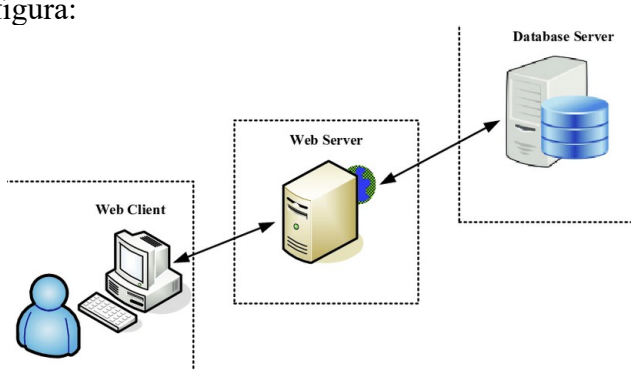
Il candidato risolva i seguenti esercizi:

1- Data la seguente figura:



si spieghi il processo di funzionamento di un web server durante la richiesta HTTP.

Client → (Richiesta) HTTP → 402 HTTP/GET "xml" → Server
Client ← (Risposta) "OK" ← Server

Risposta:

1. Il client invia una richiesta HTTP al server
   - (Esempio: Browser (Chrome / Firefox) chiede una pagina a google.com)
2. Il server analizza la richiesta attraverso
   - La porta (servizio) 80 per HTTP oppure 443 per HTTPS
3. Il server elabora la richiesta e risponde dando una pagina
   - HTML, CSS, immagini, etc. + PHP, Python, etc.
4. Il server costruisce la risposta HTTP completa di status code, header e body

Alternativamente:

Il web server opera attraverso un ciclo di request-response basato sul protocollo HTTP.

- Quando il client invia una richiesta HTTP, il server la riceve attraverso il socket di ascolto sulla porta 80 (HTTP) o 443 (HTTPS). Il server analizza l'header della richiesta per determinare il metodo (GET, POST, etc.), l'URI richiesto e i parametri.
- Successivamente, il server elabora la richiesta: se si tratta di contenuto statico (HTML, CSS, immagini), lo recupera direttamente dal filesystem; se è contenuto dinamico, invoca l'interprete appropriato (PHP, Python, etc.) o si interfaccia con il database server per generare la risposta.
- Infine, il server costruisce la risposta HTTP completa di status code, header e body, inviandola al client attraverso la connessione TCP stabilita.

2- Quali sono i principali protocolli utilizzati dai web server?
   - Parla di HTTP, HTTPS e delle loro differenze.

Risposta:

HTTP è un protocollo che manda i *dati in chiaro* (esposti), mentre HTTPS sfrutta la *crittografia asimmetrica* (=le parti della rete hanno delle loro chiavi e poi c'è anche la chiave pubblica) tramite TLS/SSL (la comunicazione è criptata subito da quando la connessione viene stabilita).

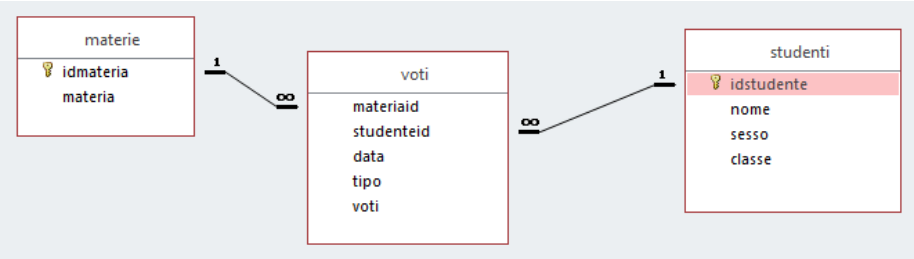
Alternativamente:

I protocolli fondamentali sono HTTP (HyperText Transfer Protocol) e HTTPS (HTTP Secure).

- HTTP è un protocollo stateless del livello applicativo che opera su TCP, tradizionalmente sulla porta 80. Definisce metodi (GET, POST, PUT, DELETE), status code (200, 404, 500) e header per il trasferimento di risorse web.
- HTTPS rappresenta l'evoluzione sicura di HTTP, operante sulla porta 443, che incapsula il traffico HTTP in un tunnel crittografato tramite TLS/SSL.

La differenza sostanziale risiede nella sicurezza: mentre HTTP trasmette dati in chiaro, HTTPS garantisce confidenzialità, integrità e autenticazione attraverso certificati digitali. HTTPS è ormai standard per applicazioni che gestiscono dati sensibili e influenza positivamente il ranking SEO.

3- Raggiungi mediante browser (http://localhost/) il *web server* installato, utilizzando il gestionale di *phpMyAdmin* crea la struttura in figura (Database Studente):



(Lo faresti tramite interfaccia grafica = Col programma in mano)

```php
// (1) Stabilire parametri di connessione
$host = "localhost"; // o l'indirizzo del tuo server DB
// host = stazione = chi si connette alla rete
$user = "tuo_username";
$password = "tua_password";
$database = "tuo_database";

// (2) Creazione della connessione
// mysqli = (i) improved = mysqli più sicuro (migliorato)
$conn = new mysqli($host, $user, $password, $database);

// (3) Controllo della connessione
// connect_error = controlla errore di connessione
if ($conn->connect_error) {
  die("Connessione al database fallita: ". $conn->connect_error);
}else{
  echo "Connessione al database riuscita!<br>";
  // Esempio di query per creare una tabella
  $create_materie_query = "CREATE TABLE IF NOT EXISTS materie (
              idmateria INT AUTO_INCREMENT PRIMARY KEY,
              materia VARCHAR(100) NOT NULL,
            );";
}
```

```php
// (4) Esempio esecuzione query
if ($conn->query($create_materie_query) === TRUE) {
  echo "Tabella 'materie' creata con successo!<br>";
} else {
  echo "Errore nella creazione della tabella: " . $conn->error . "<br>";
}

// Stesso per tabelle “voti” e “studenti”...
```

4- Crea uno script PHP con il codice lato server che consente la connessione al database Studente precedentemente creato, con messaggio all’utente di “Avvenuta connessione” o di “Connessione NON avvenuta”.

```php
<?php
// (1) Stabilire parametri di connessione
$host = "localhost";
$user = "tuo_username";
$password = "tua_password";
$database = "Studente";

// (2) Creazione della connessione
// mysqli = (i) improved = mysqli più sicuro (migliorato)
$conn = new mysqli($host, $user, $password, $database);

// (3) Controllo della connessione
// connect_error = controlla errore di connessione
if ($conn->connect_error) {
  die("Connessione NON avvenuta: ". $conn->connect_error);
}else{
  echo "Avvenuta connessione<br>";
}
```

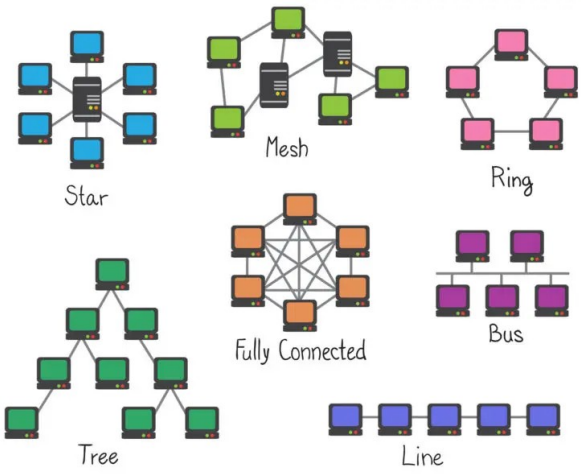
5- Progettazione di una rete LAN:

Scenario:
Immagina di dover progettare una rete LAN per un piccolo ufficio che ha 10 computer, una stampante di rete e un server. L'ufficio ha anche bisogno di accesso a Internet.

- Quale topologia della rete sceglieresti per l'ufficio e perché?
- Quali dispositivi sono necessari per costruire la rete LAN e quali sono le loro funzioni?

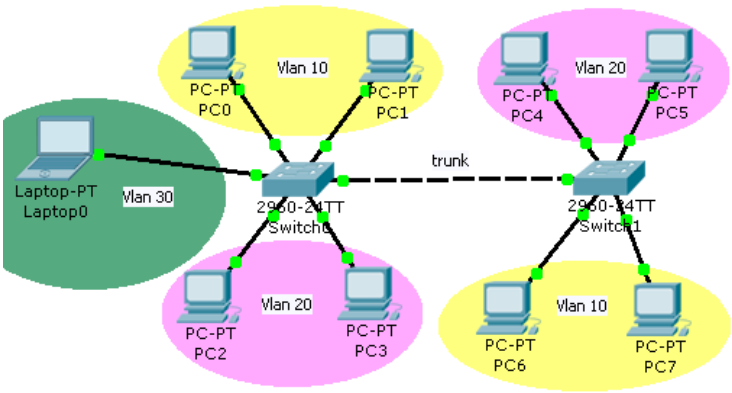
Risposta:

Topologie →
- Stella (Star)
- Albero (Tree)
- Maglia (Mesh)
- Anello (Ring)
- Maglia completamente connessa (Fully connected)



Scegliamo la topologia a stella con switch centrale.

- 10 PC
- 1 Stampante
- 1 Server



VLAN = LAN virtuali = Sei tu che decidi come frammentare gli indirizzi.

- Switch collegano le VLAN tra di loro (a titolo di esempio, 2 VLAN con 5 PC da una e 5 dall'altra)

VLAN 1: 192.168.1.1 / 128
VLAN 2: 192.168.1.129 / 255

> Questa architettura offre vantaggi significativi: isolamento dei guasti (il malfunzionamento di una workstation non compromette l'intera rete), facilità di gestione e troubleshooting, scalabilità per future espansioni, e prestazioni ottimali grazie alla commutazione dedicata per ogni porta.
>
> **Dispositivi necessari:**
>
> - **Switch manageable 24 porte Gigabit:** Core della rete, permette segmentazione VLAN e QoS
> - **Router/Firewall:** Gateway verso Internet con funzionalità di NAT, DHCP e sicurezza perimetrale
> - **Access Point wireless:** Connettività mobile per dispositivi BYOD
> - **Server rack:** Housing per file server e web server
> - **UPS:** Continuità operativa per apparati critici

UPS = Uninterrupted Power Supply = Fonte di alimentazione continua
- Quando c'è un blackout, hai questi che ti salvano il lavoro e mantengono tutto operativo..

Esercitazione Campagnaro – Parte 2

Prima parte:

Un'azienda decide di aprire una filiale in una città vicina. Nella nuova sede dovranno essere installati e configurati circa 30 nuovi computer e 3 stampanti di rete. In questa nuova succursale dovranno inoltre essere installati 1 file server per l'archiviazione e 1 web server per il sito intranet aziendale che non deve essere accessibile però da Internet.

Nella sede centrale i dispositivi sono configurati con indirizzi IP del tipo 192.168.1.0/24 e dovranno poter accedere al file server e al sito intranet sviluppato e pubblicato nella rete della nuova sede. L'ISP ha già consegnato in questa nuova sede il router per il collegamento ad Internet preconfigurato con indirizzo IP privato 192.168.0.1/24 e indirizzo pubblico 84.23.67.121/29.

ISP = Internet Service Provider = Fornitore di servizi Internet → TIM / Vodafone / etc.

L'azienda richiede:
1. una configurazione dei dispositivi semplice da gestire
2. una configurazione di rete che preveda alti standard di sicurezza
3. una documentazione dell'architettura di rete comprensiva degli indirizzamenti utilizzati
4. una documentazione che riporti i servizi di rete previsti e la loro configurazione

Il sito intranet aziendale, previa autenticazione, permette agli utenti di specificare i lavori svolti durante la giornata al fine di consuntivare a fine mese le attività suddivise per utente o suddivise per cliente.

> La configurazione richiede un approccio a doppio livello di indirizzamento. La sede centrale utilizza 192.168.1.0/24, mentre la nuova filiale opererà su 192.168.0.1/24 per evitare conflitti di routing. Il router pre-configurato con IP pubblico 84.23.67.121/29 gestirà il NAT e il collegamento VPN site-to-site con la sede centrale.
>
> **Documentazione richiesta:**
>
> 1. **Configurazione semplificata:** Schema di indirizzamento IP, configurazione DHCP scope, configurazione base switch/router
> 2. **Standard di sicurezza:** Implementazione WPA3 per wireless, configurazione firewall rules, policy di accesso utenti
> 3. **Architettura comprensiva:** Diagramma topologico completo, documentazione VLAN, piano di backup e disaster recovery
> 4. **Servizi e configurazioni:** Documentazione server roles, configurazione DNS/DHCP, procedure di manutenzione
>
> Il sito intranet aziendale richiederà autenticazione Active Directory integrata e interfaccia per timesheet management con database backend per tracking delle attività per cliente/progetto.

NAT (Network Address Translation): Mascherare l'IP interno uscendo con un nuovo IP esterno.

DHCP (Routing dinamico)

WPA3 = Wireless crittografato

Backup / Disaster recovery

Seconda parte:

1. Spiegare i vantaggi ed il funzionamento del TCP/IP → Modello logico per le reti.
2. Spiegare cos'è una VPN basata sul protocollo IPSec, quali sono le sue caratteristiche e le problematiche specifiche → Controllo tunnel sicuro tra host della rete.
3. Scrivere la definizione di sicurezza informatica (ISO) e descriverne gli specifici attributi → Struttura standard per i controlli nelle organizzazioni

1. **TCP/IP:** Il modello TCP/IP offre affidabilità attraverso acknowledgment, controllo di flusso e ritrasmissione automatica. Vantaggi: universalità, scalabilità, fault tolerance. Funzionamento: segmentazione dati in pacchetti, routing attraverso internetwork, riassemblaggio a destinazione con garanzia di ordine e integrità.
2. **VPN IPSec:** Protocollo di tunneling che opera a livello rete (Layer 3) creando tunnel crittografici tra endpoint. Caratteristiche: autenticazione mutual attraverso certificati o PSK, crittografia AES per confidenzialità, integrity checking tramite HMAC. Problematiche: overhead computazionale, complessità configurativa, possibili incompatibilità tra vendor diversi, performance degradation su connessioni ad alta latenza.
3. **Sicurezza informatica ISO 27001:** Framework sistematico per gestione della sicurezza delle informazioni basato su approccio risk-based. Attributi fondamentali: **Confidenzialità** (accesso autorizzato alle informazioni), **Integrità** (accuratezza e completezza dei dati), **Disponibilità** (accessibilità quando necessario). Include inoltre autenticità, non-ripudio e accountability per gestione completa del rischio informativo.