tụ, các Router sẽ trao đổi với nhau nếu có sự thay đổi về đường đi xảy ra.

D. Router trao đổi các gói tin LSA với nhau và chạy thuật toán tìm đường đi ngắn nhất dựa trên cơ sở dữ liệu LSA này.

1. Giá trị AD (Administrative Distance) mặc định của OSPF là? A. 90.

B. 110.

C. 120.

D. 150.

1. Giá trị AD (Administrative Distance) mặc định của RIP là? A. 90.

B. 110.

C. 120.

D. 150.

1. Giá trị AD (Administrative Distance) mặc định của Static Routing là? A. 90.

B. 110.

C. 120.

D. 1.

1. Một VLAN là một tập các thiết bị nằm cùng miền .
   1. Autonomous System.
   2. Broadcast Domain.
   3. Bandwidth Domain.
   4. Collision Domain.
2. Thiết bị nào sau đây được dùng để kết nối các VLAN?
   1. Switch.
   2. Bridge.
   3. Router.
   4. Hub.
3. Giao thức nào sau đây được dùng để phân phối thông tin về cấu hình VLAN đến các Switch khác trong mạng?
   1. STP.
   2. VTP.
   3. EIGRP.
   4. SNMP.
   5. CDP.
4. Giao thức STP dùng để làm gì?
   1. Dùng để cập nhật định tuyến trong môi trường Switch.
   2. Dùng để chống “Routing Loop” trong mạng.
   3. Dùng để tránh “Switching Loop” trong mạng.
   4. Dùng để quản lý việc thêm, xóa, sửa thông tin VLAN trong hệ thống có nhiều Switch.
   5. Dùng để phân hoạch mạng thành nhiều miền đụng độ.
5. Để kiểm tra Interface fa0/5 có được gán cho VLAN Sales không, thì ta sử dụng lệnh nào sau đây?
   1. Show vlan.
   2. Show mac-address-table.
   3. Show vtp status.
   4. Show spanning-tree root.
6. Show ip interface brief. Tại sao Switch không bao giờ học một địa chỉ “Broadcast”?
   1. Frame Broadcast không bao giờ được gửi tới Switch.
   2. Địa chỉ Broadcast sử dụng định dạng không đúng trong bảng chuyển mạch trên Switch.
   3. Địa chỉ Broadcast không bao giờ là địa chỉ nguồn trong một Frame.
   4. Địa chỉ Broadcast chỉ dùng trong Layer 3.
   5. Switch không bao giờ chuyển tiếp các gói tin Broadcast.
7. Cho mô hình mạng:

MAC: 0000.5e10.1200



**Fa0/1**

**SW1**

**Fa0/2**

**Fa0/1**

**Fa0/1**

MAC: 0000.6e10.1200

**Fa0/2 Fa0/2**

**SW2 SW3**

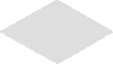
MAC: 0000.7e10.1200

Tất cả các Switches được cấu hình STP mặc định và tất cả các kết nối qua Port FastEthernet. Port nào sẽ chuyển vào trạng thái “Blocking”?

* 1. Switch SW1 - Port Fa0/1.
  2. Switch SW1 - Port Fa0/2.
  3. Switch SW2 - Port Fa0/2.
  4. Switch SW2 - Port Fa0/1.
  5. Switch SW3 - Port Fa0/1.
  6. Switch SW3 - Port Fa0/2.

1. Cho mô hình mạng:

**Router:**



**Interface fa0/1.1 encapsulation dot1q 10**

**ip address 192.168.1.65 255.255.255.192**

**Interface fa0/1.2 encapsulation dot1q 20**

**Router**

**Fa0/1**

**Fa0/1**

**ip address 192.168.1.129 255.255.255.224**

**Fa0/2**

**Fa0/3**

**Fa0/4**

**Switch:**

**Port Fa0/1: trunk**

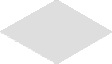
**Port Fa0/2, Fa0/3: VLAN 10 Port Fa0/4: VLAN 20**

**HA HB HC**

Những thông tin cấu hình nào sau đây là đúng cho các Host trong mô hình trên?

* 1. Địa chỉ IP của HA: 192.1.1.65.
  2. Subnet Mask của HA: 255.255.255.224.
  3. Địa chỉ IP của HB: 192.1.1.125.
  4. Default Gateway của HB: 192.1.1.65.
  5. Địa chỉ IP của HC: 192.1.1.66.
  6. Subnet Mask của HC: 255.255.255.224.

1. Cho mô hình mạng:



**VLAN 1**

**82 host**

**172.16.1.126**

**Router**

**Switch**

**VLAN 2**

**114 host**

**172.16.1.129**

Những phát biểu nào sau đây là đúng trong mô hình mạng trên?

* 1. Subnet Mask được sử dụng là 255.255.255.192.
  2. Subnet Mask được sử dụng là 255.255.255.128.
  3. Địa chỉ IP 172.16.1.25 có thể được gán cho các Host thuộc VLAN 1.
  4. Địa chỉ IP 172.16.1.205 có thể được gán cho các Host thuộc VLAN 1.
  5. Cổng LAN trên Router được cấu hình với một địa chỉ IP.
  6. Cổng LAN trên Router được cấu hình với nhiều địa chỉ IP.

1. Cho mô hình mạng:

**R(config)#interface fastethernet 0/1.1 R(config-if)#encapsulation dot1q 1**



**Router**

**VLAN 2**

**R(config-if)#ip address 192.168.1.1 255.255.255.0 R(config)#interface fastethernet 0/1.2**

**R(config-if)#encapsulation dot1q 2**

**R(config-if)#Ip address 192.168.2.1 255.255.255.0**

**R(config)#interface fastethernet 0/1.3**

**R(config-if)#encapsulation dot1q 3**

**R(config-if)#ip address 192.168.3.1 255.255.255.0**

Router trong mô hình mạng được cấu hình như trên. Switch kết nối với Router qua đường Trunk. Trên Switch cấu hình 3 VLAN: VLAN 1, VLAN 2, và VLAN 3. Một máy tính A kết nối vào VLAN 2. Hỏi địa chỉ **Default Gateway** phải đặt cho máy tính này là địa chỉ nào sau đây?

A. 192.168.1.1.

B. 192.168.1.2.

C. 192.168.2.1.

D. 192.168.2.2.

E. 192.168.3.1.

F. 192.168.3.2.

1. Hai tham số được STP sử dụng để bầu chọn “Root Bridge”?
   1. Bridge Priority.
   2. Địa chỉ IP.
   3. Địa chỉ MAC.
   4. Phiên bản IOS.
   5. Tốc độ kết nối.

# CHƯƠNG 5

**DỊCH VỤ MẠNG**

Chương này trình bày đặc điểm và nguyên tắc hoạt động của một số dịch vụ phổ biến dùng trong hệ thống mạng như DHCP, DNS, Web, FTP, E-mail. Học xong chương này, người học có khả năng:

* Trình bày được vai trò, đặc điểm và nguyên tắc hoạt động của một số dịch vụ mạng phổ biến như DHCP, DNS, Web, FTP, E-mail.
* Cấu hình được các dịch vụ DHCP, DNS, Web, FTP, E-mail.
* Thiết kế được các loại ứng dụng trong một hệ thống mạng cụ thể.

## Tổng quan

Mỗi dịch vụ mạng cung cấp các chức năng giúp người dùng tương tác với các ứng dụng trên mạng. Xét ở góc độ quản trị hệ thống, việc hiểu rõ về nguyên tắc hoạt động, cài đặt và cấu hình các dịch vụ này rất quan trọng để vận hành tốt hệ thống mạng. Một số dịch vụ mạng phổ biến được trình bày trong chương này gồm:

* + - Dịch vụ DHCP: Là dịch vụ cấp phát địa chỉ IP tự động cho các người dùng trong hệ thống mạng.
    - Dịch vụ DNS: Dịch vụ phân giải tên miền.
    - Dịch vụ Web: Dịch vụ cung cấp trang Web cho người sử dụng truy cập.
    - Dịch vụ FTP: Dịch vụ truyền tập tin trên mạng.
    - Dịch vụ E-mail: Dịch vụ thư điện tử.

## Dịch vụ DHCP

### Giới thiệu

Dịch vụ DHCP cung cấp địa chỉ IP tự động cho các thiết bị trong mạng. Đây là một dịch vụ được sử dụng phổ biến đơn giản hóa trong việc cấu hình, quản lý địa chỉ trong mạng.

DHCP hoạt động theo dạng Client/Server. Máy chủ đóng vai trò DHCP Server được cấu hình các tham số để cấp phát. Các tham số gồm: tên, địa chỉ mạng, dãy địa chỉ cấp phát, Default Gateway, địa chỉ DNS, thời gian người dùng sử dụng địa chỉ IP này.

### Nguyên tắc hoạt động Trường hợp 1:

Quá trình trao đổi thông tin giữa DHCP Server và DHCP Client trong trường hợp chúng nằm cùng miền quảng bá diễn ra như sau:

# DHCP

**client**

**Switch**

DHCPDISCOVER DHCPOFFER DHCPREQUEST



DHCPACK

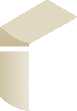
**DHCP**

**server**

***Hình 5.1:*** *DHCP Server và Client cùng miền quảng bá*

* Bước 1: DHCP Client gửi gói tin DHCPDISCOVER dạng Broadcast đến DHCP Server.
* Bước 2: DHCP Server gửi lại gói DHCPOFFER dạng Broadcast cho DHCP Client.
* Bước 3: DHCP Client gửi gói DHCPREQUEST dạng Broadcast cho DHCP Server.
* Bước 4: DHCP Server gửi gói DHCPACK dạng Broadcast cho DHCP Client.

**Trường hợp 2:** DHCP Client và DHCP Server nằm khác miền quảng bá (khác mạng).



**DHCP Relay Agent**

Network3:

**192.168.12.0/30**

**R1**

Gi0/0

Gi0/1

Gi0/1

**R2**

Gi0/0

(2)

(1)

(4)

(3)

**DHCP**

**client**

**DHCP**

**server**

Network2:

**172.16.10.0/24**

Network1:

**172.16.20.0/24**

***Hình 5.2:*** *DHCP Server và Client khác miền quảng bá*

Trong trường hợp DHCP Server và DHCP Client nằm khác miền quảng bá, thì cần thiết phải sử dụng một thiết bị trung gian (gọi là DHCP Relay Agent hay DHCP Helper) để chuyển tiếp yêu cầu từ DHCP Client đến DHCP Server. Bởi vì, trong trường hợp này các gói tin (Local) Broadcast từ Client bị Router chặn nên sẽ không đến được DHCP Server.

Trong hình trên, Router R1 đóng vai trò là thiết bị trung gian giữ vai trò chuyển tiếp các gói tin xin IP của các Client trong Network 2 đến DHCP Server đang ở Network 1. Chi tiết quá trình này diễn ra như sau:

* Bước 1: DHCP Client gửi gói tin DHCPDISCOVER dạng Broadcast.
* Bước 2: DHCP Relay Agent (R1) nhận được gói tin DHCPDISCOVER và chuyển tiếp gói tin này (dạng Unicast) đến DHCP Server.
* Bước 3: DHCP Server gửi lại gói DHCPOFFER (Unicast) trả lời cho R1.
* Bước 4: R1 phát lại gói DHCPOFFER (dạng Broadcast) cho DHCP Client.
* Bước 5: DHCP Client gửi gói DHCPREQUEST dạng Broadcast.
* Bước 6: R1 chuyển tiếp gói DHCPREQUEST cho DHCP Server.
* Bước 7: DHCP Server gửi gói DHCPACK (Unicast) trả lời cho R1.
* Bước 8: R1 phát gói DHCPACK (dạng Broadcast) cho DHCP Client.

Trong quá trình Client thuê IP từ DHCP Server, khi đến 50% thời gian thuê, Client gửi gói tin DHCPREQUEST để kiểm tra DHCP Server có còn tồn tại trên hệ thống không. Nếu DHCP Server không trả lời bằng gói tin DHCPACK thì đến 87,5% thời gian thuê, Client sẽ gửi thêm lần nữa. Nếu không nhận tín hiệu trả lời từ DHCP Server thì Client sẽ phát gói tin DHCPDISCOVER để tìm kiếm và xin IP từ các DHCP Server trên mạng.

Trong quá trình liên lạc giữa DHCP Client và DHCP Server, DHCP Server lắng nghe các thông tin yêu cầu cấp phát IP ở Port 67 (UDP) và Client sử dụng Port 68 (UDP) để trao đổi với DHCP Server.

Ví dụ về các thông số địa chỉ của các gói tin trao đổi giữa DHCP Client và DHCP Server.

|  |  |
| --- | --- |
| Gói tin | SMac = Địa chỉ MAC của máy gửi (Client) |
| DHCPDISCOVER | DMac = FF:FF:FF:FF:FF:FF |
|  | SIP = 0.0.0.0, DIP = 255.255.255.255 |
|  | Sport = 68, Dport = 67 |
| Gói tin DHCPOFFER | SMac = Địa chỉ MAC của máy gửi (Server) DMac = địa chỉ MAC của Client  SIP = IP của Server, DIP = 255.255.255.255  Sport = 67, Dport = 68 |
| Gói tin | SMac = Địa chỉ MAC của máy gửi (Client) |
| DHCPREQUEST | DMac = FF:FF:FF:FF:FF:FF |
|  | SIP = 0.0.0.0, DIP = 255.255.255.255 |
|  | Sport = 68, Dport = 67 |
| Gói tin DHCPACK | SMac = Địa chỉ MAC của máy gửi (Server) DMac = địa chỉ MAC của Client  SIP = IP của Server, DIP = IP được cấp cho Client  Sport = 67, Dport = 68 |

### Cấu hình cấp phát IP động

Trên DHCP Server thiết lập cấp phát IP động cho một mạng gọi là Scope, các tham số cấu hình cho mỗi Scope gồm:

* + - * Scope Name (Pool): Tên mô tả cho mạng cần cấp phát.
      * Network: Địa chỉ mạng.
      * IP Range: Xác định dãy địa chỉ IP sẽ cấp phát (xác định địa chỉ đầu và địa chỉ cuối, hoặc xác định địa chỉ đầu và số lượng IP cần cấp phát).
      * Lease Duration: Thời gian thuê IP.
      * DNS Server: IP của DNS Server để phân giải tên miền.
      * Default Gateway: Địa chỉ Default Gateway là địa chỉ IP của Router.
      * Reservation: IP dành riêng một thiết bị.

Hai tham số DNS và Default Gateway là các giá trị chọn lựa, không bắt buộc, tùy vào mô hình mạng mà người quản trị có sử dụng hay không.

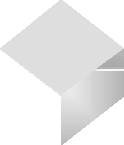
### Cấu hình DHCP trên Windows Server

Client

**Network: 192.168.12.0/24**

DHCP

server



Scope Name: **P-KeToan**

Network: **192.168.12.0/24**

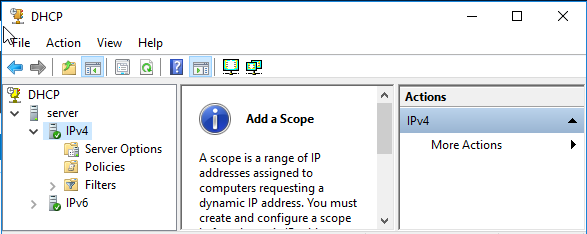
IP Range: 1**92.168.12.50 – 192.168.12.200**

Default-Gateway: **192.168.12.1**

DNS: **8.8.8.8**

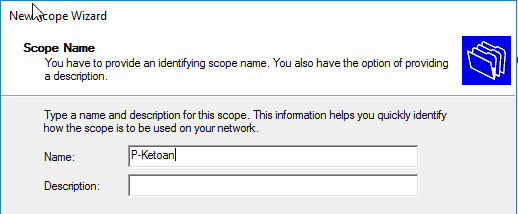
***Hình 5.3:*** *Mô hình cài đặt thử nghiệm DHCP Server*

Cửa sổ cấu hình trên Windows Server:

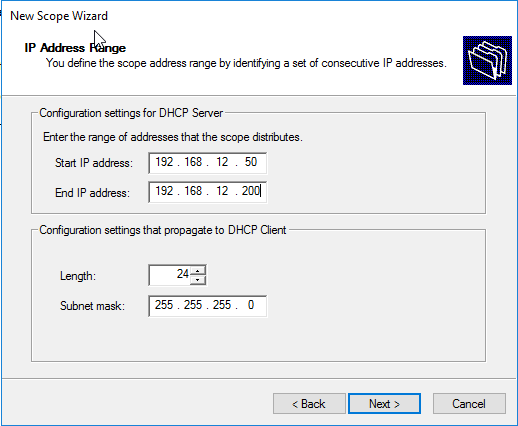


***Hình 5.4:*** *Giao diện cấu hình DHCP Server trên Window Server*

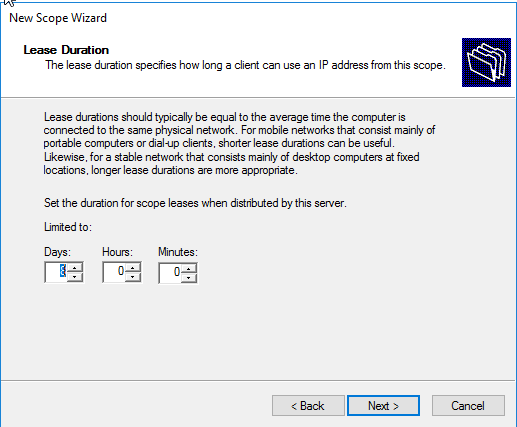
Click chuột phải vào **IPv4**, chọn **New Scope.**



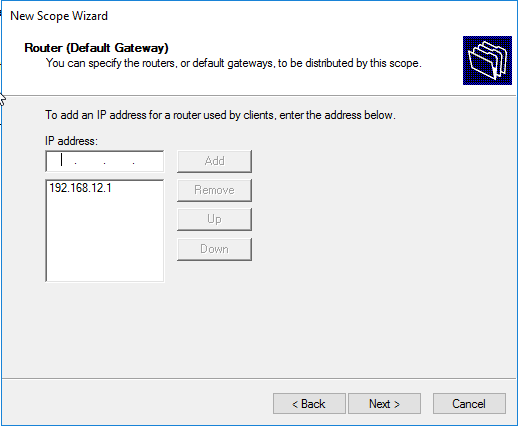
***Hình 5.5:*** *Đặt tên cho Scope*



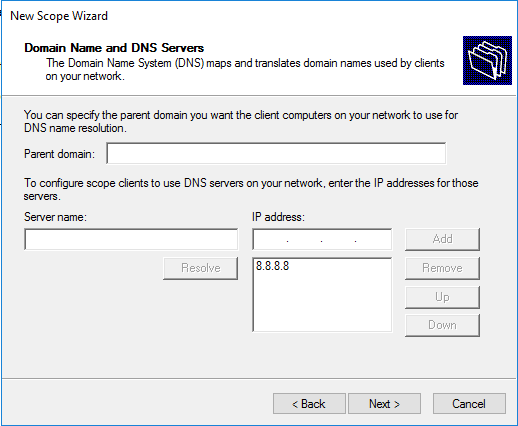
***Hình 5.6:*** *Đặt dãy địa chỉ IP cho Scope và Subnet Mask*



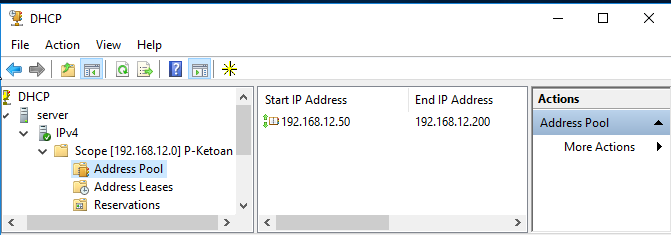
***Hình 5.7:*** *Thiết lập thời gian cho thuê IP*



***Hình 5.8:*** *Thiết lập địa chỉ Default Gateway cho Scope*

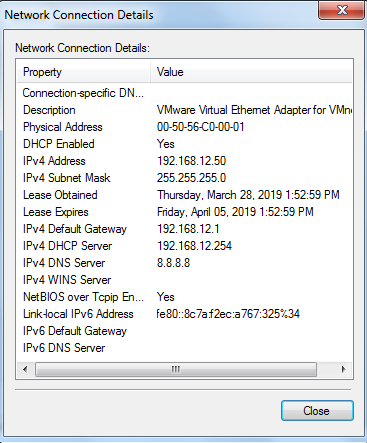


***Hình 5.9:*** *Thiết lập địa chỉ DNS*



***Hình 5.10:*** *Kết quả cấu hình cho một Scope*

- Kiểm tra trên máy Client:



***Hình 5.11:*** *Kiểm tra kết quả xin cấp phát IP từ máy Client*

### Cấu hình trên Linux

Để cấu hình DHCP Server trên Linux, chúng ta cài đặt dịch vụ dhcp\* và thực hiện cấu hình bằng cách chỉnh sửa các nội dung trong tập tin: /etc/dhcpd.conf. Một số tham số cấu hình mẫu sau đây:

#vi /etc/dhcp/dhcpd.conf

subnet 192.168.12.0 netmask 255.255.255.0{

option routers 192.168.12.1;

option subnet-mask 255.255.255.0;

option domain-name-servers 8.8.8.8;

range 192.168.12.50 192.168.12.200;

default-lease-time 21600;

max-lease-time 43200;}

### Khả năng dự phòng DHCP Server trong hệ thống:

Các thiết bị trên mạng cần IP để cho thiết bị của mình có thể liên lạc được với các thiết bị khác trên mạng. Do đó, việc thiết lập khả năng dự phòng cho DHCP Server là cần thiết để tránh tình trạng DHCP Server bị hư hỏng không cấp được IP cho các Client trên mạng. Việc thiết lập

này có thể dùng thêm Server và cấp phát cho IP với các dãy địa chỉ lệch nhau, khi đó tránh được khả năng cấp phát trùng lặp và tạo khả năng dự phòng cho hệ thống.

### Tấn công DHCP và giải pháp

* + - * Điểm yếu của DHCP Server.

Dịch vụ DHCP là dịch vụ mạng phổ biến, các thiết bị có khả năng làm chức năng cấp phát IP động (DHCP Server) tồn tại rất nhiều trên mạng như các Access Point, các Router,... Để kiểm soát việc cấp phát IP động cho các thiết bị trong mạng là vấn đề quản trị quan trọng cần lưu ý. Bất kỳ một thiết bị nào nếu kích hoạt tính năng cấp phát IP động (DHCP Server) đều có khả năng cấp phát cho các thiết bị trong mạng. Do đó, khi một thiết bị nhận IP từ một DHCP không được cấu hình đúng (vô tình hay cố ý) đều có khả năng không thể truy cập bình thường vì các thông số cấu hình khác với IP được hoạch định cho mạng hiện tại.

Một số công cụ tấn công DHCP Server bằng cách làm cho DHCP Server không còn IP trống đã khai báo để cấp phát cho người dùng. Việc tấn công này thực hiện và sau đó, kẻ tấn công có thể tự thiết lập DHCP Server giả để cấp phát và tiến hành các công cụ nghe trộm hay đánh cắp thông tin như kiểu tấn công Man-In-The-Middle.

### Một số giải pháp:

**Chống giả DHCP Server:**

Việc giả mạo các DHCP Server để cấp phát cho các người dùng trong mạng và nghe trộm thông tin như trên rất nguy hiểm, gây ảnh hưởng cho người dùng, có thể gián đoạn các hoạt động của người dùng. Hơn nữa, các thiết bị có khả năng cấp phát IP động có rất nhiều như các Access Point cấp phát Wifi là tình trạng phổ biến. Nhiều đơn vị tự mua và gắn vào hệ thống mạng hiện hữu để có thể sử dụng các thiết bị không dây như điện thoại di động, máy tính bảng,… mà không báo cáo hay nhờ sự hỗ trợ kỹ thuật từ bộ phận quản trị mạng. Điều này cũng gây nhiều phiền toái trong một hệ thống mạng. Khi đó, có thể phân đoạn mạng đó được AP cấp phát IP động và không có khả năng truy cập vào các hệ thống bình thường của đơn vị.

Từ những vấn đề trên cho thấy rằng dù vô hình hay cố ý, kiểm soát các DHCP Server tồn tại trong hệ thống là vô cùng quan trọng. Các giải pháp chống giả DHCP Server có thể sử dụng như: giải pháp trên Switch có hỗ trợ chứng năng DHCP Snooping hay giải pháp trên môi trường Domain Controller hỗ trợ chứng thực, cấp phép cho các DHCP Server hoạt động trong hệ thống mạng.

* 1. **Dịch vụ DNS**

### Giới thiệu

Mỗi thiết bị trên mạng có địa chỉ IP dùng để định danh trong các hoạt động trao đổi dữ liệu giữa chúng. Tuy nhiên, việc sử dụng các địa chỉ ít mang tính gợi nhớ, con người thường dễ nhớ hơn thông qua tên như [www.microsoft.com](http://www.microsoft.com/) hay [www.google.com.](http://www.google.com/) Do đó, với mỗi tên miền, máy tính cần tìm địa chỉ IP tương ứng trước khi nó có thể giao tiếp với máy tính đó. Quá trình chuyển đổi từ tên ra địa chỉ IP và ngược lại là chứng năng chính của DNS.

Tập tin HOST.TXT giúp cho người dùng đỡ khó khăn hơn bằng cách ánh xạ giữa địa chỉ IP và tên của đối tượng cần truy cập. Qua quá trình phát triển mạnh mẽ của hệ thống mạng cho thấy sự không phù hợp của việc sử dụng tập tin này. Sự không phù hợp này thể hiện ở khả năng mở rộng, đụng độ tên miền, sự nhất quán. Điều này dẫn đến việc ra đời một dịch vụ mới để thực thi công việc này, đó là dịch vụ DNS. Năm 1984, Paul Mockapetris cho ra đời phiên bản đầu tiên và không ngừng được cập nhật, cải tiến sau này.

Dịch vụ DNS là dịch vụ phân giải tên miền, là thành phần thiết yếu của Internet. Để dễ hiểu về dịch vụ này, người ta hay liên tưởng đến danh bạ điện thoại mà mọi người vẫn hay sử dụng hàng ngày trong việc tìm kiếm số điện thoại để liên lạc thông qua tên được lưu tương ứng. DNS cũng hoạt động như cuốn danh bạ trên Internet. Do đó, các máy tính có thể tìm kiếm các địa chỉ IP tương ứng từ các tên miền.

Dịch vụ DNS hoạt động theo cơ chế Client/Server. Phần Server gọi là DNS Server hay Name Server chứa các thông tin cơ sở dữ liệu của DNS. Phần DNS Client hay còn gọi là Resolver là các hàm thư viện dùng

để tạo các truy vấn và gửi đến các DNS Server. Cơ sở dữ liệu của DNS là cơ sở dữ liệu phân tán, cung cấp khả năng mở rộng và có độ tin cậy cao.

DNS sử dụng giao thức TCP và UDP ở tầng Transport, hoạt động ở Port 53. DNS liên quan đến 3 thành phần chính: tổ chức không gian tên miền, các DNS Server và DNS Client hay còn gọi là Resolver.

### Các thành phần của hệ thống DNS

Sơ đồ tổ chức của DNS:

DNS được tổ chức theo cấu trúc hình cây đảo ngược, mỗi Node trên cây là một miền (Domain) hoặc miền con (Sub Domain)

Root



org

net

vn

….

….

edu

com

hcmute

sgu

….

fit

fhq

….

Top-Level Domain (TLD)

Second-Level Domain

Third-Level Domain

com

***Hình 5.12:*** *Tổ chức không gian tên miền Internet*

### DNS Zone:

Hệ thống tên miền được quản lý theo các Zone (DNS Zone). Một Zone là một nhóm các Domain hay Sub Domain và được gán sự quản lý cho một cơ quan có thẩm quyền. Một Domain có thể được quản lý bởi nhiều cơ quan có thẩm quyền.

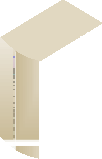
### Authoritative Name Server:

Mỗi DNS Zone có ít nhất một Server đóng vai trò là Server có thẩm quyền, Authoritative Name Server, để công bố thông tin của Zone, cung cấp các thông tin trả lời cho các truy vấn DNS.

Name Server:

DNS Server (hay còn gọi là Name Server) lưu trữ thông tin về tên miền của một hoặc số Zone. Mỗi DNS Server có thể quản lý một Zone hoặc nhiều Zone.

**DNS servers**



11.11.11.11

22.22.22.22

33.33.33.33

abc.com

xyz.net

**zones**

***Hình 5.13:*** *DNS Server và Zone*

Có 2 loại Name Server là Authoritative và Caching. Trong đó, Authoritative Server lưu trữ và duy trì dữ liệu, được chia làm 2 vai trò là: Master - cho phép chỉnh sửa dữ liệu, và Slave - chỉ làm nhiệm vụ nhân bản dữ liệu; Caching Server lưu trữ dữ liệu thu được từ Authoritative Server.

Cơ chế phân giải tên miền: Root Name Server là máy chủ quản lý các Name Server ở mức Top-Level Domain. Khi có truy vấn về một tên miền nào đó thì Root Name Server phải cung cấp tên và địa chỉ IP của Name Server quản lý Top Level Domain. Đến lượt các Name Server của Top Level Domain cung cấp danh sách các Name Server có quyền trên các Second Level Domain mà tên miền này thuộc vào. Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn.

### Truy vấn tên miền

Có hai loại truy vấn được sử dụng trong dịch vụ DNS: truy vấn đệ quy và truy vấn tương tác.

* + - * **Truy vấn đệ quy**: Khi DNS Server nhận được truy vấn loại này, nó sẽ trả lời lại kết quả phân giải mà nó có. Nếu không có câu trả lời thì DNS Server sẽ thực hiện gửi truy vấn đến các DNS Server khác để yêu cầu phân giải. Sau đó, nó sẽ gửi kết quả cho DNS Client.
      * **Truy vấn tương tác**: Khi DNS Server nhận được truy vấn loại này, nó sẽ trả lời kết quả tốt nhất mà nó có ở thời điểm đó. DNS Server không thực hiện bất cứ các truy vấn nào thêm.

### Cấu hình DNS

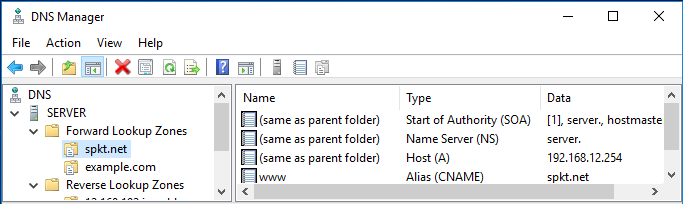
* Phân giải thuận: Là các thiết lập cơ chế phân giải để ánh xạ tên sang địa chỉ IP. Các Record sử dụng trong phân giải tên thuận là: A, CNAME.
* Phân giải nghịch: Là các thiết lập phân giải IP sang tên. Các Record thường dùng trong phân giải tên nghịch là: PTR.

### Cấu hình DNS trên Windows Server:

Ví dụ: Phân giải các tên miền tương ứng với các địa chỉ như sau:

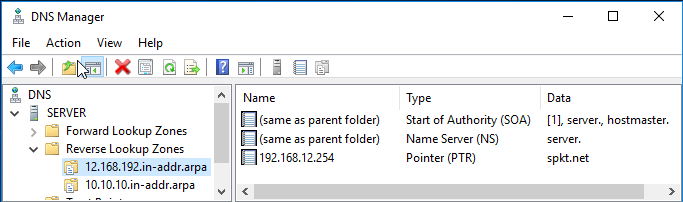
|  |  |
| --- | --- |
| Tên miền | Địa chỉ |
| [www.spkt.net](http://www.spkt.net/) (spkt.net) | 192.168.12.254 |
| [www.example.com](http://www.example.com/) (example.com) | 10.10.10.200 |

Tạo Zone thuận:



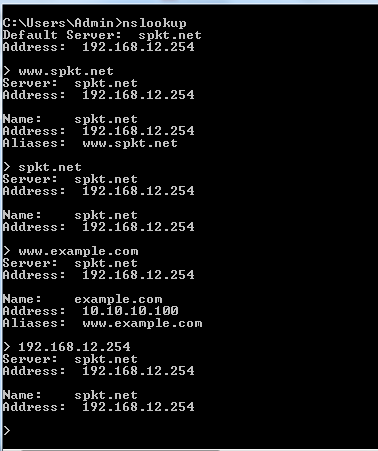
***Hình 5.14:*** *Cấu hình phân giải thuận trên Windows Server*

Tạo Zone nghịch:



***Hình 5.15:*** *Cấu hình phân giải nghịch trên Windows Server*

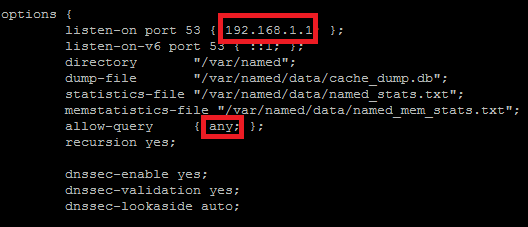
Kiểm tra kết quả phân giải:



***Hình 5.16:*** *Kiểm tra kết quả phân giải với NsLookup*

### Cấu hình DNS trên Linux:

Sau khi cài đặt dịch vụ DNS trên Linux, phần cấu hình thực hiện theo các bước sau:

Bước 1. Chỉnh địa chỉ Server DNS lắng nghe trên Port 53 (/etc/named.conf).

***Hình 5.17:*** *Điều chỉnh địa chỉ của DNS Server và các tham số*

Bước 2. Điều chỉnh #vi /etc/named.rfc1912.zones, khai báo File chứa phân giải thuận và nghịch.

zone “spkt.net” IN { type master;

file “spkt.net.zone”; allow-update { none;}; allow-query { any;};

};

zone “1.168.192.in-addr.arpa” IN { type master;

file “spkt.net.rr.zone”; allow-update {none;}; allow-query { any;};

};

Bước 3. Tạo CSDL cho Zone thuận và Zone nghịch vừa khai báo ở bước 2.

|  |  |  |
| --- | --- | --- |
| #vi /var/named/spkt.net.zone | | |
| $TTL 1D  @ IN SOA dns1.spkt.net. root.spkt.net. (  0 ; serial  1D ; refresh  1H ; retry  1W ; expire  3H ) ; minimum | | |
|  | IN NS | dns1.spkt.net. |
| spkt.net. | IN A | 192.168.1.10 |
| www | IN CNAME | spkt.net |
| dns1 | IN A | 192.168.1.1 |
| #vi /var/named/spkt.net.rr.zone | | |
| $TTL 1D  @ IN SOA dns1.spkt.net. root.spkt.net. (  0 ; serial  1D ; refresh  1H ; retry  1W ; expire  3H ) ; minimum | | |
|  | IN NS | dns1.spkt.net. |
| 1 | IN PTR | dns1.spkt.net. |
| 10 | IN PTR | spkt.net |

Bước 4. Gán quyền cho 2 File vừa tạo. #chown named:named spkt.net.zone #chown named:named spkt.net.rr.zone

## Dịch vụ WEB

### Giới thiệu

Dịch vụ World Wide Web (viết tắt là WWW hoặc Web) là một dịch vụ cung cấp thông tin trên hệ thống mạng. Các thông tin này được lưu trữ dưới dạng siêu văn bản và thường được thiết kế bằng ngôn ngữ HTML (Hypertext Markup Language).

Siêu văn bản là các tài liệu có thể là văn bản, hình ảnh tĩnh, hình ảnh động, âm thanh,... được liên kết với nhau qua các mối liên kết và được truyền trên mạng dựa trên giao thức HTTP (Hypertext Transfer Protocol), qua đó người dùng có thể xem các tư liệu có liên quan một cách dễ dàng.

### Các thành phần trong dịch vụ Web

HTTP Request

**Web**

**Server Database**



**Client**

(1)

Web Browser

(2)

HTTP Response

Web Application

***Hình 5.18:*** *Các thành phần trong dịch vụ Web*

Hệ thống dịch vụ Web thông thường bao gồm 3 thành phần chính: Web Browser, Web Application Server và Database.

* Web Browser là các chương trình phần mềm được cài đặt ở máy tính người dùng, có chức năng gửi các yêu cầu truy cập, nhận kết quả từ Web Server và hiển thị nội dung.
* Web Application Server là Server cài đặt dịch vụ quản trị Website, chứa nội dung trang Web, tiếp nhận và xử lý các yêu cầu từ Web Browser. Database là nơi lưu trữ cơ sở dữ liệu cho trang Web, thông thường nó được đặt trên một Server độc lập với

Web Application Server, tiếp nhận và xử lý các yêu cầu truy vấn thông qua các ngôn ngữ cơ sở dữ liệu.

Để truy cập vào các trang Web, người dùng nhập địa chỉ (URL) vào ô địa chỉ của Web Browser. Mỗi URL là một liên kết xác định một trang trên Web (Web Page), bao gồm 3 thành phần: Protocol, Domain Name:Port và File Directory/File Name.

Ví dụ:

<http://www.example.com/index.html>

Protocol Domain-name File-name

***Hình 5.19:*** *Tên miền với Port mặc định*

http://www.example.com:8080/abc/xyz.html

Protocol Domain-name File-name

***Hình 5.20:*** *Tên miền với Port đã được điều chỉnh thành 8080*

### Triển khai dịch vụ Web:

Để triển khai dịch vụ Web, các bước cần thực hiện như sau:

### Client 192.168.12.0/24

**Web server**

**IP: 192.168.12.100**

DNS: 192.168.12.200

### 192.168.12.254

**Web Browser**

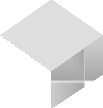
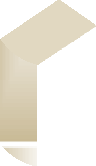
[http://192.168.12.254](http://192.168.12.254/)

[http://www.spkt.net](http://www.spkt.net/)

[**www.spkt.net**](http://www.spkt.net/) **– 192.168.12.254**

### DNS Server 192.168.12.200

***Hình 5.21:*** *Mô hình triển khai dịch vụ Web*



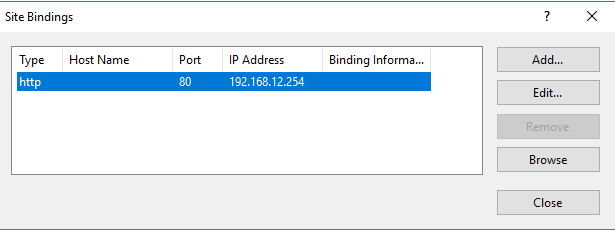
Bước 1. Chuẩn bị trang Web. Để có trang Web có thể sử dụng các công cụ lập trình Web như PHP, ASP.NET, JSP,…

Bước 2. Cài đặt và cấu hình Web Server:

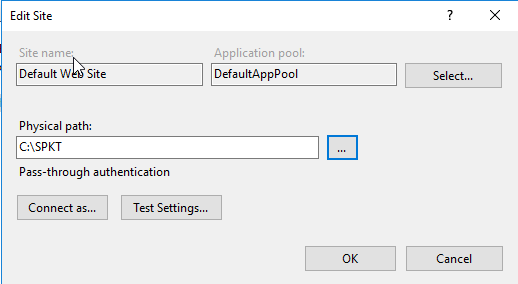
* + Lựa chọn hệ điều hành: Windows Server, Linux,…
  + Cài đặt dịch vụ Web: Là ứng dụng hỗ trợ cho việc cấu hình. Ví dụ như dịch vụ Web Server (IIS) trên Windows Server,…
  + Cấu hình dịch vụ Web: Bao gồm các bước như xác định tên, đường dẫn đến thư mục chứa trang Web (ở bước 1), cổng dịch vụ (mặc định là 80,…).

Bước 3. Cấu hình dịch vụ DNS để phân giải tên miền. Bước 4. Kiểm tra kết quả ở máy tính người dùng.

Ví dụ triển khai trên Windows Server (IIS):



***Hình 5.22:*** *Cấu hình Site Binding*



***Hình 5.23:*** *Cấu hình đường dẫn thư mục chứa mã nguồn Web*

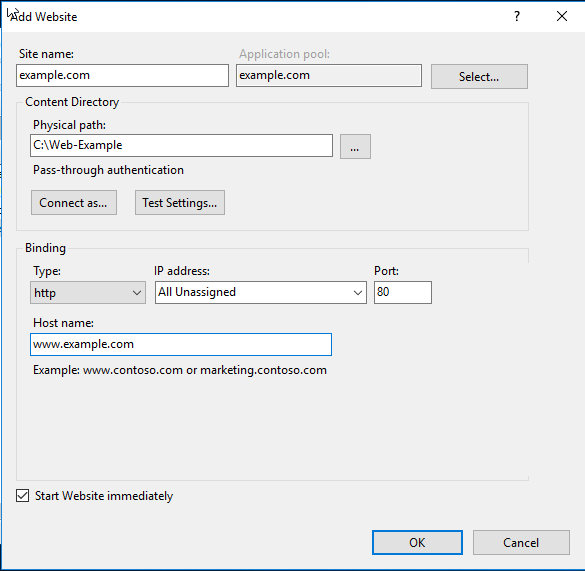
### Triển khai nhiều Website trên 1 Web Server

Một Web Server có thể đặt nhiều Website. Ví dụ trên một Server có thể đặt nhiều trang Web như [www.example.com,](http://www.example.com/) www.baigiang.org,... Trong trường hợp này, trên Web Server sẽ tạo ra các thư mục tương ứng chứa Website và trong bước cấu hình sẽ cấu hình tương ứng phần Binding trên trang Web với Port 80 của ứng dụng Web.

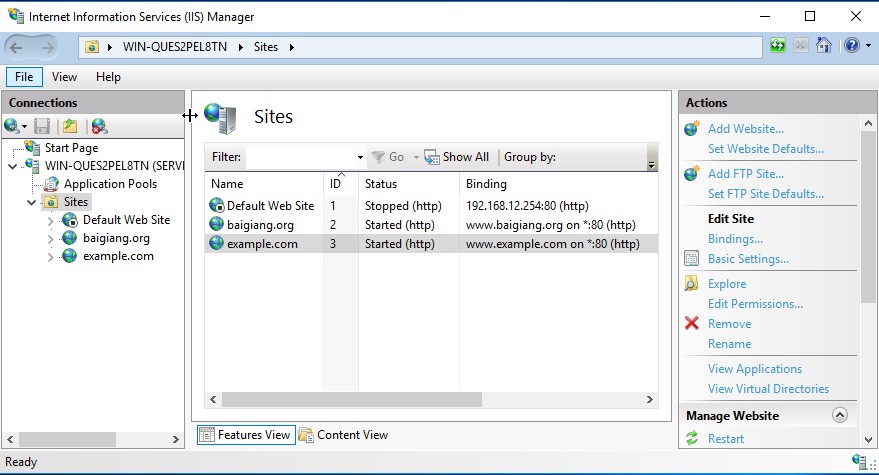
Web Server lắng nghe ở Port 80 (TCP) để tiếp nhận, xử lý và phản hồi các yêu cầu của Web Browser. Trong một số trường hợp khác như tạo ra các trang Web thử nghiệm,… người ta có thể cấu hình cho Web Server lắng nghe ở một Port khác.

### - Triển khai trên Windows Server:

***Hình 5.24:*** *Cấu hình cho Website baigiang.org*



***Hình 5.25:*** *Cấu hình cho Website example.org*



***Hình 5.26:*** *Thông tin cấu hình các Website*

### - Triển khai trên Linux:

Chỉnh sửa trong File httpd.conf.

#vi /etc/httpd/conf/httpd.conf

<VirtualHost \*:80>

DocumentRoot /var/www/spkt  thư mục chứa web ServerName ten-domain  thay đổi cho phù hợp ServerAlias www.ten-domain  thay đổi cho phù hợp

</VirtualHost>

## Dịch vụ FTP

### Giới thiệu

FTP (File Transfer Protocol) là giao thức truyền File trên mạng sử dụng giao thức TCP ở tầng Transport.

### Các thành phần của dịch vụ FTP

**Client**

**FTP Server**

Request



(1)

(2)

Response

***Hình 5.27:*** *Mô hình dịch vụ FTP*

FTP hoạt động ở 2 cổng: Control Port (21) và Data Port (20 hoặc Port khác). FTP Server lắng nghe các yêu cầu dịch vụ từ FTP Client trên cổng 21. Đường kết nối qua cổng 21 tạo nên một kênh điều khiển, cho phép các lệnh được chuyển qua. Để truyền dữ liệu giữa 2 máy thì dùng một kênh khác (Port khác).

### Phân loại Active FTP và Passive FTP Active FTP:

* + - * Client gửi yêu cầu kết nối với Port ngẫu nhiên (N>1023) đến Port 21 của FTP Server, thông báo về việc mở Port N+1 để nhận dữ liệu từ Server.
      * Server xác nhận.
      * Server dùng Port 20 để truyền dữ liệu cho Client.
      * Client xác nhận đã nhận dữ liệu.



DATA

1031



PORT 1031

OK

Data channel

OK

CMD

1030

CMD 21

DATA 20

***Hình 5.28:*** *Hoạt động của Active FTP*

**Passive FTP**: Client khởi tạo 2 phiên kết nối đến Server.

* + - * Client gửi yêu cầu kết nối với Port ngẫu nhiên (N>1023) đến Port 21 của FTP Server.
      * Server xác nhận.
      * Client mở Port N+1 để nhận dữ liệu từ Server.
      * Server dùng Port >1023 để truyền dữ liệu cho Client.



DATA

1031

CMD

1030

CMD

21



PASV

1378

OK - 1378

Data channel

OK

DATA

20

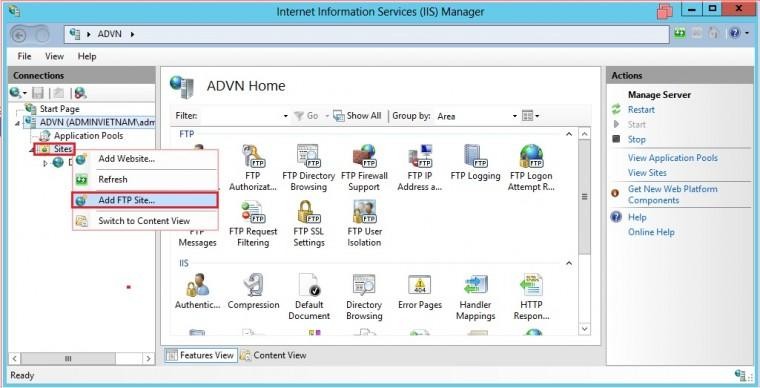
***Hình 5.29:*** *Hoạt động của Passive FTP*

### Triển khai dịch vụ FTP

Chúng ta có thể triển khai dịch vụ FTP trên hệ điều hành Windows hoặc Linux với các gói phần mềm cài đặt tương ứng. Với Windows, chúng ta dùng IIS (tương tự như triển khai Web). Với Linux, chúng ta có thể dùng gói cài đặt VSFTPD.

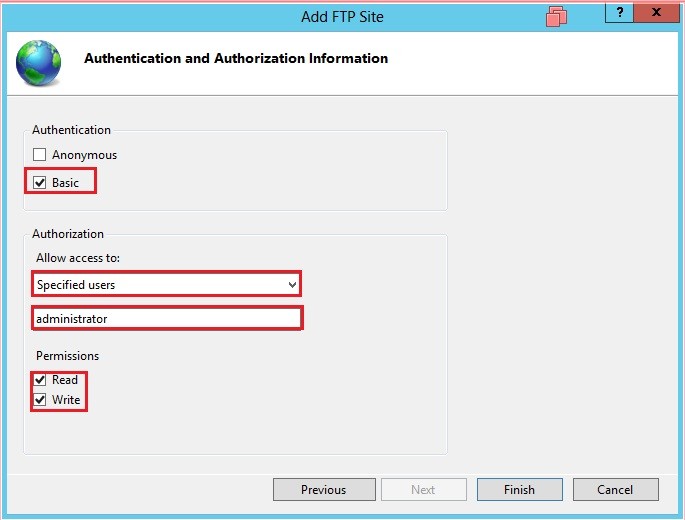
Khi triển khai một FTP Server trên Windows, cần cài sẵn IIS sau đó thực hiện một số tác vụ:

* + - * Tạo 1 thư mục FTP để chứa dữ liệu.
      * Tạo User để đăng nhập vào FTP.
      * Phân quyền Full Control cho User trên thư mục FTP.
      * Tạo mới FTP Site.



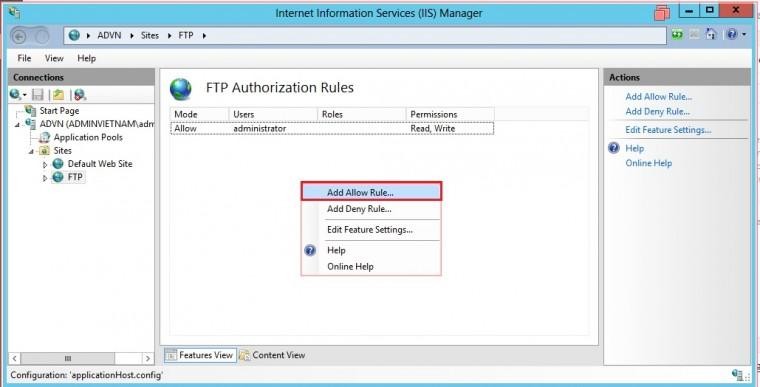
***Hình 5.30:*** *Cửa sổ cấu hình FTP Server*

* + - * Cấu hình chứng thực FTP - Authentication.



***Hình 5.31:*** *Cấu hình chứng thực*

* + - * Cấu hình FTP - Authorization.



***Hình 5.32:*** *Cấu hình quyền truy cập*

Thực hiện test dịch vụ FTP trên một máy tính khác (hoặc test tạm thời trên máy cài FTP Server). Dùng Web Browser để đăng nhập FTP qua địa chỉ IP với tài khoản FTP (ta có thể truy cập FTP bằng tên miền, chỉ cần tạo một Alias trong cấu hình DNS).

***Hình 5.33:*** *Đăng nhập sử dụng dịch vụ*



***Hình 5.34:*** *Kết quả truy cập FTP Server*

Các hệ điều hành Windows đều hỗ trợ FTP Client qua Web hoặc Command Line, ta có thể cài một trình FTP Client khác như: FileZilla, WinSC, Cyberduck.

### Dịch vụ E-MAIL

* + 1. **Giới thiệu**

Dịch vụ E-mail (hay dịch vụ thư điện tử) là một hình thức trao đổi thư từ thông qua mạng Internet. Dịch vụ này được sử dụng rất phổ biến, hữu ích hiện nay.

### Các thành phần của dịch vụ E-mail

* + - * E-mail Client: Các phần mềm với chức năng soạn thảo nội dung, gửi và nhận thư từ E-mail Server, lưu trữ thư.
      * E-mail Server:

Tại mỗi Mail Server thông thường gồm hai dịch vụ: POP3 (Post Office Protocol 3) làm nhiệm vụ giao tiếp Mail giữa Mail Client và Mail Server, SMTP (Simple E-mail Transfer Protocol) làm nhiệm vụ giao tiếp Mail giữa các máy Mail Server.

Khi người dùng gửi một E-mail, máy tính của người dùng sẽ gửi dữ liệu đến SMTP Servre. Server sẽ nhìn vào địa chỉ trong E-mail và chuyển tiếp nó đến với Server của người nhận E-mail.

### Một số giao thức trong dịch vụ E-mail

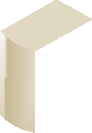
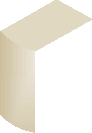
* + - * POP3 được sử dụng để rút trích E-mail từ một Mail Server. POP3 Server lắng nghe ở Port 110 (TCP), ở phía Client sử dụng Port được sinh ngẫu nhiên (lớn hơn 1024).

**SMTP**

**Server**

**POP3**

**Server**



Gửi e-mail

Nhận e-mail

**E-mail Client**

***Hình 5.35:*** *Hệ thống E-mail*

Khi người dùng kiểm tra E-mail, E-mail Client kết nối đến POP3 Server (ở Port 110). POP3 Server yêu cầu chứng thực. Sau khi chứng thực thành công, Server cho phép người dùng truy cập đến các dữ liệu của người dùng.

Ưu điểm của POP3 là khả năng “offline”, các E-mail được tải xuống và lưu trữ trong máy người dùng. Khi đó, người dùng có thể truy

cập nội dung E-mail mà không cần thiết phải kết nối Internet. Một số chương trình E-mail Client phổ biến như Microsoft Outlook,…

* + - * Giao thức IMAP: Giao thức này hoạt động cũng tương tự như POP3. Nó có một số ưu điểm như: đầu tiên IMAP chỉ cần Download phần Header của E-mail, khi người dùng chọn đọc E- mail thì phần nội dung mới được tải về.
      * SMTP: SMTP hoạt động ở Port 25 (TCP), là giao thức ở tầng Ứng dụng, định nghĩa các quy luật về gửi và nhận E-mail giữa các Server.

### Hoạt động của SMTP:

Mail Client tạo kết nối TCP đến SMTP Server và tải lên (Upload) nội dung E-mail và địa chỉ đích đến. Thông qua tên miền, Name Server phân giải để xác định việc tự xử lý hay phải chuyển tiếp. Nếu nó biết về người nhận, SMTP Server sẽ chuyển thư đến đó. Nếu nó không biết nó sẽ chuyển đến SMTP Server khác. Trong DNS, Record MX (Mail Exchange) được dùng hỗ trợ cho việc phân phối các E-mail.

* + - * + Giao thức S/MIME: Dùng để bảo mật trong dịch vụ E-mail sử dụng các cơ chế mã hóa và chữ ký số.
        + Giao thức PGP: Giống như giao thức S/MIME.

### Triển khai dịch vụ E-mail

Chúng ta cần chọn một phần mềm E-mail Server để cài trên một máy, ví dụ như MS Exchange, Mdeamon trên Windows hay Postfix, Sendmail trên Linux. Phía Client sẽ dùng một phần mềm Mail Client để truy xuất E-mail như Outlook Express trên Windows hay Thunderbird trên Linux, hay Webmail trên giao diện Web.

Khi cài đặt mail Server Exchange trên Windows, ta cần chú ý một số tác vụ:

* + - * Cài đặt một bản Windows Server và một số gói phụ thuộc.
      * Cài đặt Active Directory Domain Services và các dịch vụ liên quan.
      * Cài đặt DNS.
      * Tạo các tài khoản người dùng - chính là các tài khoản E-mail.
      * Cài đặt Exchange Server và cập nhật.
      * Cấu hình Exchange Server để có thể gửi nhận Mail.

Phía Mail Client cần khai báo địa chỉ Mail Server và Username/Password nếu dùng các phần mềm Mail Client trên máy tính. Hoặc chỉ cần mở Web Browser và nhập tên miền của máy Mail Server rồi đăng nhập với Username/Password để vào hộp thư cá nhân.

## Tổng kết chương

Nhu cầu sử dụng các dịch vụ mạng ngày càng cao, yêu cầu phía nhà cung cấp dịch vụ mạng càng cần thiết để đáp ứng nhu cầu người dùng, như: Web, Mail, FTP,… Chương này đã trình bày đặc điểm và nguyên tắc hoạt động của một số dịch vụ phổ biến dùng trong hệ thống mạng như DHCP, DNS, Web, FTP, E-mail. Mỗi dịch vụ mạng cung cấp các chức năng giúp người dùng tương tác với các ứng dụng trên mạng. Việc hiểu rõ về nguyên tắc hoạt động, cài đặt và cấu hình các dịch vụ này sẽ giúp người quản trị vận hành tốt hệ thống mạng, đáp ứng nhu cầu sử dụng các dịch vụ mạng.

## Câu hỏi và bài tập

1. DNS Record nào ánh xạ từ Hostname ra IP?
   1. A.
   2. CNAME.
   3. PTR.
   4. MX.
   5. SOA.
2. NS Record nào được sử dụng khi phân giải từ IP ra tên miền?
   1. A.
   2. CNAME.
   3. PTR.
   4. MX.
   5. SOA.
3. Chức năng Reservation trong DHCP Server cho phép thực hiện điều gì sau đây?
   1. Dùng để thiết lập địa chỉ Default Gateway cho các máy tính trong một Scope.
   2. Dùng để thiết lập thời gian cho thuê IP trong một Scope.
   3. Dùng để cấp phát IP cố định cho một Host dựa vào Hostname của Host đó.
   4. Dùng để cấp phát IP cố định cho một Host dựa vào địa chỉ MAC của Host đó.
4. Thứ tự các gói tin trao đổi giữa DHCP Client và DHCP Server để xin cấp phát địa chỉ IP động là?
   1. DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK.
   2. DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, DHCPACK.
   3. DHCPREQUEST, DHCPOFFER, DHCPDISCOVER, DHCPACK.
   4. DHCPREQUEST, DHCPDISCOVER, DHCPACK, DHCPOFFER.
5. Câu nào sau đây là đúng khi nói về gói tin DHCPDISCOVER?
   1. Địa chỉ IP đích trong gói tin này là địa chỉ IP của DHCP Server.
   2. Địa chỉ IP nguồn trong gói tin này là địa chỉ IP của DHCP Server.
   3. Địa chỉ MAC đích trong gói tin này là địa chỉ MAC của DHCP Server.
   4. Địa chỉ MAC nguồn trong gói tin này là địa chỉ MAC của DHCP Client.
   5. Địa chỉ MAC nguồn trong gói tin này là địa chỉ MAC của DHCP Server.
6. DHCP Server sử dụng giao thức nào ở tầng Transport và cổng bao nhiêu để lắng nghe các yêu cầu cung cấp địa chỉ IP từ DHCP Client?
   1. TCP/67.
   2. UDP/67.
   3. TCP/68.
   4. UDP/68.
   5. TCP/23.
   6. UDP/23.
7. Thời điểm nào DHCP Client sẽ liên lạc với DHCP Server để gia hạn thời gian thuê địa chỉ IP?
   1. 25% thời gian thuê.
   2. 50% thời gian thuê.
   3. 90% thời gian thuê.
   4. Khi hết thời gian thuê.
   5. DHCP Client sẽ không cần liên lạc với DHCP Server, địa chỉ IP được cấp một lần và sử dụng cho đến khi Client chuyển tới một mạng khác.
8. Câu nào sau đây mô tả đúng về phân giải thuận (Forward Lookup) trong DNS?
   1. Phân giải IP từ DNS cục bộ mà không cần sự giúp đỡ của các DNS khác.
   2. Phân giải tên ra địa chỉ IP.
   3. Phân giải IP ra tên.
   4. Chuyển tiếp yêu cầu phân giải tên miền đến một DNS Server khác.
9. Câu nào sau đây là đúng nhất về phân giải ngược (Reverse Lookup) trong DNS?
   1. Yêu cầu phân giải được chuyển đến cho một DNS Server khác để phân giải.
   2. Phân giải từ IP ra tên miền.
   3. Yêu cầu phân giải ngược được thực hiện trên DNS Server cục bộ mà không cần trợ giúp từ các DNS Server khác.
   4. Phân giải từ tên miền ra địa chỉ IP.
10. DNS sử dụng giao thức và cổng nào cho các truy vấn trực tiếp?
    1. UDP/53.
    2. TCP/53.
    3. UDP/67.
    4. TCP/68.
11. DNS sử dụng giao thức và cổng nào cho việc chuyển tiếp các Zone?
    1. UDP/53.
    2. TCP/53.
    3. UDP/67.
    4. TCP/68.
12. Các thông số cấu hình nào trong DHCP Server là tham số tùy chọn khi cấu hình cấp phát địa chỉ IP cho các máy trong mạng?
    1. IP & Subnet Mask.
    2. IP và Default Gateway.
    3. Default Gateway và DNS.
    4. Subnet Mask và DNS.
13. Giao thức nào sau đây dùng để gửi E-mail?
    1. NTP.
    2. IMAP4.
    3. POP3.
    4. SMTP.
14. Giao thức nào sau đây được dùng để nhận E-mail?
    1. POP3.
    2. SNMP.
    3. ARP.
    4. Telnet.
15. Dãy địa chỉ nào sau đây là dãy địa chỉ APIPA? A. 169.254.0.1 to 169.254.0.254.

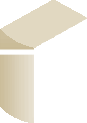
B. 169.254.0.1 to 169.254.0.255.

C. 169.254.0.1 to 169.254.255.254.

D. 169.254.0.1 to 169.254.255.255.

1. Cho mô hình mạng:

Network: **192.168.1.0/24**



**Router**

**Router**

**Fa0/1 Fa0/1**

**RA**

**Fa0/0** .1

.1

.2

**RB**

**Fa0/0**

.1

Network: **172.16.2.0/24**

**Web Server**

.2

**PCA**

Network: **172.16.1.0/24**

**PCA** thiết lập một kết nối đến **Web Server**. *Những câu nào sau đây* mô tả những thông tin khi dữ liệu bắt đầu xuất phát từ **PCA** đến **Web Server**?

* 1. Port đích (Destination Port) có giá trị 80.
  2. Địa chỉ IP đích (Destination IP Address) của gói tin là địa chỉ IP của cổng fa0/0 của Router **RA**.
  3. Địa chỉ IP đích (Destination IP Address) của gói tin là địa chỉ IP của Card mạng của **Web Server**.
  4. Địa chỉ MAC đích (Destination MAC Address) của Frame là địa chỉ MAC của cổng fa0/0 của **Router RA**.

1. Trong FTP Active, Server FTP dùng cổng nào để truyền dữ liệu đi cho Client:

A. 21.

B. 22.

C. 23.

D. Bất kỳ.

1. Trong các mô hình sau, mô hình nào là mô hình mạng được dùng phổ biến hiện nay:
   1. Peer To Peer.
   2. Remote Access.
   3. Terminal Mainframe.
   4. Client Server.
2. Dịch vụ Web dùng cặp giao thức và cổng nào?
   1. HTTP/81.
   2. HTTPS/80.
   3. HTTP/443.
   4. HTTPS/443.
3. Trong FTP Passive, sau khi Server xác nhận yêu cầu truyền dữ liệu được gửi từ Port N của Client thì:

* Client mở Port N+1 để nhận dữ liệu từ Server.
* Client mở Port 20 để nhận dữ liệu từ Server.
* Server dùng Port 20 để truyền dữ liệu cho Client.
* Server dùng Port N+1 để truyền dữ liệu cho Client.

# CHƯƠNG 6

**CÁC MÔ HÌNH QUÂN TRỊ HỆ THỐNG**

Chương này sẽ đề cập đến mô hình quản trị mạng Workgroup và Domain, cách thiết lập quyền truy xuất dữ liệu trong Domain, chia sẻ dữ liệu trên mạng và việc quản lý chính sách nhóm. Mô hình dạng Workgroup chỉ phù hợp với mạng nhỏ chỉ vài chục máy trạm - nơi mà các User bình đẳng nhau và từng User sẽ tự quản lý tài nguyên của mình tại mỗi máy cá nhân. Để quản lý một cách tập trung, mô hình Domain được sử dụng nhiều trong các doanh nghiệp. Các thành phần trong Domain, các kiến trúc và các dịch vụ triển khai giúp việc quản lý người dùng và dữ liệu trên mạng đạt hiệu quả cao.

## Giới thiệu

Quản lý hệ thống mạng bao gồm các hoạt động: lập kế hoạch, cài đặt và cấu hình, vận hành, xử lý sự cố và duy trì để đảm bảo hệ thống hoạt động liên tục, đáp ứng nhu cầu người sử dụng và đảm bảo hệ thống an toàn, hạn chế các truy cập bất hợp pháp.

Có 2 mô hình quản lý hệ thống mạng:

* + - Mô hình Workgroup hoặc là Peer To Peer.
    - Mô hình sử dụng Domain.

## Mô hình quản trị không sử dụng Domain

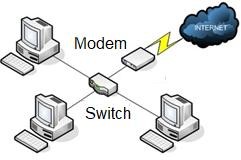
Mô hình mạng Workgroup còn gọi là mô hình mạng Peer To Peer là mô hình mà trong đó các máy tính có vai trò như nhau được nối kết với nhau. Các máy tính tự bảo mật và quản lý các tài nguyên của riêng mình, và tự chứng thực cho người dùng cục bộ.

### Một số đặc trưng:

* Các dữ liệu và tài nguyên được lưu trữ phân tán tại các máy cục bộ, các máy tự quản lý tài nguyên cục bộ của mình.
* Các Server trong hệ thống mạng có tính chất độc lập, mỗi ứng dụng/dịch vụ có thể phát sinh tài khoản cho người sử dụng.
* Kiến thức quản trị không quá phức tạp, tiết kiệm chi phí đầu tư Server cho việc triển khai Domain.
* Khó đảm bảo tính nhất quán, triển khai áp đặt chính sách/ứng dụng khó khăn, mất nhiều thời gian.
* Phù hợp cho các mạng nhỏ và vừa, dưới mười máy tính và yêu cầu bảo mật không cao.

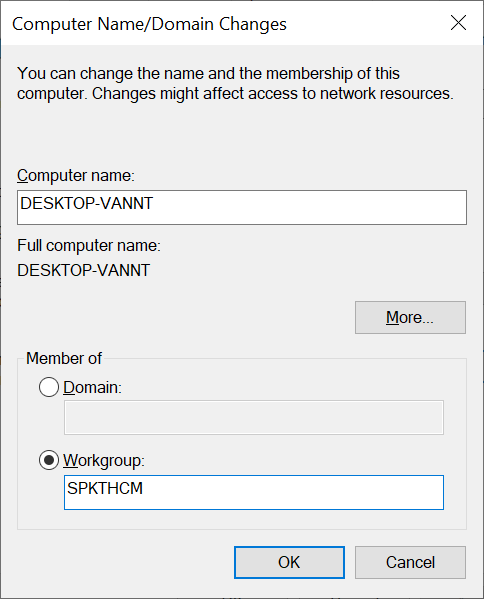
Thông tin người dùng trong một tập tin SAM (Security Accounts Manager) đã được mã hóa và lưu ở trên máy tính cục bộ:

\Windows\system32\config\SAM.



***Hình 6.1:*** *Mô hình quản trị Workgroup*

Cấu hình 1 máy tính gia nhập vào 1 Workgroup trên Windows:

* Click **Start**, click **Control Panel** và double-click **System**.
* Click Advanced System Settings, click Computer Name.
* Click Change, trong Workgroup Box nhập tên nhóm làm việc mà ta muốn gia nhập vào:

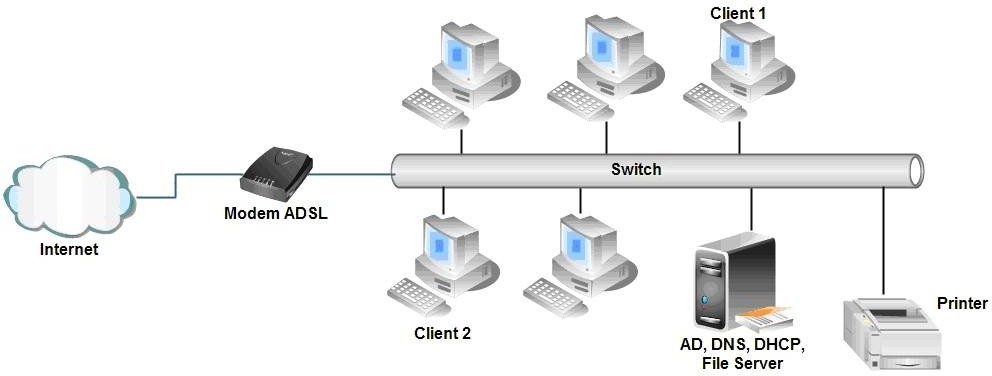
***Hình 6.2:*** *Thiết lập tên cho Workgroup*

## Mô hình quản trị sử dụng Domain

Khác với mô hình Workgroup, mô hình Domain hoạt động theo cơ chế Client Server, trong hệ thống mạng phải có ít nhất một máy tính làm chức năng điều khiển vùng (Domain Controller), máy tính này sẽ điều khiển toàn bộ hoạt động của hệ thống mạng.

### Một số đặc trưng:

* Việc chứng thực người dùng và quản lý tài nguyên mạng được tập trung lại tại các Server trong miền.
* Có ưu điểm về quản trị nhất quán, phân quyền, áp đặt chính sách tốt hơn, kiểm soát hoạt động của hệ thống chặt chẽ, người dùng có thể truy xuất các tài nguyên mạng mà họ được phép truy cập.
* Các Server cung cấp dịch vụ được ủy quyền mới hoạt động được, giúp giảm thiểu các rủi ro xảy ra trong hệ thống.
* Triển khai phần mềm, các chính sách bảo mật nhanh chóng và tự động hóa.
* Phù hợp cho các công ty vừa và lớn, đa chi nhánh.



***Hình 6.3:*** *Máy chủ quản lý tập trung bên trong mạng*

### Các thành phần trong Domain

* + - 1. **Directory Services**

Là một mô hình tổ chức dữ liệu, thông tin và mối quan hệ giữa chúng với nhau, cho phép quản lý tập trung các đối tượng, giúp đơn giản hóa việc quản lý tài nguyên. Là một dịch vụ hoạt động như một tổng đài

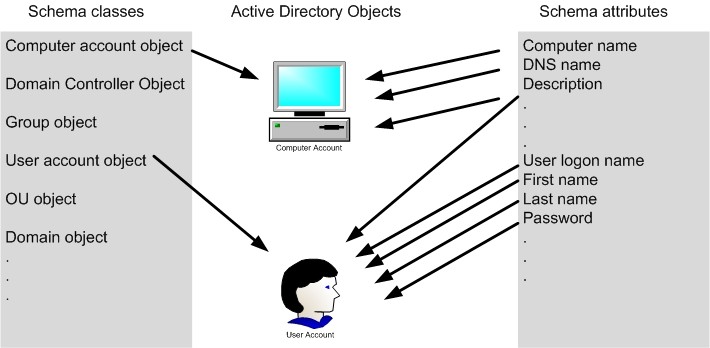
(Switchboard) chính trong các OS máy chủ, nó hỗ trợ các nguồn Resources độc lập và phân tán có thể làm việc với nhau, có thể kết nối với nhau. Là một dịch vụ cơ sở làm nền tảng để hình thành một hệ thống Active Directory. Nó được chứa trong NTDS.DIT và các chương trình quản lý, khai thác tập tin này.

Các thành phần trong Directory Services:

* Object (đối tượng): Bao gồm các máy in, người dùng mạng, các Server, các máy trạm, các thư mục dùng chung, dịch vụ mạng,… là thành tố căn bản nhất của dịch vụ danh bạ.
* Attribute (thuộc tính): Một thuộc tính mô tả một đối tượng. Các đối tượng khác nhau có danh sách thuộc tính khác nhau, tuy nhiên, các đối tượng khác nhau cũng có thể có một số thuộc tính giống nhau. Ví dụ như một máy in và một máy trạm cả hai đều có một thuộc tính là địa chỉ IP.
* Schema (cấu trúc tổ chức): Một Schema định nghĩa danh sách các thuộc tính dùng để mô tả một loại đối tượng nào đó.

Schema Classes: Định nghĩa các kiểu đối tượng được lưu trữ trong AD.

Schema Attributes: Định nghĩa các thông tin về kiểu của từng đối tượng trong AD.

Schema có đặc tính là tùy biến được - các thuộc tính dùng để định nghĩa một lớp đối tượng có thể sửa đổi được.

***Hình 6.4:*** *Các thành phần trong AD*

* + Container (vật chứa): Một vật chứa có thể chứa các đối tượng và các vật chứa khác. Vật chứa cũng có các thuộc tính như đối tượng mặc dù vật chứa không thể hiện một thực thể thật sự nào đó như đối tượng. Có ba loại vật chứa là:
    - Domain: Khái niệm này được trình bày chi tiết ở phần sau.
    - Site: Một Site là một vị trí. Site được dùng để phân biệt giữa các vị trí cục bộ và các vị trí xa xôi. Ví dụ: các chi nhánh của 1 công ty.
    - OU (Organizational Unit): Gồm người dùng, nhóm, máy tính và những OU khác. Một OU không thể chứa các đối tượng nằm trong Domain khác.

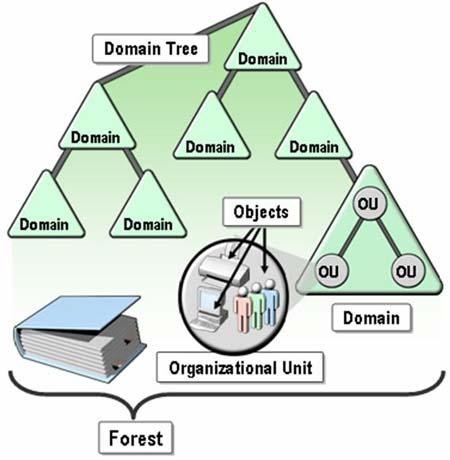
Ta có thể xây dựng một mô hình thứ bậc của các vật chứa để mô hình hóa cấu trúc của một tổ chức bên trong một Domain. Ta nên sử dụng OU để giảm thiểu số lượng Domain cần phải thiết lập trên hệ thống.

### Active Directory

Là một dịch vụ được Microsoft phát triển và là trái tim của hệ thống Domain Controller. Ra đời từ phiên bản Windows NT 4.0 Server và tồn tại trong các phiên bản Windows Server đến ngày nay. Nó cung cấp một số tính năng quan trọng giúp thiết kế, triển khai, quản trị hệ thống một cách dễ dàng và hiệu quả. Như khả năng lưu trữ tập trung, toàn bộ dữ liệu và thông tin hệ thống được lưu trữ tập trung, cho phép người dùng có thể truy cập dữ liệu từ bất kỳ đâu. Active Directory sử dụng dịch vụ thư mục giúp việc quản lý và truy xuất tài nguyên dễ dàng. Ngoài ra, với tính năng đồng bộ dữ liệu cho phép triển khai tính năng dự phòng, giảm thiểu rủi ro và nâng cao hiệu suất hoạt động của mạng.

Dữ liệu của Active Directory được tổ chức như Service Directory theo kiến trúc logic và vật lý nhất định nhằm quản lý được hệ thống mạng lớn, cung cấp một mức độ ứng dụng mới cho môi trường xí nghiệp.

### Kiến trúc Active Directory

* + - 1. **Kiến trúc logic của Active Directory**

***Hình 6.5:*** *Kiến trúc logic của Active Directory*

Kiến trúc logic giúp ta có thể định hình giao diện của dịch vụ thư mục của tổ chức theo một cấu trúc logic của cơ quan hay đơn vị đó. Active Directory được tạo thành từ 5 thành phần: Objects, Organizational Units, Domain, Domain Tree, Forest.

* + - * + **Object** (đối tượng): Bao gồm các máy in, người dùng mạng, các Server, các máy trạm, các thư mục dùng chung, dịch vụ mạng.
        + **Organizational Units (OU)**: Là một đối tượng chứa được sử dụng để tổ chức các đối tượng trong Domain thành các nhóm luận lý giúp dễ dàng quản trị. Một OU có thể chứa các đối tượng như tài khoản User, nhóm User, máy tính, máy in, chương trình, thư mục chia sẻ hoặc các OU khác trong cùng Domain. Cấu trúc OU trong một Domain độc lập với cấu trúc OU của domain khác. OU là một cách để phân quyền quản trị trên một Domain giúp giảm nhẹ công tác quản trị trên Domain.
        + **Domain**: Là đơn vị chức năng nòng cốt của cấu trúc logic AD. Nó là phương tiện để quy định một tập hợp những người dùng, máy tính, tài nguyên chia sẻ có những quy tắc bảo mật giống nhau, từ đó giúp cho việc quản lý các truy cập vào các Server dễ dàng hơn. Domain có các chức năng chính:

Một khu vực quản trị (Administrative Boundary): Các chính sách bảo mật, các quan hệ ủy quyền với các Domain khác.

Quản lý bảo mật các tài nguyên chia sẻ.

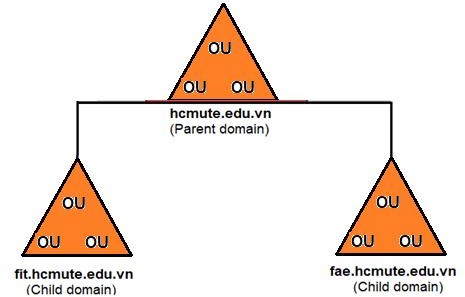
Cung cấp các Server dự phòng làm chức năng điều khiển vùng (Domain Controller), đồng thời đảm bảo các thông tin trên các Server này được đồng bộ với nhau.

* + - * + **Domain Tree**: Là một nhóm các Domain được tạo bằng cách thêm một hoặc nhiều Domain con (Child Domain) vào một Domain (Parent Domain) nào đó. Cây có các đặc điểm sau:

Tuân theo cấu trúc không gian tên miền DNS. Tên miền của một Domain cấp dưới là tên tương đối của Domain đó ghép thêm tên của miền cấp trên.

Mọi Domain trên cây sử dụng chung một danh mục gọi là

**Global Catalog** chứa thông tin về các đối tượng trên cây.



***Hình 6.6:*** *Domain Tree*

* + - * + **Forest**: Là tập hợp các Domain Tree có thiết lập quan hệ và ủy quyền cho nhau.

### Kiến trúc vật lý của Active Directory

Gồm các thành phần: Site, Domain Controller.

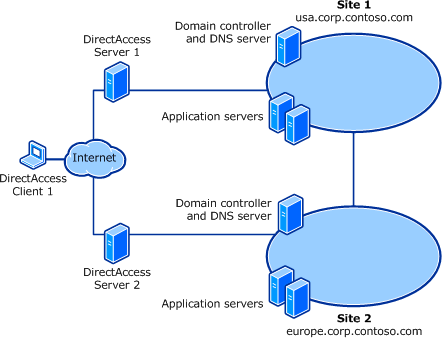
* + - * + **Site**: Là tập hợp của một nhóm máy tính trên cùng một Subnet, nhóm các Subnet và Domain Controller có kết nối tốc độ cao. Một Site có thể thuộc về nhiều Domain; một cách tương tự, một

Domain có thể chứa nhiều Site. Site còn được sử dụng để tối ưu hóa hoạt động sao chép (Replication) trên thư mục. Người quản trị có thể lập lịch để việc sao chép giữa các Site (Intersite) được thực hiện vào các giờ mạng rảnh còn việc sao chép trong cùng Site (Intrasite) có thể thực hiện thường xuyên hơn.

Các thành phần của Site:

**Subnets**: Là mạng con trong Site, gồm máy tính và các thiết bị nối mạng.

**Site Links**: Dùng để kết nối 2 hoặc nhiều Site. Xác định thời gian và tần số đồng bộ giữa 2 Site.

**Bridgehead Servers**: Việc đồng bộ giữa các Site xảy ra giữa các Server đầu cầu ở mỗi Site.

***Hình 6.7:*** *Kết nối giữa các Site*

* + - * + **Domain Controller** (DC): Là một máy điều khiển miền, quản lý tất cả các tương tác của User trên Domain như xác nhận đăng nhập mạng hoặc tìm kiếm đối tượng trên Active Directory. Các đặc điểm của DC:

Mỗi DC chứa thông tin về Active Directory của Domain và sao chép thông tin đó cho các DC khác thuộc Domain.

Các DC trong một Domain tự động sao chép thông tin về các đối tượng thuộc Domain cho nhau. Khi có một thay đổi trên

Active Directory, thay đổi đó được tự động cập nhật cho các DC trong Domain.

Sử dụng nhiều DC trong một Domain cho phép tăng cường khả năng chịu lỗi.

### Các thành phần trong AD

* **Schema**: Là danh sách các quy tắc định nghĩa các loại đối tượng và các loại thông tin về đối tượng có thể chứa trong Active Directory. Nói một cách khác Schema bao gồm một tập các quy tắc định nghĩa nội dung và cấu trúc của Active Directory.
* **Global Catalog**: Là cơ sở dữ liệu quản lý thông tin về các đối tượng trên một Tree hoặc Forest. Mặc định Global Catalog được tạo ra một cách tự động trên Domain Controller trong một Forest. Server chứa Global Catalog được gọi là Global Catalog Server. Global Catalog thực hiện hai chức năng chính trên Active Directory, đó là:
  + Cho phép User thực hiện các thao tác đăng nhập (Log-on) bằng cách cung cấp thông tin về thành viên nhóm cho Active Directory.
  + Cho phép tìm kiếm thông tin trên Active Directory bất kể Domain nào trong Forest chứa dữ liệu thực sự.

### Quy tắc viết tên đối tượng trên Active Directory

Mỗi đối tượng trên Active Directory được xác định thông qua tên. Active Directory sử dụng các quy tắc viết tên đó là: tên đầy đủ (Distinguished Name), tên tương đối (Relative Distinguished Name), tên định danh duy nhất toàn cục (Globally Unique Identifier).

### Tên đầy đủ (Distinguished Name DN)

Là cách viết tên đầy đủ nhất, tên đầy đủ bao gồm tên Domain chứa đối tượng và toàn bộ đường dẫn trên cấu trúc cây Domain đến đối tượng.

Ví dụ: DC=com,DC=microsoft,OU=dev,CN=Users,CN=Firstname.

Trong đó DC, OU và CN là các thuộc tính của tên đầy đủ, nghĩa của các ký hiệu như sau:

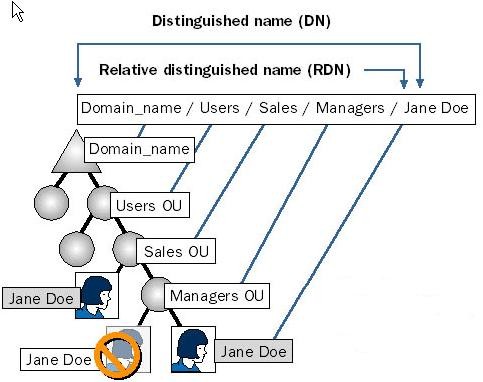
Thuộc tính Ý nghĩa

DC Domain Component Name

OU Organizational Unit Name

CN Common Name

### Tên tương đối (Relative Distinguished Name RDN)

* Tên tương đối của một đối tượng là phần của tên đầy đủ mà cũng chính là một thuộc tính của đối tượng đó. Ví dụ tên tương đối của Firstname của một đối tượng User là Firstname, tên tương đối của đối tượng cha là Users.
* Tên tương đối các đối tượng có thể trùng trên Active Directory nhưng không thể có hai đối tượng cùng tên tương đối trong cùng OU.

***Hình 6.8:*** *Sơ đồ tên tương đối DN*

### Tên định danh duy nhất toàn cục (GUID)

Là một giá trị 128 bit được gán cho mỗi đối tượng mỗi khi đối tượng được tạo ra trên Active Directory. Đối tượng trên Active Directory có thể bị di chuyển hoặc đổi tên nhưng giá trị này không bao giờ thay đổi.

### Cài đặt Domain Controler trên Windows Server

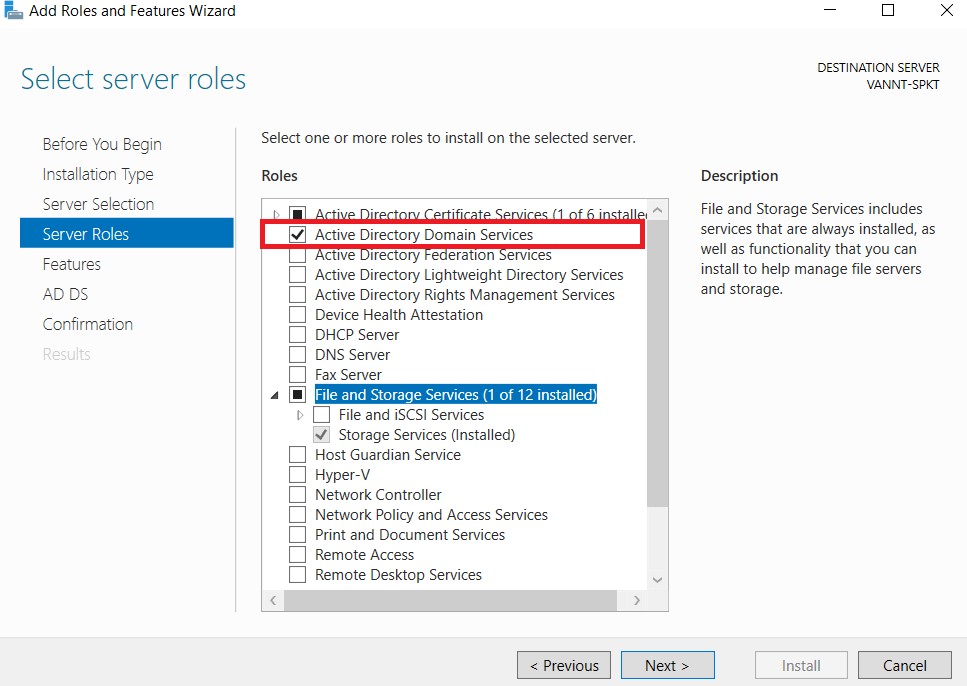
* + - 1. **Yêu cầu cài đặt**

Khai báo đầy đủ các thông số TCP/IP, DNS Server có địa chỉ chính là địa chỉ IP của Server cần nâng cấp. Nên cấu hình dịch vụ trước khi nâng cấp Server, hoặc cài đặt DNS tự động trong quá trình nâng cấp. Muốn tạo máy DC thì phải cần đến dịch vụ miền AD (ADDS - Active Directory Domain Services). Các minh họa cài đặt dưới đây được thực hiện trên Windows Server 2016. Các Version Windows Server, giao diện có thể khác một chút khi tiến hành cài đặt và cấu hình.

### Cài đặt ADDS

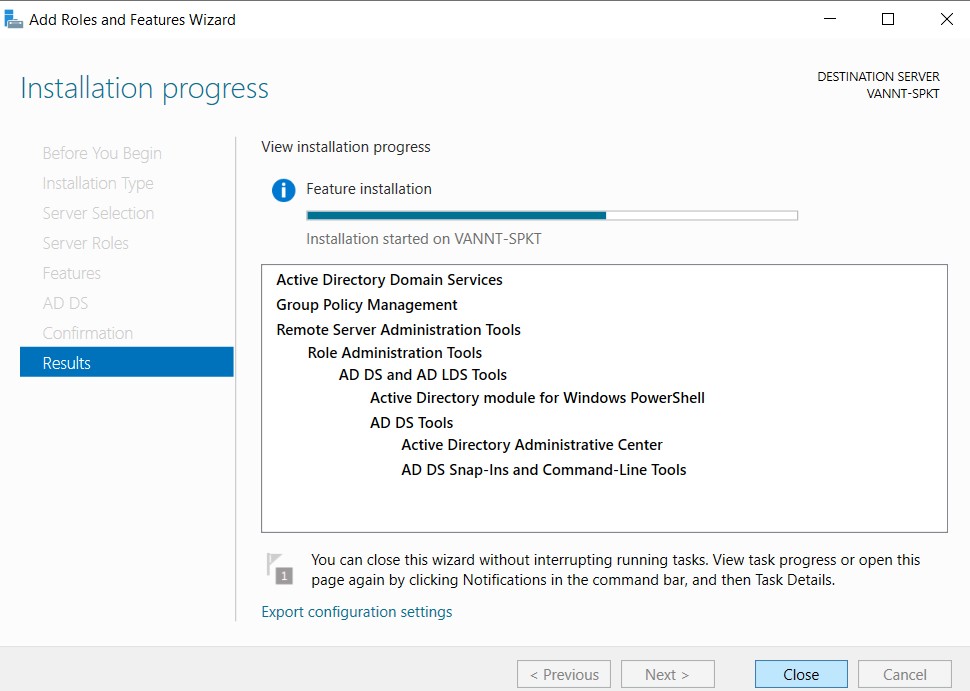
Dịch vụ miền AD (ADDS) sẽ lưu trữ thông tin về các đối tượng trong mạng và tổ chức các thông tin này sao cho những người dùng có thể tiếp cận một cách dễ dàng. ADDS dùng DC để giúp những người dùng mạng truy nhập vào các tài nguyên mạng chỉ cần thông qua việc Log-in của User vào hệ thống.

Thực hiện: Từ Server Manager, chọn Add Roles and Features\Server Roles.



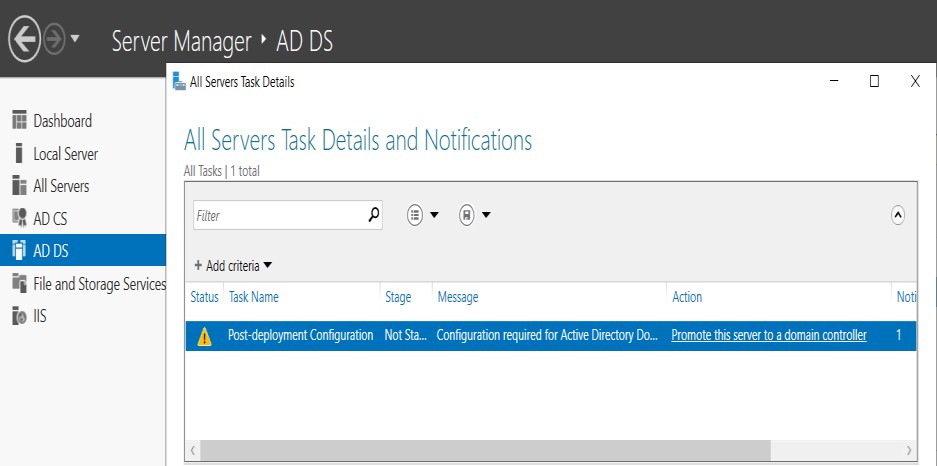
***Hình 6.9:*** *Cài đặt dịch vụ AD*

Trong quá trình cài đặt, một số gói phụ thuộc sẽ được yêu cầu cài đặt. Kết quả cài đặt:



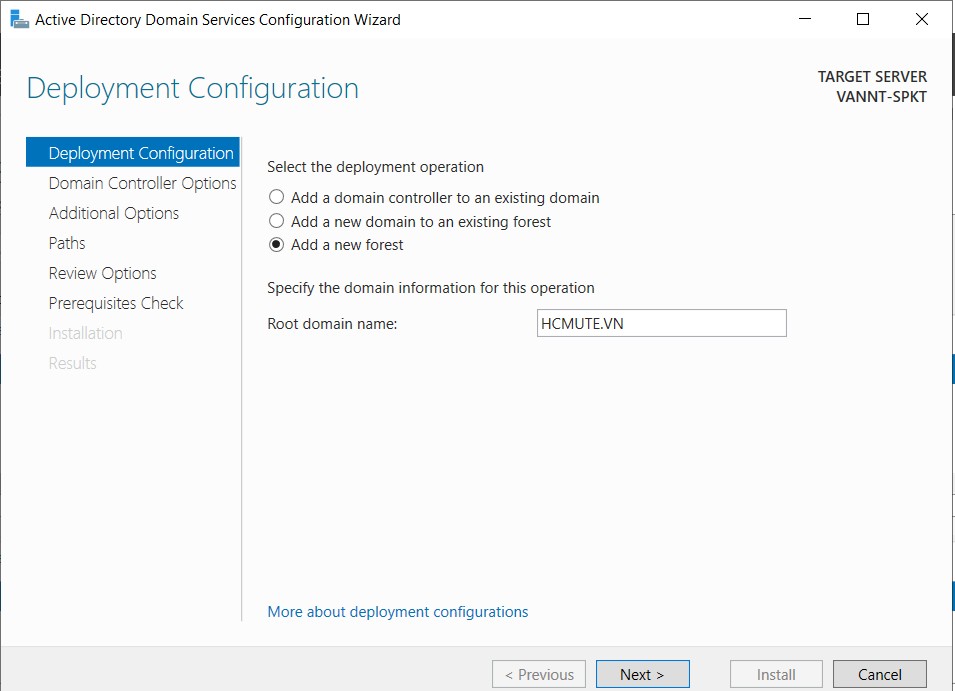
***Hình 6.10:*** *Quá trình cài đặt AD*

### Cài đặt Domain Controller

Để bắt đầu tạo Domain Controller, vào link “Promote this server to a domain controller” tại màn hình giao diện Server Manager/ADDS:

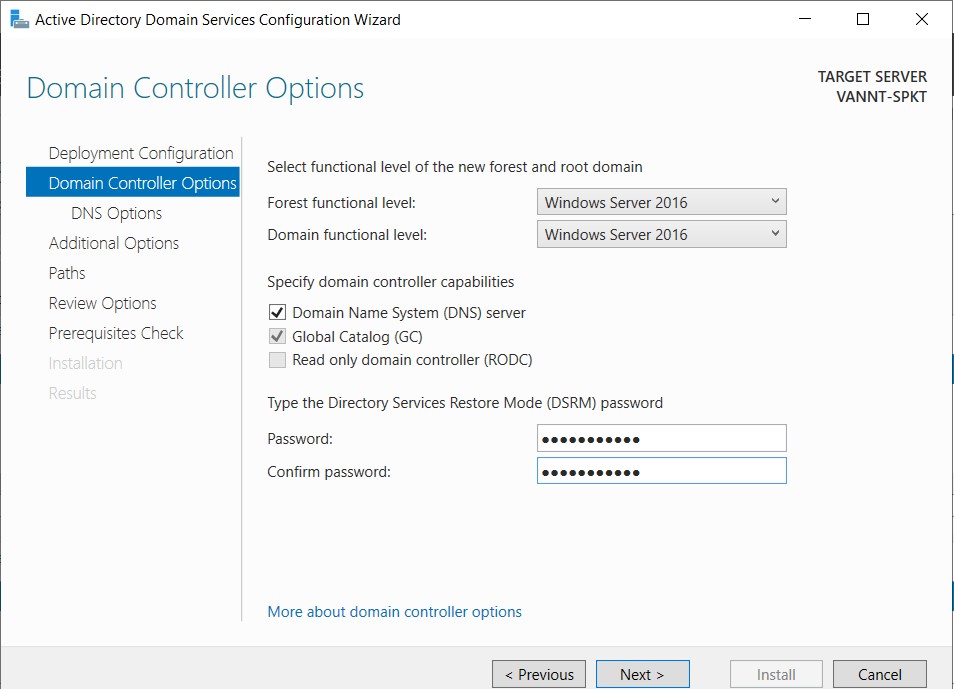
***Hình 6.11:*** *Giao diện cấu hình AD*

Chúng ta cần khai báo DC được tạo là đầu tiên hay thêm vào một Forest đã có, dưới đây là 1 Domain trong 1 Forest mới:



***Hình 6.12:*** *Đặt tên cho Domain*

Trong quá trình tạo, một số khai báo khác như đường dẫn, DNS,… Quá trình tạo DC sẽ yêu cầu nhập mật khẩu DSRM - Directory Services Restore Mode, là một thành phần trong chế độ khởi động Safe Mode của Windows Server khi đã thực hiện nâng cấp lên Domain Controllers. DSRM cho phép người quản trị (Administrator) có thể Repair, Recorver, Restore cơ sở dữ liệu của Active Directory. DSRM không được dùng để đăng nhập ở chế độ khởi động bình thường của Windows Server khi đã nâng cấp thành Active Directory.

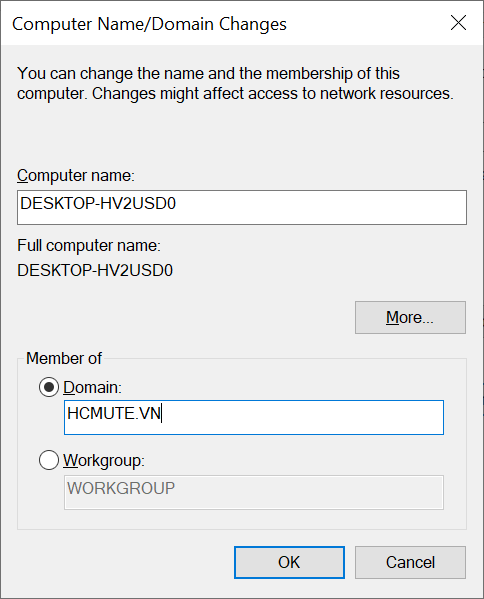


***Hình 6.13:*** *Cấu hình Password cho Mode Restore*

Cần khởi động lại máy khi quá trình tạo DC kết thúc.

### Gia nhập máy trạm vào Domain

Dùng một máy trạm trong mạng, gia nhập vào Domain vừa tạo. Chọn Control Panel\All Control Panel Items\System\Advanced System Setting, chọn Computer Name, nhập Domain:



***Hình 6.14:*** *Máy Client gia nhập vào Domain*

### Xây dựng các Domain Controller đồng hành

Trong các hệ thống Active Directory lớn, nếu chỉ có một Domain Controller thì Server này có thể bị quá tải khi nhiều User cùng yêu cầu chứng thực. Bên cạnh đó khi Domain Controller này bị lỗi thì toàn bộ hệ thống sẽ bị ngưng hoạt động, các User sẽ không được chứng thực. Trong phần này sẽ hướng dẫn các bạn triển khai Additional Domain Controller (ADC) - DC đồng hành sẽ chạy song song với Domain Controller chính để đảm bảo hệ thống luôn sẵn sàng.

Các bước thức hiện:

* + - * + Chọn 1 Server muốn cài DC đồng hành.
        + Cài ADDS (như bước cài đặt máy DC đầu tiên ở trên).
        + Cài DC đồng hành.

Ở màn hình Deployment Configuration, chúng ta cần chọn kiểu DC, do cần xây dựng Additional DC nên ta chọn “Add a domain controller to an existing domain”. Nhập tên Domain. Cần xác thực là người quản trị cấp miền thì mới có quyền tạo Additional DC.

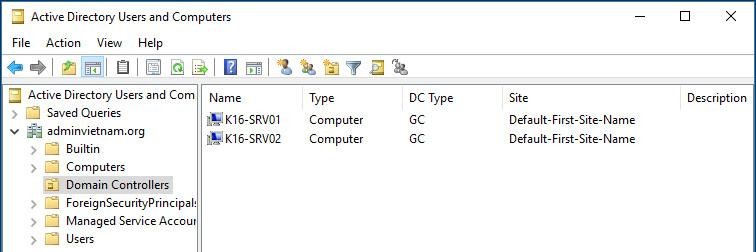
Tại Domain Controller Options, đặt mật khẩu khôi phục hệ thống Domain khi có sự cố.

Tại Addtional Options, chọn Server để đồng bộ dữ liệu - chính là Server đã xây dựng DC đầu tiên.

Paths, chỉ định đường dẫn lưu trữ CSDL của hệ thống miền.

Cuối cùng chọn Install để cài đặt.

- Sau khi cài đặt xong, chúng ta có thể kiểm tra DC đồng hành đã được cài đặt thành công hay chưa bằng cách dùng công cụ Active Directory Users and Computers. Ví dụ:



***Hình 6.15:*** *Công cụ quản trị trên Domain*

### Xây dựng Child Domain

Khi công ty có nhu cầu mở rộng, cần xây dựng thêm Domain để quản lý người dùng và tài nguyên thì Domain con là lựa chọn để mở rộng từ Domain cha đang tồn tại. Ví dụ Child Domain “fit.hcmute.vn” được tạo từ Domain cha “hcmute.vn”.

Các bước thực hiện:

* + - * + Chọn 1 Server muốn cài Child Domain.
        + Cài ADDS (như bước cài đặt máy DC đầu tiên ở trên).
        + Cài Child Domain.

Ở màn hình Deployment Configuration, chúng ta cần chọn kiểu DC, do cần xây dựng Child Domain nên ta chọn “Add a new domain to an existing forest”. Nhập thông tin Domain gồm: Domain cha, tên Child Domain. Cần xác thực là người quản trị cấp miền thì mới có quyền tạo Child Domain.

Tại Domain Controller Options, đặt mật khẩu khôi phục hệ thống Domain khi có sự cố.

Đặt lại tên NetBIOS hoặc sử dụng tên NetBIOS mặc định.

Paths, chỉ định đường dẫn lưu trữ CSDL của hệ thống miền.

Cuối cùng chọn Install để cài đặt.

### Quản trị User, Group trên Windows Server

User và Group là những thành phần cơ bản để quản lý và sử dụng tài nguyên trên máy tính hay trên hệ thống mạng. Tùy vào mức độ được cấp quyền mà người dùng có quyền truy xuất vào những tài nguyên nào trong hệ thống mạng (Domain), hoặc trên máy tính (Local) trong trường hợp Windows Server chưa lên Domain.

User là một đối tượng để xác định cá nhân nào sử dụng trong hệ thống. Thông tin về User Account có nhiều tham số nhưng một Account phải có tối thiểu 2 tham số là **Username** và **Password**.

Group là một nhóm các User có cùng tính chất. Group được tạo ra nhằm đơn giản hóa quá trình quản lý và phân quyền.

### Quản lý User và Group trên máy cục bộ (Local Host)

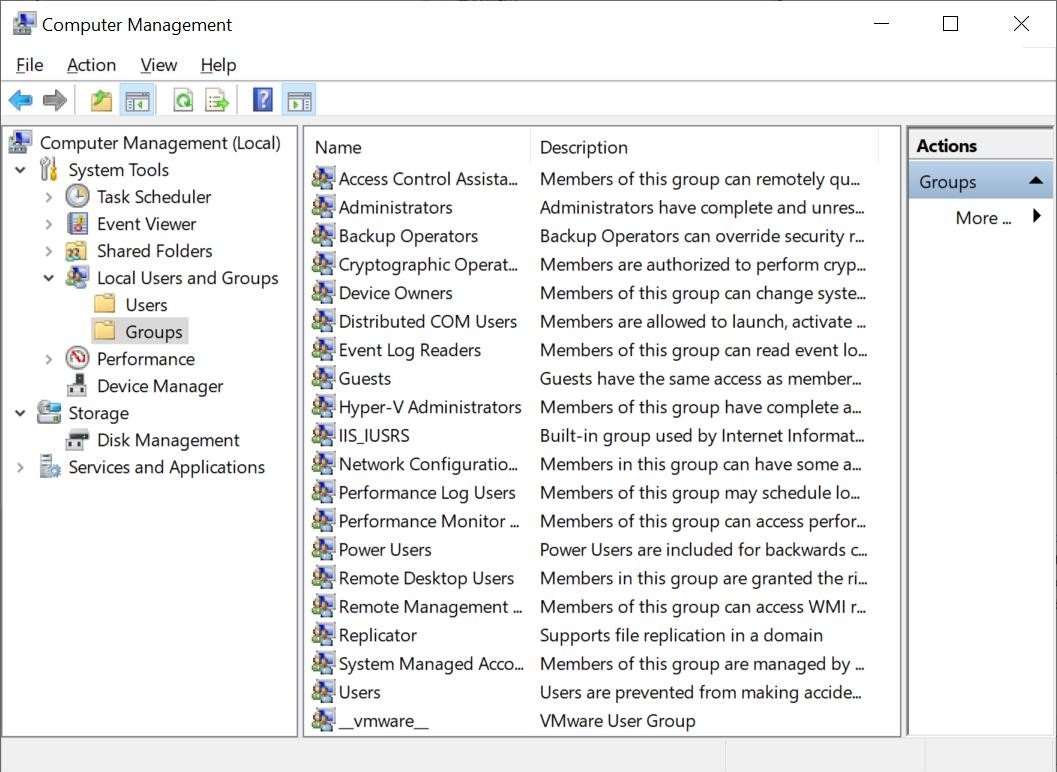
Việc quản lý cục bộ có thể thực hiện ở: Windows XP Pro, Windows Vista và Windows 7 Professional, Ultimate, Windows Server (chưa dựng Domain). User và Group cục bộ chỉ có giá trị trên máy và tài nguyên trên chính máy chứa nó. Trong máy có một số User và Group được tạo sẵn, chúng không thể xóa, nhưng có thể Disable.

Có hai User được tạo sẵn (Built-in Account):

|  |  |
| --- | --- |
| Administrators | Tài khoản có quyền cao nhất trong hệ thống. Administrator bị Disabale thì vẫn có thể Log-in vào chế độ Safe Mode, vì vậy việc tạo Password của User  này là rất quan trọng để bảo mật cho hệ thống. |
| Guest | Tài khoản khách, thường bị Disabale. |

Có một số Groups được tạo sẵn:

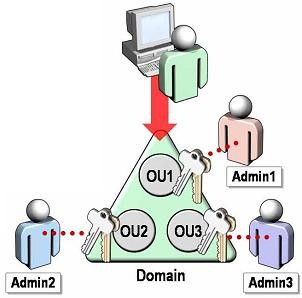
|  |  |
| --- | --- |
| Administrators | Các thành viên thuộc nhóm có thể thực hiện tất cả các  chức năng quản trị trên máy tính. Mặc định, tài khoản User Administrator thuộc về nhóm này. |
| Backup Operators | Các thành viên thuộc nhóm có thể chạy chương trình Windows Backup để sao lưu và khôi phục dữ liệu. |
| Guests | Các thành viên thuộc nhóm chỉ có thể truy xuất một cách hạn chế trên các tài nguyên đã được gán quyền sở hữu. Thành viên thuộc nhóm này không thể làm thay đổi Desktop. Mặc định, tài khoản User Guest  thuộc về nhóm này. |
| Power Users | Các thành viên thuộc nhóm có thể tạo mới, điều chỉnh tài khoản User cục bộ và chia sẻ tài nguyên. |
| Users | Các thành viên thuộc nhóm chỉ có thể thực hiện một số tác vụ nhất định tùy thuộc vào quyền sở hữu được gán. Khi một tài khoản User cục bộ được định nghĩa,  tài khoản đó sẽ thuộc về nhóm Users. |
| Một số Groups khác | Xem trong Computer Management\Local Users and Groups\Groups. |

Tạo User và Group cục bộ được thực hiện trong Computer Management\Local Users and Groups, và được lưu trong File SAM, nó chỉ có giá trị trên máy chứa thông tin tài khoản đó.

***Hình 6.16:*** *Các Group mặc định trên Domain*

### Quản lý User, Group và OU trên hệ thống mạng (Domain)

Sau khi xây dựng thành công máy chủ Domain Controller trên Windows Server bằng cách cài đặt dịch vụ ADDS, chúng ta sẽ tạo và quản lý các User, Group và OU trong hệ thống mạng Domain bằng công cụ Active Directory Users and Computers. Khác với các User và Groups cục bộ chỉ được dùng tài nguyên trong máy tính cục bộ, các User và Groups trong hệ thống mạng Domain có thể sử dụng các tài nguyên trên mạng tùy theo quyền được cấp. Các thông tin User, Group và OU sẽ được lưu trữ tại Server Domain.

* Organizational Unit (OU): Là một đối tượng trong Active Directore, nó chứa các đối tượng bên trong như User, Computer, Group và OU. Chức năng của OU:
  + Dùng ủy quyền quản trị (Delegation of Administration). Cho phép OU có quyền quản lý các đối tượng User, Group như chỉnh sửa thông tin, thêm, xóa các đối tượng trong OU này. Việc ủy quyền này sẽ giảm tải trách nhiệm của người quản trị chính Administrator.
  + Dùng áp dụng các chính sách (Group Policy). Group Policy sẽ được tự động áp dụng cho các đối tượng là User và Computer bên trong 1 OU. Một OU có thể được áp dụng nhiều Group Policy.

***Hình 6.17:*** *Các Object trên Domain*

* Group: Là đối tượng của Active Directory. Các User thành viên của Group sẽ có quyền truy cập tài nguyên mà Group đó có được phân quyền truy cập. Thành viên của Group là User và Group. Group được chứa trong các OU.

Có hai kiểu Group là Security Groups và Distribution Groups.

* Security Groups: Được sử dụng để cấp quyền cho phép hoặc không cho phép truy cập.
* Distribution Groups: Dùng để phân phối E-mail (chủ yếu dùng cho Microsoft Exchange), đối với các User không cần truy cập tài nguyên hoặc Log-in máy tính sẽ được đưa vào kiểu Group này.
* Phạm vi Group (Group Scopes) gồm có:
  + Domain Local: Có thể có thành viên là bất kỳ Domain nào trong Forest, có thể cấp quyền trong cùng Domain.
  + Global: Có thể có thành viên cùng Domain, có thể cấm quyền trong bất kỳ Domain nào trong Forest.
  + Universal: Có thể có thành viên trong bất kỳ Domain nào trong Forest, có thể cấp quyền bất kỳ Domain hoặc Forest.
* User và Computer:

User là lớp cuối cùng trong kiến trúc của Active Directory. User có thể là thành viên của một hoặc nhiều Group và được thừa hưởng chính sách từ Group. User cũng được chứa trong các OU. User cũng là đối tượng chủ yếu được áp dụng các Group Policy. Computer cũng tương tự như User, chỉ khác đó là một máy tính cụ thể nào đó.

Administrators: Tài khoản có quyền cao nhất trong hệ thống Domain. Administrator có thể bị Disabale nhưng vẫn có thể Log-in vào chế độ Safe Mode, vì vậy việc tạo Password của User này là rất quan trọng để bảo mật cho hệ thống.

Người dùng Administrator sẽ có quyền tạo User, Group, hoặc OU. Dùng: Start\Programs\Administrative Tools\Active Directory Users and Computers. Nhấp phải chuột trên mục Users\New: chọn User, Group, hoặc OU.

Khi tạo các đối tượng User, Group, hoặc OU cần khai báo các thông tin thuộc tính đầy đủ để thuận tiện trong quản lý. Các tác vụ khi quản lý các đối tượng như: chỉnh sửa, thêm, vô hiệu hóa (Disable), xóa.

### Quản lý User Profile

User Profile là 1 tập hợp các File và các thiết lập về môi trường làm việc của người dùng. Hệ thống tạo hồ sơ người dùng vào lần đầu tiên người dùng đăng nhập vào máy tính. Tại các lần đăng nhập tiếp theo, hệ thống tải hồ sơ của người dùng, sau đó các thành phần hệ thống khác cấu hình môi trường của người dùng theo thông tin trong hồ sơ.

Các dạng Profile:

### Local Profile:

Hồ sơ người dùng cục bộ được tạo lần đầu tiên khi người dùng đăng nhập vào máy tính. Hồ sơ được lưu trữ trên đĩa cứng cục bộ của máy tính. Các thay đổi được thực hiện đối với hồ sơ người dùng cục bộ dành riêng cho người dùng và máy tính thực hiện các thay đổi.

### Roaming Profile:

Bản sao của hồ sơ cục bộ được sao chép vào và lưu trữ trên một chia sẻ máy chủ. Hồ sơ này được tải xuống bất kỳ máy tính nào mà người

dùng đăng nhập trên mạng. Các thay đổi được thực hiện đối với hồ sơ người dùng chuyển vùng được đồng bộ hóa với bản sao máy chủ của hồ sơ khi người dùng đăng xuất. Ưu điểm của việc chuyển vùng hồ sơ người dùng là người dùng không cần phải tạo hồ sơ trên mỗi máy tính mà họ sử dụng trong mạng.

### Mandatory Profile:

Hồ sơ người dùng bắt buộc là loại hồ sơ mà quản trị viên có thể sử dụng để chỉ định cài đặt cho người dùng. Chỉ quản trị viên hệ thống mới có thể thực hiện các thay đổi đối với hồ sơ người dùng bắt buộc. Các thay đổi do người dùng thực hiện đối với cài đặt trên màn hình sẽ bị mất khi người dùng đăng xuất.

### Temporary Profile:

Hồ sơ tạm thời được phát hành mỗi khi tình trạng lỗi ngăn hồ sơ của người dùng tải. Cấu hình tạm thời bị xóa vào cuối mỗi phiên và các thay đổi do người dùng thực hiện đối với cài đặt và tệp trên máy tính để bàn sẽ bị mất khi người dùng đăng xuất. Cấu hình tạm thời chỉ có sẵn trên máy tính chạy Windows 2000 trở lên.

## Quản trị truy xuất dùng NTFS

### Giới thiệu

NTFS - New Technology File System là hệ thống tập tin tiêu chuẩn của Windows NT, kể cả các phiên bản Windows 2000 trở về sau này. NTFS thay thế hệ thống tập tin FAT (File Allocation Table) vốn là hệ thống tập tin phổ biến cho các hệ điều hành Windows của Microsoft. NTFS có nhiều cải tiến hơn FAT như:

### NTFS đáng tin cậy, thể hiện:

* + NTFS dùng nhật ký File và thông tin kiểm tra để khôi phục tính toàn vẹn của hệ thống tệp khi máy tính được khởi động lại.
  + Nếu có lỗi vùng dữ liệu trên đĩa (Sector), NTFS sẽ tự động gán lại vùng Sector bị lỗi và phân bổ một vùng mới cho dữ liệu. Đồng thời, NTFS cũng đánh dấu vùng Sector nào không sử dụng được.

### Bảo mật:

* + Các tệp NTFS sử dụng hệ thống tệp mã hóa (EFS) để bảo mật các tệp và thư mục, nó có thể được mã hóa để sử dụng cho một hoặc nhiều người dùng.
  + NTFS cũng lưu trữ danh sách kiểm soát truy cập (ACL - Access Control List) với mọi tệp và thư mục trên phân vùng NTFS.

### Cải tiến tăng trưởng bộ nhớ:

* + Sử dụng các cấu trúc dữ liệu tiên tiến để cải thiện hiệu suất
  + NTFS hỗ trợ các tệp lớn hơn và số lượng tệp trên mỗi ổ đĩa lớn hơn FAT hoặc FAT32. Cụ thể, số lượng tập tin tối đa trong 1 phân vùng 4.294.967.295 (232 − 1), dung lượng ổ đĩa tối đa là 16 EiB (Exbibyte, 1 EiB = 1.073.741.824 Gigabytes) trên thực tế là 256 TiB (Tebibyte, 1 TiB = 1,024 Gibibytes).
  + Hỗ trợ nhiều quyền người dùng.

### Các quyền truy xuất NTFS

Quyền truy xuất NTFS là hệ thống tập hợp các quyền cho phép hoặc không cho phép Group hay User truy cập vào các đối tượng chứa trên một phân vùng NTFS bao gồm các Folder và File.

Quyền NTFS có thể được định cấu hình trên các thư mục và tệp.

* 6 quyền cơ bản và 14 quyền đặc biệt cho các thư mục.
* 5 quyền cơ bản và 13 quyền đặc biệt cho tệp.

### Các quyền cơ bản trên hệ thống NTFS

|  |  |
| --- | --- |
| Quyền truy cập | Diễn giải |
| Read | * Xem nội dung thư mục và đọc tập tin * Xem thuộc tính thư mục và tập tin |
| Read & Execute | * Read * Duyệt thư mục và chạy chương trình trong thư mục |
| List Folder Contents | * Read * Duyệt thư mục và chạy chương trình trong thư mục |
| Write | * Thay đổi thuộc tính thư mục và tập tin * Tạo mới thư mục và tập tin * Ghi lên tập tin |

|  |  |
| --- | --- |
| Modify | * Read & Excute * Write * Xóa thư mục con và tập tin |
| Full Control | * Modify * Thay đổi quyền sở hữu trên thư mục và tập tin * Sở hữu thư mục và tập tin |

* + - 1. **Các quyền đặc biệt trên hệ thống NTFS**

Quyền đặc biệt chỉ được check khi tiến hành cấu hình thêm các quyền nhỏ trong Advanced Permissions để giúp người quản trị có thể phân quyền chi tiết hơn. Sau đây là mối quan hệ giữa quyền cơ bản và quyền đặc biệt:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Permissions** | **Basic**  **Full Control** | **Basic Modify** | **Basic**  **Read & Execute** | **Basic List**  **Folder Contents** | **Basic Read** | **Basic Write** |
| Travers Folder/Execute File | x | x | x | x |  |  |
| List Folder/Read Data | x | x | x | x | x |  |
| Read Attributes | x | x | x | x | x |  |
| Read Extended Attributes | x | x | x | x | x |  |
| Create Files/Write Data | x | x |  |  |  | x |
| Create Folders/Append Data | x | x |  |  |  | x |
| Write Attributes | x | x |  |  |  | x |
| Write Extended Attributes | x | x |  |  |  | x |
| Delete Subfolders and Files | x |  |  |  |  |  |
| Delete | x | x |  |  |  |  |
| Read Permissions | x | x | x | x | x | X |
| Change Permissions | x |  |  |  |  |  |
| Take Ownership | x |  |  |  |  |  |
| Synchronize | x | x | X | x | x | x |

### Các quy tắc phân quyền NTFS

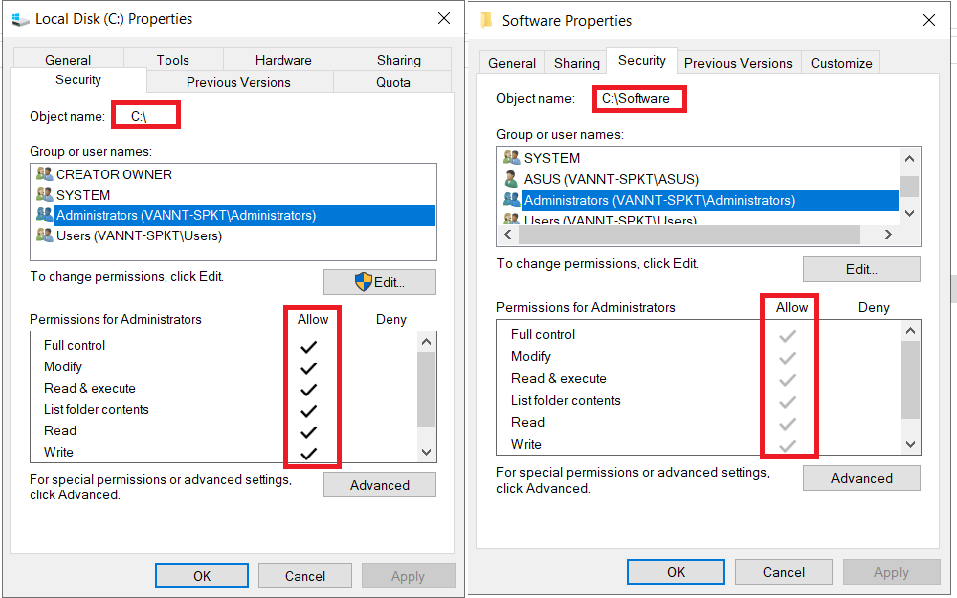
Khi thiết lập quyền truy xuất NTFS trên thư mục và File cần tuân thủ các quy tắc:

### - Sự tích lũy quyền thừa kế:

* Quyền thực sự của một User trên một thư mục hoặc tập tin là tổng quyền sở hữu mà User được gán với quyền sở hữu gán cho nhóm mà User thuộc về.
* Ví dụ: Một User được gán quyền **Read** trên một thư mục, User cũng thuộc về một **nhóm** có quyền **Write** trên thư mục đó. Như vậy quyền của User trên thư mục sẽ là **Read và Write.**

### Kế thừa:

* + Quyền sở hữu gán cho một thư mục được mang xuống (thừa kế) cho các thư mục con và tập tin chứa trong thư mục đó.
  + Tuy nhiên sự thừa kế này có thể điều chỉnh được. Các quyền NTFS kế thừa sẽ có dấu check bị mờ đi.
  + Ví dụ: Thư mục **Software** là thư mục nằm trong phân vùng ổ đĩa **C**, nó được kế thừa các quyền của ổ đĩa C:, khi xem thuộc của thư mục **Software** có dấu check bị mờ - xem trong Properties của thư mục – hình,… Để có thể phân quyền lại, ta phải loại bỏ tính kế thừa (**Inheritance**) của thư mục cần phân quyền: click vào thư mục **Software**, chọn **Properties**, trong **Security Setting**, chọn **Advanced,** chọn lên dòng **Replace all child object permission with inheritable permissions from this object**.



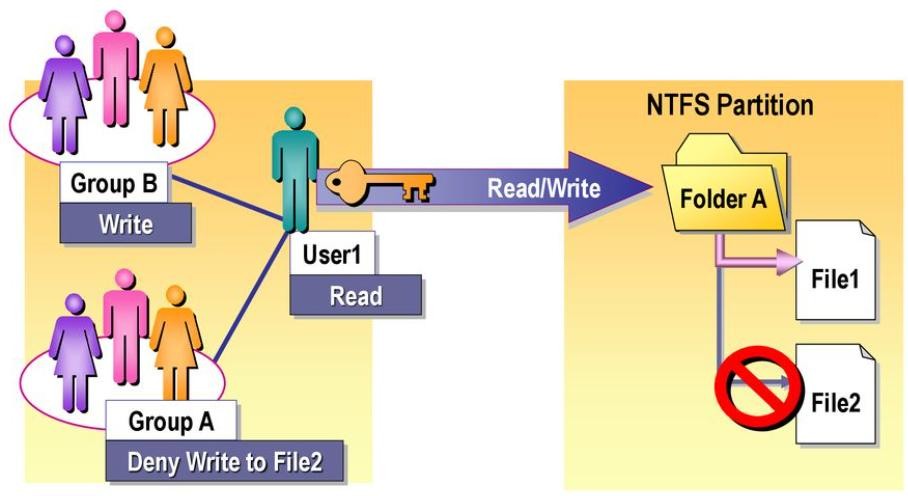
***Hình 6.18:*** *Phân quyền truy cập*

### Ưu tiên:

* + Quyền sở hữu tập tin có độ ưu tiên cao hơn quyền sở hữu trên thư mục.
  + Một User không có quyền truy xuất một thư mục vẫn có thể truy xuất tập tin chứa trong thư mục đó bằng cách sử dụng quy tắc viết tên UNC (Unique Name Convention) hoặc tên đường dẫn cục bộ để mở tập tin.

### Phủ nhận quyền sở hữu:

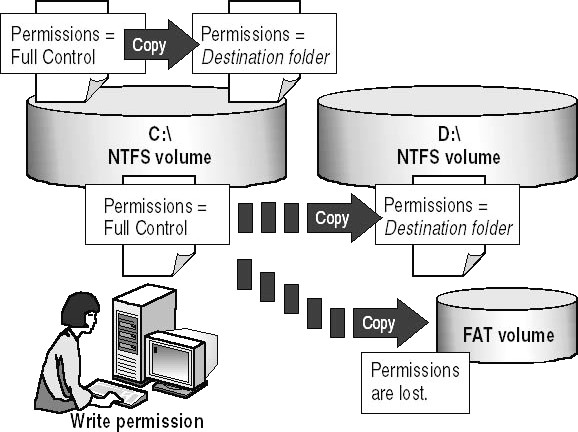
* + Một quyền sở hữu của một User có thể bị ngăn chặn bằng cách phủ nhận (Deny) quyền đó.
  + Ví dụ: User1 có quyền Read trên FolderA và là một thành viên của nhóm A và nhóm B. Nhóm A bị phủ nhận quyền Write trên File2, nhóm B có quyền Write trên thư mục FolderA. User có thể Read và Write trên File1, User cũng có thể Read File2 nhưng không thể Write trên File2 vì User thuộc về nhóm A, nhóm này bị phủ nhận quyền Write trên File2.



***Hình 6.19:*** *Phủ nhận quyền truy cập dữ liệu*

### Di chuyển/sao chép thư mục/tập tin

Khi sao chép thư mục hoặc tập tin từ thư mục này sang thư mục khác hoặc từ Volume này sang Volume khác (sử dụng hệ thống tập tin NTFS), cần lưu ý một số đặc điểm sau:

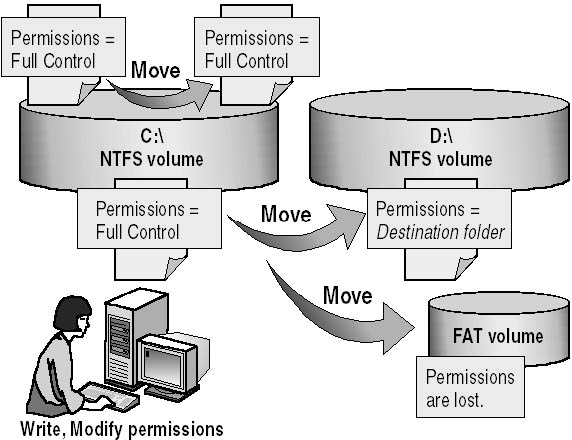
* + Thư mục/tập tin sẽ mang quyền sở hữu của thư mục đích.
  + Người sao chép phải có quyền Write.
  + Người sao chép sẽ trở thành CREATOR.
  + Khi sao chép thư mục hoặc tập tin sang Volume sử dụng FAT, các quyền sở hữu sẽ không còn hiệu lực vì hệ thống tập tin FAT không có tính bảo mật.

***Hình 6.20:*** *Quyền truy cập khi Copy dữ liệu*

Khi di chuyển thư mục/tập tin, quyền sở hữu có thể thay đổi hoặc không thay đổi tùy thuộc vào thư mục đích nằm ở đâu.

Trường hợp di chuyển trên cùng Volume NTFS:

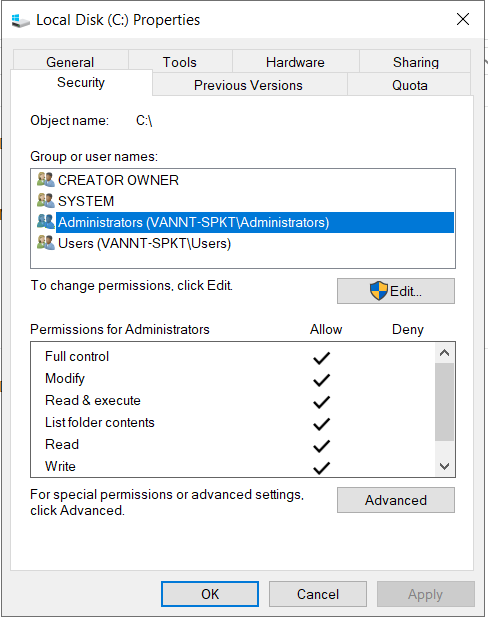
* Người thực hiện lệnh di chuyển phải có quyền Write trên thư mục đích.
* Người thực hiện lệnh di chuyển phải có quyền Modify trên thư mục nguồn vì nguồn sẽ được xóa sau khi di chuyển.
* Người sở hữu trên thư mục/tập tin không thay đổi. Trường hợp di chuyển sang Volume NTFS khác:
* Tập tin/thư mục sẽ thừa kế quyền sở hữu trên thư mục đích.
* Người thực hiện lệnh di chuyển phải có quyền Write trên thư mục đích.
* Người thực hiện lệnh di chuyển phải có quyền Modify trên thư mục nguồn vì nguồn sẽ được xóa sau khi di chuyển.
* Người thực hiện lệnh di chuyển sẽ trở thành CREATOR OWNER của thư mục/tập tin.

Trường hợp di chuyển thư mục hoặc tập tin sang Volume sử dụng FAT, các quyền sở hữu sẽ không còn hiệu lực vì hệ thống tập tin FAT không có tính bảo mật.

***Hình 6.21:*** *Quyền truy cập khi di chuyển dữ liệu*

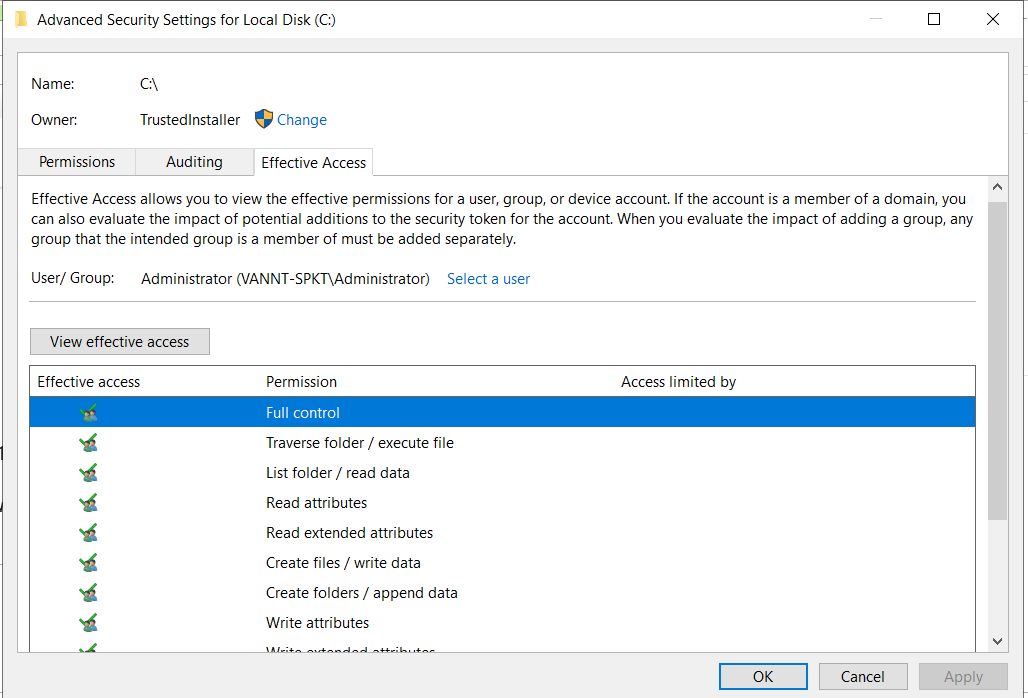
- Gán/thay đổi quyền:

Để gán hoặc điều chỉnh quyền sở hữu trên thư mục hoặc tập tin, thực hiện như sau:

Tại thư mục/tập tin muốn gán hoặc điều chỉnh quyền sở hữu, chọn Properties, click tại thẻ **Security** chọn các quyền muốn thiết lập.

***Hình 6.22:*** *Cấu hình thay đổi quyền truy cập*

* Quyền có hiệu lực:

Đây là kết quả của các quyền được chỉ định trực tiếp cho tệp hoặc thư mục và quyền được thừa kế từ các thư mục mẹ. Để xem các quyền hiệu lực, trong hộp **Advanced Security Settings**, click **Effective Permissions**, chọn người dùng hoặc nhóm, sau đó click **View Effictive Access**:

***Hình 6.23:*** *Một số chức năng cấu hình phân quyền nâng cao*

## Chia sẻ dữ liệu trên mạng

### Đặc điểm của chia sẻ dữ liệu

Chia sẻ dữ liệu (Share) là một trong những công việc chủ yếu khi quản trị một hệ thống mạng. Khi dữ liệu được chia sẻ sẽ cho phép nhiều người dùng cùng một lúc qua mạng. Người dùng có thể truy cập vào một tập tin và thư mục con trong thư mục chia sẻ nếu họ được cấp giấy phép.

Chia sẻ dữ liệu có các đặc điểm sau:

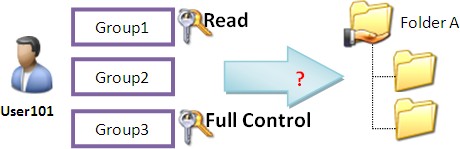
* Chỉ áp dụng cho thư mục, không áp dụng cho tập tin.
* Chỉ áp dụng cho những User từ máy khác truy xuất vào thư mục, không áp dụng cho User cục bộ trên máy chứa thư mục chia sẻ.
* Là cách duy nhất để bảo vệ dữ liệu chia sẻ trên Volume FAT vì các quyền bảo mật NTFS không có tác dụng trên Volume FAT.
* Khi một thư mục được chia sẻ, quyền mặc định trên thư mục là Read gán cho nhóm Everyone.
* Chia sẻ thư mục có thể thực hiện trong một nhóm mạng Workgroup hoặc trong một Domain.

Các quyền trên thư mục chia sẻ:

|  |  |
| --- | --- |
| **Read** | * Xem thư mục. * Đọc nội dung tập tin. * Xem thuộc tính thư mục tập tin. * Thực thi chương trình. |
| **Change** | * Có quyền **Read**. * Tạo thư mục, tập tin. * Sửa đổi nội dung tập tin. * Thay đổi thuộc tính. * Xóa thư mục, tập tin. |
| **Full Control** | * Có quyền **Read** và **Change**. * Gán, rút quyền sở hữu. * Sở hữu tập tin. |

### Các quy tắc khi chia sẻ thư mục

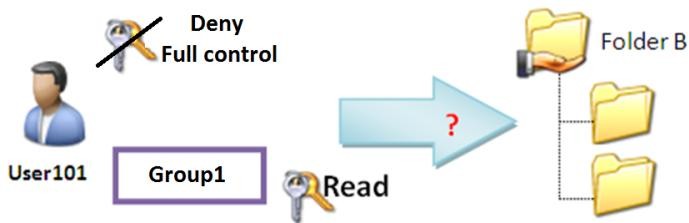
* **Quyền thực sự trên thư mục chia sẻ:**
  + Là kết hợp của quyền được gán và quyền sở hữu gán cho nhóm.
  + Ví dụ User có quyền **Read** thuộc về nhóm Group3 có quyền **Full Control** thì quyền thực sự của User sẽ là **Full Control -** quyền này bao hàm quyền Read của Group2.



***Hình 6.24:*** *Quyền trên thư mục chia sẻ*

### Phủ nhận quyền:

* + Việc phủ nhận một quyền làm mất tác dụng của quyền đã gán cho User hoặc nhóm User. Nếu một User bị phủ nhận quyền sở hữu trên một thư mục chia sẻ, User sẽ không có khả năng truy xuất thư mục mặc dù User thuộc về nhóm đã được gán quyền trên thư mục chia sẻ.
  + Ví dụ: User101 thuộc về nhóm Group1, nhóm này được gán quyền Read trên thư mục FolderB. Tuy nhiên User101 bị phủ nhận quyền Full Control trên FolderB, vậy User101 không có quyền gì trên FolderB.



***Hình 6.25:*** *Phủ nhận quyền trên thư mục chia sẻ*

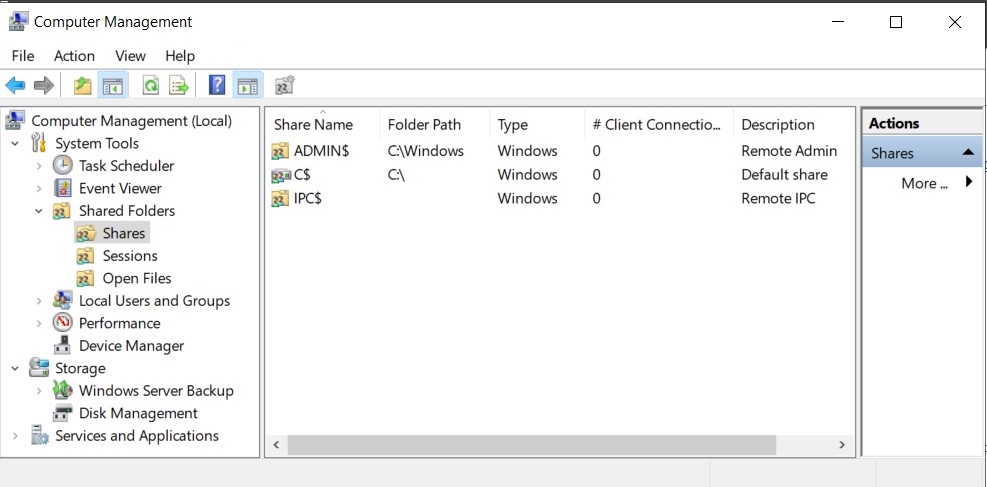
### Chia sẻ thư mục có quyền NTFS:

* + Khi sao chép một thư mục sử dụng thêm quyền NTFS để việc kiểm soát dữ liệu thư mục chia sẻ, thư mục nguồn vẫn còn chia sẻ nhưng thư mục đích thì không.
  + Đối với các thư mục chia sẻ nằm trên Volume FAT, quyền trên thư mục chia sẻ là cách duy nhất để bảo vệ dữ liệu. Tuy nhiên, đối với các thư mục chia sẻ nằm trên Volume NTFS thì được gán quyền đầy đủ hơn.

### Gán/thay đổi quyền:

* + Gán quyền chia sẻ cho nhóm thay vì gán cho từng User.
  + Gán quyền chia sẻ một cách chặt chẽ nhất nhưng vẫn đảm bảo cho User có thể thực hiện được các tác vụ cần thiết của mình. Ví dụ nếu User chỉ cần đọc, không bao giờ xóa hoặc tạo tập tin trên một thư mục thì chỉ cần gán quyền Read trên thư mục đó.
  + Nên tổ chức dữ liệu sao cho các thư mục sẽ có cùng quyền sở hữu chứa trong cùng một thư mục. Ví dụ nếu User cần chạy một số ứng dụng nào đó thì nên chứa thư mục của các ứng dụng đó trong cùng thư mục.
  + Nên sử dụng tên chia sẻ gợi nhớ giúp User dễ dàng định vị và nhận dạng dữ liệu chia sẻ.

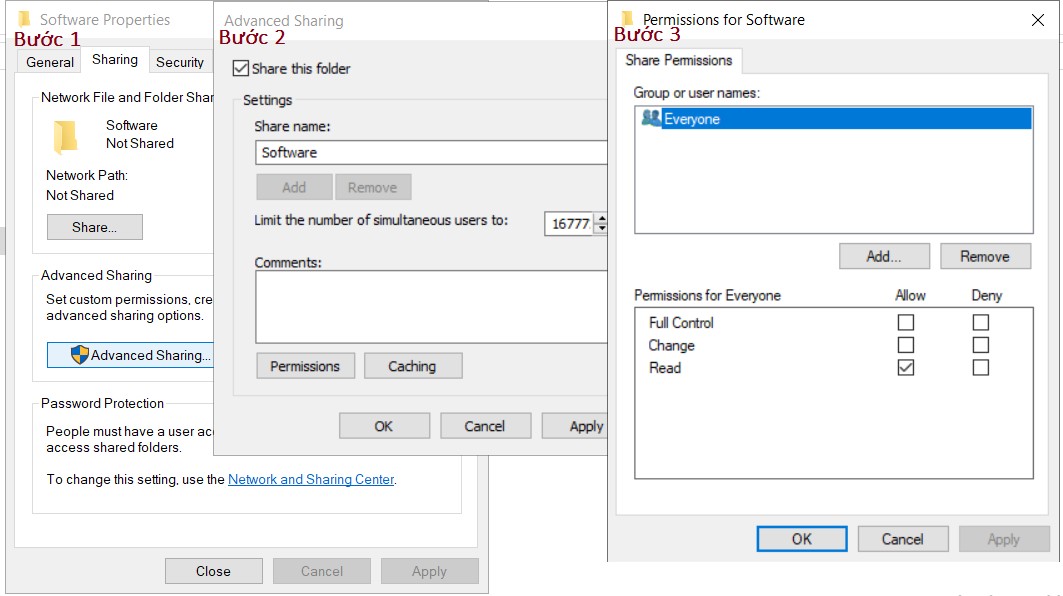
### Thư mục chia sẻ mặc định

Các thư mục được chia sẻ mặc định gồm thư mục gốc của mỗi Volume, thư mục gốc hệ thống và thư mục chứa chương trình điều khiển máy in. Để xem các thư mục chia sẻ này, vào Computer Management, click Shared Folders, click Shares.

***Hình 6.26:*** *Các thư mục chia sẻ mặc định*

### Thực hiện chia sẻ thư mục

* Các thông tin cần khai báo khi chia sẻ:
  + Tên chia sẻ: Share Name.
  + Số User truy xuất vào thư mục chia sẻ: Limit the number of simultaneous users to.
  + Quyền: Permissions.
* Các bước thực hiện chia sẻ:
  + Chọn thư mục, click Properties, click Network and Sharing Center.
  + Nhập tên chia sẻ và số User.
  + Click Permissions để gán quyền.



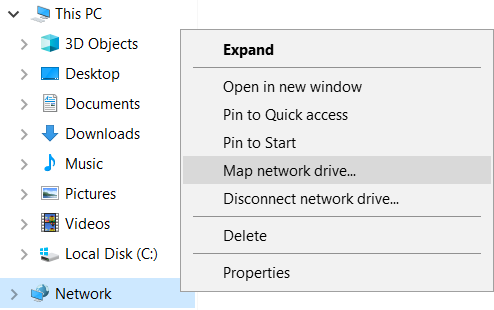
***Hình 6.27:*** *Chia sẻ thư mục và gán quyền truy cập*

* Share ẩn và Share công khai:
  + Để Share ẩn người ta thêm dấu $ phía sau cùng của Share Name. Với Share ẩn, User cần biết chính xác tên của thư mục Share là gì và điền chính xác tên đó cùng với dấu $ phía sau cùng thì mới có thể truy cập được.
  + Đối với Share công khai, người dùng không cần phải gõ chính xác địa chỉ và tên thư mục Share, người dùng chỉ cần truy cập vào địa chỉ IP hoặc tên máy thực hiện Share dữ liệu là được.

### Truy xuất dữ liệu chia sẻ

Có 3 phương pháp thường sử dụng để sử dụng dữ liệu chia sẻ:

* Thông qua biểu tượng My Network Places.
* Định nghĩa ánh xạ ổ đĩa:



***Hình 6.28:*** *Ánh xạ ổ đĩa mạng*

* Sử dụng tiện ích dòng lệnh Net use: net use <ổ đĩa:> <Tên UNC> rồi bấm Enter (UNC: Universal Naming Convention).

Ví dụ: Để chia sẻ thư mục My Document với Share Name là My\_ Docs, nhập lệnh như sau tại dòng lệnh rồi bấm Enter:

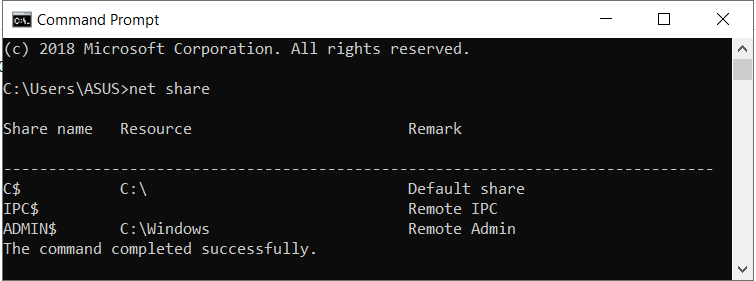
C:\> net use k: \\servername\My\_Docs

### Kiểm soát dữ liệu chia sẻ

Quản lý các thư mục chia sẻ cho phép người quản trị mạng có cái nhìn đầy đủ về các thư mục đã chia sẻ trên mạng, tránh tình trạng chia sẻ những thư mục không cần thiết.

Để xem danh sách các thư mục chia sẻ có thể thực hiện bằng các cách sau:

- Sử dụng tiện ích dòng lệnh Net Share:



***Hình 6.29:*** *Kiểm tra các thư mục chia sẻ trên máy tính*

- Sử dụng cửa sổ Computer Management: vào Computer Management, click Shared Folders, click Shares.

## Kết hợp quyền thư mục được chia sẻ và quyền NTFS

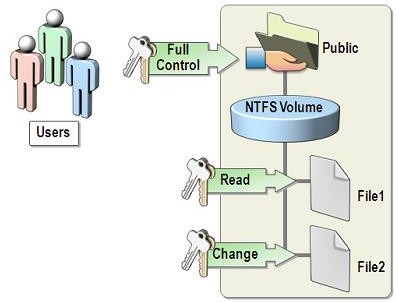
Khi bạn sử dụng quyền đối với thư mục chia sẻ trên ổ đĩa NTFS, các quy tắc sau sẽ được áp dụng:

* Có thể áp dụng quyền NTFS cho các tệp và thư mục con trong thư mục chia sẻ.
* Có thể áp dụng các quyền NTFS khác nhau cho từng tệp và thư mục con chứa bên trong một thư mục chia sẻ.
* Ngoài quyền trên thư mục chia sẻ, User cần được kiểm soát quyền truy xuất bằng quyền NTFS trên tập tin và thư mục con

trong thư mục chia sẻ. Điều này khác với việc chia sẻ một thư mục trên Volume FAT, quyền chia sẻ là quyền cơ chế bảo mật duy nhất.

* Khi kết hợp quyền trên thư mục chia sẻ với quyền NTFS, quyền thực sự sẽ là quyền chặt chẽ (hạn chế) hơn trong hai loại quyền.

Ví dụ: Nhóm Everyone có quyền **Full Control** trên thư mục chia sẻ Public và quyền NTFS là Read trên tập tin FileA. Như vậy quyền thực sự của nhóm Everyone trên tập tin FileA là **Read**, còn quyền thực sự của nhóm Everyone trên tập tin FileB là **Change**.



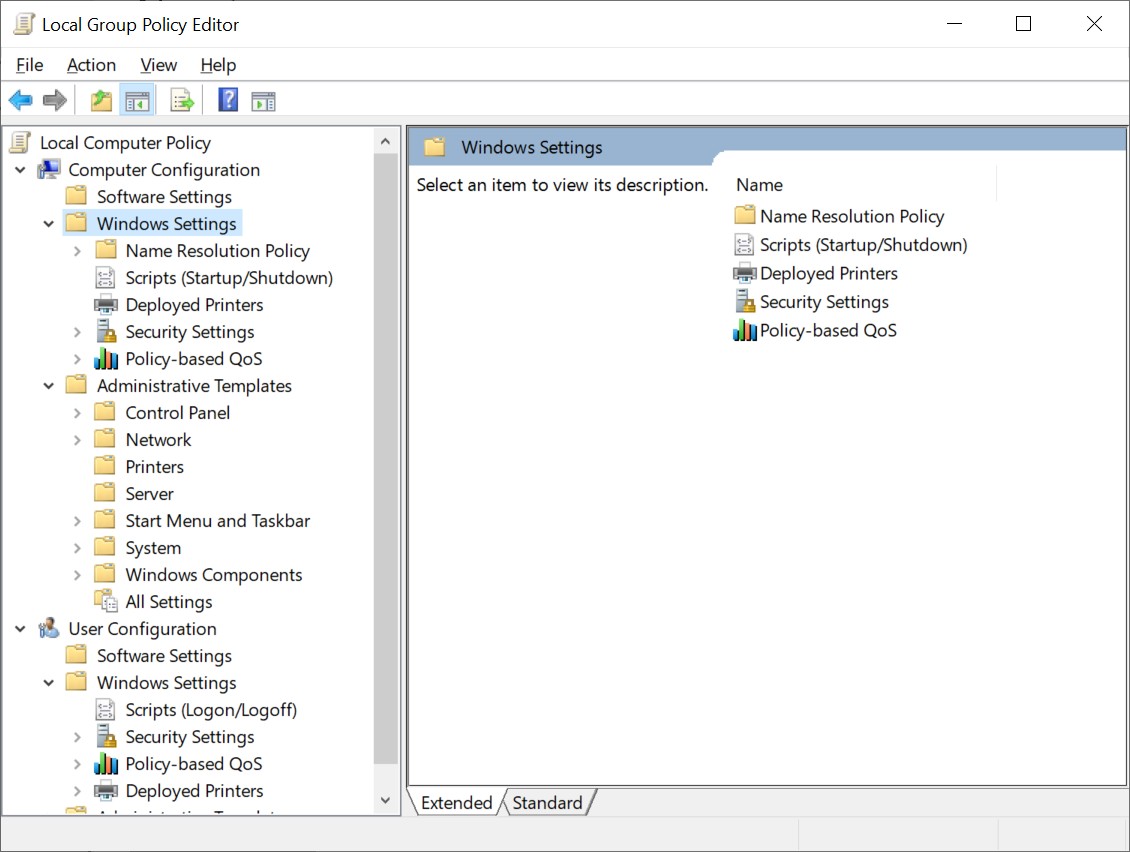
***Hình 6.30:*** *Kết hợp quyền NTFS và quyền chia sẻ*

## Thiết lập các chính sách quản trị (GPO)

Group Policy là tập hợp các thiết lập cấu hình cho Computer và Users, xác định cách thức để các chương trình, tài nguyên mạng và hệ điều hành làm việc với người dùng và máy tính trong 1 tổ chức. Group Policy sẽ giúp việc quản lý người dùng chặt chẽ và hiệu quả hơn.

Group Policy có thể triển khai ở 2 dạng:

- Tại máy tính cục bộ - dùng Local Group Policy Editor trong Control Panel\All Control Panel Items\Administrative Tools để thiết lập các chính sách về Computer và Users gồm các mục: phần mềm, Windows, quản trị.

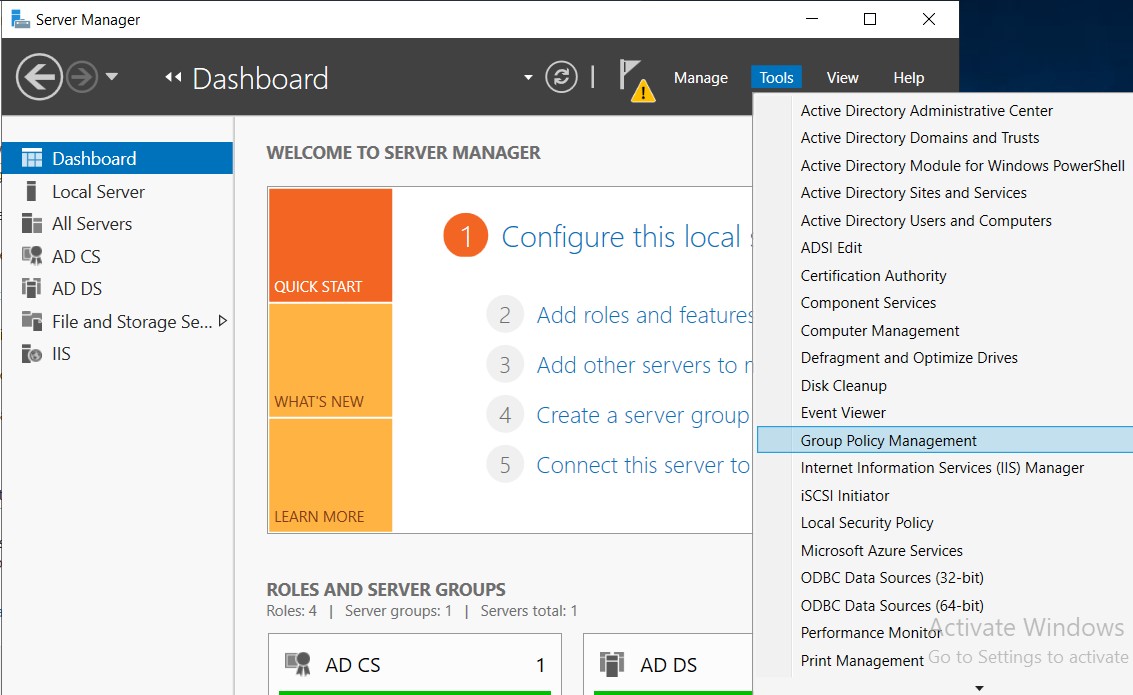


***Hình 6.31:*** *Giao diện cấu hình các chính sách quản trị (GPO)*

* Trong Domain: Các Group Policy được áp dụng cho các Site, Domain và OU (Organizational Unit). Các Group Policy áp dụng cho các đối tượng gọi là Group Policy Object (GPO).

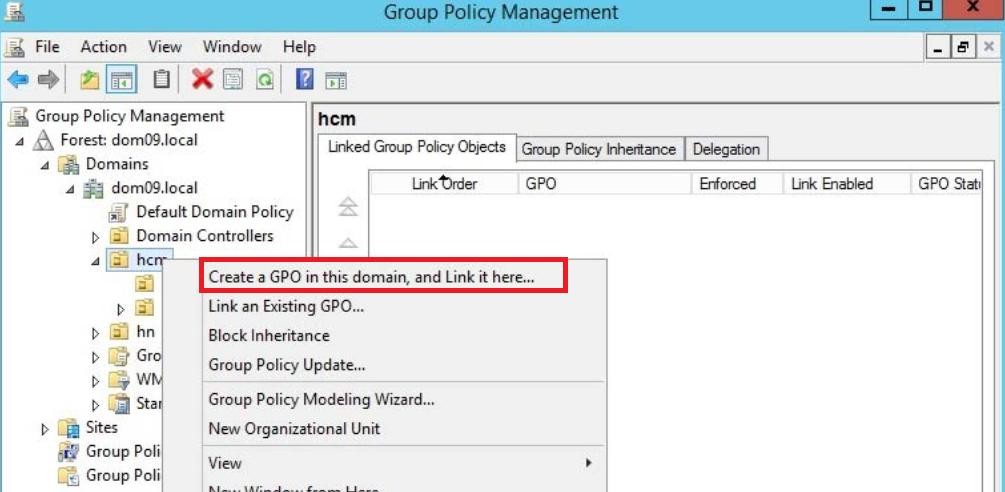
Các đặc điểm của GPO:

* + Các GPO được lưu trữ một phần trong cơ sở dữ liệu của AD và một phần trong Share SYSVOL. Mục đích sử dụng GPO trong Domain là nhằm triển khai các chính sách từ miền máy chủ Domain Controller xuống Users.
  + CPO có tính kế thừa: Các OU con tự động liên kết và áp dụng các GPO đã được tạo ra trong các OU cha, đây là thuộc tính mặc định của OU. Có thể ngăn chặn tính kế thừa trong Group Policy: “Block Policy Inheritance”.
  + Chương trình để tạo ra và chỉnh sửa GPO có tên là Group Policy Object Editor (đây là 1 dạng Console tên là gpedit.msc, Console của Active Directory Users and Computers là dsa.msc).

Cấu hình GPO: Chọn Server Manager\Tool, chọn Group Policy Management:

***Hình 6.32:*** *Giao diện chọn chức năng cấu hình GPO*

Sau đó, chúng ta sẽ tạo GPO cho các OU trong Domain. Ví dụ:



***Hình 6.33:*** *Tạo mới một GPO*

Các Group Policy thông dụng:

* Triển khai phần mềm cho một hoặc nhiều máy trạm nào đó một cách tự động.
* Ấn định quyền hạn cho một số người dùng mạng.
* Giới hạn những ứng dụng mà người dùng được phép chạy.
* Kiểm soát hạn ngạch sử dụng đĩa trên các máy trạm.
* Thiết lập các kịch bản (Script) đăng nhập (Log-on), đăng xuất (Log-out), khởi động (Start-up), và tắt máy (Shut-down).
* Chuyển hướng (Redirector) một số Folder trên máy khách (như Computer, My Document) lên DC,…

## Tổng kết chương

Các kiến thức về mô hình mạng Workgroup và Domain được mô tả đầy đủ với các thành phần, kiến trúc và các dịch vụ triển khai. Mô hình Domain được sử dụng quản lý người dùng và tài nguyên hiệu quả với các hỗ trợ về chia sẻ thư mục, gán quyền truy xuất NTFS và thiết lập các chính sách nhóm.

## Câu hỏi và bài tập

1. Máy hoạt động trong mô hình Workgroup được gọi là?
   1. Server.
   2. Client.
   3. Peer To Peer.
   4. Workstation.
2. Mô hình Workgroup sử dụng User đăng nhập là?
   1. Domain User.
   2. Local User.
   3. Anonymous.
   4. Bất kỳ loại User nào.
3. Thành phần nào **không** thuộc kiến trúc logic của Active Directory?
   1. Domain.
   2. Domain Controller.
   3. Object.
   4. Organizational Units (OU).
4. Thành phần nào thuộc kiến trúc vật lý của Active Directory?
   1. Domain.
   2. Domain Controller.
   3. Object.
   4. Organizational Units (OU).
5. Organizational Units (OU) có thể chứa gì?
   1. Domain.
   2. Domain Controller.
   3. Object.
   4. Forest.
6. Dịch vụ nào sẽ lưu trữ thông tin về các đối tượng trong Domain?
   1. Active Directory Domain Services (ADDS).
   2. Active Directory Lightweight Directory Services (ADLDS).
   3. Active Directory Federation Services (ADFS).
   4. Active Directory Rights Management Services (ADRMS).
7. Khi Roamming Profile cho User đến máy DC1, lưu trong thư mục đã chia sẻ Homedir. Câu lệnh là?
   1. \\DC1\Homedir\Username.
   2. \\DC1\Homedir\%Username%.
   3. \\DC1\Homedir\%User%.
   4. \\DC1\Homedir\User.
8. Máy chủ DC là?
   1. Máy chủ quản lý miền.
   2. Máy chủ quản lý User và Computer.
   3. Máy chủ các tài nguyên trong mạng công ty.
   4. Máy chủ cung cấp các dịch vụ và quản lý toàn bộ mạng.
9. Để truy cập thư mục Data được Share ẩn trên PC01, sử dụng lệnh?
   1. \\PC01\Data$.
   2. \\Data$.
   3. \\PC01/Data.
   4. \\Data.
10. User U1 phân quyền NTFS bị cấm truy xuất tới thư mục Data, biết thư mục Data được chia sẻ cho nhóm Everyone với quyền Read, lúc này U1 có quyền?
    1. U1 không thể truy xuất thư mục chia sẻ Data.
    2. U1 có thể đọc dữ liệu trong thư mục Data.
    3. U1 có thể truy xuất thư mục chia sẻ Data, nhưng chỉ có quyền đọc.
    4. U1 có toàn quyền truy xuất thư mục chia sẻ Data.
11. User U1 thuộc 2 Group G1 và G2, G1 có quyền List, Read, Read & Execute trên thư mục Data, G2 bị cấm quyền truy xuất thư mục Data. Quyền của U1 là?
    1. U1 chỉ có thể xem nội dung thư mục Data, nhưng không mở được các File trên thư mục này.
    2. U1 không có quyền truy xuất thư mục Data.
    3. U1 có thể đọc và thực thi các tập tin chương trình đặt trong thư mục Data.
    4. U1 có quyền truy xuất thư mục Data.
12. Nhóm Users gồm các User Hoa, Tuan, An có quyền Read & Write trên thư mục Documents.

* Các User Hoa, Tuan, An có quyền gì trên thư mục Pictures?
* Muốn cho An có quyền Read trên thư mục Private còn các User Hoa và Tuan không có quyền gì cả thì phải làm gì?

Documents



Pictures

Pr

Read & Write



Users



ivate

An



Hoa Tuan

1. Trong môi trường Microsoft, mô hình nào có các thông tin người dùng được lưu trữ tập trung và người dùng phải chứng thực khi đăng nhập vào mạng:
   1. Server.
   2. Client.
   3. Domain.
   4. Workgroup.
2. Jery vừa thuộc nhóm Marketing và nhóm Accounting, User Jery có quyền Read thư mục D:\Data. Trong khi đó, nhóm Marketing có quyền Write thư mục D:\Data, nhưng nhóm Accounting bị cấm quyền Write File D:\Data\vb2.txt. Vậy Jery có quyền gì trên File vb2.txt?
   1. Read.
   2. Read & Write.
   3. Write.
   4. Không có quyền gì.
3. Quyền nào là quyền đặc biệt trên NTFS?
   1. Take Ownership.
   2. Execute.
   3. Write.
   4. Modify.
4. Quyền nào là quyền cơ bản trên NTFS?
   1. Take Ownership.
   2. Delete.
   3. Synchronize.
   4. Modify.
5. Trong Windows, User Profile là nơi?
   1. Lưu tất cả các thông tin liên quan đến User (Desktop, Start Menu,...).
   2. Là thư mục gốc của User khi đăng nhập.
   3. Là nơi lưu tất cả các thuộc tính của User.
   4. Các User khác có thể đọc thư mục này.
6. Máy PC01 chia sẻ thư mục Shared với tên là Shared\_PC01, máy trong LAN có thể truy cập trực tiếp thư mục này bằng lệnh?
   1. \\PC01/Shared.

B. \\PC01.

C. \\PC01\shared\_pc01.

D. \\PC01/SharedShared\_PC01.

1. Để Share ẩn một thư mục, ta thêm?
   1. Chữ & vào sau tên chia sẻ.
   2. Chữ & vào trước tên chia sẻ.
   3. Chữ $ vào sau tên chia sẻ.
2. Chữ $ vào trước tên chia sẻ.Quyền Change trên thư mục chia sẻ không được làm gì?
   1. Gán, rút quyền sở hữu.
   2. Tạo thư mục, tập tin.
   3. Thay đổi thuộc tính.

# CHƯƠNG 7

**XÓA THƯ MỤC, TẬP TIN. AN NINH MẠNG**

Chương này sẽ đề cập đến một số khái niệm về an ninh mạng, phân loại các lỗ hổng bảo mật. Học xong chương này, người học có khả năng:

* Trình bày được một số khái niệm cơ bản về lĩnh vực an ninh mạng.
* Trình bày được một số đặc điểm cơ bản của các loại lỗ hổng bảo mật.
* Trình bày được các bước cơ bản của quá trình tấn công xâm nhập, khai thác lỗ hổng.
* Trình bày được các cách phòng chống, hạn chế hậu quả trong an toàn thông tin.
* Trình bày được vai trò của hệ thống giám sát mạng.
* Trình bày được những đặc điểm quan trọng của hệ thống giám sát.
* Cài đặt được một tấn công đơn giản.

## Giới thiệu

Trong thời đại công nghệ thông tin ngày nay, đặc biệt là công nghệ mạng phát triển cực kỳ mau lẹ, từ đó phát sinh vấn đề an toàn thông tin là một thách thức rất lớn bao trùm hầu hết từ phần cứng đến phần mềm và cả vai trò của người sử dụng. Ba mục tiêu chính trong an toàn thông tin, được biết đến với tên gọi là mô hình CIA (Confidentiality, Integrity, Availability), cần được đảm bảo là: tính bí mật, tính toàn vẹn và tính sẵn sàng. Bất kỳ sự vi phạm nào trong ba tính chất trên đều dẫn đến nguy cơ mất an toàn thông tin.

* + - Tính bí mật: Đảm bảo rằng chỉ những người dùng hợp pháp mới có thể truy cập được hệ thống, dữ liệu.
    - Tính toàn vẹn: Đảm bảo rằng dữ liệu không bị thay đổi bởi những người không được phép.
    - Tính sẵn sàng: Đảm bảo rằng dữ liệu, hệ thống có thể phục vụ được việc truy cập của người dùng hợp pháp.

Để đảm bảo an toàn tuyệt đối cho một hệ thống CNTT là một việc khó bởi các điểm yếu, mối đe dọa, rủi ro tồn tại ở rất nhiều thành phần trong một hệ thống CNTT. Có thể chia vấn đề bảo mật ra làm 3 giai đoạn:

* + - Time to compromise: Thời gian để xâm nhập vào một hệ thống.
    - Time to discover: Thời gian phát hiện xâm nhập.
    - Time to recovery: Thời gian khôi phục hệ thống.

**Time to compromise Time to discover Time to recover**

**Outcome:**

**Time to compromise Time to discover Time to recover**

***Hình 7.1:*** *Ba giai đoạn trong bảo vệ hệ thống*

Như vậy, đứng về phương diện người làm an ninh mạng thì mục tiêu quan trọng để bảo mật cho một hệ thống CNTT là làm sao để:

* Tăng thời gian Time To Compromise, nghĩa là sử dụng các giải pháp để làm khó kẻ tấn công, làm cho chúng mất rất nhiều thời gian mới có thể tìm ra các điểm yếu bảo mật và xâm nhập vào hệ thống.
* Giảm thời gian Time To Discover, nghĩa là sử dụng các giải pháp để nhận diện sớm các bất thường, nhận diện sớm hệ thống đang bị tấn công.
* Giảm thời gian Time To Recovery, nghĩa là sử dụng các giải pháp để phòng khi hệ thống bị tấn công thì vẫn có khả năng khôi phục lại hiện trạng như trước khi bị tấn công.

Xây dựng hệ thống bảo mật nhiều lớp (hay bảo mật theo chiều sâu

- Defense In Depth):

Như đã đề cập ở trên, các điểm yếu bảo mật tồn tại trong từng phần cấu thành nên hệ thống CNTT. Do đó, để có thể thực hiện các biện pháp phòng chống có hiệu quả, giải pháp bảo mật nhiều lớp nên được xem xét áp dụng để việc bảo mật toàn diện có hiệu quả. Hệ thống bảo mật nhiều lớp còn có tên gọi khác là bảo vệ theo chiều sâu (Defense In Depth).



Defense in depth

Defense in depth

***Hình 7.2:*** *Bảo mật theo chiều sâu*

Vấn đề bảo mật ngày càng quan trọng cho các tổ chức, doanh nghiệp. Để không ngừng nâng cao năng lực bảo mật cho hệ thống CNTT, các tổ chức nên chú ý phát triển 3 yếu tố quan trọng, viết tắt là P-P-T, đó là: Con người - Quy trình - Công nghệ. Nâng cao khả năng quản trị bảo mật cho hệ thống với: chính sách an toàn thông tin, hệ thống ghi nhận sự kiện ATTT và đào tạo nâng cao nhận thức.

Một nguyên tắc quan trọng khác khi làm về an ninh mạng là “nguyên tắc quyền tối thiểu”, nghĩa là chỉ cung cấp các quyền cần thiết nhất đủ cho người dùng các chương trình hay tiến trình thực hiện các tác vụ của mình. Đi kèm với nguyên tắc này, một thuật ngữ được sử dụng nhiều trong vấn đề an ninh mạng là “Hardening”. Ý nghĩa của nó là các cổng trên thiết bị phần cứng, các ứng dụng, các dịch vụ,… nào không cần

sử dụng thì phải tắt đi hay xóa đi. Điều này giúp làm giảm các nguy cơ phát sinh tấn công hệ thống.

Trong lĩnh vực rộng lớn của an toàn thông tin, trong chương này chúng ta chỉ tập trung vào một số vấn đề cơ bản của an ninh mạng. Trong đó đề cập đến các loại lỗ hổng trong mạng, cách khai thác và phòng chống ở các mức độ khác nhau.

## Phân loại lỗ hổng mạng

Hiểu được những điểm yếu trong bảo mật là một vấn đề hết sức quan trọng để tiến hành những chính sách bảo mật có hiệu quả. Những điểm yếu trong bảo mật mạng có thể được phân thành 3 loại như sau:

* Điểm yếu về mặt kỹ thuật:

Điểm yếu trong kỹ thuật gồm có điểm yếu trong giao thức, trong các hệ điều hành và các thiết bị phần cứng.

* Điểm yếu trong cấu hình hệ thống:

Đây là lỗi do người quản trị tạo ra. Lỗi này do các thiếu sót trong việc cấu hình hệ thống như: sử dụng các cấu hình mặc định, Password đơn giản,…

* Điểm yếu trong chính sách bảo mật:

Chính sách bảo mật diễn tả cách thức, quy định và vị trí thực hiện. Đây là điều kiện quan trọng giúp việc bảo mật có hiệu quả tốt nhất. Mỗi công ty, tổ chức nên xây dựng chính sách bảo mật đặc thù cho đơn vị mình.

## Các dạng tấn công mạng

Có nhiều dạng tấn công mạng đã được biết đến, có thể phân loại dựa vào những tiêu chí khác nhau. Nếu dựa vào hành động của cuộc tấn công thì có thể chia tấn công làm 2 loại: tấn công chủ động và tấn công bị động.

* Tấn công chủ động: Kẻ tấn công làm thay đổi hoạt động của hệ thống và hoạt động của mạng khi tấn công làm ảnh hưởng đến tính toàn vẹn, sẵn sàng và xác thực của dữ liệu.
* Tấn công bị động: Kẻ tấn công cố gắng thu thập thông tin từ hoạt động của hệ thống và hoạt động của mạng làm phá vỡ tính bí mật của dữ liệu.

Nếu dựa vào nguồn gốc của cuộc tấn công thì có thể phân loại tấn công làm 2 loại: tấn công từ bên trong và tấn công từ bên ngoài.

* Tấn công từ bên trong: Là những tấn công xuất phát từ bên trong hệ thống mạng. Người sử dụng muốn truy cập, lấy thông tin nhiều hơn quyền cho phép.
* Tấn công từ bên ngoài: Là những tấn công xuất phát từ bên ngoài Internet hay các kết nối truy cập từ xa.

## Một số tấn công mạng phổ biến

### Tấn công vào các trang Web

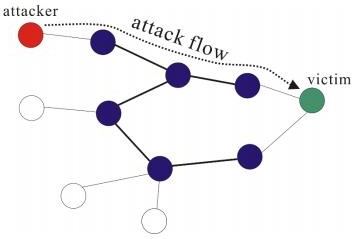
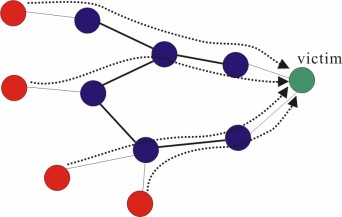
Web là dịch vụ được sử dụng rất phổ biến trên mạng, do đó nó là mục tiêu của nhiều cuộc tấn công. Website bị hacker tấn công chủ yếu do các vấn đề:

Lỗi kiểm soát truy cập: Việc truy cập vào các ứng dụng Web không được bảo vệ an toàn sẽ bị các hacker đoán mật khẩu để truy cập một cách trái phép. Ví dụ, tấn công Cross Site Scripting (XSS) hoặc Cross Site Request Forgery (CSRF), trong đó kẻ tấn công cố gắng đánh chặn các thông tin đăng nhập của người dùng thông qua trình duyệt của chính họ.

Lỗ hổng phần mềm: Những phần mềm dùng viết và quản lý Website cũng có những lỗ hổng như: máy chủ Web, cơ sở hạ tầng, công cụ viết Web,... Ví dụ các lỗ hổng phần mềm như Remote Code Execution (RCE), Remote/Local File Inclusion (R/LFI) - đây là hai lỗ hổng liên quan đến máy chủ Web; SQL Injection (SQLi) - lỗ hổng của SQL;... Các kẻ tấn công có thể khai thác các lỗ hổng này để tấn công vào các Website.

### Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ (DoS hay DDoS) là sự nỗ lực làm cho những người dùng bình thường không thể sử dụng tài nguyên của một hay nhiều máy tính hoặc làm cho hệ thống đó chậm đi một cách đáng kể, bằng cách làm quá tải tài nguyên của hệ thống.

***Hình 7.3:*** *Tấn công DoS và DDoS*

Điểm khác biệt cơ bản giữa tấn công DoS và DDoS là: tấn công DoS xuất phát từ một nguồn còn tấn công DDoS xuất phát từ rất nhiều nguồn tấn công, tạo thành một hệ thống mạng lưới gọi là mạng Botnet. Hệ thống Botnet ngày càng lớn về quy mô và trở nên rất nguy hiểm cho bất cứ một hệ thống mạng nào. So với tấn công DoS, tấn công DDoS có sức mạnh lớn hơn rất nhiều lần với số lượng gói tin rất lớn ào ạt gửi tới nạn nhân nhằm chiếm dụng tài nguyên và làm tràn ngập đường truyền của mục tiêu xác định.

Dấu hiệu của một vụ tấn công từ chối dịch vụ gồm có:

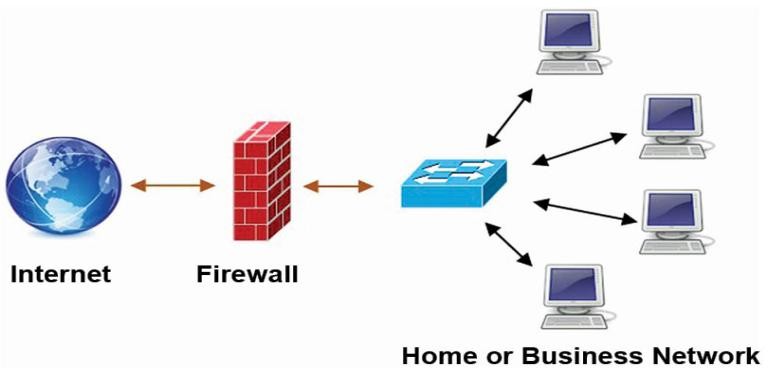
* Mạng thực thi chậm khác thường khi mở tập tin hay truy cập Website.
* Không thể dùng một Website cụ thể.
* Không thể truy cập bất kỳ Website nào.
* Tăng lượng thư rác nhận được.

### Tấn công bằng mã độc

Mã độc là một loại phần mềm được tạo ra và chèn vào hệ thống một cách bí mật với mục đích thâm nhập, phá hoại hệ thống hoặc lấy cắp thông tin, làm gián đoạn, tổn hại tới tính bí mật, tính toàn vẹn và tính sẵn sàng của máy tính nạn nhân. Một số mã độc phổ biến như: Virus, Worm, Trojan,...

## Các hệ thống an ninh mạng

Không có một giải pháp nào là hoàn hảo, có khả năng phát hiện, ngăn chặn tất cả các loại tấn công mạng. Để đảm bảo an toàn thông tin

nói chung và an ninh mạng nói riêng, các giải pháp kết hợp nên được thực hiện nhằm phát hiện nhanh, ngăn chặn các tấn công mạng, kịp thời khôi phục hệ thống, chủ động và tự động vận hành. Thực hiện các giải pháp bảo vệ theo chiều sâu, chia thành nhiều lớp phòng vệ. Một số giải pháp an ninh mạng phổ biến hiện nay được trình bày sau đây.

***Hình 7.4:*** *Bảo vệ mạng LAN với Firewall*

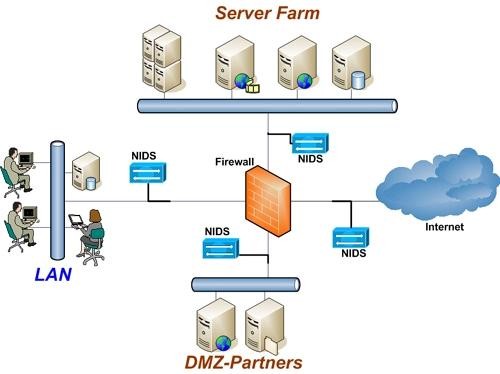
### Firewall

Firewall là phần cứng hoặc phần mềm máy tính giúp bảo vệ các hệ thống khỏi sự truy cập trái phép. Chức năng cơ bản nhất của tường lửa là kiểm soát các truy cập vào/ra hệ thống thông qua các luật (Rules). Các luật của Firewall được thiết kế theo chính sách bảo mật của tổ chức. Firewall giám sát tất cả các kết nối đi vào/ra hệ thống mạng và cho phép hoặc từ chối truy cập theo các luật được xác định trước.

Có các dạng Firewall:

* + - * Packet Filter: Tường lửa lọc gói hoạt động ở lớp Mạng của mô hình OSI và kiểm tra mọi gói đi qua để khớp với danh sách kiểm soát truy cập được xác định trước. Một số yếu tố mà tường lửa lọc gói sử dụng để đưa ra quyết định như địa chỉ IP nguồn, địa chỉ IP đích,...
      * Circuit Level Gateways: Firewall này hoạt động ở lớp Phiên của mô hình OSI. Nó không lọc các gói riêng lẻ. Thay vào đó, nó giám sát tất cả các yêu cầu thiết lập phiên mới và kiểm tra xem việc bắt tay ba bước TCP đã được hoàn thành hay chưa để xác minh tính hợp lệ của phiên.
      * Application Level Gateways: Firewall này hoạt động ở lớp Ứng dụng của mô hình OSI. Loại tường lửa này lọc lưu lượng dựa trên các lệnh dành riêng cho ứng dụng, như HTTP GET hoặc POST.

### IDS/IPS

Hệ thống phát hiện xâm nhập (IDS) là một hệ thống lắng nghe, giám sát lưu lượng mạng và phát cảnh báo khi phát hiện bất kỳ loại xâm nhập nào vào hệ thống mạng. Ngay khi IDS phát hiện ra một vụ xâm nhập và đưa ra cảnh báo, quản trị viên có thể thực hiện hành động thích hợp để ngăn chặn hoặc giảm tác động của xâm nhập. IDS chủ yếu làm việc bằng cách sử dụng chữ ký, do đó nó có một cơ sở dữ liệu chữ ký được xác định trước cho các loại tấn công khác nhau. Ngoài ra, IDS còn hoạt động dựa vào các dấu hiệu bất thường - tức hệ thống sẽ tìm ra những điểm khác so với các dữ liệu bình thường và cảnh báo chúng là xâm nhập. Tập luật là thành phần quan trọng nhất của một hệ thống phát hiện xâm nhập. Đây là tập sẽ định ra dấu hiệu (mẫu) để so sánh, đối chiếu với dữ liệu ở đầu vào. Tùy vào mục tiêu bảo vệ, IDS có 2 dạng: Host Based IDS và Network Based IDS.

***Hình 7.5:*** *Một số thiết bị an ninh trong hệ thống mạng*

Hệ thống ngăn chặn/phòng chống xâm nhập (IPS) là hệ thống theo dõi, ngăn ngừa kịp thời các hoạt động xâm nhập không mong muốn. Chức năng chính của IPS là xác định các hoạt động nguy hại, lưu giữ các thông tin này, sau đó kết hợp với Firewall để dừng ngay các hoạt động này, và cuối cùng đưa ra các báo cáo chi tiết về các hoạt động xâm nhập trái phép trên. Hệ thống IPS được xem là trường hợp mở rộng của hệ thống IDS, cách thức hoạt động cũng như đặc điểm của 2 hệ thống này tương tự nhau. Điểm khác nhau duy nhất là hệ thống IPS ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với hệ thống. Hệ thống IPS sử dụng tập luật tương tự như hệ thống IDS.

### SIEM

SIEM (Security Information and Event Management) được thiết kế để thu thập các sự kiện an ninh từ các thiết bị đầu cuối và lưu trữ dữ liệu một cách tập trung, cho phép phân tích tập trung và báo cáo sự kiện an toàn của một hệ thống mạng, có thể phát hiện các cuộc tấn công mà không thể phát hiện được theo các phương pháp thông thường.

Kiến trúc của SIEM:

* Phần mềm được cài đặt trên máy chủ cục bộ.
* Phần cứng hoặc máy ảo dành riêng cho SIEM.
* Dịch vụ đám mây SIEM. Lợi ích của SIEM:

Quản lý tập trung: Tập hợp dữ liệu thông qua giải pháp nhật ký (Log) tập trung. Mỗi hệ thống đầu cuối cần có hệ thống ghi lại sự kiện an ninh và thường xuyên truyền Log về máy chủ SIEM. Máy chủ SIEM nhận dữ liệu nhật ký từ rất nhiều thiết bị khác nhau và sau đó thực hiện thống kê, phân tích, báo cáo. Tạo ra báo cáo duy nhất cho thấy sự tương quan giữa các sự kiện an ninh của các thiết bị.

Giám sát an toàn mạng: Nhiều thiết bị có khả năng ghi Log sự kiện an ninh nhưng thiếu khả năng phân tích để xác định các hành vi độc hại. SIEM có khả năng cho thấy sự tương quan sự kiện giữa các thiết bị, sau đó cấu trúc lại chuỗi sự kiện và xác định cuộc tấn công

Cải thiện hoạt động xử lý sự cố hiệu quả: Cung cấp giao diện quản lý đơn giản để xem xét tất cả các dữ liệu nhật ký an ninh từ nhiều thiết bị, xác định nhanh chóng tất cả các thiết bị đầu cuối bị ảnh hưởng bởi cuộc tấn công, cung cấp cơ chế cách ly các thiết bị đầu cuối đã bị tấn công.

### Một số giải pháp nâng cao hiệu quả bảo mật

* Nâng cao nhận thức về an toàn thông tin cho toàn thể tổ chức, doanh nghiệp, bao gồm các hoạt động thay đổi quan điểm của cấp lãnh đạo; tập huấn, đào tạo nâng cao nhận thức an toàn bảo mật thông tin cho toàn bộ nhân viên và cấp quản trị trong doanh nghiệp, trong tổ chức; thử nghiệm, diễn tập các kiểu tấn công giả mạo vào doanh nghiệp.
* Ưu tiên ngân sách cho các hoạt động về an toàn thông tin, bao gồm các hoạt động đầu tư trang thiết bị, công cụ, dụng cụ, giải pháp; chi phí cho các hoạt động thường xuyên về an toàn thông tin, lương cho chuyên gia và đội ngũ làm an toàn thông tin, các hoạt động đào tạo - vận hành; các hoạt động đánh giá, diễn tập về an toàn thông tin.
* Nhân sự về an toàn thông tin: xây dựng đội ngũ chuyên về an toàn thông tin; tạo điều kiện cho những người làm an toàn thông tin tham gia các khóa đào tạo chuyên môn và chuyên sâu, các hội thảo diễn đàn chuyên môn.
* Xây dựng các quy trình, quy định hoặc chuẩn quốc tế về an toàn thông tin. Xây dựng hệ thống ISMS (Information Security Management System) - hệ thống quản lý bảo mật thông tin mô tả các kiểm soát mà một tổ chức cần thực hiện để đảm bảo rằng nó bảo vệ một cách hợp lý tính bảo mật, tính sẵn có và tính toàn vẹn của tài sản khỏi các mối đe dọa và lỗ hổng.

## Hệ thống giám sát mạng

### Giới thiệu

Trong những hệ thống mạng lớn, người quản trị mạng cần có công cụ để có thể theo dõi hoạt động của hệ thống. Việc theo dõi hoạt động của hệ thống bao gồm theo dõi tình trạng hoạt động của các thiết bị và

dịch vụ nhằm hạn chế các rủi ro gây ra. Từ đó giúp người quản trị kịp thời khắc phục, đảm bảo hệ thống hoạt động ổn định.

Bên cạnh việc theo dõi các gói tin để phát hiện những dấu hiệu tấn công mạng đã tìm hiểu ở các phần trên thì việc giám sát những hoạt động khác của hệ thống mạng như giám sát các luồng lưu lượng mạng, hoạt động của CPU, bộ nhớ, trạng thái hoạt động các máy chủ, theo dõi trạng thái hoạt động của các dịch vụ mạng trên nó và trạng thái của các thiết bị mạng (Router, Switch,…) là một trong những yêu cầu đặt ra để giám sát hệ thống một cách hiệu quả hơn. Điều này giúp cho người quản trị mạng có thể nắm bắt được tình trạng hoạt động của toàn bộ hệ thống mạng một cách nhanh chóng và tiện lợi.

Một hệ thống IDS/IPS có thể phát hiện và phòng chống các cuộc tấn công xâm nhập mạng dựa vào các dấu hiệu tấn công được lưu trữ và cập nhập thường xuyên. Tuy nhiên cũng không tránh khỏi những trường hợp có những dạng tấn công mới mà những dấu hiệu chưa được biết tới, tập luật của hệ thống phát hiện chưa được cập nhật.

Với sự kết hợp hệ thống giám sát trực quan, những hoạt động của những thiết bị trong hệ thống được theo dõi và hiển thị thời gian thực các hoạt động của hệ thống một cách trực quan thông qua những đồ thị về lưu lượng mạng, trạng thái hoạt động của CPU, RAM, dịch vụ mạng,… cho phép người quản trị có những phân tích để đưa ra các giải pháp phù hợp tránh những nguy hại cho hệ thống mạng.

Ngoài ra, người quản trị có thể thiết lập những ngưỡng cảnh báo kết hợp với hệ thống báo động để người quản trị nhanh chóng có được những thông tin về những cuộc tấn công hay phát hiện những bất thường trong hệ thống. Những bất thường ở đây như là một dịch vụ mạng ngừng hoạt động, máy chủ ngừng hoạt động, hay CPU hoạt động quá tải (đặt ngưỡng cảnh báo),…

### Các giao thức của hệ thống giám sát

Để có thông tin cho việc giám sát trạng thái hoạt động của các thiết bị và dịch vụ mạng, trong hệ thống giám sát sử dụng giao thức SNMP (Simple Network Management Protocol).

SNMP là một giao thức chính được sử dụng cho mục đích theo dõi tình trạng hoạt động của các thiết bị và dịch vụ trong hệ thống mạng. SNMP làm nhiệm vụ thu thập thông tin từ các thiết bị mạng (Router, Switch, Server,…) cần giám sát và gửi về cho chương trình giám sát để phân tích và sử dụng để hiển thị ra giao diện quản trị các thông tin cần thiết theo mục đích của chương trình giám sát.

Trong SNMP có 3 vấn đề cần quan tâm: Manager, Agent và MIB.

* **MIB**: Là cơ sở dữ liệu dùng phục vụ cho Manager và Agent.
* **Manager**: Nằm trên máy chủ giám sát hệ thống mạng.
* **Agent**: Là một chương trình nằm trên các thiết bị cần giám sát, quản lý. Agent có thể là một chương trình riêng biệt (ví dụ như Daemon trên Unix) hay được tích hợp vào hệ điều hành. Ví dụ như trong IOS của các thiết bị Cisco. Nhiệm vụ của các Agent là thông báo các thông tin đến cho thành phần điều khiển được cấu hình nằm trên máy chủ giám sát.

SNMP sử dụng UDP làm giao thức truyền tải thông tin giữa các Manager và Agent. Việc sử dụng UDP, thay vì TCP, bởi vì UDP là phương thức truyền mà trong đó hai đầu thông tin không cần thiết lập kết nối trước khi dữ liệu được trao đổi, thuộc tính này phù hợp trong điều kiện mạng gặp trục trặc, hư hỏng,...

Manager

SNMP trap

Agent, MIB



Switch

SNMP Get

NMS Server



Managed device



SNMP Set

***Hình 7.6:*** *Các gói tin cơ bản trong SNMP*

### Các hoạt động giám sát

- Giám sát lưu lượng:

Giám sát lưu lượng được áp dụng ở các thiết bị mạng dùng là vai trò quan trọng trong việc chuyển tải các lưu lượng trên đường truyền như ở các Router, Core Switch,…

* Giám sát tình trạng hoạt động:

Giám sát tình trạng hoạt động của các thiết bị là theo dõi trạng thái còn hoạt động hay đã ngưng hoạt động. Trong những hệ thống có triển khai các thiết bị dự phòng thì khó nhận ra một thiết bị đang trong tình trạng ngưng hoạt động vì trong khi đó hệ luồng lưu lượng sẽ đi qua thiết bị dự phòng.

* Giám sát dịch vụ:

Giám sát dịch vụ thường được triển khai áp dụng ở các máy chủ để theo dõi tình trạng hoạt động của các dịch vụ cần giám sát. Có thể xảy ra trường hợp máy chủ vẫn đang hoạt động như dịch vụ bị tắt đi.

* Giám sát tài nguyên của thiết bị:

Giám sát các tài nguyên như hoạt động của CPU, RAM, dung lượng đĩa cứng,… giúp theo dõi tình trạng hoạt động, khả năng đáp ứng, từ đó tiến hành các biện pháp nâng cấp, thay thế.

## SDN, KDN và xu hướng quản trị

### Một số khái niệm

Trước hết hãy xem xét lại các thiết bị mạng hoạt động chuyển tiếp dữ liệu như thế nào. Các kết nối vật lý kết nối các thiết bị với nhau bằng cáp mạng hoặc dùng mạng không dây. Switch chuyển tiếp dữ liệu là các Ethernet Frame, Router chuyển tiếp các gói tin. Chúng sử dụng các giao thức khác nhau để học các thông tin hữu dụng, như các giao thức định tuyến học các đường đi ở tầng Mạng.

Mọi thứ mà các thiết bị mạng có thể làm được phân loại trong các mặt phẳng cụ thể. Trong phần này trình bày 3 loại mặt phẳng thường dùng nhất là: Data Plane, Control Plane và Management Plane.

- Data Plane:

Mặt phẳng dữ liệu (Data Plane) liên quan đến các tác vụ chuyển tiếp dữ liệu của các thiết bị mạng, liên quan đến các vấn đề nhận dữ liệu, xử lý và chuyển tiếp nó. Một số hành động được thực hiện trên các thiết bị mạng trong Data Plane:

+ Mở gói và đóng gói (Router, Switch Layer 3).

+ Gắn thêm và bỏ Header trong 802.1Q (Router, Switch).

+ So khớp địa chỉ MAC đích với bảng địa chỉ MAC (Layer 2 Switch).

+ So khớp địa chỉ IP đích với thông tin trong bảng định tuyến (Router, Layer 3 Switch).

+ Mã hóa dữ liệu và thêm IP Header mới (trong VPN).

+ Chuyển đổi địa chỉ IP (trong NAT).

+ Lọc gói tin (trong ACL, Port Security).

- Control Plane:

Router cần biết các đường đi trong bảng định tuyến trước khi Data Plane có thể chuyển tiếp các gói tin. Layer 2 Switch cần thiết lập bảng địa chỉ MAC trước khi nó có thể chuyển tiếp các Ethernet Frame ra cổng nào để đến đích. Switch phải sử dụng STP khóa một số cổng để đảm bảo Data Plane hoạt động tốt và chống Switching Loop.

Khái niệm mặt phẳng điều khiển (Control Plane) liên quan tới các hành động điều khiển của Data Plane. Hầu hết các hành động này phải thực hiện với việc tạo ra các bảng cho Data Plane sử dụng, các bảng này như là bảng định tuyến, bảng ARP, bảng địa chỉ MAC trên Switch,… Bằng các tác vụ thêm, xóa, sửa các dòng trong các bảng này, Control Plane xử lý việc điều khiển những gì mà Data Plane thực hiện. Một số giao thức trong Control Plane như các giao thức định tuyến, các giao thức và thiết bị mạng truyền thống tích hợp Data Plane và Control Plane vào mỗi thiết bị.

**R1 R2 R3**

Packet

Data

Plane

Packet

Data

Plane

Packet

Data

Plane

Packet

Control Plane

Control Plane

Control Plane

***Hình 7.7:*** *Mặt phẳng điều khiển và mặt phẳng dữ liệu*

- Một số giao thức Control Plane phổ biến như:

+ Các giao thức định tuyến.

+ IPv4 ARP.

+ IPv6 NDP.

+ Học địa chỉ MAC trên Switch.

+ STP.

Nếu không có các giao thức và các hoạt động của Control Plane, Data Plane trên các thiết bị mạng truyền thống không thể hoạt động được. Router có thể không được dùng nếu các đường đi không thể học được từ các giao thức định tuyến. Nếu không có các dòng địa chỉ MAC học được trong bảng MAC, Switch chỉ có thể chuyển tiếp các gói tin Unicast bằng cách gửi chúng ra tất cả các cổng của nó. Do đó, Data Plane dựa vào Control Plane để đưa ra các thông tin hữu dụng.

- Management Plane:

Mặt phẳng quản trị (Management Plane) bao gồm các giao thức cho phép người quản trị điều khiển các thiết bị. Telnet và SSH là 2 giao thức phổ biến của Management Plane.

### Controller

Từ những năm 2010, một số hướng tiếp cận mới được hình thành. Trong đó có phương pháp chuyển Control Plane làm việc trong phần mềm chạy như một ứng dụng tập trung gọi là Controller. Hầu hết Control Plane truyền thống sử dụng kiến trúc phân tán, chạy trên nhiều thiết bị. Ví dụ như mỗi Router chạy một tiến trình OSPF riêng. Để phối hợp hoạt động, Control Plane sử dụng các thông điệp để giao tiếp với nhau. SDN sử dụng kiến trúc tập trung với Control Plane tập trung, gọi là SDN Controller, để tập trung điều khiển các thiết bị mạng.

Controller

Control

Plane

Control

Plane

Control

Plane

Packet

Data

Plane

Packet

Data

Plane

Packet

Data

Plane

Packet

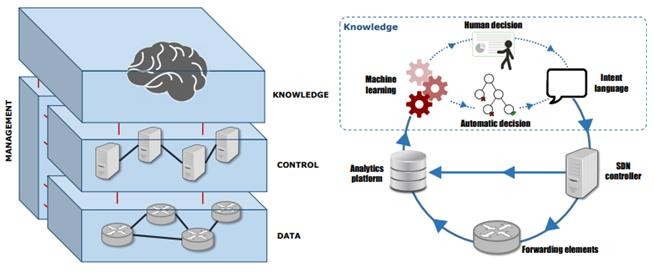
Network device Network device Network device

***Hình 7.8:*** *Quản lý tập trung với Controller*

### SDN

SDN (Software Defined Network) là một cách thức để xây dựng mạng. Các thiết bị mạng vẫn được triển khai và chuyển tiếp dữ liệu nhưng các chức năng của Control Plane và vị trí của nó có sự thay đổi. Các Control Plane chuyển từ mô hình phân tán sang mô hình tập trung.

### KDN

KDN (Knowledge Defined Network) dựa vào các kỹ thuật Mechine Learning và các kỹ thuật nhận thức để vận hành hệ thống mạng. Trong đó, Knowledge Plane được sử dụng mang lại nhiều điểm nổi bật như sự tự động hóa (Recognize Act) và sự đề xuất dựa trên các quy luật nhận diện (Recognize Explain Suggest) hỗ trợ cho sự vận hành, tối ưu và khắc phục sự cố đạt hiệu quả.

***Hình 7.9:*** *Mặt phẳng và quy trình hoạt động của KDN*

## Tổng kết chương

Mỗi ngày thế giới phải đối mặt với hàng nghìn cuộc tấn công an ninh mạng. Thiệt hại từ mất an toàn thông tin lên tới hàng nghìn tỷ USD do các vụ đánh cắp dữ liệu hoặc các vụ tấn công nhằm vào các hệ thống thông tin trọng yếu. Trong thế giới kết nối, an ninh mạng có thể coi là một trong những trụ cột của nền kinh tế số. Hiểu biết được các vấn đề về an ninh mạng, chúng ta sẽ nâng cao ý thức trong việc bảo vệ thông tin cá nhân và tổ chức, đồng thời cũng nắm được các kỹ thuật để bảo vệ hệ thống mạng máy tính khỏi các tấn công như: Firewall, IDS/IPS, SIEM,...

## Câu hỏi và bài tập

1. Phát biểu nào sau đây không đúng về vùng DMZ?
   1. Thường chứa E-mail Server, hoặc Web Server.
   2. Có thể bao gồm Front End Firewall và Backend Firewall.
   3. Chứa các Server chỉ phục vụ cho người dùng bên trong.
   4. Để nâng cao sự bảo mật cho hệ thống.
2. Điều nào sau đây không đúng khi nói về lỗ hổng 0-day?
   1. Là lỗ hổng nhà sản xuất chưa kịp vá.
   2. Là lỗ hổng phá hoại hệ thống trong vòng một ngày.
   3. Là lỗ hổng hacker chưa công bố rộng rãi.
   4. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ.
3. Việc gỡ bỏ những dịch vụ và giao thức không cần thiết gọi là:
   1. Nonrepudiation.
   2. Hardening.
   3. Auditing.
   4. Hashing.
4. Giao thức nào được dùng để mã hóa dữ liệu trao đổi giữa Web Browser và Web Server?
   1. IPSec.
   2. HTTP.
   3. SSL.
   4. VPN.
5. Tấn công một máy tính bằng cách gửi các gói TCP Handshake không đúng thứ tự đến đích (Wrong Order) xảy ra ở tầng nào?
   1. Network Interface Layer.
   2. Internet Layer.
   3. Transport Layer.
   4. Application Layer.
6. Kỹ thuật tấn công nào sau đây có thể vượt qua các cơ chế bảo mật vật lý và logic để có thể truy cập vào hệ thống?
   1. Brute Force.
   2. Denial of Service.
   3. Social Engineering.
   4. Port Scanning.
   5. Man-In-The-Middle.
7. Các dịch vụ chạy trên hệ thống thường được hacker xác định dựa vào đâu?
   1. Địa chỉ IP của hệ thống.
   2. Active Directory.
   3. Tên của hệ thống.
   4. Chỉ số Port.
8. Chức năng của giao thức IPSec hoạt động ở tầng nào trong mô hình OSI?
   1. Data Link.
   2. Transport.
   3. Session.
   4. Network.
   5. Application.
9. Cách tốt nhất để nhận ra hành vi bất thường và đáng ngờ trên hệ thống mạng của bạn là gì?
   1. Nhận biết được các cuộc tấn công mới nhất.
   2. Cấu hình IDS để phát hiện và cảnh báo các lưu lượng bất thường.
   3. Nhận biết được các hoạt động bình thường hệ thống.
   4. Nghiên cứu dấu hiệu hoạt động của các loại tấn công quan trọng trên hệ thống.
10. Trong IDS, khái niệm False Positive nghĩa là gì?
    1. Không có tấn công nhưng hệ thống vẫn phát cảnh báo.
    2. Có tấn công và hệ thống phát cảnh báo.
    3. Có tấn công nhưng hệ thống không phát cảnh báo.
    4. Không có tấn công và hệ thống không phát cảnh báo.
11. Bạn là người tư vấn giải pháp an toàn thông tin, một khách hàng của bạn quan tâm đến việc chống lại giả mạo và nhiễm độc ARP trong mạng của họ. Giải pháp nào dưới đây KHÔNG áp dụng cho mục đích này?
    1. Sử dụng Port Security trên các Switch.
    2. Sử dụng công cụ giám sát ARP trong mạng (kiểu như ARPwatch).
    3. Sử dụng Firewall giữa các phân vùng trong LAN.
    4. Nếu trong một mạng nhỏ thì sử dụng ARP tĩnh.
12. Phát biểu nào sau đây không đúng về vùng DMZ?
    1. Thường chứa E-mail Server, hoặc Web Server.
    2. Có thể bao gồm Front End Firewall và Backend Firewall.
    3. Chứa các Server chỉ phục vụ cho người dùng bên trong.
    4. Để nâng cao sự bảo mật cho hệ thống.
13. Kiểu tấn công nào sau đây không phải khai thác các lỗ hổng của ứng dụng Web?
    1. Cross Site Scripting.
    2. SQL Injection.
    3. Social Engineering.
    4. Cross Site Request Forgery.
14. Các cổng hoạt động của các dịch vụ Web, DNS, Telnet theo thứ tự là?

A. 80, 53, 23.

B. 80, 20, 23.

C. 53, 23, 80.

D. 20, 23, 80.

1. Mục tiêu của đảm bảo an toàn cho một hệ thống CNTT được biết đến với mô hình có tên gọi là CIA gồm các tính chất?
   1. Tính bí mật, tính xác thực, tính toàn vẹn.
   2. Tính bí mật, tính toàn vẹn, tính sẵn sàng.
   3. Tính toàn vẹn, tính sẵn sàng, tính xác thực.
   4. Tính bí mật, tính toàn vẹn, tính chống chối bỏ.
2. Giải pháp nào sau đây được xem là tốt nhất để chống lại tấn công dựa vào việc bắt gói tin trên mạng (Sniffing)?
   1. Sử dụng Switch thay cho Hub.
   2. Sử dụng mạng có dây, không nên sử dụng mạng không dây.
   3. Sử dụng Gateway.
   4. Sử dụng các kỹ thuật mật mã để mã hóa dữ liệu khi truyền.
3. Mục tiêu chính của các kỹ thuật điều khiển truy cập trong hệ thống CNTT là?
   1. Để cấp toàn bộ quyền truy cập cho người dùng đã được chứng thực.
   2. Để giới hạn các quyền và hoạt động của người dùng đã được chứng thực.
   3. Để ngăn chặn các người dùng trái phép vào các tài nguyên hệ thống.
   4. Để bảo vệ máy tính khỏi nhiễm virus.
4. Giao thức nào sau đây được sử dụng để truyền thông tin giám sát giữa Manager và Agent trong hệ thống giám sát mạng?
   1. UDP.
   2. SNMP.
   3. TCP.
   4. IP.
5. Switch Layer 2 xem xét địa chỉ MAC đích trong Frame và lựa chọn để chuyển tiếp Frame này chỉ ra cổng Gi0/1. Hành động này diễn ra là một phần của mặt phẳng nào của Switch?
   1. Mặt phẳng dữ liệu.
   2. Mặt phẳng quản lý.
   3. Mặt phẳng điều khiển.
   4. Mặt phẳng bảng.
6. Một Router sử dụng OSPF để học các mạng và thêm chúng vào bảng định tuyến. Hành động này xảy ra ở mặt phẳng nào của Router?
   1. Mặt phẳng dữ liệu.
   2. Mặt phẳng quản lý.
   3. Mặt phẳng điều khiển.
   4. Mặt phẳng bảng.

# TÀI LIỆU THAM KHẢO

1. Wendell Odom, *CCNA 200-301 Official Cert Guide*, Volume 1, Cisco Press, 2020.
2. Wendell Odom, *CCNA 200-301 Official Cert Guide*, Volume 2, Cisco Press, 2020.
3. Jordan Krause, *Mastering Windows Server 2019*, 2nd Edition, PACK, 2019.
4. Christine Bresnahan & Richard Blum, *LPIC-1 Linux Professional Institute Certification Study Guide*, Sybex, 2019.
5. Christine Bresnahan & Richard Blum, *LPIC2 - Linux Professional Institute Certification Study Guide - Second Edition*, Sybex, 2016.
6. Mestres A., Rodriguez-Natal A., Carner J., Barlet-Ros P., Alarcón E., Solé M.,... & Estrada G. (2017), *Knowledge-defined networking*, ACM SIGCOMM Computer Communication Review, 47(3), 2-10.

# Giáo trình mạng máy tính căn bản

(Giáo trình dành cho sinh viên ngành Công nghệ thông tin)

## Huỳnh Nguyên Chính (chủ biên), Nguyễn Thị Thanh Vân Trường Đại học Sư phạm Kỹ thuật Thành phố Hồ Chí Minh

### NHÀ XUẤT BẢN ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

**Trụ sở:**

Phòng 501, Nhà Điều hành ĐHQG-HCM, phường Linh Trung, thành phố Thủ Đức, Thành phố Hồ Chí Minh.

ĐT: 028 62726361

E-mail: [vnuhp@vnuhcm.edu.vn](mailto:vnuhp@vnuhcm.edu.vn)

**Văn phòng đại diện:**

Tòa nhà K-Trường Đại học Khoa học Xã hội & Nhân văn, số 10-12 Đinh Tiên Hoàng, phường Bến Nghé, Quận 1,Thành phố Hồ Chí Minh

ĐT: 028 62726390

Website: [www.vnuhcmpress.edu.vn](http://www.vnuhcmpress.edu.vn/)

### Chịu trách nhiệm xuất bản và nội dung

TS ĐỖ VĂN BIÊN

### Biên tập

NGUYỄN THỊ NGỌC ANH

### Sửa bản in

PHƯỚC HUỆ

### Trình bày bìa

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT THÀNH PHỒ HỒ CHÍ MINH

### Đối tác liên kết

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT THÀNH PHỒ HỒ CHÍ MINH

Xuất bản lần thứ 1. Số lượng in: 250 cuốn, khổ 16 x 24cm. Số XNĐKXB: 1946-2022/CXBIPH/4-25/ĐHQGTPHCM. QĐXB số: 198/QĐ-

NXB cấp ngày 12/7/2022. In tại: Công ty TNHH In và Bao bì Hưng Phú; Địa chỉ: 162A/1, KP1A, phường An Phú, TP Thuận An, Bình Dương. Nộp lưu chiểu: Năm 2022. ISBN: **978-604-73-9135-6.**

Bản quyền tác phẩm đã được bảo hộ bởi Luật Xuất bản và Luật Sở hữu

trí tuệ Việt Nam. Nghiêm cấm mọi hình thức xuất bản, sao chụp, phát tán nội dung khi chưa có sự đồng ý của tác giả và Nhà xuất bản.

### ĐỂ CÓ SÁCH HAY, CẦN CHUNG TAY BẢO VỆ TÁC QUYỀN!





**ISBN: 978-604-73-9135-6**

786047 391356

**NXB ĐHQG-HCM**

9