

Prova Scritta del corso di Reti di Calcolatori

18 febbraio 2021

Docente: Luciano Bononi

Rispondere alle domande scrivendo solo nello spazio consentito, oppure nel retro del foglio. Fornire sempre una breve motivazione o il procedimento di calcolo della risposta, ove previsto.

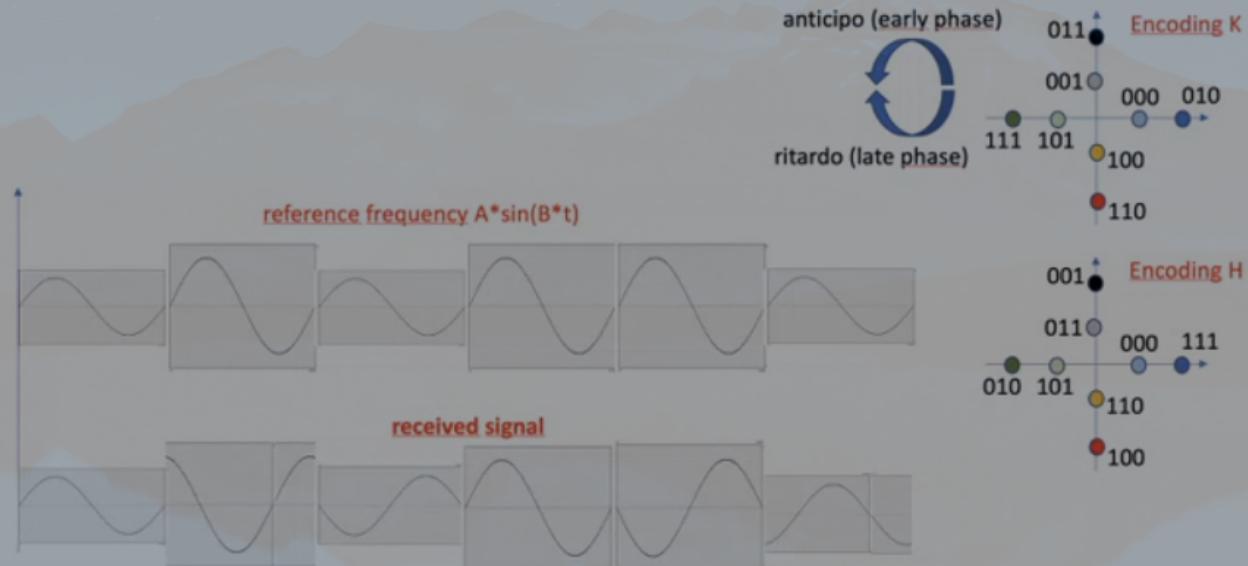
Se decidete di ritirarvi e NON consegnare, mandate una email a luciano.bononi@unibo.it seguendo le informazioni della pagina web del compito e attendete la mia email di risposta prima di abbandonare la stanza.

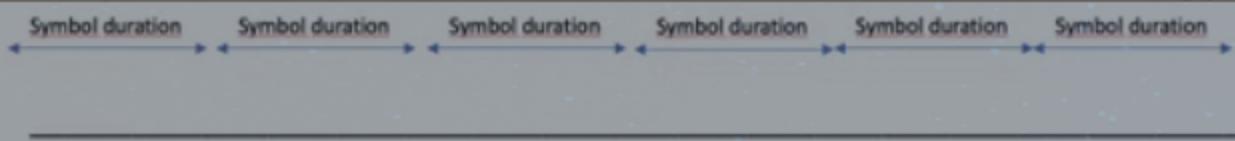
1[5]) E' possibile comunicare usando solo tecnologia Ethernet a 10 km di distanza? Perchè?

La comunicazione diretta non è possibile per la degradazione del segnale oltre i 200 metri. tuttavia, inserendo elementi attivi di livello fisico (repeater, hub) o MAC (switch) è possibile costituire una comunicazione multi-hop per tratti molto lunghi, anche se aumenta il ritardo del segnale e aumenta il rischio di collisione. Se poi venisse costruita una backbone di livello 3 (rete con router) con tutte le tecnologie MAC di tipo Ethernet, la comunicazione non avrebbe problemi particolari a coprire la distanza di 10 KM.

2[12]) un sistema wireless riceve il segnale disegnato in basso (received signal). Per comodità è mostrato anche il segnale di riferimento $A \cdot \sin(B \cdot t)$ (fase zero).

- A) cosa rappresentano i parametri A e B nella formula del segnale di riferimento?
- B) quale delle due codifiche è meglio utilizzare tra K e H e perchè? (da adesso sia essa la codifica scelta X)
- C) come chiamereste la tecnica di codifica utilizzata?
- D) se il segnale ricevuto è quello in basso quale è la sequenza di bit ricevuti mediante codifica scelta X?
- E) se ogni Byte è seguito da un bit di parità (pari), quali Byte ricevuti sono sbagliati e quali corretti?
- F) quali sono i valori dei Byte ricevuti in esadecimale (non considerando il bit di parità)?





- A) A=fattore di Ampiezza e B=frequenza dell'onda
- B) K è meglio di H per la minima distanza di Hamming tra simboli adiacenti, che riduce il rischio di bit

consecutivi errati, e rende più efficaci le tecniche di rilevazione e correzione errore

C) 8-QAM (in quanto varia ampiezza e fase su 8 simboli)

D) a = bassa ampiezza, A= alta ampiezza:

$$a(0) = 000$$

$$A(-90) = 011$$

$$a(-180) = 101$$

$$A(0) = 010$$

$$A(-180) = 111$$

$$a(+90) = 100$$

$$\text{sequenza} = 000\ 011\ 101\ 010\ 111\ 100$$

$$\begin{array}{ll} \text{E)} & 00001110\ 1 \\ & \quad 01011110\ 0 \end{array}$$

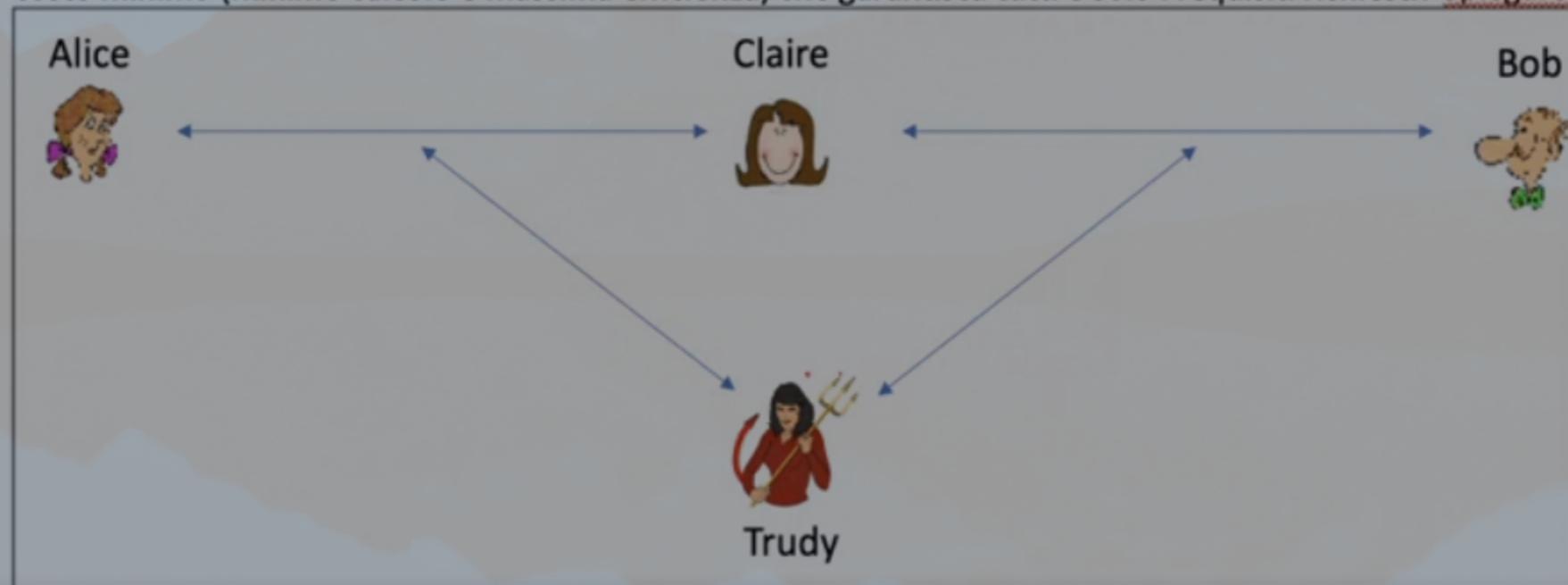
primo byte corretto (4 uno) secondo byte sbagliato (5 uno)

$$\begin{array}{ll} \text{F)} & \text{OE}\ \text{5E} \end{array}$$

3[5]) per quali delle seguenti tipologie di applicazione UDP è una buona scelta?

HTTP	si	no	(perchè?) non tollera errori
SMTP	si	no	(perchè?) non tollera errori
DHCP	si	no	(perchè?) tollera errori e ritrasmette il pacchetto
ICMP	si	no	(perchè?) tollera errori e ritrasmette il pacchetto
DNS	si	no	(perchè?) tollera errori e ritrasmette il pacchetto
Download di file	si	no	(perchè?) non tollera errori
Download immagine JPEG	si	no	(perchè?) non tollera errori
streaming video	si	no	(perchè?) tollera errori ma non ritrasmette pacchetti

4[15]) Alice spedisce a Bob un messaggio **M1** molto grande con garanzia di **non ripudiabilità** (ovvero Alice non potrà mai dimostrare di avere spedito un messaggio diverso da quello ricevuto da Bob) e di **Privacy**. Tuttavia il messaggio di Alice deve essere **firmato digitalmente dal notaio Claire**, che non deve capire il contenuto ma deve apporre la propria firma digitale, prima di inoltrare il messaggio a Bob. Bob infine vuole anche essere sicuro che il messaggio ricevuto da Claire non sia un **Replay attack** di Trudy (N.B. fare attenzione a dove si possono generare i replay attack). Come può essere realizzato lo schema di cifratura di costo minimo (minimo calcolo e massima efficienza) che garantisca tutti e solo i requisiti richiesti? Spiegare.



**Da Alice a Claire:
il messaggio M_1 è molto grande quindi non è opportuno cifrarlo con chiave pubblica/privata, se possibile**

(nè da Alice a Claire, nè da Claire a Bob).

Alice calcola hash $H(M1)$ e firma digitalmente l'hash $KA-(H(M1))$.

Inoltre Alice cifra $KS(M1)$ usando chiave simmetrica KS .

Alice cifra la chiave KS con la chiave pubblica di Bob e infine inserisce un nonce $R1$ firmato digitalmente da Alice.

Alice costruisce il pacchetto $P = [KS(M1), KA-(H(M1)), KB+(KS), KA-(R1)]$ e lo manda a Claire-

Da Claire a Bob

Claire riceve P e decodifica $KA+(KA-(R1))$ per vedere se il nonce $R1$ è originale (non replay da Alice a Claire).

Claire genera un Hash di P : $H(P)$ e lo firma digitalmente $KC-(H(P))$ garantendo che il pacchetto inoltrato da Alice a Claire è originale e non modificato da Claire.

Claire genera un nonce $R2$ e lo firma digitalmente $KC-(R2)$, garantendo non replay da Claire a Bob.

Claire spedisce a Bob il pacchetto $P' = [P, KC-(H(P)), R2]$ e lo manda a Bob.

Bob

Bob riceve P' e esegue le seguenti operazioni su P' : (si noti che al suo interno P è in chiaro)

$KC+(KC-(H(P)), R2)$ ottenendo $H(P)$, $R2$ e verifica l'originalità del nonce $R2$ (non replay da Claire a Bob).

Bob calcola $H(P)$ e lo compara con $H(P)$ ricevuto (integrità).

Bob apre P e esegue $KA+(KA-(R1))$ e verifica $R1$ sia originale (non replay da Alice a Claire... non deve fidarsi solo di Claire).

Bob apre $KB-(KB+(KS))$ e ottiene KS .

Bob apre $KA+(KA-(H(M1))) = H(M1)$ e lo tiene da parte per la verifica di integrità del messaggio di Alice.

Bob apre $KS(KS(M1))$ e ottiene $M1$.

Bob calcola $H(M1)$ e lo confronta con $H(M1)$ contenuto in P di Alice e se sono uguali accetta il messaggio $M1$.

Sintesi della soluzione: $M1$ grande cifrato solo con chiave simmetrica, mai eseguite doppie cifrature indentate, replay attack evitato sui singoli passi A-C, C-B, confidenzialità di $M1$, $M1$ non ripudiabile da Alice. Claire può garantire che Alice ha mandato il messaggio $M1$ (anche se non ne conosce il contenuto) se chiamata a dimostrarlo al tribunale (così come lo stesso Bob).

5[10]) N router spediscono ognuno Y pkt/s al Router 1 da sinistra. Ogni pacchetto ha dimensione K kilobits. Allo stesso modo M router spediscono Y pkt/s di dimensione K kilobits al Router 2 da destra. Il Backbone link centrale tra router 1 e router 2 ha un contratto di uso che fissa il limite massimo di utilizzo percentuale al valore α da Router 1 a Router 2, e $(1-\alpha)$ da Router 2 a Router 1. La capacità massima del Backbone link è di $Y*N*M$ kilobit/s. In quale caso il Backbone link causerà di certo congestione a uno dei due router e quale sarà il router congestionato? spiegare. Quale è il valore limite di dimensione di α per non creare congestione in nessuno dei router 1 e 2?

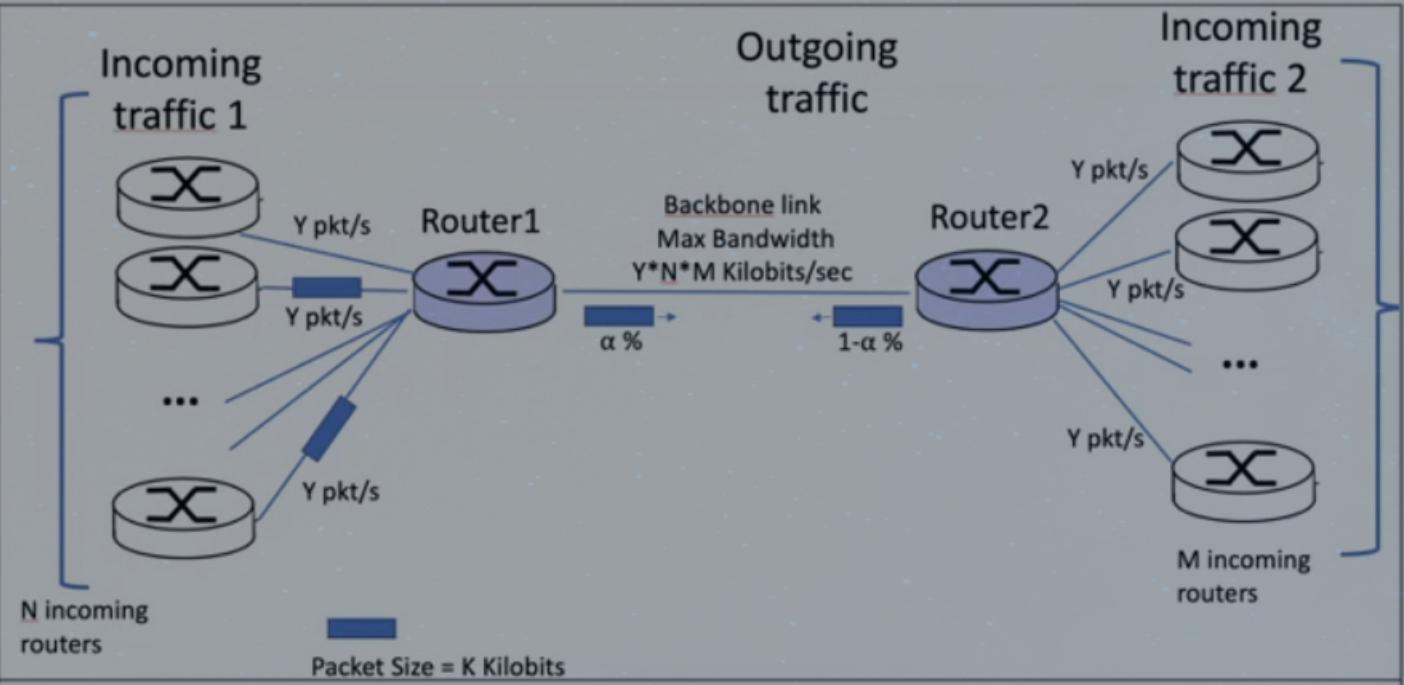
Calcolo dei parametri: date le 6 cifre meno significative del vostro numero di matricola 0000abcdef

N= somma della prime due cifre da destra a sinistra diverse da zero (es. e+f) =

M= somma delle prime due cifre diverse da zero selezionate da sinistra a destra (es. a+b) =

N=.....

M=.....



Procedimento: (suggerimento: usare notazione algebrica e solo alla fine sostituire i valori numerici)

1) Congestione R1 se e solo se: $NYK \geq \alpha(YNM)$

2) Congestione R2 se e solo se: $MYK \geq (1-\alpha)(YNM)$

da qui derivo algebricamente

$$1) K \geq \alpha M$$

$$2) K \geq (1-\alpha)N = N - \alpha N \Leftrightarrow K \geq N - \alpha N$$

quindi avremo congestione se $K \geq \min(\alpha M, N - \alpha N)$

Sostituendo i valori numerici di N e M è possibile trovare la condizione del caso numerico.

Es. supponendo $N = 10, M= 20$

Si ha quindi congestione se $K \geq \min(20\alpha, 10-10\alpha)$

6 [5]) Come funziona un Socket TCP tra client e server (lato client e lato server)?

Un socket TCP è la coppia (indirizzo IP, numero di porta applicazione).

Un socket TCP richiede handshake a 3 vie per negoziare apertura connessione TCP tra socket richiedente e welcoming socket lato server. Il richiedente inizia la richiesta e attende conferma dal server. Con la eventuale conferma arrivano i parametri di configurazione proposti dal server. Se il client accetta i parametri conferma l'apertura connessione con il terzo messaggio di handshake. Intanto il server crea un nuovo client socket lato server (su porta alta) che darà servizio al singolo client rendendo la comunicazione 1 a 1 tra i due socket TCP e consentendo al server di gestire eventuali client socket in parallelo. Tutti i dati scambiati sono resi affidabili dal protocollo TCP, e viene attuata controllo di ongestione e di flusso. Al termine della comunicazione il client (o il server) chiedono la chiusura della connessione, confermata dall'altro lato, e i socket e i buffer sono eliminati.

7[5]) Due host A e B devono comunicare tra loro un flusso enorme di dati in parallelo (da A a B e da B a A)

1

contemporaneamente. La rete tra host A e host B ha latenza costante pari a 125 ms (RTT = 250 ms). Tutti i pacchetti dati hanno dimensione 1 KB. Se la capacità di comunicazione minima della rete è pari a 64 KB/s e se un acknowledgment TCP è pari al 12,5% della dimensione di un segmento dati (inclusi gli overheads), quale dovrebbe essere il valore della Congestion Window CWND ideale di TCP su A e B per massimizzare le prestazioni di rete?

La comunicazione è parallela e asintotica in termini di quantità di dati (quindi da intendersi bidirezionale e simmetrica), per cui la banda minima si può intendere divisa equamente 32KB + 32 KB sui due lati.

La latenza di rete RTT equivale a 0,25 Sec, quindi in grado di contenere l'invio e ricezione sospeso di $32/4 = 8$ KB di dati. Però tali dati devono essere inclusivi del traffico degli ack, che è pari al 12.5% (1/8).

Quindi rimangono 7 KB dati e 1KB di ack per ogni RTT su ognuno dei due lati.

Di conseguenza, il valore ideale di Congestion Window è 7. Eccedendo tale valore si satura il collegamento oltre la capacità minima e si obbliga il ricevente a fare maggiore buffering dei dati.

8[10]) Date "abcdef" le 6 cifre del numero di matricola, chi dovrebbe essere il router (con ultimo indirizzo IP valido) della rete che contiene l'host 10.196."2ef"."1ef" se la maschera di rete fosse 255.255.192.0?

IPv4 del Router: _____

e se la maschera di rete fosse /14? _____

+Calcoli [computation]

Supponiamo l'indirizzo del caso in esempio sia 10.196.211.111.

tradotto in binario: 00001010 11000100 11010011 01101111

maschera di rete : 11111111 11111111 11000000 00000000 (255.255.192.0 = /18)

tradotto in binario: 00001010 11000100 11010011 01101111 (in rosso l'host)

router : 00001010 11000100 11111111 11111110 (= 10.196.255.254)

se maschera di rete / 14:

maschera di rete : 11111111 11111100 00000000 00000000 (255.252.0.0 = /14)

tradotto in binario: 00001010 11000100 11010011 01101111 (in rosso l'host)

router : 00001010 11000100 11111111 11111110 (= 10.199.255.254)

9[23] Definire gli indirizzi IPv4 assegnabili nelle reti LOCALI sotto indicate per le esigenze definite:
Usare lo spaio sul foglio per traccia procedimento e calcoli.

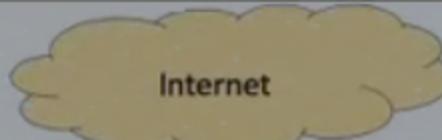
Network N = 10.24.136.0/21

Router IP:

Netmask:

First host:

Last host:



Matricola: a b c d e f

2ef =

5ef =

Subnet A (max «2ef» host)

Default Gateway:

Router IP:

Netmask:

First host:

Last host:

Subnet A

Subnet A1 of A (max 42 host)

Default Gateway:

Router IP:

Netmask:

First host:

Last host:

Subnet A1

Subnet A2

Subnet B

Subnet B (max «5ef» host)

Default Gateway:

Router IP:

Netmask:

First host:

Last host:

Subnet A2 of A (max 29 host)

Default Gateway:

Router IP:

Netmask:

First host:

Last host:



Spiegare qui sotto il procedimento [explain how you got the results here]

Supponiamo B di 520 host e A di 220 host.

B è la porzione maggiore, per cui partiamo da B.

Subnet B (520 -> servono 1024 cioè 10 bit di host)

Rete N:

Rete: 10.24.136.0/21

Netmask: 255.255.248.0

First host: 10.24.136.1/21

Last host = 10.24.143.253/21

IP router = 10.24.10001|111.11111110 = 10.24.143.254/21

rete B: 520 host -> 1024 indirizzi (/22)

Rete: 10.24.136.0/22

Default gateway: 10.24.143.254/21

Netmask: 255.255.252.0

First host: 10.24.136.1/22

Last host = 10.24.139.253/22

IP router = 10.24.100010|11.11111110 = 10.24.139.254/22

I

rete A: 220 host -> 256 indirizzi (/24)

Rete: 10.24.140.0/24

Default gateway: 10.24.143.254/21

Netmask: 255.255.255.0

First host: 10.24.140.1/24

Last host = 10.24.140.253/24

IP router = 10.24.140.254/24

rete A1: 42 host -> 64 indirizzi (/26)

Rete: 10.24.141.0/26

Default gateway: 10.24.140.254/24

Netmask: 255.255.255.192

First host: 10.24.141.1/26

Last host = 10.24.141.61/24

IP router = 10.24.141.62/24

rete A2: 29 host -> 32 indirizzi (/27)

Rete: 10.24.141.64/27

Default gateway: 10.24.140.254/24

Netmask: 255.255.255.224

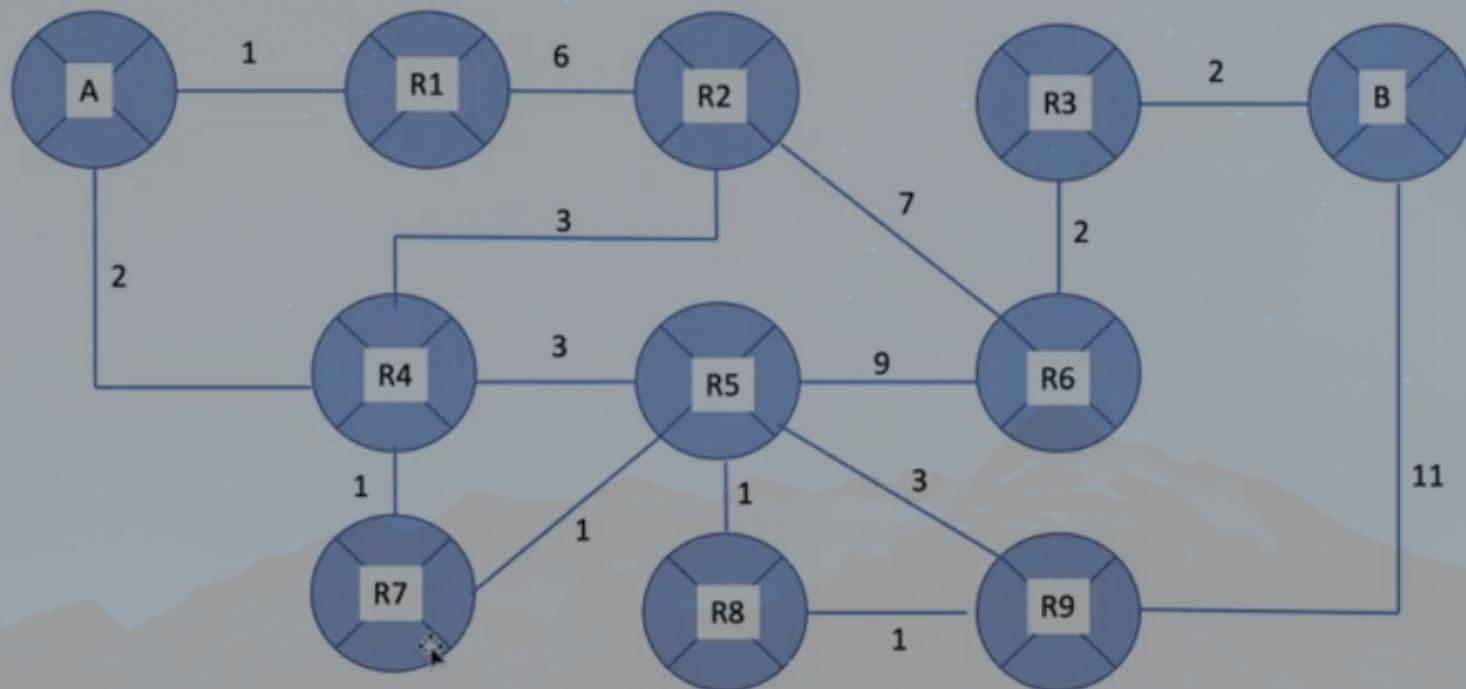
First host: 10.24.141.65/27

Last host = 10.24.141.93/27

IP router = 10.24.141.94/27

10 [10]) Applicando un protocollo di routing Link State, quale è il cammino di costo minimo tra A e B e quale è la tabella di instradamento del nodo R4 ottenuta verso tutte le destinazioni di rete (R1, R2, ... R9) nella rete sotto disegnata? Esprimere la tabella di R4 come sequenza di righe nella forma [destinazione finale Rx, prossimo router al quale inoltrare Ry]

10 [10]) Applicando un protocollo di routing Link State, quale è il cammino di costo minimo tra A e B e quale è la tabella di instradamento del nodo R4 ottenuta verso tutte le destinazioni di rete (R1, R2, ... R9) nella rete sotto disegnata? Esprimere la tabella di R4 come sequenza di righe nella forma [destinazione finale Rx, prossimo router al quale inoltrare Ry]



Spiegare qui sotto il procedimento [e l'algoritmo usato con i suoi dati]

Costo minimo A -> B = 16 ed è il cammino A-R4-R2-R6-R3-B (vedi tabella algoritmo Dijkstra sotto indicato)

Tabella di R4

A a costo 2 inoltrando direttamente ad A

R1 a costo 3 inoltrando ad A

R2 a costo 3 inoltrando direttamente a R2

R3 a costo 12 inoltrando a R2

R5 a costo 2 inoltrando a R7

R6 a costo 10 inoltrando a R2

R7 a costo 1 inoltrando direttamente a R7

R8 a costo 3 inoltrando a R7

R9 a costo 4 inoltrando a R7

B a costo 14 inoltrando a R2