

Chapter 5: Network services

HTTP

Hyper Text Transfer Protocol

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

HTTP

Hyper Text Transfer Protocol

NGUYỄN THỊ THANH VÂN
CNTT - SPKT

6791504

NỘI DUNG

- I. Giao thức HTTP
- II. Nguyên tắc hoạt động của Web Server.
- III. Đặc điểm của IIS .
- IV. Cài đặt và cấu hình IIS .

Thanh Vân - CNTT

I. Giao thức HTTP

- ❖ HTTP- Hyper Text Transfer Protocol là một giao thức cho phép Web Browser và Web Server có thể giao tiếp với nhau.
- ❖ Ứng dụng web là một ứng dụng chủ/khách (client/server) sử dụng giao thức HTTP để tương tác giữa người dùng với hệ thống khác.
- ❖ Trình khách (client) là các trình duyệt web như Internet Explorer (IE), FireFox, Google Chrome, Opera,...
- ❖ Trình chủ (server) tiếp nhận và xử lý các yêu cầu từ trình khách, ví dụ: Apache, IIS,...
- ❖ HTTPS cung cấp cơ chế bảo mật thông tin khi chuyển chúng xuyên qua mạng

Thanh Vân - CNTT

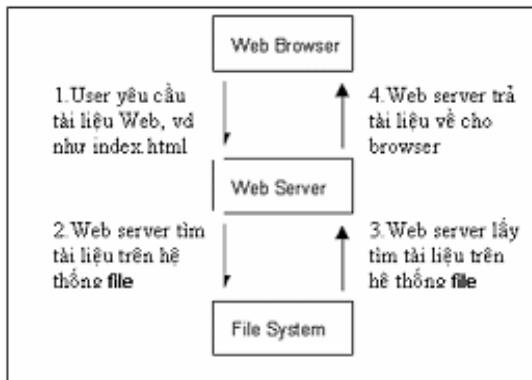
Các phiên bản

- HTTP 0.9, (World Wide Web - W3C) công bố năm 1991
- HTTP 1.0, [RFC 1945](#) (1996) cho phép thông điệp định dạng kiểu giao thức mở rộng thư Internet đa chức năng MIME: như kiểu Text, Image, Audio, Video, Application.
- HTTP 1.1: [RFC 2608](#) (1997) -> [RFC 2616](#) (1999).
HTTP 1.1 có các yêu cầu nghiêm ngặt hơn để đảm bảo tính tin cậy khi thực hiện các tính năng của nó

II. Hoạt động của Web Server

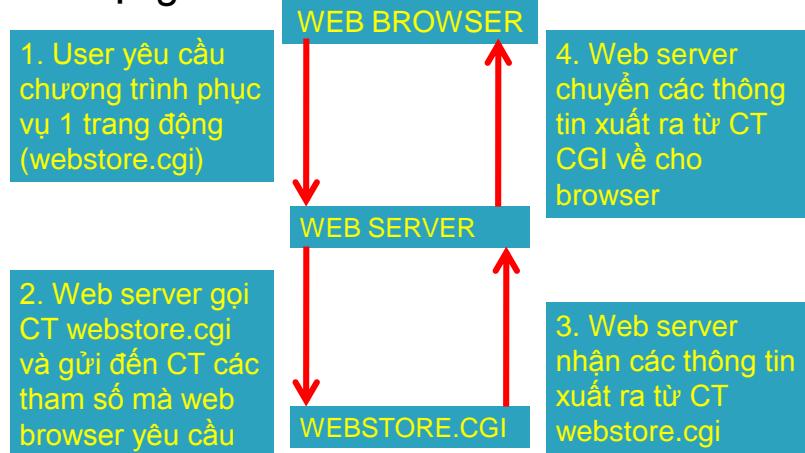
❖ Web tĩnh:

- Ban đầu Web Server chỉ phục vụ các tài liệu HTML và hình ảnh đơn giản.
- Web Server ở mức độ cơ bản, nó chỉ phục vụ các nội dung tĩnh.



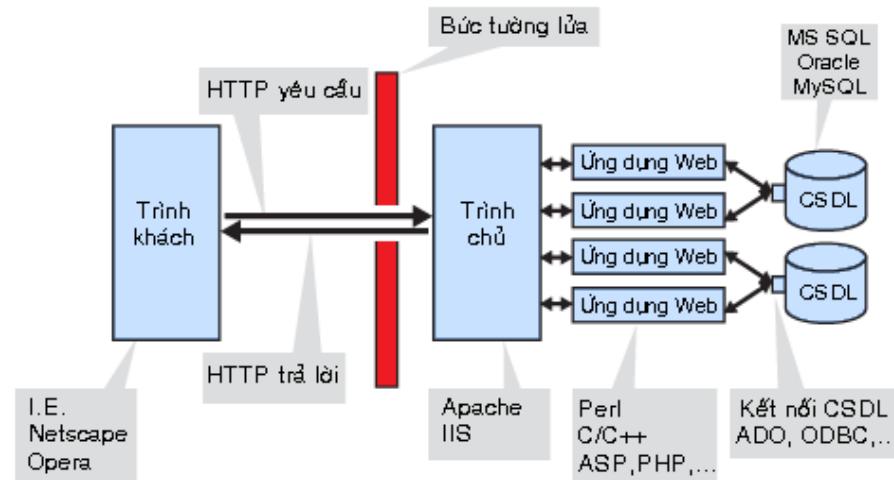
II. Hoạt động của Web Server

- Web động:



Thanh Vân - CNTT

II. Hoạt động của Web Server

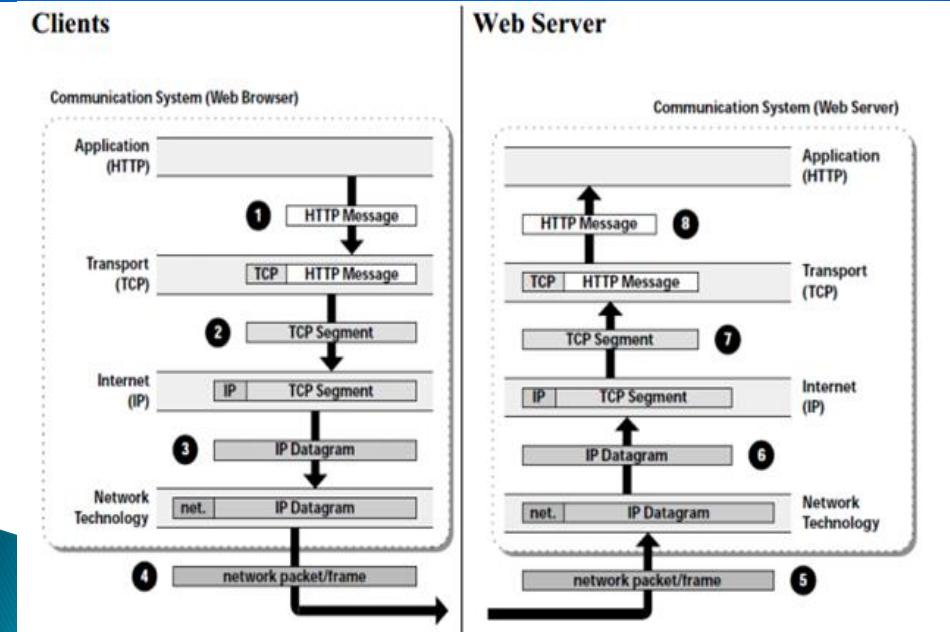


Thanh Vân - CNTT

HTTP: URI, URL, URN

- HTTP cho phép một tập các phương thức hoặc câu lệnh (methods/commands) và các tiêu đề mở-đóng (open-ended header) để chỉ ra mục đích của một yêu cầu.
- HTTP được xây dựng trên nguyên tắc tham chiếu được cung cấp bởi:
 - định danh tài nguyên thống nhất (Uniform Resource Identifier - URI), hoặc
 - định vị tài nguyên thống nhất (Uniform Resource Locator - URL) hay
 - tên tài nguyên thống nhất (Uniform Resource Name - URN),
=> nhằm chỉ ra nguồn tài nguyên áp dụng phương thức.
- Thông điệp được gửi theo định dạng tương tự với định dạng sử dụng thư Internet theo quy định của MIME.

HTTP with TCP/IP



Mô hình HTTP

Mô hình đơn giản: User Agent – Origin Server

Chuỗi yêu cầu ----->

UA -----v----- O

<----- Chuỗi đáp ứng

Mô hình phức tạp: User Agent ... Origin Server

Chuỗi yêu cầu ----->

UA -----v----- A -----v----- B -----v----- C -----v----- O

<----- Chuỗi đáp ứng

Mô hình HTTP

Mô hình phức tạp với bộ nhớ cache

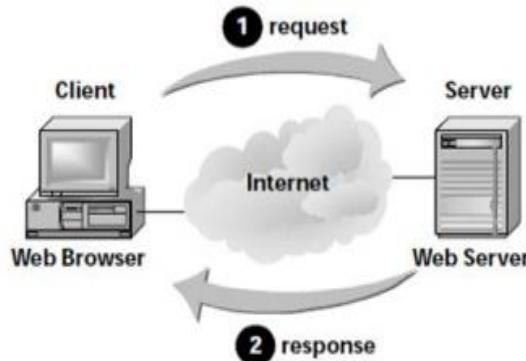
Chuỗi yêu cầu ----->

UA -----v----- A -----v----- B -----v----- C -----v----- O

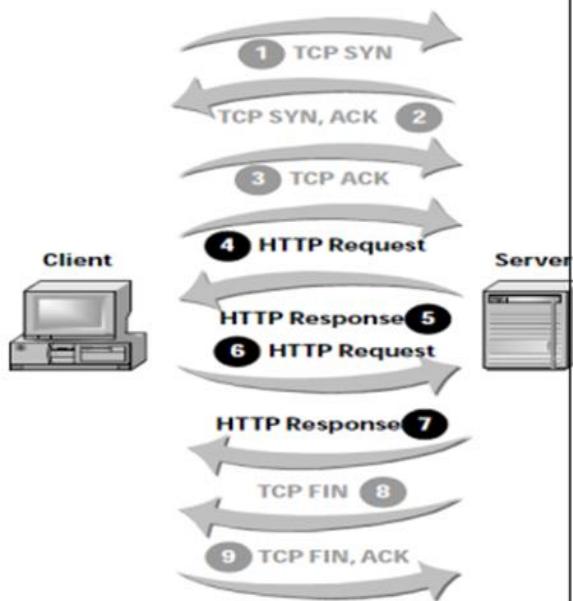
<----- Chuỗi đáp ứng

Hoạt động

- Connection: TCP connection
- Duy trì trạng thái kết nối (Persistence)

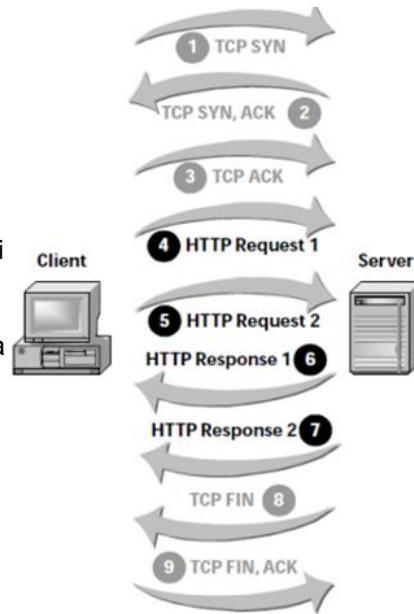


Persistence



Pipelining

- PipeLining: nhằm cải thiện hiệu năng.
- PipeLining cho phép
 - Client không phải đợi phản hồi từ Server cho một yêu cầu trước đó rồi mới được thực hiện 1 yêu cầu khác mà nó cho phép Client gửi nhiều yêu cầu cùng lúc trong khi chưa nhận được phản hồi từ Server.



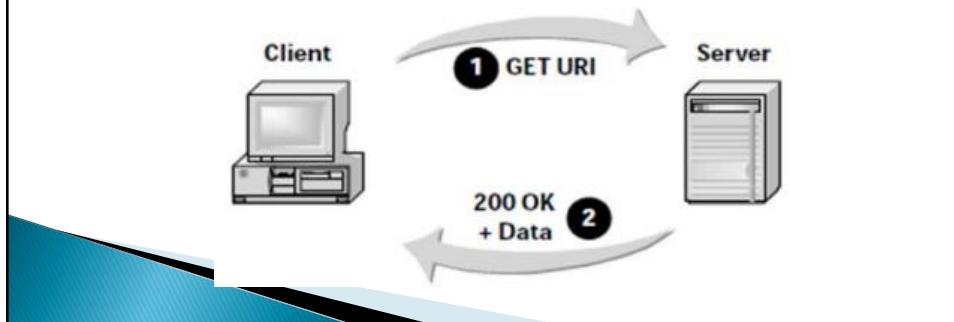
Các methods cơ bản

- **GET** – Web Page Retrieval
- **POST**
- **PUT**
- **DELETE**
- **OPTION**
- **HEAD**
- **TRACE**

Các methods cơ bản: GET

- **GET – Web Page Retrieval:**

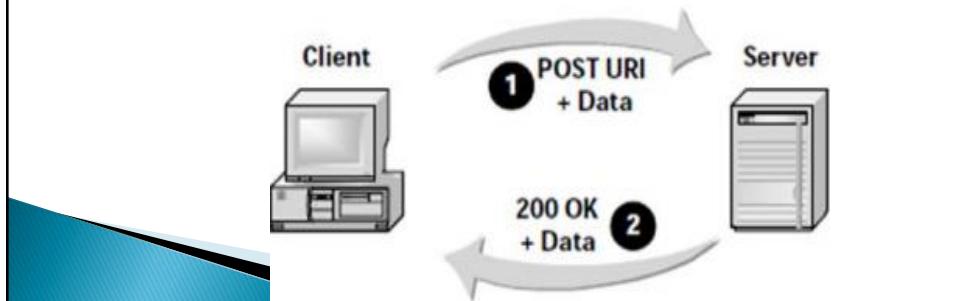
- GET là thao tác đơn giản nhất trong 4 thao tác được định nghĩa trong HTTP.
- GET là cách mà Client lấy một đối tượng hoặc tài nguyên nào đó từ Server.



Các methods cơ bản: POST

- **POST – Web Form:**

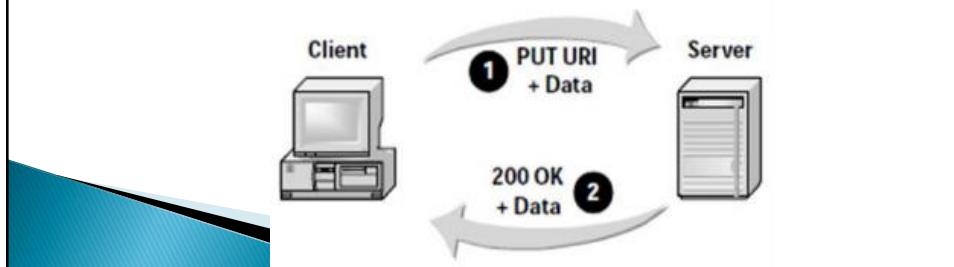
- POST là cách thức mà Client gửi thông tin lên cho Server. Các browser thường sử dụng phương thức POST để gửi 1 form lên Server
- URI xác định đối tượng có thể xử lý dữ liệu – chương trình hoặc script



Các methods cơ bản: PUT

- **PUT – File Upload:**

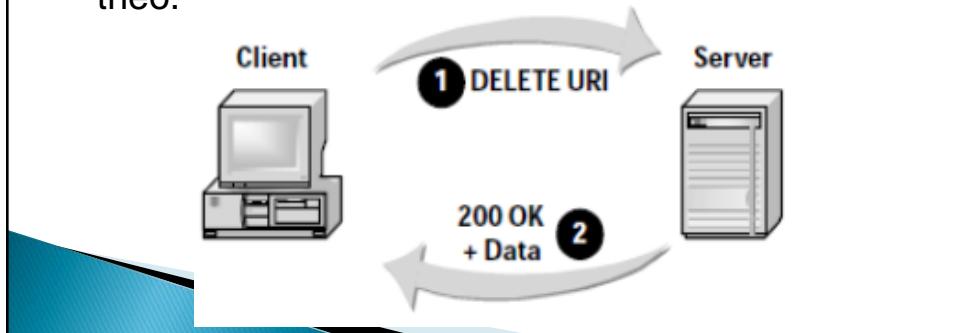
- PUT cũng là cách thức để Client gửi dữ liệu lên cho Server
- URI xác định đối tượng mà Server có thể đặt dữ liệu (một đường dẫn hoặc tên file)



Các methods cơ bản: DELETE

- **DELETE**

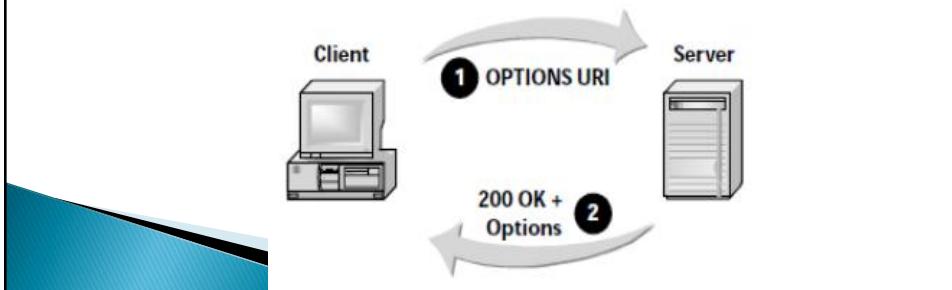
- Client gửi yêu cầu cùng với URI của đối tượng cần xóa trên Server.
- Server sẽ trả về “status code” và dữ liệu kèm theo.



Các methods cơ bản: OPTION

- **OPTIONS:**

- Các Client sử dụng thông điệp OPTIONS để biết được khả năng của một máy chủ.
- Nếu Client gửi thông điệp OPTIONS cùng với URI thì Server sẽ hồi đáp bằng 1 tùy chọn phù hợp với đối tượng mà Client yêu cầu.



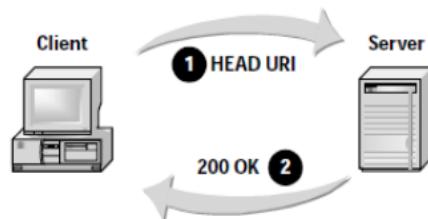
Các methods cơ bản: HEAD

- **HEAD:**

- Giống như của GET. Nhưng ko trả về đối tượng thật sự được yêu cầu. Cụ thể, Server chỉ trả về mã trạng thái chứ không trả về dữ liệu.
- Client sử dụng HEAD khi muốn kiểm tra một đối tượng có tồn tại hay chưa nhưng không muốn lấy đối tượng đó.

Ví dụ: Có thể sử dụng thông điệp HEAD để đảm bảo liên kết đến một đối tượng hợp lệ mà không tiêu tốn băng thông.

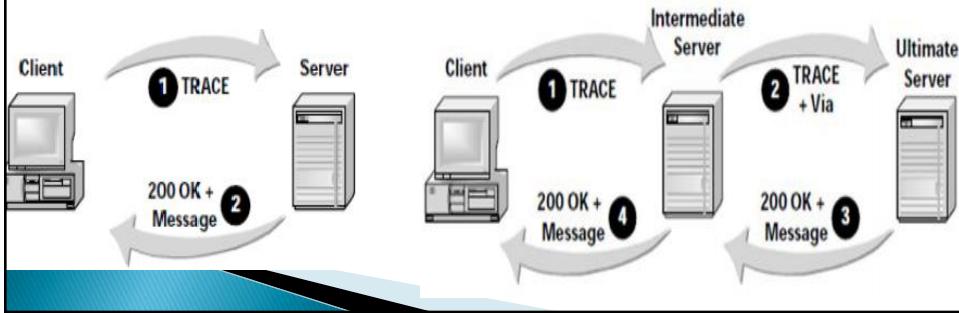
- Cache trong trình duyệt cũi điệp HEAD để xem một đc không



Các methods cơ bản: TRACE

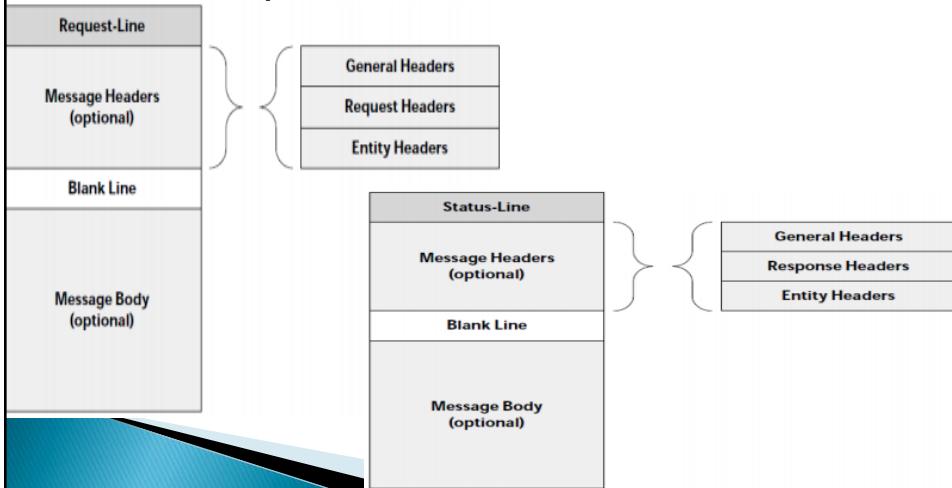
- **TRACE:**

- Thông điệp TRACE là cách mà Client dùng để kiểm tra đường mạng dẫn đến Server.
- Khi Server nhận được 1 thông điệp TRACE, Server sẽ hồi đáp bằng cách copy thông điệp TRACE vào thông điệp hồi đáp.



Thông điệp HTTP

- HTTP Request
- HTTP Response



III. Đặc điểm của IIS .

- IIS - Internet Information Services là các dịch vụ dành cho máy chủ chạy trên nền Hệ điều hành Window nhằm cung cấp và phân tán các thông tin lên mạng, nó có nhiều dịch vụ: Web Server, FTP Server,...
- Nhiệm vụ của IIS là tiếp nhận yêu cầu của máy trạm và đáp ứng lại yêu cầu đó bằng cách gửi về máy trạm những thông tin mà máy trạm yêu cầu.
- IIS sử dụng các giao thức mạng phổ biến là **HTTP ,** **FTP, SMTP**

Thanh Vân - CNTT

III. Đặc điểm của IIS

- IIS được cài trong secure mode
- Hỗ trợ nhiều tính năng chứng thực:
 - ✓ [Anonymous Authentication](#): ko dùng username/pass
 - ✓ [Basic Authentication](#): Có dùng username/pass (plaintext)
 - ✓ [Digest Authentication](#): u/p có mã hóa
 - ✓ [Windows Authentication](#): Dùng kỹ thuật băm (NTLM or Kerberos protocols) để xác nhận thông tin của users.
 - ✓ [Client Certificate Mapping Authentication](#)

Server tạo ra các giấy Client Certificate và yêu cầu Client khi truy xuất tới Server thì phải gửi giấy chứng nhận.

- ✓ [Forms Authentication](#)

Cho phép user logon vào một form (html logon page) để chứng thực

- ✓ [ASP.NET Impersonation Authentication](#)

Có thể dùng ứng dụng ASP.NET dưới sự bảo mật khác với bảo mật mặc định của ASP.NET

Thanh Vân - CNTT

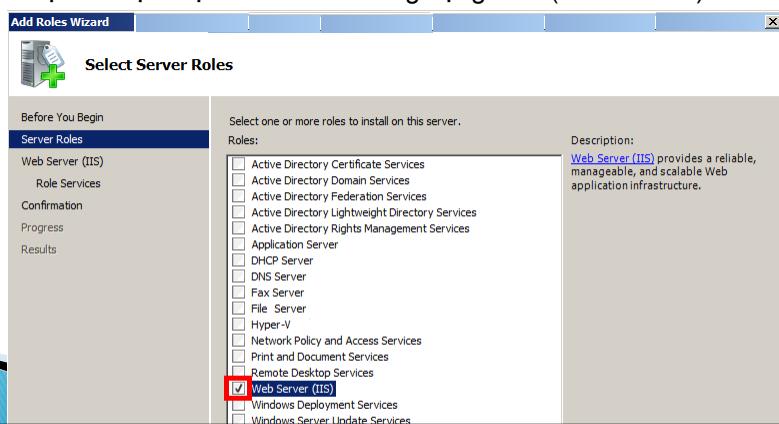
IIS 7.0

- ❖ Ưu điểm so với IIS 6.0:
 - ❖ với những cải tiến tốc độ,
 - ❖ độ ổn định và khả năng an ninh,
 - ❖ máy chủ web uyển chuyển và dễ dùng,
 - ❖ đủ mạnh để chạy các ứng dụng web trong tương lai

Thanh Vân - CNTT

IV. Cài đặt IIS 7.0

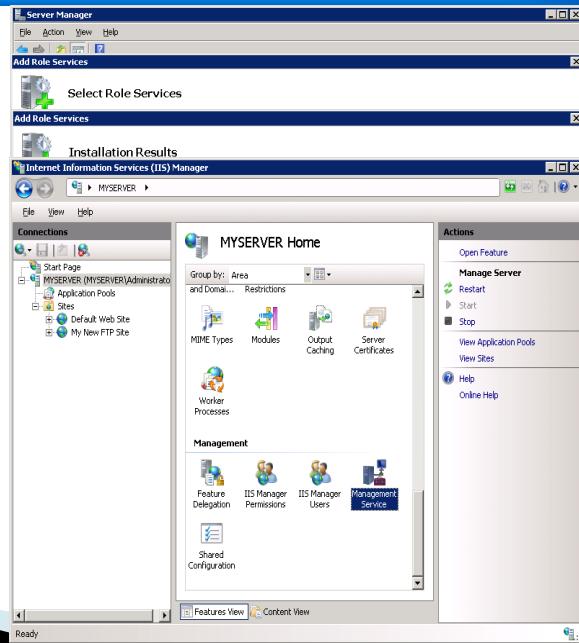
- ❖ Start Menu \ Server Manager (hoặc có thể chọn ở : Start Menu – Administrative Tools – Server Manager).
 - Trong “Roles” chọn “Add Roles”. Click chọn “Web Server (IIS)” ở mục Roles. Chọn “Next”.
 - Chọn cài đặt các dịch vụ cần thiết cho ứng dụng Web(ASP.NET...)
 - Finish



Thanh Vân - CNTT

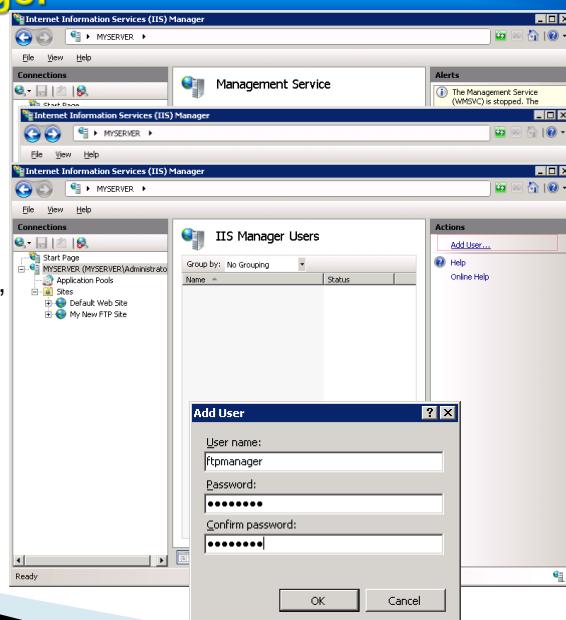
Cài đặt dịch vụ quản trị của IIS

- Vào “Server Manager” – Trong “Roles” mục “Role Services” chọn “Add Role Service”.
- chọn “Management Service”
- Install\Close.
- Giao diện



Configure the IIS Management Service and Add an IIS 7 Manager

- Open IIS 7 Manager. In the **Connections** pane, click the server\ Double-click the **Management Service**
- Double-click the **IIS Manager Users** |
- **IIS Manager Users** feature, click **Add User** in the **Actions** pane.



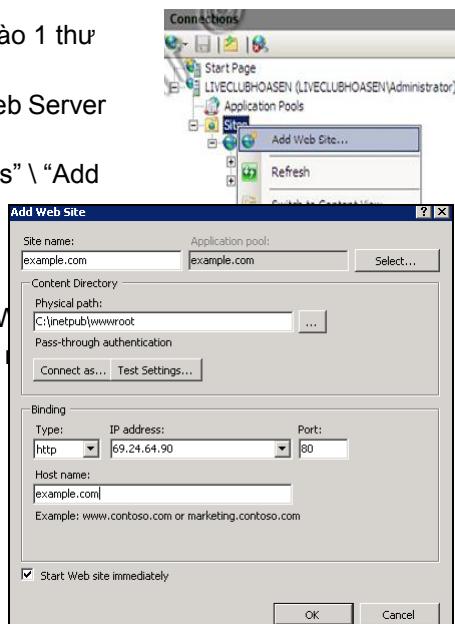
V. Cấu hình Web services

1. Tạo mới một Web site.
2. Tạo Virtual Directory.
3. Cấu hình chứng thực cho Web Site
4. Cấu hình Web Hosting.
5. Sao lưu và phục hồi cấu hình Web Site.

Thanh Vân - CNTT

1. Tạo mới một Web site.

- Chuẩn bị nguồn web (vd.html), lưu vào 1 thư mục: (Default: C:\inetpub\wwwroot)
- “Server Manager” chọn “Roles” - “Web Server (IIS)” - “Internet Information Server”.
- Phía bảng “Connections”, chọn “sites” \ “Add Web Site”.
- Cần cung cấp các thông tin:
 - Name,
 - Physical path: thư mục home của Web Site
 - Connect as: Select the connection
 - Binding:
 - Type: HTTP.
 - Chỉ định IP. Port
 - Host name: Chỉ định tên host (đã được phân giải = DNS)

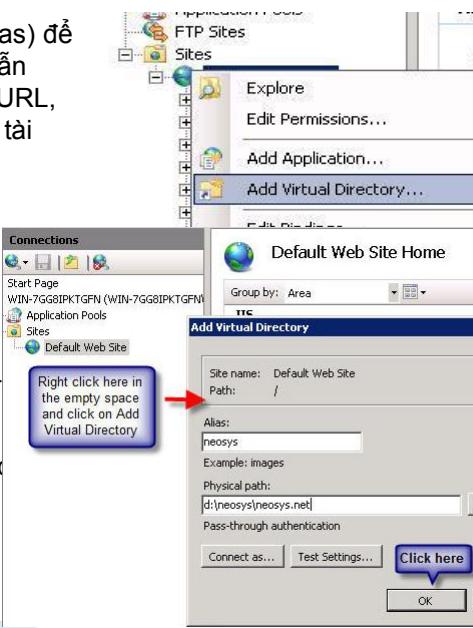


Thanh Vân - CNTT

2. Tạo Virtual Directory.

- (Virtual Directory hay còn gọi là Alias) để ánh xạ một tài nguyên từ đường dẫn thư mục vật lý thành đường dẫn URL, thông qua đó ta có thể truy xuất tài nguyên này qua Web Browser.
- Thực hiện:
 - Web Site \ Add Virtual Directory
 - Alias: chỉ định tên alias
 - Physical path:
Chỉ định thư mục cục bộ hoặc đường dẫn mạng cần ánh xạ,
 - Connect as... : Select the connection method
 - OK
 - Test: [http://\[IP\]/aliasname](http://[IP]/aliasname)

Thanh Vân - CNTT



3. Bảo mật cho Web Site

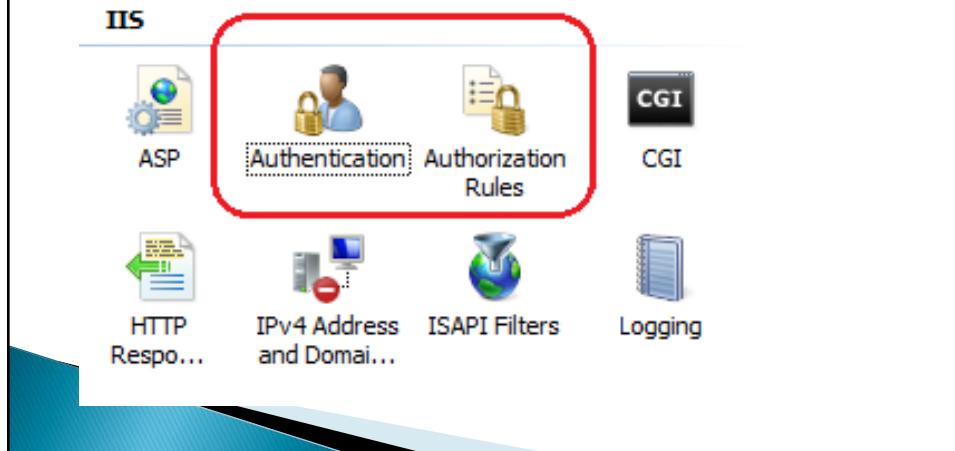
Một số tính năng bảo mật cho Web Site như:

- ❖ Authentication And Access Control:
6 phương thức chứng thực, kết hợp quyền
- ❖ IP address and domain name restriction:
Cung cấp một số tính năng giới hạn host và network truy xuất vào Web Site.
- ❖ Secure communication: bảo mật trong giao tiếp giữa Client và Server: [Client Certificate Mapping Authentication](#)

Server tạo ra các giấy Client Certificate và yêu cầu Client khi truy xuất tới Server thì phải gửi giấy chứng nhận

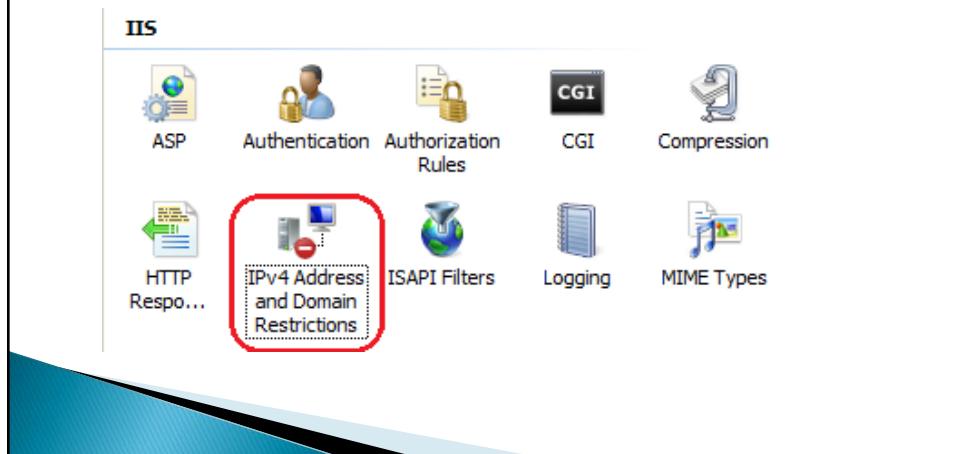
Bảo mật cho Web Site (1)

Authentication And Access Control:



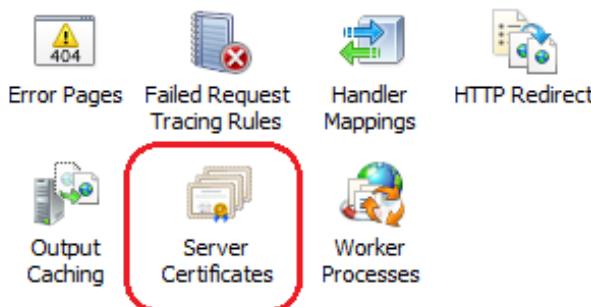
Bảo mật cho Web Site (2)

IP address and domain name restriction:



Bảo mật cho Web Site (3)

Secure communication (Client Certificate):



3.1. Cấu hình chứng thực cho Web Site

Các kiểu chứng thực Web Site như:

- Anonymous Authentication: ko dùng username/pass
- Basic Authentication: Có dùng username/pass (plaintext)
- Digest Authentication: u/p có mã hóa
- Windows Authentication: Dùng kỹ thuật băm (NTLM or Kerberos protocols) để xác nhận thông tin của users. (same domain)
- Forms Authentication

Cho phép user logon vào một form (html logon page) để chứng thực

- ASP.NET Impersonation Authentication

Có thể dùng ứng dụng ASP.NET dưới sự bảo mật khác với bảo mật mặc định của ASP.NET

3.1. Cấu hình chứng thực cho Web Site

- Chọn Enable:
kích hoạt kiểu chứng thực
- Chọn Action>Edit:
để thiết lập cấu hình cho từng loại
chứng thực

The screenshot shows the IIS Manager interface. On the left, the 'Connections' tree shows 'WebServer' with 'Application Pools' and 'Sites'. Under 'Sites', 'Default Web Site' is expanded, showing 'aspnet_client', 'hmpweb', and 'hmplogin'. A red arrow points from the 'Default Web Site' node in the tree to the 'Windows Authentication' row in the main table. On the right, the 'Authentication' table lists several authentication methods:

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	HTTP 401 Challenge
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

A context menu is open over the 'Windows Authentication' row, with the 'Enable' option highlighted. Other options in the menu include 'Help' and 'Online Help'.

3.2. Hạn chế truy nhập website

The screenshot shows the 'Role Services' configuration page. On the left, there's a sidebar with 'Confirmation', 'Progress', and 'Results'. The main area displays a graphic of a computer monitor and server tower with a red 'stop' sign overlay. Below the graphic, the text 'IPv4 Address and Domain...' is visible. On the right, a large list of role services is shown, with 'IP and Domain Restrictions' checked under the 'Security' section.

Role Services	Status
ISAPI Filters	<input checked="" type="checkbox"/>
Server Side Includes	<input type="checkbox"/>
Health and Diagnostics	<input type="checkbox"/>
HTTP Logging	<input checked="" type="checkbox"/>
Logging Tools	<input type="checkbox"/>
Request Monitor	<input checked="" type="checkbox"/>
Tracing	<input type="checkbox"/>
Custom Logging	<input type="checkbox"/>
ODBC Logging	<input type="checkbox"/>
Security	<input type="checkbox"/>
Basic Authentication	<input checked="" type="checkbox"/>
Windows Authentication	<input checked="" type="checkbox"/>
Digest Authentication	<input checked="" type="checkbox"/>
Client Certificate Mapping Authentication	<input checked="" type="checkbox"/>
IIS Client Certificate Mapping Authentication	<input checked="" type="checkbox"/>
URL Authorization	<input type="checkbox"/>
Request Filtering	<input checked="" type="checkbox"/>
IP and Domain Restrictions	<input checked="" type="checkbox"/>
Performance	<input type="checkbox"/>
Static Content Compression	<input checked="" type="checkbox"/>

4. Cấu hình Web Hosting.

- ❖ IIS cho phép ta tạo nhiều Web Site trên một Web Server (Web Hosting)
- ❖ Cần khai báo các thông số như:
 - ❖ host header name,
 - ❖ địa chỉ IP và
 - ❖ số hiệu cổng Port.
- ❖ Có 3 cách tạo
 - ❖ Tạo nhiều Web Site dựa vào Host Names: Named-based
chỉ cần một IP để đại diện cho tất cả các host name.
 - ❖ Tạo nhiều Web Site dựa vào địa chỉ IP: IP-based
Tương ứng một tên Web Site ta phải cung cấp 1 IP.
 - ❖ Tạo nhiều Web Site dựa vào Port: Port-based

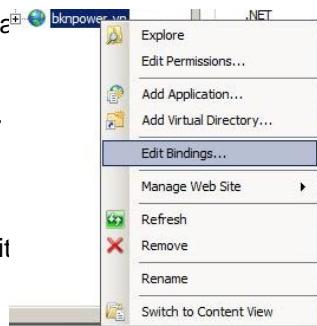
Thanh Vân - CNTT

Cấu hình Web Hosting: Named-based

- ❖ Tạo nhiều Web Site dựa vào Host Header Names:
- ❖ Các bước tạo:
 - ❖ Dùng DNS hoặc file hosts để ánh xạ tên (hostname) và IP.
 - ❖ Cùng 1 IP phân giải thành nhiều tên khác nhau
 - ❖ Tạo các thư mục chứa các website khác nhau.
 - ❖ Tạo các Web site: Click Add Web Sites
 - ❖ Nhập Site name
 - ❖ Physical path: Chỉ định thư mục chứa web site
 - ❖ Binding: Type (HTTP), IP (All Unsigned), Port (80)
 - ❖ Host name: tên host đã được phân giải ở trên
 - ❖ OK để hoàn tất quá trình
- ❖ Test: đăng nhập vào các website khác nhau đã tạo trên

Thanh Vân - CNTT

Cấu hình Web Hosting: IP-based

- ❖ Tạo nhiều Web Site dựa vào IP:
- ❖ Các bước tạo:
 - ❖ Ta phải thêm nhiều địa chỉ IP cho card mạng. 1 website – 1 IP
 - ❖ Dùng DNS hoặc file hosts để ánh xạ tên (hostname) 
 - ❖ 1 IP phân giải thành 1 tên host tương ứng.
 - ❖ Tạo các thư mục chứa các website khác nhau.
 - ❖ Tạo các Web site: Click Add Web Sites
 - ❖ Nhập Site name
 - ❖ Physical path: Chỉ định thư mục chứa web site
 - ❖ Binding: Edit Binding để thêm các IP
 - ❖ Host name: tên host tương ứng với IP đã được phân giải
 - ❖ OK để hoàn tất quá trình
- ❖ Test: đăng nhập vào các website khác nhau đã tạo trên

Thanh Văn - CNTT

Cấu hình Web Hosting: Port-based

- ❖ Tạo nhiều Web Site dựa vào port:
- ❖ Các bước tạo:
 - ❖ Dùng DNS hoặc file hosts để ánh xạ tên (hostname) và IP.
 - ❖ Cùng 1 IP phân giải thành nhiều tên khác nhau
 - ❖ Tạo các thư mục chứa các website khác nhau.
 - ❖ Tạo các Web site: Click Add Web Sites
 - ❖ Nhập Site name
 - ❖ Physical path: Chỉ định thư mục chứa web site
 - ❖ Binding: Type (HTTP), IP (1.1.1.1), Port (80, 8080...)
 - ❖ Host name: tên host đã được phân giải ở trên
 - ❖ OK để hoàn tất quá trình
- ❖ Test: đăng nhập vào các website + port khác nhau đã tạo trên

Thanh Văn - CNTT

6. Sao lưu và phục hồi cấu hình Web Site

- ❖ IIS lưu trữ thông tin cấu hình theo định dạng Extensible Markup Language (XML) có tên: lưu ở:systemroot\System32\Inetsrv
 - ❖ MetaBase.xml và
 - ❖ MBSchema.xml
- ❖ Có thao tác trực tiếp vào hai tập tin này để thay đổi thông tin cấu hình về IIS.
- ❖ Lưu thông tin cấu hình
 - ❖ Click phải vào tên Web Site \chọn All Task, \Save Configuration to a file
 - ❖ Sau đó ta chỉ định tập tin cấu hình, đường dẫn thư mục lưu trữ thông tin cấu hình,
 - ❖ mật khẩu mã hóa cho tập tin cấu hình.

Thanh Vân - CNTT

6. Sao lưu và phục hồi cấu hình Web Site

- ❖ Phục hồi cấu hình Web Site từ file cấu hình *.XML:
 - ❖ Click phải vào tên thư mục Web Sites chọn New, chọn Web Site (from file)...
 - ❖ sau đó hộp thoại Import configuration:
 - ❖ Chỉ định tập tin cấu hình từ nút Browse...
 - ❖ Click Read File,
 - ❖ tập tin chỉ định được Import vào hộp thoại Select a configuration to import,
 - ❖ OK để hoàn tất quá trình

Thanh Vân - CNTT

Thực hành

- Thực hành theo yêu cầu

Thanh Vân - CNTT