



**La Sapienza**

Università degli Studi di Roma

Dipartimento di Informatica e Sistemistica



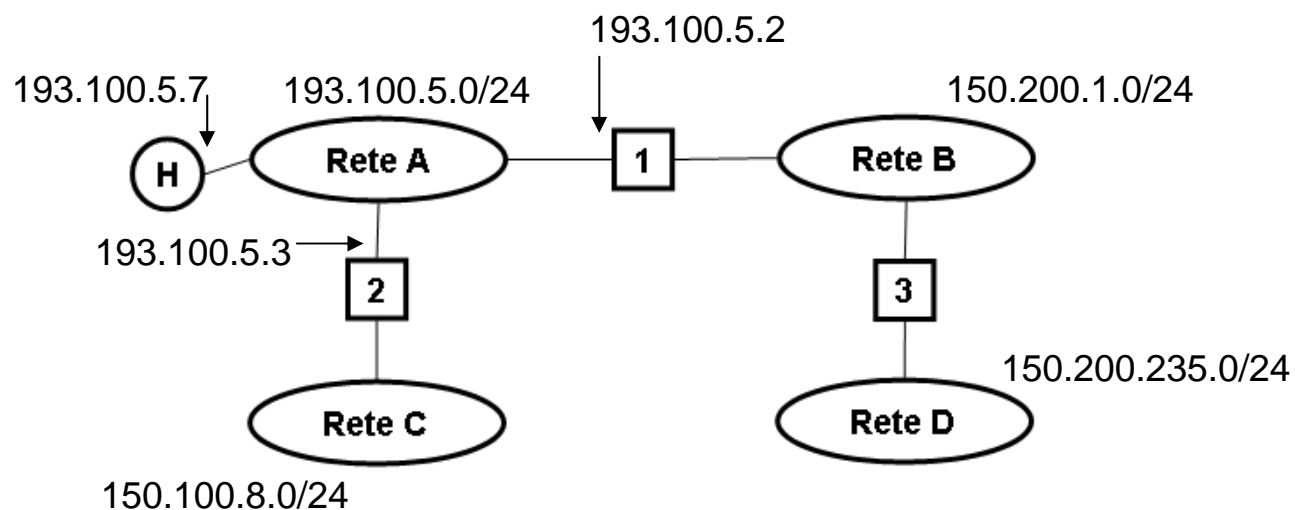
# RETI DI CALCOLATORI II

Esame del 11/02/2009

Soluzione esercizi [traccia]



### Quesito 1.a – Assegnazione indirizzi alle sottoreti ed ai router



Rete	Indirizzo	Maschera	Router	Indirizzo
Rete A	193.100.5.0	255.255.255.0	Router 1	193.100.5.2
Rete B	150.200.1.0	255.255.255.0	Router 2	193.100.5.3
Rete C	150.100.8.0	255.255.255.0	Router 3	?
Rete D	150.200.235.0	255.255.255.0		



**Quesito 1.b** – Compressione tabella di routing host H

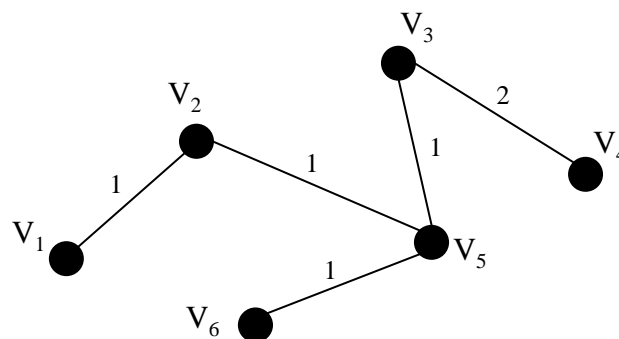
<b>Destination</b>	<b>Mask</b>	<b>Next hop</b>
193.100.5.0	255.255.255.0	-
150.100.8.0	255.255.255.0	193.100.5.3
150.200.0.0	255.255.0.0	193.100.5.2



### Quesito 2.a – Applicazione algoritmo Dijkstra

Step	T	L(2)	Path	L(3)	Path	L(4)	Path	L(5)	Path	L(6)	Path
1	1	1	1-2	$\infty$	---	$\infty$	---	$\infty$	---	4	1-6
2	1,2	1	1-2	4	1-2-3	$\infty$	---	2	1-2-5	4	1-6
3	1,2,5	1	1-2	3	1-2-5-3	6	1-2-5-4	2	1-2-5	3	1-2-5-6
4	1,2,5,3	1	1-2	3	1-2-5-3	5	1-2-5-3-4	2	1-2-5	3	1-2-5-6
5	1,2,5,3,6	1	1-2	3	1-2-5-3	5	1-2-5-3-4	2	1-2-5	3	1-2-5-6
6	1,2,5,3,6,4	1	1-2	3	1-2-5-3	5	1-2-5-3-4	2	1-2-5	3	1-2-5-6

### Quesito 2.b – Spanning tree [ $V_1$ radice]



### Quesito 2.c – OSPF



### Quesito 3.a

L'anomalia si verifica a fronte di una falsa informazione d'instradamento che arriva al nodo B dal nodo C e dal nodo A; tale informazione si riferisce ad un presunto percorso d'instradamento offerto da questi nodi verso la rete di destinazione ma che in realtà passa per B stesso ed è dovuto ad un ritardo nella convergenza dell'algoritmo.

Affinché **possa** avvenire l'anomalia è necessario che i router A e C instradino verso la rete di destinazione utilizzando [nel percorso d'instradamento] il link BD e quindi il router B. Si può facilmente verificare che questo può accadere solo se  $x \geq 3$ .

Ad ulteriore riprova, considerando l'instradamento verso la rete di destinazione per diversi valori di  $x$ :

- ❑ Se  $x = 1$ , A instrada verso C, B verso C [o verso D] e C verso D; l'anomalia non può verificarsi in quanto:
  - Il link BD non è addirittura utilizzato [se B instrada verso C]
  - A fronte della rottura del link BD il percorso comunicato da A e C al nodo B è sempre un percorso reale
- ❑ Se  $x = 2$ , A instrada verso C [o verso B], B verso D e C verso D; l'anomalia non può verificarsi in quanto, a fronte della rottura del link BD, il percorso comunicato da C al nodo B è sempre un percorso reale
- ❑ Se  $x = 3$ , A instrada verso B, B verso D e C verso D [o verso B]; l'anomalia può verificarsi se C instradata verso B [anche se termina immediatamente]; viceversa, lo scenario diverrebbe analogo al caso  $x=2$



### Quesito 3.b

A fronte della rottura del link BD, il router B invia triggered updates ad A e C. Nel frattempo, può accadere che i 2 router inviino a B un aggiornamento periodico che ancora ignora le nuove condizioni della rete e che si riferisce, pertanto, ad un percorso fittizio verso la rete di destinazione [che passa per B stesso e che quest'ultimo assumerà come utilizzabile]. Questa circostanza innesca l'anomalia.

Qualora invece i triggered updates emessi da B vengano processati da A e C **prima** del timeout per l'emissione dei loro aggiornamenti periodici, i 2 router ricalcoleranno la rotta verso la rete di destinazione [A instraderà verso C e C verso D] emettendo a loro volta dei triggered updates verso B. In queste condizioni, anche con  $x \geq 3$  i router utilizzeranno fin da subito un percorso d'instradamento reale e l'anomalia non si verificherà.



## Quesito 7

1. H invia un messaggio STUN [**binding request**] allo STUN server remoto utilizzando come porta sorgente la porta UDP [locale] che sarà utilizzata da SERVICE; la risposta dello STUN server [**binding response**] conterrà le informazioni sul mapping [SERVICE\_PUBLIC\_IP, SERVICE\_PUBLIC\_PORT]
  - STUN utilizza UDP per cui la stessa richiesta forzerà la creazione di una entry nella NAT mapping table del router [fino a quel momento vuota]
  - La risposta dello STUN server è significativa per le ipotesi sulla tipologia di NAT implementata
2. H attiva SERVICE sulla porta UDP locale
3. H diffonde su Internet le informazioni SERVICE\_PUBLIC\_IP e SERVICE\_PUBLIC\_PORT utilizzando il protocollo SERVICE\_PUBLISHING\_PROTOCOL
4. H invia periodicamente pacchetti di “keep alive” in modo da assicurare la permanenza del binding anche in assenza di traffico generato o diretto da o verso SERVICE
  - La destinazione dei pacchetti potrebbe essere lo STUN server ma anche un qualunque altro host Internet [grazie all’ipotesi sulla tipologia di NAT implementata]
  - Una soluzione alternativa, ma meno efficiente, potrebbe essere quella di utilizzare delle richieste STUN periodiche come meccanismo di keep alive