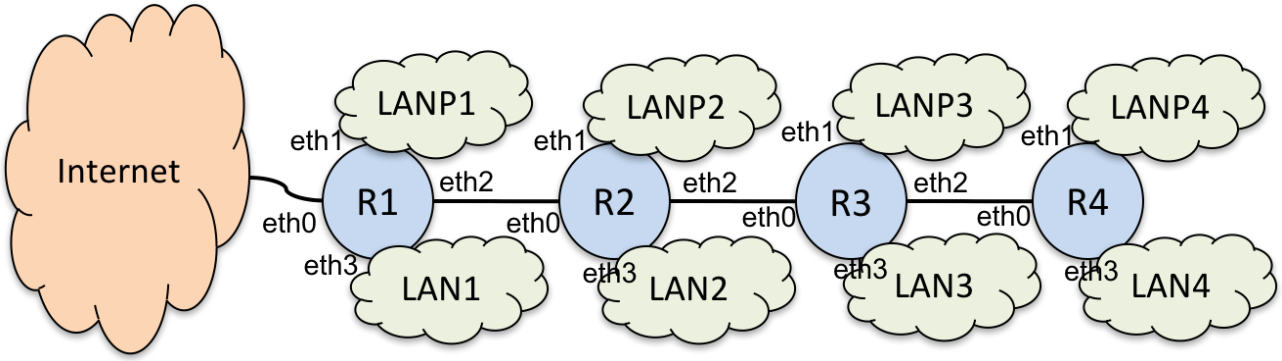
UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Ingegneria
e Scienza dell'Informazione

Corso di Laurea in informatica

Reti di calcolatori

31-5-2017 — Dry Run di una prova d'esame
(più altri esercizi con traccia di soluzione)

Esercizio 1 (configurazione di una rete locale)



Una azienda ha un accesso a Internet attraverso un router ed una rete interna divisa in otto sottoreti "routate" come indicato nella figura. Le otto sottoreti sono quattro normali o pubbliche e quatto (LANPn) interne o private. Tutte le otto sottoreti sono di tipo /24.
L'azienda possiede una il seguente pool di indirizzi pubblici: 130.175.4.0/22, mentre l'indirizzo per l'interfaccia verso Internet è assegnato da un pool a disposizione dell'ISP, ad esempio 120.120.0.0/16.

1. Assegnare opportunamente gli indirizzi IP pubblici e privati alle otto sottoreti sulle otto LAN dell'azienda, specificando anche la network mask.
2. Assegnare gli indirizzi a tutte le interfacce di rete dei router, tenendo conto che ciascun router ha 4 interfacce di rete tranne R4 che ne ha solo 3 ovviamente.
3. Definire le tabelle di routing di R2 ed R4.

Esercizio 2 (su TCP)

Consideriamo una connessione TCP su cui viene trasferito un file di dimensioni molto grandi, dove quindi possiamo trascurare il transitorio iniziale legato allo slow start. La receiver window è posta a 64kbyte (il massimo ammesso senza l'opzione di "scaling window"). La velocità di trasmissione a livello fisico è di 1Gbit/s, mentre l'RTT (Round Trip Time) è dominato da un ritardo di propagazione di 110ms.

1. Si calcoli il numero di segmenti a cui corrisponde la receiver window se la MTU di IP è quella consentita dalle normali reti Ethernet.
2. Si calcoli il throughput a regime ottenuto con questa connessione a livello applicativo e a livello IP.
3. All'istante t_0 (istante arbitrario durante la trasmissione) viene perso un pacchetto IP; si disegni l'andamento della dimensione della congestion window (CNGWIN) dall'istante della perdita a quando la finestra ritorna al valore di regime pari alla receiver window.

4. Si ripeta l'esercizio al punto 3 nel caso in cui vengono persi tre segmenti consecutivi;
5. Si ripeta infine questo esercizio (al punto 4.) nel caso in cui il primo segmento perso venga ri-perso quando viene ritrasmesso (i successivi due sono invece ritrasmessi in modo corretto).

Esercizio 3 (Configurazione rete)

Un'azienda deve progettare la propria interna (rete locale) in base alle seguenti specifiche:

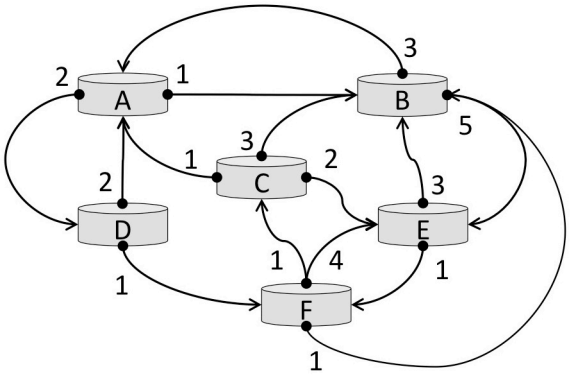
- la rete è composta da 4 sottoreti fisiche separate, interconnesse tra loro da 4 router;
- non si vogliono mai avere più di 2 "hop" (funzione di instradamento e commutazione) tra una sottorete e l'altra, ed anche verso Internet;
- una sottorete è dedicata alla sala macchine dell'università, progettata per supportare fino a circa 400 server con indirizzo IP pubblico;
- una seconda sottorete, anche essa con indirizzi IP pubblici, è dedicata ai dipendenti occupati in ricerca e sviluppo ed agli impiegati con funzioni direttive e deve poter accomodare fino a 1000-1200 postazioni di lavoro;
- le altre due sottoreti hanno indirizzi IP privati e sono dedicate al resto del personale (circa 500 unità) ed alla wireless LAN in cui si presume che ci possano essere fino a 10.000 diversi dispositivi collegati contemporaneamente;
- gli indirizzi IP pubblici devono essere presi dal "pool" 128.152.0.0/20, gli indirizzi privati possono essere scelti a piacimento, ma deve essere possibile il routing diretto all'interno della rete aziendale.

Con questi vincoli:

1. si disegni la topologia logica della rete (interconnessione di router e LAN che supportano le sottoreti); esiste più di una soluzione corretta, è sufficiente identificarne una;
2. si assegnino gli indirizzi IP pubblici e privati alle diverse sottoreti, specificando anche la network mask;
3. si assegnino gli indirizzi a tutte le interfacce di rete dei router, tenendo conto che l'indirizzo del router di interconnessione verso Internet deve essere preso dal pool dell'università;
4. configurare la tabella di routing di uno dei router a scelta spiegando il motivo della configurazione.

Esercizio 4 (Routing in Internet)

Si consideri la rete disegnata in figura. Tutti i router usano OSPF come protocollo di calcolo delle rotte per l'instradamento dei pacchetti. Il costo dei link non è simmetrico.



1. Usando gli algoritmi propri di OSPF, ed assumendo che i costi siano già stati distribuiti, si calcoli la tabella di instradamento dei nodi A ed E e si disegni il Minimum Spanning Tree corrispondente con radice in A ed E rispettivamente.
2. Quanti pacchetti transitano nella rete per la distribuzione in flooding del costo dei link del nodo C? E del nodo F?
3. Definire in modo chiaro il funzionamento del protocollo di flooding usato da OSPF.

Tracce di possibili soluzioni

Esercizio 1

NOTA: ai fini della comprensione, le spiegazioni in questo esercizio sono estremamente prolisse e talvolta ridondanti. In un esame spiegate brevemente il ragionamento seguito vicino alla vostra soluzione senza dilungarvi in eccessive spiegazioni che rischiano solamente di farvi perdere tempo.

Iniziamo con la configurazione delle reti con IP pubblici. Abbiamo 4 sottoreti di tipo /24 da configurare partendo dal pool di indirizzi 130.175.4.0/22. La rete di partenza è dunque

```
130.175.00000100.00000000 Rete
255.255.11111100.00000000 Netmask (255.255.252.0)
```

Possiamo suddividerla quindi nelle 4 reti in /24

```
LAN1: 130.175.4.0/24
LAN2: 130.175.5.0/24
LAN3: 130.175.6.0/24
LAN4: 130.175.7.0/24
```

Nella rappresentazione binaria (solo gli ultimi due byte a destra):

```
130.175.00000100.00000000 Rete LAN1
255.255.11111111.00000000 Netmask (255.255.255.0)

130.175.00000101.00000000 Rete LAN2
255.255.11111111.00000000 Netmask

130.175.00000110.00000000 Rete LAN3
255.255.11111111.00000000 Netmask

130.175.00000111.00000000 Rete LAN4
255.255.11111111.00000000 Netmask
```

Assegniamo l'indirizzo IP alle interfacce dei router collegati a queste reti prendendo un qualunque indirizzo host appartenente alle sottoreti. In questo caso, il primo:

```
R1 eth3: 130.175.4.1
R2 eth3: 130.175.5.1
R3 eth3: 130.175.6.1
R4 eth3: 130.175.7.1
```

In maniera analoga configuriamo le LAN con indirizzi privati partendo dal pool 192.168.0.0/16, configurando 4 reti di tipo /24

```
LANP1: 192.168.0.0/24 Netmask 255.255.255.0
LANP2: 192.168.1.0/24 Netmask 255.255.255.0
LANP3: 192.168.2.0/24 Netmask 255.255.255.0
LANP4: 192.168.3.0/24 Netmask 255.255.255.0
```

(Nota: in aula avevamo preso indirizzi 10... ma è del tutto analogo) e assegnando i seguenti indirizzi IP alle interfacce dei router ad esse collegate

```
R1 eth1: 192.168.0.1
R2 eth1: 192.168.1.1
```

```
R3 eth1: 192.168.2.1
R4 eth1: 192.168.3.1
```

Il passo successivo consiste nel configurare le reti "punto a punto" di collegamento fra i router. Abbiamo bisogno di 3 reti (R1-R2, R2-R3, R3-R4) ciascuna con 2 indirizzi IP. Considerando anche l'indirizzo di rete e di broadcast, abbiamo bisogno di 4 bit per identificare la rete. Configuriamo dunque 3 reti di tipo /30, prendendole dal pool privato 172.16.0.0/16:

```
R1-R2: 172.16.0.0/30 Netmask 255.255.255.252
R2-R3: 172.16.0.4/30 Netmask 255.255.255.252
R3-R4: 172.16.0.8/30 Netmask 255.255.255.252
```

In binario:

```
172.016.000.00000000 R1-R2
255.255.255.11111100 Netmask

172.016.000.00000100 R2-R3
255.255.255.11111100 Netmask

172.016.000.00001000 R3-R4
255.255.255.11111100 Netmask
```

Gli indirizzi assegnabili sono 2 per rete, ossia

```
172.16.0.1 (R1 eth2) 172.16.0.2  (R2 eth0)
172.16.0.5 (R2 eth2) 172.16.0.6  (R3 eth0)
172.16.0.9 (R3 eth2) 172.16.0.10 (R4 eth0)
```

L'ultimo indirizzo IP da assegnare è quello dell'interfaccia eth0 del router R1. Il testo dice che questo indirizzo ci viene dato dall'ISP e viene preso dal pool 120.120.0.0/16. Scegliamo un qualunque indirizzo assegnabile di questa rete e lo assegniamo a R1 eth0, ad esempio 120.120.0.1.
L'ultimo punto richiede di definire le tabelle di routing di R2 ed R4. Ogni elemento della tabella è composto dalle seguenti informazioni: indirizzo di rete (destinazione), netmask associata, next hop e interfaccia di uscita. La tabella di routing di R2 è la seguente

	Destination	Netmask	Next hop	Interface
1	172.16.0.0	/30	CD	eth0
2	172.16.0.4	/30	CD	eth2
3	172.16.0.8	/30	172.16.0.6 (R3)	eth2
4	192.168.1.0	/24	CD	eth1
5	130.175.5.0	/24	CD	eth3
6	192.168.2.0	/23	172.16.0.6 (R3)	eth2
7	130.175.6.0	/23	172.16.0.6 (R3)	eth2
8	0.0.0.0	/0	172.16.0.1 (R1)	eth0

Le prime tre righe sono le 3 reti punto-punto fra i router (nell'esame si possono anche evitare, con l'ovvia implicazione che non sono raggiungibili attraverso R2). CD indica "consegna diretta". La quarta e la quinta riga sono le due reti LANP2 e LAN2 alle quali R2 è direttamente collegato. Le righe 6 e 7 puntano alle reti private LANP3 e LANP4 ed alle reti pubbliche LAN3 e LAN4, rispettivamente. Qui abbiamo "aggregato" le rotte, inserendo 2 righe invece di quattro. Ad esempio, per quanto riguarda le reti LANP3 e LANP4 abbiamo i seguenti indirizzi e netmask:

```
LANP3:   192.168.0000010.0
NETMASK: 255.255.1111111.0 (/24)
LANP4:   192.168.0000011.0
NETMASK: 255.255.1111111.0 (/24)
```

Tuttavia i due indirizzi di rete hanno una parte in comune, ossia i primi 23 bit. Quindi il router può eseguire il confronto sulla maschera a 23 bit e inoltrare i pacchetti a R3, che poi penserà a smistare il traffico verso la rete corretta. NB: questo non va in conflitto con le reti LANP1 e LANP2, poiché il prefisso di rete è diverso. Facendo un match con la sottorete /23:

```
LANP1:   192.168.0000000.0
         255.255.1111110.0 (/23)
--------------------------
Risultato:     192.168.0.0 (non corrisponde a 192.168.2.0)

LANP2:   192.168.0000001.0
         255.255.1111110.0 (/23)
--------------------------
Risultato:     192.168.0.0 (non corrisponde a 192.168.2.0)
```

L'ultima riga infine indica l'azione da fare quando una destinazione non corrisponde a nessuna delle righe precedenti. In questo caso, l'ultima riga fa si che i pacchetti destinati alle reti LANP1, LAN1 e ad Internet vengano inoltrati ad R1.

La tabella di routing di R4 è più semplice:

	Destination	Netmask	Next hop	Interface
1	172.16.0.8	/30	CD	eth0
2	192.168.3.0	/24	CD	eth1
3	130.175.7.0	/24	CD	eth3
4	0.0.0.0	/0	172.16.0.9 (R3)	eth0

Le prime tre righe indicano le tre reti alle quali R4 è direttamente collegato (R3-R4, LANP4, LAN4).

Esercizio 2

1. Se MTU=1500 MSS = MTU=H_{IP} -H_{TCP} = 1500-20-20=1460, quindi il in una receiver window ci sono 65536/1460 = 44 MSS più un segmento di dimensioni 1269 byte.
2. Il throughput è dato dal rapporto tra i dati inviati e il tempo impiegato ad inviarli. Poiché la trasmissione di una finestra di dati impiega molto meno (circa 0.53ms) di due volte il tempo di propagazione il througput a livello applicativo sarà circa T_a= 65536*8/220[ms] = 23.8 Mbit/s, mentre quello a livello IP ci calcola tenendo conto del numero di pacchetti inviati moltiplicati 1500: T_{IP} = (1500*44+1309)*8/220[ms] = 24.5 Mbit/s, supponendo che venga sempre inviato anche il segmento di dimensione non massima.
3. La perdita viene rilevata alla fine dell'RTT in cui "cade" t_0 con i primi tre ACK duplicati, sempre nell'ipotesi che vengano inviati 45 segmenti per RTT, dopo i tre ACK duplicati che consentono la ritrasmissione del segmento perso, vengono ricevuti altri 41 ACK duplicati, e di questi ACK bisogna tenere conto per descrivere l'evoluzione della fase di Fast Recovery, in quanto per ogni ACK duplicato viene inviato un nuovo segmento "fuori" dalla finestra originale. Se chiamiamo 1 il segmento perso, quindi il primo della finestra nel momento della ritrasmissione, allora durante la fase di Fast Recovery vengono inviati i segmenti 46--89.
   L'ACK del pacchetto ritrasmesso conferma il segmento 45>= del puntatore superiore della finestra al momento della perdita, quindi termina il Fast Recovery, si pone CNGWND=22 (approssimazione all'intero inferiore del numero di segmenti) e si entra in Congestion Avoidance. Poiché i 44 segmenti trasmessi durante il Fast Recovery innescano tutti l'invio di ACK validi, durante il primo RTT seguente all'uscita dal Fast Recovery la finestra cresce di due segmenti, poi continuerà a crescere di un segmento per RTT fino a raggiungere di nuovo 45, dopo 22+2 RTT dall'istante t_0.
   La dinamica della finestra è schematizzata in Fig. 1.
4. Il comportamento è analogo al punto 3 fino alla ricezione dell'ACK relativo al primo segmento ritrasmesso, tenendo però conto che gli ACK duplicati sono solamente 3+40, perché mancano gli ACK dei segmenti 2 e 3, anche loro persi.
   A questo punto però i segmenti inviati nella fase di Fast Recovery saranno di nuovo ACK duplicati relativi al segmento 2, anche esso perso e quindi si effettua un nuovo Fast Retranmit dopo 3 DupACK per il segmento 2 e si continua il Fast Recovery.
   Anche dopo il recupero del segmento due la dinamica è sostanzialmente identica e allo stesso modo si recupera il segmento 3.
   Durante questi tre RTT di Fast Recovery vengono trasmessi i segmenti 46--87 + 88--129 + 130--171.
   Dopo il riscontro del segmento 3 si esce dal Fast Recovery e si prosegue sostanzialmente come al punto 3 e la finestra tornerà a 45 dopo 22+4 RTT.
   La dinamica della finestra è schematizzata in Fig. 2.
5. In questo caso si procede come al punto 3, però, dopo la ritrasmissione di 1, i segmenti trasmessi "fuori finestra" portano semplicemente altri ACK duplicati per il segmento 1, che il trasmettitore TCP non può usare per rifare un Fast Recovery, quindi va in timeout.
   Non sappiamo quanto sia l'RTO, ma sappiamo che è sicuramente maggiore di 220 ms; possiamo ipotizzare che sia poco più grande, visto che RTT è dominato dal tempo di propagazione e quindi sarà piuttosto stabile e RTTVAR sarà molto vicino a 0. Per semplicità lo approssimiamo con RTO = 1RTT.
   Quando scade RTO viene ritrasmesso il segmento 1 e si aspetta il suo ACK, che ovviamente arriva dopo un ulteriore RTT e richiede l'invio del segmento 2, anche esso perso.
   Dopo un timeout TCP riparte in Slow Start con CNGWND=1 e SSHTR=22, ma avviene una dinamica piuttosto interessante. CNGWND=1 viene inviato Il segmento 2.
   Dopo un ulteriore RTT l'ACK del segmento 2 riscontra 2 richiedendo 3, che viene trasmesso insieme a 4 perché siamo in Slow Start, la trasmissione di 4 è duplicata, perché non era perso ... ma il trasmettitore TCP ovviamente non lo sa. Il ricevitore TCP quanto riceve 3 invierà l'ACK relativo a tutto quello che ha già ricevuto, poiché non ci sono altre perdite e quindi invia ACK di 87, mentre scarta il segmento 4 in quanto duplicato e invia un DupACK di 87, in quanto è l'ultimo segmento ricevuto correttamente.
   Quando il trasmettitore riceve il primo ACK di 87 invia 88 e 89 (ACK valido quindi la finestra cresce), mentre quando riceve il DupACK non fa nulla.

Di qui in avanti l'evoluzione è "regolare" quindi in ulteriori 4 RTT CNGWND raggiunge 22, si entra in congestion avoidance e si prosegue come ai punti 3. e 4., quindi la finestra raggiunge 45 dopo 1+1+1+1+1+4+23=32 RTT.
La dinamica della finestra è schematizzata in Fig. 3.

È evidente che in questo caso andare in timeout comporta tutto sommato un danno di prestazioni limitato, ma qeusto solamente perchè abbiamo approssimato RTO=1RTT, in caso RTO >> di RTT ovviamente la perdita di prestazioni è enorme.

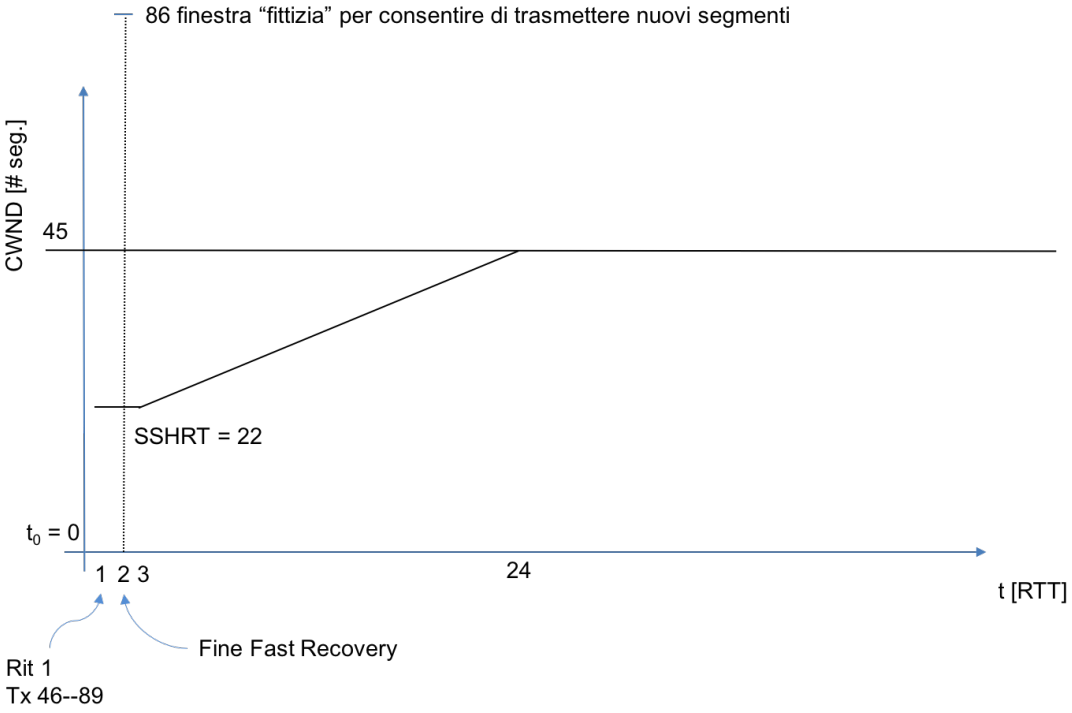


Fig. 1: Dinamica della finestra con una singola perdita

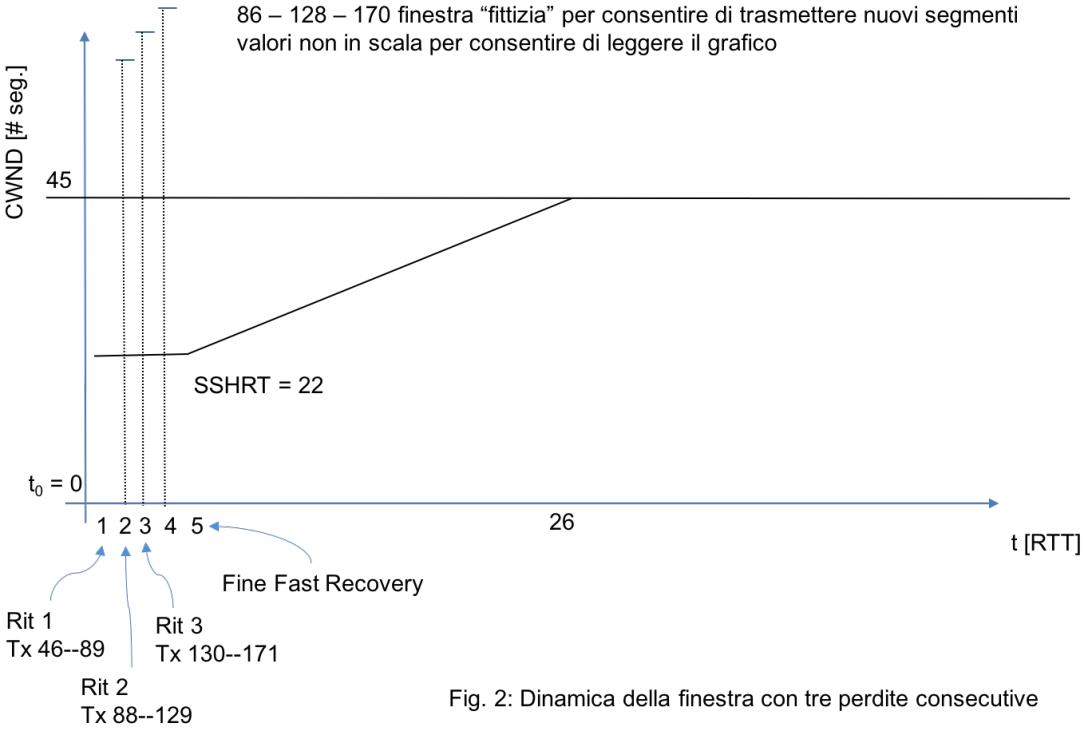


Fig. 2: Dinamica della finestra con tre perdite consecutive

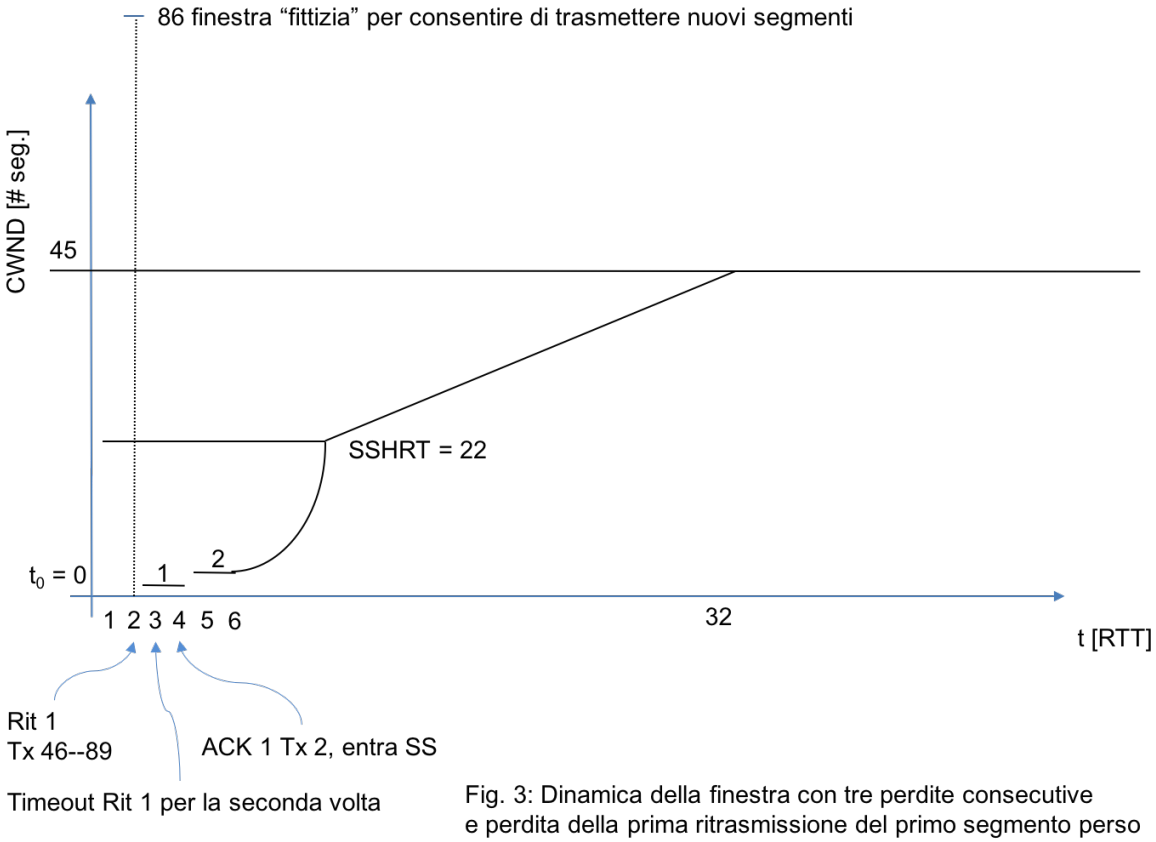


Fig. 3: Dinamica della finestra con tre perdite consecutive
e perdita della prima ritrasmissione del primo segmento perso

Esercizio 3

Rete di connessione verso internet: 2 indirizzi (interfaccia del border router verso l'interfaccia del router dell'ISP, supponendo che questa sia la configurazione, ma siete liberi di scegliere) → 2 bit → /30

Rete 128.152.0.0/30: Addr Min 128.152.0.1 -- Addr Max 128.152.0.2. Totale: 2

Server: 400 indirizzi → 9 bit → /23

Rete 128.152.2.0/23: Addr Min 128.152.2.1 -- Addr Max 128.152.3.254. Totale: 510

Dipendenti: 1200 indirizzi → 11 bit → /21

Rete 128.152.8.0/21: Addr Min 128.152.8.1 -- Addr Max 128.152.15.254: Totale: 2046

Personale: 500 indirizzi → 9 bit → /23

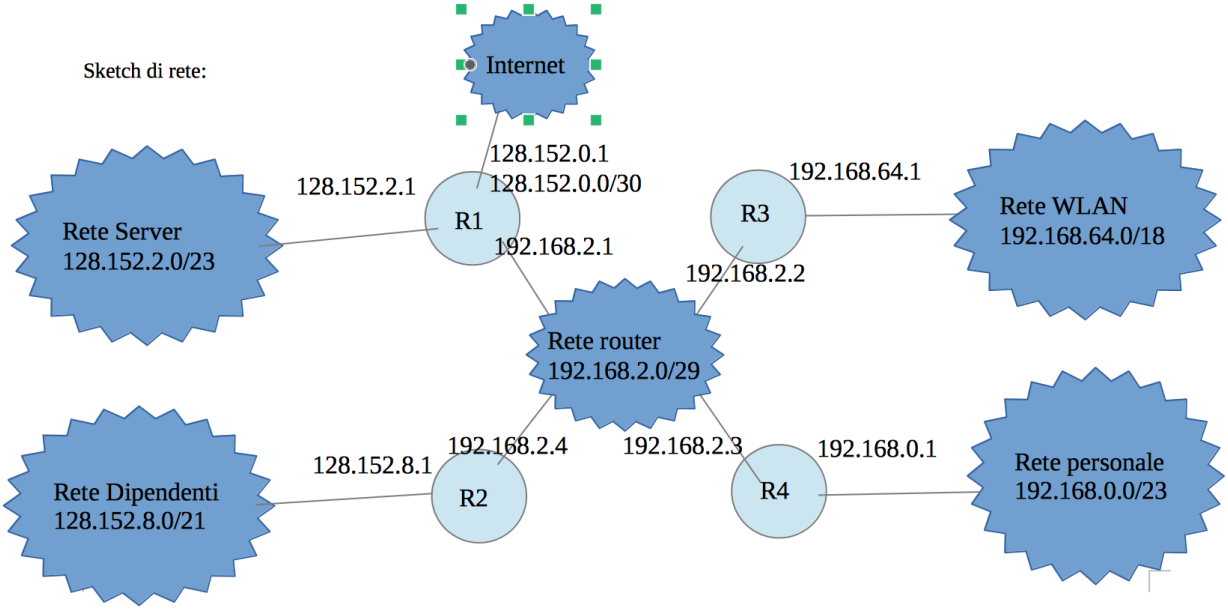
Rete 192.168.0.0/23: Addr Min 192.168.0.1 -- Addr Max 192.168.1.254. Totale: 510

WLAN: 10000 indirizzi → 14 bit → /18

Rete 192.168.64.0/18: Addr Min 192.168.64.1 -- Max 192.168.127.254. Totale: 16382

Rete fra i router: 4 indirizzi → 3 bit → /29

Rete 192.168.2.0/29: Min 192.168.2.1 -- Addr Max 192.168.2.6. Totale: 6




```
Rete per il collegamento a Internet
128.152.0.0/30
netw 10000000.10011000.00000000.00000000
minh 10000000.10011000.00000000.00000001
maxh 10000000.10011000.00000000.00000010

Rete server
128.152.2.0/23
netw 10000000.10011000.00000010.00000000
minh 10000000.10011000.00000010.00000001
maxh 10000000.10011000.00000011.11111110

Rete dipendenti
128.152.8.0/21
netw 10000000.10011000.00001000.00000000
minh 10000000.10011000.00001000.00000001
maxh 10000000.10011000.00001111.11111110

Rete del personale
192.168.0.0/23
netw 11000000.10101000.00000000.00000000
minh 11000000.10101000.00000000.00000001
maxh 11000000.10101000.00000001.11111110

Rete dei router
192.168.2.0/29
netw 11000000.10101000.00000010.00000000
minh 11000000.10101000.00000010.00000001
maxh 11000000.10101000.00000010.00000110

Rete WLAN
192.168.64.0/18
netw 11000000.10101000.01000000.00000000
minh 11000000.10101000.01000000.00000001
maxh 11000000.10101000.01111111.11111110
```

NOTA AGGIUNTIVA: spesso si crea confusione sulla frase sotto (o frasi simili)

“gli indirizzi IP pubblici devono essere presi dal “pool” 128.152.0.0/20, gli indirizzi privati possono essere scelti a piacimento, **ma deve essere possibile il routing diretto all’interno della rete aziendale.**”

Per routing diretto interno si intende che gli host della rete aziendale devono essere in grado di comunicare senza passare per un NAT, quindi di fatto che tutte le sottoreti private devono avere pool di indirizzi disgiunti per non creare ambiguità.

Un'altra domanda che sorge spesso è: “**Come fa un host con IP pubblico a inviare un pacchetto ad un IP privato senza passare per un NAT?**”. A lezione abbiamo visto che gli indirizzi IP privati non sono “routabili” sulla rete Internet perché esistono molteplici istanze di tali reti nel mondo, quindi un indirizzo privato non è univoco, ma può essere associato a molte interfacce. L'indirizzo IP 192.168.0.2 che il router ADSL di casa assegna al portatile sarà assegnato ad altri migliaia di dispositivi al mondo da altrettante migliaia di router ADSL. Tuttavia qui siamo all'interno di una rete aziendale che noi stiamo gestendo, e non c'è alcuna differenza fra gli IP pubblici e quelli privati **all'interno di essa**. La differenza è che quelli pubblici possono essere raggiunti **dall'esterno**, mentre **quelli privati no** (se non tramite NAT o altre tecniche). Sarà il router di collegamento ad Internet che si preoccuperà, in caso, di filtrare i pacchetti provenienti dalla rete aziendale che abbiamo come IP Source Address un indirizzo privato. La differenza fra IP pubblici e privati è semplicemente una convenzione nata prima per consentire la realizzazione di reti “chiuse” con tecnologia TCP/IP senza dover chiedere un pool di indirizzi pubblici all'autorità di assegnazione degli indirizzi, e in seguito anche per ovviare al problema del limitato numero di IP disponibili, con “l'invenzione” del NAT che consente una parziale raggiungibilità di Internet da parte di host con IP privati. I router all'interno della rete aziendale conoscono la struttura della rete interna (se li abbiamo configurati per farlo o se usano correttamente una istanza di un qualsiasi protocollo di routing intra-AS) quindi, ad esempio, l'host 128.152.2.1 della rete server può benissimo inviare un pacchetto con destinazione 192.168.0.1 della rete del personale. Questo verrà preso in carico dal router collegato alla rete 128.152.2.0/23 e lo inoltrerà al router responsabile della rete 192.168.0.0/23.

Soluzione del punto 4. Scegliamo di mostrare la configurazione della tabella di routing del router collegato alla rete dei dipendenti (R2). Definiamo come interfaccia "int0" quella con IP 128.152.8.1 e "int1" quella con IP 192.168.2.4.

Destinazione	Next-hop	Interfaccia
128.152.8.0/21	direct	int0
192.168.2.0/29	direct	int1
192.168.64.0/18	192.168.2.2 (R3)	int1
192.168.0.0/23	192.168.2.3 (R4)	int1
128.152.2.0/23	192.168.2.1 (R1)	int1
0.0.0.0/0	192.168.2.1 (R1)	int1

Essendo il traffico verso Internet smistato dallo stesso router responsabile della rete 128.152.2.0/23, possiamo aggregare le due rotte, eliminando la penultima riga e mantenendo solo quella per il default gateway (l'ultima). Inoltre, omettiamo la rete 128.152.0.0/30 supponendo che il router R1 non la annunci poiché rete di collegamento punto a punto verso Internet.

Esercizio 4

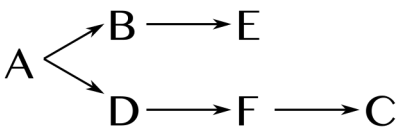
Punto 1: OSPF è un protocollo di tipo link state ed utilizza l'algoritmo di Dijkstra per calcolare i cammini minimi verso tutti gli altri nodi della rete. Iniziamo con il nodo A. L'evoluzione dell'algoritmo è indicata nella seguente tabella. In rosso gli aggiornamenti della tabella.

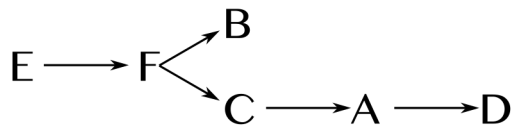
Visitati	B	C	D	E	F
A	1,A	inf	2,A	inf	inf
A,B	1,A	inf	2,A	6,B	inf
A,B,D		inf	2,A		3,D
A,B,D,F		4,F			3,D
A,B,D,F,C		4,F			3,D
A,B,D,F,C,E					3,D

Allo stesso modo, eseguiamo l'algoritmo di Dijkstra per il nodo E, ottenendo la seguente tabella

Visitati	A	B	C	D	F
E	inf	3,E	inf	inf	1,E
E,F	inf	2,F	2,F	inf	1,E
E,F,B	5,B	2,F	2,F	inf	
E,F,B,C	3,C		2,F	inf	
E,F,B,C,A	3,C			5,A	
E,F,B,C,A,D				5,A	

I minimum spanning tree con radice nei nodi A ed E sono dunque i seguenti:





mentre le tabelle di routing sono le seguenti

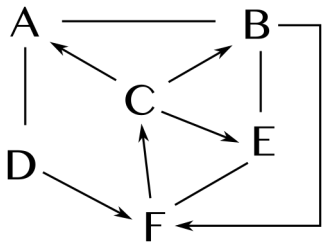
A:

Destinazione	Next-hop
B	~~A~~ B (corretto il 7/02/2017)
C	D
D	~~A~~ D (corretto il 7/02/2017)
E	B
F	D

E:

Destinazione	Next-hop
A	F
B	F
C	F
D	F
F	F

Punto 2: In entrambe i casi stiamo parlando di flooding controllato su link punto a punto, quindi il numero di pacchetti inviati è pari al numero di link esistenti. Il numero dei link in questo caso è 14. Nell'immagine che mostra la topologia, ogni punto rappresenta un'interfaccia. Seguendo il protocollo di flooding alla lettera ogni pacchetto di flooding (che sia visto per la prima volta) viene inoltrato su TUTTE le interfacce, tranne quella di provenienza. Questa è dunque la risposta più corretta. Una risposta "parzialmente" corretta è considerare la presenza di due link asimmetrici (ad esempio da A a D e da D ad A) come una singola rete e quindi singolo dominio di broadcast. In quel caso la topologia nell'immagine diventa la seguente



Quindi il numero di pacchetti inviati è 10. La cosa importante è specificare le vostre assunzioni, quindi i motivi che vi hanno portato a dare una particolare risposta. Numeri ingiustificati verranno considerati risposte errate.

Punto 3: Come abbiamo già detto al punto 2, OSPF utilizza un flooding controllato, ossia quando un router riceve un **nuovo** update (mai ricevuto prima) da un'interfaccia, lo inoltra su tutte le interfacce meno quella dal quale l'ha ricevuto.