

1[5]) Cosa significa che il livello trasporto realizza un servizio End-to-End? E cosa si intende con multiplexing e demultiplexing dei dati tra mittente e destinatario?

2[5]) Dove sono implementati, perchè sono implementati, da chi sono implementati, e quali aspetti rendono diversi il controllo di flusso e il controllo di congestione?

3[5]) I protocolli ICMP e SNMP sono analoghi? spiegare

4[15]) aiutate Alice e Bob a definire **un protocollo valido** per il seguente obiettivo: Alice vuole spedire un numero N di messaggi segreti $m_1 \dots m_N$ (brevi) a Bob, ma nè Alice nè Bob sanno a priori il numero N (nel senso che prima o poi Alice decide quale sia l'ultimo messaggio m_N della sequenza e lo invia). Nell'invia l'ultimo messaggio m_N Alice vuole anche specificare a Bob in modo affidabile che quello sia l'ultimo messaggio. Inoltre Alice e Bob vogliono essere sicuri che i messaggi siano tutti ricevuti, e possano essere ordinati correttamente da Bob nell'ordine con cui sono stati numerati e spediti da Alice. Trudy può fare qualsiasi cosa, ma non cancellare i pacchetti (però li può ritardare quanto vuole purchè un tempo finito). Come si fa a essere sicuri che Bob ottenga in **modo privato** (nessuno a parte Alice conosce sia il contenuto dei **messaggi** $m_1 \dots m_N$ inviati da Alice, sia il **numero di messaggi** N) e sicuro (nessuno abbia **modificato il contenuto di nessuno dei messaggi** $m_1 \dots m_N$ inviati da Alice o **modificato il loro ordine e il loro numero** ritardando o aggiungendo o duplicando ma non eliminando alcuni dei messaggi).

Pensare a tutti i modi in cui Trudy potrebbe inserirsi generando problemi al raggiungimento dell'obiettivo (anche solo potere contare il numero di messaggi N) e cercare di prevenirli, spiegando azioni e motivazioni.

protocollo:

m1, m2, mN....

ALICE: $KB+(N, KA-(H(N)))$

ALICE: for $i = 1$ a N {

$KB+(mi, KA-(H(mi)), i, KA-(H(i)))$

}

BOB: attende e riceve N

BOB while $(\#i < N)$ {

memorizza mi (dopo le opportune verifiche)

calcola $H(mi)$ e lo confronta con $KA+(KA-(H(mi)))$. Se sono uguali il msg è integro.

Inserisce il messaggio mi nel buffer di ricezione alla posizione i , dopo avere verificato che i sia uguale a $KA+(KA-(H(i)))$

Per l'affidabilità, BOB deve inviare un ack del messaggio mi ricevuto ad Alice.

Bob: $KA+(ACK(i, KB-(H(i))))$

if $(i == N)$ then finito()

5[12]) una rete locale di classe C con topologia a stella e uno switch centrale unico ha capacità massima dei collegamenti pari a **10 Mbps** e collega 254 client interni in un dominio IPv4 unico. In ogni istante al **massimo 100** dei 254 client trasmettono con UDP **X messaggi al secondo**, ognuno della dimensione **costante pari a 25 Bytes** destinati verso il client destinatario identificato con l'indirizzo IPv4 definito prendendo il proprio numero di host (mittente) e sommando il valore 100 e poi facendo il modulo 250 e poi sommando 1 al risultato (ad esempio, il client mittente host 80 manda al destinatario con numero di host $(180 \bmod 250) + 1 = 181$, il nodo host 180 manda al nodo $(280 \bmod 250) + 1 = 30 + 1 = 31$). Ogni destinatario prima riceve per intero gli X messaggi, e poi si attiva e li ri-trasmette al mittente successivo, e la cosa continua all'infinito.

a) Assumendo che a partire con le trasmissioni siano i primi host da 1 a 100, e di raggiungere la saturazione costante della capacità di rete locale, **quanti messaggi X al secondo** potranno essere inviati al massimo dai 100 client attivi in trasmissione in ogni istante nel futuro? Lo switch non fa buffering se non per il pacchetto in transito.

b) è possibile aumentare il valore di X se inseriamo due sottoreti e rispettivi router nel dominio di classe C, malgrado il limite di 10 Mbps del collegamenti? Spiegare

1 ---x--- S ---x--- 101
2 ---x--- S ---x--- 102
100 --- S --- 201

Ogni client trasmette max X pacchetti al secondo.
X capacità massima 10 Mbps
Host i può trasmettere a host $(100+i)$ al massimo $25 \cdot 8 =$

I

$200 \text{ bit (dimensione pacchetto)} \cdot X \leq 10 \text{ Mbps}$
 $X \leq 10.000.000 / 200 = 50.000$

Spiegare:

Num matrici = $16.000.000 / 256 = 62500$ matrici * 32 bit = overhead di trasmissione pari a 2.000.000 bit.

Indirizzo rete : _____

Calcoli [procedimento richiesto]

55 rete di classe A 55.0.0.0 / 8

55 . 01101111 (111 decimale)

55 . 01110000 (112 decimale)

55 . 011 00000 . x. y

indirizzo di rete: 55.96.0.0 / 11

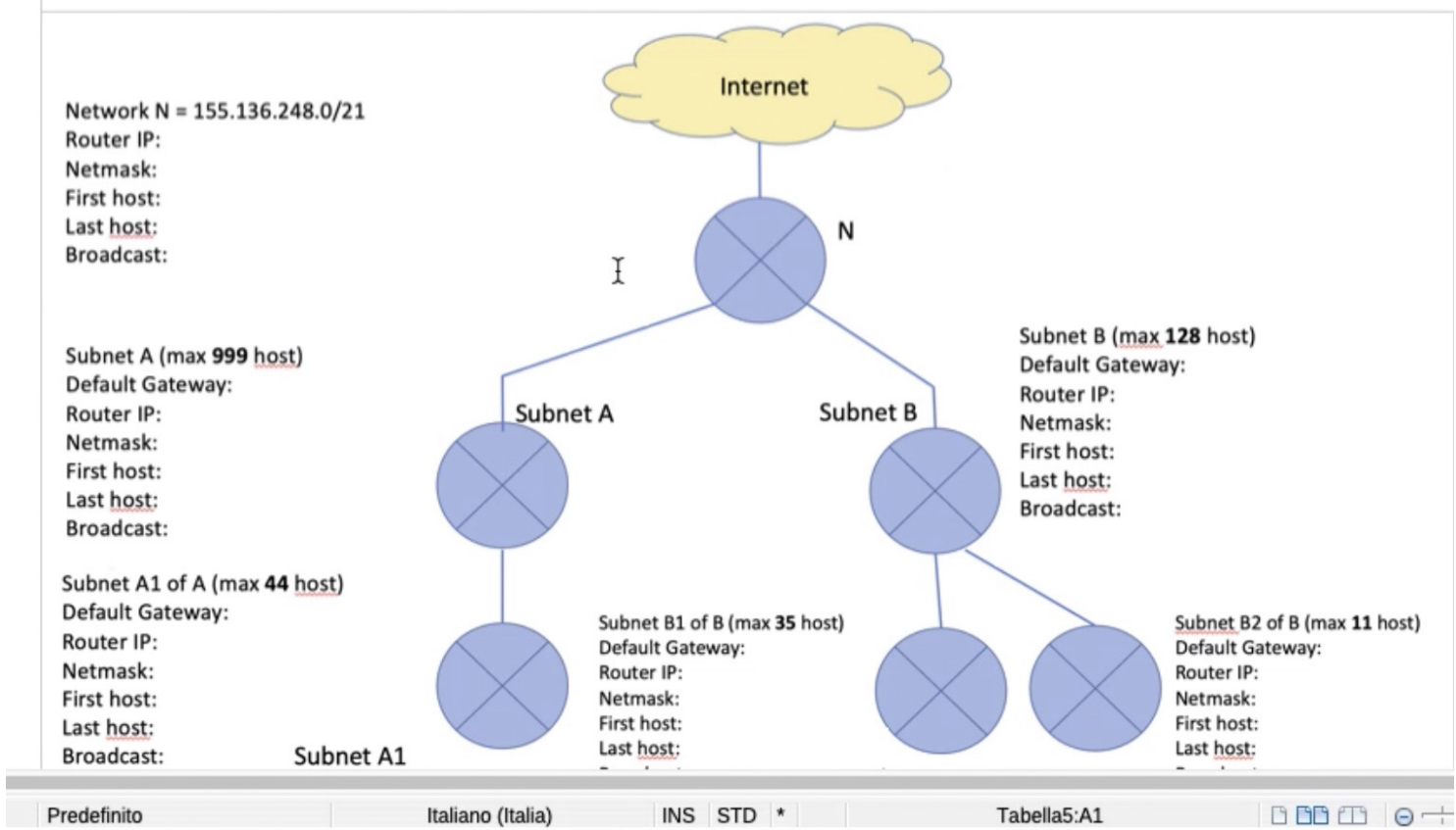
netmask : 255. 224.0.0 (/11)

b) indirizzo del router (come ultimo host indirizzabile prima del broadcast)

55 . 011 11111 . 11111111 . 11111110 = 55.127.255.254

9[25]) La rete N è connessa a Internet da un Router N collegato a un router A (e alla sua sottorete A) e a un router B con sottorete B. Nella sottorete A a sua volta è collegato un router A1 e alla rispettiva sottorete A1. Nella sottorete B a sua volta è collegato un router B1 e alla rispettiva sottorete B1 e un router B2 e la rispettiva sottorete B2. Lo schema mostra solo i router e i loro collegamenti con interfaccia Ethernet. Definire lo spazio di indirizzi delle reti e sottoreti N, A, A1 e B, B1 e B2, e definire gli indirizzi IPv4 da assegnare agli host e ai router come da schema indicato.

Usare lo spazio sul foglio per fornire traccia del procedimento e calcoli.



10[10]] Un sistema di comunicazione wireless usa la seguente codifica (encoding k): specificare
a) i bit della sequenza binaria di 18 bit che sono trasmessi per la sequenza esadecimale 0EAF...(completare fino a 18 bit aggiungendo zero a destra)
c) esprimere l'etichetta binaria dei simboli trasmessi sotto i relativi simboli della domanda b
b) quali forme d'onda radio saranno generate dall'encoder per trasmettere i 18 bit indicati, disegnandole nei 6 box predisposti sull'asse del tempo, tenendo conto della forma sinusoidale di riferimento $A \cdot \sin(B \cdot t)$ fornita (segnale in fase zero nelle due ampiezze utilizzate in esempio).

