ESAME DI STATO DI ISTITUTO TECNICO SETTORE TECNOLOGICO

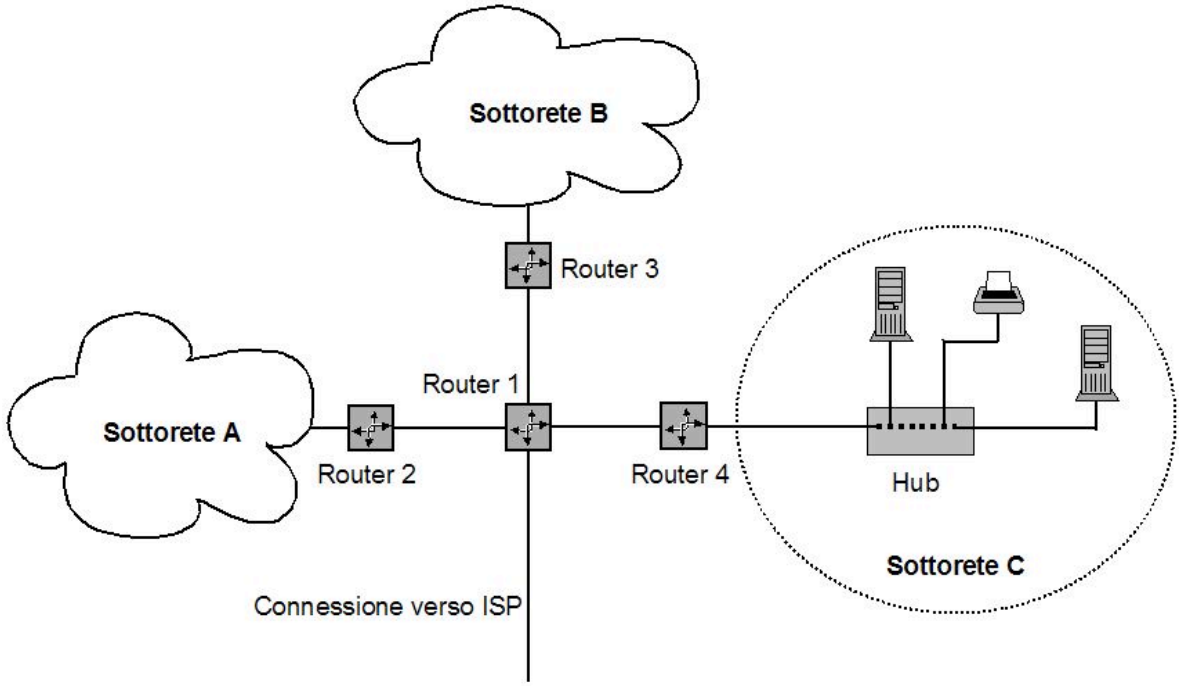
Indirizzo: INFORMATICA E TELECOMUNICAZIONI

Articolazione: TELECOMUNICAZIONI

Esempio[1] di prova di TELECOMUNICAZIONI

PRIMA PARTE

Una rete aziendale è divisa in sottoreti come illustrato nello schema di massima.



Valgono, inoltre, le seguenti condizioni:

- nelle sottoreti A, B sono presenti, rispettivamente, 30, 60 host;
- la sottorete C, costituita da 20 host connessi ad un unico Ethernet-hub, funziona secondo lo standard 100BaseT;
- tutte le sottoreti operano alla velocità di 100 [Mbps];
- le sottoreti A e C appartengono rispettivamente a gruppi di lavoro che si occupano di progetti distinti, ma dipendono entrambi dai servizi offerti dalla sottorete B.
- l'indirizzamento degli elaboratori è conforme a quanto indicato nella tabella seguente:

	Sottorete A	Sottorete B	Sottorete C	Sottorete dei Router
Indirizzo IP sottorete	192.168.0.0/26	192.168.0.64/26	192.168.0.128/26	192.168.0.192/26
Maschera sottorete	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192

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

[1] Si veda www.istruzione.it/allegati/2015/Esempi_seconde_prove_IT_2014_15.zip
o il sito www.istruzione.lombardia.gov.it/avviso-esami-di-stato-secondo-grado2015/
cliccando sul link Esempi di seconda prova scritta Istituti Tecnici

a) Individui i punti di debolezza della struttura di rete sia in termini di affidabilità sia in termini di risposta a seguito di incremento nel traffico.

b) Proponga una struttura alternativa di rete che consenta di superare i problemi individuati al punto precedente e motivi le scelte effettuate.

c) Identifichi e illustri le modifiche da apportare al piano di indirizzamento, nell'ipotesi di ampliamento del sistema con l'aggiunta di un'ulteriore sottorete comprendente venticinque elaboratori.

d) Valuti il tempo massimo di consegna dei pacchetti tollerabile (tempo di latenza) perché sopra al livello trasporto la velocità non scenda a meno di 1 [Mbps] in assenza di errori e quando:

- a livello trasporto lo scambio delle trame è regolato da una procedura di controllo di flusso del tipo stop and wait;
- le intestazioni di ciascun livello di protocollo hanno una dimensione di 20 [Byte].
- La dimensione del payload di livello trasporto è fissa e vale 1024 [Byte].

SECONDA PARTE

Il candidato scelga due fra i seguenti quesiti e per ciascun quesito scelto formuli una risposta della lunghezza massima di 20 righe.

1. Proporre e discutere brevemente una modifica alle condizioni imposte al punto "d" della traccia, per ottenere, a parità di tempo di consegna dei pacchetti, un incremento della velocità vista sopra al livello trasporto.

2. In relazione alla sottorete C, individuare i problemi che si incontrerebbero se si volesse aumentare il numero degli elaboratori e indicare una possibile soluzione.

3. Spiegare, nell'ambito dell'architettura OSI, le funzione del livello 4, trasporto, mettendo in evidenza le differenze rispetto a quelle del livello 2, data link.

4. Spiegare in cosa consistono gli indirizzi privati IPv4 e quale uso se ne può fare nell'ambito di una rete come quella proposta dalla traccia.

Durata massima della prova: 6 ore
È consentito soltanto l'uso di manuali tecnici (references riportanti solo la sintassi, non guide) dei linguaggi utilizzati.
Non è consentito lasciare l'aula prima che siano trascorse 3 ore dall'inizio della prova.

SOLUZIONE[2]

a) La struttura di rete presenta almeno i seguenti punti critici:
   1. *single point of failure* nell'interconnessione fra le subnet, in quanto essa avviene tramite il solo Router 1; in caso di guasto del Router 1 gli host delle subnet A e C non possono più accedere ai servizi della subnet B e nessun host può accedere a Internet (connessione verso ISP, *Internet Service Provider*);
   2. utilizzo di hub Ethernet, che limitano le prestazioni della rete in quanto gli host possono operare esclusivamente in Half Duplex, esiste il problema delle collisioni (che aumentano all'aumentare del numero di host e del traffico), per cui la velocità effettiva di trasferimento dei dati (throughput) diminuisce all'aumentare del traffico in rete e del numero di host (molto qualitativamente si può stimare come velocità nominale/numero host);
   3. mancanza di almeno un firewall a protezione della rete aziendale nel collegamento verso l'ISP e quindi verso Internet;
   4. i collegamenti fra i router richiedono subnet IP diverse per cui il blocco di indirizzi IPv4 192.168.0.192/26 va indicato come blocco per le **sottoreti** dei router, in quanto da esso si devono ricavare almeno tre sottoreti per i tre collegamenti Router1 <-> Router2; Router1 <-> Router3; Router1 <-> Router4;
      il collegamento di connessione del Router1 verso l'ISP va configurato con indirizzi IPv4 presi da questo blocco (quarta subnet IP) solo se il Router 1 **non** è il router tramite cui si accede a Internet, per cui l'interfaccia del Router 1 indicata come connessione verso ISP in realtà porta a un altro router/firewall interno alla rete aziendale, tramite cui si accede a Internet;
      invece, nel caso in cui il Router1 sia anche il router tramite cui si accede a Internet, andrebbe evidenziato che nella rete aziendale si utilizzano indirizzi IPv4 privati mentre all'interfaccia esterna (interfaccia WAN verso l'ISP) del Router 1 va assegnato un indirizzo IPv4 pubblico, che può essere statico o dinamico, e che va attivata nel Router 1 la funzione NAT (*Network Address Translation*) nella sua versione PAT (*Port Address Translation*) per consentire l'accesso a Internet agli host (computer, ecc.) della rete aziendale, che sono configurati con indirizzi IPv4 privati (si veda la risposta al punto 4 della seconda parte).

b) Una soluzione alternativa è quella di sostituire gli hub e i router interni con degli switch amministrabili in configurazione ridondata, in modo da evitare l'impiego di router interni, più lenti degli switch. Si realizza così una rete organizzata in modo gerarchico, in cui sono presenti degli switch collegati a maglia, mentre ogni switch di accesso viene collegato a due altri switch di livello superiore, in modo tale da mantenere la connettività di rete anche se uno switch si guasta. E' così possibile rendere più efficiente, affidabile e veloce la rete aziendale.
   La separazione degli host appartenenti a gruppi di lavoro diversi può avvenire configurando delle VLAN (Virtual LAN); se si desidera mantenere comunque la suddivisione in sottoreti (subnet IP) proposta dal testo è possibile impiegare degli switch Layer 3 (o *multilayer switch*) al posto dei router interni, FIGURA 1.
   E' inoltre previsto l'impiego almeno di un firewall a protezione della rete.
   Come approfondimento (opzionale) si potrebbe poi aggiungere che:

- negli switch va attivato il protocollo STP (*Spanning Tree Protocol*) per evitare la creazione di *loop* tra gli switch in configurazione ridondata, loop che porterebbero rapidamente a deteriorare le prestazioni della rete per via dei "*broadcast storm*", cioè del fatto che frame emessi in broadcast (da uno a tutti) potrebbero circolare indefinitamente lungo i loop in quanto gli switch che formano il loop stesso se li inviano continuamente;
- in considerazione del fatto che l'accesso a Internet è una risorsa essenziale per lo svolgimento delle attività dell'azienda è poi possibile prevedere un accesso a Internet tramite due router in configurazione ridondata di tipo *hot standby*, con un protocollo di tipo FHRP (*First Hop Redundancy Protocol*) che fa vedere agli host un solo default gateway verso Internet e che dinamicamente è in grado di commutare la connessione al router in hot standby nel caso in cui il router che sta operando si guasti.
  In linea di principio ne deriva un'infrastruttura di rete ad alta disponibilità (*High Availability*, Figura 1).
  Infine si potrebbe citare il fatto che le reti aziendali attuali tendono sempre più spesso a essere reti convergenti, che consentono sia lo scambio di dati fra host sia comunicazioni audio (e video) fra le persone, con tecnologie di tipo VoIP (*Voice over IP*) e applicazioni di telefonia su IP (*ToIP, Telephony over IP*) per le quali è opportuno implementare adeguate politiche di qualità del servizio (QoS, *Quality of Service*).

[2] La soluzione è a cura del prof. Onelio Bertazioli e dell'ing. Marco Paganini, Istruttore Cisco Academy presso eForHum (www.eforhum.it).

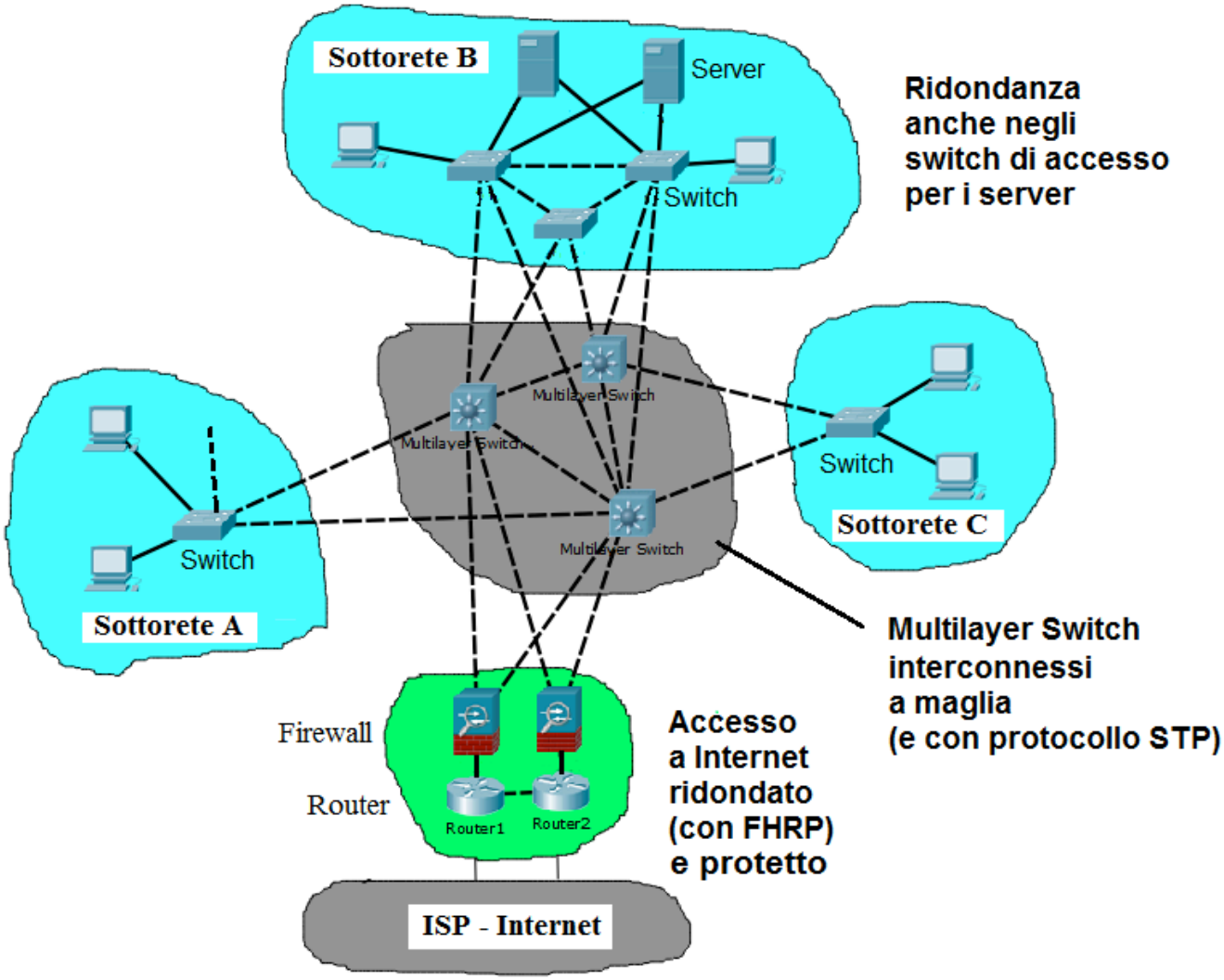


FIGURA 1 Schematizzazione di principio della rete aziendale.

c) Con l'infrastruttura di rete proposta dal testo le caratteristiche e gli indirizzi IPv4 disponibili per le sottoreti (subnet) IP e per gli host (computer, ecc.) che appartengono loro sono i seguenti:

- subnet A -> prefisso di rete di 26 bit; 6 bit per la parte host; 64 indirizzi totali
  62 indirizzi IPv4 per gli host: da 192.168.0.1 a 192.168.0.62;
  indirizzi occupati: 30; indirizzi liberi: 32
  broadcast 192.168.0.63;
  indirizzo di sottorete 192.168.0.0/26
  subnet mask 255.255.255.192

- subnet B -> prefisso di rete di 26 bit; 6 bit per la parte host; 64 indirizzi totali
  62 indirizzi IPv4 per gli host: da 192.168.0.65 a 192.168.0.126;
  indirizzi occupati: 60; indirizzi liberi: 2
  broadcast 192.168.0.127;
  indirizzo di sottorete 192.168.0.64/26
  subnet mask 255.255.255.192

- subnet C -> prefisso di rete di 26 bit; 6 bit per la parte host; 64 indirizzi totali
  62 indirizzi IPv4 per gli host: da 192.168.0.129 a 192.168.0.190;
  indirizzi occupati: 20; indirizzi liberi: 42
  broadcast 192.168.0.191;

indirizzo di sottorete 192.168.0.128/26
subnet mask 255.255.255.192

- il blocco di indirizzi IPv4 a disposizione per le *sottoreti fra i router* ha un prefisso di rete di 26 bit; 6 bit per la parte host;
  esso va ulteriormente suddiviso in 3 o 4 subnet, con subnet mask /30 (255.255.255.252), per i collegamenti fra i router (FIGURA 2);
  gli indirizzi della subnet verso ISP sono assegnati dall'ISP stesso se il Router 1 è il router di accesso a Internet.

Poiché le sottoreti fra i router comprendono un numero molto limitato di host (le interfacce dei router) è possibile ricavare dal suo blocco di indirizzi IPv4 un'altra subnet (la D), che comprenda un totale di 32 indirizzi (subnet mask /27 -> 5 bit per la parte host dell'indirizzo) e che consenta l'ampliamento della rete aziendale. A tale scopo si può operare nel seguente modo.
Suddividiamo in due parti il blocco di indirizzi IPv4 a disposizione (192.168.0.192/26) impiegando la subnet mask /27.
Il primo blocco così ottenuto viene utilizzato configurare i 25 host della sottorete (subnet D) aggiunta:

- subnet D -> indirizzo IP di subnet 192.168.0.192/27; subnet mask 255.255.255.224;
  numero di indirizzi IPv4 a disposizione degli host: da 192.168.0.193 a 192.168.0.222;
  indirizzo di broadcast 192.168.0.223

Suddividiamo in due parti il secondo blocco, 192.168.0.224/27, utilizzando la subnet mask /28; si ottengono i seguenti blocchi di indirizzi IPv4:
- blocco 3 -> indirizzo IP di subnet 192.168.0.224/28; subnet mask 255.255.255.240;
- blocco 4 -> indirizzo IP di subnet 192.168.0.240/28; subnet mask 255.255.255.240;

Il blocco 3 può essere a sua volta suddiviso in almeno tre parti, assegnabili alle subnet definibili per i collegamenti fra i router, ciascuna composta da 2 host (le due interfacce dei router interconnesse), utilizzando la subnet mask /30:

- subnet E (Router 1 <-> Router 2) indirizzo IP di subnet 192.168.0.224/30; subnet mask 255.255.255.252;
  indirizzi IPv4 degli host 192.168.0.225, 192.168.0.226;
  broadcast 192.168.0.227;
- subnet F (Router 1 <-> Router 3) indirizzo IP di subnet 192.168.0.228/30; subnet mask 255.255.255.252;
  indirizzi IP degli host 192.168.0.229, 192.168.0.230;
  broadcast 192.168.0.231;
- subnet G (Router 1 <-> Router 4) indirizzo IP di subnet 192.168.0.232/30; subnet mask 255.255.255.252;
  indirizzi IP degli host 192.168.0.233, 192.168.0.234;
  broadcast 192.168.0.235
- subnet H (Router 1 <-> Router-verso-ISP, se il Router 1 non è il router di accesso a Internet)
  indirizzo IP di subnet 192.168.0.236/30; subnet mask 255.255.255.252;
  indirizzi IP degli host 192.168.0.237, 192.168.0.238;
  broadcast 192.168.0.239

L'altro blocco di indirizzi IPv4, il 192.168.0.240/28, che mette a disposizione 14 indirizzi IPv4 per gli host, rimane libero e a disposizione per ulteriori espansioni della rete.

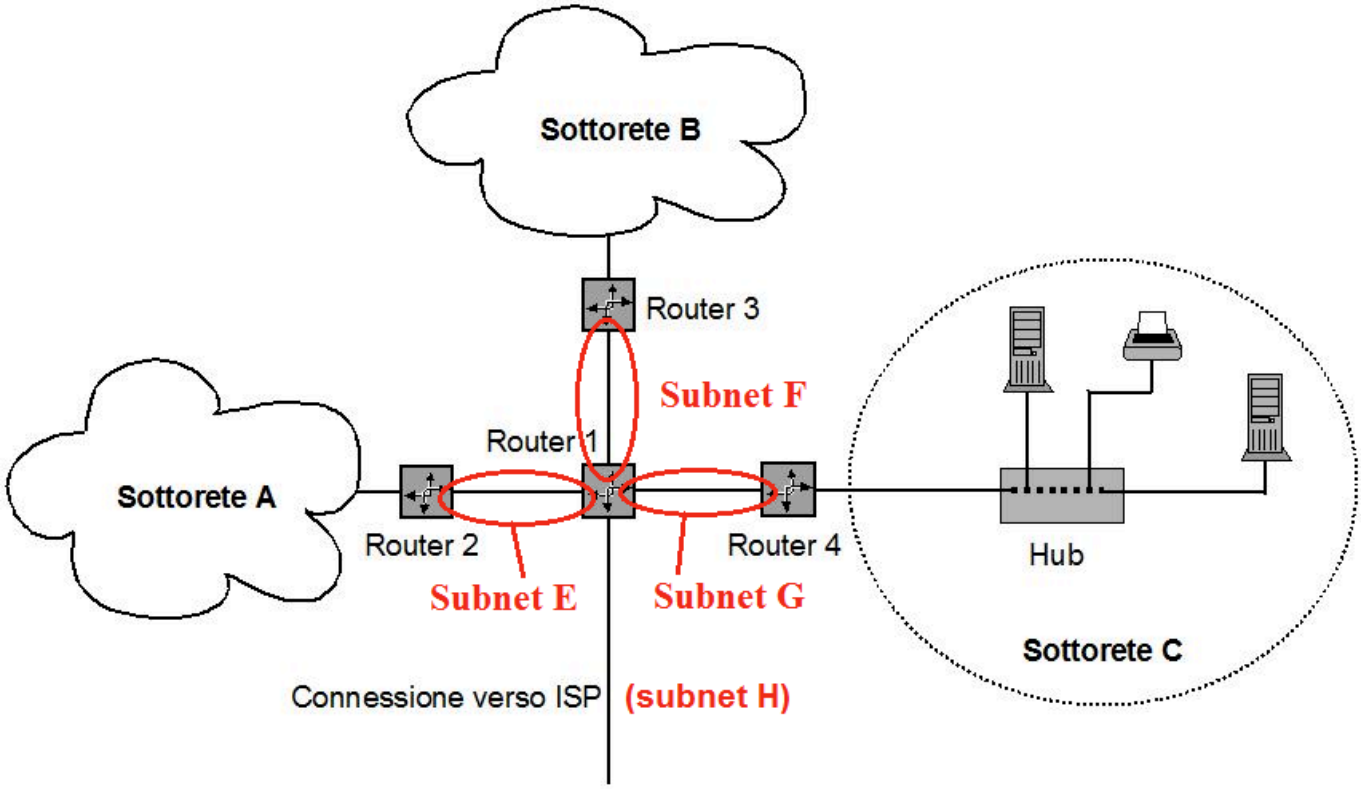


FIGURA 2 Sottoreti che interconnettono i router.

d) Valuti il tempo massimo di consegna dei pacchetti tollerabile (tempo di latenza) perché sopra al livello trasporto la velocità non scenda a meno di 1 [Mbps] in assenza di errori e quando:

- a livello trasporto lo scambio delle trame (o *frame*) è regolato da una procedura di controllo di flusso del tipo stop and wait;
- le intestazioni di ciascun livello di protocollo hanno una dimensione di 20 [Byte].
- La dimensione del payload di livello trasporto è fissa e vale 1024 [Byte].

Si fa l'ipotesi che all'interno della rete aziendale si utilizzi esclusivamente la tecnologia Ethernet per gli strati OSI 1 e 2.

Adottando un controllo di flusso con metodo *stop and wait* il trasferimento di informazioni fra un host (computer) sorgente e un host destinazione avviene con la seguente procedura (FIGURA 3):

- l'host sorgente genera e bufferizza una 4-PDU (*Protocol Data Unit* dello strato 4 OSI denominata usualmente *segmento*), la quale viene incapsulata in un pacchetto (IP), o 3-PDU (PDU dello strato 3 OSI) a sua volta incapsulato in un *frame* (o trama) Ethernet (PDU dello strato 2 OSI);
- lo strato 1 (o strato fisico) dell'host sorgente trasmette in linea il frame Ethernet; se la comunicazione avviene all'interno della stessa subnet (sottorete) essa giunge direttamente al destinatario, mentre se sorgente e destinazione sono su subnet IP diverse il frame Ethernet giunge al router che funge da gateway, il quale estrae il pacchetto (IP), esamina l'header e determina la subnet IP di destinazione, incapsulando nuovamente il pacchetto in un frame Ethernet che sarà inviato all'host di destinazione;
- l'host di destinazione riceve il frame, controlla che non vi siano errori con il metodo del CRC (*Cyclic Redundancy Check*), estrae il pacchetto, controlla che l'header non contenga errori (verificando il checksum), estrae il segmento (4-PDU) e controlla che non vi siano errori verificando il checksum in esso contenuto;
- se non vi sono errori l'host di destinazione genera una 4-PDU (segmento) di ACK per informare l'host sorgente che la 4-PDU (segmento) con i dati è giunta correttamente; l'ACK del protocollo di trasporto è incapsulato in un pacchetto e in un frame Ethernet che viene inviato all'host sorgente;

- dopo aver ricevuto l'ACK l'host sorgente può trasmettere il segmento (4-PDU) successivo, che viene come sempre incapsulato in un pacchetto e in un frame Ethernet.

  In questo contesto il *Round Trip Time*[3] (RTT, tempo di andata e ritorno) può essere definito come l'intervallo di tempo che intercorre fra l'inizio dell'invio di una 4-PDU (un segmento) e la fine della ricezione della conferma di corretta ricezione (ACK).
  Se si fa l'ipotesi che un pacchetto si ritenga consegnato quando l'host sorgente ha ricevuto la conferma di corretta ricezione (ACK), il tempo di consegna si può ritenere all'incirca uguale al *Round Trip Time* (RTT).

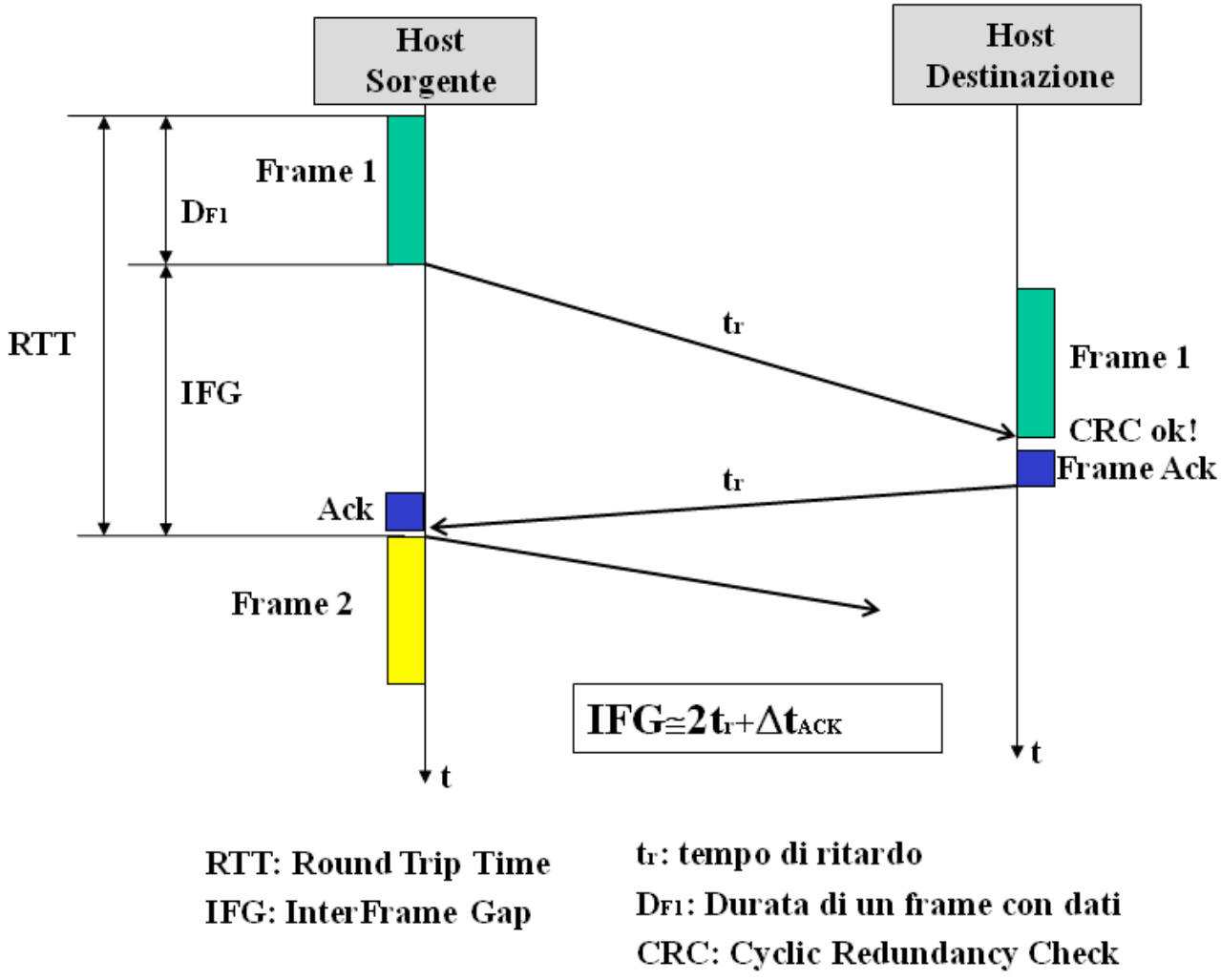


FIGURA 3 Principio del metodo stop and wait e Round Trip Time (RTT).

Per semplicità si trascurano i tempi di elaborazione degli host, come quelli necessari per determinare che non vi siano errori nei frame (2-PDU), nei pacchetti (3-PDU) e nei segmenti (4-PDU), e si fanno i calcoli a livello di frame Ethernet (strato 2). Nei frame Ethernet i byte effettivamente aggiunti dal corrispondente protocollo sono i seguenti:

- preambolo e SFD, *Start Frame Delimiter*, -> 8 Byte;
- indirizzi MAC sorgente e destinazione -> 12 Byte;
- campo Protocol Type -> 2 Byte;
- campo di coda FCS, Frame Check Sequence, -> 4 Byte.

[3] Per una definizione precisa dell'RTT e della metodologia per determinare il throughput massimo supportato dal protocollo TCP si veda l'RFC 6349 "Framework for TCP Throughput Testing", rilasciata dall'Internet Engineering Task Force (IETF).

L'intervallo di tempo che intercorre tra la fine di un frame e l'inizio del frame successivo viene anche denominato *InterFrame Gap* (IFG).
La latenza massima consentita può essere calcolata imponendo come velocità di trasferimento delle informazioni (V_{Info}), o *throughput*, il valore V_{Info} = 1 Mbps (Megabit per second o Mbit/s).
Fissata la V_{Info} e sapendo che il payload è pari a P = 1024 B (B = Byte) è possibile calcolare il numero di frame che è necessario emettere in un secondo per trasferire 1 Mbit:

$$N_{Frame} = \frac{V_{Info}}{P \cdot 8} = \frac{10^6}{8192} = 122 \quad Frame/s$$

Il tempo che intercorre fra l'inizio di un frame e l'inizio del frame successivo (Δt_F), all'incirca pari all'RTT e pari alla somma della durata di un frame (D_F) e dell'IFG, può quindi essere calcolato come

$$\Delta t_F \cong RTT = D_F + IFG = \frac{1}{122} \cong 8{,}2 \quad ms$$

Con le ipotesi fatte, si ha che il tempo di consegna massimo di ciascun pacchetto (latenza, $\Delta t_{L\max}$) risulta così all'incirca pari a:

$$\Delta t_{L\max} = RTT \cong 8{,}2 \quad ms$$

Se si desidera calcolare anche l'IFG (InterFrame Gap) e stimare il tempo di ritardo (t_r) massimo che il collegamento può introdurre, è necessario determinare la durata di un frame Ethernet che trasporta dati (D_{F1}) operando come segue.
L'IFG può essere considerato, in prima approssimazione, come la somma dei ritardi di propagazione nelle due direzioni e della durata del frame che trasporta l'ACK (il quale non contiene dati per cui può avere il payload Ethernet di lunghezza minima, pari a 46 Byte).
Noti:

- la velocità di trasmissione lorda (o Bit Rate, BR) supportata dallo strato fisico, pari a BR=100 Mbit/s;
- il tempo di bit, pari a $t_{bit} = 1/BR = 10^{-8} \quad s$;
- la dimensione in byte del payload della 4-PDU, P=1024 B;
- le dimensioni degli header delle 4-PDU (segmento) e 3-PDU (pacchetto), ciascuno pari a 20 B;
- le dimensioni dell'header e del campo di coda dei frame Ethernet, rispettivamente pari a 22 B e 4 B

è possibile calcolare il numero totale di byte (B) e di bit che compongono un frame che trasporta dati:

$$N_{Byte/frame} = 1024 + 20 + 20 + (22 + 4) = 1090 \quad B$$
$$N_{bit/frame} = 1090 \cdot 8 = 8720 \quad bit$$

La durata di un frame (D_{F1}) risulta così pari a:

$$D_{F1} = N_{bit} \cdot t_{bit} = 8720 \cdot 10^{-8} = 87{,}2 \quad \mu s$$

L'IFG è quindi all'incirca pari a:

$$IFG \cong \Delta t_F - D_{F1} = 8{,}2 \cdot 10^{-3} - 0{,}0872 \cdot 10^{-3} \cong 8{,}11 \quad ms$$

Per calcolare il tempo di ritardo massimo consentito per il collegamento (t_r) in una direzione, trascurando i ritardi di elaborazione, si deve determinare la durata di un frame Ethernet che trasporta solo l'ACK del protocollo di trasporto (D_{F2}) operando nel seguente modo.

Ipotizziamo poi che il frame che trasporta l'ACK abbia il payload Ethernet di dimensione minima, pari a 46 B, comprendente solo gli header dei protocolli dello strato 3 (IP) e dello strato 4 (TCP), pari a 40 B, oltre a un riempimento (*padding*) di 6 B, per cui si ha:

$$N_{Byte/frame} = 46 + (22 + 4) = 72 \quad B$$

$$N_{bit/frame} = 72 \cdot 8 = 576 \quad bit$$

$$D_{F2} = N_{bit} \cdot t_{bit} = 576 \cdot 10^{-8} = 5{,}76 \quad \mu s$$

$$t_r \cong \frac{IFG - D_{F2}}{2} \cong \frac{8{,}11 \cdot 10^{-3} - 0{,}00576 \cdot 10^{-3}}{2} \cong 4{,}05 \quad ms$$

SECONDA PARTE

Il candidato scelga due fra i seguenti quesiti e per ciascun quesito scelto formuli una risposta della lunghezza massima di 20 righe[4].

1. Proporre e discutere brevemente una modifica alle condizioni imposte al punto "d" della traccia, per ottenere, a parità di tempo di consegna dei pacchetti, un incremento della velocità vista sopra al livello trasporto.

L'incremento della velocità sopra il livello di trasporto può essere ottenuto (come avviene in pratica) apportando al protocollo del livello di trasporto stesso le seguenti modifiche:

- si adotta la dimensione massima consentita per il payload della 4-PDU, denominata MSS (*Maximum Segment Size*), pari a **MSS=1460 B** in ambiente Ethernet;
  l'MSS è calcolato sottraendo alla dimensione massima del payload di un frame Ethernet, pari a 1500 B (che corrispondente anche alla massima dimensione che può avere un pacchetto IP, detta MTU - *Maximum Transmission Unit*) gli header (intestazioni) dei protocolli IP e TCP ciascuno dei quali è tipicamente pari a 20 B: MSS = 1500-20-20 = 1460 B;
- si adotta un controllo di flusso a finestra di trasmissione, per cui un host può trasmettere un certo numero di 4-PDU (*segmenti*) senza attendere la conferma di corretta ricezione (ACK); tale numero dipende dalla dimensione della finestra di trasmissione che si utilizza (Windows size, W_{size});
  in assenza di errori valori elevati della finestra di trasmissione consentono di massimizzare la V_{Info} (o throughput) in quanto si può continuare a trasmettere più a lungo senza dover attendere la conferma di corretta ricezione;
- Il protocollo di trasporto può operare in full duplex, per cui l'ACK può essere inviato in una 4-PDU che trasporta dei dati in direzione opposta.

Il protocollo di trasporto a correzione d'errore utilizzato per lo strato 4 della suite TCP/IP (il TCP, *Transmission Control Protocol*) ha proprio queste caratteristiche.
Estendendo opzionalmente la traccia proposta, è possibile stimare, per esempio, la massima V_{Info} (o *throughput*) teorica che si può ottenere nel caso ideale in cui:

- si adotti la dimensione massima consentita per il payload della 4-PDU (MSS=1460 B);
- non vi siano errori;
- l'IFG sia pari al valore minimo consentito dallo standard Ethernet 100BASE-TX -> IFG = 12 B;
- i byte di informazione siano tutti trasferiti all'interno di una stessa finestra di trasmissione, senza dover attendere quindi l'ACK.

Il processo di incapsulamento che si ha nella pratica può essere riassunto come mostrato in FIGURA 4.

[4] Nello svolgimento che segue sono stati inseriti commenti e opzioni che potrebbero essere utili anche in altri contesti, superando così le 20 righe di risposta.

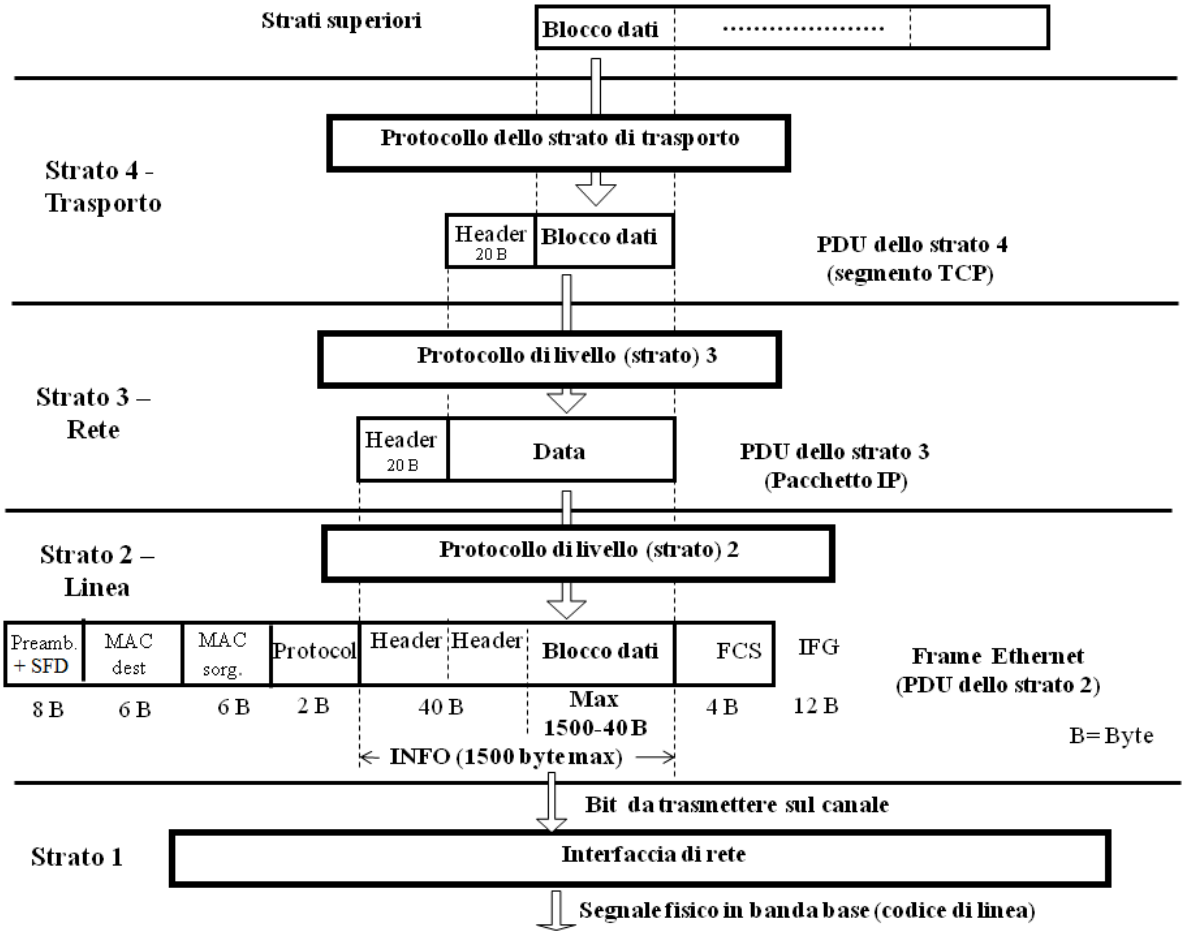


FIGURA 4 Processo di incapsulamento

In questo caso la dimensione totale di un frame Ethernet, comprendendo anche l'IFG, risulta pari a

$$N_{Byte/frame} = 1460 + 20 + 20 + (22 + 4 + 12) = 1538 \quad B$$
$$N_{bit/frame} = 1538 \cdot 8 = 12304 \quad bit$$

Noto il bit rate lordo (BR), il numero massimo di frame/s trasferibili risulta pari a:

$$N_{Frame} = \frac{BR}{N_{bit/frame}} = \frac{10^8}{12304} \cong 8127 \quad Frame/s$$

La massima velocità di informazione teorica è stimabile quindi come il prodotto fra il numero di bit di informazione trasferiti nel payload di un segmento ed il numero di frame (e quindi di segmenti) al secondo trasmessi:

$$V_{Info\_max} \cong (N_{Frame/s}) \cdot (MSS \cdot 8) = 8127 \cdot (1460 \cdot 8) \cong 96 \quad Mbit/s$$

Infine, sempre opzionalmente, indicando con BR il bit rate lordo supportato dallo strato fisico (BR=100 Mbit/s nel nostro caso) e trascurando i ritardi di elaborazione, si può far notare che, in prima approssimazione, il massimo numero di bit che possono essere trasmessi senza attendere la conferma di corretta ricezione (ACK), il quale in assenza di errori consente di ottenere la massima velocità di informazione teorica del protocollo di trasporto, si può stimare come:

$$N_{bit\_max} = BR \cdot RTT \quad bit$$

In questa formula l'RTT può essere considerato come l'intervallo di tempo minimo entro cui arriva la conferma di corretta ricezione (ACK) e quindi il tempo per cui l'host sorgente può continuare a trasmettere senza dover attendere l'ACK stesso.
Il valore N_{bit_max} calcolato è noto anche come "prodotto banda-ritardo" o *Bandwith-Delay Product* (BPD).
Esso può essere utilizzato per dimensionare la finestra di trasmissione (W_{size}) del protocollo TCP (e quindi i buffer di trasmissione e ricezione) al fine di ottenere le migliori prestazioni, che come minimo dovrebbe essere pari a:

$$W_{size} = \frac{BPD}{8} = \frac{N_{bit\_\max}}{8} \quad Byte$$

2. In relazione alla sottorete C, individuare i problemi che si incontrerebbero se si volesse aumentare il numero degli elaboratori e indicare una possibile soluzione.

   Poiché nella sottorete C si impiega un hub, all'aumentare del numero di elaboratori e del traffico aumentano le collisioni e quindi diminuisce l'effettiva velocità con cui si trasferiscono i dati (cioè il throughput). Inoltre l'impiego di più hub in cascata può porre dei limiti alla distanza massima consentita da un collegamento fisico, che può essere inferiore alla distanza massima specificata dallo standard 100BASE-TX, pari a 100 m.
   La soluzione consiste nel sostituire gli hub con degli switch, preferibilmente amministrabili, ottenendo un aumento delle prestazioni, grazie anche al fatto che gli host possono operare in full duplex.
   Opzionalmente si può citare il fatto che gli switch amministrabili offrono anche prestazioni quali: possibilità di configurare delle VLAN (Virtual LAN) per segmentare la sottorete; possibilità di adottare politiche di sicurezza come il *port security*, che consiste nel configurare le porte degli switch in modo da consentire su ciascuna porta l'inoltro in rete solo a frame che contengono degli specifici indirizzi MAC sorgente; in altri termini si consente l'accesso alla rete solo a host che hanno degli specifici indirizzi MAC; in questo modo si ostacolano fortemente collegamenti abusivi alle porte dello switch, ecc.

3. Spiegare, nell'ambito dell'architettura OSI, le funzioni del livello 4, trasporto, mettendo in evidenza le differenze rispetto a quelle del livello 2, data link.

   Nell'ambito dell'architettura OSI le funzioni del livello 4 (o strato - *layer* - 4) sono essenzialmente le seguenti:
   - identificazione dei protocolli dello strato superiore, sorgente e destinazione, che devono trasferire dati **end-to-end**, cioè da host (computer ecc.) sorgente a host destinazione; ciò consente a più applicazioni di condividere una stessa connessione di rete, realizzando così una forma di multiplazione;
   - possibilità di segmentazione e riassemblaggio nella corretta sequenza dei messaggi informativi che si devono trasferire end-to-end;
   - possibilità di garantire una comunicazione affidabile **end-to-end** implementando meccanismi di *correzione d'errore* e *controllo di flusso end-to-end*.

   Nella pratica una 4-PDU (Protocol Data Unit dello strato 4) è spesso denominata *segment* (segmento).

   Le funzioni principali di un protocollo dello strato (livello) 2, o *data link layer*, sono le seguenti:
- indirizzamento delle schede di rete e delle entità dello strato 2 che si scambiano 2-PDU **su un collegamento fisico (canale o link)**; per esempio i protocolli Ethernet / MAC (Media Access Control) utilizzano a tale scopo gli indirizzi MAC (MAC address), noti anche come indirizzi fisici o indirizzi hardware, mentre in ambito WAN il protocollo LAPD, utilizzato nelle reti ISDN/GSM, utilizza a tale scopo il campo Address del frame, che contiene gli identificativi SAPI (*Service Access Point Identifier*) e TEI (*Terminal Endpoint Identifier*);
- rivelazione d'errore sui frame scambiati attraverso un link fisico, tipicamente con il metodo del CRC (*Cyclic Redundancy Check*);
- possibilità di effettuare la correzione d'errore e il controllo di flusso per garantire una comunicazione affidabile **su un link (canale) fisico**, tipicamente caratterizzato da livelli elevati di rumore, distorsioni o interferenze, come i link radio;
- possibilità di identificare il protocollo dello superiore (strato 3) che deve inviare/ricevere il pacchetto incapsulato nel payload (o campo informativo) del frame.

Nella pratica una 2-PDU (Protocol Data Unit dello strato 2) è normalmente denominata *frame* (trama).

In sostanza, quindi, la differenza fondamentale fra i protocolli dello strato 4 e i protocolli dello strato 2 è la seguente:

- i protocolli dello **strato 4** (*transport layer*) **operano end-to-end**, cioè risiedono negli host sorgente e destinazione (in particolare nei sistemi operativi di computer, ecc.) e ne controllano lo scambio di dati;
- i protocolli dello **strato 2** (*data link layer*) **operano link per link**, cioè risiedono nelle interfacce di rete (schede di rete Ethernet, ecc.) di host (computer, ecc.) ed apparati di rete (switch, router) e controllano la comunicazione su uno specifico link (canale) fisico.

Nella pratica i protocolli di trasporto della suite TCP e IP sono i seguenti:

- il TCP (*Transmission Control Protocol*), che operando in modo *connection-oriented* implementa tutte le funzioni sopraccitate, consentendo così una scambio di dati *affidabile* tra host (o sistemi finali, *end systems*, nella terminologia OSI), ma che può essere rallentato dalla necessità di instaurare le connessioni logiche, implementare il controllo di flusso, ecc.;
- l'UDP (*User Datagram Protocol*), che invece opera in modo *connectionless* ed implementa solo la prima funzione (identificazione), consentendo così una scambio dati più veloce, anche se non affidabile, fra host.

Per esempio il trasferimento di un file che avviene con il protocollo di applicazione FTP (*File Transfer Protocol*) ha come requisito essenziale l'affidabilità, per cui si appoggia sul protocollo di trasporto TCP, mentre l'invio con tecnologie VoIP (Voice over IP) di segnali audio e/o video digitalizzati ha come requisito la velocità del trasferimento di informazioni digitalizzate, per minimizzare i ritardi, e può tollerare un numero limitato di errori, per cui il protocollo di applicazione (l'RTP, *Real Time Protocol*) si appoggia sul protocollo di trasporto UDP.

Vi sono invece molti protocolli dello strato 2, ciascuno in grado di controllare la comunicazione su un determinato tipo di link (canale) fisico, come per esempio i seguenti:

- Ethernet II e MAC IEEE 802.3 nelle reti locali;
- PPP (*Point To Point Protocol*) negli accessi a Internet commutati e in quelli di tipo ADSL;
- HDLC nei collegamenti dedicati;
- LAPD nelle reti ISDN e GSM;
- LAPF nelle reti Frame Relay, ecc.

4. Spiegare in cosa consistono gli indirizzi privati IPv4 e quale uso se ne può fare nell'ambito di una rete come quella proposta dalla traccia.

Gli indirizzi IPv4 privati sono tre blocchi di indirizzi IPv4 che possono essere utilizzati liberamente da qualsiasi organizzazione, senza la necessità di doverli acquisire da un Registro Internet Regionale (RIR, *Regional Internet Register*), purché essi vengano utilizzati all'interno di reti private e con i seguenti vincoli:

- si deve garantire l'univocità degli indirizzi IPv4 all'interno di una stessa rete privata (o in un sistema di reti/sottoreti private interconnesse, come quelle indicate dal testo);
- non sono utilizzabili per accedere a Internet in quanto non vengono instradati verso Internet dai router (e per questo sono anche detti *non routable IPv4 address*).

Gli indirizzi IPv4 privati sono stati introdotti per limitare il problema dell'esaurimento degli indirizzi IPv4, in quanto reti private non direttamente connesse possono utilizzare gli stessi indirizzi IPv4 privati.
I tre blocchi di indirizzi IPv4 privati sono i seguenti:

- **10.0.0.0/8**, blocco che va da 10.0.0.0 a 10.255.255.255 con subnet mask 255.0.0.0 (o /8 cioè i primi 8 bit della subnet mask sono degli "1" mentre i rimanenti 24 sono "0");
- **172.16.0.0/12**, blocco che va da 172.16.0.0 a 172.31.255.255, con subnet mask 255.240.0.0 (o /12 cioè i primi 12 bit della subnet mask sono degli "1"mentre i rimanenti 20 sono "0");
- **192.168.0.0/16**, blocco che va da 192.168.0.0 a 192.168.255.255, con subnet mask 255.255.0.0 (o /16 cioè i primi 16 bit della subnet mask sono degli "1"mentre i rimanenti 16 sono "0").

Un'organizzazione, come l'azienda indicata dal testo, può scegliere liberamente di utilizzare il numero di indirizzi IPv4 privati di cui ha necessità, assegnandoli ai propri host e utilizzando la subnet mask che ritiene più appropriata per limitare le dimensioni delle proprie sottoreti (subnet) IP.
Nell'esempio proposto dal testo è stato utilizzato dall'azienda per le proprie reti private il blocco di indirizzi IPv4 192.168.0.0/24, con subnet mask iniziale 255.255.255.0 (cioè /24).
Il blocco è stato suddiviso in 4 parti "allungando" di due bit la parte posta a "1" della subnet mask (detta anche *prefix* in quanto consente di identificare il prefisso di rete/sottorete di un indirizzo IPv4), e utilizzando questi due bit per definire i 4 blocchi di indirizzi IPv4 da utilizzare all'interno delle 4 subnet specificate dal testo.
Gli indirizzi IPv4 privati possono essere assegnati agli host in modo dinamico, tramite un server DHCP (*Dynamic Host Configuration Protocol*), oppure possono essere configurati su essi manualmente (indirizzi IPv4 statici).
Per consentire l'accesso a Internet agli host a cui sono stati assegnati degli indirizzi IPv4 privati è necessario che il router tramite cui si accede a Internet abbia a disposizione almeno un indirizzo IPv4 pubblico (cioè registrato e unico a livello globale), tipicamente almeno quello dell'interfaccia esterna (WAN) che lo interconnette con l'ISP (Internet Service Provider), e che implementi la funzione NAT (*Network Address Translation*).
Grazie alla funzione NAT il router:

- in trasmissione sostituisce nei pacchetti IPv4 diretti verso Internet gli indirizzi IPv4 privati con un indirizzo IPv4 pubblico (instradabile su Internet), tenendo traccia degli host che li hanno emessi;
- in ricezione esegue l'operazione inversa, sostituendo nei pacchetti IPv4 ricevuti da Internet (come risposta a richieste partite dagli host) l'indirizzo IPv4 pubblico con l'indirizzo IPv4 privato degli host di destinazione.

Una variante molto utilizzata della funzione NAT (*Network Address Translation*) viene denominata PAT (*Port Address Translation* o *Port based NAT*), in quanto si utilizzano i *port number* dei protocolli di trasporto TCP e UDP per tenere traccia degli indirizzi IPv4 degli host sorgente da cui provengono i pacchetti IPv4 con indirizzi privati e a cui viene sostituito uno stesso indirizzo IPv4 pubblico. La funzione PAT è nota anche come *Network Address Port Translation (NAPT)* o *IP masquerading* o ancora *NAT overload*.
Il router crea una *tabella PAT* in cui vengono inserite le associazioni

port_number:IPv4_privato <-> port_number:IPv4_pubblico

In questo modo quando il router riceve un pacchetto da Internet, consultando la tabella PAT è in grado di identificare, grazie al *port number* (univoco) di destinazione, qual è l'indirizzo IPv4 privato associato all'indirizzo IPv4 pubblico.
Si ricorda che i *port number* (numeri di porta o numeri di porto) sono gli identificativi con cui il protocollo di trasporto identifica le applicazioni sorgente e destinazione a cui offre i propri servizi. I port number sorgente e destinazione sono inseriti nell'header dei segmenti TCP (o UDP) e consentono di sapere da quali applicazioni (http, ftp, ecc.) provengono i dati da trasferire nel payload del segmento o a quali applicazioni essi vanno inoltrati (destinazione).

Riferimenti bibliografici:

- Manuale Cremonese di Informatica e Telecomunicazioni ed. Zanichelli
- Onelio Bertazioli - Corso di Telecomunicazioni vol. 3- ed. Zanichelli