## 🧪 EXPERIMENT 7 — Study of HTTP, HTTPS, and FTP using Packet Tracer

**Aim:**
Study and analyze performance of **HTTP, HTTPS, and FTP protocols** using Cisco Packet Tracer.

**Objectives:**
Understand the concept and working of HTTP, HTTPS, and FTP protocols.

**Theory (Summary):**

**FTP (File Transfer Protocol)**

- Standard protocol for file transfer between client and server.
- Works on **port 21** (control) and **20** (data).
- Uses **TCP** (reliable).
- Can perform upload (PUT), download (GET), delete, rename.

**HTTP (HyperText Transfer Protocol)**

- Used for transferring web pages.
- Works on **port 80**.
- Data sent in plain text (not secure).

**HTTPS (HTTP Secure)**

- Secure version of HTTP.
- Works on **port 443**.
- Uses **SSL/TLS** for encryption.

**FTP Configuration Steps in Packet Tracer:**

1. Configure IPs of Laptop (Client) and Server.
2. Connect via ftp 192.168.1.2 and login (cisco/cisco).
3. Upload file using put filename.
4. Verify upload in Server → Services → FTP.
5. Upload HTML file to HTTP directory and access via browser.

**Conclusion:**
Successfully analyzed HTTP, HTTPS, and FTP protocols using Packet Tracer.

---

### 🔹 Oral / Viva Questions and Answers

1. **Difference between HTTP and HTTPS?**
   ➤ HTTPS adds SSL/TLS encryption for secure data transfer; HTTP is plain text.

2. **Which protocol does FTP use?**
   ➤ TCP (Transmission Control Protocol).

3. **Port numbers:**
   ➤ HTTP – 80, HTTPS – 443, FTP – 20 & 21.

4. **What is FTP used for?**
   ➤ Uploading and downloading files between client and server.

5. **Which commands are used in FTP?**
   ➤ put, get, delete, rename, cd.

6. **Can multiple clients connect to an FTP server?**
   ➤ Yes, multiple clients can connect simultaneously.

7. **What happens when we open a website using HTTPS?**
   ➤ The browser performs an SSL/TLS handshake to establish a secure session.