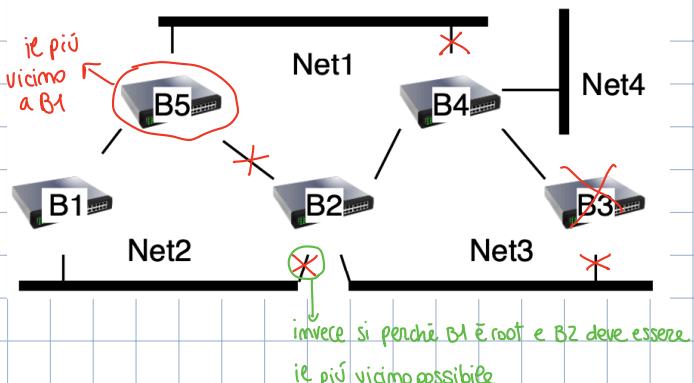
banda utile massima?

$$\text{banda utile} = 10^6 \cdot 0,305 = 305084,7 \text{ bit/s} = 305,1 \text{ kbit/s}$$

## 6. SPANNING TREE

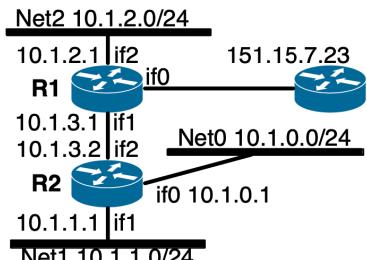
- a. switch che si disattiva? B3
- b. da NET1 a NET4

~~B4 B5, B1, B2, B4~~

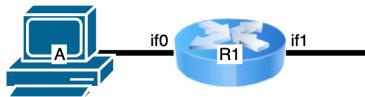


## 7. Tabella di INOLTRO di R2

dest	if	next hop
10.1.1.0/24	if1	-
10.1.0.0/24	if0	-
10.1.3.0/24	if2	-
*/*	if2	10.1.3.1



8. PC: 192.168.7.32 da server DHCP  
Router ha if1 = 192.168.0.74



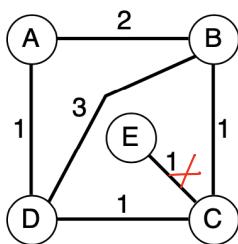
metrMask minima (per entrambi uguali)?  
↳ if0 e if1

# host  $\Rightarrow$  192.168.0.0/23  $\Rightarrow$  192.168.1.255  $\Rightarrow$  /22 per averci in due sottoreti diverse  
/22  $\Rightarrow$  192.168.3.255  
/21  $\Rightarrow$  192.168.7.255

## 9. vettore distanze: tutti solo ai vicini

- a. routing finale di D

host	cost	next hop
A	1	A
B	2	C
C	1	C
E	2	C



b. può la rete essere instabile? si se si rompe E-C allora C setta E too e B pubblicizza a C E 2 perciò B setta E 3 B ...

## 10. a. TRAFFIC CLASS e FLOW LABEL

- b. NO

- c. richieste al DNS  $\rightarrow$  UDP

d. segmentaz. allarme urgente  $\rightarrow$  TCP UDP deve annullare subito (TCP è lento)

- b. query (anche INSERT)  $\rightarrow$  UDP TCP (rischi 2 INSERT)

- c. Stampa remota  $\rightarrow$  TCP

12. TCP trasmette a  $b = 10^9$  b/s

e delay = 60s (al max)

seqNum = 32bit al max =  $2^{32} = 4,3 \cdot 10^9$

Adv.Window = 16bit

può un pacchetto essere accettato al posto di uno nuovo per il "intraposround"?

in 60s riesco a pompate  $2^{32}$ ?

$$\frac{10^9 \text{ bit}}{8} \cdot 60 \text{ s} = 60 \cdot 10^9 \text{ bit, quindi si}$$

13. TCP

lum = 1000 byte

SeqNum = 5000, 6000, 4000, 7000 (in ordine)

riceve due ACK: 6000 Adv.Window: 12000  $\Rightarrow$  arriviamo in disordine, conta quello con ACK maggiore

ACK: 4000 Adv.Window: 8000

vogli dire che ha fatto fino a 5899, gli manca 6000 + 1000, 7000 + 1000

quanti byte può ancora inviare

$$12000 - (2000) = 10000$$

14. TCP Cong. Control

SLOW START, FAST RETRANSMIT

MSS = 1400

$$\hookrightarrow 3 \text{ ACK uguali} \Rightarrow \text{ssthresh} = \frac{\text{cwnd}}{2}$$

alla fine del 1° round  $\Rightarrow$  cwnd = 4 MSS

alla fine del 2° round  $\Rightarrow$  cwnd = 8 MSS

alla fine del 3° round  $\Rightarrow$  ricevo 6 ack su 8  $\Rightarrow$  cwnd = 8 + 6 = 14

Se mom vengono ricevuti gli ACK di due segmenti nel terzo round, cong. win. all'inizio del quarto?

15. a. sicure

b. Sì, perché so che c'è sicure e mom modifica i messaggi

16. password = almeno 8 caratteri

$$\begin{array}{c} 1 \text{ MAIUSC}, 1 \text{ CIFRA}, 1 \text{ SEGNO SPECIALE} \\ \downarrow \quad \downarrow \quad \downarrow \\ 26 \quad 10 \quad 12 \end{array}$$

a. quante sono le pw di 8 caratteri? (con MAIUSC - CIFRA - SEGNO SPECIALE - CIFRA)

$$26 \cdot 26^5 \cdot 10 \cdot 12 \cdot 2 = 7,4 \cdot 10^{10} \text{ pw}$$

b. posso tentare 100.000 pw al secondo, in media dopo quanto viene indovinata?

$$\frac{10^5 \text{ pw}}{\text{s}} \text{ e ho } 7,4 \cdot 10^{10} \text{ pw, in media } \frac{7,4 \cdot 10^{10}}{10^5 \cdot 2} = 370000 \text{ s}$$

17. 1.  $A \rightarrow B : M$

2.  $B \rightarrow A : N$

3.  $A \rightarrow B : H(K, M), H(K, N)$

"non c'è stato", i.e. NONCE fa da TIMESTAMP

a.  $M$  è integro per  $B$ ? Sí

b. è puntuale? NO perché la NONCE è separata, se fosse  $H(K, M, N)$  allora era puntuale

c. A può ripudiare il messaggio? Sí non c'è un terzo

18. ALICE stessa manda a charlie e bob CONFIDENTIALE (con la stessa chiave di sessione)

PGP

il TIMESTAMP è della FIRMA

a. vediamo lo stesso timestamp? Sí perché vengono firmati assieme

b. Bob può scoprire anche se charlie ha lo stesso messaggio? Sí perché può prendere e decifrare il mess, poi calcola  $E_{PU_{CHARLIE}} = c$  e lo confronta

c. NO

19.

$N$  è NONCE

a. A è autenticato per B? Sí perché B invia a C K e C invia K ad A solo lui può leggerlo

b. B è autenticato per A? ~~Sí~~ NO perché il NONCE può essere modificato

c. K è puntuale? Sí perché N è assieme a K

1.  $A \rightarrow B : Id_A, N$

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

3.  $C \rightarrow A : E_{K_A}(A, K, N)$

4.  $A \rightarrow B : E_K(M)$

1. a. INTERNET

b. LINK-LAYER

c. TRANSPORT, INTERNET

d. TRANSPORT

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

1 simb. ha 4 bit

FEC con codice rate  $\frac{1}{2}$ 

SNR minimo?

$$B_R = 2B \text{ al max}$$

$$= 1000 \cdot 10^6 \text{ simb/s}$$

$$\text{bitrate} = B_R \cdot 4 = 4000 \cdot 10^6 \text{ bit/s} \text{ e con FEC} \Rightarrow \text{bitrate}/2 = 2000 \cdot 10^6 \text{ bit/s} = 2 \text{ Gb/s}$$

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

$$S/N = \frac{2 \cdot 10^9}{2 \cdot 500 \cdot 10^6} - 1 = 3$$

$$\text{SNR} = 10 \log_{10} \left( \frac{S}{N} \right) = 10 \log_{10} (3) = 4,77 \text{ dB}$$

3.

pol. gen:  $x^3 + 1 \Rightarrow 1 \ 0 \ 0 \ 1 \Rightarrow$  aggiungo <sup>3</sup>~~3~~ bitse resto ha  $n$  bit lo shift di  $n-1$  (i.e grado)

$$\begin{array}{r}
 \text{-----} \\
 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \\
 1 \ 0 \ 0 \ 1 \\
 0 \ 0 \ 1 \ 0 \ 0 \ 1 \\
 1 \ 0 \ 0 \ 1 \\
 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \\
 1 \ 0 \ 0 \ 1 \\
 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1
 \end{array}$$

= invia 1 0 1 1 0 1 0 1 0 0 1

4. 10Mb/s su coax

3 host

$$K = 0, \dots, 2^c - 1 \quad c \text{ è il tentativo}$$

a.

$$\begin{array}{ll}
 \text{tx} \rightarrow \text{coll} \quad K = 0, 1 & c = 1 \\
 \text{tx} \rightarrow \text{coll} \quad K = 0, 1, 2, 3 & c = 2
 \end{array}$$

$$\begin{array}{c}
 0 \ 1 \\
 0 \ 1 \\
 0 \ 1
 \end{array}$$

bastano 2 tentativi perché uno trasmetta, 3 perché anche il secondo trasmetta, 4 perché tutti trasmettano

b. <sup>risumo dei tre</sup>  $p(\text{host trasmette 1 FRAME al secondo TENTATIVO}) = ?$  ovvero somma al secondo tentativo, che prob. ho di trasmettere?  $\Rightarrow$  le PROBABILITÀ le fai a coppie

ho 3 host che possono scegliere tra (0,1) perché tra il primo e il secondo, ho le combinaz.  $2^3 = 8$  e mi interessano (110), (011), (101)

5. cella WiFi

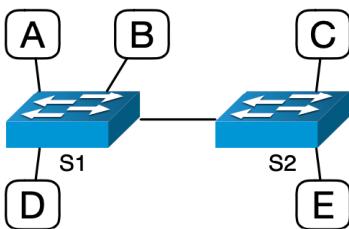
5, se fossero 6 sarebbe un esagono e riuscirebbero a vedersi

6.

a. no, vengono inviati in

broadcast (A,B,D) viene inviato a C che è al posto di A

b. cambia dopo il prossimo pacchetto deve aspettare che scada il timeout della entry



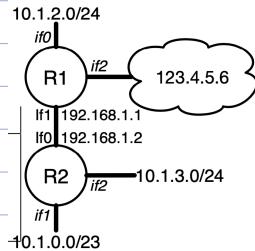
7. a. NON SONO GIUSTE

R1:	Net/CIDR	if	next hop
	10.1.0.0/23	if1	192.168.1.2
	10.1.2.0/24	if0	-
	192.168.1.0/24	if1	-
	*/*	if2	10.1.3.1

123.4.5.6

10.1.3.0/24 if1 192.168.1.2

R2:	Net/CIDR	if	next hop
	10.1.0.0/23	if1	-
	10.1.3.0/24	if2	<del>10.1.2.0/24</del> -
	192.168.1.0/24	if0	-
	*/*	if0	192.168.1.1



8. a. l'indirizzo pubblico di R2

b. no, bisogna anche aprire la SW R2

9.

LINK-STATE : info dei vicini a tutti (Flooding)

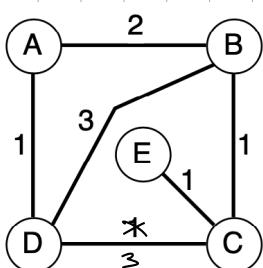
- a. B invia le info su A,C,D  
D invia le info su A,C,B

dest cost next hop

B 2 B

C 2 D

D 1 D



- b. LSU originato da D (D-C è 3), quale è il next hop da A per raggiungere C? B

10. AS2, AS4 transito

- a. R1, R2, R6, R5, R7

b. AS1-AS2-AS3 perché basta arrivare, non serve che sia ottimale

11. a. `accept()` → dalla LISTEN alla SYN-RCVD, perché è bloccante  
 b. si per entrambe, se non sarebbero raggiungibili (il server, il client può usare una porta effimera)

12. TCP con  $FIN=1$

- a. da ESTABLISHED a CLOSE\_WAIT  
 b. no, è lui che li può mandare alla comitoparte finché non invia  $FIN=1$ , a meno che non gli arrivino dati vecchi  
 c. Sì

13. TCP

$$MSS = 1460 \text{ B} \rightarrow \text{al massimo invio } 1460 \text{ B}$$

$$\text{a. in realtà } C \cdot RTT = 4000 \text{ bit} = 500 \text{ B} + 40 \text{ B di intestazioni}$$

$$C = 10 \text{ KB/s} = 80 \cdot 10^3 \text{ bit/s}$$

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

$$\text{b. } \frac{500}{540} = 0,926 = 92,6\%$$

- 14.

$$\frac{\lambda}{(500 \cdot 1000) \text{ B/s}} \rightarrow 1,25 \text{ MB/s}$$

TEORIA DELLE CODE

$$\text{in: } (500 \cdot 10^3) \text{ B/s} = 5 \cdot 10^5 = 0,5 \text{ MB/s}$$

$$\text{out: } 1,25 \text{ MB/s}$$

$$\lambda = 500 \text{ pac/s (quante richieste in un secondo?)}$$

$$S = \text{quanti secondi per una richiesta (ovvero quanti sec. per 1000 B?)} = \frac{1000 \text{ B}}{1,25 \cdot 10^6 \text{ B/s}} = 8 \cdot 10^{-4} \text{ s}$$

$$\text{im media il ritardo } R = \frac{S}{(1-\lambda S) \cdot 2} = \frac{8 \cdot 10^{-4} \text{ s}}{(1-8 \cdot 10^{-4} \cdot 500) \cdot 2} = 1,3 \cdot 10^{-3} \text{ s}$$

15. a. PASSIVO, comfid.

~~PASSIVO~~

- b. ATTIVO, comfid.

- c. ATTIVO, integrità

16. AES con CBC  $\Rightarrow$  blocchi 128 bit = 16 B

si vuole leggere byte in posiz. 1341

CBC:  $C_0 : IV$

$C_i : (M_i \oplus C_{i-1})$

- a.  $[1341 : 16] = 83 \quad 83 \cdot 16 = 1328 \rightarrow$  byte inizio: 1327 bisogna caricare anche il blocco 82 per decifrare 83  
 byte fine: 13423

- b. tutte le successive

17. a. NO, perché non c'è una nonce e nel 2. può inviare K diverso

~~b. nel 3 chiunque può fingersi A, ovvero modificare A~~

~~c. deve firmare la sua identità  $\rightarrow A \rightarrow KDC: E_{PKA}(A, E_{KA}(B, K))$~~

18. a. ~~Si~~ NO chiunque può spacciarsi per A al passo 1

b. Si

c.  $CA \rightarrow A : T, E_{PKA}(A, L, H(PKA, T))$   $CA \rightarrow A : T, L, E_{PKA}(A, H(PKA, T, L))$

1. a. NO  
b. SI  
c. SI

2.  $B = 4\text{kHz}$

$$\text{bitrate} = 56\text{ kb/s}$$

$$BR = 2B \Rightarrow BR = 8 \cdot 10^3 \text{ simb/s}$$

$$\text{bitrate} = BR \cdot m.\text{bit}$$

- a. m.bit per simbolo

$$m.\text{bit} = \frac{\text{bitrate}}{BR} = \frac{56 \cdot 10^3}{8 \cdot 10^3} = 7$$

- b.  $\text{SNR} = 20 \text{ dB}$

$$C = B \cdot \log_2 (1 + S/N)$$

$$\text{S/N} = 10 \log_{10} (S/N) \Rightarrow S/N = 10^{\frac{\text{SNR}}{10}} = 100$$

$$C = B \cdot \log_2 (101) = 26632,8 \text{ bit/s} = 26,6 \text{ kb/s}$$

3. BISYNC

DLE per fare ESCAPE del carattere di ETX, poi trasmetto un ETX

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

$$C = 2\text{ Mb/s} = 2 \cdot 10^6 \text{ b/s}$$

quanto è grande il payload?

$$\text{dim. frame} = C \cdot RTT = 10 \cdot 10^{-3} \cdot 2 \cdot 10^6 = 20 \cdot 10^3 \text{ bit} = 20 \text{ kb} = 2,5 \text{ kB}$$

5. rete 802.11  $\Rightarrow 2.4$

rete Bluetooth  $\Rightarrow 2.45$

- a. esiste la possibilità di interferenza? Sì perché Bluetooth con frequency hopping posso fare interferenza  
b. vince Bluetooth perché è TDM senza carrier sense

6. 2

7. pay = 960 B

More Fragments = 1

$$\text{MTU} = 400 \text{ B}$$

a.  $400 - 20 = \frac{380}{8} \cdot 8 = 376 \text{ B}$

- b. ~~1~~ perché hai gli altri frammenti dopo

8. A, B stesso ip

B inizia a funzionare dopo A.

a. tutto il traffico (di B) arriva ad A finché non si aggiornano le tabelle

b. arriviamo ad A finché le entry non si esauriscono

9. vettore dist. con SPT. H.

a.	net	cost	met hop
	A	3	B
	B	2	B
	D	4	F
	E	3	F
	F	2	F
	C	0	-

b.	net	cost	met hop
	A	3	B
	B	2	B
	C	0	/

10. a. quelli iscritti al gruppo dentro la propria rete

b. iscrive l'host al gruppo

11. UDP

bitrate = 128 kb/s (solo payload)

payload = 1200 B

intestaz UDP = 8B

" IP = 20B

a. trasmetti un frame ogni  $\frac{1200 \cdot 8}{128 \cdot 10^3} = 0,075 \text{ s}$

se si perde, la lacuna è 75 ms

b. 128 kb/s senza payload,  $E = \frac{1228}{1200} = 1,03 \Rightarrow \text{bitrate grezzo} = E \cdot \text{bit netto} = 130986,7 \text{ bit/s} = 131 \text{ kb/s}$

12. a. 32 bit

b. sì, ~~se si perde un pacchetto~~ se prendo un seqNum vicino agli ultimi, dopo pochi byte riporto da 0

13. TCP

W = 200 B ogni 10ms

MSS = 1460 B

RTT = 80 ms =  $80 \cdot 10^{-3} \text{ s}$

a.  $C = \frac{200 \cdot 8 \text{ bit}}{10 \cdot 10^{-3} \text{ s}} = 160 \text{ kb/s}$

payload =  $C \cdot RTT = 160 \cdot 10^3 \text{ [bit/s]} \cdot 80 \cdot 10^{-3} = 12800 \text{ bit} = 1600 \text{ B}$

ma per Nagle me invia sempre 1460 B

b. in media  $\frac{160 \text{ kb}}{1 \text{ s}} = 20 \cdot 10^3 \text{ B im un sec} \Rightarrow 13 \text{ pacchetti}$

14. RED

MINTH = 20 KB

MAXTH = 100 KB

quanto è piena la coda sul router?

perde circa il 10% dei pacchetti

$$p(\text{scarto}) = \frac{(\text{AVGLEN} - \text{MINTH})}{(\text{MAX} - \text{MINTH})} \Rightarrow \text{AVGLEN} = \frac{p(\text{MAX} - \text{MIN}) + \text{MIN}}{1} \\ = 0,1(80) + 20 = 28 \text{ KB}$$

15.

a. NO

b. SI

c. SI se vuoi confidenzialità, seno' non serve

16. AES

$A \rightarrow B : i, E_k(i) \oplus M$

a. SI

b. SI perché posso reinvioare un pacchetto e farlo sembrare giusto

17.

a. SI, gira cifrata

b. NO, al passo 2 si può fare se qualcuno si mette in mezzo

c. NO, perché al 3 puoi fare un replay (data che non c'è la NONCE)

1.  $A \rightarrow KDC : Id_A, Id_B, H(Id_A, Id_B, K_A)$
2.  $KDC \rightarrow A : E_{K_A}(K_S, Id_B, E_{K_B}(Id_A, Id_B, K_S))$
3.  $A \rightarrow B : E_{K_B}(Id_A, Id_B, K_S)$

18.

a. NO perché è stato firmato

b. SI

c. SI

1.  $A \rightarrow B : Id_A, M$
2.  $B \rightarrow A : N$
3.  $A \rightarrow B : E_{PR_A}(H(M, N))$

19. DIFFIE HELLMAN

a. NO

b. NO, dall'hash non puoi risalire a K

c. SI