A.S. 2007-2008

Testo Esame di Stato 2007-2008

YABC – ESAME DI STATO DI ISTITUTO TECNICO INDUSTRIALE

CORSO SPERIMENTALE – PROGETTO «ABACUS»
Indirizzo: INFORMATICA

Tema di: SISTEMI DI ELABORAZIONE E TRASMISSIONE DELLE INFORMAZIONI

Il proprietario di una catena di supermercati intende aprire dieci nuovi punti vendita.

La sede centrale comprende uffici e due magazzini collegati mediante una rete locale.

Ciascun punto vendita dovrà disporre di un magazzino attiguo per lo stoccaggio delle merci; l'approvvigionamento verrà effettuato con richieste dirette alla sede centrale.

Gli uffici si occupano dei rapporti con i punti vendita e con i magazzini (verifica delle giacenze, evasione degli ordini, ...). La base di dati deve consentire la memorizzazione delle informazioni relative alle vendite e agli ordini dei prodotti dei vari punti vendita, che devono potersi interfacciare con la sede centrale; allo stesso modo i clienti devono poter visualizzare i cataloghi dei prodotti e i corrispondenti listini per poter eventualmente acquistare via Web.

Il candidato, fatte le opportune ipotesi aggiuntive:

1. proponga uno schema generale del sistema che metta in evidenza le diverse funzioni;
2. scelga la tipologia di rete che ritiene più idonea, ne indichi le sue caratteristiche e progetti in dettaglio alcune sue parti;
3. analizzi e progetti uno schema concettuale e il corrispondente schema logico del data base della sede centrale;
4. proponga una soluzione per la gestione via Web dell'interfaccia con i punti vendita al dettaglio, oppure, a scelta, con i clienti;
5. illustri le metodologie di collaudo;
6. effettui un'analisi massima dei costi.

Durata massima della prova: 6 ore.
È consentito soltanto l'uso di manuali tecnici e di calcolatrici tascabili non programmabili.
Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

SOLUZIONE

Premessa e ipotesi aggiuntive

L'analisi del testo contiene una richiesta implicita che aggiunge una caratteristica a una tipica organizzazione di rete isolata privata con interfaccia pubblica: la connessione di host remoti alla LAN isolata, i «dieci punti vendita». Questi dieci host, per come sono descritti, devono usufruire dei servizi standard della rete isolata privata, ma non si trovano all'interno della rete privata. La soluzione obbligata è la gestione di una **VPN** (Virtual Private Network) che consenta ai dieci punti vendita di accedere alla LAN privata attraverso la rete pubblica.

Un'altra parte del testo che non è del tutto implementabile in questa sede riguarda la richiesta 6. A questo quesito sarà risposto in termine meno generico possibile, dato che l'analisi dei costi non è un argomento specificatamente trattato nel programma scolastico.

Siccome poi non sono richiesti specifici Servizi di rete relativi all'organizzazione descritta, saranno indicati solo quelli ritenuti necessari (scartando, per esempio, un servizio di posta elettronica gestito internamente).

Per sufficiente genericità si decide di riferirsi al progetto prescindendo dal sistema operativo server adottato, ovvero dal sistema operativo che gestisce utenti, routing e servizi. Per quanto possibile si daranno indicazioni circa entrambi i sistemi operativi più diffusi, Microsoft Windows Server (2000/2003 e successivi) e Linux.

Per quanto assunto sia dal testo sia dalle ipotesi aggiuntive, nella sede centrale verrà adottato un modello di rete comprendente una rete locale isolata (TRUST), una rete locale perimetrale (DMZ) e una porzione di rete pubblica (INTERNET) servita da un collegamento HDSL flat a 1Mbit/s in ingresso e in uscita, con tre indirizzi pubblici rilasciati dall'ISP (per esempio, 82.13.0.1, 82.13.0.2, 82.13.0.3).

Si ipotizzano presenti sulla rete TRUST gli uffici (per esempio, 5) e i due magazzini.

Si ipotizzano sulla rete DMZ un server Web e, su tutte tre le reti un server router **R** che ospiterà il server VPN.

Su ogni punto vendita si prevede una LAN con un'interfaccia su rete pubblica di tipo ADSL (con IP su rete pubblica dinamico), un router con client VPN, Internet e LAN (collocato nel punto vendita) e un host collocato sulla LAN (magazzino del punto vendita).

Progettazione Livelli 1 e 2 OSI

`Sede centrale`

Per quanto riguarda la rete TRUST, vengono immessi in questa rete un totale di 5 + 2 = 7 host (uffici e magazzini).

Il livello Fisico e Dati (OSI 1 e 2) delle connessioni viene realizzato in tecnologia Ethernet 802.3u (FastEthernet 10/100/1Gb/s) secondo il modello di rete a stella «switched».

Nessun dato prevede tratte superiori ai 90 m classici per la portata del mezzo 100BaseT, quindi nessuna assunzione particolare viene fatta in merito.

È sufficiente un dominio di collisione e quindi un solo switch a 16 o 24 porte (considerando che a esso dovrà connettersi anche il router **R** ed eventuali macchine temporanee come portatili o eventuali access point per WI-FI in questo caso non considerati come necessari).

Per quanto riguarda la rete DMZ, la scelta ricade di nuovo su Ethernet 802.3u, con un solo switch a 8 porte. Su questa rete, accessibile pubblicamente, saranno disposte la macchina router e quella server Web.

La porzione di rete pubblica INTERNET invece è costituita da uno switch/router HDSL a 8 porte, che riceve in ingresso dalla rete pubblica geografica il segnale DSL con le caratteristiche offerte dal provider (ISP) e sul quale si collocheranno il router **R** e il server Web.

Tutti questi apparati di livello 1-2 (due switch e il router) potrebbero essere installati in uno stesso armadio di commutazione dotato di gruppo di continuità e quanto necessario, se le distanze materiali tra la sezione TRUST sono inferiori ai classici 90 m supportati da Ethernet XBaseT.

Lan remota (un Ufficio vendite qualsiasi)

In questo caso è sufficiente un solo switch (per esempio a 8 porte), sempre su tecnologia Ethernet 802.3u su cui collocare il server VPN (punto vendita), l'host (magazzino) e il modem ADSL.

Come prima, il tutto potrebbe essere inglobato in apposito armadio dotato di gruppo di continuità e quant'altro.

Progettazione Livello 3 OSI e Servizi di rete

Le interconnessioni delle tre reti previste dal progetto, TRUST, DMZ e INTERNET, compresa la VPN, avviene con un router **R** opportunamente dislocato.

Per semplicità consideriamo un router costituito da un elaboratore PC con tre interfacce fisiche di rete: una sulla rete TRUST, una sulla rete DMZ, una verso la rete INTERNET.

Il modello di riferimento per il livello 3 è IP dello stack TCP/IP della rete omonima.

I Servizi di rete necessari per tale progetto sono:

- Servizio di Dominio per consentire l'accesso con autenticazione agli utenti sulla rete.
- Servizio DHCP per permettere la configurazione automatica degli host della rete TRUST.
- Servizio di Firewall, per impedire accessi dall'esterno sulla rete TRUST e accessi indesiderati sulla rete DMZ.
- Servizio di NAT, in particolare sNAT per consentire agli host della rete TRUST di accedere ai servizi pubblici standard (HTTP, POP3, SMTP, FTP, NNTP).
- Servizio di NAT, in particolare dNAT, per rendere raggiungibili dall'esterno host pubblici sulla rete DMZ.
- Servizio DNS privato per consentire la risoluzione dei nomi interna alla rete TRUST e DMZ.
- Servizio di Condivisione disco e stampanti (NBT) per consentire la condivisione di spazi disco e stampanti all'interno delle reti TRUST e DMZ.
- Servizio HTTP pubblico.
- Servizio di DNS pubblico per risolvere i nomi pubblici della rete Internet mondiale.
- Servizio **VPN** pubblico per consentire agli host remoti di diventare host sulla rete TRUST.

Tutti questi servizi saranno dislocati su macchine server individuate sulla rete.

Schema di indirizzamento (livello 3 OSI)

Dati i presupposti, si vengono a determinare due sottoreti isolate (TRUST e DMZ) su cui distribuire un pool di indirizzi. Viene deciso di usare la classe di indirizzi dedicata alle reti isolate e previste dal modello IP 192.168.0.0 e un subnetting con 4 bit per le sottoreti, sui 16 a disposizione dal modello.

In questo caso la notazione è 192.168.0.0/20 o subnet mask 255.255.240.0.

Questo modello consente 2^4 subnet differenti, ognuna con 2^{12} host indirizzabili (in realtà sarebbero $2^{12} - 2$ host indirizzabili, dato che il primo e l'ultimo indirizzo della subnet sono riservati alla subnet stessa e al broadcast).

Lo schema scelto è ridondante, dato che le subnet reali sono solo 2 (TRUST e DMZ): 14 subnet rimangono inutilizzate.

Assegniamo quindi la subnet 192.168.0.0 alla rete TRUST.

Assegniamo poi la subnet 192.168.16.0 alla rete DMZ.

La rete **TRUST** avrà a disposizione quindi gli indirizzi 192.168.0.1 – 192.168.0.255; 192.168.1.0 – 192.168.1.255; 192.168.2.0 – 192.168.2.255; ecc. fino a 192.168.15.0 – 192.168.15.254.

In totale: 254*16 = 4064 indirizzi utilizzabili.

Nome di rete: 192.168.0.0.
Nome del broadcast: 192.168.15.255.
Subnet mask: 255.255.240.0.

La rete **DMZ** avrà a disposizione quindi gli indirizzi 192.168.16.1 – 192.168.16.255; 192.168.17.0 – 192.168.17.255; 192.168.18.0 – 192.168.18.255; ecc. fino a 192.168.31.0 – 192.168.31.254.

In totale: 254*16 = 4064 indirizzi utilizzabili.

Nome di rete: 192.168.16.0.
Nome del broadcast: 192.168.31.255.
Subnet mask: 255.255.240.0.

Per quanto riguarda la VPN lato server, si decide di assegnare a ogni connessione entrante un indirizzo IP appartenente alla rete TRUST, cosicché anche gli host client adotteranno indirizzi locali appartenenti alla rete TRUST (cioè 192.168.0.0).

Anche in questo caso lo schema è ridondante, avendo a disposizione più di 4000 indirizzi utili.

Sulla **LAN remota** (punti vendita) si decide di assegnare un indirizzamento sempre appartenente al gruppo 192.168.0.0/20 con identica subnet mask ma id di sottorete 240, ovvero la rete 192.168.240.0.

Essa avrà a disposizione 4064 indirizzi, da 192.168.240.1 – 192.168.240.255; 192.168.241.0 – 192.168.241.255; ecc. fino a 192.168.255.0 – 192.168.255.254.

In totale: 254*16 = 4064 indirizzi utilizzabili.

Nome di rete: 192.168.240.0.
Nome del broadcast: 192.168.255.255.
Subnet mask: 255.255.240.0.

Dislocazione dei servizi e routing (livello 7 e 3 OSI)

Per una corretta e bilanciata dislocazione dei servizi è necessario aggiungere al progetto almeno una macchina server che faccia da PDC (Domain Controller); nel caso, prevedere il servizio anche duplicato su una seconda macchina della rete.

A questo punto si possono dislocare i servizi elencati precedentemente.

Sul server **R** saranno collocati: Routing, Firewall, NAT, eventuale Proxy e server VPN. Questo server deve:

1. fare sNAT per tutte le macchine in TRUST;
2. bloccare il traffico proveniente dall'esterno e verso la TRUST;
3. controllare il traffico proveniente dall'esterno e verso DMZ;
4. consentire il traffico tra TRUST e DMZ;
5. DNS pubblico;
6. server VPN, accettando le connessioni client VPN.

Sul server PDC sono collocati i servizi:

1. DHCP per la distribuzione delle configurazioni livello 3 degli host sulla rete TRUST.
2. Dominio, per l'autenticazione degli utenti e delle macchine.
3. DNS privato, per risolvere i nomi delle reti TRUST e DMZ.

Sul server Web devono essere collocati i servizi:

1. HTTP, per gestire il sito a servizio delle vendite su Web.
2. Server SQL.
3. Eventuale DC secondario e DNS pubblico e privato.

I servizi NBT (NetBIOS) per spazio disco e condivisioni stampanti è disponibile su tutte le macchine con opportuna impostazione dei diritti di accesso forniti dal Dominio.

Gli indirizzi IP delle interfacce delle macchine **R** e Web dovranno essere esclusi dal DHCP e impostati manualmente.

Sulla **LAN remota** possiamo adottare uno schema di rete WORKGROUP e non a dominio.

La macchina Gateway, che effettua la connessione ADSL, dovrà ospitare il server VPN e consentire l'aggregamento alla LAN centrale.

Data la scarsa numerosità degli host (due soli) si può optare per configurazioni TCP/IP statiche senza usare DHCP.

Come sopra, i servizi NBT (NetBIOS) per spazio disco e condivisioni stampanti sono disponibili su tutte le macchine con opportuna impostazione dei diritti di accesso forniti dal modello Workgroup.

Si noti come l'host di magazzino non possa associarsi alla LAN centrale. I dati in esso presenti saranno gestiti dalla macchina Gateway che si connette con la VPN.

Configurazioni di rete (livello 3 OSI)

Gli host della rete TRUST avranno la seguente configurazione, ottenuta via DHCP:

Indirizzo IP: come da schema.
Subnet mask: come da schema.
Default Gateway: indirizzo IP della macchina **R** (sulla sua interfaccia in TRUST).
DNS: indirizzo IP della macchina PDC.

Gli host della rete **DMZ** avranno la seguente configurazione (statica):

Indirizzo IP: come da schema.
Subnet mask: come da schema.
Default Gateway: indirizzo IP della macchina **R** (sulla sua interfaccia in DMZ).
DNS: indirizzo IP della macchina **R** (sulla sua interfaccia in DMZ).

Consultare lo schema per un esempio numerico, compresi gli indirizzi pubblici ottenuti dall'ISP e opportunamente distribuiti con dNAT sugli host della rete DMZ.

Per la **Rete remota** invece, avremo:

– Gateway **VPN**:

  Indirizzo IP: statico, come da schema.
  Subnet mask: come da schema.
  Default Gateway: fornito dall'ISP in fase di connessione.
  DNS: fornito dall'ISP in fase di connessione.

Indirizzo IP su interfaccia **VPN**: acquisito come da schema LAN centrale, così come gli altri parametri (Gateway e DNS).

– **Host** (magazzino):

  Indirizzo IP: statico, come da schema.
  Subnet mask: come da schema.
  Default Gateway: Indirizzo IP del router.
  DNS: Indirizzo IP del router.

Configurazione TCP/IP, Routing e Firewalling

Come esemplificazione, si riporta la configurazione e la tabella di routing di un host su Trust e del router **R** nella rete della Sede:

```
Host U1
  Indirizzo IP:        192.168.0.1
  Subnet mask:         255.255.240.0
  Gateway predefinito: 192.168.15.254
```

Indirizzo	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	192.168.15.254	192.168.0.1	1 (pacchetti stranieri)
192.168.0.0	255.255.240.0	(192.168.0.1)	192.168.0.1	1 (sulla rete di provenienza)
192.168.15.255	255.255.255.255	(192.168.0.1)	192.168.0.1	1 (broadcast di rete)

(si tralasciano il loopback e gli altri broadcast).

```
Router R
  Indirizzo IP:        192.168.15.254   (TRUST)
  Subnet mask:         255.255.240.0
  Gateway predefinito: –

  Indirizzo IP:        192.168.31.254   (DMZ)
  Subnet mask:         255.255.240.0
  Gateway predefinito: –

  Indirizzo IP:        82.13.0.1        (Internet)
  Subnet mask:         255.0.0.0
  Gateway predefinito: 82.13.0.254      (ricevuto dall'ISP)
```

Indirizzo	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	82.13.0.254	82.13.0.1	1 (pacchetti stranieri)
192.168.0.0	255.255.240.0	–	192.168.15.254	1 (sulla rete di provenienza)
192.168.16.0	255.255.240.0	–	192.168.31.254	1 (sulla rete di provenienza)
192.168.15.255	255.255.255.255	–	192.168.15.254	1 (broadcast su TRUST)
192.168.31.255	255.255.255.255	–	192.168.31.254	1 (broadcast su DMZ)

(si tralasciano il loopback e gli altri broadcast).

Sul router **R** possiamo implementare le seguenti ACL per il Firewall:

regola	permit/deny	liv 3-4	Interfaccia1	Interfaccia2	liv 5-6-7	direzione
ACL1	permit	any	192.168.15.254	192.168.31.254	eq any	in/out
ACL2	permit	tcp	192.168.15.254	82.13.0.1	eq HTTP	out
ACL3	permit	tcp	192.168.15.254	82.13.0.1	eq DNS	out
ACL4	permit	tcp	82.13.0.1	192.168.15.254	eq HTTP	out
ACL5	permit	tcp	82.13.0.1	192.168.15.254	eq DNS	out

Tutto ciò che non è permesso (permit) viene automaticamente negato (deny).

Si considera Interfaccia1 come soggetto di in/out, cioè una direzione in significa che Interfaccia1 è server (se TCP).

Commento:

ACL1 consente tutto il traffico TCP/IP tra TRUST e DMZ.
ACL2 consente tutto il traffico client HTTP da TRUST a Internet (richieste dei client TRUST).
ACL3 consente tutto il traffico client DNS da TRUST a Internet (richieste dei client TRUST).
ACL4 consente tutto il traffico server HTTP da Internet a TRUST (risposte ai client TRUST).
ACL5 consente tutto il traffico server DNS da Internet a TRUST (risposte ai client TRUST).

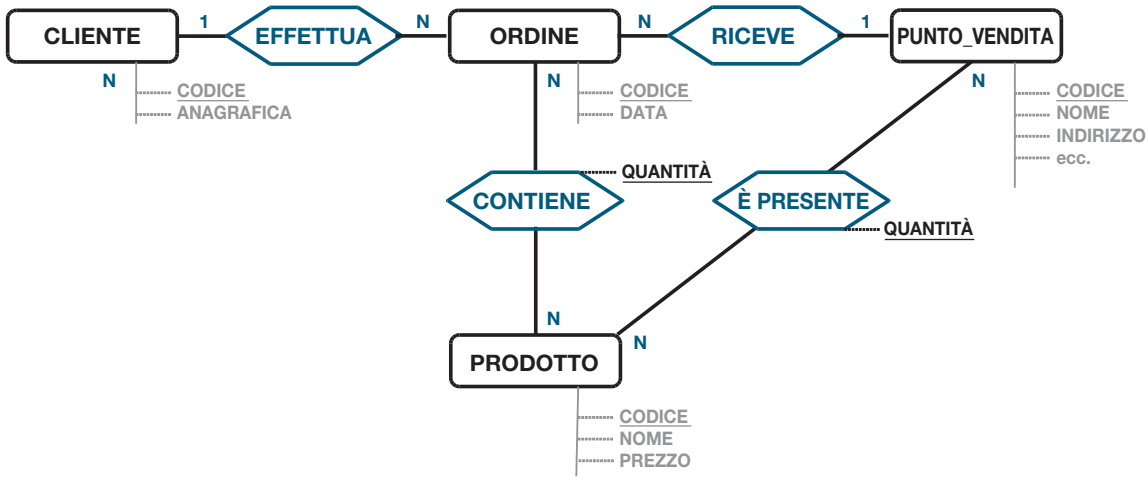
Interfaccia Web per vendita al dettaglio

Si è deciso di implementare la vendita al dettaglio tramite server Web e relativo codice HTML/ASP (o Php) sulla macchina Web della sede centrale.

Un utente di rete pubblica, accedendo a tale sito, avrà a disposizione una serie di pagine Web che lo guideranno alla consultazione dei listini e alla fase di ordine e pagamento.

La gestione della vendita effettiva, una volta ricevuto l'ordine dalla sede centrale, sarà distribuita tramite la VPN sulla sede più appropriata.

La base di dati in appoggio alla richiesta sarà sviluppata tramite server SQL installato sulla macchina Web. Lo schema di soluzione concettuale della base di dati da gestire è il seguente:



La proposta è un diagramma entità/associazioni (E/R) che realizza appunto lo schema concettuale.
Lettura dello schema:

- Un cliente effettua uno o più ordini – Un ordine è effettuato da un solo cliente (associazione 1:N).
- Un punto vendita riceve uno o più ordini – Un ordine è ricevuto in un solo punto vendita (associazione 1:N).
- Un prodotto è presente in uno o più punti vendita – In un punto vendita sono presenti uno o più prodotti (associazione N:N).
- Un ordine contiene uno o più prodotti – Un prodotto è presente in uno o più ordini (associazione N:N).

Non vengono definite parzialità o totalità delle associazioni per non appesantire il tutto.
Viene poi richiesto di passare allo schema logico equivalente (schema relazionale):

Cliente (**Codice**, anagrafica).
Ordine (**Codice**, data, evaso, ***codice_cliente***, codice_punto_vendita).
Punto_Vendita (**Codice**, nome, indirizzo).
Prodotto (**Codice**, nome, prezzo).
Contiene (***Codice_ordine, codice_prodotto***, quantità) [rappresenta le righe d'ordine].
È Presente (***Codice_punto_vendita, codice_prodotto***, quantità).

In grassetto le chiavi primarie, in grassetto corsivo le chiavi esterne.

Codice SQL e PHP

Creazione delle tabelle (script SQL):

```
CREATE TABLE 'Cliente' (
  'Codice' bigint(20) NOT NULL AUTO_INCREMENT,
  'Anagrafica' varchar(100) NOT NULL,
  PRIMARY KEY ('Codice')
) ;
CREATE TABLE 'Contiene' (
  'Codice_ordine' bigint(20) NOT NULL,
  'Codice_prodotto' bigint(20) NOT NULL,
  'Quantità' decimal(10,0) NOT NULL,
  KEY 'Codice_ordine' ('Codice_ordine','Codice_prodotto')
);
CREATE TABLE 'E_presente' (
  'Codice_punto_vendita' bigint(20) NOT NULL,
  'Codice_prodotto' bigint(20) NOT NULL,
  'Quantità' decimal(10,0) NOT NULL,
```

```
  KEY 'Codice_punto_vendita' ('Codice_punto_vendita','Codice_prodotto'),
  KEY 'Codice_prodotto' ('Codice_prodotto')
);
CREATE TABLE 'Ordine' (
  'Codice' bigint(20) NOT NULL AUTO_INCREMENT,
  'Data' date NOT NULL,
  'Evaso' char(1) NOT NULL,
  'Codice_cliente' bigint(20) NOT NULL,
  'Codice_punto_vendita' bigint(20) NOT NULL,
  PRIMARY KEY ('Codice'),
  KEY 'Codice_cliente' ('Codice_cliente','Codice_punto_vendita'),
  KEY 'Codice_punto_vendita' ('Codice_punto_vendita')
);
CREATE TABLE 'Prodotto' (
  'Codice' bigint(20) NOT NULL AUTO_INCREMENT,
  'Nome' varchar(50) NOT NULL,
  'Prezzo' decimal(10,0) NOT NULL,
  PRIMARY KEY ('Codice')
);
CREATE TABLE 'Punto_Vendita' (
  'Codice' bigint(20) NOT NULL AUTO_INCREMENT,
  'Nome' varchar(30) NOT NULL,
  'Indirizzo' varchar(100) NOT NULL,
  PRIMARY KEY ('Codice')
);
```

Codice Associazioni tra le tabelle (script SQL):

```
ALTER TABLE 'Contiene'
  ADD CONSTRAINT 'Contiene_Ordine' FOREIGN KEY ('Codice_ordine') REFERENCES 'Ordine'
('Codice');

ALTER TABLE 'E_presente'
   ADD CONSTRAINT 'E_presente_prodotto' FOREIGN KEY ('Codice_prodotto') REFERENCES
'Prodotto' ('Codice'),
  ADD CONSTRAINT 'E_presente_punto_vendita' FOREIGN KEY ('Codice_punto_vendita') RE-
FERENCES 'Punto_Vendita' ('Codice');

ALTER TABLE 'Ordine'
   ADD CONSTRAINT 'Ordine_punto_vendita' FOREIGN KEY ('Codice_punto_vendita') REFE-
RENCES 'Punto_Vendita' ('Codice'),
  ADD CONSTRAINT 'Ordine_cliente' FOREIGN KEY ('Codice_cliente') REFERENCES 'Clien-
te' ('Codice');
```

Per la gestione via Web dell'interfaccia con i punti vendita si realizza un sito Web di consultazione dei prodotti e per l'effettuazione degli ordini da parte dei clienti.

Per semplificare la trattazione presentiamo qui il codice di una pagina PHP che recupera le informazioni dal database (si ipotizza un database MySQL) e visualizza l'elenco dei prodotti.

```
<html>
<head>
<title>Visualizzazione Prodotti</title>
</head>
<body>
<?php
```

```
$host = "localhost";
$user="esame";
$password="stato";
$connect = mysql_connect($host,$user,$password) or die("Impossibile connettersi
all'host");
if(mysql_select_db("supermercati",$connect)==0)
{
 echo("Il database non esiste");
      exit;
}
$sql="SELECT * FROM Prodotto";
$result = mysql_query($sql);
if(mysql_num_rows($result)!=0)
{
 echo "<table border='1'>
      <tr> <th>Codice</th>
 <th>Nome del Prodotto</th>
 <th>Prezzo</th>
          </tr>";
          while($row = mysql_fetch_array($result))
          {
                       echo "<tr>";
  echo "<td>" . $row["Codice"] . "</td>";
  echo "<td>" . $row["Nome"] . "</td>";
  echo "<td>" . $row["Prezzo"] . "</td>";
  echo "</tr>";
            }
            echo "</table>";
}
else
 echo("Nessun Prodotto disponibile ...");
?>
</body>
</html>
```

Risposte ai quesiti

I punti 1. 2. 3. e 4. presenti nel testo sono stati affrontati nello svolgimento.

Dei punti esplicitamente ricordati, invece, rimangono esclusi:

- metodologie di collaudo;
- analisi dei costi.

Si sorvola sul collaudo dei sistemi operativi adottati, che si suppongono installati a dovere (in particolare la versione server sulle due macchine della rete principale che ospitano i Domain Controller).

Il collaudo si concentrerà soprattutto sulla correttezza dell'impostazione della rete, sia locale sia pubblica, sia nella sede centrale sia nelle sedi periferiche.

In caso di piattaforma Microsoft, il funzionamento del livello fisico è possibile anche senza aver installato applicativi e pianificato indirizzi IP, tramite i protocolli di default forniti di livello 1 e 2 dal sistema operativo.

Una volta pianificati gli indirizzi IP, si collauderà la raggiungibilità delle stazioni (comando ping) utilizzando i semplici indirizzi IP ed effettuando il collaudo da tutte le macchine significative verso tutte le macchine significative.

Quindi si verificherà la risoluzione degli indirizzi tramite DNS, prima interno poi pubblico, sempre utilizzando il comando ping (stavolta con i nomi stringa delle macchine locali e poi con url noti di rete pubblica).

Infine, con il comando tracert (o equivalente) si verificheranno i percorsi dei pacchetti per verificare gli instradamenti.

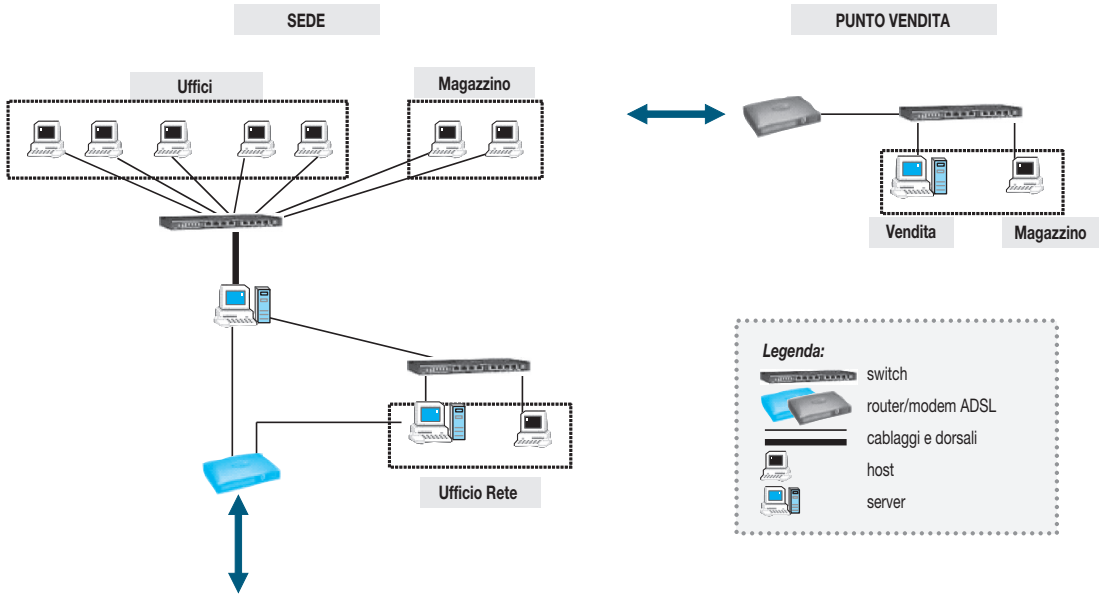
Le tabelle di routing degli host possono essere verificate con il comando route print, mentre possono essere gestite sui router (inserimento e cancellazione di regole) con le opzioni del comando route.

Per verificare il funzionamento della VPN si usa un modo analogo (comando ping) una volta che un client VPN ha accettato una connessione entrante. In questo caso il test si presenta meno agevole; sarebbe opportuno effettuarlo tramite una macchina pubblica a cui accedere, dalla rete principale, tramite un applicativo di controllo di desktop remoto.

L'analisi dei costi viene esplicitamente tralasciata, dato che non si tratta di una competenza acquisibile in sede scolastica, né prevista dai programmi curricolari.

Schemi

Schema cablaggio strutturato



Schema topologia e indirizzamento