A.S. 2015-2016

ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITIA - INFORMATICA E TELECOMUNICAZIONI
ARTICOLAZIONE INFORMATICA

Tema di: SISTEMI E RETI - ***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

Una scuola superiore con 1000 studenti è ospitata in un moderno edificio a due piani.

Negli uffici di segreteria e presidenza, situati al piano terra, ci sono 15 postazioni di lavoro fisse connesse da un'infrastruttura di rete Ethernet con apparati a 100 Mb/s. Questa rete, d'ora in poi denominata "rete amministrativa", è collegata ad Internet attraverso una linea ADSL a 7 Mb/s.

I computer presenti nei 10 laboratori didattici e le altre postazioni fisse a disposizione dei docenti sono anch'essi collegati tramite una seconda rete Ethernet (d'ora in poi denominata "rete didattica") con apparati a 100 Mb/s; la rete didattica è totalmente separata da quella amministrativa e si connette alla rete Internet mediante una seconda linea ADSL a 24 Mb/s. L'attuale separazione fisica delle due reti garantisce che le informazioni trattate all'interno della rete amministrativa non siano accessibili dalla rete didattica.

La scuola ha esigenze crescenti di servizi di rete, sia per quanto riguarda l'attività amministrativa (che sempre più viene svolta su portali esterni ministeriali e privati come per il registro elettronico), sia per quanto riguarda la didattica innovativa e multimediale. Per questo motivo la scuola intende aggiornare la sua infrastruttura al fine di conseguire i seguenti obiettivi:

a) sostituire, per l'accesso ordinario ad Internet, le due linee ADSL con un'unica linea più performante, per connettere alla rete globale sia la rete didattica che quella amministrativa, pur continuando a mantenere separato il traffico delle due reti; si decide comunque di mantenere con altro scopo una delle due linee ADSL preesistenti, per disporre di una linea di riserva da utilizzare in caso di malfunzionamenti sulla nuova connessione Internet unica;

b) aumentare la banda disponibile per i computer presenti nei laboratori didattici e dei docenti;

c) offrire una piattaforma interna per la didattica multimediale e per servizi in streaming, accessibile sia dalla rete locale interna alla scuola che tramite Internet;

d) garantire la sicurezza della rete interna da possibili minacce, sia interne che esterne.

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

1. rappresenti graficamente uno schema logico dell'infrastruttura di rete esistente;

2. proponga un progetto anche grafico per l'evoluzione di tale infrastruttura, che soddisfi le esigenze sopra esplicitate, indicando le risorse hardware e software necessarie; approfondisca in particolare le caratteristiche della nuova connessione Internet, i meccanismi per mantenere la separazione del traffico tra le due reti interne, la migrazione degli apparati, gli strumenti di sicurezza, la gestione della linea ADSL di riserva;

3. proponga i principali servizi da implementare, esemplificando le relative configurazioni per uno di essi a sua scelta;

4. specifichi le misure necessarie a prevenire possibili interruzioni nel servizio della piattaforma multimediale

SECONDA PARTE

1. In relazione al tema proposto nella prima parte, la scuola intende sviluppare per le classi quinte una didattica basata sul principio del BYOD (Bring Your Own Device), che consiste nell'utilizzo in classe dei dispositivi mobili degli studenti (smartphone, tablet, Pc portatili, …) per la didattica ordinaria, con accesso ad Internet.
   Il candidato integri opportunamente il progetto, evidenziando in particolare:
   - l'hardware e i servizi necessari all'implementazione di tale infrastruttura;
   - le modalità di limitazione dell'accesso a docenti e studenti delle quinte;
   - le problematiche che si potrebbero presentare e le possibili soluzioni.

2. In relazione al tema proposto nella prima parte, si immagini di volere gestire sul server Web un sistema di semplici news interne alla scuola, caratterizzate da un autore, un titolo, un contenuto testuale, un possibile contenuto multimediale e una data di inserimento, che potranno essere inserite dai membri del comitato di redazione.
   Il candidato progetti lo schema concettuale e logico della porzione della base di dati necessaria alla gestione delle news. Progetti poi le pagine Web per la visualizzazione dei dati relativi ad uno specifico articolo, e ne codifichi in un linguaggio a sua scelta una parte significativa.

3. Vista la crescente quantità di informazioni che transitano sulla rete Internet, le tecniche che consentono di garantire la riservatezza delle comunicazioni rivestono sempre maggiore importanza.
   A tale proposito il candidato esponga le caratteristiche principali della crittografia simmetrica e asimmetrica e le loro modalità di impiego.

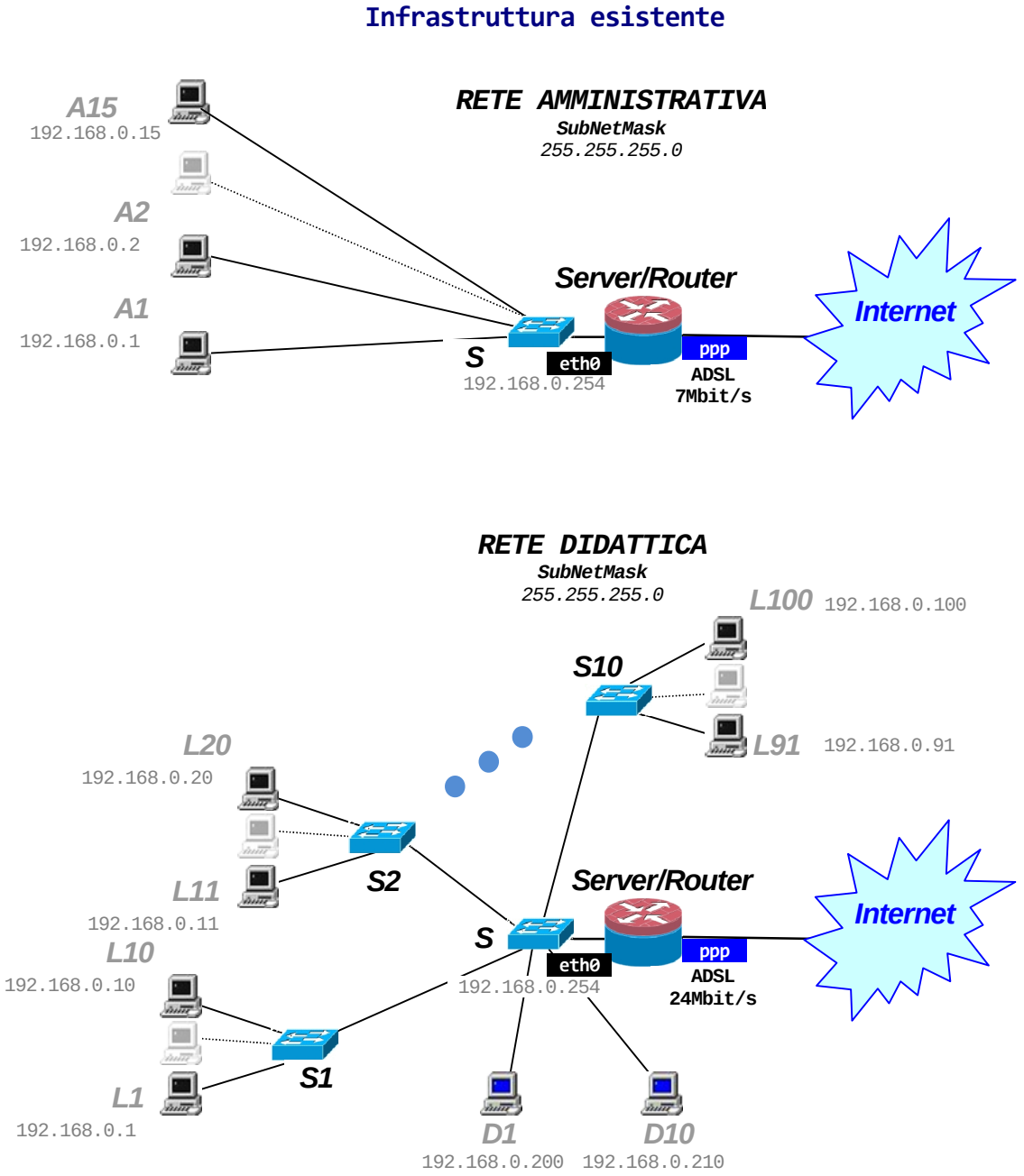
4. Le società che possiedono più sedi, o che hanno personale che opera in trasferta, necessitano di tecnologie idonee ad uno scambio dati in tempo reale ma al tempo stesso sicuro.
   Si espongano le possibili soluzioni che rispondono a questo tipo di esigenza, discutendone in dettaglio le caratteristiche a livello di protocolli.

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.

SOLUZIONE

PRIMA PARTE Quesito 1

In base ai dati del testo l'infrastruttura della rete esistente risulta schematizzabile dal seguente grafico funzionale:

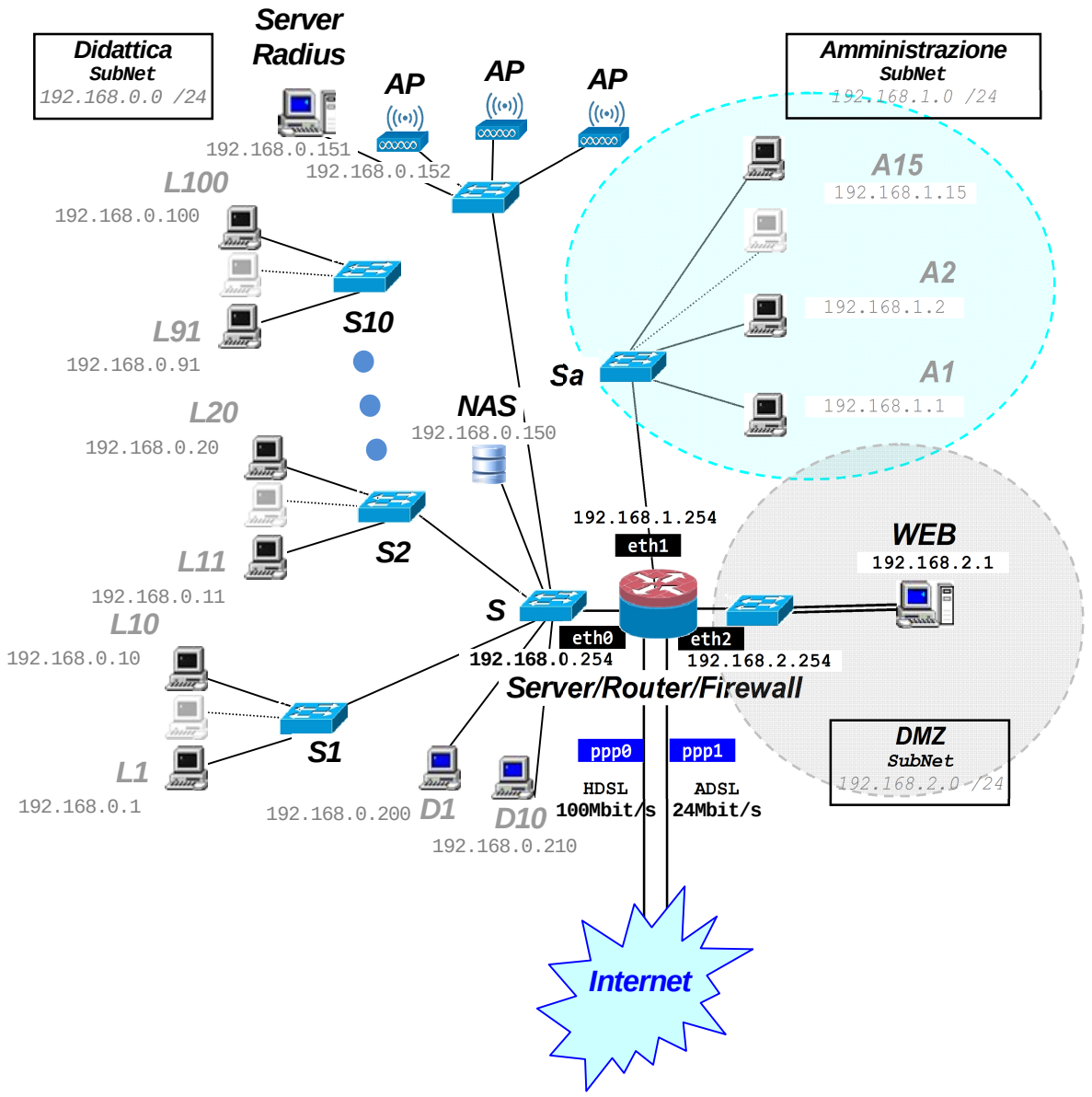


Nella **Rete Amministrativa** sono collocate le 15 stazioni (A1, ..., A15), tutte connesse ad un unico Switch S.
Nella **Rete Didattica** si ipotizza che in ogni laboratorio siano presenti 10 Personal Computer connessi a 10 Switch (L1,.., L100 PC nei Laboratori) e 10 postazioni per i Docenti (D1, ..., D10).
Per entrambe le reti si è ipotizzata una struttura semplice, con una sola subnet e con piani di indirizzamento sul gruppo privato di indirizzi 192.168.0.0.

PRIMA PARTE Quesito 2

In base ai dati del testo l'infrastruttura della nuova rete risulta schematizzabile dal seguente grafico funzionale:

Nuova Infrastruttura



La **Nuova Infrastruttura** si compone di tre subnet (**Didattica**, **Amministrazione**, **DMZ**) per separare i flussi di dati.
Le due subnet Didattica e Amministrazione sono di tipo **Trust** (sicure).
La subnet DMZ è necessaria per esporre i servizi pubblici previsti dal testo (sito con servizi streaming, news,...) tramite un **server WEB**.
La LAN viene configurata tramite **Dominio** (Active Directory o SAMBA), con almeno quattro gruppi di utenze: Amministratori, Amministrativi, Docenti, Studenti.
Per garantire una maggiore tolleranza ai guasti si prevede un secondo server di Dominio (assente nello schema) oltre al server di Dominio collocato su **Server/Router/Firewall**.

Sono previsti inoltre un **NAS** (per il backup del dominio, compreso il backup del server WEB) e un **server RADIUS** per l'autenticazione dei dispositivi mobili tramite i tre Access Point (tramite database LDAP fornito dal Dominio), che garantiscono il servizio **BYOD** richiesto su tre classi quinte.
Verso Internet è prevista una nuova connessione (su **ppp0**) HDSL 100 Mbit/s e viene conservata la preesistente linea (su **ppp1**) ADSL 24Mbit/s utilizzata come backup e configurata in **failover** sul Server.

La LAN viene potenziata attraverso l'adozione di cablaggi e switch managed da 1Gbit/s (**GigaEthernet**), quindi i vecchi apparati a 100Mbit/s non possono migrare con efficienza.
Le dorsali vengono 'raddoppiate' in banda utilizzando **Link Adapter** tra gli switch, così come i collegamenti NAS, Server Radius e tutti quelli che fanno capo al **Server/Router/Firewall.**

PRIMA PARTE Quesito 3

La rete descritta necessita dei seguenti servizi generali:

1. Servizio **DHCP** per la configurazione automatica degli host
2. Servizio di autenticazione utenti della LAN (protocollo **SMB e LDAP**)
3. Servizio **DNS** privato per la risoluzione dei nomi degli host della rete Trust
4. Servizio **NAT/PAT** per la partecipazione degli host della rete Trust su rete pubblica (NB)
5. Servizio di **Firewall** per il controllo dei flussi e la sicurezza

A questi servizi generali vanno aggiunti quelli richiesti dal testo:

6. Servizio **Web Server** (per i servizi pubblici esposti)
7. Servizio **Database Server** (per la gestione delle News e servizi di Didattica multimediale)

Quindi, in aggiunta va previsto:

8. Servizio **DNAT** per 'pubblicare' su Internet il sito interno

Eventualmente può essere prevista l'adozione del protocollo (e relativo servizio)

9. **HTTPS** per garantire l'autenticazione del sito presso i client Internet

NB. In alternativa al servizio NAT si può utilizzare un servizio Proxy

Per quanto riguarda la gestione della sicurezza, si individuano i servizi:

a. per l'accesso (interno) alla rete WiFi, il protocollo **WPA2** modalità personal (ovvero WPA2 modalità Enterprise tramite server RADIUS (o DIAMETER)
b. il protocollo **Kerberos** per l'autenticazione delle utenze interne sul Dominio (SMB o SAMBA)
c. Modello TRUST/DMZ con protezione **Firewall** per il controllo degli accessi dall'esterno

1. SERVIZIO DHCP

Il client **DHCP** è attivo su ogni macchina automaticamente.
Il server DHCP può essere collocato sulla macchina Server/Router/Firewall (o una qualsiasi macchina della rete Trust, ma sempre accesa, quindi un server).
Il server DHCP deve essere configurato in modo tale che, ad esempio per la subnet **Didattica**:

```
option subnet-mask: 255.255.255.0
option router:            192.168.0.254
option domain-server:     192.168.0.254 (NB)
range:              192.168.0.1 192.168.0.200
lease:              21000
```

NB. Si da' per attivo il server DNS interno sulla macchina Server/Router/Firewall

Eventualmente si possono 'prenotare' con attribuzione statica sia l'indirizzo della macchina Server/Router/Firewall (192.168.0.254), del dispositivo NAS (192.168.0.150), del Server RADIUS (192.168.0.151) e degli Access Point (192.168.0.152,...)

Esempio per Server/Router/Firewall su **eth0**:

```
host server:        fixed 192.168.0.254 MAC: 00:06:5B:66:33:6F
ecc…
```

2. SERVIZIO DI AUTENTICAZIONE

Il sistema a **Dominio**, con nome di dominio "**Itis-Pr**", è la radice dello schema **LDAP**.

Il server di dominio è individuato nella macchina Server/Router/Firewall. In questo caso la rete soffre di un problema di **single point of failure** sulla macchina Server/Router/Firewall. In alternativa si può prevedere un secondo server di dominio su una macchina della rete Trust
I vari host andranno inseriti nel dominio da parte delle utenze amministrative ipotizzate.
Una volta inserito l'host nel dominio, la parte client di SMB (SAMBA) per reti a dominio viene attivata automaticamente (p. es., la richiesta di login all'avvio).

3. SERVIZIO DNS (interno)

Il servizio DHCP provvede a popolare la tabella dei record DNS automaticamente di tutti i **record A** necessari per la risoluzione dei nomi interni, a partire dal nome del server DNS stesso.
Esempi di record A:

```
ns      A       192.168.0.254
L1      A       192.168.0.1
L2      A       192.168.0.2
...     ...     ...
```

Andranno anche specificati nella configurazione il **nome di dominio** della rete e la durata della **cache DNS**
I nomi qualificati degli host saranno quindi: Itis-Pr.L1, Itis-Pr.L2, ecc...

```
$TTL   20000
Itis-Pr      NS     ns
```

4. NAT/PAT

La parte client di NAT/PAT sugli host non esiste, perchè il servizio è trasparente agli host.
Il processo quindi va configurato sulla macchina Server/Router/Firewall, ovvero l'unica che ha una interfaccia sulla rete pubblica. Il servizio va abilitato associando ogni subnet interessata al servizio, ad una interfaccia pubblica.
Nel nostro caso si associa la subnet Didattica 192.168.0.0 (/24) su **eth0** e la la subnet Amministrazione 192.168.1.0 (/24) su **eth1** all'unica interfaccia **ppp0** del Server/Router/Firewall (**ppp1** è in *failover*, ovvero in alternativa).

5. FIREWALL

Il servizio di Firewall va attivato sulla macchina Server/Router/Firewall e deve prima di tutto garantire la protezione dagli accessi non autorizzati provenienti dalla rete pubblica. Data la natura istituzionale della rete è necessario utilizzare un Firewall in grado di fare **deep ispection** con black list autoaggiornate dalla casa madre.
Una **ACL** impostabile potrebbe essere la seguente:

	IN	OUT	IPs	IPd	P	sP	dP	azione
1	ppp0	eth2	*	*	TCP	*	80	permit
2	ppp0	eth2	*	*	TCP	*	443	permit
3	ppp0	eth*	*	*	UDP	53	53	permit
4	eth0	ppp0	*	*	TCP	*	80	permit
5	eth0	ppp0	*	*	TCP	*	443	permit
6	eth0	ppp0	*	*	UDP	53	53	permit
7	eth1	eth2	*	*	*	*	*	deny
...								
n	*	*	*	*	*	*	*	deny

La ACE 1 consente alla WAN di connettersi al Web Server in HTTP (eventualmente specificare IPd)
La ACE 2 consente alla WAN di connettersi al Web Server in HTTPS (eventualmente specificare IPd)
La ACE 3 consente alla WAN di utilizzare DNS pubblico
Le ACE 4,5,6 consentono i rispettivi servizi dall'interno verso l'esterno (su subnet **Didattica**). Da ripetersi per subnet **Amministrazione**.
La ACE 7, ad esempio, evita che la subnet **Amministrazione** acceda alla **DMZ**.
La ACE n indica che tutti gli altri flussi sono negati.

Si ricorda che la navigazione delle macchine in Trust avviene tramite la porta ppp0 del Server/Router/Firewall via NAT.

PRIMA PARTE Quesito 4

Le possibili interruzioni del servizio per la piattaforma multimediale, che viene realizzata sulla macchina WEB in DMZ (dovendo essere accessibile dalla rete pubblica) riguardano principalmente:

a. **Blocco della macchina** server (WEB)
b. **Blocco della connessione** Internet

Nel primo caso si prevede un ripristino efficiente tramite copia salvata su NAS (es., se il server WEB è virtualizzato).

Nel secondo caso la contromisura consiste nella seconda linea pubblica (su **ppp1**) configurata in **failover**.
In questo caso sarebbe opportuno che il fornitore di connettività NON sia il medesimo che offre la connessione principale (su **ppp0**), per evitare che un eventuale blocco del fornitore interrompa entrambe le connessioni.

SECONDA PARTE Quesito 1

La realizzazione di una infrastruttura per gestire dispositivi mobili, in questo caso per didattica BYOD (*Bring Your Own Device*) può implicare alcune problematiche che non si pongono laddove la gestione di una rete WiFi è semplicemente residenziale (es., casalinga).

Il problema maggiore riguarda l'**autenticazione** (e quindi la sicurezza) dei dispositivi.
Per una rete WiFi residenziale è sufficiente una autenticazione di tipo WiFi **Personal** (tramite PSK, volgarmente la *password* di rete).
In ambito pubblico (aziendale o istituzionale) ciò non è sufficiente, dato che la PSK, essendo condivisa, non rimane segreta per utenti eterogenei.
E' quindi necessario realizzare un sistema di autenticazione WiFi di tipo **Enterprise**, ovvero tramite un server dedicato (es., un server RADIUS/DIAMETER) che consente l'accesso agli utenti utilizzando gli account della rete a Dominio.
Entrambe le modalità utilizzano **WPA2** come sistema di autenticazione wireless, ma l'uso di un sistema Enterprise garantisce anche l'autenticazione per singolo utente, e quindi anche per gruppi di utenze.

Proprio sfruttando opportune politiche sui **gruppi di utenze** (es., Docenti, Studenti, ma anche gruppi per singole classi, come le classi quinte indicate nel testo), si possono impostare limitazioni adeguate.

Una soluzione alternativa consiste nell'impostare sul server di autenticazione gruppi estranei al Dominio, per esempio generati dalla piattaforma **Google Apps for Education** (es. Classroom), in modo da poter usufruire anche dei servizi di didattica offerti dal portale.

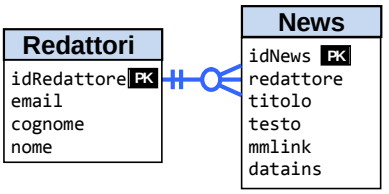
SECONDA PARTE Quesito 2

Per la realtà d'interesse identifichiamo le due entità “News” e “Redattori” tra le quali troviamo 1'associazione “inserisce” di tipo 1/N , per cui il modello concettuale può essere il seguente:

Diagramma E/R

Il modello logico che ne deriva è formato (almeno) dalle 2 tabelle di seguito elencate:

Diagramma Logico



da cui il modello fisico su database:

```
CREATE TABLE Redattori (
  idRedattore INT(11) NOT NULL AUTO_INCREMENT,
  email VARCHAR(50),
  cognome VARCHAR(30),
  nome VARCHAR(30),
  PRIMARY KEY (idRedattore) )

CREATE TABLE News (
  idNews INT(11) NOT NULL AUTO_INCREMENT,
  redattore INT(11),
  titolo VARCHAR(30) NOT NULL,
  testo VARCHAR(1024) NOT NULL,
  mmlink VARCHAR(50),
  datains (DATE),
  PRIMARY KEY (idNews)
  FOREIGN KEY (redattore) REFERENCES redattori(idRedattore) )
```

Dopo gli opportuni accessi si avrà disponibile una pagina web con il semplice elenco degli articoli consultabili da cui poi accedere ai singoli contenuti; al netto delle parti inerenti la gestione degli errori, la sicurezza della navigazione e le varie funzionalità tipiche, la porzione di codice per la semplice consultazione delle news può essere la seguente:

news.php

```
<html>
<head>
<title> Ultime notizie </title>
<link rel="stylesheet" href="news.css" type="text/css">
<?php
      $connect = mysql_connect("DBserver", "DBuser", "DBpsw") or die;
      $giornomin = date()-10;
      $comandoSQL = "SELECT * FROM news INNER JOIN Redattori
                        ON  News.redattore = Redattori.idRedattore
                        WHERE datains >='" . $giornomin . "'";
      $risultatoRicercaNews = mysql_query($comandoSQL);
?>
</head>
<body>
<p>Lista news</p>
<?php
if (mysql_num_rows($risultatoRicercaNews) != 0) {
echo "<TABLE>"
echo "<TR>";
echo "<TD>Autore</TD> <TD>Data</TD> <TD>Titolo</TD>;
echo "</TR>";
while ($row = mysql_fetch_array($risultatoRicercaNews)) {
echo "<TR>";
echo "<TD>" . $row["cognome"] . "</TD>";
echo "<TD>" . $row["datains"] . "</TD>";
echo "<TD> <A HREF='dettaglio.php?cod=" . $row["idNews"] . "'>" .
                                    $row["titolo"]. "</A></TD>";
echo "</TR>";
}
echo "</TABLE>"
}
?>
</body>
</html>
```

SECONDA PARTE Quesito 3

La crittografia si applica su un messaggio 'in chiaro' per ottenere un testo 'cifrato' e quindi la segretezza dell'informazione contenuta nel messaggio (tramite cifratura).
Una volta ricevuto il messaggio cifrato, un utente può riottenere il testo 'in chiaro' (il messaggio) applicando la decifratura.

Nel caso della **crittografia simmetrica**, la decifratura si ottiene solo se si possiede la chiave (key) utilizzata per cifrare il messaggio.
La cifratura simmetrica risente del problema dello **scambio della chiave**: mittente e destinatario devono condividere il segreto della chiave, e questo espone il sistema ad una debolezza strutturale (la chiave VA scambiata).
In compenso la cifratura simmetrica è un sistema estremamente veloce ed efficiente per garantire la sicurezza, utilizzata quindi per messaggi di grandi dimensioni o messaggi da gestire in tempo reale (es., messaggi in rete).

La **crittografia asimmetrica**, in questo senso, è duale alla crittografia simmetrica: **non soffre** del problema dello scambio della chiave, ma **non è efficiente** in termini di prestazioni di cifratura e decifratura.
L'uso delle due chiavi (pubblica, per cifrare, privata per decifrare) consente il segreto sostanziale della chiave (quella privata, che NON si scambia mai). Ma l'algoritmo di cifratura (e di decifratura) risulta troppo lento.

La soluzione ideale consiste nel risolvere il problema dello scambio della chiave (simmetrica) attraverso la crittografia asimmetrica (in fondo una chiave è un messaggio breve); una volta scambiata la chiave simmetrica tramite cifratura asimmetrica, ai può utilizzare la crittografia simmetrica per lo scambio sicuro e segreto dei dati.

La crittografia asimmetrica, inoltre, consente di **autenticare** un messaggio: usata 'al contrario' (chi si vuol far autenticare cifra il messaggio con la propria chiave privata), consente al destinatario di verificare l'identità del mittente (decifrando con la chiave pubblica del mittente).

SECONDA PARTE Quesito 4

Per ottenere un servizio pubblico di scambio dati privati (cioè dati e informazioni appartenenti ad una organizzazione, società, istituzione, azienda, ...) la soluzione ideale risulta rendere l'Intranet privata (ovvero tutti i servizi aziendali) accessibile da remoto, per esempio tramite **VPN**.
L'accesso alla rete aziendale tramite VPN consente a un utente aziendale 'mobile' di operare sui servizi interni come se fosse connesso in locale.

In questo caso diventa cruciale la questione della sicurezza, dato che informazioni nativamente private (della Intranet locale) devono per forza di cose circolare su rete pubblica.
VPN affronta questo problema tramite il protocollo tunnel **IPSec**.
IPSec garantisce:

1. **Autenticazione simmetrica** (dei client VPN e del server VPN aziendale) tramite lo scambio di chiavi di Diffie-Helmann (sottoprotocollo **IKE**).
2. **Integrità e segretezza** tramite sottoprotocollo **ESP**.

Da notare che IPSec non necessità di autenticazione tramite Certificato Digitale perché il servizio non è pubblico (ma riservato agli utenti della VPN dotati di account privati).

Testi di:

prof. Paolo Ollari
prof. Francesc'Antonio Franco
prof. Alberto Paganuzzi

ITIS "L. Da Vinci", Parma