Ministero dell'Istruzione dell''Università e della Ricerca

ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITTL – INFORMATICA E TELECOMUNICAZIONI

ARTICOLAZIONE TELECOMUNICAZIONI

Tema di: SISTEMI E RETI

Tipologia c

ESEMPIO PROVA

Il candidato (che potrà eventualmente avvalersi delle conoscenze e competenze maturate attraverso esperienze di alternanza scuola-lavoro, stage o formazione in azienda) svolga la prima parte della prova e risponda a due tra i quesiti proposti nella seconda parte.

PRIMA PARTE

Due edifici aziendali, distanti qualche km, ma facenti parte della stessa struttura produttiva, impiegano due reti indipendenti strutturate come di seguito definito.

Edificio 1.

Rete interna, collegata ad internet tramite un ISP (*Internet Service Provider*), costituita da due sottoreti distinte separate da un router, definite come:

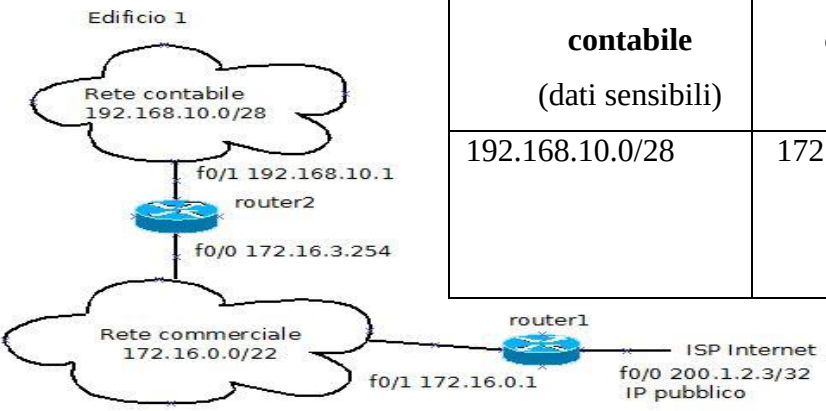
- rete del settore commerciale, dedicata agli specifici operatori;
- rete contabile, dedicata agli specifici operatori, che dovrà farsi carico delle problematiche legate alla presenza di dati sensibili.

L'edificio 1 risulta già adeguatamente cablato in termini di rete e si dovrà eventualmente intervenire solo sugli aspetti relativi alla sicurezza.

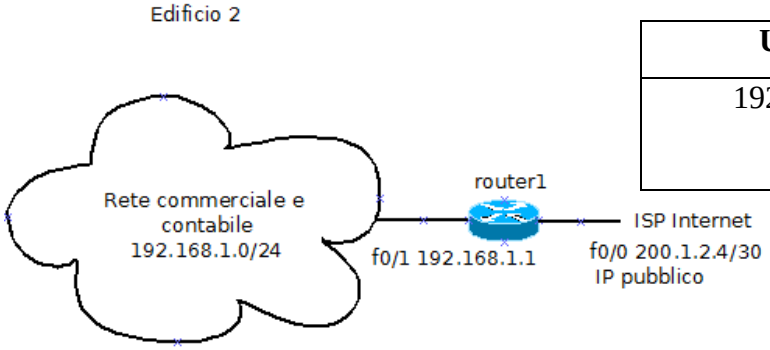
Edificio 2.

Rete unica ad uso commerciale e contabile, definita in un unico spazio di indirizzamento e collegata ad internet tramite un ISP.

I seguenti schemi ne riassumono le caratteristiche:



Sottorete contabile (dati sensibili)	**Sottorete commerciale**	**ISP IP pubblico**
192.168.10.0/28	172.16.0.0/22	200.1.2.3/30 ERRATO: è l'ind. di broadcast della subnet 200.1.2.0/30



Unica rete	**ISP IP pubblico**
192.168.1.0/24	200.1.2.4/30 ERRATO: è un indirizzo di subnet

Il candidato, formulata ogni ipotesi aggiuntiva che ritenga opportuna, predisponga quanto segue:

a. individui i punti di debolezza e le possibili soluzioni da adottare nell'edificio 1, in termini di sicurezza delle reti;

b. progetti la struttura di rete e di indirizzamento dell'edificio 2, che prevede un numero massimo di 7 host per la rete contabile e 15 host per quella commerciale;

c. descriva una soluzione tecnica per separare nell'edificio 2 la rete commerciale dalla rete contabile; gli utenti della rete commerciale non devono poter accedere alla rete contabile; entrambe le utenze devono poter accedere ad Internet aggiungendo, se necessario, anche nuovi apparati;

d. proponga una struttura di collegamento tra i settori commerciali dei due edifici, attraverso la rete Internet, che permetta agli operatori addetti alle postazioni commerciali di comunicare tra loro, con particolare attenzione alla sicurezza e riservatezza dei dati che vengono scambiati tra le due reti.

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.

QUESITO N. 1

Con riferimento al punto D) della prima parte della prova, indicare le caratteristiche principali del protocollo che si è inteso utilizzare.

QUESITO N. 2

Proporre una struttura di collegamento tra i settori contabili dei due edifici, attraverso la rete Internet, che permetta agli operatori addetti alle postazioni contabili di comunicare tra loro, con particolare attenzione alla sicurezza e riservatezza dei dati che vengono scambiati tra le due reti, anche prevedendo l'acquisizione di ulteriori indirizzi IP statici dall' ISP.

QUESITO N. 3

Descrivere le caratteristiche più importanti relative alle tecniche di crittografia a chiave simmetrica ed asimmetrica.

QUESITO N. 4

Nell'ipotesi di istituire un servizio di scambio di messaggi di testo, descrivere, eventualmente anche con un esempio utilizzando un linguaggio a scelta, un socket di comunicazione di tipo client/server adatto allo scopo e definire una possibile architettura hardware.

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 del punto a)

Aspetti relativi alla sicurezza che si possono implementare:

1. **Sicurezza a livello fisico**; gli apparati di rete devono essere posti in locali e in armadi appositi, in modo da essere accessibili solo dal personale tecnico autorizzato, con i locali protetti da sistemi di allarme anti-intrusione; ci devono essere gruppi di continuità (UPS) per sopperire a eventuali interruzioni dell'energia elettrica;

2. **sicurezza a livello 2 OSI**; gli switch devono essere di tipo amministrabile, così da poter prendere misure di sicurezza quali:
   - *port security*, su ciascuna porta di uno switch collegata a un PC lo switch stesso accetta solo frame che hanno come indirizzo MAC sorgente quello del PC stesso; nel caso si colleghi un altro PC (non autorizzato) si ha una violazione e la porta si disattiva (va in *shutdown*);
   - disattivare (shutdown) le porte dello switch non utilizzate e/o porle in una VLAN isolata;
   - impostare password forti per l'accesso alla gestione dello switch, sia da porta console sia da rete (telnet, SSH), e modificare lo username richiesto per l'accesso;
   - utilizzare sono protocolli sicuri (SSH, HTTPS) per la gestione da remoto dello switch;
   - disattivare le modalità di accesso alla gestione dello switch non utilizzate (via telnet, via HTTP);
   - creare una VLAN di amministrazione a cui sono collegati solo i PC dei tecnici abilitati alla gestione dello switch e restringere l'accesso solo a quei PC.

3. Sicurezza perimetrale

L'accesso a Internet va protetto adeguatamente impiegando almeno un **firewall**; in considerazione del fatto che il numero di PC che compongono la rete può essere elevato, risulta conveniente utilizzare un **firewall hardware**, o **firewall appliance**, in grado di controllare il traffico garantendo comunque un throughput elevato; i firewall software integrati nei router di accesso a Internet hanno in genere prestazioni inferiori ai firewall hardware, che sono macchine dedicate e specializzate per le funzioni di firewall.
Il firewall può anche svolgere la funzione di *content filter*, per impedire l'accesso a siti malevoli, non sicuri, ecc. Esso può anche integrare antispam e antivirus.
Il firewall può poi realizzare la/le VPN con le quali ci si collega via Internet all'edificio 2 (e ad altre eventuali sedi anche di aziende partner).
E' anche possibile inserire in rete:

- un *server syslog* che tiene traccia del traffico in entrata e in uscita, registra situazione anomale ecc.
- un IDS/IPS (*Intrusion Detection /Intrusion Prevention Systems*, per esempio basato sul software open source e free *Snort*)

4. **Configurazione di una Access Control List (ACL) sul Router2** (router all'interno della rete dell'edificio 1) che neghi l'accesso alla sottorete contabile da parte dei PC della sottorete commerciale.

5. **Controllo degli accessi ai sistemi informatici e protezione dei dati trasmessi e memorizzati**; vanno prese misure di protezione quali:
   - strumenti di identificazione che, a seconda dei casi, possono essere username e password forte, smart card, sistemi biometrici (per esempio impronte digitali)
   - controller di dominio (amministrazione centralizzata degli utenti)

- crittografia sia per la trasmissione sicura dei dati sia per la loro archiviazione (i dati sensibili possono essere memorizzati sugli hard disk in modo criptato), nonché per l'autenticazione con certificati digitali ecc.; vanno impiegati strumenti software per la comunicazione sicura come TLS/SSL (https), IPsec ecc.

6. **Monitoraggio del funzionamento dei sistemi informatici e delle applicazioni**, assicurando anche aggiornamenti e patch di sicurezza del software

Poiché la sottorete IP (subnet) del settore commerciale ha come indirizzo IP di rete il 172.16.0.0 e come subnet mask una /22, costituita da 22 bit a "1" e 10 bit a "0", essa può comprendere fino a $2^{10} - 2 = 1022$ host. La struttura della rete commerciale potrebbe quindi essere resa più affidabile impiegando un'architettura di rete gerarchica e ridondata che preveda almeno lo strato di accesso, a cui appartengono gli *switch Layer 2* a cui sono collegati gli host (PC ecc.), e lo strato di distribuzione, a cui appartengono degli *switch Layer 3* (per esempio tre collegati a maglia).
In questo caso va attivato il protocollo STP (*Spanning Tree Protocol*), per evitare la formazione di loop tra gli switch, loop che sono causa di "broadcast storm" (gli switch trasmettono continuamente lungo i loop i frame aventi come indirizzo di destinazione quello di broadcast che vanno a saturare rapidamente la banda disponibile).
Visto il numero elevato di PC e la presenza della sottorete del settore contabile, con dati sensibili, risulta poi conveniente configurare un numero adeguato di VLAN, impedendo la comunicazione tra VLAN del settore contabile e VLAN del settore commerciale tramite una Access Control List sul Router-2, così come può essere conveniente porre su una apposita VLAN il traffico derivante da Access Point Wi-Fi presenti in rete.
Entrambi i router (Router-2 e Router-1) devono implementare la funzione NAT:

- Il Router-2, interno, deve implementare anche la funzione NAT, in modo da mascherare la struttura di indirizzamento interna della rete contabile e costituire un *endpoint* della VPN che collega le due sedi contabili, come richiesto dal quesito 2.
- Il Router-1, che dà l'accesso a Internet, deve implementare la funzione NAT per consentire l'accesso a Internet ai PC delle due sottoreti, che sono configurati con indirizzi IPv4 privati, in quanto per l'accesso a Internet è necessario che nei pacchetti IP siano contenuti indirizzi IPv4 pubblici.

Soluzione[1] per i punti b) e c)

Nel caso più semplice l'infrastruttura di rete che si viene a realizzare può essere del tipo riportato in FIGURA 1.

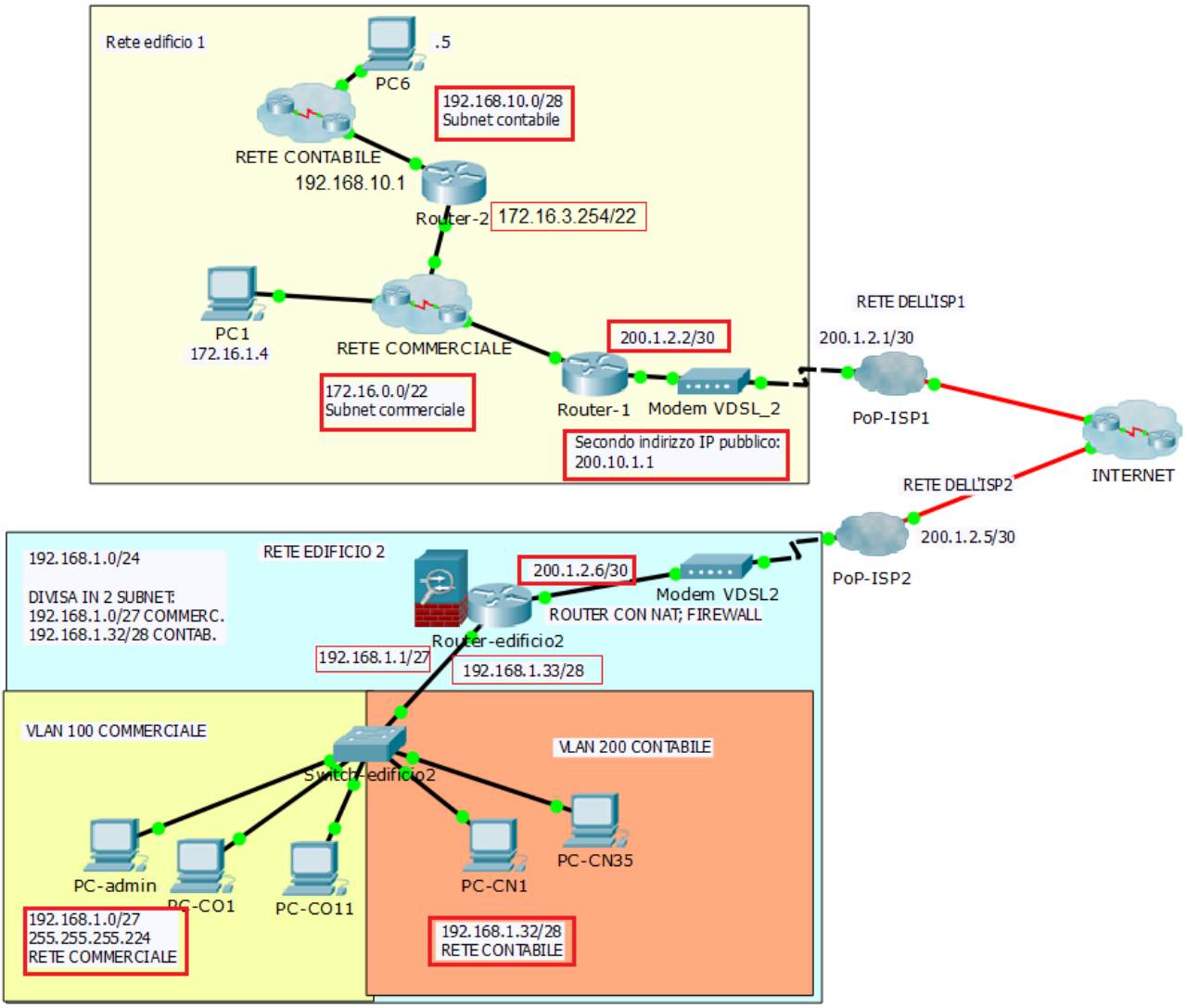


FIGURA 1 Architettura di rete proposta

Per quanto concerne il piano di indirizzamento ricaviamo dal blocco di indirizzi IPv4 privati a disposizione (192.168.1.0/24) due sottoblocchi che abbiano un numero di indirizzi IPv4 il più possibile vicino al numero effettivo di host, ciò per motivi di sicurezza.

- **Piano di indirizzamento per la rete commerciale**
  Essendo la sottorete commerciale di 15 host sono necessari almeno 17 indirizzi IPv4 (1 per la subnet e 1 per il broadcast), per cui gli indirizzi IP devono avere una parte host di almeno 5 bit e un prefisso di rete che al massimo ha 27 bit.
  Scegliamo quindi la subnet mask /27 (255.255.255.224) che consente di avere nella subnet fino a 32-2=30 indirizzi per gli host.
  La sottorete commerciale può quindi essere configurata con il blocco di indirizzi IP 192.168.1.0/27

[1] A scopo didattico sono presentate più soluzioni, complete e funzionanti, di complessità crescente.

La configurazione IP dei PC (indirizzo IP, subnet mask, gateway, server DNS) può essere fatta tramite un server DHCP oppure in modo statico (visto il numero esiguo di PC). Per motivi di sicurezza può essere conveniente dare in ogni caso indirizzi statici, in modo da individuare facilmente i PC nel caso di analisi di traffico ecc.
Il piano di indirizzamento per la sottorete commerciale sarà quindi del tipo:

Sottorete commerciale /27 max 30 host

Indirizzi IPv4	Subnet Mask	Note
192.168.1.0	255.255.255.224	Indirizzo della sottorete (Subnet Address)
192.168.1.1	255.255.255.224	Default Gateway, Interfaccia Gi0/0.1 del router
192.168.1.2	255.255.255.224	Può essere assegnato allo switch
192.168.1.3	255.255.255.224	
192.168.1.4	255.255.255.224	Altri indirizzi assegnabili staticamente ad altri apparati di rete (access point, ecc.)
192.168.1.5	255.255.255.224	
192.168.1.6	255.255.255.224	
192.168.1.7	255.255.255.224	
192.168.1.8	255.255.255.224	
192.168.1.9	255.255.255.224	
192.168.1.10	255.255.255.224	----------
192.168.1.11	255.255.255.224	
192.168.1.12	255.255.255.224	
192.168.1.13	255.255.255.224	
192.168.1.14	255.255.255.224	
192.168.1.15	255.255.255.224	
192.168.1.16	255.255.255.224	Indirizzi IP assegnati ai client via DHCP statico
192.168.1.17	255.255.255.224	con alcuni indirizzi di scorta
192.168.1.18	255.255.255.224	
192.168.1.19	255.255.255.224	
192.168.1.20	255.255.255.224	
192.168.1.21	255.255.255.224	
192.168.1.22	255.255.255.224	
192.168.1.23	255.255.255.224	
192.168.1.24	255.255.255.224	----------
192.168.1.25	255.255.255.224	Assegnabili in modo statico a eventuali server
192.168.1.26	255.255.255.224	
192.168.1.27	255.255.255.224	
192.168.1.28	255.255.255.224	
192.168.1.29	255.255.255.224	
192.168.1.30	255.255.255.224	
192.168.1.31	255.255.255.224	Indirizzo di broadcast (Broadcast Address)

- **Piano di indirizzamento per la rete contabile**
  Essendo la sottorete contabile di 7 host sono necessari almeno 9 indirizzi IPv4 (1 per la subnet e 1 per il broadcast), per cui gli indirizzi IP devono avere una parte host di almeno 4 bit e un prefisso di rete che al massimo ha 28 bit.
  Scegliamo quindi la subnet mask /28 (255.255.255.240) che consente di avere nella subnet fino a 16-2=14 indirizzi per gli host.
  Poiché l'indirizzo di broadcast della rete commerciale è il 192.168.1.31, a sottorete contabile può quindi essere configurata con il blocco di indirizzi IP 192.168.1.32/28.
  La configurazione IP dei PC (indirizzo IP, subnet mask, gateway, server DNS) può essere fatta tramite un server DHCP oppure in modo statico (visto il numero esiguo di PC). Per motivi di sicurezza può essere conveniente dare in ogni caso indirizzi statici, in modo da individuare facilmente i PC nel caso di analisi di traffico ecc.

Il piano di indirizzamento per la sottorete contabile sarà quindi del tipo:

Sottorete contabile /28 (max 14 host)

Indirizzi IPv4	Subnet Mask	Note
192.168.1.32	255.255.255.240	Indirizzo della sottorete (Subnet Address)
192.168.1.33	255.255.255.240	Default Gateway, Interfaccia Gi0/0.2 del router
192.168.1.34	255.255.255.240	Altri indirizzi assegnabili staticamente agli apparati di rete
192.168.1.35	255.255.255.240	
192.168.1.36	255.255.255.240	
192.168.1.37	255.255.255.240	----------
192.168.1.38	255.255.255.240	Indirizzi IP assegnati ai client via DHCP statico
192.168.1.39	255.255.255.240	
192.168.1.40	255.255.255.240	
192.168.1.41	255.255.255.240	
192.168.1.42	255.255.255.240	
192.168.1.43	255.255.255.240	
192.168.1.44	255.255.255.240	----------
192.168.1.45	255.255.255.240	Indirizzi assegnabili in modo statico a eventuali server
192.168.1.46	255.255.255.240	
192.168.1.47	255.255.255.240	Indirizzo di broadcast (Broadcast Address)

Nel caso in cui si prevedano numerosi altri inserimenti in rete (per esempio di PC, smartphone, tablet via Wi-Fi) è possibile optare per una subnet mask **/26** (255.255.255.192) per la rete commerciale, che mette a disposizione 62 indirizzi IP per gli host, e una **/27** (255.255.255.224) per la rete contabile, che mette a disposizione 30 indirizzi IP per gli host.

Infrastruttura di rete dell'edificio 2
Per l'infrastruttura di rete si possono proporre per esempio 3 soluzioni di complessità ed affidabilità crescenti.

1. Soluzione non ridondata
Per l'edificio 2 visto che ci sono pochi PC (7+15=22 host in totale) e si tratta di una filiale, se si desidera limitare i costi si può utilizzare un solo switch amministrabile su cui si configurano tre VLAN (FIGURA 1):

- VLAN 1, di gestione (*management VLAN*) a cui si collega il PC utilizzato dall'amministratore di rete collegato in modo sicuro (*port security*), per esempio alla porta FastEthernet 0/1
- **VLAN 100 name Commerciale**, a cui si collegano i PC dei commerciali (supponiamo siano 13 dato consideriamo come host anche le interfacce dei router e lo switch amministrabile) sulle porte fa0/2-14
- **VLAN 200 name contabile**, a cui si collegano i PC dei contabili (supponiamo siano 6 dato consideriamo come host anche le interfacce dei router) sulle porte fa0/19-24;
  i PC siano collegati in modo sicuro alle rispettive porte (*port security*), che accettano solo frame contenenti i loro indirizzi MAC; in caso di violazione la porta va in shutdown (si disattiva).

  La porta GigabitEthernet0/1 dello switch, collegata alla Gi0/0 del router, viene configurata come *trunk*

Le rimanenti porte dello switch possono essere spente (poste in shutdown) se si desidera evitare ulteriori inserimenti in rete (in questo caso ritenuti abusivi).

Come switch si può utilizzare uno switch dotato di 24 porte fastethernet (100BASE-TX) e due porte gigabitEthernet (1000BASE-T) oppure uno switch dotato di porte tutte GigabitEthernet (soluzione preferibile).
Il collegamento tra switch e router avviene con connessioni Gigabit Ethernet; nel caso di rete completamente nuova è inoltre consigliabile avere un cablaggio almeno in categoria 6, in modo da poter supportare tutti i collegamenti (anche verso i PC) a 1 Gbit/s.
Inoltre si possono inserire almeno 2 access point Wi-Fi, a standard 802.11ac, per consentire un accesso wireless rispettivamente alla rete contabile e alla rete commerciale

Come router si può utilizzare, per esempio, un router con sistema operativo e modulo di crittografia, in grado di svolgere anche la funzione di firewall e di implementare le VPN.
In alternativa, per migliorare le prestazioni ed il controllo del traffico da/verso Internet e la gestione delle VPN, può essere utilizzato un firewall hardware, in grado di fornire una soluzione più completa di protezione della rete, di VPN, di controllo del traffico e di *load balancing*, e un router con integrato un modem xDSL tramite cui si accede a Internet.

Condivisione dell'accesso a Internet.
Per far condividere l'accesso a Internet ad entrambe le reti sull'interfaccia fisica interna (per esempio la GigabitEthernet0/0) si possono configurare *due sottointerfacce*:

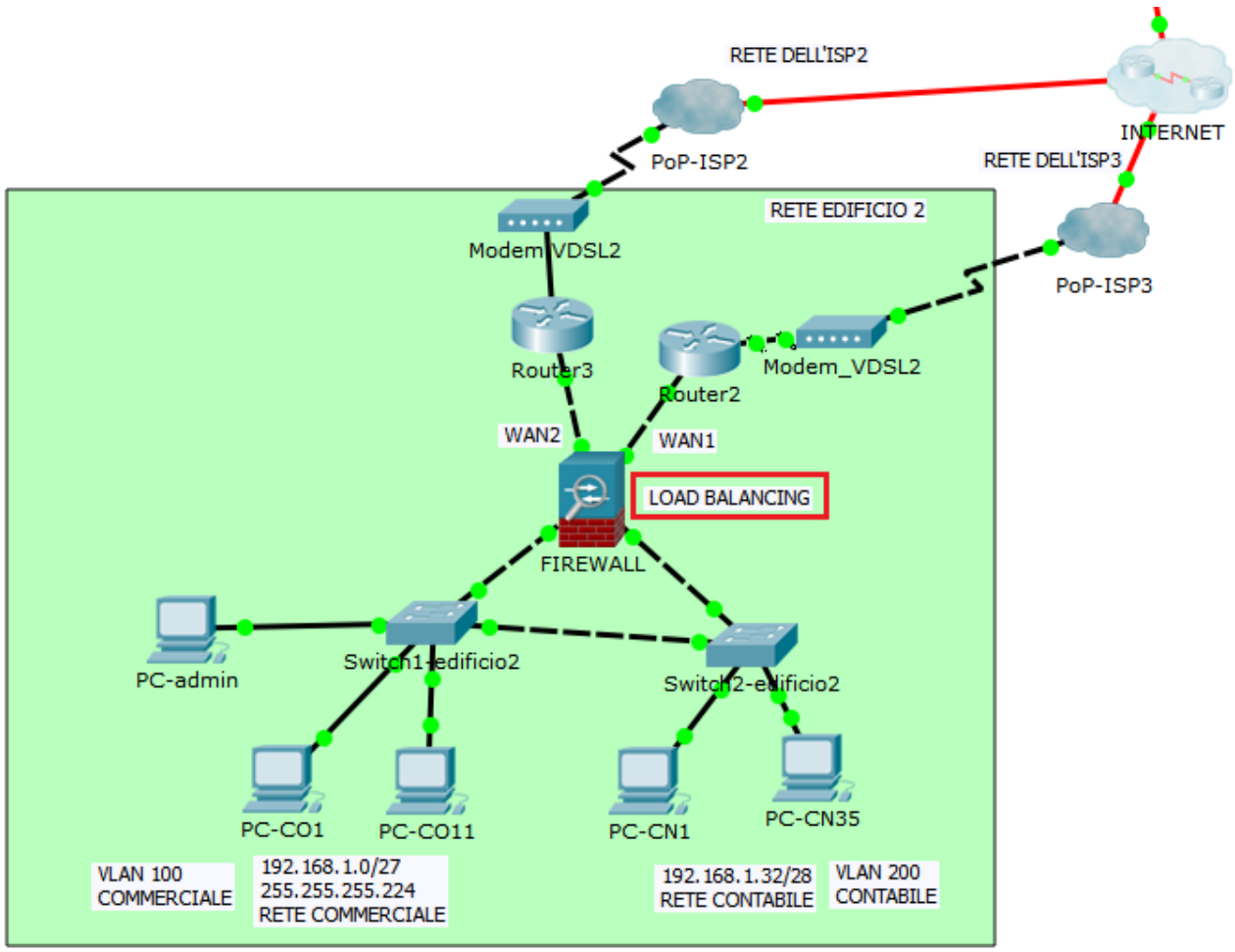
- Gi0/0.1, avente indirizzo IP 192.168.1.1/27, con incapsulamento 802.1q (*dot1q*) e appartenente alla VLAN 100;
- Gi0/0.2, avente indirizzo IP 192.168.1.33/28, con incapsulamento 802.1q (*dot1q*) e appartenente alla VLAN 200.

Per separare le reti commerciale e contabile si configurano sul router due *Access Control List* (ACL) standard, per esempio la 1 e la 99, e le si applica alle due sottointerfacce impedendo (*deny*) ai pacchetti IP contenenti l'indirizzo di rete di una subnet di transitare sulla sottointerfaccia a cui è collegata l'altra subnet.

Infine Poiché sulle reti interne si utilizzano indirizzi IPv4 privati, è necessario implementare nel router la funzione NAT/PAT (o NAT overload), preferibilmente richiedendo un indirizzo IPv4 pubblico statico al'ISP.

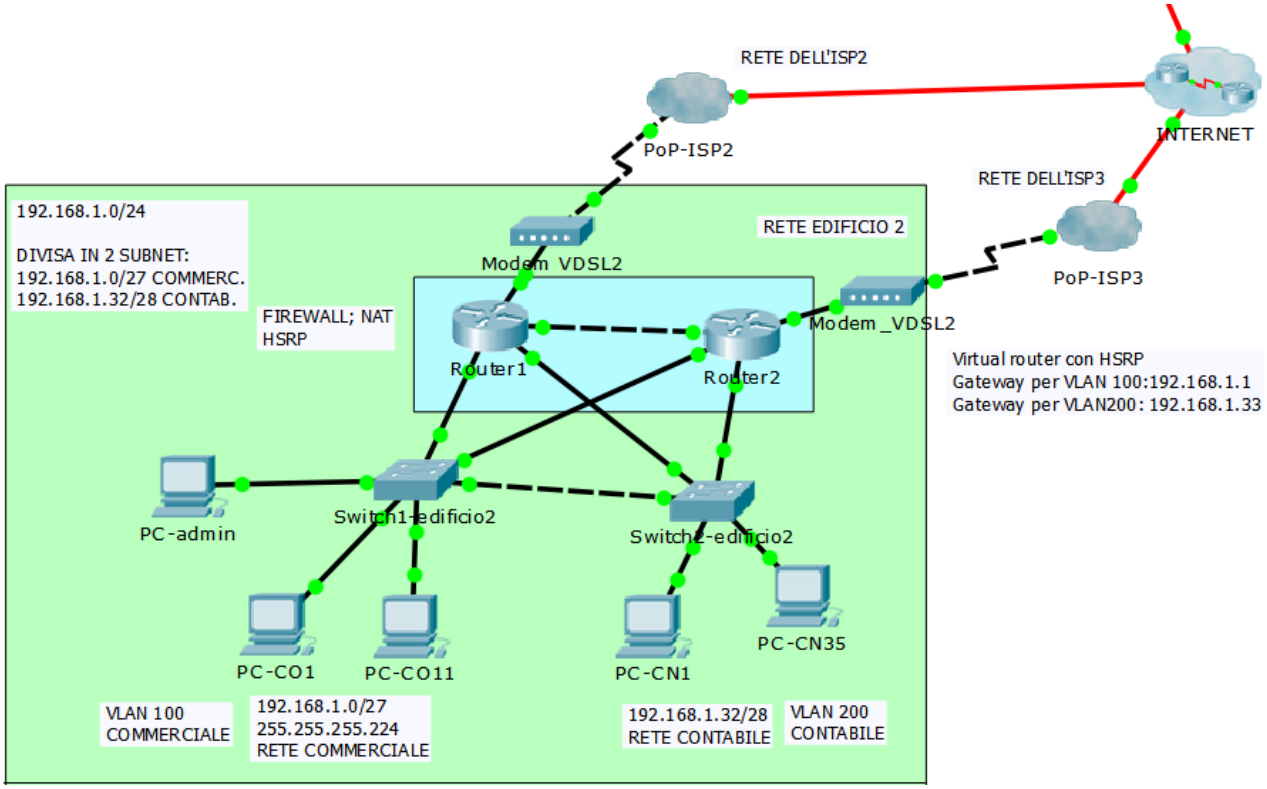
2. Soluzione ridondata

Se si desidera aumentare l'affidabilità della rete dell'edificio 2 è possibile ridondare gli switch ed inserire un modulo switch nel router.
E' anche possibile utilizzare due connessioni Internet (WAN1 e WAN2) con bilanciamento di carico (*load balancing*) fatto tramite un firewall hardware, in modo da aumentare sia l'affidabilità sia le prestazioni dell'accesso a Internet.



3. Soluzione ad alta disponibilità

Infine se si desidera avere una rete ad alta disponibilità, che non presenti il *single point of failure* dato dal router o dal firewall, è anche possibile utilizzare due collegamenti a Internet con due router che implementano un protocollo di tipo *FHRP (First Hop Redundancy Protocol)*, come *l'HSRP (Hot Standby Routing Protocol)* di Cisco.



Soluzione ad alta disponibilità e alte prestazioni

Soluzione per il punto d)

1. Scelta della connettività esterna verso Internet

Come prima cosa va scelto il tipo di connettività a Internet per le reti dei due edifici.
Poiché si impiega Internet per interconnettere le reti dei due edifici dell'azienda, per entrambe le reti dei due edifici la connettività esterna verso Internet dovrebbe essere preferibilmente:

- *di tipo simmetrico* (stessa velocità in upstream e downstream);
- *a banda ultralarga*, in tecnologia FTTC (*Fiber To The Cab/Curb*, fibra fino all'armadio posto sul marciapiede), in cui la rete di accesso dell'ISP è per la gran parte in fibra ottica e solo l'ultimo tratto di qualche centinaio di metri è su doppino in rame,preferibilmente con banda minima garantita, o meglio ancora FTTH (*Fiber To The Home*, connessione completamente su fibra ottica) se la zona è coperta dal servizio.

In questo modo si garantisce una sufficiente velocità di connessione tra le due sedi. Nel caso le connettività FTTC e FTTH non siano disponibili si può optare per una soluzione in tecnologia SHDSL (simmetrica).
Nel caso di soluzione con cablaggio in rame l'interfaccia WAN (esterna) dei router che danno l'accesso a Internet viene collegata al modem xDSL esterno (nel caso di FTTC in tecnologia VDSL2/vectoring, se disponibile).
Infine poiché l'accesso a Internet costituisce una risorsa indispensabile per le attività di un'azienda, può essere conveniente utilizzare un accesso a Internet ridondato, per esempio con una coppia di router che accedono a due ISP diversi, con bilanciamento di carico e/o utilizzano un protocollo di tipo FHRP (First Hop Redundancy Protocol), come l'HSRP (Hot Standby Protocol), come indicato nei punti b) e c).

2. Scelta della struttura di collegamento delle sottoreti commerciali dei due edifici.

Per realizzare il collegamento tra le sottoreti commerciali dei due edifici attraverso Internet, garantendo sicurezza e riservatezza dei dati scambiati, si configurano i due router/firewall che danno l'accesso a Internet per realizzare una **VPN site-to-site** (*Virtual Private Network* da sede a sede) basata sulla suite **IPsec**; in questo modo i due router attivano un *tunnel* attraverso Internet che garantisce sicurezza e riservatezza grazie a *IPsec*: i dati scambiati sono autenticati e crittografati (per esempio autenticazione con algoritmo **SHA**, *Secure Hash Algorithm***,** e crittografia con **3DES**, *Triple Data Encryption Standard*, o **AES**, *Advanced Encryption Standard*).
La VPN può essere implementata utilizzando un firewall hardware oppure un router di accesso a Internet dotato di sistema operativo che integra anche le funzioni di firewall e VPN.
Si rimanda ai libri di testo per la trattazione dettagliata delle VPN site-to-site e di IPsec.

SECONDA PARTE

QUESITO N. 1
Con riferimento al punto D) della prima parte della prova, indicare le caratteristiche principali del protocollo che si è inteso utilizzare.
Si rimanda ai libri di testo per la trattazione della suite di protocolli di sicurezza **IPsec**; altri protocolli utilizzabili per le VPN sono PPTP e L2TP/IPsec.

QUESITO N. 2
Proporre una struttura di collegamento tra i settori contabili dei due edifici, attraverso la rete Internet, che permetta agli operatori addetti alle postazioni contabili di comunicare tra loro, con particolare attenzione alla sicurezza e riservatezza dei dati che vengono scambiati tra le due reti, anche prevedendo l'acquisizione di ulteriori indirizzi IP statici dall' ISP.

In questo caso va richiesto un ulteriore indirizzo IP pubblico, di tipo statico, da utilizzare per realizzare una seconda VPN site-to-site basata su IPsec in cui il traffico "interessante", cioè che transita attraverso il "tunnel" VPN è quello che ha come indirizzi IP quelli delle due reti contabili *opportunamente "nattate"*.
Per esempio:

- il router interno della sottorete contabile dell'edificio 1 effettua un NAT tra gli indirizzi interni (192.168.10.x/28) e l'indirizzo della sua porta tramite cui si accede alla sottorete commerciale (per esempio il 172.16.3.254/22),
- il Router-1 che dà l'accesso a Internet per l'edificio 1 effettua un NAT tra l'indirizzo interno 172.16.3.254 e il nuovo indirizzo IP pubblico statico (per esempio il 200.10.1.1);

Se le VPN vengono realizzate tramite i router (che integrano anche un firewall) si ha così che:

- la VPN1 crea un *tunnel* che collega le due sedi commerciali e quindi ha come *endpoint* i due indirizzi pubblici iniziali (200.1.2.2 lato edificio 1 e 200.1.2.6 lato edificio 2);
- la VPN2 crea un *tunnel* che collega le due sedi contabili e quindi ha come *endpoint* l'indirizzo pubblico del router dell'edificio 2 (200.1.2.6) e l'ulteriore indirizzo IP pubblico acquistato per la rete dell'edificio 1 (per esempio il 200.10.1.1), il quale viene "nattato" verso l'indirizzo IP privato dell'interfaccia del router interno (172.16.3.254).

QUESITO N. 3
Descrivere le caratteristiche più importanti relative alle tecniche di crittografia a chiave simmetrica ed asimmetrica.
Per la trattazione di questo punto si rimanda ai libri di testo

QUESITO N. 4
Nell'ipotesi di istituire un servizio di scambio di messaggi di testo, descrivere, eventualmente anche con un esempio utilizzando un linguaggio a scelta, un socket di comunicazione di tipo client/server adatto allo scopo e definire una possibile architettura hardware.

Soluzione[2] *a cura del prof. Giorgio Meini*

Premesso che per i servizi di *Instant Messaging* (IM) in tempo reale esistono protocolli applicativi specifici in forma di standard aperti (ad esempio XMPP per il quale esistono anche soluzioni software *open-source* sia per il lato server che per il lato client), il quesito pare finalizzato alla produzione di codice che interagisca con un'interfaccia di tipo *socket*, normalmente resa disponibile in forma di API del sistema operativo nella forma di funzioni in linguaggio C.
La prima scelta da effettuarsi per programmare a questo livello è il protocollo di trasporto che si intende utilizzare: UDP o TCP; dato che molti servizi IM reali prevedono anche ad alto livello il concetto di "connessione" tra due utenti è naturale la scelta di TCP.
I servizi di IM reali si dividono in servizi "centralizzati", in cui lo scambio di messaggi di testo tra due utenti avviene tramite un server che può conservare – eventualmente in forma cifrata – i messaggi per una consultazione successiva, e servizi "decentralizzati" in cui i messaggi sono scambiati direttamente tra due utenti: come esempio di codifica si sceglie quest'ultima soluzione.
L'implementazione delle funzionalità di scambio di messaggi di testo utilizzando un *socket* TCP risulta piuttosto semplice, ma un servizio di IM richiede anche una funzionalità di contatto dell'utente che è normalmente identificato mediante un *nickname* che deve essere risolto nell'indirizzo IP e nel numero di porta TCP su cui il proprio server IM – se attivo – è in ascolto: questa funzionalità dovrebbe essere centralizzata – ad esempio mediante un database esposto da un server DBMS – in modo che per ogni utente registrato al servizio sia possibile gestire dinamicamente e in tempo reale lo stato di presenza/assenza, l'indirizzo IP ed il numero di porta TCP di contatto. Nel codice di esempio non è riportata la gestione della funzionalità di risoluzione del *nickname*.
Il codice che segue implementa un server con interfaccia a riga di comando per sistema operativo Windows che deve essere eseguito da ogni utente che vuole essere contattabile per il servizio di IM: si tratta di un server iterativo in quanto non sono permesse più connessioni contemporanee da parte dello stesso utente, ma è necessario utilizzare un *thread* per rendere asincrona la funzionalità di visualizzazione dei messaggi ricevuti da quella di inoltro dei messaggi digitati.

[2] A scopo didattico la soluzione è completa e funzionante.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <process.h>
#include <winsock2.h>

int chat = 0;

/* thread visualizzazione messaggi ricevuti */
unsigned long WINAPI receive_thread(void* arg)
{
 char buffer[16];
 char message[1024];
 int index;
 int i, n;
 unsigned long par = 1;
 SOCKET socket_id = *(SOCKET*)arg;

 ioctlsocket(socket_id, FIONBIO, &par); // socket non bloccante
 index = 0;
 while (chat)
     {
      if ((n = recv(socket_id, buffer, sizeof(buffer), 0)) <= 0)
             {
              if ((n < 0) && (WSAGetLastError() == WSAEWOULDBLOCK))
                {
           Sleep(100); // attesa 100ms
                 continue;
                }
              chat = 0;
              printf("PREMERE IL TASTO <INVIO>\r\n");
        break;
       }
      else
         {
          for (i=0; i<n; i++) // ricerca carattere terminatore
            if (buffer[i] == '\r' || buffer[i] == '\n')
              {
               message[index] = '\0';
               if (strlen(message) > 0)
                 printf("[%s]\r\n", message);
               index = 0;
               break;
              }
            else
                {
                 if (index >= sizeof(message))
                   index = 0;
                 message[index] = buffer[i];
                 index++;
                }
         }
     }
 ExitThread(0);
}
```

```
int main(int argc, char* argv[])
{
 WSADATA wsaData;
 SOCKET req_sock, com_sock;
 struct sockaddr_in local_add, remote_add;
 int add_size;
 char* IP;
 int c;
 char message[1024];
 HANDLE thread;
 int index;
 unsigned short port;

 if (argc != 2)
   {
    printf("Uso: %s numero-di-porta\r\n", argv[0]);
    return -1;
   }
 port = (unsigned short)atoi(argv[1]);
 /* inizializzazione server-socket */
 if (WSAStartup(0x0202, &wsaData) != 0)
   return -1

 if ((req_sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) == INVALID_SOCKET)
   {
    WSACleanup();
    return -1;
   }

 memset(&local_add, 0, sizeof(local_add));
 local_add.sin_family = AF_INET;
 local_add.sin_addr.s_addr = 0; // localhost
 local_add.sin_port = htons(port);

 if (bind(req_sock, (struct sockaddr*)&local_add, sizeof(local_add)) == SOCKET_ERROR)
   {
    closesocket(req_sock);
    WSACleanup();
    return -1;
   }

 if (listen(req_sock, 1) == SOCKET_ERROR)
   {
    closesocket(req_sock);
    WSACleanup();
    return -1;
   }
```

```
 printf("SERVIZIO ATTIVO (PORTA=%u)\r\n", port);
 while (1)
     {
          /* accettazione connessione client */
          add_size = sizeof(remote_add);
          if ((com_sock = accept(req_sock, (struct sockaddr*)&remote_add, &add_size)) ==
         INVALID_SOCKET)
            continue;
          IP = inet_ntoa(remote_add.sin_addr);
          printf("CONVERSAZIONE INIZIATA DA %s (INVIARE UN MESSAGGIO VUOTO PER
TERMINARE)\r\n",IP);
          chat = 1;
      thread = CreateThread(NULL,4096,&receive_thread,&com_sock,0,NULL);
          /* ciclo trasmissione messaggi digitati */
          index = 0;
          while (chat)
              {
               c = getchar();
               if (c == '\r' || c == '\n') // controllo digitazione carattere terminatore
             {
              message[index] = '\0';
              if ((strlen(message) > 0) && chat)
                        {
                 send(com_sock, message, strlen(message), 0);
                          send(com_sock, "\r\n", 2, 0); // trasmissione caratteri terminatori
                 index = 0;
                 }
              else
                     {
                          chat = 0;
                  WaitForSingleObject(thread, INFINITE); // attesa terminazione thread
                          closesocket(com_sock);
                          break;
                         }
                       }
                else
                        {
               if (index >= sizeof(message))
                 index = 0;
               message[index] = (char)c;
               index++;
              }
               }
     printf("CHIUSURA CONVERSAZIONE\r\n");
    }

 closesocket(req_sock);
 WSACleanup();
 return 0;
}
```

Il codice che segue implementa un client con interfaccia a riga di comando per sistema operativo Windows che deve essere eseguito da ogni utente che vuole contattare un altro utente del servizio di IM: è necessario utilizzare un *thread* per rendere asincrona la funzionalità di visualizzazione dei messaggi ricevuti da quella di inoltro dei messaggi digitati.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <process.h>
#include <winsock2.h>

int chat = 0;

/* funzione di conversione di un indirizzo IP dal formato dotted al formato binario */
unsigned long IP_to_bin(char IP[])
{
 unsigned long add;
 unsigned char byte;
 char *token;

 if ((token = strtok(IP,".")) == NULL)
   return 0x00000000;
 byte = (unsigned char)atoi(token);
 add = (unsigned long)byte * 16777216;
 if ((token = strtok(NULL,".")) == NULL)
   return 0x00000000;
 byte = (unsigned char)atoi(token);
 add += (unsigned long)byte * 65536;
 if ((token = strtok(NULL,".")) == NULL)
   return 0x00000000;
 byte = (unsigned char)atoi(token);
 add += (unsigned long)byte * 256;
 if ((token = strtok(NULL,".")) == NULL)
   return 0x00000000;
 byte = (unsigned char)atoi(token);
 add += (unsigned long)byte * 1;
 return add;
}

/* thread visualizzazione messaggi ricevuti */
unsigned long WINAPI receive_thread(void* arg)
{
 char buffer[16];
 char message[1024];
 int index;
 int i, n;
 unsigned long par = 1;
 SOCKET socket_id = *(SOCKET*)arg;

 ioctlsocket(socket_id, FIONBIO, &par); // socket non bloccante
 index = 0;
```

```
while (chat)
    {
     if ((n = recv(socket_id, buffer, sizeof(buffer), 0)) <= 0)
           {
            if ((n < 0) && (WSAGetLastError() == WSAEWOULDBLOCK))
              {
          Sleep(100); // attesa 100ms
               continue;
              }
            chat = 0;
            printf("PREMERE IL TASTO <INVIO>\r\n");
       break;
      }
     else
        {
         for (i=0; i<n; i++) // ricerca carattere terminatore
           if (buffer[i] == '\r' || buffer[i] == '\n')
             {
              message[index] = '\0';
              if (strlen(message) > 0)
                printf("[%s]\r\n", message);
              index = 0;
              break;
             }
           else
              {
               if (index >= sizeof(message))
                 index = 0;
               message[index] = buffer[i];
               index++;
              }
        }
    }
 ExitThread(0);
}

int main(int argc, char* argv[])
{
 WSADATA wsaData;
 SOCKET sock;
 struct sockaddr_in remote_add;
 int c;
 char message[1024];
 HANDLE thread;
 int index;
 unsigned short port;
 unsigned long address;

 if (argc != 3)
   {
    printf("Uso: %s indirizzo-IP numero-di-porta\r\n", argv[0]);
    return -1;
   }
 address = IP_to_bin(argv[1]);
 port = (unsigned short)atoi(argv[2]);
```

```
/* inizializzazione server-socket */
if (WSAStartup(0x0202, &wsaData) != 0)
  return -1;
if ((sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) == INVALID_SOCKET)
  {
   WSACleanup();
   return -1;
  }
memset(&remote_add, 0, sizeof(remote_add));
remote_add.sin_family = AF_INET;
remote_add.sin_addr.s_addr = htonl(address);
remote_add.sin_port = htons(port);
if (connect(sock, (struct sockaddr*)&remote_add, sizeof(remote_add)) == SOCKET_ERROR)
  {
   printf("IMPOSSIBILE INIZIARE CONVERSAZIONE\r\n");
   closesocket(sock);
   WSACleanup();
   return -1;
  }

printf("CONVERSAZIONE INIZIATA (INIVIARE UN MESSAGGIO VUOTO PER TERMINARE)\r\n");
chat = 1;
thread = CreateThread(NULL, 4096, &receive_thread, &sock, 0, NULL);
/* ciclo trasmissione messaggi digitati */
index = 0;
while (chat)
    {
         c = getchar();
         if (c == '\r' || c == '\n') // controllo digitazione carattere terminatore
       {
        message[index] = '\0';
        if ((strlen(message) > 0) && chat)
              {
           send(sock, message, strlen(message), 0);
                send(sock, "\r\n", 2, 0); // trasmissione caratteri terminatori
           index = 0;
          }
        else
              {
               chat = 0;
            WaitForSingleObject(thread, INFINITE); // attesa terminazione thread
               closesocket(sock);
               break;
              }
          }
         else
             {
          if (index >= sizeof(message))
            index = 0;
          message[index] = (char)c;
          index++;
         }
     }
```

```
 printf("CHIUSURA CONVERSAZIONE\r\n");
 closesocket(sock);
 WSACleanup();
 return 0;
}
```

Bibliografia

Oltre ai testi scolastici di Sistemi e reti (anche per l'articolazione Informatica), si consiglia l'utilizzo:

- del **Manuale Cremonese di Informatica e Telecomunicazioni** (2a edizione)

- del libro di testo:
  Onelio Bertazioli
  Corso di Telecomunicazioni volume 3
  ed. Zanichelli

- del libro di testo (in particolare per la risposta al quesito 4)
  Giorgio Meini Fiorenzo Formichi
  Tecnologie e progettazione di sistemi informatici e di telecomunicazioni volume 3
  ed. Zanichelli