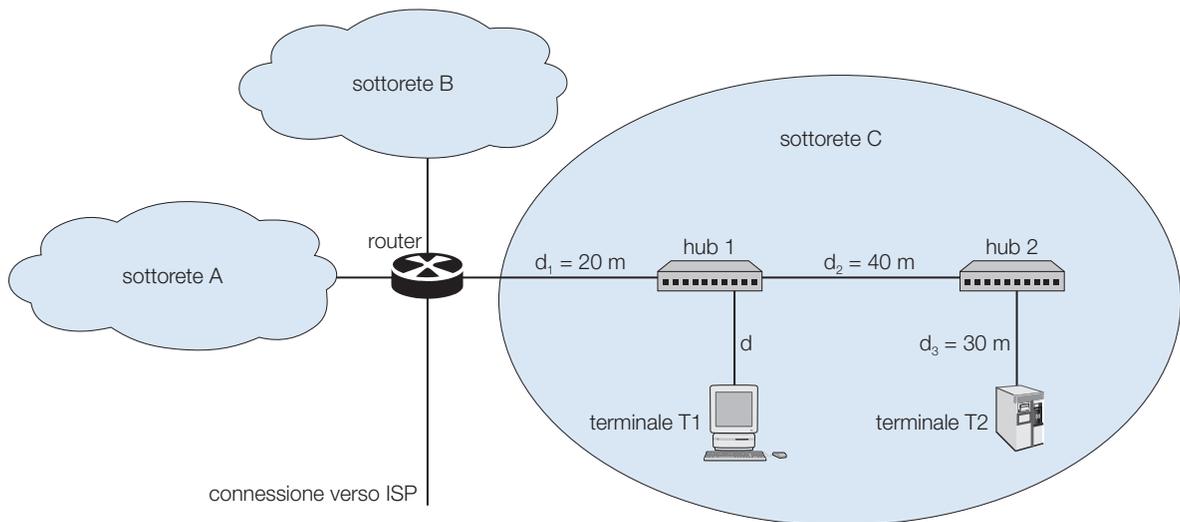


M286 – Esame di stato di istituto tecnico industriale A.S. 2010 – Seconda prova scritta

Indirizzo: ELETTRONICA E TELECOMUNICAZIONI
Tema di: TELECOMUNICAZIONI E PROGETTAZIONE
TELECOMUNICAZIONI

(Testo valevole per i corsi di ordinamento e per i progetti
sperimentali assistiti)

Una rete aziendale è suddivisa in tre sottoreti come descritto dallo schema di massima che segue.



Oltre a quanto indicato, valgono le seguenti condizioni:

- la sottorete A è costituita da 200 host;
- la sottorete B è costituita da 80 host;
- la sottorete C funziona secondo lo standard Ethernet (802.3) alla velocità di 100 Mbps, è costituita da 25 host di cui una parte collegata a Hub1 e una parte a Hub2; la velocità di propagazione dei segnali sulle linee può essere ritenuta di $2 \cdot 10^8\text{ m/s}$ e il ritardo di propagazione attraverso ciascun hub è stimabile in $1\ \mu\text{s}$;
- lo scambio dei dati avviene usando protocolli che prevedono l'aggiunta di un header di 20 byte sia a livello trasporto, sia a livello rete; solo il livello trasporto è confermato e il controllo di flusso avviene con procedura stop and wait.

Il candidato, formulata ogni ipotesi aggiuntiva che ritiene opportuna, produca quanto segue.

1. Descriva gli aspetti fondamentali dello standard di funzionamento della sottorete C esaminando, in particolare, quali conseguenze comporti l'uso dei due hub connessi in cascata.

2. Sapendo che T_1 e T_2 sono i terminali più lontani dal rispettivo hub, calcoli il massimo valore che può assumere la distanza d tra T_1 e Hub1, nell'ipotesi che le trame trasmesse abbiano una lunghezza minima di 64 byte.
3. Individui e illustri una soluzione che permetta di aumentare la distanza tra terminale T_1 e Hub1 senza alterare la struttura della sottorete C.
4. Sapendo che l'Internet Service Provider può assegnare indirizzi IP di classe C contigui da 192.220.15.0, proponga un piano di indirizzamento che minimizzi il numero di indirizzi da richiedere all'ISP e lasci il minor numero di indirizzi inutilizzati in ciascuna delle sottoreti.
5. Riguardo alla comunicazione tra due terminali della sottorete C, stimi la massima velocità di trasmissione dell'informazione vista sopra il livello trasporto e spieghi come possa essere incrementata senza aumentare la velocità di trasmissione a livello fisico.

Soluzione

A mio parere il tema d'esame può essere svolto nei due seguenti modi.

- *Soluzione 1*: svolta con un approccio che riporti le problematiche proposte in un contesto pratico e attuale.
- *Soluzione 2*: svolta con un approccio teorico svincolato dalle soluzioni effettivamente impiegate nelle reti attuali.

Soluzione 1

Come ipotesi aggiuntiva si ritiene di dover adeguare la struttura di rete e i protocolli impiegati a quanto viene effettivamente utilizzato nelle reti attuali. Di conseguenza:

- si sostituiscono gli hub con degli switch amministrabili;
- si impiegano i protocolli della suite TCP/IP per le funzioni degli strati OSI 3-7; il protocollo di trasporto che si impiega, il TCP (*Transmission Control Protocol*), aggiunge normalmente un header (intestazione) di 20 byte ma opera a finestra di trasmissione e non in modalità stop and wait.

Quesito 1

Per la prima richiesta si può rispondere come segue.

- a. Si sintetizza il principio di funzionamento del metodo di accesso multiplo CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*) impiegato nelle LAN Ethernet (famiglia di standard¹ IEEE 802.3) per disciplinare l'accesso al mezzo trasmissivo:
 - in una rete con hub si opera sempre in Half-Duplex (HD) per cui può trasmettere una sola stazione alla volta e le stazioni si contendono l'accesso al mezzo trasmissivo;
 - prima di iniziare a trasmettere, una stazione deve verificare che sulla coppia di ricezione (RX) non vi sia segnale (*Carrier Sense*);

¹ Per la precisione lo standard IEEE 802.3 originario, che si riferiva a reti a 10 Mbit/s su cavo coassiale (10BASE5), ha avuto diversi «emendamenti» (*amendment*) che hanno aggiunto funzionalità e migliorato le prestazioni; per esempio le LAN Ethernet a 100 Mbit/s (come la 100BASE-TX) sono standardizzate come IEEE 802.3u.

- quando una stazione inizia a trasmettere continua a verificare (CD, *Collision Detection*) che sulla coppia di ricezione non vi sia il segnale trasmesso da qualche altra stazione, e questo viene indicato con il termine *collisione*;
 - quando una stazione rileva una collisione interrompe la trasmissione e invia un segnale di disturbo (detto *jam*) che comunica a tutti l'avvenuta collisione; le stazioni che hanno rilevato la collisione interrompono ogni trasmissione e attendono un tempo calcolato in modo pseudocasuale prima di ritentare.
- b. Si illustra il principio di funzionamento degli hub e degli switch nel modo seguente.
- Un *hub* è un apparato che opera esclusivamente sullo strato fisico (strato 1 OSI): esso ritrasmette su tutte le altre sue porte il segnale che riceve da una porta, comportandosi perciò come se fosse un bus (FIGURA 1A, a pagina seguente). L'insieme di tutti gli host (computer, stampanti di rete ecc.) collegati agli hub di una rete costituisce un *dominio di collisione*. I difetti degli hub sono essenzialmente i seguenti:
 - consentono solo comunicazioni in Half-Duplex, in quanto una sola stazione alla volta può trasmettere dati in rete;
 - il numero di collisioni che si verificano aumenta all'aumentare del numero di host, nonché del numero di hub e della lunghezza dei cavi di collegamento (per via dei ritardi da essi introdotti);
 - all'aumentare del numero di collisioni si determina una diminuzione dell'effettiva velocità di trasferimento di informazioni (nota anche come *throughput* o *goodput*); si può indicare che la soluzione al problema è sostituire gli hub con gli switch.
 - Uno *switch* è un apparato che opera sugli strati OSI 1 e 2 (per questo è anche detto *switch layer 2*); uno switch analizza l'intestazione (*header*) dei frame² Ethernet/MAC IEEE 802.3 utilizzando gli indirizzi MAC in essa contenuti nel seguente modo:
 - l'indirizzo MAC sorgente contenuto nei frame che giungono a ciascuna porta dello switch viene inserito in una *tabella di switching* (nota anche come CAM, *Content Addressable Memory*) associandolo al numero della porta stessa;
 - l'indirizzo MAC di destinazione, invece, viene utilizzato per ricercare nella tabella di switching la porta di uscita a cui è associato l'indirizzo MAC di destinazione stesso; se la tabella contiene questa informazione il frame viene inoltrato solo su quella porta (FIGURA 1B, a pagina seguente).

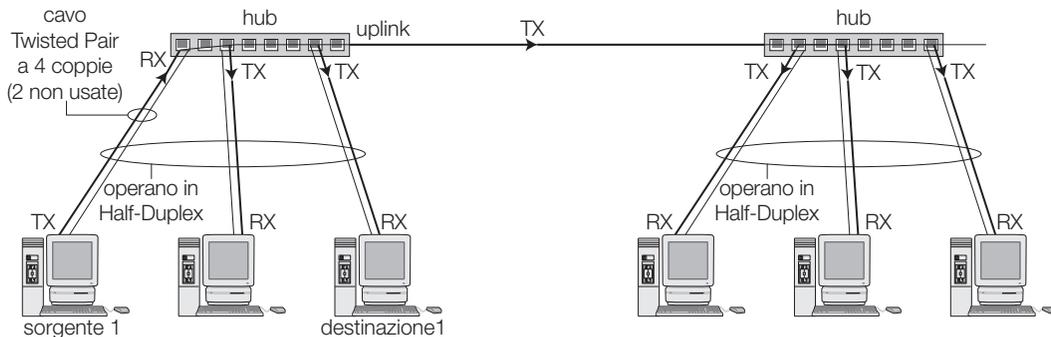
Poiché nelle reti 100BASE-TX il collegamento fra switch e PC viene realizzato separando su due coppie diverse le direzioni di trasmissione e ricezione (Full-Duplex a divisione di spazio) è possibile la comunicazione in Full-Duplex (trasmissione e ricezione contemporanee) al verificarsi delle seguenti condizioni:

² Si preferisce utilizzare il termine inglese *frame* invece di *trama*, in quanto il termine *trama* viene utilizzato di preferenza nell'ambito dei sistemi PCM/TDM per descrivere a livello fisico come viene organizzata la trasmissione.

- i PC sono direttamente collegati agli switch;
- un PC deve scambiare dati con un altro PC (comunicazione di tipo *unicast*, cioè da uno a uno);
- nella tabella di switching sono memorizzati gli indirizzi MAC delle schede Ethernet dei PC, associati alle porte di uscita tramite cui essi sono raggiungibili.

Nelle comunicazioni in Full-Duplex non si fa uso del CSMA/CD in quanto non si possono avere collisioni, aumentando così la velocità di informazione. Uno switch si comporta come un hub solo quando:

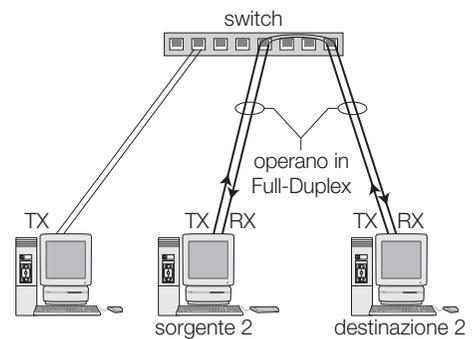
- deve inoltrare dei frame aventi indirizzo MAC di destinazione coincidente con quello di broadcast (tutti 1, ff-ff-ff-ff-ff-ff in esadecimale), comunicazione da uno a tutti, oppure con un indirizzo di multicast (comunicazione da uno a un gruppo di stazioni);
- nella tabella di switching non è ancora memorizzato l'indirizzo MAC della stazione di destinazione.



A

c. Facoltativamente è inoltre possibile:

- illustrare la standardizzazione delle LAN fatta con il progetto IEEE 802;
- disegnare e commentare la struttura di un frame Ethernet II/IEEE 802.3; essa verrà utilizzata per i calcoli del quesito 5;
- indicare che le tecnologie Ethernet forniscono i primi due strati OSI, mentre nella comunicazione fra PC gli strati superiori sono forniti dalla suite TCP/IP. Senza i protocolli TCP/IP la rete non funziona;
- evidenziare le tendenze evolutive della tecnologia Ethernet (multilayer switch, VLAN ecc.);
- illustrare le tipologie di mezzi trasmissivi e i principi del sistema di cablaggio strutturato;
- illustrare le topologie di rete a stella e a maglia;
- indicare che in una rete con un numero rilevante di PC è consigliabile impiegare switch amministrabili in modo da poterli configurare per aumentare la sicurezza della rete, restringendo gli accessi alle porte degli switch (*port security*), e/o per segmentare la rete in VLAN (*Virtual LAN*); le porte che interconnettono gli switch amministrabili sono dette *trunk* (giunzioni).



B

FIGURA 1
A) Principio di funzionamento di un hub.
B) Switch e comunicazione in Full-Duplex.

Per quanto riguarda la seconda richiesta del punto 1, il collegamento di due switch in cascata permette di estendere le dimensioni fisiche di una rete. Bisogna però notare che l'insieme dei computer (o host, più in generale) collegati agli switch di una rete costituisce un *dominio di broadcast*. All'aumentare delle dimensioni del dominio di broadcast diminuiscono le prestazioni della rete perché per le comunicazioni in broadcast uno switch si comporta come un hub.

Una soluzione efficiente a questo problema consiste nell'impiegare switch amministrabili, in modo da suddividere la rete in un certo numero di VLAN (*Virtual LAN*, LAN virtuali). La comunicazione fra PC collegati a VLAN diverse può avvenire tramite un *router*.

Quesito 2

Impiegando gli switch la distanza massima fra PC e switch è di 100 m complessivi, da porta Ethernet del PC a porta Ethernet dello switch. Se lo si desidera è possibile fare riferimento agli standard del cablaggio strutturato per indicare che il cablaggio fisso (in canalina) può essere lungo al massimo 90 m, per lasciare 5 + 5 m ai cavi di interconnessione fra apparati e prese di rete Ethernet.

Nel caso di cablaggio su fibra ottica (essenzialmente per collegare tra loro degli switch o uno switch a un router) le distanze possono essere maggiori e variano in relazione al tipo di fibra ottica impiegata. Si può anche ricordare che nella modalità Full-Duplex non viene attivato il metodo CSMA/CD, per cui la massima distanza fra le stazioni dipende solo dai parametri trasmissivi (massima attenuazione ammessa ecc.).

Quesito 3

Introducendo degli switch al posto degli hub si evita il problema delle collisioni e quindi si può estendere la distanza tra T1 e Switch1 fino a un massimo di 100 m (come prescritto dagli standard Ethernet su coppia simmetrica); nel caso la distanza superi i 100 m è necessario inserire un ulteriore switch. La topologia fisica rimane la stessa, per cui la struttura della sottorete si può ritenere inalterata.

Quesito 4

Facoltativamente è possibile descrivere prima l'architettura della suite di protocolli TCP/IP, il formato degli indirizzi IPv4, il metodo delle classi, il subnetting e il metodo classless. Si fa notare che gli indirizzi proposti sono *indirizzi IP pubblici*, e quindi non devono essere sprecati.

Poiché il numero totale degli host è rilevante si opta quindi per una soluzione diversa, che può essere la seguente: si suppone che la rete proposta sia una normale rete aziendale privata, per cui al suo interno si possono utilizzare gli *indirizzi IPv4 privati*, costituiti dai seguenti tre blocchi di indirizzi³ IP: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16.

³ Poiché una subnet mask è composta da 32 bit dei quali i primi n sono tutti 1 e i rimanenti $32-n$ sono tutti 0, il numero dopo lo «/» che segue l'indirizzo IP indica sinteticamente quale subnet mask si impiega fornendo il numero di bit a 1 consecutivi che sono presenti nella subnet mask. Per esempio, /8 corrisponde alla subnet mask 255.0.0.0 in quanto i primi 8 bit sono a 1 e i rimanenti 24 bit sono a 0.

Impiegando gli indirizzi IP privati, se non vi sono particolari esigenze di sicurezza, non è necessario procedere alla minimizzazione degli indirizzi IP a disposizione delle subnet, in quanto essi sono riutilizzabili liberamente in altre reti non interconnesse con quella in esame.

È così possibile utilizzare un indirizzo di rete in classe C diverso per ogni sottorete, utilizzando la subnet mask /24 (corrispondente a 255.255.255.0), come per esempio:

- 192.168.100.0/24 per la subnet A;
- 192.168.200.0/24 per la subnet B;
- 192.168.300.0/24 per la subnet C.

Il piano di indirizzamento di ciascuna subnet può così seguire i seguenti criteri:

- i primi indirizzi IP sono assegnati agli apparati di rete configurabili (router, switch amministrabili, eventuali Access Point ecc.);
- gli ultimi indirizzi IP sono assegnati ai server presenti in rete;
- un range intermedio di indirizzi IP viene assegnato ai computer (host) client tramite un server DHCP (*Dynamic Host Configuration Protocol*) configurato allo scopo.

Per consentire l'accesso a Internet il router deve implementare la funzione NAT (*Network Address Translation*) che consente a una molteplicità di host appartenenti a una rete privata, che impiega indirizzi IP privati, di accedere a Internet impiegando un *numero limitato* di indirizzi IP pubblici (se la rete è di piccole dimensioni basta un solo indirizzo IP pubblico).

Il router sostituisce nei pacchetti IP in uscita l'indirizzo IP privato con uno pubblico, tenendo traccia della sostituzione effettuata, in modo che il pacchetto possa essere inoltrato su Internet, mentre ripristina l'indirizzo IP privato nei pacchetti di risposta che giungono da Internet, in modo da inoltrarli all'host corretto all'interno della rete privata.

In questo modo il numero di indirizzi IP pubblici da richiedere all'ISP sarebbe limitato a quello degli eventuali server web dell'azienda esposti su Internet (e collocati su una DMZ, *DeMilitarized Zone*) e ai pochi indirizzi IP pubblici da far condividere ai PC, tramite NAT, per l'accesso a Internet, tra i quali si può comprendere anche quello da assegnare all'interfaccia del router tramite cui si accede alla rete dell'ISP.

Quesito 5

Per la soluzione di questo punto è utile illustrare il concetto di incapsulamento delle PDU visto nell'ambito del modello OSI e della suite TCP/IP.

Facoltativamente si possono descrivere le tecniche di correzione degli errori basate su ritrasmissione (ARQ, timeout), e il metodo stop and wait.

Si effettua l'ipotesi aggiuntiva di considerare il protocollo di trasporto TCP (*Transmission Control Protocol*), il quale ha un header di 20 byte ma opera la correzione d'errore e controllo di flusso a finestra di trasmissione scorrevole (*sliding window*), che in linea di principio può essere descritto nel modo seguente.

- La sorgente può trasmettere un certo numero di segmenti TCP (incapsulati in frame Ethernet) consecutivamente, senza attendere la conferma di corretta ricezione di ciascun segmento, nota come ACK (*Acknowledge*).
- La gestione delle ritrasmissioni dei segmenti giunti errati in ricezione (o persi) si basa su un timeout: se il protocollo TCP sorgente non riceve una conferma di corretta ricezione (ACK) dei segmenti trasmessi entro un tempo prestabilito esso ritrasmette i segmenti non confermati.

Inoltre, nel rispondere al primo quesito si suppone che operando su una rete locale non vi siano errori e quindi non vi siano ritrasmissioni. In questo contesto la velocità di trasmissione di 100 Mbit/s comprende l'invio sia di dati sia degli header dei protocolli coinvolti.

Il processo di incapsulamento e la struttura di un frame Ethernet II sono illustrati in FIGURA 2.

Il numero di byte (B) che compongono un frame Ethernet II risulta pari a:

$$N = 8 \text{ (preambolo e SFD)} + 6 \text{ (ind. MAC dest.)} + 6 \text{ (ind. MAC sorg.)} + 2 \text{ (Protocol type)} + 1500 \text{ (max info)} + 4 \text{ (FCS)} = 1526 \text{ B}$$

A essi va aggiunto il periodo di assenza di trasmissione finale che separa due frame, detto IFG (*Inter Frame Gap*), che equivale a 96 tempi di bit (come minimo nel caso di frame trasmessi senza attendere l'ACK) e quindi a 12 byte, per cui è possibile considerare un frame come se fosse costituito da: $N_B = 1526 + 12 = 1538$ byte; e, quindi, da un numero di bit pari a: $N_b = 1538 \cdot 8 = 12\,304$ bit/frame.

Sapendo che i protocolli degli strati 3 e 4 introducono ciascuno 20 B di header si ha che in un frame i byte utili per il trasporto di informazioni sopra il livello di trasporto sono pari a $N_{Bu} = 1500 - 40 = 1460$ byte, corrispondenti a un numero di bit pari a: $N_{bu} = 1460 \cdot 8 = 11\,680$ bit/frame.

Sapendo che in una LAN FastEthernet 100BASE-TX la velocità di trasmissione lorda è pari a 100 Mbit/s, il numero di frame/s trasmessi risulta pari a:

$$N_{frame} = \frac{100 \cdot 10^6}{12304} = 8127,44 \text{ frame/s}$$

Il numero di bit/s informativi trasferiti, cioè la velocità di informazione, o bit rate (BR_A), disponibile sopra il livello di trasporto, nota anche come *throughput*, è così stimabile come:

$$BR_A = 8127,43_{\text{frame/s}} \cdot 11\,680_{\text{bit/frame}} = 94,9 \text{ Mbit/s}$$

In realtà la velocità di informazione è inferiore in quanto vi possono essere dei ritardi aggiuntivi dovuti per esempio ai tempi necessari per la rivelazione d'errore sui frame, tramite il ricalcolo del CRC (*Cyclic Redundancy Check*), l'invio delle conferme di corretta ricezione (ACK) ecc.

Il secondo quesito può essere affrontato nel seguente modo.

L'impiego del protocollo di trasporto TCP, che opera a finestra di trasmissione, consente di ottenere velocità di informazione nettamente superiori a quelle ottenibili con il metodo stop and wait, in quanto:

- il TCP può inviare più segmenti in successione (incapsulati in frame separati solo dall'IFG) senza attendere il riscontro;
- il TCP invia solo le conferme di corretta ricezione (ACK), che possono essere trasmesse anche in frame contenenti informazioni inviate nella direzione opposta nel caso in cui la comunicazione sia Full-Duplex;
- le ritrasmissioni sono gestite autonomamente dal protocollo TCP sorgente attraverso il meccanismo del timeout (se un segmento non riceve una conferma di corretta ricezione entro un tempo prestabilito viene ritrasmesso).

Invece, con il metodo stop and wait si trasmette una PDU (incapsulata in un frame) e prima di passare alla PDU successiva è necessario attendere la conferma di corretta ricezione (ACK), una richiesta di ritrasmissione (NACK) oppure un timeout in caso di errori.

In questo modo l'Inter Frame Gap (IFG) medio aumenta molto, diminuendo significativamente il numero di frame/s trasmessi e quindi la velocità di informazione a disposizione dello strato di applicazione.

Per inciso, opera un trasferimento di file con correzione e controllo di flusso di tipo stop and wait il protocollo di applicazione TFTP (*Trivial File Transfer Protocol*) che però:

- impiega PDU costituite da un header di 4 byte e da un campo informativo di 512 byte;
- si appoggia sul protocollo di trasporto UDP, che aggiunge un header di 8 byte.

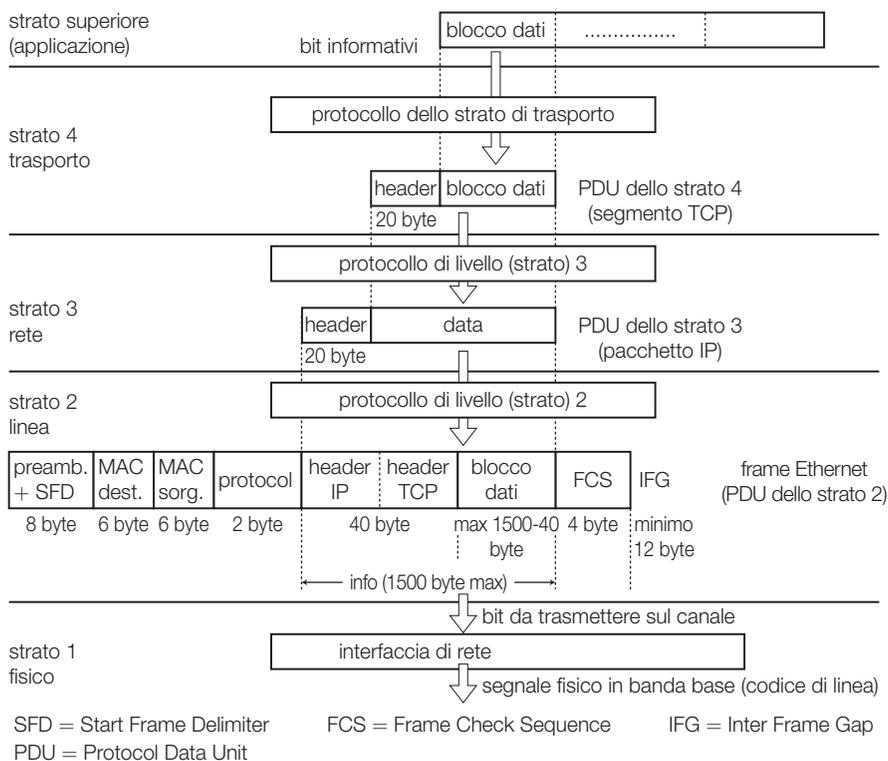


FIGURA 2
Incapsulamento dei blocchi di dati (bit informativi sopra il livello di trasporto).

Facoltativamente si potrebbe anche far presente che per poter aumentare la velocità di informazione (bit rate, BR) senza aumentare la velocità di trasmissione a livello di segnale fisico, detta anche velocità di modulazione (V_m) ed espressa in baud o simboli/s, si può anche ricorrere a una codifica di canale multistato (o multilivello) e alla cancellazione d'eco.

Indicando con M il numero di stati (livelli) utili al trasferimento di informazioni che può assumere il segnale trasmesso in linea e con V_m la velocità di modulazione, o symbol rate, si ha infatti il seguente legame:

$$BR = V_{m[\text{baud}]} \cdot \log_2 M \text{ bit/s}$$

La tecnologia Ethernet utilizza la trasmissione in banda base con un opportuno codice di linea.

Se si utilizza un codice di linea a 2 livelli utili (come il Manchester utilizzato nelle Ethernet 10 BASE T o l'MLT-3 utilizzato nelle Fast Ethernet 100 BASE TX) allora un simbolo (livello) emesso ha associato un solo bit, per cui la velocità di trasmissione lorda (in bit/s) coincide con la velocità di modulazione del segnale fisico (simboli/s).

Se si utilizza un codice di linea a 4 livelli utili ($M = 4$) allora la velocità di trasmissione in termini di bit/s raddoppia a parità di velocità di modulazione (simboli/s).

Come esempio si può illustrare l'evoluzione da Fast Ethernet 100BASE-TX a Gigabit Ethernet 1000BASE-T su cablaggio almeno in categoria 5e, in cui la velocità di trasmissione viene aumentata da 100 Mbit/s a 1000 Mbit/s senza aumentare la velocità di trasmissione a livello di segnale fisico in linea, operando nel seguente modo.

Nelle 100 BASE TX si trasmette in realtà a 125 MBaud con codice di linea⁴ MLT-3, che associa un bit a ciascuno stato, per cui la velocità lorda arriva a 125 Mbit/s su ciascuna coppia.

Si sostituisce il codice MLT-3 con il codice PAM5, che ha un numero di stati utili pari a $M = 4$ per cui il bit rate in linea raddoppia e diviene pari a 250 Mbit/s.

Si utilizzano le 4 coppie di un cavo Ethernet (UTP ecc.) in parallelo, impiegando la tecnica della cancellazione d'eco per realizzare il Full-Duplex, portando il bit rate lordo supportato a 1000 Mbit/s:

$$BR = 4 \cdot 125 \cdot 10^6 \cdot \log_2 4 = 1000 \text{ Mbit/s}$$

Soluzione 2

Quesito 1

Alla prima richiesta si può rispondere illustrando i principi generali delle LAN Ethernet (come visto nella soluzione 1), descrivendo nel dettaglio almeno:

⁴ Nelle 100BASE-TX il codificatore MLT-3 è preceduto da una precodifica di tipo 4B-5B che evita la presenza di lunghe sequenze di 0, ma porta la velocità di trasmissione a $(5/4) \cdot 100 \cdot 10^6 = 125 \text{ Mbit/s}$.

- il metodo di accesso multiplo CSMA/CD (*Carrier Sense Multiple Access/ Collision Detection*) impiegato nelle LAN Ethernet;
- il principio di funzionamento degli hub (FIGURA 1A) e i loro difetti, indicando quindi come sia consigliabile sostituire gli hub con gli switch.

Alla seconda richiesta si può rispondere nel seguente modo. L'interconnessione di più hub in cascata⁵ aumenta il ritardo complessivo, o latenza, in quanto oltre ai ritardi di propagazione dei mezzi trasmissivi utilizzati si aggiunge il ritardo di elaborazione di ciascun hub. Tutto ciò aumenta la probabilità di avere collisioni perché aumenta la probabilità che due stazioni lontane inizino a trasmettere contemporaneamente, in quanto il segnale inviato da una di esse arriva con un ritardo maggiore all'altra estremità. Maggiore è il ritardo e più probabile è avere delle collisioni⁶. Più collisioni vi sono e minore è la velocità di informazione presentata allo strato di applicazione in quanto aumentano i tempi di acquisizione del canale (cioè la possibilità di poter trasmettere effettivamente dei dati).

Quesito 2

La comunicazione fra le interfacce di rete Ethernet (o stazioni) avviene tramite uno scambio di *frame*, cioè *Protocol Data Unit* (PDU) dello strato 2, strutturati secondo lo standard MAC 802.3/Ethernet II.

Nelle LAN Ethernet lo strato fisico delle stazioni (indicato come PHY, *physical layer*, negli standard) ha il compito di effettuare la ricetrasmisione sul cavo dei bit che costituiscono ciascun frame passato allo strato fisico dallo strato MAC.

Terminata la trasmissione di un frame, però, una stazione deve attendere un tempo denominato *InterFrame Gap* (IFG) o *InterPacket Gap* (IPG) prima di iniziare a trasmettere il frame successivo (come mostrato in FIGURA 3). Lo standard IEEE 802.3 prescrive che l'IFG come minimo debba avere una durata equivalente a 96 tempi di bit, corrispondenti a 12 byte.

Il metodo CSMA/CD prescrive, però, che una stazione può trasmettere effettivamente dei dati solo se nessun'altra stazione sta trasmettendo. Una stazione deve quindi poter rilevare le collisioni in tempo utile per interrompere la trasmissione prima di aver completato l'invio del primo frame. Vengono quindi imposti dei limiti alla distanza massima alla quale possono essere poste le due stazioni più lontane.

I limiti sono posti dallo standard Ethernet 802.3 specificando i ritardi massimi consentiti quando si trasmette un frame avente la dimensione minima, pari a 64 byte, a cui vanno aggiunti gli 8 byte di preambolo e SFD (*Start Frame Delimiter*), per un totale di 72 byte, affinché sia possibile rilevare con sicurezza le eventuali collisioni. In questo contesto si introducono i seguenti parametri (FIGURA 3, a pagina seguente).

- *Collision windows* (*finestra di collisione*): è l'intervallo di tempo massimo entro il quale deve venire rilevata una collisione.

⁵ La porta che collega un hub con un altro hub viene denominata *uplink*.

⁶ Esiste una regola detta 5-4-3 per cui, in una rete con hub, tra due terminali (host) si possono avere al massimo 5 segmenti di cavo, 4 hub, 3 segmenti di LAN con collegati degli host.

- *Slot time* (tempo di «apertura»): è l'intervallo di tempo dopo il quale una stazione è sicura di avere acquisito il mezzo trasmissivo, in quanto il CSMA/CD ha risolto le contese e non si possono più verificare collisioni. Nelle LAN Ethernet a 10 Mbit/s (10BASE-T) e Fast Ethernet a 100 Mbit/s (100BASE-TX) la durata dello slot time è pari al tempo necessario per trasmettere i primi 512 bit (comprendenti preambolo e SFD) di un frame. Poiché a 100 Mbit/s il tempo di bit è pari a $t_{bit} = \frac{1}{100 \cdot 10^6} = 10 \text{ ns}$ la durata dello slot time è pari a:

$$\Delta t_{slot} = 512 \cdot 10 \cdot 10^{-9} = 5,12 \mu\text{s}$$

- *Round trip delay* (ritardo andata-ritorno): in questo contesto può essere considerato come l'intervallo di tempo massimo che intercorre fra l'istante di tempo in cui una stazione inizia a trasmettere e l'istante di tempo in cui, rilevata una collisione, la stazione interrompe la trasmissione⁷. Il round trip delay viene valutato fra le due stazioni più lontane e dipende da tutti i ritardi: tempo di propagazione sul mezzo trasmissivo, ritardi introdotti dagli apparati di rete (hub in questo caso), ritardi introdotti dalle schede di rete (trascurati in questo caso).

Il round trip delay massimo non può superare la *finestra di collisione*, che a sua volta deve essere inferiore allo slot time. In questo modo quando si verifica una collisione viene trasmessa solo una parte del frame, che quindi costituisce un frammento (*fragment*) di frame avente lunghezza inferiore a quella minima specificata dagli standard e viene scartato dal ricevitore.

In sostanza, quindi, lo standard IEEE 802.3 relativo alle LAN Ethernet a 100 Mbit/s (100BASE-TX) prescrive che una stazione:

- deve rilevare una collisione prima che sia trascorso uno slot time, corrispondente alla durata di 512 tempi di bit, e quindi a 64 byte;
- in caso di collisione deve interrompere la trasmissione prima di aver trasmesso un frame completo.

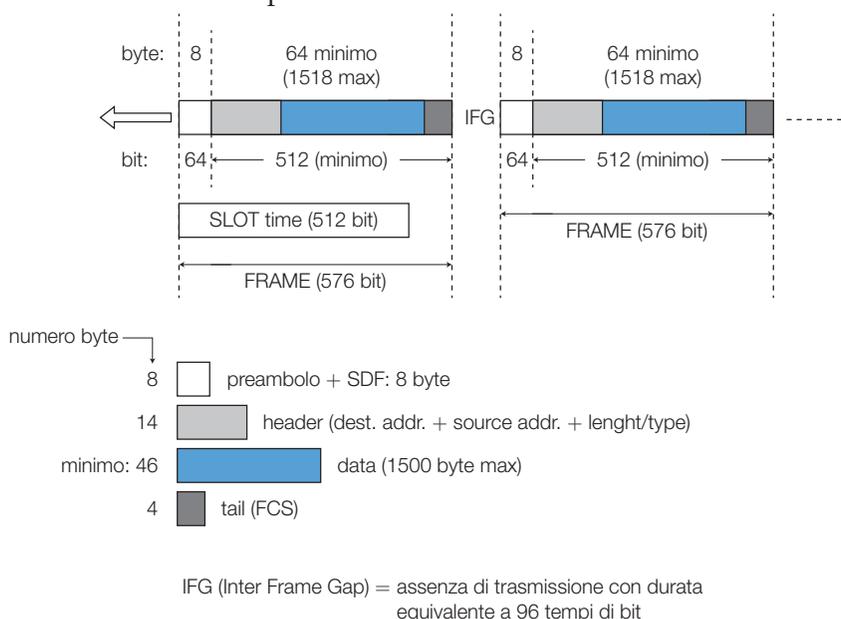


FIGURA 3 Composizione di un frame MAC 802.3/Ethernet e slot time.

7 Dopo avere inviato anche la sequenza di jam, di 32 bit.

Si può quindi affermare che conoscendo la velocità di propagazione sul mezzo trasmissivo e i ritardi introdotti dagli apparati di rete (hub) si può stimare la distanza massima a cui possono essere messe le due stazioni più lontane.

Per determinare la distanza massima d richiesta dal quesito 2. si deve quindi imporre che il ritardo totale tra andata e ritorno del segnale fra i due terminali più lontani, o round trip delay (RTD), debba essere inferiore allo slot time: $RTD < 5,12 \mu\text{s}$. Il ritardo massimo ammesso in una direzione deve quindi essere inferiore a:

$$t_{r_{\max}} < \frac{RTD}{2} = \frac{5,12_{\mu\text{s}}}{2} = 2,56 \mu\text{s}$$

Siccome tra i due terminali più lontani, oltre al cavo di lunghezza d incognita, sono interposti due cavi di lunghezza nota (cavo 2 lungo 40 m e cavo 3 lungo 30 m) e due hub, ognuno dei quali introduce un ritardo pari a $1 \mu\text{s}$, si può scrivere un bilancio dei ritardi con la seguente relazione:

$$t_{r_{\max}} < (t_{rcavo2} + t_{rcavo3} + t_{rHub2} + t_{rHub1} + t_{rcavo_d})$$

Nota la velocità di propagazione sui cavi e la loro lunghezza è possibile calcolare i ritardi introdotti dai cavi 2 e 3, che risultano pari a:

$$t_{r_{-3}} = \frac{30_m}{2 \cdot 10^8_{m/s}} = 0,15 \mu\text{s}; \quad t_{r_{-2}} = \frac{40_m}{2 \cdot 10^8_{m/s}} = 0,2 \mu\text{s}$$

Possiamo quindi determinare il ritardo massimo che può essere introdotto dal cavo avente lunghezza incognita, d , che deve soddisfare la seguente relazione:

$$t_{r_d} < t_{r_{\max}} - (t_{r_{-2}} + t_{r_{-3}} + t_{r_{Hub1}} + t_{r_{Hub2}}) = 2,56_{\mu\text{s}} - (0,15_{\mu\text{s}} + 0,2_{\mu\text{s}} + 1_{\mu\text{s}} + 1_{\mu\text{s}}) = 0,21 \mu\text{s}$$

La lunghezza massima del cavo tra T1 e Hub1 dovrebbe quindi essere inferiore a:

$$d_{\max} < 2 \cdot 10^8 \cdot 0,21 \cdot 10^{-6} = 42 \text{ m}$$

Quesito 3

Una prima alternativa consiste nel sostituire l'hub con uno switch, in quanto quest'ultimo ha costi contenuti che sono ampiamente ripagati dai benefici che offre. In questo modo si può estendere la distanza tra T1 e Switch1 fino a un massimo di 100 m (come prescritto dagli standard Ethernet su coppia simmetrica). La topologia rimane a stella per cui la struttura della sottorete si può ritenere inalterata.

Una seconda alternativa, che però penalizza ulteriormente le prestazioni della rete, sarebbe quella di configurare le schede di rete dei PC affinché operino a 10 Mbit/s. In questo modo lo slot time diventerebbe dieci volte quello calcolato per il quesito 2, in quanto la durata di un bit diviene pari a 100 ns. La distanza massima a questo punto viene limitata dalla massima

attenuazione tollerabile e diviene quella imposta dallo standard 802.3 per le reti su cavi a coppie simmetriche (U/UTP ecc.), che è pari a 100 m.

Altre soluzioni, come impiego di fibre ottiche al posto di cavi in rame, non sono proponibili perché del tutto antieconomiche, se le distanze non superano i 100 m. L'introduzione di un ulteriore hub o repeater aumenterebbe la latenza e quindi aggraverebbe il problema delle collisioni.

Quesito 4

Si fa notare che gli indirizzi proposti sono *indirizzi IPv4 pubblici*, e quindi non devono essere sprecati.

Poiché l'Internet Service Provider può assegnare indirizzi IPv4 di classe C, per minimizzare il numero di indirizzi IP da richiedere si impiega il metodo del subnetting nella realizzazione del piano di indirizzamento.

Si ricorda che negli indirizzi IP di classe C i primi 24 bit costituiscono il prefisso di rete (*network prefix*), mentre gli ultimi 8 bit identificano gli host all'interno della rete. Poiché il prefisso di rete seguito dalla parte host costituita da tutti 0 costituisce l'indirizzo IP della rete o sottorete, mentre il prefisso di rete seguito dalla parte host costituita da tutti 1 costituisce l'indirizzo IP di broadcast, un indirizzo di classe C mette a disposizione degli host $2^8 - 2 = 254$ indirizzi IP.

Per definire un piano di indirizzamento ottimizzato che minimizzi lo spreco di indirizzi IP si può operare nel seguente modo.

La sottorete A è composta da 200 host per cui necessita di un intero indirizzo di classe C: per essa il piano di indirizzamento può essere il seguente.

- a)** La sottorete A è identificata dall'indirizzo IP di rete 192.220.15.0 (a cui di default è associata la subnet mask 255.255.255.0):
- si assegna il primo indirizzo IP, in modo statico, all'interfaccia del router che funge da gateway, ovvero 192.220.15.1;
 - si riservano alcuni indirizzi IP per gli eventuali apparati di rete amministrabili esistenti o da installare in seguito (hub, switch, Access Point ecc.), per esempio gli indirizzi IP da 192.220.15.2 a 192.220.15.10; essi saranno indirizzi IP statici;
 - si definisce un range di indirizzi per i PC (host), da configurare in modo dinamico per mezzo di un server DHCP, per esempio da 192.220.15.30 a 192.220.15.230 se non si prevede che si colleghino altri PC oltre ai 200 iniziali; se non vi sono stringenti requisiti di sicurezza è anche possibile estendere il range di indirizzi dinamici per tenere conto di eventuali inserimenti in rete di nuovi PC;
 - se nella rete è presente un computer server si assegna a esso, in modo statico, l'ultimo indirizzo IP, il 192.220.15.254;
 - l'indirizzo IP di broadcast ha la parte host costituita da tutti 1 per cui è 192.168.15.255;
 - per tutti la subnet mask è 255.255.255.0, il gateway è 192.220.15.1; si configura sui PC che accedono a Internet almeno l'indirizzo IP di un server DNS (*Domain Name System*), meglio due, per esempio gli indirizzi degli OpenDNS 208.67.220.220 e 208.67.222.222 (www.opendns.com).

b) Per le sottoreti B e C è possibile effettuare un subnetting su un indirizzo IP di classe C adiacente, per esempio il 192.220.16.0, in modo da ripartirlo sulle due sottoreti B e C. Il subnetting (FIGURA 4) consiste nell'estendere il prefisso di rete in modo da poter definire più sottoreti «allungando» la subnet mask di un numero di bit (posti a 1) sufficienti alla numerazione delle sottoreti stesse. Si opera quindi nel seguente modo:

- la sottorete B è composta da 80 host per la cui numerazione sono sufficienti 7 bit; è così possibile assegnare alla sottorete B l'indirizzo 192.220.16.0 e allungare la subnet mask di un bit; la subnet mask diventa così costituita da 25 «1» e seguiti da 7 zeri (/25), per cui la subnet mask espressa in decimale è 255.255.255.128; per la numerazione degli host sono a disposizione gli ultimi 7 bit, per cui gli indirizzi IP assegnabili agli host vanno da 192.220.16.1 a 192.220.16.126; l'indirizzo 192.220.16.127 è quello di broadcast; l'assegnazione degli indirizzi segue i criteri elencati al punto a);
- la sottorete C è composta da 25 host per la cui numerazione sono sufficienti 5 bit; la porzione degli indirizzi IP lasciata libera dalla sottorete B può quindi essere divisa in 4 parti allungando di altri due bit la subnet mask che diventa 255.255.255.224, sinteticamente indicata come /27 (27 «1» e 5 «0»); si ha così che l'indirizzo IP della sottorete C è 192.220.16.128, con subnet mask 255.255.255.224; per gli host sono disponibili gli indirizzi IP che vanno da 192.220.16.129 a 192.220.16.158; l'indirizzo di broadcast è 192.220.16.159; per tutti gli host la subnet mask è 255.255.255.224; l'assegnazione degli indirizzi segue i criteri elencati al punto a).

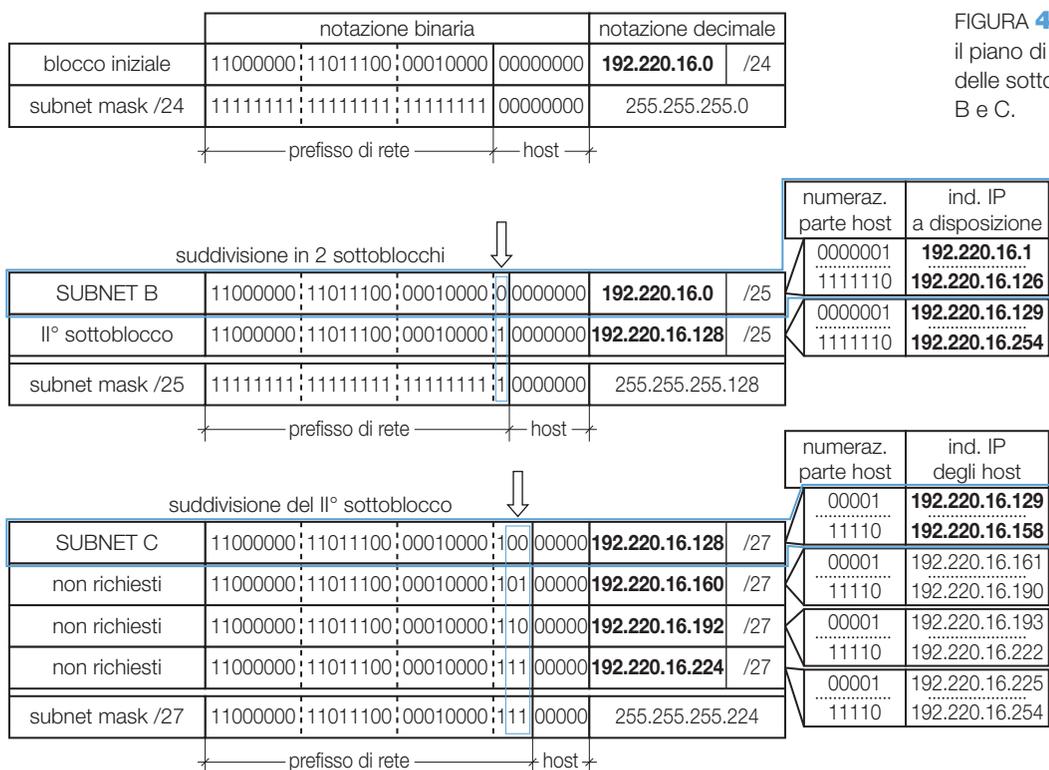


FIGURA 4 Subnetting per il piano di indirizzamento delle sottoreti (subnet) B e C.

All'ISP si richiedono solo i blocchi di indirizzi IP così determinati:

- un intero blocco di indirizzi IP di classe C, il 192.220.15.0/24;
- due porzioni di indirizzi IP appartenenti a un blocco di indirizzi di classe C, la 192.220.16.0/25 e la 192.220.16.128/27.

Si suppone infine che l'interfaccia esterna del router che connette all'ISP venga configurata con un indirizzo IP pubblico scelto dall'ISP stesso, in quanto esso è vincolato a quello che l'ISP assegna all'interfaccia del proprio router; i due indirizzi IP devono appartenere alla stessa subnet, che può essere costituita esclusivamente dalle due interfacce dei router, e in questo caso ha come subnet mask 255.255.255.252 (indicata sinteticamente come /30).

Quesito 5

Si descrive di seguito il principio con cui opererebbe un protocollo di trasporto che implementasse il metodo di correzione degli errori e controllo di flusso stop and wait.

- Il protocollo sorgente invia una PDU che trasporta un blocco di dati, comunemente detta *segmento*, incapsulata in un pacchetto IP che a sua volta è incapsulato in un frame.
- Il destinatario controlla (tramite il metodo del CRC e del checksum) se nelle PDU ricevute (frame, pacchetto IP, segmento del protocollo di trasporto) sono presenti errori; se non sono presenti errori invia alla sorgente una conferma di corretta ricezione denominata ACK (*Acknowledge*); in caso contrario scarta il frame (e quindi il segmento) e se implementa il metodo ARQ (*Automatic Repeat reQuest*) invia un frame di NACK (*Not Acknowledge*) che richiede la ritrasmissione del segmento contenente errori, mentre se adotta il metodo del timeout non fa nulla: è la sorgente che, se non riceve entro un tempo prestabilito l'ACK, allo scadere del tempo (timeout) ritrasmette il segmento.
- La sorgente trasmette il segmento successivo solo dopo aver ricevuto l'ACK.

Nel fare i calcoli è necessario fare riferimento ai frame generati dallo strato 2 (Ethernet). In assenza di errori si ha che l'InterFrame Gap (IFG), cioè l'intervallo di tempo che lato sorgente intercorre tra la fine di un frame e l'inizio del frame successivo, è in prima approssimazione considerabile pari al round trip delay (RTD) più il tempo necessario a trasmettere il frame di ACK (FIGURA 5, a pagina seguente).

Per massimizzare la velocità di informazione si suppone di operare con frame aventi la dimensione massima del campo informativo, nota come MTU (*Maximum Transmission Unit*); nel caso di frame Ethernet l'MTU è pari a 1500 byte.

Ricordando il processo di incapsulamento e la struttura di un frame Ethernet, illustrati in FIGURA 2, è possibile determinare il numero di byte e di bit che compongono un frame Ethernet avente un campo informativo di 1500 byte:

$$N = 8 \text{ (preambolo e SFD)} + 6 \text{ (ind. MAC dest.)} + 6 \text{ (ind. MAC sorg.)} + 2 \text{ (Protocol type)} + 1500 \text{ (max info)} + 4 \text{ (FCS)} = 1526 \text{ byte}$$

$$N_B = 1526 \text{ byte} \Rightarrow N_b = 1526 \cdot 8 = 12\,208 \text{ bit}$$

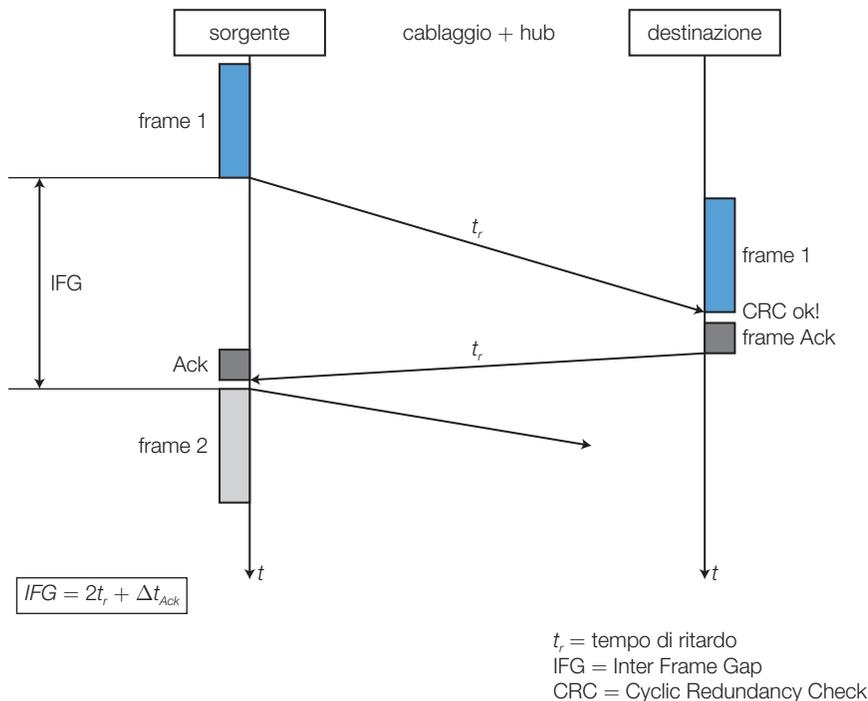


FIGURA 5 Determinazione dell'IFG.

A 100 Mbit/s la durata di un bit è di 10 ns, per cui la durata di un frame è pari a:

$$\Delta t_{frame} = 12\,208 \cdot 10^{-8} = 122 \mu\text{s}$$

Il numero di byte (N'_B) e di bit (N'_b) che compongono un frame di ACK, avente il campo informativo minimo, pari a 46 byte, risulta pari a:

$$N'_B = 8 \text{ (preambolo e SFD)} + 6 \text{ (ind. MAC dest.)} + 6 \text{ (ind. MAC sorg.)} + 2 \text{ (Protocol type)} + 46 \text{ (min info)} + 4 \text{ (FCS)} = 72 \text{ byte}$$

$$N'_B = 72 \text{ byte} \Rightarrow N'_b = 72 \cdot 8 = 576 \text{ bit}$$

La durata di un frame di ACK è pari a:

$$\Delta t_{ACK} = 576 \cdot 10^{-8} = 5,76 \mu\text{s}$$

Poiché il round trip delay, pari al doppio del tempo di ritardo introdotto dal collegamento fra sorgente e destinazione, è nel caso peggiore pari a $RTD = 2t_r = 5,12 \mu\text{s}$, il periodo di assenza di trasmissione finale che separa due frame, cioè l'IFG (*Inter Frame Gap*), è in prima approssimazione (sono trascurati i ritardi di elaborazione delle schede di rete) pari a:

$$IFG = RTD + \Delta t_{ACK} = 5,12_{\mu\text{s}} + 5,76_{\mu\text{s}} = 10,88 \mu\text{s}$$

Il tempo che intercorre fra l'inizio di un frame e l'inizio del frame successivo è quindi considerabile pari alla somma fra la durata di un frame e l'IFG:

$$\Delta t_{totale} = 122_{\mu\text{s}} + 10,88_{\mu\text{s}} = 132,88 \mu\text{s}$$

Il numero di frame al secondo che la sorgente può trasmettere è quindi pari a:

$$N_{frame} = \frac{1}{132,88 \cdot 10^{-6}} = 7525,587 \text{ frame/s}$$

Sapendo che i protocolli degli strati 3 e 4 introducono ciascuno 20 byte di header, si ha che i byte utili per il trasporto di informazioni sopra il livello di trasporto messi a disposizione da un frame sono pari a (FIGURA 2):

$$N_{Bu} = 1500 - 40 = 1460 \text{ byte/frame}$$

Corrispondenti a:

$$N_{bu} = 1460 \cdot 8 = 11\,680 \text{ bit/frame}$$

Il numero di bit/s informativi trasferiti, cioè la velocità di informazione (o *throughput*, BR_A) disponibile sopra il livello di trasporto, è così stimabile come:

$$BR_A = 7525,587_{\text{frame/s}} \cdot 11\,680_{\text{bit/frame}} \cong 88 \text{ Mbit/s}$$

In realtà la velocità di informazione è inferiore in quanto vi sono dei ritardi aggiuntivi dovuti per esempio ai tempi necessari per la rivelazione d'errore sui frame, tramite il ricalcolo del CRC (*Cyclic Redundancy Check*) ecc.

Il secondo quesito può essere affrontato nel seguente modo.

Per aumentare la velocità di informazione senza modificare la velocità di modulazione è possibile impiegare un protocollo di trasporto che opera a finestra di trasmissione, come il TCP.

In questo modo l'Inter Frame Gap medio si riduce molto, aumentando così il numero di frame/s trasmessi e quindi la velocità di informazione a disposizione dello strato di applicazione (si veda la soluzione 1).