QUẢN TRỊ MẠNG – LÝ THUYẾT

1 Dịch vụ truyền thông TCP/IP cung cấp cho ứng dụng:

Mạng **TCP/IP** cung cấp ba dịch vụ truyền thông cho ứng dụng:

- Dịch vụ **TCP**: truyền thông end-to-end, truyền thông tin cậy hướng liên kết; Dịch vụ này do giao thức Tcp cung cấp.
- Dịch vụ **UDP**: truyền thông end-to-end, truyền không tin cậy phi liên kết theo thời gian thực; Dịch vụ này do giao thức Udp cung cấp.
- Dịch vụ **IP**: truyền thông host-to-host, truyền không tin cậy phi liên kết; dịch vụ này cho giao thức Ip cung cấp.

Khi phát triển ứng dụng mạng đầu tiên cần lựa chọn loại dịch vụ truyền thông end-to-end sẽ được sử dụng. Hai loại dịch vụ này được gọi chung là dịch vụ giao vận.

Dịch vụ truyền host-to-host chỉ được sử dụng khi phát triển một số loại ứng dụng đặc biệt (như ping, tracert).

1.1 Dịch vụ và giao thức TCP

Giao thức **TCP** cung cấp cho ứng dụng dịch vụ hướng kết nối (connection-oriented service), dịch vụ truyền tin cậy (reliable data transfer service).

Dịch vụ hướng kết nối: trong truyền thông qua giao thức TCP, các chương trình phải trao đổi thông tin kiểm soát trước khi dữ liệu của ứng dụng được truyền đi. Thủ tục này được gọi là 'bắt tay ba bước' và tạo ra một kết nối TCP (TCP connection) giữa hai chương trình. Đây là loại kết nối song công (full-duplex), nghĩa là hai chương trình có thể đồng thời gửi dữ liệu cho nhau. Khi ứng dụng hoàn thành việc gửi dữ liệu, kết nối TCP có thể được hủy bỏ.

Dịch vụ truyền tin cậy: TCP đảm bảo các chương trình tham gia truyền thông có thể truyền toàn bộ dữ liệu mà không bị lỗi và tới theo đúng thứ tự. Nói một cách khác, khi một chương trình nguồn truyền dữ liệu đi, TCP đảm bảo chương trình đích sẽ nhận được đúng dữ liệu đó, không mất hoặc dư thừa byte nào.

Tcp được sử dụng nếu đặt ra yêu cầu cao về tính toàn vẹn của dữ liệu khi truyền nhưng có thể chấp nhận tốc độ truyền thấp.

1.2 Dịch vụ và giao thức UDP

UDP là một giao thức đơn giản cung cấp dịch vụ phi liên kết (connectionless service) cho ứng dụng. Khi sử dụng UDP không tạo ra kết nối giữa các chương trình tham gia truyền thông, và do đó, cũng không có các thủ tục bắt tay như TCP. Dữ liệu truyền theo UDP ở dạng các gói tin gọi là Datagram.

UDP cung cấp dịch vụ truyền dữ liệu không tin cậy (unreliable data transfer service). Khi một chương trình gửi dữ liệu qua UDP, giao thức UDP không đảm bảo dữ liệu đó sẽ đến đích, đồng thời, các dữ liệu truyền tới đích có thể không theo đúng thứ tự như khi nó được gửi đi.

UDP không có cơ chế kiểm soát nghẽn, do đó máy nguồn có thể gửi dữ liệu theo bất kỳ tốc độ nào.

Giao thức UDP thường được sử dụng trong các ứng dụng thời gian thực do các ứng dụng loại này có thể chấp nhận thất thoát dữ liệu nhưng yêu cầu tốc độ truyền dữ liệu cao hơn. Do tường lửa trên các thiết bị luôn có xu hướng chặn phần lớn các loại dòng dữ liệu UDP nên cần chú ý khi lựa chọn giao thức UDP.

2 Mô hình, bộ giao thức OSI và TCP/IP

<table>
<tr><th></th><th>Các tầng OSI</th><th>Họ giao thức TCP</th><th colspan="5">TCP/IP Stack</th></tr>
<tr><td>7</td><td>Tầng ứng dụng</td><td rowspan="3">Tầng ứng dụng</td><td rowspan="3">HTTP</td><td rowspan="3">FTP</td><td rowspan="3">SMTP</td><td rowspan="3">RIP</td><td rowspan="3">DNS</td></tr>
<tr><td>6</td><td>Tầng trình diễn</td></tr>
<tr><td>5</td><td>Tầng phiên</td></tr>
<tr><td>4</td><td>Tầng giao vận</td><td>Tầng giao vận</td><td colspan="3">TCP</td><td colspan="2">UDP</td></tr>
<tr><td>3</td><td>Tầng mạng</td><td>Tầng Internet</td><td colspan="5">ICMP,IP, IGMP</td></tr>
<tr><td>2</td><td>Tầng liên kết dữ liệu</td><td rowspan="2">Tầng mạng</td><td colspan="5" rowspan="2">Ethernet, ATM, Frame Relay,..</td></tr>
<tr><td>1</td><td>Tầng vật lý</td></tr>
</table>

2.1 Mô hình OSI

Open Systems Interconnection Reference Model (Mô hình tham chiếu kết nối các hệ thống mở) là mô hình căn bản về các tiến trình truyền thông, thiết lập các tiêu chuẩn kiến trúc mạng ở mức Quốc tế, là cơ sở chung để các hệ thống khác nhau có thể liên kết và truyền thông được với nhau. Mô hình OSI tổ chức các giao thức truyền thông thành 7 tầng, mỗi một tầng giải quyết một phần hẹp của tiến trình truyền thông, chia tiến trình truyền thông thành nhiều tầng và trong mỗi tầng có thể có nhiều giao thức khác nhau thực hiện các nhu cầu truyền thông cụ thể.

Lớp 7 - Lớp Application

Đây là lớp gần gũi nhất với người dùng cuối. Nó cung cấp giao diện giữa các ứng dụng với các lớp phía dưới. Nhưng chú ý rằng các chương trình bạn đang sử dụng (như một trình duyệt web - IE, Firefox hay Opera ...) không thuộc về lớp Application.Telnet, FTP, client email (SMTP), HyperText Transfer Protocol (HTTP) là những ví dụ của lớp Application.

Lớp 6 - Lớp Presentation

Lớp này đảm bảo việc trình bày dữ liệu, mà các thông tin liên lạc qua lớp này nằm trong các hình thức thích hợp đối với người nhận. Nói chung, nó hoạt động như một dịch giả của mạng. Ví dụ, bạn muốn gửi một email và tầng trình bày sẽ định dạng dữ liệu của bạn sang định dạng email. Hoặc bạn muốn gửi ảnh cho bạn bè của bạn, lớp Presentation sẽ định dạng dữ liệu của bạn vào các định dạng GIF, JPG hoặc PNG ....

Lớp 5 - Lớp Session

Nhiệm vụ của lớp 5 là thiết lập, duy trì và kết thúc giao tiếp với các thiết bị nhận.

Lớp 4 - Lớp Transport

Lớp này duy trì kiểm soát dòng chảy của dữ liệu và thực hiện kiểm tra lỗi và khôi phục dữ liệu giữa các thiết bị. Ví dụ phổ biến nhất của tầng giao vận là Transmission Control Protocol (TCP) và User Datagram Protocol (UDP).

Lớp 3 - Lớp Network

Lớp này cung cấp địa chỉ logic mà router sẽ sử dụng để xác định đường đi đến đích.Trong hầu hết các trường hợp, địa chỉ logic ở đây có nghĩa là các địa chỉ IP (bao gồm nguồn & địa chỉ đích IP).

Lớp 2 - Lớp Data Link Layer

Các lớp liên kết dữ liệu định dạng các thông điệp vào một khung dữ liệu(Frame), và thêm vào đó một header chứa các địa chỉ phần cứng nơi nhận và địa chỉ nguồn của nó. Tiêu đề này chịu trách nhiệm cho việc tìm kiếm các thiết bị đích tiếp theo trên một mạng nội bộ.

Chú ý rằng lớp 3 là chịu trách nhiệm cho việc tìm kiếm con đường đến đích cuối cùng (mạng) nhưng nó không quan tâm về việc ai sẽ là người nhận tiếp theo. Vì vậy lớp 2 giúp cho dữ liệu truyền được điểm đến tiếp theo.

Lớp này là chia nhỏ thành 2 lớp con: điều khiển logic liên kết (LLC) và kiểm soát truy cập media (MAC).

Các chức năng LLC bao gồm:

+ Quản lý các khung cho các lớp trên và dưới

+ Kiểm soát lỗi

+ Điều khiển luồng

Lớp con MAC mang địa chỉ vật lý của mỗi thiết bị trên mạng.Địa chỉ này là thường được gọi là địa chỉ MAC của thiết bị.Địa chỉ MAC là một địa chỉ 48 bit được ghi vào NIC trên thiết bị của nhà sản xuất.

Lớp 1 - Lớp Physical

Lớp vật lý định nghĩa các đặc tính vật lý của mạng chẳng hạn như kết nối, cấp điện áp và thời gian.

Lớp	Miêu tả	Các giao thức phổ biến	Đơn vị dữ liệu giao thức	Thiết bị hoạt động trong lớp này
Ứng dụng	+ Giao diện người dùng	HTTP, FTP, TFTP, Telnet, SNMP, DNS ...	Dữ liệu (Data,Message)	
Trình bày	+ Đại diện dữ liệu, mã hóa và giải mã	+ Video (WMV, AVI ...) + Bitmap (JPG, BMP, PNG ...) + Audio (WAV, MP3, WMA ...)	Dữ liệu (Data,Message)	
Phiên	+ Thiết lập, theo dõi và chấm dứt các phiên kết nối	+ Tên SQL, RPC, NETBIOS ...	Dữ liệu (Data,Message)	
Vận chuyển	+ Dòng điều khiển (Buffering, Windowing, Congestion Avoidance) giúp ngăn ngừa sự mất mát của các phân đoạn trên mạng và sự cần thiết phải truyền lại	+ TCP (Connection-Oriented, đáng tin cậy) + UDP (Connectionless, không đáng tin cậy)	Segment	
Mạng	+ Xác định đường dẫn + Địa chỉ logic(Nguồn/Đích)	+ IP + IPX + AppleTalk	Packet / Datagram	Router
Liên kết dữ liệu	+ Địa chỉ vật lý Bao gồm 2 lớp: + Lớp trên: Logical Link Control (LLC) + lớp dưới: Media Access Control (MAC)	+ LAN + WAN (HDLC, PPP, Frame Relay ...)	Frame	Switch, Bridge
Vật lý	Mã hóa và truyền các bit dữ liệu + Tín hiệu điện + tín hiệu vô tuyến điện	+ FDDI, Ethernet	Bit (0, 1)	Hub, Repeater ...

2.2 Mô hình TCP/IP

Các tầng trong mô hình TCP/IP

Tầng ứng dụng (Application layer) chịu trách nhiệm làm việc với dữ liệu người dùng. Các giao thức thuộc tầng này sẽ sử dụng một trong hai giao thức của tầng giao vận để truyền thông tin tới điểm cuối. Các giao thức tầng ứng dụng thường gặp: Telnet, FTP, DNS, SMTP, SNMP, TFTP, NFS, DHCP. Các giao thức tầng này được thực thi trực tiếp trong ứng dụng.

Tầng giao vận (Transport layer) chứa hai giao thức TCP (Transmission Control Protocol) và UDP (User Datagram Protocol), chịu trách nhiệm phục vụ tầng tầng ứng dụng và đảm bảo truyền thông điểm cuối – điểm cuối giữa các máy trong mạng. Các giao thức này được thực thi ở dạng phần mềm và cài đặt trực tiếp trong hệ điều hành.

Tầng internet/tầng mạng (Internet layer/Network layer) chịu trách nhiệm vận chuyển các gói tin qua mạng. Tầng này chứa tất cả các giao thức định tuyến (IGMP, ICMP, RIP, OSPF) và giao thức vận chuyển dữ liệu người dùng IP. Các thiết bị hoạt động ở tầng này (router) có nhiệm vụ nhận gói tin, xác định điểm đến của gói tin, và chuyển gói tin về phía máy đích.

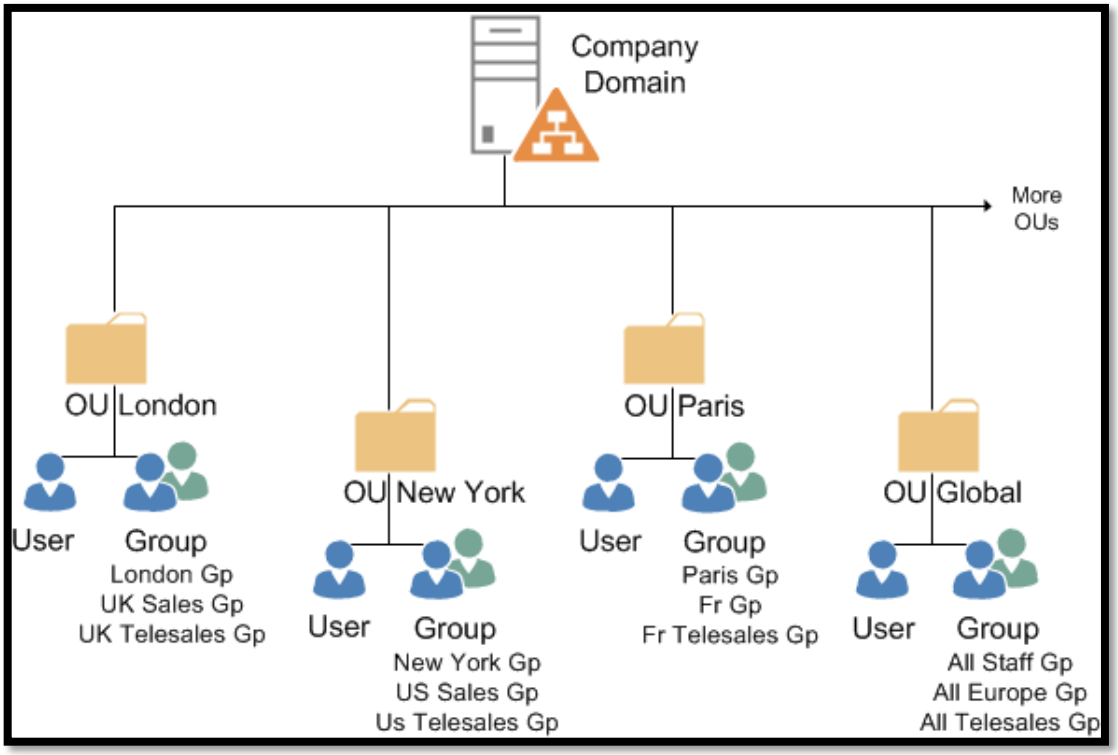
Tầng này cũng chứa các giao thức gửi và nhận thông báo lỗi và các thông điệp điều khiển. Các giao thức ở tầng này có thể được thực hiện ở cả phần cứng và phần mềm. Giao thức IP trên máy tính được thực hiện ở dạng hàm hệ thống, trên router được thực hiện ở phần cứng.

Tầng liên kết/tầng giao diện mạng (Link layer/ Network Interface layer) chịu trách nhiệm hoạt động với trình điều khiển thiết bị và các giao diện phần cứng để kết nối máy tính với môi trường truyền. Một số giao thức tầng liên kết: ATM, Ethernet, PPP, Frame Relay, Token Ring, FDDI. Các giao thức ở tầng này được thực thi hầu hết trong phần cứng.

3 Một số khái niệm trên Windows Servers

Mô hình mạng **peer-to-peer** (Mạng ngang hàng): Workgroup (Các máy tính kết nối với nhau thông qua mạng LAN, tài nguyên được phân tán trên từng máy).

Mô hình **client-server**: Domain (Một máy làm DC và các máy còn lại tham gia vào domain).



3.1 Domain

Domain: tập hợp các máy tính nối mạng, các tài nguyên được quản lý tập trung (trên domain controller).

Windows Server 2000/2003/2008 lưu trữ dữ liệu của domain theo Active Directory.

3.2 Active Directory

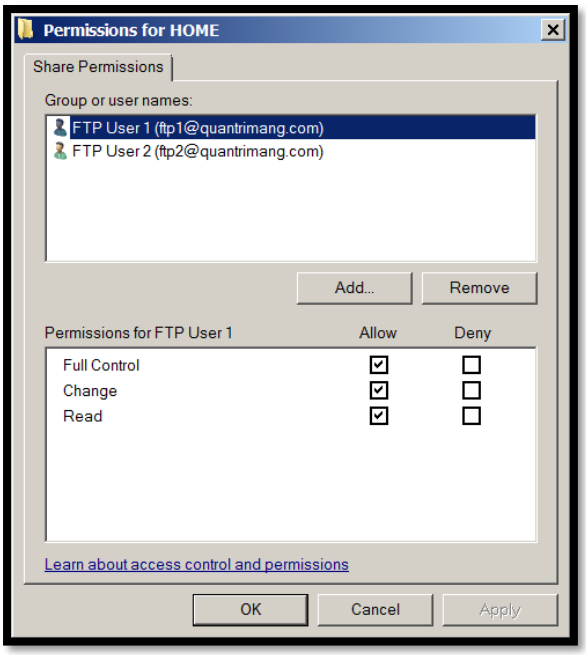
Active Directory là tổ chức có thứ bậc lưu trữ và quản lý thông tin về tài nguyên trên mạng Windows Server. Server chạy AD Domain Services gọi là Domain Controller (DC).

Chức năng của AD:

- Cho phép tạo ra nhiều tài khoản người dùng với mức độ quyền khác nhau
- Lưu trữ thông tin người dùng vào máy tính
- Chứng thực và quản lý đăng nhập
- Duy trì bản chỉ mục, giúp cho quá trình tìm kiếm tài nguyên mạng diễn ra nhanh hơn (Tổng hợp các tài nguyên được chia sẻ phân tán trên các máy, lưu trữ thành danh sách. Hiển thị chỉ mục, liên kết đến tài nguyên nằm trên một máy cụ thể)
- Chia nhỏ Domain thành nhiều Sub-domain hay Organizational unit (OU)

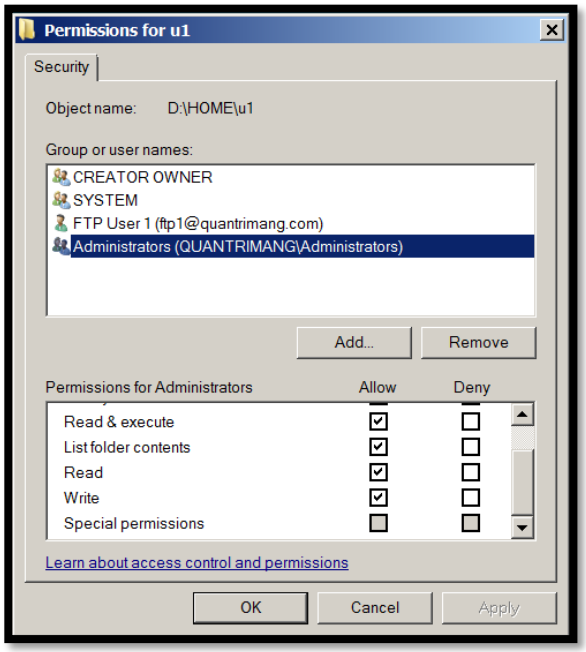
3.3 Share Permissions

Share permissions là quyền của người dùng để truy cập dữ liệu (folder) dùng chung từ xa qua mạng (Network Access), không tác động với người dùng ngồi trực tiếp trên máy (Local Access). (Nằm ở tab Sharing → Advanced Sharing).



- **Full Control:** Toàn quyền (Change + Read), có quyền chỉnh sửa và lấy quyền sở hữu NTFS các tệp (edit permissions and take ownership).
- **Change:** Đọc, sao chép, thực thi, chỉnh sửa, tạo mới, xoá
- **Read:** Đọc, sao chép, thực thi

3.4 NTFS Permissions



NTFS Permissions là quyền truy cập dữ liệu (folder, file) cụ thể trên một máy tính cụ thể, tác động lên Network Access và Local Access. NTFS permission có tính thừa kế (quyền của folder cha thế nào thì khi tạo folder con sẽ có quyền tương tự). (Nằm ở tab Security → Edit).

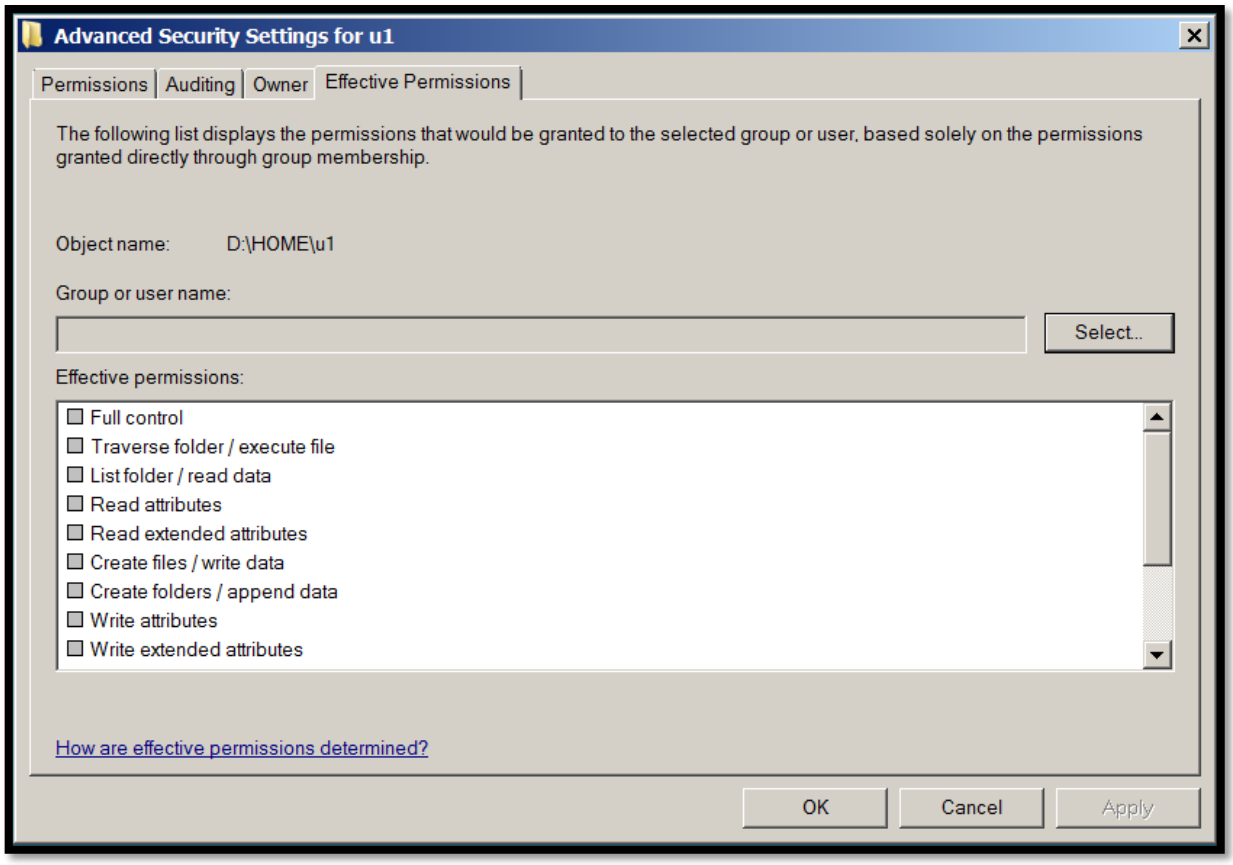
NTFS permission gồm 2 nhóm chính:

Standard permission (6 bộ quyền):

- **Full control:** bằng quyền **Modify** + quyền Change Permission (là quyền được cho phép thiết lập lại các bộ quyền) + Take Ownership.
- **Modify:** bằng quyền **Write** + quyền xoá.
- **Read & execute:** xem nội dung các file (.doc, .ppt, .xls,…) và thực thi các file nếu file đó là chương trình (.exe, .bat,…).
- **List folder contents:** liệt kê nội dung, đi vào bên trong folder (có thể mở folder để xem có các file, sub folder nào trong đó).
- **Read:** xem tài nguyên (xem thư mục và nội dung của thư mục con).
- **Write:** xem, chỉnh sửa tệp, tạo mới folder, chép dữ liệu vào folder nhưng không thể xóa các đối tượng.

		NTFS Basic Permission					
		Full control	Modify	Read&excute	List folder contents	Read	Write
Share Permission	Full control	x	x	x	x	x	x
	Change		x	x	x	x	x
	Read			x	x	x	

*__Special permissions__ sẽ bị mờ (Nằm ở tab Security → Advanced → Effective Permissions).



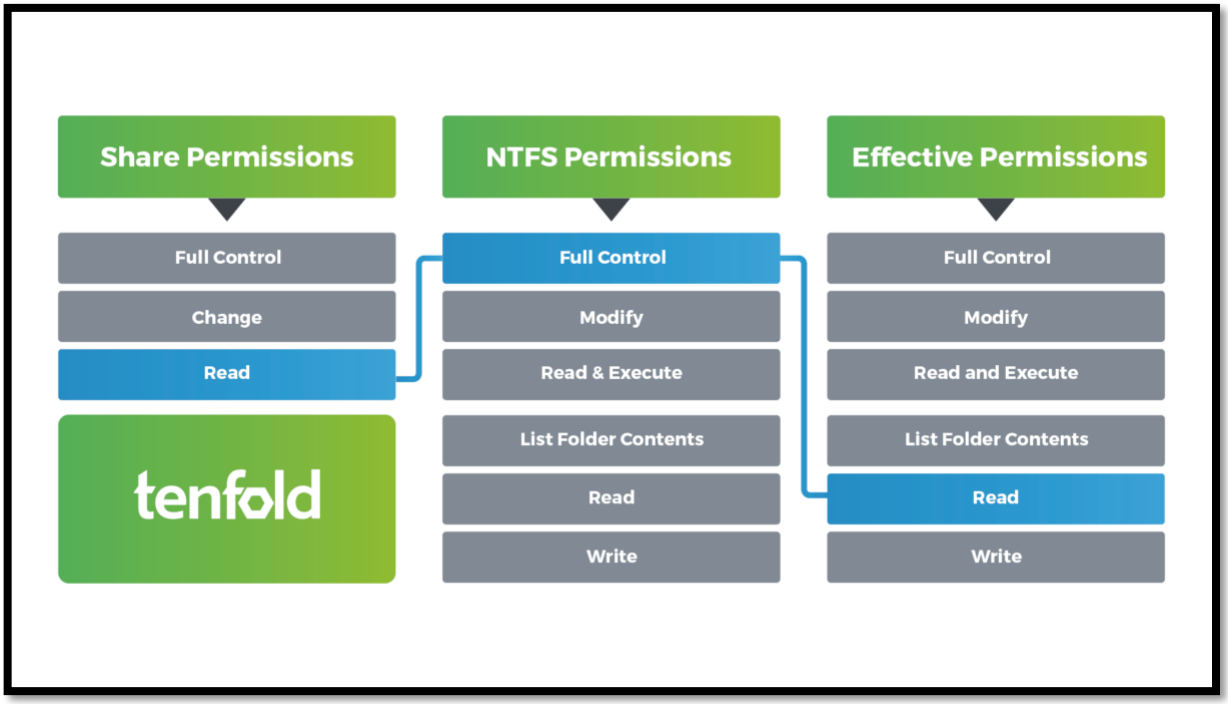
Special permission (14 bộ quyền):

- **Full control:** toàn quyền, giống Standard permission
- **Traverse folder / execute file:** quyền nhảy cấp (tại thư mục này không có quyền đi vào và thực thi nhưng lại có quyền tại thư mục con bên trong).
- **List folder / read data:** đi vào thư mục và đọc dữ liệu trong thư mục đó.
- **Read attributes:** đọc thuộc tính của folder và file (Read-only, Hidden,…).
- **Read extended attributes:** đọc thuộc tính mở rộng (Archive, Encrypt).
- **Create files / write data:** tạo file, ghi và chỉnh sửa dữ liệu.
- **Create folders / append data:** tạo và chỉnh sửa tên 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) khác nhau sẽ có các thuộc tính mở rộng khác nhau.
- **Delete subfolders and files:** xóa các file và các folder con bên trong.
- **Delete:** cho phép xóa tài nguyên (folder, subfolder, file).
- **Read permissions:** cho phép user, group thấy các quyền hạn mà ta đã cấu hình.

- **Change permissions:** cho phép thay đổi các quyền hạn đối với file, folder.
- **Take ownership:** cho phép lấy, chiếm quyền sở hữu file, folder của người khác.

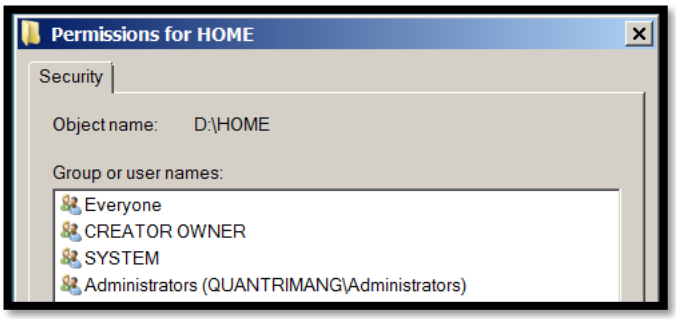
***Lưu ý khi phân quyền:**

- Có thể chỉ cấp quyền Read để ngăn user thay vì Deny (quyền Deny sẽ ghi đè lên các quyền khác nếu được chọn).
- Nếu một user nằm ở 2 group, group nào có quyền lớn hơn thì user sẽ có quyền đó (Deny, Read → Deny | Read, Modify → Modify).
- Khi thực hiện phân quyền phải thực hiện từ folder cha đi xuống.
- Khi sử dụng cả Share Permissions và NTFS Permissions, quyền thấp nhất sẽ được áp dụng (Deny, Read → Read | Read, Modify → Read).



3.5 Các group định danh cơ bản khi phân quyền

Là group quy định để lấy thành viên.



- **Administrators:** đây là group quản trị hệ thống, User thuộc group này sẽ có quyền quản trị.
- **SYSTEM:** đây là group định danh của hệ thống (mặc định Full Control)
- **CREATOR OWNER:** đây là group chứa những User có toàn quyền đối với tài nguyên do họ tạo ra (Ai tạo ra tài nguyên nào thì người đó thuộc group Creator Owner trên tài nguyên đó, có toàn quyền đối với tài nguyên do mình tạo ra).

- **Users:** những User tạo ra mặc định sẽ thuộc vào group Users.

3.6 Các quyền liên quan

- **Quyền kế thừa:** là những bộ quyền mà thư mục con thừa hưởng từ thư mục cha
- **Cấm quyền (Deny):** là quyền cấm tường minh (chỉ định rõ user cần cấm)
- **Cấm ngầm định:** ngăn không cho một group có quyền trong một thư mục chỉ định bằng cách Remove group đó ra khỏi thư mục cần (Ví dụ: xoá group KETOAN ra khỏi thư mục NHANSU)

Khi cắt/xoá quyền kế thừa:

- **Copy:** giữ lại các đối tượng ở folder cha và folder con (Ví dụ: nếu folder cha có group KETOAN thì folder con cũng có group KETOAN)
- **Remove:** xoá tất cả các quyền kế thừa, các đối tượng trong NTFS Permissions, kể cả các group hệ thống (Administratos, SYSTEM, CREATOR OWNER)