SOLUZIONI SECONDA PROVA SCRITTA ESAME DI STATO 2024

Indirizzo: INFORMATICA E TELECOMUNICAZIONI

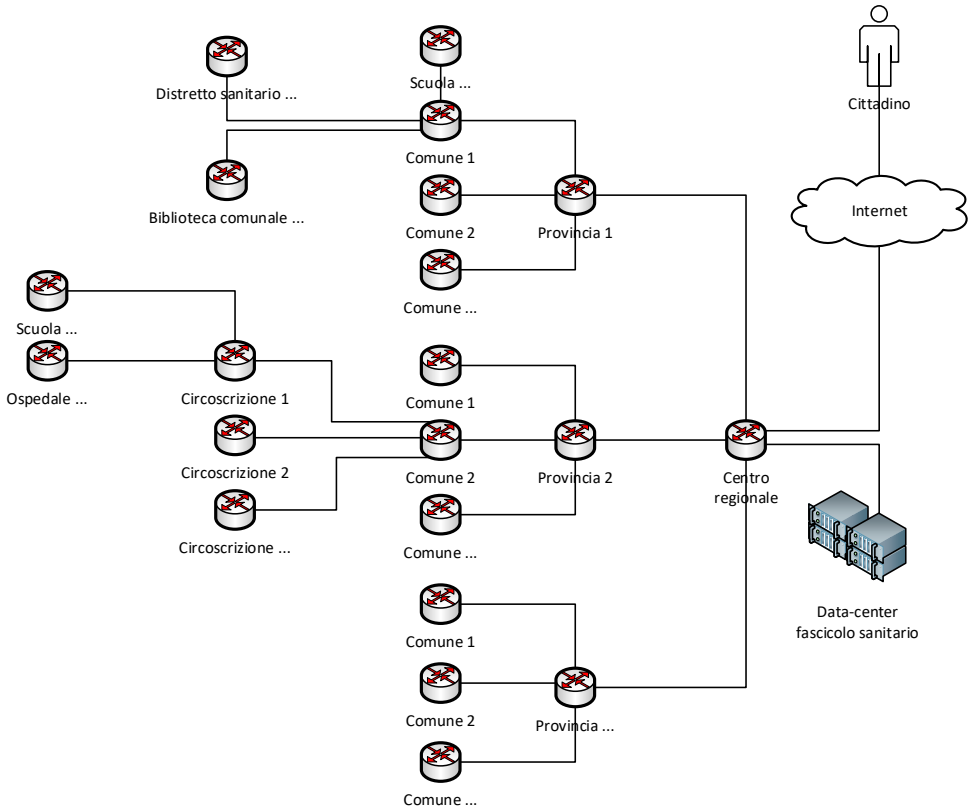
Articolazione: INFORMATICA

Disciplina: SISTEMI E RETI

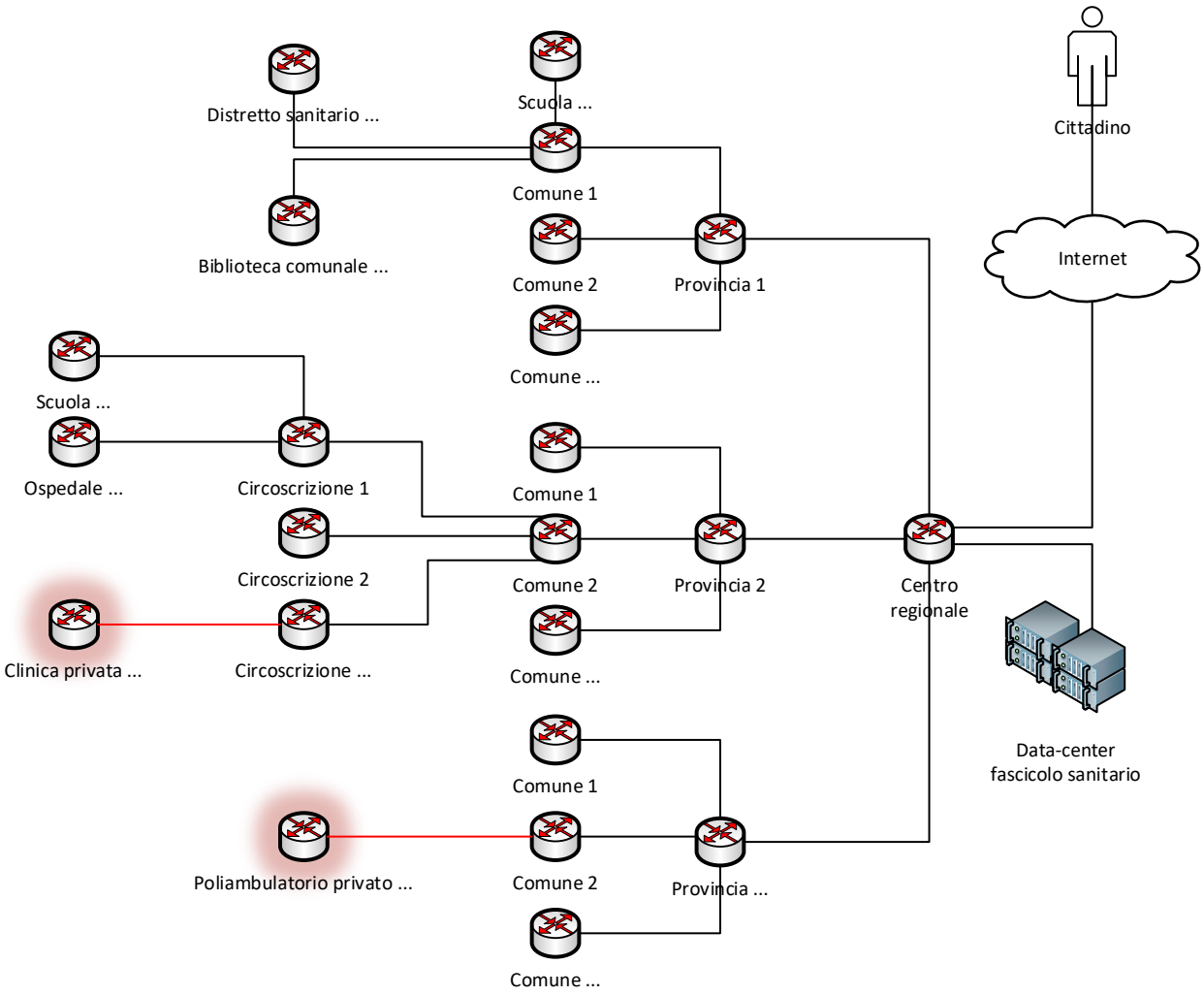
SOLUZIONE PRIMA PARTE

0. La soluzione proposta verte esclusivamente su conoscenze e competenze normalmente disponibili allo studente che conclude il percorso di studi dell'Indirizzo «Informatica e telecomunicazioni» articolazione «Informatica», con particolare riferimento alle linee guida ministeriali per la disciplina «Sistemi e reti» e ai temi trattati nel corso in tre volumi «Sistemi e reti» di G. Meini, F. Formichi, M. Sartor e A. Parodi, Zanichelli Editore S.p.A.

1. Per la preesistente rete WAN regionale in fibra ottica si ipotizza una struttura gerarchica articolata sui vari livelli degli enti locali territoriali (regione, provincia e comune) con interconnessione al livello comunale degli enti locali, delle scuole e delle strutture sanitarie pubbliche presenti nel territorio comunale: per i comuni più grandi è ipotizzabile un ulteriore livello gerarchico territoriale, per esempio a livello della circoscrizione. La figura è una rappresentazione parziale dell'infrastruttura della rete regionale con esemplificazione di alcune organizzazioni connesse:



Il limite di una rete WAN con una topologia fisica gerarchica è ovviamente la mancanza di collegamenti ridondanti finalizzati, oltre che a distribuire il carico di traffico della rete su più percorsi, a rendere maggiormente robusta l'infrastruttura rispetto all'ipotesi di sovraccarichi temporanei di traffico o a guasti di singoli collegamenti o dispositivi di rete.
La connessione delle singole strutture sanitarie private avverrà a livello del nodo della rete WAN regionale presente nel territorio in cui sono localizzate, anche al fine di ottimizzare la spesa dei fondi della componente M6C2 del PNRR per la realizzazione dei nuovi collegamenti in fibra ottica; la figura illustra la connessione di alcune strutture sanitarie private alla rete precedentemente ipotizzata:



Lo schema di indirizzamento della rete WAN regionale è basato sulla classe di indirizzi IPv4 10.0.0.0/8: a partire dal fatto che per la connessione delle strutture sanitarie private verrà dichiaratamente impiegata la sottorete 10.100.0.0/16 è ipotizzabile che il secondo byte dell'indirizzo sia sempre impiegato per identificare il settore (scuole primarie, scuole secondarie, uffici scolastici, uffici e enti comunali, uffici e enti

provinciali, uffici e enti regionali, ospedali e distretti sanitari, poliambulatori, ecc.)[1]; dovendo garantire la non sovrapposizione degli indirizzi delle varie reti IP interconnesse dalla rete WAN regionale è necessario che parte dei 16 bit rimanenti sia impiegata per identificare univocamente le specifiche reti LAN delle singole organizzazioni (enti locali, scuole, strutture sanitarie pubbliche e private).
Per esemplificare: la sottorete 10.100.0.0/16 dedicata alle strutture sanitarie private deve garantire la connessione di almeno 2000 strutture garantendo un'adeguata scalabilità per il futuro: è possibile riservare 12 bit per identificare la struttura (garantendo quindi fino a 4096 identificativi distinti) e i rimanenti 4 bit per indirizzare gli host della struttura con una sottorete avente come *netmask* 255.255.255.240 garantendo 14 indirizzi IP utili al netto degli indirizzi di rete e di *broadcast*; dovendo assegnare uno degli indirizzi della sottorete all'interfaccia di *default-gateway* del router restano disponibili 13 indirizzi, un numero superiore agli 8 richiesti come requisito minimo. Per esempio, la struttura con identificativo 1234 (in formato binario: 01001101-0010), avrà a disposizione i seguenti indirizzi:

10.100.77.32/28 (indirizzo di rete)
10.100.77.46 (indirizzo *default-gateway*)
da 10.100.77.33/28 a 10.100.77.45/28 (indirizzi utili)
10.100.77.47/28 (indirizzo di *broadcast*)

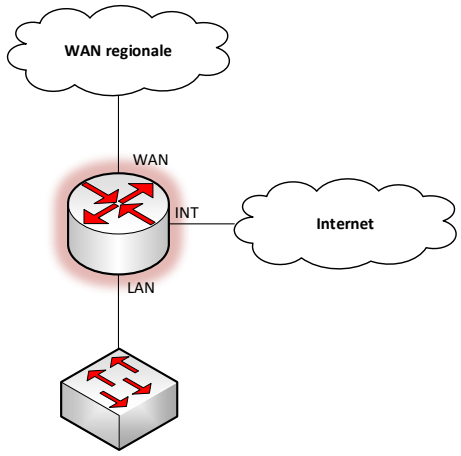
Per il *data-center* che ospita i server che gestiscono i dati del fascicolo sanitario sarà usata una specifica sottorete, per esempio 10.99.0.0/16: nella stessa sottorete sarà collocato il server che esegue l'applicazione *manager* SNMPv3 per il controllo e il monitoraggio dei router delle strutture sanitarie private.
La necessaria scalabilità della rete nella fase di interconnessione delle strutture sanitarie private richiede l'adozione di un protocollo di routing dinamico che per la dimensione della stessa può essere individuato in OSPFv2.

2. Il dispositivo da fornire a ciascuna delle strutture sanitarie private è un router che avrà un'interfaccia per la connessione alla specifica tecnologia di fibra ottica impiegata per la connessione alla rete WAN regionale e una porta Ethernet cablata in rame con banda 1Gbps (standard 1000Base-T, IEEE.802.3ab) o 10Gbps (standard 10GBase-T, IEEE-802.3an) per l'interconnessione con lo switch di livello *core* della rete LAN dell'organizzazione[2]; il dispositivo potrebbe avere un'ulteriore interfaccia Ethernet per la connessione alla rete Internet tramite un ISP mediante un modem per la specifica tecnologia FTTx impiegata (rame o fibra ottica).
   La configurazione della porta di connessione alla rete WAN regionale dovrà prevedere l'impostazione di un indirizzo IP e della relativa *netmask* coerentemente con il collegamento *point-to-point* verso il router del livello gerarchico territoriale, mentre la configurazione della porta Ethernet utilizzerà uno degli indirizzi IPv4 assegnati

[1] Una specifica sottorete – per esempio 10.0.0.0/16 – sarà riservata per l'indirizzamento dei collegamenti *point-to-point* tra i router della rete WAN.

[2] In aggiunta o alternativa il router potrebbe integrare un *access-point* per la realizzazione di una rete Wi-Fi.

all'organizzazione, l'eventuale interfaccia verso la rete Internet prevederà l'acquisizione automatica dell'indirizzo IP e sarà di conseguenza configurata come client DHCP; inoltre sul router dovrà essere abilitato il protocollo di routing dinamico utilizzato per la rete WAN regionale:



Nel caso di un dispositivo Cisco con sistema operativo IOS il seguente *script* esemplifica la configurazione di base utilizzando il linguaggio CLI:

```
enable
configure terminal
interface WAN
ip address 10.0.123.2 255.255.255.252
no shutdown
exit
interface LAN
ip address 10.100.77.46 255.255.255.240
no shutdown
exit
interface INT
ip address dhcp
no shutdown
exit
router ospf 123
network 10.0.123.0 0.0.0.3 area 0
network 10.100.77.32 0.0.0.15 area 0
passive interface LAN
passive interface INT
exit
ip route 0.0.0.0 0.0.0.0 INT
exit
```

Per una corretta funzionalità del router devono essere configurati anche i seguenti servizi:

- *agent* SNMPv3 (*Simple Network Management Protocol*) in modo da garantirne il controllo/monitoraggio remoto dall'interfaccia WAN[3];
- NAT/PAT (interfaccia INT esterna e interfaccia LAN interna) per consentire la navigazione della rete Internet ai dispositivi della rete LAN;
- DHCP per l'assegnazione dinamica degli indirizzi IPv4 del blocco assegnato alla struttura sanitaria privata agli *host* per richieste ricevute dall'interfaccia LAN.

Allo scopo di rendere sicure le reti LAN delle strutture sanitarie private, è possibile configurare sui router un *firewall* implementato mediante ACL tenendo conto che la connessione alla rete WAN regionale ha il solo scopo di comunicare con i server del *data-center* che ospita il fascicolo sanitario e con il server che esegue l'applicazione *manager* SNMPv3 per il controllo/monitoraggio remoto del router e che la connessione con la rete Internet ne garantisce la sola navigazione utilizzando il servizio DNS di Google:

Interfaccia WAN (ingresso)

Protocollo	Indirizzo origine	Porta origine	Indirizzo destinazione	Porta destinazione	Esito
TCP	10.99.0.0/16	qualsiasi[4]	10.100.77.32/28	qualsiasi	accettato se non richiesta di connessione
UDP	10.99.0.0/16	10161/10162	10.0.123.2	10161/10162	accettato (SNMPv3)
qualsiasi	qualsiasi	qualsiasi	qualsiasi	qualsiasi	scartato

Interfaccia INT (ingresso)

Protocollo	Indirizzo origine	Porta origine	Indirizzo destinazione	Porta destinazione	Esito
TCP	qualsiasi	qualsiasi	10.100.77.32/28	qualsiasi	accettato se non richiesta di connessione
UDP	8.8.8.8 (servizio DNS Google)	53	10.100.77.32/28	53	accettato (DNS)
qualsiasi	qualsiasi	qualsiasi	qualsiasi	qualsiasi	scartato

Bloccando la riconfigurazione locale del router le ACL individuate ne impediscono l'uso per accedere a reti diverse da quella del *data-center*.

[3] Molti produttori di dispositivi di rete rendono disponibili protocolli proprietari per il controllo/monitoraggio remoto; il protocollo SNMPv3 rappresenta una soluzione standard per questa esigenza.

[4] Se il fascicolo sanitario è accessibile esclusivamente mediante l'API di un *web-service* REST è possibile limitare la porta a 443 (HTTPS).

3. Una volta sostituito il router preesistente con quello fornito dalla società di gestione della WAN regionale[5] l'unica modifica da apportare alla configurazione degli host della struttura sanitaria privata consiste nella riconfigurazione dei parametri di connettività alla rete LAN/WAN (indirizzo IPv4, *netmask*, indirizzo *default-gateway*, indirizzo server DNS): nel caso in cui sull'interfaccia LAN del router sia stato configurato il servizio DHCP è sufficiente impostare tutti gli *host* per l'acquisizione dinamica dei parametri di connettività. Ovviamente la novità rappresentata dall'accesso ai server del *data-center* che ospitano il fascicolo sanitario richiederà l'installazione di applicazioni specifiche per usufruire di tale servizio.

4. Il GDPR (*General Data Protection Regulation*) dell'Unione europea classifica i dati personali di tipo sanitario come dati sensibili ai quali deve essere applicata una particolare protezione in termini sia di riservatezza che di integrità e disponibilità (obiettivi RID: Riservatezza, Integrità, Disponibilità). Pur potendo prevedere la cifratura simmetrica dei dati memorizzati nei server che ospitano il fascicolo sanitario, questa soluzione comporterebbe una complessa gestione delle chiavi di decifrazione e della loro conservazione non essendo solo il cittadino, proprietario dei dati, l'unico legittimato ad accedervi. Assumendo elevato il livello di sicurezza offerto dal *data-center* (anche sotto l'aspetto del *back-up* dei dati e quindi della loro disponibilità) è possibile limitarsi a garantirne la riservatezza/integrità nel corso del trasferimento da e verso il *data-center*: a questo scopo l'adozione del protocollo TLS rappresenta una soluzione standard senz'altro adeguata. La vera complessità nella gestione di un servizio come il fascicolo sanitario è rappresentata dall'autenticazione/autorizzazione degli operatori che vi accedono: se per l'autenticazione le tecniche sono consolidate (servizi e protocolli di autenticazione, *smart-card* protette da password/PIN, dati biometrici, ecc.), l'autorizzazione ad accedere a dati sensibili, in particolare da parte di operatori privati, deve necessariamente implementare il principio del privilegio minimo per cui deve essere gestita la concessione/revoca dell'autorizzazione di accesso a specifici dati da parte del cittadino a specifiche strutture sanitarie.
   Infine la mole dei dati prodotti, spesso di tipo multimediale, può non consentirne il trasferimento in tempo reale verso i server che ospitano il fascicolo sanitario, soluzione senz'altro preferibile per l'immediata disponibilità da parte di diverse strutture sanitarie pubbliche o private: in questo caso è possibile prevederne la temporanea memorizzazione su un server locale a favore di un successivo trasferimento, per esempio nel corso della notte quando la rete è meno congestionata; per quanto temporanea la memorizzazione di dati sensibili deve garantire il rispetto degli obiettivi RID prevedendo tecnologie e misure adeguate per il server (sistema UPS, unità di memoria persistenti di tipo RAID, cifratura delle unità di memoria persistente, configurazione di un *firewall* software, rigoroso controllo degli accessi a livello sia fisico che logico, ecc.).

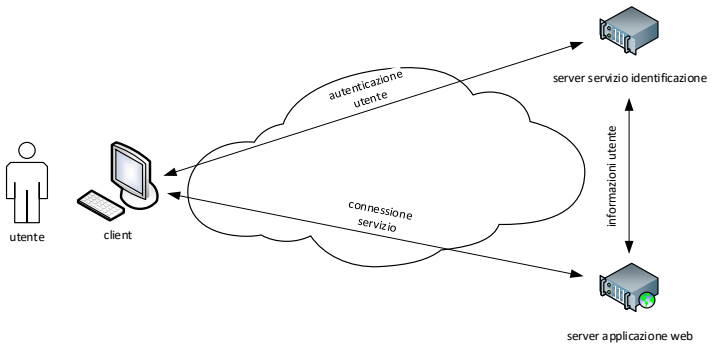
[5] Deve essere valutata la possibilità di riconfigurare il router/modem preesistente come solo modem per la connessione alla rete Internet tramite ISP, per esempio abilitando il protocollo PPPoE (PPP *over* Ethernet).

SOLUZIONE SECONDA PARTE

I. È probabile che sia previsto un accesso alternativo ai server che ospitano il fascicolo sanitario, per esempio prevedendo una VPN che usa la rete pubblica Internet e implementata impiegando il protocollo IPsec per realizzare un tunnel tra il router della struttura sanitaria locale e il router del centro regionale che rappresenta l'interfaccia tra la rete WAN regionale e il *data-center*; tuttavia, è ragionevole ipotizzare la presenza di un server locale per la memorizzazione temporanea dei dati sanitari prevedendo le tecnologie e le misure descritte nella trattazione del punto 4 della prima parte. Dovendo eliminare i dati dal server locale solo quando è certo il completamento del loro trasferimento sui server del *data-center* che ospita il fascicolo sanitario, è necessario il ricorso a protocolli applicativi che comunichino l'esito dell'operazione, come avviene per esempio con l'impiego di *web-service* REST basati sul protocollo HTTP.

II. Anche dal punto di vista normativo l'accesso tramite rete Internet a dati personali gestiti dalla pubblica amministrazione deve richiedere l'identificazione formale del richiedente allo scopo di autorizzarne l'accesso. In Italia a oggi i due sistemi maggiormente utilizzati per l'identificazione formale dei cittadini sono lo SPID (Sistema Pubblico di Identità Digitale) e la CIE (Carta d'Identità Elettronica); entrambi separano il servizio di identificazione (che nel caso dello SPID può essere erogato da diversi operatori accreditati) dall'accesso ai dati o ai servizi richiesti secondo la seguente successione di operazioni:

1. l'utente richiede l'accesso a un'applicazione web utilizzando un browser come client;
2. l'applicazione genera una richiesta per il servizio di identificazione, la cifra in modo che solo il servizio di identificazione la possa decifrare e la trasferisce al browser dell'utente;
3. il browser trasmette la richiesta ricevuta al server del servizio di identificazione;
4. il servizio di identificazione autentica l'utente (per esempio richiedendo username e password, oppure richiedendo un OTP, *One-Time Password*, generato utilizzando un canale precedentemente associato all'identità dell'utente come un'APP installata su uno smartphone dotato di SIM);
5. il servizio di identificazione trasmette al browser l'esito del processo di autenticazione, cifrato in modo che solo l'applicazione web lo possa decifrare, ed eventualmente un *token* di accesso al servizio stesso di durata temporale limitata;
6. il browser trasmette all'applicazione web la risposta ricevuta dal servizio di autenticazione;
7. l'applicazione web decifra la risposta del servizio di identificazione e decide se fare o meno accedere l'utente ai propri servizi/dati;
8. l'applicazione web utilizza il *token* ricevuto per richiedere informazioni relative all'utente al server del servizio di identificazione.



Il ricorso a un'autenticazione qualificata a più fattori avviene eventualmente nella fase 4 del procedimento ed è finalizzata a elevare la sicurezza dell'autenticazione utilizzando un canale distinto da quello di richiesta delle credenziali di accesso e precedentemente associato all'utente: un tipico esempio consiste in una OTP generata casualmente e inviata come SMS a un numero telefonico.

III. Disponendo di un solo indirizzo IP pubblico, la tecnica da impiegare è quella del *port-forwarding*, in questo caso associando all'indirizzo IPv4 privato del server i numeri di porta 80 (protocollo HTTP), 443 (protocollo HTTPS) e 22 (protocollo SSH).
Nel caso di un dispositivo Cisco con sistema operativo IOS in cui l'interfaccia INT sia quella verso la rete pubblica Internet e l'interfaccia LAN sia quella verso la rete locale dell'azienda in cui è presente il server che si suppone avere indirizzo IP 192.168.0.1, il seguente *script* esemplifica la configurazione necessaria utilizzando il linguaggio CLI (`x.y.w.z` è l'indirizzo IP pubblico statico):

```
ip nat inside source static protoc x.y.w.z 80 192.168.0.1 80
ip nat inside source static protoc x.y.w.z 443 192.168.0.1 443
ip nat inside source static protoc x.y.w.z 22 192.168.0.1 22
interface LAN
ip nat inside
interface INT
ip nat outside
```

IV. Il problema più comune consiste nella misconfigurazione dei parametri di connessione alla rete LAN dell'*host*: nel caso di un dispositivo con S.O. Windows è possibile richiedere all'utente di digitare il comando testuale `ipconfig` per visualizzare indirizzo IP, *netmask* e indirizzo *default-gateway*; se non risultano configurati è stata sovrascritta la configurazione statica, o non è andata a buon fine la configurazione dinamica, eventualmente per un malfunzionamento del server DHCP della rete. Nel caso che il comando testuale `ipconfig` fornisca un risultato coerente con la configurazione della rete in cui è inserito l'*host* il problema potrebbe essere la raggiungibilità del router che rappresenta il *gateway* verso la rete Internet, verificabile richiedendo all'utente la digitazione del comando testuale ping avente come parametro l'indirizzo *default-gateway* fornito come risposta dal comando testuale `ipconfig`: la mancata risposta al comando identifica un problema (fisico o di configurazione) nella rete LAN *wireless* o cablata a cui appartiene l'*host*. Nel caso che il comando `ping` abbia successo, il problema potrebbe essere la mancata o errata configurazione

dell'indirizzo IP del server DNS verificabile richiedendo all'utente la digitazione del comando testuale `ipconfig/all`.