Sessione ordinaria 2015
Seconda prova scritta

Ministero dell'Istruzione, dell'Università e della Ricerca

M886 – ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITTL – INFORMATICA E TELECOMUNICAZIONI

ARTICOLAZIONE TELECOMUNICAZIONI

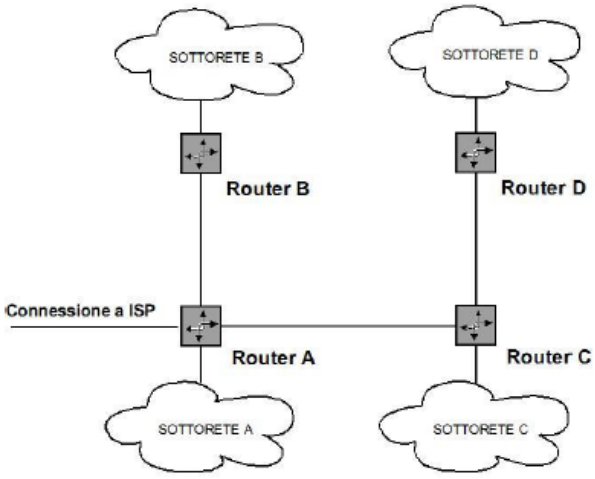
Tema di: TELECOMUNICAZIONI

Tipologia: C (Art. 9 Comma 2 D.M. 10 del 29.01.2015)

Il candidato svolga la prima parte della prova e risponda a due tra i quesiti proposti nella seconda parte.

PRIMA PARTE

Una rete locale serve un ente di ricerca, i cui uffici e laboratori sono ospitati in due edifici posti alla distanza di 100 m l'uno dall'altro; la rete opera alla velocità di 1Gbps ed è suddivisa in quattro sottoreti, collegate secondo lo schema di massima descritto in figura e caratterizzate dal numero di host indicato in tabella.



Sottorete	Numero host
Sottorete A	60
Sottorete B	48
Sottorete C	25
Sottorete D	48

I router A e B si trovano nel primo edificio, mentre gli altri due sono nel secondo. La rete, che si era sviluppata per soddisfare precedenti esigenze, deve essere ristrutturata tenendo in conto che gli host appartenenti alla sottorete D sono aumentati rispetto al passato; le sottoreti B e D vengono usate da gruppi diversi di ricercatori, coinvolti sempre più di frequente in progetti comuni, mentre le postazioni presenti nelle sottoreti A e C sono usate dagli uffici amministrativi dell'ente.

Si sa, inoltre, che il collegamento tra i router A e C è realizzato in fibra ottica posta in apposito cavidotto interrato.

Il candidato, formulate le eventuali ipotesi aggiuntive che ritiene opportune:

1. dopo aver messo in evidenza i punti di debolezza della rete rispetto alle nuove esigenze descritte dalla traccia, proponga e giustifichi una modifica alla struttura di rete in modo da ridurre i tempi di consegna dei pacchetti e la vulnerabilità del sistema ai guasti, senza aumentare sensibilmente i costi per la modifica e la gestione del sistema;

Sessione ordinaria 2015
Seconda prova scritta

Ministero dell'Istruzione, dell'Università e della Ricerca

M886 – ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITTL – INFORMATICA E TELECOMUNICAZIONI

ARTICOLAZIONE TELECOMUNICAZIONI

Tema di: TELECOMUNICAZIONI

2. proponga e discuta le tabelle di instradamento dei router impiegati nella nuova struttura di rete;
3. proponga e discuta un opportuno piano di indirizzamento basato sull'uso di indirizzi privati IPv4;
4. valuti la minima velocità a livello fisico necessaria per sostenere un'applicazione che richiede un ***data rate*** di almeno 64 Kbps, quando le condizioni di traffico sono tali da avere un tempo di latenza di 30 ms, in relazione ad un qualunque elaboratore appartenente alla rete, che debba stabilire una comunicazione regolata dai protocolli illustrati nella tabella sottostante.

Livello di protocollo	*Procedura di trasferimento trame*	*Lunghezza header trame*	*Lunghezza payload*
Applicazione	Non confermata	12 byte	Massimo 1024 byte
Trasporto	Non confermata	8 byte	Massimo 1024 byte
Rete	Non confermata	20 byte	Massimo 1024 byte
Linea	Non confermata	26 byte	Massimo 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** esclusi eventuali grafici, schemi e tabelle.

1. Esamina nel dettaglio i pro e i contro della possibile realizzazione in ponte radio di una connessione tra i due edifici su cui si estende la rete proposta nella prima parte della prova.
2. Spiega come si potrebbe procedere all'indirizzamento nel caso in cui, pur mantenendo la struttura di rete illustrata nella prima parte della prova, si voglia raddoppiare il numero degli elaboratori presenti in ciascuna sottorete.
3. Nell'ambito dei dispositivi di interconnessione, spiega la funzione rispettivamente di router e switch, mettendone in evidenza le differenze.
4. Nell'ambito dei protocolli di livello 2 dell'architettura di rete ***OSI***, spiega in cosa consiste un controllo di flusso realizzato con tecnica ***stop-and-wait*** indicando in quali casi sia conveniente applicarlo.

Durata massima della prova: 6 ore.
È consentito l'uso di manuali tecnici e di calcolatrice non programmabile.
È consentito l'uso del dizionario bilingue (italiano-lingua del paese di provenienza) per i candidati di madrelingua non italiana.
Il candidato è tenuto a svolgere la prima parte della prova ed a rispondere a 2 tra i quesiti proposti.
Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

SOLUZIONE[1]

1. D. Dopo aver messo in evidenza i punti di debolezza della rete rispetto alle nuove esigenze descritte dalla traccia, proponga e giustifichi una modifica alla struttura di rete in modo da ridurre i tempi di consegna dei pacchetti e la vulnerabilità del sistema ai guasti, senza aumentare sensibilmente i costi per la modifica e la gestione del sistema.

R.
La struttura di rete presenta almeno i seguenti punti di debolezza:

a) utilizzo di router non strettamente necessari: non essendovi una topologia a maglia, ridondata, l'impiego di 4 router non è strettamente necessario;
b) impiego di router all'interno della rete, i quali hanno prestazioni inferiori rispetto agli switch Layer 3 sia in termini di ritardi introdotti (tempo di inoltro dei pacchetti) sia in termini di configurabilità (gli switch Layer 3 supportano le VLAN, la QoS, ecc.);
c) *single point of failure* nell'interconnessione fra le subnet, in quanto essa avviene tramite il solo Router A; in caso di guasto del Router A nessun host può accedere a Internet (connessione verso ISP, *Internet Service Provider*) e le sottoreti C e D risultano isolate dalle altre sottoreti;
d) un solo collegamento fra i due edifici; in caso di interruzione/guasto del collegamento in fibra ottica fra i due edifici, le sottoreti C e D risultano isolate dalle altre e dall'accesso a Internet;
e) mancanza di almeno un firewall a protezione della rete aziendale nel collegamento verso l'ISP e quindi verso Internet.

Inoltre si potrebbe far notare che:

- nello schema di rete non è indicata la presenza di **server** e/o di un **data center** utilizzati, si suppone, dai ricercatori (alcuni server) e dagli amministrativi (altri);
- non è esplicitato che si intende realizzare una rete convergente (con QoS - *Quality of Service*), in grado di supportare comunicazioni in audio e video, oltre che dati (anche se il punto 4 fa supporre che si utilizzino tecnologie VoIP per la comunicazione audio) e che si può segmentare la rete e/o il traffico tramite VLAN (*Virtual LAN*);
- poiché la rete è quella di un ente di ricerca è consigliabile che possa usufruire di servizi cloud, di connessioni VPN (*Virtual Private Network*) verso altri centri di ricerca, di servizi di webmeeting/webconference per effettuare da remoto meeting e videoconferenze con esperti e collaboratori, il che richiede una connessione a Internet affidabile (ridondata) e, se possibile, a banda ultralarga con accesso su fibra ottica.

Premessa

Nella rete proposta, con 4 Router a servizio delle sottoreti A-B-C-D, sono presenti ben **8 sottoreti**, dato che i tre collegamenti (link) tra i Router, nonché il collegamento verso l'ISP, devono costituire altrettante subnet, separate dalle sottoreti degli utenti. Ciascuna di queste subnet (non esplicitate nella figura) comprende due soli indirizzi IP (le due interfacce dei router collegate in punto-punto tra loro), per cui è possibile utilizzare la subnet mask 255.255.255.252 (o /30, cioè costituita da 30 "1" e due "0" in binario) con due soli IP utilizzabili.
Si osserva poi che la rete **non è ottimizzata** per il traffico specificato. Infatti, la presenza di **4 Router** implica un notevole lavoro degli stessi, specie per far passare il traffico tra i due gruppi di ricercatori delle sottoreti B e D, le più "distanti" topologicamente, che sono invece spesso coinvolte "in progetti comuni". Inoltre gli eventuali server dei ricercatori soffrono dello stesso problema dei Client, almeno quelli usati dai ricercatori che stanno nella sottorete remota rispetto ai server stessi.

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

È possibile prevedere una transizione graduale verso una nuova struttura di rete prevedendo, per esempio, i seguenti passi.

Passo 1: eliminazione dei Router B e D

I **Router B** e **D** di fatto sono **inutili** nell'architettura della rete in quanto le sottoreti relative possono essere direttamente servite dai Router A e C semplicemente dotandoli di almeno 3 interfacce gigabitEthernet. In un'ottica di risparmio (... "senza aumentare sensibilmente i costi...") si può pensare solo all'eliminazione dei Router B e D, mantenendo i Router A e C (che rinominiamo Router-AB e Router-CD, FIGURA 1), arrivando così addirittura a miglioramento delle prestazioni praticamente a **costo zero**. Questa soluzione è però tecnologicamente superata e limitata in termini prestazionali.

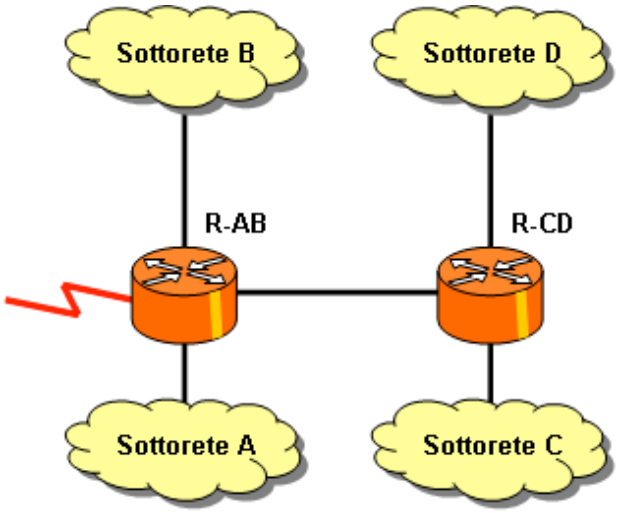


FIGURA 1. Semplificazione della topologia di rete.

Passo 2: sostituzione di Router-AB e Router-CD con switch Layer 3 (o multilayer switch)

Per ottimizzare le prestazioni della rete indicata, riducendo come richiesto i tempi di consegna dei pacchetti, si può proporre di **sostituire** i due Router (R-AB e R-CD) con due **Switch Layer 3**, molto più performanti per la gestione del traffico all'interno delle LAN in quanto operano con tecnologie hardware, al contrario dei router che operano essenzialmente in modo software.
Inoltre gli switch Layer 3 offrono tutta una serie di prestazioni aggiuntive rispetto ai router (QoS, VLAN, porte PoE - *Power over Ethernet* - per alimentare telefoni IP, access point Wi-Fi ecc.) per cui risulta opportuno effettuare questa scelta.

Se per la connessione verso l'ISP, e quindi verso Internet, è preferibile[2] o necessario[3] impiegare un router, si potrebbe inizialmente mantenere il Router-AB e sostituire con uno Switch Layer 3 solamente il Router-CD di FIGURA 1.

Sull'aspetto della richiesta riduzione delle **vulnerabilità**, si osserva che la semplificazione della rete, che avrebbe solo 2 apparati contro i 4 precedenti, comporta **benefici evidenti**, per il "principio zero" dell'ingegneria: **ciò che non c'è, non si guasta**.

[2] Per limitare il costo degli switch Layer 3.
[3] Le specifiche non indicano se la connessione verso l'**ISP** è di tipo seriale o Ethernet; nel primo caso si dovrebbe comunque impiegare un router per disporre della connessione **seriale**, dato che gli Switch Layer 3 hanno solo porte Ethernet.

Per quanto riguarda la protezione della rete da attacchi esterni che potrebbero sia porre fuori uso la rete sia determinare furti di progetti ecc., è consigliabile impiegare almeno un firewall hardware (*appliance*) ad alte prestazioni.

Passo 3: struttura di rete ridondata

Rimane comunque il problema della vulnerabilità del collegamento singolo fra i due edifici e del *single point of failure*. A tale problema si può ovviare realizzando un secondo collegamento fra i due edifici tramite un ponte radio costituito da una coppia di bridge Wi-Fi o HIPERLAN, per esempio a standard IEEE 802.11ac in modo da avere velocità di trasmissione elevate, operare nella banda dei 5 GHz, meno congestionata di quella a 2,4 GHz, ecc.
In questo caso è possibile realizzare una rete con topologia a maglia che comprenda uno strato di distribuzione costituito da 3 switch Layer 3 interconnessi a maglia, FIGURA 2.

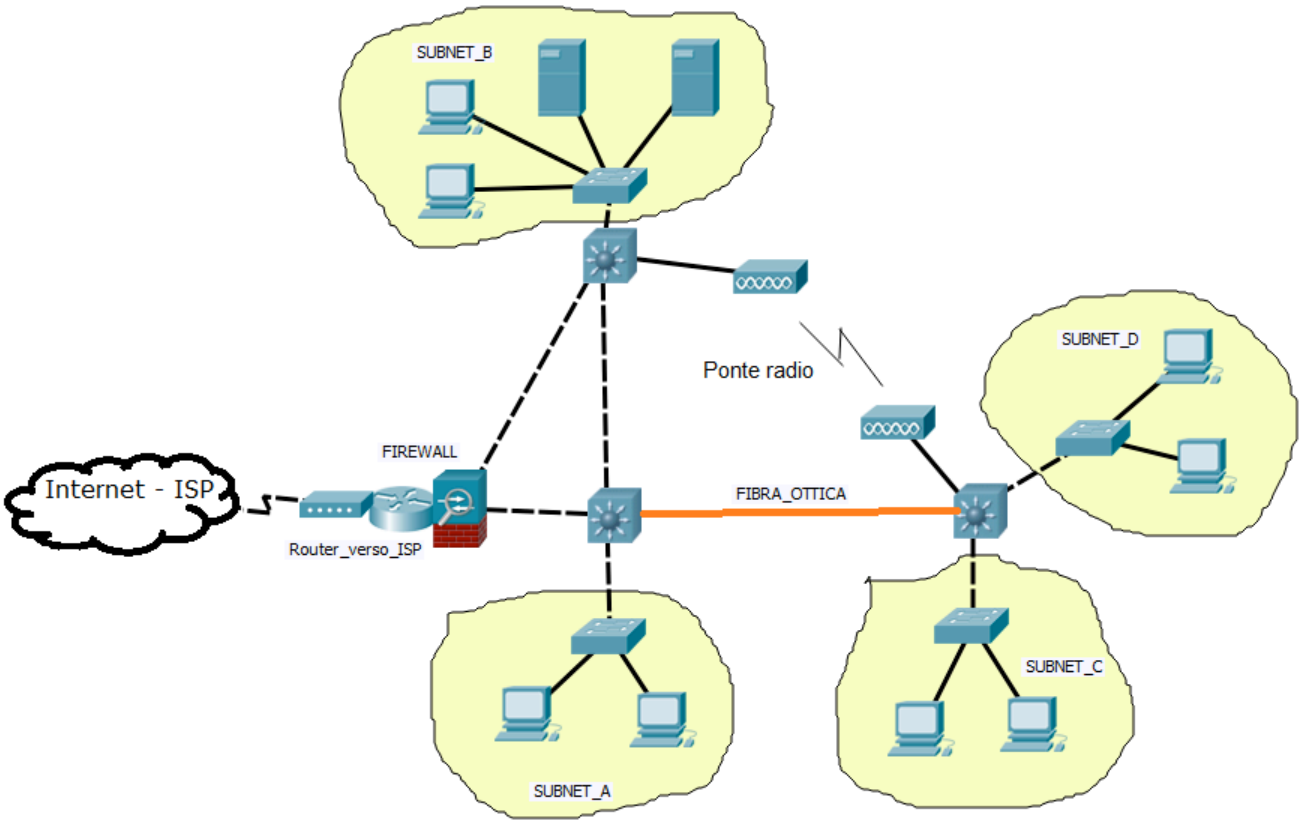


FIGURA 2. Struttura di rete ridondata.

Se le esigenze di alta disponibilità e tolleranza ai guasti (o *fault-tolerance*) della rete fossero ancora più spinte, si può ipotizzare di ridondare gli apparati di rete (Layer 3) e/o l'accesso a Internet, sostituendo a ogni apparato una coppia di apparati che gestiscono la ridondanza con un protocollo di tipo **FHRP-First Hop Redundancy Protocol**[4] e utilizzando due connessioni[5] verso Internet. Per la duplicazione del Firewall o del Router verso l'ISP, che non fungono da default gateway, esistono protocolli analoghi.

[4] Come HRSP (Hot Standby Router Protocol), VRRP(Virtual Router Redundancy Protocol) o GLBP(Gateway Load Balancing Protocol); essi si presentano agli host come se fossero un unico apparato che funge anche da default gateway; nel caso in cui un apparato si guasti subentra automaticamente l'altro senza dover modificare la configurazione IP degli host, che non si accorgono di quanto è avvenuto.

[5] Le connessioni ridondate verso Internet vengono dette *Dual-Homed* se sono verso uno stesso ISP, che fornisce due connessioni, e *Multihomed* se sono verso due ISP diversi, che possono fornire una o due connessioni ciascuno (*Dual-Multihomed*)

Nel proseguire la discussione dei punti proposti è conveniente affrontare prima il punto 3 (piano di indirizzamento) e poi il punto 2 in quanto l'esame delle tabelle di instradamento (o tabelle di routing) risulta più chiaro se si esplicitano gli indirizzi IP.

3. Piano di indirizzamento

D. Proponga e discuta un opportuno piano di indirizzamento basato sull'uso di indirizzi privati IPv4 .

R.

Premessa

Dal punto di vista dello schema di **indirizzamento**, per la rete di partenza proposta dalla traccia d'esame è teoricamente possibile un subnetting variabile su una rete di classe C, per esempio la 192.168.1.0/24 (subnet mask 255.255.255.0), effettuato come segue (si noti l'inversione tra le sottoreti **C** e **D**, per lasciare la C, più piccola, in fondo):

- Sottorete A: 192.168.1.0/26 termina a 192.168.1.63 (broadcast)
- Sottorete B: 192.168.1.64/26 termina a 192.168.1.127 (broadcast)
- Sottorete **D**: 192.168.1.128/26 termina a 192.168.1.191 (broadcast)
- Sottorete **C**: 192.168.1.192/27 termina a 192.168.1.223 (broadcast)
- Sottorete A-B: 192.168.1.224/30 termina a 192.168.1.227 (broadcast)
- Sottorete A-C: 192.168.1.228/30 termina a 192.168.1.231 (broadcast)
- Sottorete C-D: 192.168.1.232/30 termina a 192.168.1.235 (broadcast)
- Sottorete ISP: IP e Subnet Mask forniti dall'ISP

Tuttavia questo schema di indirizzamento è **molto stretto**, specie per la sottorete A, e per un eventuale ulteriore aumento della sottorete D, per cui nelle proposte si deve offrire uno schema più facilmente scalabile.

Per non offrire un piano di indirizzamento troppo stretto, si può abbandonare l'ipotesi di uso di una sola rete di Classe C e, per esempio, ricavare gli indirizzi per le subnet dal blocco di indirizzi IPv4 privati di Classe A 10.0.0.0/8, che offre anche il piccolo vantaggio di creare indirizzi più facili da scrivere.
Iniziamo a proporre un piano di indirizzamento per la struttura di rete non ridondata, che comprende 2 soli router (o switch Layer 3).
Per le sottoreti degli utenti (A, B, C, D) scegliamo di differenziarle già dalla terza cifra dell'indirizzo di rete, cioè di trarle da diverse subnet con subnet mask /24 del blocco di indirizzi IPv4 privati 10.0.0.0/8, in modo che, qualunque sia la crescita dell'ente di ricerca, ogni sottorete possa arrivare a comprendere fino a un massimo di 254 host semplicemente variando la lunghezza della subnet mask (si veda il punto 2 della seconda parte). Il piano di indirizzamento che si propone è quindi il seguente (FIGURA 3):

- **subnet A** -> indirizzo di sottorete 10.0.1.0 /26, subnet mask 255.255.255.192
  prefisso di rete di 26 bit (/26); 6 bit per la parte host dell'indirizzo IPv4
  $2^6 - 2 = 62$ indirizzi IPv4 disponibili per gli host, da 10.0.1.1 a 10.0.1.62;
  indirizzi occupati: 60; indirizzi liberi: 2
  indirizzo di broadcast 10.0.1.63;
- **subnet B** -> indirizzo di sottorete 10.0.2.0 /26, subnet mask 255.255.255.192
  prefisso di rete di 26 bit (/26); 6 bit per la parte host dell'indirizzo IPv4
  $2^6 - 2 = 62$ indirizzi IPv4 disponibili per gli host, da 10.0.2.1 a 10.0.2.62;
  indirizzi occupati: 48; indirizzi liberi: 14
  indirizzo di broadcast 10.0.2.63;

- **subnet C** -> indirizzo di sottorete 10.0.3.0 /27, subnet mask 255.255.255.224
  prefisso di rete di 27 bit (/27); 5 bit per la parte host dell'indirizzo IPv4
  $2^5 - 2 = 32$ indirizzi IPv4 disponibili per gli host, da 10.0.3.1 a 10.0.3.30;
  indirizzi occupati: 25; indirizzi liberi: 7
  indirizzo di broadcast 10.0.3.31;
- **subnet D** -> indirizzo di sottorete 10.0.4.0 /26, subnet mask 255.255.255.192
  prefisso di rete di 26 bit (/26); 6 bit per la parte host dell'indirizzo IPv4
  $2^6 - 2 = 62$ indirizzi IPv4 disponibili per gli host, da 10.0.4.1 a 10.0.4.62;
  indirizzi occupati: 48; indirizzi liberi: 14
  indirizzo di broadcast 10.0.4.63;
- **subnet AC-CD** (collegamento fra i router)-> indirizzo di sottorete 10.0.7.0 /30, subnet mask 255.255.255.252
  prefisso di rete di 30 bit (/30); 2 bit per la parte host dell'indirizzo IPv4
  $2^2 - 2 = 2$ indirizzi IPv4 disponibili per gli host: 10.0.7.1 e 10.0.7.2;
  indirizzi occupati: 2; indirizzi liberi: 0
  indirizzo di broadcast 10.0.7.3.

Le reti non utilizzate 10.0.0.0/24, 10.0.5.0/24 e 10.0.6.0/24 permettono una crescita ordinata del piano di indirizzamento[6], nell'ipotesi che l'ente di ricerca possa dotarsi di altre tre sottoreti di ricercatori o amministrativi. Come normalmente avviene, ipotizziamo infine che gli indirizzi per la subnet del collegamento verso Internet[7] siano forniti dall'ISP (*Internet Service Provider*).

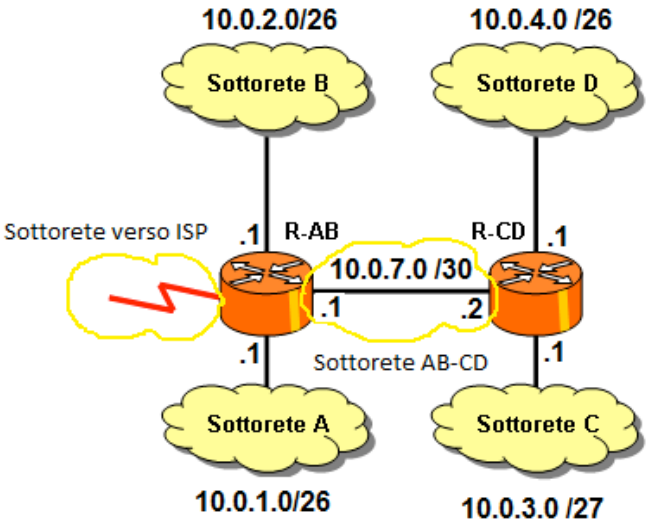


FIGURA 3. Piano di indirizzamento proposto.

Il piano di indirizzamento nel caso di rete ridondata con topologia a maglia può seguire gli stessi criteri e aggiungere le subnet necessarie per i collegamenti ridondati fra gli switch Layer 3 e verso Internet.

---

[6] Inoltre risulta facile implementare la funzione di **NAT** per tutte le subnet da 0 a 7, creando un'ACL (Access Control List) che traduce tutti gli indirizzi della subnet 10.0.0.0 /21.

[7] L'apparato L3 (Router o Switch) collegato all'ISP deve implementare la funzione **NAT** sugli IP privati, per esempio utilizzando come IP pubblico quello assegnato dall'ISP all'interfaccia più esterna delle rete (per esempio denominata serial0/0/0) con i comandi:

- R(config)#**ip nat inside source list** 1 **interface s**0/0/0 **overload**
- R(config)#**access-list** 1 **permit** 10.0.0.0 0.0.7.255 *N.B. Wildcard Mask opzionale*

2. Tabelle di instradamento

D. Proponga e discuta le tabelle di instradamento dei router impiegati nella nuova struttura di rete.
R.
Prendendo in considerazione il caso di rete non ridondata, l'instradamento nella rete è semplice ed è sufficiente operare con **routing statico**.
Nei router non vanno configurate le sottoreti direttamente connesse alle loro interfacce, in quanto esse sono rilevate e inserite nella tabella di instradamento (o tabella di routing) automaticamente.
Se si desidera che tutti gli host di tutte le sottoreti possano comunicare fra loro ed accedere a Internet si devono configurare le tabelle di routing dei router nel seguente modo[8].
Il router AB deve avere le seguenti rotte (o route):

- una rotta verso la sottorete 10.0.3.0/27, che raggiunge inoltrando i pacchetti all'interfaccia del router CD avente indirizzo IP 10.0.7.2 (*next hop*);
- una rotta verso la sottorete 10.0.4.0/27, che raggiunge inoltrando i pacchetti all'interfaccia del router CD avente indirizzo IP 10.0.7.2 (*next hop*);
- una rotta di default (*default route*) verso il router dell'ISP (e quindi verso Internet), che si raggiunge configurando come *next hop* l'indirizzo IP dell'interfaccia di tale router, oppure configurando come interfaccia su cui inoltrare i pacchetti l'interfaccia che è collegata al router dell'ISP.

Per il router CD è invece sufficiente configurare solo la *default route*, avente come *next hop* l'interfaccia con indirizzo 10.0.7.1 del router AB, in quanto qualsiasi sia la destinazione dei pacchetti è necessario instradarli in quella direzione.
Un utile ausilio alla compilazione della tabella di routing può essere una tabella di progetto come la seguente.

Esempio di tabella di progetto.

	Router-AB	**Router-CD**	
Sottorete IP di destinazione	**Next Hop**	**Next Hop**	**Commento**
10.0.1.0/26	Rete direttamente connessa (C)	10.0.7.1	Il router-CD inoltra sulla default route i pacchetti IP destinati alla sottorete 10.0.1.0/26
10.0.2.0/26	Rete direttamente connessa (C)	10.0.7.1	Il router-CD inoltra sulla default route i pacchetti IP destinati alla sottorete 10.0.1.0/26
10.0.3.0/27	10.0.7.2	Rete direttamente connessa (C)	Il router-AB inoltra verso l'interfaccia del router CD a cui è collegato con fibra ottica i pacchetti IP destinati alla sottorete 10.0.3.0/27
10.0.4.0/26	10.0.7.2	Rete direttamente connessa (C)	Il router-AB inoltra verso l'interfaccia del router CD a cui è collegato con fibra ottica i pacchetti IP destinati alla sottorete 10.0.4.0/26
0.0.0.0/0 (default route)	Indirizzo IP router ISP	10.0.7.1	Il router AB inoltra verso il router dell'ISP tutti i pacchetti aventi destinazione diversa da quella delle sottoreti A, B, C, D. Il router-CD deve inoltrare qualsiasi pacchetto IP all'interfaccia (10.0.7.1) del router AB a cui è connesso tramite il link in f.o.

[8] Esempi di comandi IOS Cisco per configurare le rotte sono i seguenti (usiamo D per indicare il generico Device, che può essere un Router o uno Switch L3):

- D-AB(config)**#ip route 10.0.3.0 255.255.255.224 10.0.7.2** *route verso la sottorete C*
- D-AB(config)**# ip route 10.0.4.0 255.255.255.192 10.0.7.2** *route verso la sottorete D*
- D-AB(config)**#ip route 0.0.0.0 0.0.0.0 s**0/0/0 *default route verso Internet tramite l'interfaccia seriale verso l'ISP*
- D-CD(config)**#ip route 0.0.0.0 0.0.0.0** 10.0.7.1 *default route verso sinistra*

La tabella di routing del router AB è quindi del tipo:

Indirizzo IP di (sotto) rete	Subnet mask	Next hop	Distanza amministrativa
10.0.1.0	255.255.255.192	- (C)	0
10.0.2.0	255.255.255.192	- (C)	0
10.0.3.0	255.255.255.224	10.0.7.2	1
10.0.4.0	255.255.255.192	10.0.7.2	1
0.0.0.0	0.0.0.0	Interf. router ISP	1

La tabella di routing del router CD è quindi del tipo:

Indirizzo IP di (sotto) rete	Subnet mask	Next hop	Distanza amministrativa
10.0.3.0	255.255.255.224	- (C)	0
10.0.4.0	255.255.255.192	- (C)	0
0.0.0.0	0.0.0.0	10.0.7.1	1

Nel caso di rete con topologia ridondata la configurazione delle rotte è più complessa, in quanto è possibile:

- definire la rotta (cioè il percorso) che, in condizioni normali, devono seguire i pacchetti lasciando come distanza amministrativa quella di default, che è 1;
- assegnare alle rotte da seguire in caso di interruzione del collegamento principale (in f.o.) una distanza amministrativa maggiore (per esempio 200), in modo tale che vengano prese in considerazione solo se la rotta principale non è più attiva per via di guasti o interruzioni.

In alternativa si può attivare e configurare un protocollo di routing dinamico, come il RIP, che gestisce automaticamente le rotte nella tabella di routing.

4. Velocità minima

D. Valuti la minima velocità a livello fisico necessaria per sostenere un'applicazione che richiede un ***data rate*** di almeno 64 kbps, quando le condizioni di traffico sono tali da avere un tempo di latenza di 30 ms, in relazione a un qualunque elaboratore appartenente alla rete, che debba stabilire una comunicazione regolata dai protocolli illustrati nella tabella sottostante.

Livello di protocollo	*Procedura di trasferimento trame*	*Lunghezza header trame*	*Lunghezza payload*
Applicazione	Non confermata	12 byte	Massimo 1024 byte
Trasporto	Non confermata	8 byte	Massimo 1024 byte
Rete	Non confermata	20 byte	Massimo 1024 byte
Linea	Non confermata	26 byte	Massimo 1024 byte

R.
In considerazione del valore indicato come *data rate* (64 kbit/s) e della lunghezza che hanno gli header delle PDU (*Protocol Data Unit*) dei protocolli che regolano la comunicazione, si può ipotizzare che il caso proposto dal punto 4 sia un caso di comunicazione VoIP con applicativi/softphone/telefoni IP che utilizzano un codec PCM (conforme alla Raccomandazione ITU-T G.711).
Infatti in un comunicazione VoIP di questo tipo:

- il codec produce un flusso di bit caratterizzato da un data rate di 64 kbit/s (netti);
- si utilizza il protocollo di applicazione RTP (*Real Time Protocol*), che ha un header di 12 byte (B);
- si utilizza il protocollo di trasporto (strato 4) UDP, protocollo *connectionless*, senza riscontro (procedura di trasferimento non confermata), che ha un header di 8 B;
- ogni segmento (PDU) del protocollo UDP è incapsulato in un pacchetto IPv4 (strato 3), che ha un header di 20 (B);

- ogni pacchetto IP è incapsulato in un frame Ethernet (strato 2) che ha un header (comprensivo anche dell'FCS, *Frame Check Sequence*) di 26 B: 8 B di preambolo e SFD - *Start Frame Delimiter*; 12 B di indirizzi MAC destinazione e sorgente; 2 B di *protocol type* (o *Ethertype)*; 4 B di FCS.

La domanda può quindi essere considerata come il calcolo dell'effettiva occupazione di banda digitale a livello fisico di una direzione di una connessione VoIP, o se si preferisce del *data rate* lordo (bit/s totali necessari) con cui si trasferisce a livello fisico un flusso VoIP (in una direzione), in quanto la tracciaspecifica che la rete opera a 1 Gbps, per cui la velocità di trasmissione effettiva con cui si opera sul mezzo fisico è di 1 Gbit/s.
Il tempo di latenza può essere considerato come il tempo che intercorre fra l'invio del primo bit di un frame e la ricezione dell'ultimo bit del frame stesso, dato che si impiega il protocollo di trasporto UDP che è senza riscontro (*connectionless*), cioè non effettua né correzione d'errore né controllo di flusso.
Si noti che in termini generali operando in modalità connectionless, senza conferma della corretta ricezione delle PDU, la latenza è considerabile come la somma della durata di un frame (rapporto fra il numero di bit che compongono il frame e la velocità di trasmissione oppure prodotto fra il numero di bit che compongono il frame e il tempo di bit) e dei ritardi introdotti dal collegamento (tempi di propagazione sul mezzo fisico e ritardi introdotti dagli apparati).

Nel caso in esame, però, si può effettuare un'analisi semplificata in quanto il valore della latenza è relativamente elevato e non sono noti i tempi di ritardo dei collegamenti (dell'ordine dei μs su distanze massime attorno ai 300 m) e degli apparati, per cui è presumibile che la latenza stessa sia dovuta essenzialmente a come operano gli applicativi/softphone/telefoni IP.
Procediamo quindi nel seguente modo.
Considerando un data rate pari a 64 kbps si ha che in 30 ms si devono trasferire almeno:

$$Payload = 64000 \cdot \frac{30}{1000} = 1920 \quad bit \text{ , pari a } Payload = \frac{1920}{8} = 240 \quad byte \text{ (B).}$$

Possiamo quindi ipotizzare che il *payload* del protocollo RTP sia pari a 240 B (viene specificato che 1024 è il massimo possibile), per cui sommando gli header dei vari protocolli si ha che un frame è composto da $240 + 12 + 8 + 20 + 26 = 306 \quad B$, pari a $306 \cdot 8 = 2448 \quad bit$, i quali devono essere trasferiti in 30 ms.
Per inciso si noti che il payload del protocollo RTP non può essere uguale a 1024 B, in quanto il payload del protocollo di livello 2 (o protocollo di linea) è di 1024 B e quindi è necessario sottrarre a tale valore gli header dei protocolli IP, UDP e RTP. Il massimo valore utilizzabile per il payload del protocollo RTP è quindi pari a:

$$Max\_Payload\_RTP = 1024 - 20 - 8 - 12 = 984 \quad Byte$$

In un secondo si devono quindi trasmettere 2448*(1000/30) bit e quindi la minima velocità di trasmissione a livello fisico, corrispondente all'occupazione di banda digitale, risulta pari a

$$V_{TX} = 2448 \cdot \frac{1000}{30} \cong 81{,}6 \quad kbit/s$$

Il valore corrisponde all'incirca all'effettiva occupazione di banda digitale (o se si preferisce alla minima velocità di trasmissione a livello fisico richiesta) da una direzione di una comunicazione VoIP in cui i terminali utilizzano un codec[9] PCM a 64 kbit/s (codec G.711).
Essendo la rete di tipo gigabit Ethernet si possono quindi avere molte comunicazioni VoIP contemporanee senza incidere in modo significativo sulle prestazioni offerte alle altre applicazioni.

[9] Nella pratica si trasmettono 50 frame al secondo e si utilizza un payload di 160 B per il protocollo RTP.

SECONDA PARTE

Il candidato scelga due fra i seguenti quesiti e per ciascun quesito scelto formuli una risposta della **lunghezza massima di 20 righe** esclusi eventuali grafici, schemi e tabelle.

1. D. Esamina nel dettaglio i pro e i contro della possibile realizzazione in ponte radio di una connessione tra i due edifici su cui si estende la rete proposta nella prima parte della prova.

R.
La distanza fra i due edifici è limitata a 100 m e si può ipotizzare che essi insistano su uno stesso fondo privato (un campus) in quanto esiste un cavidotto che li collega.
Date queste premesse è possibile considerare l'impiego delle tecnologie Wi-Fi o HIPERLAN per realizzare un collegamento in ponte radio fra i due edifici, impiegando una coppia di apparati Wi-Fi/HIPERLAN da esterno configurati per operare come *bridge*.

Vantaggi:
- su un fondo privato l'impiego di tali apparati, che operano nelle bande ISM (*Industrial, Scientific and Medical*) a 2,4 GHz o 5 GHz, è libero in quanto non sono richieste né licenze né autorizzazioni d'uso; se si attraversa suolo pubblico va richiesta una semplice autorizzazione d'uso ministeriale;
- impiegando apparati di nuova generazione, conformi allo standard IEEE 802.11ac, si opera nella banda di frequenze non soggetta a licenza attorno ai[10] 5 GHz, meno soggetta a interferenze, con canali aventi banda fino a 80 MHz e tecniche di modulazione avanzate (fino alla 256QAM) il che, in condizioni ottimali, consente velocità di trasmissione nominali molto elevate (per esempio fino 866 Mbit/s), comparabili con quelle indicate dal testo della prova;
- se gli edifici si trovano in visibilità ottica la realizzazione del collegamento è molto rapida ed economica in quanto non richiede opere infrastrutturali né scavi;
- a seconda delle esigenze, il collegamento in ponte radio può essere utilizzato come collegamento che si affianca a quello esistente oppure come collegamento di riserva nel caso il collegamento principale (su fibra ottica) si interrompa, aumentando l'affidabilità della struttura di rete.

Svantaggi:
- i collegamenti radio sono intrinsecamente meno protetti dal punto di vista della qualità del segnale ricevuto, in quanto possono essere soggetti a fading, ad attenuazione variabile in funzione delle condizioni meteo, a rumore, a interferenze (specie se si opera nella banda ISM dei 2,4 GHz) ecc., fattori che possono comportare un aumento della probabilità d'errore;
- se le condizioni in cui si opera non sono ottimali è necessario diminuire la velocità di trasmissione al fine di evitare una probabilità d'errore elevata;
- i collegamenti radio sono intrinsecamente meno protetti dal punto di vista delle intercettazioni, per cui vanno impiegate adeguate tecniche di autenticazione e crittografia sui dati trasmessi via radio (per esempio adottando la tecnica WPA2), nonché antenne ad elevata direttività (alto guadagno) che tra l'altro limitano la copertura radio allo stretto necessario;
- se gli edifici non sono in visibilità ottica gli ostacoli che si interpongono fra essi (in particolare quelli che rientrano nella prima zona di Fresnel) determinano un notevole aumento dell'attenuazione, che può diventare eccessiva, per cui può essere necessario eseguire opere infrastrutturali (tralicci, ecc.) che ripristino la visibilità ottica oppure interporre un ripetitore.

[10] per esempio fra 5,4 e 5,725 GHz, frequenze utilizzate anche dagli apparati HIPERLAN/2 per cui tali apparati sono anche noti come HIPERLAN 802.11ac

2. D. Spiega come si potrebbe procedere all'indirizzamento nel caso in cui, pur mantenendo la struttura di rete illustrata nella prima parte della prova, si voglia raddoppiare il numero degli elaboratori presenti in ciascuna sottorete.

R.

Un indirizzo IPv4 è composto da 32 bit dei quali i primi *n* costituiscono il prefisso di (sotto)rete e gli ultimi *h = 32 - n* costituiscono la parte host. L'individuazione del prefisso di rete di un indirizzo IPv4 avviene grazie alla subnet mask, che espressa in notazione binaria è una sequenza di 32 bit dei quali i primi *n* sono posti a 1 ed i rimanenti *h* = 32 - *n* sono posti a 0. La lunghezza della subnet mask è data dal numero di bit posti a 1 che la compongono e coincide con la lunghezza del prefisso di rete, per cui è spesso indicata affiancando all'indirizzo IPv4 la notazione */n*. Un'operazione di *and* in binario fra un indirizzo IPv4 e la subnet mask fornisce l'indirizzo IPv4 di (sotto)rete, caratterizzato dalla parte host posta a zero.
Ne consegue che i dispositivi (host) che appartengono a una stessa sottorete IP hanno degli indirizzi IPv4 aventi lo stesso prefisso di rete e che si differenziano per la parte host.

Con una parte host di *h* bit sono così disponibili in totale $m = 2^h$ indirizzi IPv4, dei quali quelli effettivamente utilizzabili sono $k = 2^h - 2$ in quanto l'indirizzo avente parte host posta a 0 è riservato all'indirizzo di (sotto)rete mentre quello avente parte host posta tutta a 1 viene utilizzato come indirizzo di broadcast.
Date queste premesse e tenendo conto delle scelte fatte al punto 3 della prima parte, il piano di indirizzamento che consente il raddoppio del numero del numero di elaboratori presenti in ciascuna sottorete può essere ottenuto semplicemente accorciando di un bit le subnet mask utilizzata in precedenza.
Il nuovo piano di indirizzamento risulta quindi il seguente:

- **subnet A** -> indirizzo di sottorete 10.0.1.0 /25, subnet mask 255.255.255.128 (che posta in formato binario fornisce una sequenza di 25 "1" seguita da 7 "0");
  prefisso di rete di 25 bit (/25); 7 bit per la parte host dell'indirizzo IPv4;
  $2^7 - 2 = 126$ indirizzi IPv4 disponibili per gli host, da 10.0.1.1 a 10.0.1.126;
  indirizzi occupati: 120; indirizzi liberi: 6
  indirizzo di broadcast 10.0.1.127;
- **subnet B** -> indirizzo di sottorete 10.0.2.0 /25, subnet mask 255.255.255.128
  prefisso di rete di 25 bit (/25); 7 bit per la parte host dell'indirizzo IPv4
  $2^7 - 2 = 126$ indirizzi IPv4 disponibili per gli host, da 10.0.2.1 a 10.0.2.126;
  indirizzi occupati: 96; indirizzi liberi: 30
  indirizzo di broadcast 10.0.2.127;
- **subnet C** -> indirizzo di sottorete 10.0.3.0 /26, subnet mask 255.255.255.192
  prefisso di rete di 26 bit (/26); 6 bit per la parte host dell'indirizzo IPv4
  $2^6 - 2 = 62$ indirizzi IPv4 disponibili per gli host, da 10.0.3.1 a 10.0.3.62;
  indirizzi occupati: 50; indirizzi liberi: 12
  indirizzo di broadcast 10.0.3.63;
- **subnet D** -> indirizzo di sottorete 10.0.4.0 /25, subnet mask 255.255.255.128
  prefisso di rete di 25 bit (/25); 7 bit per la parte host dell'indirizzo IPv4
  $2^7 - 2 = 126$ indirizzi IPv4 disponibili per gli host, da 10.0.4.1 a 10.0.4.126;
  indirizzi occupati: 96; indirizzi liberi: 30
  indirizzo di broadcast 10.0.4.127.

3. D. Nell'ambito dei dispositivi di interconnessione, spiega la funzione rispettivamente di router e switch, mettendone in evidenza le differenze.

R.

Un router viene definito come un apparato di livello (o strato, layer) 3 poiché opera a livello IP (strato 3 OSI). Esso ha la funzione di nodo di rete IP in quanto instrada i pacchetti IP che giungono alle sue interfacce verso le reti IP di destinazione. Un router quindi interconnette reti o sottoreti IP diverse, cioè consente la comunicazione fra host che appartengono a reti o sottoreti aventi indirizzo IP di rete diverso.

Per poter effettuare gli instradamenti un router consulta la propria tabella di routing (o tabella di inoltro).

In linea di principio una tabella di routing è una tabella costituita da un certo numero di righe; ogni riga viene detta route (rotta) e indica dove va instradato un pacchetto IP affinché possa giungere a una certa rete IP di destinazione; può anche essere definita una default route che indica dove va instradato un pacchetto IP affinché possa raggiungere una qualsiasi rete IP di destinazione che non sia già presente in un'altra route.

La compilazione della tabella di routing può avvenire:

manualmente, quando si opera con il routing statico; l'amministratore di rete inserisce manualmente, tramite appositi comandi, i parametri che formano la route[11];

automaticamente, quando si opera con il routing dinamico attivando e configurando almeno un protocollo di routing (ne sono esempio il protocollo RIP e l'OSPF); in questo caso i router si scambiano informazioni sulle reti che possono raggiungere, nonché sulle caratteristiche dei percorsi, tramite il protocollo di routing e possono così compilare e tenere aggiornate automaticamente le proprie tabelle di routing.

Nella sua accezione originaria uno switch Ethernet viene definito come un apparato di livello (o strato, layer) 2 poiché opera a livello di protocollo Ethernet/MAC (*Medium Access Control*), appartenente allo strato 2 OSI. Esso ha la funzione di instradare i frame Ethernet/MAC che giungono alle sue interfacce verso le schede di rete Ethernet di destinazione, ciascuna identificata dal proprio indirizzo MAC (noto anche come indirizzo fisico o indirizzo hardware); uno switch costituisce quindi un nodo di rete operante all'interno di una LAN per consentire la comunicazione fra gli host di una stessa LAN (configurati anche per appartenere a una stessa subnet IP). Uno switch opera consultando la propria tabella di switching, che è considerabile come una tabella costituita da un certo numero di righe; ogni riga indica su quale interfaccia va inoltrato un frame affinché possa raggiungere la scheda di rete identificata dall'indirizzo MAC presente nella riga stessa; fanno eccezione i frame il cui indirizzo MAC di destinazione è quello di broadcast (costituito da 48 "1", FFFFFFFFFFFF in esadecimale) i quali vengono inoltrati su tutte le interfacce (tranne quella da cui giungono) in quanto sono diretti a tutte le schede di rete appartenenti alla LAN. Normalmente la tabella di switching viene compilata automaticamente dallo switch. Nel caso di switch amministrabili è possibile configurare la tabella di switching in modo da creare delle VLAN (Virtual LAN), impedire accessi non autorizzati alle porte dello switch ecc.

Riassumendo, quindi, un router ha la funzione di interconnettere reti IP diverse, mentre uno switch viene utilizzato per realizzare una LAN Ethernet, i cui host vanno però configurati anche come appartenenti alla stessa subnet IP affinché possano comunicare direttamente, cioè senza l'intervento di router.

L'evoluzione tecnologica degli apparati ha portato a integrare le funzioni di switch e router, realizzate con apposito hardware che velocizza le operazioni effettuate, in un unico apparato che viene comunemente indicato come **switch Layer 3** o **Multilayer Switch**. Questi apparati normalmente non dispongono di interfacce seriali, atte al collegamento verso alcuni tipi di WAN.

[11] Tipicamente sono i seguenti: indirizzo IP della rete di destinazione; subnet mask; next hop (indirizzo IP dell'interfaccia del prossimo router a cui va inoltrato il pacchetto) o interfaccia di uscita su cui inoltrare il pacchetto affinché possa raggiungere la rete di destinazione; distanza amministrativa (o costo) che consente di stabilire delle priorità quando vi sono più route che portano verso una stessa rete di destinazione: minore è il valore della distanza amministrativa e più alta è la priorità (di default è 1).

4. D. Nell'ambito dei protocolli di livello 2 dell'architettura di rete ***OSI***, spiega in cosa consiste un controllo di flusso realizzato con tecnica ***stop-and-wait*** indicando in quali casi sia conveniente applicarlo.

R.
Nell'ambito dei protocolli di livello 2 un controllo di flusso con metodo *stop-and-wait*, corrispondente anche a un metodo di rivelazione e correzione d'errore di tipo **ARQ** (*Automatic Repeat reQuest*), consiste nel regolare un trasferimento di frame tra un host (computer) sorgente e un host destinazione attraverso la seguente procedura (FIGURA 4):

- l'host sorgente bufferizza una 2-PDU (*Protocol Data Unit* dello strato 2 OSI denominata usualmente *frame*);
- lo strato 1 (o strato fisico) dell'host sorgente trasmette in linea il frame;
- l'host di destinazione riceve il frame e controlla che non vi siano errori con il metodo del CRC (*Cyclic Redundancy Check*);
- se non vi sono errori l'host di destinazione risponde con un frame di ACK (*ACKnowledge*) per informare l'host sorgente che il frame inviato è giunto correttamente;
- solo dopo aver ricevuto l'ACK l'host sorgente può trasmettere il frame successivo;
- se l'host sorgente riceve un NACK (*Not ACK*) ciò significa che il frame è giunto errato, (o non è giunto se non riceve l'ACK entro un certo tempo), per cui l'host sorgente ritrasmette lo stesso frame.

In questo contesto il *Round Trip Time* (RTT, tempo di andata e ritorno), corrispondente alla *latenza*, può essere definito come l'intervallo di tempo che intercorre fra l'inizio dell'invio di una 2-PDU e la fine della ricezione della conferma di corretta ricezione (ACK).

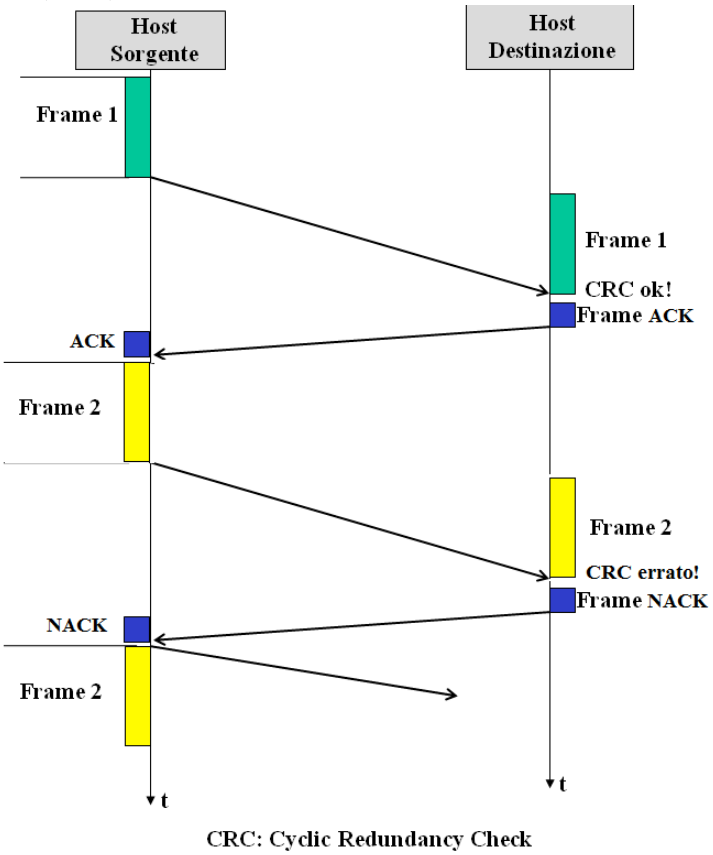


FIGURA 4. Principio del metodo *stop-and-wait*.

Il metodo *stop-and-wait* si presta a essere impiegato almeno nei seguenti casi:

- quando il collegamento presenta una probabilità d'errore non trascurabile, come nei collegamenti radio in cui si possono avere livelli di rumore e di interferenze relativamente elevati; infatti in presenza di errori non si devono ritrasmettere molti frame, come avviene nel caso dei metodi a finestra di trasmissione che ritrasmettono tutti i frame a partire da quello errato (metodo definito *go back N*);
- quando deve essere garantita la corretta sequenza dei frame ricevuti e si vuole evitare di doverli riordinare in caso d'errore, come avviene con i metodi a finestra di trasmissione che ritrasmettono solo i frame errati (*selective retransmission*).

Riferimenti bibliografici:

- *Manuale Cremonese - Informatica e Telecomunicazioni* - Zanichelli Editore SpA
- Onelio Bertazioli - *Corso di Telecomunicazioni vol. 3* - Zanichelli Editore SpA