ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITIA – INFORMATICA E TELECOMUNICAZIONI
ARTICOLAZIONE INFORMATICA **Tema di:** SISTEMI E RETI

ESEMPIO 1 Tipologia c

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

Un giornale locale negli anni novanta realizzò una propria banca dati telematica per la distribuzione elettronica di un notiziario settimanale. Gli utenti, previo abbonamento, 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 cento articoli.

Il nuovo direttore del giornale desidera effettuare l'ammodernamento del sistema, realizzando una nuova 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 direttore;
- trenta computer distribuiti a due a due negli uffici dei giornalisti;
- due computer e una stampante professionale nell'ufficio dei redattori;
- altre apparecchiature mobili (smartphone, pc portatili, …), che vengono usate all'occorrenza dai giornalisti o da collaboratori occasionali.

Inoltre, in un locale protetto, vi è un sistema su cui risiedono la banca dati e il server Web.
Il giornale ha un sito web contenente informazioni e una sintesi degli articoli pubblicati accessibili a tutti senza autenticazione; contiene inoltre una sezione riservata agli abbonati, i quali possono accedere agli articoli completi. Gli abbonati sono ora circa 5.000.
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. descriva possibili tecniche di protezione della rete locale e dei server interni dagli accessi esterni;
3. 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;
4. discuta vantaggi e svantaggi dell'offrire il servizio mediante l'attuale soluzione gestita internamente, oppure utilizzando un servizio esterno (hosting o housing), esponendo le motivazioni che inducono alla scelta.

SECONDA PARTE

Il candidato risponda a due quesiti a scelta tra quelli sotto riportati.

5. In relazione al tema proposto nella prima parte, il sito del giornale consente di differenziare gli accessi tra utenti generici non registrati, abbonati al servizio per la consultazione degli articoli completi, direttore e redattori per l'aggiornamento dei contenuti. Il candidato realizzi il modello concettuale e logico della porzione di base di dati che consente di differenziare gli accessi in base alla tipologia di utente. Progetti poi le pagine Web necessarie a gestire tali accessi all'area riservata e ne codifichi in un linguaggio a sua scelta una parte significativa.
6. In relazione al tema proposto nella prima parte, il giornale offre servizi autenticati di consultazione. Il candidato spieghi il funzionamento dei protocolli https e ssl e gli strumenti di cui è necessario dotarsi per la loro implementazione.
7. 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.
8. La rete offre agli utenti numerosi servizi, quali posta elettronica, servizio web, FTP, DNS, CHAT, ecc., che possono essere di tipo connesso o non connesso. Si descrivano le caratteristiche dei servizi connessi e non connessi riferendosi ad esempi concreti.

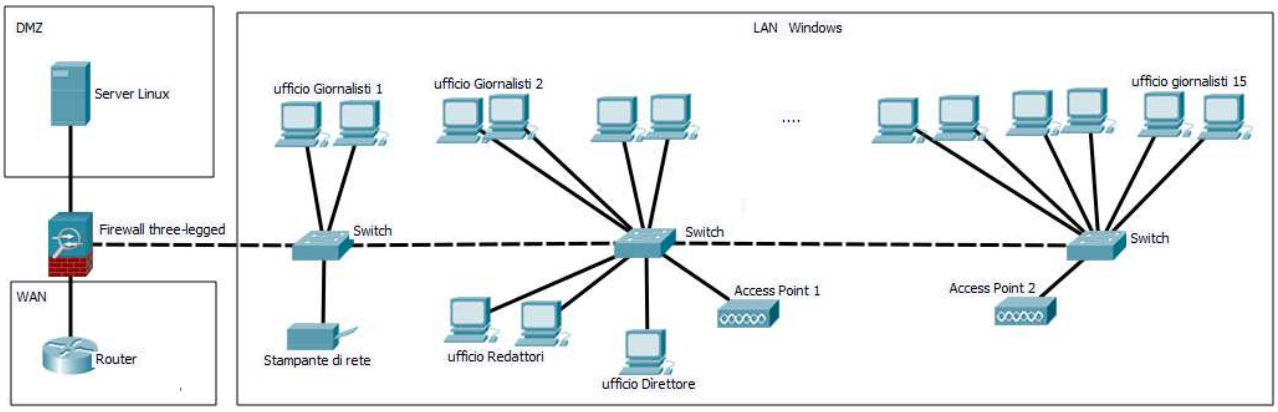
Durata massima della prova: 6 ore.
È consentito soltanto l'uso di manuali tecnici (references riportanti solo la sintassi, non guide) dei linguaggi utilizzati.
È consentito l'uso del dizionario bilingue (italiano-lingua del paese di provenienza) per i candidati di madrelingua non italiana.
Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

Prima parte

Ipotesi aggiuntive

1. Il Giornale vuole ammodernare un sistema informativo progettato e realizzato negli anni 90: considerando i progressi tecnologici realizzati da allora, il sistema verrà progettato e realizzato ex-novo, senza tener in alcun conto del sistema preesistente.
2. La sede del giornale è situata in unico piano e il cablaggio delle postazioni fisse può essere realizzato a muro in canalina.
3. La traccia prende in considerazione solo le attività giornalistiche e non tiene conto degli uffici di segreteria e amministrazione, né delle altre figure professionali di supporto (grafici, tecnici informatici, system e db administrators, web designer, ecc.) e indica esplicitamente che in un unico sistema, collocato in un locale protetto, risiedono la banca dati e il server Web. Per semplicità, la soluzione fa riferimento solo a quanto strettamente richiesto dalla traccia.
4. Per l'aggiornamento dei contenuti del sito web, si adotta un CMS (Content Management System) ovvero un software installato sul server che facilita la gestione dei contenuti di siti web. In tal modo tutti i giornalisti abilitati a farlo possono pubblicare e gestire autonomamente gli articoli dell'edizione online.

Punto 1 e Punto 2



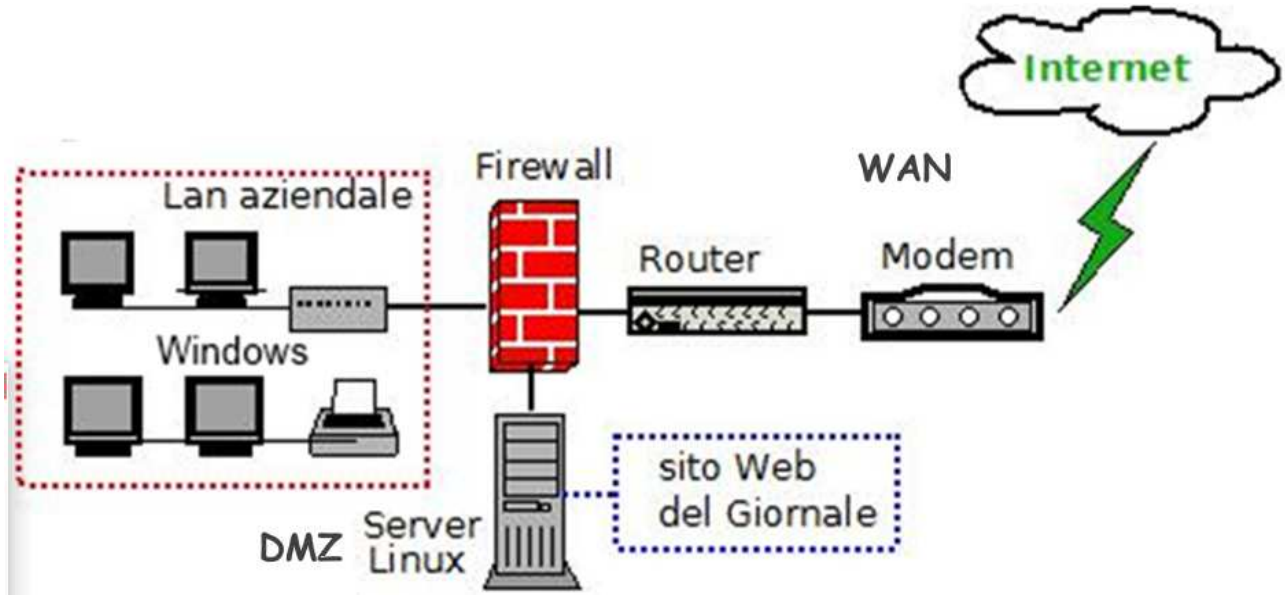
Schema dell'infrastruttura di rete

Per ragioni di affidabilità e sicurezza si sceglie di impiegare un server Linux mentre per quel che riguarda la rete aziendale si preferisce utilizzare Windows, considerando la larghissima diffusione di questo sistema operativo in ambiente desktop. Per gestire l'interazione tra Windows e Linux, sul server si utilizza Samba, un software che:

- agisce da server per i client Windows e permette la condivisione di risorse hardware, software e dati. Grazie a Samba le directory presenti sul server Linux appaiono agli utenti della rete aziendale come normali cartelle di Windows accessibili via rete.
- agisce da controllore di domini in una rete Windows per l'autenticazione degli utenti

Linux funge da server File e server Web e svolge le funzioni di DHCP (Dynamic Host Configuration Protocol) e DC (Domain Controller) per gli utenti autenticati. Il server fornisce inoltre i servizi esterni di email e FTP .

Per proteggere la rete dagli attacchi esterni, si adotta il classico schema che utilizza una DMZ (DeMilitarized Zone ovvero "zona demilitarizzata") creata utilizzando un firewall con tre interfacce Ethernet (three-legged firewall). Questa soluzione viene adottata per consentire ai server collocati nella DMZ di fornire servizi all'esterno senza pregiudicare la sicurezza della rete aziendale interna. Nel nostro caso se il server Web, esposto verso Internet, subisse un attacco esterno, non ci sarebbero ripercussioni nella rete interna perché il firewall la isola sia dalla DMZ che da Internet.



Scegliendo di configurare la Lan e la DMZ con due reti private di classe C 192.168.1.0/24 e 192.168.10.0/24:

1. Il segmento Wan è connesso all'interfaccia IF_EXT eth0 (Ethernet0/0) del firewall con IP statico fornito dal provider
2. La Lan aziendale interna è connessa all'interfaccia IF_LAN eth1 del firewall con indirizzo IP 192.168.1.1 e subnet mask 255.255.255.0
3. Il segmento DMZ è connesso all'interfaccia IF_DMZ eth2 del firewall con indirizzo IP 192.168.10.1 e subnet mask 255.255.255.0

Il ruolo del firewall è centrale nella rete e perché questa funzioni correttamente, bisogna impostare, generalmente attraverso finestre di dialogo user-friendly, le regole NAT (Network Address Translation) che permettono agli Host della Lan di "uscire" su Internet e le regole ACL (Access Control Lists) che definiscono i criteri di protezione e filtraggio. In particolare bisogna configurare le regole di "Port Forwading" e abilitare le richieste che vengono fatte sulle porte del server Linux ("aprendo" la porta TCP 80 per l'HTTP, la porta TCP 21 per l'FTP, la porta 22 per SSH, le porte 137, 138 e 139 oppure 445, 389 e 901 per Samba, ecc)

Oltre al firewall, si adottano ovviamente tutte le altre misure di sicurezza di carattere organizzativo, tecnologico e procedurale, sia preventive che di "recupero", idonee a garantire la protezione dei sistemi informatici e dei dati in essi contenuti.

- Misure di protezione fisica: il server, ampiamente "ridondato" e collegato ad un gruppo di continuità, è collocato in un locale condizionato, dotato di sorveglianza, con porta blindata e sistema di controllo degli accessi.
- Misure di protezione logica: antivirus in ogni pc, autenticazione, screen saver protetti, backup giornalieri dei dati
- Misure di protezione organizzativa: incarichi previsti dalla legge 196/2003 sulla sicurezza e la protezione dei dati, applicazione di best practices, ecc

Caratteristiche del collegamento della rete ad Internet

Riguardo alla versione web del giornale, la traccia parla di 5000 abbonati che possono accedere e leggere gli articoli completi, ma anche di un numero imprecisato di utenti che, senza autenticarsi, possono leggere una sintesi degli articoli. Sono numeri, che pur non essendo elevatissimi, richiedono comunque una connettività adeguata e con banda minima garantita e un servizio affidabile e stabile nel tempo. Viene utilizzata dunque una **Connessione HDSL** (una connessione simmetrica che consente di raggiungere velocità notevoli sia in download che in upload) **con banda garantita di 4Mbps** e con almeno un indirizzo IP pubblico statico.

Hardware e software della Lan aziendale

- La rete utilizza la classica topologia a stella ed è basata sullo standard Gigabit Ethernet (IEEE 802.3ab livello 1-2 ISO/OSI) e sullo standard TCP/IP (livello 3-4 ISO/OSI).
- Trattandosi di un'installazione ex-novo, si realizza un cablaggio strutturato (secondo i dettami EIA/TIA 568) che consente di utilizzare cavi ethernet sia per la fonia che per i dati (telefoni e LAN) e assicura flessibilità e possibilità di sviluppi futuri. Si utilizzano cavi STP cat-5e, schermati e in grado di assicurare una velocità massima di 1 Gbps.
- Si utilizza una stampante di rete, con funzioni scanner e fax, per la fruizione da parte di tutto il personale.
- La connettività dei dispositivi mobili viene assicurata da 2 access point, collocati in posizioni ottimali per "coprire" l'intera sede del giornale, aventi le seguenti caratteristiche:
  - standard 802.11n con trasmissione massima a 300 Mbps alle frequenze 2.4 GHz e 5 GHz
  - protezione con sistema di crittografia WPA2
- La rete aziendale collega tra di loro circa 40 postazioni fisse e una stampante-scanner-fax, attraverso 3 switch di buona qualità, con porte di collegamento almeno da 1 Gbps..
- Tutti i PC, per il lavoro editoriale e grafico che dovranno supportare, sono di fascia medio alta e sono dotati di una buona scheda grafica e di un monitor di 21.5 " con elevata risoluzione e bassi tempi di risposta. Sono equipaggiati con sistema operativo Windows e dotati di software professionali di office automation e di elaborazione grafica. Inoltre sono configurati localmente per l'autenticazione di dominio che consente l'accesso alle risorse della rete locale. In ogni postazione è installato un client di posta elettronica.
- L'inserimento e la modifica degli articoli nell'edizione Web del giornale, vengono gestiti dai giornalisti, abilitati a farlo. attraverso il software CMS accedendo al server Web tramite un browser.

Piano di indirizzamento IP

Rete aziendale interna
rete 192.168.1.0/24 (subnet mask 255.255.255.0)
indirizzo di broadcast: 192.168.1.255
Gateway: 192.168.1.1 (indirizzo Ip dell'interfaccia IF_LAN del firewall)

I pc, la stampante di rete e gli access point hanno indirizzi statici, compresi (ad esempio) nel range 192.168.1.10 - 192.168.1.100 mentre ai dispositivi mobili l'indirizzo IP viene fornito dal servizio DHCP degli access point, in un range che non crea conflitto con quello previsto per gli indirizzi statici (ad esempio 192.168.1.110 -192.168.1.200).

Server Linux
rete 192.168.10.0/24 (subnet mask 255.255.255.0)
indirizzo di broadcast: 192.168.10.255
indirizzo IP: 192.168.10.100 (ad esempio)
Gateway: 192.168.10.1 (indirizzo Ip dell'interfaccia IF_DMZ del firewall)

Hardware e software del server Web

- **Server di fascia alta** dotato di sistemi Fault Tolerance e avente le seguenti caratteristiche di massima:
  - alimentatore ridondante
  - scheda madre con processore multicore, memoria Ram 16 GB
  - tre dischi rigidi SCSI da 1 TB, in modalità Raid5
  - sistema di backup

- **Sistema operativo**
  - Si sceglie di installare un Sistema Operativo Linux con licenza GPL. Tra le varie distribuzioni, per le sue note caratteristiche di sicurezza e stabilità, si preferisce la distribuzione Debian
  - Nel server è installato Samba che fornisce servizi di condivisione di file e stampanti e permette di ottenere interoperabilità tra Linux e Windows.
- **Ambiente Web**
  1. Server Web (il programma che fa funzionare le pagine web). Si sceglie Apache completo dei moduli php, perl e pyton
  2. Server FTP (il programma che permette di copiare, cancellare e modificare le pagine/file web sul server via rete) Si sceglie WsFTP
  3. Database (DBMS) (il software che si occupa di immagazzinare e gestire i dati relativi ai contenuti del sito) Si sceglie MySQL.
  4. Software di amministrazione del DB . Si sceglie PhpMyAdmin
- **Software applicativo**
  Software CMS (Content Management System): in commercio ce ne sono diversi, alcuni molto professionali, specializzati per l'editoria
- **PuTTY**
  Per l'amministrazione in remoto del server Linux, sui Pc Windows si utilizza PuTTY che è un software molto "leggero" in grado di connettersi, utilizzando i protocolli SSH, Telnet ed rlogin, ad un qualsiasi sistema remoto. Basta avviare PuTTY, (un piccolo eseguibile che si avvia con un doppio click), scegliere il protocollo (nel nostro caso SSH - porta 22), inserire l'indirizzo IP del server remoto e il nostro PC diventa un terminale Linux.

Punto 3

Tralasciando altri servizi, seppure fondamentali, quali il servizio Web, l'FTP e la posta elettronica, prendiamo in esame i 3 servizi di esempio citati nella traccia: il servizio di identificazione degli utenti, il servizio di assegnazione della configurazione di rete e il servizio di risoluzione di nomi

1. Il servizio di identificazione degli utenti (DC-Domain Controller) può essere gestito egregiamente da Samba che ha il compito di far interagire Windows con Linux, fornendo una piattaforma comune per l'impiego condiviso delle risorse. Il servizio DC permette agli utenti della rete di:
   - autenticarsi sul dominio, attraverso le credenziali di username e password
   - accedere a tutte le risorse condivise nel dominio stesso
   - fornire un livello di protezione per l'accesso
2. Il servizio di assegnazione della configurazione di rete è assicurato da DHCP (Dynamic Host Configuration Protocol), un protocollo di livello applicativo che permette ai dispositivi di rete di ricevere la configurazione IP necessaria per poter operare su una rete basata su IP (Internet Protocol). Nei sistemi Linux il DHCP è implementato nel demone dhcpd.
3. Il servizio di risoluzione di nomi è gestito da DNS (Domain Name System). In una rete locale con server Linux e client Windows, per far si che le comunicazioni di rete avvengano in modo efficiente, è necessario avere un server DNS che sia in grado di risolvere i nomi host dei vari PC in rete locale. Per fare questo Linux utilizza il software Bind che opera in stretto contatto con il server DHCP il quale assegna dinamicamente la configurazione IP ai vari host e contestualmente aggiorna i record DNS su Bind.
   Il server DNS viene utilizzato anche per risolvere i nomi di dominio Internet, impostando uno o più forwarders (indirizzi IP di server DNS esterni tipo 8.8.8.8 di Google) da consultare se un dominio non è stato definito sul server DNS locale.

Punto 4

Oltre alla soluzione adottata dal giornale che consiste nella gestione interna del server Web, esistono due alternative gestite da un provider esterno: l'hosting e l'housing.
L'**hosting** è un servizio che ospita più siti Web su una singola macchina, assegnando a ognuno di essi un IP differente. Con il servizio di hosting il sito condivide memoria di massa e banda disponibile con altri siti web.
L'**housing** invece è un servizio in cui il server, di proprietà del cliente, viene ospitato presso il data-center del Provider che fornisce il collegamento a larga banda alla rete internet e il servizio di sorveglianza e di assistenza hardware. La manutenzione sistemistica è invece affidata al cliente. A differenza dell'hosting il sito ospitato non condivide le risorse con altri siti web.
E' chiaro che, considerando il livello di prestazioni richiesto, la soluzione Hosting è da escludere; per cui mettiamo a confronto solo la soluzione "interna" e quella "in housing.

Soluzione "interna"

Vantaggi	**Svantaggi**
Pieno controllo sui propri dati ed applicazioni	Investimento iniziale elevato per l'acquisto e la configurazione del server
Utilizzo di politiche personalizzate per la sicurezza e la privacy dei dati	Necessità di personale tecnico informatico per la gestione del server, con costi annuali elevati
Eventuale utilizzo del server per applicazioni Intranet	Costi annuali elevati per la connessione DSL a larga banda
Possibilità di intervenire immediatamente in caso di guasti e/o malfunzionamenti hardware e software	Costi annuali significativi per la manutenzione e l'upgrade dell'hardware e del software
Possibilità di intervenire sulla configurazione del Server per migliorare i servizi erogati	

Soluzione "in housing"

Vantaggi	**Svantaggi**
Pieno controllo del proprio spazio, possibilità di gestirlo ed effettuare tutte le configurazioni che si ritengono necessarie	All'interno dell'azienda deve comunque essere presente una figura professionale in grado di amministrare da remoto un sistema informativo complesso
Nessun investimento iniziale e costi annuali complessivi relativamente modesti. Non occorre una connettività Internet particolarmente performante	Non si dispone di un server per eventuali applicazioni locali
Gradualità degli investimenti: possibilità di richiedere al Provider nuovi servizi o prestazioni più performanti, man mano che crescono le esigenze aziendali	Non si ha la possibilità di intervenire immediatamente in casi di guasti hardware e software. Bisogna aprire un ticket di assistenza e aspettare l'intervento del provider

Seconda parte

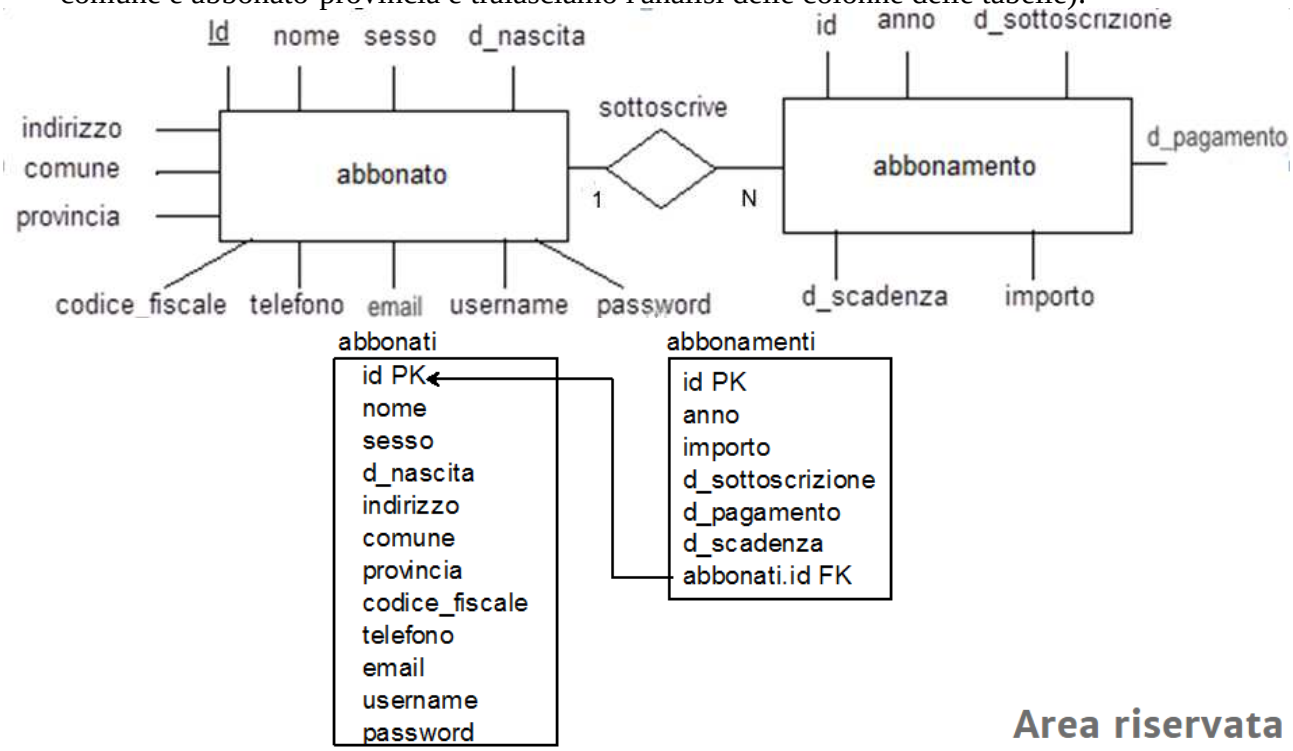
Si sceglie di svolgere i quesiti 1 e 2. Il quesito 3 può essere sviluppato spiegando che cos'è in generale la crittografia e illustrando, in particolare, il funzionamento della crittografia asimmetrica. Il quesito 4, riguardante i servizi Internet connessi e non connessi, può essere svolto facendo riferimento ai servizi Web o FTP (servizi connessi che utilizzano il protocollo TCP) e ai servizi che utilizzano flussi audio e video (non connessi che utilizzano il protocollo UDP).

Quesito 1

In relazione al tema proposto nella prima parte, il sito del giornale consente di differenziare gli accessi tra utenti generici non registrati, abbonati al servizio per la consultazione degli articoli completi, direttore e redattori per l'aggiornamento dei contenuti. Il candidato realizzi il modello concettuale e logico della porzione di base di dati che consente di differenziare gli accessi in base alla tipologia di utente. Progetti poi le pagine Web necessarie a gestire tali accessi all'area riservata e ne codifichi in un linguaggio a sua scelta una parte significativa.

La differenziazione tra utenti generici non registrati e utenti registrati, avviene utilizzando una procedura di login sulla home page del sito. Gli utenti autenticati, potranno leggere integralmente gli articoli online, al contrario gli utenti generici potranno leggere solo una sintesi degli articoli proposti nella edizione Web del giornale.

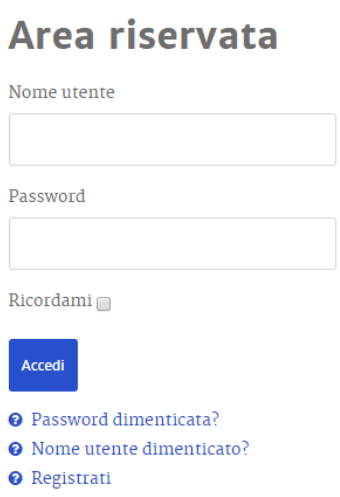
- Le modalità di aggiornamento dei contenuti vengono gestite dal software CMS
- Il modello concettuale riguarda dunque esclusivamente gli utenti registrati, cioè gli abbonati che ogni anno sottoscrivono l'abbonamento. Per quest'ultima relazione si propone il seguente modello concettuale e logico (per semplicità non teniamo conto delle relazioni abbonato-comune e abbonato-provincia e tralasciamo l'analisi delle colonne delle tabelle):



Facendo riferimento ad un tipico form utilizzato per accedere ad un'area riservata, le pagine Web necessarie a gestire gli accessi degli abbonati riguardano le funzioni di login, di registrazione e di recupero username e password.

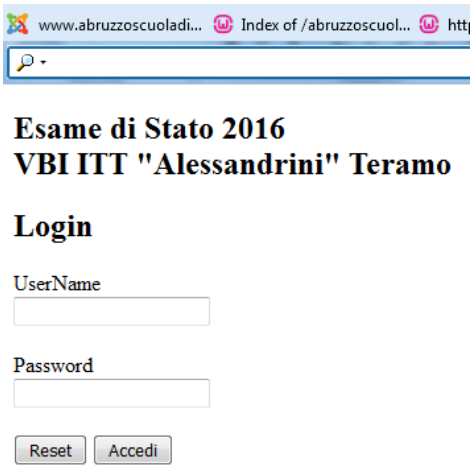
Tra queste, utilizzando il Database MySql e le tecnologie HTML5, CSS3, PHP e JavaScript, si sceglie di codificare la procedura di login.

Per ragioni di tempo, il codice proposto è essenziale e non contiene codice CSS e controlli JavaScript.



formaccesso.html

```
<!DOCTYPE html>
<head>
<title>Login</title>
</head>
<form method="POST" action="eseguiaccesso.php">
<h2> Esame di Stato 2016</br>
 VBI ITT "Alessandrini" Teramo</h2>
<h2>Login</h2>
UserName</br>
<input type='text' name='username'></br>
</br>Password</br>
<input type='password' name='password'></br>
</br><input type='reset' value='Reset'>
<input type='submit' value='Accedi' >
</form>
</body>
</html>
```



eseguiaccesso.php

```
<?php
$conn=mysqli_connect("localhost","root","mypassword","sistemi");
$username=$_POST["username"];
$password=$_POST["password"];
$s="SELECT * FROM abbonati
    WHERE username='$username'
    AND password=md5('$password')";
$q=mysqli_query($conn,$s);
$numrighe=mysqli_num_rows($q);
if($numrighe==0)
{
     echo "Credenziali errate!";
}
else
{
     echo "<h1>Benvenuto!</h1>";
}
mysqli_close($conn);
?>
```

Quesito 2

In relazione al tema proposto nella prima parte, il giornale offre servizi autenticati di consultazione. Il candidato spieghi il funzionamento dei protocolli https e ssl e gli strumenti di cui è necessario dotarsi per la loro implementazione.

HTTPS (Hyper Text Transfer Protocol Secure) è la versione "sicura" di HTTP, il protocollo di rete attraverso il quale i dati vengono scambiati tra il client (browser) e il server (il sito web a cui si è connessi).
HTTPS ha lo scopo di prevenire gli attacchi di eventuali hacker che, inserendosi nella comunicazione tra client e server, intercettano i dati che i due nodi si scambiano. Esso garantisce l'identificazione del sito web che si sta visitando e del server web che lo ospita. Inoltre, i dati che i due nodi si scambiano vengono criptati, proteggendo l'utente dal pericolo di essere intercettato o di visitare siti manomessi.
La porta standard utilizzata da HTTPS è la porta 443 (nel caso del protocollo HTTP viene utilizzata la porta 80).
Il protocollo SSL (Secure Sockets Layer) è obsoleto ed è stato sostituito dal TSL (Transport Layer Security). Entrambi sono i protocolli di crittografia che consentono una comunicazione sicura tra due nodi di una rete TCP/IP (come ad esempio Internet) fornendo autenticazione, integrità dei dati e cifratura e operando al di sopra del quarto livello della catena ISO/OSI.
I protocolli HTTPS e TSL lavorano insieme: infatti il protocollo HTTPS è conosciuto anche come HTTP over TLS, HTTP over SSL e HTTP Secure: i dati inviati tramite HTTPS vengono protetti tramite il protocollo TLS (oppure tramite SLL ma questo protocollo da qualche tempo è ritenuto non sicuro). Come già detto TLS (o SLL) fornisce i tre livelli di protezione fondamentali: crittografia, integrità dei dati e autenticazione.
La procedura di criptazione dati è relativamente semplice, si basa su una chiave pubblica che il server invia al client ad ogni connessione, per permettergli di inviare in modo sicuro la propria chiave. Questi pacchetti criptati possono essere letti solo dal server che ha rilasciato la chiave pubblica poiché sarà l'unico host a possedere la chiave privata, la sola in grado di decriptare le informazioni ricevute.
Su una distribuzione Debian di solito il modulo per la gestione del protocollo HTTPS viene installato di default al momento dell'installazione di Apache, quindi basterà abilitarlo. Durante l'attivazione di HTTPS occorre richiedere un certificato di sicurezza TLS (o SSL) valido, emesso da un ente certificatore che verifica se il sito per cui si adotta il protocollo HTTPS appartiene effettivamente all'azienda che ha richiesto il certificato.