



ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Internet Services

Phạm Huy Hoàng - SOICT/HUST
hoangph@soict.hust.edu.vn

1

Nội dung

- Kết nối tầng giao vận
- Kết nối tầng ứng dụng
- Dịch vụ IP cơ bản: DNS, Mail, Web
- Kết nối dịch vụ mạng riêng và mạng public Internet



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

2

2

Vị trí trong kiến trúc phân tầng

| |
|------------------------------------|
| Application (HTTP, Mail, ...) |
| Transport (UDP, TCP ...) |
| Network (IP, ICMP...) |
| Datalink (Ethernet, ADSL...) |
| Physical (bits...) |

Hỗ trợ các ứng dụng trên mạng

Truyền dữ liệu giữa các ứng dụng

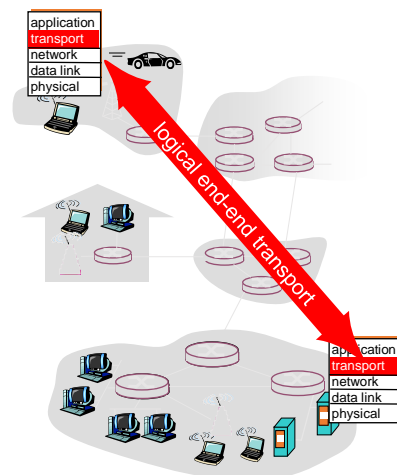
Chọn đường và chuyển tiếp gói tin giữa các máy, các mạng

Hỗ trợ việc truyền thông cho các thành phần kết tiếp trên cùng 1 mạng

Truyền và nhận dòng bit trên đường truyền vật lý

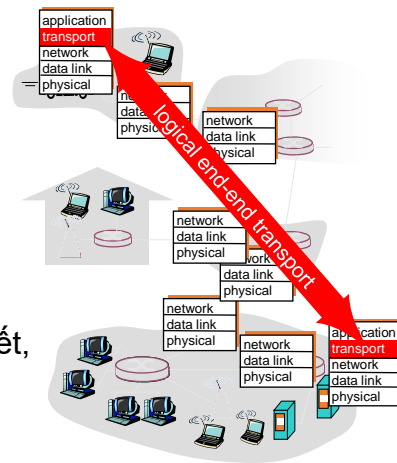
Kết nối tầng giao vận (1)

- Cung cấp phương tiện truyền giữa các ứng dụng cuối
 - Các ứng dụng là các tiến trình chạy trên các máy.
- Bên gửi:
 - Nhận dữ liệu từ ứng dụng
 - Đặt dữ liệu vào các đoạn tin và chuyển cho tầng mạng
 - Nếu dữ liệu quá lớn, nó sẽ được chia làm nhiều phần và đặt vào nhiều đoạn tin khác nhau
- Bên nhận:
 - Nhận các đoạn tin từ tầng mạng
 - Tập hợp dữ liệu và chuyển lên cho ứng dụng



Kết nối tầng giao vận (2)

- Được cài đặt trên các hệ thống cuối
 - Không cài đặt trên các routers, switches...
- Hai dạng dịch vụ giao vận
 - Tin cậy, hướng liên kết, e.g. TCP
 - Không tin cậy, không liên kết, e.g. UDP



Ứng dụng IP cơ bản và dịch vụ giao vận

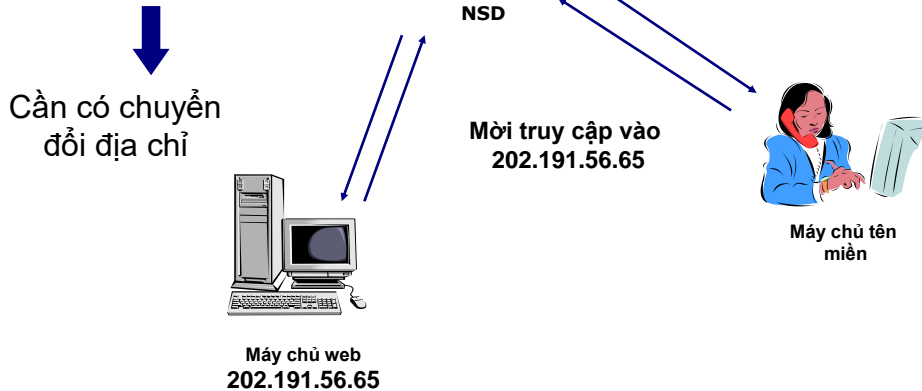
| Ứng dụng | Giao thức ứng dụng | Giao thức giao vận |
|------------------------|---|--------------------|
| domain name | DNS | UDP |
| e-mail | SMTP | TCP |
| remote terminal access | Telnet | TCP |
| Web | HTTP | TCP |
| file transfer | FTP | TCP |
| streaming multimedia | giao thức riêng (e.g. RealNetworks) | TCP or UDP |
| Internet telephony | giao thức riêng (e.g., Vonage, Dialpad) | thường là UDP |

Giới thiệu chung

- Tên miền: định danh trên tầng ứng dụng cho các nút mạng
 - Trên Internet được quản lý tập trung
 - Quốc tế: ICANN
 - Việt Nam: VNNIC
- DNS(Domain Name System): hệ thống tên miền gồm các máy chủ quản lý thông tin tên miền và cung cấp dịch vụ DNS
- Vấn đề phân giải tên miền sang địa chỉ IP
 - Người sử dụng dùng tên miền để truy cập dịch vụ
 - Máy tính và các thiết bị mạng không sử dụng tên miền mà dùng địa chỉ IP khi trao đổi dữ liệu
- Làm thế nào để chuyển đổi tên miền sang địa chỉ IP?

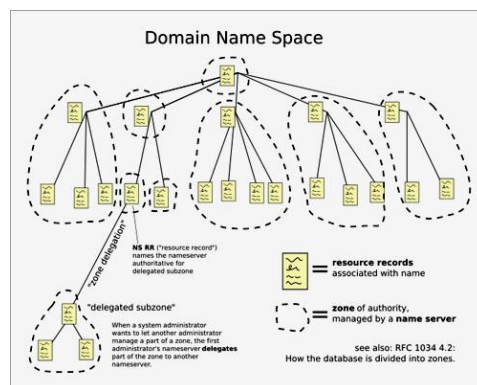
Chuyển đổi địa chỉ và ví dụ

- Máy tính dùng địa chỉ IP
- NSD dùng tên miền



Không gian tên miền

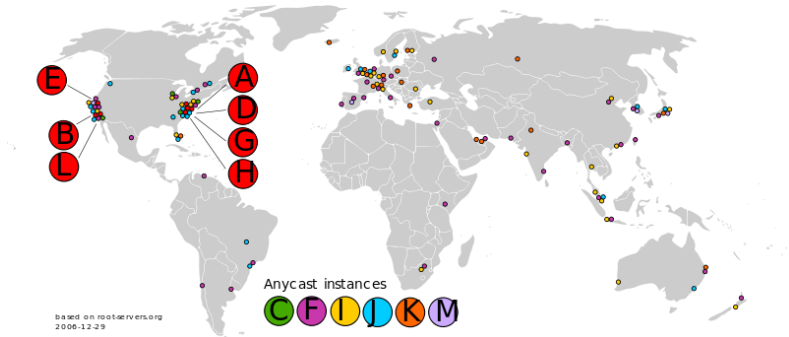
- Kiến trúc : hình cây
 - Root: Nút gốc
 - Chia thành các zone
- Mỗi nút là một tập hợp các bản ghi mô tả tên miền tương ứng với nút đó. Ví dụ:
 - SOA
 - NS
 - A



Hình ảnh từ: Wikipedia

Hệ thống máy chủ DNS

- Máy chủ tên miền gốc (Root server)
 - Trả lời truy vấn cho các máy chủ cục bộ
 - Quản lý các zone và phân quyền quản lý cho máy chủ cấp dưới
 - Có 13 hệ thống máy chủ gốc trên mạng Internet (<http://www.root-servers.org>)



Hệ thống máy chủ DNS (tiếp)

- Máy chủ tên miền cấp 1 (Top Level Domain)
 - Quản lý tên miền cấp 1
- Máy chủ được ủy quyền (Authoritative DNS servers)
 - Quản lý tên miền cấp dưới
- Máy chủ của các tổ chức: của ISP
 - Không nằm trong phân cấp của DNS
- Máy chủ cục bộ: dành cho mạng nội bộ của cơ quan tổ chức
 - Không nằm trong phân cấp của DNS

Phân giải tên miền

- Tụ phân giải
 - File HOST:
 - Windows: C:\WINDOWS\system32\drivers\etc\
 - Linux: /etc/hosts
 - Bộ đệm của ứng dụng
- Dịch vụ phân giải tên miền: client/server
 - Giao thức tầng ứng dụng: DNS
 - Sử dụng dịch vụ UDP/TCP với cổng dịch vụ là 53
 - Phân giải đệ quy (Recursive Query)
 - Phân giải tương tác (Interactive Query)

Thông điệp DNS

- DNS Query và DNS Reply:
Chung khuôn dạng
- Identification: Định danh của truy vấn
 - Thông điệp trả lời phải có giá trị Identification trùng với thông điệp truy vấn
- Flags: Các cờ điều khiển
- #Question: Số lượng tên miền được truy vấn
- QUESTION: các tên miền được truy vấn

| Identification | Flags |
|----------------|-----------------|
| #Question | #Answer RRs |
| #Authority RRs | #Additional RRs |
| QUESTION | |
| ANSWER | |
| AUTHORITY | |
| ADDITIONAL | |

Thông điệp DNS

- #Answer RRs: Số lượng bản ghi trả lời
- ANSWER: Các bản ghi trả lời
- # Authority RRs: Số lượng bản ghi các máy chủ được ủy quyền khác
- AUTHORITY: Các bản ghi của máy chủ được ủy quyền khác
- #Additional RRs: Số lượng các bản ghi bổ sung
- ADDITIONAL: Các bản ghi bổ sung

| Identification | Flags |
|----------------|-----------------|
| #Question | #Answer RRs |
| #Authority RRs | #Additional RRs |
| QUESTION | |
| ANSWER | |
| AUTHORITY | |
| ADDITIONAL | |

Ví dụ: dig linux.com

```
; <> DiG 9.9.2-P1 <> linux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
ADDITIONAL: 3
;; QUESTION SECTION:
;linux.com. IN A
;; ANSWER SECTION:
linux.com. 1786 IN A 140.211.167.51
linux.com. 1786 IN A 140.211.167.50
;; AUTHORITY SECTION:
linux.com. 86386 IN NS ns1.linux-foundation.org.
linux.com. 86386 IN NS ns2.linux-foundation.org.
;; ADDITIONAL SECTION:
ns1.linux-foundation.org. 261 IN A 140.211.169.10
ns2.linux-foundation.org. 262 IN A 140.211.169.11
```

TTL: thời gian(s) lưu giữ
trả lời trong cache

Ví dụ: dig linux.com

```
; <> DiG 9.9.2-P1 <> linux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
ADDITIONAL: 3
;; QUESTION SECTION:
;linux.com. IN A
;; ANSWER SECTION:
linux.com. 1786 IN A 140.211.167.51
linux.com. 1786 IN A 140.211.167.50
;; AUTHORITY SECTION:
linux.com. 86386 IN NS ns1.linux-foundation.org.
linux.com. 86386 IN NS ns2.linux-foundation.org.
;; ADDITIONAL SECTION:
ns1.linux-foundation.org. 261 IN A 140.211.169.10
ns2.linux-foundation.org. 262 IN A 140.211.169.11
```

Tên các máy chủ DNS server trả lời truy vấn.
Nếu phần ANSWER rỗng, DNS Resolver gửi truy vấn tới các máy chủ này

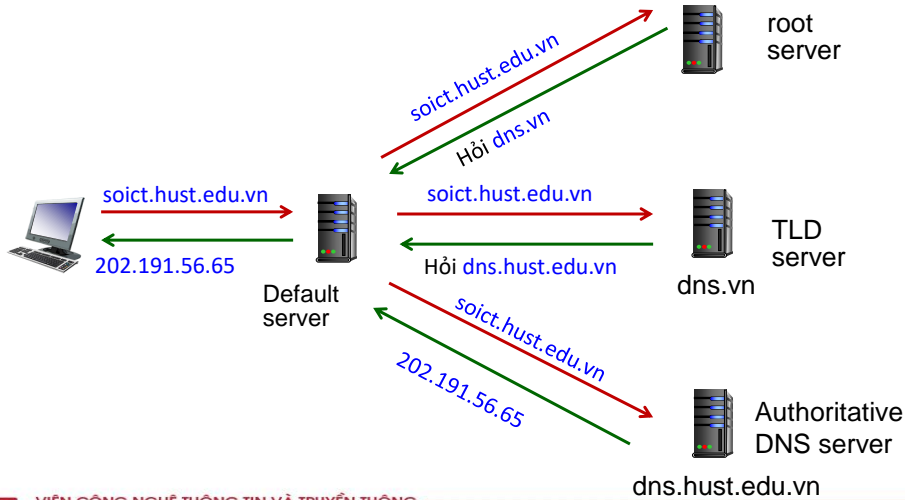
Ví dụ: dig linux.com

```
; <> DiG 9.9.2-P1 <> linux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
ADDITIONAL: 3
;; QUESTION SECTION:
;linux.com. IN A
;; ANSWER SECTION:
linux.com. 1786 IN A 140.211.167.51
linux.com. 1786 IN A 140.211.167.50
;; AUTHORITY SECTION:
linux.com. 86386 IN NS ns1.linux-foundation.org.
linux.com. 86386 IN NS ns2.linux-foundation.org.
;; ADDITIONAL SECTION:
ns1.linux-foundation.org. 261 IN A 140.211.169.10
ns2.linux-foundation.org. 262 IN A 140.211.169.11
```

Địa chỉ IP của các máy chủ trả lời truy vấn.
Thông tin này được lưu vào cache

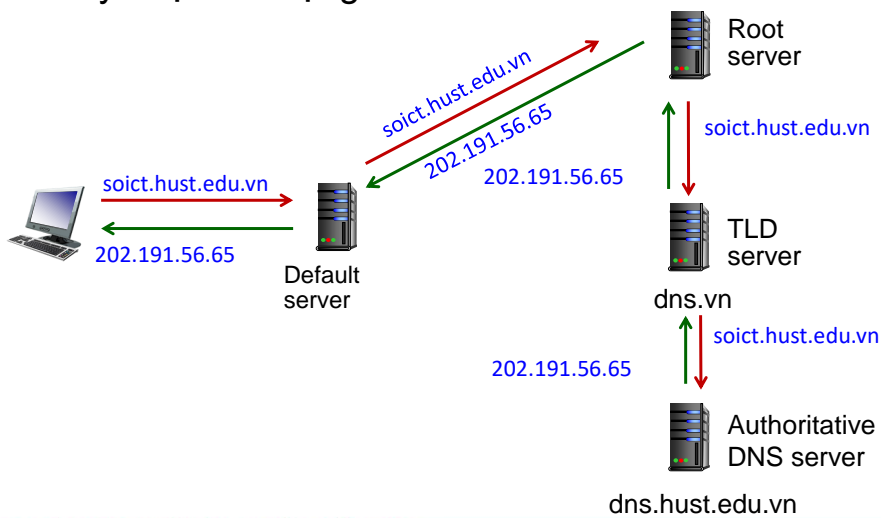
Phân giải tương tác

- Cơ chế mặc định trên các máy chủ DNS



Phân giải đệ quy

- Tùy chọn mở rộng



HTTP và Web

- Internet trước thập kỷ 1990s:
 - Hầu như chỉ sử dụng hạn chế trong cơ quan chính phủ, phòng nghiên cứu...
 - Các dịch vụ email, FPT không phù hợp cho chia sẻ thông tin đại chúng
 - Không có cơ chế hiệu quả để liên kết các tài nguyên thông tin nằm rải rác trên Internet
- Năm 1990, Tim Berners-Lee giới thiệu World Wide Web:
 - Trao đổi thông tin dưới dạng siêu văn bản (hypertext) sử dụng ngôn ngữ HTML (Hypertext Markup Language)
 - Các đối tượng không cần đóng gói “tất cả trong một” như trên các văn bản trước đó
 - Siêu văn bản chỉ chứa chứa liên kết (hypertext) tới các đối tượng khác (định vị bằng URL).

Uniform Resource Locator

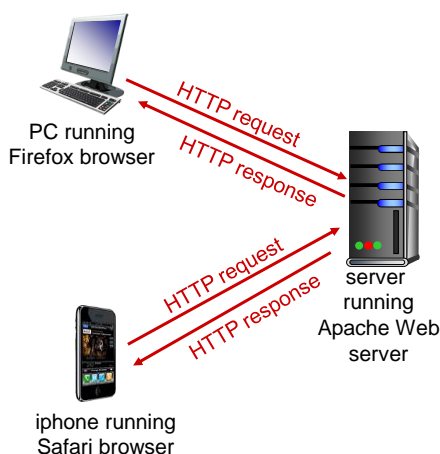
- Định vị một tài nguyên bất kỳ trên mạng và cách thức để truy cập tài nguyên đó

`protocol://hostname[:port]/directory-path/resource`

- *protocol*: Giao thức (http, ftp, https, smtp, rtsp...)
- *hostname*: tên miền, địa chỉ IP
- *port*: cổng ứng dụng (có thể không cần)
- *directory path*: đường dẫn tới tài nguyên
- *resource*: định danh của tài nguyên

HTTP và Web

- WWW: World Wide Web
 - trao đổi dữ liệu siêu văn bản HTML (HyperText Markup Language) trên mạng
- HTTP: HyperText Transfer Protocol
 - Mô hình Client/Server
 - Client yêu cầu truy nhập tới các trang web (chứa các đối tượng web) và hiển thị chúng trên trình duyệt
 - Server: Nhận yêu cầu và trả lời cho client



Hình ảnh từ: "Computer Networking: A Top Down Approach", Jim Kurose

Hoạt động của HTTP

- Thiết lập liên kết TCP
 - Server mở một TCP socket chờ yêu cầu kết nối tại cổng 80 (mặc định)
 - Client khởi tạo một liên kết TCP tới server
 - Server chấp nhận yêu cầu, tạo liên kết
- Trao đổi thông điệp HTTP (giao thức ứng dụng)
 - HTTP Request: Thông điệp yêu cầu
 - HTTP Response: Thông điệp trả lời
- Đóng liên kết TCP

Khuôn dạng HTTP Request

- Mã ASCII (dễ dàng đọc được dưới dạng văn bản)

Dòng yêu cầu → GET /~tungbt/index.htm HTTP/1.1\r\n

Các dòng tiêu đề → Host: soict.hust.edu.vn\r\n
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7\r\n
Keep-Alive: 115\r\n
Connection: keep-alive\r\n

Báo kết thúc tiêu đề → \r\n

Các phương thức yêu cầu

HTTP/1.0

- GET
- POST
- HEAD
 - yêu cầu máy chủ loại một số đối tượng ra khỏi thông điệp trả lời

HTTP/1.1

- GET, POST, HEAD
- PUT
 - tải file lên máy chủ, đường dẫn chỉ ra trong URL, file để trong body
- DELETE
 - Xóa file chỉ ra bởi đường dẫn

Lưu ý: Có 2 cách để gửi tham số đến server: POST hoặc GET

<http://www.google.com/search?q=computer+network&flags=68&num=10>



Khuôn dạng HTTP Response

Dòng trạng thái trả lời

Các dòng tiêu đề

```
HTTP/1.1 200 OK\r\n
Date: Thu, 31 Jul 2014 00:00:14 GMT\r\n
Server: Apache/2.2.15 (CentOS)\r\n
Last-Modified: Wed, 30 Jul 2014 23:59:50 GMT\r\n
ETag: "17dc6-a5c-bf716880"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 2652\r\n
Connection: close\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
data data data data data ...
```

Dữ liệu đáp ứng yêu cầu



Mã trạng thái trả lời

Trong dòng đầu tiên của thông điệp trả lời, ví dụ

200 OK

- request succeeded, requested object later in this message

301 Moved Permanently

- requested object moved, new location specified later in this message (Location:)

400 Bad Request

- request message not understood by server

404 Not Found

- requested document not found on this server

505 HTTP Version Not Supported

Hiển thị (rendering) nội dung trang web

- Mô hình xử lý cơ bản tại trình duyệt:
 - Nhận thông điệp HTTP Response
 - Hiển thị:
 - Xử lý mã HTML, CSS, Javascripts
 - Gửi thông điệp HTTP Request yêu cầu các đối tượng khác(nếu có)
 - Bắt và xử lý sự kiện
- Các sự kiện có thể xảy ra:
 - Sự kiện của người dùng: OnClick, OnMouseOver...
 - Sự kiện khi hiển thị: OnLoad, OnBeforeUnload...
 - Theo thời gian: setTimeout(), clearTimeout()...

Các chế độ của HTTP

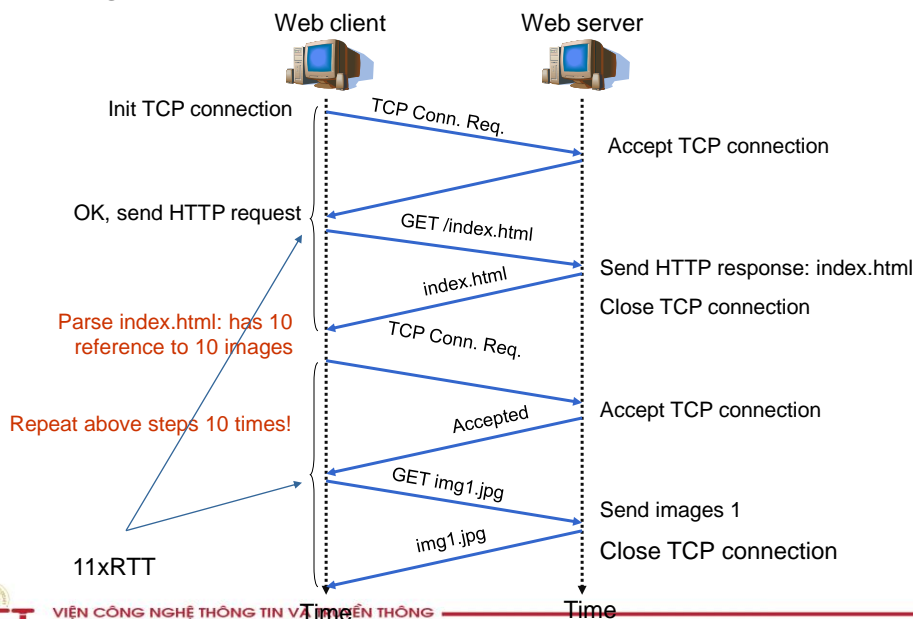
HTTP không duy trì

- Chỉ một đối tượng web được gửi qua liên kết TCP
- Sử dụng mặc định trong HTTP/1.0
- HTTP 1.0: RFC 1945

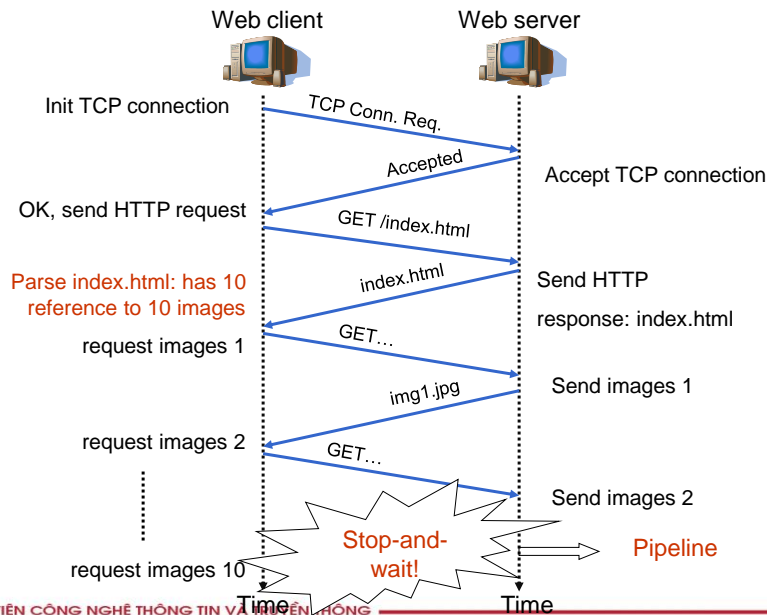
HTTP có duy trì

- Nhiều đối tượng có thể được gửi qua một liên kết TCP.
- Sử dụng mặc định trong HTTP/1.1
- HTTP 1.1: RFC 2068

Hoạt động của HTTP/1.0



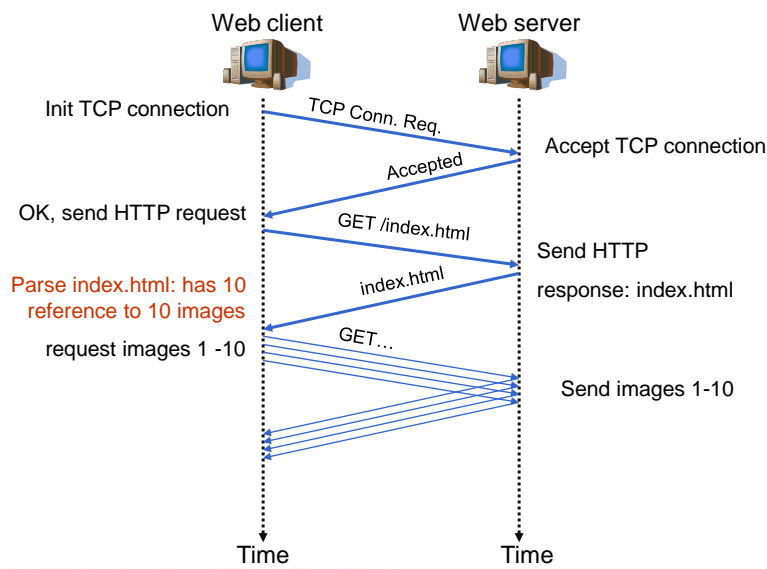
Hoạt động của HTTP/1.1



33

33

HTTP/1.1 với pipeline



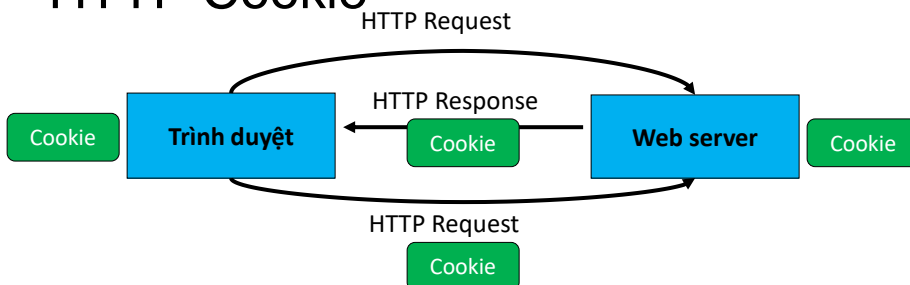
34

34

HTTP là giao thức stateless

- Một phiên hoạt động của HTTP:
 - Trình duyệt kết nối với Web server
 - Trình duyệt gửi thông điệp yêu cầu HTTP Request
 - Web server đáp ứng với một thông điệp HTTP Response
 - ...lặp lại...
 - Trình duyệt ngắt kết nối
- Các thông điệp HTTP Request được xử lý độc lập
- Web server không ghi nhớ trạng thái của phiên HTTP
 - Nếu dịch vụ Web cần xác thực người dùng thì người dùng sẽ phải đăng nhập lại cho mỗi thông điệp HTTP Request gửi đi ☹

HTTP Cookie



- Cookie: dữ liệu do ứng dụng Web tạo ra, chứa thông tin trạng thái của phiên làm việc
 - Server có thể lưu lại cookie (một phần hoặc toàn bộ)
- Sau khi xử lý yêu cầu, Web server trả lại thông điệp HTTP Response với cookie đính kèm
 - Set-Cookie: key = value; options;
- Trình duyệt lưu cookie
- Trình duyệt gửi HTTP Request tiếp theo với cookie được đính kèm

HTTPS

- Hạn chế của HTTP:
 - Không có cơ chế để người dùng kiểm tra tính tin cậy của Web server → lỗ hổng để kẻ tấn công giả mạo dịch vụ hoặc chen mã độc vào trang web HTML
 - Không có cơ chế mã hóa giữ mật → lỗ hổng để kẻ tấn công nghe lén đánh cắp thông tin nhạy cảm
- Secure HTTP: sử dụng liên kết SSL/TLS thay cho TCP để truyền các thông điệp HTTP
 - Xác thực:
 - Người dùng truy cập vào đúng Website mong muốn
 - Dữ liệu trong quá trình truyền không bị thay đổi
 - Bảo mật: dữ liệu được giữ bí mật trong quá trình truyền

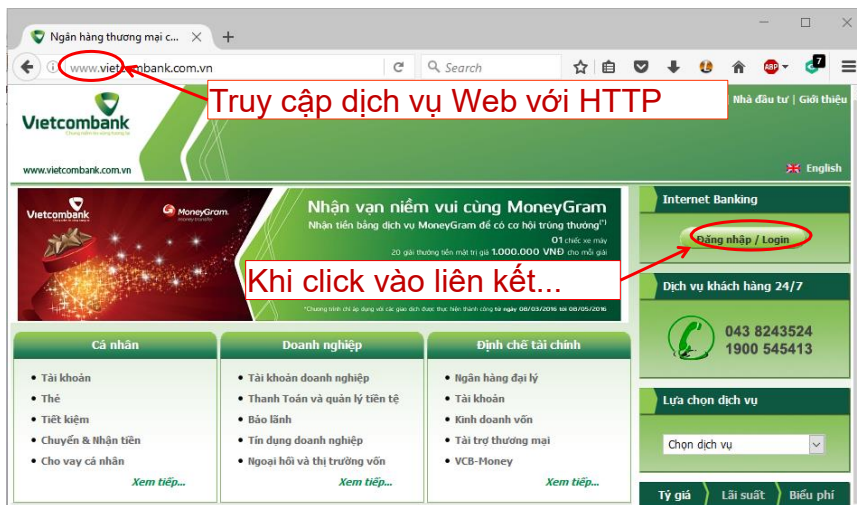


Số hiệu cổng ứng dụng: 443
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

37

37

HTTP trên trình duyệt Web



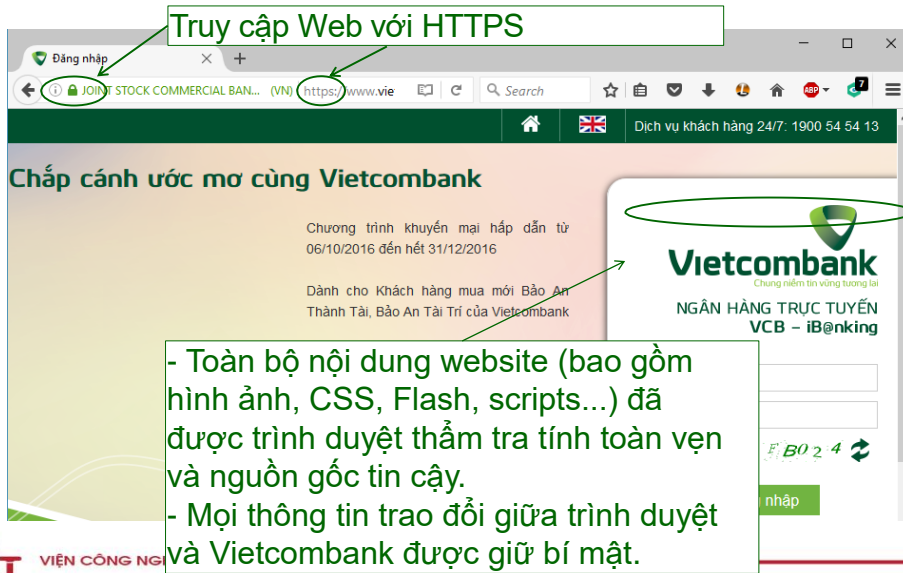
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

38

38

HTTPS trên trình duyệt Web

Truy cập Web với HTTPS



Chấp cánh ước mơ cùng Vietcombank

Chương trình khuyến mại hấp dẫn từ 06/10/2016 đến hết 31/12/2016

Dành cho Khách hàng mua mới Bảo An Thành Tài, Bảo An Tài Trĩ của Vietcombank

Vietcombank
Chung niềm tin vững tương lai
NGÂN HÀNG TRỰC TUYẾN
VCB – iB@nking

Đăng nhập

- Toàn bộ nội dung website (bao gồm hình ảnh, CSS, Flash, scripts...) đã được trình duyệt thẩm tra tính toàn vẹn và nguồn gốc tin cậy.
- Mọi thông tin trao đổi giữa trình duyệt và Vietcombank được giữ bí mật.

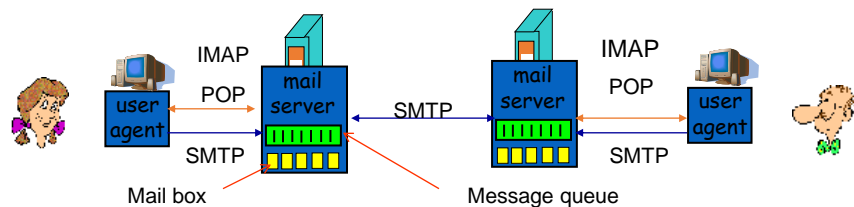
39

39

40

Dịch vụ email

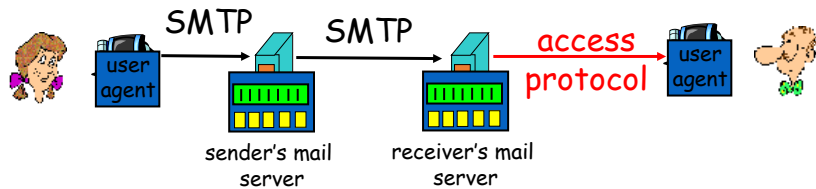
- MUA (Mail User Agent)
 - Lấy thư từ máy chủ
 - Gửi thư đến máy chủ
 - VD: Outlook, Thunderbird...
- MTA (Mail Transfer Agent):
 - Chứa hộp thư đến của NSD (mail box)
 - Hàng đợi để gửi thư đi
 - VD: Sendmail, MS Exchange...
- Giao thức:
 - Chuyển thư: SMTP-Simple Mail Transfer Protocol
 - Nhận thư
 - POP – Post Office Protocol
 - IMAP – Internet Mail Access Protocol



Giao thức SMTP

- Tài liệu mô tả: RFC 2821
- TCP, port 25: Chuyển thư từ client đến server và giữa các server với nhau
- Tương tác yêu cầu/trả lời
 - Yêu cầu: Lệnh với mã ASCII
 - Trả lời: mã trạng thái và dữ liệu

Các giao thức nhận thư



- POP: Post Office Protocol [RFC 1939]
 - Đăng nhập và lấy hết thư về
- IMAP: Internet Mail Access Protocol [RFC 1730]
 - Phức tạp hơn POP
 - Cho phép lưu trữ và xử lý thư trên máy chủ

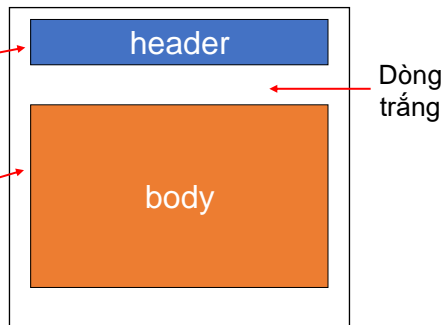
Web Mail

- Sử dụng Web browser như một MUA
- MUA và MTA giao tiếp thông qua HTTP
- Mails được lưu trữ trên máy chủ
- E.g.
 - Gmail,
 - Hotmail,
 - Yahoo! Mail, etc.
- Ngày nay, rất nhiều các MTA cho phép truy cập thông qua giao diện web
 - <http://mail.hust.edu.vn>
 - <http://mail.soict.hust.edu.vn>

Khuôn dạng thông điệp thư điện tử

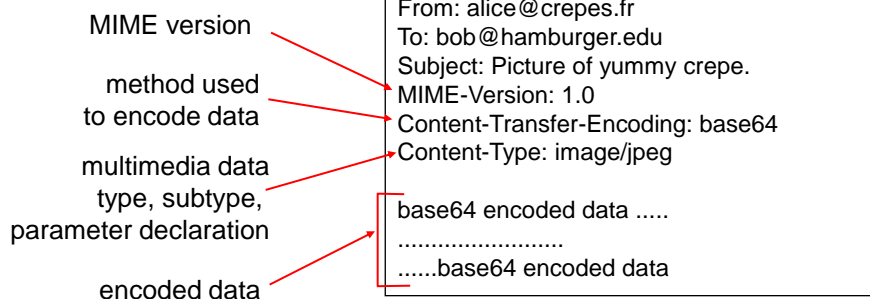
RFC 822: Định nghĩa khuôn dạng

- Phần đầu
 - To:
 - From:
 - Subject:
- Phần thân
 - Biểu diễn dưới dạng mã ASCII

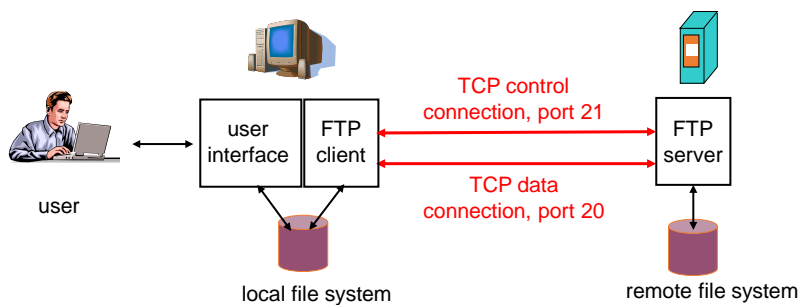


Tiêu chuẩn MIME

- Biểu diễn nội dung email có chứa dữ liệu đa phương tiện
- MIME: multimedia mail extension, RFC 2045, 2056
- Thêm một dòng trong phần đầu chỉ rõ khuôn dạng dữ liệu gửi đi



FTP: File Transfer Protocol



- Mô hình Client-server
- Trao đổi file giữa các máy
- Sử dụng TCP, cổng dịch vụ 20, 21
- Điều khiển **Out-of-band** :
 - Lệnh của FTP : cổng 21
 - Dữ liệu: cổng 20
- Người dùng phải đăng nhập trước khi truyền file
- Một số server cho phép người dùng với tên là anonymous