Domande Reti

1) **Si consideri la tecnica go-back-N per la ritrasmissione di frame errate all'interno di una finestra di livello 2 e si ipotizzi di utilizzare NACK() per segnalare al trasmettitore la frame mancante nella sequenza. In queste condizioni, l'efficienza della ritrasmissione sarebbe migliorata se utilizzassimo ACK cumulativi al posto di NACK()?**

L'efficienza di ritrasmissione non sarebbe migliorata in quanto il protocollo go-back-N prevede comunque la ritrasmissione dell'intera finestra.

Utilizzando un NACK, si implementa una nuova tipologia di avvertimento di errore alla sorgente, portando alla modifica dei formati dell'header, rendendolo più "pesante" da trasmettere.

2) **Come funziona l'opzione Time-Stamp su una connessione TCP in cui si suppone che il ricevente restituisca un ACK ad ogni segmento ricevuto?**

L'*opzione di timestamp* di TCP fu inventata per aiutare TCP a calcolare il ritardo sulla rete sottostante ed è usata anche per gestire il caso in cui i numeri di sequenza di TCP superano 2^{32} (noto come *Protect Against Wrapped Sequence*, PAWS).

Oltre ai campi richiesti di tipo e lunghezza, un'opzione timestamp include due valori: un valore di timestamp e un valore di timestamp di risposta di eco. Un mittente inserisce il tempo dal suo orologio attuale nel campo di timestamp quando invia un pacchetto e un ricevente copia il campo di timestamp nel campo di risposta all'eco, prima d'inviare una conferma di ricezione per il pacchetto. Quando arriva una conferma di ricezione, quindi, il mittente può calcolare accuratamente il tempo trascorso dal momento in cui il segmento è stato inviato.

3) **Elencare le differenza fra Bridge e Switch in una rete IEEE 802.3**

Il bridge è un dispositivo che divide i domini di collisione e, tramite l'utilizzo di opportune tabelle, effettua forwarding, ossia permette lo scambio di frame fra due domini di collisione differenti. Lo Switch funziona come un bridge solo che non svolge CSMA-CD (continua a farlo il bridge), eliminando la contesa migliorano le prestazioni. Inoltre, gli Switch, effettuano flow control, ossia controllano lo stato di memoria in modo tale da avvisare le stazioni quando questa è in procinto di riempirsi, questa tecnica evita il packet dropping. ~~Lo switch è stato introdotto perchè su un server possono essere spedite tantissime frame provenienti da vari host, e se il server fosse direttamente accessibile tutto colliderebbe, quindi si mette uno switch in mezzo che bufferizza il tutto. ???~~
Non operando in CSMA-CD, i collegamenti tra Switch e dispositivo non sono più ad accesso condiviso, ma punto-punto, questo porta ad un netto miglioramento delle prestazioni perchè evita i fenomeni di collisione.

4) **Descrivere e motivare la sequenza di pacchetti scambiata dal protocollo DHCP.**

Il protocollo DHCP (Dynamic Host Configuration Protocol) è un protocollo che tramite il quale un host ~~si autoconfigura assegnandosi un IP~~ ha la possibilità di avere un indirizzo IP, senza che sia manualmente configurato. Questo indirizzo gli viene assegnato da un server DHCP, il quale si può trovare o meno nella stessa LAN; in quest'ultimo caso, il server viene definito DHCP relay. Il funzionamento di questo protocollo prevede lo scambio di 4 pacchetti:

- Discover: viene inviato dal client tramite indirizzi speciali (255.255.255.255 indirizzo destinazione broadcast e 0.0.0.0 sorgente) e contiene un transaction ID per associare le risposte del server, è casuale
- Offer: il server risponde al client con lo stesso transaction ID , l'IP che gli propone, la subnet mask e il tempo di lease, ossia il tempo durante il quale potrà utilizzare questo indirizzo.

- Request: é la risposta del client contenente gli stessi parametri, serve ad accettare l'indirizzo e i parametri proposti. Viene utilizzata per bloccare la scadenza dell'indirizzo lato server.
- Ack: contiene sempre gli stessi parametri di Offer e Request, serve a validare il client e quindi per confermare al client che il request è arrivato al server.

Se il client non dovesse ricevere alcuna offer da parte del server, continua con la "pioggia" di discover. Il server, invece, riserva l'indirizzo IP specificato nella offer per un determinato periodo di tempo, per evitare di esaurire il pool degli indirizzi disponibili.
Se salta una delle 4 parti, il 4 way handshake non è completo e quindi l'indirizzo IP non viene assegnato.

5) **Descrivere l'algoritmo di bit stuffing usato da trasmettitore e ricevitore su una linea punto punto mostrando perché esso consente al ricevitore di identificare una frame senza introdurre ritardi in ricezione.**

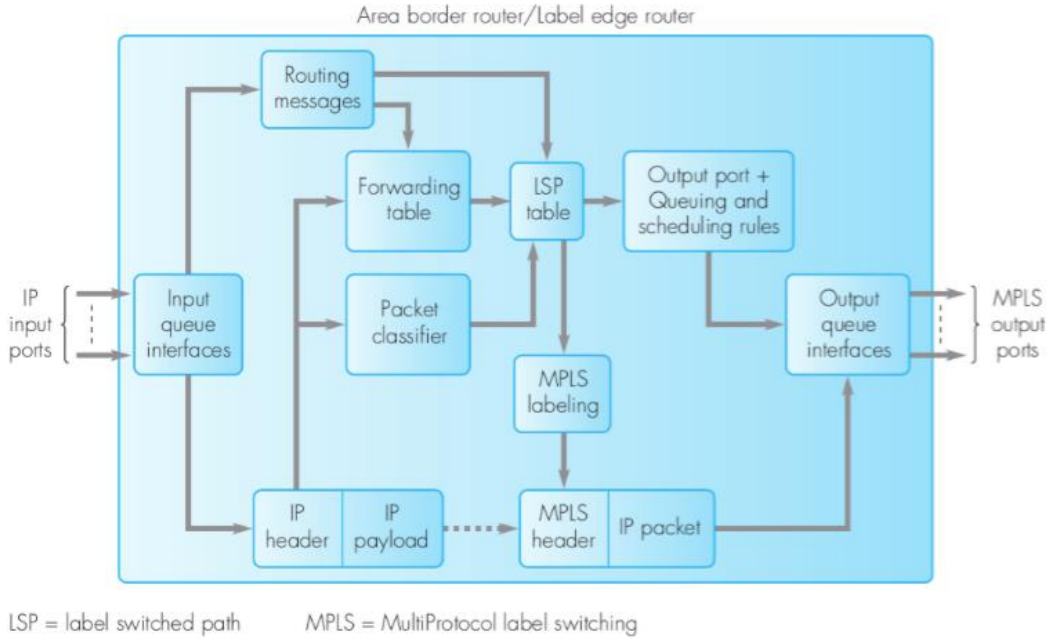
E' una tecnica utilizzata nel livello 2 (Data Link) ed è un miglioramento del character stuffing che risultava inefficiente. All'inizio e alla fine del dato viene aggiunto un flag di 8 bit (01111110). Quindi il frame diventa *01111110 - DATO - 01111110*. ~~Se nel dato si presenta una sequenza uguale al flag~~ viene inserito uno 0 ogni cinque 1. Quindi:
*01111110 - ... 01111110...11111111... - 01111110 diventa 01111110 - ... 011111**0**10...11111**0**111...-01111110*
Il ricevitore, essendo a conoscenza di questo meccanismo, utilizza un contatore di 1, se questo contatore è gia a 5 e il prossimo bit è uno 0 sa che si tratta ancora del dato, in caso contrario sa che è il flag di fine.

6) **In TCP la politica di ritrasmissione opera in parte secondo lo schema go-back-N e in parte secondo quello di Selective Repeat. Quali scelte algoritmiche possiamo citare fra quelle coerenti con Selective Repeat?**

Tra le scelte algoritmiche che possiamo fare troviamo: l'implementazione del fast retrasmit, in modo da ritrasmettere il segmento perso ed evitare che il timer relativo a quest'ultimo scada. S-ACK, in modo che anche il sender lavori utilizzando lo schema di selective repeat

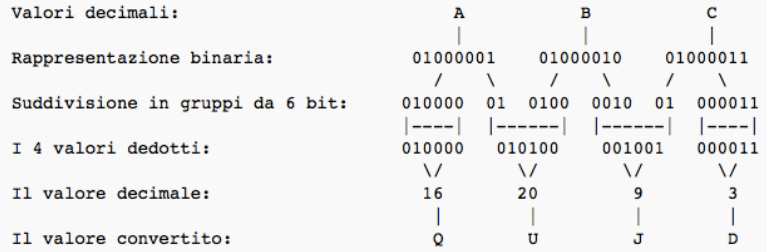
7) **Si consideri un router di bordo di un'area MPLS. Descrivere la sequenza di operazioni che trasformano un pacchetto IP in ingresso in un pacchetto MPLS nelle code di uscita.**

MPLS è un protocollo a priorità che aggiunge ai pacchetti di livello 3 una etichetta.



Quindi alla ricezione di un pacchetto IP, l'indirizzo di destinazione viene usato per determinare la porta di uscita, mentre il valore DiffServ contenuto in DS (primi 6 bit del campo ToS) viene analizzato dal modulo LSP. Con queste informazioni viene creato l'header MPLS per l'hop e quindi scelte le regole di scheduling del pacchetto.

8) **Sia data una stringa binaria di ingresso di 24 bit e l'ipotesi di usare la codifica Base64 per il trasferimento fra due MTA. Descrivere con uno schema a blocchi i passi eseguiti per la codifica e per generare il formato NVT in trasmissione**



Mancano dei passaggi:

Uso i 4 valori prodotti come indice per l'accesso alla tabella B64, per estrarre il carattere voluto.

Da quel carattere, accedo alla tabella ASCII per estrarre i 7 bit che rappresentano il carattere.

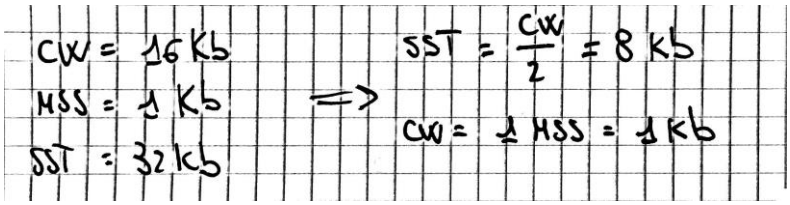
Metto come bit più significativo uno 0, per farli diventare 8 bit.

9) **Una frame di 2Kb deve essere trasmessa fra due calcolatori connessi da un canale di comunicazione in fibra lungo 30Km e avente banda di 20Mbs. Calcolare l'utilizzo del canale se il livello data-link usa un protocollo Selective Repeat con numeri di sequenza rappresentati con 3 bit.**

$tp = 30*10^3 / 3*10^8 = 1*10^{-4}$ $tx = 2000/20*10^6 = 0{,}1*10^{-3}$ $k = 2^3/2 = 4$

$U = 4*(1*10^{-4} / 1*10^{-4} + 2*10^{-4}) * 100 = 133\%$???

10) **L'attuale finestra di congestione (CW) TCP è pari a 16 Kb, MSS di 1 Kb e SST pari a 32 Kb. Stabilire i nuovi valori di SST e CW nella ipotesi di ricevere un**

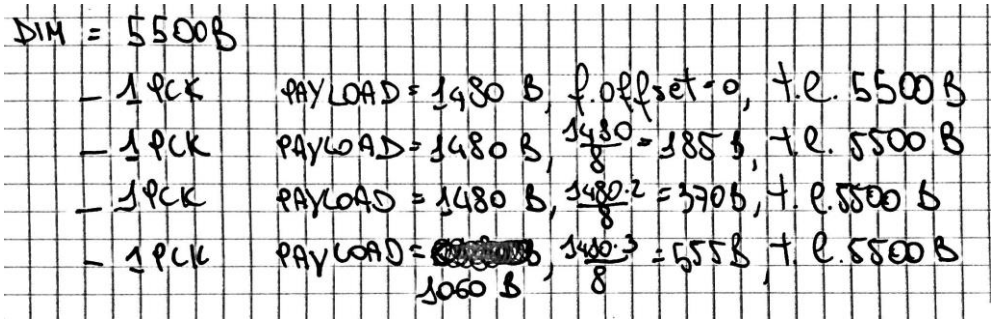


retransmission timeout.

11) **Descrivere le differenze algoritmiche fra go-back-N e Selective Repeat e specificare l'impatto che hanno sulla numerazione della sequenza all'interno della finestra di trasmissione.**

L’algoritmo go-back-n è un algoritmo tramite il quale il ricevitore notifica il mittente che un pacchetto è stato perso, allora egli dovrà rimandare tutti i pacchetti a partire dal primo perso, questo serve a garantire la corretta sequenza dei pacchetti in arrivo. In questo modo il ricevitore non deve allocare memoria se non per il pacchetto appena arrivato che è da mandare al livello ISO/OSI successivo, tuttavia il ricevitore non ha memoria, non può quindi memorizzare tutti i pacchetti e obbliga il mittente a rispedire tutti i pacchetti. Un altro svantaggio è che impiega più tempo. L’algoritmo di Selective Repeat prevede che sia trasmettitore che ricevitore hanno un buffer grande K, mentre prima il ricevitore aveva un buffer a cella singola. In questo modo il ricevitore ha memoria dei pacchetti arrivati quindi il trasmettitore può inviare solo il pacchetto perso. **Go-back-N viene utilizzato** quando il ricevitore ha poca memoria e quando gli errori sulla rete sono pochi. **Selective Repeat** : quando la rete ha il tasso di errore elevato e quando il ricevitore è dotato di sufficiente memoria. Sono comunque utilizzati tutti e due, per esempio TCP può funzionare in entrambi i modi. Impatto sulla numerazione di sequenza: nel GBN, abbiamo bisogno di un numero di sequenza che mi sappia confermare N+1 byte. In SR, invece, deve saper confermare 2N byte. In entrambi i casi, N è la dimensione della finestra.

12) **Una connessione TCP produce un segmento di dimensione 5500 B. Descrivere i frammenti (con i relativi campi significativi) generati dal livello IP sottostante se**



la rete di transito è una LAN Ethernet.

13) **Supponiamo che una stazione CSMA/CD non rispetti la dimensione minima del frame in fase di trasmissione. Quali conseguenze potrà subire nell’accesso a canale condiviso?**

Supponiamo ci siano due stazioni A e B con A che spedisce un pacchetto a B. Se A non rispettasse la dimensione minima del pacchetto potrebbe accadere che A finisca di trasmettere prima che i primi bit del pacchetto arrivino a B il quale potrebbe fare CS e, vedendo il canale libero, spedire a sua volta un pacchetto. Dato che A ha già finito di trasmettere, non sa se il pacchetto che gli arriva è il suo oppure quello di B e quindi non si accorge della collisione. Per questo la dimensione minima di un pacchetto deve essere 2tp.

14) **Perché un sistema NAT genera una propria numerazione di porta diversa da quella della stazione interna, sorgente del traffico?**

Le porte vengono utilizzate per indicizzare univocamente le risposte che provengono da uno stesso indirizzo Internet esterno verso gli Host interni della sottorete. Ogni Host definisce una porta e NAT le registra, potrebbe accadere però che due host definiscano porte uguali, per questo NAT le cambia evitando conflitti.

15) **Cosa si intende con il termine *packet scheduling* e quale algoritmo di scheduling viene preferibilmente utilizzato?**

Il packet scheduling indica la strategia con cui vengono gestiti/spediti i pacchetti. Generalmente si utilizza MPLS che è un protocollo a priorità che fa uso di etichette (label). Abbiamo diversi algoritmi di scheduling, tra cui:

FIFO, non porta alcuna garanzia sul ritardo

Priorità, su alcuni pacchetti può portare starvation

Round robin, divide equamente la banda tra i vari flussi. Ne esiste anche una versione conservativa dove, se per una determinata categoria di flusso non è stato trovato alcun traffico, si passa direttamente a quella successiva senza aspettare la scadenza del quanto di tempo.

Token bucket filter, dove ogni flusso ha un "secchio" in cui raccogliere dei "gettoni". Ogni gettone permette l'invio di una certa quantità di traffico. Per poter inviare il proprio flusso, è necessaria la giusta quantità di gettoni.

Weighted fair queuing, ad ogni flusso viene dato un peso Wi, questo gli permette di avere a disposizione una banda pari a Wi/Sommatoria(Wi).

Random early detection, dove vengono fissati due watermark: basso < alto < capacità totale. Da qui si ricavano 3 regole:

Se la lunghezza della coda < basso → accodo pacchetto

Se la lunghezza della coda è compresa tra basso ed alto → scarto un pacchetto a caso già in coda, ed accodo il nuovo pacchetto

Se la lunghezza della coda > alto → packet drop

Questa tecnica permette di bilanciare il packet dropping, ed evitare che venga influenzato negativamente un solo flusso

16) **Per quale ragione TCP utilizza lo slow start su una connessione appena aperta?**

Lo slow start è una tecnica per la gestione della congestione ~~che evita che si intasi la rete.~~ Nella fase di slow start, ad ogni ACK ricevuto viene incrementata la CW esponenzialmente (CW = 2*CW).Viene utilizzato per testare le capacità della rete. Nella fase iniziale, dove non si sa ancora nulla sulla quantità di banda disponibile, la finestra viene "raddoppiata" ad ogni ACK ricevuto, per far si che le connessioni veloci non siano troppo influenzate dalla fase di slow start.

17) **L'Access Border Router (ABR) di una backbone area MPLS assegna la label 77 ad un flusso di pacchetti IP. Consideriamo ora un altro router backbone area sul cammino minimo dei pacchetti di quello stesso flusso. Tale router può utilizzare la label 77 per identificare un diverso flusso di pacchetti o può usarla solo per lo stesso flusso?**

Può utilizzarla anche per un altro flusso in quanto le label, a differenza degli indirizzi IP, hanno significato ad ogni Hop, infatti in caso di sovraccaricamento di un router gli ABR potrebbero cambiare l'etichetta per instradare il pacchetto in un percorso diverso.
In base all'interfaccia di arrivo e all'etichetta, ciascun pacchetto viene inoltrato sulla corretta interfaccia di uscita. L'etichetta, all'arrivo, identifica anche il modo in cui il pacchetto deve trattato. Di conseguenza, prima di arrivare sulla linea d'uscita, la sua etichetta verrà cambiata, in modo da avere lo stesso tipo di trattamento anche sul router di destinazione.

18) **Sia data una stringa binaria di ingresso di 24 bit e l'ipotesi di usare la codifica Base64 per il trasferimento fra due MTA. Descrivere con uno schema a blocchi i passi seguiti per la codifica e per generare il formato NVT in trasmissione.**

vedi domanda 8

19) **Una frame di 4Kb deve essere trasmessa tra due calcolatori connessi da un canale di comunicazione in fibra lungo 100Km e avente banda di 100Mps. Calcolare l'utilizzo del canale se il livello data-link usa un protocollo Selective Repeat con numeri di sequenza rappresentati con 4 bit.**

$tp = 100*10^3/3*10^8 = 33,3*10^{-5}$ $tx = 4*10^3/100*10^6 = 4*10^{-5}$ $k = 2^4/2 = 8$

$U = 8*(4*10^{-5} / 4*10^{-5} + 66,6*10^{-5})*100 = 3,7\%$

20) **L'attuale finestra di congestione (CW) TCP è pari a 36KB, MSS di 1KB e SST pari a 32KB. Stabilire i nuovi valori di SST e CW nella ipotesi di aver ricevuto il 3° ACK duplicato.**

Secondo RFC 5681 dopo 3 ACK duplicati SST viene posto alla metà della dimenisone della finestra corrente (WC, detta anche flight size) → ~~dimezzato~~ (36/2=18) e la CW viene posta uguale a SST (18). Questo è il protocollo fast retrasmit, evita la fase di slow start.

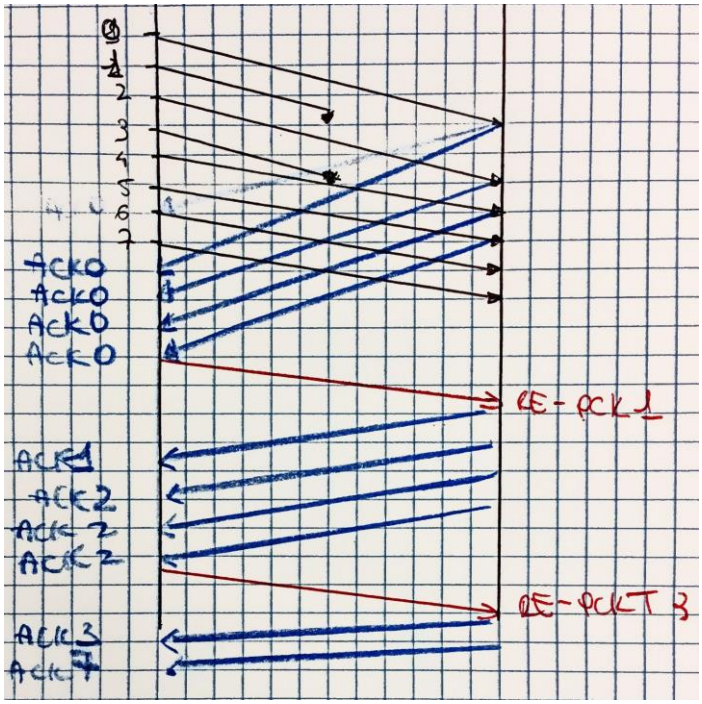
21) **Su una connessione TCP i segmenti trasmessi sono S5 e S6 che sono ricevuti correttamente. Alla ricezione dei rispettivi ACK il sender rileva le misure M5=20 msec, M6=22 msec. Indicare il valore di RTO usato alla trasmissione della sequenza S7 ipotizzando che S5 sia inviato con RTO=32 msec e D=4.**

RTT5 = RTO - 4D = 32 - 16 = 16

RTT6 = 0.9*16 + 0,1*20 = 16
D6 = 0.9*4 + 0.1*(|16-20|) = 4
RTO6 = 16+4*4 = 32

RTT7 = 0.9*16 + 0.1*22 = 16.6
D7 = 0.9*4 + 0.1*(|16-22|) = 4.2
RTO7 = 16.6 + 4*4.2 = 33.4

22) Su una connessione TCP viene trasmessa una finestra di 8 segmenti con sequenza 0-7. Si ipotizzi che i segmenti con sequenza 1 e 3 non raggiungano la destinazione. Descrivere con l'ausilio di uno schema come TCP gestisce la ritrasmissione in base alla politica di Fast Retransmit. Indicare anche la dinamica



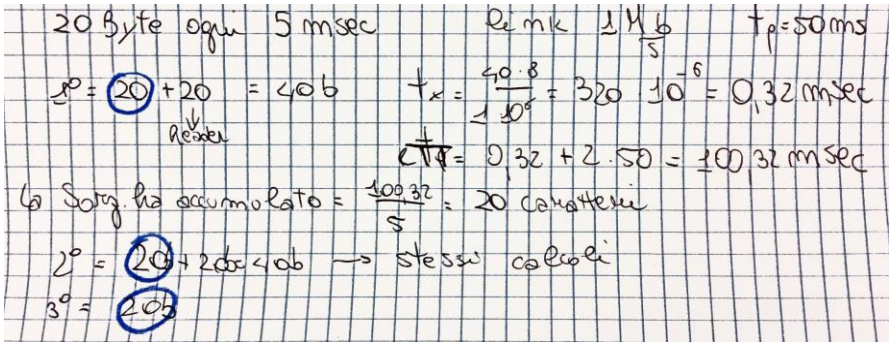
della CW ipotizzando che il valore attuale sia 48K con SST a 32K.

1) cw = 48k sst=32k
2) cw = 24 sst=24
3) cw = 12 sst=12
???

23) **Spigare la politica di Selective-ACK in TCP mostrando i benefici rispetto alla politiche di ritrasmissione adottata di default.**

ACK selettivo invece che ACK cumulativo. Viene specificato il segmento appena arrivato ~~e il segmento precedente~~ ed il numero di sequenza da validare. Permette di validare insieme sia il segmento che la finestra. Così riesco a ritrasmettere i pacchetti che non sono arrivati appena mi torna l'ACK, risolvendo anche multiple loss. S-ACK viene settato come attivo nel primo segmento SYN che il mittente manda al destinatario, ovviamente come campo Opzione. Questa tecnica è molto utile su una rete sulla quale si verificano molti errori. Rispetto alla politica di ritrasmissione TCP l'utilizzo dei SACK è più efficiente perché evita che vengano rispediti tutti i pacchetti a partire da quello perso ma solo quello perso.

24) Sia data una connessione TCP con applicazione iterativa lato trasmissione che produce 20 Byte ogni 5 msec. Se la ritrasmissione avviene su un link da 1Mbps 50msec di ritardo di propagazione dimensionare i primi 3 segmenti inviati sulla connessione ipotizzando l'uso dell'algoritmo di Nagle (nei conti non si consideri l'header di livello 2).



25) **Un host nel dominio di.unimi.it invia una mail a fratta@cs.polimi.it. Descrivere i passi necessari per risolvere il nome cs.polimi.it con una tecnica iterativa e il ruolo giocato dal client di posta elettronica a bordo della macchina utente.**

Essendo di tipo iterativo, il server autoritativo dei nomi conosce gli indirizzi dei domini che (secondo la gerarchia) sono sopra di lui. In sequenza:
di => unimi => it => polimi => cs
In questo modo, non devo risalire alla root.
I ruoli giocati all'interno delle macchine utente, sono:

- Sender manda il messaggio al proprio server di posta, utilizzando il suo User Agent.

(Nel mezzo, i server di scambiano i messaggi utilizzando il Message Transfert Agent, che fa leva su SMTP)

- Il receiver, quando avrà voglia (visto che questo tipo di comunicazione è asincrona), interrogherà il suo server (quello destinazione) per verificare la presenza di nuove e-mail.

26) **Come funziona il label switching a livello 3 e perché è considerato più efficiente del routing su IP?**

Multi Protocol Label Switching è un protocollo di livello 3 che permette di instradare flussi di traffico tra origine (Ingress Node) e destinazione (Egress Node) tramite l'utilizzo di identificativi (label) tra coppie di router adiacenti ed operazioni semplici sulle etichette stesse. L'approccio all'instradamento è molto diverso rispetto al routing tradizionale. Ogni pacchetto ha associata una label, che determina la linea di uscita del pacchetto e il suo trattamento (queuing & scheduling). Questo permette di risparmiare tempo per quanto riguarda il processing, poichè i router non devono esaminare l'indirizzo Ip del pacchetto, ma solo la sua etichetta.

27) **Descrivere la tecnica di source routing nei due approcci di routing: Link State e Distance Vector.**

Nell'ambito dell'Internet Protocol il source routing è la tecnica di specificare all'interno dell'header IP il tragitto (route) che il pacchetto deve seguire. L'algoritmo Distance Vector è un algoritmo distribuito che consente ad ogni router di costruire una **routing table** (Vector) che contiene il **costo di ogni percorso** (Distance) per raggiungere tutti gli altri. Ogni router si costruisce la propria tabella valutando il costo dei link che lo connettono ai propri vicini successivamente ogni router spedisce ai router vicini il proprio vector, cosicchè **ogni router possa scegliere il percorso più rapido** per raggiungere gli altri, controllando se esiste un percorso migliore fornito da un altro router, e, se questo evento si verifica, aggiornando la propria entry. Questa procedura viene ripetuta ad ogni intervallo di tempo per un numero definito di volte, cioè fino a quando tutti i router non abbiano determinato il percorso minimo per tutti gli altri. Questo protocollo può creare problematiche come il count to infinity. Il Link state è simile al Distance vector routing ma quando mi arriva un pacchetto di informazione (link state) della rete lo mando a tutti i nodi tranne a quello che me l'ha mandato (FLOODING) in questo modo tutti i nodi si trasmettono le misure dei costi

(col DV routing solo ai nodi adiacenti) inoltre un nodo è indipendente dagli altri perché ha tutte le informazioni che gli servono per avere una visione completa della rete. La strada più corta (Short Path First) viene calcolata attraverso l'**algoritmo di Dijkstra**. Insieme al vettore di stato viene spedito un numero di sequenza (per accorgersi di loop) e un fattore di aging (per eliminare i pacchetti che continuano a girare nella rete). Le problematiche sono che genera overhead.

28) **Ethernet, e lo standard IEEE 802.3, nascono per risolvere l'accesso a contesa ad un canale condiviso adottando un politica a controllo totalmente distribuito. Tuttavia le installazioni IEEE 802.3 stanno evolvendo nella direzione di adottare switch ai quali le stazioni sono connesse mediante un canale punto-punto. Commentare le differenze concettuali dei due approcci evidenziando cosa si perde e cosa si guadagna dal punto di vista di chi deve progettare una rete aziendale**.

Ethernet è una politica a controllo totalmente distribuito questo significa che se si danneggia una sorgente o si verifica un errore il sistema continua a funzionare dato che ogni elemento è indipendente e non influisce sugli altri (a differenza delle politiche centralizzate come token). Lo switch permette di dividere i domini di collisione e quindi di ridurre le collisioni, tuttavia ha un prezzo maggiore rispetto all'HUB.

29) **Descrivere il protocollo DHCP specificando perché usa un approccio a 4 vie quando un three-way handshake sarebbe sufficiente per accordare DHCP client e DHCP server.**

Il protocollo DHCP (Dynamic Host Configuration Protocol) è un protocollo tramite il quale un host si autoconfigura assegnandosi un IP. Il funzionamento di questo protocollo prevede lo scambio di 4 pacchetti:

- Discover: viene inviato dal client tramite indirizzi speciali (255.255.255.255 broadcast e 0.0.0.0 sorgente) e contiene un transaction ID per associare le risposte del server
- Offer: il server risponde al client con lo stesso transaction ID , l'IP che gli propone, la subnet mask e il tempo di lease, ossia il tempo durante il quale potrà utilizzare questo indirizzo.
- Request: é la risposta del client contenente gli stessi parametri, serve ad accettare l'indirizzo e i parametri proposti.
- Ack: contiene sempre gli stessi parametri di Offer e Request, serve a validare il client e quindi per confermare al client che il request è arrivato al server.

Viene appunto usato anche un quarto messaggio (al posto del three way hand shake) che serve a confermare al client che la sua risposta è arrivata al server.

30) **Un data link layer usa bit stuffing con un preambolo di frame 01110. Mostrare quale sequenza di bit è trasmessa a partire dai dati 0110 0111 0111 1110 e come agisce il ricevitore per non introdurre ritardi nella ricezione di un frame.**

01110 - 0110 011**0**1 011**0**1 1**0**11**0**0 - 01110

01110 - 011**0**0 011**0**1 011**0**1 1**0**11**0**0 - 01110

Il ricevitore, essendo a conoscenza di questo meccanismo, utilizza un contatore di 1, se questo contatore è gia a 2 e il prossimo bit è uno 0 sa che si tratta ancora del dato, in caso contrario sa che è il flag di fine.

31) **Descrivere gli effetti prodotti su un'entità TCP da una primitiva listen() generata lato server.**

La listen crea la coda delle richieste di connessione in ingresso. La dimensione di questa coda viene decisa all'apertura della connessione. Finita la listen, passa alla accept, dove il server si blocca in attesa dell'arrivo delle connessioni.

32) **Motivare l’esigenza di una dimensione minima per le frame IEEE 802.3**
Supponiamo ci siano due stazioni A e B con A che spedisce un pacchetto a B. Se A non rispettasse la dimensione minima del pacchetto potrebbe accadere che A finisca di trasmettere prima che i primi bit del pacchetto arrivino a B il quale potrebbe fare CS e, vedendo il canale libero, spedire a sua volta un pacchetto. Dato che A ha già finito di trasmettere, non sa se il pacchetto che gli arriva è il suo oppure quello di B e quindi non si accorge della collisione. Per questo la dimensione minima di un pacchetto deve essere 2tp.

33) Alle stazioni di una LAN sono assegnati gli indirizzi IP da 10.10.0. 0 a 10.10.0.08. Il router che fornisce accesso a Internet svolge le funzioni di NAT. Riportare la struttura delle tabelle NAT nel caso in cui le stazioni 10.10.0.2 e 10.10.0.8 hanno contemporaneamente una connessione TCP aperta verso il web server sulla macchina 193.128.20.0

Subscriber port		**ISP port**	
Ip Address	**Port**	**Ip Address**	**Port**
10.10.0.2	**2750**	192.183.20.0	80
10.10.0.8	**2751**	192.183.20.0	80

34) **Commentare la politica di ritrasmissione TCP confrontandola con le tecniche Go-back-N e Selective Reapeat**
TCP come politica di Default usa Go-Back N, che si caratterizza per avere il ricevente bloccato in attesa del prossimo frame. Se il ricevente riceve qualcosa di diverso dal frame che si aspettava lo scarta, quindi in caso di errori nella sequenza di ricezione il trasmettitore deve inviare più del dovuto. Opzionalmente TCP può utilizzare l’approccio Selective-Repeat, caratterizzato dal permettere la ricezione di frame fuori ordine che vengono bufferizzati. Se il ricevente non riceve un determinato frame e continua a riceverne i successivi, invece di scartarli li memorizza in un buffer e resta in attesa del frame mancante. Con questo approccio il sender ritrasmette solo frame di cui non ha ricevuto l’ACK e perciò si ha un miglior impiego della banda. Se il “sender” riceve 3 ACK consecutivi che riportano lo stesso numero di sequenza di segmenti TCP, vuol dire che il “receiver” sta ricevendo segmenti successivi a quello che si aspetta (che probabilmente è andato perso).
In questa situazione, che viene interpretata come situazione di congestione lieve, viene adottata la politica “Fast Retransmit”. Tale politica consiste nell’inviare immediatamente il segmento che si capisce essere quello mancante al ricevente per evitare che si crei congestione.

35) **Quali vantaggi introduce il Fast Retransmit di TCP e quali sono le condizioni per il suo utilizzo?**
Fast retrasmit è una tecnica che riduce il tempo che un sender attende prima di ritrasmettere un segmento perso, guadagnando in termini di tempo. Per convenzione il fast retrasmit si utilizza dopo che il sender ha ricevuto il 3° ack duplicato, quindi ora TCP rispedisce immediatamente il segmento senza aspettare lo scadere del timer di trasmissione. Si utilizza anche un timer RTO utile quando si verifica che il mittente non ha più segmenti da inviare, scaduto questo può essere avviata la ritrasmissione.

36) **Le LAN A e B sono collegate mediante un bridge B. Gli host H1 e H2 sono rispettivamente collegati alla LAN A e alla LAN B. Come può H1 risolvere l'IP address di H2 nel suo MAC address?**

La comunicazione di pacchetti a livello 3 prevede la necessità di conoscenza di due indirizzi, l'indirizzo IP e l'indirizzo MAC. Il protocollo ARP dato un indirizzo IP fornisce l'indirizzo MAC, fa utilizzo di due messaggi, ARP request e ARP reply. Questo protocollo opera nella seguente modalità: attraverso una tabella crea corrispondenza tra IP e MAC se per esempio A vuole parlare con B, di cui conosce solo l'indirizzo IP

- Se l'indirizzo IP di B non è associato a nessun MAC, verrà generato un Messaggio **ARP request broadcast** diretto a tutti i nodi della rete
  - Ogni nodo salva l'informazione contenuta nell'ARP request, ovvero la corrispondenza tra IP e MAC del nodo A
  - B manda una risposta **ARP reply** al solo nodo A
  - A salva la corrispondenza tra IP e MAC del nodo B

37) **Il lato server di una sessione FTP sulla macchina 192.16.20.0 apre una connessione attiva sulla propria porta 20 verso il client. Come può il server conoscere la porta lato client da connettere?**

La porta 21 viene utilizzata per lo scambio di informazioni di controllo. Durante questo scambio viene anche comunicata la porta (genericamente la 20) su cui il client intende aprire una connessione passiva. Se, a seguito di tutti i controlli, la connessione è fattibile, il server aprirà una connessione attiva sulla porta comunicata per lo scambio dei file.

38) **Descrivere il funzionamento della tecnica di Label Switching fra due router di una backbone OSPF. Spiegare anche perché tale tecnica velocizza il processing dei processing dei pacchetti.**

Per creare connessioni nei nodi interni, MPLS aggiunge un'etichetta (*label*) ai pacchetti IP da instradare, e suddivide, in generale, l'instradamento complessivo prima con un instradamento IP ai bordi o frontiera della rete tramite router MPLS/IP che inseriscono l'etichetta sul pacchetto IP in transito inoltrandoli ai router interni e poi con un instradamento a commutazione di etichetta nei router MPLS. MPLS è quindi in sostanza una tecnologia d'ausilio all'instradamento IP che, invece di richiedere a ciascun nodo di controllare la propria tabella di routing per stabilire l'interfaccia d'uscita del traffico, permette di stabilire, controllando la label d'ingresso, quali siano le label e l'interfaccia d'uscita per il traffico.

39) **Descrivere la ragione per cui il protocollo BGP supera i limiti del Distance Vector**

BGP usa un approccio Distance Vector, ma opportunamente modificato, sa evitare il count to infinity. Utilizza quello che viene chiamato Path Vector, indica esplicitamente tutto il percorso da fare per raggiungere un AS boundary router. Partendo dai Distance Vector, il Path Vector viene costruito usando le tabelle dei propri vicini e scegliendo il cammino minimo che porta alla destinazione; in questo caso il termine "vicino" può non indicare solo distanza o bit-rate, ma anche distanza dovuta a scelte politiche: questo perchè gli AS boundary routers possono anche trovarsi in diversi stati.

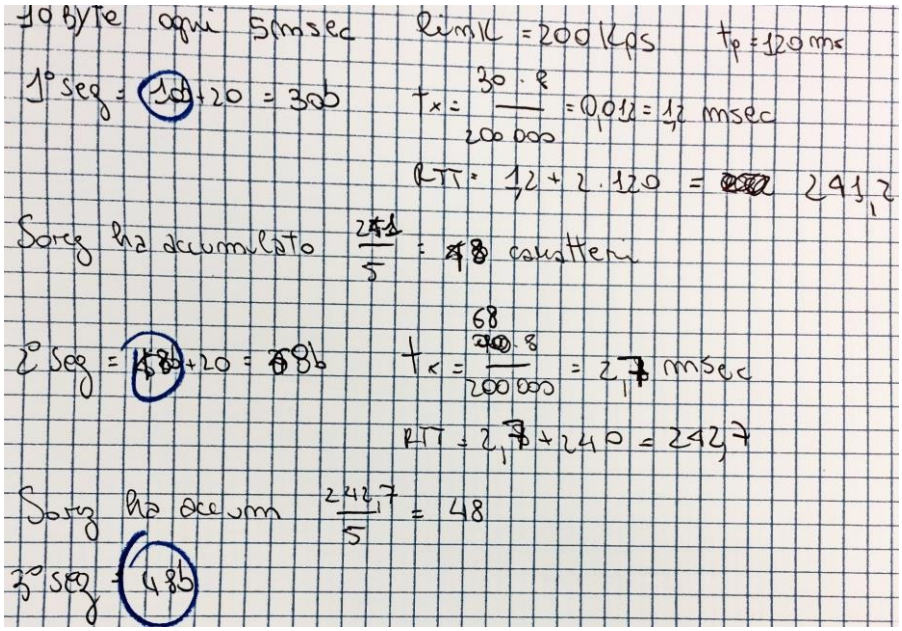
40) **Giustificare la dimensione di 512B per la minima frame di una LAN Gigabit Ethernet**

Questa grande velocità implica un grande problema: mantenendo la lunghezza massima di 2.5 Km e ovviamente volendo ancor poter rilevare le collisioni, ci si è accorti che, visto che su questo cavo un bit ci mette $800/(2*10^6) = 4\mu s$ a tornare indietro bisognerebbe mandare almeno 50000 bit, Quindi la lunghezza massima è stata diminuita a 200 m, da cui sono derivati frame da 4000 bit = 512 byte.

41) **Frame da 2000 bit sono trasmessi su un canale da 1 Mbps con ritardo di propagazione di 100 msec. Utilizzando 4 bit per il numero di sequenza delle frame calcolare l'utilizzo del canale ottenibili con Go-back-N.**

tx = 2000/(1*10^6) = 2 * 10^{-3} k=2^4-1=15 U=15*(2*10^{-3}/(2*10^{-3} + 200))*100 = 14,85%

42) **Sia data una connessione TCP con applicazione interattiva lato trasmissione che produce 10B ogni 5 msec. Se la trasmissione avviene su un link da 200Kbps e 120 msec di ritardo di propagazione dimensionare i primi 3 segmenti inviati sulla connessione ipotizzando l'uso dell'algoritmo di Nagle.**



43) **Su una connessione TCP appena aperta i primi segmenti sono S1 e S2 che sono ricevuti correttamente. Alla ricezione dei rispettivi ACK il sender rileva le misure M1 = 20 msec, M2 = 22 msec. Indicare il valore RTO usato dalla trasmissione delle sequenze S2 e S3.**

RTT1 = M, D1=M/2=10, RTO=60 <—prima misurazione

RTT2 = 0.9*20 + 0.1*20 = 20
D2 = 0.9*10 + 0.1(|20-20|) = 9
RTO2 = 20 + 9*4 = 56

RTT3 = 0.9*20 + 01*22 = 20.2
D2 = 0.9 * 9 + 0.1(|22-20|) = 8.3
RTO3 = 20.2 + 4*8.3 = 53,4

44) **Descrivere il significato della di una porta tagged in IEEE 802.1Q**

~~Una porta tagged è una porta che è visibile su VLAN differenti, altrimenti è untagged.~~

Una porta tagged è una porta in grado di ricevere i pacchetti da più VLAN, ossia l'interfaccia è membra di più VLAN; questo in termine cisco viene detto Trunk.
L'alternativa alla porta tagged, è la untagged, membra di una sola VLAN.

45) **Una connessione TCP produce un segmento di dimensione 5000B. Descrivere i frammenti (con i relativi campi significativi) generati dal livello IP sottostante se la rete di transito è una LAN Ethernet.**

1- payload = 1480B, offset = 0, total length = 5000
2- payload = 1480B, offset = 1480/8 = 185, total length = 5000
3- payload = 1480B, offset = (1480*2)/8 = 370, total length = 5000
4- payload = 560, offset = (1480*3)/8 = 555, total length = 5000

46) **Descrivere le tecniche adottate da OSPF per limitare i costi del protocollo su una backbone area di grandi dimensioni.**

Per Aree di Backbone piccole semplicemente si usa Link State su tutto il sistema, trovando il path migliore per ogni coppia di router. In caso di aree grandi OSPF utilizza un approccio gerarchico, esso permette infatti la divisione di un dominio anche di grandi dimensioni in aree di dimensioni inferiori. Ciascun router non ha quindi più la necessità di essere in grado di raggiungere tutte le reti del dominio, ma è sufficiente che esso sia in grado di raggiungere la corretta area.

47) **Descrivere funzionalità e caratteristiche dell'intestazione estesa "Instradamento" in IPv6.**

~~Se c'è 43 nei bit meno significativi del Next Header, allora si usa Routing. Serve per implementare il source routing. Quindi nell'header ci saranno campi utili a questo scopo come next header e i vari indirizzi.~~

Viene utilizzato per implementare il source routing. Oltre ai classici campi presenti in tutti i next header (posizione del successivo next header, tipo, lunghezza), possiede anche altri campi inerenti all'instradamento come:

- Segment left: indice che indica a quale punto del source routing si è arrivati
- Source rounting bitmap: sono 24 bit in cui i 23 meno significativi indicano il tipo di routing da effettuare: se il bit è = 0 → loose routing, ossia il router che deve essere attraversato non è adiacente. Se bit = 1 → strict routing, il router è adiacente.
- Indirizzi da attraversare: una lista di 23 indirizzi, il cui accesso è possibile grazie al campo segment left.

Nota: la dimensione di questo header è di 46 byte, perchè ogni indirizzo è su 16 byte, ed il campo lunghezza conta i multipli di 8 byte, tranne il primo.

48) **Gestione della finestra di congestione di TCP. Politiche, metriche e significato.**

- Slow start: ogni entità TCP mantiene una variabile Wc detta congestion window variable. All'apertura della connessione il mittente non conosce la capacità e setta quindi Wal valore di MSS concordato. Il mittente invierà quindi un singolo segmento e farà partire un timer di ritrasmissione, se non sarà ricevuto l'ACK prima che il timer scada il segmento verrà reinviato, se invece sarà ricevuto, Wc verrà incrementato a 2 MSS. Il mittente potrà quindi inviare due segmenti ed opererà nel modo indicato precedentemente incrementando Wc per ogni ACK ricevuto. Notiamo che in questo modo la variabile Wc viene incrementata esponenzialmente, questa fase viene detta slow start e continua finchè viene ricevuto un ACK duplicato, un timer di ritrasmissione scade, si raggiunge una certa soglia detta SST (Slow Start Threshold).
- Congestion Avoidance: una volta che la SST è stata raggiunta si entra in una seconda fase detta Congestion Avoidance. Durante essa la variabile Wc viene incrementata di 1/WC per ogni ACK ricevuto. Questa fase continua fino a che non viene raggiunta una nuova soglia e, da quel punto in poi, WC resta costante.
- Fast Retrnsmit: dopo che il sender ha ricevuto il 3° ack duplicato, ritrasmette il segmento perso senza aspettare lo scadere del timer. A seconda della gravità se:
  - Il mittente riceve 3 ACK duplicati: Il livello di congestione viene considerato leggero e quindi, alla ricezione del terzo ACK duplicato il valore di Wc viene dimezzato, SST viene dimezzata e

la procedura riparte dalla fase congestion avoidance. Questa metodologia è detta Fast Recovery.

- Scade RTO: Il livello di congestione viene considerato grave e quindi il valore di Wc viene resettato ad 1, si ricomincia con la procedura slow start e SST viene dimezzata.

49) **Elencare i parametri negoziati da due entità di trasporto all'atto della apertura di una connessione.**

L'apertura della connessione è caratterizzata da uno scambio di segmenti prefissati, cioè:

- Il client manda un segmento con bit SYN attivo
- Il server risponde con SYN+ACK, cioè dice al mittente che ha accettato il suo SYN
- Il client manda un segmento con bit ACK attivo, per validare il SYN+ACK del server

Inoltre, nell'apertura della connessione vengono anche scelti gli ISN (InitialSequenceNumber): essi sono entrambi diversi da 0 e cambiano in ogni connessione, garantendo così che un segmento relativo a una specifica connessione che però è stata chiusa non possa interferire con la prossima.
Ciascuna entità TCP tiene un record di connessione identificata da un connection ID, costituito da una coppia di socket. Quindi connection ID : socket1 (IPS PortS) , socket2 (IPD PortD).
I parametri negoziati sono: la dimensione del buffer di ricezione, la MSS, il timestamp ed il numero di sequenza.

50) **L'Access Border Router (ABR) di una backbone area MPLS assegna la label 38 ad un flusso di pacchetti IP. Considerando gli altri router di backbone area sul cammino minimo dei pacchetti di quel flusso, possiamo affermare che essi usano la stessa label per lo switching dei pacchetti? Quali altre informazioni contengono le tabelle di MPLS?**

vedi risposta 17, non sono sicuro. Le altre informazioni sono:

- Label: identifica la politica per questo hop e contiene l'identificatore per la porta d'uscita
- CoS: stabilisce le regole di scheduling
- Time to Live: determina il numero massimo di router che possono essere attraversati da un pacchetto.

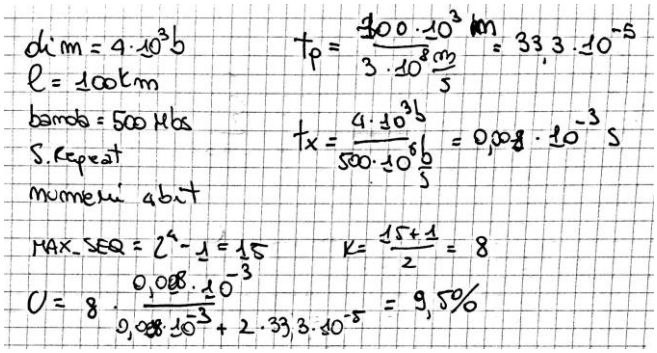
51) **Sia data una stringa binaria di ingresso di 24 bit e l'ipotesi di usare la codifica Base64 per il trasferimento fra due MTA. Descrivere i passi seguiti per la codifica e per generare il formato NVT.**

vedi domanda 8.

52) **Giustificare la codifica 8B6T di una rete Fast Ethernet**

E' una codifica alternativa a quella Manchester, 8 bit binari vengono codificati su segnali ternari (1, 0, -1), questo consente di compattare 4 bit in 3 bit. Questo permette di aumentare il bit rate di trasmissione. Far passare 3 digit su un ciclo di clock introduce delle complicazioni. La capacità del ricevitore deve esser superiore, deve infatti essere capace di distinguere 3 digit diversi invece che 2 (1 e 0). ~~Si può ovviare a questo problema sincronizzando le macchine nel preambolo.~~ Un altro problema si ha quando si devono

53) **Una frame di 4Kb deve essere trasmessa tra due calcolatori connessi da un canale di comunicazione in fibra lungo 100Km e avente banda 500Mbs. Calcolare l'utilizzo del canale se il livello data-link usa un protocollo Selettive Repeat con**



numeri di sequenza rappresentati da 4 bit.

54) **L'attuale finestra di congestione (CW) TCP è pari a 36 KB, MSS 1 KB e SST pari a 30KB. Stabilire i nuovi valori di SST e CW nella ipotesi che si riceva il 3° ACK duplicato.**

Secondo RFC 5681 dopo 3 ACK duplicati SST viene posto alla metà della dimenisone della finestra corrente (WC, detta anche flight size) → (36/2=18) e la CW viene posta uguale a SST (18).

55) **In una rete Gigabit Ethernet a velocità di trasmissione è due ordini di grandezza superiore rispetto allo standard originale di 10Mbps. Quali problemi comporta e come sono risolti per mantenere compatibilità di frame?**

Mantenendo la dimensione della frame invariata e con il nuovo Bit-Rate lo slot time diventa T = 512 bit * 10^9 = 0,512 µs ma il tempo di propagazione sul cavo di 2,5 Km rimane lo stesso (50 µs) che non va bene. E quindi si devono apportare delle modifiche sulla
dimensione minima della frame oppure sulla distanza del cavo oppure una via di mezzo che è quella scelta dallo standard. Le modifiche apportate sono le seguenti:
Distanza massima del cavo 200 m (dal host al ripetitore. quindi da un host all'altro 400 m). Tp = 400 / 2*10^8 = 2 µs e quindi lo slot time T = 2Tp = 4 µs. Dimensione minima della frame = 512 byte dato da Fs = T * Bit-rate = (4*10^-6) * 10^9 = 4000bit = 500 byte ai quali vengono aggiunti 12 byte per mantenere un margine di sicurezza e quindi Fs = 512 byte. Fra i due host i frame hanno dimensione diversa, come faccio a renderli compatibili? Il buffer della porta di IO se riceve una frame da 64b le trasforma in 512b e le trasmette sul filo. Per fare questa estensione si può fare:
clamping: tiene nel buffer la frame più piccola finche non riceve altro fino a raggiungere 512b. Lo svantaggio è che causa attese se per esempio viene spedito un solo pacchetto.
carrier extension: viene aggiunto un padding che poi sarà rimosso in ricezione

56) **Illustrare lo schema DHCP evidenziando gli aspetti più importanti del protocollo**

Il protocollo DHCP (Dynamic Host Configuration Protocol) è un protocollo che tramite il quale un host si autoconfigura assegnandosi un IP. Il funzionamento di questo protocollo prevede lo scambio di 4 pacchetti:

- Discover: viene inviato dal client tramite indirizzi speciali (255.255.255.255 broadcast e 0.0.0.0 sorgente) e contiene un transaction ID per associare le risposte del server
- Offer: il server risponde al client con lo stesso transaction ID , l'IP che gli propone, la subnet task e il tempo di lease, ossia il tempo durante il quale potrà utilizzare questo indirizzo.

- Request: é la risposta del client contenente gli stessi parametri, serve ad accettare l'indirizzo e i parametri proposti.
- Ack: contiene sempre gli stessi parametri di Offer e Request, serve a validare il client e quindi per confermare al client che il request è arrivato al server.

57) **Illustrare la situazione di deadlock fra due entità TCP che viene risolta con il persist timer. Quale architettura può consentire a due host IPv6 di comunicare attraverso una rete IPv4?**

Dato che il window update è stato perso ci troviamo in una situazione di deadlock in quanto entrambi i lati stanno aspettando l'altro. Per evitare che questa situazione si presenti ogni volta che il mittente setta la sua variabile W_S a zero viene fatto partire un timer, allo scadere del quale, se non è stato ricevuto un window update, viene inviato un segmento detto window probe.
A seguito della ricezione di un segmento probe viene inviato un ACK che indicherà la dimensione della finestra, se essa sarà ancora pari a zero il timer ripartirà, altrimenti ricomincerà il flusso di dati. Questa procedura viene ripetuta ogni 60s fino a che non viene ricevuto un valore della finestra diverso da zero o la connessione viene chiusa. La comunicazione fra ipv4 e ipv6 può avvenire tramite dual stack, quindi router e switch devono essere dotati del multiprotocollo, oppure tramite tunneling.

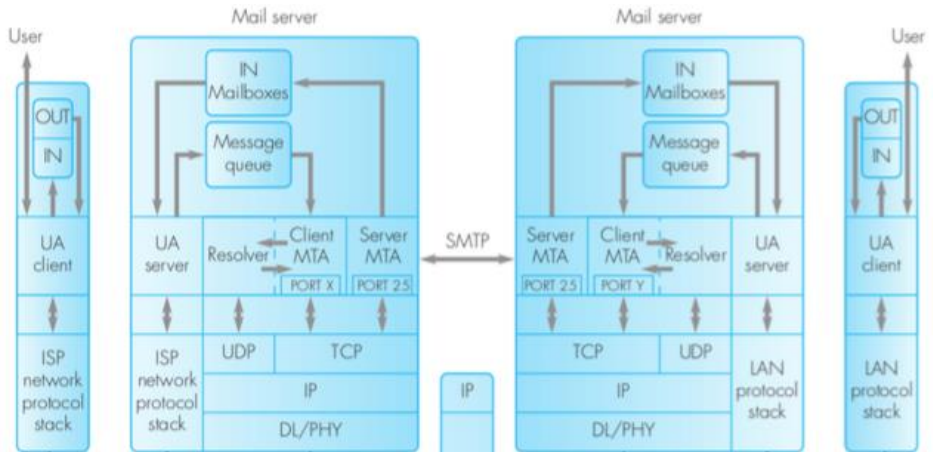
58) **Si consideri una reta a maglia i cui nodi propagano informazioni di costo sui link ai fini del routine. Considerare le tecniche Distance Vector e Link State dal punto di vista prestazionale 1) indicando quale delle due tecniche propaga più rapidamente le misure di adiacenza di un nodo a tutti gli altri nodi e 2) specificando approssimativamente quanti messaggi ogni tecnica richiede. Motivare le risposte.**

1) Distance vector è una tecnica tramite la quale ogni stazione costruisce la propria tabella con costi di link e distanza e successivamente la spedisce ai router adiacenti per calcolare il percorso più rapido. L'approccio link state impiega di meno a spedire le misure di adiacenza, non soffre del problema count to infinity ma prevede lo scambio di molti messaggi.
2) Messaggi distance vector: O(numero router)
   Messaggi link state: $O(n^2)$ <—flooding

59) **Su una connessione TCP il lato client esegue la primitiva connect(). Descrivere la sequenza di eventi previsti dal protocollo TCP per la gestione del comando.**

La connect lato client, fa scattare una richiesta di connessione lato server. Appena ne arriva una il server la accetta, si sblocca dallo stato di wait e procede con una fork dedita alla creazione di un processo figlio il cui scopo sarà quello di effettuare il vero e proprio scambio di dati col sender. Questo figlio, avrà una porta di ricezione diversa da quella del padre. Questo viene fatto per evitare di occupare la porta well-known del server per una sola comunicazione. Per salvare le corrispondenze porta sender – porta "figlio", TCP salva una tabella di smistamento.

60) **Descrivere l'architettura di un server di posta elettronica dal livello 4 al livello 7**.



Come visualizzato in figura, ogni utente si appoggia a un server di posta elettronica, ed esistono due componenti funzionali:
User Agent
- Dell'utente, risiede a livello 7 e gestisce la scrittura/lettura gestione delle mail, consentendone la trasmissione in rete attraverso TCP
- Del server, permette di interagire con gli UA dei client

Message Transfert Agent
- Risiede nel livello 7 del server di posta e si occupa di cercare il server di posta elettronica del destinatario, interrogando il DNS locale
- Si occupa anche di sincronizzare i dati con i client, mantenendo per ognuno di essi una IN mailbox nota come message store

61) **Su una connessione TCP i valori attuali di RTT e RTO sono rispettivamente 30ms e 34ms. Se l'ACK successivo viene ricevuto dopo 36 ms dalla trasmissione del segmento associato, stimare il valore di RTO con cui verrà spedito il prossimo segmento.**

RTT è maggiore di RTO, quindi viene RTO successivo viene raddoppiato a 68.

62) **Sapendo che in una sottorete l'host A ha indirizzo IP 172.28.30.145, si calcolino netmask e indirizzo IP del gateway, sapendo che gli sarà allocato l'ultimo indirizzo IP disponibile, e in modo che sia possibile collegare ulteriori 28PC.**

28 ind —> 5 bit (/27) netmask: 255.255.255.224 gateway: 172.28.30.173

63) **Frame da 1000 bit sono trasmessi su un canale in fibra da 50Mbs e lungo 120Km. Usando 3 bit di numero di sequenza delle frame, calcolare l'utilizzo del canale ottenibile con Go-Back-N.**

$tx = 1000bit/50*10^6 = 20*10^{-6}$ $tp = 120*10^3 / 3*10^8 = 400*10^{-6}$

$k = 2^3 - 1 = 7$ $U=7*(20*10^{-6} / (20*10^{-6} + 2*400*10^{-6}))*100 = 17\%$

64) **Una connessione TCP che adotta l'algoritmo di Clark ha dimensione di receiver window 5000B e MSS 2000B. Se a lato receiver c'è un'applicazione interattiva che consuma 1B ogni 10msec, e a lato sender c'è sempre disponibilità di dati da spedire, dire ogni quanto il receiver invia un window update, assumendo che i ritardi di propagazione siano trascurabili.**

min(5000/2, 2000) = 2000 consumati in 2000B*10msec = 20 sec

65) **Su una connessione TCP con MSS 1KB, SST a 32Kb sono stati spediti correttamente, dal suo inizio, 36 segmenti. Se il 37° segmento genera un RTO, indicare i nuovi valori di SST e congestion window.**

SST = 16Kb, C_w = 1Kb