1. Khái niệm & công dụng

| **Giao thức** | **Khái niệm** | **Công dụng chính** |
| --- | --- | --- |
| **TCP/IP** | TCP/IP là bộ giao thức cơ bản của Internet, gồm TCP (Transport Control Protocol) và IP (Internet Protocol), cùng với các giao thức phụ khác như UDP, ICMP… Nó quy định cách các máy tính chia nhỏ, gửi, nhận dữ liệu qua mạng. | Dùng làm tầng truyền vận & mạng cho các giao thức ứng dụng như HTTP, FTP, DNS… IP chịu trách nhiệm định địa chỉ & định tuyến gói tin, TCP đảm bảo tính đáng tin cậy (kiểm tra lỗi, đảm bảo thứ tự, retransmission nếu mất gói). |
| **HTTP (Hypertext Transfer Protocol)** | Giao thức ứng dụng dùng để truyền tải siêu văn bản (HTML, CSS, hình ảnh, script…) giữa client (thường trình duyệt) và web server. Là giao thức không bảo mật (plaintext). | Truy cập website: tải trang web, gửi yêu cầu, nhận nội dung trang; các thao tác như GET, POST, PUT… |
| **HTTPS (HTTP Secure)** | Là HTTP chạy "trên" một kết nối được mã hóa bằng SSL/TLS (Secure Sockets Layer / Transport Layer Security). Nó đảm bảo các thông điệp giữa client và server được mã hóa, xác thực server, và tính toàn vẹn dữ liệu. | Dùng khi cần bảo mật: đăng nhập, thanh toán, thông tin cá nhân, giao dịch nhạy cảm, để tránh bị nghe lén, giả mạo, thay đổi dữ liệu. |
| **FTP (File Transfer Protocol)** | Giao thức ứng dụng dùng để chuyển file giữa client và server qua mạng TCP/IP; hỗ trợ các lệnh như upload, download, liệt kê thư mục, xoá file, v.v. | Dùng để chia sẻ tệp, sao lưu, quản lý tệp từ xa, dịch vụ lưu trữ file, cập nhật website, truyền file giữa các máy chủ. |
| **DNS (Domain Name System)** | Là hệ thống & giao thức để ánh xạ tên miền dễ nhớ (ví dụ [www.example.com](http://www.example.com/)) thành địa chỉ IP máy chủ, để các thiết bị có thể tìm được nhau qua mạng. | Khi bạn gõ một tên miền vào trình duyệt, máy tính hỏi DNS để biết IP, rồi mới kết nối tới server; cũng phục vụ gửi email, dịch vụ mạng khác, load balancing, phân giải tên miền. |

1. Quy trình hoạt động

Dưới đây là mô tả quy trình hoạt động cơ bản của từng giao thức:

**HTTP**

1. Người dùng nhập URL dạng http://example.com/path vào trình duyệt.
2. Trình duyệt (client) thực hiện DNS lookup để tìm địa chỉ IP của example.com.
3. Thiết lập kết nối TCP tới máy chủ tại IP đó, cổng 80 (mặc định HTTP).
4. Client gửi yêu cầu HTTP (HTTP Request) — có thể là GET, POST, HEAD…, kèm tiêu đề (headers), thông tin như agent, cookies,…
5. Server xử lý yêu cầu, gửi về HTTP Response: mã trạng thái (200, 404, 500…), header, sau đó nội dung (HTML, CSS, hình ảnh…).
6. Client nhận và hiển thị nội dung trang web.

**HTTPS**

Quy trình giống HTTP với bước thêm cho bảo mật:

1. Client yêu cầu kết nối HTTPS tới server, cổng mặc định là **443**.
2. Máy chủ gửi **chứng chỉ SSL/TLS** cho client.
3. Client kiểm tra tính xác thực của chứng chỉ (CA issuer, thời hạn, tên miền có khớp không, v.v.).
4. Hai bên thực hiện **bắt tay TLS (TLS handshake)**: thỏa thuận thuật toán mã hóa, trao đổi khóa (public key, private key) để thiết lập kênh mã hóa.
5. Sau khi kênh bảo mật được thiết lập, mọi HTTP request/response được mã hóa qua TLS.
6. Sau khi kết thúc trao đổi, client hoặc server có thể đóng kết nối TLS/TCP.

**FTP**

1. Client khởi tạo kết nối TCP tới server FTP, thường cổng **21** cho điều khiển (control channel).
2. Client đăng nhập (nếu cần): gửi username/password đến server.
3. Để truyền file hoặc danh sách thư mục, FTP mở một kết nối dữ liệu (data channel): có thể server mở, hoặc client mở, tùy chế độ Active hoặc Passive FTP.
4. Thực hiện các lệnh FTP: LIST, RETR (download), STOR (upload), DELE, MKD, v.v.
5. Sau khi hoàn tất trao đổi file, đóng kết nối dữ liệu, rồi kết thúc phiên FTP (QUIT).

**DNS**

1. Khi client (ví dụ trình duyệt, hệ điều hành) cần phân giải tên miền, client gửi truy vấn (query) tới máy chủ DNS cấu hình (resolver).
2. Nếu resolver đã có trong cache địa chỉ IP, trả về ngay, không cần hỏi tiếp.
3. Nếu không, resolver sẽ hỏi dần từ cấp cao hơn: máy chủ gốc (root server), sau đó máy chủ TLD (ví dụ .com, .net,..), rồi máy chủ tên miền chịu trách nhiệm (authoritative name server).
4. Khi nhận được địa chỉ IP, resolver trả lại cho client.
5. Client dùng địa chỉ IP đó để thiết lập kết nối (ví dụ HTTP, HTTPS, FTP…).

**TCP/IP (tổng quan)**

* IP chịu trách nhiệm: chia gói dữ liệu, gắn header chứa địa chỉ nguồn & đích, đưa qua mạng, các router định tuyến gói.
* TCP cung cấp: thiết lập kết nối (three‑way handshake: SYN, SYN‑ACK, ACK), đảm bảo các gói đến đầy đủ, đúng thứ tự, retransmission khi mất gói, đóng kết nối (four‑way handshake).
* Giao thức ứng dụng như HTTP, FTP, DNS dùng TCP/IP làm tầng truyền dưới

III. Mục đích sử dụng

| **Giao thức** | **Mục đích chính** |
| --- | --- |
| HTTP | Truy cập web, tải nội dung web, khi không cần bảo mật cao. |
| HTTPS | Đảm bảo an toàn thông tin người dùng, giao dịch nhạy cảm; xác thực server; chống MITM; bảo vệ quyền riêng tư. |
| FTP | Truyền file lớn, upload/download file từ/đến các máy chủ; quản lý file trên server; backup; chia sẻ file. |
| DNS | Là "sổ địa chỉ" của Internet, giúp ánh xạ tên miền sang IP; giúp người dùng không phải nhớ địa chỉ IP; quản lý tên miền; Routing; load balancing. |
| TCP/IP | Là cơ sở hạ tầng truyền tải – cho mọi giao thức trên mạng Internet; đảm bảo kết nối, định tuyến, tin cậy nếu cần; phân mảnh gói tin; hồi đáp lỗi; hoạt động mạng tổng thể. |

IV: Ưu điểm & nhược điểm

| **Giao thức** | **Ưu điểm** | **Nhược điểm** |
| --- | --- | --- |
| **HTTP** | Đơn giản, dễ triển khai; không phải xử lý mã hóa; giảm độ trễ vì không phải thiết lập kênh bảo mật; tương thích cao. | Không bảo mật: dữ liệu truyền plaintext; dễ bị nghe lén, giả mạo, chỉnh sửa; không xác thực server; không phù hợp cho thông tin nhạy cảm. |
| **HTTPS** | Bảo mật cao; mã hóa dữ liệu; xác thực máy chủ; bảo vệ tính toàn vẹn của dữ liệu; tăng tin cậy người dùng; hiện nay tiêu chuẩn gần như yêu cầu mọi website nên hỗ trợ HTTPS. | Phức tạp hơn: cần chứng chỉ SSL/TLS, quản lý chứng chỉ; có chi phí nếu dùng chứng chỉ thương mại; thiết lập handshake làm tăng độ trễ nhỏ so với HTTP; độ tính toán cao hơn (mã hóa/giải mã); có thể gặp lỗi nếu chứng chỉ không hợp lệ. |
| **FTP** | Chuyển file hiệu quả; hỗ trợ upload & download; nhiều client FTP, tương thích rộng. | Không mã hóa (FTP “plain” dễ bị nghe lén); firewall thường khó cấu hình (vì sử dụng hai kết nối: control + data); cấu hình phức tạp hơn nếu muốn bảo mật (cần FTPS / SFTP); không phù hợp cho môi trường cần bảo mật nghiêm ngặt. |
| **DNS** | Thật sự cần thiết để tên miền dễ nhớ; giúp routing nhanh; có cache để tăng tốc; hỗ trợ nhiều chức năng mở rộng (ví dụ record mail exchange, alias, load balancing,…). | Mặc định không mã hóa → dễ bị nghe lén / giả mạo; nếu DNS server bị tấn công / cấu hình sai thì ảnh hưởng lớn; độ trễ nếu phải truy vấn nhiều máy chủ; cache stale; tấn công DNS spoofing / poisoning. |
| **TCP/IP** | Rất mạnh, nền tảng cho Internet; TCP cung cấp tính đáng tin cậy; IP cho phép định tuyến qua mạng khác nhau; hệ mở, tiêu chuẩn quốc tế; mở rộng tốt. | TCP có overhead (handshake, quản lý kết nối, retransmission, kiểm soát tắc nghẽn) → độ trễ & tài nguyên; IP (phiên bản IPv4) có hạn địa chỉ; thiếu bảo mật mặc định; UDP (cùng lớp IP) thì không đáng tin cậy; mạng phức tạp cần quản lý tốt (routing, attack,…). |

V. Vẽ sơ đồ hoặc tìm kiếm hình ảnh thể hiện chức năng của các thành phần trên trong mô hình kết nối mạng với internet

