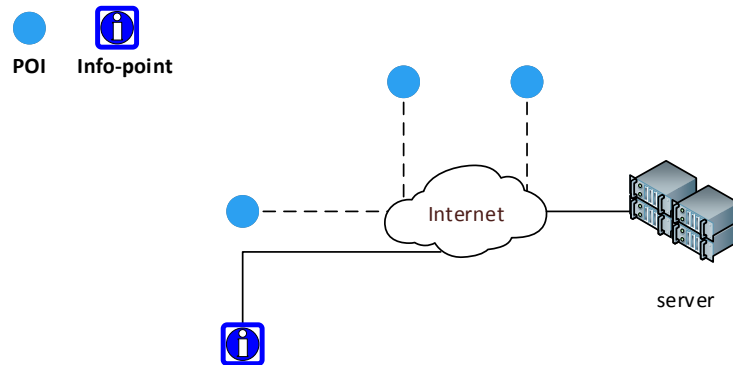


PRIMA PARTE

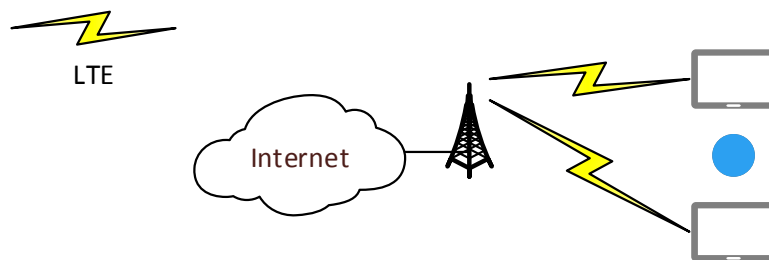
1. Il servizio ha la seguente infrastruttura di rete complessiva:



a)

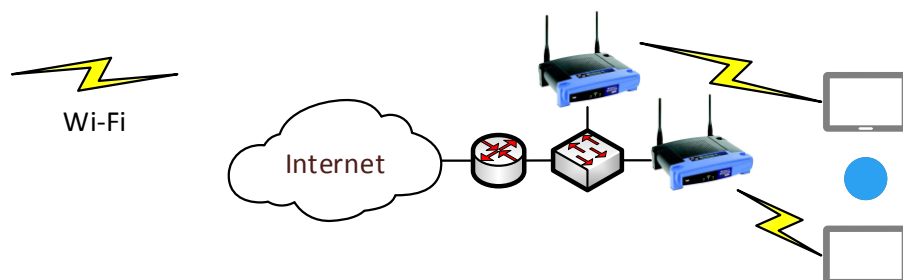
Nel singolo POI (*Point Of Interest*) si possono verificare due distinte situazioni:

- non vi è nessuna infrastruttura di rete W-LAN e i tablet accedono al server tramite la rete Internet utilizzando il modem LTE integrato per l'accesso alla rete dati dell'operatore di telefonia mobile:



l'operatore della rete dati mobili assegna gli indirizzi IPv4/IPv6 pubblici ai tablet utilizzando un server DHCP;

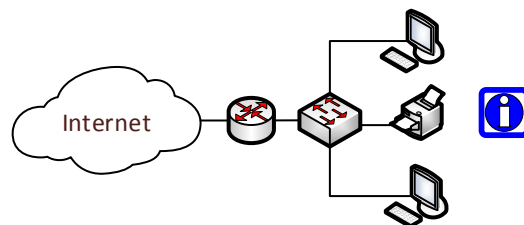
- vi sono uno o più *access-point* che consentono la connessione dei tablet alla rete W-LAN locale IEEE-802.11 (Wi-Fi) e, tramite questa, al server esposto sulla rete Internet:



gli *access-point* sono connessi alla rete Internet mediante una rete Ethernet cabalata utilizzando un router-switch che integra un modem DSL ed un *firewall*; i tablet sono consegnati ai visitatori già configurati con le credenziali di accesso IEEE-802.11i (WPA-2) alla rete W-LAN e ricevono un indirizzo IPv4 dinamico da un server DHCP integrato nel router-switch, o negli *access-point*; l'accesso alla rete Internet avviene utilizzando NAT/PAT con un singolo indirizzo IPv4/IPv6 pubblico.

È possibile elevare il livello di protezione dell'infrastruttura di rete presso il singolo POI configurando un server RADIUS IEEE-802.1X prevedendo un *account* per ogni singolo tablet.

Ogni singolo Info-point ha alcune postazioni di lavoro connesse al server tramite la rete Internet ed una stampante per i biglietti:



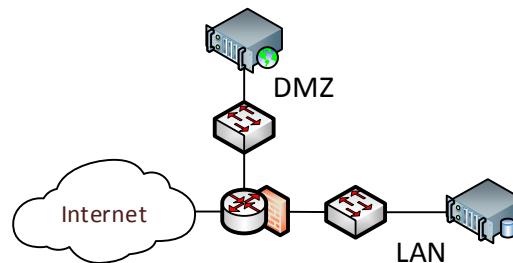
i PC delle postazioni di lavoro sono connessi alla rete Internet mediante una rete Ethernet cabalata utilizzando un router-switch che integra un modem DSL ed un firewall; gli indirizzi IPv4 possono essere assegnati staticamente utilizzando NAT/PAT per l'accesso alla rete Internet.

Il server deve rendere disponibile un DBMS (ad esempio MySQL) per ospitare il database di gestione del servizio e i file dei contenuti multimediali relativi ai vari POI ed un web-server (ad esempio Apache + PHP) per l'erogazione delle pagine web dinamiche richieste dai tablet consegnati ai visitatori e dalle postazioni di lavoro degli Info-point; sono possibili diverse soluzioni:

- la configurazione come server virtuale usufruendo di un servizio *cloud* di tipo IaaS (ad esempio AWS),
- il ricorso, date le caratteristiche standard richieste, ad un servizio di *hosting* (ad esempio Aruba),
- la gestione di un server fisico presso il *data-center* del Comune;

l'ultima soluzione richiede di garantire la continuità di servizio e la sicurezza del sistema, cosa che risulta normalmente proibitiva in termini organizzativi ed economici per un servizio con queste caratteristiche; inoltre la difficoltà di stimare a priori il numero di visitatori che usufruiscono del servizio e conseguentemente del traffico dati generato rende sicuramente preferibile la prima soluzione che può "scalare" – anche sotto l'aspetto dei costi – in funzione dell'uso effettivo delle risorse computazionali (CPU, RAM, spazio di memorizzazione permanente, ...) e di comunicazione (banda, ...).

Nel caso si opti comunque per una soluzione *on-premises* è opportuno separare il server fisico che ospita il web-server da collocare nella rete DMZ, dal server fisico che ospita il DBMS da collocare nella rete LAN configurando il router-firewall di interconnessione con la rete Internet con opportune regole di filtraggio del traffico di rete:



Il server che ospita il web-server, che deve risultare accessibile dalla rete Internet, avrà un indirizzo IPv4/IPv6 privato statico associato ad un corrispondente indirizzo pubblico mediante NAT statico, mentre il server che ospita il DBMS, che deve risultare accessibile esclusivamente dal web-server, avrà un indirizzo IPv4 privato statico.

b)

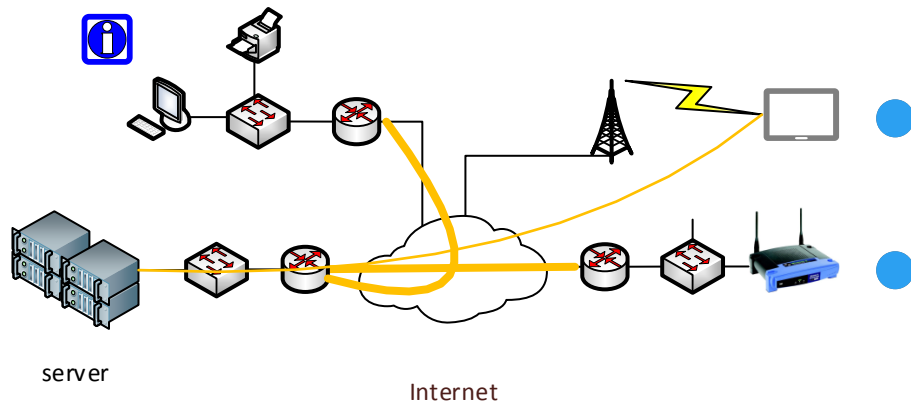
I tablet consegnati ai visitatori, oltre che disporre di un browser o di una specifica APP per la visualizzazione delle pagine web con i contenuti multimediali dei POI, devono avere le seguenti caratteristiche di connettività e geolocalizzazione:

- W-LAN IEEE-802.11 (WI-FI).
- W-WAN LTE.
- GPS (per la geolocalizzazione *indoor* il sistema operativo Android è in grado di utilizzare le reti *wireless* LAN/WAN rilevate);

dato che devono semplicemente richiedere ed ottenere pagine web, la loro connessione al web-server avviene tramite la rete Internet utilizzando i protocolli di rete standard IP/TCP/HTTP: è senz'altro opportuno che l'accesso al web-server sia protetto utilizzando il protocollo TLS e che il server sia dotato di un certificato X.509 che ne garantisca l'autenticità ai client che si connettono.

La credenziale che consente l'accesso alla pagina web multimediale di descrizione di un POI è costituita dalla password stampata sul biglietto che sarà richiesta dalla pagina web principale: la password potrà essere utilizzata esclusivamente per il numero di volte previsto dalla tariffa di acquisto.

Data la natura privata di tutte le comunicazioni, sia quella tra tablet e server che quella tra Info-point e server, e il fatto che i tablet sono configurabili prima di essere consegnati ai visitatori, è possibile elevare il livello generale di sicurezza prevedendo l'impiego generalizzato di VPN:



Per gli Info-point e i POI dotati di infrastruttura di rete è preferibile usare una VPN router-to-router utilizzando il protocollo IPsec in modalità tunnel; per i tablet che si connettono tramite la rete dati di telefonia mobile è invece possibile utilizzare una tecnologia end-to-end come open-VPN configurata sul web-server e per la quale esiste un client specifico per sistema operativo Android.

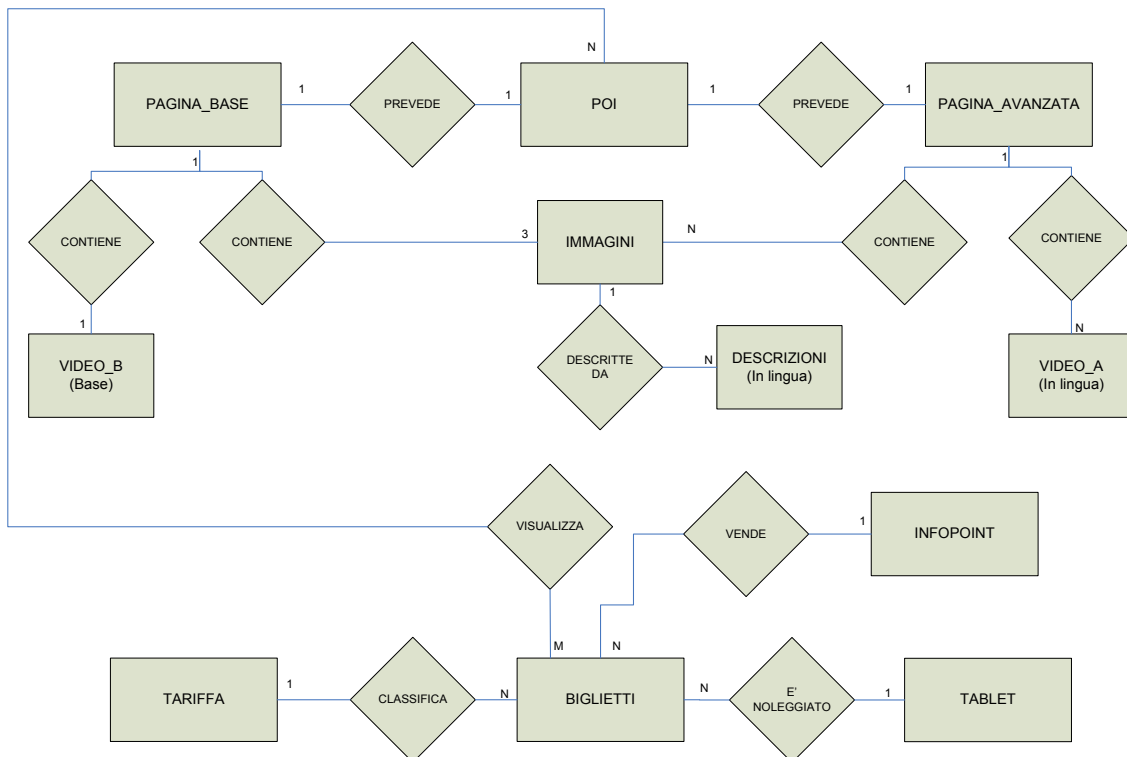
c)

Per garantire che la pagina web multimediale di descrizione di un POI possa essere richiesta solo in prossimità dello stesso sono possibili diverse tecniche, tra cui:

- memorizzare nel database le coordinate geografiche di ogni POI ed il suo raggio approssimativo di estensione: la pagina web che trasmette al web-server la password rileva e trasmette anche la posizione del tablet, il server è quindi in grado di determinarne la distanza dal centro dei POI più vicini e restituire la pagina web multimediale di descrizione solo se essa è inferiore al raggio di estensione;
- installare nei POI dei tag RFID/NFC con memorizzato un identificativo univoco dello stesso riportato nel database: se il tablet è dotato dello specifico lettore, la pagina web che trasmette al web-server la password acquisisce e trasmette anche l'identificativo ed il web-server è quindi in grado di determinare il POI da cui proviene la richiesta e condizionare di conseguenza la risposta;
- solo nel caso che tutti i POI dispongano di un'infrastruttura di rete e che i tablet siano vincolati ad inviare richieste esclusivamente tramite le reti W-LAN dei POI (è sufficiente disabilitare il traffico dati sulla rete di telefonia mobile e impedire la connessione a reti Wi-Fi non configurate), è possibile memorizzare nel database l'indirizzo IP pubblico del router di interconnessione con la rete Internet di ogni singolo POI in modo da permettere al web-server di determinare la provenienza delle richieste (nel caso si adotti una rete VPN, nel database dovranno essere memorizzati gli intervalli di indirizzi assegnati alla rete W-LAN di ciascun POI in quanto le richieste al web-server manterranno l'indirizzo di provenienza).

2.

Modello concettuale



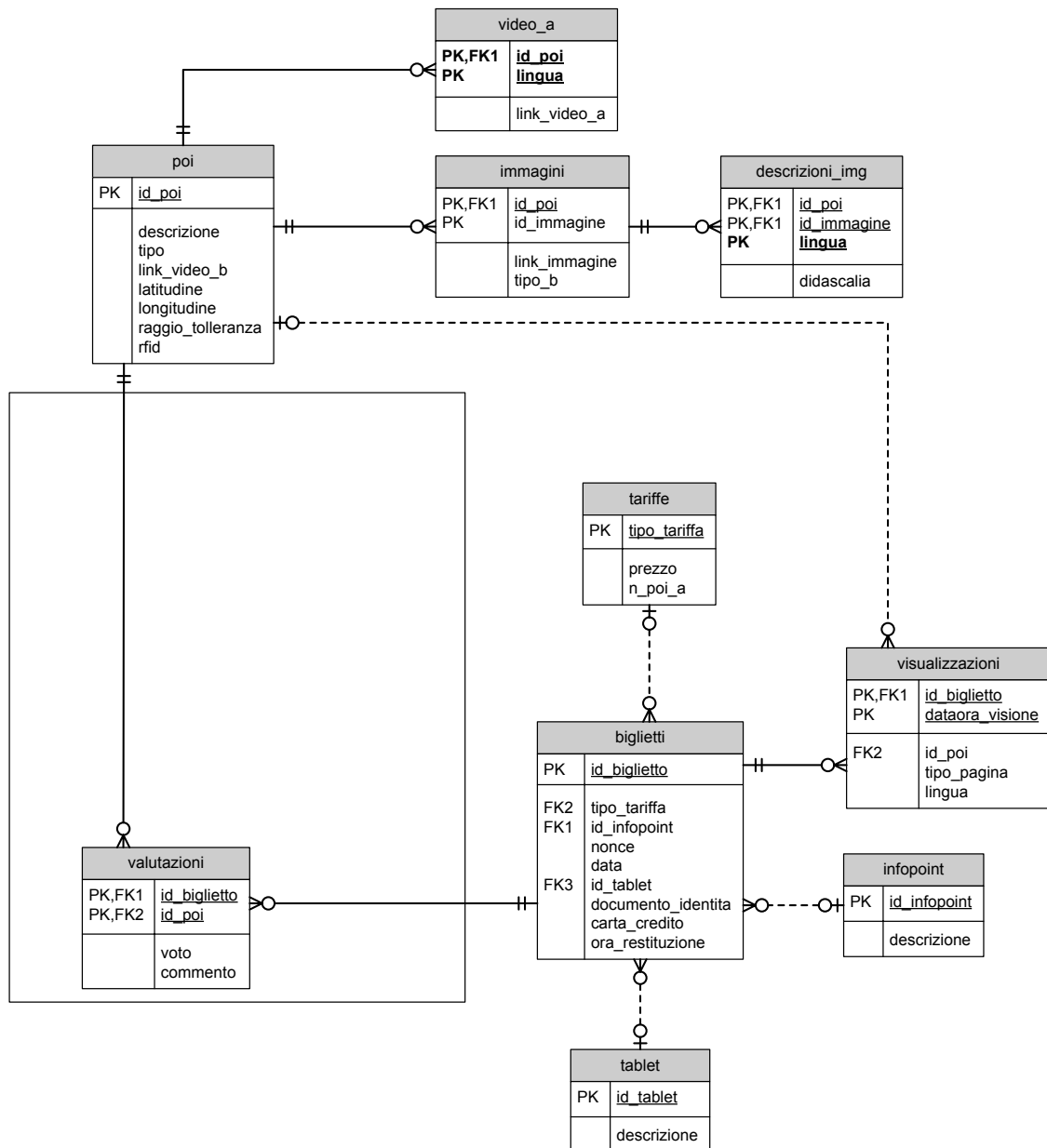
Modello logico

Nel modello logico non sono presenti le tabelle che rappresentano le entità *PAGINA_BASE* e *PAGINA_AVANZATA*:

- per la pagina base il collegamento al video, essendo unico, è stato inserito direttamente nella tabella *POI*, mentre per le immagini si è optato per l'uso dell'attributo *tipo_b* che identifica le sole immagini visualizzabili nella pagina base;
- per la pagina avanzata è stata prevista la tabella *video_a* che prevede i collegamenti del video del *POI* nelle varie lingue che l'utente può selezionare se abilitato ad una visualizzazione avanzata, per le immagini è possibile accedere a tutte quelle presenti con la didascalia nella lingua selezionata dall'utente.

Gli attributi *latitudine*, *longitudine* e *raggio_tolleranza* della tabella *POI* servono – a partire dalle coordinate della posizione attuale di un tablet – a determinare se esso si trova fisicamente nel contesto di un *POI* del quale possa attivare o meno la visualizzazione della pagina web multimediale di descrizione in base ai parametri del biglietto (tipo di visualizzazione A o B, lingua prescelta, ...).

La sezione del modello inclusa nel rettangolo implementa la richiesta del quesito I della seconda parte.



Dato che con l'acquisto di un biglietto si potrà disporre dell'utilizzo di un tablet, la tabella *biglietti* avrà la seguente struttura:

Campo	Descrizione
<i>id_biglietto</i>	numero seriale di emissione del biglietto
<i>tipo_tariffa</i>	tariffa applicata al biglietto (B, I, P)
<i>id_infopoint</i>	codice dell'info-point di acquisto del biglietto e di consegna del tablet
<i>nonce</i>	password univoca associata al biglietto
<i>data</i>	data/ora di emissione del biglietto e di ritiro del tablet
<i>id_tablet</i>	numero di matricola del tablet ritirato
<i>documento_identita</i>	identificativo del documento di identità consegnato per il ritiro del tablet (valorizzazione alternativa a <i>carta_credito</i>)
<i>carta_credito</i>	identificativo della carta di credito fornita per il ritiro del tablet (valorizzazione alternativa a <i>documento_identita</i>)
<i>ora_restituzione</i>	orario di restituzione del tablet (non valorizzato fino a che non viene restituito)

3. Il codice seguente realizza in linguaggio HTML/JavaScript/PHP le pagine di richiesta e di visualizzazione della descrizione di un POI nell'ipotesi di un DBMS MySQL in esecuzione sullo stesso server che esegue il web-server Apache con PHP abilitato come *server-side scripting language*, utente *root* privo di password e database denominato "POI".

Le pagine web dinamiche visualizzate sono prive di un layout grafico da realizzarsi con l'uso di CSS.

La pagina "checkPOI.php" rileva automaticamente latitudine e longitudine della posizione corrente dal dispositivo di geolocalizzazione del tablet e richiede all'utente la password riportata sul biglietto; la pressione del pulsante di invio fornisce questi dati alla pagina "pagePOI.php"¹.

La pagina "pagePOI.php":

- invoca la funzione *distance* per calcolare la distanza tra la posizione rilevata dal tablet e la posizione dei POI presenti nel database e determina, in base al raggio di tolleranza, se il tablet si trova in un POI noto o meno;
- restituisce la pagina web multimediale di descrizione del POI individuato.

checkPOI.php

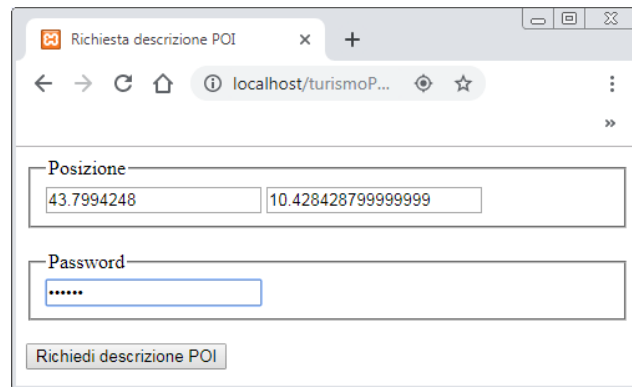
```
<html>
<head>
<title>Richiesta descrizione POI</title>
<script>
function getLocation() {
    navigator.geolocation.getCurrentPosition(position, error);
}
function position(pos) {
    document.getElementById("lat").value=pos.coords.latitude;
    document.getElementById("long").value=pos.coords.longitude;
}
function error(err)
{
    switch(err.code)
    {
        case err.PERMISSION_DENIED:
            window.alert("Accesso al servizio di localizzazione proibito.");
            break;
        case err.POSITION_UNAVAILABLE:
            window.alert("Servizio di localizzazione non disponibile.");
            break;
        case err.TIMEOUT:
            window.alert("Timeout del servizio di localizzazione.");
            break;
        case err.UNKNOWN_ERROR:
            window.alert("Errore di accesso al servizio di localizzazione.");
            break;
    }
}
</script>
</head>
```

¹ questa soluzione è stata adottata per semplicità, anche se consente all'utente di posticipare la richiesta della pagina di descrizione di un POI e di effettuarla in una posizione diversa

```

<!-- determina le coordinate della posizione corrente -->
<body onload="getLocation()">
  <form id="poiLL" method="GET" action="pagePOI.php">
    <fieldset name="posizione">
      <legend>Posizione</legend>
      <input type="text" placeholder="latitudine" id="lat"
        name="latitudine">
      <input type="text" placeholder="longitudine" id="long"
        name="longitudine">
    </fieldset>
    <br>
    <fieldset name="password">
      <legend>Password</legend>
      <input type="password" name="password">
    </fieldset>
    <br>
  </form>
  <input id="btn" type="submit" value="Richiedi descrizione POI"
    form="poiLL">
</body>
</html>

```



pagePOI.php

```

<html>
  <head>
    <title>
      Assessorato al turismo di...
    </title>
  </head>
  <body>
    <?php
      $connection = mysqli_connect("localhost", "root", "", "POI");
      if (mysqli_connect_errno($connection))
        die("Errore di connessione al DBMS My-SQL.");
      if (trim($_GET['password'])=="")
        die ("Password non specificata.");
      $query="SELECT *
        FROM biglietti
        WHERE nonce='".$_GET['password']."'";
      $respwd = mysqli_query($connection, $query);
      if (mysqli_num_rows($respwd) == 0)
        die("Password non abilitata.");
      $query="SELECT *
        FROM poi;";
      $respoi = mysqli_query($connection, $query);
      if (!$respoi)
        die("Errore esecuzione query SQL.");
    </?php>
  </body>
</html>

```



```

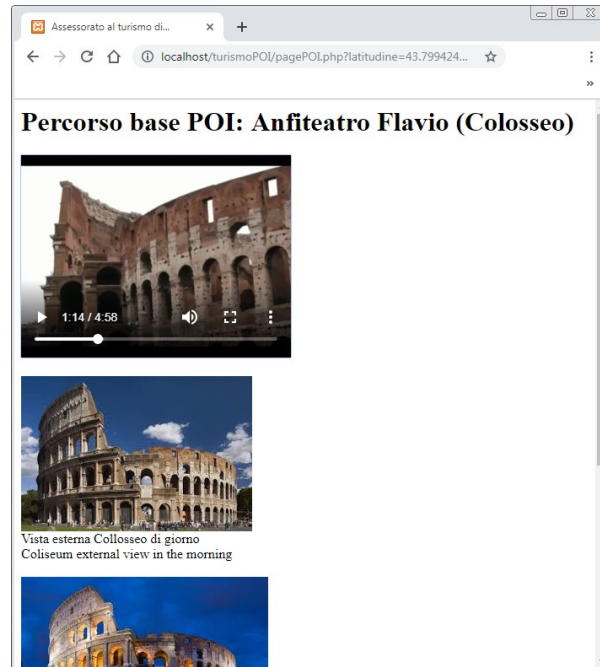
if (mysqli_num_rows($respoi) == 0)
    die("Nessun POI trovato.");
$latit = $_GET['latitudine'];
$longit = $_GET['longitudine'];
$id_poi = -1;
$distmin = -1;
while ($rowpoi = mysqli_fetch_assoc($respoi))
    {
        $dist = distance($latit, $rowpoi['latitudine'], $longit,
                        $rowpoi['longitudine']);
        if ($dist<= $rowpoi['raggio_tolleranza'])
            {
                if (($distmin == -1) || ($dist<$distmin))
                    {
                        $id_poi = $rowpoi['id_poi'];
                        $distmin = $dist;
                    }
            }
    }
if ($id_poi == -1)
    die("POI non censito.");
$query = "SELECT poi.descrizione, link_video_b, link_immagine,
            didascalial, lingua
            FROM poi, immagini, descrizioni_img
            WHERE poi.id_poi = immagini.id_poi
                  AND immagini.id_poi = descrizioni_img.id_poi
                  AND immagini.id_immagine = descrizioni_img.id_immagine
                  AND poi.id_poi = '$id_poi'
                  AND immagini.tipo_B = 'S'
                  AND descrizioni_img.lingua IN ('ENG','ITA')
            ORDER BY immagini.id_immagine, lingua DESC;";
$result = mysqli_query($connection, $query);
if (!$result)
    die("Errore esecuzione query SQL.");
if (mysqli_num_rows($result) == 0)
    die("Nessun dato POI trovato.");
$row = mysqli_fetch_assoc($result);
?>
<h1>
    <?php echo "Percorso base POI: ".$row['descrizione']; ?>
</h1>
<!-- Video -->
<video width="320" height="240" controls>
    <?php echo '<source src="'.$row['link_video_b'].'" type="video/mp4">';
    ?>
</video>
<br>
<br>
<!-- Immagini 1, 2 e 3 -->
<?php
    for ($i=1; $i<=3; $i++)
        {
            echo '';
            echo "<br>";
            echo $row['didascalial']; //didascalial Italiano
            $row = mysqli_fetch_assoc($result);
            echo "<br>";
            echo $row['didascalial']; //didascalial Inglese
            echo "<br><br>";
            if ($i<3)
                $row = mysqli_fetch_assoc($result);
        }
mysqli_free_result($result);

```

```

echo "</tbody>\n";
echo "</table>\n";
mysqli_close($connection);
?>
</body>
</html>

```



4. Le varie tipologie di tariffe previste (Base, Intermedia, Piena) classificano i biglietti e le pagine web multimediali di descrizione dei POI a cui danno accesso: la tabella *tariffe* potrebbe quindi avere una valorizzazione come la seguente:

<i>tipo_tariffa</i>	<i>prezzo</i>	<i>n_poi_a</i>
B	10	0
I	20	3
P	30	-1

Il campo *tipo_tariffa* identifica la tipologia di tariffa, il campo *prezzo* rappresenta il prezzo in € per un biglietto e il campo *n_poi_a* rappresenta il numero di pagine web multimediali di tipo avanzato che possono essere visualizzate (-1 = illimitato).

La richiesta di accesso ad una pagina web multimediale di descrizione di un POI viene sempre registrato nella tabella *visualizzazioni*: a fronte di una richiesta è quindi possibile – per la tariffa Intermedia – determinare il numero di visualizzazioni avanzate già effettuate per autorizzarne o meno una nuova, in modo indipendente dal POI per il quale viene richiesta.

SECONDA PARTE

- I. L'integrazione del database per gestire commenti e valutazioni è realizzata tramite la tabella valutazioni evidenziata nel riquadro del modello logico del database fornito al punto (2) della prima parte.

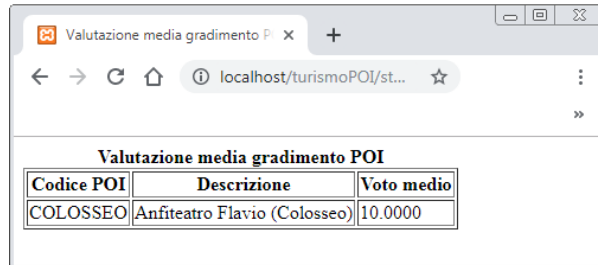
Lo *script* PHP che segue fornisce la statistica relativa al voto medio assegnato dai visitatori ai singoli POI:

```
<html>
<head>
  <title>Valutazione gradimento POI</title>
</head>
<body>
  <?php
    $connection = mysqli_connect("localhost", "root", "", "POI");
    if (mysqli_connect_errno($connection))
    {
      echo "Errore di connessione al DBMS MySQL." ;
      die();
    }
    $query = "SELECT poi.id_poi, poi.descrizione, AVG(voto) AS voto_medio
              FROM poi, valutazioni
              WHERE poi.id_poi = valutazioni.id_poi
              GROUP BY poi.id_poi, poi.descrizione;";
    $result = mysqli_query($connection, $query);
    if (!$result)
    {
      echo "Errore esecuzione query SQL." ;
      die();
    }
    if (mysqli_num_rows($result) == 0)
    {
      echo "Nessun dato trovato." ;
      die();
    }
  ?>
  <table border>
  <caption>
    <b>Valutazione media gradimento POI</b>
  </caption>
  <thead>
  <tr>
    <th>Codice POI</th>
    <th>Descrizione POI</th>
    <th>Voto medio</th>
  </tr>
  </thead>
  <tbody>
  <?php
    while ($row = mysqli_fetch_assoc($result))
    {
      ?>
      <tr>
        <td><?php echo ($row['id_poi']); ?></td>
        <td><?php echo ($row['descrizione']); ?></td>
        <td><?php echo ($row['voto_medio']); ?></td>
      </tr>
    <?php
    }
    mysqli_free_result($result);
```

```

        echo "</tbody>\n";
        echo "</table>\n";
        mysqli_close($connection);
    ?>
</body>
</html>

```



- II. Volendo escludere la fruizione delle pagine web multimediali di descrizione dei POI da parte dei dispositivi personali la soluzione più semplice appare quella – già indicata al punto (1.b) della prima parte – di permettere l’accesso al web-server esclusivamente mediante VPN.

Per consentire l’uso dei dispositivi personali è invece necessario che il web-server sia pubblicamente accessibile: la limitazione di visualizzazione dei contenuti richiesta può essere ottenuta verificando, anche nel caso delle pagine base, il numero di visualizzazioni già effettuate: la tabella *visualizzazioni* del database progettato al punto (2) della prima parte comprende tutte le informazioni necessarie per implementare questa politica di limitazione.

- III. Il linguaggio SQL consente di assegnare ad un utente di un database gestito da un DBMS uno o più privilegi – generali, o relativi a specifici oggetti (tabelle, procedure, ...) – tra i seguenti:

Privilegio	Descrizione
CREATE	permette all’utente di creare un oggetto specifico nel database
CREATE ANY	permette all’utente di creare un qualsiasi oggetto nel database
ALTER	permette all’utente di modificare la struttura di un oggetto specifico nel database
ALTER ANY	permette all’utente di modificare la struttura di un qualsiasi oggetto nel database
DROP	permette all’utente di eliminare un oggetto dal database
DROP ANY	permette all’utente di eliminare un qualsiasi oggetto dal database
SELECT	permette all’utente di leggere i dati di una specifica tabella
INSERT	permette all’utente di aggiungere i dati a una specifica tabella
UPDATE	permette all’utente di modificare i dati di una specifica tabella
DELETE	permette all’utente di eliminare i dati di una specifica tabella
EXECUTE	permette all’utente di eseguire una specifica <i>stored procedure</i>

È anche possibile creare dei “ruoli” definiti da un insieme di privilegi ed assegnare agli utenti i ruoli così creati.

Ad esempio se nel database della segreteria scolastica è presente una tabella *Alumni* contenente dati relativi agli alunni ed una tabella *Docenti* contenente dati relativi ai docenti è possibile creare i seguenti ruoli:

```
CREATE ROLE segreteria_alunni;  
GRANT SELECT ON Alunni TO segreteria_alunni;  
GRANT INSERT ON Alunni TO segreteria_alunni;  
GRANT UPDATE ON Alunni TO segreteria_alunni;  
GRANT DELETE ON Alunni TO segreteria_alunni;  
CREATE ROLE segreteria_docenti;
```

```
CREATE ROLE segreteria_docenti;  
GRANT SELECT ON Docenti TO segreteria_docenti;  
GRANT INSERT ON Docenti TO segreteria_docenti;  
GRANT UPDATE ON Docenti TO segreteria_docenti;  
GRANT DELETE ON Docenti TO segreteria_docenti;
```

Nell'ipotesi che gli utenti del DBMS Mario e Maria lavorino rispettivamente nella segreteria docenti e nella segreteria alunni è possibile assegnare loro i rispettivi ruoli:

```
GRANT segreteria_docenti TO Mario;  
GRANT segreteria_alunni TO Maria;
```

È preferibile riservare i privilegi di sistema (CREATE, ALTER e DROP) all'amministratore del DBMS (utente DBA).

IV. Le principali tecnologie di comunicazione che consentono la realizzazione di una WAN aziendale tra sedi remote sono le seguenti:

- *leased-line* (E1/E3);
- *frame-relay* e ATM;
- Internet VPN (*Virtual Private Network*) con accesso cablato (DSL, FTTB/FTTH) o wireless (LTE).

Il ricorso alla tecnologia VPN è il più pratico ed economico anche se limitato in termini di prestazioni (tempi di risposta, banda disponibile). Il protocollo standard più utilizzato per la realizzazione di Internet VPN è IPsec:

- nella modalità "tunnel" viene impiegato per connettere in modo sicuro (riservato e autenticato) i router che interfacciano la rete LAN di diverse sedi aziendali alla rete Internet (VPN *site-to-site*);
- nella modalità "trasparente" viene impiegato per connettere in modo sicuro (riservato e autenticato) attraverso la rete Internet due computer, normalmente un server aziendale con un client esterno alla rete aziendale (VPN *end-to-end*).

Per la realizzazione di VPN *end-to-end* è molto utilizzato il software openVPN che realizza una VPN a livello di trasporto, anziché a livello di rete.

Nel caso di studio proposto le due sedi aziendali dovrebbero essere connesse mediante una VPN IPsec *site-to-site* configurata sui router che interfacciano le LAN aziendali alla rete Internet: utilizzando la modalità tunnel del protocollo IPsec è possibile unificare le due LAN aziendali in un'unica rete IP; gli agenti sul territorio possono accedere ai server aziendali mediante una VPN realizzata con openVPN installando lo specifico software client sul proprio PC:

