

# Tài liệu học mạng máy tính căn bản

Tài liệu học mạng máy tính căn bản

Hệ thống: Ho Chi Minh City University of Technology and Education

Khoá học: Mạng máy tính căn bản\_ Nhóm 03

Book: Tài liệu học mạng máy tính căn bản

Được in bởi: Nguyễn Huỳnh Minh Tiến

Ngày: Wednesday, 8 January 2020, 7:47 AM

# Table of contents

1. Tổng quan
2. Mô hình mạng
3. Các khái niệm trong LAN
4. IP Addressing
5. Subnetting
6. ICMP
7. Local User and Group
8. Thuộc tính user and group
9. NTFS Permission
10. File Server và Share Permission
11. Domain Network
12. Home Folder và User Profile
13. Deployment Software
14. Local Group Policy
15. Group Policy Object
16. Group Policy Object – Phần 2
17. Group Policy Object – Phần 3
18. Security Templates
19. Audit Policy – Giám sát hệ thống
20. File Server Resource Manager
21. Monitor Server Performance
22. Remote Desktop Service
23. Windows Routing – Phần 1
24. Windows Routing – Phần 2
25. Distributed File System (DFS)
26. Print Server
27. Hyper-V
28. Disk Management (phần 1)
29. Disk Management (phần 2)
30. Windows Server Backup (Phần 1)
31. Windows Server Backup (Phần 2)
32. Windows Server Backup: Restore Data, System State

# 1. Tổng quan

**Mạng máy tính** là gì ? . Nói một cách đơn giản nó bao gồm các thiết bị mạng, các PC hay laptop kết nối lại với nhau.

**Giao tiếp Host- Host** (Communication Host-Host)



Giao tiếp Host Host

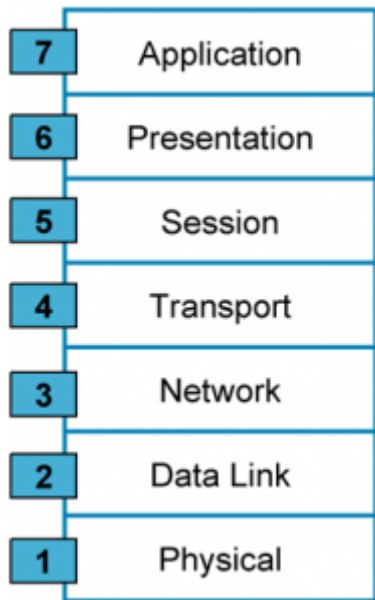
Để truyền thông từ host đến host thì chúng ta phải xây dựng các mô hình truyền dữ liệu.

Mô hình cũ cách đây vài chục năm (older model)

- Dựa trên sự độc quyền (máy IBM chỉ giao tiếp được với IBM không giao tiếp được với các hãng khác)
- Các ứng dụng và phần mềm chỉ được cung cấp bởi chính nhà sản xuất ( các máy tính HP thì chỉ chạy được phần mềm của HP)

**Nhược điểm:** Không có tính tương thích lẫn nhau giữa các dòng sản phẩm (độc quyền).

Do độc quyền thì rất khó phát triển nên năm 1984, Tổ chức tiêu chuẩn thế giới ISO đã phát minh ra bộ tiêu chuẩn dành cho ngành công nghiệp mạng gọi là **OSI (Open System Interconnection)**. Mô hình này chia mạng máy tính thành 7 lớp (layer) tương ứng với 7 nhóm công việc.



Mô hình OSI

**Lợi ích của việc phân lớp:**

- Giảm thiểu được độ phức tạp, nâng cao việc chuyên môn hóa khi sản xuất (các công ty mạnh về nhóm công việc nào thì sẽ sản xuất các thiết bị hoặc phần mềm cho nhóm công việc đó).
- Có sự chuẩn hóa giữa các dòng sản phẩm ( các lớp trong mô hình sẽ quy định các chuẩn kĩ thuật để các nhà sản xuất tuân theo).
- Đảm bảo tính tương tính về mặt công nghệ ( thiết bị của các hãng có thể giao tiếp với nhau).
- Thúc đẩy sự phát triển của ngành công nghệ mạng (do tính độc quyền đã bị phá bỏ).

**Chức năng của 7 lớp (layer) trong mô hình OSI:**

**Physical (lớp vật lý):** truyền dòng bit nhị phân qua đường truyền vật lý. Nó định nghĩa các đặc tính kĩ thuật về điện, cơ, quang.

Ví dụ: giữa PC với Switch phải nối bằng cáp thẳng thì đó là do lớp vật lý quy định, hay khoảng cách của cáp mạng là 100m cũng do lớp vật lý quy định.

Thiết bị tiêu biểu: NIC, cáp (đồng trục, UTP, cáp quang...), Hub, connector (RJ45...), repeater.

### Data Link

- điều khiển dữ liệu truy nhập vào đường truyền vật lý.
- giao tiếp với lớp trên nó là lớp Network.
- Cung cấp cơ chế dò lỗi dữ liệu

Thiết bị tiêu biểu: Switch

### Network

- Định tuyến các gói dữ liệu.
- Chọn ra đường đi tối ưu nhất để phân phối dữ liệu ( định nghĩa ra các giao thức định tuyến).
- Cung cấp địa chỉ logic để định danh các điểm truyền gói tin ( địa chỉ IP).

Thiết bị tiêu biểu: Router, Switch layer 3 ....

Ta đã có đường truyền vật lý, cách truy xuất đường truyền vật lý và cách chọn ra đường đi tối ưu nhất. Lúc này PC chỉ quan tâm đến việc quản lý kết nối giữa 2 đầu.

### Transport:

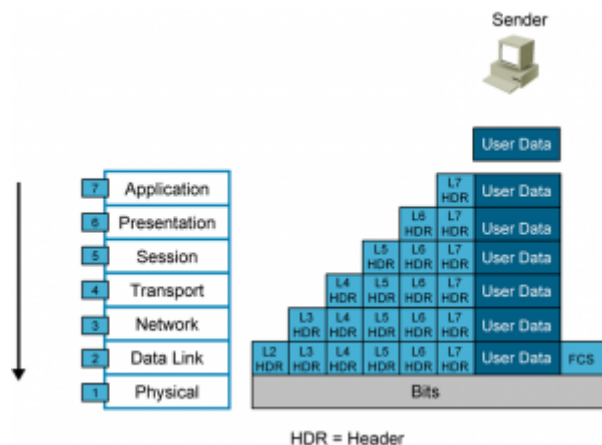
- quản lý các kết nối đầu cuối:
- đảm bảo dữ liệu truyền một cách tin cậy giữa các host.
- cung cấp cơ chế dò lỗi, phục hồi dữ liệu.

**Session:** thiết lập, quản lý và giải phóng các session (phiên làm việc) giữa các ứng dụng

**Presentation:** đảm bảo dữ liệu của nơi nhận và nơi gửi có thể hiểu được nhau và tầng này còn đảm nhận việc mã hóa và nén dữ liệu

**Application:** giao tiếp trực tiếp với người dùng , cung cấp các ứng dụng mạng, dịch vụ mạng (HTTP, FTP vv), cung cấp cơ chế xác thực người dùng.

### Đóng gói dữ liệu trong mô hình OSI khi giao tiếp Host-Host (Data Encapsulation)



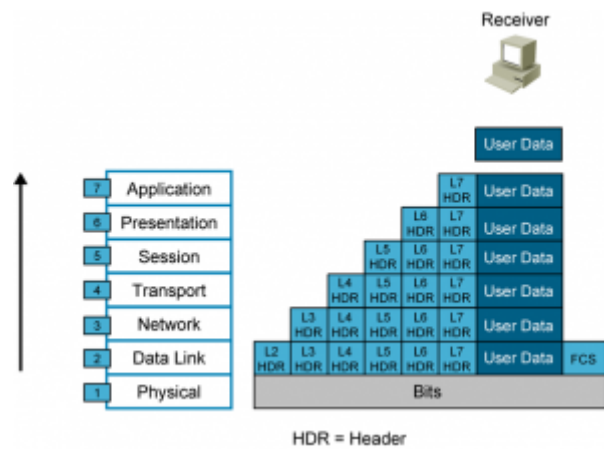
Đóng gói dữ liệu

Hình trên là tiến trình đóng gói dữ liệu tại đầu gửi

Chúng ta có cảm giác là 7 lớp ở bên nhận sẽ giao tiếp ngang hàng với 7 lớp ở bên gửi, nhưng không phải như thế.

Khi 1 host gửi mẫu dữ liệu (User Data) thì User Data sẽ đi từ lớp 7 xuống lớp 1. Khi qua mỗi lớp thì User Data sẽ được đóng các Header. Header là phần thông tin quản lý của 1 gói tin, giống như khi ta gửi 1 kiện hàng thì sẽ có 2 phần là "kiện hàng" và "thông tin của kiện hàng".

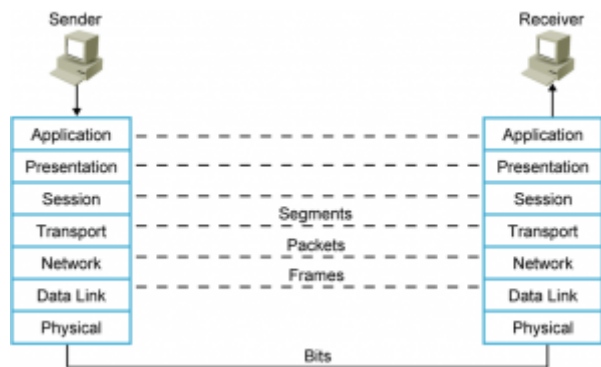
Khi User Data xuống lớp 6 thì toàn bộ nội dung của gói tin lớp 7 sẽ trở thành Data User của lớp 6 và lớp 6 sẽ đóng thêm Layer 6 Header. Và cứ thế tương tự, riêng ở Layer 2 thì có đóng thêm phần kiểm tra lỗi FCS. Đến lớp 1 thì tất cả dữ liệu được chuyển thành các Bit nhị phân rồi đi chuyển trên đường truyền.



Gỡ Header

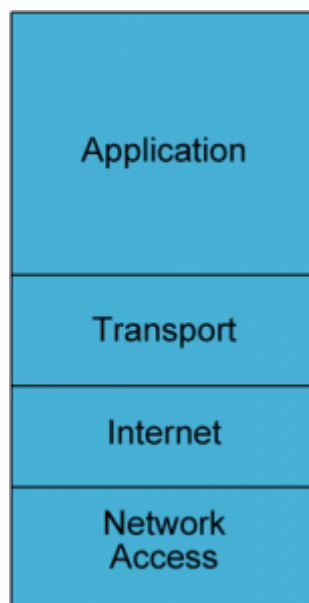
Đến nơi nhận các dòng Bit sẽ được chuyển thành đơn vị dữ liệu của lớp 2. Khi dữ liệu đến lớp 3 thì sẽ được gỡ bỏ layer 2 Header. Và cứ thế mỗi lần đi lên nó sẽ bỏ đi 1 Header khi đến người dùng thì nó trả lại nguyên vẹn User Data.

**Đơn vị dữ liệu của các lớp:** Dữ liệu ở lớp 1 gọi là Bit, lớp 2 là Frame, lớp 3 là Packet và lớp 4 là Segment



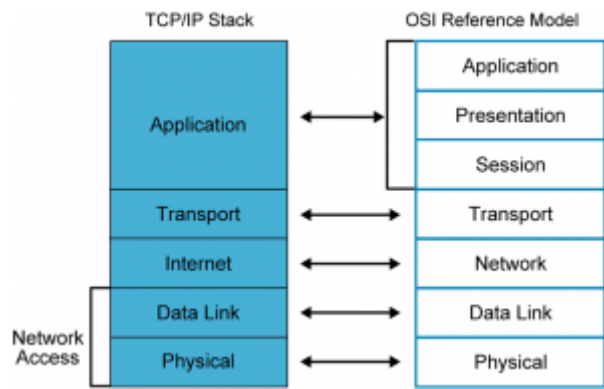
Các đơn vị dữ liệu

### Mô hình TCP/IP (TCP/IP Model)



Mô hình TCP/IP

Gồm 4 lớp, nó gom lớp 5->7 của mô hình OSI thành lớp Application



## TCP/IP vs OSI

**Câu hỏi thường gặp:** Mô hình TCP/IP và mô hình OSI thì mô hình nào được dùng trong thực tế nhiều hơn?

**Trả lời:** Khi xây dựng ra 1 mô hình, nó sẽ gồm có 2 phần:

Mô hình tham chiếu: mô hình gồm bao nhiêu lớp, tên các lớp v.v .

Chồng giao thức: các giao thức sử dụng trong từng lớp.

OSI có mô hình OSI và chồng giao thức OSI. TCP/IP có mô hình TCP/IP và chồng giao thức TCP/IP. Thì ngày nay đa số các hệ thống sử dụng các giao thức của chồng giao thức TCP/IP nhưng lại toàn tham chiếu đến mô hình OSI (ta hay nói thiết bị lớp mấy v.v là toàn tham chiếu đến mô hình OSI).

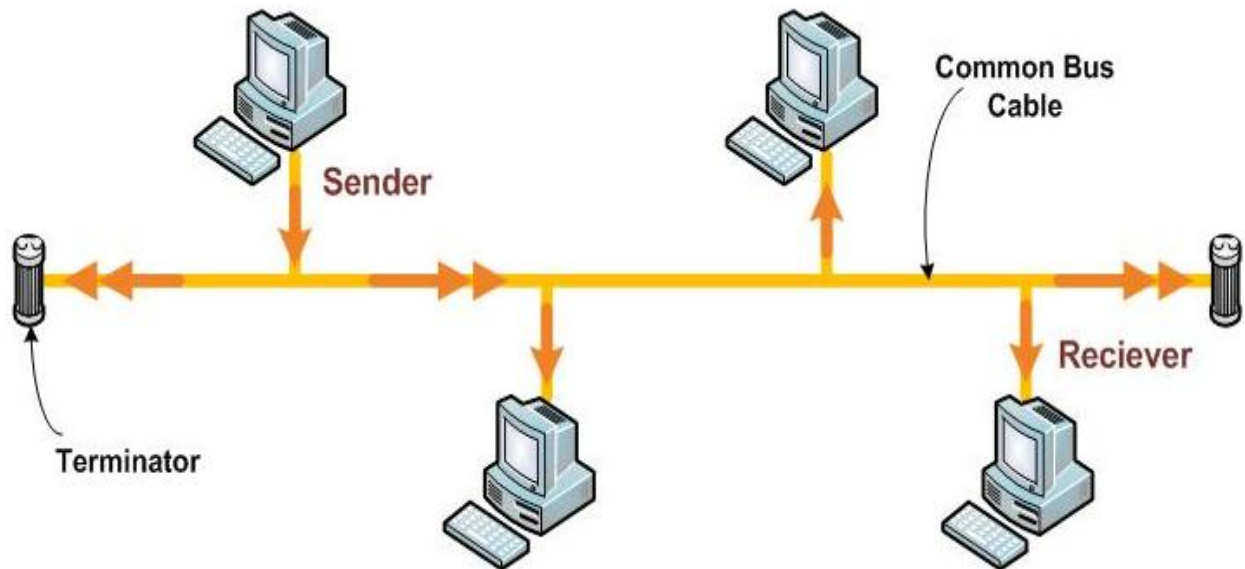
### Ghi chú:

Các thiết bị của JUNIPER sử dụng mô hình TCP/IP 5 lớp, có nghĩa là chia lớp Network Access thành Data link và Physical.

Câu văn dễ nhớ khi học mô hình OSI: **A**nh **P**hai **S**ống **T**ới **N**gày **Đ**ộng **P**hòng

## 2. Mô hình mạng

Mô hình mạng (Network topology) đơn giản là kết nối về mặt hình học của mạng, gồm các loại chính  
Bus (chuẩn IEEE 802.4)  
Star (IEEE 802.11)  
Ring (IEEE 802.5)

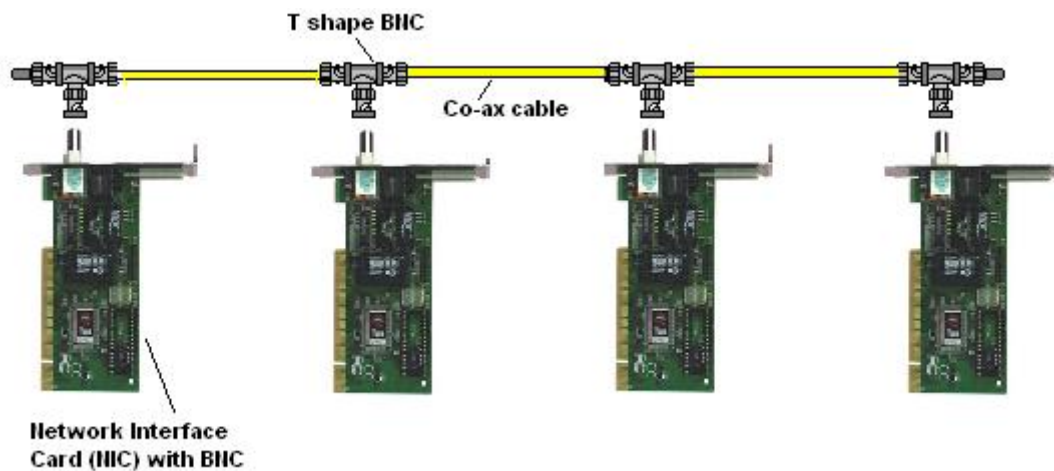


bus topology

### BUS

Trước đây khoảng 20 năm người ta sử dụng mạng Bus rất nhiều. Sử dụng cáp đồng trục (giống loại truyền hình cáp hiện nay) nối trực tiếp các máy tính loại với nhau.

Tại mỗi card mạng người ta sử dụng T-connector (hình dạng giống chữ T), một đầu nối với card mạng, 2 đầu còn lại nối vào 2 cộng dây cáp (nhà bạn nào share truyền hình cáp ra nhiều nhánh sẽ hình dung ngay).



T-connector

Khi một máy cần phát tín hiệu cho một máy khác, nó sẽ phát tín hiệu Broadcast đến tất cả các máy, nhưng chỉ máy nào mang địa chỉ đích mới lấy được tín hiệu, các máy khác thấy không phải tín hiệu gửi cho mình sẽ bỏ qua.

Nếu tín hiệu chạy giữa 2 đầu không ngừng thì nó sẽ dội tới lui trong dây cáp, không cho các máy khác gởi tín hiệu. Do đó tại 2 đầu cuối cùng của mạng sẽ có thêm 2 thiết bị gọi là Terminator (có điện trở khoảng 50 Ohm) để hấp thụ các tín hiệu điện, làm thông cáp.

**Ưu điểm:** dễ lắp đặt, chi phí thấp.

### Nhược điểm:

- Dễ xung đột dữ liệu.
- Kết nối giữa connector với card mạng, connector với dây cáp, connector với connector là các kết nối cơ học sau 1 thời gian sử dụng sẽ độ tiếp xúc không còn tốt (cứ gỡ ra, gắn vào nhiều lần) dẫn tới bị hở mạch. Một

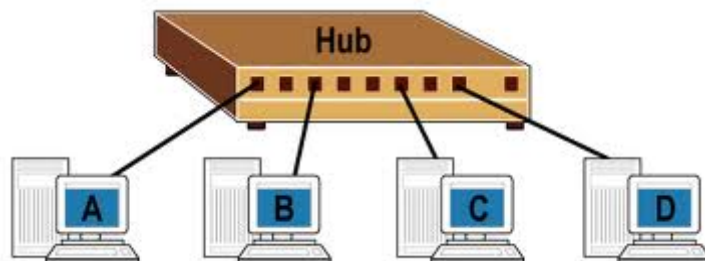
điểm bất kì hở mạch thì toàn bộ phân đoạn mạng đó bị tê liệt.

- Khó nhận biết điểm nào bị hở, phải dò cho nên khó khắc phục sự cố.
- Khó bảo trì

Cách tìm nơi hở mạch: dùng terminator chặn từng phân đoạn rồi thử, nếu dữ liệu truyền tốt thì chặn chỗ khác (cách làm thủ công).

lưu ý: phân đoạn ở đây là đoạn mạng được giới hạn bởi 2 terminator.

### Star



star topology

là mô hình được sử dụng cho tới tận ngày nay

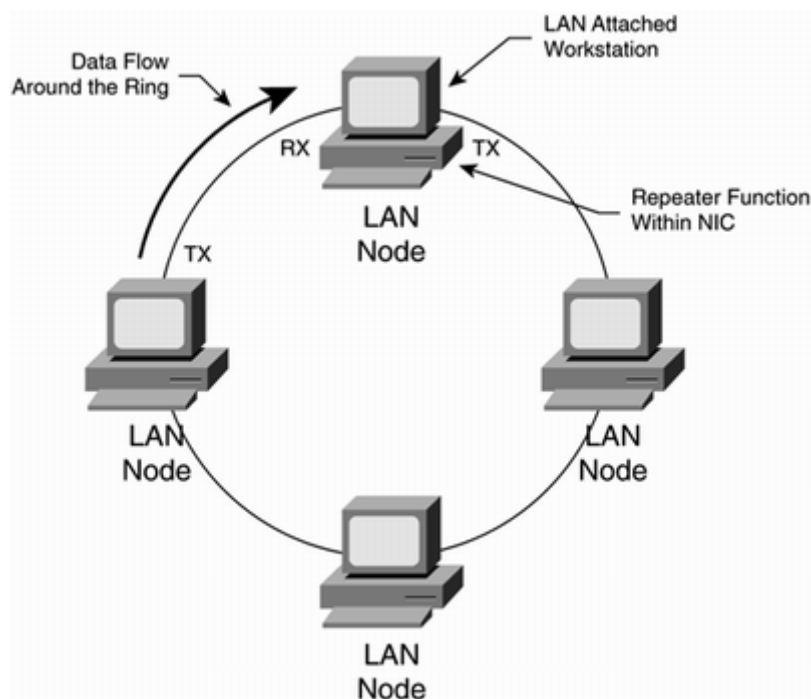
- Các máy tính kết nối với nhau thông qua một thiết bị trung tâm là Hub/Switch. Tín hiệu được truyền từ máy này sang máy khác thông qua Hub/Switch.
- Sử dụng connector là Rj45 để gắn vào card mạng và các port trong Hub/Switch
- Sử dụng cáp xoắn đôi (UTP,STP).

### Ưu điểm:

- Nếu 1 điểm tiếp xúc hở thì chỉ ảnh hưởng chính máy đó, hệ thống hoạt động bình thường.
- Dễ bảo trì, phát hiện lỗi
- Có thể mở rộng hoặc thu hẹp tùy nhu cầu sử dụng

**Khuyết điểm:** nếu Hub/Switch hỏng thì hệ thống bị ngưng trệ.

### Ring



Ring topology

Dữ liệu theo theo dạng vòng khép kín. Để đảm bảo trong một thời điểm chỉ có một Node (máy) được truyền thì nó phải có Token ring (thẻ bài). Khi máy tính đầu tiên trong mô hình Ring bật lên thì nó sẽ phát ra "xung" gọi là Token Ring (thẻ bài) và thẻ này sẽ lưu thông trong mạng theo 1 chiều duy nhất (xem hình). Máy nào muốn truyền dữ liệu thì sẽ nắm thẻ bài này. Khi dữ liệu đã đến nơi nhận thì máy gửi sẽ giải phóng thẻ bài và thẻ bài lại tiếp tục di chuyển.

### Ưu điểm:



Là mô hình truyền dữ liệu tốt nhất do dữ liệu sẽ được khuếch đại bởi các Node giữa đường truyền.  
( A – B – D : A truyền dữ liệu qua D sẽ được B khuếch đại).

### **Nhược điểm**

Không được sử dụng phổ biến do chi phí đắt.

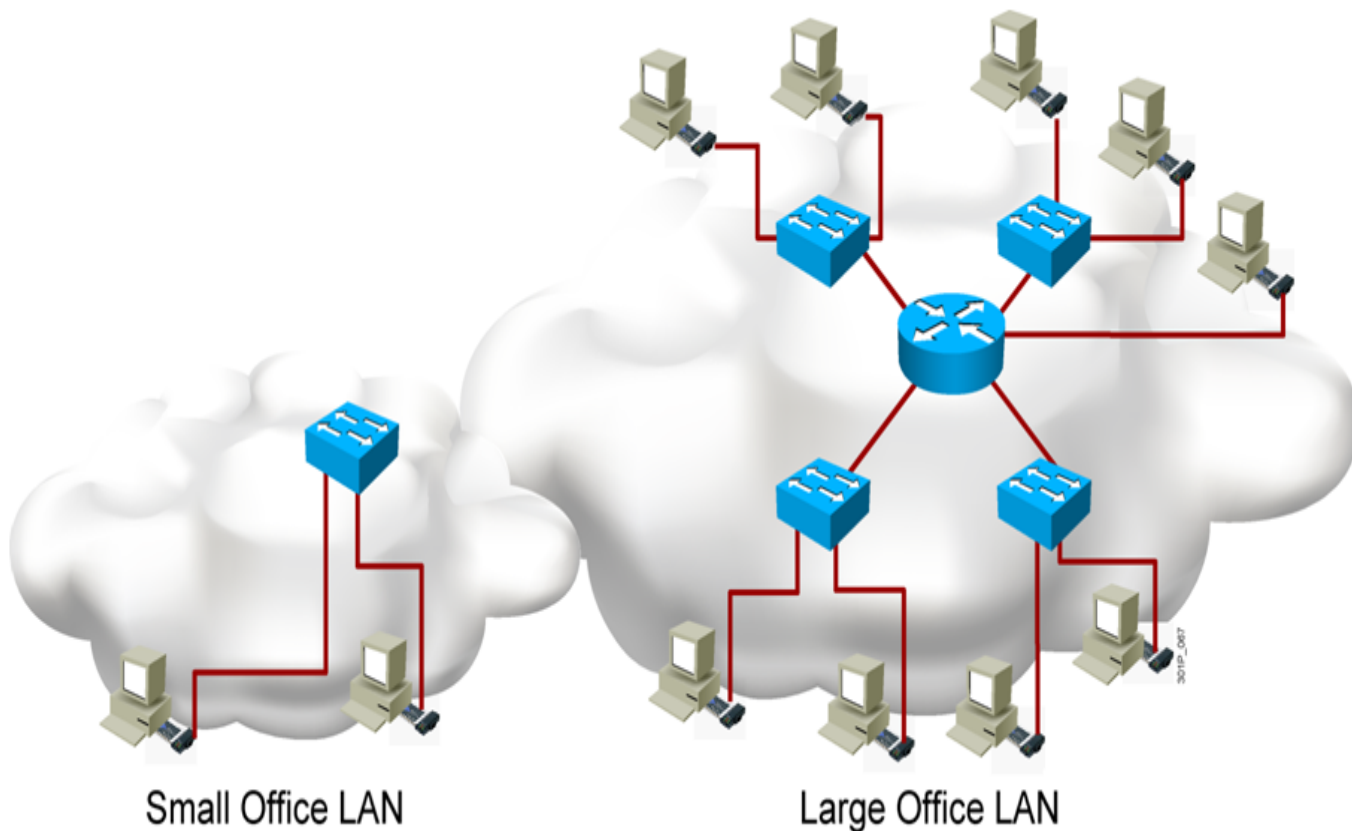
Do dữ liệu di theo vòng một chiều nên một máy chết sẽ kéo theo các máy khác ngừng hoạt động.

**Các bạn tự tìm hiểu thêm về cáp UTP, STP và cách bấm cáp nhé.**

# 3. Các khái niệm trong LAN

## Local Area Network (Lan)

Mạng Lan (mạng nội bộ) có thể là mạng kích thước nhỏ với 1 con switch hay router và cũng có thể mở rộng kích thước như mạng trong công ty, bệnh viện v.v.



Local Area Network

## Các thành phần cơ bản của mạng Lan

- Máy tính: PC, laptop, server.
- Các kết nối: card mạng, các phương tiện truyền dẫn (cáp UTP, quang v.v), connector (RJ45 v.v)
- Thiết bị mạng: Hub, Switch, Router, Wireless Router v.v.
- Giao thức mạng: IP, ARP, Ethernet, DHCP.

## Tính năng của mạng Lan

- Chia sẻ dữ liệu và các ứng dụng.
- Chia sẻ các tài nguyên (máy in, fax v.v)
- Cung cấp kết nối đến các mạng khác (mạng internet hoặc các mạng Lan khác).

## Công nghệ mạng Lan:

Có rất nhiều công nghệ mạng Lan, trong đó công nghệ phổ biến nhất ngày nay là Ethernet (hay còn gọi là chuẩn giao tiếp Lan Ethernet).

Đây là các cột mốc quan trọng của Ethernet.

1970: mạng truyền gói qua radio để xây dựng mạng Lan (gọi là mạng ALOHA).

1973: công ty Xerox phát minh ra Ethernet.

1977: Hoa kì cấp chứng nhận bản quyền 4063220 cho Ethernet.

1982: DIX (gồm 3 công ty Digital, Intel, Xeros) đưa ra chuẩn truyền dữ liệu 10Mb/s (cực kì lớn vào thời điểm đó).

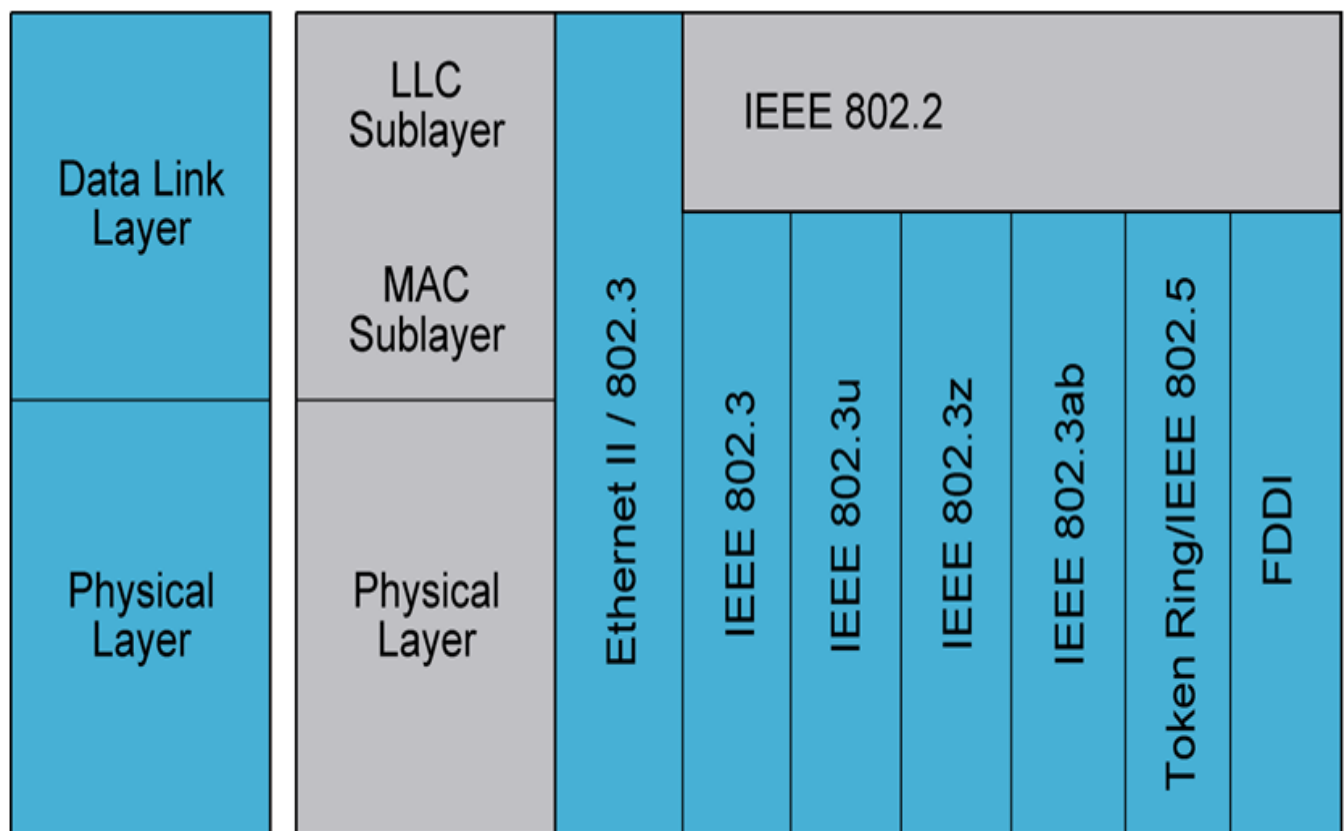
1992: COh Hub đầu tiên ra đời.

2002: IEEE sinh ra chuẩn 802.3ae (10 billion bps)

## Các chuẩn mạng Lan

Chủ yếu tập trung ở lớp Data link và Physical trong mô hình OSI.

lớp Data link chia thành 2 lớp con: LLC ( chuyên lo giao tiếp với các hệ thống lớp 3), MAC điều khiển việc truy nhập vào đường truyền phía dưới.



## OSI Layers

## LAN Specification

Ethernet

Chuẩn Ethernet II/ 802.3 chạy cả 2 lớp .

Các chuẩn 802.3 hay token ring, FDDI thì chỉ chạy đến lớp Mac, để giao tiếp với lớp 3 thì nó cần header riêng (IEEE 802.2 chuyên lo công việc của LLC).

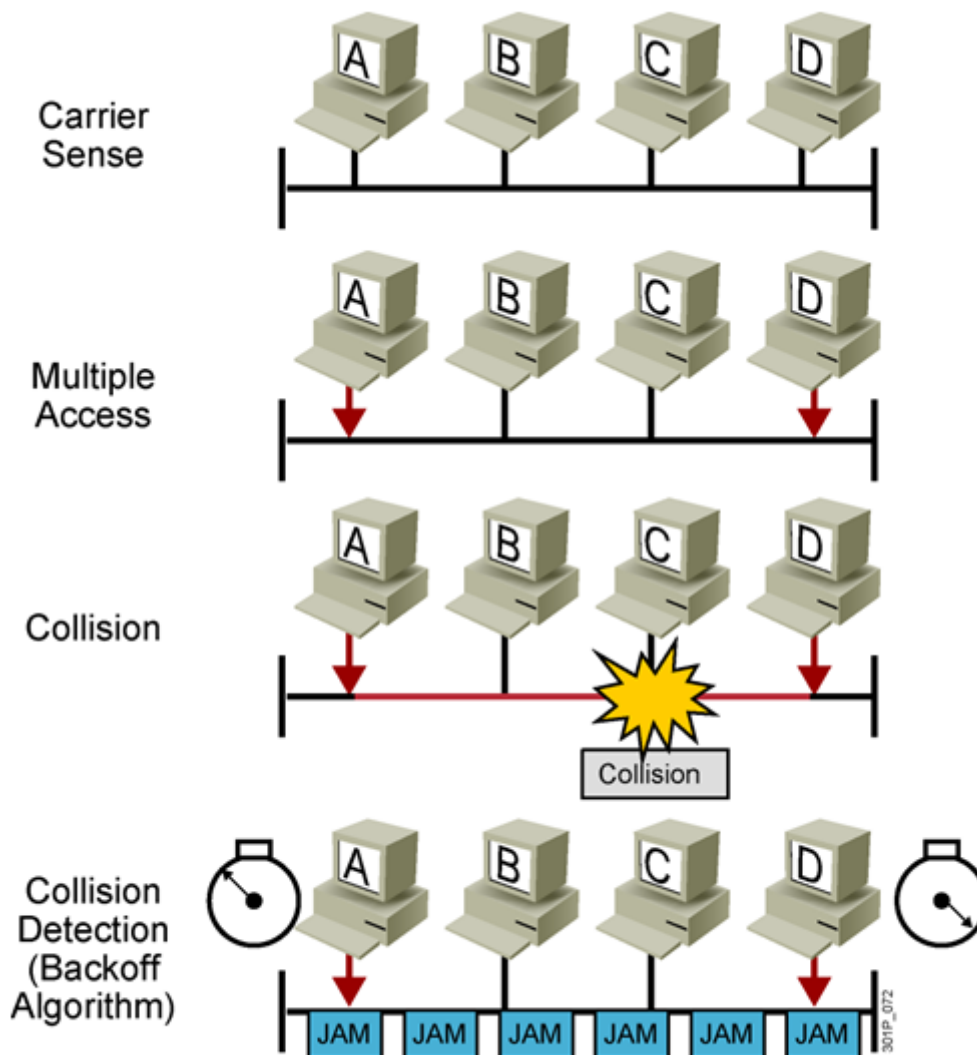
**Cơ chế CSMA/CD** ( Carrier Sense Multiple Access/Collision Detection: cơ chế phát hiện đụng độ)

Đây là cơ chế được dùng phổ biến trong công nghệ Ethernet.

Ví dụ: Mô hình mạng Bus ngày xưa, nếu như có 1 PC gửi dữ liệu dữ liệu thì các PC khác đều nhận được.

A gửi B 1 frame thì gói tin có dạng: Source: Mac A Dest: Mac B.

Khi đó máy nào mà thấy gói tin này không phải gửi cho mình thì sẽ "drop" bỏ nó.



## Carrier Sense Multiple Access Collision Detection (CSMA/CD)

CSMA/CD

### Vấn đề:

2 máy gửi cùng 1 lúc thì sẽ xảy ra tình trạng nhiễu loạn tín hiệu điện làm cho các frame bị đụng độ (collision) dẫn tới các frame bị lỗi các máy tạm thời dừng truyền và gửi lại.

Tập hợp các máy có thể xảy ra đụng độ với nhau gọi là **Collision domain**.

Để đảm bảo rằng khi các máy gửi cho nhau thì không được truyền 1 cách đồng thời thì máy tính sẽ dùng bộ cảm biến để lắng nghe xem đường truyền có rảnh hay không, nếu rảnh thì đẩy gói tin vào, nếu không rảnh thì nó chỉ nhận mà thôi (tại một thời điểm, 1 máy chỉ có thể truyền hoặc nhận thì ta gọi đó là kiểu truyền **Half duplex**, giống như gọi điện thoại: 2 bên cùng nói thì ai nghe ???).

Nếu 2 máy cùng lắng nghe đường truyền cùng 1 lúc thì vẫn xảy ra xung đột.

Lúc này người ta sẽ dùng giải thuật **CSMA/CD**: Khi xảy ra xung đột thì bộ cảm biến xung đột sẽ đẩy ra các tín hiệu gọi là "Jam" làm cho xung đột trầm trọng hơn, dẫn đến các máy đều biết có xung đột xảy ra. Khi các máy đều biết có xung đột xảy ra thì mỗi máy sẽ tạo ra bộ **Timer** (mỗi bộ timer ở mỗi máy là hoàn toàn khác nhau). Các máy sẽ chờ cho bộ Timer giảm dần đến "0" rồi mới truyền tiếp => tránh được xung đột ở lần kế tiếp.

### Ghi chú:

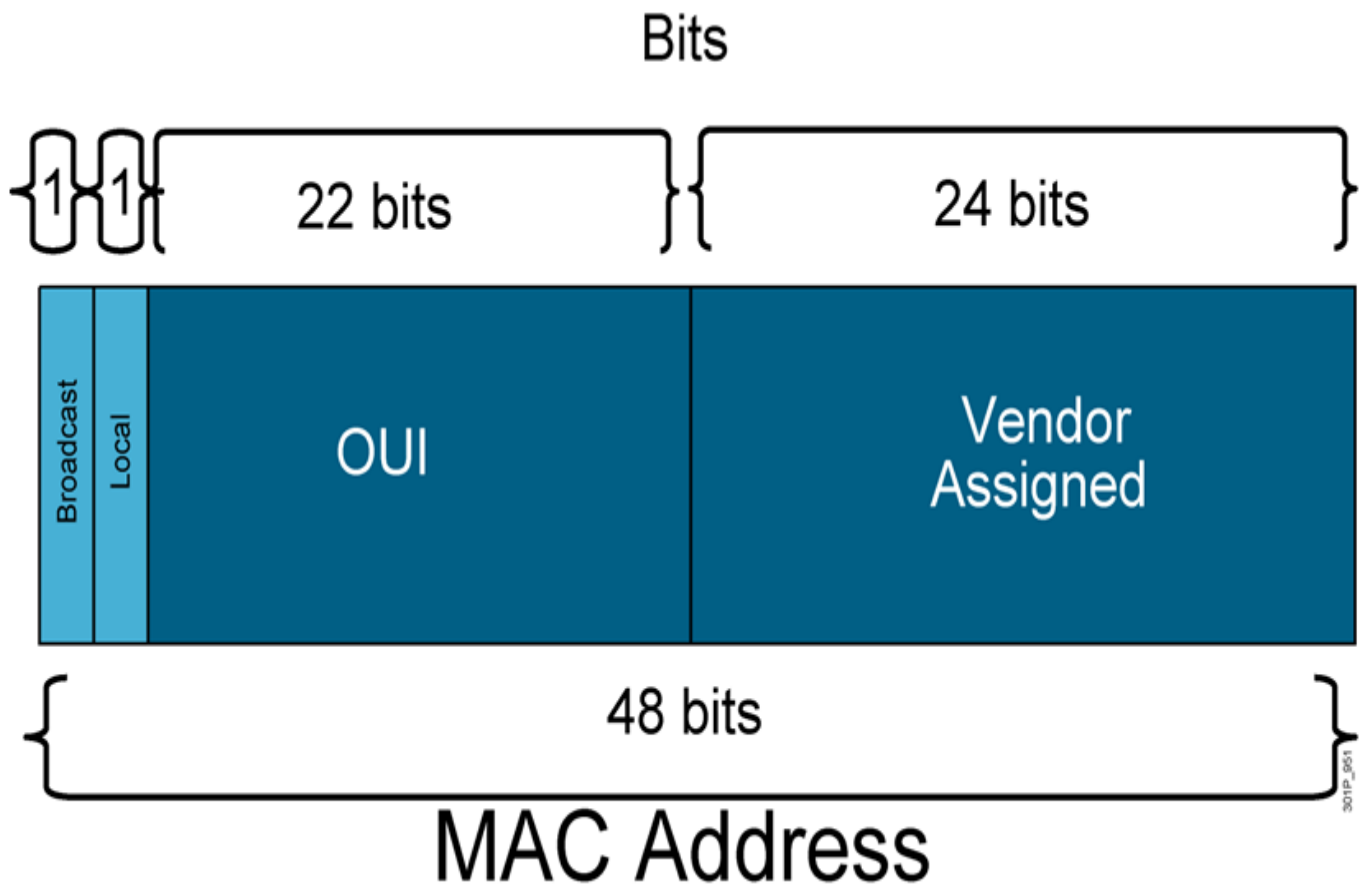
Trong Wireless thì có cơ chế CSMA/CA (avoidance): chống đụng độ chứ không chỉ giới hạn ở việc phát hiện.

Thiết bị Hub có kiểu truyền là Half duplex nên vẫn sử dụng cơ chế CSMA/CD, Switch hỗ trợ cả half, full duplex).

Mỗi port của Switch, Router là 1 collision domain, một con hub (repeater) hay nhiều con hub(repeater) kết nối lại với nhau thì vẫn chỉ là 1 collision domain.

**Mac address (Media Access Control)**: là loại địa chỉ vật lý của môi trường lớp 2. Là loại địa chỉ duy nhất trên thế giới

Dãy địa chỉ MAC dài 48 bit nhị phân (có khoảng  $2^{48}$  địa chỉ MAC). Được biểu diễn dưới dạng Hexa.



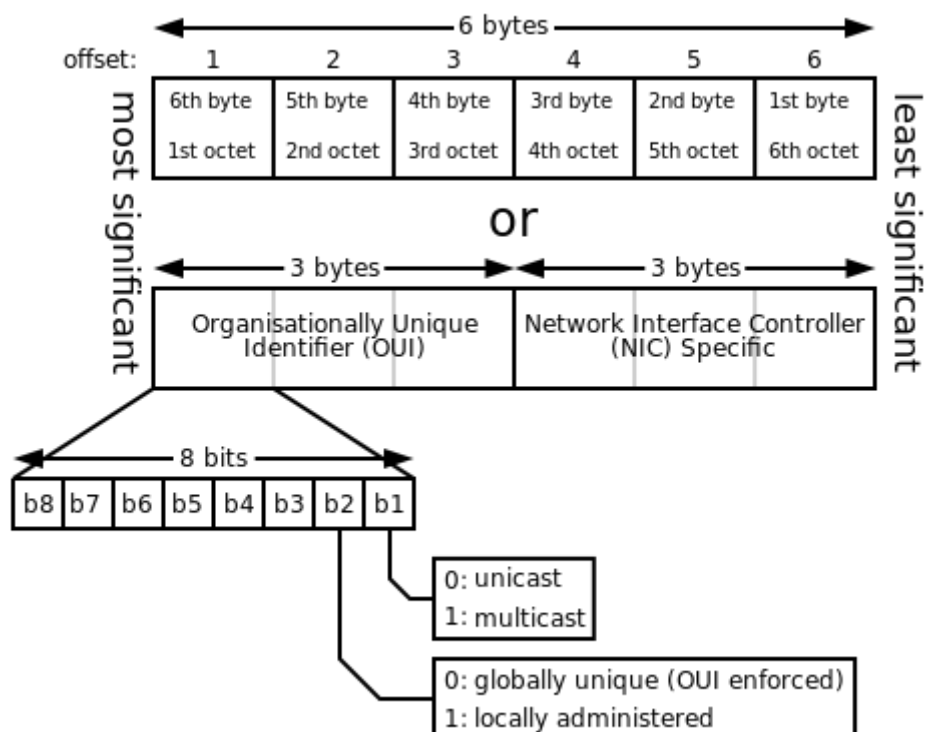
MAC address

**24 bit OUI:** tổ chức IEEE cấp cho các nhà sản xuất ( là duy nhất). Trong 24 bit đó thì có:

**1 bit local:** cho biết MAC này là thật( bit =0, gọi là global) hay giả (bit =1 hay còn gọi là local). Vì vậy với dãy 24 bit OUI thì bit local luôn bằng 0.

**1 bit broadcast:** cho biết địa chỉ MAC này là unicast (bit =0) hay multicast (bit =1).

**24 bit Vendor Assigned:** cho nhà sản xuất chỉ định để gán cho các thiết bị mà họ sản xuất ra ( cũng là duy nhất).



MAC address

VD: phân tích MAC: 06-00-00-00-00-00: 06

hexa chuyển qua nhị phân: 0000 1110

bit thứ nhất = 0 : đây là địa chỉ Unicast

bit thứ hai =1 : đây là MAC local

00-00-0c-43-2e-08: địa chỉ global OUI MAC.

Địa chỉ MAC Broadcast có dạng: FF-FF-FF-FF-FF-FF

### Các dạng kết nối từ Lan tới Internet:

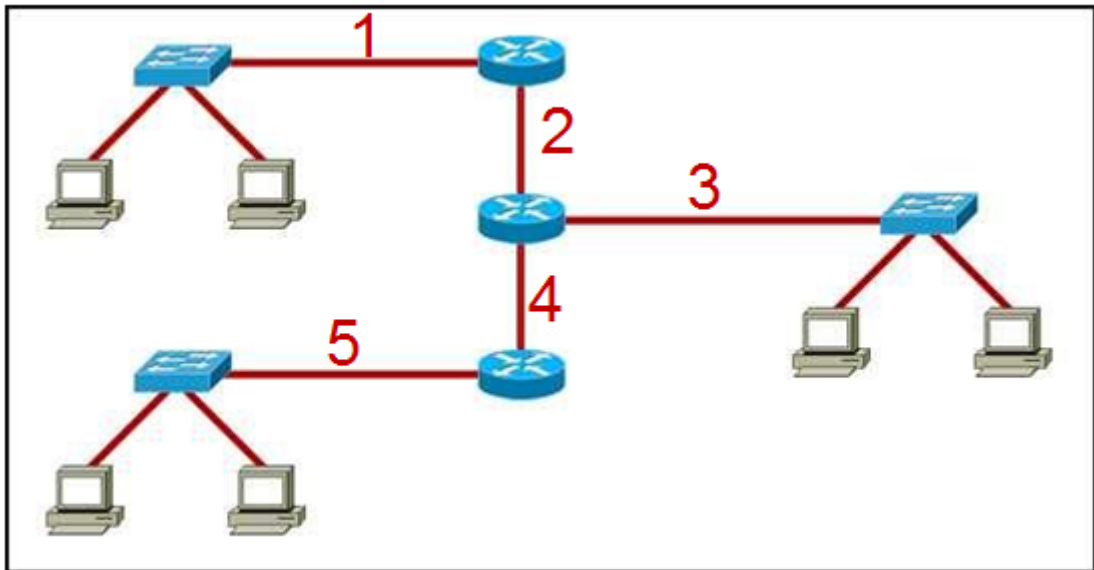
**DSL:** truy cập internet bằng đường dây điện thoại (ví dụ: dịch vụ ADSL).

**Cable:** (internet qua truyền hình cáp), sử dụng modem cáp (ai xài internet SCTV chắc biết), cáp truyền hình để kết nối internet.

**Serial:** sử dụng thiết bị CSU/DSU kết nối giữa công ty và các ISP. (dịch vụ thông dụng là: Leaseline).

**Các bạn tìm hiểu thêm về Broadcast Domain, cách xử lý gói tin của Switch khi nhận gói tin là unicast, multicast và broadcast.**

**Bài tập:** Xác định có bao nhiêu Collision Domain, Broadcast Domain ở hình sau:



# 4. IP Addressing

## 1. Địa chỉ IP ( Internet Protocol) là gì?

Khái niệm về địa chỉ IP rất dễ hiểu. Nó giống như là địa chỉ của 1 ngôi nhà. Ví dụ như: Trường Đại Học Sư Phạm TPHCM có địa chỉ là 280 An Dương Vương. “Trường Đại Học Sư Phạm TPHCM” chính là các thiết bị điện tử, điển hình là cái laptop bạn đang sử dụng. Còn “280 An Dương Vương” chính là địa chỉ IP của chiếc laptop đó. Trong một hệ thống mạng, các máy tính hoặc thiết bị điện tử liên lạc với nhau thông qua địa chỉ IP. Lưu ý rằng có 1 khái niệm khác cũng nói về địa chỉ của máy tính đó là MAC. MAC khác IP ở chỗ nó là địa chỉ duy nhất của mỗi máy tính. Còn IP thì có thể thay đổi.

IP có 2 version là: IPv4 (32 bit) và IPv6 (128 bit). Tuy nhiên trong bài này tôi chỉ nói về IPv4 – version phổ biến nhất hiện nay.

## 2. Hình thức

Ipv4 có 4 byte (tức là 32 bit)

Cấu trúc của nó có thể hiểu đơn giản như sau:

**Số.Số.Số.Số** ( $0 \leq \text{Số} \leq 255$ )

Mỗi 1 “**Số**” như vậy gọi là 1 **octet** (**1 octet = 8bit**)

Đi kèm với địa chỉ IP là 1 subnet mask. Cấu trúc của subnet mask cũng tương tự như IP

Ví dụ:

IP: 192.168.1.50

Subnet Mask (SM): 255.255.255.0

Các bạn có thể thấy các “**Số**” trong subnet mask đặc biệt hơn IP đó là nó chỉ có 2 con số là “255” và “0”. Chính 2 con số đó sẽ giúp chúng ta xác định được 2 khái niệm khác khác là **Net ID** và **Host ID** (Các bạn có thể tìm hiểu thêm 2 khái niệm này trên mạng).

Sau đây tôi sẽ mô phỏng cách xác định Net ID và Host ID trong 1 địa chỉ mạng.

<i>IP</i>	:	192 . 168 . 1 . 50
<i>Subnet Mask (SM)</i>	:	255 . 255 . 255 . 0

<div style="border-top: 1px solid blue; width: 150px; margin: 0 auto;"></div>	<div style="border-top: 1px solid blue; width: 50px; margin: 0 auto;"></div>
Net ID	Host ID

=> Net ID: 192 . 168 . 1 . 0  
=> Host: 0 . 0 . 0 . 50

*hoặc*

<i>IP</i>	:	10 . 7 . 3 . 5
<i>SM</i>	:	255 . 0 . 0 . 0

<div style="border-top: 1px solid blue; width: 100px; margin: 0 auto;"></div>	<div style="border-top: 1px solid blue; width: 100px; margin: 0 auto;"></div>
Net ID	Host ID

=> Net ID : 10.0.0.0  
=> Host ID: 0.7.3.5

Mô phỏng cách xác định Net ID và Host ID

Khi các máy tính cùng NetID thì mặc định liên lạc được với nhau.

Lưu ý:

Lớp A: Default subnet mask là: 255.0.0.0 (/8)

Lớp B: \_\_\_\_\_:255.255.0.0 (/16)

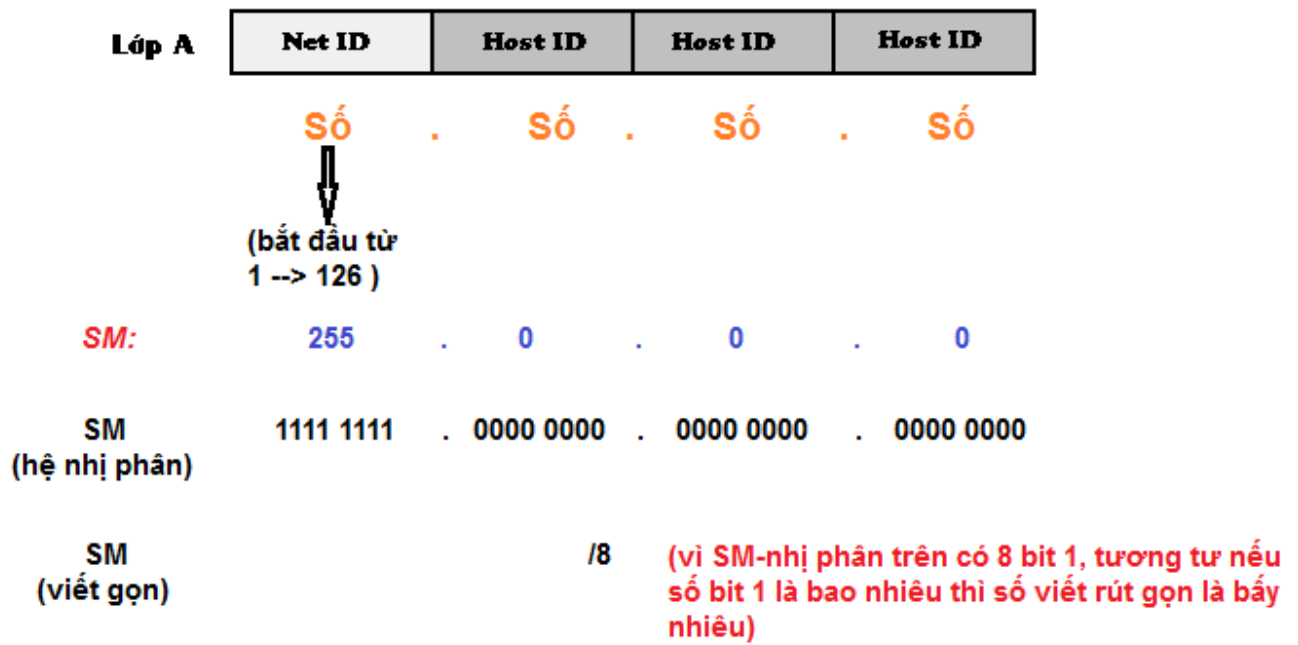
Lớp C: \_\_\_\_\_:255.255.255.0 (/24)

### 3. Các lớp IP

IP có 5 lớp: A,B,C,D và E. Nhưng chúng ta chỉ quan tâm tới A, B và C. Còn D,E là nhóm multicast và để nghiên cứu nên ta ko nhắc tới.

3 lớp IP (A, B và C) được phân biệt dựa vào số bit đầu và độ dài Net ID, Host ID của IP. Sau đây là cách phân biệt các lớp IP.





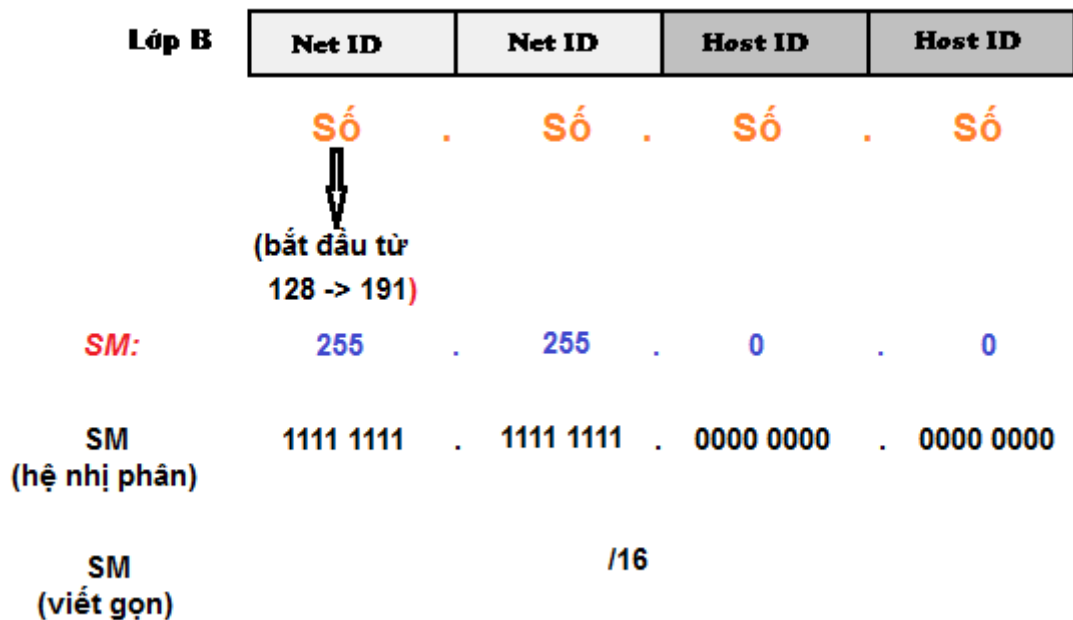
Địa Chỉ IP lớp A

Ví dụ: Các địa chỉ lớp A

10.10.3.1 / 8

32.221.32.3/8

72.212.220.200/8



Địa Chỉ IP lớp B

Ví dụ: Các địa chỉ lớp B

128.43.222.100/16

182.155.32.50/16

<b>Lớp C</b>	<b>Net ID</b>	<b>Net ID</b>	<b>Net ID</b>	<b>Host ID</b>
	Số	Số	Số	Số
	↓ (bắt đầu từ 192 -> 223)			
<b>SM:</b>	255	255	255	0
<b>SM (hệ nhị phân)</b>	1111 1111	1111 1111	1111 1111	0000 0000
<b>SM (viết gọn)</b>				/24

Địa Chỉ IP lớp C

Ví dụ: Các địa chỉ IP lớp C

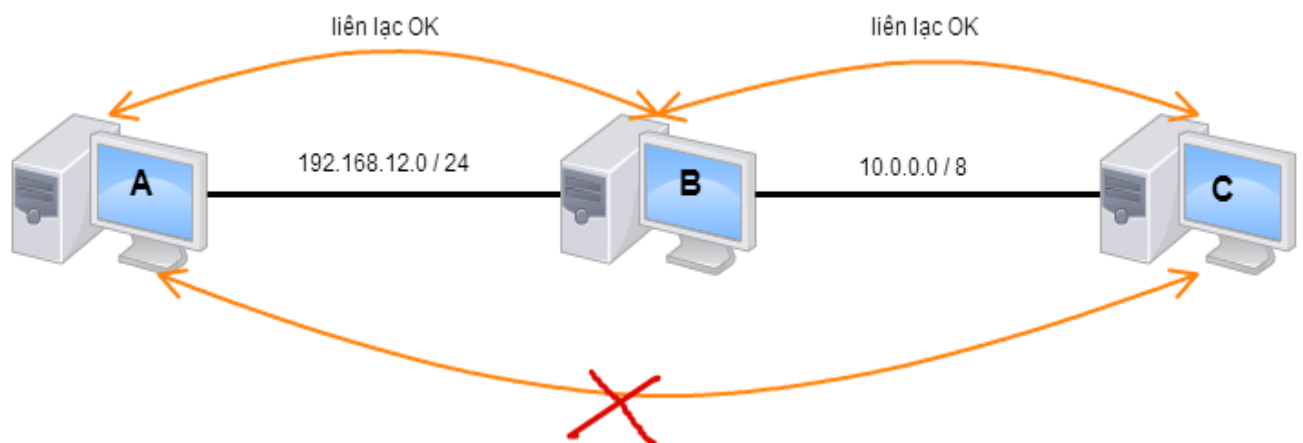
192.168.10.20/24

220.220.200.100/24

#### 4. Static IP

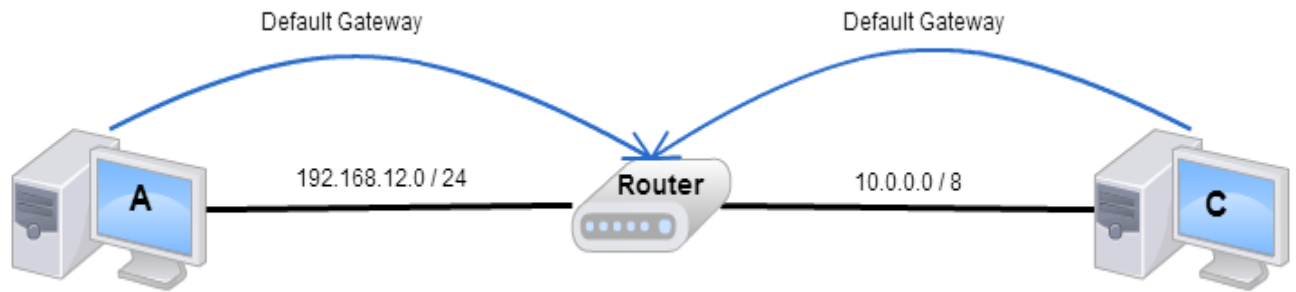
Static IP

Các máy tính cùng Net ID có thể liên lạc được với nhau mà không cần thông qua bất kỳ 1 thiết bị router nào.



Các máy có cùng net id thì có thể liên lạc với nhau. Ngược lại thì không.

Ngược lại các máy tính khác Net ID muốn liên lạc được với nhau cần các thiết bị router và các máy tính đó phải khai báo default gateway về router.



2 máy A và C khác net id nên phải có 1 router ở giữa định tuyến 2 net đó. Ngoài ra cả A và C đều phải default gateway về router để có thể liên lạc được với nhau.

### 5. Phương thức gửi gói tin

Như đã nêu ở trên các máy tính liên lạc với nhau thông qua địa chỉ Ip. Chúng gửi dữ liệu cũng như trao đổi thông tin bằng cách gửi các gói tin lẫn nhau. Có 3 phương thức tìm gửi tin mà tôi sẽ nói ngắn gọn như sau, đó là:

- + Unicast: có nghĩa là 1 PC gửi cho 1 PC
- + Multicast: có nghĩa là 1 PC gửi cho 1 nhóm PC
- + Broadcast: có nghĩa là 1 PC gửi cho mọi 1 PC trong cùng hệ thống mạng

### 6. Phân loại IP (theo tổ chức IANA)

Địa chỉ IP thường có hai loại Public và Private.

**Private IP** : là địa chỉ nằm trong mạng LAN sử dụng 3 lớp IP A, B và C

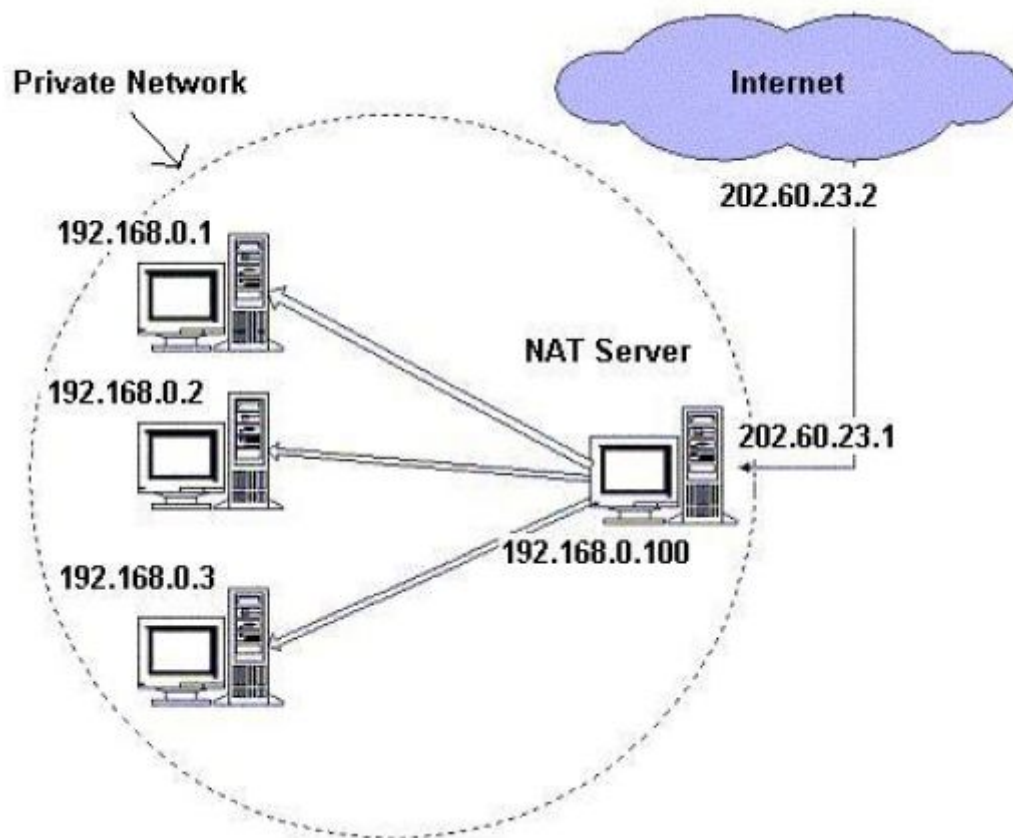
A: 10.x.x.x

B: 172.16.x.x -> 172.31.x.x

C: 192.168.x.x

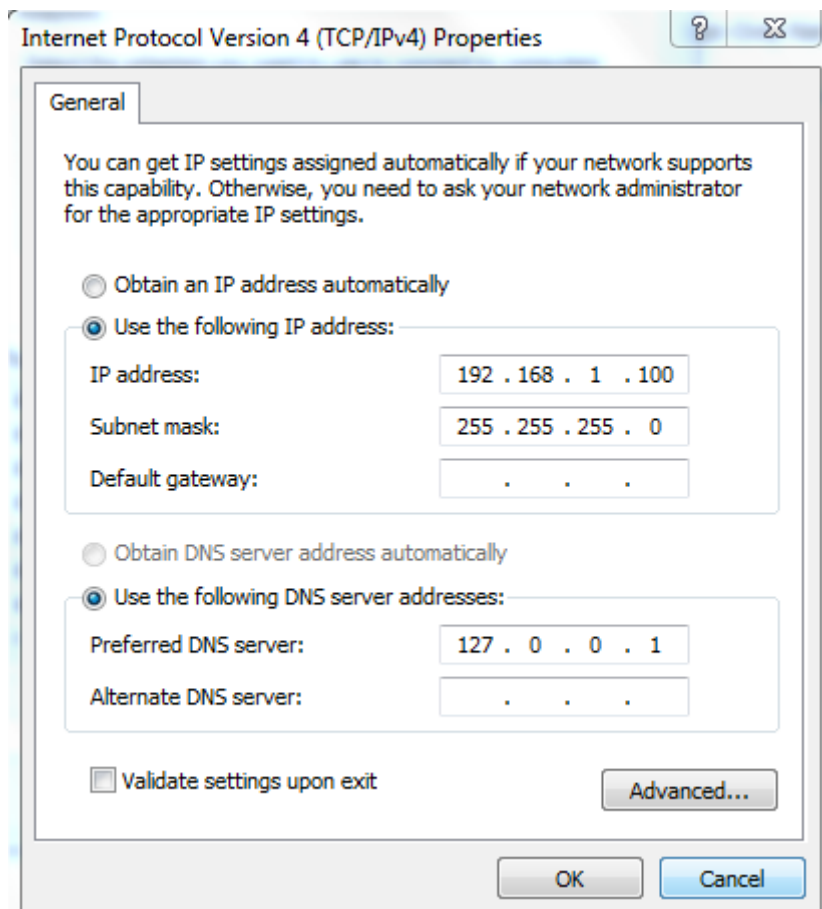
**Public IP**: được gán tới mỗi máy tính mà nó kết nối tới Internet và địa chỉ đó là duy nhất. Trong trường hợp này, không có sự tồn tại của hai máy tính với cùng một địa chỉ IP trên tất cả mạng Internet. Cơ chế này của địa chỉ IP giúp có máy tính này có thể tìm thấy máy tính khác và trao đổi thông tin. Người sử dụng sẽ không kiểm soát địa chỉ public IP mà được gán tới mỗi máy tính. Địa chỉ public IP được gán tới mỗi máy tính bởi nhà cung cấp dịch vụ Internet (gọi là ISP).

Một địa chỉ public IP có thể là "động" (dynamic) hoặc "tĩnh" (static). Một địa chỉ public IP tĩnh không thay đổi.



Private IP

Ngoài ra, còn có khái niệm về IP loopback. IP loopback là IP tự trở về bản thân nó. Và mặc định IP Loopback có địa chỉ là 127.0.0.1



Đặt Loopback IP

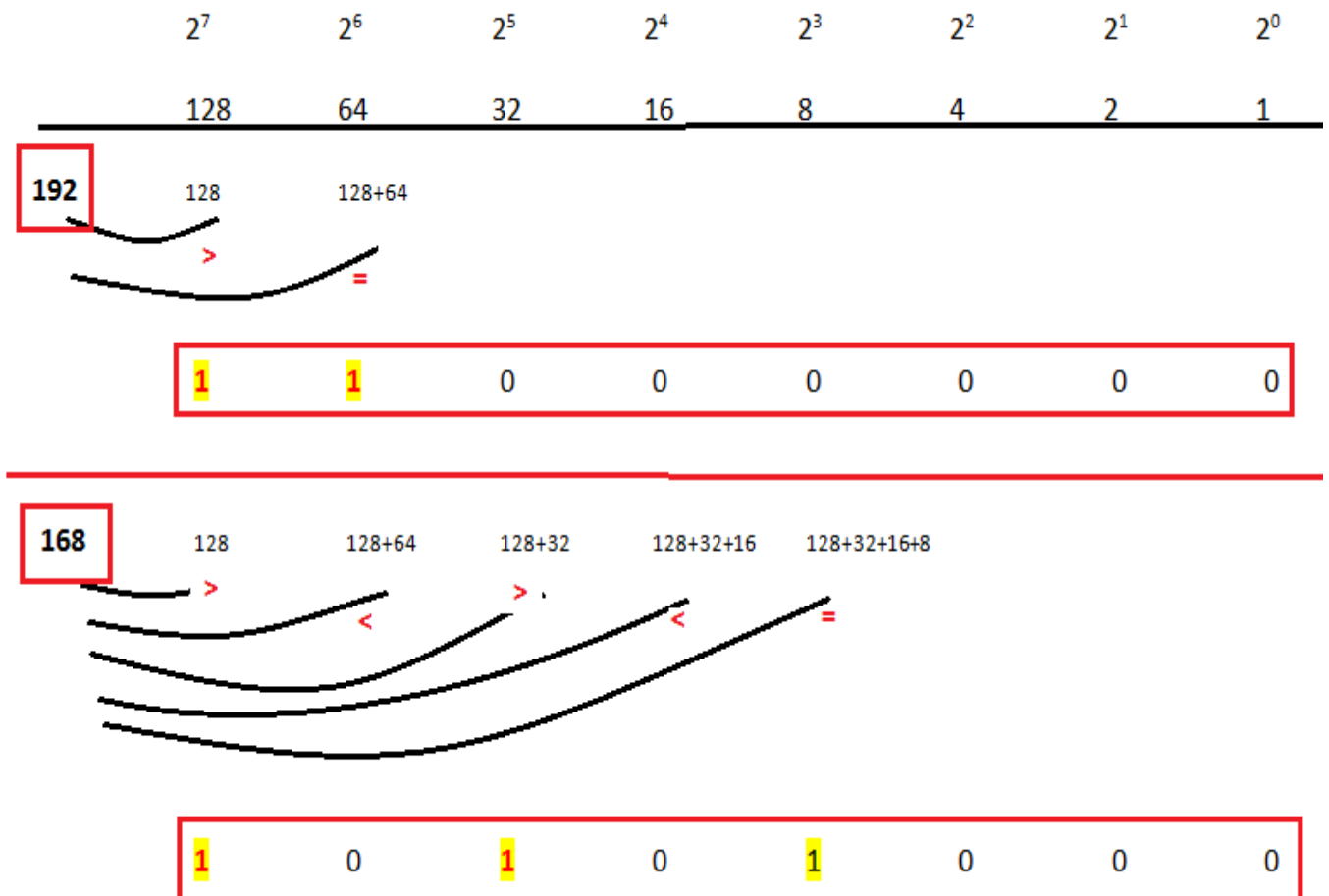
Ở hình trên các bạn có thể thấy trong ô **Preferred DNS server** tôi đặt là 127.0.0.1. Tôi có thể thay đổi địa chỉ này bằng chính IP của máy tôi là 192.168.1.100 như đã điền trên ô **IP Address**. Tức là 2 địa chỉ này tương đương. Các bạn sẽ sử dụng IP loopback trong việc xây dựng Domain Network, DNS,...

## 5. Subnetting

Hệ nhị phân (hệ đếm cơ số 2) là 1 số có thể được ráp nối lại bởi 2 chữ số (0 và 1). Vd: 100, 010, 1000100,...

+ Cách đổi từ hệ nhị phân sang thập phân.

Ví dụ như ta muốn đổi từ 192 và 168 sang hệ nhị phân, ta làm như sau



Đổi thập phân sang nhị phân

Cách đổi trên có thể tóm gọn như sau: Đầu tiên bắt đầu ta lấy 128 so sánh với số cần đổi (SCĐ), tiếp đó ta cứ cộng dồn 128 với các số sau theo nguyên tắc:

Nếu kết quả cộng dồn đó < SCĐ thì bit tương ứng bên dưới cũng sẽ là 1.

Nếu kết quả cộng dồn đó > SCĐ thì bit tương ứng bên dưới sẽ là 0 và ta sẽ bỏ số cộng dồn đó ra (như phép đổi 168 là ta bỏ 2 số 64 và 16).

Nếu kết quả cộng dồn đó = SCĐ thì bit tương ứng bên dưới sẽ là 1 và tất cả các bit theo sau là 0. Phép chuyển đổi dừng lại tại đây và ta có kết quả cuối cùng.

+ Cách đổi nhị phân sang thập phân

Rất đơn giản các bạn chỉ cần xếp các bit nhị phân vào bảng trên và xét vị trí nào có bit 1 thì ta lấy các số vị trí đó cộng lại với nhau sẽ ra số thập phân cần tìm.

### 2. Subnetting

Subnetting (chia subnet) là hành động chia Net ID thành các subnet ID. Vậy Subnet ID là gì? Và tại sao phải chia subnet? Ví dụ công ty ABC có 2 chi nhánh: Sài Gòn và Hà Nội. Như các bạn cũng đã biết để 2 server ở hai chi nhánh này liên lạc được với nhau thì thứ nhất chúng phải có đường truyền vật lý thuê từ nhà cung cấp dịch vụ, thứ 2 là ta phải tổ chức đặt IP cho 2 chi nhánh này. Nhưng công ty chỉ có 1 IP Public là 1 Net ID được thuê từ nhà cung cấp. Vậy ta phải chia Net ID đó thành nhiều Net ID con (hay còn gọi là Subnet ID) cho 2 chi nhánh của cty ABC. Sau đây tôi sẽ cho các bạn công thức để chia subnet và để hiểu rõ hơn thì các bạn nên xem ví dụ bên dưới.

- Công thức:

Gọi **n** là số bit 1 tăng thêm của Subnet Mask (hay còn gọi là số bit mượn)

Gọi **m** là số bit 0 còn lại của Subnet Mask (**m = 32 - n - SM hiện tại**). Ta làm theo 5 bước

1. Số Subnet:  $2^n$
2. Số Host/Subnet :  $2^m - 2$  ( vì phải trừ đi địa chỉ NetID và Broadcast )
3. Bước nhảy:  $2^m$
4. Subnet mask mới: **256 - Bước nhảy**
5. Các Subnet ID:

+ Subnet ID đầu tiên = **0**

+ Subnet ID kế tiếp = **Subnet hiện tại + Bước nhảy**

6. Trong Subnet ID:

+ Host đầu: **Subnet ID + 1**

+ Host cuối: **Subnet ID + Bước nhảy - 2**

+ Địa chỉ Broadcast: **Host cuối + 1**

Lưu ý: Tổng số subnet có 2 cách tính :  $2^{m-2}$  (ngày xưa dùng) và  $2^m$ .

Do Router ngày xưa nó không phân biệt được subnet all zero và subnet all one. để hiểu rõ hơn, các bạn search " chia subnet trừ 2 hay không" sẽ hiểu rõ

**Ví dụ:** Ta phải chia Net ID: 203.162.4.0/24 tăng 2 bit (n = 2)

1. Số Subnet:  $2^n = 2^2 = 4$
2. Số Host trên Subnet :  $2^6 - 2 = 62$
3. Bước nhảy:  $2^6 = 64$
4. Subnet mask mới:  $256 - \text{Bước nhảy} = 256 - 64 = 192$

Subnet mới: 255.255.255.255.192 = 11111111.11111111.11111111.11000000 => /26

5. Các Subnet ID:

+ Subnet ID đầu tiên = **0**

=> **203.162.4.0/26**

+ Subnet ID kế tiếp = **Subnet hiện tại + Bước nhảy**

203.162.4.64/26

203.162.4.128/26

203.162.4.192/26

**Kết quả:**

Subnet ID	Host đầu: Subnet ID + 1	Host cuối: Subnet ID + Bước nhảy - 2	Broadcast: Host cuối + 1
203.162.4.0/26	203.162.4.1	203.162.4.62	203.162.4.63
203.162.4.64/26	203.162.4.65	203.162.4.126	203.162.4.127
203.162.4.128/26	203.162.4.129	203.162.4.190	203.162.4.191
203.162.4.192/26	203.162.4.193	203.162.4.254	203.162.4.255

**Một bài toán khác về IP. Ta có địa chỉ của 1 host, vậy làm sao để suy ra được host đó thuộc vùng mạng (Net ID) nào?**

Ví dụ ta có 1 host như sau:

IP: 203.162.4.**165**

SM: 255.255.255.224

Ta thấy 255.255.255.224 = 11111111 . 11111111 . 11111111 . 111**00000**

=> Số bit 0 còn lại của SM là: m = 5

=> Bước nhảy =  $2^m = 2^5 = 32$

=> Ta lấy **165** : 32 = 5,15625

=> Ta lấy phần nguyên của kết quả trên tức là 5 x 32 = 160

=> Host trên thuộc Net ID: 203.162.4.**160**

### 3. VLSM (Variable Length Subnet Masking)

Đối với cách chia trên ta thấy số IP (hay còn gọi là host) trong mỗi 1 subnet là như nhau. Vậy giả sử cty XYZ được cung cấp Public IP là **203.162.4.0/24** cho 3 chi nhánh là SG, HN, DN. Và 3 chi nhánh này có số yêu cầu về IP khác nhau như sau:

+ SG cần 52 IP

+ HN cần 25 IP

+ DN cần 22 IP

Nếu ta dùng cách chia mạng con đều nhau như trên thì chắc chắn một điều sẽ không đáp ứng được yêu cầu của cty XYZ. Chỗ thì cần nhiều, chỗ thì cần ít. Nếu cấp đều nhau thì chỗ sẽ bị thiếu IP và ngược lại có chỗ sẽ bị dư thừa IP. Chính vì lý do thực tế đó nên sinh ra cách chia Subnet tối ưu hơn đó là VLSM. Sau đây tôi sẽ trình bày cách chia subnet theo yêu cầu như ví dụ trên theo chuẩn VLSM.

Đầu tiên ta thấy nhu cầu của mỗi chi nhánh phải thỏa điều kiện sau:

**Số lượng host (IP) của 1 subnet mà cty cấp cho mỗi chi nhánh >= Số host (IP) yêu cầu của mỗi chi nhánh**

Ta có **Số lượng host (IP) của 1 subnet =  $2^m - 2$**

=>  **$2^m - 2 >=$  Số host (IP) yêu cầu của mỗi chi nhánh**

Ta nên chia subnet theo thứ tự yêu cầu IP giảm dần của các chi nhánh, bắt đầu là SG với số lượng IP yêu cầu là 52

Ta có:  $2^m - 2 >= 52$

=>  $m = 6$

=>  $n = 2$  (Các bạn xem lại ví dụ về cách chia subnet ban đầu để hiểu hơn)

=> Bước nhảy =  $2^m = 2^6 = 64$

Theo như công thức ở mục 2 thì ta có:

+ Subnet ID đầu tiên = **0**

=> **203.162.4.0/26**

Và Subnet Mask mới của mỗi Subnet ID trên sẽ được tính theo công thức: SM cũ + n

=> Subnet Mask mới của Subnet ID **203.162.4.0** sẽ là  $24 + 2 = 26$

+ Subnet ID kế tiếp = Subnet hiện tại + Bước nhảy

Vậy kết quả sẽ được tóm tắt như bảng sau:

Chi Nhánh	Số IP yêu cầu	Subnet ID	Subnet Mask	Host đầu: Subnet ID + 1	Host cuối: Subnet ID + Bước nhảy - 2	Broadcast: Host cuối + 1
SG	52	<b>203.162.4.0</b>	/26	203.162.4.1	203.162.4.62	203.162.4.63
HN	25	<b>203.162.4.64</b>	/27	203.162.4.65	203.162.4.94	203.162.4.95
DN	22	<b>203.162.4.96</b>	/27	203.162.4.97	203.162.4.126	203.162.4.127


Như các bạn cũng đã thấy số lượng IP được chia cho mỗi chi nhánh đã đủ với yêu cầu ban đầu và không quá dư thừa. Và thực tế thì VLSM là cách chia được dùng để làm công việc chia Subnet ID của các doanh nghiệp. Thật ra các bạn cũng có thể dùng máy tính, hoặc các ứng dụng để tính toán và chia subnet 1 cách tự động

## 6. ICMP

Trình bày cách hiểu đơn giản về ICMP, Ping nhằm phục vụ cho nhu cầu test, chuẩn đoán lỗi trong các bài Lab mà các bạn gặp phải. Để hiểu chuyên sâu thì các bạn nên đọc trong cuốn TCP/IP Vol 1.

ICMP (Internet Control Message Protocol) : là giao thức giúp ta kiểm tra các kết nối lớp 3 xem các hệ thống có thông với nhau không.

ICMP có rất nhiều ứng dụng, trong đó ứng dụng Ping được sử dụng nhiều nhất.

 ping 0  
Host 1 ping Host 2

Để kiểm tra Host A với địa chỉ "IP A" có đi đến được Host B với "IP B" hay không thì trên Host A thực hiện Ping đến IP B.

Ping sử dụng 2 thông điệp "ICMP echo request" và "ICMP echo reply" để thực hiện quy trình ping.

Khi Host A ping B thì lập tức A gửi một loạt các gói tin (thông thường PC gửi 4 gói) ICMP echo request.

Host B nhận được bao nhiêu ICMP echo request thì sẽ trả về bấy nhiêu gói ICMP echo reply.

### Các thông số:

**bytes:** kích thước của gói tin.

**time:** thời gian hồi đáp.

**TTL** (time -to-live) là một trường dài 8 bit. Giá trị tối đa là 255, cứ mỗi khi đi qua con Router thì giá trị TTL giảm đi 1 đơn vị, khi Router nhận gói tin có TTL = 0 thì nó sẽ tự "drop" gói tin đó.

**Ý nghĩa của TTL:** dùng để chống lại sự lặp vòng (routing loop)


Các kết quả có thể trả về sau khi Ping:

### Ping thành công

 ping 1  
Reply

### Ping không thành công :


**Request time out:** PC gửi gói tin ICMP request đi, sau khoảng thời gian "time out" mà không thấy gói tin trở về.

 ping 3  
Request time out

### Nguyên nhân:

- Do đường truyền vật lý (kiểm tra lại kết nối, cáp).
- IP không tồn tại, máy PC đích bị tắt
- Máy đích bị chặn bởi Firewall, firewall cấm ping (tắt firewall, hoặc cấu hình lại).
- Gửi thành công nhưng firewall bên máy đích chặn ping => không reply được.

### Destination host unreachable:

 ping 2  
Host unreachable

### TH 1: 2 host khác lớp mạng

Gói tin đi đến default gateway nhưng default gateway lại không biết đường đi tới đích (không có trong bảng định tuyến). Nó gửi lại gói "reply from < IP default gateway > destination host unreachable" với ý nghĩa: gói tin đến Router là "cụt đường".

### TH2: 2 host cùng lớp mạng

Đương nhiên khi 2 host cùng lớp mạng thì không có sự góp mặt của Router, Host A gửi nếu không thể đến được thì trả về gói "reply from < IP source> destination host unreachable".

### Nguyên nhân:

- Router không biết đường đi.



- IP không tồn tại, máy PC đích bị tắt.
- Do đường truyền vật lý.

Lệnh Ping giúp cho chúng ta chuẩn đoán nhanh chóng và hiệu quả các sự cố mạng, ping là ứng dụng luôn được sử dụng đầu tiên khi có lỗi xảy ra.

## 7. Local User and Group

Ở bài này chúng ta sẽ tìm hiểu các vấn đề về **User và Group**.

Yêu cầu:

2 máy ảo chạy server 2012

2012may1: IP: 192.168.1.100/24 (IP thế nào tùy các bạn chọn).

2012may2: IP: 192.168.1.101/24.

Name	State	CPU Usage	Assigned Memory	Uptime
2012may1	Running	0 %	513 MB	01:15:39
2012may2	Running	0 %	513 MB	01:15:41

máy ảo

Tắt firewall (Run -> firewall.cpl), 2 máy ping lẫn nhau, đảm bảo thông suốt.

**User account:** là một bộ thông tin, dùng để định danh người dùng trên hệ thống.

Từ sau bản MS-Dos thì Microsoft ra đời các hệ điều hành (HDH) Windows. Ta có thể chia thành 2 nhóm như sau:

Nhóm 1: Win 95, 98, me.

Nhóm 2: Win NT, 2000, XP, 2003, 2008, 7, 2008R2 v.v .

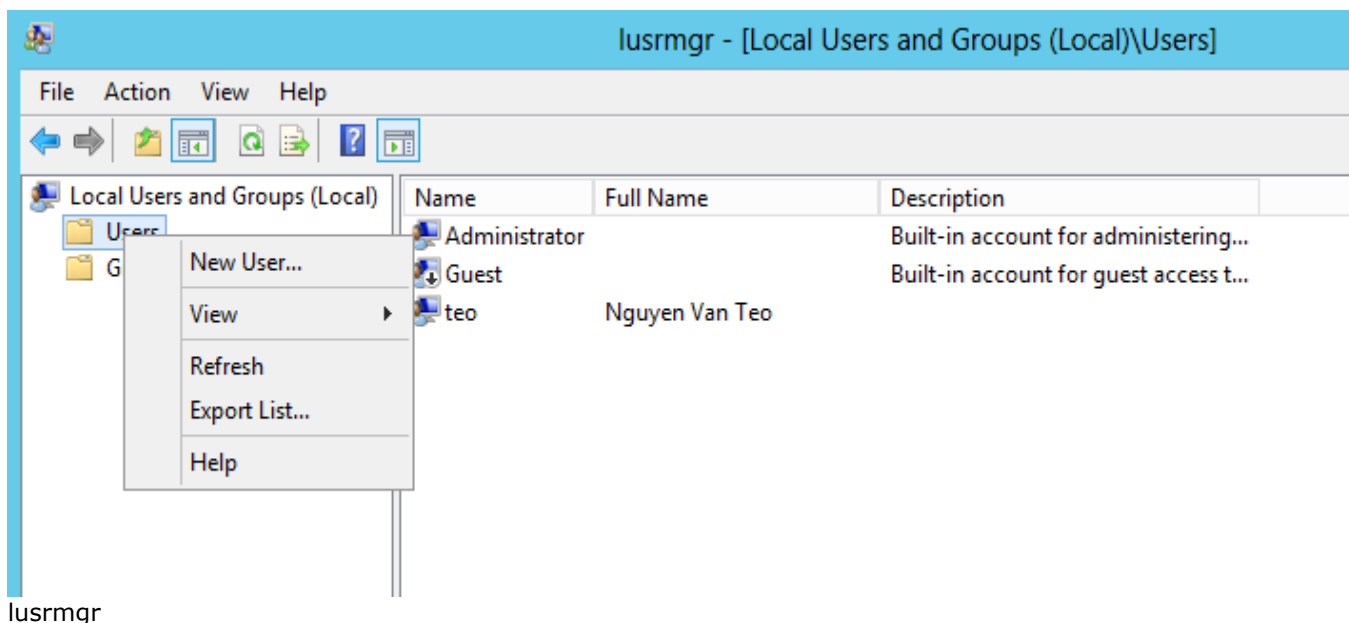
**Ở nhóm 1:** Khi cài HDH thì máy tính làm việc ở mode: simple user. Simple user: máy tính chỉ phục vụ cho một người dùng, không có sự phân biệt giữa các người dùng khác nhau. bất kì ai ngồi trên máy làm việc thì được toàn quyền trên máy tính.

**Vấn đề:** muốn bảo vệ dữ liệu thì chỉ còn mỗi việc không cho ai ngồi trên máy.

**Nhóm 2:** Các máy tính hoạt động ở mode: Multiple User, phục vụ cho nhiều người dùng và mỗi người dùng có một không gian làm việc riêng ( Profile).

Khi cài đặt HDH Windows thì mặc định có 2 tài khoản luôn tồn tại: administrator và guest đều là Built-in account.

Cách tạo User Account: start -> run : lusrmgr.msc (giao diện quản lý user và group)



User account gồm 2 thông tin quan trọng là:

- **User name:** không phân biệt hoa thường.
- **Password:** mặc định windows server bắt ta đặt password phức tạp.

Password được xem là an toàn (phức tạp) khi:

- tối thiểu 8 kí tự.
- password ít ý nghĩa.
- xuất hiện 3 trong 4 nhóm.

4 nhóm gồm:

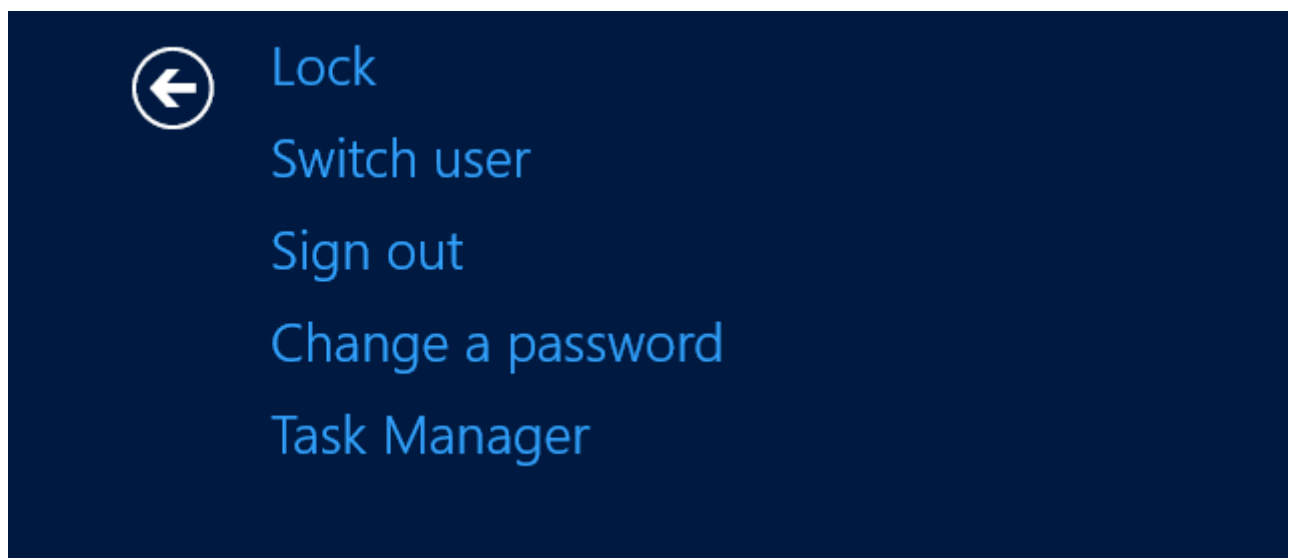
- a -> z.
- A -> Z.
- 0 -> 9.

- **Kí tự ASCII:** @, #, &, v.v ( muốn biết các kí tự ASCII vào: start -> All Programs -> System tools -> Character Map ).

**Ví dụ: TuH0cm@ng123**

Password của các tài khoản sẽ được lưu trong file **SAM** với đường dẫn: C:\windows\system32\config.

Khi bấm Ctrl Alt Del thì xuất hiện:



Ctrl Alt Del

**Clock:** khóa màn hình lại, các ứng dụng vẫn còn hoạt động.

**Switch user:** log on (đăng nhập) bằng tài khoản khác nhưng các ứng dụng vẫn không bị đóng ở tài khoản hiện tại.

**Sign out:** kết thúc phiên làm việc.

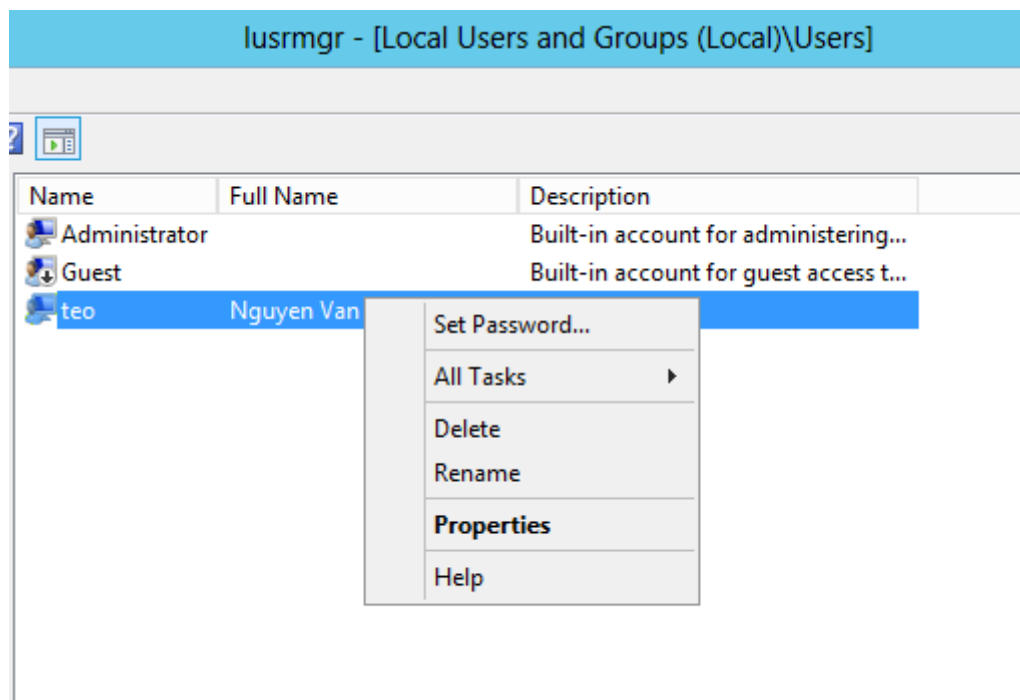
Lần đầu tiên khi user Teo log-on, thì hệ thống tạo cho user môi trường làm việc riêng (user Profile).

User Profile: bao gồm

- Dữ liệu hay các thiết lập trên desktop ( đổi hình nền v.v).
- Các lưu trữ trong Document.
- Application data.
- v.v (sẽ tìm hiểu kĩ ở bài User Profile).

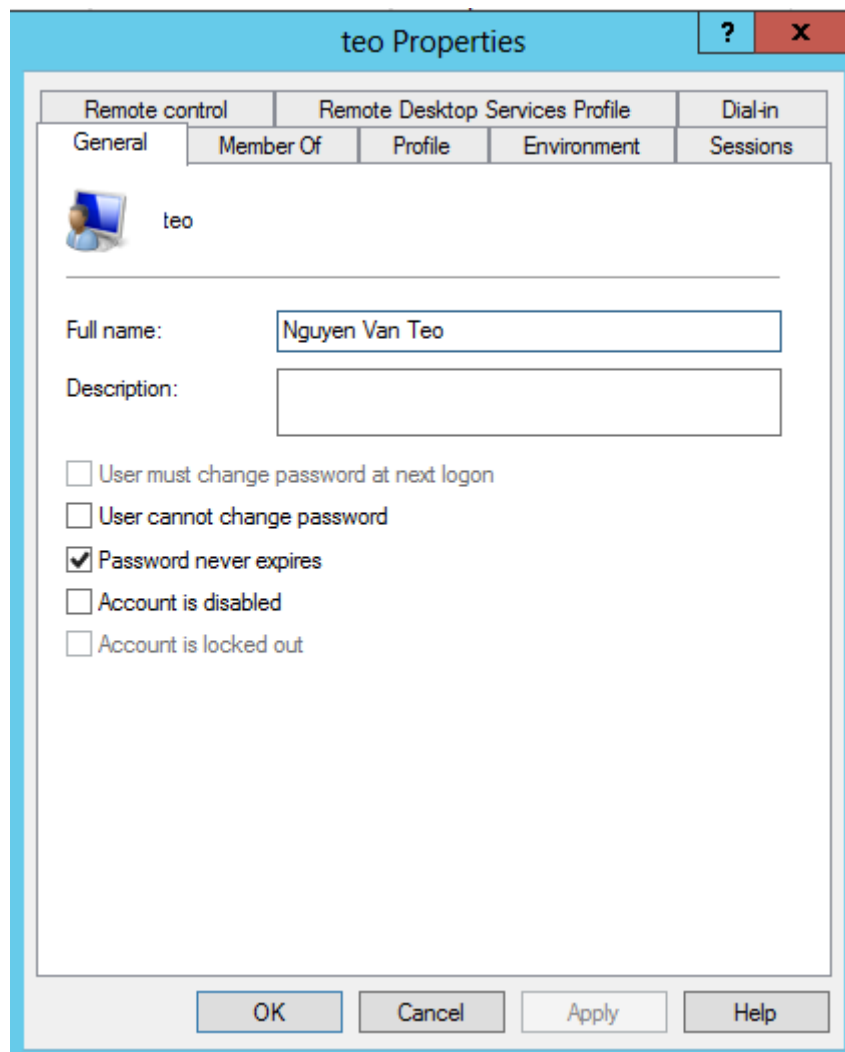
Khi log on user Ti thì Windows sẽ tạo cho user Ti profile riêng, user Ti không thể xâm nhập vào môi trường làm việc của Teo.

Thuộc tính cơ bản của User Account: Properties tài khoản



Properties

### Tab General



General

– **User must change password at next log on:** người dùng phải đổi password ở lần đăng nhập kế tiếp. Khi user đổi pass rồi thì "mất dấu check" ở thuộc tính này.

+ Dùng để cho user tự đặt mật khẩu khi mới tạo account.

+ Nếu trong quá trình sử dụng, ta thấy tài khoản này đang bị dò password thì ta sẽ yêu cầu đổi pass (hoặc user tự bấm Ctrl + Alt + Del để đổi pass).

– **User cannot change password:** người dùng không thể đổi password.

+ Dùng khi có các tài khoản dùng chung cho nhiều người.

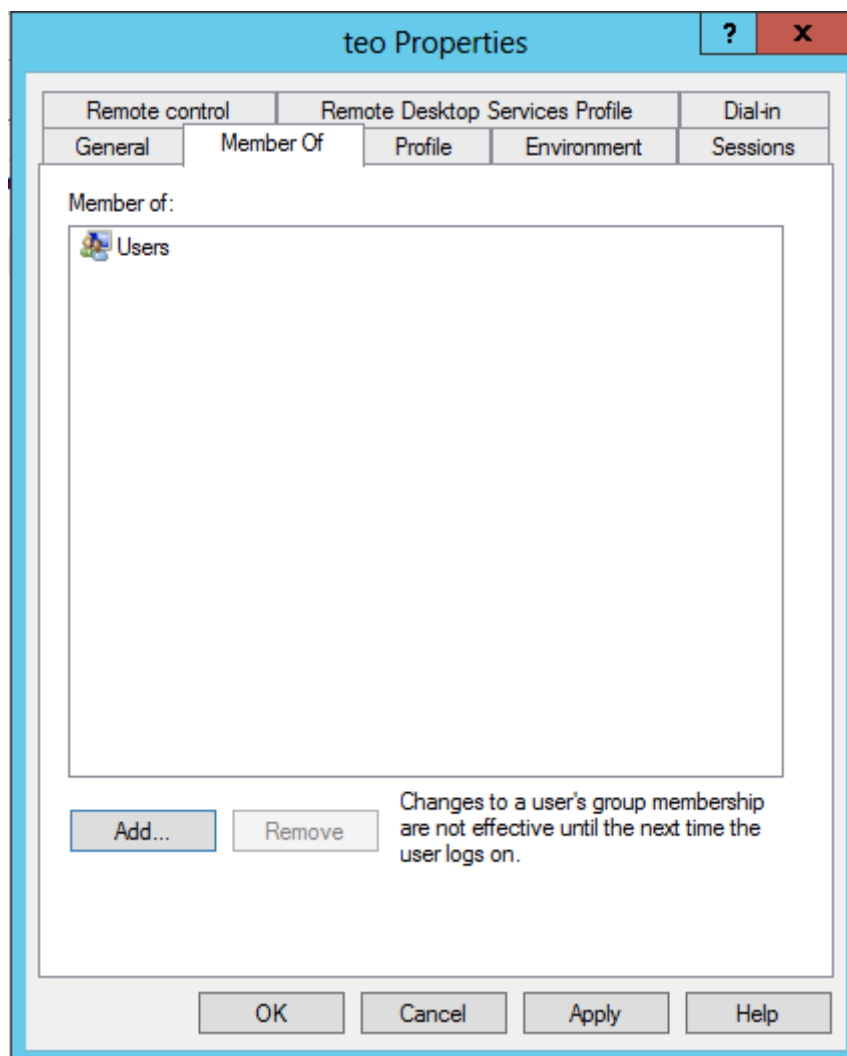
– **Password never expired:** password không bao giờ hết hạn, nếu không check thì mặc định password user chỉ có giá trị trong 42 ngày. Sau 42 ngày bắt buộc người dùng đổi pass.

+ Dùng cho các tài khoản tạo ra nhằm mục đích khai báo cho các tác vụ trên hệ thống (vd: backup phải khai báo tài khoản có quyền backup, mà chương trình backup thì chạy liên tục, khi đến 42 ngày thì nó dùng tài khoản này => backup không thể thực hiện )

– **Account is disabled:** tài khoản không thể log on hay truy xuất các tài nguyên trên hệ thống.

+ Dùng khi có các tài khoản không sử dụng nữa, ta không nên xóa mà cứ disable

## Tab Member Of


























### Member Of

Mặc định khi user được tạo ra thì nó là thành viên của 1 group.

Group là đối tượng trong hệ thống (system object), dùng để chứa user account hoặc group account khác

Chức năng phục vụ cho công tác quản lý, phân quyền (thay vì phân quyền chi tiết từng user thì ta dùng group cho nhanh)

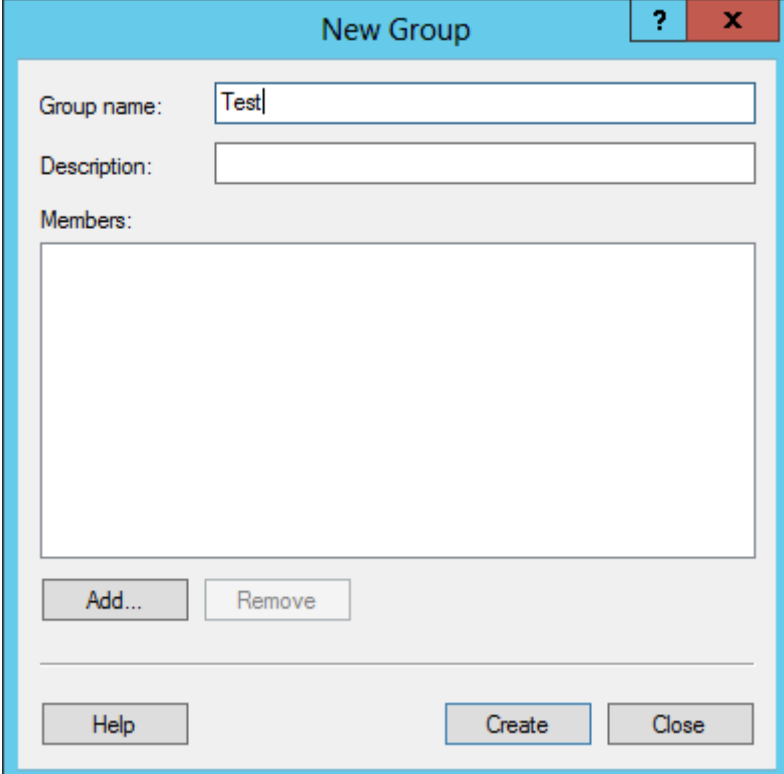
Name	Description
 Access Control Assist...	Members of this group can remotely query authorization attr...
 Administrators	Administrators have complete and unrestricted access to the...
 Backup Operators	Backup Operators can override security restrictions for the so...
 Certificate Service DC...	Members of this group are allowed to connect to Certificatio...
 Cryptographic Operat...	Members are authorized to perform cryptographic operations.
 Distributed COM Users	Members are allowed to launch, activate and use Distributed ...
 Event Log Readers	Members of this group can read event logs from local machi...
 Guests	Guests have the same access as members of the Users group ...
 Hyper-V Administrators	Members of this group have complete and unrestricted acce...
 IIS_IUSRS	Built-in group used by Internet Information Services.
 Network Configuratio...	Members in this group can have some administrative privile...
 Performance Log Users	Members of this group may schedule logging of performanc...
 Performance Monitor ...	Members of this group can access performance counter data...
 Power Users	Power Users are included for backwards compatibility and p...
 Print Operators	Members can administer domain printers
 RDS Endpoint Servers	Servers in this group run virtual machines and host sessions ...
 RDS Management Ser...	Servers in this group can perform routine administrative acti...
 RDS Remote Access S...	Servers in this group enable users of RemoteApp programs a...
 Remote Desktop Users	Members in this group are granted the right to logon remotely
 Remote Management...	Members of this group can access WMI resources over mana...
 Replicator	Supports file replication in a domain
 Users	Users are prevented from making accidental or intentional sy...
 WinRMRemoteWMIU...	Members of this group can access WMI resources over mana...

Group mặc định

Đây là các Group mặc định có sẵn trên windows, dựa vào các chức năng mà ta có các group khác nhau, có 2 nhóm

- nhóm 1 : có chức năng quản lý hệ thống, vd: group Administrators ( tạo user, chỉnh giờ, tắt máy v.v)
- nhóm 2: nhóm được phép truy cập, sử dụng tài nguyên, vd: group Users.

Ta cũng có thể tạo group riêng: ( phải chuột -> New Group)



Group

muốn add user, ta bấm Add.

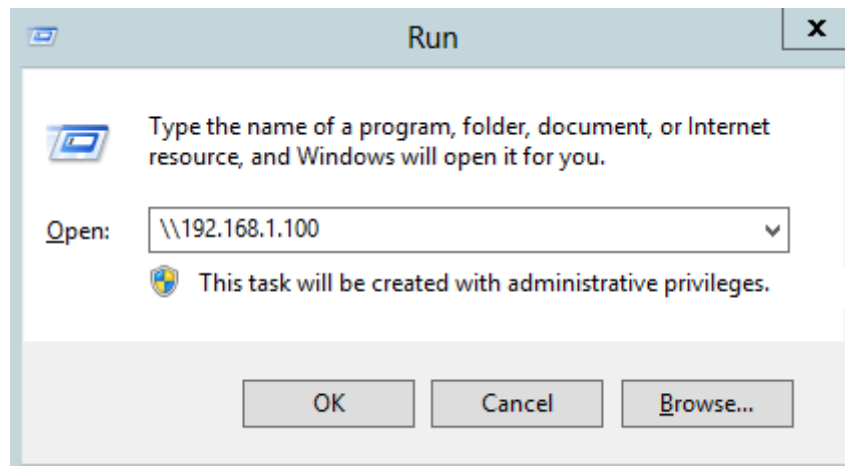
User thuộc group nào thì sẽ có quyền tương ứng với group đó.

### Truy xuất tài nguyên trong Lan:

Các máy tính trong mạng Workgroup gọi là local computer, user thuộc local computer (hay còn gọi là local user) chỉ được phép log-on hay sử dụng tài nguyên trên chính máy đó ( ứng dụng, máy in v.v), không thể dùng để truy cập tài nguyên ở máy khác. User thuộc 2012may1 muốn truy xuất tài nguyên của 2012may2 phải dùng tài khoản có trên 2012may2.

Sử dụng cú pháp:

**Network Access:** \\<IP> hoặc <computer name> vd: \\192.168.1.100



Network Access

Khi thực hiện Network Access giữa 2 máy tính thì diễn ra các bước sau:

Bước 1: Nếu tài khoản hiện tại đang đăng nhập (trên máy nguồn) có cùng user name, password với máy đích thì được phép truy cập tài nguyên, nếu không đúng thì qua bước 2.

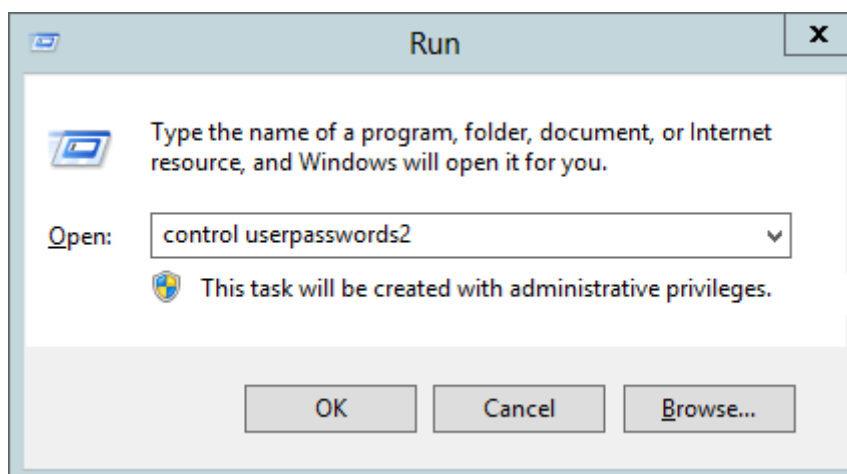
Bước 2: Yêu cầu tài khoản Guest, nếu máy đích có tài khoản guest (mặc định bị disable) thì được phép, không có thì chuyển qua bước 3.

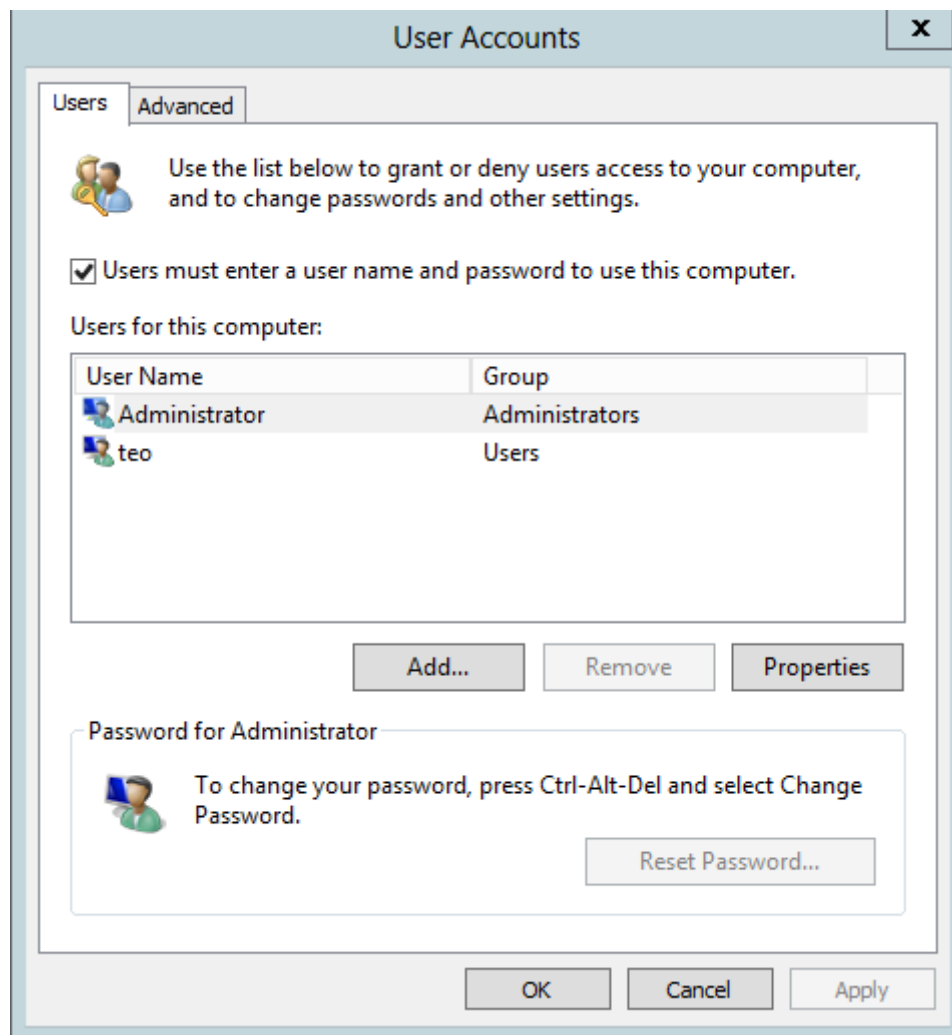
Bước 3: Hiện thị hộp thoại đăng nhập user name, password.

**Nếu trong máy tính có nhiều tài khoản, ta muốn chỉ định 1 tài khoản bất kì, khi máy tính khởi động là tự động log-on tài khoản đó, làm như sau :**

Ta dùng quyền admin để cấu hình

Run (phím Windows + R) -> control userpasswords2



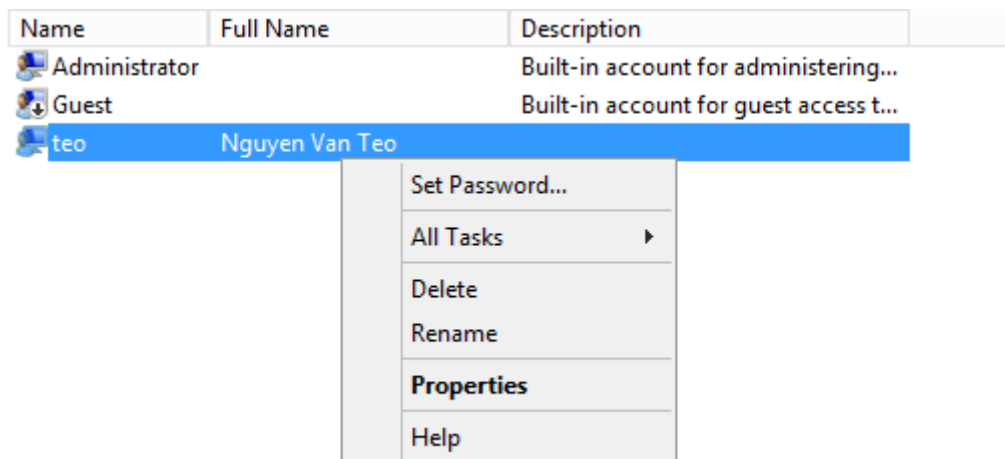


User Accounts

Ta thấy có dấu check: User must enter a user name and password to use this computer: người dùng phải điền username, pass để sử dụng.

Bỏ check -> **apply** : xuất hiện hộp thoại, ta chỉ định tài khoản bất kì để nó đăng nhập tự động. Sau đó Restart để kiểm tra.

**Nếu User quên pass mà không còn cách nào để đăng nhập, ta phải dùng set password**



Set Password


Xuất hiện hộp thoại cảnh báo sẽ bị mất dữ liệu



Name	Full Name	Description	Actions
Administrator		Built-in account for administering...	Users ▲
Guest		Built-in account for guest access t...	More Actions ►
teo	Nguyen Van Teo		teo ▲
			More Actions ►

Set Password for teo



Resetting this password might cause irreversible loss of information for this user account. For security reasons, Windows protects certain information by making it impossible to access if the user's password is reset.

This data loss will occur the next time the user logs off.

You should use this command only if a user has forgotten his or her password and does not have a password reset disk. If this user has created a password reset disk, then he or she should use that disk to set the password.

If the user knows the password and wants to change it, he or she should log in, then press CTRL+ALT+DELETE and click Change Password.

For additional information, click Help.

Proceed

Cancel

Help

Vậy tại sao khi reset password lại có thể bị mất dữ liệu ?

Đối với những dữ liệu được mã hóa (sử dụng password để mã hóa) vì vậy nếu có password mới thì không thể giải mã được các dữ liệu đã được mã hóa trước đó. Còn khi ta đổi 1 cách hợp lệ (Ctrl + Alt + Del -> Change Password) thì sẽ có quá trình chuyển giao giữa pass mới và pass cũ => không mất dữ liệu.

### Các lệnh liên quan tới User và Group

- **Thêm user:** net user <user name cần tạo> <password> /add
- vd: net user hoang 123 /add
- **Xóa user:** net user <user name cần xóa> /del
- **Reset password:** net user <user name> <password mới>
- **Liệt kê các tài khoản:** net user
- **Xem thông tin chi tiết về user:** net user <user name>

Administrator: C:\Windows\system32\cmd.exe

```

Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net user teo
User name                teo
Full Name                Nguyen Van Teo
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        7/17/2014 7:39:46 AM
Password expires         Never
Password changeable      7/17/2014 7:39:46 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               7/19/2014 7:31:10 AM
Logon hours allowed      All
  
```

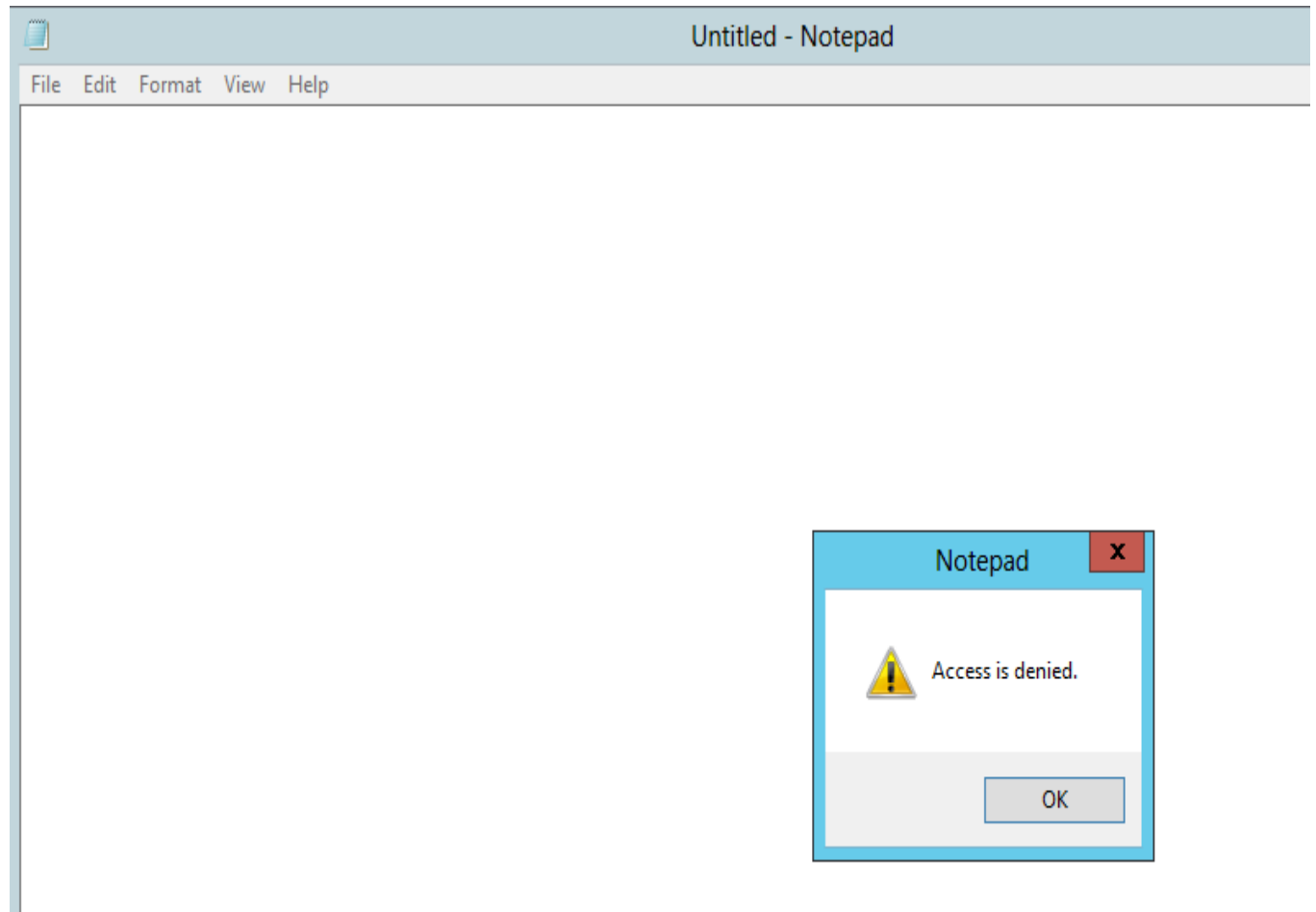
Net User

## Ví dụ về các sự cố:

### Vấn đề gặp phải khi Reset Password:

User Teo: tạo file teo.txt, điền nội dung bất kì vào file. Properties teo.txt, chọn Advance. Check vào **Encrypt contents to secure data** ( mã hóa dữ liệu, chỉ có owner mới đọc được, ngay cả admin cũng không thể) -> OK

Sau đó reset password của user Teo: truy cập vào teo.txt lập tức bị **Access is denied**.



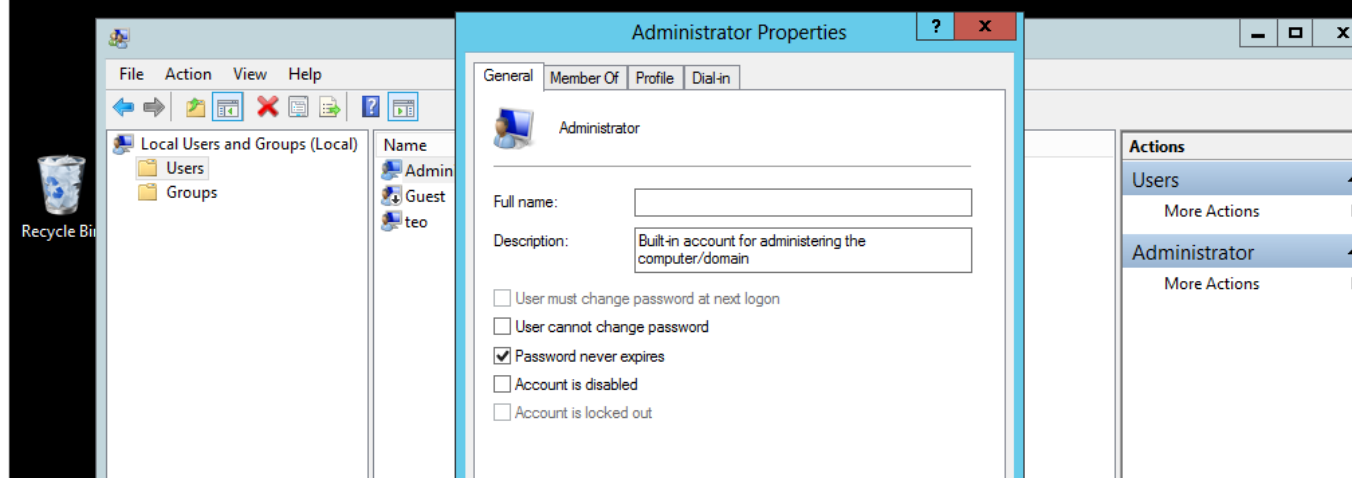
Access is denied

Đổi lại pass cũ: đọc file bình thường.

### Vấn đề gặp phải khi Administrator bị disable:

Account Administrator bị user Teo phá và disable ( đã add Teo vào nhóm Administrators). Vậy làm sao để Administrator có thể tự enable lại.

Trường hợp này, ta phải sử dụng giao diện Safe Mode ( các bạn tự tìm hiểu giao diện này). Ở giao diện này tài khoản Administrator dù bị disable vẫn có thể đăng nhập .Thử check vào password never expires.



Safe Mode

Restart và thấy Administrator có thể đăng nhập.


## 8. Thuộc tính user and group

Chuẩn bị:

1 máy server 2012: 2012may1.


### Thuộc tính của user:

dsa.msc -> chọn user và Properties -> **Tab General** : lưu trữ thông tin user (mail, address, v.v)

thuoc tinh user va group 1  
Tab General

**Tab Address** cũng tương tự

### Tab Account

thuoc tinh user va group 2  
Tab Account


ta thấy 2 kiểu log-on của hệ thống

User logon name: KT1@tuhocmang.com (kiểu UPN)

User logon name (Pre-2000): tuhocmang\KT1 (NetBios Name)

Thuộc tính: Logon Hours (giờ logon) chỉ định thời gian user được logon, mặc định là 24/24.

Chọn **Logon Hours**


thuoc tinh user va group 3  
Logon Hours

**Logon Permitted**: cho phép log on

**Logon Denied**: cấm logon


Để chỉ định thời gian logon thì ta bấm Logon Denied để xóa trắng rồi dùng chuột khoanh vùng rồi chọn Logon Permitted.

Ví dụ: ta chỉ định thời gian log on: 7hAM -> 5hPM thứ 2 đến thứ 7.

thuoc tinh user va group 4  
Logon Hours


**Log on To**: Chỉ định user được phép log on vào máy trạm nào, mặc định là trên tất cả workstation thì user đều có quyền log on

Để cô lập vị trí thì ta có thể chỉ định computer cụ thể (vd ta add: 2012may2).


thuoc tinh user va group 1 5  
Logon Workstation

Trên đây là những thuộc tính thường dùng, ngoài ra còn thêm thuộc tính Member Of và Organization v.v.

Để cấu hình cùng lúc các User thì ta chọn KT1 rồi sau đó bấm phím " Ctrl" để chọn thêm các user khác rồi Properties.

thuoc tinh user va group 6  
cấu hình nhiều user

Sau đây, ta sẽ bàn về Group. Chọn container " Users" -> New Group

thuoc tinh user va group 7  
tạo Group

Khi tạo Group trên Domain ta phải khai báo thêm 2 thông tin: **Group scope** và **Group Type**.

**Group Type** : gồm 2 loại Security, Distribution.

Thì như đã biết mục đích của việc tạo group là để quản lý, thay vì phân quyền cho từng user cho file server.

**Security**: Group loại này cho phép ta có thể phân quyền theo group,

Ngoài ra còn có chức năng phân bổ Mail: khi sử dụng Mail Exchange, ta muốn gửi cho cả group thay vì phải nhập tên từng user (ở phần "To").

**Distribution:** chỉ có chức năng phân bổ mail, không thể phân quyền.

**Group Scope** ( phạm vi của group) gồm 4 loại: Local, Domain Local, Global, Universal.



thuộc tính user và group 7b

Tóm tắt về group scope

Trong môi trường local, Local group chỉ chứa các local user (ở Domain thì dùng Restricted Group Policy để add các nhóm khác vào Local Group).

Ở Domain có khái niệm "Group Nesting" (lồng group) nghĩa là một Group này có thể là thành viên của group khác (Member Of).

### Lưu ý:

Universal Group: có thể sử dụng ở mọi domain trong một forest (log-on, truy cập tài nguyên v.v). Universal group và các thành viên chứa trong nó được lưu trong Global Catalog (GC). Tất cả những sự thay đổi trong Universal group đều được "replicate" đến các Global Catalog server trong forest.

Global Group, Domain local: chỉ có ảnh hưởng trong cùng domain.

Global Group và Domain local group cũng được "replicate" đến các GC trong forest nhưng các thành viên bên trong thì không.

( Vd: Global group A chứa user B và Global group C thì B, C không được "replicate" khi có sự thay đổi, nó chỉ "replicate" duy nhất các thuộc tính liên quan đến A ).

Link tham khảo: <http://blogs.msmvps.com/acefekay/2012/01/06/using-group-nesting-strategy-ad-best-practices-for-group-strategy/>

Group scope: [http://technet.microsoft.com/en-us/library/cc755692\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc755692(v=ws.10).aspx)

Như mình đã đề cập ở các bài trước, Group giúp cho HDH dễ dàng hơn trong việc quản lý, liệt kê các quyền trong ACL (access control list). Nếu có 300 user, thay vì phải liệt kê ra các quyền của 300 user (hay nói đúng hơn là 300 SID), "performance" cho việc liệt kê sẽ giảm.

Một vấn đề nữa khuyến cáo ta nên sử dụng group: Khi người dùng nghỉ việc, thường thì ta sẽ disable tài khoản đó, 1 số khác sẽ xóa hẳn tài khoản, lúc này trên ACL vẫn tồn tại SID của user đó ( không có User Name vì tài khoản đã bị xóa), lúc này ta phải xóa các SID trong ACL.

**Organization Unit (OU):** ở phần 1 mình đã nói sơ về OU, phần này sẽ nói thêm.

OU giúp cho chúng ta:

+ Tổ chức Domain dạng phân cấp( hình cây): Công ty có Ban Giám Đốc, rồi Các Phòng Ban từng phòng ban có các user. Trong AD ta có thể biểu diễn như thế bằng OU.

+ (Delegate Control: Ủy quyền quản lý các đối tượng trên domain cho user khác). Trong hệ thống lớn, ta phải giao bớt quyền cho nhân viên khác, nhưng ta không thể giao nhân viên quyền Administrator mà chỉ nên giao quyền để quản lý từng OU. (User không cần quyền admin, có thể dùng RSAT để quản lý OU)

Phải chuột vào tuhocmang.local -> New -> Organization Unit



thuộc tính user và group trong domain 9

tạo OU

Nhập trên OU



thuộc tính user và group trong domain 10

Tạo OU

Ta thấy có dấu check: Protec container from accidental deletion: bảo vệ, không cho xóa. -> OK

Phải chuột " Công ty A" -> New -> Organization Unit: tạo OU Nhân su và KeToan.





thuộc tính user và group trong domain 11


OU

Do là mô hình cây nên nếu muốn đối tượng nào làm "cha" thì chọn đối tượng đó rồi New.

Để chuyển đổi tượng (user, group, computer) từ OU này sang OU khác, ta chọn Move

thuộc tính user và group trong domain 12  
Move User, Group

thuộc tính user và group trong domain 10  
Move

thuộc tính user và group trong domain 14  
Move

Vào OU NhanSu tạo user Ns2, Ns2.

### Cấu hình Delegate Control:


Mặc định user chỉ được đọc cấu hình trong Active Directory Users and Computers (ADUC).

#### Tình huống 1:

Ta có nhu cầu ủy nhiệm user KT1 có quyền quản lý user, group trong phạm vi OU KeToan.

Chuột phải vào OU kế toán -> Delegate Control -> Next


Users or Groups: chỉ định user hoặc group mình cần giao quyền : Add -> chọn KT1

thuộc tính user và group trong domain 10  
Delegate Control OU

#### Next

**Tasks to Delegate:** các tác vụ ta muốn ủy nhiệm: Windows xây dựng sẵn các quyền ( **common tasks**) hoặc ta có thể tùy chỉnh thêm ( **custom task**)

Ở đây ta chọn "Create, delete and manage user account" và "Create, delete and manage Group"

thuộc tính user và group trong domain 16  
Delegate Control OU

#### Next -> Finish.

**Test:** Logon user KT1 "Reset password" KT2 thành công.


#### Tình huống 2: Cấu hình NS1 toàn quyền trên OU NhanSu.

Làm các bước đầu như tình huống 1

**Tasks to delegate:** ta nhận thấy common tasks thì không đủ toàn quyền, ta chọn custom task -> Next


**Active Directory Object Type:** Chọn loại đối tượng nào

Ta chọn: this folder, existing ..... : nghĩa là áp cho các loại đối tượng đang tồn tại và áp đặt lên các đối tượng được tạo về sau.

thuộc tính user và group trong domain 17  
Delegate Control OU

#### Next

**Permission:** chọn full control

thuộc tính user và group trong domain 18  
Delegate Control OU

#### Next -> Finish.

#### Tình huống 3:

Ns1 không có quyền trong OU KeToan nhưng vẫn nhìn thấy các đối tượng trong OU KeToan, ta muốn chỗ nào nó không có quyền thì không cho thấy.

Chọn OU KeToan -> Properties : Ta thấy có 3 thuộc tính (Tab) nhưng thực ra có nhiều tab, ta phải làm cho nó hiển thị

Trong giao diện **ADUC** -> **View** -> **Advance Feature** để hiển thị.

Properties OU Ketoan -> Tab Security

Tab này liệt kê những quyền của user đối với OU.

Nếu muốn bỏ quyền Delegate Control đối với user nào thì remove user đó trong tab Security.

Để không cho nhìn thấy thì ta chỉ cần add user/Group rồi chọn Deny – Full Control.



thuộc tính user và group trong domain 20



thuộc tính user và group 21

**Kết quả:** Log on user NS1 không còn thấy OU KeToan.

**Tình huống 4:**

Xóa các OU trong ADUC.

Do có dấu check trong khi tạo OU để bảo vệ OU chống xóa nhầm, nên muốn xóa ta phải bỏ check

Tab Object -> bỏ check.



thuộc tính user và group 22

## 9. NTFS Permission

Khi xây dựng File server để user lưu trữ dữ liệu thì ta có nhu cầu thiết lập các quyền hạn, chức năng liên quan đến dữ liệu. Microsoft cung cấp cho ta bộ quyền NTFS để thiết lập quyền trên dữ liệu đối với user

Yêu cầu: dữ liệu phải được lưu trữ trên phân vùng có định dạng NTFS.

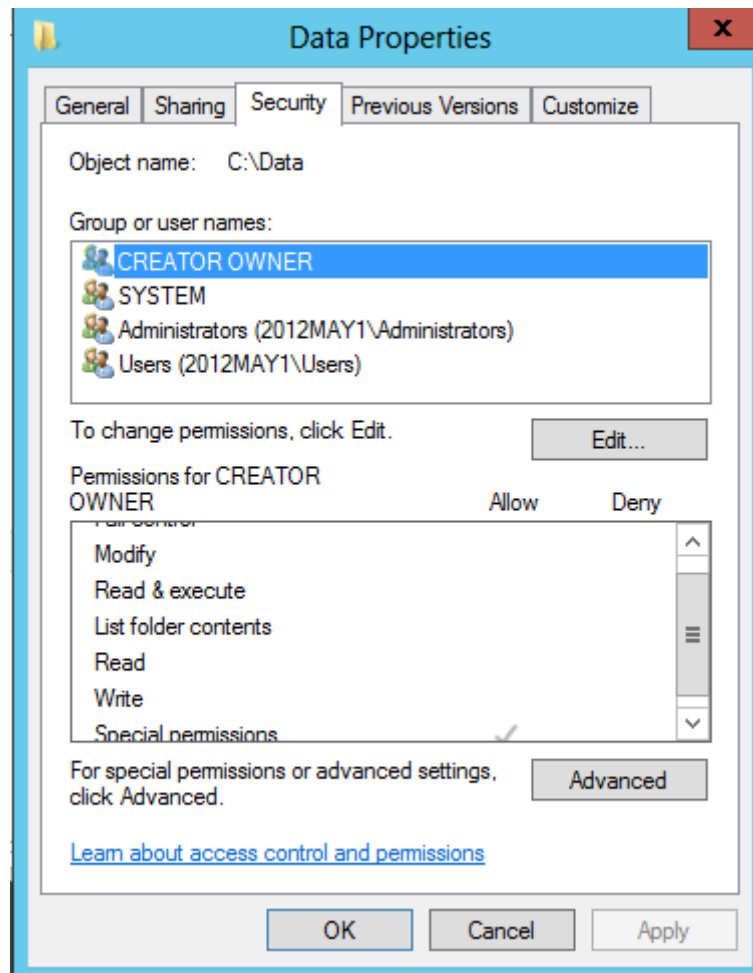
Nếu phân vùng đang ở định dạng Fat 32 thì ta dùng lệnh sau để chuyển từ định dạng Fat32 sang NTFS.

start -> run -> cmd

convert [drive]: /FS:NTFS

Vd: **convert D: /FS:NTFS** (lưu ý chuyển từ NTFS sang FAT, FAT32 dùng lệnh này không được).

Tạo Folder bất kì, chọn Properties, Tab Security: đây là giao diện của bộ quyền NTFS (còn gọi là ACL: Access Control List).



ACL

Giao diện gồm 2 phần:

- Đối tượng cần phân quyền.
- Các permission tương ứng.

NTFS permission gồm có các đặc tính sau:

- **Tính thừa kế:** quyền của folder cha thế nào thì khi tạo folder con sẽ có quyền tương tự.
- **Tác động lên cả file và folder.**
- **Tác động lên Network Access (truy cập qua mạng) và Local Access.**

NTFS permission gồm 2 nhóm chính: Standard permission và Special permission

Standard permission gồm 6 bộ quyền



– **Read**: cho phép user đọc nội dung file.

– **List folder contents**: liệt kê nội dung folder (user có thể mở folder để xem có các file, sub folder nào trong đó).

– **Read and execute**: Có thể đọc nội dung các file ( file \*.doc, ppt. xls v.v) và thực thi các file nếu file đó là chương trình (.exe, .bat v.v).

\* Khi phân quyền user thì ta nên cho cả 3 quyền này.

– **Write**: chỉnh sửa, tạo mới dữ liệu.

+ Nếu user có quyền write trên file thì user có thể chỉnh sửa dữ liệu, nếu là folder thì có thể tạo mới các đối tượng trong folder, chép dữ liệu vào folder. Nhưng không thể xóa các đối tượng.

– **Modify**: bằng các quyền ở trên gộp lại và thêm quyền delete ( đọc, chỉnh sửa, xóa các đối tượng).

– **Full control**: là Modify và cộng thêm:

+ Quyền: change permission (là quyền được cho phép thiết lập lại các bộ quyền).

+ Quyền: Take Ownership

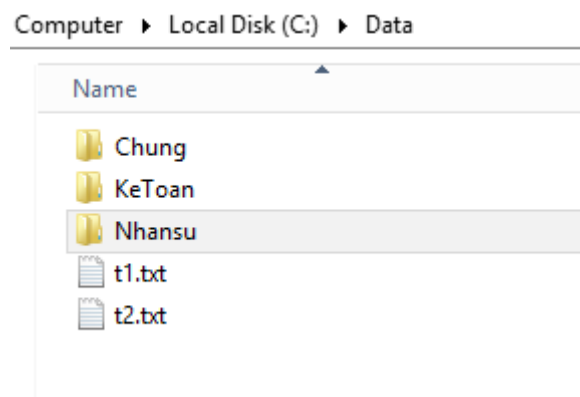
Ta sẽ làm 1 ví dụ về standar permission:

Tạo 4 user: KT1, KT2 thuộc group KeToan. NS1, NS2 thuộc group NhanSu.

Vào ổ đĩa C tạo folder Data.

Trong Data tạo 3 folder Chung, KeToan, NhanSu, và 2 file t1.txt và t2.txt (nội dung tùy ý).

Mỗi folder con tạo 1 file txt (cũng nội dung tùy ý).



Folder

Yêu cầu: thiết lập quyền cho các folder.

Data: cho group KeToan, NhanSu có quyền Read and execute.

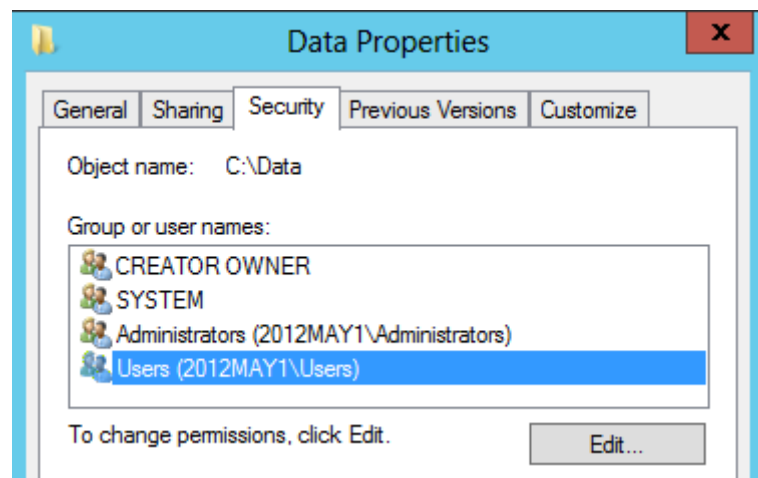
Chung: tất cả có quyền full.

Ketoan: chỉ group KeToan có quyền full, cấm group NhanSu.

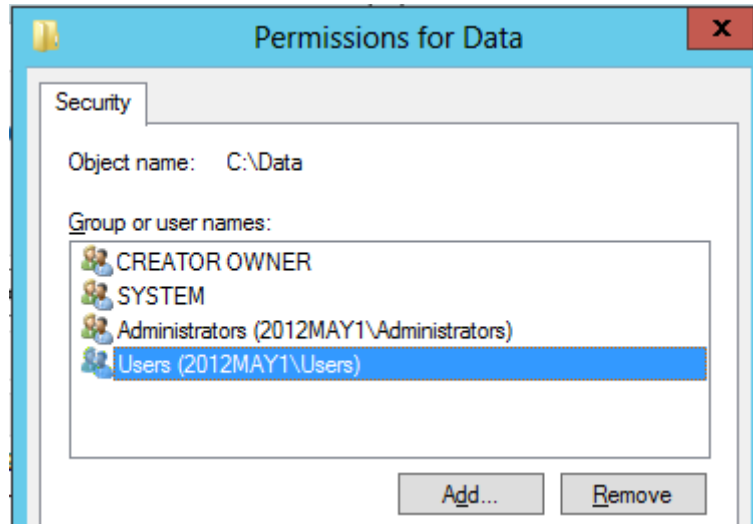
Nhansu: chỉ group NhanSu có quyền full, cấm group KeToan.

\* Lưu ý: khi thực hiện phân quyền phải thực hiện từ folder cha di xuống.

Do folder Data chỉ cho group KeToan và NhanSu truy cập nên ta phải xóa group Users (Users đại diện cho tất cả user, được kế thừa từ ổ C), chọn Edit



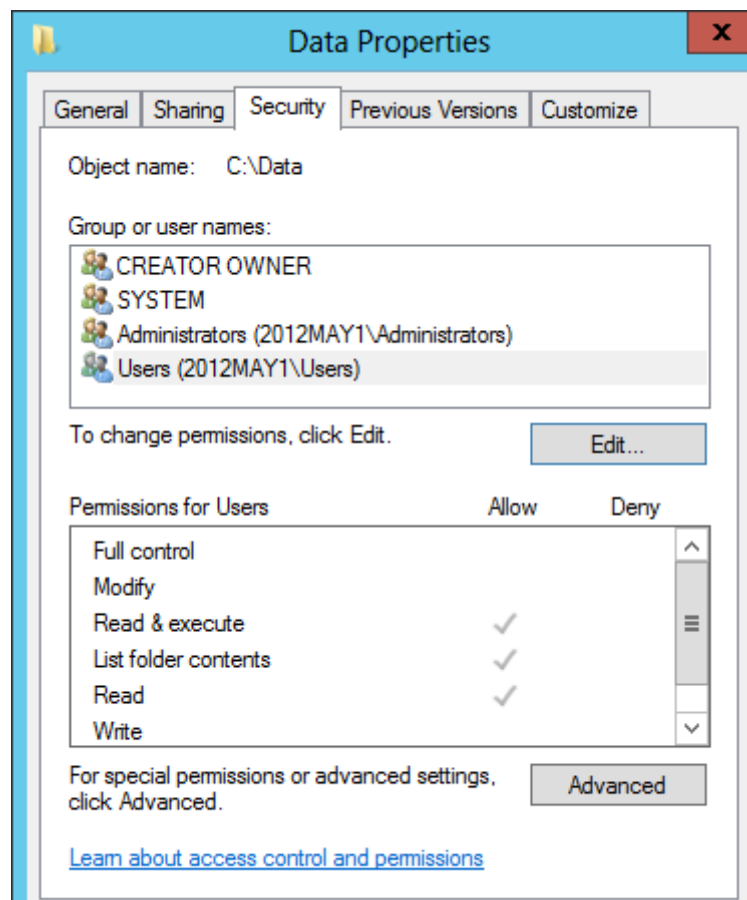
Chọn Users -> Remove.



Xuất hiện thông báo: Không thể remove group Users vì group này đang chịu quyền thừa kế từ folder cha



Để gỡ bỏ quyền thừa kế: Chọn Advance



Chọn Disable inheritance

Name: C:\Data

Owner: Administrators (2012MAY1\Administrators) Change

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

	Type	Principal	Access	Inherited from	Applies to
	Allow	SYSTEM	Full control	C:\	This folder, subfolders and files
	Allow	Administrators (2012MAY1\A...	Full control	C:\	This folder, subfolders and files
	Allow	Users (2012MAY1\Users)	Read & execute	C:\	This folder, subfolders and files
	Allow	Users (2012MAY1\Users)	Special	C:\	This folder and subfolders
	Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only

Add

Remove

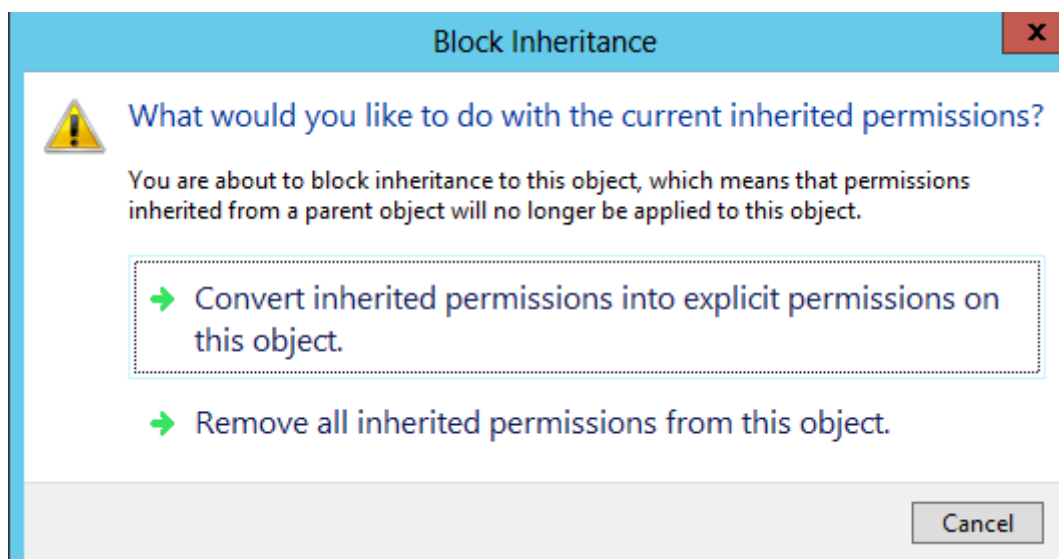
View

Disable inheritance

☐ Replace all child object permission entries with inheritable permission entries from this object

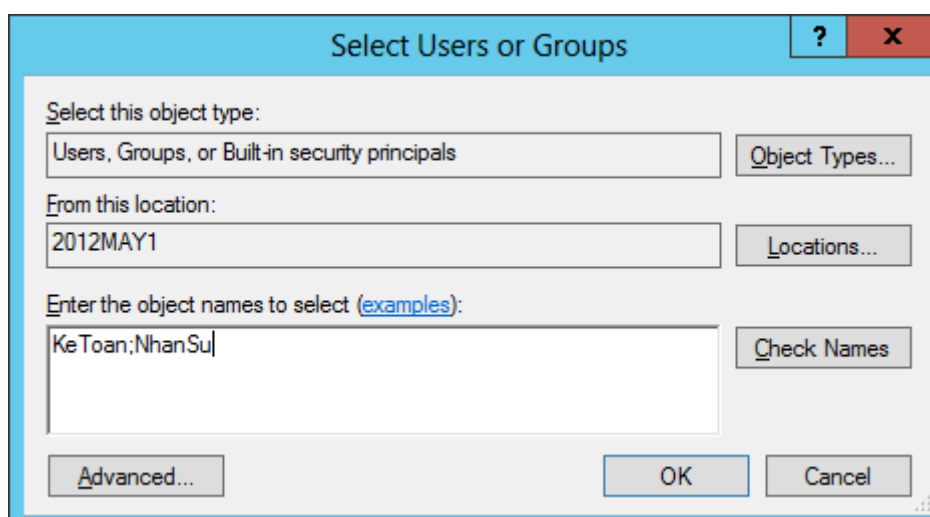
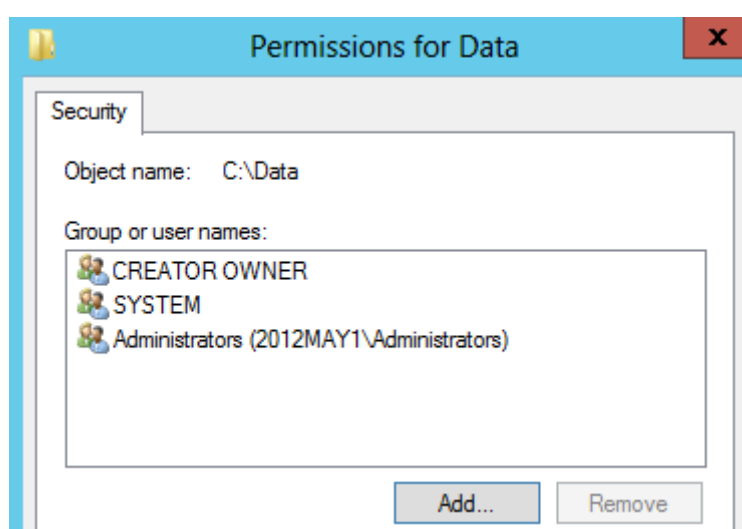
Xuất hiện bảng thống báo:

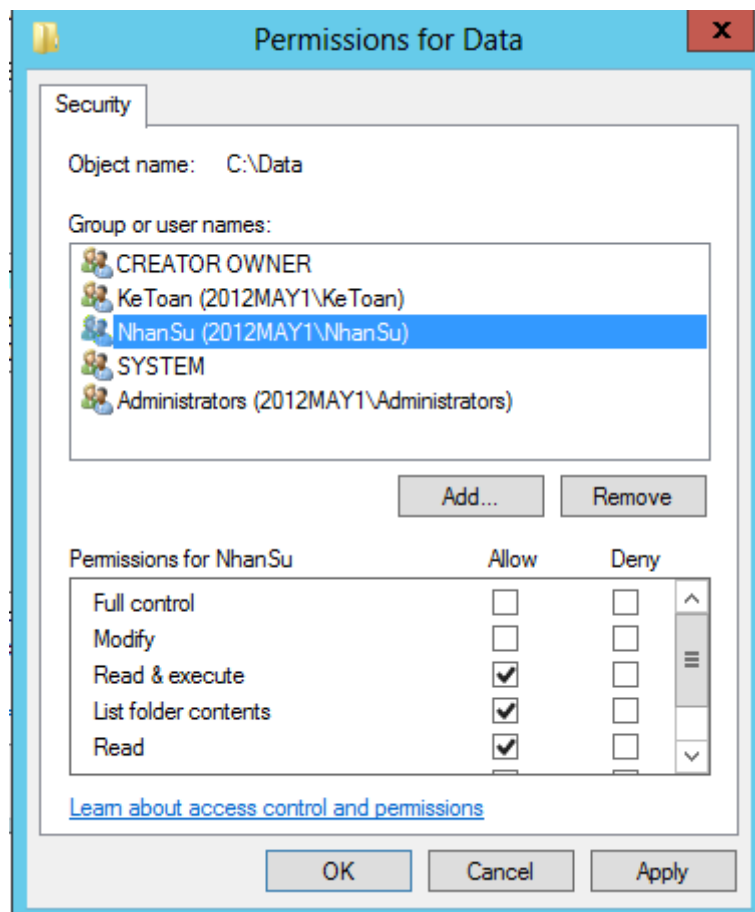
- Remove all inherited permission from this object: xóa tất cả các quyền thừa kế, các đối tượng trong ACL kể cả các group hệ thống (Creator Owner, System, Administrators).
- Convert inherited permission into .... : giữ lại các đối tượng ở folder cha và folder con, nếu folder cha có group Ketoan thì folder con cũng có group Ketoan (khuyến nên dùng).



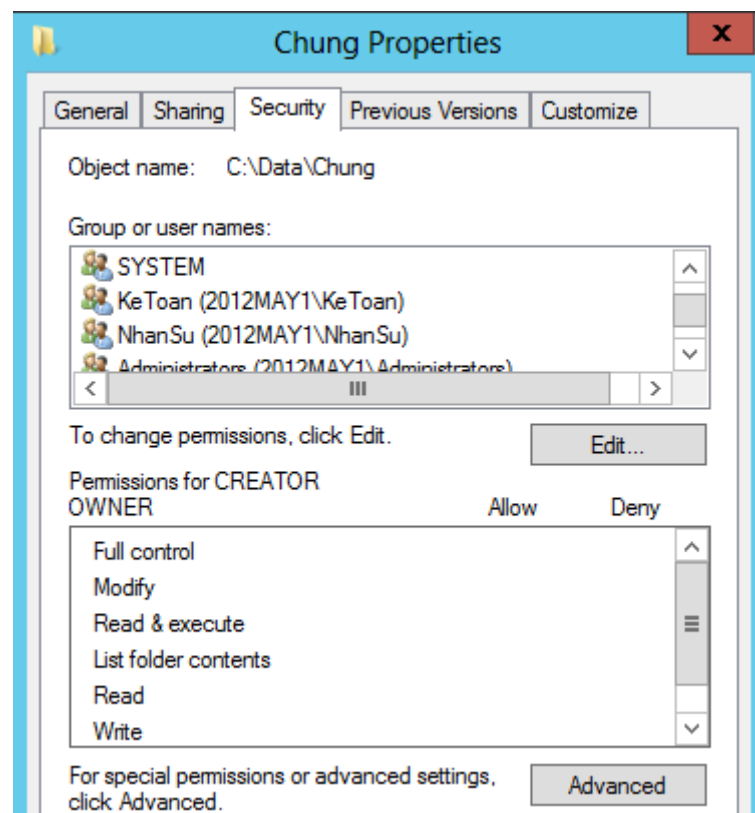
=> Remove thành công.

Folder Data: add group KeToan, NhanSu và cho quyền Read and Execute.

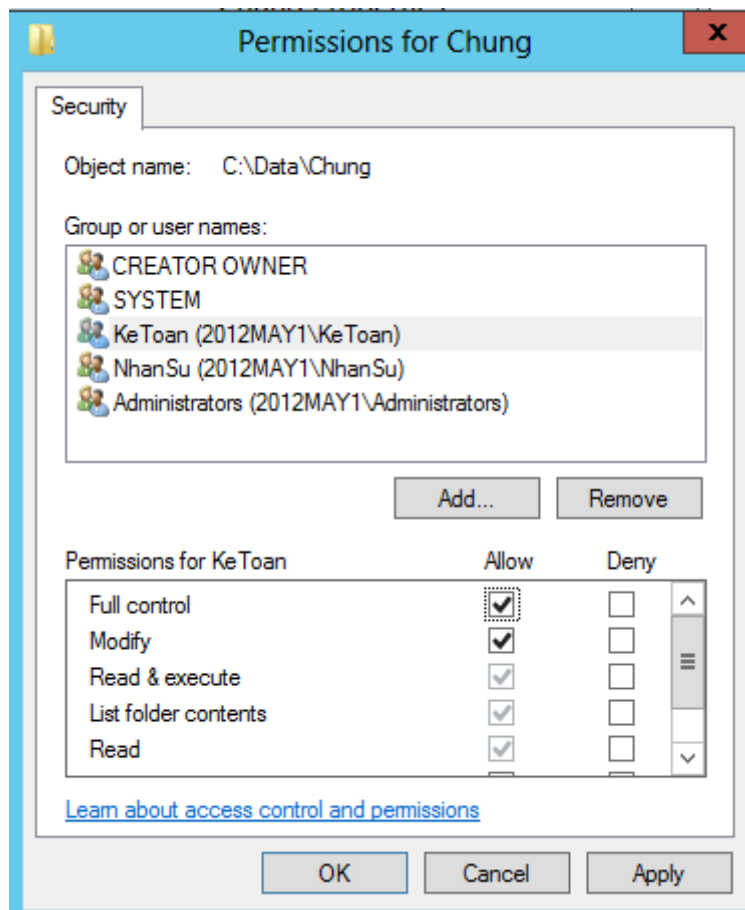




Folder Chung thừa kế các quyền và các đối tượng thì folder Data.



Chọn Full Control cho Group Ketoan, NhanSu

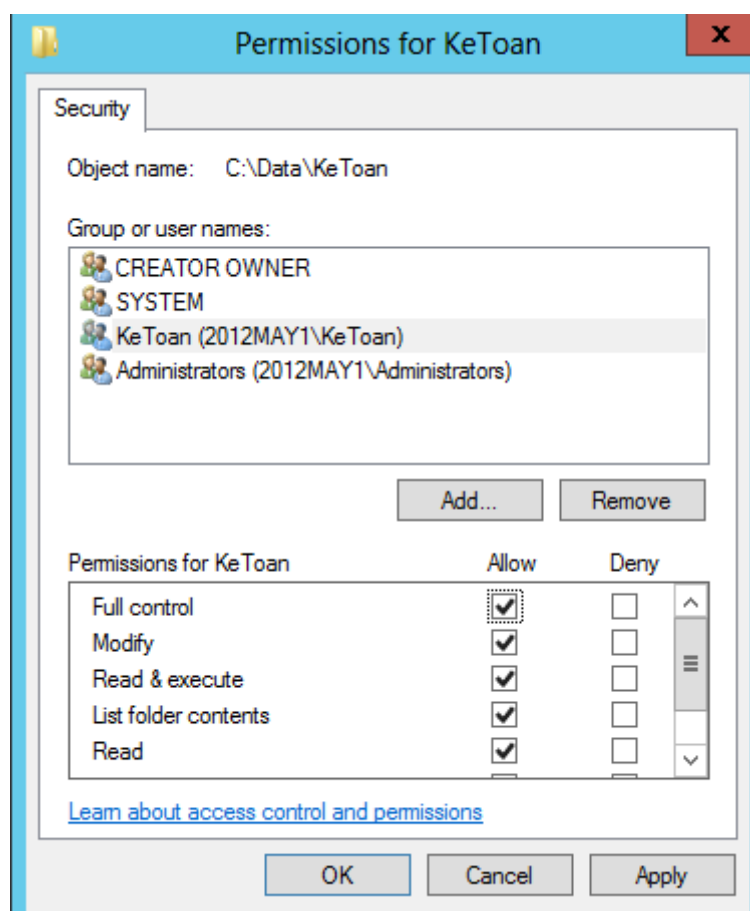


Folder Ketoan: chọn Full Control cho Ketoan.

Cách cấm group NhanSu (2 cách)

- Không đưa đối tượng vào bảng ACL (bỏ quyền thừa kế và xóa group NhanSu).
- Cho quyền deny đối tượng

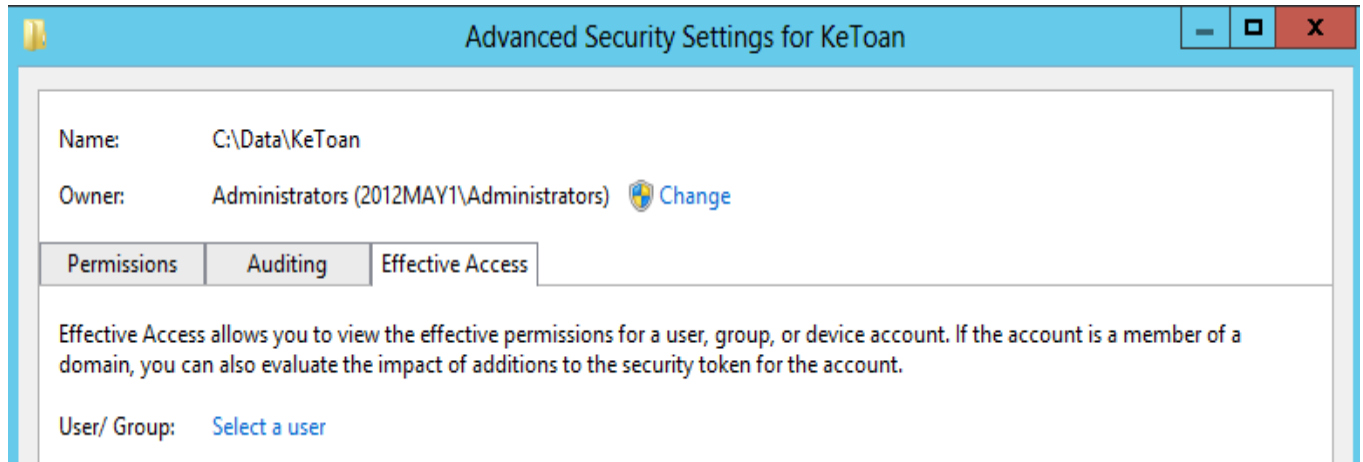
\* (hạn chế deny cho đối tượng group vì nếu xảy ra trường hợp: "NS1" có nhu cầu vào folder Ketoan làm việc thì ta phải cấp quyền Read cho NS1 nhưng do group NhanSu bị deny nên deny ưu tiên hơn => NS1 không có quyền. Còn dùng cách trên thì chỉ cần add thêm NS1 rồi cấp quyền Read là xong ).



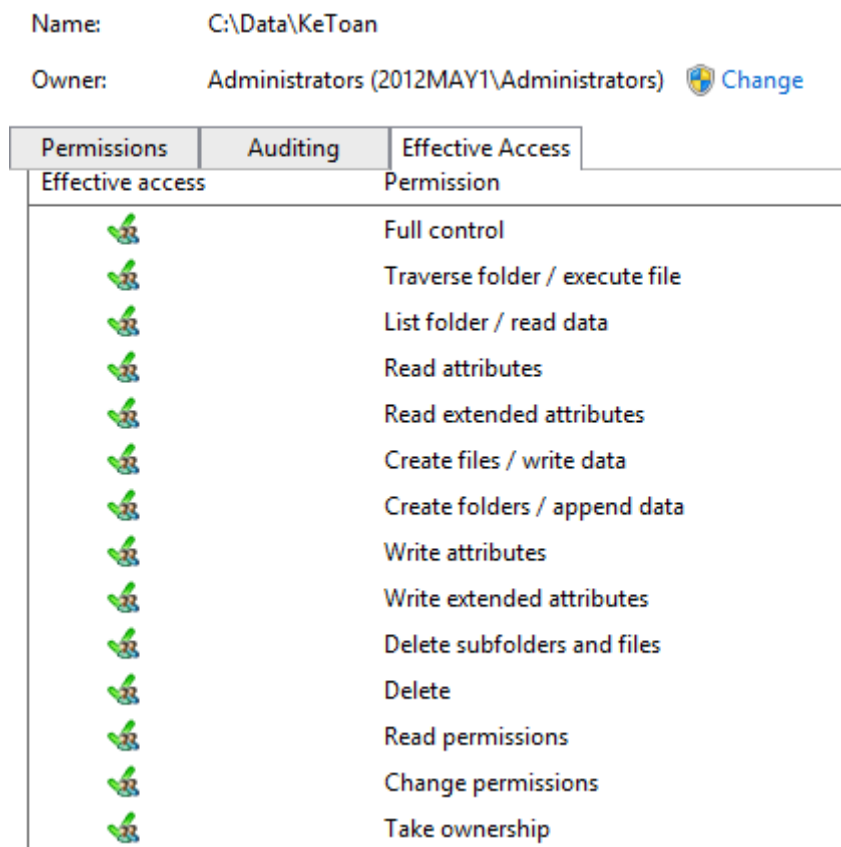
## Folder Nhansu làm tương tự

### Cách Test quyền cho các user:

Cách 1 (thực tế thường dùng): Chọn folder KeToan -> Tab security -> Advance -> Tab Effective Access



Select a user: gõ vào KT1 -> view effective access



Gõ vào User: NS1

View effective access

Effective access	Permission	Access limited by
✗	Full control	File Permissions
✗	Traverse folder / execute file	File Permissions
✗	List folder / read data	File Permissions
✗	Read attributes	File Permissions
✗	Read extended attributes	File Permissions
✗	Create files / write data	File Permissions
✗	Create folders / append data	File Permissions
✗	Write attributes	File Permissions
✗	Write extended attributes	File Permissions

Cách 2: Đăng nhập vào từng user để test (!!!).

### Các lưu ý khi phân quyền:

- Phân quyền từ folder cha đến folder con.
- Nếu 1 user nằm ở 2 group, 1 group bị Deny, và 1 group có quyền Read thì user đó sẽ bị quyền Deny.
- Nếu 1 user nằm ở 2 group thì group nào có quyền lớn hơn thì user sẽ có quyền đó ( group quyền Read và group quyền Modify thì user có quyền Modify).


### Tình huống 1:

Đối với Folder Ketoan, group Ketoan có quyền full control, vì thế các user trong group kế toán có thể xóa tài nguyên của nhau. Ta có nhu cầu KT1 không được phép chỉnh sửa, xóa tài nguyên của người khác, chỉ được chỉnh sửa, xóa tài nguyên của mình tạo ra. Để phân quyền chi tiết như thế thì ta phải dùng Special permission.

**Special permission** là sự chi tiết hóa các quyền của Standar permission.

Giao diện Special permission: Properties folder Data -> tab security -> Advance, chọn group Ketoan Edit

Name: C:\Data\KeToan

Owner: Administrators (2012MAY1\Administrators)  [Change](#)





Permissions

Auditing

Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

	Type	Principal	Access	Inherited from	Applies to
	Allow	CREATOR OWNER	Full control	None	Subfolders and files only
	Allow	SYSTEM	Full control	None	This folder, subfolders and files
	Allow	KeToan (2012MAY1\KeToan)	Full control	None	This folder, subfolders and files
	Allow	Administrators (2012MAY1\A...	Full control	None	This folder, subfolders and files

Add

Remove

Edit

Chọn Show basic permission (đây là giao diện của special permission)



Principal: KeToan (2012MAY1\KeToan) [Select a principal](#)

Type:

Applies to:

---

Advanced permissions: [Show basic permissions](#)

<input checked="" type="checkbox"/> Full control	<input checked="" type="checkbox"/> Write attributes
<input checked="" type="checkbox"/> Traverse folder / execute file	<input checked="" type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input checked="" type="checkbox"/> Delete subfolders and files
<input checked="" type="checkbox"/> Read attributes	<input checked="" type="checkbox"/> Delete
<input checked="" type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input checked="" type="checkbox"/> Create files / write data	<input checked="" type="checkbox"/> Change permissions
<input checked="" type="checkbox"/> Create folders / append data	<input checked="" type="checkbox"/> Take ownership

☐ Only apply these permissions to objects and/or containers within this container

[Clear all](#)

## 14 quyền special permission

Special Permission gồm 14 quyền:

**Full control:** toàn quyền, giống Full control của standar permission.

**Traverse folder/ execute file:** Quyền thực thi file + quyền đi vào folder, ta chỉ vào được khi dùng lệnh "cd". VD: **cd C:\Data** nếu ta sử dụng quyền Traverse folder/ execute cho folder Data).

**List folder / Read data:** Đi vào thư mục và đọc dữ liệu trên thư mục đó.

**Read Attributes:** đọc thuộc tính folder và file ( Read only, Hidden v.v).

**Read Attributes:** đọc thuộc tính mở rộng (Archive, Encrypt).

**Create file/ Write data:** tạo file và ghi, chỉnh sửa dữ liệu.

**Create folder/ Append data:**

– Cho phép tạo folder

– Ghi ghi dữ liệu vào phía cuối file ( ghi nối tiếp) , chứ không xóa, chỉnh sửa phần dữ liệu sẵn có (chỉ áp dụng cho file).

**Write Attributes:** Cho phép thay đổi các thuộc tính của file, folder (read-only, hidden).

**Write Extended Attributes:** Cho phép chỉnh sửa các thuộc tính mở rộng của file, folder. Thuộc tính mở rộng được xác định bởi các chương trình (program), các chương trình khác nhau có các thuộc tính mở rộng khác nhau.

**Delete Subfolders and files:** Xóa các folder con và các file.

**Delete:** Cho phép xóa tài nguyên (folder, subfolder, file).

**Change permission:** Cho phép thay đổi các quyền hạn đối với file, folder.

Read permission: cho phép user, group thấy các quyền hạn mà ta đã cấu hình.

**Take Ownership:** Cho phép lấy quyền sở hữu file, folder của người khác.

Ngoài ra ta còn có 7 thành phần có thể liên kết với 14 bộ quyền special permission

Principal: Teo (2012MAY1\Teo) [Select a principal](#)

Type: Allow

Applies to: This folder, subfolders and files

Basic permissions:

- ☐ This folder only
- ☐ This folder, subfolders and files
- ☐ This folder and subfolders
- ☐ This folder and files
- ☐ Subfolders and files only
- ☐ Subfolders only
- ☐ Files only
- ☐ Read & execute
- ☐ List folder contents
- ☐ Read
- ☐ Write
- ☒ Special permissions

Applies to

**This folder only:** chỉ áp dụng quyền vào folder này ( các subfolder, file không bị áp đặt)

**This folder, subfolders, files:** áp lên folder, các folder con và các file trong các folder.

**This folder and subfolders:** áp lên folder và subfolders.

**This folder and files:** áp lên folder và các file ( subfolder không bị áp quyền).

**Subfolder and files only:** chỉ subfolder và các file bên trong mới bị áp đặt quyền.

**Subfolder only:** chỉ có quyền trên subfolder.

**Files only:** chỉ áp đặt quyền trên các file.

**Để thực hiện như ví dụ trên, ta chỉ cần cho group Ketoan quyền như hình:**

Principal: KeToan (2012MAY1\KeToan) [Select a principal](#)

Type: Allow


Applies to: This folder, subfolders and files

Advanced permissions:

<input type="checkbox"/> Full control	<input type="checkbox"/> Write attributes
<input checked="" type="checkbox"/> Traverse folder / execute file	<input type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input type="checkbox"/> Delete subfolders and files
<input checked="" type="checkbox"/> Read attributes	<input type="checkbox"/> Delete
<input checked="" type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input checked="" type="checkbox"/> Create files / write data	<input type="checkbox"/> Change permissions
<input checked="" type="checkbox"/> Create folders / append data	<input type="checkbox"/> Take ownership

Trên folder Ketoan, KT1 tạo file KT1.txt. Kiểm tra ta thấy KT2 chỉ có thể đọc KT1.txt

Name: C:\Data\KeToan\KT1\KT1.txt









Owner: KT1 (2012MAY1\KT1)  [Change](#)

Permissions Auditing Effective Access

Effective Access allows you to view the effective permissions for a user, group, or device account. If the account is a member of a domain, you can also evaluate the impact of additions to the security token for the account.

User/ Group: KT2 (2012MAY1\KT2) [Select a user](#)

View effective access

Effective access	Permission	Access limited by
	Full control	File Permissions
	Traverse folder / execute file	
	List folder / read data	
	Read attributes	
	Read extended attributes	
	Create files / write data	
	Create folders / append data	
	Write attributes	File Permissions

Đối với KT1 thì lại có toàn quyền trên folder, file do nó tạo ra. Vậy tại sao lại như thế ?

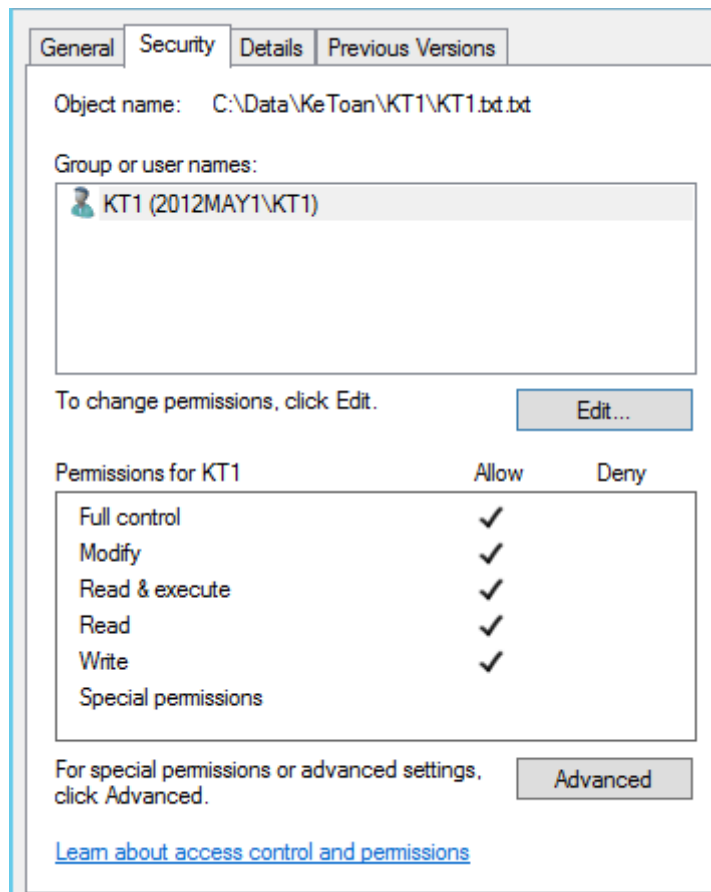
Trước tiên ta phải tìm hiểu về **Group định danh**:

- Là group quy định điều kiện để lấy member (thành viên).
- Bao gồm:
- **Users** (mặc định khi user tạo ra là thuộc group này)
- **Administrators**.
- **System**: group định danh hệ thống (mặc định full control).
- **Creator Owner**: chứa member là những user tạo ra tài nguyên (ai tạo ra tài nguyên thì người đó thuộc nhóm Creator Owner trên tài nguyên đó)

Group Creator Owner có quyền full control. Vì KT1 tạo ra KT1.txt => KT1 có quyền full control trên KT1.txt. Nếu mất Creator Owner thì không thể phân quyền.

## Tình huống 2:

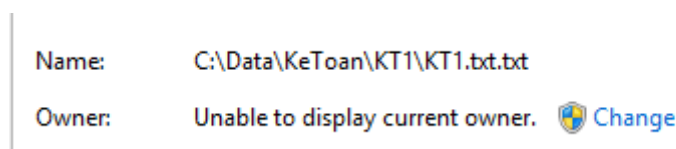
KT1 xóa hết các đối tượng trong tab security trong file KT1.txt



Administrator muốn đọc được KT1.txt thì phải làm cách nào ??

Administrator có 1 quyền rất đặc biệt là: Take ownership (chiếm sở hữu trên tài nguyên), chỉ có group administrators mới có.

Administrator Properties KT1.txt -> Advance



Bấm Change: Chọn group, user muốn chiếm sở hữu.

Lưu ý: Chỉ có Group Administrator có quyền take ownership (các user khác nếu có quyền full control cũng không thể take ownership) bởi vì hệ thống có 1 policy:

**Computer configuration -> Windows Setting -> Security Setting -> Local policy -> User right assignment**

**Take ownership of files or other object (mặc định Administrator).**

**Cách áp permission của 1 folder lên mọi tài nguyên bên trong nó.**

Properties: folder KeToan -> Tab security -> Advance:

Check vào Replace all child object permission entries with inheritable permission entries from this object

# 10. File Server và Share Permission

server2012may1: IP 192.168.1.100/24

server2012may2: IP 192.168.1.101/24

Turn off: windows firewall.

Tạo KT1, KT2 group Ketoan. NS1, NS2 group NhanSu

Tạo Folder Data trong ổ C máy server2012may1.

## File Server (FS)

Nói 1 cách đơn giản, file server là một server dùng để lưu trữ dữ liệu và chia sẻ cho người dùng sử dụng.

Yêu cầu cho FS:

### Hardware:

Ổ cứng (HDD, SSD) lớn, có khả năng chịu lỗi (sẽ đề cập ở các bài sau).

Có ít nhất 1 card mạng online.

### Software:

Nếu FS sử dụng HĐH windows client thì bị giới hạn số kết nối đồng thời

Win XP: cho phép 10 kết nối đồng thời.

Win 7, 8: 20 kết nối (có thể chỉnh registry để tăng kết nối).

Nếu FS sử dụng HĐH họ Server thì có thể nói số kết nối cao hơn (bản Datacenter hỗ trợ tối đa 16777216 kết nối)

Dùng lệnh net config server để xem:

 hình 1

Net config server

\* Khi truy cập vào Server (file server, print server hay remote vào server, v.v) thì các user cần có thêm các license để hợp pháp hóa việc truy cập, license đó gọi là CAL (Client Access License).

( vào đây để tìm hiểu thêm về CAL).

Để File Server (print server v.v) và các Client có thể liên lạc được với nhau thì cả 2 phải đáp ứng các điều kiện sau:

### Về Service:

Mở Start -> Run -> Services.msc

Phải đảm bảo 3 dịch vụ sau phải ở trạng thái (status) running và Startup type: Automatic

– Server

– Workstation

– Computer Browser

Nếu File Server bị disable Server Services, thì client truy cập vào sẽ thấy thông báo:

 tuhocmang2

thiếu Server service

Nếu Workstation service bị disable thì xuất hiện thông báo:

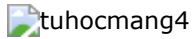
 tuhocmang3

thiếu Workstation service

**Về Firewall:** nếu có firewall thì phải mở port TCP, UDP port 445

**Về Policy:** chỉnh các policy thích hợp (xem phần cuối của bài local group policy)

**Về NIC:** Start -> run -> ncpa.cpl -> Properties biểu tượng network connection trong windows, phải đảm bảo 2 option:



- + Client for Microsoft Network.
- + File and Printer sharing for Microsoft Network.

Đương nhiên, để người dùng có thể truy cập tài nguyên trong File Server ta phải share các tài nguyên đó

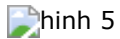
### Cách Share Folder:

Properties Folder -> tab sharing

Ta thấy có 2 cách share tài nguyên

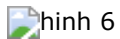
Share (giao diện File Sharing) và Advanced Sharing

Chọn Share:

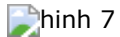


File sharing

Ở giao diện này thì chỉ có 2 quyền: **Read và Read/ Write**



Chọn **Advanced Sharing**:



Check vào share this folder

**Share name:** là trên hiển thị khi người dùng truy cập tài nguyên (ta có thể đặt tên khác để người dùng không thể biết dữ liệu nằm trong folder nào).

### Chọn Permission



Share permission

Đây là giao diện của Share Permission, gồm 3 quyền cơ bản:

- **Read:** đọc, copy dữ liệu. (giống như read/ execute trong NTFS)
- **Change:** = Read + chỉnh sửa, xóa dữ liệu (giống Modify trong NTFS)
- **Full:** toàn quyền (giống full control trong NTFS).

Ta thấy có sự tương đồng giữa Share Permission và NTFS Permission. **Khi 1 Folder vừa sử dụng Share permission và NTFS permission thì quyền áp lên user là giao của 2 bộ quyền trên.**

VD: Share: cho full control, NTFS cho Read/ Execute thì giao của Full và Read => Read.

Share: Read, NTFS: Full => kết quả Read.

Share: Read, NTFS: Write => kết quả là không có quyền nào cả

Và lưu ý rằng: Share Permission chỉ tác động đến người dùng Network Access (\\), không tác động với người dùng local access (ngồi trực tiếp trên máy).

**Mẹo: Khi share folder, để đảm bảo giữ nguyên bộ quyền NTFS thì thực hiện share permission với group Users: allow full control.**

Ta share folder Data.

Cách truy cập tài nguyên:

**Cách 1:** Dùng UNC (Universal naming convention): đường dẫn mạng (hay còn gọi là đường dẫn tuyệt đối)

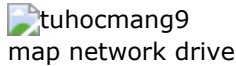
Cú pháp: \\[IP] hoặc [tên server]\Share name : \\192.168.1.100

Nhược điểm: gây khó khăn với người dùng.

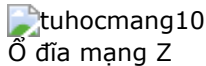
**Cách 2:** Map Share folder thành ổ đĩa mạng trên máy tính (Map Network Drive), ánh xạ ổ đĩa mạng từ share folder trên File Server (thực hiện trên client). Client chỉ cần vào ổ đĩa này và thao tác với dữ liệu.

start -> run -> \\192.168.1.100

Properties -> chọn Map Network Drive

tuhocmang9  
map network drive

Ta check vào Reconnect at sign-in: tự động connect lại khi user đăng nhập lần kế tiếp -> Finish

tuhocmang10  
Ổ đĩa mạng Z

Ta thấy xuất hiện ổ Z

Nếu không thích sử dụng nữa thì chuột phải vào ổ Z -> disconnect.

Cách thứ 2 để tạo Map Network Drive:

Dùng lệnh: **net use [drive] \\[IP File server]\\[tên share folder] /user:[username] [pass]**

VD: net use Z: \\192.168.1.100\data /user:hoang 123.

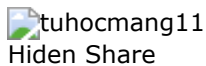
Đăng nhập với username nào thì sẽ có quyền tương ứng với username đó. Nếu không đánh user, pass thì mặc định chứng thực với user đang sử dụng.

(1 ổ đĩa mạng chỉ map được 1 folder)

**Tình huống 1:** Ta không muốn người dùng thấy 1 folder nào đó mà ta đã share. (Hidden Share -Share ẩn).

Trên File server tạo folder QuanTrong. Properties Folder -> Tab Sharing -> Advanced Sharing

Share name: sau tên folder ta thêm dấu "\$" => dấu "\$" để làm ẩn folder.

tuhocmang11  
Hidden Share

Nếu user muốn truy cập thì phải đánh đúng tên

vd: \\192.168.1.100\QuanTrong\$

**System Share:** mặc định hệ thống share ẩn các ổ đĩa, nhằm phục vụ cho các user thuộc group administrator từ xa truy cập (C\$, D\$, E\$ v.v).

Để quản lý Share folder và các user đang truy cập tài nguyên đó ta dùng các tool sau:

Tool 1: Trên File Server : start -> run -> compmgmt.msc (giao diện computer management)

tuhocmang12  
Share Folders

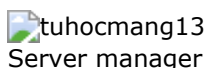
**Shares** : liệt kê các folder đã share.

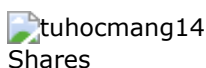
**Sessions:** liệt kê các user đang sử dụng tài nguyên mà ta share.

**Open Files:** Xem user đang truy cập file nào

Công cụ này còn giúp ta share folder bất kì : **Chuột phải Shares -> New Share.**

Tool 2: Mở Server Manager (góc dưới cùng bên trái màn hình) -> File and Storage Service -> Shares

tuhocmang13  
Server manager

tuhocmang14  
Shares

**Tình huống 2:** Khi share folder, user truy cập tài nguyên vào các folder mà user đó không có quyền sẽ bị báo "deny". Ta có nhu cầu đối với những folder mà user không có quyền truy cập thì ta ẩn, không cho hiển thị lên. Ta dùng tính năng Access-Base Enumeration (ABE) để xử lý tình huống

Trong giao diện **Shares** (File and Storage Service), ta chọn folder **Data (cứ chọn folder cha)**

**Phải chuột properties -> Setting -> check vào Enable access-base enumeration.**



hình 15

Access-base enumeration

Kết quả: User chỉ thấy những folder mà mình có quyền Read (hoặc tương đương). Các bạn tự test tình huống này nhé.

Bonus: Giao thức truy cập tài nguyên (SMB) của Microsoft

Ở các phiên bản cũ thì Windows sử dụng NBT (Net Bios Name over TCP/IP) sử dụng các port 137, 138, 139. Đến thời win 2000, XP trở lên thì cung cấp thêm khả năng chạy SMB trực tiếp trên TCP/IP (port 445).

Nếu client không bị cấm xài NetBT, nó sẽ thử kết nối tới server bằng cả cổng 139 và 445 cùng lúc. Nếu có trả lời từ 445, nó sẽ gửi lệnh reset cổng 139, và chỉ tiếp tục sử dụng phiên SMB trên cổng 445. Nếu không có trả lời từ cổng 445, nó sẽ chỉ tiếp tục phiên SMB trên cổng 139 nếu có trả lời từ đó. Nếu cả hai cổng đều không trả lời – dĩ nhiên khỏi nói tiếp.

Nếu client bị cấm xài NetBT, nó sẽ chỉ thử kết nối tới server ở cổng 445. Nếu kết nối có đáp ứng, mọi chuyện sẽ tiếp tục trên cổng này. Nếu không có phản hồi, khỏi nói tiếp (nếu máy chủ file chạy Windows NT 4.0 sẽ bị trường hợp này).

Nếu server không bị cấm NetBT, nó sẽ nghe trên các cổng 137, 138 UDP và các cổng 139, 445 TCP. Nếu bị cấm NetBT, nó chỉ nghe trên cổng 445 TCP.

Các cổng liên quan:

137 UDP/TCP: cho dịch vụ NetBIOS Name Service (netbios-ns), là một phần trong họ giao thức NetBIOS (Network Basic Input/Output System) trên các trạm M\$, sử dụng chủ yếu để ánh xạ giữa hostname và địa chỉ của các trạm trong mạng NetBIOS.

138 UDP: NETBIOS Datagram Service (netbios-dgm), là một phần trong họ giao thức NetBIOS trên các trạm M\$, sử dụng chủ yếu truyền tải dữ liệu hai chiều giữa các trạm trong mạng NetBIOS. Giao thức này cũng được Messenger service sử dụng (lệnh net send ...)

139 TCP: NetBIOS Session Services (netbios-ssn), là một phần trong họ giao thức NetBIOS trên các trạm Microsoft, sử dụng cho chia sẻ file, máy in.

445 TCP, UDP: SMB over TCP , chia sẻ file, máy in

Bạn chỉ nên mở TCP, UDP 445 để đảm bảo vấn đề bảo mật.



# 11. Domain Network

## Chuẩn bị:

Server: 2012may1, 2012may2 (hoặc 1 client chạy window 8). Đặt IP cho 2 máy.

Khi xây dựng 1 hệ thống mạng, quản lý các đối tượng, ta có thể chọn hệ thống mạng Workgroup hoặc Domain (Để nhận biết máy tính đang tham gia mạng Workgroup hay Domain ta vào: run -> sysdm.cpl: nếu có Workgroup thì đang tham gia mạng workgroup).

**Mạng workgroup:** sử dụng khi số máy tính trong hệ thống máy nhỏ, các PC độc lập với nhau (local computer), tài nguyên trên PC nào thì PC đó tự quản lý. Mạng workgroup chỉ tồn tại 1 loại user là local user, local user chỉ có thể log-on, truy cập tài nguyên trên local computer đó.

**Ưu điểm** của loại này là chi phí thấp. Chỉ cần máy tính, cable, switch là có thể xây dựng mạng workgroup.

**Mạng Domain** (domain network) sử dụng khi số máy nhiều.

Ưu điểm quản lý tập trung các dịch vụ, đối tượng. Nhưng tốn chi phí vì cần ít nhất 1 máy làm Domain Controller (DC). Các máy tính client tham gia vào domain thì gọi là workstation (domain member).

Một máy tính khi cài đặt dịch vụ Active Directory (AD) thì sẽ trở thành DC, DC lưu trữ AD Database đảm nhiệm chức năng:

- Quản lý tập trung hệ thống (user được tạo trong AD database có thể log on bất cứ máy nào trong mạng domain, truy cập tài nguyên mà không cần tạo user trên workstation như mạng workgroup).
- Chứng thực user log on, truy cập tài nguyên trong hệ thống (mạng workgroup thì user chứng thực ngay trên local).
- Triển khai Policy tác động lên user, computer trong hệ thống domain (mạng workgroup thì phải thiết lập policy trên từng máy).
- Triển khai ứng dụng tự động cho user (thay vì đến từng máy cài).

## Xây dựng mạng Domain:

**Đầu tiên ta phải nâng cấp DC** (xây dựng Domain Controller)

### Điều kiện:

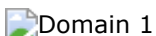
- Phải là phiên bản HDH Server. (trừ phiên bản Web)
- Tồn tại 1 card mạng online (có kết nối, nếu không có card online thì ta dùng card Loopback của Mirosoft).
- Tồn tại DNS server (điều kiện này thì có trước hay sau cũng được, Windows có thể tự xây dựng trong quá trình nâng cấp DC)

**Bước 1:** Chỉnh prefer DNS về chính máy DC (hoặc về DNS server), để truy cập tài nguyên, quản lý các đối tượng bằng tên.

**Bước 2:** Cài đặt dịch vụ Active Directory Domain Services (ADDS) và cấu hình AD.

### Thực hiện:

Trên Server: 2012may1 vào run -> ncpa.cpl để prefer DNS, do hệ thống không có DNS nên sẽ prefer về chính máy 2012may1.



Prefer DNS

Trên các HDH cũ như 2003, 2008 thì ta cần đánh lệnh dcpromo để nâng cấp, thì khi đánh lệnh này thì Windows sẽ tự động cài dịch vụ ADDS, chúng ta chỉ cần nâng cấp máy thành DC.

Từ 2012 thì ta phải tự cài ADDS và sau đó mới nâng cấp.

Mở Server Manager



Server manager

Menu Manage (bên phải) chọn **Add Roles and Features**.

Ở giao diện **Add Roles and Features** ta **Next 3 lần**.

## Server Roles: check vào **Active Directory Domain Services**

Xuất hiện bảng yêu cầu add thêm các feature cần thiết -> **Add feature ->Next**



Domain 3  
Add Roles and Features

Ta Next mặc định và **Install**



Domain 4  
Add Role ADDS



Domain 5  
Add Role ADDS

### Sau khi cài đặt ADDS xong, ta tiếp tục nâng cấp DC



Domain 6  
Nâng cấp DC

Ta có thể nâng cấp bằng cách click vào dòng "**Promote this server to a domain controller**" hoặc nhấn vào "**tam giác màu vàng**" ở Server Manager rồi chọn "Promote ...."

Xuất hiện giao diện nâng cấp DC



Domain 7  
Deployment Configuration

### Deployment Configuration: Có các tùy chọn sau

- Add a domain controller to existing domain: thêm 1 DC vào domain có sẵn (nâng cấp Additional DC)
- Add a new domain to an existing forest: thêm domain vào forest có sẵn
- Add a new forest: xây dựng 1 forest ngay từ đầu (các khái niệm về forest v.v sẽ được đề cập sau).

Do ta đang làm hành động xây dựng DC trên forest đầu tiên nên chọn **Add a new forest:** "tuhocmang.local".

Nguyên tắc đặt tên domain là

- + Không nên đặt trùng với tên website, nên đặt .local như mình.
- + Chỉ chứa các kí tự a->z, A->Z, -,0->9.

-> **Next**

### Domain Controller Option:



Domain 8  
Domain Controller Options

Mỗi domain đều có functional level (FL), phiên bản server là 2012 nhưng windows vẫn cho ta chọn các FL là các HDH đời cũ như 2003, 2008, 2008R2.

Nếu chọn FL đời mới thì ta có thể sử dụng các tính năng mới mà các HDH cũ không có (tính năng DFS trên 2008 mà 2003 không có). Nhưng nếu trong hệ thống có các server sử dụng HDH cũ như 2008 làm DC thì có thể các server HDH mới làm DC không thể giao tiếp với các server sử dụng HDH cũ.

Nếu để FL thấp thì ta có thể dùng tính năng "raise functional level" để nâng lên FL cao nhưng các FL cao thì không thể xuống FL thấp được.

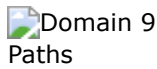
Hạ tầng có sẵn DNS server rồi thì không cần check vào Domain Name System (DNS). Không có thì check vào dịch vụ DNS sẽ được cài trên máy DC.

**Global Catalog (GC), RODC** sẽ đề cập ở bài sau.

**DSRM passwords:** password này được dùng cho quá trình **restore lại AD Database**.

-> **Next** mặc định đến phần:

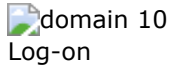
**Paths:** nơi lưu trữ AD Database (ta nên để Database ở các ổ đĩa cấu hình RAID1,5 hoặc SAN để an toàn)



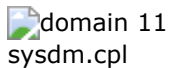
-> **Next** (phần **NETBIOS name**: hệ thống sẽ lấy 15 ký tự trước dấu "." để làm NetBios name. Ta để mặc định hoặc chỉnh sửa tùy nhu cầu) và **Install**.

Sau khi nâng cấp xong Windows sẽ yêu cầu Restart

Đây là màn hình đăng nhập sau khi nâng cấp Domain



Vào sysdm.cpl



Lưu ý: máy DC không còn tồn tại local user, chỉ còn domain user (vào compmgmt.msc sẽ không còn local user and group). Các local user ta đã tạo thì tự động chuyển sang domain user.

Để quản lý các đối tượng trong Domain ta sử dụng công cụ: Active Directory Users and Computers (ADUC)

Có 2 cách để mở ADUC

1/ Start -> run -> dsa.msc

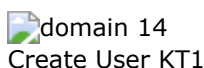
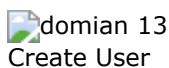
2/ Mở Server -> Tools -> Active Directory Users and Computers



Các **Container** như Built-in, Computers, Users v.v làm nhiệm vụ chứa các đối tượng trong domain. **Container Computer** chứa các máy gia nhập domain, Container Users chứa các đối tượng là user.

**Còn Domain Controllers là OU** ( Organization Unit). Ta có thể tạo thêm các OU, OU cũng như Container dùng để chứa các đối tượng nhưng có thêm khả năng quản lý các đối tượng bên trong (ví dụ: áp đặt policy vào các đối tượng trong OU v.v).

Ta tạo thử 1 đối tượng: **chọn Users -> New User**



Tạo user KT1

User log on name ( dùng để đăng nhập) có 2 kiểu log on:

+ UPN (user principal name) có dạng <user name>@<domain name>. VD: KT1@tuhocmang.local

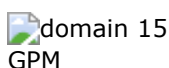
+ Pre-Windows 2000: <NetBios name>\<user name>.

VD: tuhocmang\KT1. Đây là kiểu log on cũ, dành để tương thích với những máy tính trước windows 2000 (98, v.v). HDH mới thì dùng kiểu nào cũng hiểu hết.

Password: Domain yêu cầu phải password phức tạp.

Để chỉnh lại password ta chỉnh lại policy. Trong môi trường domain tồn tại công cụ Group Policy Management (phần này chỉ nói cách chỉnh policy về password, sẽ có phần chuyên sâu về Group Policy Management).

**Start -> run -> gpmmc.msc hoặc vào Server Manager -> Tools -> Group Policy Management.**



Ta bung Domains -> tuhocmang.local -> Group Policy Objects: xuất hiện 2 policy tồn tại mặc định trên domain là

– Default Domain Controller và Default Domain Policy.

Những tùy chỉnh trong Default Domain Policy sẽ tác động lên **toàn domain** => chỉnh password policy thì dùng cái này.

Phải chuột Default Domain Policy -> Edit

Policies -> Windows setting -> Security Setting -> Account Policies -> Password Policies

#### domain 16 Password Policy

Sau khi nâng cấp DC thì mặc định Policy cấm các user thường log on vào máy DC. Ta muốn user log on vào máy DC thì phải chỉnh lại Policy.

Chọn Default Domain Controller Policy (policy này chỉ tác động lên DC) -> Edit

Policies -> Windows setting -> Security Setting -> Local Policies -> User Right Assignment

-> Allow log on locally

#### domain 17 Allow log on locally

Add Group: Users vào.

Sau đó: gpupdate /force để cập nhật.

Sau khi có DC, thì ta phải join các client computer vào Domain

#### **Điều kiện Join:**

– Có 1 NIC online

– Hệ DH tối thiểu Win 98 (HDH server và client đều có thể join domain)

**Bước 1:** Khai báo Prefer DNS về máy chủ DNS Server (ở bài này DNS được tích hợp vào trong DC nên chỉnh về IP của DC) để nó có thể phân giải theo tên

#### domain 18 Prefer DNS

Mở run -> cmd: đánh lệnh nslookup -> tuhocmang.local phải phân giải được ra IP của DC

#### domain 19 nslookup

#### **Bước 2:**

run -> sysdm.cpl -> Tab Computer name chọn Change

#### domain 20

Domain: đánh vào tuhocmang.com hoặc có thể đánh tên NetBios Name là tuhocmang -> OK

Xuất hiện thông báo:

#### domain 21

Nó hỏi: mình dùng tài khoản nào để gia nhập domain: ta có thể khai báo tài khoản admin hoặc user domain.

#### domain 22 join domain

Restart để hoàn tất việc join domain

Các user domain có thể đăng nhập trên bất cứ máy nào tham gia domain (domain member).

#### **Các vấn đề lưu ý:**

+ User Local vẫn tồn tại trên các máy domain member.

+ Domain Admin có toàn quyền trên domain member (vì sau khi join domain thì group Administrators (local) chứa group domain Administrators).

- + Local admin chỉ có toàn quyền trên local computer, Domain admin có toàn quyền trên domain.
- + Nếu admin ngồi trên domain member muốn quản lí chức năng Server từ xa (AD, Web server, v.v) thì cần cài bộ công cụ Remote Server Admin Tools (RSAT).
- + Nếu đang ngồi trên domain member là server thì mở

Server Manager -> Add Roles and Features -> click Next mặc định đến Features -> Remote Server Administration Tools (không check, chỉ bung ra thôi) -> check vào AD DS tools ( tool này dùng để quản lý ADUC) -> Next và Install. (cài bằng quyền Domain Admin)

#### domain 23 RSAT

- + Nếu đang ngồi trên domain member là windows client thì download RSAT cho HDH tương ứng

"search RSAT win 8" sẽ ra link download

<http://www.microsoft.com/en-us/download/details.aspx?id=28972>

Download về và cài đặt

#### domain 24 RSAT client

Sau khi cài đặt xong, ta vào appwiz.cpl -> turn Windows features on or off -> Remote Server Administration Tools : mặc định sau khi cài thì các tools quản lý đã được check, muốn gỡ cái nào thì bỏ check.

- + Dùng tài khoản user mặc định chỉ join được 10 lần, muốn join >10 lần các bạn vào link này tham khảo:

<http://tuhocmang.com/chuyen-de-tu-hoc/cau-hinh-khong-gioi-han-so-lan-join-domain-cho-user.html>

- + Sau khi join domain thì computer account có SID của nó và SID đại diện cho nó trong domain.

+ Firewall trên 2008 trở lên tự động mở port các dịch vụ mà ta thiết lập trên server => nâng cấp DC xong thì port của các dịch vụ liên quan đến Active Directory sẽ được mở.

Một số port cần thiết của AD:

[http://technet.microsoft.com/en-us/library/dd772723\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd772723(v=ws.10).aspx).

# 12. Home Folder và User Profile

## Chuẩn bị:

Domain Controller, File Server (chung 1 máy): 2012may1 IP: 192.168.2.100/24

Member computer: 2012may2 IP: 192.168.2.101/24

Tạo OU CongTy

Tạo OU KeToan -> Group KeToan chứa KT1, KT2.

Tạo OU NhanSu ->Group NhanSu chứa NS1, NS2.

Trên File Server, mỗi user muốn lưu trữ dữ liệu thì ta nên cho mỗi user 1 folder riêng tương ứng với tên user đó để dễ quản lý, sau đó ta cấp quyền NTFS cho folder đó, rồi ta Map Network drive folder đó về computer của user. Vậy nếu có 100 user ta phải làm 100 lần như trên !!!!.

Windows cung cấp ta chức năng **Home Folder**.

**Home Folder (HF)** là 1 thuộc tính của domain user, cho phép tạo ra nơi lưu trữ dữ liệu của user trên File Server. Sau khi cấu hình Home Folder xong, hệ thống tự động thực hiện:

- + Tạo Folder tương ứng với tên mỗi user.
- + Phân quyền NTFS Full Control cho user tương ứng.
- + Map Network Drive.

## Các bước làm:

**Bước 1:** Tạo folder Data trên File Server (2012may1) và share: Advance sharing ->Everyone ->**Full Control (bắt buộc)**. Qua **Tab Security, remove group Users** (để không ai vào được folder của người khác).

**Bước 2:** Cấu hình Home Folder

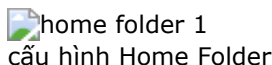
Mở dsa.msc -> Properties user KT1 -> tab Profile

Chọn Connect: để Map Network Drive

**To:** ổ Z sẽ được Map từ folder Data\KT1. Ta phải khai báo đường dẫn mạng:

VD: \\192.168.2.100\Data\%username%

Biến: %username% là biến môi trường, trả về đúng với tên user mà ta đang thao tác. Biến này rất quan trọng khi chúng ta cấu hình nhiều user cùng lúc.

home folder 1  
cấu hình Home Folder

Ta Apply thì thấy biến %username% tự trả về KT1.

Khi cần tạo nhiều user thì nên làm các bước sau (Hoặc dùng phím CTRL để chọn nhiều user)


**Bước 1:** tạo trước các user mẫu (template) (New -> user).

**Bước 2:** cấu hình thuộc tính cho user mẫu

VD: Giả sử KT2 là user mẫu của OU KeToan, ta sẽ cấu hình các thuộc tính chung như sau

- + Cho KT2 vào group KeToan.
- + Khai báo thuộc tính : company, department (Phòng Ke Toan) v.v
- + Cấu hình Home Folder: \\192.168.2.100\Data\%username%
- + v.v

**Bước 3:** Tạo mới user bằng cách Copy từ user mẫu

home folder 2  
Tạo User từ User mẫu (template user)


Kiểm tra: Thấy user mới có các thuộc tính chung giống KT2.

Cấu hình tương tự cho NS1, NS2.

**Kiểm tra:** Folder Data có các folder NS1, NS2, KT1, KT2

**Properties** folder NS1 -> **Tab Security** ta thấy User NS1: Full Control và Group "Users" : **Read and Execute**.

Logon NS1 thấy ổ đĩa mạng


 home folder 3  
Home Folder của user NS1

## User Profile

User Profile là môi trường làm việc riêng của từng người dùng, lưu trữ tất cả thông tin cấu hình của người dùng khi sử dụng máy tính.

### User Profile bao gồm:

- + Những thiết lập trên desktop.
  - + Document.
  - + Picture, download, music, favourite.
  - + Application Data : khi ta chạy các ứng dụng trên hệ thống, thì tất cả thông tin ta làm việc trên ứng dụng (các thiết lập, các cấu hình v.v) đó sẽ tự động lưu trên Profile (Application Data).
- VD: cấu hình tài khoản mail outlook thì những thiết lập đó lưu trong Application Data.
- + v.v

 user profile 1  
Profile của user domain NS1

Mỗi user sẽ có 1 profile mà chỉ user đó sử dụng đúng máy tính nào đó thì mới lấy ra đúng thư mục tương ứng.

### VD: Các bạn tự test trường hợp:

KT1 sử dụng máy: 2012may1 trên desktop tạo KT1.txt. Khi KT1 logon trên 2012may2, thì KT1.txt không xuất hiện trên desktop của máy 2012may2.

Loại Profile này gọi là **Local User Profile**.

**Local Profile:** người dùng chính ở đâu thì phải về chính máy đó mới xuất hiện những tùy chỉnh của mình.

Nơi lưu trữ Local User Profile:


**%SystemDrive%\Users\%UserName%**

Trong đó %SystemDrive% là Volume gốc của OS hiện hành (C:, D:, vv...) còn %UserName% là tên "User logon name".

Khi người dùng logon lần đầu tiên thì tự động trong folder Users hệ thống tạo ra folder tương ứng với **user logon name** của người dùng đó. Những tùy chỉnh của người dùng đều lưu trong folder đó.

Trong môi trường domain, các member computer có thêm **local user profile** ( máy DC không có).


Trong Folder User ta thấy tồn tại Folder Default ( folder này mặc định bị ẩn) và Public (đây là folder **All User** trong các HDH cũ).

 user profile 2  
Profile: Default và Public


**Khi user lần đầu tiên log on** thì máy tính sẽ tự động lấy thông tin trong Default và Public để phát sinh profile, như vậy Default chỉ tác động 1 lần duy nhất.

**Lần thứ 2 log on** thì máy tính sẽ lấy thông tin trong folder profile riêng của user và folder Public để tạo thành môi trường làm việc của user khi log on.

**VD:** Ta muốn có file NoiQuyCongTy.doc luôn có trên desktop của user thì chỉ cần copy file đó vào thư mục desktop của folder Default

 user profile 3  
Folder: Desktop trong Default

Còn đối với các user đã log on thì ta không tác động bằng Default mà phải ta dùng Public. Copy file đó vào Public Desktop.


 user profile 4  
Public Desktop

**Vấn đề:** Đặc trưng của hệ thống domain là người dùng có thể logon trên bất cứ máy tính nào là member domain. Mặc định Windows sử dụng local profile nên nếu dữ liệu user lưu trong profile thì khi logon trên máy khác chắc chắn sẽ không có.

**Vấn đề tiềm ẩn:** Sếp muốn có file nội quy trên màn hình desktop, nếu có 100 máy ta phải copy vào folder Public Desktop trên tất cả các member domain !!!

**Ta có nhu cầu:** User đi tới đâu thì profile tương ứng đi theo đó (local profile không thể đáp ứng được)

Lúc này ta phải sử dụng loại Profile thứ 2 mà windows hỗ trợ: **Roaming Profile**. Để triển khai giải pháp này thì hệ thống phải là Domain Network.

 user profile 5  
Quá trình Roaming Profile

Lúc này, profile của các user sẽ được lưu trữ trên File Server, DC sẽ copy toàn bộ Profile của user về máy tính mà user đang logon. Khi user log off thì nó sẽ tự động đem các thông tin mà user thay đổi ở Profile trong quá trình làm việc đem về File Server. Quá trình này gọi là Synchronize (đồng bộ).

### Triển khai Roaming Profile (RP)

**Bước 1:** Tại File Server (2012may1) tạo share Folder, và share everyone : Full Control (Security để mặc định). Nếu xóa group users trong Security thì quá trình Synchronize khi user log off không thể truy xuất vào folder của user đó => Profile không có chỗ lưu trữ => mất Profile.

Windows sẽ tự động chỉnh quyền sao cho folder Profile của user nào thì chỉ user đó mới có quyền truy cập, kể cả Administrator cũng không có quyền vào.

**Bước 2:** tại giao diện ADUC cấu hình Roaming Profile cho các user có nhu cầu.

Trên 2012may1


Tạo folder RP rồi làm như bước 1.

Vào **dsa.msc**

Chọn các user có nhu cầu -> **Properties** -> **Tab Profile** (hoặc làm 1 user rồi sau đó copy cũng được)

**Profile Path:** nếu dòng này để trống thì mặc định dùng user profile. Ta muốn lưu profile vào folder RP thì khai báo

**\\192.168.2.100\RP\%username%**

 user profile 6  
Cấu hình Roaming Profile

Vậy là ta đã cấu hình xong

**Cách test:** KT1 logon tạo KT1.txt trên desktop, sau đó logoff rồi log on máy khác.

### Lưu ý:

Cấu hình RP chỉ nên dùng cho các user có nhu cầu, hay thay đổi vị trí làm việc. Khi triển khai đại trà thì nếu 100 user log on làm việc thì kết nối đến File Server để lấy Profile mà dung lượng Profile thì không nhỏ (ít cũng vài chục MB) dẫn đến tắc nghẽn hệ thống, chiếm hết băng thông (8h logon thì 10h mới làm việc được !!!).

Nếu user vừa log on trên win XP, vừa logon trên win 7, 8 thì sẽ có 2 Profile (xuất hiện 2 folder trên File Server: folder KT1 và folder KT1.V2).


Vì mặc định Administrator không có quyền trong profile nên ta muốn truy cập ta phải làm như sau (nếu làm không đúng thì user sẽ bị mất profile):

Giả sử ta muốn vào Profile của NS1

### Bước 1: Take Ownership



**Properties** folder -> **Tab Security** -> **Advanced**

 user profile 7

Take ownership folder chứa profile

Chọn: **Continue**

Phần **Owner**: chọn **Change** -> **add tài khoản Administrator** (hoặc add group Administrators) vào.


**Check Replace owner on subcontainers and objects** (để nó take ownership cho các đối tượng bên trong luôn)

-> **Ok** toàn bộ

Lúc này Administrator là owner mới còn User không có khả năng vào Profile của mình.

**Bước 2: cấp quyền để User (NS1) truy cập, synchronize profile.**

**Properties Folder NS1** -> **Edit** -> Add: NS1 cho quyền: **Full Control**

 user profile 8


Trả lại quyền cho User

Ở cửa sổ **Security** -> Chọn tiếp **Advanced**

Để đảm bảo NS1 truy suất được tất cả đối tượng bên trong ta check vào

Replace all child objects entries with inheritable permission entries from this subject -> Aplly

Sau đó ở phần **Owner** -> ta change owner lại cho NS1 rồi check tiếp vào 2 mục: **Replace** như hình -> **Apply**

 user profile 9

Trả quyền Ownership cho NS1

**Test:** NS1 log on trên 2012may1 tạo folder " Owner", sau đó log off rồi log on trên 2012may2. Nếu thấy folder "Owner" thì quá trình take Ownership và trả lại Ownership diễn ra thành công.

# 13. Deployment Software

Chuẩn bị:

DC: 2012may1 (192.168.2.100)

Member computer domain: win8 (192.168.2.102)

## Tình huống

Công ty có nhu cầu 100 máy tính trong công ty phải có phần Microsoft office => phải cài trên từng máy => tốn thời gian

**Nhu cầu 1:** 100% phải cài bản update mới nhất. Giải pháp: đi từng máy cài

**Nhu cầu 2:** chỉ có phòng Kế toán mới được xài office, Nhân sự không được

## Giải pháp 1:

File chạy ứng dụng office nằm trên C:\Program Files\Microsoft Office, ta chỉ phân quyền Deny : Read and Execute cho user trên folder này

100 máy làm 100 lần -> lúc này thì thua rồi !!!!!.

Windows cung cấp cho ta các giải pháp để **đáp ứng nhu cầu trên** gồm:

**Application virtualization, Deploy software** sử dụng GPO (triển khai phần mềm thông qua GPO), **Remote Application, SCCM** ( System Center Configuration Manager).

Bài này ta chỉ đề cập đến Deploy Software (DS) thông qua GPO

DS tác động đến 2 đối tượng: user và computer.

**Đối với user:** DS chỉ deploy khi người dùng log on.

**Đối với computer:** deploy khi khởi động máy tính.

GPO cung cấp cho ta 2 phương pháp để triển khai phần mềm xuống:

Đối với user account: 2 phương pháp:

**Assigned** : khi user log on thì ứng dụng đã cài hoàn tất.

**Published**: khi user log on thì ứng dụng chưa được cài mà GPO chỉ làm chuyện đơn giản là: lấy Source phần mềm đem về máy tính user trong mục Programs and Features . User phải vào đây để cài.

Đối với computer account chỉ có Assign ( ý nghĩa như trên).

Điều kiện để sử dụng: đuôi phần mềm phải là \*.msi, nếu các đuôi khác như \*.exe thì phải dùng các chương trình convert để chuyển từ exe -> msi.

**Link download:** Winstle ( cách sử dụng có trên mạng, nên convert trên máy trắng, chưa cài gì thì mới convert thành công)

<http://www.mediafire.com/download/c8asvb23udmo47c/SWIADMLE.MSI>

## Triển khai:

**Bước 1:** share source cài đặt tại File Server.

Lưu ý: khi share source phải tạo folder cha, sau đó tạo thêm folder con và chứa source phần mềm trong đó. Rồi Share folder cha (nếu chỉ tạo 1 folder thì lúc deploy được, lúc deploy không được).

Ở lab này ta tạo: folder Deploy Software folder Adobe Reader

(Share folder Deploy Software: everyone: Read là đủ)



DS 1  
Phân Quyền Share

**Bước 2:** tạo GPO

**Gpmc.msc** -> chọn OU Nhân Su -> **Creat a GPO ....**

Name: **GPO 9: deploy Adobe Reader** -> **Edit**



DS 2

Deploy Adobe Reader

Ở dòng File Name nhập nơi lưu trữ source software ( phải dùng đường dẫn UNC)

**\\192.168.2.100\Deploy Software**



DS 3

Đường dẫn đến folder lưu trữ Source

Ta **Browse** về file **msi** trong folder **Adobe Reader**

Sau khi chọn file msi xong xuất hiện bảng thông báo cho ta chọn các phương thức deploy:

Ta chọn **Published**



DS 4

Chọn phương thức deploy



DS 5

Muốn deploy phần mềm nào thì cứ làm tương tự.

Ta double click vào **Adobe Reader X (bên phải) -> Tab Deployment**

Ta có thể tùy chỉnh lại phương thức deploy.



DS 6

Tùy chỉnh lại các phương thức deploy

Lưu ý: nếu ta chọn **Advanced** (trong phần chọn phương pháp deploy) thì nó sẽ tự động vào cửa sổ **Deployment**.

Phần: **Deployment Options:**

Ta thấy có option: **Uninstall this application when it falls out of the scope of management** (quan trọng nhất).

Nếu ta không chọn option này thì

NS1 thuộc OU NhanSu, khi ta muốn đổi NS1 qua OU KeToan thì cái Adobe Reader ta deploy cho OU NhanSU vẫn còn trên máy NS1. ( CÔNG ty có quy định là OU KeToan được được deploy Adobe Reader)

Nếu chọn thì khi move NS1 qua OU KeToan , sau khi NS1 log off thì hệ thống sẽ gỡ Adobe vì NS1 không còn là thành viên OU NhanSu

Option: Do not display this packet ... Nếu dùng phương pháp published thì không được check

Qua **Tab Upgrades**: Nếu ứng dụng có bản update thì ta Add vào, tự động GPO sẽ cài bản update hoặc deploy xuống cho người dùng cài.

**Tab Modifications** : bị mờ (tham khảo link cuối bài)



DS 7

**đánh lệnh: Gpupdate /force**

**Test:** log on NS1 trên win 8

Những user nào mà ta cấu hình deploy bằng Assigned thì log on lâu vì phải đợi phần mềm cài đặt.

NS1 ta đã chỉ định phương thức Published nên phải vào Programs and Features

Vào run -> appwiz.cpl -> Install a Program from the network



DS 8

Cài đặt soft

Chọn Adobe -> Install

**Lưu ý:** các máy tính sau khi được cài Adobe Reader thì chỉ những user trong OU mà được dùng Adobe Reader mới sử dụng được trên máy tính đã được cài, GPO sẽ tự động phân quyền để các user thuộc các OU khác không thể sử dụng được.

Khi deploy Office 2003, người dùng phải tự add key, muốn tự động add key thì tham khảo link sau ( sử dụng tab Modifications):

<http://giang.nhatnghe.vn/deploy.htm>

Các đời office sau thì có nhiều file MSI nên không thể dùng cách này được, phải triển khai bằng Script nếu dùng GPO.

**Link tham khảo deploy office 2010:** ( Dùng Script)

### Deploy Office 2010 with Group Policy



**Link tham khảo deploy office 2013** ( Dùng Script)

<http://community.spiceworks.com/topic/352128-microsoft-and-office-2013-msi>

<http://technet.microsoft.com/en-us/library/ff602181.aspx>

<http://allancrumpton.blogspot.com/2013/02/office-2013-gpo-group-policy.html>

# 14. Local Group Policy

Khi user đăng nhập thì họ chịu những áp đặt của HDH, trong quá trình quản lý ta có nhu cầu hạn chế hay thêm vào các quyền hạn của họ khi truy cập ứng dụng hay truy cập tài nguyên.

Các thời HDH windows cũ thì ta phải mở các file system.ini để cấu hình. Từ windows 98 trở lên, Microsoft cho phép ta thực hiện cấu hình bằng Registry, bằng công cụ này thì admin có thể thiết lập các quy định áp đặt lên hệ thống, user. Vì việc chỉnh sửa registry rất phức tạp, Microsoft lấy 1 số key trong registry để tạo thành Group Policy (chính sách nhóm) giúp các admin có thể chỉnh sửa dễ dàng.

Group Policy có thể áp dụng lên local computer hay môi trường domain.

Group Policy trên local computer được gọi là Local Group Policy (local policy).

Công cụ quản lý local policy:

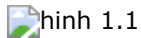
## Cách 1:

run -> **gpedit.msc** (xuất hiện công cụ quản lý là Local Group Policy Editor).

 hình 1

## Cách 2:

- run -> mmc (giao diện console root), menu **File chọn Add/Remove Snap-in.**
- chọn Group Policy Object Editor, để mặc định **Local computer** -> **add** rồi save lại.

 hình 1.1

 hình 2

Policy gồm 2 phần:

**Computer Configuration:** nếu thiết lập các policy trong phần này thì đối tượng bị tác động là computer và user account

**User Configuration:** đối tượng bị tác động là user account.

Các giá trị có trên Policy của Windows:

- **Not configured/Defined:** không can thiệp vào policy, để mặc định theo Microsoft ( giá trị mặc định có lúc sẽ là disable policy, có lúc sẽ là enable policy).

- **Enabled:** bật policy.

- **Disable:** tắt policy.

## Cách áp đặt policy đã hiệu chỉnh cho hệ thống:

- Một số Policy sẽ tự động có hiệu lực.
- Ta vào run -> cmd, dùng lệnh: gpupdate /force để bắt buộc hệ thống cập nhật policy.
- Nếu gpupdate /force mà vẫn chưa thấy có hiệu lực thì log off sau đó log on lại.
- 3 bước trên không dùng được thì Restart server (lưu ý: chỉ dùng khi 3 cách trên không có hiệu lực).

## Một số policy thường dùng:

1/ Bật/Tắt chức năng "Display shutdown event tracker": đây là chức năng bắt ta khai báo lý do nếu tắt server.

 hình 3

- Computer configuration\ Administrative Templates\ System: bên phải chọn Display shutdown event tracker

 hình 4

## 2/ Các policy liên quan đến Control Panel

User Configuration\ Administrative Templates\ Control Panel

+ Show only specified Control Panel items: chỉ cho phép sử dụng 1 số item trong control panel do admin chỉ định.

enable rồi click show, ta nhập **đúng tên item** trên control panel mà ta cho phép hiển thị

ví dụ chỉ cho phép hiển thị item fonts



### đánh lệnh: gpupdate /force

Kết quả:

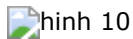


+ **Prohibit access to Control Panel and PC settings**: cấm truy cập Control Panel. Bất lợi của policy này là những thiết lập liên quan đến control panel đều bị cấm ( Screen solution, Properties Computer, v.v đều bị cấm).

### 3/ Các policy liên quan đến Desktop

#### User Configuration\ Administrative Templates\ Desktop

+ Remove Recycle Bin icon from desktop: mất icon Recycle Bin ở desktop (muốn mất thì enable policy này).



### 4/ Các policy liên quan đến Start Menu và Taskbar

#### User Configuration\ Administrative Templates\ Start Menu and Taskbar

+ Remove Run menu from Start menu: cấm chạy menu Run (bấm Windows + R cũng bị cấm).

### 5/ Các policy liên quan đến System

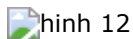
+ Prevent access to the command prompt: cấm sử dụng cmd.

+ Don't run specified Windows application: cấm các ứng dụng của Windows.

enable, chọn show

Mỗi ứng dụng sẽ có file thực thi (\*.exe), chỉ cần add file thực thi là policy cấm được ứng dụng.

ví dụ: cấm internet explore (IE), file thực thi của IE là iexplore.exe



+ Run only specified Windows application: chỉ cho chạy các ứng dụng được chỉ định.

### Local Security Policy (chính sách bảo mật)

Nó nằm trong Computer Configuration\ Windows Settings\ Security Settings hoặc có thể mở nó bằng lệnh **secpol.msc**

Các security policy thường gặp:

#### Account Policies (chính sách tài khoản):

**1/ Password Policies**: những chính sách liên quan đến mật khẩu



+ Minimum password length: quy định chiều dài tối thiểu của mật khẩu.

- + Minimum password age: tuổi thọ tối thiểu của 1 password, nếu quy định là 2 thì sau 2 ngày password mới có thể được đổi.
- + Maximum password age: tuổi thọ tối đa của 1 password (mặc định 42 ngày). Lúc này user nếu không muốn thay đổi password thì có thể đặt lại password cũ, do đó ta cần 1 policy để ngăn cản việc này là:
- + Enforce password history: nếu chọn 3 thì nó sẽ nhớ 3 password trước đó của user. Lần 1 đặt pass: 12 3 thì nó sẽ nhớ lại, và nó sẽ nhớ tối đa cái số mà ta chỉ định. Theo yêu cầu của Microsoft thì nên để 24 (!!).
- + Password must meet complexity requirements: phải đặt password phức tạp (xem lại bài Local User and Group). Nếu không muốn đặt phức tạp thì disable.
- + Store passwords using reversible encryption: mặc định windows lưu user, password dưới dạng mã hóa trong file SAM (Security Account Manager), có 2 dạng mã hóa là **Reversible** (có thể dịch ngược – mã hóa 2 chiều) và **Irreversible** (không thể dịch ngược – mã hóa 1 chiều). Nếu enable thì hệ thống sẽ mã hóa 2 chiều, làm giảm độ an toàn khi có người nào đó lấy được file SAM.

## 2/ Account lockout Policy: các chính sách khóa tài khoản

- + Account lockout threshold: ngưỡng để quy định khóa tài khoản (mặc định là không khóa). Nếu ta chỉ định threshold là 3 thì nếu nhập sai password 3 lần thì sẽ khóa tài khoản (lần 4 nhập đúng cũng không được). Dùng để chống dò mật khẩu.
- + Account lockout duration (T1) : khóa tài khoản trong vòng bao nhiêu phút (giả sử ta khóa trong 30 phút)
- + Reset account lockout counter after (T2): nhờ có bộ đếm (counter) mà hệ thống thống kê được số lần đăng nhập sai, policy này quy định thời gian bộ đếm reset lại về 0. Lúc này người dùng mới có thể tiếp tục đăng nhập

Lưu ý: thời gian  $T1 \geq T2$ .

Khi tài khoản bị khóa thì sẽ hiện dấu check Account is locked out



hình 16

Nếu người dùng không muốn đợi đến hết thời gian T2 để đăng nhập thì có thể nhờ admin bỏ check .

Nếu  $T1 = 0$  thì tài khoản sẽ bị khóa cho đến khi admin bỏ check.

## Local Policies: các chính sách cục bộ

**User rights assignment:** gán quyền cho người dùng.

- + Allow log on locally: cho phép đăng nhập trên máy.
- + Deny log on locally: cấm đăng nhập trên máy ( nếu user vừa được Allow, vừa bị Deny thì Deny mạnh hơn => bị cấm log on).
- + Shut down the system: cho phép user nào được tắt máy.
- + Change the system time: cho phép chỉnh giờ hệ thống.

## Security Option:

Trong giao diện log-on, mặc định hệ thống hiển thị các user đang có => không bảo mật, ta dùng policy

- + Interactive logon: Do not display last user name (không hiển thị user name cuối cùng và đồng thời không hiện ra các user khi đăng nhập).
- + Interactive logon: Do not require CTRL + ALT + DEL : khi log-on không cần bấm tổ hợp 3 phím
- + Shutdown: Allow system to be shutdown without having to log on: cho phép tắt máy mà không cần log on.
- + Account: Rename administrator account : đổi tên tài khoản administrator.

## Các policy liên quan đến vấn đề truy cập tài nguyên mạng.

- + Secpol.msc -> security options -> local policies

### -> Security Options

Network access: Sharing and security model for local accounts: Các chế độ truy cập mạng

- Classic (default) : cho phép chứng thực bằng các tài khoản trên local computer của máy chia sẻ.
- Guest: chỉ cho phép vào bằng tài khoản guest.

Account: Limit local account use of blank password to console log on only: cấm tài khoản không có password truy cập tài nguyên

#### -> **User Rights Assignment**


Access this computer from the network: cho phép user, group truy cập tài nguyên (mặc định là tất cả user).


Deny access to this computer from the network : cấm user, group nào đó truy cập tài nguyên (nếu vừa allow, vừa deny thì deny ưu tiên hơn).

\*\*\*\*\*

Như mình đã trình bày, các policy ta vừa kể trên là Local Group Policy áp đặt cho tất cả user trên hệ thống. Từ Windows Vista trở lên, Microsoft hỗ trợ công cụ áp policy cho 1 user cụ thể là Local User Policy.

Start -> Run -> MMC -> Add/Remove Snap-in -> Group Policy Object Editor -> Browse -> tab user chỉ định user cụ thể -> OK (muốn thêm bao nhiêu user thì làm lại bấy nhiêu lần).


 hình 18

 hình 19

**Lưu ý 1:** Các policy lưu trong 1 file là:

Đường dẫn: **C:\ Windows \ System32 \ Group Policy**

Mặc định folder Group Policy bị ẩn, ta phải hiển thị các file ẩn.

 hình 21

 Hình 22

Machine: lưu các policy của máy tính, User: các policy liên quan đến user.

Ta xóa folder này và restart thì WIndows sẽ phát sinh cấu hình default => mất policy.

#### **Lưu ý 2:**

Ta nhận thấy Administrator có thể đăng nhập vào safe mode khi bị disable, thì để bảo mật tài khoản Administrator (built-in) ta cần làm các bước sau:

- + Tạo user add vào group **Administrators**.
- + Rename tài khoản **Administrator built-in**.
- + Đặt password phức tạp cho Administrator built-in.

Nếu các bạn muốn tìm hiểu thêm về các policy thì download file này

Tài liệu GPEDIT.MSC



# 15. Group Policy Object

## Chuẩn bị:

máy DC: 2012may1 IP: 192.168.2.100/24

1 máy computer member domain: 2012may2 192.168.2.101/21

Tạo cấu trúc OU theo hình cây: OU CongTy chứa 2 OU con là KeToan, NhanSu

Trong OU KeToan chứa: Group KT và KT1, Kt2. OU NhanSu làm tương tự

Như đã đề cập, việc xây dựng OU ngoài mục đích để quản lý, dễ dàng ủy nhiệm cho việc quản lý thì chức năng quan trọng của OU là giúp ta triển khai chính sách (policy) ở cấp độ domain

Group Policy bao gồm 2 loại: local policy và domain policy. Local Policy chính ở đâu thì chỉ có nơi đó tác động.

Domain Policy thì chỉ cần chỉnh ở 1 nơi mà tác động ở nhiều nơi (toàn Domain hoặc các OU cụ thể).

Để triển khai bộ Domain Policy thì ta phải thông qua một đối tượng (AD object) trung gian là Group Policy Object (GPO). Local Policy thì ta chỉnh trực tiếp (gpedit.msc: Local Group Policy Editor).

GPO là 1 AD object dùng để chứa những policy được thiết lập nhằm tác động trên hệ thống. 1 GPO có thể chứa 1 hoặc nhiều Policy khác nhau. Cùng 1 Policy có thể chứa trên nhiều GPO khác nhau.

Lưu ý:

- + Trên 1 GPO chỉ nên chỉnh 1 Policy (tốt nhất là nên như thế) hoặc 1 nhóm policy có quan hệ với nhau về mặt luận lý ( 1 nhóm policy liên quan đến OU KeToan).

- + Đặt tên GPO phải tường minh, mô tả được chức năng của policy ( VD: GPO1 – restrict control panel)

- + GPO chỉ tác động lên 3 đối tượng (object) trong AD (Active Directory): OU, User, Computer account.

(GPO có thể tác động vào nhiều OU, User, computer account và ngược lại). Như vậy Group không bị tác động.

- + GPO có tính kế thừa: GPO mà tác động domain thì tất cả các đối tượng đều bị tác động. GPO tác động lên 1 OU thì các đối tượng bên trong (OU con, user, computer) đều bị tác động . Do đó các chính sách chung của công ty, của phòng ban ta có thể dùng tính kế thừa để triển khai nhanh gọn.

Mở Công cụ quản lý GPO

Run -> gpmmc.msc: Group Policy Management.

 GPO 1  
gpmmc.msc

Ở bài Domain Network – Phần 1, mình đã hướng dẫn cách áp đặt policy để đặt password đơn giản bằng Default Domain Policy. Thực chất Default Domain Policy là một GPO, tác động đến toàn domain (tính kế thừa xuống các đối tượng con).


Domain Controller Security Policy: Là GPO tác động đến OU Domain Controller (là OU chứa DC). GPO này chỉ tác động đến DC.

- + Các bạn tự thiết lập các policy ở Phần 1 .

Công ty có nhu cầu : Nhân viên công ty cấm **Control Panel** => **Tạo GPO ở OU công ty** ( lưu ý: GPO tác động tới đâu thì làm việc ở vị trí đó)

 GPO 2  
Policy

Chọn vào **OU CongTy** -> **Create a GPO in this domain and Link it here ...**

 GPO 3  
Create GPO

Khai báo tên GPO -> OK

Sau khi tạo GPO xong, **phải chuột GPO** -> **Edit** để tìm policy cấm control panel

 GPO 4  
Edit

**Enable** Policy này lên.

 GPO 5  
Cấm Control Panel

**Tương tự** tạo thêm các policy trên OU CôngTy:

**+ GPO 2: ẩn Recycle Bin**

Sau khi thực hiện các chính sách của công ty thì các phòng ban cũng có các chính sách riêng.

**Phòng Kế Toán:** Cấm sử dụng IE

**+ GPO 3: cam IE**

**Phòng Nhân Sự:** Cấm sử dụng command line, cấm mở công cụ Active Directory Users and Computers.

**+ GPO 4: cam cmd**

**+ GPO5: cam mo ADUC**


**Cách chỉnh GPO5:** User configuration -> Policies -> Administrative template -> Windows Component -> Microsoft Management Console -> Restricted/ Permitted Snap-in -> Active Directories Sites and Services

Ta Enable Policy này

 GPO 6  
cấm ADUC

Sau đó chạy lệnh **gpupdate /force**

**Lưu ý:** Ta nên vẽ sơ đồ hình cây về tổ chức kèm theo các GPO để dễ quản lý

 GPO 7  
Các GPO áp đặt

 GPO 8  
Sơ đồ

**Ta Test từng user thì thấy rằng:**

User KT1, KT2 sẽ chịu ảnh hưởng của GPO: Default Domain Policy, 1, 2, 3.

User NS1, NS2 sẽ chịu ảnh hưởng của GPO: Default Domain Policy, 1, 2, 4, 5

Group KeToan và NhanSu không bị ảnh hưởng.

**=> Chúng ta đã thấy tính kế thừa của GPO.**

**Tình huống:** Ta muốn cấm các user trong OU KeToan mở ADUC. Thay vì phải tạo thêm 1 GPO tác động lên OU KeToan thì ta chỉ cần lấy GPO 5 tác động lên OU KeToan. Ta sử dụng tính năng "Link" của GPO.

Ta chọn vào OU KeToan -> chọn **Link an existing GPO**

 GPO 9  
Link GPO

Xuất hiện giao diện SELECT GPO

Ta chọn GPO 5 ( hoặc các GPO khác tùy nhu cầu)

 GPO 10  
Select GPO

**Tình huống:** Khi thực hiện chính sách cấm Control Panel thì nhân viên than phiền nhiều nên ta muốn bỏ tác động của GPO 1 lên người dùng. Để bỏ tác động của GPO, ta có 2 cách:

**Cách 1:** xóa hẳn GPO (chỉ dùng khi tổ chức bỏ hẳn chính sách đó lên toàn công ty)

 GPO 4

Chọn Delete để xóa

### **Chọn Delete.**



GPO 11

Đã xóa GPO 1

Ta thấy sau khi bỏ thì OU CongTy mất GPO 1, nhưng GPO 1 vẫn còn tồn tại ở trong **Group Policies Object**. Nếu muốn dùng lại GPO 1 cho OU CongTy thì lại tiếp tục sử dụng tính năng "Link an existing GPO".

**Cách 2:** Bỏ tính năng Link GPO ( Bỏ tính kế thừa của 1 GPO xuống các đối tượng con)



GPO Link

Bỏ tính kế thừa của GPO

### **Bỏ check Link Enabled**

**Các bạn tự kiểm tra kết quả các tình huống.**

# 16. Group Policy Object – Phần 2

Chuẩn bị

- Xem cách chuẩn bị của Phần 1.
- Cấu hình Policy: GPO 1, 2, 3, 4, 5 như Phần 1.

**Tình huống:** Trong hệ thống, ta có nhu cầu GPO cha không tác động vào OU con . Để giải quyết được vấn đề này ta có 2 cách thực hiện cho 2 tình huống khác nhau.

**Cách 1:** Tạo GPO phủ định (OU Cha cấm Recycle Bin mà OU con cho phép Recycle Bin)

Một máy tính, user có thể bị tác động của các policy như: Local Policy, Domain Policy, OU Policy, Child OU Policy, v.v ( GPO áp cho OU con) . Ngoài ra còn có Site Policy ( Policy tác động lên 1 hoặc nhiều domain). Thứ tự tác động của Policy như sau:

Đầu tiên, PC được khởi động thì sẽ bị tác động bởi:

- + Local Policy, sau đó lần lượt là
- + Site Policy
- + Domain Policy
- + OU Policy
- + Child OU Policy (OU con). ( Từ cao xuống thấp)

Đề cập sâu hơn thì: trong quá trình tác động từ khi máy tính được bật cho đến khi hiện ra màn hình đăng nhập thì PC bị áp đặt bởi các policy trong mục Computer Configuration.

- + Computer Configuration Local Policy
- + Computer Configuration Site Policy
- + Computer Configuration Domain Policy
- + Computer Configuration OU Policy
- + Computer Configuration Child OU Policy

Khi user log on thì nó sẽ bị ảnh hưởng của các Policy trong User Configuration cũng theo thứ tự như trên.

Như vậy, nếu các Policy từ Local đến Child OU mà không bị đụng chạm ( phủ định) thì kết quả cuối cùng là bị ảnh hưởng bởi tổng các policy.

Nếu có đụng chạm ( phủ định 1 policy nào đó) thì thứ tự ưu tiên sẽ đi từ Child OU cho đến Local Policy ( VD: OU cha cấm Control Panel mà OU con cho phép Control Panel thì kết quả là cho phép Control Panel).

**Tình huống:** OU NhanSu được phép truy cập Control Panel

**Triển khai:**

**Run -> gpmmc.msc -> Ou NhanSu -> Create GPO ...**

Đặt tên: GPO 6: Cho Phep Control Pannel

 GPO 12

Tạo GPO phủ định

**Rồi Edit -> Cấu hình Policy như đã học (Disable).**


**Test:** các bạn tự test Policy.

**Cách 2:** Dùng phương thức **Block Inheritance** ( Khóa đặc tính kế thừa của OU). **Đây là 1 thuộc tính của OU**

**Triển khai:**

Chọn OU NhanSU -> **Block Inheritance**

Lúc này OU NhanSu sẽ không còn chịu ảnh hưởng của GPO 1, 2 từ OU cha do đã mất tính kế thừa.

 GPO 13  
Block Inheritance

**Lưu ý: Dùng cách 2 khi ta không muốn OU chịu bất kì tác động nào từ các GPO của OU cha.**

#### Tình huống:

GPO 1: cấm control pannel là **quy định chung của công ty, bắt buộc** phải được áp đặt, **dù có bỏ quyền thừa kế hoặc bị phủ định đi chăng nữa**. Ta sử dụng tính năng **Enforced** có trên GPO.

 GPO 14  
Enforced

Những GPO mà Enforced sẽ có hình "**ổ khóa**".

**Tình huống:** Ta **ủy nhiệm** cho NS1 quản lý OU NhanSu mà OU NhanSu lại có GPO 5 : cấm mở ADUC.

**Nên ta có nhu cầu biệt đãi người dùng (bạc đãi hoặc ưu đãi)**. Do GPO là 1 AD Object nên GPO cũng có bộ quyền Security.

Sở dĩ một user chịu tác động của 1 GPO là do bất kì user nào trong domain đều có 2 quyền: **Read và Apply Group Policy**. Nếu user không có **1 trong 2 quyền** này thì GPO không thể tác động đến user đó.

+ Nếu chỉ muốn cấm NS2 ADUC (**bạc đãi**) : tạo GPO cấm ADUC rồi cho 2 NS2 2 quyền trên. Rồi Group Authenticated User deny 2 quyền đó.

+ Nếu chỉ muốn NS1 được sử dụng ADUC (**biệt đãi**) thì cho Group Authenticated User 2 quyền, NS1 deny quyền Read, Apply (hoặc deny 1 trong 2 quyền đều được).

#### Triển khai:

**Biệt đãi** người dùng trên GPO nào thì làm việc trên GPO đó.

Gpmc.msc -> Chọn OU Nhan Su -> Chọn GPO 5 -> Nhìn bên phải tìm tab Delegation

 GPO 15

Chọn **Advanced**

Ta add user: NS1 và check vào : **Deny quyền Read rồi Apply -> OK**


 GPO 16

Log on NS1 thấy mở được gpmc và GPO 5 là: inaccessible do ta Deny Read (nếu chỉ **deny Apply** thì vẫn thấy GPO 5)

 GPO 17

**Trên cùng 1 OU có 2 GPO:** vừa cấm Control Pannel, vừa cho phép Control Pannel . **GPO nào xếp trên thì ưu tiên hơn.**

Chọn OU Nhan Su, bên phải chọn tab: Linked Group Policies Object: có nút mũi tên. Ta dùng nút này để sắp xếp các Policy theo nhu cầu.

 GPO 18  
Sắp xếp GPO

#### GHI CHÚ:

+ Để xem tổ chức có bao nhiêu GPO: dùng **Group Policy Objects trong gpmc**

+ Để xem 1 GPO đang tác động đến những OU nào: chọn GPO bất kì, bên phải chọn Tab **Scope**

 GPO 19

+ Để xem 1 OU đang chịu tác động của những GPO nào :

Chọn OU bất kì: chọn **Tab: Group Policy Inheritance** ( phủ định, thừa kế, Enforced v.v)

+ Để xem trong 1 GPO đã chỉnh những policy nào:

Chọn GPO bất kì -> bên phải chọn Tab **Setting**

 GPO 20

Ghi chú: Group Authenticated User nhỏ hơn group users , chỉ những user đã log on thành công thì mới là member trong group này (tối ưu hơn)

# 17. Group Policy Object – Phần 3

ứng dụng thực tế của GPO là Folder Redirection và Scripts.

## Chuẩn bị

– Như cũ

## Tình huống:

**KT1** muốn **Documents** trong Profile luôn đi theo mình khi ngồi bất kể vị trí nào, ta sử dụng **Roaming Profile**. Tuy nhiên dùng Roaming Profile sẽ kéo theo Application Data, Desktop, v.v đi theo KT1 mà ta chỉ muốn 1 mình folder Documents. Việc sử dụng Roaming Profile đại trà như chúng ta đã biết cũng gây ra nhiều vấn đề. Trong môi trường domain, Windows cung cấp cho ta tính năng **Folder Redirection** (Tái định hướng profile).

Folder Redirection (FR) cho phép chúng ta lựa chọn thông tin trong profile để tái định hướng.

FR cho phép ta có thể roaming tất cả các thông tin trong profile:

**Nguyên lý hoạt động :** Giống với Roaming Profile nhưng sau khi chúng thực tại DC thì DC sẽ xem user đó thuộc OU nào, GPO nào tác động tới. Nếu có GPO về FR thì user đó bị tác động (cấu hình dễ hơn, ít tốn thời gian hơn Roaming Profile)

**Triển khai:** tại 2 vị trí

**Vị trí 1 tại File Server:** Tạo folder lưu trữ, share Full Control (nhớ là không đung chạm gì đến NTFS) . Lúc này AD sẽ tự động khởi tạo folder ứng với tên user, tự phân quyền chỉ mình user tương ứng được truy cập.

**Vị trí 2 tại GPMC:** tạo GPO tác động lên OU có nhu cầu.

## Cấu hình:

**Bước 1:** Tạo Folder tên: RF và share full.

**Bước 2:** run -> gpmc.msc

Chọn OU KeToan -> **Creat a GPO ....**

Name: GPO 7: Folder Redirection -> Edit để cấu hình Policy

 FR 1  
Create GPO 7


**User Configuration -> Windows Setting -> Folder Redirection**

 FR 2  
GPO: Folder Redirection

Ta thấy tất cả các thông tin trong profile.

Ở tình huống trên ta chỉ muốn Roaming **Documents** nên ta cấu hình với Documents


Chọn **Documents** -> **Tab Target**

 FR 3  
Target Setting

Ta có 2 lựa chọn

**Basic:** Tất cả mọi folder profile của user trong các group trong OU sẽ cùng 1 nơi lưu trữ (thường dùng).Ta sẽ triển khai cái này

**Advanced:** Mỗi Group trong OU có 1 folder lưu trữ riêng

 FR 4  
Minh họa: Advanced

**Target folder location:** có 4 tùy chọn

 FR 5  
Target folder location

**Redirect to the user's home directory:** Nếu ta đã cấu hình Home Folder cho user thì hệ thống sẽ tự đưa các thông tin profile ta thiết lập vào thư mục home folder của từng người dùng.

**Create a folder for each user under the root path:** Tạo ra từng folder cho từng người dùng. (Lưu trữ profile trong folder ta chỉ định theo đường dẫn)

**VD:** 192.168.2.100\FR. Hệ thống sẽ tự tạo các folder tương ứng với tên người dùng.

**Redirect to the following location:** Tất cả profile sẽ chung 1 đường dẫn

**Redirect to the local profile location** ( tái định hướng quay về lưu trữ trên local). Mục đích ta dùng option này khi nào ???

\*\*\* Profile thì thông tin nặng nhất là application data. Ta muốn Romaing tất cả thông tin nhưng chưa lại folder Application Data. Ta sẽ cấu hình Romaing Profile rồi tạo GPO – Folder Redirection để Application ở option Redirect to the local profile location để folder này chỉ lưu trữ local.

Ta chọn **Create a folder for each user under the root path**

**\\192.168.2.100\FR**



Đánh lệnh: **gpupdate/ force**

Sau đó: đăng nhập KT1 để kiểm tra.

**Chú ý:** ta chỉ cần tạo policy trong Group Policies Objects rồi link đến các OU cho đỡ công cấu hình.

### Triển khai Script

Bản chất script là 1 file chứa đoạn code thực thi các công việc thường dùng. GPO có thể thông qua các đoạn script để tác động lên user, computer ( các đoạn script thường dùng: \*.bat, \*.vbs, v.v)

Ta muốn: rename, change password, disable account local administrator thì có thể dùng script để triển khai đến các member computer (automatic tác động)

Các đoạn script thường dùng được Microsoft public trên trang: <http://gallery.technet.microsoft.com/scriptcenter>

Script chỉ tác động đến user account và computer account và chỉ chạy trong **4 thời điểm**

**Đối với user account** (2 thời điểm): Khi log on hoặc log off.

**Đối với computer** (2 thời điểm) : khi khởi động hoặc chạy trước khi shut down.

**Triển khai:**

**Tạo file Map.bat** : New -> text.txt sau đó đánh lệnh: net use Z: \\192.168.2.100\Data

Sau đó đổi tên file thành \*.bat ( Map.bat)

Trên OU NhanSu tạo **GPO 8 : Script – MapNetworkDrive – Logon** (nghĩa là cứ mỗi lần user log on là chạy script Map.bat)



GPO: Scripts

Sau đó **Edit -> User Configuration -> Windows Setting -> Scripts**



**Double click vào log on (Log on Properties)**



**Do đã tạo sẵn file script (map.bat) ta chỉ cần bỏ file đó vào folder lưu trữ bằng cách chọn: Show File.**

Những script log on sẽ nằm trong folder Log on, những script log off sẽ nằm trong folder Log off. Cả 2 folder này đều lưu trong folder **Sysvol** của máy DC.



copy file script vào folder log on

**Sau đó quay lại cửa sổ Log on Properties**

Chọn **Add -> Browse -> chọn Map.bat -> OK**



 Script 5

Add scripts vào

Đánh lệnh : **Gpupdate /force**

Các bạn tự test kết quả.

**Ghi chú:** Muốn Rename các member computer thì tạo 1 OU rồi move các computer cần áp Policy vào:

 Script 6

# 18. Security Templates

**Chuẩn bị:** 1 máy PC chạy server 2012 ( domain hay workgroup đều được)

Vào Ổ đĩa C -> tạo folder: Templates.

## Tình huống:

Công ty yêu cầu chỉnh 1 vài **local security policy** cho các máy hay chỉnh local security policy cho khoảng 30 máy trong workgroup. Lúc này thay vì ta phải đến từng máy để chỉnh (để sai sót, tốn thời gian) thì ta có thể dùng Security Templates mà Windows hỗ trợ.

Security Template là các template (mẫu) chứa các cấu hình policy mẫu. Định dạng: \*.inf

## Cách triển khai:

### Bước 1: Tạo template mới

Cách tạo: dùng **MMC**

**Run -> mmc -> File -> Add/Remove Snap-in**

Add 2 công cụ: **Security Templates** và **Security Configuration and Analysis**. -> **OK**



Add Security Templates and Security Configuration Analysis



save cửa sổ console

Sau đó save console lại.

Mặc định các template sẽ được lưu trong **C:\Users\Administrator\Documents\Security\Templates**

Ta có thể chuyển nơi lưu trữ: Phải chuột Security Templates -> **New Template Search Path...** -> Chọn folder tùy thích. (Ở đây, ta sẽ lưu trên C:\Templates).

Phải chuột C:\Templates -> **New Template...**



Tạo Templates

Ta tạo 2 template:

Template 1: chứa policy chỉnh password đơn giản.

Template 2: chứa policy chỉnh password phức tạp.

Bung Template 1 -> Account Policies -> Password Policy : Chỉnh các policy như hình



Cấu hình Policy cho template

Sau đó ta: Phải chuột Template 1 -> chọn **Save** (để cập nhập cac2 policy vào Template 1)

Template 2 làm như hình và Save



**Để so sánh các policy trong Template với cấu hình policy hiện tại trong máy tính:** Ta dùng công cụ:

## Security Configuration and Analysis

**Chuột phải vào Security Configuration and Analysis -> Open DataBase -> Đặt tên là Database 1** ( giữ nguyên đường dẫn, chỉ cần đặt tên) -> Open



Tạo Database

Sau đó xuất hiện cửa sổ: **Import Template** ( ý là: bạn muốn đưa cái template nào vào Database: ở đây ta sẽ import template 2 vào Database)

Mục **Look in:** trở về **C:\Templates** rồi chọn Template 2 -> **Open**



Chỉ định template

**Lưu ý:** Để so sánh thì ta phải bỏ template vào Database thì mới so sánh được

Đường dẫn lưu Database như sau:



Sau đó: Phải chuột vào Security Configuration and Analysis -> Analyze Computer Now...

Xuất hiện bảng: lưu log file (nếu lam2co1 lỗi thì vào đó xem) -> OK



Thực hiện quá trình phân tích, so sánh security policy

Ta thấy cửa sổ so sánh rất trực quan: Gồm 3 cột. Bên trái là tên các policy (Policy), giữa là các policy trong database (Database Setting), bên phải là các policy đang được áp dụng trên máy tính (Computer Setting).

Nếu policy trong template khác với policy hiện hành thì sẽ có dấu "**chéo đỏ**"



Bảng so sánh Security Policy

**Nếu thấy chưa vừa ý thì ta lại chỉnh sửa các template lại, Save và Analyze như trên.**

**Nếu vừa ý rồi thì ta áp template vào computer.**

**Có 2 cách áp template:**

**Cách 1:** sử dụng **Security Configuration and Analysis**

Phải chuột **Security Configuration and Analysis** -> **Configure Computer Now..** -> **OK**

Vào **gpmmc.msc** để kiểm tra (nếu là domain) hoặc **gpedit.msc** (nếu là local computer).

Để áp template cho các máy khác, ta có thể copy template đến từng máy rồi dùng công cụ Security Configuration and Analysis để áp template.

Cách 2: vào **policy** -> **security setting** -> **import policy** ( hoặc vào **run** -> **secpol.msc** -> **import Policy** )



Import Policy

Để xuất cấu hình policy thành 1 file: ta chọn **Export List** ( có thể xuất ra các file khác nhau).



Export

**Lưu ý:**

- Domain Controller có 1 security policy template mặc định (quy định các security policy như password policy v.v). Templates này lưu trong đường dẫn:

**%systemroot%\Security\Templates**



Security Template của Domain Controller

- Vì đây là Security Template nên ta chỉ có thể tạo template cho các Security Policy thôi ( trong mục Security Settings

(run->secpol.msc)

# 19. Audit Policy – Giám sát hệ thống

## Chuẩn bị:

1 máy đóng vai trò Domain Controller + File server: **2012may1**

1 máy computer domain : **2012may2**

Vào ổ C -> tạo folder: Logs.

**Audit Policy** là những policy cho phép ta giám sát hoạt động của hệ thống, cũng như tương tác của người dùng, ghi nhận các hoạt động đó một cách có chọn lọc vào Security log.

## Mục đích chính:

+ Cung cấp chức năng giám sát hoạt động ( của hệ điều hành, của AD hay user v.v ) , ghi nhận các sự kiện để xác định nguồn gốc và thiệt hại của hệ thống.

## Vd:

Xác định vào giờ nào, ngày nào, user nào chỉnh sửa, xóa tài nguyên nào.

Xác định thiệt hại: file nào bị xóa, bị chỉnh sửa

+ Đề phòng các đợt tấn công trong server

Vd: User NS1 thường xuyên bị dò password, sử dụng Audit Policy ta có thể biết user NS1 bị dò vào thời điểm nào, vị trí nào đang dò v.v ( cung cấp thêm giải pháp giám sát ngoài việc dùng account lockout policy ra).

## Triển khai

### Run -> gpmmc.msc

Muốn giám sát trên DC nên ta sẽ thao tác trên OU Domain Controllers. Nếu muốn giám sát trên member computer thì Move vào OU nào đó rồi tạo GPO để Audit:

Phải chuột **Default Domain Controllers Policy** -> **Edit** -> **Computer Configuration (audit policy chỉ có ở mục này)** -> **Policies** -> **Windows Settings** -> **Security Settings** -> **Local Policies** -> **Audit Policy**.



Audit Policy

Ta thấy có các policy tương ứng với các mục đích giám sát khác nhau.

### Để đi thiết lập Audit Policy, ta cần lưu ý:

+ Giám sát sự kiện đó thành công hay thất bại ( success, failure)

Ví dụ: giám sát user bị dò password thì phải giám sát sự kiện đăng nhập thất bại.

+ Nếu là Workgroup thì chỉnh trên từng máy, Domain Network thì cấu hình GPO trên các OU chứa member computer cần giám sát.

+ Audit Policy chỉ tác động tới **Computer account**

+ Những sự kiện ta cần giám sát

Audit account logon event: (1)

Audit account management: (2)

Audit Directory Service Access (3)

Audit Logon event (4)

Audit object access (5)

Audit Policy change (6)

Audit privilege use (7)

Audit process tracking (8)

Audit system events (9)

Có 3 đối tượng mà Audit Policy đi giám sát: ( )

## User

## Hệ thống

### Ứng dụng có trên hệ thống

+ Để giám sát hoạt động của User ta có các Policy : **(1) ,(2), (4), (5), (7).**

Ví dụ:

Giám sát user sử dụng tài nguyên trái phép ( máy in, truy cập file server, v.v) ta dùng policy (5)

Giám sát user log on ta chỉ cần cấu hình policy trên DC (vì DC là nơi chứng thực).

+ Để giám sát hoạt động của hệ điều hành ta có các Policy: **(3) (6) (9).**

+ Để giám sát sự tương tác của ứng dụng nào đó trên hệ thống như thế nào ( dùng cho ngành phần mềm: lập trình mạng, windows, linux v.v) ta có **(8).**

Công cụ dùng để đọc thông tin, sự kiện ta ghi nhận thông qua Audit Policy: Event Viewer

Lưu ý: Sự kiện xảy ra ở đâu thì mở event viewer ở đó.

VD: giám sát user truy cập file server thì mở event viewer ở file server.

Để mở Event Viewer trên Server: ta vào **Server Manager -> Tools -> Event Viewer.**



A 2  
Event Viewer

Để mở trên các PC thường vào: **run -> compmgmt.msc -> Event Viewer** . Ta dùng cách này nếu như đang ngồi từ xa mà muốn xem **Event Viewer** của Server ( dùng Connect to ...)



A 3  
Remote

Cơ bản 1 máy tính cài HDH Windwos luôn có 3 loại log: **Application, Security, System**. Máy tính cài thêm dịch vụ gì thì sẽ xuất hiện thêm Event Viewer của dịch vụ đó.

Ví dụ: Domain Controller có thêm: Directory Service, DNS server v.v

Những sự kiện giám sát bằng Audit Policy đều lưu trong **Security Log**

Ta bung **Windows Logs -> Security**. Bên phải là những sự kiện mà mặc định hệ thống sẽ tự Audit.



A 4  
Security Log

Ta thấy sự kiện rất nhiều rất khó để học và quản lý, ta có nhu cầu lưu trữ thông tin giám sát **theo chuẩn thời gian** (theo chuẩn thời gian là tối ưu nhất) thì làm như sau:

Chọn vào **Security -> chuột phải Save All Events As ...**

Lưu vào folder Logs, ta đặt tên file theo chuẩn thời gian: **2014-09-17.**



A 6

Hệ thống cho phép ta lưu log dưới 4 dạng file

**Event Files (\*.evtx):** chỉ có thể đọc log file này bằng Event Viewer.

**Text (\*.txt):** có thể đọc bằng các chương trình soạn thảo nhưng các sự kiện đều ghi ra 1 hàng, rất khó đọc. ( không nên xài).

**CSV ( \*.csv):** cũng có thể đọc bằng các chương trình soạn thảo, nhưng các sự kiện trong file được cách nhau bằng phím tab. Nếu dùng phần mềm Exell hay ACESS v.v thì có thể lọc các sự kiện.



A 7  
Filter bằng exell

Nên dùng: **Event Files, CSV**

**Lưu ý:** các sự kiện mặc định có trên event viewer là do tác động của **GPO Default Domain Controller Policy**.

**Tình huống 1:** Giám sát người dùng đăng nhập không thành công trên hệ thống => tạo GPO tác động lên OU chứa DC.

**Run -> gpmmc.msc -> chọn OU Domain Controller -> Create a GPO ...**

**Name: GPO 10:** Giam Sat Dang Nhap Trai Phep.

Lưu ý:

**Do GPO: Default Domain Controller Policy** (đã có policy Audit) ở phía trên **GPO 10** nên những policy Audit của Default sẽ ưu tiên hơn policy Audit của GPO 10 => cấu hình rồi nhưng không tác động. Muốn GPO 10 tác động thì phải UP GPO 10 lên trên GPO Default ( vì nếu có conflict thì ở trên ưu tiên hơn)



Up GPO 10

### Edit GPO 10



GPO 10

Ta thấy mặc định là **Not Defined** (nếu Not Defined thì hệ thống sẽ giám sát những Audit policy mặc định có trên Default Domain Policy và Default Domain Controller Policy).

Tình huống của chúng ta là chỉ giám sát đăng nhập không thành công thì chọn Audit policy: **Logon Events** - > **Double click-> Check vào Define these policy settings** , ta bỏ **check success và failure** thì policy xuất hiện trạng thái **No Auditing**(không giám sát)



No Auditing

Vì mặc định hệ thống giám sát nhiều sự kiện nên ở GPO 10 ta chỉnh thành No Auditing hết để cho dễ đọc ( GPO 10 ưu tiên hơn)

**Rồi chỉnh Audit Account Logon Events** ( giám sát quá trình đăng nhập) là **failure**

**Audit Logon events** ( giám sát hoạt động của hệ thống: diễn ra bất cứ sự kiện chứng thực thực nào đều ghi nhận hết: vd đăng nhập lên file server v.v): **failure**

Đánh lệnh: **gpupdate /force**

Ta vào lại **Event Viewer -> Windows Logs -> Security -> Clear Log** : để xóa log cho dễ test các sự kiện.

### Test: ta giả vờ đăng nhập sai user NS1

Sau đó Refresh Event Viewer ta thấy các sự kiện, double click vào sự kiện bất kì



Event

Xuất hiện bảng chi tiết về sự kiện

+ **EventID**: để định danh loại sự kiện. VD: EventID 4625: sự kiện đăng nhập (logon).

+ **Nơi xảy ra sự kiện**

+ **Ngày giờ**

+ **Tài khoản liên quan đến sự kiện** ( NS1)

+ v.v

**=> Nhờ vậy mà ta có thể khoanh vùng vị trí, thời gian để có các biện pháp xử lý.**

### Tình huống 2:

Ta ủy nhiệm cho NS1 quản lý OU NhanSu, ta phải giám sát NS1 ( dùng policy **Privilege use**)

**Tình huống 3:** Có File Server, công ty có nhu cầu giám sát người dùng truy suất tài nguyên trên hệ thống ( GPO)

=> Ta phải thực hiện các hành động:

- + Giám sát hành động user đăng nhập lên file server
- + Giám sát user đăng nhập không thành công ( để biết ai cố tình đăng nhập khi không có quyền)
- + Giám sát user đăng nhập thành công (để biết ai xóa, chỉnh sửa trái phép dữ liệu)

#### Triển khai:

- + GPO tác động lên file server ( ở bài này là DC)

Trên máy DC :

Tạo folder: Data : Share everyone Full Control. Tab Security: xóa group Users

Add các user: NS1: Read and Execute. NS2: Modify.



Phần quyền File Server

- + Trong folder Data: tạo **t1.txt**

**Run -> gpmmc.msc -> Domain Controllers -> Edit GPO 10**

Vào **Audit Policy** -> ta **Defined** thêm **Audit Object Access (success và failure)** -> **Gpupdate /force**

Riêng **Audit Object Access** ta phải làm thêm hành động: **xác định tài nguyên cần giám sát và đối tượng cần giám sát**

**Properties folder Data -> Tab Security -> Advanced -> Tab Auditing.**



Audit

Để chỉ định đối tượng cần giám sát Chọn **Add ->**

**Select a principal:** ta add group: **Authenticated users**. ( => đã chọn xong đối tượng giám sát).

**Type:** loại giám sát: Gồm 2 loại **All, success, failure**.

**Basic Authentication ( hay Advanced Authentication):** giám sát hành động gì. Với tình huống trên thì ta cấu hình như sau

**Failure:** ta **giám sát Full Control** ( tất cả các hành động mà failure thì giám sát)

**Success:** ta nên giám sát các hành động như xóa, sửa, change permission . Ở ví dụ này ta cho Modify luôn cho dễ.

( Giám sát nhiều hành động, nhiều đối tượng thì add nhiều lần).

**Nhớ check vào: Apply these Audit Settings to object .....** để áp đặt vào các subfolder và file bên trong.



Chỉ định đối tượng giám sát và hành động cần giám sát

#### Test:

- + KT2 đăng nhập vào **2012may2**

- + \\192.168.2.100 => không vào được

Trên DC (2012may1)

Vào Event Viewer thấy rất nhiều sự kiện, ta cần filter sự kiện **failure** để xem bằng cách:

Vào Windwos Logs -> phải chuột Security -> Filter Current Log ....



Filter sự kiện đăngnhập file server (failure)



Chọn dòng **EventID 4656** Ta thấy Access: ReadData... nghĩa là KT2 thực hiện hành động read nhưng bị cấm ( Not granted>

Các bạn tự test trường hợp NS1 xóa file t1.txt

**Lưu ý:** nếu Add group Users, khi hệ thống giám sát thì sẽ dành vùng nhớ RAM lớn để giám sát tất cả account. Nếu chọn Authenticated thì ai logon mới giám sát, vùng nhớ Ram sẽ được giảm => tối ưu hệ thống.

Tài liệu tham khảo: [http://technet.microsoft.com/en-us/library/cc766468\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc766468(v=ws.10).aspx)



# 20. File Server Resource Manager

## Chuẩn bị:

2012may1 (chạy HDH 2012 hoặc 2012R2) và 1 máy client (hoặc server tùy ý: 2012may2). Cấu hình IP. Tạo folder Data và share (phân quyền tùy thích).

## Tình huống:

– Khi chúng ta cho phép user lưu trữ dữ liệu trên file server (dùng Map Network Drive), user có thể lưu trữ phim, video v.v làm tăng đáng kể dung lượng không cần thiết của file server. Vì vậy ta có nhu cầu áp đặt hạn ngạch lưu trữ cho user (Disk Quota – thiết lập hạn ngạch đĩa cho user lưu trữ).

– Hạn chế lưu trữ file theo định dạng (vd: cấm file exe, cấm flv v.v).

Để giải quyết tình huống trên, ta chỉ cần cấu hình FSRM.

FSRM là tính năng có từ windows server 2008. FSRM có thể triển khai trên môi trường Workgroup hoặc Domain.

## Triển khai:

Trên **2012may1**

**Cài đặt Role:** File server resource manager


Vào Server Manager (2012may1)

Chọn Manager -> Add Roles and feature


Next mặc định đến:

– Server Roles: bung File and Storage service -> File and ISCSI Services -> Check vào File and Resource manager


Xuất hiện bảng yêu cầu add thêm các feature cần thiết -> Add feature ->Next

 FSRM 3  
Add role FSRM

– Features: để mặc định ->Next. rồi **Install** (Cài xong bấm Close)

 FSRM 4  
Install FSRM

Sau khi cài xong, quay lại cửa sổ Server Manager -> chọn Tool -> **File Server Resource Manager**

 FSRM 5  
Giao diện FSRM

**Quota Management:** thiết lập hạn ngạch cho ổ đĩa, folder. Để thiết lập hạn ngạch thì ta phải tạo **Quota Templates**

**Bước 1:** tạo Quota Templates

– Mặc định Windows cung cấp cho ta 1 số templates, nếu không thỏa nhu cầu ta phải tạo mới

 FSRM 6

– Phải chuột Quota Templates -> **Create Quota Template**


Template name: tùy ý (mình đặt Quota 3MB)

**Space limit:** chỉnh hạn ngạch, nếu chỉ cho phép 3MB thì chọn 3MB.

**Hard Quota:** không cho phép người dùng sử dụng quá hạn ngạch.

**Soft Quota:** cho người dùng vượt quá hạn ngạch (dùng để monitor những người dùng vượt quá quota cho phép)

**Notification Threshold** (ngưỡng cảnh báo, nếu dung lượng đến 1 ngưỡng nào đó sẽ cảnh báo đến người dùng) -> add

 FSRM 7  
Tạo quota template

Chọn Hard Quota.

Ta bấm Add để tìm hiểu tiếp



Generate notification when usage reached: 85 ( dung lượng đến 85% hạn ngạch thì gửi cảnh báo

- có thể gửi mail đến admin (send email to following administrator)
- gửi đến người dùng (dòng dưới).

Qua Tab Report: check vào generate report

Ta cần chú ý 2 giá trị

- Files by owner và Quota usage: nếu chọn 2 cái này thì khi gửi cảnh báo nó sẽ gửi thông tin gồm: tên người sử dụng và % dung lượng có thể sử dụng.



Ở ví dụ này ta không dùng Notification Threshold nên để mặc định.



Cấu hình xong template

## Bước 2: cấu hình Quota.

Chuột phải vào Quota -> **Create Quota**

**Quota path:** Browse về folder **Data** (đã tạo từ đầu).

**Derive Properties from this quota template:** chọn "Quota 3MB" vừa tạo



-> **Create**



**Test:** 2012may2 cấu hình Map network drive:



Quay về cửa sổ FSRM, chọn **File Screening Management (cấu hình sàng lọc file)**

## Bước 1: ta cấu hình File Group ( định nghĩa các nhóm file)

Chọn **File Groups:** Windows cũng định nghĩa hầu hết các loại file. Ta có thể bỏ bước này nếu không có nhu cầu khác của windows.



Ta có thể tự định nghĩa bằng cách -> **Create File Group**

**File group name:** thực thi

**File to include:** ( các file trong file group) \*.exe ( tất cả file có đuôi exe).

**File to exclude:** \*.bat -> OK



## Bước 2: Tạo File Screen Template

Bước này ta sẽ làm hành động: cho phép hay cấm các file nào.

( mặc định Windows cũng cung cấp cho ta 1 số template). Để tự định nghĩa ra template ta làm như sau

Chọn **File Screen Template -> Create File Screen Template**

**Template name:** Cam File nguy hiem

**Screening type:**

+ **Active screening:** không cho phép user lưu file

+ **Passive screening:** cho phép user lưu file

**File Group:** ta chọn "**thuc thi**" vừa tạo ở trên => ý nghĩa là: **cấm các file \*.exe** -> OK



### **Bước 3: Thực hiện hành động: gắn vào folder nào**

Chọn **File Screen** -> **Create File Screen** -> Browse về folder Data

**Derive Properties:** chọn "Cam File nguy hiem" -> **Create**

Ý nghĩa: **cấm user lưu trữ \*.exe lên folder Data.**



Các bạn tự test trường hợp: KT1 copy \*.exe vào folder KeToan trong Data.

### **Lưu ý:**

+ Admin lưu \*.exe vào folder Data cũng không được

+ Hạn chế của FSRM là user đổi đuôi file: \*.exe thành \*.exe1 thì copy vào Data được => điểm hạn chế khi triển khai.

+ Cấu hình trên từng folder của user ( nếu đang triển khai home folder). Nếu cấu hình 1 folder cha (Data) thì khi cho phép 10 Gb thì FSRM sẽ hiểu là tổng dung lượng là 10 Gb chứ không phải mỗi home folder của user được phép chứa 10 Gb dữ liệu.

+ Để dễ nhớ cách cấu hình FSRM, ta sẽ cấu hình từ dưới lên ( vd: file group rồi mới tới file screen template).

### **Bonus:**

Ngoài việc triển khai FSRM để áp đặt quota thì windows cũng cấp cho chúng ta chức năng Quota.

Chọn ổ C -> **Properties** -> **Tab Quota**

**Enable quota management:** bật chức năng quota trên ổ đĩa.

**Deny disk space to users exceeding quota limit:** nếu user đến hạn quota thì không cho sử dụng nữa. Nếu không check thì user vẫn có thể lưu trữ khi vượt quá quota quy định.

**Limit disk space to:** đặt quota: ta cho 100Mb ( lưu trữ bất cứ folder nào nhưng tổng các file không được quá 100Mb)

Nếu ta check vào ô Log thì khi user đến hạn quota thì sẽ tạo ra log file cho admin.



Khi cấu hình thế này thì ta đã áp quota cho tất cả user là 100Mb. Ta muốn set quota khác nhau cho các user khác nhau thì chọn **Quota Entries**.

### **Ở cửa sổ Quota Entries**

Để xét riêng cho user NS1 có quota là 200Mb còn user khác là 100Mb thì chọn **Quota** -> **New quota entry** -> add NS1 rồi chỉ định quota 200Mb

Ông Sếp không muốn bị áp quota: add user Sep rồi chọn **Do not limit disk usage**

### **Lưu ý:**

Quota trên Ổ đĩa khác với FSRM là chỉ có thể áp lên ổ đĩa, FSRM có thể áp lên folder. Theo cá nhân mình thì kết hợp Quota và home folder là tốt nhất.

# 21. Monitor Server Performance

Monitor Server Performance ( giám sát hiệu năng máy chủ) **Chuẩn bị:** 1 máy chạy HDH server 2012.

## Mục đích của việc giám sát hiệu năng:

- + Giám sát hoạt động của server về phần cứng (để ghi ra những chỉ số cụ thể). Để khi có sự cố, khi có sự phàn nàn của người dùng thì ta lại monitoring một lần nữa để có được chỉ số trong thời gian người dùng phàn nàn rồi so sánh với chỉ số ban đầu ( để việc đề xuất mua thiết bị có sức thuyết phục hơn).
- + Xác định thành phần nào gây ra hiện tượng hoạt động kém đối với server. CPU, Ram, Ổ cứng v.v. Vậy ai gây ra ??? . Nhờ các chỉ số so sánh ta có thể biết được thủ phạm .

Trên 1 server hay máy tính bất kì ta có **4 thành phần** cần quan tâm:

- + RAM
- + CPU
- + Physical Disk (Ổ cứng vật lý).
- + Card mạng (NIC)

Ram, Cpu, Ổ cứng: quyết định trực tiếp đến hiệu năng máy tính. NIC quyết định đến chất lượng mạng (nếu copy qua mạng chậm thì do NIC gây ra nhiều nhất, sau đó là ổ cứng rồi đến cpu, ram.)

Khi giám sát (monitor) ta có công cụ rất quen thuộc là **Task Manager**. Task Manager chỉ giám sát thời gian thực. Muốn đi giám sát chính xác thì cần có thời gian lâu dài rồi tính giá trị trung bình cho nó.

Công cụ Windows hỗ trợ để xét hiệu năng là: **Performance Monitor**. Có 2 cách mở

**Cách 1:** perfmon.msc

**Cách 2:** Mở Server Manager -> Performance Monitor Mỗi một phần cứng có nhiều giá trị để giám sát, ta cần nhớ các giá trị quan trọng sau:

+ **RAM:** Giá trị cần quan tâm: **Pages/Sec (second)**. Giá trị cho phép : 0->20. Càng thấp càng tốt. Mới mua về mà >20 thì đầu tư server thiếu RAM.

+ **CPU:** Giá trị cần quan tâm: **%Processor Time**. Giá trị cho phép: <85%. Càng thấp càng tốt. Nếu chỉ số > 85% => tốc độ xử lý cpu yếu. Cần nâng cấp cpu ( thêm cpu hoặc thay cpu mới).

+ **Physical Disk:**

Ta cần quan tâm 2 giá trị

**% disk time:** Giá trị cho phép : < 50% càng thấp càng tốt

**Current Disk Queue Length:** ( còn gọi là Average disk Queue length). Giá trị cho phép từ 0->2. Càng thấp càng tốt

Nếu %disk time cao >50%: tốc độ vòng quay của ổ cứng (HDD) không đủ nhu cầu truy suất trên hệ thống (chậm quá) Current disk Queue length >2: thông số kĩ thuật trên ổ cứng không hợp lý ( cụ thể là thông số cache, cache nhỏ => Current disk Queue length lớn, mỗi lần cpu cần truy suất thông tin ổ cứng thì đợi rất lâu => làm treo máy, windows tự restart ( do cpu không có dữ liệu xử lý, hdd tưởng là bị lỗi nên sẽ restart).

## NIC (network interface)

Ta cần quan tâm đến giá trị: **Bytes Total/sec:** càng cao càng tốt. Không có giá trị cụ thể. Thời gian đầu mới mua, ta đo giá trị Bytes Total/sec , ta sẽ đặt nó làm giá trị ban đầu gọi là X (phải thỏa tiêu chuẩn của Microsoft cộng với việc 100% người dùng hài lòng với chất lượng truy suất mạng thì giá trị này X mới thỏa yêu cầu). Sau thời gian sử dụng, nếu người dùng than phiền thì ta lại so sánh giá trị hiện tại với giá trị X. Nếu thấp hơn thì cần nâng cấp.

## Triển khai:

Run -> perfmon.msc Bung Monitoring Tools -> Performance Monitor .

Ta có 2 chế độ giám sát

### 1/ Real Time Mode ( giám sát theo thời gian thực)


- + Dùng **Task Manager**
- + Dùng **Performance Monitor**

performance 1

Chọn vào đồ thị -> Properties

performance 2


Tab Graph, bung View , Windows cung cấp cho ta 3 dạng biểu đồ để giám sát

performance 3


+ Line: dạng đồ thị (mặc định)

+ Histogram Bar: dạng biểu đồ cột

+ Report : chỉ xuất ra dạng số

performance 4  
dạng Report

Mặc định Performance Monitor chỉ giám sát CPU theo thời gian thực, muốn xem các chỉ số khác ta làm như sau. Chọn vào đồ thị ->

Add counters. Giả sử ta muốn giám sát thêm Memory (add Pages/sec) performance 5

Các thành phần giám sát sẽ chung 1 bảng đồ thị ( chung 1 hệ trục), ta cần đổi màu cho từng thành phần

Chọn Pages/sec -> Properties -> **Tab Data**

performance 6

performance 7

**Lưu ý:** Khi dùng Performance Monitor giám sát card mạng, nếu server có nhiều card mạng thì cũng chỉ có 1 hệ trục duy nhất. Khác với Task Manager, nhiều card mạng thì có nhiều bảng giám sát.

**2/ Logging Mode** ( chế độ giám sát ghi vào log file). Đây là chế độ không chỉ giám sát mà còn ghi lại các giá trị

Để triển khai Logging Mode, ta cần tạo các **Data Collector**.

Một Data Collector bao gồm 2 yếu tố

+ **Object:** đối tượng cần giám sát.

+ **Counter:** thông số cần ghi nhận

performance 8

**Data Collector Set:** là tập hợp các Data Collector


Mặc định hệ thống cấu hình sẵn 1 số Datacollector, Để tạo Data Collector Set theo ý mình.

Ta chọn **User Defined -> New -> Data Collector Set**

**Name:** Monitoring System. Check vào Create Manually ( vì ta sẽ giám sát theo ý mình, không làm theo templates). -> NEXT

performance 9

Chọn **Performance Counter** để giám sát hệ thống -> Finish


 performance 10

Chọn vào **Monitoring System** vừa tạo -> **New -> Data Collector**

 performance 11

 performance 12

Cửa sổ **Create New Data Collector -> Add**

 performance 13

Add các thông số như hình

Riêng với Network Interfaces -> ta chọn Counter rồi chỉ định Card mạng nào muốn giám sát ( muốn giám sát bao nhiêu card thì add thêm bấy nhiêu lần).

Lưu ý: Logical Disk dùng để giám sát các phân vùng của ổ cứng, nhờ đó mà ta có thể xác định phân vùng nào là nguyên nhân, ta cũng có thể xác định được ứng dụng hay dịch vụ nào đang yêu cầu (request).

Physical Disk: giám sát cả ổ cứng. Ở vd này ta chọn Logical Disk.


-> **NEXT**

 performance 14

**Sam Interval:** bao nhiêu lâu thì ghi dữ liệu 1 lần. Ta để mặc định 15 giây để test ( thực tế nên để 15 phút).

-> **Next**

Check vào: Open properties for this data collector -> **Finish**

 performance 15

Chọn vào Data Collector "**Performance**" vừa tạo -> **properties**

Log Format: chọn **Tab Seperated** để có thể đọc file log bằng phần mềm Microsoft Excel.

 performance 16

Sau đó chọn **Data Collector Set " Monitoring System" -> Properties**

**Tab Directory**

**Root Directory:** nơi lưu trữ log file ( ta có thể chỉnh sửa nơi lưu trữ). Mặc định lưu ở: %systemdrive%\Perflogs.


Để lập lịch biểu chọn tab Schedule: dùng để lập lịch cho Data Collector Set chạy

 performance 17


Cứ 10h là chạy. Chạy từ 9/10 -> 31/10. Chạy từ thứ 2 -> thứ 6. Apply -> OK

Cách Test:

chọn vào Monitoring System -> **Start** ( để khoảng 1 phút).

 performance 19

Sau đó **stop** rồi mở log file bằng excel.

 performance 20

Để cột Network có giá trị thì chúng ta phải copy 1 file nào đó qua mạng ( từ server qua client).

Tài liệu tham khảo: Ebook MOC

## 22. Remote Desktop Service

Chuẩn bị:

máy DC: 2012may1

computer member domain: 2012may2

Remote Desktop Service

Hệ thống gồm có các server và client.

### Tình huống 1

Admin đang ngồi trên client 1, muốn kết nối đến các server để cấu hình thì dùng chức năng Remote Desktop kết nối đến các server. Đây là chế độ thứ nhất gọi là **Administration Mode**: được thiết kế để các quản trị viên cấu hình trên các server

#### Đặc điểm:

- + Tích hợp sẵn trong server (free)
- + Mặc định cho phép tối đa 2 kết nối đồng thời .

### Tình huống 2

User muốn sử dụng bộ Microsoft office. Ta có thể cài từng máy ( mua license từng máy thì quá đắt). Ta có thể cài trên server, và cho phép user sử dụng chương trình ngay trên server ( mua license office, license cho các kết nối sử dụng office). Chế độ mà user sử dụng office trên server gọi là **Application Mode**. Giải pháp này được xem là giải pháp ảo hóa ứng dụng

#### Đặc điểm:

- + Cài đặt thêm các Role Service, free 120 ngày, phải mua license
- + Số kết nối phụ thuộc vào license ( mua license cho Remote Desktop và license cho số lượng kết nối)

Ngoài ra, giải pháp ảo hóa người dùng ( Virtual Desktop Infrastructure) cũng sử dụng Remote Desktop Service (có từ server 2008R2 trở lên)

Ở bài này, mình sẽ trình bày về **Administration Mode** trong RDS.

#### Ghi chú:

**Remote Desktop Service** (RDS) từ win 2008 SP2 trở về sau có tên là **Terminal Service**. Nó chỉ được đổi thành RDS từ 2008R2.

### Cách triển khai Remote Desktop (Administration Mode) :

Trên Server

run -> sysdm.cpl -> tab Remote

Mặc định hệ thống không cho phép các kết nối từ xa.

Ta chọn Allow remote connections to this computer



Ta thấy có option: **Allow connections only from.....** : chỉ cho phép các máy tính sử dụng có chế NLA remote vào hệ thống

**Network Level Authentication** (NLA). Chứng thực ở cấp độ Network. Như đã biết, mô hình OSI gồm 7 lớp (Application, Presentation, Session, Transport, Network, Data Link, Physical). Khi server tiếp nhận kết nối, thông tin sẽ chuyển từ layer 1 sang layer 7 ( Remote Desktop protocol nằm ở layer 7).

Khi client thiết lập kết nối đến, giao tiếp được với remote desktop protocol rồi tức là lúc đó phiên làm việc đã bắt đầu. Sau đó RDP mới gửi yêu cầu tới hệ thống để chứng thực user. Nếu chứng thực thành công thì RDP mới bắt đầu hoạt động. Đây là cách hoạt động khi không có NLA ( **kết nối sau đó mới chứng thực**).

Đến thời server 2008, nhận thấy những hacker có thể lợi dụng việc **kết nối sau đó mới chứng thực** để tấn công Denial Of Service: kết nối liên tục để làm cho RDP bận liên tục, từ chối tiếp nhận những kết nối hợp lệ. Cơ chế để NLA giải quyết chuyện này như sau: Khi kết nối đến layer Network thì hoạt động chứng thực đã được yêu cầu, vì thế lúc đó RDP chưa can thiệp => không thể DOS được RDP.



NLA chỉ khả thi khi server là 2008 và client là XP SP3 trở lên ( XP SP3 phải cấu hình thêm registry)

Chọn **Select user** để add user ta muốn cho remote vào server

Hoặc có thể add user đó vào group **Remote Desktop Users (Trong Local Users and Groups của máy đó)**. Để add user vào group Remote Desktop Users trên Local cho nhiều máy, thì ta có thể cấu hình Restricted Group Policy trong gpmmc.msc (thay vì phải vào từng máy add)

Ta add KT1@tuhocmang.local vào

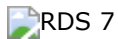


Ghi chú:

- RDP sử dụng TCP port 3389
  - Cần chú ý các policy sau:
    - + Allow log on through Remote Desktop Service (mặc định cho phép group: Administrators và Remote Desktop Users)(1)
    - + Deny log on through Remote Desktop Service
    - + Account: Limit local account use of blank passwords to console logon only.
- (nếu cấu hình trên DC thì vào OU Domain Controller chỉnh GPO như chúng ta đã biết)
- Ở các server thường: mặc định là admin được kết nối RDS.
  - Ở Domain Controller: mặc định không có đối tượng nào được remote (kể cả admin, muốn cho remote phải vào chỉnh Policy (1) trong Default Domain Controller Policy).
  - Firewall sẽ tự động mở port khi có kết nối Remote Desktop.

### Test:

KT1 đăng nhập rồi: run -> mstsc (remote desktop connection), điền thông tin user, password



Từ Server 2012 trở lên thì công cụ Remote Desktop Service Manager không tồn tại. Vậy nếu ta muốn tắt phiên làm việc từ xa của 1 user thì làm như sau.

Mở Task manager -> Tab User -> Disconnect ( làm trực tiếp trên máy bị remote)



# 23. Windows Routing – Phần 1

**Router gồm 2 loại: router cứng** (cisco, juniper, hp .v.v.) và **router mềm** (các máy tính cài phần mềm để làm chức năng định tuyến)

Các thành phần cơ bản của 1 router:

+ **Routing interface** (có thể hiểu đơn giản là card mạng): Là nơi giao tiếp giữa router với các phân đoạn mạng.

+ **Routing table**: bảng định tuyến, là nơi lưu trữ các đường đi đến các lớp mạng mà router dùng để định tuyến các gói tin.

+ **Routing protocol**: Các giao thức để định tuyến, gồm 2 loại

**1/ static route**: cấu hình bảng định tuyến bằng tay cho router

**2/ dynamic route**: router tự động tìm đường rồi bổ sung vào bảng định tuyến. Các giao thức thường dùng: EIGRP (cisco), OSPF, RIP


Windows Server hỗ trợ 2 giao thức: OSPF và RIPv2.

Lưu ý: Không phải router mới có routing table mà máy PC cũng có routing table. Hai máy tính cùng NetID muốn ping thấy nhau cũng cần có routing table. Khi ping thì máy PC sẽ mở routing table của chính nó ra để xem xét đi hướng nào.

Để xem routing table trên máy tính (cả windows, linux) ta dùng

**netstat -rn**

Riêng trên windows, ta có thể dùng lệnh **route print**

 routing windows 1

Có 5 cột:

**1/ Network Destination**: Chứa thông tin các NetID mà máy tính có thể biết.

Có 2 dạng NetID hoặc IP của 1 máy tính cụ thể.

NetID: 0.0.0.0: là super net, chứa tất cả NetID. Dòng này chỉ có khi ta khai báo default gateway trên PC.

**2/ Netmask**: subnet mask của Network Destination.

**3/ Interface**: Nơi xuất phát của gói tin.

VD: để đi đến 192.168.1.55 thì phải xuất phát từ cổng có IP là 192.168.1.102

**4/ Gateway**: Nơi chuyển tiếp gói tin (là địa chỉ IP của con router)

**5/ Metric**: Nếu có nhiều route đến cùng 1 đích thì route nào có metric thấp hơn sẽ được ưu tiên.

**Ghi chú**: Router tự nhận biết các phân đoạn mạng kết nối trực tiếp đến nó.

Vậy là xong phần cơ bản rồi, giờ chúng ta bắt đầu cấu hình với mô hình sau:

Sẽ có 2 mô hình cho bài học này.

**Mô hình 1 (đơn giản)**

 so do routing đơn giản

**Mô hình 2**: Chúng ta sẽ làm Lab theo mô hình này

 so do routing phức tạp

Ở đây mình nhằm: Server 2: 192.168.3.2

## Chuẩn bị theo mô hình

– Router 1 và Router 2 sử dụng **windows server 2012R2**.

– Add 2 card mạng cho mỗi Router.

VD: Router 1: Nic 1 + Nic 2. Router 2: Nic 2 + Nic 3.

– Server 1: trở gateway về 192.168.1.1

– Server 2: trở gateway về 192.168.3.1


Tính năng để giúp Windows server biến thành Router là **Routing**.

Để cài đặt tính năng này ta làm như sau:

Cửa sổ Server Manager -> Manager -> Add Roles and Features


Ta bấm **Next** mặc định đến


Server Roles: Check Remote Access (Nếu xuất hiện bảng thông báo add thêm các thành phần bổ sung thì ta nhấn add)

routing windows 2


Ta **Next** mặc định cho đến : **Role Services**, check vào **Routing**

Sau đó Next hết rồi **Finish**.

routing windows 2

routing windows 3

Quá trình cài đặt đang diễn ra

routing windows 4

Sau khi cài xong, máy tính đã biến thành router mềm.


Tương tự ta làm cho con còn lại.

## 24. Windows Routing – Phần 2

Ở phần 1, chúng ta đã cùng nhau cài đặt tính năng **Routing and Remote Access, Lan routing** trên **Server 2012** để giúp máy tính biến thành router ảo. Tiếp theo phần 2 của **Windows Routing**, chúng ta sẽ cấu hình tính năng **Lan routing** để định tuyến các phân đoạn mạng trong hệ thống.

Để vào **Routing and Remote Access** trên **Server 2012** làm như sau: **Run (Ctrl + R)-> rrasmgmt.msc**


Giao diện Routing and Remote Access

 routing windows 5

Giao diện Routing and Remote Access


Mặc định tính năng bị disable, ta chọn **Configure and Enable Routing and Remote Access**

Xuất hiện bảng điều khiển -> Next

 routing windows 6

Các tính năng trong routing and remote access: gồm có Dial-up (quay số ), VPN, NAT...


Ta chọn **Custom Configuration**

 routing windows 7


Các tính năng có thể cấu hình (1 hoặc nhiều): VPN, Nat, routing.

Ta chọn Lan routing.

Nếu chỉ check Lan routing mà về sau muốn cấu hình thêm VPN thì các bạn không cần cấu hình lại vì vào bên trong sẽ cho phép ta cấu hình bổ sung

 routing windows 8

Finish.


 routing windows 9

Giao diện sau khi Enable Routing and Remote Access


Network Interfaces: liệt kê các card mạng của máy tính.

IPv4: Các tính năng dùng IPv4

IPv6: Các tính năng dùng IPv6

 routing windows 11

Trường hợp này, máy tính có 2 card mạng nên trong Network Interfaces sẽ xuất hiện 2 card.

 routing windows 12

**Bây giờ, ta bắt đầu cấu hình theo mô hình đã chọn ở Phần 1:**

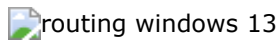
 so do routing phuc tap

Server 2: 192.168.3.2 (chứ không phải .1.2)

Trước hết chúng ta sẽ cấu hình Static Routes trên Routing and Remote Access

### Trường hợp 1: Cấu Hình Static Routes

Static routes -> New static route



Chúng ta cùng phân tích:

Router 1 muốn đến được Server 2 thì phải hỏi Router 2.

Chúng ta bắt đầu add route.

**Interface:** gói tin sẽ ra bằng ethernet 2 (tức là card mạng có IP là: 192.168.1.1)

**Destination:** Nơi đến có thể là 1 host hay 1 subnet

Nếu là 1 subnet: thì làm như hình

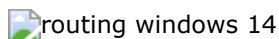
Nếu là 1 host (dùng để cô lập, chỉ cho phép định tuyến đến 1 host duy nhất):

Destination: 192.168.3.2

**Network mask:** ta đánh: 255.255.255.255.

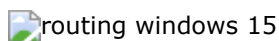
**Gateway:** địa chỉ IP của router kết tiếp (tức là con router mà ta hỏi đường)

**Metric:** độ ưu tiên. Nếu có 2 route cùng đến 1 destination, route nào có metric nhỏ hơn sẽ ưu tiên hơn.

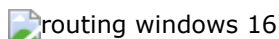


Sau khi cấu hình xong phải Restart lại **routing and remote access**

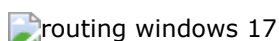
**All Tasks -> Restart**



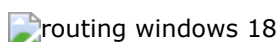
**Chúng ta ping thử từ router 1:**



Vào **Static Routes -> Show IP Routing Table...** để xem bảng định tuyến của Router 1



**Ở router 2, muốn đến được Server 1, ta làm tương tự**

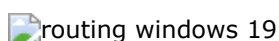


Trường hợp 2: Dynamic Routing Protocol. Microsoft hỗ trợ: Rip V2, OSPF.


Chúng ta sẽ cấu hình Rip V2.

Trên ROuter 1:


Chọn **General -> New Routing Protocol.**




**Chọn RIP Version 2 for Internet Protocol**

routing windows 20

Sau đó chọn RIP -> New Interface..

routing windows 21

Ta sẽ chọn card mạng dùng RIP. Ở đây **Router 1** giao tiếp với **Router 2** để trao đổi bảng định tuyến qua **Ethernet 2** bằng giao thức **RIP** nên ta sẽ cấu hình Ethernet 2 sử dụng RIP

routing windows 22

Cấu hình tổng quan RIP


Để mặc định là có thể chạy. Ở đây, mình giải thích 1 số option:

Periodic update mode: option cho phép trong 1 khoảng thời gian nào đó, Router 1 sẽ update bảng định tuyến qua Ethernet 2 và gửi cho neighbor là Router 2 (mặc định là 30 giây, ai học CCNA sẽ biết ).

Incoming Packet protocol: có thể chọn update bằng broadcast hay multicast. (Vì mặc định Rip v1: broadcast 255.255.255.255, Rip v2 multicast 224.0.0.9). Ở đây ta chọn update gói tin = RipV2 broadcast

Incoming Packet protocol: RIp v1 and 2: nhận update = V1, V2

Activate Authentication: Chứng thực xong mới update, ở đây không cần nên bỏ trống.

routing windows 23

**Ở router 2 làm tương tự là xong.**

Để hiểu rõ các option, các bạn nên tìm hiểu về RIP, OSPF thêm (**lâu không dùng nên mình cũng quên rồi, đang ôn lại** )

### **Bonus**

Để **add route** bằng command line: tham khảo lệnh **route add** và lệnh **netsh interface**, 2 lệnh này rất cần nếu hệ thống đang triển khai router dựa vào windows server

# 25. Distributed File System (DFS)

DFS (Distributed File System): Hệ thống file phân tán có từ thời 2k8.

Đối tượng triển khai: **File Server**

Mục đích triển khai: Hướng đến 2 mục tiêu (hoặc 1 trong 2).

**Mục tiêu 1:** Chia tải và chịu lỗi

+ **Chia tải** (Load Balancing): tại 1 thời điểm, nếu file server chỉ có 1, nó tiếp nhận quá nhiều kết nối thì sẽ xử lý không nổi => ta nên xây dựng từ 2 file server trở lên để có thể chia tải

=> dữ liệu trên các file server cần phải đồng nhất ( muốn đồng nhất thì admin copy từ server này sang server kia nếu có sự thay đổi !!!! )

+ **Chịu lỗi** (Fail Over): Nếu có 1 file server mà bị chết bất ngờ thì tiêu... Ta cần nhiều server để dự phòng => dẫn đến server 1 hỏng thì phải thông báo cho user để họ chuyển sang truy cập server khác !!!!).

Chỉ riêng việc chia tải và chịu lỗi cũng làm một admin rồi

DFS giúp ta chia tải tự động, đồng bộ dữ liệu tự động. Chịu lỗi trong suốt đối với user ( 1 server chết thì user cũng không biết, vẫn có thể truy suất file server bình thường).

**Mục tiêu 2:** Tập hợp dữ liệu

Công ty có nhiều chi nhánh, mỗi chi nhánh có 1 file server => dữ liệu trên các file khác biệt nhau

Tại văn phòng chính, ta muốn dữ liệu trên các file server của chi nhánh tập hợp về văn phòng chính

Ta có 2 cơ chế làm việc này

+ Nhân viên cắm USB đến các chi nhánh copy dữ liệu mỗi chiều ( !!!! )

+ Tự động tập hợp về văn phòng chính ( **dùng DFS** ).

Mình đã trình bày mục đích cũng như tình huống để sử dụng DFS. Ta hãy cùng tìm hiểu về các khái niệm liên quan đến DFS

**Namespace:** đường dẫn luận lý mà user sẽ truy cập.

Trong namespace là cây thư mục

Có 2 loại thư mục:

+ **Loại 1:** Chỉ mang tính chất cấu trúc ( chỉ dùng để bố trí, phân nhóm, sắp xếp dữ liệu)

+ **Loại 2:** Có target folder – Là 1 share folder ( dữ liệu lưu trữ ở file server).

Namespace được lưu trữ trong **Namespace Server**

Namespace Server quản lý Namespace và đường dẫn vật lý đến các target folder (Namespace server được xem như **người dẫn đường**)

**Yêu cầu khi triển khai DFS:**

+ Số lượng File Server ít nhất là 2 trở lên.

+ Namespace Server nên có 2 cái trở lên ( vì nếu 1 cái thì khi hỏng sẽ không thể dẫn đường đến các file server)

Có 2 loại môi trường:

**Stand Alone:** dành cho các server ở workgroup muốn triển khai DFS ( chỉ có thể tạo 1 namespace server)

**Domain:** có thể tạo 2 namespace server trở lên

Có thể tích hợp : **File server vào namespace server**

**Thực tế khi triển khai DFS:** ta cần 2 server vật lý. Trên mỗi server ta sẽ đồng thời là file server và namespace server (như vậy ta có 2 file server, 2 namespace server).

Cấu trúc namespace sẽ được lưu trữ trên namespace server trong thư mục **DFS root**. Nó chứa cấu trúc dữ liệu lưu trữ trên file server.

Nếu lấy Namespace server và File server chung 1 máy thì thường hay bị nhầm lẫn giữa **cấu trúc namespace** với không gian lưu trữ dữ liệu (file server) => dẫn đến việc admin nhầm lẫn cấu hình cho phép người dùng lưu trữ trên DFS root (DFS root để quản lý nên chỉ những người có chức năng mới được cấp quyền).

**Replication Group:** là thông số sẽ xác lập việc đồng bộ giữa các file server bao gồm 3 yếu tố:

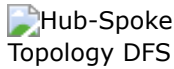
+ **Yếu tố 1: Các file server nào, đồng bộ các folder nào**

+ **Yếu tố 2: Topology** : là cấu trúc mà các server trao đổi thông tin. Gồm **3 loại**:

**1/ Hub-Spoke:** ( Các Spoke đồng bộ về Hub)

Điều kiện: ít nhất 2 spoke member và 1 hub member ( tối thiểu 3 máy).

Dùng trong trường hợp: tập hợp dữ liệu( tập hợp dữ liệu ở chi nhánh (Spoke) về văn phòng chính (Hub).



**2/ Full Mash:** (Bao nhiêu server cũng được)

Một Server sẽ đồng bộ với mọi server còn lại

Dùng cho mục tiêu chia tải và chịu lỗi

**3/ Custom:** Giống Full Mash nhưng bỏ vài hướng kết nối. Chúng ta có thể tự mình tạo cơ chế đồng bộ dựa vào dạng này (VD: Ring topology)

+ **Yếu tố 3: Cơ sở cho hoạt động đồng bộ.** Có thể chọn 1 trong 2

**a/ Percent Bandwidth:** định ra hoạt động đồng bộ sẽ chiếm bao nhiêu phần trăm (%) trong tổng băng thông khả dụng (Bandwidth). Hoạt động đồng bộ sẽ thực hiện 24/7. Thường dùng cho mục tiêu chia tải và chịu lỗi.

**b/ Schedule:** chạy theo lịch đặt sẵn, khi chạy sẽ chiếm 100% bandwidth.

Dùng cơ sở này cho mục tiêu tập hợp dữ liệu( vd: cứ 10h tối là các spoke sẽ tập hợp dữ liệu về Hub)

**Triển khai:**

**2012may1:** DC đóng vai trò vừa namespace server vừa là file server.

**2012may2:** Member computer vừa namespace server vừa là file server.

## **Bước 1: Trên Namespace Server và File Server**

Mở **Server Manager** -> **Manage** -> **Add Roles and Features** -> **Next** đến

**Select Server Roles:** Búng **File and Storage Service** -> Check vào **DFS Namespace và DFS Replication**

( Nếu File Server và Namespace Server riêng thì File Server cài DFS Replication, Namespace Server cài DFS Namespace)

-> **Next**



**Next mặc định và Install**



Làm tương tự cho **2012may2**

## **Bước 2: Thực hiện trên File Server**

Trên File Server: tạo và phân quyền các thư mục chứa dữ liệu



**Trên máy 2012may1:** tạo folder **Data** chứa 2 folder con (subfolder) là **NhanSu**(xóa group Users, Group NhanSu: Modify) và **KeToan** (xóa group Users, Group KeToan: Modify)

**Trên máy 2012may2:** tạo folder **Data.bak** chứa 2 subfolder: **NhanSu.bak** và **KeToan.bak**, phân quyền như trên.

Lưu ý: 2012may2 có thể đặt tên folder giống như 2012may1 (tùy ý đặt tên).

### Bước 3 : Thực hiện trên Namespace Server

Tạo Namespace (khi tạo namespace phải chỉ định Namespace server)

Kiểm tra DFS Namespace service và DFS Replication service trên 2 máy phải ở trạng thái " running".

Run -> services.msc



Vào **Server Manager -> Tools -> DFS Management**



Chọn vào **Namespace -> New Namespace**

#### Namespace Server

**Server:** chỉ định namespace server, ta browse về máy 2012may1



#### Namespace Name and Settings

**Name:** DataCongTy

**Chọn Edit Setting:**



Ta thấy cấu trúc namespace "**DataCongTy**" được lưu trong folder DFS root.

**Share folder permissions:** phân quyền trên cấu trúc namespace: ta chọn cái thứ 3

**Administrators have full access, other users have read-only permissions:** admin có toàn quyền, user chỉ cần đọc được cấu trúc là có thể truy cập được, không cần đụng vào cấu trúc namespace làm gì .

**Hoặc** ta có thể chọn use custom permissions: để phân quyền tùy nhu cầu -> **NEXT**

**Namespace Type:** Domain-based namespace: (vì đang làm trên môi trường domain)



#### Ta NEXT và Create



Sau đó bung **Namespaces** -> hiện ra đường dẫn luận lý: **\\tuhocmang.local\DataCongTy**. Đường dẫn này chưa chứa dữ liệu nào. **Đây mới chỉ là yếu tố luận lý**



Chọn vào đường dẫn -> **Add Namespace Server**



Ta **Browse** về **server 2012may2** ( cấu hình 2 namespace để đảm bảo 1 trong 2 namespace bị failed thì người dùng vẫn có thể truy xuất dữ liệu)



Phần **Edit Settings** ta cũng phân quyền như trên -> OK



Qua **tab Namespace Server**, xuất hiện **2 Namespace Server**



( 2 Namespace server sẽ tự đồng bộ namespace)

#### **Bước 4: Tại File Server tạo Replicaiton group**

Mở cửa sổ **DFS Management**

Chọn **Namespaces** -> **Add Namespace to display**: để đồng bộ với namespace server khác (nếu chưa tự đồng bộ) -> Browse về 2012may2



Chọn **Replication** -> **New Replication Group**



#### **Replication Group Type:**

Do ta đang muốn cấu hình **file server** hướng đến **mục tiêu thứ 1: chia tải và chịu lỗi** nên chọn **Multipurpose replicatiton group** -> **Next**

#### **Name and Domain:**

**Name of replication:** DongBoDaTaCongTy -> **Next**



#### **Replication Group Member:**

Add các máy làm **File Server**: ta add **2012may1** và **2012may2** -> **Next**



**Topology Selection:** Chọn **Full Mesh** -> **Next**



**Replication Group Schedule and Bandwidth** (đã nói ở đầu bài). Ta chọn 64MB



**Primary Member:** chọn **2012may1**



**Folders to Replicate:** Đồng bộ những folder nào



Chọn **Add**



**Local Path of folder to replicate:** ta **Browse** về folder **KeToan**

Folder KeToan ta đã phân quyền **NTFS** rồi (mặc định là giữ lại các quyền NTFS trên folder )

Nếu muốn chỉnh quyền lại thì ta chọn **Permissions**

Ta thấy rằng, ta cần đồng bộ thêm folder NhanSu. Nhưng ta chỉ cần add 1 folder KeToan thôi. Các folder còn lại thì nên Add sau.

-> **Next.**

**Local Path Of KeToan on Other Member:** Chỉ định folder sẽ đồng bộ với folder KeToan. Ta muốn folder **KeToan** trên 2012may1 sẽ đồng bộ với folder **KeToan.bak** trên 2012may2

 DFS 24

Chọn **Edit ->Enable ->Browse** về folder **KeToan.bak**

 DFS 25

**Make the selected replicated folder on this member read-only:** Nếu check vào folder này thì permission trên folder KeToan.bak sẽ như folder KeToan ( quyền sẽ giống Primary Server)

Ở bước này, hệ thống chỉ cho ta chọn 1 folder, đó là lý do tại sao **Local Path of folder to replicate** ta chỉ chỉ định 1 folder trên 2012may1.

Còn việc đồng bộ giữa NhanSu trên 2012may1 và NhanSu.bak trên 2012may2 ta sẽ làm sau.

**Ta Next và Create**

 DFS 26

Ta tiếp tục chọn **New Replicated Folder** để cấu hình cho folder **NhanSu** đồng bộ với folder **NhanSu.bak**.

**Bước 5: Share and Publish**

**Trên 2012may1**

Mở **DFS Management -> Namespace -> phải chuột \\tuhocmang.local\DataCongTy -> New Folder**

 DFS 27

**Name:** Data

**Folder Target:** Không khai báo gì cả. -> **OK**

 DFS 28

**Data:** là 1 thư mục mang tính cấu trúc (Loại 1). Bây giờ ta đi **share và publish**.

Chọn **Replication -> Add Replication to Display -> Chọn DongBoDataCongTy**

 DFS 29

Chọn vào **DongBoDataCongTy -> Bên phải chọn Tab Replicated Folder -> Phải chuột KeToan -> Share and Publish in Namespace**

 DFS 30

**Publishing Method:** Chọn **Share and publish the replicated folder in a namespace -> Next**

 DFS 31

**Share Replicated Folder:** chọn 2012may1

 DFS 32

**Chọn Edit**

 DFS 33

Nó yêu cầu ta **share folder KeToan và share với quyền gì**. Ta chọn **Edit Permission** -> cho **everyone Full control** (vì ta đã phân quyền NTFS rồi)

**Sau đó chọn tiếp 2012may2 -> Edit**

**New:** share name đặt là **KeToan.bak** cho dễ quản lý (share name đặt giống 2012may1 khó quản lý)



**Namespace Path:** Ta sẽ publish folder này ở cấp nào:



Ta **Browse về Data =>** đường dẫn để truy xuất dữ liệu sẽ bắt đầu bằng:  
**\\tuhocmang.local\DataCongTy\Data**

**New folder name:** có thể tạo tên mới để che cấu trúc folder đi ( thay vì mặc định là KeToan)

-> **Next**



Ta thấy **KeToan** đại diện cho KeToan và KeToan.bak

-> **Share**

Nếu muốn thay đổi đường dẫn ta vào **Data -> KeToan -> Move Folder** để đổi tên lại. ( giả sử đổi lại như hình).



Làm tương tự cho folder NhanSu (**Share and Publish**)



## TEST

+ KT1 truy cập:

**\\tuhocmang.local\DataCongTy\Data\KeToan** -> tạo folder KT1

Trên folder KeToan và KeToan.bak xuất hiện folder KT1 ( đồng bộ)

+ Disable card mạng 2012may2, KT1 truy cập đường dẫn bình thường ( Chịu lỗi)

KT1 xóa folder KT1 -> Enable card mạng 2012may2 -> vào KeToan.bak thấy mất folder KT1 (đồng bộ)

### Lưu ý:

+ Primary Server và Secondary Server là như nhau, chỉ khác là đường dẫn mặc định lấy tên folder của primary Server.

+ DFS Replication chỉ làm việc trên Domain.

+ DFS xây dựng trên môi trường workgroup chỉ hỗ trợ Load Balacing, không hỗ trợ Failover.

### 1 số link tham khảo:

[http://msdn.microsoft.com/it-it/library/cc781582\(v=ws.10\).aspx](http://msdn.microsoft.com/it-it/library/cc781582(v=ws.10).aspx)

<http://blogs.technet.com/b/askds/archive/2011/09/16/active-directory-site-topology-not-just-for-dcs.aspx>

[http://technet.microsoft.com/en-us/library/cc784885\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc784885(v=ws.10).aspx)

<http://mizitechinfo.wordpress.com/category/windows-server-2012-r2/>

<http://blogs.technet.com/b/filecab/archive/2005/12/06/415625.aspx> :

## 26. Print Server

**Chuẩn bị:** Ở phần này thì chỉ cần 1 máy tính bất kì và máy in.

Máy in là thiết bị quan trọng trong hệ thống mạng. Tùy nhu cầu sử dụng mà ta có các các cấu hình khác nhau.

**Chuẩn kết nối máy in gồm có:**

+ Kết nối trực tiếp: LPT( chuẩn IEEE 1284), USB



Chuẩn LPT

+ Thông qua switch (máy in mạng có địa chỉ IP, port): Wireless, cổng mạng RJ45.

**Mô hình máy in thường dùng:**



Printer 1

Mô hình máy in cổng USB



Printer 2

Mô hình có Print Server

Print Server như hình trên thì mình thấy hiện tại cũng ít dùng.

Khi mua máy in về, kết nối máy in với hệ thống, máy tính nào muốn sử dụng máy in phải đi cài đặt driver tương ứng mới detect được máy in. Cài Driver xong thì sẽ xuất hiện biểu tượng máy in trong **Devices and Printers**.

Windows cũng hỗ trợ cơ chế Plug and Play: mỗi nhà sản xuất thiết bị khi làm ra sản phẩm thì đưa driver cho Microsoft để tích hợp vào windows, cắm vào là chạy, không cần driver ( windows hỗ trợ nhiều máy in hơn win 7).

**Các khái niệm cần biết:**

a/ **Print Device:** là các máy in vật lý.

b/ **Printer:** Các máy in luận lý ( là biểu tượng máy in sau khi cài driver xong).

1 Printer có thể đại diện cho nhiều Print Device (1 Printer quản lý nhiều Print Device).

1 Print Device có thể có nhiều Printer hay 1 Printer sẽ tương ứng với 1 Print Device tùy vào nhu cầu sử dụng.

c/ **Local Printer:** Đối với Print Server, mọi Printer mà nó quản lý gọi là Local Printer.

d/ **Network Printer:** Biểu tượng máy in (luận lý) trên client.

e/ **Print Server:** Máy tính gắn trực tiếp vào máy in

Vào **Control Panel** -> **Devices and Printers** để quản lý máy in.

Nếu có nhiều printer, thì ta chọn "**Set as default printer**" cho máy in nào đó tùy nhu cầu, khi chọn "**in**" ( CTRL P) thì mặc định in máy Default Printer.



Printer 9

Để share máy in cho mọi người trong mạng sử dụng: chọn Local Printer -> Printing preferences -> tab sharing check vào **Share this printer**.

Trên client: dùng: **\\[ địa chỉ IP của Print Server]**, chọn vào printer -> **Connect** để kết nối và sử dụng máy in. Lúc này client sẽ dùng driver trên print server để cài đặt.

< Printer 10 >

Khi người dùng chọn "Print" để in thì ta nói người dùng đang thực hiện 1 Print Job.

## Cơ chế làm việc (với máy in gắn trực tiếp):

Client gửi gói tin đến server, server kết nối với **Print Device**. Công tác in (**Print Job**) phải đi qua 1 trung gian là **Print Server** (nghĩa là print job sẽ được lưu trong thư mục của print server rồi từ đó mới chuyển đến print device để xử lý).

Vị trí lưu trữ của print job trước khi tới print device là **Spool Folder**. Cứ 1 print job sẽ khởi tạo ra 2 file **\*.SHD** và **\*.SPL**. Các file này được đọc, ghi và bị xóa sau khi kết thúc một print job => dẫn đến tình trạng **phân mảnh**. Phân mảnh nhiều, lâu dẫn đến hỏng print job và các dữ liệu liên quan làm tốc độ bị suy giảm, ảnh hưởng đến hiệu suất hoạt động.

Mặc định Spool Folder được lưu trong: C:\Windows\system32\spool\printer.

Nếu 1 thời điểm có nhiều print job, nguyên tắc hoạt động của printer là **FIFO (First In First Out)**. Ai gửi trước thì print job sẽ được thực thi trước.

### Lưu ý:

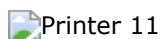
+ Do việc in có thể ảnh hưởng đến ổ đĩa, ta nên thay đổi vị trí thư mục spool folder (chuyển về thư mục trong ổ đĩa khác với hệ điều hành). Ở windows 8 và 2012 thì mình chưa tìm được cách chuyển spool folder. Các bạn nào biết thì cmt ở dưới nhé.

+ Ta có thể cho 1 máy không quan trọng làm Print Server.

+ Ổ đĩa có tốc độ cao cũng làm cho print job nhanh (ngoài ra còn phụ thuộc việc xử lý của máy in). ta có thể cấu hình cho ổ đĩa là RAID 0 để tăng tốc độ cho ổ đĩa.

## Quản lý máy in

Chọn Local Printer -> Printer Properties -> Tab Security. Mặc định Everyone đều có quyền in, muốn cấm ai thì **Deny**.



Ta có các quyền sau:

**Print:** quyền in, mỗi người dùng đều có thể print và quản lý (cancel, pause, restart) print job do mình tạo ra.

**Manage Document:** quản lý các print job của người dùng khác.

**Manage Printers:** quyền quản lý (cấu hình permission), rename, share delete, cấu hình printing preferences và quản lý các print job.

**Special Permission:** được dùng để thay đổi Print Owner (mặc định user nào cài printer thì user đó làm owner).

Trong việc quản lý máy in thì ta có các tình huống cần giải quyết

### Tình huống 1: bài toán công ty nghèo.

Công ty chỉ có 1 máy in. Sếp có print job sau nhưng vẫn muốn được in trước (giả sử công ty chỉ có 1 con HP 2035).

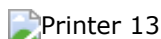
Như đã biết 1 Print device có thể có nhiều printer. Để add thêm printer ta làm như sau

Vào **Control Panel -> Devices and Printers -> Add Printer**



Chọn HP 2035 (do mình có nhiều máy in, nếu có 1 máy in kết nối thì chỉ xuất hiện 1 máy) -> Next.

Chọn Use the driver that is currently installed



**Printer Name:** Sep Uu Tien



Share Printer vừa tạo.

 Printer 15

Next rồi Finish.

 Printer 16

 Printer 17

Đây là 2 printer tham chiếu đến 1 print device.

**Mặc định:** 2 Printer này có **Priority** ngang nhau, print job nào đến trước thì in trước. Ta sẽ phân quyền **Printer "Sep Uu Tien"** chỉ cho 1 mình ông sếp sử dụng (**Everyone: Deny, add vào username của sếp**) và set cho Printer "Sep Uu Tien" có độ ưu tiên hơn.

Chọn **Printer "Sep Uu Tien"** -> **Printer Properties** -> **Tab Advance** -> **Printer Properties**

**Priority: 10** (Priority càng cao thì càng ưu tiên hơn)

 Printer 18

## **Tình huống 2: Lập lịch biểu cho Printer.**

Những tài liệu không quan trọng trong công ty nhưng dài ( tài liệu học tập, cá nhân) ta muốn để buổi tối in

### **Triển khai:**

Tạo thêm 1 Printer đặt tên " In Buoi Toi".

Chọn vào Printer " In Buoi Toi" và cấu hình Available From. Khi in những tài liệu không quan trọng thì cứ in bằng Printer " In Buoi Toi".

 Printer 19

**Tình huống 3:** Print Server là hệ điều hành 32 bit dùng driver máy in tương thích với bit, client 32 bit kết nối đến server, connect để lấy driver từ print server về. Nhưng nếu client sử dụng hệ điều hành 64 bit thì thế nào ?

### **Triển khai:**

**Cách 1:** Trên server tạo share folder chứa driver máy in 64 bit, user lấy về cài đặt.

**Cách 2:** Microsoft cho phép ta cài thêm driver ( cho dù driver đó không tương thích với server)

Chọn vào Printer -> Printer Properties -> Tab Sharing -> chọn Additional Drivers

 Printer 20

 Printer 21

Ta Browse về file cài đặt driver.

 Printer 22

## **Tình huống 4: bài toán công ty giàu**

Công ty có nhiều máy in. Có nhu cầu xây dựng hệ thống cân bằng tải cho máy in. Chỉ dành cho trường hợp máy in được đặt tập trung. nếu 1 máy ở tầng 1, 1 máy ở tầng 10 thì thua !!!.

Các máy in phải cùng chức năng (hoặc là cùng in màu, hoặc là cùng in đen v.v).

Ta sẽ tạo 1 printer trỏ đến nhiều máy in.

Giả sử ta có 3 máy in như hình

 Printer 24

Lúc này máy tính đã detect được 3 máy in. chọn 1 printer bất kì -> Printing Properties -> Tab Port



Ta check vào Enable Printer pooling

Chọn vào máy in mà ta muốn Load Balancing ( ở đây mình chọn HP 1160). Lúc này 1 printer đã trở đến cả 2 print device.

Ta tắt share biểu tượng printer HP1160



# 27. Hyper-V

Như các bạn đã biết thì Hyper-V, chương trình tạo máy ảo, được Microsoft tích hợp miễn phí vào HDH Windows 8 phiên bản pro trở lên. Để cài đặt Hyper-V thì CPU phải hỗ trợ công nghệ ảo hóa.

Nếu CPU của bạn là Intel thì download Intel Processor Identification Utility và cài đặt



Intel Processor Identification Utility

Nếu CPU của bạn là AMD thì download phần mềm tại đây

Hoặc ta có thể download phần mềm CoreInfo của Microsoft để kiểm tra : Link download



Cách dùng Core info

Cách cài đặt Hyper-v trên Windows 8

**Start -> Run -> appwiz.cpl**



appwiz

Chọn **Turn Windows features on or off** và check vào **Hyper-V**.



cài đặt Hyper-V

Sau đó máy tính sẽ restart 2 lần để cài đặt lớp ảo hóa.

Sau khi khởi động lại: Start -> Hyper-V. ta sẽ thấy giao diện quản lý máy ảo (Hyper-V Manager).

Để tạo máy ảo: New -> **Virtual Machine**



tạo máy ảo

Next -> Điền tên và nơi lưu trữ máy ảo



tạo máy ảo

Chỉ định Ram cho máy ảo, nên check vào **Dynamic Memory** vì nếu ta chỉ định 2 gb thì máy ảo xài bao nhiêu Ram thì lấy bấy nhiêu trong giới hạn 2 gb, không check thì lấy luôn 2gb từ Ram máy thật.



**Cấu hình card mạng (virtual Switch):** ta sẽ cấu hình sau, Next



**Cấu hình Hard disk:** Có thể tạo mới, lấy ổ đĩa có sẵn ở đây mình chọn "sẽ tạo sau"



Next và Finish

Tạo ổ cứng ảo:



Chọn định dạng ổ cứng ảo: Hyper-V cung cấp 2 định dạng cho ổ cứng ảo:

**VHD** (là 1 file có đuôi là \*.vhd) : hỗ trợ tối đa 2 TB

**VHDX**: hỗ trợ tối đa 64 TB, có tính chịu lỗi cao (nếu bị cúp điện do có lưu lại log). Nhưng chỉ hỗ trợ các HDH win 8, 2012 trở lên.



Chọn loại ổ cứng: có 3 loại ổ cứng

**Fixed Size**: dung lượng cố định (cho 20 gb thì ngay lập tức file ổ cứng ảo nặng 20 gb mặc dù chưa sử dụng). Cho hiệu năng cao nhất.

**Dynamically Expanding**: dung lượng động (xài bao nhiêu thì mất bấy nhiêu), dễ bị phân mảnh dữ liệu.

**Differencing**: là loại ô thường dùng cho Lab. Loại này phụ thuộc vào 1 file ổ cứng ảo (gọi là Parent), không chạy một mình được.

– ta tạo một file ổ cứng ảo (base.vhd) chạy HDH 2012.

– Sau đó ta tạo một file ổ cứng loại Differencing (vd: Test.vhd) thì Test.vhd sẽ chỉ lưu những sự thay đổi của nó so với file Parent là base.vhd. Khi máy ảo gắn vào Test.vhd vẫn chạy HDH 2012 của ổ cứng base.vhd và những sự thay đổi của Test.vhd

Do đó loại Differencing giúp tiết kiệm dung lượng ổ cứng, dễ dàng triển khai các máy ảo, thích hợp cho môi trường Lab



Differencing

Chọn ổ cứng **Parent**



## Next rồi Finish

Cấu hình **Virtual Switch** .



Có 3 loại Virtual Switch:

**Private**: nối các máy ảo lại với nhau, máy ảo không thể liên lạc với máy thật (host) và bên ngoài (Lan, Internet)

**Internal**: nối các máy ảo và host lại với nhau không thể liên lạc được với bên ngoài

**External**: tạo ra 1 switch sử dụng card mạng vật lý của host (cho nên phải có ít nhất 1 card thật). Các máy ảo dùng switch này có thể

liên lạc được với mạng Lan, Internet.



Chọn thử External -> **Create Virtual Switch**



Muốn xóa Switch thì chọn **remove**.

Một số phím tắt:

Ctrl + Alt + End = Ctrl + Alt + Del.

Alt: thoát chuột trong máy ảo.

Ctrl + Alt + Pause: phóng to máy ảo.

Các vấn đề như Snapshot hay Revert tương tự như Vmware Workstation.

# 28. Disk Management (phần 1)

Ở phần này, chúng ta sẽ tìm hiểu về ổ cứng (HDD)

## Chuẩn bị:

Add 3 ổ cứng vào máy ảo.

Ta có 2 cơ chế quản lý đĩa

## Basic và Dynamic.

Mặc định windows quản lý theo cơ chế basic.

Đối với cơ chế basic: 1 ổ đĩa nằm trên 1 ổ cứng vật lý.


Ta dùng Dynamic khi có nhu cầu:

- + Tăng tốc độ truy suất dữ liệu.

- + Tăng khả năng chịu lỗi vật lý (ổ đĩa chết vẫn truy suất được dữ liệu).

Có nhiều tool để quản lý đĩa (trong hiren boot rất nhiều), trên windows có công cụ Disk Management.


Để vào Disk Management: run -> **diskmgmt.msc**.

 diskmgmt 1

Ta thấy cơ chế quản lý đĩa: Basic

Ta thấy disk1, disk2, disk3 bị chéo đỏ (offline), chưa sử dụng được. Đối với hệ điều hành (HDH) windows, khi gắn thêm ổ cứng vật lý thì phải khai báo với HDH.

chọn disk1 -> chọn Online

 diskmgmt 2

Chọn tiếp disk1 -> Intialize disk

 diskmgmt 3

Windows yêu cầu ta chọn: dùng MBR hay GPT để lưu trữ thông tin phân vùng ( mỗi ổ đĩa đều có 1 MBR hay 1 GPT).

 diskmgmt 4

## Đối với MBR:

Trên 1 ổ cứng chia được tối đa 4 thành phần luận lý (4 phân vùng) .

Khi chia phân vùng ta có thể chọn: Primary Partition và Extended Partition.

Đặc điểm của Extended :

- + Chỉ tạo tối đa được 1 phân vùng ( muốn thêm thì thêm ổ cứng).

- + Khi tạo Extended thì ta mới chỉ mới đánh dấu phân vùng để định nghĩa dung lượng (chưa dùng để lưu trữ dữ liệu). Muốn dùng thì phải chia nhỏ. Thành phần luận lý bên trong Extended gọi là Logical Drive, lúc này mới có thể sử dụng được (1 logical drive tương đương 1 ổ đĩa). Ta tạo bao nhiêu logical drive cũng được.

Primary: tối đa 4 phân vùng.

Primary có thuộc tính Active, giúp load HDH.

Câu hỏi: ta có thể sử dụng đồng thời bao nhiêu ổ đĩa (Logical và Primary). Muốn người dùng sử dụng được ổ đĩa thì bắt buộc mỗi ổ đĩa phải được đại diện bằng chữ cái từ A -> Z (28).

=> tối đa dùng được 26 ổ đĩa đồng thời.

A, B dùng cho đĩa mềm (muốn dùng thì phải chỉnh registry, nhưng mình chưa biết cách chỉnh !!!!!)

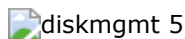
Do kiến thức mình có giới hạn, mình gửi các bạn các link tham khảo về MBR và GPT:

<http://forum.bkav.com.vn/showthread.php/79096-gpt-disk-vs-mbr-disk>

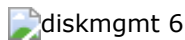
<http://tuvantinhoc1088.com/tri-thuc/cac-van-de-khac/14217-s-khac-nhau-gi-a-gpt-va-mbr-khi-phan-vung-dia.html>

Ta chọn **MBR**.

Ta tạo thử phân vùng Primary: 50 MB.

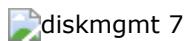


-> Next rồi chỉ định dung lượng là 50M



Gán kí tự cho ổ đĩa. Ta để mặc định. Nếu chỉ tạo phân vùng mà chưa muốn người dùng sử dụng phân vùng đó thì chọn: **"Do not assign a drive letter or drive path"**

Nếu muốn gán 1 folder thành phân vùng, ta chọn Option thứ 2.



Định dạng phân vùng: Từ server 2012 trở đi, Windows hỗ trợ định dạng Refs. Ta chọn NTFS

### **Allocation unit size (hay Cluster size):**

Ta cùng nhau ôn 1 chút về ổ cứng

Đối với công nghệ HDD:

Cấu tạo luận lý: được cấu tạo bởi những vòng tròn đồng tâm (track). Trên những track này, được trang bị những hạt từ tính vô cùng bé. Dữ liệu chính là sự sắp xếp của các hạt từ tính.

Ví dụ: ta đánh chữ A, (máy tính không biết chữ A là gì cả) A được định dạng là 65 (mã ASCII). Vật liệu từ tính sẽ có 2 trạng thái mũi tên (mũi tên phải và mũi tên trái)

Để mô tả trạng thái ta dùng hệ số nhị phân – 0,1 (do có 2 giá trị tương ứng)

65: 01000001.

<https://www.youtube.com/watch?v=4iaxOUYalJU>

### **(xem ở phút thứ 2:00 và 3:58)**

Để sắp xếp, đọc được các hạt từ tính ta sẽ dùng kim đọc (là 1 lá thép cực mỏng), cuối lá thép có 1 cuộn dây. Khi có dòng điện chạy qua cuộn dây sẽ phát sinh từ trường, từ trường sẽ biến lá thép mỏng thành nam châm tĩnh điện. Dưới tác động của từ trường thì nó sẽ sắp xếp các hạt từ tính theo chiều, trật tự nhất định. Kim đọc này chỉ quay được ở 1 khung nhất định cho nên người ta chia nhỏ đơn vị track ra thành các vòng cung, là phạm vi di chuyển của kim đọc trên ổ cứng. Tương ứng với mỗi 1 cung ta gọi là 1 sector. Về mặt vật lý, sector là khái niệm nhỏ nhất (1sector = 512 bytes)

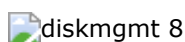
Đối với HDH windows thì ta có thêm khái niệm luận lý là cluster size để lưu trữ dữ liệu (linux gọi là inode).

Ví dụ: ta có dữ liệu A : (có size là: 68 KB), dữ liệu B (10 KB)

Bản chất khi lưu trữ A, B thì ta không lưu trên 1 cluster size mà nó chẻ ra thành các cluster size để lấp đầy dữ liệu. Nếu ta quy định cluster size là 16KB thì khi lưu trữ A thì A sẽ chia nhỏ thành 5 phần và lưu trên 5 cluster size. Cluster size thứ 5 sẽ lưu trữ 4KB => cluster còn trống 12KB.

Và điều lưu ý là dữ liệu A chưa chắc nằm trên các cluster size liền kề mà nằm rải rác trên các cluster size trống (nếu có 5 cluster size trống liền kề nhau thì OK).

Để lưu trữ dữ liệu B thì phải luôn bắt đầu bằng 1 cluster size mới. Cho dù B chỉ có 10KB thì vẫn lưu trên 1 cluster size khác => các cluster size trống chính là hiện tượng phân mảnh ổ cứng (dung lượng còn trống trên 1 cluster size không dùng để lưu trữ dữ liệu)



Cluster size quá lớn: độ phân mảnh sẽ nhiều. Tuy nhiên nếu cluster size lớn (vd: 32KB) thì để lấy được thông tin dữ liệu A, kim đọc chỉ cần đọc 3 cluster size (thay vì 5 nếu là 16KB).

Đối với nơi lưu trữ dữ liệu nhỏ (word, excel) thì dùng cluster size nhỏ .

Đối với nơi lưu trữ dữ liệu lớn (phim v.v) thì nên dùng cluster size lớn để giúp truy suất dữ liệu nhanh.

Nếu không xác định được thì cứ để **Default**.

Bảng Default Allocation Unit Size: <http://support2.microsoft.com/kb/140365>

Khi format 1 ổ đĩa ta có **quick format và format**.

**Giống nhau:** đều không thấy được dữ liệu.

**Khác nhau:** Như đã đề cập, dữ liệu A sẽ nằm rải rác trên các cluster size trống. Vậy làm thế nào mà ổ cứng biết được dữ liệu nào đang ở cluster size nào. Trên mỗi phân vùng đều có Master File Table (MFT – đối với NTFS). Đây là bảng định vị cluster size tương ứng với dữ liệu. Nó ghi thông tin phân vùng, cluster size là bao

nhiều, File system là gì v.v.

Quick Format: xóa bảng thông tin (MFT), nhưng không xóa trực tiếp dữ liệu.


Format: xóa hết.

Ghi chú:

Khi tạo ra phân vùng, nếu muốn người dùng không sử dụng được thì: remove kí tự

 diskmgmt 9

Chọn Change Drive Letter and Path -> chọn Remove

 diskmgmt 10

### **Refs:**

- + hỗ trợ khả năng chịu lỗi về nguồn điện tốt hơn NTFS (trường hợp tắt điện đột xuất).
- + cho phép đặt tên file dài ( >256 kí tự)
- + Cho phép lưu dụng lượng 1 file tối đa: 16 Exabytes (1 Ex = 1024 Petabytes ~ 1tr Terabytes )
- + Phân vùng tối đa: 1 Yottabytes (1Yo = 1024 zettabytes ~ 1tr Ex)

Khi chia phân vùng bằng diskmgmt.msc thì khi ta tạo phân vùng thì mặc định là primary partition trước. Khi có 3 primary thì tạo thêm sẽ tự động ra logical partition.

### **Các bài viết đọc thêm :**

[http://vi.wikipedia.org/wiki/BIOS#H.E1.BA.A1n\\_ch.E1.BA.BF\\_c.E1.BB.A7a\\_BIOS](http://vi.wikipedia.org/wiki/BIOS#H.E1.BA.A1n_ch.E1.BA.BF_c.E1.BB.A7a_BIOS)

<http://www.itvnshare.com/2014/07/gpt-va-mbr-2-kien-truc-phan-vung-o-ia.html>

<http://mobileworld.vn/threads/uefi-la-gi-nhung-dieu-can-biet-ve-uefi-thay-the-cho-bios.106760/#.VFDm17J35No>

<http://www.howtogeek.com/136078/what-should-i-set-the-allocation-unit-size-to-when-formatting/>

<http://serverfault.com/questions/543472/in-ntfs-whats-the-difference-between-sector-size-block-size-and-cluster-size>

<http://stackoverflow.com/questions/12345804/difference-between-blocks-and-sectors>

# 29. Disk Management (phần 2)

**Chuẩn bị:** Add 3 ổ cứng ảo vào máy ảo.

**Như đã đề cập ở Phần 1:**

Ta dùng **Dynamic Disk** khi có **1 trong 2** nhu cầu sau (hoặc cả 2)

+ Tăng tốc độ truy suất dữ liệu.

+ Tăng khả năng chịu lỗi vật lý cho ổ cứng.

Mục tiêu của Dynamic Disk là cung cấp tính năng Raid (Redundant Array of Inexpensive Disks)

Raid có 2 loại:

**Raid cứng** (hardware): Là chương trình được tích hợp sẵn trên chip card Raid hoặc trên Mainboard.

**Raid mềm** (software): đây là ứng dụng sau khi cài HDH (HDH lỗi thì Raid cũng đi luôn !)

Khi dùng Dynamic Disk thì không còn khái niệm Primary, Extended, Logical partition. Một ổ đĩa là 1 volume, tạo bao nhiêu volume cũng được.

Để chuyển từ Basic -> Dynamic ta làm như sau:

**Diskmgmt.msc**

Chọn ổ cứng: Phải chuột -> **Convert to Dynamic disk.**



Raid 1



Raid 2

Tương tự, ta làm cho các ổ cứng còn lại.

Ta có khái niệm **Simple volume**:

**Simple Volume:** đây là phân vùng trung gian giữa khi chuyển từ Basic sang Dynamic. Các Logical, Primary, Extended sẽ thành simple volume khi ổ cứng chuyển từ Basic sang Dynamic.

Hiệu năng của Simple volume không khác gì so với Basic.



Raid 3

phân vùng F là simple volume

**Spanned Volume**

Được cấu tạo từ nhiều phần (có thể bằng nhau hoặc không bằng nhau) của các ổ đĩa vật lý.

Ví dụ:

Ta tạo phân vùng Spanned từ 3 ổ cứng như sau:



Raid 4

**Disk 1:** góp 50GB. Disk 2 góp 100GB. Disk 3 góp 50GB. Ta có được phân vùng Spanned 200GB.

Ta có copy file A : 200GB từ Ổ cứng di động vào phân vùng Spanned. Thì khi lưu trữ nó sẽ lưu ở disk 1 trước. Nếu hết dung lượng mà disk 1 góp thì sẽ lưu sang **disk 2** rồi đến **disk 3**.

Do nó ghi tuần tự nên tại 1 thời điểm nó chỉ sử dụng 1 ổ cứng cho đến khi dung hết phần đóng góp của ổ cứng đó

**Mục đích sử dụng:** Gia tăng dung lượng 1 volume, có tổng dung lượng bằng dung lượng đóng góp.

Không có khả năng chịu lỗi. Không tăng được tốc độ truy suất. Không làm thay đổi cấu trúc truy suất file.

**Raid 0 (Striped volume)**

**a/ Cấu tạo:** từ nhiều phần có dung lượng bằng nhau trên nhiều ổ cứng vật lý khác nhau (  $\geq 2$  )

**b/ Dung lượng:** bằng tổng dung lượng thành phần.

### c/ Nguyên lý đọc ghi:

#### Nguyên lý ghi:

**Gian đoạn 1:** tách dữ liệu thành nhóm N bit. (với N là số ổ cứng vật lý đồng thời)

N = 2: tách dữ liệu thành nhóm 2 bit.

N = 3: tách dữ liệu thành nhóm 3 bit.

**Gian đoạn 2:** ghi N bit lên N ổ cứng đồng thời.

#### Nguyên lý đọc: (ngược lại)

Bước 1: Đọc N bit.

Bước 2: Ghép các nhóm N bit thành dữ liệu.

Ví dụ: ta có A (65): 01000001.

**Lợi ích:** tăng tốc độ truy suất gấp N lần Basic. (thực tế thì chưa tới N lần do phải tốn thời gian chia dữ liệu).

**Khả năng chịu lỗi vật lý:** Không có (1 ổ đĩa chết là dữ liệu cũng không đọc được.)

**Ứng dụng:** cho server cần tốc độ, không cần an toàn (Vd: nơi lưu trữ spool folder của Print server).

### Raid 1 (Mirror volume)

**a/ cấu tạo:** Từ 2 phần có dung lượng bằng nhau trên 2 ổ cứng vật lý khác nhau (N=2, Max =2)

**b/ Dung lượng:** bằng dung lượng thành phần ( VD: mỗi ổ cứng góp 100G thì volume có dung lượng là 100G)

#### c/ Nguyên lý đọc ghi:

Tại 1 thời điểm chỉ sử dụng 1 trong 2 ổ cứng vật lý. Dữ liệu được đọc/ghi trên 1 ổ cứng vật lý sẽ tự g đồng bộ sang ổ cứng vật lý còn lại.

=> A = 65: 01000001

=> ghi dãy bit này trên cả 2 ổ đĩa.

**d/ Tốc độ truy suất:** tương đương Basic.

**e/ Khả năng chịu lỗi:** 50% (hư 1 cái thì còn cái khác, hư 2 cái thì die !!)

**f/Ứng dụng:** Dùng cho server cần độ an toàn cao.

### Raid 5

**a/ Cấu tạo:** Cấu tạo từ nhiều phần có dung lượng bằng nhau từ nhiều ổ cứng khác nhau (N >= 3)

**b/ Dung lượng:** = (N-1) \* dung lượng thành phần

#### c/ Nguyên lý đọc ghi:

**Bước 1:** Tách dữ liệu thành nhóm (N-1) bit.

**Bước 2:** Đếm bit 0 hoặc bit 1 trong từng nhóm.

Nếu nhóm lẻ (kết quả XOR bằng 1): thêm bit 1

Nếu nhóm chẵn (Kết quả XOR bằng 0): thêm bit 0

**(Hoặc XOR từng nhóm, kết quả cuối cùng của từng nhóm sẽ là bit thêm vào)**

Do Raid 5 sử dụng thuật toán XOR nên ta sử dụng toán XOR để biết nhóm chẵn hay lẻ.

**0 XOR 0 = 0**

**0 XOR 1 = 1**

**1 XOR 0 = 1**

**1 XOR 1 = 0**



## **Cách sửa lỗi**

### **Giải sử hư ổ cứng đầu tiên**

### **Giải sử hư ổ cứng thứ 3**

### **Giải sử hư ổ cứng thứ 2**

Bước 2: Có thể đếm như trên hoặc dùng phép XOR là ra kết quả

**d/ Tốc độ truy suất:** Basic < Raid 5 < Raid 0.

**e/ Khả năng chịu lỗi vật lý:** 3 ổ cứng được phép hư 1, 5 thì hư 2.

(Còn phần 3 là phần cuối của Disk Management)

### **Tham khảo:**

<http://en.wikipedia.org/wiki/RAID>

### **Cài đặt HDH lên raid**

[https://www.google.com.vn/?gfe\\_rd=cr&ei=h7hzVMP8JM-CvAS9wYKgbg#q=cai+dat+HDH+len+raid](https://www.google.com.vn/?gfe_rd=cr&ei=h7hzVMP8JM-CvAS9wYKgbg#q=cai+dat+HDH+len+raid)

<http://ngoc.nhatnghe.vn/storage/storage.htm>

<http://blog.open-e.com/how-does-raid-5-work/>

<http://riceball.com/d/content/raid-5-parity-what-it-and-how-does-it-work>

<http://www.thegeekstuff.com/2011/10/raid10-vs-raid01/>

<http://forum.thegioimaychu.vn/cau-hinh-raid/130990-help-raid-10-bi-hu-1-o-cung-dung-card-raid-ibm-m1015-sas.html>

# 30. Windows Server Backup (Phần 1)

Mục đích chính của backup:

- + Nếu hệ thống gặp sự cố còn có cơ sở để phục hồi dữ liệu.
- + Khôi phục dữ liệu một cách nhanh nhất, đầy đủ nhất.

Đây là công việc hàng đầu, quan trọng nhất khi quản lý hệ thống.

Đầu tiên ta cần tìm hiểu: thành phần quan trọng khi backup (ngoài Data) là System State

System State là Database của hệ thống, bao gồm:

- + Boot files: các file liên quan đến quá trình khởi động.
- + Registry (theo mình thì đây là thành phần quan trọng nhất).
- + Com+ ( thư viện liên kết động – Component Service – môi trường để phát triển phần mềm).
- + Chứa tất cả đối tượng (object) của windows (user, group, local group policy, v.v).
- + Certificate Services (nếu có cài đặt).
- + Cluster Database (nếu có). v.v

Trong domain network thì system state còn là nơi lưu trữ

- + AD Database
- + Sysvol

VD: lỡ xóa GPO, chỉnh registry hay GPO thì có thể dùng system state để restore ( khôi phục) lại

Các công cụ backup thường dùng: NT Backup (server 2003R2 trở về trước), Windows Server Backup (Server 2008 trở về sau), Acronic (thường dùng), Sysmantec Backup Exec, System Center Data Protection Manager (SCDPM).

Có 2 dạng backup: File-level backup và Block-level backup.

**File-level Backup:** là phương thức được sử dụng hầu hết trong các phần mềm backup. Nó sẽ đọc các cluster size theo thứ tự chúng xuất hiện **trên file**.

Ở bài học Disk Management (Phần 1), mình đã trình bày quá trình lưu dữ liệu trên ổ cứng, thì khi backup với file-level backup, nó sẽ đọc tất cả các cluster size theo thứ tự của 1 file (tức là: file A gồm 4 cluster theo thứ tự a, b, c, d thì nó sẽ đọc cluster a trước rồi cứ tiếp tục). Sau đó so sánh với lần backup trước. Nếu có thay đổi sẽ backup lại toàn bộ file. Khuyết điểm của dạng này là thời gian backup lâu. Nếu 1 file dung lượng lớn có sự thay đổi so với lần backup trước (ví dụ: file 5GB mà chỉ có sự thay đổi trong 1 cluster size) thì sẽ backup toàn bộ file (tồn dung lượng).

**Phần mềm tiêu biểu:** Windows NT Backup.

**Block-level backup:** Can thiệp sâu hơn. Nó chỉ đọc các block (sector) theo thứ tự chúng xuất hiện trên ổ cứng. Tức là nó sẽ vượt qua (bypass) file system trong HDH để làm việc trực tiếp với ổ cứng (Disk hoặc Volume).

Vi dụ: Khi ta backup ổ C (gồm các block từ 1 -> 1000) thì nó sẽ so sánh từng khối dữ liệu (block or sector) ở thời điểm này so với thời điểm backup gần nhất, do đó thời gian backup sẽ nhanh hơn, tiết kiệm dung lượng ổ lưu trữ (thay vì phải so sánh từng file).

**Phần mềm tiêu biểu:** Windows Server Backup, Backup Exec System Recovery, Acronis.

Trước khi đi vào việc tìm hiểu Windows Server Backup, mình sẽ giới thiệu về **Shadow Copy** (hay còn gọi là **Volume Shadow Copy Service – VSS**). VSS service là thành phần quan trọng của Windows Server Backup nên mình sẽ nói về Shadow Copy trước để các bạn dễ hiểu

(tính năng này đã mất trên win 8, chỉ còn trên server 2012).

**Shadow Copy** là tính năng có trên file system NTFS. Shadow Copy được thiết lập theo chuẩn thời gian: (ví dụ ta thiết lập: cứ đến 10h là tự động copy các file trên folder Share thành bản sao gọi là Shadow Copy).

Nó giúp chúng ta giải quyết 2 tình huống sau:

+ Đối với HDH server cũ dùng NT Backup. Hạn chế của công cụ này là khi có 1 hay nhiều file đang được sử dụng trong quá trình backup thì quá trình backup sẽ không thể thực thi tiếp được. Khi kết hợp với Shadow Copy thì nếu thấy 1 file đang được mở thì NT Backup sẽ truy suất vào file Shadow copy để backup. Giúp tiến trình backup luôn hoạt động.

+ Người dùng muốn phục hồi dữ liệu (file data.txt). Nếu hệ thống có backup thì phải restore chỉ để phục hồi 1 file. Triển khai Shadow Copy, giúp cho người dùng tạo ra các bản copy theo chuẩn thời gian do người dùng thiết lập qua đó có thể tự khôi phục dữ liệu.

### Cách cấu hình:

Vào C -> tạo folder Shadow -> data.txt (thêm nội dung là: "123") -> save lại. Sau đó **Share** folder **Shadow**  
Phải chuột ổ C -> Properties -> tab **Shadow copies** (mặc định tính năng này bị disable) -> **Enable**.

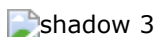
 shadow 1

Xuất hiện bảng thông báo -> **yes**.

Sau khi bấm yes thì lập tức tính năng Shadow Copy sẽ truy xuất ổ đĩa C kiểm những folder, file nào đang được share và tạo bản copy tại thời điểm ta enable.

Sau đó ta cấu hình thời gian mà Shadow Copy tự động nhân bản (nếu cấu hình không chặt chẽ thì dung lượng ổ cứng sẽ tăng nhanh, hoặc cấu hình nhân bản trong lúc cao điểm user truy xuất hệ thống thì sẽ làm giảm hiệu năng hệ thống).

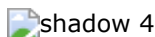
Chọn Setting

 shadow 3

Storage Area: chọn nơi lưu trữ các bản sao.

Để thiết lập thời gian -> chọn **schedule**

Mặc định Windows thiết lập 2 thời điểm

 shadow 4

7h sáng hàng ngày: để copy các dữ liệu từ chiều hôm trước

12h trưa: copy các thông tin phát sinh từ sáng.

Tùy mục đích mà ta điều chỉnh schedule cho hợp lý.

### Cách Test.

Mở Data.txt chỉnh sửa thành "456" -> save lại

Mở tab Shadow Copies trong ổ C

(bấm create now để copy các file ngay lập tức)

Khi muốn restore dữ liệu về thời điểm nào thì Properties Data.txt -> Tab Previous version (tab này chỉ có khi enable tính năng Shadow)

 shadow 5

Chọn thời điểm -> **Restore**.

# 31. Windows Server Backup (Phần 2)

**Phần 2** mình sẽ đi vào cách cấu hình.

**Chuẩn bị:** Máy ảo chạy server 2012, ổ cứng ảo phải có 2 phân vùng, nếu chỉ có 1 thì add thêm ổ cứng.

Windows NT backup và 1 số chương trình backup khác khi backup sẽ dựa vào thuộc tính Archive. Khi chúng ta chỉnh sửa, hay tạo mới 1 file nào đó, lập tức hệ thống sẽ gán cho file đó thuộc tính Archive (A).

Windows dựa vào thuộc tính A để xác định đâu là file mới trong hệ thống.

Windows Server Backup thì không còn căn cứ vào thuộc tính A.

Việc so sánh giữa NT Backup và Windows Server Backup mình sẽ đề cập ở bài sau.

Windows Server Backup có 2 loại backup:

- VSS full backup
- VSS Copy backup (mặc định là loại này)

VSS full backup: backup xong thì xóa luôn thuộc tính A.

VSS copy backup: backup dữ liệu nhưng không xóa thuộc tính A. Ta nên dùng loại này khi server có kèm theo phần mềm backup khác (vì như đã biết các chương trình backup phải dựa vào thuộc tính A)

Cách cấu hình Backup trên Server 2012 (hoặc 2012R2).

## Triển khai:

+ Có 2 đối tượng Group có thể backup là: **Administrator và Backup Operator**.

+ Khi backup 1 folder nào đó được phân quyền NTFS thì Group Backup Operator phải có ít nhất là quyền Read.

Bước 1:

Mở Server Manager -> Manage -> Add Roles and Features -> Ta next mặc định đến cửa sổ

Select Feature: check vào Windows Server Backup. Rồi Next mặc định -> **Install**.

 backup 1

Bước 2: Mở chương trình Windows Server Backup:

Server manager -> Tools -> Windows Server Backup hoặc (start -> run -> **wbadmin.msc**)

 backup 2

Ta có 2 tùy chọn backup

- + **Backup once:** chỉ backup 1 lần sau khi ta cấu hình.
- + **Backup Schedule:** chạy theo lịch biểu mà ta thiết lập

Ta chọn Backup Schedule

**Getting Started: -> Next**

Select Backup Configuration:

**Full Server** (bare metal backup): sao lưu tất cả các ổ đĩa có trên server.

Custom: tùy chọn folder, ổ đĩa để sao lưu. Ta chọn **Custom -> Next**


 backup 3

**Select Items for server:** Chọn Add Items: để chọn nơi muốn backup

Ở đây ta chọn folder Data trong ổ đĩa C -> Next

 backup 4

(lưu ý: để chỉnh loại backup thì sau khi **chỉ định nơi backup**, ta chọn **Advanced setting -> tab VSS Settings**)

 backup 15

**Specify Backup Time:** lập lịch để backup chạy

 backup 5

Ta có 2 option

+ **Once a day:** lịch biểu chạy 1 lần backup trong 1 ngày

+ **More than once a day:** lập lịch để chạy backup nhiều lần trong 1 ngày:

12hPM: backup trong giờ nghỉ trưa.

12hAM: backup lần thứ 2 vào rạng sáng.

(cần kết hợp với UPS để phòng trường hợp cúp điện (backup sẽ không diễn ra)).

-> Next.

**Specify Destination File:** Chọn nơi lưu trữ file backup

+ Back up to hard disk... : lưu file backup trên 1 ổ cứng khác (nên sử dụng, không nên lưu trên ổ đĩa chứa hệ điều hành).

+ Back up to a volume: lưu trên 1 phân vùng ( chung ổ đĩa với HDH => không an toàn)

+ Back up to a shared network volume: lưu trên 1 share folder troeng hệ thống mạng (không khuyên dùng)

Không nên dùng cách thứ 3 : do khi lập lịch back up (schedule) thì dữ liệu sẽ bị ghi đè (replace). Trong khi 2 cách trên thì dữ liệu sẽ được lưu trữ nối tiếp (append) nghĩa là cách 3 chỉ có 1 bản backup trong khi 2 cách trên có bản back up cho từng thời điểm.

Ta chọn cách 1 (do mình đã add thêm ổ cứng ảo) -> Next

 backup 6

**Select Destination Disk:** chọn ổ cứng để lưu file backup -> Next


 backup 7

Xuất hiện thông báo: format ổ cứng và lúc này ổ cứng chỉ có tác dụng chứa file backup ( ổ cứng sẽ bị ẩn và chúng ta không thể truy cập, lưu trữ các file khác) -> Ok

 backup 8

 backup 9

-> **Finsish**

 backup 10

Vậy là đã lập lịch thành công. Mặc định file backup sẽ được ghi đè vào từng thời điểm backup. Khi restore thì chỉ cần chọn thời điểm cần restore trên file back up.

### Lưu ý

- Chỉ có user trong group Administrators và Backup Operators mới có quyền thực thi chức năng backup.
- Có thể tạo VHD file rồi attach vào disk management để lưu file backup (tạo thành ổ đĩa ảo chứa file backup) như bài Lab để tạo máy ảo.

Khi làm việc với Windows Server Backup (WSB), mình có nhận xét như sau

- WBS sử dụng VSS nên khi nhận thấy dữ liệu đang được sử dụng trong quá trình backup. nó lập tức tạo ra 1 snapshot. Do đó quá trình backup không bị ảnh hưởng.

- Sử dụng block-level backup giúp cho quá trình backup nhanh, tiết kiệm dung lượng.

Nhưng WBS cũng có không ít những hạn chế sau:

- Khi lập schedule thì mặc định backup sẽ chạy từ thứ 2 đến CN ( NT backup 2003 có khả năng lập lịch theo ngày).

- Không hỗ trợ lưu file backup ra Tape.

Download: Tài liệu Backup

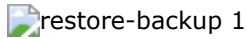
# 32. Windows Server Backup: Restore Data, System State

## Chuẩn bị:

Lấy kết quả từ 2 phần trước.

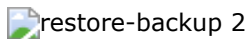
Khi hệ thống bị sự cố, nếu chúng ta có chiến lược backup phù hợp thì việc khôi phục dữ liệu rất dễ dàng. Sau đây mình sẽ hướng dẫn các bạn restore data bằng Windows Server Backup

Mở Windows Server Backup (wbadmin.msc)

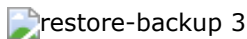


Chọn **Recover...**

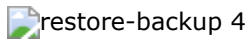
Chọn nơi lưu trữ file Backup, do mình lưu ở ổ cứng trong server nên chọn **This server**.



**Select Backup Date:** Chọn thời điểm để restore

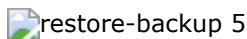


**Recovery Type:** Muốn restore từng file hay folders thì chọn option đầu tiên. Nếu muốn restore cả ổ C thì chọn Volumes ( dĩ nhiên để restore cả volume thì bạn phải backup nó trước).



Chọn file, folder cần restore. Bạn có thể chọn 1 hay nhiều file để restore ( đây là 1 trong những điểm hay của windows server backup)

Ở trường hợp này mình chọn Restore cả folder Data.



**Recovery Options:** các tùy chọn khôi phục file.

Recovery destination: bạn có thể chọn nơi khôi phục file gốc (không nhất thiết là phải ở vị trí lúc backup)

Có 3 option:

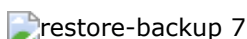
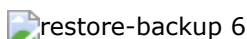
Create copies....: tạo ra 1 bản copy – tức là không chép đè lên file cũ (lúc này ta có 2 version: 1 version lúc chưa restore và 1 version backup)

Overwrite: khôi phục đè, lúc này chỉ còn lại 1 bản (lúc backup)

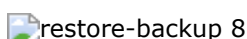
Do not Recover...: Tại nơi restore (recovery destination), nếu tồn tại file, folder trùng tên với các file, folder của bản backup thì sẽ giữ nguyên,

không restore nữa. Chỉ restore những file, folder không có trong recovery destination


Nên chọn Option 1, nó giúp ta so sánh, chọn lựa (theo mình thì đây là điểm cải tiến hay của Windows Server Backup).



Quá trình khôi phục bắt đầu



Do mình chọn Option 1 nên hệ thống sẽ tạo 1 bản copy ( 2 thời điểm giúp ta dễ dàng chọn lựa)

 restore-backup 9

Cách khôi phục system state trên Domain Controller

Ta backup System State như hình

 Backup - Restore System State 1

Đối với Domain Controller, khi restore system state phải vào Directory Services Repair Mode (Mode này sẽ stop AD service, giúp ta có thể khôi phục system state)

Và phải đăng nhập bằng quyền của built-in Administrator với password là pass lúc ta nâng cấp DC.

 Backup - Restore System State 2

Nếu lỡ xóa các đối tượng trong AD thì ngoài việc restore system state thì ta có thể sử dụng các cách sau

- + Sử dụng Active Directory Recycle Bin.
- + Dùng tool ADrestore.