* **IP – Internet Protocol**

+ Giao thức IP cấp cho mỗi thiết bị một **địa chỉ IP duy nhất**, giúp định danh trong mạng.

+ IP còn chịu trách nhiệm **định tuyến** các gói dữ liệu đến đúng nơi tiếp nhận.

* **TCP – Transmission Control Protocol**

+ Đảm bảo các gói dữ liệu đến đúng thứ tự và không bị mất mát.

+ Nếu một gói tin bị mất, TCP sẽ tự động yêu cầu gửi lại.

* **HTTP/HTTPS – HyperText Transfer Protocol (Secure)**

+ Là giao thức chính để truyền tải nội dung web.

+ **HTTPS** là phiên bản bảo mật hơn, sử dụng mã hóa SSL/TLS, giúp ngăn chặn đánh cắp dữ liệu khi truyền trên mạng.

* **FTP – File Transfer Protocol**

+ Dùng để **truyền tải file** giữa client và server.

+ Được ứng dụng trong các dịch vụ lưu trữ hoặc cập nhật nội dung website.

* **DNS – Domain Name System**

+ Là giao thức có thể chuyển đổi tên miền (ví dụ:[www.google.com](http://www.google.com/)) thành địa chỉ IP (ví dụ: 142.250.190.206).

+ Giúp người dùng không cần nhớ các dãy số IP mà chỉ cần nhớ tên miền dễ đọc.

Quy trình của giao thức trên:

+ Bạn nhập địa chỉ website vào trình duyệt.

+ Trình duyệt gửi yêu cầu tới **DNS Server** để lấy IP tương ứng với tên miền.

+ Với IP đã nhận, trình duyệt gửi yêu cầu HTTP đến **Web Server** của trang web.

+ Server xử lý, chia nội dung thành các packet và gửi về.

+ Trình duyệt nhận các packet, kiểm tra thứ tự và tái dựng nội dung trang web.

| **Giao thức** | **Ưu điểm** | **Nhược điểm** |
| --- | --- | --- |
| **TCP/IP** | - Đáng tin cậy: đảm bảo dữ liệu đúng, đầy đủ; phát hiện lỗi, truyền lại nếu mất gói. - Linh hoạt: hoạt động qua nhiều loại mạng. - Được tiêu chuẩn hóa và hỗ trợ rộng rãi. | - Overhead cao hơn so với giao thức không đảm bảo (như UDP).   - Thiết lập kết nối ban đầu tốn thời gian (handshake). - Không phù hợp cho truyền dữ liệu thời gian thực mà độ trễ phải cực thấp nếu mất gói được truyền lại. |
| **HTTP** | - Đơn giản, phổ biến, dễ triển khai. - Tương tác dễ dàng: client‐server, request/response. - Hỗ trợ cache, headers để tối ưu hóa. | - Không mã hóa (nếu dùng HTTP thường), thông tin có thể bị nghe trộm hoặc giả mạo.  - Không xác thực hai chiều; dễ bị tấn công trung gian (man‑in‑the‑middle). |
| **HTTPS** | - Bảo mật: mã hóa dữ liệu; đảm bảo tính riêng tư, tính toàn vẹn (integrity).   - Xác thực server, đôi khi client.   - Tin cậy hơn khi truyền thông nhạy cảm. | - Overhead (thời gian thiết lập SSL/TLS, chi phí tính toán mã hóa). - Quản lý chứng chỉ, chi phí nếu TLS certificated không miễn phí. - Nếu cấu hình không đúng có thể có lỗ hổng (ví dụ sử dụng thuật toán mã hóa yếu). |
| **FTP** | - Dễ sử dụng cho việc truyền file lớn hoặc nhiều file.   - Hỗ trợ quản lý file từ xa (xem thư mục, di chuyển, xóa, đặt quyền).  - Tương đối nhanh khi không cần mã hóa. | - Bảo mật kém - Cấu hình active/passive có thể khó do firewall / NAT.   - Không tối ưu trong môi trường yêu cầu bảo mật cao hiện nay. |
| **DNS** | - Giúp người dùng dễ nhớ tên miền thay vì IP. - Tổ chức phân tán, lớn mạnh, nhanh.  - Hỗ trợ nhiều loại bản ghi; có thể dùng để phân phối tải, cân bằng tải, dự phòng. | - Nếu máy chủ DNS bị tấn công hoặc giả mạo (DNS spoofing), có thể dẫn đến người dùng bị dẫn đến trang giả mạo. - Tính riêng tư: nếu DNS truy vấn không được mã hóa, người thứ ba có thể thấy bạn truy cập tên miền nào.  - Thỉnh thoảng độ trễ nếu phải truy vấn DNS nhiều cấp (root → TLD → authoritative) hoặc server chậm. |

Hình ảnh mô tả:

A diagram of a computer network

Description automatically generated