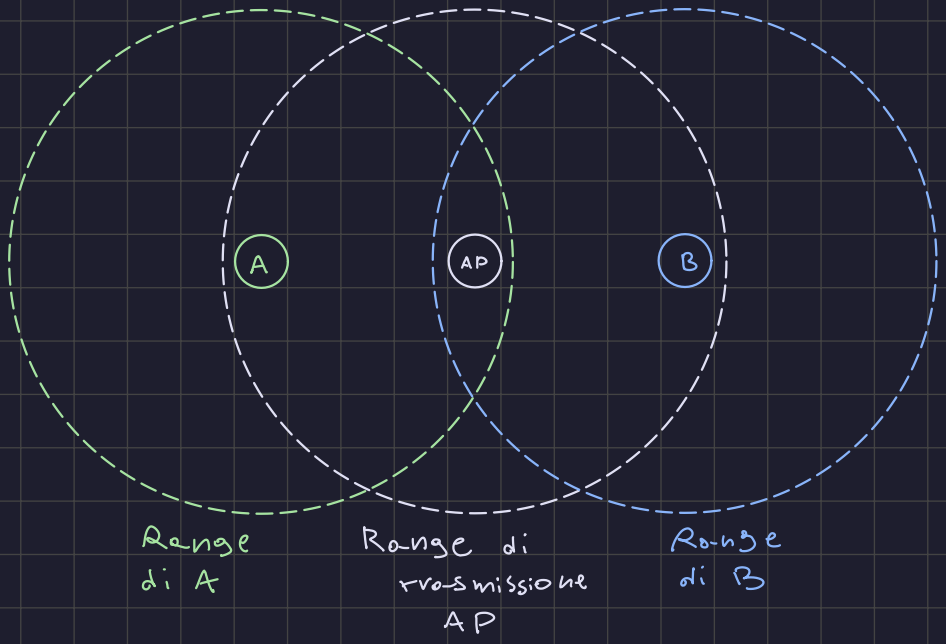
Esame 04/07/23

Domande sulla teoria (4 punti ciascuna)

Lo studente risponda in maniera concisa, ma precisa, alle seguenti domande riguardanti la parte teorica. E' necessario che lo studente ottenga almeno 7 punti (su un totale di 12 punti a disposizione). In caso contrario, gli esercizi non verranno considerati e il voto finale sarà insufficiente.

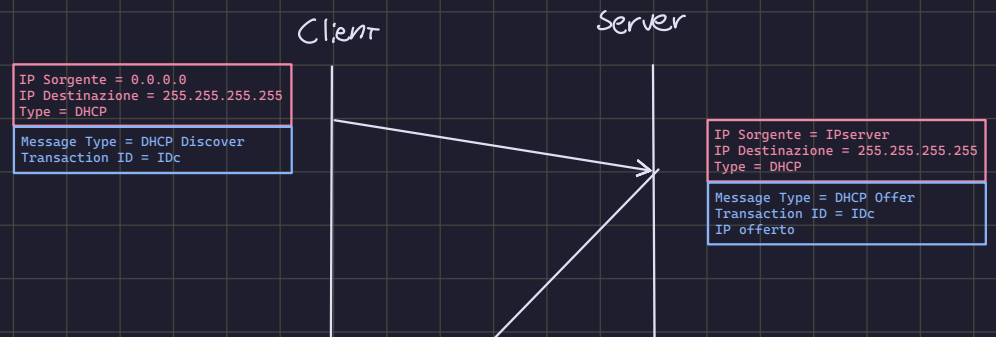
1. Si descriva il problema del "terminale nascosto" (hidden terminal problem) nelle Wireless LAN e la soluzione adottata dallo standard 802.11, indicando in particolare chi genera le diverse trame, chi le riceve e cosa succede se più stazioni generano trame di controllo contemporaneamente.
2. In riferimento al livello di rete, si spieghi che cosa succede quando un host si connette ad una rete ed ha bisogno di ricever un indirizzo IP, specificando le informazioni principali nei messaggi scambiati in rete.
3. Si consideri una connessione TCP già instaurata e lo scambio di segmenti dovuti ad una HTTP GET. Si indichi il valore assunto dai campi dell'header TCP "Sequence Number (SN) e "Acknowledge Number" (AckN) in entrambe le direzioni, spiegando le ragioni dei valori indicati.

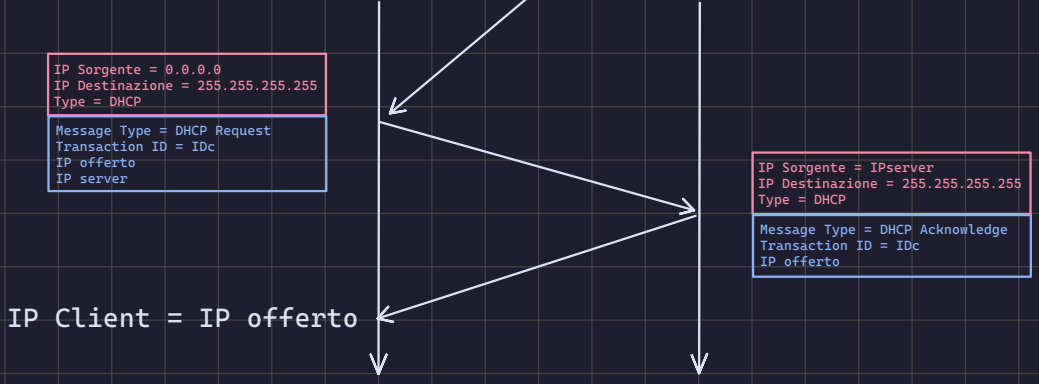
1. Il problema del terminale nascosto nasce quando due stazioni sono posizionate all'interno del range di trasmissione, cioè quel limite oltre il quale il segnale non è più riconoscibile, dell'access point, ma non nel range reciproco come nell'esempio successivo:



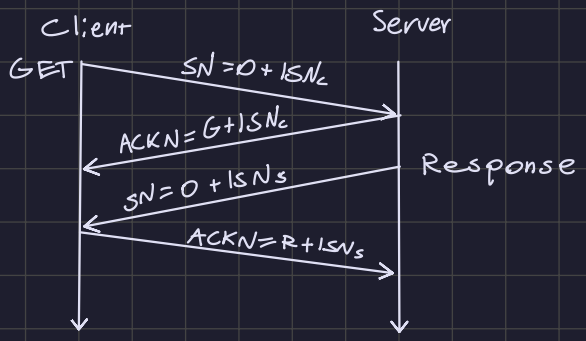
Se la stazione A trasmette una trama all'AP mentre B sta trasmettendo si verifica una collisione perchè l'AP riceve due segnali che non riesce a demodulare, però nè la stazione A, nè la stazione B riescono a rilevare la collisione perchè non essendo nel range di trasmissione reciproco non si percepiscono. Per rilevare una collisione chi trasmette deve ascoltare il canale e rilevare una potenza più alta di quella trasmessa, cosa che in questo caso non può succedere.
La soluzione a questo problema è stata definita nello standard 802.11 che introduce uno scambio di messaggi prima di trasmettere la trama. Chi ha una trama da trasmettere lo annuncia attraverso un messaggio RTS (Request To Send). Il destinatario che riceve un RTS se ha il canale libero invia un messaggio CTS (Clear to Send) che segnala a chi vuole trasmettere che il canale è libero. Tutte le stazioni che non sono coinvolte in questa trasmissione riceveranno i CTS e non essendo i destinatari interrompono la ricezione per un tempo indicato all'interno dell'header del messaggio ricevuto.

2. Quando un host si collega ad una rete e ha bisogno di ricevere un indirizzo IP deve inviare una richiesta al server DHCP. Visto che il nuovo host non conosce com'è fatta la rete invierà un messaggio di tipo DHCP Discover in broadcast perchè non conosce l'IP del server DHCP. Nel campo IP sorgente inserirà l'IP riservato 0.0.0.0 siccome l'host non ha ancora nessun IP e l'host creerà anche un ID da inserire nel campo Transaction ID per identificare la richiesta di un indirizzo IP. Quando il server DHCP riceve il messaggio invierà, sempre in broadcast, un messaggio DHCP offer che contiene l'IP da assegnare al nuovo host e il Transaction ID uguale a quello della richiesta. L'host saprà che è il destinatario della offer in base al Transaction ID e una volta ricevuto l'IP deve, per ragioni di sicurezza, inviare un messaggio DHCP Request, sempre in broadcast, che contiene l'IP che gli è stato offerto e l'IP del server DHCP. Questo viene fatto perchè un altro dispositivo può impersonare il server DHCP. Una volta che il server DHCP riceve il messaggio DHCP Request invia un messaggio DHCP Acknowledge che conterrà l'IP offerto all'host e quando l'host riceverà questo messaggio potrà utilizzare l'IP che gli è stato assegnato. Un esempio di questo scambio è il seguente:





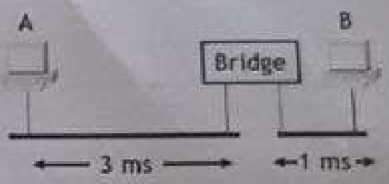
3. Con il protocollo TCP il destinatario deve inviare al mittente la conferma di aver ricevuto il pacchetto, questo meccanismo viene chiamato Positive Acknowledgment with Retransmission e consiste nel inviare un messaggio chiamato Acknowledge che contiene un numero, l'acknowledge number. Questo numero corrisponde al sequence number successivo che il destinatario si aspetta. Il sequence number è un numero che indica l'offset rispetto al byte iniziale del pacchetto. Solitamente al sequence number viene sommato un numero generato dall'host chiamato Initial Sequence Number. Se consideriamo lo scambio di messaggi dovuti ad un messaggio HTTP GET che ha come lunghezza del payload G e un messaggio HTTP Response di lunghezza R si ha la seguente evoluzione supponendo che i messaggi non vengano segmentati:



Il primo messaggio inviato è il messaggio HTTP GET che avrà come Sequence Number 0 + Initial Sequence Number del Client siccome è il primo messaggio e avrà come offset 0. Il server invia il riscontro inviando come Ack Number la lunghezza del payload ricevuto G + Initial Sequence Number, siccome quello è l'offset del prossimo pacchetto che si aspetta. In questo caso il pacchetto non è stato segmentato quindi il client non invia più niente. Il server allora genera la HTTP Response e la invia al client con Sequence number uguale a 0 + Initial Sequence Number del server per lo stesso motivo di prima. Il client una volta ricevuto invierà il riscontro al server settando l'Ack Number a R + Initial Sequence Number del server.

Esercizio 1 (7 punti)

Si consideri la configurazione in figura, dove due segmenti di rete sono collegati da un Bridge; su ciascun segmento vi è una stazione (A e B rispettivamente). Il Bridge è un particolare tipo di stazione che memorizza ciascuna trama che arriva da un segmento di rete e, una volta ricevuta completamente, la ritrasmette sull'altro segmento di rete (tale comportamento è valido, in modo indipendente l'uno dall'altro, in entrambi i sensi); le trame restano in memoria del Bridge fino a quando la trasmissione sull'altro segmento non è andata a buon fine.



Le stazioni e il Bridge utilizzano un protocollo ***CSMA*** 1-persistent. Le caratteristiche del sistema sono:

- velocità dei segmenti: 1 Mbit/s;
- lunghezza delle trame generate dalle stazioni: 1500 byte;
- ritardo di propagazione pari ad 3 ms tra la stazione A e il bridge; ritardo di propagazione pari a 1 ms tra la stazione B e il bridge;

Le stazioni generano le seguenti trame:

- stazione A: tre trame (A1, A2 e A3) agli istanti tA1=500, tA2=539 msec e tA3=565 msec, tutte dirette a B;
- stazione B: tre trame (B1, B2 e B3) agli istanti tB1=495, tB2=525 msec e tB3=545 msec, tutte dirette ad A.

In caso di collisione, si supponga che le stazioni decidono di ritrasmettere Z millisecondi dopo la fine della trasmissione della trama corrotta; il numero Z viene deciso secondo il seguente metodo:

- si attende un tempo pari a Z = Sc * N + T, dove
  - Sc = somma delle cifre che compongono l'istante di inizio trasmissione
  - N = numero di collisioni subite da quella trama
  - T tempo di trama

ad esempio, se l'istante di inizio trasmissione è 418 msec, Z = (4+1+8)*N + T

Determinare:

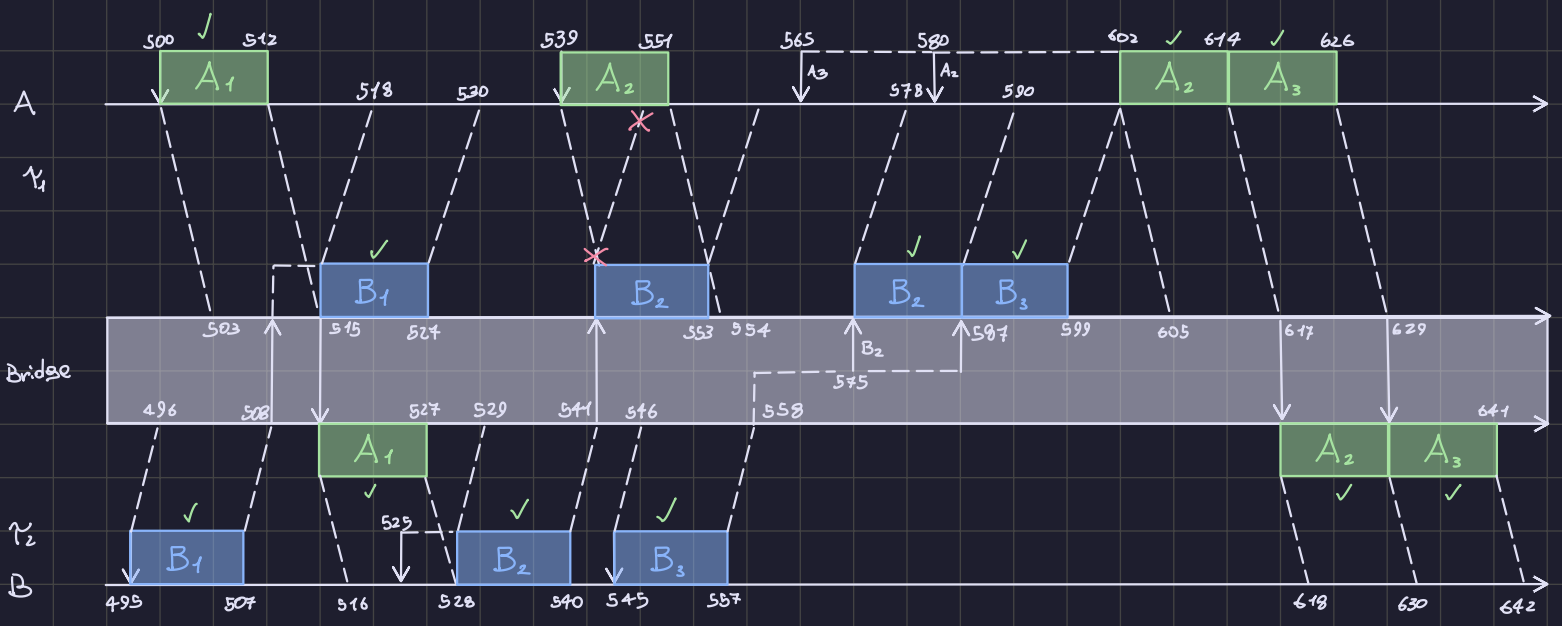
1. graficamente le trasmissioni delle diverse trame, indicando se avviene collisione, in quali istanti essa viene eventualmente avvertita e da quali apparati;
2. il periodo di vulnerabilità del sistema preso in considerazione.

$V = 1\ Mbit/s \quad L = 1500\ byte \quad T = \frac{L}{V} = \frac{1500 \cdot 8}{1 \cdot 10^6} = 12\ ms$

$\tau_1 = 3\ ms \quad \tau_2 = 1\ ms$

A: $t_{A1} = 500$ ms → B; $t_{A2} = 539$ ms → B; $t_{A3} = 565$ ms → B

B: $t_{B1} = 495$ ms → A; $t_{B2} = 525$ ms → A; $t_{B3} = 545$ ms → A



Alla collisione tra B2 e A2:

$z_{A2} = (5+3+1) \cdot 1 + 12 = 29$ ms → 551+29 = 580ms

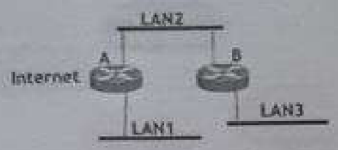
$z_{B2} = (5+4+1) \cdot 1 + 12 = 22$ ms → 553+22 = 575 ms B2 Ritrasmette per primo

Il periodo di vulnerabilità, cioè quel periodo in cui può verificarsi una collisione (dipende dal protocollo utilizzato), di questo sistema è 2τ perchè viene utilizzato il protocollo CSMA Persistent, quindi una collisione può avvenire soltanto nel periodo del ritardo di propagazione tra 2 canali. Tra la stazione A e il bridge il periodo di vulnerabilità sarà 6ms, mentre tra B e il bridge sarà 2ms.

Esercizio 2 (7 punti)

Si consideri la rete rappresentata in Figura, collegata ad Internet attraverso il router A (router di default per la rete). Si hanno i seguenti vincoli:

- Le LAN 1, 2 e 3 devono poter contenere rispettivamente almeno 100, 300 e 400 host;
- la LAN 1 contiene un host con indirizzo 201.176.154.201.



Dati i suddetti vincoli:

1. Si specifichi il blocco CIDR più piccolo da assegnare alla rete;
2. Si assegnino gli indirizzi di rete e di broadcast alle LAN 1, 2 e 3, utilizzando il blocco CIDR individuato nel punto precedente.
3. Si scriva la tabella di routing del router B, considerando come metrica il numero di hop e assumendo che il router A abbia annunciato di poter raggiungere qualsiasi host su Internet in 3 hop.

Lan 1: 100 → 128 → 2^7 host

Lan 2: 300 → 512 → 2^9 host

Lan 3: 400 → 512 → 2^9 host

1. Il blocco CIDR più piccolo si ottiene dal blocco in base due che contiene la somma di tutti i blocchi da assegnare agli host, anch'essi in base 2:

Blocco CIDR = 128 + 512 · 2 = 1152 → 2048 → 2^{11} host

Sappiamo che l'indirizzo di rete avrà bisogno di 11 bit di suffisso, quindi si può ricavare dall'indirizzo appartenente alla lan 1 che è stato fornito:

201 . 176 . 154 . 201

↓

201 . 176 . 1 0 0 1 1 0 1 0 . 1 1 0 0 1 0 0 1

Un indirizzo di rete è caratterizzato da tutti i bit di suffisso posti a 0, mentre un indirizzo di broadcast è caratterizzato da tutti i bit di suffisso posti a 1:

Rete: 201 . 176 . 1 0 0 1 1 0 0 0 . 0 0 0 0 0 0 0 0

Prefisso

↓

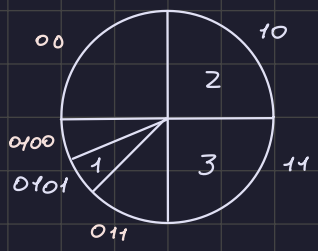
201 . 176 . 152 . 0 / 21

Broodcast: 201 . 176 . 1 0 0 1 1 1 1 1 . 1 1 1 1 1 1 1 1

Prefisso

↓

201 . 176 . 159 . 255 / 21



2. La lan 1 ha bisogno di 7 bit di suffisso, quindi avrà 25 bit di prefisso, di cui 4 appartengono alla sottorete. Possiamo ricavare a quale sottorete appartiene la lan 1 utilizzando l'indirizzo ip che ci è stato fornito:

Rete: 201 . 176 . 1 0 0 1 1 0 1 0 . 1 0 0 0 0 0 0 0

Prefisso Sottorete

↓

201 . 176 . 154 . 128 / 25

Broodcast: 201 . 176 . 1 0 0 1 1 0 1 0 . 1 1 1 1 1 1 1 1

Prefisso Sottorete

↓

201 . 176 . 154 . 255 / 25

La lan 2 ha bisogno di 9 bit di suffisso, quindi avrà 23 bit di prefisso, di cui 2 appartengono alla sottorete:

Rete: 201 . 176 . 1 0 0 1 1 1 0 0 . 0 0 0 0 0 0 0 0

Prefisso Sottorete

↓

201 . 176 . 156 . 0 / 23

Broodcast: 201 . 176 . 1 0 0 1 1 1 0 1 . 1 1 1 1 1 1 1 1

Prefisso Sottorete

↓

201 . 176 . 157 . 255 / 23

La lan 3 ha bisogno di 9 bit di suffisso, quindi avrà 23 bit di prefisso, di cui 2 appartengono alla sottorete:

Rete: 201 . 176 . 1 0 0 1 1 1 1 0 . 0 0 0 0 0 0 0 0 0

Prefisso | Sottorete

↓

201 . 176 . 158 . 0 /23

Broadcast: 201 . 176 . 1 0 0 1 1 1 1 1 . 1 1 1 1 1 1 1 1 1

Prefisso | Sottorete

↓

201 . 176 . 159 . 255 /23

3. La tabella di routing del router B è la seguente:

dst	next hop	cst
Lan 1	A	2
Lan 2	B	1
Lan 3	B	1
Internet	A	3
B	B	0
A	A	1

Esercizio 3 (7 punti)

Un'applicazione A deve trasferire 56100 byte all'applicazione B utilizzando il protocollo TCP. Si supponga che la connessione tra A e B sia già stata instaurata. La trasmissione dei segmenti inizia al tempo t=0. Sono noti i seguenti parametri:

- MSS concordata pari a 1100 byte;
- RCVWND annunciata da B ad A pari a 24200 byte; a partire dal tempo t_a>6.0 la destinazione annuncia una RCVWND pari a 3300 byte; a partire dal tempo t_b>22.0 la destinazione annuncia una RCVWND pari a 17600 byte;
- SSTHRESH iniziale = RCVWND;
- CWND= 1 segmento a t=0;
- RTT pari a 1.0 secondo, costante per tutto il tempo di trasferimento;
- RTO base = 2*RTT; nel caso di perdite consecutive dello stesso segmento, i timeout seguenti raddoppiano fino ad un massimo di 4 volte il RTO base (incluso), dopodiché la connessione viene abbattuta;
- il tempo di trasmissione dei segmenti è trascurabile rispetto RTT;
- il ricevitore riscontra immediatamente i segmenti.

Inoltre si supponga che la rete vada fuori servizio nei seguenti intervalli di tempo:

- da t_1=5.5s a t_2=7.5s;
- da t_3=11.5s a t_4=14.5s;

Si tracci l'andamento della CWND nel tempo e si determini in particolare:

1. il valore finale di CWND (sia graficamente, sia esplicitandolo);
2. i valori assunti dalla SSTHRESH durante il trasferimento (graficamente);
3. il tempo necessario per il trasferimento dei dati (sia graficamente, sia esplicitandolo);
4. il numero di segmenti trasmessi ad ogni intervallo, specificando se ne vengono ricevuti i riscontri o meno (sia graficamente, sia esplicitando i valori).

L = 56100 byte

MSS = 1100 byte

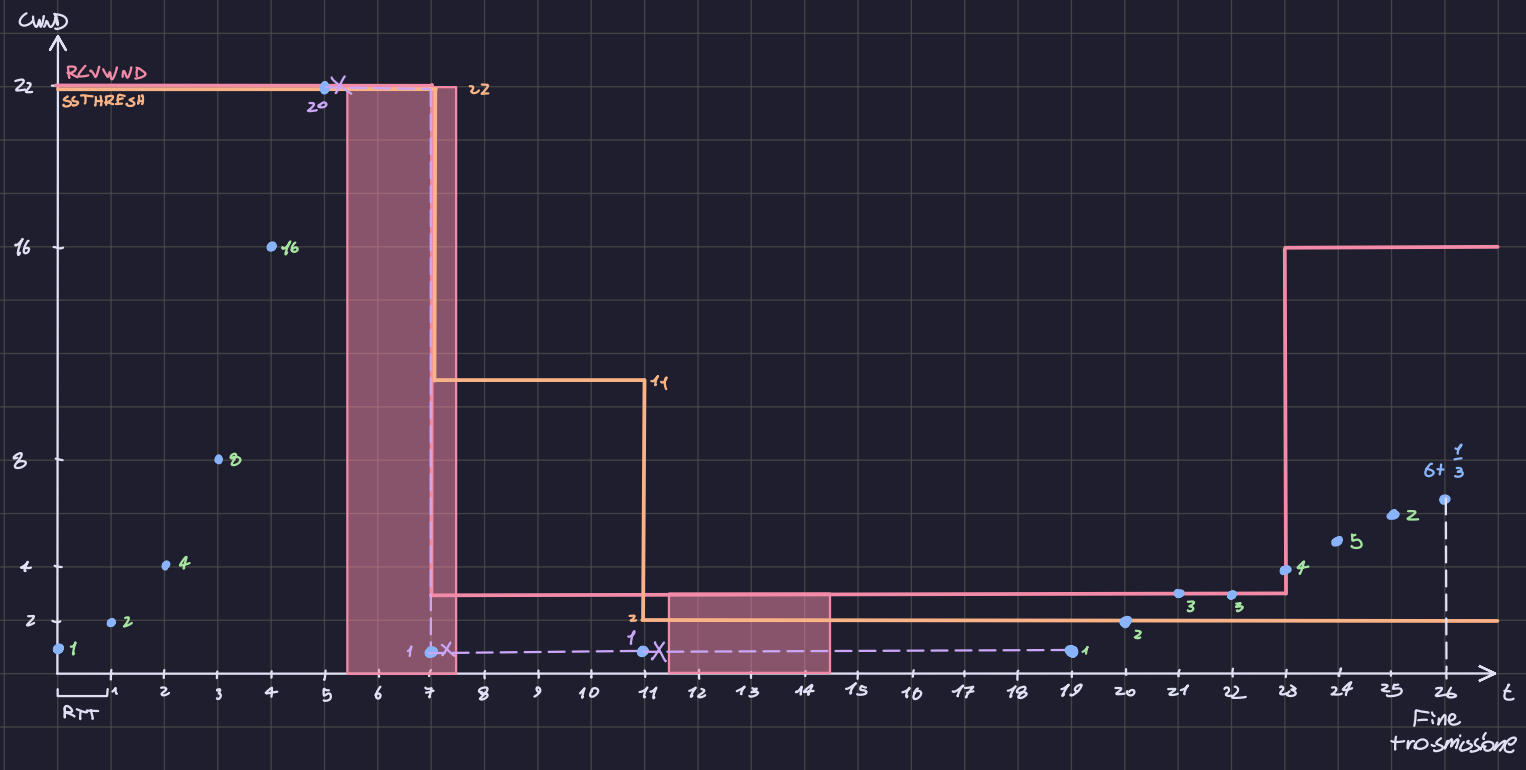
SSTHRESH = RCVWND

RTT = 1 s costante

RCVWND = { 24200 byte $t \leq 6$ = 22 segmenti; 3300 byte $t > 6$ = 3 segmenti; 17600 byte $t > 22$ = 16 segmenti }

DOWN = { (5.5, 7.5) ; (11.5, 14.5) }

$T = \frac{L}{MSS} = \frac{56100}{1100} = 51$ segmenti



#segmenti trasmessi = 1 + 2 + 4 + 8 + 16 + ~~22~~ 20 + ~~1~~ + ~~1~~ + 1 + 2 + 3 + 3 + 4 + 5 + 6 (2)

1 3 7 15 31 ~~51~~ 32 34 37 40 44 49 51

Il tempo necessario per trasmettere tutti i segmenti è di 26 secondi e il valore finale di cwnd è 6 + 1/3 perchè a t = 25 la cwnd vale 6, ma mancano soltanto 2 segmenti da inviare, quindi quando arrivano i riscontri la cwnd verrà aggiornata a cwnd = min(rcvwnd,cwnd_old + #ack/cwnd_old), in questo caso arrivano soltanto 2 riscontri, quindi cwnd = 6 + 2/6 = 6 + 1/3