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

Una scuola negli anni novanta realizzò una propria banca dati telematica per la distribuzione elettronica di un giornalino scolastico settimanale. Gli utenti, previa registrazione, si collegavano via modem e linea telefonica per la lettura degli articoli e l'invio di posta elettronica.

Da uno studio preliminare risultava che:

1. ad ogni articolo erano associati un titolo, un'immagine ed eventualmente un filmato;
2. un numero settimanale si componeva di circa venti articoli.

Il nuovo dirigente scolastico desidera effettuare l'ammodernamento delle apparecchiature informatiche a disposizione del personale scolastico, realizzando una nuova porzione di rete locale per il collegamento dei computer e di altri dispositivi, la cui collocazione è la seguente:

- un computer e una stampante nell'ufficio del dirigente;
- venti computer e una stampante di rete professionale negli uffici della segreteria e dell'ufficio tecnico;
- dieci computer e una stampante di rete professionale nell'aula docenti;
- altre apparecchiature mobili (smartphone, pc portatili, …), che vengono usate all'occorrenza dal personale o da visitatori occasionali.

Inoltre, in un locale protetto, vi è un sistema su cui risiedono la banca dati e il server Web.

La scuola ha un sito web contenente informazioni e una sintesi degli articoli/circolari pubblicati accessibili a tutti senza autenticazione; contiene inoltre una sezione riservata agli utenti autorizzati, che sono ora circa 2.000.

Il candidato, formulate le opportune ipotesi aggiuntive, sviluppi i seguenti punti:

1. proponga un progetto anche grafico dell'infrastruttura di rete, indicando le risorse hardware e software necessarie, esaminandone in particolare l'architettura, gli apparati e le caratteristiche del collegamento della rete ad Internet;
2. definisca un piano di indirizzamento IPv4 per l'infrastruttura di rete proposta al punto 1
3. descriva possibili tecniche di protezione della rete locale e dei server interni dagli accessi esterni;
4. proponga i principali servizi (tra cui ad es. identificazione degli utenti, assegnazione della configurazione di rete, risoluzione dei nomi, …), e ne approfondisca la configurazione di due a sua scelta;
5. discuta vantaggi e svantaggi dell'offrire il servizio mediante l'attuale soluzione gestita internamente, oppure utilizzando un servizio esterno (Cloud), esponendo le motivazioni che inducono alla scelta.

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. In relazione al punto 4 del tema proposto nella prima parte, il candidato illustri le metodologie che consentono la collocazione sicura in rete server accessibili da Internet e la mascheratura dei loro indirizzi IPv4 privati.
2. I documenti, anche importanti, viaggiano sempre più spesso in rete ponendo in evidenza la necessità di garantire sia l'integrità degli stessi che l'identità del mittente. Descrivere la tecnica che garantisce quanto sopra, anche avvalendosi di schemi.
3. Descrivere le caratteristiche più importanti relative alle tecniche di crittografia a chiave simmetrica ed asimmetrica.
4. Descriva in che modo è possibile collegare in modo sicuro, tramite Internet, la sede della scuola alla sede dell'Ufficio Scolastico Regionale, posto in un'altra città, illustrando le fasi necessarie per creare una connessione sicura tra le due sedi.

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 prima parte

Punto 1
Proponga un progetto anche grafico dell'infrastruttura di rete, indicando le risorse hardware e software necessarie, esaminandone in particolare l'architettura, gli apparati e le caratteristiche del collegamento della rete ad Internet.

Una prima soluzione che recepisce le richieste contenendo i costi può essere la seguente:
- si realizzano due subnet IP mappate su 2 VLAN, una subnet e una VLAN per segreteria, ufficio tecnico e dirigente, una subnet e una VLAN per l'aula docenti;
- la VLAN della segreteria viene realizzata su **due switch Layer 2 amministrabili** a 24 porte, in modo da avere qualche porta disponibile per eventuali ampliamenti e nel contempo avere una ridondanza almeno parziale degli apparati;
- la VLAN dell'aula docenti viene realizzata su **uno swich amministrabile a 24 porte**.

L'accesso wireless per la segreteria viene fornito con **1 o 2 Access Point a standard 802.11ac**, a seconda delle dimensioni fisiche dell'area da servire.
L'accesso wireless per l'aula docenti viene fornito con **1 Access Point a standard 802.11ac**.

Gli aspetti fisici e di protocollo dell'infrastruttura di rete possono essere i seguenti:
- cablaggio dell'edificio conforme alle norme del cablaggio strutturato, certificato almeno in **categoria 6**, meglio se in categoria 6A (se si tratta di nuova installazione, in modo da essere predisposto per future evoluzioni della rete).
- tecnologia **Gigabit Ethernet** per gli strati OSI 1 e 2; apparati di rete e computer dotati di porte Gigabit Ethernet (1000BASE-T);
- per la comunicazione in rete si adotta la **suite TCP/IP**, con indirizzi IPv4 privati.

Può essere presente un server interno per gestire in modo centralizzato servizi quali: autenticazione degli utenti e gestione delle risorse ad essi assegnate; DHCP e DNS.
L'amministratore di rete può poi prevedere servizi per il controllo e la gestione di rete quali SYSLOG ed SNMP.
Il server WEB può essere realizzato in ambiente LINUX con il pacchetto Apache, affiancato da un server FTP come per esempio VSFTP, da PHP e un database come MySQL o MariadB.

Nel caso più semplice si utilizza un solo accesso a Internet, di tipo business con banda minima garantita, in tecnologia FTTC o FTTH (se disponibile).
Per controllare, proteggere e gestire l'accesso a Internet si utilizza un firewall hardware sul quale si configurano:
- una porta come DMZ, alla quale si collega il server WEB e che viene configurata su una propria subnet;
- due porte come appartenenti alla stessa LAN1 (LAN segreteria), alle quali si collegano i due switch della segreteria, appartenenti alla stessa subnet IP; le due porte LAN1 fanno capo a uno stesso indirizzo IPv4 che funge da default gateway per la subnet della segreteria;
- una porta appartenenti alla LAN2 (LAN docenti), alle quali si collega lo switch dell'aula docenti; la porta LAN2 è configurata con un indirizzo IPv4 che funge da default gateway per la subnet dell'aula docenti;
- una porta WAN alla quale si collega il router xDSL tramite cui si ha l'accesso a Internet (nel caso di FTTC o ADSL)

Il Firewall può anche fornire il servizio DHCP per una o più subnet IP.
Il router che fornisce l'accesso a Internet implementa anche la funzione NAT, nelle due versioni NAT Statico per il server WEB e PAT (o NAT overload) per l'accesso a Internet dei PC.
E' anche possibile fare in modo che il firewall mascheri la struttura di indirizzamento interna e della DMZ implementando a sua volta la funzione NAT statica e PAT con indirizzi interni ed esterni di tipo privato.

Soluzioni più complesse possono prevedere:

- configurazione di più VLAN, aggiungendo per esempio una VLAN per l'amministrazione della rete (Management VLAN), una VLAN per gli accessi Wireless, ai quali può essere fornito l'accesso a Internet ma non quello alla rete locale, una VLAN per gli eventuali telefoni IP (VoIP), VLAN voice.
- duplice accesso a Internet con due ISP diversi, eventualmente con bilanciamento di carico (*Load Balancing*), in modo da avere una ridondanza che garantisca sempre la disponibilità dell'accesso a Internet stesso e una maggiore velocità d'accesso;
- utilizzo uno o più switch Layer 3 interno (in configurazione ridondata se si desidera avere un'alta affidabilità della rete) con funzione di distribuzione e controllo del traffico in rete tra le subnet e verso Internet.

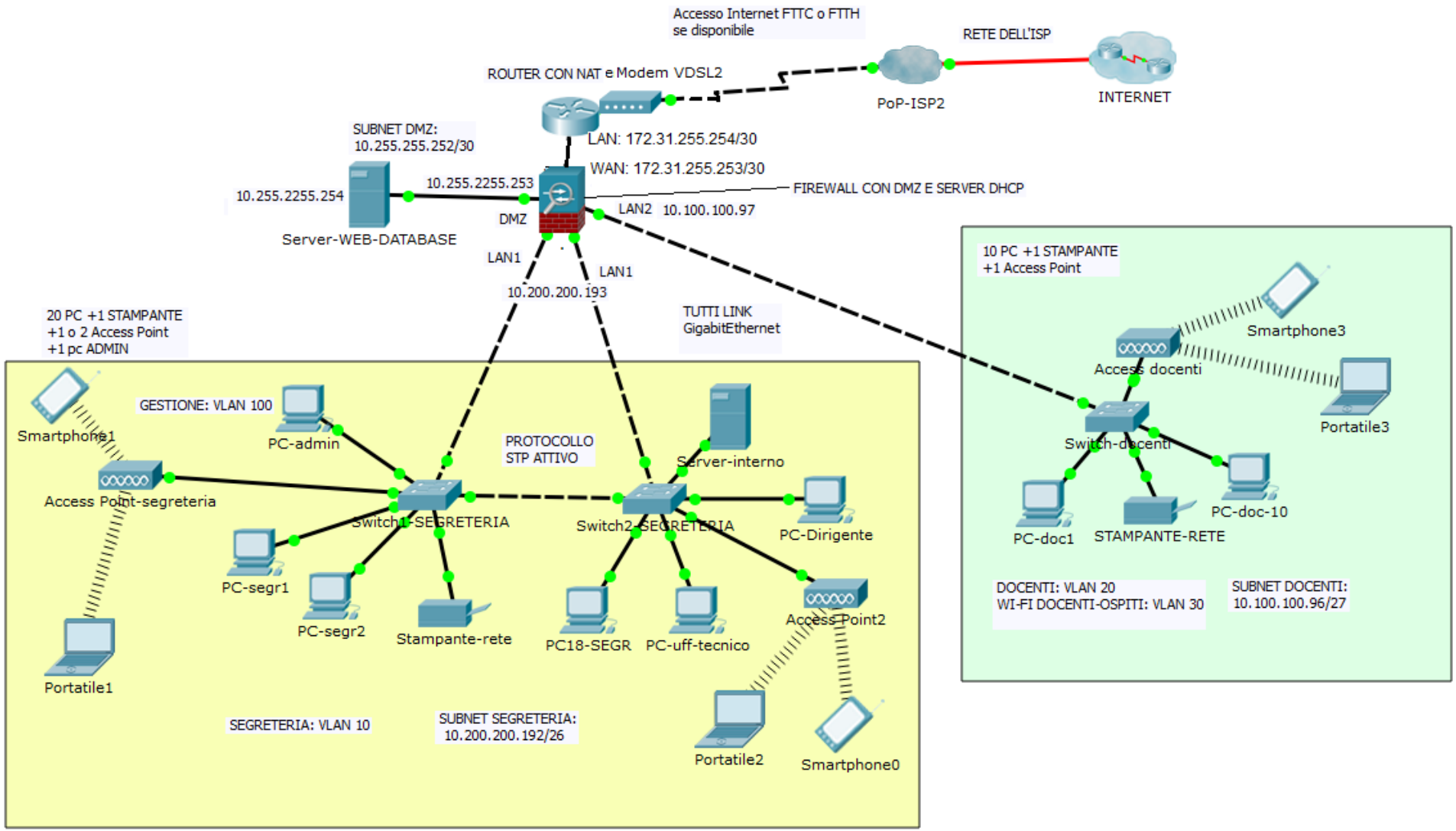

FIGURA 1 Architettura di rete fisica

Punto 2
Definisca un piano di indirizzamento IPv4 per l'infrastruttura di rete proposta al punto 1.

Per il piano di indirizzamento IPv4 preleviamo blocchi di indirizzi IPv4 privati dal 10.0.0.0/8 e dal blocco 172.16.0.0/12. Definiamo un piano di indirizzamento che impiega indirizzi IPv4 privati di uso non comune e che fornisca un numero di indirizzi IPv4 sufficiente ma non eccessivo, impiegando le seguenti subnet mask:

- /26 per la segreteria; con essa si ha una parte host degli indirizzi IPv4 di 6 bit che mette a disposizione 62 indirizzi IP, numero sufficiente per i PC e i dispositivi mobili.
- /27 per l'aula docenti; con essa si ha una parte host degli indirizzi IPv4 di 5 bit che mette a disposizione 30 indirizzi IP, numero sufficiente per i PC e i dispositivi mobili; è anche possibile aumentare il numero di indirizzi IP appartenenti alla subnet impiegando la subnet mask /26.
- /30 per la DMZ, ipotizzando di utilizzare una sola macchina fisica; /29 ipotizzando di impiegare due macchine fisiche
- /30 per la subnet che collega la porta WAN del firewall alla porta LAN (Gigabit Ethernet) del router xDSL.

Più nel dettaglio il piano di indirizzamento può essere il seguente.

- **Subnet segreteria**

Ipotizzando che per la segreteria siano sufficienti 40 indirizzi IPv4 per i PC utilizziamo il seguente blocco: 10.200.200.192/26
L'assegnazione degli indirizzi IP è statica e manuale per gli apparati di rete, è statica via DHCP (vincolando l'indirizzo IP all'indirizzo MAC) per i PC desktop, è dinamica via DHCP per i dispositivi che si collegano in modo wireless via Wi-Fi.

Il piano di indirizzamento può quindi essere il seguente.

Subnet Segreteria		
Indirizzo IPv4	**Subnet Mask /26**	**Note**
10.200.200.192	255.255.255.192	Indirizzo della subnet IP
10.200.200.193	255.255.255.192	Default Gateway: ind. IP interfacce LAN1 del Firewall
10.200.200.194	255.255.255.192	Indirizzo IP switch 1
10.200.200.195	255.255.255.192	Indirizzo IP switch 2
10.200.200.196	255.255.255.192	Indirizzo IP Access Point 1
10.200.200.197	255.255.255.192	Indirizzo IP Access Point 2
10.200.200.198	255.255.255.192	Indirizzo IP Stampante di rete
10.200.200.199	255.255.255.192	Indirizzi non utilizzati
…..	…..	
10.200.200.201	255.255.255.192	
10.200.200.210	255.255.255.192	Primo Indirizzo blocco a disposizione del server DHCP
10.200.200.211	255.255.255.192	Altri Indirizzi blocco a disposizione del server DHCP
10.200.200.212	255.255.255.192	
10.200.200.250	255.255.255.192	Ultimo Indirizzo blocco a disposizione del server DHCP
10.200.200.251	255.255.255.192	
10.200.200.252	255.255.255.192	
10.200.200.253	255.255.255.192	
10.200.200.254	255.255.255.192	Indirizzo IP server interno
10.200.200.255	255.255.255.192	Indirizzo di broadcast

- **Subnet docenti**

Ipotizzando che per l'aula docenti siano sufficienti 25 indirizzi IPv4 (10 per i PC desktop, 15 per i dispositivi mobili) utilizziamo il seguente blocco: 10.100.100.96/27.
L'assegnazione degli indirizzi IP è statica e manuale per gli apparati di rete, è statica via DHCP (vincolando l'indirizzo IP all'indirizzo MAC) per i PC desktop, è dinamica via DHCP per i dispositivi che si collegano in modo wireless via Wi-Fi. Il piano di indirizzamento può quindi essere il seguente.

Subnet docenti		
Indirizzo IPv4	**Subnet Mask /27**	**Note**
10.100.100.96	255.255.255.224	Indirizzo della subnet IP
10.100.100.97	255.255.255.224	Default Gateway: ind. IP interfaccia LAN2del Firewall
10.100.100.98	255.255.255.224	Indirizzo IP switch docenti
10.100.100.99	255.255.255.224	Indirizzo IP Stampante di rete
10.100.100.100	255.255.255.224	Primo Indirizzo blocco a disposizione del server DHCP
…..	……..	
10.100.100.125	255.255.255.224	Ultimo Indirizzo blocco a disposizione del server DHCP
10.100.100.126	255.255.255.224	Libero
10.100.100.127	255.255.255.224	Indirizzo di broadcast

Nel caso fossero necessari più indirizzi IP (per i dispositivi mobili) si possono utilizzare:
- il blocco 10.100.100.64/26, subnet mask 255.255.255.192, che fornisce 62 indirizzi IPv4 per gli host;
- il blocco 10.100.100.0/25, subnet mask 255.255.255.128, che fornisce 126 indirizzi IP per gli host
- il blocco 10.100.100.0/24, subnet mask 255.255.255.0, che fornisce 254 indirizzi IP per gli host

- **Subnet DMZ**

Se nella DMZ si pone un solo server fisico è possibile utilizzare, per esempio, il seguente blocco di indirizzi IPv4: **10.255.255.252/30** che fornisce due indirizzi IPv4 (oltre all'indirizzo di subnet 10.255.255.252/30 e all'indirizzo di broadcast 10.255.255.255/30)
- 10.255.255.253 con subnet mask 255.255.255.252 per l'interfaccia DMZ del Firewall
- 10.255.255.254 con subnet mask 255.255.255.252 per il server fisico

Nel caso in cui si utilizzino due server fisici, uno per il server Web ed uno per il database, allora è possibile utilizzare il seguente blocco di indirizzi IPv4 **10.255.255.248/29**, che fornisce 4 indirizzi IPv4 (oltre all'indirizzo di subnet 10.255.255.248/29 e all'indirizzo di broadcast 10.255.255.255/30), assegnabili per esempio nel seguente modo:
- 10.255.255.249 con subnet mask 255.255.255.248 per l'interfaccia DMZ del Firewall
- 10.255.255.250 con subnet mask 255.255.255.248 per il server 1
- 10.255.255.251 con subnet mask 255.255.255.248 per il server 2

- **Interfaccia WAN del Firewall e interfaccia LAN del router xDSL**

Nel caso in cui l'accesso a Internet avvenga tramite un router xDSL (e non semplicemente con un modem) è possibile configurare una subnet composta dall'interfaccia WAN del Firewall e dall'interfaccia LAN (Ethernet) del router xDSL, per esempio con il blocco **172.31.255.252/30**, che fornisce due indirizzi IPv4 (oltre all'indirizzo di subnet 172.31.255.252/30 e all'indirizzo di broadcast 172.31.255.255/30), assegnabili alle interfacce nel seguente modo:

- 172.31.255.253 con subnet mask 255.255.255.252 per l'interfaccia WAN del Firewall
- 172.31.255.254 con subnet mask 255.255.255.252 per l'interfaccia LAN del router xDSL

Punto 3

Descriva possibili tecniche di protezione della rete locale e dei server interni dagli accessi esterni;

Aspetti relativi alla sicurezza che si possono implementare sono i seguenti:

a) **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;

b) **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.

c) Sicurezza perimetrale

L'accesso a Internet va protetto adeguatamente impiegando un **firewall, per esempio 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.

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*)

d) **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.

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

Punto 4

Proponga i principali servizi (tra cui ad es. identificazione degli utenti, assegnazione della configurazione di rete, risoluzione dei nomi, …), e ne approfondisca la configurazione di due a sua scelta.

Oltre ai classici servizi per gli utenti (HTTP/HTTPS, FTP, SMTP e POP3, ecc.), i principali servizi che si possono implementare a supporto delle funzionalità di rete possono essere i seguenti:

- DHCP (Dynamic Host Configuration Protocol); un server DHCP assegna in modo automatico la configurazione IP alle macchine (host) connesse in rete al momento della loro accensione;
- DNS (Domain Name System); un server DNS effettua la risoluzione dei nomi host in indirizzi IP;
- Servizi di Directory (Active Directory Microsoft, LDAP, Lightweight Directory Access Protocol) e AAA (Authentication, Authorization and Accounting); per autenticare gli utenti che accedono alla rete e gestire in modo centralizzato i premessi che essi hanno; un servizio AAA può essere offerto da protocolli quali RADIUS, DIAMETER, TACACS+, KERBEROS;
- SAMBA, per la condivisione di risorse di rete in ambienti in cui sono presenti sia sistemi operativi Windows sia sistemi operativi LINUX;
- SNMP (Simple Network Management Protocol); per il monitoraggio e la gestione centralizzata degli apparati di rete e dei server.

I servizi citati sono di tipo client-server, per cui va configurato il lato server affinché possa offrire i suoi servizi ai client che ne fanno richiesta.

Il **servizio DHCP** può essere offerto tramite server (software) installati su varie tipologie di macchine: server fisici, router, access point, firewall, ecc. Esso si appoggia sul servizio di trasporto UDP[1]. In generale il server (software) DHCP va configurato almeno con i seguenti parametri:

- Indirizzo di rete (subnet) e subnet mask da utilizzare;
- indirizzo IP del default gateway (indicato anche come router);
- indirizzi IP di uno o più server DNS;
- Range di indirizzi IP da utilizzare (indirizzo IP iniziale e numero di indirizzi IP da utilizzare oppure indirizzo IP finale utilizzabile)

E' anche possibile fare in modo che la configurazione IP assegnata a determinate macchine (PC, stampante di rete ecc.) sia statica (cioè sia sempre la stessa, fixed-address) legando l'indirizzo IP all'indirizzo MAC della scheda di rete della macchina (operazione nota anche come binding).

Il **servizio DNS** consente agli host di effettuare la risoluzione dei nomi in indirizzi IP e, viceversa, consente di sapere qual è il nome host associato a un certo indirizzo IP (risoluzione inversa). Esso si appoggia sul servizio di trasporto UDP[2] e può essere offerto tramite un server (software, come per esempio Bind in ambiente LINUX) che in termini generali va configurato assegnando un nome di dominio e associando a ciascun nome host un indirizzo IP univoco, per esempio tramite due file di configurazione che fungono da database; inoltre vanno configurati uno o più indirizzi di server DNS di livello superiore, da contattare nel caso in cui il server DNS locale non sia in grado di effettuare la risoluzione di un determinato nome in indirizzo IP.

Per maggiore chiarezza in allegato si riportano degli estratti dei file di configurazione di un server DHCP e di un server DNS in ambiente LINUX.

Punto 5

Discuta vantaggi e svantaggi dell'offrire il servizio mediante l'attuale soluzione gestita internamente, oppure utilizzando un servizio esterno (Cloud), esponendo le motivazioni che inducono alla scelta.

Vantaggi soluzione gestita internamente

Controllo completo delle informazioni memorizzate sul server
Accesso immediato per l'amministrazione del server e delle informazioni in esso contenute

Svantaggi soluzione gestita internamente

Necessità di hardware, di software, di UPS adeguati e affidabili.
Possibili congestioni nel caso di picchi di richieste di utenti che accedono al server web; la connessione Internet dovrebbe essere preferibilmente simmetrica e banda ultralarga (se disponibile);
Necessità di personale tecnico in grado di gestire l'installazione, la gestione e la manutenzione dell'hardware e del software.
Necessità di implementare adeguate misure di sicurezza sia per l'accesso alle macchine fisiche sia per la protezione dei server da intrusioni e accessi illegittimi.
I costi complessivi possono essere più elevati

Vantaggi soluzione Cloud

Solleva da tutte le problematiche legate all'acquisto, alla gestione e alla manutenzione dell'hardware e del software.

[1] Port number 67 lato server e 68 lato client
[2] Port number 53

Solleva da tutte le problematiche relative alla banda disponibile e al tipo di connettività Internet dei server.
Solleva da tutte le problematiche di sicurezza per l'accesso alle macchine fisiche e la protezione dei server.
I costi complessivi possono essere inferiori.

Svantaggi soluzione Cloud
Le informazioni sono memorizzate su server esterni per cui non sono sotto il proprio diretto controllo.

Ne consegue che la soluzione Cloud sarebbe da preferire nel contesto proposto dalla traccia

Seconda parte

Per i punti 1, 2, 3 si rimanda ai libri di testo
Per il punto 4 è possibile impiegare connessioni VPN Site to Site che impiega la suite di protocolli IPsec, per la cui descrizione si rimanda ai libri di testo.

Allegato 1

Esempio di file di configurazione per server DHCP e DNS in ambiente Linux

Esempio di file di configurazione per un server DHCP in ambiente LINUX

```
#File di configurazione del server DHCP (Server Configuration file).
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 10.0.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  10.0.0.1;
        option subnet-mask              255.255.255.0;
        option domain-name              "lab8";
        option domain-name-servers 10.0.0.35, 208.67.222.222, 208.67.220.220;
        range dynamic-bootp 10.0.0.41 10.0.0.71;
        default-lease-time 21600;
        max-lease-time 43200;

        # si vuole che l'host di nome PC1 abbia sempre lo stesso indirizzo IP
      host pc1 {
         hardware ethernet 00:04:5A:7c:be:e5;
         fixed-address 10.0.0.41;
        # client-hostname "pc1";
      }
```

Esempio di file di configurazione di server DNS in ambiente LINUX

```
//
// named.conf for Red Hat caching-nameserver
//Nota bene i DNS dei forwarders sono quelli del progetto openDNS

options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        forwarders {208.67.222.222; 208.67.220.220; 212.216.112.112; 212.216.172.62;};
        forward first;
        };

//
// a caching only nameserver config
//
controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "localdomain" IN {
        type master;
        file "localdomain.zone";
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
        file "named.ip6.local";
```

```
        allow-update { none; };
};
zone "255.in-addr.arpa" IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};
zone "0.in-addr.arpa" IN {
        type master;
        file "named.zero";
        allow-update { none; };
};
zone "lab8" IN {
        type master;
        file "db.lab8";
        allow-update { none; };
        allow-transfer { any; };
};
zone "0.0.10.in-addr.arpa" IN {
        type master;
        file "db.10.0.0";
        allow-update { none; };
        allow-transfer { any; };
};

include "/etc/rndc.key";
```

```
$TTL 3h
lab8.           IN SOA server-lab8.lab8. onelio.bertazioli.computer.org. (
                                2006112201      ; serial
                                        3h      ; refresh
                                        15m     ; retry
                                        1w      ; expiry
                                        1d )    ; minimum
lab8.           IN NS  server-lab8.lab8.
server-lab8             IN A            10.0.0.150
PC1             IN A            10.0.0.41
PC2             IN A            10.0.0.42
PC3             IN A            10.0.0.43
PC4             IN A            10.0.0.44
PC6             IN A            10.0.0.46
PC7             IN A            10.0.0.47
PC8             IN A            10.0.0.48

;server-web             IN A            10.10.0.35
lab8.tele               IN CNAME    server-lab8; CNAME = ALIAS
```

```
; consente di effettuare la risoluzione inversa
$TTL  3h
0.0.10.in-addr.arpa. IN SOA server-lab8 onelio.bertazioli.computer.org. (
                                2006112201 ; Serial
                        3h    ; Refresh
                        1h    ; Retry
                        1w    ; Expire
                        1d )    ; Minimum
0.0.10.in-addr.arpa.            IN NS  server-lab8.lab8.
150.0.0.10.in-addr.arpa.                IN PTR server-lab8.lab8.
41.0.0.10.in-addr.arpa.                         IN PTR        PC1
42.0.0.10.in-addr.arpa.                         IN PTR        PC2
43.0.0.10.in-addr.arpa.                         IN PTR        PC3
44.0.0.10.in-addr.arpa.                         IN PTR        PC4
46.0.0.10.in-addr.arpa.                         IN PTR        PC6
47.0.0.10.in-addr.arpa.                         IN PTR        PC7
48.0.0.10.in-addr.arpa.                         IN PTR        PC8
```