ỦY BAN NHÂN DÂN HUYỆN CỦ CHI
TRƯỜNG TRUNG CẤP NGHỀ CỦ CHI

GIÁO TRÌNH
MÔ ĐUN: BẢO TRÌ HỆ THỐNG MẠNG
NGHỀ: QUẢN TRỊ MẠNG MÁY TÍNH
TRÌNH ĐỘ: TRUNG CẤP NGHỀ

Ban hành kèm theo Quyết định số: 89/QĐ-TCNCC ngày 15 tháng 08 năm 2024 của Hiệu trưởng Trường Trung cấp nghề Củ Chi

Năm 2024

TUYÊN BỐ BẢN QUYỀN:

LỜI GIỚI THIỆU

Giáo trình "***Bảo trì hệ thống mạng***" được biên soạn theo Chương trình khung Quản trị mạng máy tính đã được Bộ Lao động – Thương binh và Xã hội ban hành.

Trong những năm qua, dạy nghề đã có những bước tiến vượt bậc cả về số lượng và chất lượng, nhằm thực hiện nhiệm vụ đào tạo nguồn nhân lực kỹ thuật trực tiếp đáp ứng nhu cầu xã hội. Cùng với sự phát triển của khoa học công nghệ trên thế giới, lĩnh vực Công nghệ thông tin nói chung và ngành Quản trị mạng ở Việt Nam nói riêng đã có những bước phát triển đáng kể.

Chương trình khung quốc gia nghề Quản trị mạng đã được xây dựng trên cơ sở phân tích nghề, phần kỹ thuật nghề được kết cấu theo các mô đun. Để tạo điều kiện thuận lợi cho các cơ sở dạy nghề trong quá trình thực hiện, việc biên soạn giáo trình kỹ thuật nghề theo theo các mô đun đào tạo nghề là cấp thiết hiện nay.

Nội dung chính của giáo trình được chia thành 05 bài, bao gồm các nội dung:

1. Phần cứng
2. Phần mềm
3. Truy cập mạng, máy in mạng
4. Mạng Internet dùng chung
5. Bảo mật, bảo trì

Bảo trì hệ thống mạng là mô đun đào tạo nghề được biên soạn theo hình thức tích hợp lý thuyết và thực hành. Trong quá trình thực hiện, nhóm biên soạn đã tham khảo nhiều tài liệu Quản trị mạng trong và ngoài nước, kết hợp với kinh nghiệm trong thực tế. Mặc dầu có rất nhiều cố gắng, nhưng không tránh khỏi những khiếm khuyết, rất mong nhận được sự đóng góp ý kiến của độc giả để giáo trình được hoàn thiện hơn.

Xin chân thành cảm ơn!

Củ Chi, ngày … tháng … năm 2024

Nhóm biên soạn:

MỤC LỤC

BÀI 1. PHẦN CỨNG

Giới thiệu:

Phần cứng (tiếng Anh: *hardware*), đề cập đến các bộ phận vật lý hữu hình của một hệ thống máy tính; các thành phần điện, điện tử, cơ điện và cơ khí của nó như là[1] màn hình, chuột, bàn phím, máy in, máy quét, vỏ máy tính, bộ nguồn, bộ vi xử lý CPU, bo mạch chủ[2], Các dây cáp, cũng như tủ hoặc hộp, các thiết bị ngoại vi của tất cả các loại, và bất kỳ yếu tố vật lý nào khác có liên quan, tạo nên phần cứng hoặc hỗ trợ vật lý ví dụ như loa, ổ đĩa mềm, ổ đĩa cứng, ổ CDROM, ổ DVD, card đồ họa VGA, card wifi, card âm thanh, bộ phận tản nhiệt...

1. Mục tiêu:

- Xác định được sự cố về phần cứng
- Xác định được nguyên nhân gây ra sự cố
- Xử lý được kịp thời các sự cố.

2. Nội dung bài học

2.1 Sự cố card mạng

Muốn nối mạng với nhau bằng cáp, hoặc kết nối Internet bằng đường truyền, các máy tính phải được trang bị một card mạng hay còn gọi Ethernet card hay NIC (Network Interface Card). Card mạng cũng cần phải có driver để PC nhận diện được thiết bị. Mỗi card mạng sẽ chứa một địa chỉ duy nhất là địa chỉ MAC- Media Access Control (địa chỉ card mạng, địa chỉ vật lý).

Hình 1.1 Card mạng

Vì địa chỉ MAC là duy nhất cho mỗi máy, nên khi máy A gởi thông điệp cho máy B, máy A sẽ dùng địa chỉ MAC của máy B. Máy B khi nhận thông điệp này sẽ so sánh địa chỉ MAC đó xem có trùng với địa chỉ MAC của mình không, nếu trùng thì nhận, không thì bỏ qua. Đây là cách truyền dữ liệu giữa các máy trong mạng Ethernet (Chuẩn thông dụng nhất của mạng LAN)

1.1. Nhiệm vụ của card mạng

- Chuyển đổi các tín hiệu máy tính ra các tín hiệu trên phương tiện truyền dẫn và ngược lại (chuyển đổi dữ liệu song song sang dữ liệu tuần tự và ngược lại). Dễ hiểu hơn, dữ liệu trên dây dẫn sẽ được chuyển về dạng dữ liệu máy tính sử dụng thông qua card mạng.

- Gửi / nhận và kiểm soát luồng dữ liệu được truyền. Điều này là dĩ nhiên vì mọi luồng dữ liệu từ bên ngoài vào PC hay ngược lại đều qua card mạng.

1.2. Lắp ráp card mạng

- Card mạng được chia làm 2 loại:
  + Card onboard (tích hợp thẳng vào mainboard).
  + Card rời, thường được gắn bổ sung vào máy tính thông qua cổng PCI, USB. Card có kết nối thông qua cổng USB nhỏ gọn, dễ cắm và dùng ngay, tuy nhiên nó có giá cao hơn nhiều, thích hợp với máy xách tay hơn, cho nên card PCI vẫn là lựa chọn số một cho người dùng PC.

Giá card mạng hiện nay rất rẻ. Nếu sử dụng card onboard bạn không cần phải làm gì thêm ngoài việc cài dirver như đề cập dưới đây. Với card rời, bạn phải mở thùng máy và gắn card mạng vào cổng PCI trên máy tính. Có rất nhiều cổng PCI và có thể gắn tùy ý cổng nào sao cho thông thoáng máy là tốt nhất. Đảm bảo phải cắm sát, bắt vít cẩn thận để tránh trường hợp bắn tia lửa điện do hở khe cắm (cho dù là rất nhỏ nhưng cũng rất nguy hiểm). Một kết nối lỏng lẻo với cổng PCI sẽ làm card mạng hoạt động chập chờn hoặc không hoạt động.

- Mặc định khi cài đặt Windows, driver sẽ được cài tự động cho hệ thống của bạn, và ngay cả khi bạn sử dụng một card rời thì Windows cũng tự động nhận diện và cài đúng driver cho thiết bị mà không cần người dùng phải cài đặt thêm driver như Windows 9x trở về trước. Tuy nhiên vì lý do nào đó hoặc Windows không có sẵn driver cho card mạng, bạn hãy tiến hành cài driver như sau:
  + Đối với card onboard, bạn chỉ cần đưa đĩa driver của mainboard vào CDROM, trình autorun sẽ tự động chạy, bạn chọn mục LAN Driver, trình setup sẽ bắt đầu.
  + Đối với card rời, nhấp chuột phải vào My Computer, chọn Manage, click mục Device Manager. Nếu tên card mạng của bạn có dấu chấm hỏi thì hãy nhấp phải và chọn Update driver, Browse đến đĩa driver. Nếu đĩa driver có trình autorun xuất hiện thì bạn có thể click nút Install Driver dễ dàng hơn nhiều.
- Sau khi cài đầy đủ driver cho PC, để biết card đã hoạt động chưa, vào Start> Run gõ cmd. Giao diện DOS xuất hiện, bạn gõ lệnh Ping 127.0.0.1. Nếu thấy xuất hiện reply 4 lần xem như công việc hoàn hảo. Hãy kết nối dây mạng và bắt đều lướt web.

1.3. Sự cố card mạng

Bất ngờ một hôm bạn không kết nối Internet được, bạn nghĩ có thể do đường truyền hoặc rớt mạng, nhưng sau đó vẫn không thấy kết nối được, lúc này bạn có thể nghĩ đến vấn đề xuất phát từ card mạng onboard, hãy thay thế bằng một card rời.

Sau khi lắp card mạng mới, bạn đã có thể lướt web nhưng máy tính rất hay không ổn định như hay bị treo giữa chừng, hiện màn hình xanh. Nếu thử cài đặt lại Windows thì sau bước Scan phần cứng, máy không cho cài tiếp tục mà lại hiện màn hình xanh. Nguyên nhân rất có thể card onboard bị hư làm ảnh hưởng đến mainboard, hoặc xung đột giữa card rời mới gắn và card onboard. Cách tốt nhất bạn nên disable card onboard một khi nó bị hư hoặc không cần dùng bằng cách như sau:

Restart máy và gõ phím Delete nhiều lần cho đến khi màn hình BIOS xuất hiện, tìm đến mục quản lý các thiết bị onboard trên mainboard và disable Ethernet card, NIC, Network

Card (tùy loại mainboard), khởi động lại máy, hiện tượng sẽ được giải quyết. Việc cài driver cho Windows nhận diện card mạng chỉ là một phần vấn đề, bước kế tiếp bạn sẽ cài đặt bộ giao thức TCP/IP để cho máy tính một địa chỉ IP, nói cách khác là đặt tên cho PC của bạn. Các dữ liệu và thông tin được nhận về hay gửi đi qua Internet đều dựa trên địa chỉ IP của bạn và người nhận.

2.2 Sự cố phần cứng thiết bị mạng

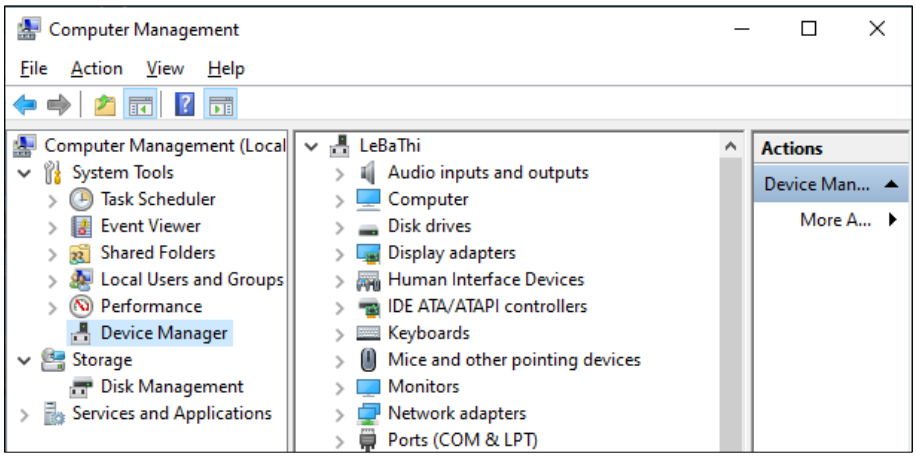
Tổng quan mạng Ethernet

- Mạng khu vực theo chuẩn quốc tế IEEE 802.3 (Ethernet) được thiết kế cho môi trường công nghiệp và mở rộng đến cấp thiết bị hiện trường.
- Kết nối các thiết bị tự động với nhau, với các máy tính và các trạm làm việc cũng như các thiết bị kết nối không dây với phương thức truyền thông đồng nhất hoặc bất đồng nhất.
- PROFINET, chuẩn mở cho tự động hoá, dựa trên chuẩn Ethernet công nghiệp và hỗ trợ việc kết nối các thiết bị từ cấp hiện trường cho đến cấp quản lý.
- Có thể áp dụng giải pháp mạng mở toàn diện.
- Tốc độ truyền thông cao, có thể lên đến 1 gigabit/s
- Ethernet Công nghiệp là một chuẩn công nghiệp, đã được kiểm chứng rộng rãi và được chấp nhận trên toàn thế giới.
- Kết nối tới mạng LAN không dây (WLAN) và các mạng LAN công nghiệp không dây (IWLAN) theo tiêu chuẩn.
- Là nền tảng IT trong tự động hoá, ví dụ như chức năng Web, thư tín điện tử (email) và kết nối IWLAN.
- Giải pháp an toàn được thiết kế đặc biệt cho tự động hóa công nghiệp với khái niệm bảo mật công nghiệp dùng SCALANCES

Sự cố phần cứng Ethernet làm mất mạng

- **Kiểm tra card mạng**

+ Bước đầu tiên, là ta hãy tiến hành kiểm tra lại card mạng. Phần cứng này là một phụ kiện gắn vào bo mạch chủ trên máy tính. Nó sẽ chuyển đổi các thông tin mà máy tính muốn gửi ra mạng, thành các tín hiệu điện có thể truyền đi trên đường cáp. Card mạng thường được gắn vào cổng PCI. Để kiểm tra card mạng, ta mở cửa sổ *Device Manager* để quan sát các thiết bị đang có trong máy tính.



Hình 1.2 Cửa sổ Device Manager

+ Trong cửa sổ ***Device Manager***, ta nhấn vào nút mũi tên trước mục ***Network adapter*** để hiện danh sách các thiết bị mạng. Hãy đảm bảo rằng ta không nhìn thấy dấu hiệu cảnh báo nào trước tên các thiết bị mạng đó. Muốn chắc chắn, ta nhấn kép chuột vào tên card mạng cần kiểm tra. Nếu trong cửa sổ ***Device Status*** hiện ra với dòng thông báo ***This Device is working correctly*** thì có nghĩa là card mạng đang hoạt động tốt.

2.3 Sự cố phần cứng dây cáp

- **Kiểm tra cáp mạng**

+ Nếu card mạng đã hoạt động ổn định sau các bước kiểm tra và sửa lỗi trên, phần cứng kế tiếp mà ta cần kiểm tra để đảm bảo kết nối mạng, chính là cáp mạng. Để kiểm tra xem sợi cáp đang sử dụng có hoạt động tốt hay không, ta nên dùng bộ thiết bị kiểm tra cáp, có bán ở các cửa hàng tin học.

+ Chỉ với loại thiết bị kiểm tra cáp đơn giản bằng đèn LED rẻ tiền, là ta đã có thể biết được sợi cáp có được bấm đúng vị trí các sợi cáp vào đầu RJ45 hay chưa, hoặc có sợi nào bị đứt hay không. Khi thử, ta cắm một đầu sợi cáp mạng vào hộp chính, đầu cáp còn lại vào hộp phụ đi kèm. Sau đó bạn bật công tắc nguồn trên hộp chính, rồi quan sát các đèn led nhấp nháy theo thứ tự đánh số từ 1 đến 8. Nếu cặp đèn nào không sáng theo thứ tự, nghĩa là đường dây đồng tương ứng trong sợi cáp đó đã đứt, hoặc chưa bấm dính vào đầu RJ45. Bạn có thể bấm lại đầu cáp, hoặc bấm một sợi cáp mới.

Hình 1.3 Thiết bị kiểm tra dây cáp mạng RJ45

+ Để có thể bấm được một sợi cáp tốt, trước hết bạn cần chọn mua loại dây cáp chính hãng và các đầu cáp tốt.

Hình 1.4 Đầu bấm mạng RJ45

+ Đầu cáp RJ45 tốt thường được làm bằng nhựa cứng, không giòn, độ trong suốt cao, thanh nhíp giữ phía sau có độ đàn hồi tốt, các miếng đồng ở đầu màu vàng óng.

Nếu cảm thấy khó phân biệt, bạn hãy tìm mua ở những cửa hàng uy tín. Sau khi tước lớp vỏ nhựa bên ngoài và sắp xếp cáp theo đúng chuẩn, bạn hãy đưa các sợi đồng vào đầu cáp RJ45, rồi đẩy mạnh chúng vào hết mức có thể. Rồi bạn kiểm tra lại từng vị trí xem màu sắc các sợi đồng trong đầu cáp đã đúng với chuẩn mình định bấm chưa. Nếu đã chính xác, bạn kiểm tra tiếp về độ sâu của các sợi cáp nhỏ đã được đẩy đến vị trí của các miếng đồng trên đầu RJ45 hay chưa, và phần vỏ cáp có vào đến vị trí chốt nhựa của đầu bấm hay chưa.

Hình 1.5 Đầu dây mạng bấm đúng

+ Cuối cùng bạn đưa đầu cáp vào khe bấm RJ45 trên kềm, rồi dùng sức bóp thật mạnh đến khi nghe một tiếng tách nhỏ. Để chắc chắn, bạn có thể bấm và giữ liên tục nhiều lần để các lá đồng bám chặt vào sợi cáp.

Hình 1.6 Bấm cáp mạng

+ Ngoài ra, bạn cũng nên chú ý đến việc đường cáp mạng bị các loại sóng điện từ gây nhiễu. Nếu bạn dẫn dây cáp đi gần các thiết bị điện dân dụng, hãy dời chúng ra xa. Lỗi thường gặp nhất là khi đường cáp mạng bị xếp chung với dây dẫn điện trong cùng một đường ống nhựa. Bạn hãy tách đường cáp mạng và cáp điện đi theo hai đường ống khác nhau.

- ***Kiểm tra Router*** Lỗi cuối cùng cần kiểm tra để máy tính có thể đi ra được internet chính là thiết bị router ADSL. Đèn led **Power** sẽ cho bạn biết thiết bị đã được cấp nguồn, và đã hoạt động. Đèn **LAN** với cổng mang số thứ tự tương ứng với lỗ cắm cáp mạng, sẽ cho biết đường kết nối giữa máy tính và router đang hoạt động tốt.
- Đặc biệt quan trọng là đèn WAN cho bạn biết tín hiệu từ nhà cung cấp dịch vụ đã được truyền đến Router nhà bạn hay chưa. Nếu đèn này không sáng, bạn hãy liên lạc với

bộ phận hỗ trợ khách hàng của nhà cung cấp dịch vụ, để thông báo cho họ biết. Còn đèn ***Internet*** thì cho biết rằng Router đã kết nối thành công, và đã có thể truyền dữ liệu ra mạng toàn cầu này. Nếu đèn **WAN** sáng, nhưng đèn ***Internet*** không sáng, thì thường là tài khoản đăng nhập của bạn có vấn đề, như sai mật khẩu, hoặc bạn chưa kịp đóng tiền phí dịch vụ của tháng trước.

2.4 Sự cố phần cứng điện

Mất điện đột ngột

- Nguồn điện bị mất đột ngột, điện áp ngay lập tức giảm còn 0V.
- Nguyên nhân chủ yếu thường là do hoạt động cắt điện của công ty điện lực, sự cố quá tải làm nhảy Áp-tô-mát, sự cố đứt, chạm chập trên đường dây dẫn điện… Sự cố này làm cho thiết bị điện, điện tử ngừng hoạt động đột ngột. Đối với PC, việc thiết bị ngừng hoạt động đột đột ngột còn làm ảnh hưởng đến dữ liệu phần mềm, các dữ liệu đang được ghi sẽ bị lỗi. Sau mỗi lần bị tắt đột ngột, máy tính có hiện tượng bị treo, đơ và lỗi. Ngoài ra, nhiều lần bị tắt đột ngột sẽ làm giảm tuổi thọ của máy tính cúng như thiết bị điện, điện tử.

Tăng áp đột ngột

- Điện áp tăng cao đột biến trong một thời gian rất ngắn.
- Nguyên nhân có thể do Sét đánh trực tiếp, Sét lan truyền trên đường đây điện, sự tăng cường thiết bị phát điện hòa vào điện lưới, các sự cố trên đường dây truyền tải điện, nhưng đại đa số là do đóng ngắt các thiết bị phụ tải trên đường dây điện sinh ra.
- Sự cố này có thể làm mất dữ liệu bộ nhớ, lỗi dữ liệu, hư phần cứng. Tệ hơn nữa, khi điện áp tăng cao đột ngột như trường hợp sét đánh sẽ làm hư hỏng thiết bị điện, điện tử ngay lập tức.

Giảm áp đột ngột

- Điện áp giảm thấp đột biến trong một thời gian rất ngắn.
- Nguyên nhân thường là do cắt giảm, sự cố ở trạm máy phát, các sự cố trên đường dây truyền tải điện, nhưng đại đa số là do đóng ngắt các thiết bị phụ tải trên đường dây điện sinh ra.
- Sự cố này dẫn đến lỗi dữ liệu, hư phần cứng, đèn bị chớp nháy, thiết bị tắt vì điện không đủ đáp ứng…

Tăng áp kéo dài

- Điện áp tăng cao kéo dài từ vài phút đến cả ngày.
- Nguyên nhân là do sự tăng cường thiết bị phát điện hòa vào điện lưới, sự cắt giảm thiết bị phụ tải, các sự cố trên đường dây truyền tải điện. Gây hư hỏng nặng cho môtơ, máy vi tính và các thiết bị điện, điện tử khác, làm bộ nhớ bị hư/mất dữ liệu, tăng nguy cơ cháy nổ…

Giảm áp kéo dài

- Điện áp giảm thấp kéo dài từ vài phút đến cả ngày.
- Nguyên nhân là do cắt giảm, sự cố ở trạm máy phát, sự tăng thêm phụ tải, các sự cố trên đường dây truyền tải điện. Sự cố làm thiết bị giảm tuổi thọ, hư hỏng do nhiệt độ phát sinh tăng cao. Nguy cơ gây cháy nổ…

Biến tần

- Sự thay đổi tần số so với tần số ổn định.

+ Nguyên nhân là do lỗi của máy phát điện không ổn định, do chất lượng nguồn điện không đảm bảo… Sự thay đổi tần số điện dẫn đến mất dữ liệu, hệ thống bị đụng (crashes), hư thiết bị.

+ Đối với động cơ điện, tần số thay đổi liên tục có thể làm động cơ hoạt động không ổn định, hư hỏng trực tiếp và có nguy cơ gây ra cháy nổ.

Trượt tần

- Xảy ra tức thời gây ra điện áp thấp, trong khoảng rất ngắn nano giây.
- Sự cố có thể làm các thiết bị nhạy cảm với nguồn điện như hệ thống Server hoạt động không ổn định, nếu thường xuyên hơn có thể làm hệ thống Restart.

Méo hài

- Dạng sóng của nguồn điện bị méo dạng, không còn dạng hình sine chuẩn.
- Thông thường gây ra do đóng ngắt các tải phi tuyến tính. Sự cố có làm giảm hiệu suất thiết bị điện như động cơ, các máy biến áp…

Nhiễu trên đường dây

- Nhiễu tạp trên đường dây điện, các tần số cao xuất hiện trong nguồn điện gây ra bởi các bộ EMI, các nguồn phát ra sóng hài như biến thế, mô-tơ điện, thiết bị HVAC (hệ thống điện lạnh, thông gió) vận hành …
- Sinh ra nhiệt cao gây hư hỏng thiết bị, hỏa hoạn và nguy cơ cháy nổ, âm thầm diễn biến trong nhiều năm mà rất khó bị phát hiện.
- Ngoài ra, nhiễu trên đường dây làm giảm chất lượng nguồn điện, ảnh hưởng nhiều đến những thiết bị cần nguồn điện chuẩn và chất lượng cao, ví dụ như những hệ thống High End (hệ thống âm thanh chất lượng cao) cần nguồn điện cực chuẩn và sạch để nuôi linh kiện và khuyếch đại công suất. Nếu những thiết bị High End được cấp nguồn từ 1 nguồn điện không sạch, nhiều nhiễu và hài có thể làm suy giảm chất lượng linh kiện trên bo mạch, dẫn đến âm thanh xử lý sẽ không còn được chính xác như trước.

2.5 Sự cố phần cứng vô tuyến

Sóng vô tuyến

- Là một kiểu bức xạ điện từ với bước sóng trong phổ điện từ dài hơn ánh sáng hồng ngoại. Sóng vô tuyến có tần số từ 3 kHz tới 300 GHz, tương ứng bước sóng từ 100 km tới 1 mm. Giống như các sóng điện từ khác, chúng truyền với vận tốc ánh sáng. Sóng vô tuyến xuất hiện tự nhiên do sét, hoặc bởi các đối tượng thiên văn. Sóng vô tuyến do con người tạo nên dùng cho radar, phát thanh, liên lạc vô tuyến di động và cố định và các hệ thống dẫn đường khác. Thông tin vệ tinh, các mạng máy tính và vô số các ứng dụng khác. Các tần số khác nhau của sóng vô tuyến có đặc tính truyền lan khác nhau trong khí quyển Trái Đất; sóng dài truyền theo đường cong của Trái Đất, sóng ngắn nhờ phản xạ từ tầng điện ly nên có thể truyền rất xa, các bước sóng ngắn hơn bị phản xạ yếu hơn và truyền trên đường nhìn thẳng.

Nguyên nhân gây ra sự cố kỹ thuật đối với sóng vô tuyến bao gồm: các nguyên nhân khách quan và các nguyên nhân chủ quan. Ta cần biết rõ các nguyên nhân này để phòng tránh, hạn chế tối đa các sự cố xảy ra.

Nguyên nhân khách quan

Sự cố gây ra do thiên tai: Chúng ta đều biết thiên tai có ảnh hưởng rất lớn không chỉ đới với vô tuyến mà đối với tất cả các loại thông tin liên lạc khác. Thường xảy ra là bão lớn làm đổ cột, lệch hướng phát sóng, mưa lớn gây tổn hao sóng điện từ, gây ẩm ướt các đầu nối cao tần và thiết bị ngoài trời, thậm chí ngập ướt thiệt bị, dông sét đánh trực tiếp hoặc cảm ứng cũng gây thiệt hại rất nặng nề cho thiết bị, đặc biệt là đối với các thiết bị vô tuyến.

Nói chung sự cố thiên tai là bất khả kháng, tuy nhiên nếu ta tích cực chủ động có biện pháp phòng ngừa thì sẽ hạn chế được đáng kế ảnh hưởng của nó.

Sự cố gây ra do lỗi kỹ thuật của thiết bị

Thông thường khi thiết kế chế tạo một sản phẩm, nhà sản xuất đã tính toán rất kỹ để thiết bị có thể hoạt động ổn định đảm bảo theo đúng tính năng kỹ thuật trong thời gian tuổi thọ của nó, nhưng không tránh khỏi có sản phẩm bị lỗi mà chỉ sau một thời gian sử dụng mới được phát hiện ra. Lỗi có thể xảy ra thuộc cả phần cứng lẫn phần mềm của thiết bị và thường do chất lượng của linh kiện lắp ráp không đồng đều hoặc do quá trình lão hóa tự nhiên của vật liệu.

Các sự cố do lỗi tự nhiên của thiết bị là sự cố bất khả kháng cần phải dự phòng để thay thế kịp thời và bảo hành lấy thiết bị mới để sử dụng.

Sự cố gây ra do môi trường tự nhiên

Môi trường tự nhiên có thể kể đến là nhiệt độ, độ ẩm ảnh hưởng đến thiết bị, hoặc địa hình địa vật, môi trường truyền sóng ảnh hưởng đến chất lượng truyền sóng vô tuyến. Ngoài ra còn phải kể đến bụi bẩn và côn trùng cũng gây tác hại không nhỏ đến chất lượng khai thác thiết bị. Chúng ta có thể hạn chế được một phần lớn các ảnh hưởng của môi trường tự nhiên bằng công tác bảo quản bảo dưỡng và tổ chức khai thác thiết bị một cách hợp lý.

Nguyên nhân chủ quan

- Sự cố do sai sót kỹ thuật trong khảo sát, thiết kế trạm, tuyến

+ Sai sót kỹ thuật ở đây thuộc về các khâu khảo sát, thiết kế, hoạch định trạm tuyến. Đó là sự thiếu tỷ mỷ chính xác trong khảo sát, thiết kế tuyến, thiết kế nhà trạm, cơ sở hạ tầng, hệ thống nguồn điện, đặc điểm thời tiết khí hậu từng vùng, mạng cáp và hệ thống an toàn… Ngoài ra còn phải kể đến tính hợp lý trong để không vượt quá tính năng kỹ thuật của thiees bị. Chẳng hạn như cự ly đường cáp tối đa từ các bộ ghép kênh đến thuê bao xa là bao nhiêu thì đảm bảo. Đồng thời sai sót kỹ thuật còn có thể xảy ra ngay trong quá trình thử tuyến khi chưa lường hết được những biến động của thời tiết, địa hình, địa vật, nhất là đối với các tuyến triển khai dã chiến.

- Sự cố do sai sót trong quá trình lắp đặt trạm tuyến

+ Trước tiên phải kể đến nhứng sai sót kỹ thuật trong lắp đặt các cấu kiện ngoài trời và trên cột ăng ten lắp không đạt yêu cầu kỹ thuật, đương cáp bị gấp khúc, xoắn, gẫy, không chống thấm nước, không đấu tiếp đất cho các thiết bị.

+ Những sai sót dễ gặp khi lắp đặt thiết bị trong phòng máy bao gồm: chọn vị trí lắp máy sai, như quá gần cửa sổ dễ bị mưa hắt, hoặc ngay ở nơi cửa gió của máy lạnh dễ bị đọng nước; sai sót thường gặp khác là việc đấu đất cho các thiết bị không đúng, dây tiếp đất vòng vèo qua nhiều thiết bị, không đấu trực tiếp vào bảng nối đất; lắp đặt các thiết bị chống sét không đảm bảo yêu cầu kỹ thuật, đấu nối các đường tín hiệu không

đảm bảo tiếp xúc tốt.

+ Ngoài ra còn có các sai sót trong việc đấu nối sử dụng nguồn điện trong trạm, hay bố trí sử dụng tần số không hợp lý, chưa thực hiện đo đạc các chỉ tiêu kỹ thuật khi thông tuyến và so sánh với thiết kế để kịp thời phát hiện và khắc phục triệt để sự cố trước khi quyết định đưa vào sử dụng.

- Sự cố do sử dụng nguồn điện không đúng yêu cầu kỹ thuật

+ Điển hình là việc sử dụng nguồn điện AC tù các tổ máy phát điện không đảm bảo điện áp, tần số, độ méo cho các thiết bị nguồn SWITCHING, UPS, có trạm đã cháy một lúc 2 bộ nguồn do sử dụng nguồn chất lượng thấp. Các thao tác cấp nguồn vaax còn sai sót như khi trạm mất điện vào giờ cao điểm ổn áp đang ở chế độ tăng áp, nếu không ngắt điện từ ổn áp vào thiết bị thì khi có điện trở lại vào giờ thấp điểm đầu ra ổn áp điện áp sẽ tăng vọt và phải có một thời gian trễ thì điện áp mới trở lại mức danh định, trong thời gian trễ đó thiết bị của chúng ta đã bị hỏng; hay như điện áp và tần số máy nổ chưa ổn định đã đóng cầu dao cấp điện cho thiết bị.

2.6 Kỹ thuật và xử lý sự cố

Bước 1: Nhận diện vào sự cố

Thông thường bạn không nhận diện được ra vấn đề, không thể tìm hướng giải quyết sự cố để nhận biết được tình trạng máy tính xẩy ra sự cố. Bạn hỏi ngay người dùng máy tính trước lúc xẩy ra sự cố có làm các bước sau không:

- Máy tính xảy ra hiện tượng gì, như thế nào
- Máy có thường xuyên xảy ra tình trạng thế không
- Máy có cài đặt phần mềm nào mới không

Bước 2: Kiểm tra hệ thống

Trước khi tiến hành cần kiểm tra hệ thống máy, các phụ kiện lắp đặt trong Case, các kết nối như Card màn hình, bàn phím, chuột (Keyboard) vv… màn hình các phụ kiện khác. Các vấn đề về sự cố có khả năng xảy ra sự cố từ các thiết bị.

Sau khi kiểm tra các thiết bị hệ thống vẫn hoạt động bình thường mà vẫn chưa xử lý được chuyển sang bước tiếp theo.

Bước 3: Tìm các tác nhân gây nên sự cố

Các nguyên nhân sự cố máy tính, hỏi chính những người sử dụng máy tính đó cung cấp thông tin về sự chính xác làm những gì trước khi sự cố xảy ra để từ đó suy đoán được lại những sự việc trước đó để tìm nguyên nhân.

- Khởi động lại máy tính bước này là quan trọng để xác định được phần nào máy tính của bạn để tập trung vào tìm kiếm và giải quyết các phần cần có những kỹ năng, kỹ thuật và những công cụ giải quyết khác nhau.
- Bước tiếp theo này chủ yếu tìm hiểu nguyên nhân dựa vào kinh nghiệm của từng cá nhân kỹ thuật viên.

Bước 4: Thiết lập

Kiểm tra các thiết lập về phần cứng trong CMOS và trong bộ quản lý thiết lập hệ thống, tạo các trình điều khiển thiết bị và cập nhật tất cả card cắm trên máy tính.

Bước 5: Các thay đổi

Khi thấy lỗi một phần cứng hay phần mềm trên máy tính, hãy xác định điều gì đã thay đổi trước khi vấn đề xảy ra.

Bước 6: **Sự cố là môi trường học tập hữu ích**

Có thể học được rất nhiều khi đối phó với đủ loại lỗi. Hãy ghi lại tất cả các cảnh báo lỗi và phương pháp khắc phục, qua đó bạn sẽ có một cuốn sổ chỉ dẫn các phát hiện và xử lý lỗi máy tính.

Bước 7: **Nếu không giải quyết được vấn đề**

Sau khi xác định nguyên nhân mà bạn không giải quyết được vấn đề, đặt máy tính về tình trạng ban đầu rồi mới tiếp tục giải quyết theo những hướng khác.

Bước 8: Yêu cầu trợ giúp

Mọi điều hiển nhiên trong chúng ta không ai có thể giải quyết được mọi sự cố, những sự cố phát sinh mới chưa từng gặp và không thể tìm ra nguyên nhân.

Khi đó cần tìm đến sự giúp đỡ từ đồng nghiệp…

Chú ý: các bước trên chỉ là để thảm khảo và vận dụng một cách linh hoạt trong công tác chuẩn đoán, không nhất thiết phải theo đứng thứ tự. Vì các sự cố xảy ra rất đa dạng và phức tạp người kỹ thuật có rất nhiều phương hướng để giải quyết.

Trên đây là những bước mang tính chất để tham khảo khắc phục và chuẩn đoán sự cố, tùy vào những kinh nghiệm xử lý của từng kỹ thuật viên.

Câu hỏi ôn tập

Câu 1: Hãy nêu các sự cố card mạng và cách giải quyết.

Câu 2: Hãy nêu các sự cố Ethernet và cách giải quyết.

Câu 3: Hãy nêu sự cố không kết nối được với nhà cung cấp dịch vụ, sự cố điện và cách giải quyết.

Câu 4: Hãy nêu các kỹ thuật xử lý sự cố.

BÀI 2. PHẦN MỀM

Giới thiệu:

Phần mềm máy tính, hay đơn giản là **phần mềm**, được người Việt hải ngoại gọi là **nhu liệu** là tập hợp dữ liệu hoặc hướng dẫn máy tính cho máy tính biết cách làm việc. Điều này trái ngược với phần cứng vật lý, từ đó hệ thống được xây dựng và thực sự thực hiện công việc. Trong khoa học máy tính và kỹ thuật phần mềm, phần mềm máy tính là tất cả thông tin được xử lý bởi hệ thống máy tính, chương trình và dữ liệu. Phần mềm máy tính bao gồm các chương trình máy tính, thư viện và dữ liệu không thể thực thi liên quan, chẳng hạn như tài liệu trực tuyến hoặc phương tiện kỹ thuật số. Phần cứng và phần mềm máy tính yêu cầu lẫn nhau và không thể tự sử dụng một cách thực tế.

1. Mục tiêu:

- Xác định được các lỗi do phần mềm gây ra cho hệ thống
- Định lại được các cấu hình phần mềm cho thiết bị.

2. Nội dung bài học

2.1 Định cấu hình card mạng

Bộ điều hợp mạng là thiết bị phần cứng dùng để kết nối những máy tính hoặc các thiết bị khác với mạng. Bộ điều hợp mạng chịu trách nhiệm cung cấp kết nối với mạng và địa chỉ vật lý của máy tính. Bộ điều hợp mạng (hoặc các thiết bị phần cứng khác) cần một bộ điều khiển (driver) để liên lạc với hệ điều hành Windows. Các driver thường có trong đĩa CD cài card mạng hoặc được cung cấp bởi Windows. Bạn phải chuẩn bị sẵn đĩa CD cài đặt driver, và có khả năng lắp ráp một số thiết bị phần cứng vào Bo mạch máy tính cũng như biết cách cấu hình CMOS và quản lý thiết bị đi kèm trong Motherboard.

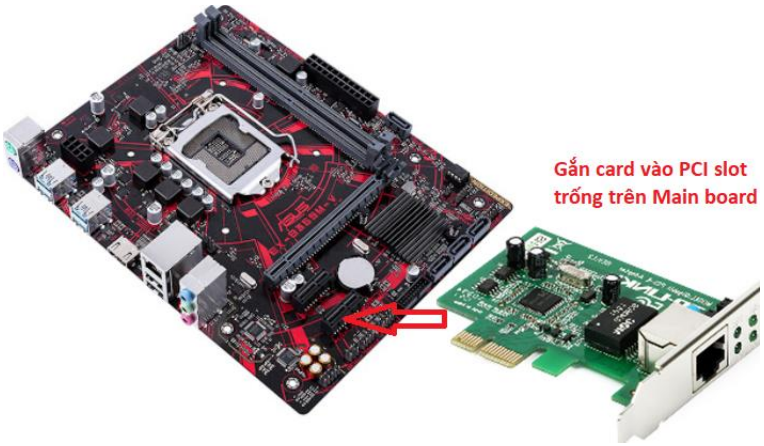
Tiến hành cài

Trước khi cài bộ điều hợp mạng, điều quan trọng là đọc các hướng dẫn đi cùng với thiết bị. Nếu bộ điều hợp mạng còn mới, nó đã tự cấu hình, với khả năng Plug and Play.

Sau khi bạn cài bộ điều hợp mạng có hỗ trợ Plug and Play, nó sẽ hoạt động khi bạn khởi động máy lần kế tiếp.

Các bước gắn NIC vào PC: Chỉ dùng cho Motherboard không có Network Adapter.

- Tắt máy.
- Mở thùng CPU
- Trên MainBoard, tìm một Slot PCI còn trống và gắn NIC vào theo hình minh họa.



Hình 2.1. Nơi gắn Card mạng trên Main

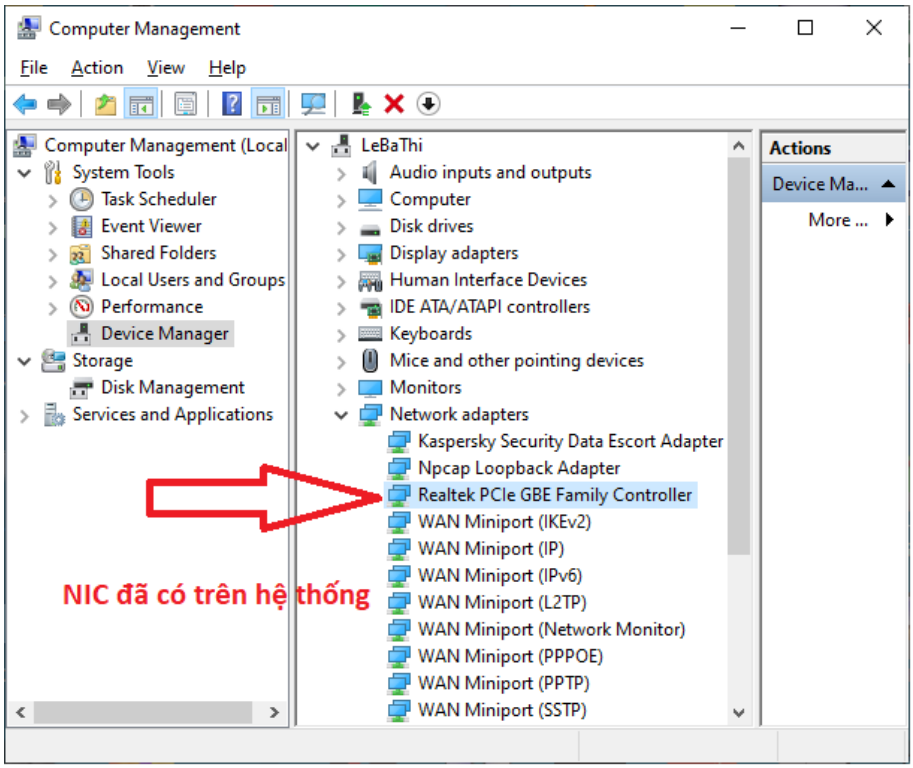
Sau khi gắn vào, bạn khởi động hệ thống và Windows sẽ chạy chương trình New HardWare Wizard (Hoặc Plug and Play) để cài Driver cho Card này. Bạn tiến hành đưa đĩa CD vào và theo các bước cho đến khi công việc cài Driver hoàn tất.

Lưu ý: Những thiết bị mới sẽ tự động tìm các thiết định và tự cấu hình. Các thiết bị cũ dựa vào chương trình cài đặt phần cứng để cấu hình. Những thiết bị thật cũ kỷ đòi hỏi bạn phải tự cấu hình bằng tay bằng thong qua switches (khóa chuyển) hoặc jumpers (cầu nối ngắt).

Khi bộ điều hợp mạng không có khả năng Plug and Play, hệ điều hành sẽ dò tìm thiết bị phần cứng mới và sẽ khởi động chương trình New Hardware Wizard và sẽ hướng bạn qua từng bước tìm và tải driver cho bộ điều hợp.

Nếu MainBoard của bạn có kèm Built-n Ethernet adapter thì bạn phải kích hoạt (Enable) nó trong CMOS bằng cách chọn LAN Deivice Enabled, sau đó bạn phải dùng dĩa cài đặt Mainboard để cài Driver cho LAN Port này.

Kiểm tra NIC đã được cài hay chưa?



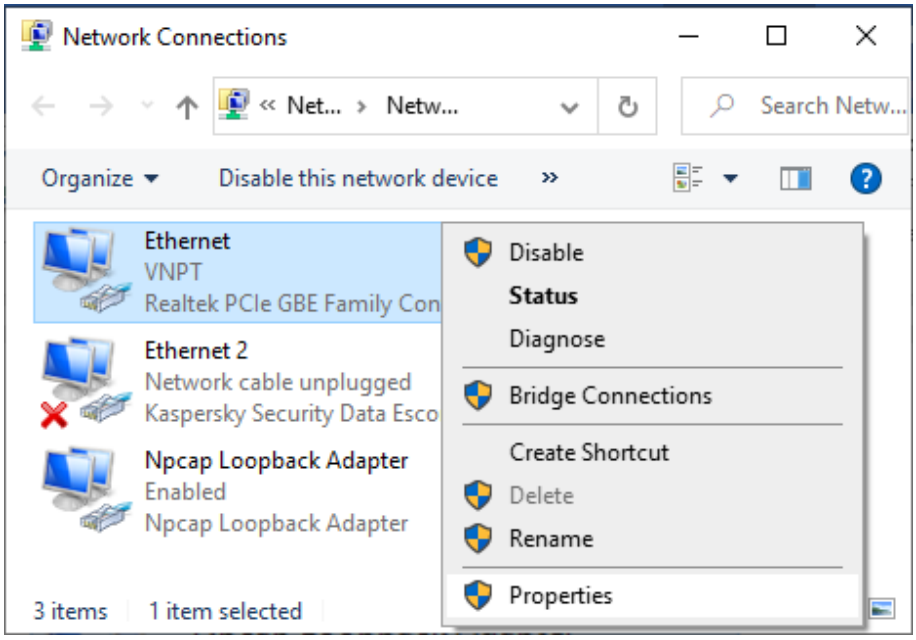
Hình 2.2. Kiểm tra card mạng

Lưu ý rằng chúng ta dùng cách xem Classic View trong Control Panel cho các bài thực hành.

Khi bộ điều hợp mạng đã được cài đặt, bạn có thể cấu hình cho nó thông qua hộp thoại Properties. Để truy cập hộp thoại này, có nhiều cách, một trong các cách là sử dụng Device Manager.

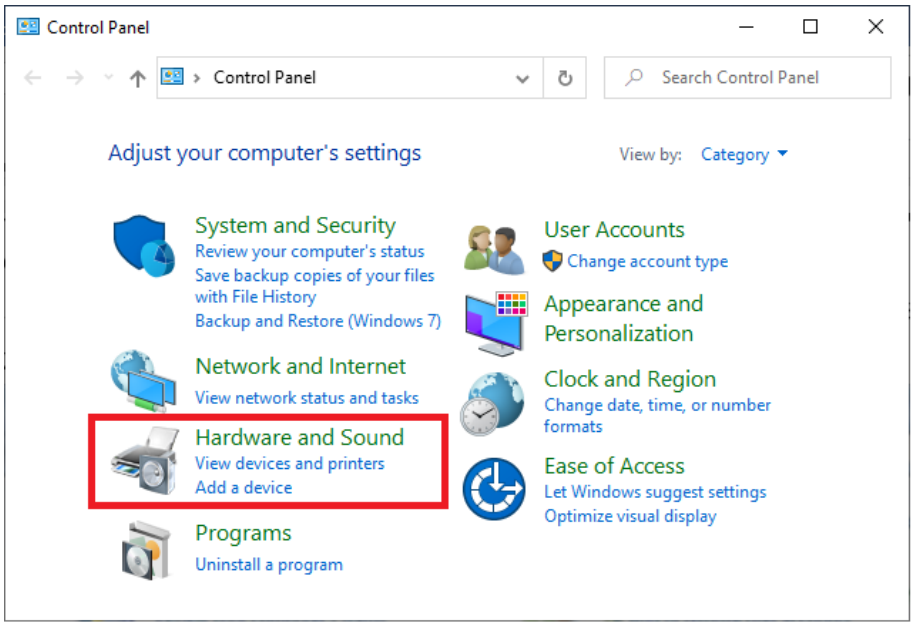
Click Start/Control Panel/ chọn Swicth to Classic View/ Chọn System/ Click chọn Tab Hardware/ Click chọn Device Manager/ Click Network Adapter. Cửa sổ Device Manager mở ra như bên dưới: Tùy vào Model của NIC bạn mua mà tên của NIC có thể khác so với hình trên nhưng cơ bản bạn không thấy có báo lỗi với dấu chấm than màu vàng.

Một cách khác để kiểm tra xem NIC hoạt động đúng không, bạn Click Start/Control Panel/ Network Connections. Trong cửa sổ Network Connection mới mở như hình dưới:



Hình 2.3 Kiểm tra NIC bằng Network Connection

Trường hợp card mạng của bạn đã gắn vào máy tính nhưng không xuất hiện trong danh sách, bạn phải thêm nó vào hệ thống bằng cách chọn menu ***Start – Control Panel***. Trong phần ***Hardware and Sound***, bạn chọn mục ***Add a device***, rồi thực hiện các bước chọn lựa theo yêu cầu.



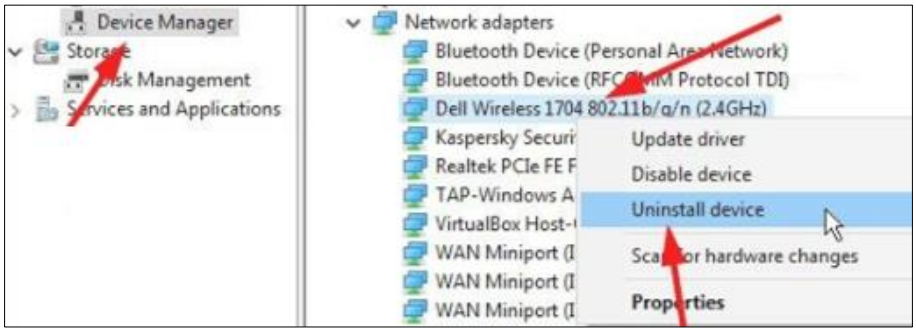
Hình 2.4 Cài đặt Device

Nếu ở bước trên, mà hệ thống không phát hiện phần cứng nào thuộc nhóm thiết bị mạng, thì rất có thể card mạng của bạn đã bị lỏng ra khỏi khe cắm, hoặc nó bị hư. Bạn hãy giải quyết bằng cách tháo card mạng ra khỏi khe cắm PCI, và dùng một cục tẩy để làm sạch các chân đồng trên card. Bạn cũng cần dùng bình xịt khí nén để làm sạch khe cắm. Sau đó bạn hãy cắm card mạng trở vào khe thật chắn chắn, sao cho card mạng nằm vuông góc với bo mạch chủ. Bạn cũng đừng quên xiết con ốc vặn để cố định card mạng vào thùng máy.

Lưu ý rằng trước khi mở thùng máy ra để làm vệ sinh theo các bước trên, bạn nhớ tắt máy tính, rút cáp nguồn, và rút dây mạng ra khỏi card mạng. Sau đó, bạn sẽ thấy card mạng sẽ xuất hiện trong danh sách của ***Device Manager***, nhưng có dấu hiệu hình tam giác màu vàng có dấu chấm than phía trước. Dấu hiệu đó cảnh báo cho bạn biết phần cứng này chưa thể hoạt động trong hệ thống. Để giải quyết, bạn bấm phải chuột trên card mạng bị lỗi, rồi chọn mục ***Uninstall***. Sau đó bạn tiến hành khởi động lại Windows để hệ thống tự động phát hiện lại và cập nhật phần mềm điều khiển.

Có cách khác để sửa lỗi này là bạn bấm phải chuột trên card mạng bị lỗi, và chọn mục ***Update Driver Software,*** rồi chọn chức năng dò tìm tự động ***Search automatically***.

Nếu quá trình dò tìm tự động không thể phát hiện ra được phần mềm điều khiển thiết bị phù hợp với card mạng hiện tại trong bộ cài đặt gốc của mình hay tải xuống từ internet, bạn sẽ cần phải chỉ ra nơi chứa trình điều khiển thiết bị thường là CD đính kèm khi mua.



Hình 2.5. Gỡ bỏ card mạng cũ

2.2 Định cấu hình bộ định tuyến

Router là một thiết bị liên mạng ở tầng 3, cho phép nối hai hay nhiều nhánh mạng lại với nhau để tạo thành một liên mạng. Nhiệm vụ của router là chuyển tiếp các gói tin từ mạng này đến mạng kia để có thể đến được máy nhận. Mỗi một router thường tham gia vào ít nhất là 2 mạng. Nó có thể là một thiết bị chuyên dùng với hình dáng giống như Hub hay switch hoặc có thể là một máy tính với nhiều card mạng và một phần mềm cài đặt giải thuật chọn đường. Các đầu nối kết (cổng) của các router được gọi là các Giao diện (Interface).

Các máy tính trong mạng diện rộng được gọi là các Hệ thống cuối (End System), với ý nghĩa đây chính là nơi xuất phát của thông tin lưu thông trên mạng, cũng như là điểm dừng của thông tin. Về mặt kiến trúc, các router chỉ cài đặt các thành phần thực hiện các chức năng từ tầng 1 đến tầng 3 trong mô hình OSI. Trong khi các End System thì cài đặt chức năng của cả bảy tầng...

2.2.1. Giới thiệu

Có một vài phương pháp có thể cấu hình các router. Có thể được thực hiện trên mạng từ một máy chủ TFTP, có thể thực hiện thông qua giao diện menu được cung cấp khi khởi động hay có thể được thực hiện từ giao diện menu được cung cấp bởi sử dụng lệnh setup. Tuy nhiên hướng dẫn trong bài sẽ không giới thiệu các phương pháp này. Nó chỉ giới thiệu việc cấu hình từ giao diện dòng lệnh IOS. Tuy nhiên hướng dẫn sẽ rất hữu dụng đối với bất cứ ai còn lạ lẫm với các router của IOS và những người nghiên cứu CCNA.

Lý do cho việc sử dụng dòng lệnh Lý do chính cho việc sử dụng giao diện dòng lệnh thay vì một giao diện điều khiển thông qua menu cho phép thực hiện nhanh hơn là khi bạn

đầu tư thời gian vào việc nghiên cứu các lệnh, bạn có thể thực hiện nhiều hoạt động nhanh hơn nhiều so với việc sử dụng menu. Điều này tạo ra lợi thế của việc sử dụng dòng lệnh so với các giao diện menu. Còn có những điều làm cho nó trở lên đặc biệt hiệu quả khi nghiên cứu giao diện dòng lệnh của Cisco IOS rằng nó là một chuẩn cho tất cả các router của Cisco. Thêm vào đó nữa là một số câu hỏi trong bài kiểm tra về CCNA yêu cầu bạn biết về các lệnh này.

2.2.2. Bắt đầu với Router Cisco

Bắt đầu bạn có thể cấu hình router của mình từ một thiết bị đầu cuối. Nếu router đã được cấu hình và có tối thiểu một cổng được cấu hình với một địa chỉ IP nào đó thì nó sẽ có một kết nối vật lý với mạng, từ đó bạn có thể telnet đến router và cấu hình nó trên mạng. Nếu nó chưa được cấu hình thì bạn cần phải kết nối trực tiếp router với một thiết bị đầu cuối và cáp nối tiếp. Với các máy tính Windows, bạn có thể sử dụng Hyperterminal để kết nối một cách dễ dàng đến router. Cắm cáp nối tiếp vào cổng COM trên máy tính và đầu còn lại cắm vào cổng trên router. Khởi chạy Hyperterminal, chuyển tới cổng COM mà bạn sử dụng và kích OK. Thiết lập tốc độ kết nối là 9600 baud và kích OK. Nếu router chưa được bật nguồn, hãy bật nguồn cấp cho nó. Nếu bạn muốn cấu hình router từ máy tính *Linux*, cần phải có Seyon hoặc Minicom, thì tối thiểu một trong số chúng, có thể là cả hai sẽ đi kèm bản phân phối Linux của bạn.

Thông thường bạn cần phải nhất phím Enter để thấy được nhắc nhở từ phía router. Nếu nó chưa được cấu hình thì những gì bạn thấy sẽ như dưới đây:

Router>

Nếu nó đã được cấu hình từ trước với một hostname, khi đó bạn sẽ thấy:

Hostname of router>

Nếu bạn vừa mới bật router, sau khi khởi động nó sẽ yêu cầu bạn xem có muốn bắt đầu cấu hình từ đầu hay không. Hãy từ chối trả lời. Nếu bạn đồng ý thì nó sẽ đưa bạn đến giao diện menu. Chính vì vậy hãy chọn nó.

- **Các chế độ**

Giao diện dòng lệnh của Cisco IOS được tổ chức theo ý tưởng các chế độ (***mode***). Bạn chuyển vào và ra một vài chế độ khác nhau trong khi cấu hình router, chế độ nào bạn nằm trong đó sẽ quyết định những lệnh nào bạn có thể sử dụng. Mỗi một chế độ có một tập các lệnh hiện hữu cho nó, một số các lệnh chỉ có sẵn trong chế độ nào đó. Trong bất cứ chế độ nào, việc đánh một dấu hỏi chấm sẽ hiển thị một danh sách các lệnh hiện hữu trong chế độ đó.

Router>?

- **Các chế độ đặc quyền và không đặc quyền**

Khi bạn lần đầu tiên kết nối đến router và cung cấp mật khẩu (nếu cần thiết), bạn sẽ vào chế độ EXEC, chế độ đầu tiên mà bạn có thể sử dụng các lệnh từ dòng lệnh. Từ đây, bạn có thể sử dụng các lệnh không đặc quyền như ping, telnet, and rlogin. Có thể sử dụng lệnh show để thu về các thông tin hệ thống. Trong chế độ đặc quyền, bạn có thể sử dụng lệnh show version để hiển thị phiên bản của IOS mà router đang chạy. Đánh show ? sẽ hiển thị tất cả các lệnh show hiện hữu trong chế độ mà bạn đang hiện diện.

Router>show ?

Bạn phải vào chế độ đặc quyền để cấu hình cho router của mình. Thực hiện điều đó bằng cách sử dụng lệnh enable. Chế độ đặc quyền thường được bảo vệ mật khẩu trừ khi router chưa được cấu hình. Bạn có thể chọn chế độ đặc quyền không bảo vệ mật khẩu tuy nhiên tất cả đều nên đặt mật khẩu để an toàn. Khi phát lệnh enable và cung cấp mật khẩu, bạn sẽ vào chế độ đặc quyền. Để giúp người dùng theo dõi được chế độ nào họ đang ở trong, nhắc lệnh của dòng lệnh sẽ thay đổi mỗi khi bạn vào một chế độ khác. Khi bạn chuyển từ chế độ không đặc quyền sang chế độ đặc quyền, nhắc nhở sẽ thay đổi từ:

Router> Thành ***Router#***

Điều này sẽ không cần thiết nếu chỉ có hai chế độ. Tuy nhiên trong thực tế, với nhiều chế độ nên tính năng này rất cần thiết. Bạn cũng cần chú ý đến nhắc nhở mọi lúc. Bên trong chế độ đặc quyền lại có nhiều chế độ nhỏ. Khi bạn vào chế độ đặc quyền (hay có thể gọi là chế độ cha - parent), nhắc nhở sẽ kết thúc bằng dấu (#). Có nhiều chế độ mà bạn chỉ có thể vào sau khi vào được chế độ đặc quyền. Mỗi một trong các chế độ này đều có nhắc nhở như mẫu dưới đây:

Router(arguments)#

Chúng vẫn kết thúc bằng dấu (#) và được gộp vào trong chế độ đặc quyền. Nhiều chế độ có các chế độ con trong bản thân nó. Khi ban vào chế độ đặc quyền, bạn có thể truy cập vào tất cả các thông tin cấu hình cũng như các tùy chọn mà IOS cung cấp, trực tiếp từ chế độ cha hay từ một trong các chế độ con của nó.

2.2.3. Cấu hình router Cisco

Nếu bạn vừa mới bật router, nó sẽ hoàn toàn chưa được cấu hình. Nếu nó đã được cấu hình, bạn có thể xem được cấu hình hiện hành của nó. Thậm chí nếu nó chưa được cấu hình từ trước thì bạn cũng có thể tự khai thác bằng lệnh show trước khi bắt đầu cấu hình router. Vào chế độ đặc quyền bằng cách phát lệnh enable, sau đó phát một vài lệnh show để xem những gì chúng hiển thị. Nhớ rằng, lệnh show ? sẽ hiển thị tất cả các lệnh show hiện hữu trong chế độ hiện hành. Hãy thử với các lệnh dưới đây:

Router#show interfaces

Router#show ip protocols

Router#show ip route

Router#show ip arp

Khi vào chế độ đặc quyền bằng cách sử dụng lệnh enable, khi đó bạn sẽ nằm trong chế độ top-level của chế độ đặc quyền, được biết trong tài liệu này là “chế độ cha – parent”. Nó là chế độ mà bạn có thể hiển thị hầu hết các thông tin về router. Như những gì bạn biết, bạn có thể thực hiện điều đó với các lệnh show. Ở đây bạn có thể biết được về cấu hình của giao diện. Có thể hiển thị các giao thức IP đang được sử dụng là gì, chẳng hạn như các giao thức định tuyến động. Bạn có thể xem tuyến và bản định tuyến ARP và một số các tùy chọn quan trọng khác. Khi cấu hình router, bạn sẽ vào trong một số chế độ con để thiết lập các tùy chọn, sau đó trở về chế độ cha để hiển thị các kết quả. Bạn cũng trở về chế độ cha để vào các chế độ con khác. Để trở vè chế độ cha, bạn chỉ cần nhấn ctrl-z. Thao tác này sẽ làm các lệnh mà bạn vừa phát ra có hiệu lực và đưa bạn trở về chế độ cha.

Cấu hình toàn cục

Để cấu hình bất cứ tính năng nào của router, bạn phải vào chế độ cấu hình. Đây là chế độ con đầu tiên của chế độ cha. Trong chế độ cha, bạn phát lệnh config.

Router#config

Router(config)#

Như minh chứng ở trên, nhắc nhở sẽ thay đổi để chỉ thị răng bạn đang ở trong chế độ nào lúc này. Trong chế độ cấu hình, bạn có thể thiết lập các tùy chọn để sử dụng cho toàn hệ thống, được ám chỉ như là các cấu hình mang tính toàn cục. Cho ví dụ, đặt tên cho router để bạn có thể dễ dàng nhận ra nó. Bạn có thể thực hiện điều đó trong chế độ cấu hình với lệnh hostname.

Router(config)#hostname ExampleName

ExampleName(config)#

Như minh chứng ở trên, khi bạn thiết lập tên của host với lệnh hostname, nhắc nhở sẽ ngay lập tức thay đổi bằng cách thay thế Router thành ExampleName. (Lưu ý: nên đặt tên cho các router của bạn theo một lược đồ tên có tổ chức). Một lệnh hữu dụng khác được phát từ chế độ cấu hình là lệnh để chỉ định máy chủ DNS nhằm sử dụng cho router:

ExampleName(config)#ip name-server aa.bb.cc.dd

ExampleName(config)#ctrl-Z

ExampleName#

Đây cũng là nơi bạn thiết lập mật khẩu cho chế độ đặc quyền.

ExampleName(config)#enable secret examplepassword

ExampleName(config)#ctrl-Z

ExampleName#

Cho tới khi bạn nhấn ctrl-Z (hoặc đánh exit cho tới khi bạn vào được chế độ cha) lệnh của bạn mới không bị ảnh hưởng. Bạn có thể vào chế độ cấu hình, phát một vài lệnh khác nhau, sau đó nhấn ctrl-Z để kích hoạt chúng. Mỗi lần bạn nhấn ctrl-Z, bạn sẽ trở về chế độ cha và nhắc:

ExampleName#

Ở đây bạn sử dụng lệnh show để thẩm định các kết quả của các lệnh mà mình đã phát trong chế độ cấu hình. Để thẩm định các kết quả của lệnh ip nameserver, phát lệnh show host.

Cấu hình giao diện

Việc đặt tên giao diện Cisco rất đơn giản. Các giao diện riêng biệt được dẫn đến bởi thủ tục này: ***media type slot#/port#*** "Media type" là kiểu thiết bị có giao diện là cổng, chẳng hạn như Ethernet, Token Ring, FDDI, nối tiếp,… Số khe chỉ thích hợp với các router cung cấp số khe để bạn có thể cài đặt các modul. Các modul gồm có một vài cổng cho thiết bị đã cho. Serie 7200 là một ví dụ. Các modul này có thể thay nóng. Bạn có thể remove một modul nào đó ra khỏi khe của nó và thay thế nó bằng một modul khác mà không cần phải ngắt dịch vụ được cấp bởi các modul khác đã cài đặt trong router.

Các khe này được đánh số trên router. Số cổng dựa vào cổng tham chiếu với các cổng khác trong modul đó. Việc đánh số được tiến hành từ trái sang phải và tất cả đều bắt đầu từ số 0, không phải một chữ số.

Cho ví dụ, Cisco 7206 là router serie 7200 có 6 khe. Để ám chỉ cho một giao diện là

cổng thứ ba của một modul Ethernet đã được cài đặt trong khe thứ sáu, nó sẽ là giao diện 6/2. Chính vì vậy, để hiển thị cấu hình của giao diện, bạn cần sử dụng lệnh:

ExampleName#show interface ethernet 6/2

Nếu router của bạn không có các khe, giống như 1600, thì tên giao diện chỉ gồm có: ***media type port#***

Cho ví dụ:

ExampleName#show interface serial 0

Đây là một ví dụ về việc cấu hình một cổng nối tiếp với một địa chỉ IP:

ExampleName#config
ExampleName(config)#interface serial 1/1
ExampleName(config-if)#ip address 192.168.155.2 255.255.255.0
ExampleName(config-if)#no shutdown
ExampleName(config-if)#ctrl-Z
ExampleName#

Sau đó thẩm định cấu hình:

ExampleName#show interface serial 1/1

Lưu ý về lệnh no shutdown. Một giao diện có thể được cấu hình đúng và kết nối vật lý nhưng vẫn gặp phải vấn đề. Trong trạng thái này nó sẽ không hoạt động. Lệnh gây ra lỗi này là shutdown.

ExampleName(config)#interface serial 1/1
ExampleName(config-if)#shutdown
ExampleName(config-if)#ctrl-Z
ExampleName#show interface serial 1/1

Trong Cisco IOS, cách đảo hoặc xóa các kết quả cho bất cứ lệnh nào là đặt no vào đằng trước nó. Cho ví dụ, nếu bạn muốn hủy gán địa chỉ IP mà đã gán cho giao diện nối tiếp 1/1:

ExampleName(config)#interface serail 1/1
ExampleName(config-if)#no ip address 192.168.155.2 255.255.255.0
ExampleName(config-if)ctrl-Z
ExampleName#show interface serial 1/1

Việc cấu hình hầu hết các giao diện cho các kết nối LAN có thể chỉ gồm việc gán một địa chỉ lớp mạng và bảo đảm rằng giao diện không bị shutdown. Thường không cần thiết phải quy định sự gói gọn lớp liên kết dữ liệu. Lưu ý rằng thường cần phải quy định sự gói gọn lớp liên kết dữ liệu tương thích, chẳng hạn như frame-relay và ATM. Các giao diện nối tiếp mặc định phải sử dụng HDLC. Tuy nhiên việc thảo luận sâu về các giao thức liên kết dữ liệu lại nằm ngoài phạm vi của tài liệu này. Bạn sẽ cần phải tra cứu lệnh IOS encapsulation để có thêm thông tin chi tiết**.**

Cấu hình và định tuyến

Việc định tuyến IP được kích hoạt một cách hoàn toàn tự động trên các router Cisco. Nếu nó đã bị vô hiệu hóa từ trước trên router của bạn thì bạn có thể kích hoạt nó trở lại trong chế độ cấu hình bằng lệnh ip routing.

ExampleName(config)#ip routing

ExampleName(config)#ctrl-Z

Có hai cách chính một router biết được nơi nó gửi các gói. Quản trị viên có thể gán các tuyến tĩnh ***static routes***hoặc router có thể biết về các tuyến bằng cách sử dụng giao thức định tuyến động ***dynamic routing protocol.***

Ngày nay, phương pháp định tuyến tĩnh nhìn chung thường được sử dụng trong các mạng rất đơn giản hoặc trong những trường hợp mà ở đó bắt buộc cần phải sử dụng đến chúng. Để tạo một tuyến tĩnh, quản trị viên chỉ cần lệnh cho hệ điều hành để bất cứ lưu lượng mạng nào được dự trù cho địa chỉ lớp mạng cụ thể nào đó cần phải được chuyển tiếp đến một địa chỉ lớp mạng cụ thể như vậy. Trong Cisco IOS, điều này được thực hiện với lệnh ip route.

ExampleName#config
ExampleName(config)#ip route 172.16.0.0 255.255.255.0 192.168.150.1
ExampleName(config)#ctrl-Z
ExampleName#show ip route

Có hai thứ cần phải nói trong ví dụ này. Đầu tiên đó là địa chỉ đích phải chứa subnet mask cho mạng đích đó. Thứ hai, địa chỉ nó gửi chuyển tiếp đến là địa chỉ được chỉ định của router tiếp theo cùng với đường dẫn đến đích. Đây là cách chung nhất cho việc thiết lập một tuyến tĩnh. Mặc dù vậy vẫn còn có một số phương pháp khác.

2.3 Định cấu hình và quản lý người dùng

Windows Group Policy là công cụ khá mạnh được sử dụng để cấu hình nhiều khía cạnh của Windows. Hầu hết việc tinh chỉnh Windows Group Policy chỉ có Admin mới có thể thực hiện được. Nếu bạn là Admin của nhiều máy tính khác trong công ty hoặc bạn có nhiều tài khoản khác trên máy tính của mình, khi đó bạn nên tận dụng lợi thế của Windows Group Policy để kiểm soát việc sử dụng máy tính của người dùng khác.

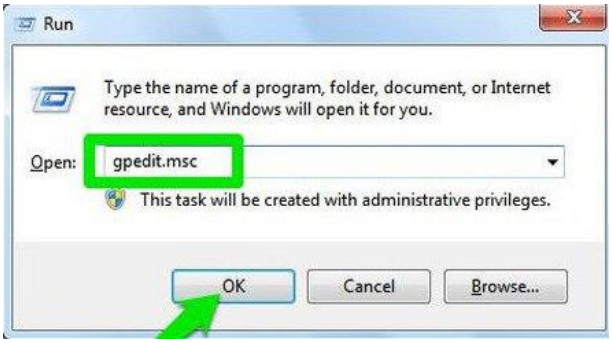
Lưu ý: Group Policy Editor không có sẵn trên phiên bản Home và phiên bản chuẩn của Windows. Bạn phải sử dụng phiên bản Professional hoặc Enterprise thì mới có thể sử dụng Group Policy.

Làm thế nào để truy cập Windows Group Policy Editor?

Mặc dù có nhiều cách để truy cập **Windows Group Policy Editor**, nhưng cách đơn giản nhất và nhanh nhất là sử dụng hộp thoại **Run** và cách này hoạt động tất cả phiên bản của Windows.

- Để truy cập Windows Group Policy Editor bạn thực hiện theo các bước dưới đây:

+ Nhấn tổ hợp phím **Windows + R** để mở cửa sổ lệnh Run, sau đó nhập "*gpedit.msc*" vào đó rồi nhấn **Enter** để mở Group Policy Editor.



Hình 2.7 truy cập Windows Group Policy Editor

Một lưu ý là bạn phải đăng nhập bằng tài khoản Admin trước khi truy cập Group Policy. Tài khoản chuẩn không cho phép truy cập Group Policy.

Những điều có thể làm với Group Policy

2.3.1. Theo dõi đăng nhập tài khoản

Trên Group Policy bạn có thể "buộc" Windows "**ghi lại" tất cả các đăng nhập thành công và thất bại** trên máy tính từ bất kỳ tài khoản người dùng nào. Bạn có thể sử dụng các thông tin này để theo dõi xem có người lạ nào đăng nhập trái phép máy tính Windows của bạn hay không.

Trên cửa sổ Group Policy Editor, bạn điều hướng theo đường dẫn dưới đây:

Computer Configuration => Windows Settings => Security Settings => Local Policies => Audit Policy

Sau đó tìm và kích đúp chuột vào **Audit logon events**.

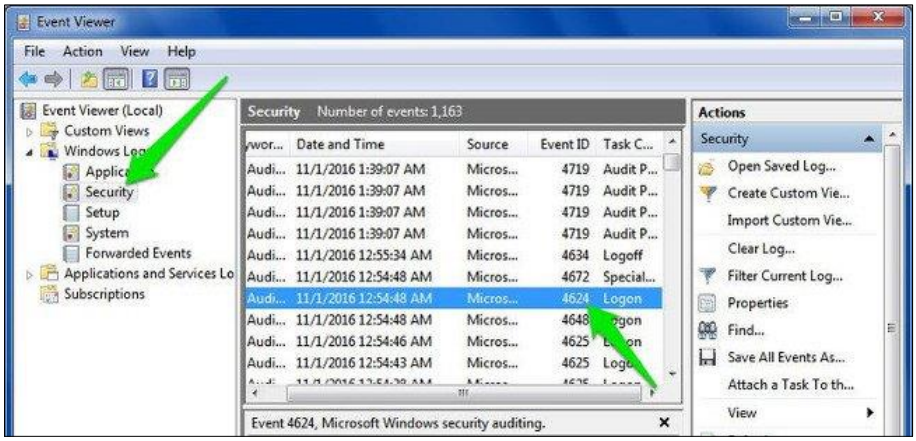
Lúc này trên màn hình xuất hiện hộp thoại Audit logon events Properties. Tại đây bạn đánh tích chọn **Success** và **Failure**, sau đó click chọn **OK** và Windows sẽ bắt đầu "ghi lại" các đăng nhập được thực hiện trên máy tính của bạn.

Hình 2.8 Định cấu hình và quản lý người dùng

Để xem các đăng nhập này bạn phải truy cập công cụ hữu ích khác của Windows - **Windows Event Viewer**. Để mở Windows Event Viewer, đầu tiên bạn nhấn tổ hợp phím **Windows + R** để mở cửa sổ lệnh Run, sau đó nhập **eventvwr** vào đó rồi nhấn Enter.

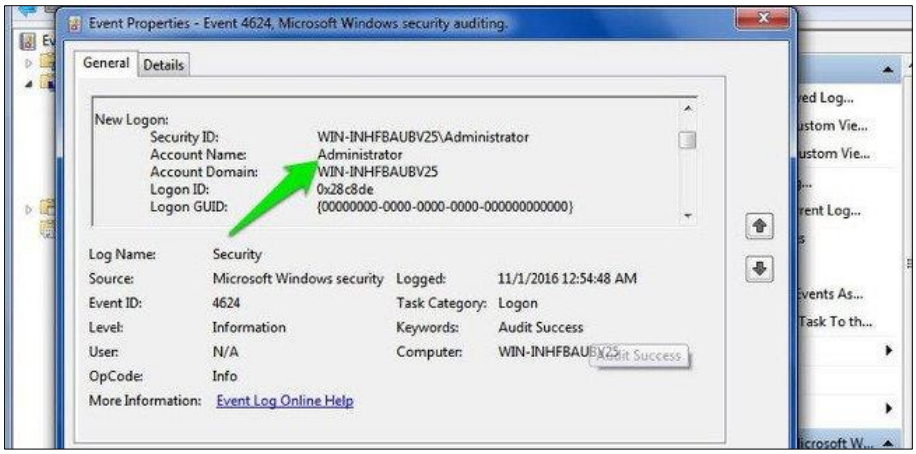
Tại đây bạn mở rộng mục **Windows Logs**, sau đó chọn tùy chọn **Security**. Tại khung ở giữa bạn sẽ nhìn thấy tất cả các sự kiện gần đây, nhiệm vụ của bạn là chỉ cần tìm các sự kiện đăng nhập thành công và thất bị tại danh sách này.

Các sự kiện đăng nhập thành công có *"Event ID: 4624*" và đăng nhập thất bại là "*Event ID: 4625*". Chỉ cần tìm các ID sự kiện để tìm các thông tin đăng nhập và xem chính xác ngày và thời gian đăng nhập.



Hình 2.9 Định cấu hình và quản lý người dùng

Kích đúp chuột vào các sự kiện này để hiển thị chi tiết tên tài khoản đăng nhập.



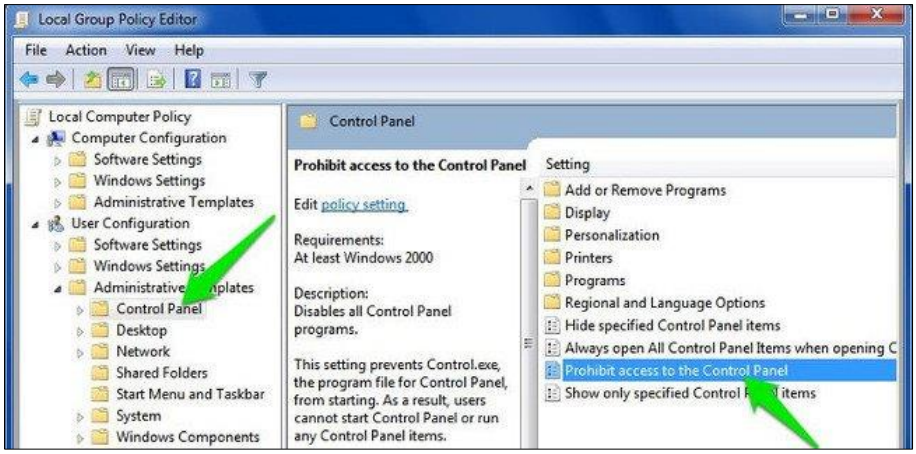
Hình 2.10 Định cấu hình và quản lý người dùng

2.3.2. Chặn truy cập Control Panel

Control Panel được xem là "trung tâm" các thiết lập của Windows, bao gồm cả thiết lập bảo mật và thiết lập sử dụng. Tuy nhiên nếu bị rơi vào tay kẻ xấu bạn sẽ không thể đoán trước được điều gì sẽ xảy ra. Để ngăn chặn các trường hợp xấu có thể xảy ra, tốt nhất bạn nên **chặn quyền truy cập Control Panel**.

Để làm được điều này, trên cửa sổ Group Policy Editor bạn điều hướng theo key:

User Configuration => Administrative Templates => Control Panel



Hình 2.11 Định cấu hình và quản lý người dùng

Tại đây tìm và kích đúp vào tùy chọn có tên "**Prohibit access to the Control Panel**".

Trên cửa sổ Prohibit access to the Control Panel, click chọn tùy chọn **Enable** để chặn truy cập Control Panel. Bây giờ tùy chọn Control Panel sẽ được gỡ bỏ khỏi Start Menu và không một ai có thể truy cập Control Panel được nữa, thậm chí ngay cả khi mở Control Panel trên cửa sổ lệnh **Run**.

Hình 2.12 Định cấu hình và quản lý người dùng

Nếu cố gắng mở Control Panel, trên màn hình sẽ hiển thị thông báo lỗi.

2.3.3. Ngăn chặn người dùng khác cài đặt phần mềm mới trên hệ thống

Sẽ phải mất một khoảng thời gian dài để có thể "dọn sạch" được lũ virus và các phần mềm độc hại đáng ghét tấn công trên máy tính của bạn khi cài đặt bất kỳ phần mềm nào. Do đó để đảm bảo an toàn cho hệ thống cũng như đảm bảo người dùng khác đăng nhập trái phép và cài đặt các phần mềm, chương trình có nhiễm các phần mềm độc hại trên máy tính của mình, bạn nên **vô hiệu hóa Windows installer trên Group Policy** đi.

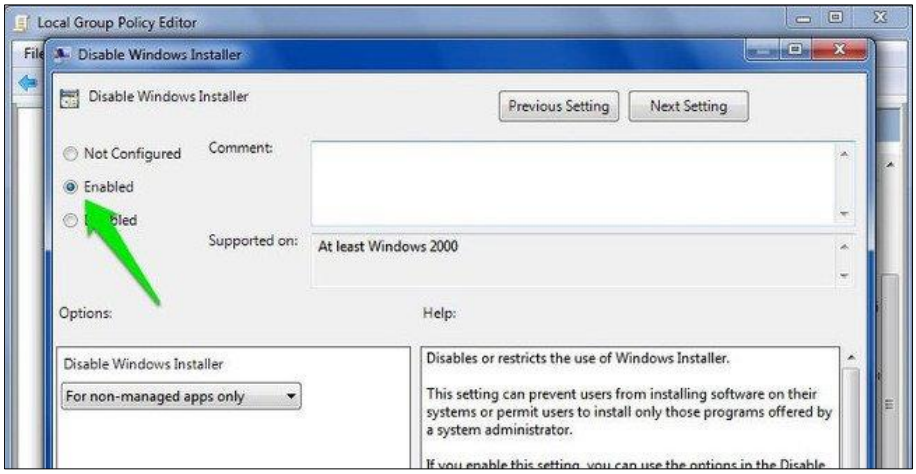
Trên cửa sổ Group Policy bạn điều hướng theo key:

Computer Configuration => Administrative Templates => Windows Components => Windows Installer

Hình 2.13 Định cấu hình và quản lý người dùng

Tại đây tìm và kích đúp chuột vào "*Disable Windows Installer*".

Trên cửa sổ Disable Windows Installer, chọn tùy chọn **Enable** và chọn **Always** từ Menu dropdown tại mục **Options**.



Hình 2.14 Định cấu hình và quản lý người dùng

Từ giờ người dùng khác không thể cài đặt bất kỳ phần mềm mới nào trên máy tính của bạn, mặc dù họ có thể tải và lưu trữ ứng dụng đó trên máy tính.

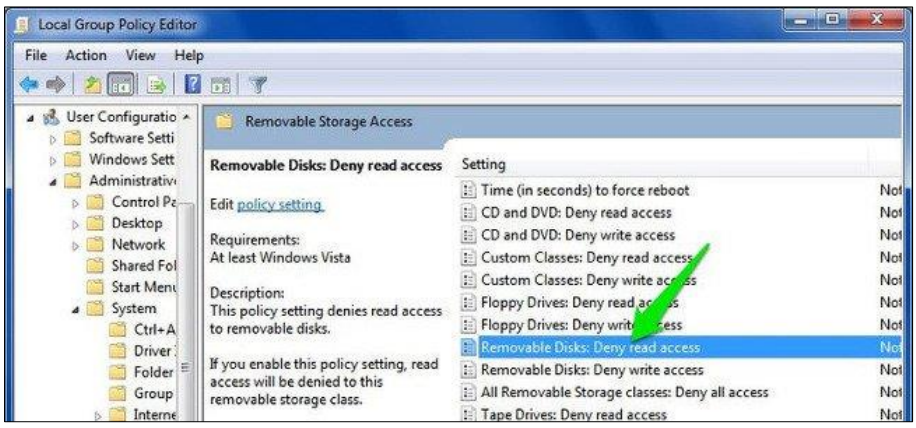
2.3.4. Vô hiệu hóa truy cập các thiết bị lưu trữ di động

Các thiết bị lưu trữ di động như USB, hoặc các thiết bị khác khá là hữu ích để sao chép và lưu trữ dữ liệu, nhưng tuy nhiên đây cũng có thể là một trong những "con đường" để virus tấn công máy tính của bạn.

Nếu ai đó vô tình (hay cố ý) kết nối một thiết bị lưu trữ có nhiễm virus với máy tính của bạn, virus có thể tấn công toàn bộ hệ thống máy tính của bạn và gây ra một số vấn đề nghiêm trọng trên máy tính.

Để chặn người khác kết nối các thiết bị lưu trữ di động trên máy tính của bạn, trên cửa sổ Group Policy bạn điều hướng theo key:

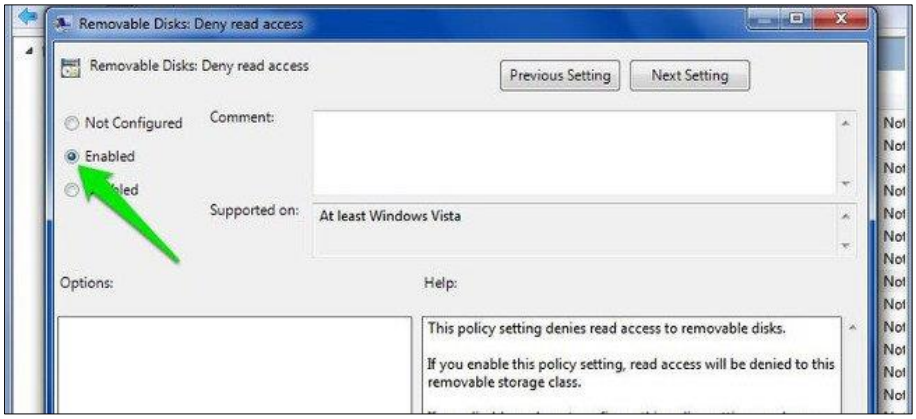
User Configuration => Administrative Templates => System > Removable Storage Access => Removable Disks: Deny read access



Hình 2.15 Định cấu hình và quản lý người dùng

Tại đây bạn tìm và kích đúp chuột vào "*Removable Disks: Deny read access*".

Trên cửa sổ Removable Disks: Deny read access, click chọn **Enable** để kích hoạt tùy chọn và máy tính của bạn sẽ không đọc bất kỳ dữ liệu từ thiết bị lưu trữ ngoài (chẳng hạn như ổ USB,…). Ngoài ra trên cửa sổ Group Policy có một tùy chọn bên dưới có tên "*Removable Disks: Deny write access*". Bạn có thể kích hoạt tùy chọn nếu **không muốn bất kỳ ai ghi (dán) dữ liệu vào thiết bị lưu trữ ngoài.**



Hình 2.16 Định cấu hình và quản lý người dùng

2.3.5. Ngăn một ứng dụng cụ thể đang chạy

Ngoài ra Group Policy còn cho phép người dùng tạo một danh sách các ứng dụng để **ngăn chặn các hoạt động của các ứng dụng này.**

Để làm được điều này, trên cửa sổ Group Policy bạn điều hướng theo key:

User Configuration => Administrative Templates => System => Don't run specified Windows applications

Hình 2.17 Định cấu hình và quản lý người dùng

Tại đây bạn tìm và mở tùy chọn "*Don't run specified Windows applications*".

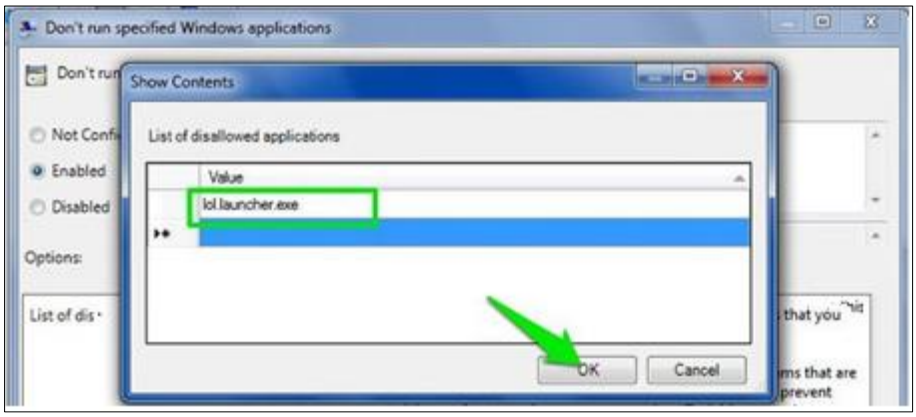
Trên cửa sổ Don't run specified Windows applications, click chọn **Enable** để kích hoạt tùy chọn và click chọn **Show** để bắt đầu quá trình tạo một danh sách ứng dụng mà bạn muốn chặn.

Hình 2.18 Định cấu hình và quản lý người dùng

Để tạo danh sách, bạn phải nhập tên thực thi của ứng dụng kèm theo .exe để có thể chặn ứng dụng, chẳng hạn như **CCleaner.exe**, CleanMem.exe hoặc lol.launcher.exe.

Cách tốt nhất để tìm chính xác tên thực thi của ứng dụng là tìm thư mục ứng dụng trên Windows File Explorer, sau đó sao chép chính xác tên thực thi của chương trình (có phần đuôi mở rộng là ".exe").

Nhập tên thực thi vào danh sách rồi click chọn **OK** để bắt đầu quá trình chặn ứng dụng.



Hình 2.19 Định cấu hình và quản lý người dùng

Ngoài ra trên cửa sổ Group Policy còn có tùy chọn **Run only specified Windows applications**. Nếu muốn vô hiệu hóa tất cả các loại ứng dụng, trừ một số ứng dụng quan trọng, bạn có thể sử dụng tùy chọn để tạo một danh sách các ứng dụng mà bạn muốn chặn.

2.3.6. Vô hiệu hóa Command Prompt và Windows Registry Editor

Command Prompt trên Windows cho phép bạn nhập những câu lệnh để máy tính thực hiện lệnh đó và truy cập hệ thống. Tuy nhiên các hacker có thể dùng lệnh Command Prompt (CMD) để truy cập trái phép những dữ liệu nhạy cảm.

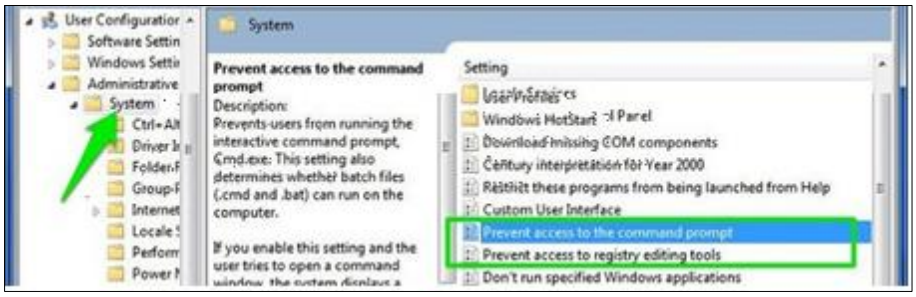
Cả Command Prompt và Windows Registry Editor là những công cụ có thể **vô hiệu hóa mọi hoạt động trên máy tính Windows, đặc biệt là Windows Registry Editor**.

Nếu muốn đảm bảo an toàn cũng như các vấn đề bảo mật trên máy tính của mình, bạn nên vô hiệu hóa Command Prompt và Windows Registry Editor đi.

Để làm được điều này, trên cửa sổ Group Policy bạn điều hướng theo đường dẫn:

User Configuration => Administrative Templates = > System

Tại đây bạn tìm và kích đúp chuột vào các tùy chọn có tên "*Prevent access to the command prompt*" và "*Prevent access to registry editing tools*". Sau đó trên cửa sổ Prevent access to the command prompt và cửa sổ Prevent access to registry editing tools bạn click chọn **Disable** để vô hiệu hóa các tùy chọn này đi.



Hình 2.20 Định cấu hình và quản lý người dùng

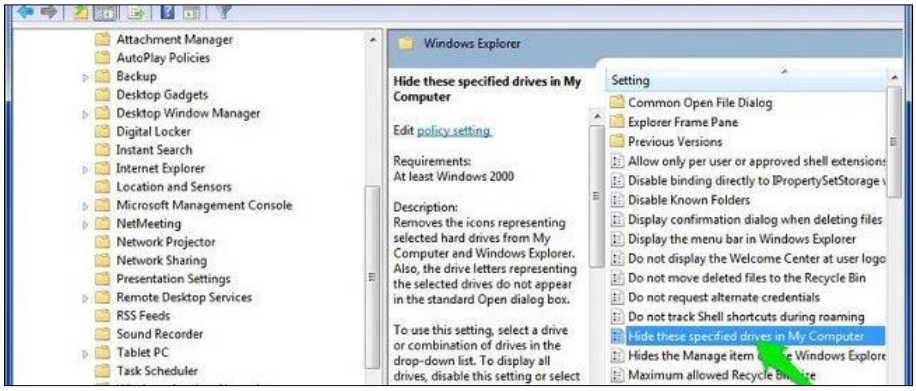
Từ giờ người dùng khác không thể truy cập Command Prompt và Registry Editor nữa.

2.3.7. Ẩn phân vùng ổ đĩa từ My Computer

Nếu một ổ đĩa cụ thể nào đó trên máy tính của bạn có chứa dữ liệu nhạy cảm và bạn không muốn người dùng khác truy cập và đánh cắp các dữ liệu đó, khi đó bạn có thể **ẩn ổ đĩa đó từ My Computer** và người dùng khác không thể tìm được chúng.

Để làm được điều này, trên cửa sổ Group Policy bạn điều hướng theo đường dẫn:

User Configuration => Administrative Templates => Windows Components => Windows Explorer => Hide these specified drives in My Computer



Hình 2.21 Định cấu hình và quản lý người dùng

Tại đây tìm và kích đúp chuột vào tùy chọn có tên "*Hide these specified drives in My Computer*".

Trên cửa sổ Hide these specified drives in My Computer click chọn Enable để kích hoạt tùy chọn.

Sau khi kích hoạt tùy chon, từ menu dropdown mục **Options**, chọn ổ mà bạn muốn ẩn. Cuối cùng click chọn **OK** để ẩn ổ đó trên hệ thống.

Hình 2.22 Định cấu hình và quản lý người dùng

2.3.8. Tinh chỉnh Start Menu và thanh Taskbar

Group Policy cung cấp cho bạn hàng tá các tinh chỉnh cho Start Menu và thanh Taskbar theo ý muốn của bạn. Các tinh chỉnh này có sẵn cho cả Admin và người dùng thường.

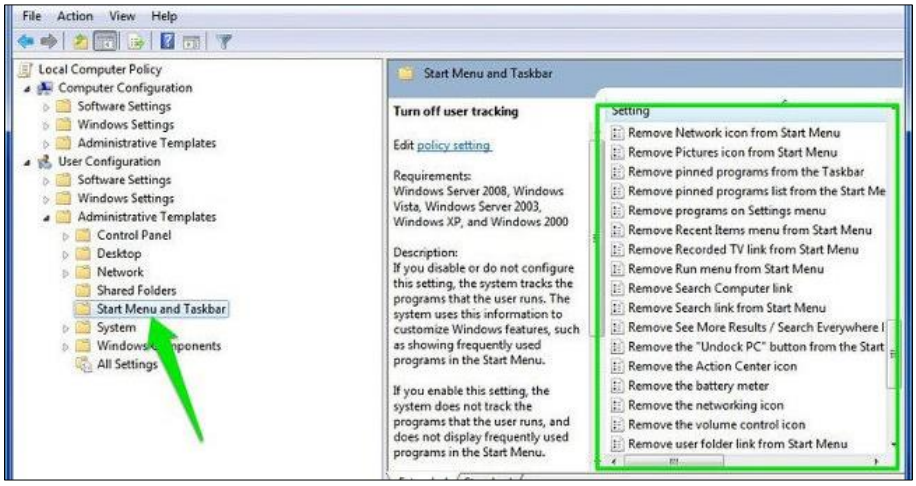
Để tinh chỉnh Start Menu và thanh Taskbar, trên cửa sổ Group Policy Editor bạn điều hướng theo đường dẫn:

User Configuration => Administrative Templates => Start Menu and Taskbar

Tại đây bạn sẽ tìm thấy tất cả các tinh chỉnh kèm theo các giải thích.

Các tinh chỉnh khá là dễ hiểu. Bên cạnh đó Windows còn cung cấp mô tả chi tiết cho mỗi tinh chỉnh.

Bạn có thể thực hiện một số thao tác như thay đổi chức năng nút Power trên Start Menu, ngăn người dùng ghim chương trình trên thanh Taskbar, hạn chế tìm kiếm trên tùy chọn Search, ẩn thông báo trên khay hệ thống, ẩn biểu tượng pin, ngăn việc thay đổi thanh Taskbar và thiết lập Start Menu, ngăn người dùng sử dụng các tùy chọn Nguồn (tắt máy, chế độ ngủ đông (hibernate),…), gỡ bỏ tùy chọn **Run** khỏi Start Menu,….



Hình 2.23 Định cấu hình và quản lý người dùng

2.3.9. Vô hiệu hóa việc buộc khởi động lại

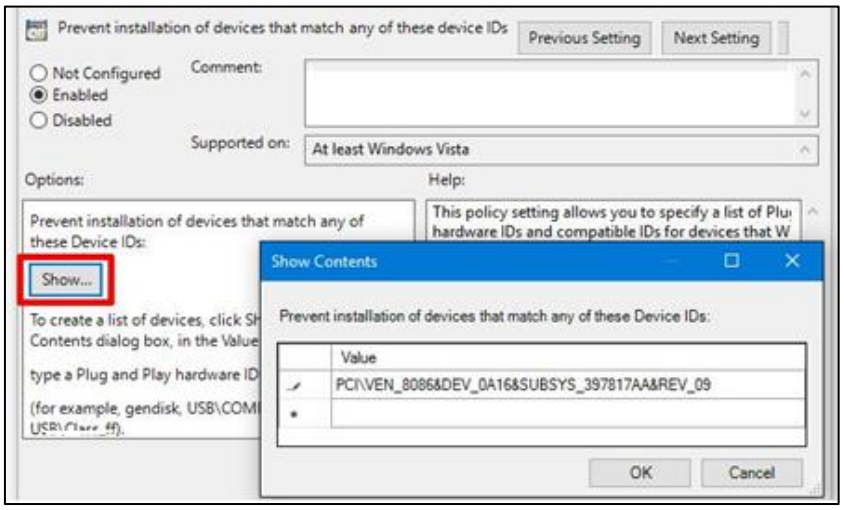
Mặc dù bạn có thể kích hoạt một số tùy chọn để trì hoãn, nhưng Windows 10 cuối cùng sẽ tự khởi động lại máy tính, nếu có các bản cập nhật đang chờ xử lý. Bạn có thể lấy lại quyền kiểm soát bằng cách kích hoạt một mục Group Policy.

Khi bạn thực hiện vô hiệu hóa việc buộc khởi động lại, Windows sẽ chỉ áp dụng các bản cập nhật đang chờ xử lý khi bạn tự khởi động lại.

Bạn sẽ tìm thấy nó ở đây:

Computer Configuration > Administrator Templates > Windows Components > Windows Update > No auto-restart with logged on users for scheduled automatic update installations

2.3.10. Vô hiệu hóa cập nhật driver tự động



Hình 2.24 Định cấu hình và quản lý người dùng

Vô hiệu hóa cập nhật driver tự động

Bạn có biết rằng Windows 10 cũng cập nhật driver thiết bị mà không có sự cho phép rõ ràng của bạn không? Trong nhiều trường hợp, điều này rất hữu ích, vì nó nhằm mục đích giữ cho hệ thống cập nhật nhất có thể.

Nhưng nếu bạn chạy một driver tùy chỉnh hoặc có lẽ driver mới nhất cho một thành phần phần cứng nhất định có lỗi khiến hệ thống của bạn gặp sự cố thì sao? Đây là lúc việc cập nhật driver tự động có hại hơn là hữu ích.

Để vô hiệu hóa cập nhật driver tự động, hãy kích hoạt:

Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions > Prevent installation of devices that match any of these device IDs

Sau khi kích hoạt, bạn sẽ phải cung cấp ID phần cứng cho các thiết bị mà bạn không muốn cập nhật driver tự động. Bạn có được những thứ này thông qua **Device Manager**, phải mất một vài bước.

2.3.11. Ẩn Balloon và Toast Notification

Thông báo trên màn hình có thể hữu ích, nhưng chỉ khi chúng cung cấp điều gì đó có giá trị. Hầu hết các thông báo mà bạn thấy đều không đáng đọc và thường làm bạn mất tập trung.

Kích hoạt giá trị này để tắt thông báo dạng bong bóng (balloon notification) trong Windows:

User Configuration > Administrative Templates > Start Menu and Taskbar > Turn off all balloon notifications

Bắt đầu với Windows 8, hầu hết các thông báo hệ thống chuyển sang dạng toast notification. Do đó, bạn cũng nên vô hiệu hóa chúng:

User Configuration > Administrative Templates > Start Menu and Taskbar > Notifications > Turn off toast notification

Đây là một cách dễ dàng để ngăn chặn sự phiền nhiễu từ các thông báo.

2.3.12. Xóa OneDrive

OneDrive được đưa vào Windows 10. Mặc dù bạn có thể gỡ cài đặt nó như bất kỳ ứng dụng nào khác, nhưng cũng có thể ngăn nó chạy bằng cách sử dụng một mục Group Policy.

Vô hiệu hóa OneDrive bằng cách kích hoạt:

Computer Configuration > Administrative Templates > Windows Components > OneDrive > Prevent the usage of OneDrive for file storage

Điều này sẽ loại bỏ khả năng truy cập OneDrive từ bất kỳ đâu trên hệ thống. Nó cũng xóa shortcut OneDrive trong thanh bên File Explorer.

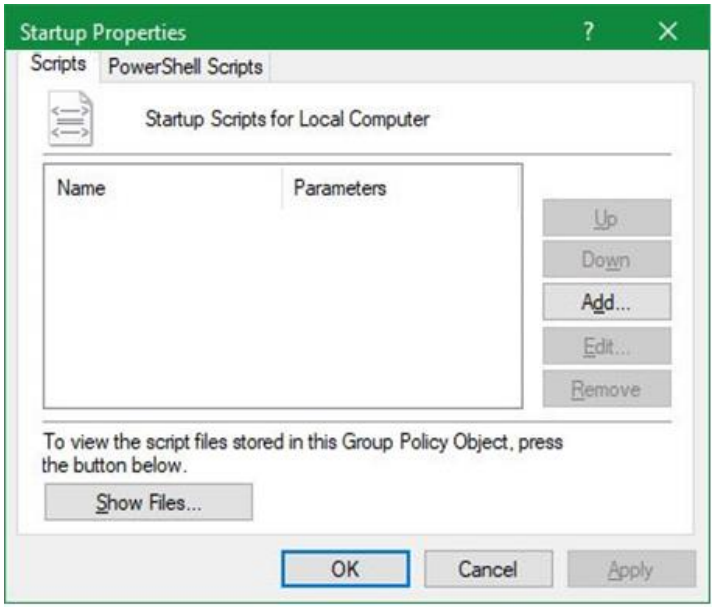
2.3.13. Tắt Windows Defender

Windows Defender tự quản lý, vì vậy nó sẽ ngừng chạy nếu bạn cài đặt ứng dụng diệt virus của bên thứ ba. Nếu công cụ này không hoạt động đúng vì một số lý do hoặc bạn muốn vô hiệu hóa nó hoàn toàn, bạn có thể kích hoạt mục Group Policy này:

Computer Configuration > Administrative Templates > Windows Components > Windows Defender > Turn off Windows Defender

Mặc dù có thể dễ dàng vô hiệu hóa, nhưng Windows Defender là một giải pháp bảo mật đủ tốt cho hầu hết mọi người. Đảm bảo thay thế Windows Defender bằng một chương trình diệt virus cho Windows đáng tin cậy khác, nếu bạn gỡ bỏ nó.

2.3.14. Chạy script khi đăng nhập/khởi động/tắt máy



Hình 2.25 Định cấu hình và quản lý người dùng

Chạy script khi đăng nhập/khởi động/tắt máy

Cuối cùng nâng cao hơn một chút, vì vậy có lẽ nó sẽ không hữu ích lắm, trừ khi bạn có thể thoải mái với các file batch và/hoặc việc viết các script PowerShell. Nếu thấy ổn, thì bạn thực sự có thể chạy các script đã nói tự động với Group Policy.

Để thiết lập script khởi động/tắt máy, hãy truy cập:

Computer Configuration > Windows Settings > Scripts (Startup/Shutdown)

Để thiết lập một script đăng nhập hoặc đăng xuất, hãy vào đây:

User Configuration > Windows Settings > Scripts (Logon/Logoff)

Làm điều này cho phép bạn chọn các file script thực tế và cung cấp các tham số cho những script đó, do vậy, nó khá linh hoạt. Bạn cũng có thể gán nhiều script cho mỗi sự kiện kích hoạt.

2.4 Định cấu hình màn hình nền

Việc thay đổi màn hình Desktop là một thao tác quá đơn giản đối với những bạn sử dụng máy tính thường xuyên rồi phải không nào?

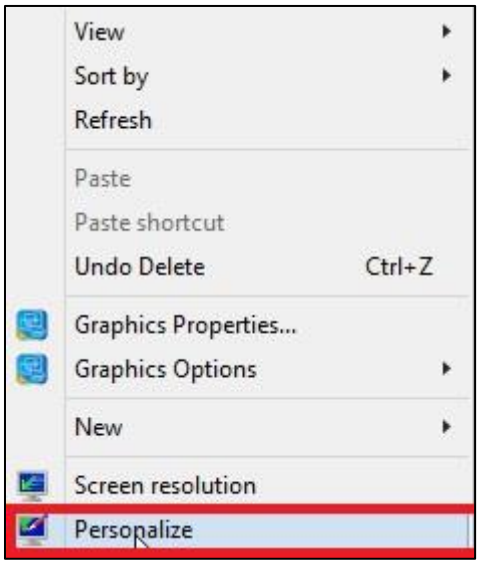
Tuy nhiên, trong giáo trình này vẫn hướng dẫn chi tiết, bởi vì với tiêu chí và mục tiêu là sẽ hướng dẫn và chia sẻ tất cả, từ dễ cho đến khó để có thể hỗ trợ tốt nhất cho độc giả, nên có lẽ bài viết trong giáo trình này chỉ phù hợp với những bạn Newber thôi nhé.

2.4.1. Sử dụng hình nền mặc định của Windows

Đối với các hệ điều hành mới như Windows 7/ Windows 8 và 8.1 hay là hệ điều hành Windows 10 thì những hình nền mặc định do Microsoft cung cấp cho người dùng là khá đẹp và rất đáng để sử dụng.

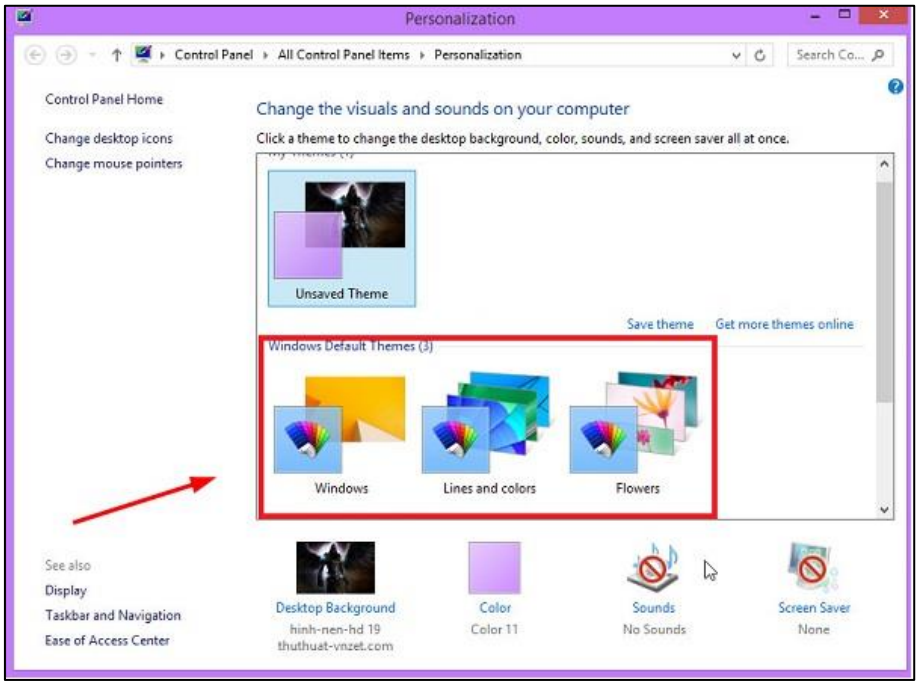
Trong giáo trình này bạn có thể làm theo hướng dẫn sau để sử dụng các hình nền mặc định khác trong Windows:

Thực hiện: Nhấn chuột phải vào khoảng không ngoài màn hình Desktop và chọn Personalize



Hình 2.26 Định cấu hình màn hình nền

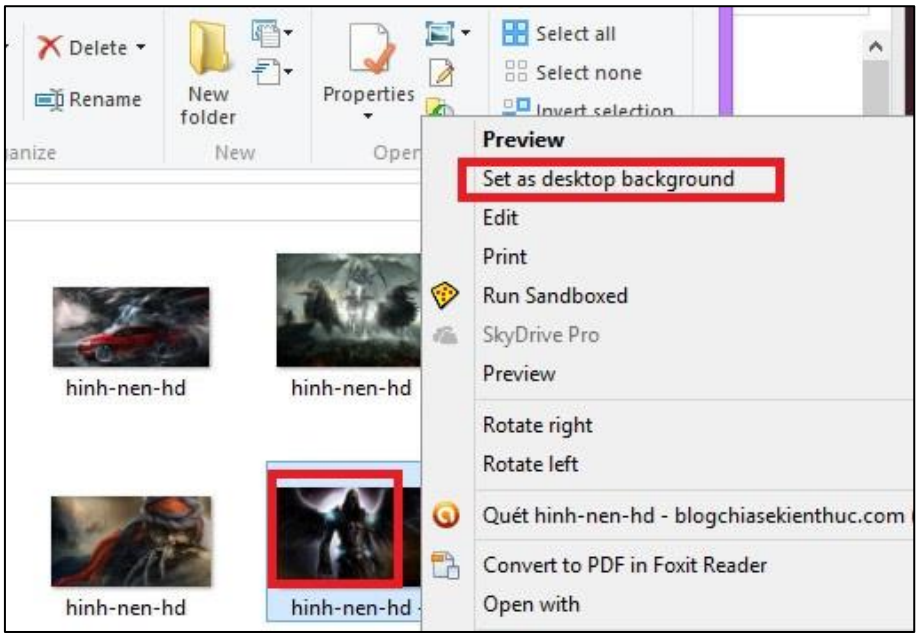
Tiếp theo chỉ việc lựa chọn hình nền (Background) – tông màu mà bạn thích thôi



Hình 2.27 Định cấu hình màn hình nền

Set (cài đặt) một hình ảnh bất kỳ làm hình nền

Cái này thì đơn giản nhất rồi, bạn chỉ cần lựa một hình ảnh mà bạn thích, sau đó nhấn chuột phải vào hình ảnh đó và chọn **Set as desktop background**



Hình 2.28 Định cấu hình màn hình nền

Tự động thay đổi hình nền Desktop

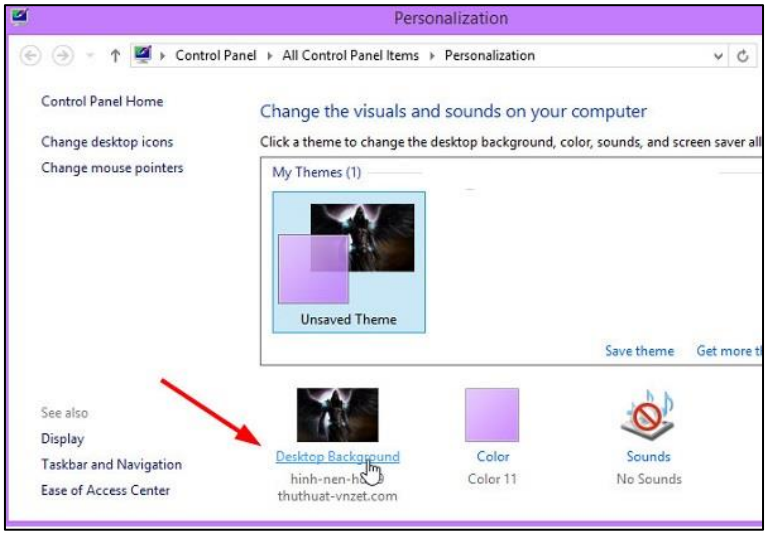
Có nghĩa là bạn sẽ sử dụng nhiều hình ảnh để làm hình nền cho máy tính, và sau một khoảng thời gian nào đó (do bạn đặt ra) nó sẽ tự động chuyển qua hình ảnh tiếp theo.

Cách này cũng rất hay, giúp bạn không bị nhàm chán khi phải sử dụng 1 hình ảnh, và mất thời gian thay đổi sau một thời gian sử dụng.

Thay đổi hình nền máy tính trên Windows 7, 8 và 8.1

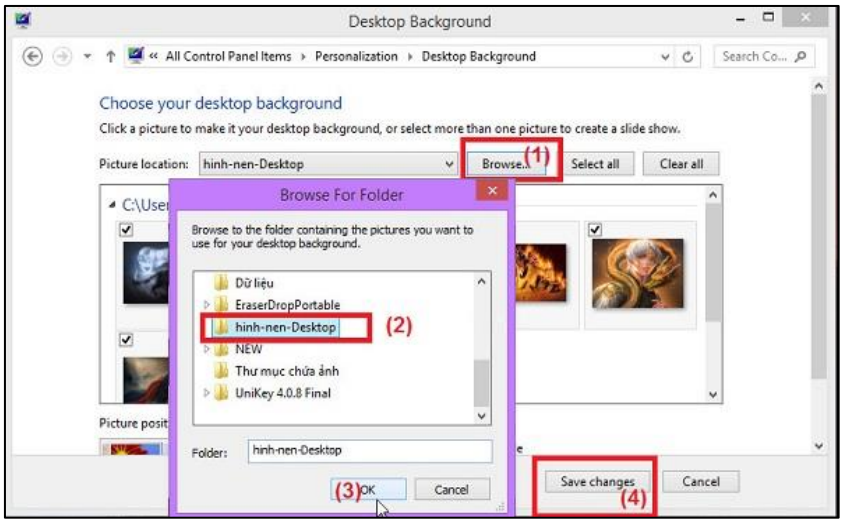
- **Bước 1:** Trước tiên bạn cần tìm một số hình ảnh đẹp mà bạn muốn làm hình nền sau đó cho chúng vào chung 1 thư mục (Folder). Nếu thích bạn có thể tải một số hình ảnh Full HD để làm hình nền máy tính.
- **Bước 2:** Để sử dụng nhiều hình ảnh làm hình nền Desktop cũng không có gì khó khăn cả.

Bạn cũng nhấn chuột phải vào Desktop => và chọn Personalize như thay đổi hình nền mặc định mình đã hướng dẫn phía trên đó. Nhưng thay vì lựa chọn các hình nền có sẵn thì bạn nhấp chuột vào Desktop BackGround



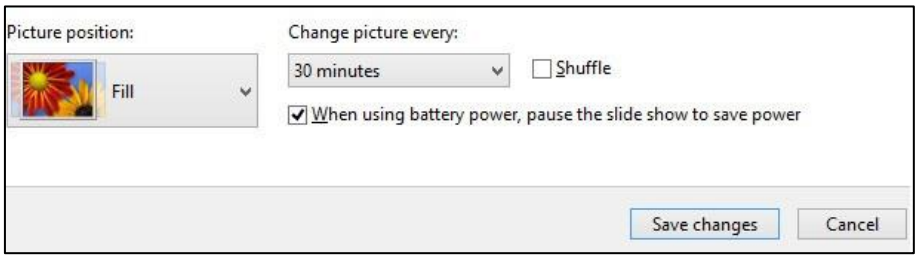
Hình 2.29 Định cấu hình màn hình nền

- **Bước 3:** Ở cửa sổ tiếp theo bạn nhấn vào Browse... và tìm đến Folder chứa ảnh bạn đã chuẩn bị sẵn. Cuối nhấn nhấn **OK** chọn **Save changes** để lưu lại.



Hình 2.30 Định cấu hình màn hình nền

- **Bước 4:** Nếu thích thì bạn có thể chỉnh lại thời gian để chuyển từ bức ảnh này sang bức ảnh khác, lựa chọn chuyển đến một bức ảnh bất kỳ (random)… để làm được việc này thì tại giao diện như hình bên trên bạn kéo xuống và thiết lập lại nhé.



Hình 2.31 Định cấu hình màn hình nền

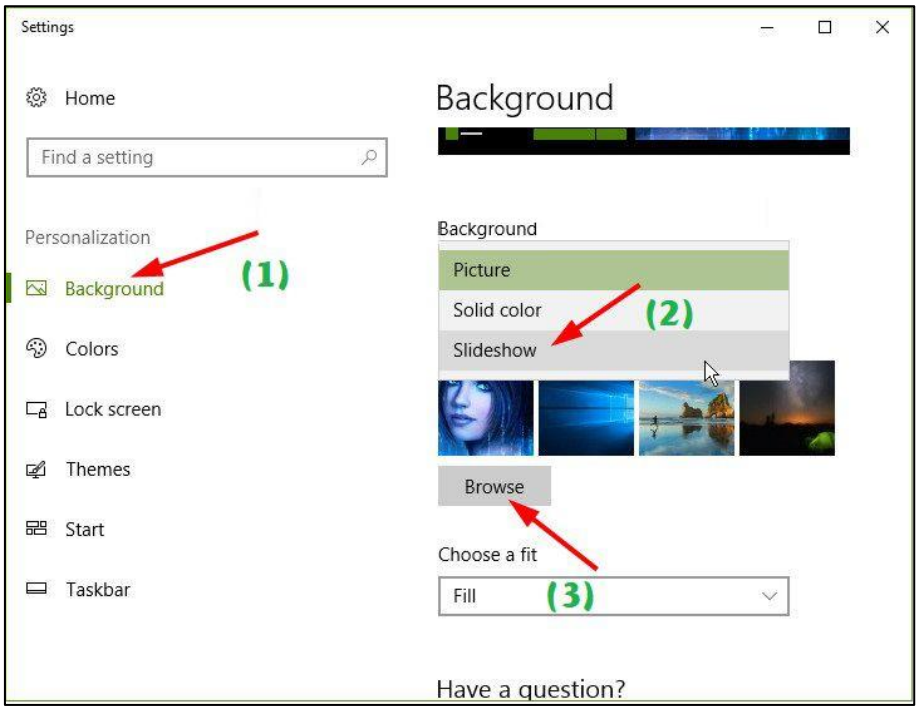
Trong đó:

- **Change picture every:** Có nghĩa là thời gian chuyển từ ảnh này sang ảnh khác là..xx.. phút.
- **Shuffle:** Chế độ Random, chuyển đến một bức ảnh ngẫu nhiên trong danh sách các bức ảnh bạn đã chọn, không theo một thứ tự nào cả.
- **When using battery power, pause the slide show to save power:** Tích vào lựa chọn này tức là khi sử dụng năng lượng pin máy tính sẽ tạm dừng trình chiếu ảnh để tiết kiệm điện.

Thay đổi hình nền máy tính trên Windows 10

- **Thực hiện:** Nhấp chuột phải vào màn hình Desktop => chọn Personalize => chọn Background => trong phần Background bạn chọn là Slideshow thay vì Picture như mặc định.

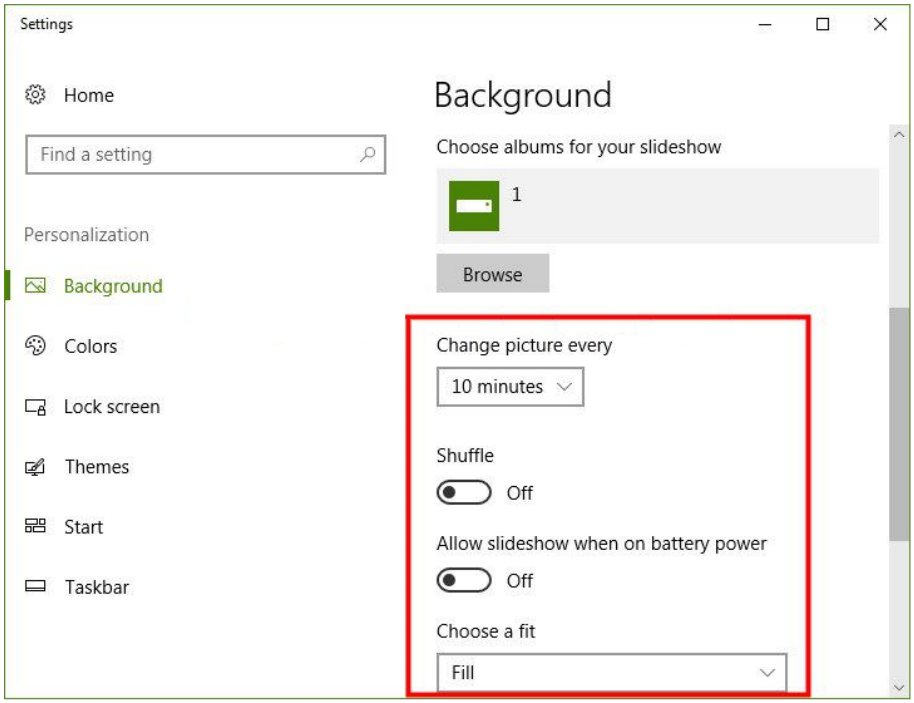
Tiếp theo bạn hãy nhấn vào Browse và chọn thư mục chứa các hình ảnh mà bạn muốn đặt làm hình nền.



Hình 2.32 Định cấu hình màn hình nền

Tiếp theo, bạn hãy thiết lập thêm các tính năng khác ví dụ như:

- **Change picture every:** Thời gian chuyển ảnh, bạn chọn thời gian mà bạn muốn.
- **Shuffle:** Xáo trộn, có nghĩa là hình ảnh sẽ hiển thị kiểm Random (ngẫu nhiên) và không theo một thứ tự nào cả.
- **Allow slideshow when on battery power:** Cho phép xem hình tự động khi sử dụng Pin.
- **Choose a fit:** Chọn kiểu hiển thị hình ảnh.



Hình 2.33 Định cấu hình màn hình nền

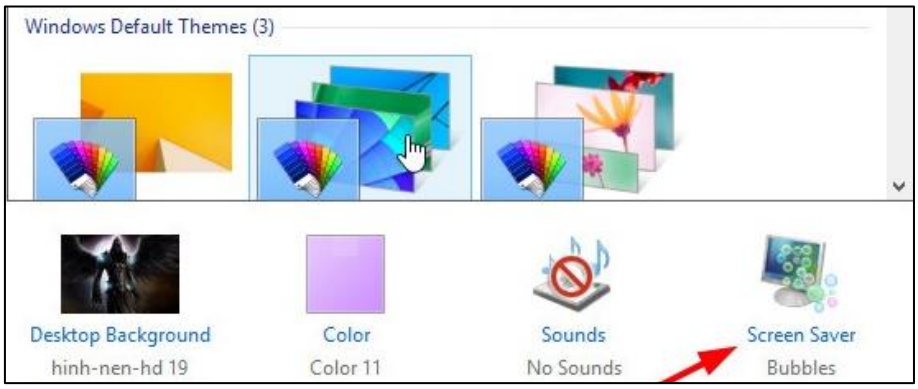
Vậy là xong rồi. Rất đơn giản vậy thôi

Cách cài đặt, thay đổi màn hình chờ cho máy tính

Áp dụng trên Windows 7, 8 và 8.1

Có nghĩa là sau một khoảng thời gian không sử dụng đế chuột và bàn phím thì máy tính sẽ tự động kích hoạt màn hình chờ. Thao tác như sau:

- **Thực hiện:** Nhấp chuột phải vào màn hình Desktop chọn Personalize như các bước thay **đổi hình nền desktop** bên trên. Tại đây bạn chọn Screen Saver



Hình 2.34 Định cấu hình màn hình nền

- Tiếp theo bạn cài đặt theo ý thích của mình:

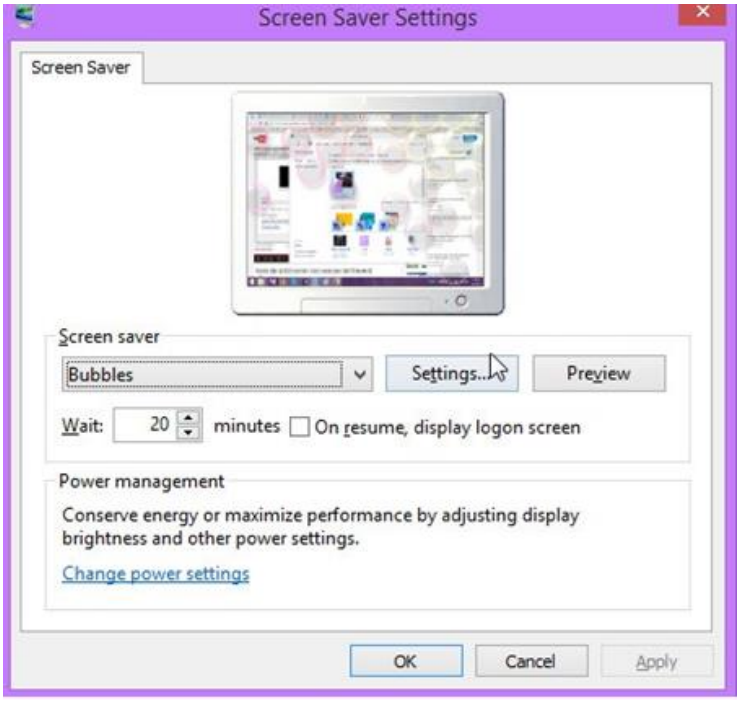
+ **Screen saver:** Mình chọn là Bubbles (màn hình chờ bong bong rất đẹp mắt), bạn có thể lựa chọn cái khác nếu không thích cái này.

+ **Settings..**: Một số hiệu ứng màn hình chờ sẽ phải vào phần Settings để cài đặt ví dụ như 3D Text, còn ví dụ như hiệu ứng Bubbles mình đã chọn bên trên sẽ không cần phải cài đặt gì.

+ **Preview**: Xem thử trước.

+ **Wait:** Sau một khoảng thời gian bao nhiêu phút không sử dụng chuột và bàn phím thì sẽ xuất hiện màn hình chờ này.

+ **On resume, display logon screen:** Tích vào lựa chọn này có nghĩa là máy tính xuất hiện màn hình chờ đồng thời kích hoạt chế độ Logon.

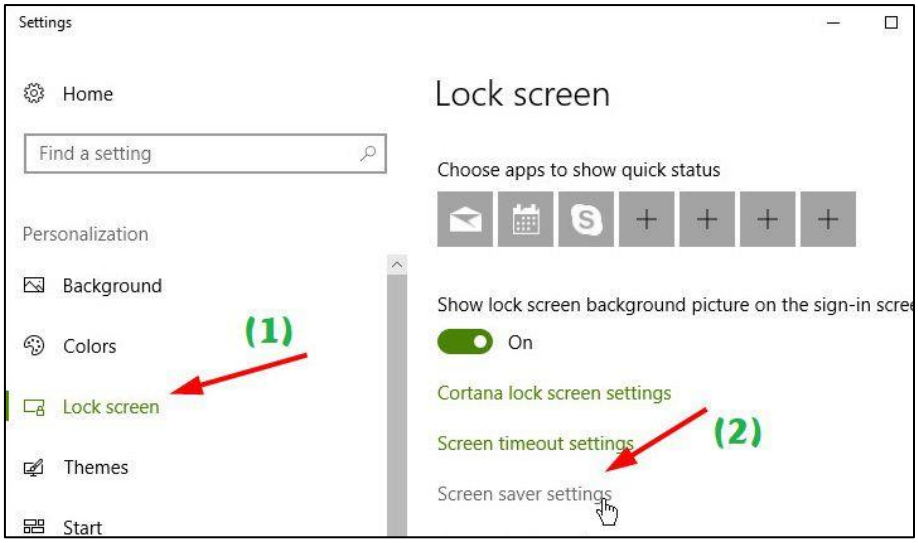


Hình 2.35 Định cấu hình màn hình nền

Áp dụng trên Windows 10

Có rất nhiều bạn hỏi về cách cài đặt màn hình chờ cho Windows 10 thế nào, vì họ không thấy mục Screen Sever ở đâu cả. Rất đơn giản thôi bạn làm như sau:

- **Cách 1:** Bạn có thể sử dụng tính năng tìm kiếm trên Windows với từ khóa screen sever.
- **Cách 2:** Nhấp chuột phải vào màn hình Desktop => chọn Personalize => chọn Lock screen => bạn kéo xuống và tìm đến phần Screen Server settings như hình bên dưới.



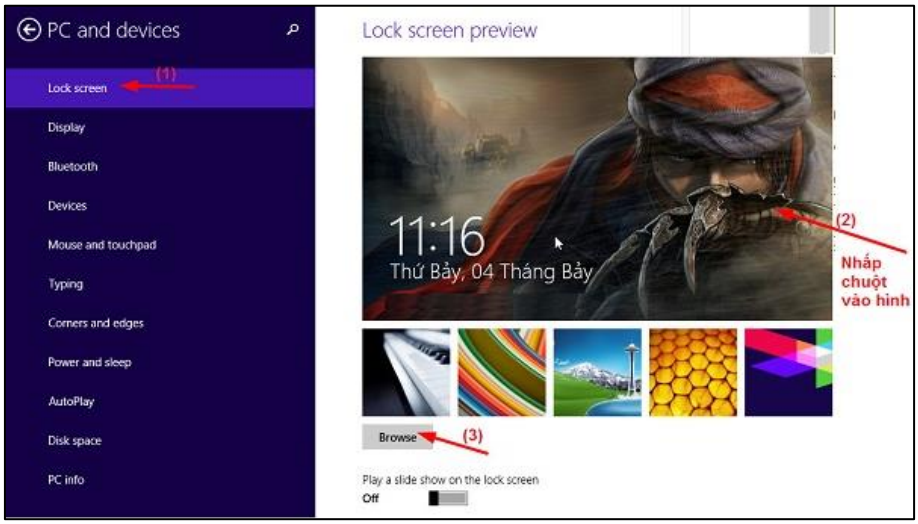
Hình 2.36 Định cấu hình màn hình nền

Vậy là đã hoàn thành, bây giờ thì bạn có thể cài đặt, thiết lập hoàn toàn tương tự như đối với Windows 7, 8, 8.1 mà trong giáo trình vừa hướng dẫn bên trên xong.

Thay đổi hình nền màn hình khóa (Look Screen)

Trên Windows 8 và 8.1

- **Thực hiện:** Đầu tiên bạn hãy nhấn phím Windows + I hoặc dê chuột vào góc phải màn hình máy tính và chọn Settings => tiếp theo chọn Change PC Settings
- Tiếp theo chọn Look Screen => nhấp chuột vào hình ảnh hiện tại => chọn Browse... và tìm đến bức ảnh bạn muốn thay thế là xong.

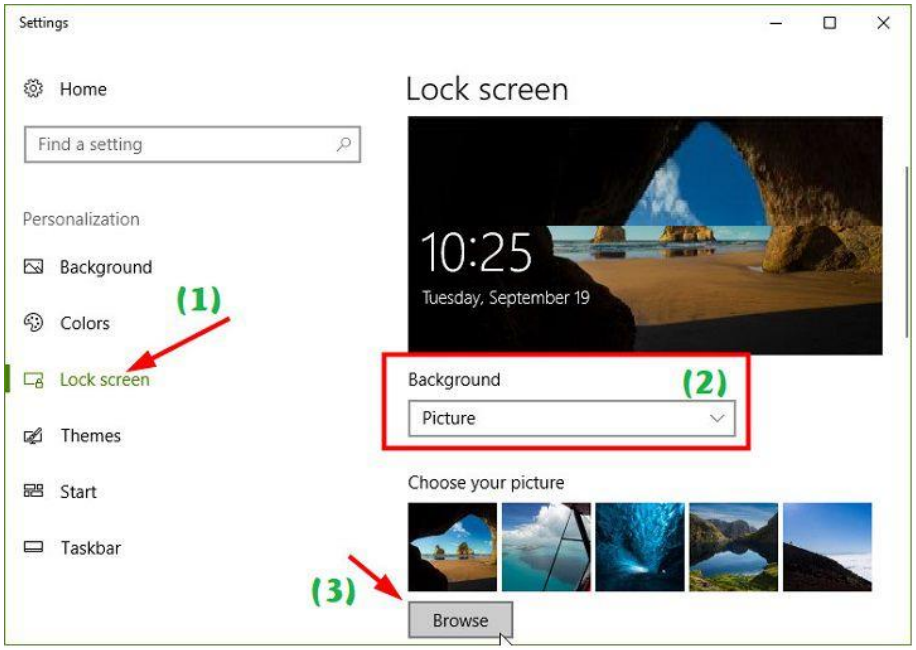


Hình 2.37 Định cấu hình màn hình nền

Trên hệ điều hành Windows 10

Thực hiện: Nhấp chuột phải vào màn hình Desktop => chọn Personalize => chọn Lock screen => trong phần Background bạn chọn là Picture (hình ảnh) hoặc Slideshow (nhiều hình ảnh) để hiển thị.

- Tiếp theo bạn hãy nhấn vào Browse và chọn hình ảnh (nếu bạn chọn là **Picture**) hoặc thư mục chứa các hình ảnh (nếu như bạn chọn là **Slideshow**).



Hình 2.38 Định cấu hình màn hình nền

Tự động lấy hình ảnh trên Bing làm hình nền máy tính mỗi ngày

- Thêm một công cụ rất hay khác nữa, hỗ trợ các bạn tự động thay đổi hình nền máy tính theo Bing, mà như các bạn đã biết thì Bing là một công cụ tìm kiếm của Microsoft với hàng trăm ngàn bức ảnh đẹp.
- Máy tính của bạn sẽ trở nên mới mẻ mỗi ngày với những hình ảnh hiển thị ngẫu nhiên này. Đây là một công cụ do chính Microsoft phát triển nên bạn hoàn toàn có thể yên tâm về độ ổn định, tính bảo mật… cũng như tính tương thích với hệ điều hành Windows.

2.5 Sự cố về phần mềm hỗ trợ gây ra cho hệ thống

Khi máy tính không khởi động đúng cách, chúng ta có thể rất bực bội. Cho dù bạn đang tạo một bản dựng hay hệ thống đột nhiên ngưng hoạt động, có thể rất khó khăn để biết phải bắt đầu từ đâu để sửa máy tính. Khó khăn càng phức tạp nếu không thể truy cập hệ điều hành.

Trong giáo trình này hướng dẫn bạn các bước nếu máy tính của bạn đang bật và màn hình hiển thị đang hoạt động, nhưng nó không cho phép bạn truy cập hệ điều hành và bị kẹt ở màn hình BIOS. Có rất nhiều nguyên nhân tiềm năng của vấn đề này, nên chúng ta sẽ xem qua một số vấn đề thường gặp để thử làm cho hệ thống hoạt động trở lại.

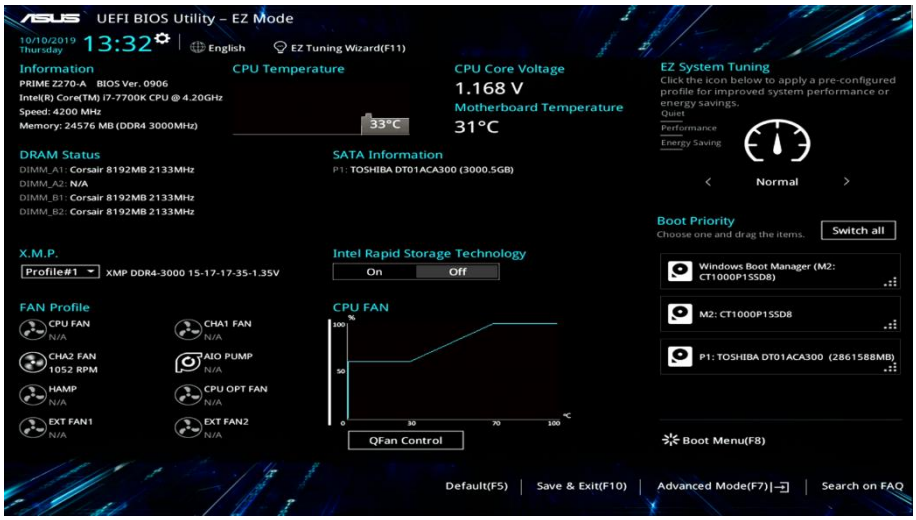
Nên nhớ rằng nếu máy tính của bạn không mở được gì cả - nghĩa là không có gì xảy ra khi nhấn nút nguồn điện, hoặc khi bạn nhấn nút, máy tính mở vài giây và tắt lại, chúng tôi đề cập đến những vấn đề đó ở đây.

Nếu bạn có thể truy cập hệ điều hành, nhưng vẫn còn gặp trục trặc, bạn sẽ cần xử lý sự cố phần mềm. Có rất nhiều nguồn tài liệu có thể được sử dụng cho các vấn đề liên quan đến sự cố hệ điều hành.

BIOS (hệ thống vào/ra cơ bản) là phần mềm được lưu trữ trên bo mạch chủ có khả năng tương tác với phần cứng hệ thống và điều khiển các chức năng cơ bản như ưu tiên khởi động. Bo mạch chủ mới hơn sử dụng UEFI thay vì BIOS. UEI là phiên bản cải thiện phần mềm được thiết kế với giao diện thân thiện với người dùng hơn và phù hợp với phần cứng mới hơn.

Hãy nghĩ đó là hệ điều hành đơn giản để bo mạch chủ điều khiển máy tính cách khởi động. Bạn sẽ thấy BIOS trước khi hệ điều hành tải, và thường gồm một menu văn bản hoặc một giao diện đơn giản cho bạn kiểm soát những đặc tính cơ bản của phần cứng. Bao gồm điều chỉnh hướng dẫn khởi động và xử lý sự cố.

BIOS có thể khác nhau giữa các bo mạch chủ, nên không có hướng dẫn giống nhau cho hoạt động. Mặc dù các nhà sản xuất đưa ra các giao diện khác nhau, chúng có chức năng tương tự. Đối với câu hỏi liên quan đến một vấn đề BIOS cụ thể, hãy kiểm tra tài liệu về bo mạch chủ.



Hình 2.39 Sự cố về phần mềm hỗ trợ gây ra cho hệ thống

Tùy thuộc vào chi tiết cụ thể của tình huống, có thể bạn cần đọc các phần khác nhau. Nếu bạn cắm USB ngoại vi mới, như bàn phím, con chuột hoặc tai nghe. Nếu gần đây bạn đã thêm một thiết bị lưu trữ mới, hãy bắt đầu với phần "Cập nhật BIOS". Nếu máy tính của bạn chưa bao giờ khởi động thành công, tốt nhất bạn nên bắt đầu đọc phần "Thông báo lỗi BIOS".

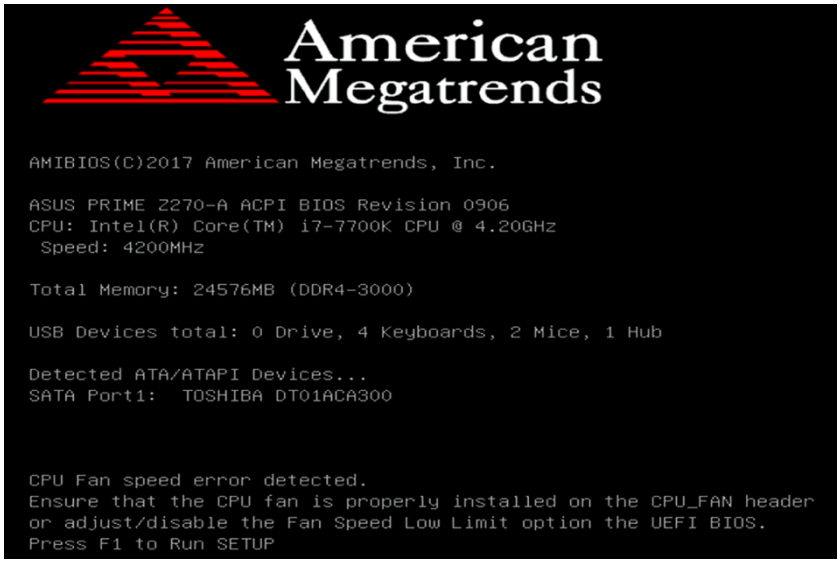
Loại trừ các nhân tố bên ngoài

Trước khi thay đổi cài đặt nào, hãy thử gỡ bỏ tất cả thiết bị ngoại vi khỏi máy tính của bạn. Bao gồm tất cả mọi thứ khác ngoại trừ cáp ngồn điện, cáp hiển thị gắn vào màn hình và bàn phím để điều hướng menu. Các thiết bị ngoại vi gắn vào máy như ổ cứng ngoài hay thậm chí là con chuột USB có khả năng gây ra vấn đề với nguồn điện, xung đột ổ đĩa, hoặc trục trặc với lệnh khởi động, và có thể làm hệ thống không khởi động được.

Nếu hệ thống của bạn khởi động thành công mà không có thiết bị nào gắn vào, hãy gắn từng thiết bị một, và khởi động lại cho đến khi bạn tìm được thiết bị ngoại vi gây ra sự cố.

Thông báo lỗi BIOS

Một khi bạn đã loại bỏ sự cố từ các thiết bị ngoại vi, đã đến lúc kiểm tra BIOS để kiếm thông báo lỗi.



Hình 2.40 Sự cố về phần mềm hỗ trợ gây ra cho hệ thống

Thông thường, nếu BIOS phát hiện ra vấn đề phần cứng, nó sẽ báo cho bạn biết trước khi bạn truy cập menu BIOS. Thông báo lỗi sẽ thay đổi tùy thuộc vào BIOS bạn đang dùng và các sự cố hiện có, nhưng đây là một số ví dụ để tham khảo:

Không thấy quạt CPU - lỗi quạt hay bộ làm mát.

Lỗi thiết bị khởi động - Có vấn đề với một trong các ổ đĩa lưu trữ của bạn.

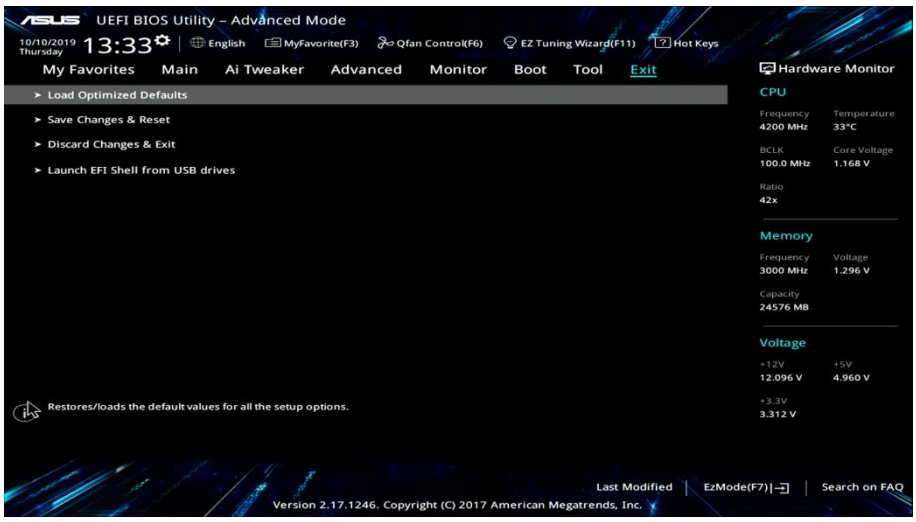
Nếu bạn thật sự gặp lỗi, và ngay lập tức không phát hiện ra vấn đề liên quan, hãy tìm hiểu chi tiết cụ thể trong tài liệu về bo mạch chủ hoặc online. Điều này có thể là một bước quan trọng để xác định vấn đề nằm ở đâu và phải thực hiện bước tiếp theo để sửa chữa.

Nếu bạn vẫn còn gặp rắc rối để tiếp cận hệ điều hành sau khi tìm hiểu và xử lý các thông báo lỗi, có lẽ cần cài BIOS lại chế độ mặc định.

Khôi phục lại mặc định

Cảnh báo: BIOS điều khiển hoạt động cơ bản của hệ thống, nên hãy cẩn thận khi thực hiện các thay đổi.

- **Truy cập menu BIOS nếu bạn chưa vào đó.** Quá trình này sẽ tùy thuộc vào nhà sản xuất, nhưng thường cần nhấn phím ngay lập tức sau khi khởi động hệ thống của bạn, thường là phím F2 hay phím DEL. Hầu hết hệ thống sẽ cho bạn biết trên màn hình phím nào phù hợp ngay sau khi khởi động. Gõ phím này nhiều lần ngay khi bạn khởi động hệ thống, và bạn sẽ thấy menu BIOS.
- **Đặt lại thành cài đặt mặc định.** Bạn sẽ muốn xem làm sao để thực hiện chính xác dựa trên hướng dẫn của nhà sản xuất bo mạch chủ, nhưng lựa chọn này thường nằm trong phần “Lưu và thoát" của menu. Điều này sẽ cài BIOS lại chế độ mặc định, có thể giúp giảm thiểu các sự cố gây ra bởi thay đổi cấu hình. Lưu và khởi động lại để áp dụng thay đổi.



Hình 2.41 Sự cố về phần mềm hỗ trợ gây ra cho hệ thống

Cập nhật BIOS

Điều này có thể không phù hợp nếu bạn đang sử dụng máy dựng trước, hoặc nếu máy tính đang hoạt động và bắt đầu trục trặc, nhưng nếu bạn đang cài đặt máy tính mới, đặc biệt nếu bạn sử dụng bo mạch chủ cũ, cập nhật BIOS có thể hữu dụng khi xử lý sự cố khởi động.

Một lần nữa, tiến trình sẽ có chút thay đổi tùy thuộc vào nhà sản xuất, nên cần tìm hiểu cụ thể. Nhà sản xuất bo mạch chủ có thể có quy trình thích hợp được ghi rõ trong hướng dẫn về bo mạch chủ hoặc trên mạng. Nhiều nhà sản xuất có các quy trình khác biệt, và một số bo mạch chủ cao cấp thậm chí có thể có tính năng tự cập nhật.

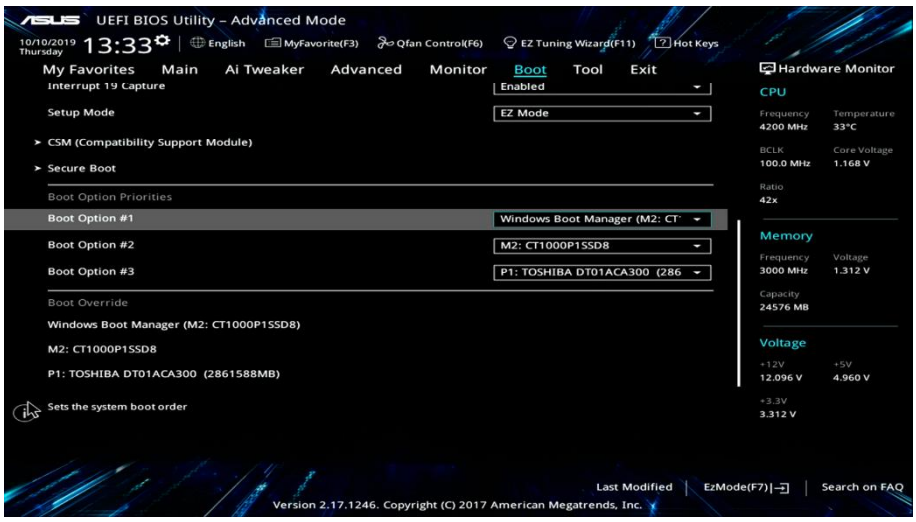
Cập nhật phần cứng có thể xử lý các vấn đề do ghép nối phần cứng mới hơn, như ổ lưu trữ với khả năng cao hơn, với các bo mạch chủ cũ hơn.

Bộ lưu trữ

Hệ điều hành được cài trên ổ đĩa lưu trữ, nên việc không tải được hệ điều hành có thể là dấu hiệu của vấn đề với ổ đĩa. Có vài cách để tìm ra các vấn đề về lưu trữ. Chúng ta sẽ bắt đầu với lệnh khởi động.

Lệnh khởi động, hoặc ưu tiên khởi động, là lệnh máy tính quét tìm các tuỳ chọn lưu trữ có sẵn và quyết định nên ưu tiên cái nào. Nếu ổ đĩa hệ điều hành không phải là lệnh cao nhất trong lệnh khởi động, có thể là do nó không được tải đúng. Điều chỉnh cài đặt này cho phép bạn khởi động từ một ổ đĩa hoặc ổ lưu trữ bên ngoài, điều này có thể có ích cho những việc như cập nhật BIOS được đề cập bên trên. Điều này cũng có thể gây ra sự cố nếu ưu tiên khởi động không chính xác, hoặc nếu hệ thống của bạn không phát hiện được thiết bị lưu trữ chính.

- **Gỡ bỏ ổ lưu trữ bên ngoài.** Để xác định lệnh khởi động, khởi động lại hệ thống, tháo gỡ bất kỳ ổ lưu trữ hay ổ đĩa flash nào, và nhập vào BIOS bằng cách nhấn phím phù hợp trong quá trình khởi động.
- **Điều hướng đến phần Khởi động của BIOS.** Tên đó có thể hơi khác biệt, nhưng bạn đang tìm phần dành cho lưu trữ, có thể gọi là menu Ưu tiên khởi động hay Lệnh khởi động.



Hình 2.42 Sự cố về phần mềm hỗ trợ gây ra cho hệ thống

Xác định ổ đĩa khởi động phù hợp

- Ổ đĩa chính nên là ổ đĩa có cài đặt hệ điều hành của bạn. Nếu bạn không biết dùng ổ đĩa nào để khởi động, bạn có thể cần phải xem ổ đĩa, như dung lượng và nhãn hiệu thường thấy trên nhãn, và thông tin này thường được nhắc đến trong BIOS. Nếu bạn không chắc ổ đĩa nào có điều hành, hãy tắt tất cả ổ đĩa trừ một ổ đĩa trong BIOS, và hãy xem hệ thống có khởi động không. Nếu không, hãy tiếp tục tiến trình loại trừ cho đến khi bạn tìm thấy ổ đĩa khởi động chính xác. Sau đó bạn có thể quay lại BIOS và tái tạo ổ đĩa lưu trữ khác. Chỉ cần đảm bảo ổ đĩa với hệ điều hành của bạn đang nằm ở đầu danh sách ưu tiên.

Lưu thay đổi.

- Một khi bạn đã được ưu tiên lệnh khởi động, lưu thay đổi và thoát ra.
- Nếu BIOS không phát hiện được ổ đĩa, có nghĩa là ổ đĩa có hệ điều hành không có trong menu lệnh khởi động, bạn có thể đang gặp vấn đề của ổ đĩa hoặc cách nó được cấu hình.
- Nếu bạn đang sử dụng lưu trữ dạng PCIe, như là ổ cứng thể rắn NVMe, có thể xảy ra vấn đề nếu cài đặt không được cấu hình phù hợp. PCIe là kết nối nối tiếp cho phép chipset và CPU kết nối và giao tiếp với phần cứng được cài đặt vào bo mạch chủ của bạn. Có một lượng khối lượng giới hạn "dòng" PCIe (Các kênh gửi và nhận dữ liệu, cần được phân giải phù hợp trong phần cứng sử dụng phần cứng sử dụng, bao gồm các giải pháp mở rộng và lưu trữ.
- Nếu đặt không đúng có thể làm giảm hiệu năng hoặc gây ra các vấn đề về tính phù hợp. Điều này cần đáng lưu tâm hơn khi mới đầu chế tạo máy tính không khởi động thành công, hoặc khi thêm phần cứng mới vào hệ điều hành cũ hơn, vì phân bổ làn không mong muốn sẽ thay đổi mà không cần cài đặt hoặc gỡ bỏ phần cứng.
- Ngoài ra, hãy cân nhắc xem có phải là do bo mạch chủ hỗ trợ chế độ khởi động phù hợp cho ổ cứng thể rắn. Nếu bạn sử dụng ổ lưu trữ NVMe M.2 hoặc thẻ bổ sung, ví dụ như, bo mạch chủ/BIOS có thể không có khả năng khởi động từ định dạng mới hơn. Có thể cần cập nhật BIOS để cài UFI mới hơn với hỗ trợ khởi động NVMe, hoặc thay đổi sang chế độ khởi động khởi động UPUI để sử dụng ổ đĩa mới. Hầu hết các bo mạch chủ hiện đại có khe M.2 sẽ không gặp phải vấn đề này, nhưng nếu bạn đang làm việc với

phần cứng cũ, cần phải xem các lựa chọn này trong phần khởi động của BIOS, hoặc cập nhật lên phiên bản mới nhất của phần mềm bo mạch chủ.

Tham khảo tài liệu về bo mạch chủ của bạn để tìm hiểu chính xác cách bo mạch chủ của bạn xử lý phân bổ PCIe và liệu nó có tương thích với UEFI hay không.

Tìm hiểu thêm về PCIe, UEFI và Lưu trữ

- Nếu bạn đang sử dụng ổ đĩa PCIe, như là NVMe SSD, có thể gây ra vấn đề nếu cài đặt không cấu hình phù hợp. PCIe là kết nối nối tiếp cho phép chipset và CPU kết nối và giao tiếp với phần cứng được cài đặt vào bo mạch chủ của bạn. Có một lượng khối lượng giới hạn "dòng" PCIe (Các kênh gửi và nhận dữ liệu, cần được phân giải phù hợp trong phần cứng sử dụng phần cứng sử dụng, bao gồm các giải pháp mở rộng và lưu trữ.
- Nếu đặt không đúng có thể làm giảm hiệu năng hoặc gây ra các vấn đề về tính phù hợp. Điều này được xem xét nhiều hơn khi ban đầu xây dựng một máy tính chưa bao giờ khởi động thành công hoặc khi thêm phần cứng mới vào hệ thống cũ, vì nó không thể phân bổ làn đường sẽ thay đổi mà không cần cài đặt hoặc gỡ bỏ phần cứng.
- Ngoài ra, hãy cân nhắc xem có phải là do bo mạch chủ hỗ trợ chế độ khởi động phù hợp cho ổ cứng thể rắn. Nếu bạn sử dụng ổ lưu trữ NVMe M.2 hoặc thẻ bổ sung, ví dụ như, bo mạch chủ/BIOS có thể không có khả năng khởi động từ định dạng mới hơn. Có thể cần cập nhật BIOS để cài UFI mới hơn với hỗ trợ khởi động NVMe, hoặc thay đổi sang chế độ khởi động khởi động UPUI để sử dụng ổ đĩa mới. Hầu hết các bo mạch chủ hiện đại có khe M.2 sẽ không gặp phải vấn đề này, nhưng nếu bạn đang làm việc với phần cứng cũ, cần phải xem các lựa chọn này trong phần khởi động của BIOS, và / hoặc cập nhật lên phiên bản mới nhất của phần mềm bo mạch chủ.
- Tham khảo tài liệu về bo mạch chủ của bạn để tìm hiểu chính xác cách bo mạch chủ xử lý phân bổ PCIe và liệu nó có tương thích với UEFI hay không.

Sự cố phần cứng

- Nếu hệ thống của bạn đã khởi động thành công trong quá khứ, nhưng BIOS không còn phát hiện ổ đĩa lưu trữ, bạn có thể xem xét vấn đề với chính ổ đĩa đó.
- Trong trường hợp này, đã đến lúc khắc phục sự cố phần cứng, điều này sẽ liên quan đến việc mở hệ thống của bạn.
- Trước khi làm như vậy, hãy chắc chắn rút cáp nguồn điện, đảm bảo bạn biết cách an toàn nhất để mở vỏ máy và lưu ý nếu làm việc trên một hệ thống được xây dựng sẵn mà bạn có thể vi phạm bảo hành. Kiểm tra với nhà sản xuất hệ thống của bạn nếu điều đó làm bạn lo ngại.
- Khi hệ thống của bạn đang mở, hãy kiểm tra xem các dây cáp được gắn vào ổ lưu trữ của bạn có được kết nối đúng cách không và có bị lỏng không. Nếu bạn sử dụng ổ đĩa M.2, hãy kiểm tra xem nó được cài đúng vào khe cắm của bo mạch chủ không.
- Nếu mọi thứ có vẻ ổn, có lẽ đến lúc xóa bỏ lưu trữ và thử nghiệm với hệ thống khác mà bạn biết có thể hoạt động được. Sẽ quá tốt nếu bạn cài ổ đĩa vào hệ thống chức năng khác để thử nghiệm. Nếu không, bộ điều hợp USB sẽ cho phép bạn cắm ổ đĩa vào cổng USB của một hệ thống khác để kiểm tra xem ổ đĩa có được phát hiện không. Điều này sẽ cho phép bạn xem liệu một hệ điều hành khác có thể phát hiện ổ đĩa hay không và chạy kiểm tra chẩn đoán bằng các công cụ như Windows Disk Utility hoặc Intel® Solid

State Drive Toolbox để xác định trạng thái của ổ đĩa.

- Nếu thiết bị lưu trữ vẫn không được phát hiện, ngay cả trên hệ thống khác biệt, có thể là ổ đĩa đã hư. Nếu ổ đĩa không còn hoạt động, có lẽ đến lúc bắt đầu tìm thiết bị thay thế mới.

CMOS

Mặc dù đó không phải là một sự cố phổ biến, đôi khi các sự cố về pin CMOS có thể ngăn hệ thống của bạn khởi động đúng cách.

Pin bán dẫn CMOS (bổ sung kim loại oxit bổ sung) trên bo mạch chủ của bạn là một con chip chạy bằng pin lưu trữ thông tin hệ thống thiết yếu như cài đặt phần cứng cơ bản và ngày. Sự thất bại của CMOS thường được biểu thị bằng đồng hồ liên tục đặt lại hoặc thông báo lỗi BIOS liên quan đến CMOS. Tuổi thọ của các loại pin này thường là khoảng một thập kỷ trong các điều kiện sử dụng thông thường, nhưng điều này có thể khác nhau. Nếu bạn sử dụng bo mạch chủ cũ hoặc đã qua sử dụng, cần kiểm tra kỹ xem pin có hoạt động tốt hay không. Chúng có giá phải chăng, và quá trình thay thế thường đơn giản.

- **Tìm pin.** Xác định vị trí CMOS trên bo mạch chủ của bạn (nó có pin màu bạc, phẳng, hình đồng xu.) Nếu bạn gặp khó khăn trong việc tìm kiếm nó, hãy tham khảo tài liệu bo mạch chủ của bạn.
- **Lắp lại pin.** Trước khi thử thay pin khác, hãy rút pin ra và lắp lại Việc tháo pin khá đơn giản. Có một chốt hoặc kẹp giữ nó tại chỗ, nhưng thông thường chúng có thể được gỡ bỏ bằng tay hoặc nhẹ nhàng bằng tuốc nơ vít, và thay thế theo cách tương tự.
- **Tháo và thay pin CMOS.** Nếu nối lại không khắc phục được sự cố, hãy thử thay thế. Pin CMOS phổ biến nhất là CR2032, nhưng khi bạn tháo pin, hãy chắc chắn rằng bạn lưu ý các tính năng của nó để tìm một sự thay thế giống hệt nhau.
- **Khởi động hệ thống của bạn.** Sau khi bạn đã nối lại hoặc thay pin thành công, hãy khởi động lại hệ thống của bạn và nhập vào BIOS. Sau đó, bạn sẽ muốn cài đặt ngày giờ, lưu và thoát.

Phần cứng Khác

Ngoài dung lượng lưu trữ, có thể các phần cứng khác gây ra lỗi không khởi động được, đặc biệt nếu được thông báo bằng thông báo lỗi. Nó có giá trị kiểm tra tất cả hệ thống cáp của bạn và đảm bảo tất cả các phần cứng khác của bạn được đặt đúng vị trí nếu không có gì khác hoạt động. Bạn có thể làm theo hướng dẫn này để biết chi tiết từng bước về cách kiểm tra từng phần cứng của bạn và xem điều này có giải quyết được vấn đề không.

Thử nghiệm thêm

Nếu bạn đã thử tất cả các đề xuất trên mà vẫn bị kẹt trên màn hình BIOS, kiểm tra cấu hình phần cứng hiện tại của bạn với một bo mạch chủ mới có thể là bước tiếp theo hữu ích. Bạn sẽ cần phải cài đặt lại CPU, bộ tản nhiệt và gắn lại tất cả các bộ phận cần thiết, nhưng sẽ giúp loại bỏ vấn đề bo mạch chủ.

Kiểm tra với phần cứng thay thế luôn là điều nên làm nếu bạn có tùy chọn đó và có thể đặc biệt hữu ích nếu BIOS chỉ cho bạn hướng đến một thành phần cụ thể.

Hầu hết các sự cố máy tính đều có thể được khắc phục, nhưng nếu bạn đang xử lý một hệ thống cũ, thì có thể đã đến lúc nâng cấp. Phần cứng máy tính có thể tồn tại trong một thời gian dài khi được bảo trì đúng cách, nhưng khi công nghệ máy tính tiếp tục phát triển,

ngay cả những thành phần đáng tin cậy nhất cuối cùng cũng cần được cập nhật để có trải nghiệm người dùng lý tưởng.

Chắc hẳn bạn đang làm việc trên một chiếc máy tính, mọi thứ đang hoạt động tốt với trải nghiệm là tuyệt vời. Nhưng khi có những khó khăn về kỹ thuật, mọi thứ có thể trở nên bực bội và khó chịu. Ngay cả một cái gì đó có vẻ đơn giản, như đóng băng hoặc treo máy thì đôi khi cũng làm cho chúng ta gặp lúng túng không biết xử lý chúng như thế nào.Cách xử lý các vấn đề phổ biến nhất để khi có chuyện gì xảy ra, có thể khắc phục nhanh chóng và hiệu quả. **11 vấn đề phổ biến về sự cố máy tính và cách tự khắc phục sự cố** ngay trong giáo trình này.

Cách đối phó với màn hình xanh chết chóc Màn hình xanh chết chóc (Blue Screen OF Death) là một lỗi STOP liên quan đến Microsoft Windows. Thông thường, nó chỉ ra một vấn đề nghiêm trọng, rất có thể liên quan đến phần cứng hoặc trình điều khiển. Khi màn hình xanh xuất hiện, nó sẽ hiển thị thông tin thích hợp về sự cố. Phần thông tin quan trọng nhất là lỗi STOP, bao gồm mã lỗi cho sự cố máy tính của bạn gặp phải. Cách tốt nhất để tìm hiểu những gì đã xảy ra là thực hiện tìm kiếm trên web đơn giản cho mã lỗi này. Hãy chắc chắn rằng bạn viết nó xuống trước khi máy tính khởi động lại. Nếu bạn bỏ lỡ, bạn luôn có thể sử dụng trình xem sự kiện Windows để xem thật kỹ lỗi hệ thống.

Sửa lỗi thiếu File DLL

Một tập tin DLL về cơ bản là một chức năng duy nhất mà các nhà phát triển có thể bao gồm với các ứng dụng của họ. Các tệp này chứa các hướng dẫn cho máy tính và HĐH (hệ điều hành). Cách tốt nhất để xử lý các tệp DLL bị thiếu là dựa vào Trình kiểm tra tệp hệ thống - một tiện ích Windows tích hợp. Nó sẽ quét các tệp hệ thống trên ổ cứng chính của máy tính của bạn và kiểm tra xem có thiếu sót hay hỏng gì không. Các tập tin hoàn toàn có thể tồn tại, nhưng chúng có thể bị hỏng theo thời gian. Điều này thậm chí có thể xảy ra nếu một ổ cứng bắt đầu bị lỗi. Trình kiểm tra tệp hệ thống sẽ quét tất cả các thư mục cần thiết và sẽ thay thế hoặc sửa chữa các tệp khi cần. Bạn cũng có thể sử dụng CD cài đặt Windows hoặc cài đặt ISO để sao chép thủ công các tệp DLL cần thiết, nhưng điều này phức tạp hơn nhiều. Các bước bổ sung lại File DLL:

- **Bước 1:** Truy cập vào trang web cung cấp file DDL cho máy tính Windows 7/10.
- **Bước 2:** Trong giao diện chính của nó, các bạn điền tên file **.dll** bị thiếu trong thông báo lỗi khi cài đặt game – phần mềm vào ô "Search for your missing DLL files" sau đó bấm Enter để tìm kiếm.
- **Bước 3:** Trong danh sách kết quả tìm kiếm, bạn sẽ thấy tên file DLL của mình ngay tại mục Fileaname hãy chọn vào nó.
- **Bước 4:** Tại trang mới mở, bạn đừng vội làm gì cả vì tất cả bạn thấy hiện giờ chỉ là quảng cáo mà hãy kéo xuống tìm dòng có các thông tin như "Bits & Version – File size – Zip file size – Language – Description – Checksums…" sau đó bấm nút **Download** màu cam bên cạnh đó. Ở đây tùy file mà chúng có nhiều phiên bản phác nhau, các bạn hãy chọn một phiên bản phù hợp với phiên bản hệ điều hành Windows của mình là 32bit hay 64bit.
- **Bước 5**: Trang tải xuống sẽ mở ra, ở đây bạn hãy chờ vài giây để file tự động tải về rồi chỉ việc chọn thư mục lưu trữ. Sau khi tải file **.dll** phù hợp hoàn tất, chúng ta sẽ

tiếp tục làm công việc cuối cùng bằng cách sao chép file **.dll** đó rồi dán vào vào thư mục hệ thống qua 1 trong 2 đường dẫn sau:

C:\Windows\System32\ (dành cho Windows 32bit)

C:\Windows\SysWOW64\ (dành Windows 64bit)

Ứng dụng chạy chậm

Tình trạng chậm máy tính khiến các ứng dụng chạy kém là cực kỳ phổ biến. Tuy nhiên, đây không phải là một sửa chữa dễ dàng vì có rất nhiều yếu tố có thể góp phần làm chậm lại. Một máy tính cũng có thể bị chậm nếu ổ cứng đầy - thường thì đây là ổ cứng chính mà HĐH được cài đặt và chạy. Nhưng một ổ cứng bị hỏng hoặc gần hết tuổi thọ cũng có thể gây ra sự chậm chạp đáng kể.

Đầu tiên, bạn cần xác định chính xác những gì gây ra sự chậm lại. Cách tốt nhất để làm điều này là nhân đôi vấn đề bằng cách tắt tất cả mọi thứ và mở từng ứng dụng và xử lý từng cái một Mở Trình quản lý tác vụ Windows bằng cách giữ CTRL + ALT + Delete và sau đó chọn tùy chọn liên quan (Task Manager). Các cửa sổ Trình quản lý tác vụ sẽ xuất hiện. Hãy chắc chắn rằng bạn đang xem chương trình (Processes). Tại đây, bạn có thể thấy tất cả các ứng dụng hiện đang chạy trên máy tính của mình. Đóng các ứng dụng không hồi đáp, trong cửa sổ Task Manager bạn sẽ tìm thấy danh sách các chương trình đang chạy trên máy tính và nút End task nằm ở góc dưới cùng bên phải. Nếu muốn thoát một chương trình nào đó đang bị lỗi, không hồi đáp bạn chon chương trình đang chạy trên máy tính rồi ấn End task. Windows sẽ đóng các chương trình ngay lập tức. Khi bạn tự tin, tất cả các ứng dụng người dùng sẽ không còn chạy. Mở từng ứng dụng và công cụ của bạn và kiểm tra xem có bị chậm không. Điều này sẽ cho phép bạn tìm ra thủ phạm.

Virus máy tính

Virus máy tính và phần mềm độc hại có thể khiến PC của bạn bị mất cắp thông tin cá nhân nhạy cảm, mở cửa sau cho tin tặc đột nhập chiếm quyền điều khiển và các hành động khác có lợi cho người phát tán virut. Đầu tiên: Tải xuống chương trình diệt virus. Tiếp theo, bật chức năng cập nhật dữ liệu để phần mềm đó nhận biết được có virut mới. Và cuối thực hiện việc quyết sâu máy tính.

Lưu ý, nếu bạn không thể loại bỏ được vì gặp phải những vấn đề lớn thì việc thuê bên ngoài là cần thiết. Khởi động lại máy tính của bạn và xác minh chúng đã bị xóa. Lặp lại quy trình loại bỏ vi-rút ở chế độ an toàn (Safe mode): Đầu tiên, khởi động lại máy tính. Nhấn phím F8 để hiển thị BIOS. Chọn bắt đầu Safe mode. Và cuối cùng là chạy quét virus.

Khắc phục sự cố kết nối Internet hoặc kết nối mạng

Một vấn đề phổ biến khác có thể gây ra nhiều đau đầu là kết nối internet. Đây có thể là sự cố với bộ định tuyến hoặc thậm chí phần cứng, phần mềm liên quan đến máy tính của bạn. Khi đó, bạn thực hiện việc khởi động lại Windows xem có thể khắc phục sự cố không hoặc kết nối PC của bạn bằng cáp ethemet khác. Cuối cùng, kiểm tra cài đặt DNS/IP và cấu hình bộ định tuyến của bạn để biết các kết nối bị chặn. Nếu không, bạn hãy liên hệ trực tiếp với nhà cung cấp dịch vụ internet (ISP). Hoặc bạn liên hệ với bên cung cấp PC để được hỗ trợ.

Cách đối phó với lỗi ổ cứng

Ổ cứng không có tuổi thọ mãi mãi nõ cũng xảy ra sự cố, do vậy bạn thường xuyên sao lưu dữ liệu trên máy tính, đây là việc rất cần thiết. Bạn nên chạy chương trình chuẩn đoán trên ổ đĩa (Chkdsk) để kiểm tra tình trạng của ổ đĩa. Khi ổ cứng bị hỏng, cách duy nhất để khắc phục sự cố là thay thế nó. Bạn có thể tự làm điều này bằng cách mua và cài đặt một cái mới, hoặc bạn có thể mang máy tính của mình đến cửa hàng - nhưng nó sẽ đắt hơn nhiều. Xem thêm: Danh sách ổ cứng tốt nhất năm 2019

Khắc phục tiếng ồn lạ

Máy tính không bao giờ im lặng. Tại bất kỳ thời điểm nào, nhiều chức năng diễn ra có thể gây ra tiếng ồn. Chẳng hạn, ổ đĩa cứng và ổ đĩa quang, tạo ra tiếng ồn riêng biệt khi bật nguồn và khi chúng được sử dụng. Quạt làm mát cũng có thể tạo ra tiếng ồn khi chúng quay. Card đồ họa hoặc GPUS cũng có một quạt bật khi chúng nóng lên. Nhiều thành phần trong số này có thể tạo ra những tiếng động lạ khi chúng thất bại hoặc bắt đầu già đi. Để đối phó với những tiếng động lạ, trước tiên bạn phải cách ly vấn đề. Chỉ ra thành phần phần cứng nào tạo ra tiếng ồn, nếu có thể. Sau đó chạy một công cụ chẩn đoán hoặc đơn giản là thay thế phần cứng.

Khắc phục sự cố quá nhiệt

Khi dòng điện chạy qua các bộ phận bên trong máy tính được sử dụng, chúng nóng lên. Đó là tự nhiên. Điều này bao gồm CPU, ổ cứng, card đồ họa, nguồn điện, ổ đĩa ngoài và trong và thậm chí cả bo mạch chủ. Khi nhiệt bên trong máy tính tăng quá cao, nó có thể gây ra lỗi nghiêm trọng và thậm chí có thể làm hỏng các thành phần. Đó chính xác là lý do tại sao một bộ xử lý có quạt làm mát riêng. Điều tương tự áp dụng cho một card đồ họa hoặc nguồn điện. Các thành phần này cần phải ở trong một phạm vi nhiệt độ hợp lý. Cách tốt nhất để xử lý vấn đề quá nhiệt là theo dõi nhiệt độ bên trong vỏ máy tính hoặc khung máy tính của bạn và sau đó hành động. Nếu **CPU hoặc bộ xử lý quá nóng**, bạn có thể cần phải gắn lại chip bằng cách phủ nó bằng miếng dán nhiệt mới và lắp đặt quạt mới. Nếu đó là **GPU hoặc card đồ họa**, bạn có thể sẽ cần phải thay thế thế - nhưng trong một số trường hợp hiếm hoi, bạn có thể sửa chữa hoặc gửi lại cho nhà sản xuất để thay thế.

Nếu nhiệt độ bên trong vỏ quá nóng và nó khiến mọi thứ ngưng hoạt động - điều đó không phổ biến nhưng vẫn xảy ra. Vì thế bạn lắp đặt quạt case bên trong khung máy. Bạn cũng có thể sắp xếp lại các thành phần và phần cứng bên trong thùng máy, để có đủ không gian cho không khí vào và ra.

Ứng dụng không cài đặt

Có nhiều lý do tại sao một ứng dụng có thể không cài đặt trên máy tính của bạn. Khả năng cao nhất là máy tính và phần mềm của nó không tương thích với ứng dụng nói trên. Có các yêu cầu hệ thống tối thiểu để chạy mọi thứ từ một chương trình đơn giản đến một trò chơi chuyên sâu về phần cứng. Nếu máy tính của bạn không đáp ứng các nhu cầu này, bạn có thể gặp sự cố chậm và đôi khi ứng dụng thậm chí sẽ không chạy. Bạn nên so sánh các yêu cầu hệ thống tối thiểu cần thiết để chạy phần mềm với thông số kỹ thuật của máy tính của bạn. Nếu bạn không đáp ứng các yêu cầu đó, thì đơn giản là bạn không thể chạy chương trình mà không cần nâng cấp. Điều này là hiếm, nhưng nó có thể xảy ra. Hầu hết thời gian phần mềm vẫn sẽ chạy, nhưng nó sẽ làm rất kém. Tuy nhiên, có khả năng là nó sẽ không hoàn thành quá trình cài đặt, tuy nhiên. Trong trường hợp đầu tiên - nơi phần

mềm không tương thích với phiên bản HĐH của bạn - bạn không thể làm được gì nhiều. Bạn có thể thử và tìm phiên bản tương thích của phần mềm bạn muốn chạy hoặc bạn có thể tìm kiếm một giải pháp thay thế.

Máy tính luôn bất ngờ khởi động lại hoặc tắt

Nếu máy tính của bạn đột nhiên khởi động lại chính nó mà không có bất kỳ dấu hiệu nào, rất có thể là một cái gì đó bên trong máy tính đang quá nóng. Hầu hết các máy tính hiện đại tự động thiết lập lại hoặc tắt khi chúng phát hiện nhiệt độ cao bất thường để tránh làm hỏng bất kỳ thành phần nào quá nóng. Giả sử bạn là người dùng trung bình không bị rối với tốc độ quạt hoặc ép xung, bước tiếp theo là xác định thành phần nào quá nóng. Điều đầu tiên bạn nên làm là mở máy tính lên để bạn có thể thấy rõ tất cả các quạt, bao gồm cả quạt tản nhiệt trên CPU và quạt trên card đồ họa của bạn. Bật máy tính lên và đảm bảo tất cả các quạt đều quay. Nếu bạn nhận thấy bụi tích tụ cao trong quạt, bạn có thể loại bỏ chúng bằng cách sử dụng một bình nén khí. Ngoài ra, đảm bảo không có quá nhiều dây cáp hoặc các chướng ngại vật khác có thể chặn luồng khí từ quạt. Nếu quạt không quay hoặc bị hỏng, bạn sẽ phải thay thế nó hoặc thành phần mà nó được gắn vào.

Câu hỏi ôn tập

- Hãy nêu và khắc phục các lỗi do phần mềm gây ra cho hệ thống.
- Hãy thiết lập lại các cấu hình phần mềm cho thiết bị.

BÀI 3. TRUY CẬP MẠNG, MÁY IN MẠNG

Giới thiệu:

Truy cập mạng là khả năng của các cá nhân và tổ chức có thể kết nối bằng cách sử dụng thiết bị đầu cuối máy tính và các thiết bị khác; và khả năng tiếp cận các dịch vụ như email và World Wide Web. Các công nghệ khác nhau, với tốc độ rất khác nhau đã được các nhà cung cấp dịch vụ Internet (ISPs) sử dụng để cung cấp dịch vụ này.

Hiện nay, việc sử dụng máy in đã dần trở nên dễ dàng hơn, tuy nhiên, cài đặt máy in như thế nào để sử dụng thì không phải bất kì nhân viên văn phòng nào cũng rõ. Và trong giáo trình này chúng tôi sẽ giới thiệu cho bạn đọc cách cài máy in qua mạng.

Thông thường, một chiếc máy in sẽ có trách nhiệm in giấy tờ cho hàng loạt chiếc máy tính được chia sẻ quyền thông qua đường dẫn mạng. Như vậy, để máy tính hoặc laptop có thể gửi lệnh yêu cầu điều khiển đến máy in, các bạn cần phải thiết lập sao cho máy in có thể in qua mạng được.

1. Mục tiêu:

- Xác định được các sự cố kết nối mạng, sửa chữa được các sự cố đó
- Quản lý hoạt động in và khắc phục được các sự cố của máy in dùng chung trên mạng.

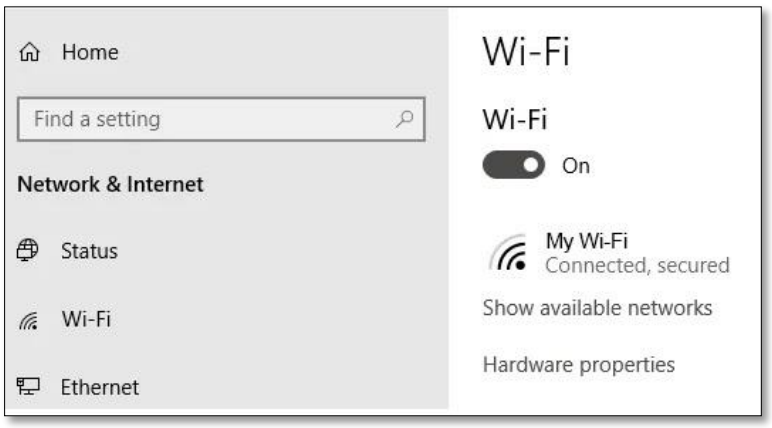
2. Nội dung bài học

2.1 Xử lý sự cố kết nối mạng

Nếu đang phải đau đầu với các sự cố kết nối mạng, chẳng hạn như không có kết nối mạng hay có biểu tượng mạng nhưng không thể truy cập Internet, ... trong giáo trình này bạn đọc cùng tham khảo để tìm hiểu cách đơn giản khắc phục sự cố kết nối mạng**.**

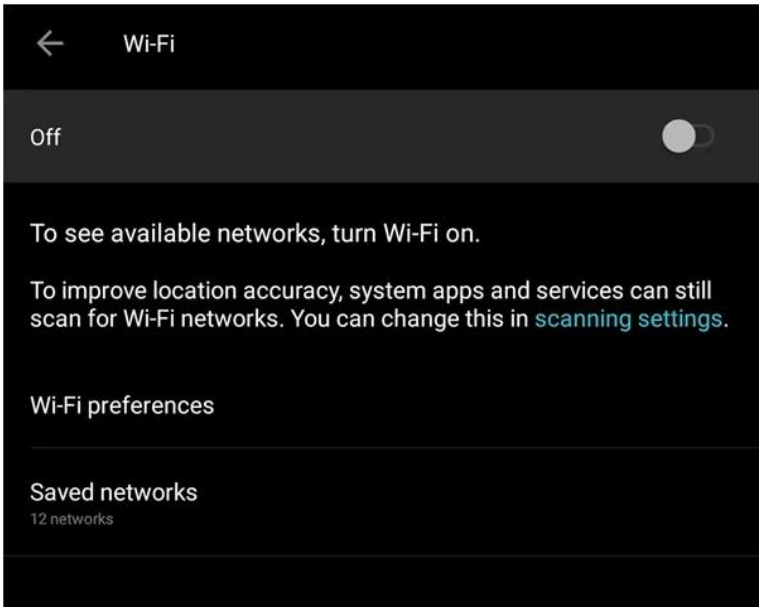
Cách 1: Kiểm tra các cài đặt Wifi

- Để khắc phục các sự cố kết nối mạng, đầu tiên kiểm tra các cài đặt Wifi bằng cách truy cập **Settings** =>**Network & Internet** =>**Wifi** và bật Wifi.



Hình 3.1 Xử lý sự cố kết nối mạng

Trên các thiết bị điện thoại và máy tính bảng, đảm bảo đã được bật Wifi để kết nối với mạng.



Hình 3.2 Xử lý sự cố kết nối mạng

Ngoài ra bạn cũng nên kiểm tra chế độ máy bay (Airplane Mode) bật hay tắt.

Cách 2: Kiểm tra điểm truy cập mạng

- Kiểm tra các kết nối mạng WAN (wide area network) và LAN (local area network). Theo thuật ngữ của layman, đây là cáp Ethernet được kết nối trên router (bộ định tuyến) và các thiết bị máy tính.

Hình 3.3 Xử lý sự cố kết nối mạng

- Nếu nghi ngờ dây cáp mạng là thủ phạm gây ra lỗi, sự cố kết nối mạng, thử thay dây cáp mới và kiểm tra xem lỗi, sự cố còn hay không.

Cách 3: Đặt router ở gần vị trí thiết bị sử dụng Internet

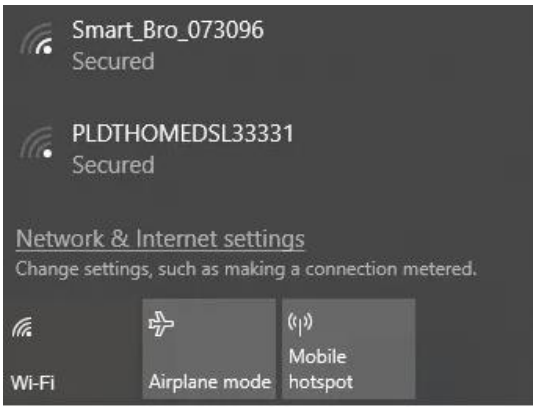
- Có thể bạn chưa biết, tường và đồ nội thất khác, lò vi sóng, ... có thể là thủ phạm, vật cản các tín hiệu mạng, gây ra các sự cố kết nối mạng. Giải pháp là di chuyển router sang vị trí khác ở vị trí trung tâm ngôi nhà hoặc gần các thiết bị bạn cần sử dụng để đạt được cường độ tín hiệu tốt nhất.

Cách 4: Khởi động lại Router

- Đôi khi giải pháp khởi động lại router (bộ định tuyến) cũng có thể giúp khắc phục các sự cố, kết nối mạng.
- Trong trường hợp nếu khởi động lại router không giúp khắc phục các sự cố, bạn có thể cân nhắc đến giải pháp reset lại router. Tuy nhiên nếu áp dụng giải pháp này sẽ khôi phục router về cài đặt gốc, đồng nghĩa với việc bạn sẽ phải cấu hình lại mọi thứ, bao gồm cả SSID và mật khẩu.

Cách 5: Kiểm tra tên và mật khẩu Wifi

- Giải pháp tiếp theo để sửa lỗi, khắc phục các sự cố kết nối mạng là kiểm tra tên mạng (hay còn gọi là SSID) và mật khẩu của mạng. Nếu như trước đây bạn có thể kết nối mạng tự động trong phạm vi của router, nhưng bây giờ thì không, có thể là do kết nối mạng đã bị thay đổi.



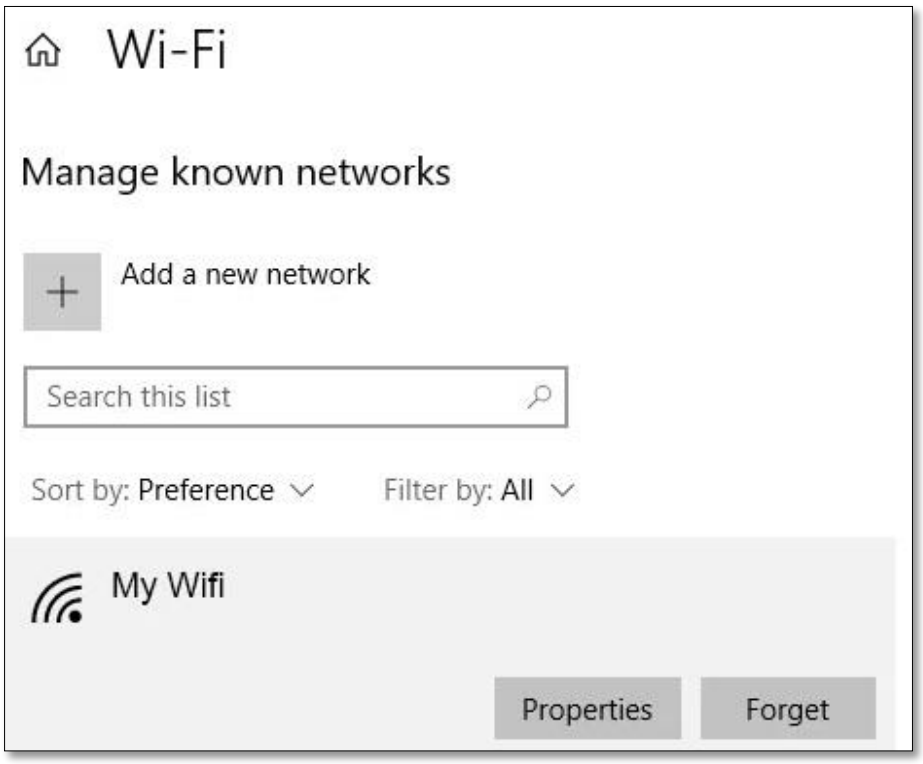
Hình 3.4 Xử lý sự cố kết nối mạng

- Hiểu một cách đơn giản có thể là do các Admin cập nhật mật khẩu hoặc SSID thành mật khẩu khác.

Cách 6: Kiểm tra các cài đặt DHCP

- Các cài đặt DHCP trên router cho phép máy tính tham gia kết nối mạng tự động. Nếu DHCP được kích hoạt, người dùng sẽ không gặp phải các rắc rối và không phải cài đặt địa chỉ IP và máy chủ DNS theo cách thủ công.

- Để chỉnh sửa cài đặt DHCP, bạn truy cập **Windows Settings** =>**Network & Internet** =>**Wifi.** Trong mục Wifi, click chọn **Manage Known Networks,** sau đó chọn một mạng và click chọn **Properties.**



Hình 3.5 Xử lý sự cố kết nối mạng

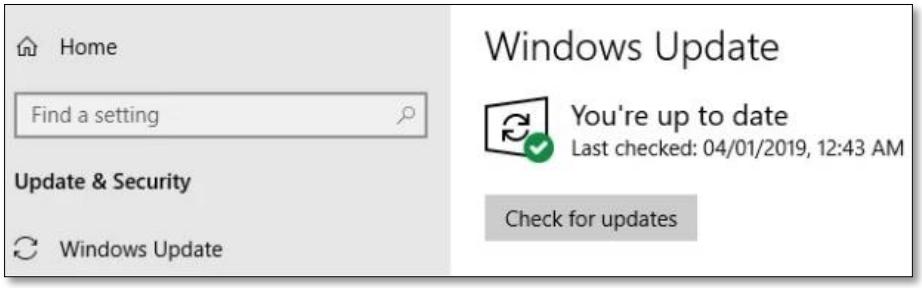
- Trong mục IP Settings, click chọn **Edit.** Từ menu thả xuống, chọn **Automatic (DHCP).**

Hình 3.6 Xử lý sự cố kết nối mạng

+ **Lưu ý:** Nếu chọn tùy chọn **Manual,** bạn sẽ phải cài đặt địa chỉ máy chủ DNS và địa chỉ IP theo cách thủ công.

Cách 7: Cập nhật Windows khắc phục sự cố kết nối mạng

- Một nguyên nhân khác gây ra các sự cố kết nối mạng có thể là do hệ thống của bạn đang có vấn đề. Rất có thể Microsoft sẽ phát hành các bản sửa lỗi, thử cập nhật máy tính Windows của bạn lên phiên bản mới nhất và kiểm tra xem lỗi mạng còn hay không.



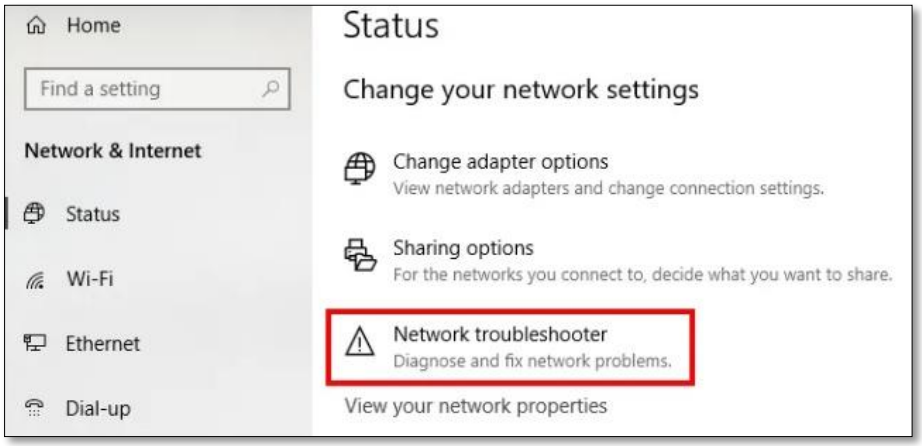
Hình 3.7 Xử lý sự cố kết nối mạng

- Truy cập **Windows Settings => Update & Security => Windows Update.** Click chọn **Check for Updates**. Nếu có các bản cập nhật có sẵn, Windows sẽ tải xuống và cài đặt các bản cập nhật này.

Cách 8: Sử dụng Windows Network Diagnostics

- Trên Windows được tích hợp công cụ có tên gọi Windows Network Diagnostics, cho phép người dùng khắc phục các sự cố kết nối mạng.

- Truy cập **Windows Settings** =>**Network & Internet** =>**Status**. Trong mục **Change Your Network Settings**, click chọn **Network Troubleshooter**.



Hình 3.8 Xử lý sự cố kết nối mạng

- Windows Network Diagnostics sẽ chạy và kiểm tra xem nguyên nhân gây ra các sự cố kết nối là do đâu và khắc phục các sự cố này.

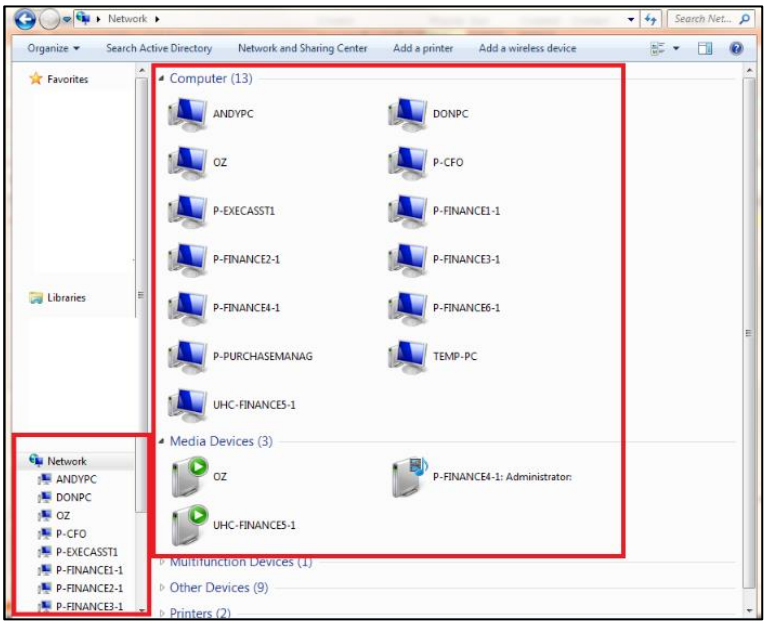
Hình 3.9 Xử lý sự cố kết nối mạng

Trong giáo trình này vừa hướng dẫn bạn 8 cách đơn giản khắc phục sự cố kết nối mạng, ngoài ra tuỳ theo tình hình thực tế sẽ có những lỗi khác và biện pháp khắc phục cũng khác.

2.2 Dọn dẹp My Network Places

Trên Windown nếu bạn mở thư mục tài liệu thì ở phía bên trái trong ngăn điều hướng, bạn bấm NETWORK, bạn sẽ thấy danh sách một số máy tính trên cùng một mạng và nếu bạn có quyền truy cập vào các PC đó thì bạn có thể mở một cái lên và xem các thư mục USER và những thứ đó trong đó.

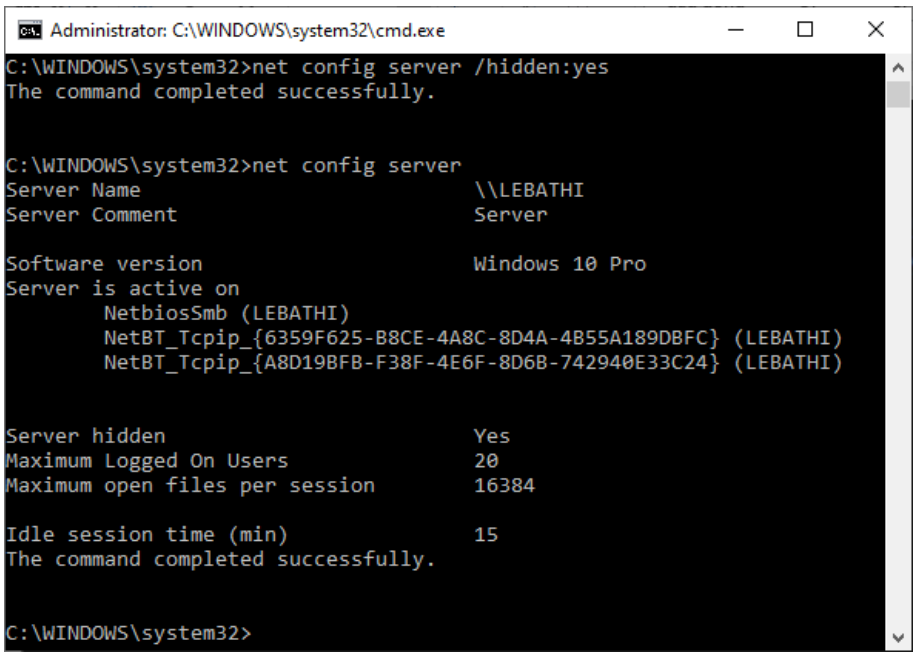
Vậy làm thế nào để loại bỏ các máy tính hiển thị trong danh sách này trên các máy tính Windown khác. Điều này rất rủi ro về bảo mật (mặc dù bạn cần một tài khoản có quyền truy cập vào các máy tính đó để xem mọi thứ trong đó).



Hình 3.10 Dọn dẹp My Network Places

"Đầu tiên, vào Menu Start -> chọn Run nhập: "cmd ". Trong dấu nhắc đợi lệnh, nhập các lệnh sau:

Net config server /hidden:yes



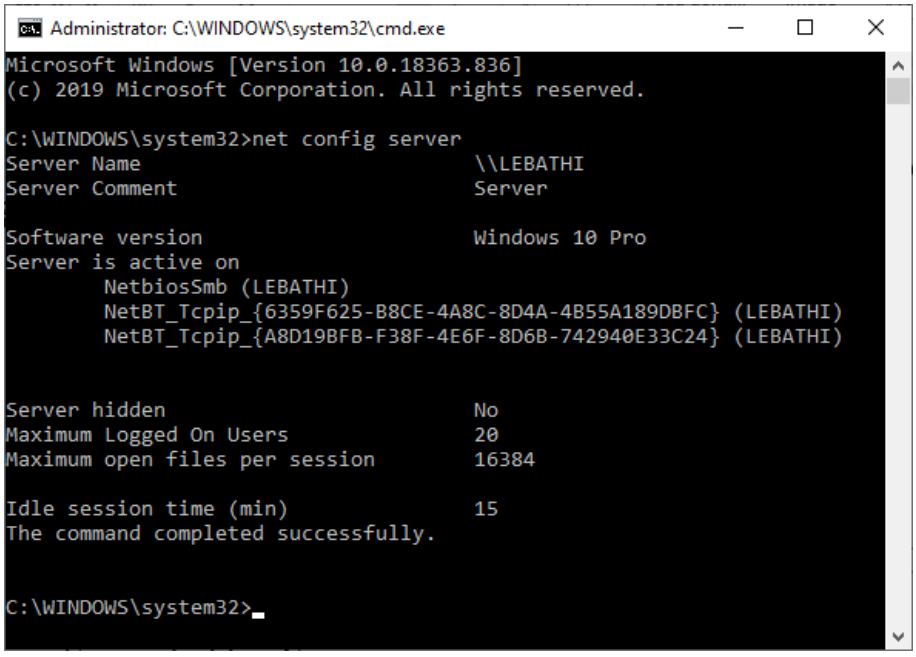
Hình 3.11 Dọn dẹp My Network Places

Lệnh này sẽ ẩn máy của bạn khỏi vùng lân cận mạng nhưng các thư mục được chia sẻ của bạn vẫn có thể được truy cập được.

Lưu ý: trong Windows Vista, bạn cần mở lệnh nhắc với tư cách Quản trị viên: Menu Start > chọn Run nhập "cmd"> bấm tổ hợp phím CTRL + Shift + Enter và nhấn Tiếp tục. Nếu không bạn sẽ nhận được thông báo này: **System error 5 has occurred** và **Access is denied**.

- Để kiểm tra xem máy tính của bạn có bị ẩn trong vùng lân cận mạng hay không, hãy nhập lệnh này trong dấu nhắc lệnh

Net config server



Hình 3.12 Dọn dẹp My Network Places

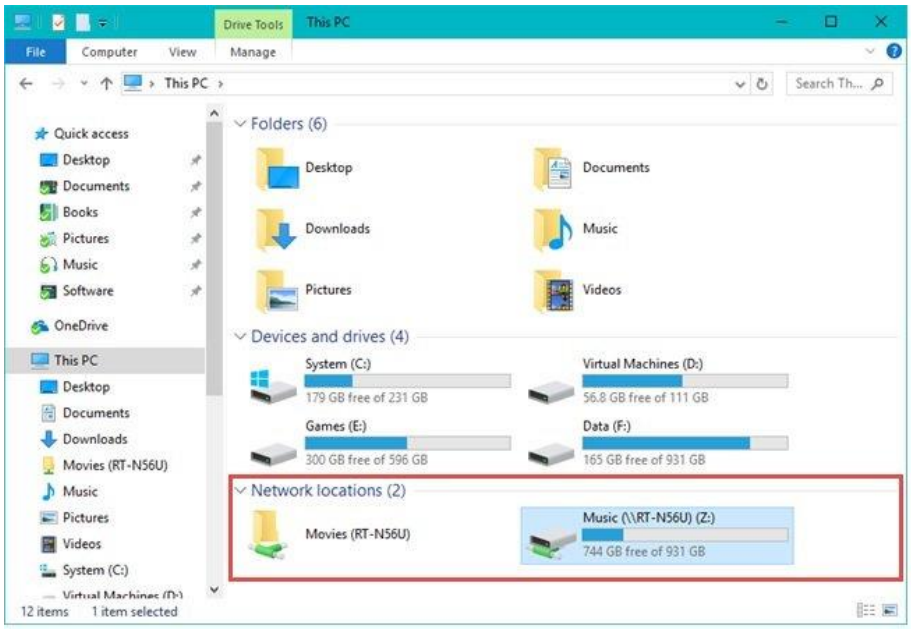
- Cách hiển thị lại máy tính của bạn trong Vùng lân cận mạng

Net config server /hidden:no

Ánh xạ ổ đĩa mạng và các thư mục chia sẽ khác là một cách tốt để giữ dữ liệu từ xa trong mạng cục bộ của bạn. Tuy nhiên, tại máy tính của bạn cũng có thể muốn xóa một số ánh xạ này và chỉ giữ lại những ánh xạ mà bạn thực sự sử dụng hàng ngày. Trong giáo trình này sẽ hướng dẫn cho bạn chính xác làm thế nào?.

Tổng cộng 8 bước

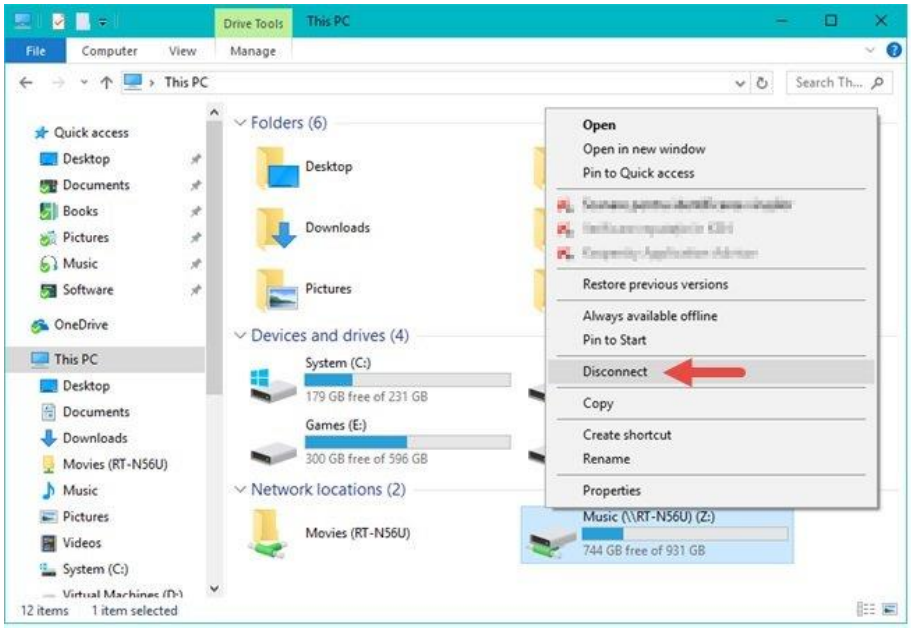
- **Bước 1**: Sử dụng Windows / File Explorer để xóa ổ đĩa mạng được ánh xạ khỏi Windows



Hình 3.13 Dọn dẹp My Network Places

+ Nếu cần xóa ánh xạ ổ đĩa đã tạo trước đó, điều đầu tiên bạn phải làm là mở File Explorer nếu bạn sử dụng Windows 10 hoặc Windows 8.1 hoặc Windows Explorer nếu bạn sử dụng Windows 7. Sau đó, ở bên trái của cửa sổ, chọn **This PC** nếu bạn sử dụng Windows 10 hoặc Windows 8.1 và Máy tính nếu bạn sử dụng Windows 7.

- **Bước 2**: Xóa ánh xạ ổ đĩa



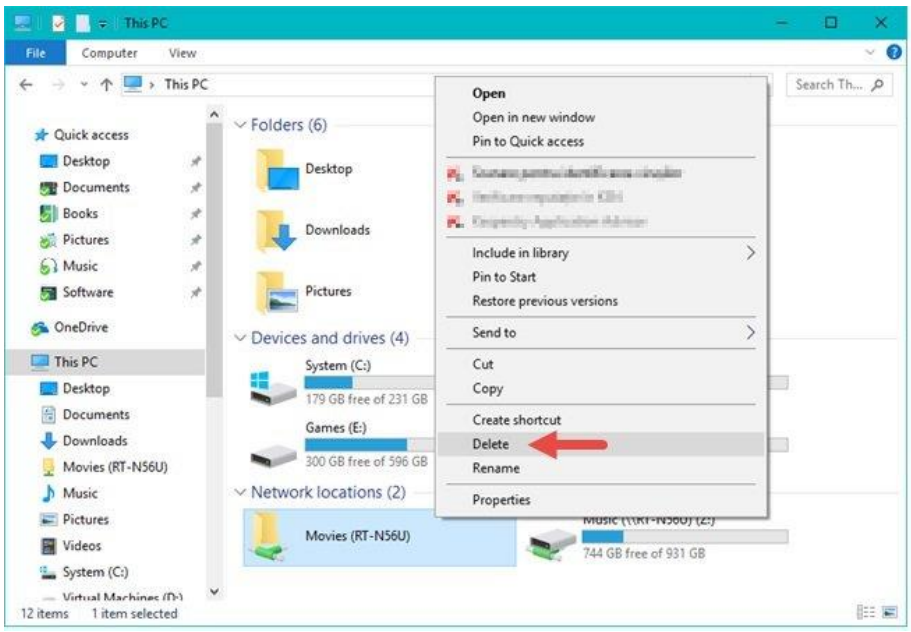
Hình 3.14 Dọn dẹp My Network Places

+ To delete a drive mapping toward a network location, right-click on it and select

Disconnect.

+ Để xóa ánh xạ ổ đĩa mạng, nhấp chuột phải vào ổ cần xoá và chọn Disconnect.

- **Bước 3**: Xóa ánh xạ ổ đĩa

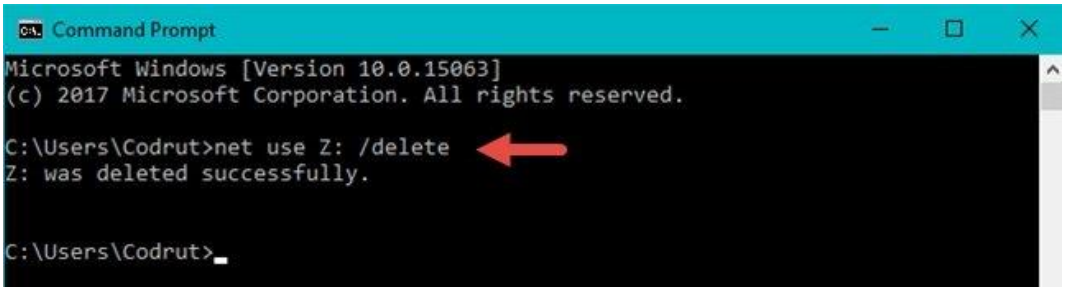


Hình 3.15 Dọn dẹp My Network Places

+ Để xóa ánh xạ ổ đĩa thư mục mạng hoặc FTP, nhấp chuột phải vào nó và chọn Delete.

+ Các ổ đĩa, thư mục ánh xạ đã xóa sẽ ngừng hiển thị. Để khôi phục chúng, bạn sẽ phải tạo lại.

- **Bước 4**: Sử dụng Dấu nhắc Lệnh để xóa ổ đĩa mạng được ánh xạ khỏi Windows



Hình 3.16 Dọn dẹp My Network Places

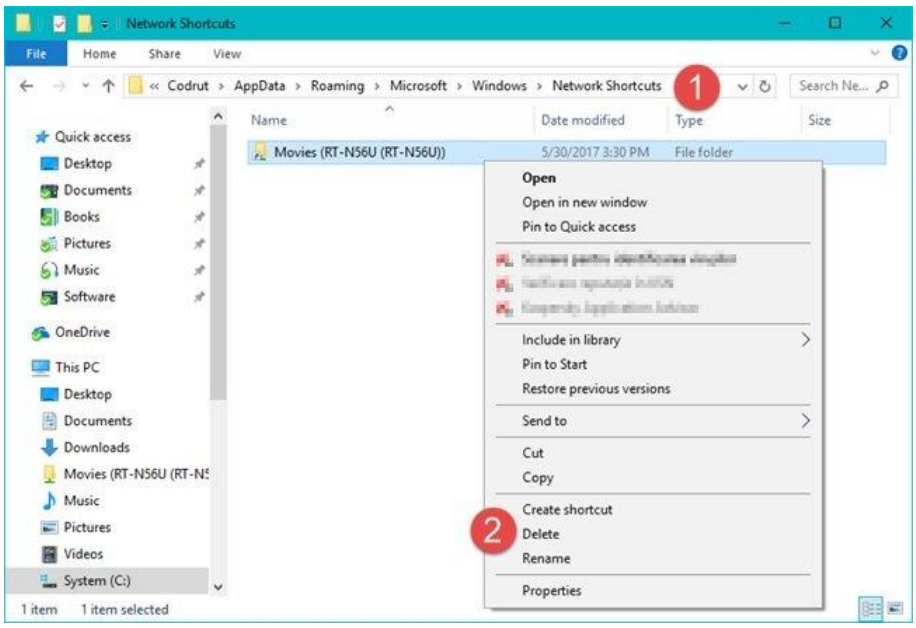
+ Một phương pháp hoạt động trong tất cả các phiên bản Windows hiện đại là sử dụng Dấu nhắc lệnh. Mở nó và gõ: net sử dụng ký tự ổ đĩa / xóa. Sau đó, nhấn Enter.

+ Ví dụ: Ta có ánh xạ ổ đĩa Z, vì vậy ta phải gõ: **net Z: /delete**.

+ Bạn được thông báo rằng ổ đĩa được ánh xạ đã bị xóa thành công và ổ đĩa mạng biến mất ngay lập tức khỏi File/Windows Explorer.

+ Một thực tế quan trọng cần xem xét là điều này chỉ hoạt động đối với ánh xạ ổ đĩa có chữ cái được gán. Đối với ánh xạ vị trí mạng như máy chủ FTP hoặc máy chủ web, lệnh này không hoạt động.

- **Bước 5**: Sử dụng Windows/File Explorer để xóa ánh xạ vị trí mạng khỏi PC của bạn bằng cách xóa lối tắt của nó.



Hình 3.17 Dọn dẹp My Network Places

+ Ánh xạ vị trí mạng thực sự là một phím tắt được lưu dưới dạng tệp trên PC Windows của bạn. Nếu bạn không thể xóa nó bằng phương pháp đầu tiên thì bạn có thể thử những cách khác.

+ Một trong số đó là sử dụng File/Windows Explorer để xóa lối tắt của nó. Mở File/Windows Explorer và điều hướng đến "C:\Users\ Your_User_Name\ AppData\ Roaming \ Microsoft \ Windows \ Network Shortcut." **Your_User_Name** là tên tài khoản người dùng Windows của bạn.

+ Trong thư mục mạng, bạn sẽ tìm thấy tất cả ánh xạ vị trí mạng. Chọn những cái bạn không còn muốn sử dụng và xóa chúng bằng cách sử dụng menu chuột phải và chọn Xóa hoặc bằng cách nhấn **Delete** trên bàn phím của bạn.

- **Bước 6**: Nếu bạn đang sử dụng Windows 7, bạn cũng phải xác nhận rằng bạn muốn xóa mục đã chọn

Hình 3.18 Dọn dẹp My Network Places

Nếu bạn đang sử dụng Windows 7, bạn cũng phải xác nhận rằng bạn muốn xóa (các mục đã chọn). Nếu bạn đang sử dụng Windows 10 hoặc 8.1, mọi thứ sẽ bị xóa ngay lập tức mà không cần xác nhận thêm.

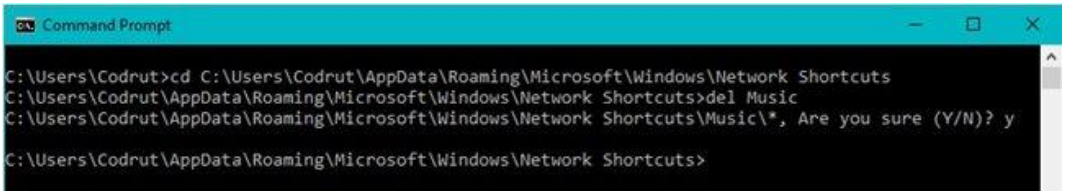
- **Bước 7**: Sử dụng Dấu nhắc Lệnh để xóa ánh xạ vị trí mạng khỏi PC của bạn bằng cách xóa lối tắt của nó

Hình 3.19 Dọn dẹp My Network Places

+ Bạn cũng có thể sử dụng Dấu nhắc lệnh để duyệt PC và xóa ánh xạ mạng khỏi nó bằng cách xóa lối tắt của nó.

+ Mở Dấu nhắc lệnh và sử dụng lệnh CD (Change Directory) để điều hướng đến vị trí của thư mục này. Nhập **CD "C: \Users\ Your_User_Name\ AppData\ Roaming\ Microsoft\ Windows\ Network Shortcut"**, trong đó **Your_User_Name** là tên của tài khoản người dùng Windows của bạn.

- **Bước 8**: Sử dụng lệnh **Del** (Xóa) để xóa lối tắt cho ánh xạ mạng



Hình 3.20 Dọn dẹp My Network Places

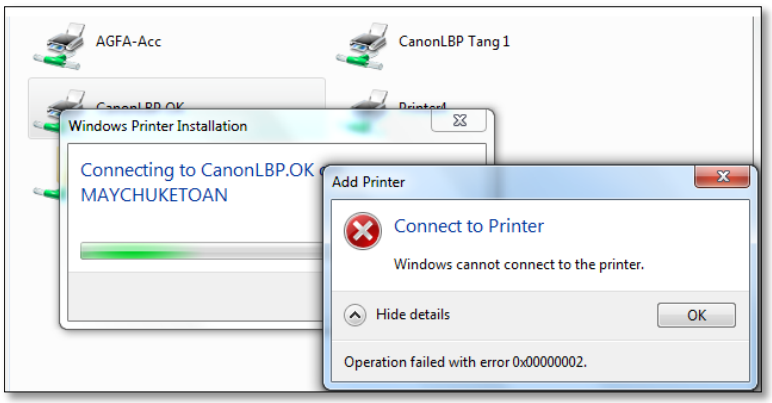
+ Sau đó, sử dụng lệnh del (Xóa) để xóa lối tắt cho ánh xạ mạng mà bạn không còn muốn nữa. Chẳng hạn, nếu bạn muốn xóa bản đồ mạng có tên Music, bạn nên chạy lệnh này: del Music. Bạn được yêu cầu xác nhận xóa.

+ Để xác nhận rằng có muốn xoá hay không bằng cách gõ chữ y. Khi bạn thực hiện việc đó, ánh xạ mạng sẽ biến mất ngay lập tức khỏi máy tính hoặc thiết bị Windows của bạn.

2.3 Sự cố trong máy in dùng chung

Để giúp bạn tìm ra lỗi kết nối máy in và cách khắc phục do trong quá trình cài đặt diễn ra giữa chừng thì bị ngừng.

Máy in không nhận lệnh, tài liệu in ra giấy trắng, hay như lỗi không nhận tín hiệu giữa máy tính với máy in. Với lỗi này, trên màn hình sẽ có thông báo lỗi **Windows cannot connect to printer**. Windows không thể kết nối với máy in.



Hình 3.21 Sự cố trong máy in dùng chung

Trong giáo trình này chia sẻ đến bạn đọc giải pháp sửa lỗi máy in không nhận lệnh vô cùng đơn giản, tiết kiệm thời gian nhất.

2.3.1. Đi tìm nguyên nhân lỗi kết nối máy in

Trước khi đi vào tìm hiểu nguyên nhân lỗi kết nối máy in và cách khắc phục bạn cần

phân biệt tình trạng và lỗi máy in đang mắc phải: Trường hợp máy vẫn báo đèn (xanh/đỏ/vàng) khi nhấn lệnh in mà không ra, lỗi này liên quan đến phần cứng hoặc hộp mực.

Cần phải tìm ra lỗi kết nối máy in và cách khắc phục được trong trường hợp khi nhấn lệnh in mà máy lại không nhận được lệnh in. Không nhận được bất kỳ tín hiệu kết nối nào từ máy tính đến máy in. Theo nhiều nghiên cứu chi tiết, người ta đã thống kê ra được một số nguyên nhân chủ yếu yếu dẫn đến việc máy in không nhận lệnh. Từ đó để đưa ra những giải pháp sửa lỗi máy in không nhận lệnh.

- Nguyên nhân thứ nhất: Máy tính bị lỗi win là trường hợp tuy không xảy ra thường xuyên nhưng bạn cũng cần lưu ý. Qúa trình lỗi win ảnh hưởng đến việc in và nhận lệnh.

+ Lưu ý: không nên bỏ sót bất kỳ chi tiết nào khi tìm kiếm nguyên nhân lỗi máy in và cách khắc phục của tình trạng máy không nhận lệnh.

+ Nguyên nhân thứ hai: Là do lỗi ở phần dây cáp kết nối: Rất nhiều trường hợp máy in đã bật và có tín hiệu màu xanh, tất cả đã sẵn sàng nhưng vẫn không thể ra bản in được. Tất nhiên khi đó bạn hãy kiểm tra dây cáp kết nối giữa máy in và máy tính, xem xem nó đã được kết nối chưa? Dây nối có gặp vấn đề gì không?

+ Nguyên nhân thứ ba: Là do chưa bật nguồn máy in: Có đôi khi bạn mất cả ngày loay hoay đi tìm kiếm những lỗi bên trong, hay những lỗi cao siêu nào khác nhưng lại bỏ qua chi tiết rất nhỏ – "nguồn của máy in". Chắc chắn rằng nguồn điện đã có, máy in đã được bật sẵn.

+ Nguyên nhân cuối cùng: Có thể do lỗi driver: Nguồn đã bật, đèn tín hiệu màu xanh, mọi thứ đã sẵn sàng nhưng máy vẫn không hoạt động. Bạn nên xe lại phần mềm, nếu chưa có hoặc lỗi hãy down và cài lại phần mềm cho máy.

2.3.2. Cách khắc phục nhanh chóng từng lỗi máy in

Lỗi Windows cannot connect to printer:

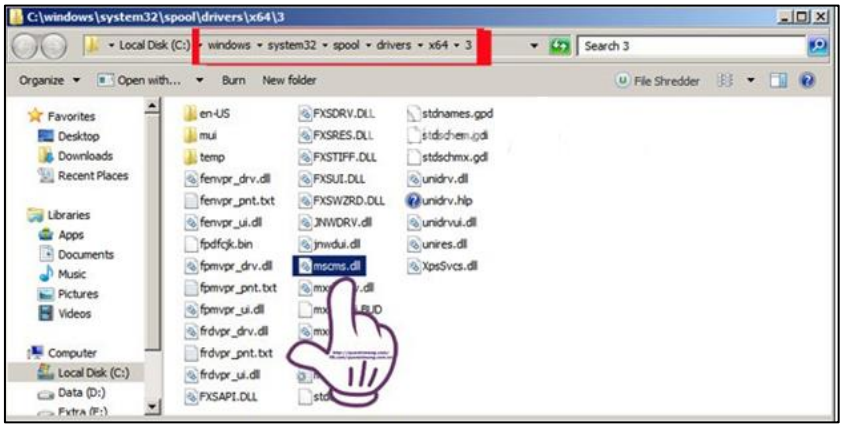
- Nếu như bạn nhìn thấy thông báo **Windows cannot connect to printer** và kèm theo mã lỗi như hình dưới, thì có thể do thiếu file mscms.dll.

Trước hết bạn truy cập theo đường dẫn sau: C:\Windows\system32\ và chọn file có tên là mscms.dll.

- Tiếp theo, chúng ta sẽ copy file mscms.dll vào thư mục trên máy tính theo đường dẫn bên dưới:

C:\Windows\system32\spool\drivers\x64\3\ nếu đang sử dụng Windows 7 64-bit .

C:\windows\system32\spool\drivers\w32x86\3\ nếu đang sử dụng Windows 7 32-bit.

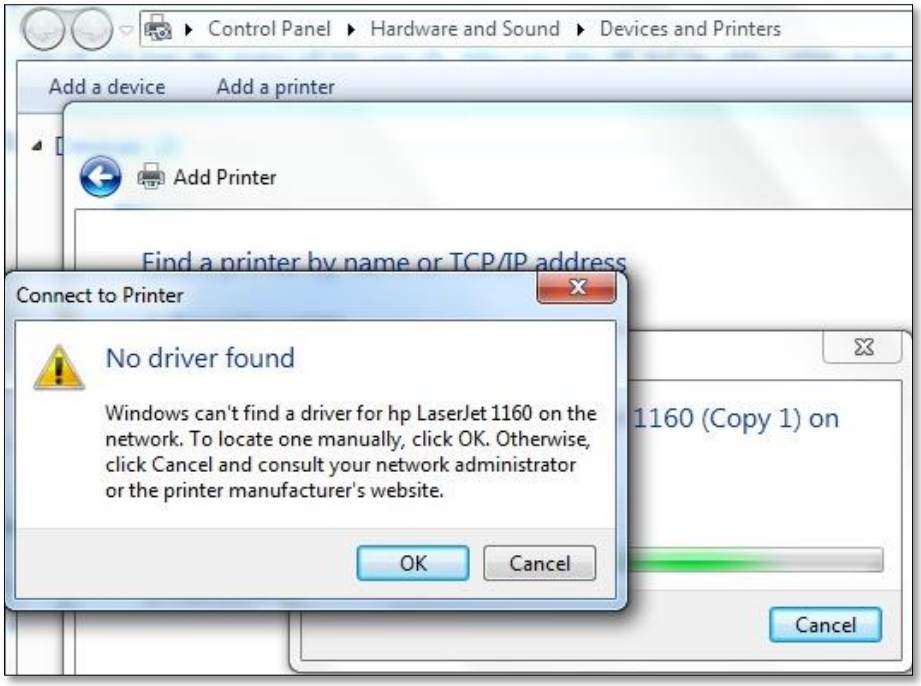


Hình 3.22 Sự cố trong máy in dùng chung

Cuối cùng bạn nên tiến hành khởi động lại máy in và thực hiện thao tác chia sẻ các máy in trong mạng LAN như thông thường. Máy tính sẽ không xuất hiện thông báo lỗi như trên và chúng ta sẽ kết nối lại được với máy in.

Kết nối máy in với Windows:

- Một máy in có thể được kết nối thông qua Ethernet hoặc Wi-Fi, hay nó có thể kết nối trực tiếp qua cổng USB với máy tính trên. Việc chia sẻ máy in trên máy chủ hay trên máy tính với máy in được kết nối qua cổng USB có thể được chia sẻ với người dùng khác trên mạng.

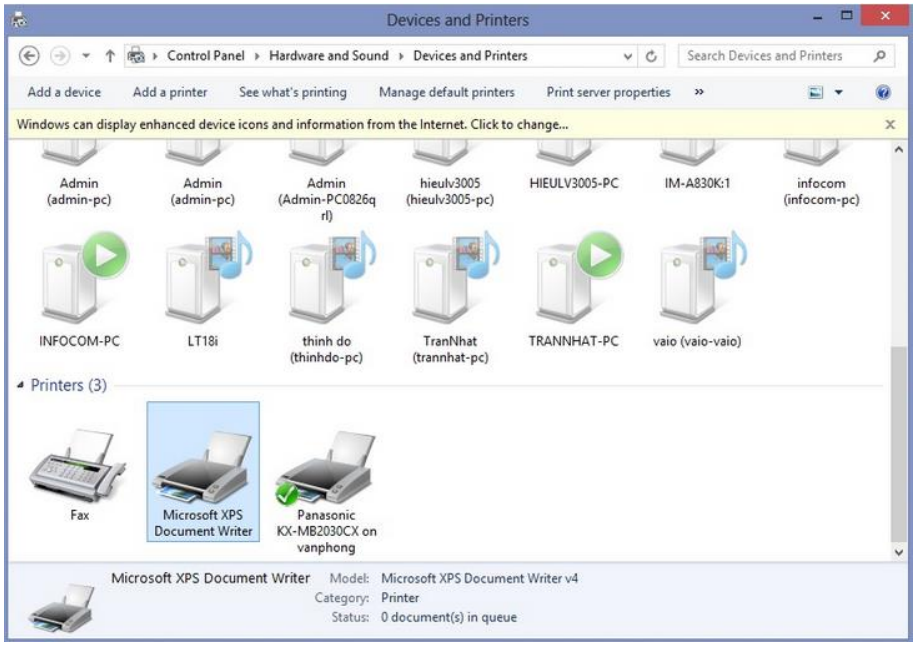


Hình 3.23 Sự cố trong máy in dùng chung

- Windows có một trình tên là Add Printer Wizard truy cập từ Devices and Printers trong Control Panel. (Đối với Windows phiên bản cũ hơn bao gồm cả Vista, phần này là mục Printers). Việc thêm máy in là khá là khác nhau về các chi tiết trên các phiên bản Windows khác nhau. Nhưng lỗi kết nối máy in và cách khắc phục các bước chung, cơ bản vẫn giống nhau.
- Khi vào liên kết Add Printer, Windows sẽ thực hiện việc tự động tìm kiếm máy in trên mạng. Khi máy in được tìm thấy, nó sẽ bật lên và bạn có thể chọn và tiến hành in.

Thêm một máy in không có trong danh sách:

- Mục kế tiếp trong cửa sổ Add Printer Wizard là Find a printer by name or TCP/IP Address (tìm máy in theo tên hoặc địa chỉ TCP/IP).



Hình 3.24 Sự cố trong máy in dùng chung

- Trên thực tế bạn có thể tìm kiếm trong các thư mục, nhưng nếu trong cửa sổ đầu tiên ở bước trên không có tên máy in thì khả năng lựa chọn này cũng không xuất hiện.
- Đối với tùy chọn "Select a printer by name", bạn có thể nhập tên máy in cần kết nối theo mẫu \\COMPUTERNAME\PRINTERNAME, trong đó COMPUTERNAME là tên của máy chủ (hoặc máy tính mà máy in được cài đặt) trên mạng. Nó có thể tìm thấy thông qua Control Panel -> System and Security -> System (trong Windows 7). Nếu không biết tên máy in (PRINTERNAME), hãy hỏi người sử dụng trực tiếp máy in đó hoặc liên hệ đến bộ phận IT trong cơ quan để biết tên.
- Nếu gặp may mắn, việc lựa chọn máy in theo cách này sẽ cho phép bạn truy cập được. Nếu vẫn không thể kết nối hoặc tên của máy in bị ẩn, bạn có thể thử giải pháp "Add a printer using a TCP/IP or hostname" (thêm máy in sử dụng giao thức TCP/IP hoặc tên máy). Lúc này bạn cần phải có địa chỉ IP tĩnh của máy. Để lấy địa chỉ IP tĩnh của máy in, bạn có thể vào Control Panel chọn Printers, nhấn chuột phải vào biểu tượng máy in cần xem, chọn Printer Properties và chọn thẻ Ports, xác định tên máy in, bạn sẽ thấy địa chỉ IP. Sau đó quay trở lại máy tính và gõ địa chỉ IP trong mục Hostname hoặc IP Address và nó sẽ tự động xuất hiện trong trường Port name (hình dưới). Nhấn Next và để nó tự động kết nối.
- Có hàng loạt các vấn đề khác có thể làm cho Windows không thể kết nối được với máy in, ngay cả khi máy tính của bạn có thể nhận dạng và xác định. Bạn có thể tìm kiếm thêm trên các diễn đàn về IT để tìm lỗi kết nối máy in và cách khắc phục hoặc có thể làm theo những bước cơ bản để xử lý!

2.4 Quản lý hoạt động in mạng

Bạn sẽ kiểm soát được việc in ấn trong văn phòng khi biết cách ***quản lý máy in trong mạng LAN***. Sau đây là những việc bạn cần làm để có thể quản lý dễ dàng hơn.

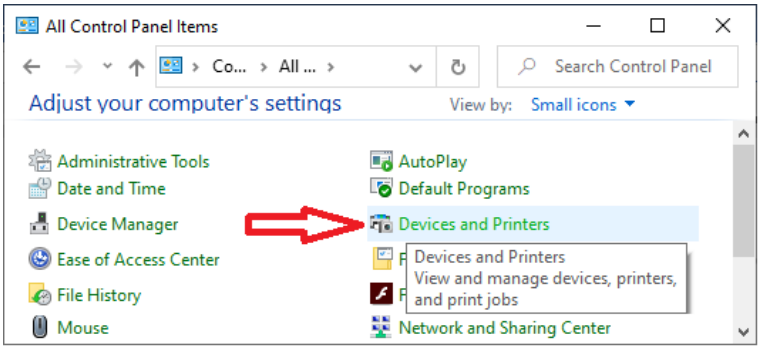
Hệ thống mạng LAN trong các văn phòng, nhà cao tầng,... thật sự rất tiện ích, vì nó có thể giúp nhiều người sử dụng được một đường truyền internet, thông qua hệ thống đó các

máy tính còn có thể sử dụng chung dữ liệu, chung ứng dụng, chung các thiết bị ngoại vi như máy in, máy scan,...

Tuy nhiên trong vài trường hợp, chính các tiện ích này cũng sẽ là nguyên nhân tạo ra rắc rối. Đơn cử, như việc chia sẻ máy in, nếu bạn không giới hạn, không biết cách quản lý thì rất khó để kiểm soát lượng in ấn mỗi ngày trong một văn phòng đông đúc.

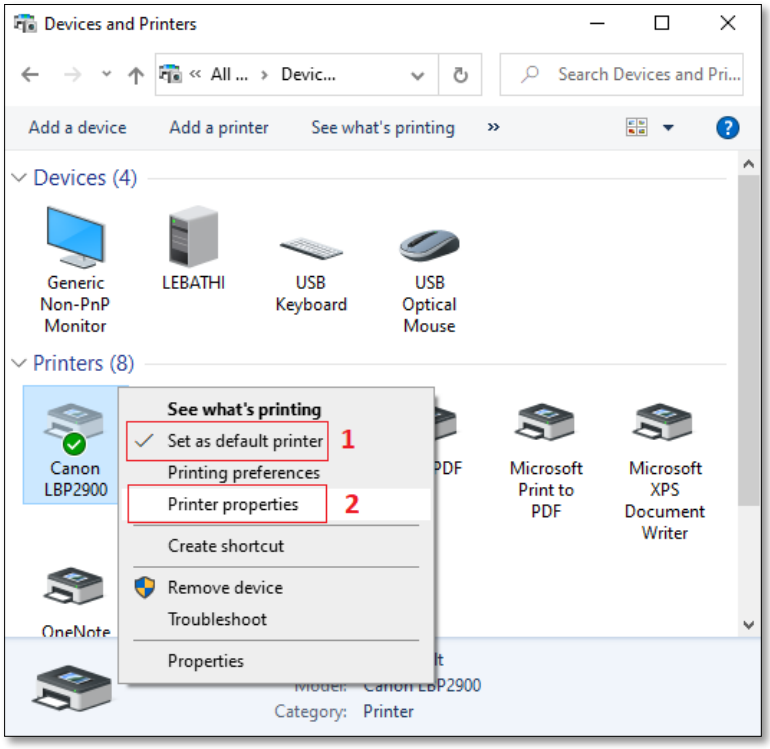
Để có thể dễ dàng thực hiện kiểm soát bạn cần biết cách quản lý ngay từ đầu. Trong giáo trình này sẽ hướng dẫn bạn quản lý máy in trong mạng LAN.

- **Bước 1:** Đầu tiên bạn cần mở Control Panel rồi chọn Devices and Printers.



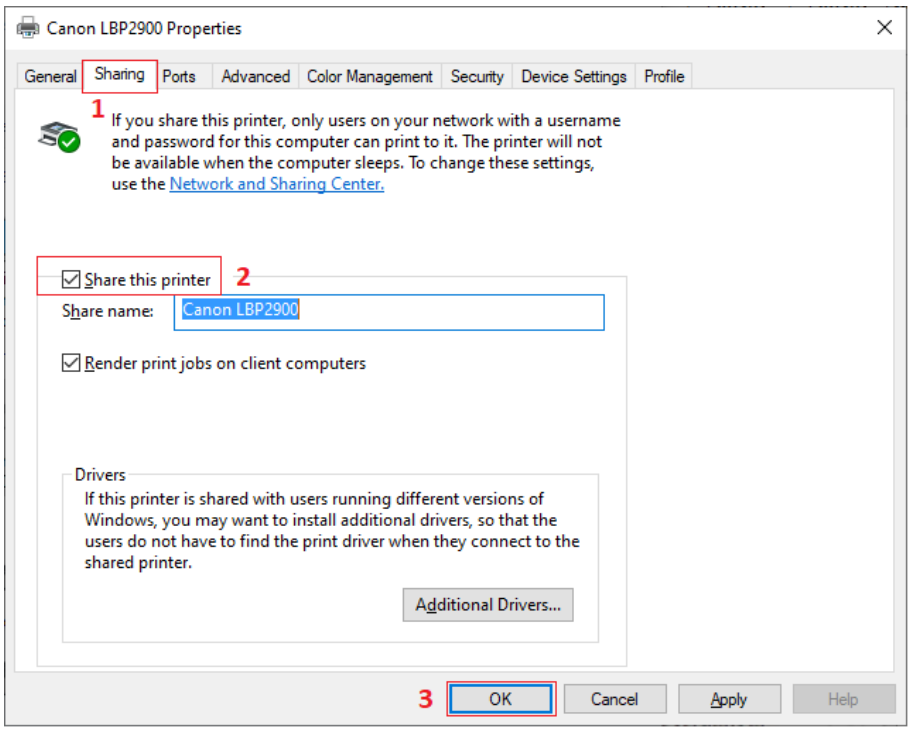
Hình 3.25 Quản lý hoạt động in mạng

- **Bước 2:** Check dòng Set as default printer => Rồi nhấn Printer properties.



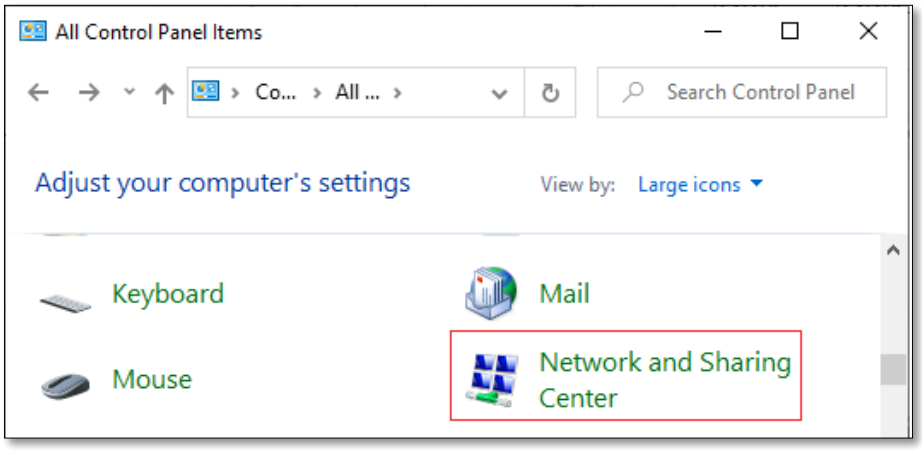
Hình 3.26 Quản lý hoạt động in mạng

- **Bước 3:** Trong hộp thoại mới mở ra, hãy chọn tab Sharing rồi check vào dòng Share this printer => Bấm OK.



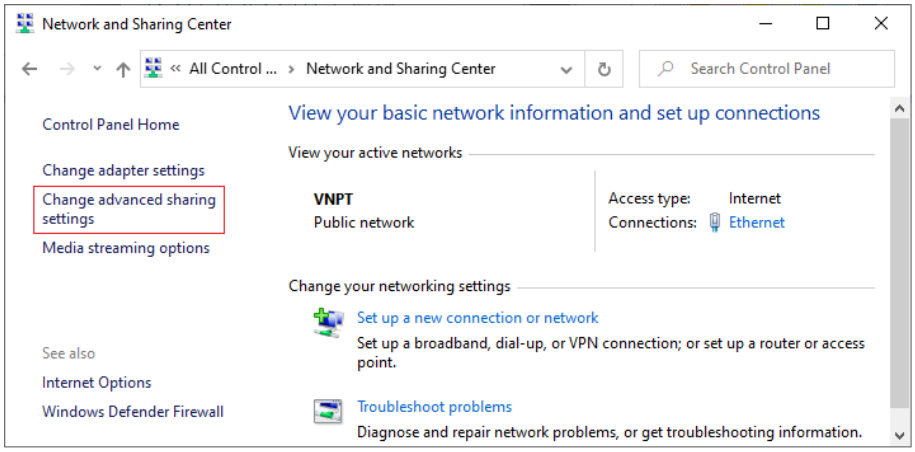
Hình 3.27 Quản lý hoạt động in mạng

- **Bước 4:** Quay lại Control Panel, nhưng lần này hãy click Network and Sharing Center.



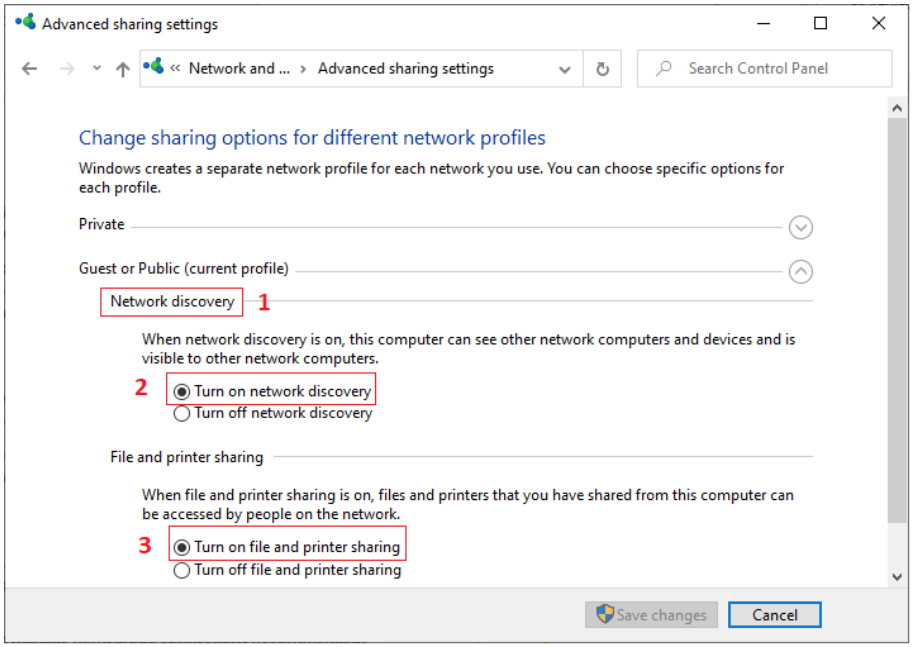
Hình 3.28 Quản lý hoạt động in mạng

- **Bước 5:** Nhấn vào Change advanced sharing settings để lưu lại thiết lập.



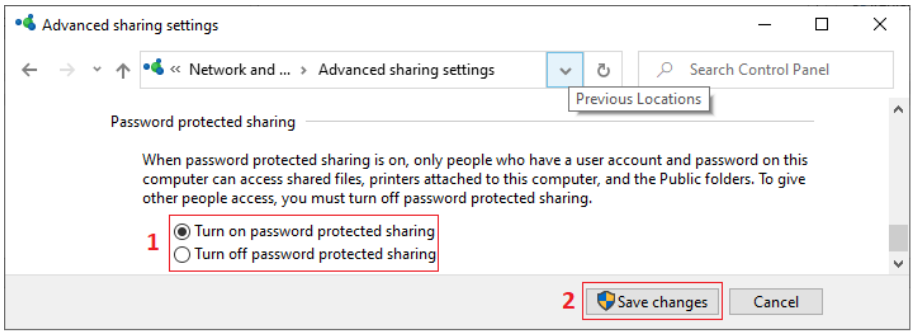
Hình 3.29 Quản lý hoạt động in mạng

- **Bước 6:** Hãy đánh dấu vào các tùy chọn như hình bên dưới.



Hình 3.30 Quản lý hoạt động in mạng

- **Bước 7:** Tiếp theo đó kéo xuống mục Password protecting sharing rồi đánh dấu vào tùy chọn Turn on password protected sharing.



Hình 3.31 Quản lý hoạt động in mạng

Bước này bạn cần lưu ý thật kỹ, lựa chọn "Turn on password protected sharing" đồng nghĩa bạn buộc người sử dụng máy in được chia sẻ phải nhập pass mới có thể in ấn. Và với thiết lập như thế những người dùng nào được bạn cấp pass mới có thể sử dụng máy in, từ đó quản lý việc in ấn dễ dàng hơn.

2.5 Xử lý sự cố máy in mạng

Xử lý sự cố lỗi 101:

Tất nhiên, máy in đôi lúc có thể không được cài đặt thành công. Nó có thể không xuất hiện trong danh sách máy in có sẵn, hoặc bạn có thể nhận được thông báo rằng Windows không thể kết nối với máy in. Bước đầu tiên bạn cần kiểm tra ngay là máy in và các máy tính muốn thêm có nằm trên cùng một mạng hay không và tính năng chia sẻ máy in của máy tính kết nối trực tiếp với máy in đã được bật chưa.

Nếu như không thấy máy in được liệt kê trong mục Add Printer Wizard hay không thể kết nối khi nhấn vào tên của nó. Lúc này bạn hãy nhấn vào liên kết có tên là “The printer that I want isn’t listed”. Việc tên máy in của bạn không nằm trong Add Printer Wizard không có nghĩa là không có máy in đó.

Bộ phận IT trong một số cơ quan thường mặc định ẩn tên của máy in trên mạng. Mặc

dù việc này là đúng về vấn đề bảo mật hoặc nguyên tắc nghiệp vụ nhưng về cơ bản nó có thể gây trở ngại cho một số người nào đó muốn tìm ra lỗi kết nối máy in và cách khắc phục có nhu cầu chính đáng.

Trong cửa sổ tiếp theo, bạn sẽ được lựa chọn thêm máy in cục bộ hoặc thêm từ mạng có dây, hay không dây hoặc qua kết nối với máy in Bluetooth. Bạn nên dùng tùy chọn thứ hai.

IP máy tính chưa thông nhau

Khi 2 máy tính chưa nhìn thấy nhau qua địa chỉ IP, chắc chắn máy tính của bạn không thể sử dụng được máy in. Lúc này bạn cần phải kiểm tra máy tính của bạn và máy chia sẻ máy in trong hệ thống mạng LAN đã thông nhau chưa.

- Kiểm tra 2 máy tính đã thông nhau chưa trong mạng LAN
  + **Bước 1:** Dùng Windows+R mở hộp thoại RUN Gõ lệnh cmd Nhấn OK.
  + **Bước 2:** Gõ lệnh ipconfig để xem địa chỉ IP máy tính chủ có kết nối trực tiếp với máy in.
  + **Bước 3:** Làm tương tự với máy của bạn để xem địa chỉ IP, Sau đó ghi nhớ, trở lại máy tính chủ gõ tiếp lệnh ping + địa chỉ máy tính của bạn để xem 2 máy tính đã thông nhau chưa. Trong trường hợp hai máy tính chưa thông với nhau bạn cần thực hiện việc chia sẻ lại.

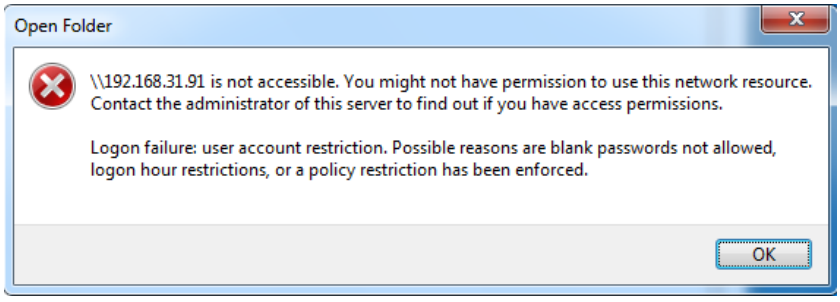
Cài Drive máy in

- Dù được chia sẻ từ máy tính khác, nhưng máy tính của bạn cần phải được cài Drive máy in đó mới có thể sử dụng.

Sửa lỗi share trong mạng LAN

Trên Windows một số máy khi truy cập vào dữ liệu đã share như máy in của máy khác trong cùng mạng LAN bị báo yêu cầu phải nhập User và password hoặc thông báo như hình:

Logon failure: user account restriction. Possible reasons are ***blank passwords not allowed***, logon hour restrictions, or a policy restriction has been enforced.



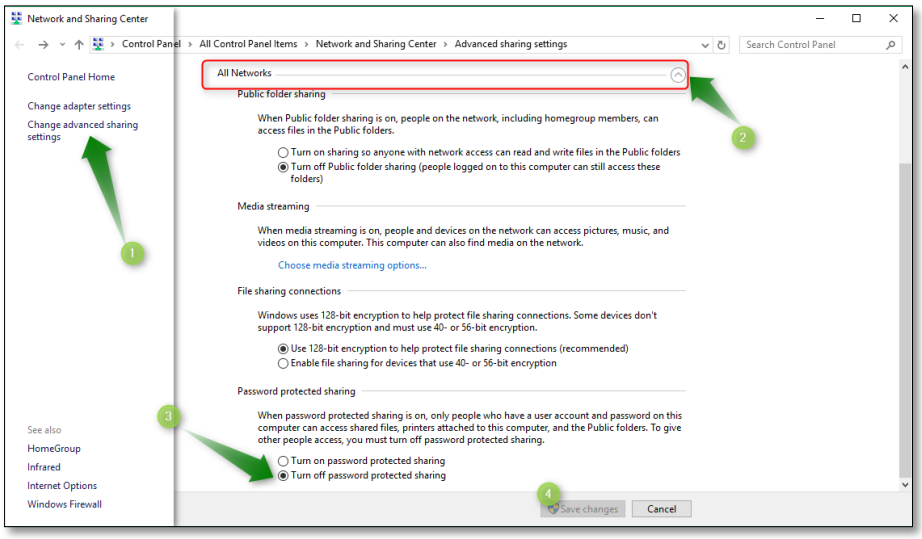
Hình 3.32 Xử lý sự cố máy in mạng

Gặp lỗi này thì bạn xử lý bằng cách:

- Lưu ý: chỉnh trên cả 2 máy: máy share và máy muốn truy cập vào.

Tắt yêu cầu password khi share trong Network Profile

- Click phải vào biểu tượng Network gần đồng hồ rồi chọn **Open Network and Sharing Center**. Tiếp tục chọn vào dòng **Change advanced sharing settings** -> tìm đến dòng All Network (ở phía gần cuối), mở ra rồi chọn dòng **Turn off password protected sharing** rồi lưu lại.

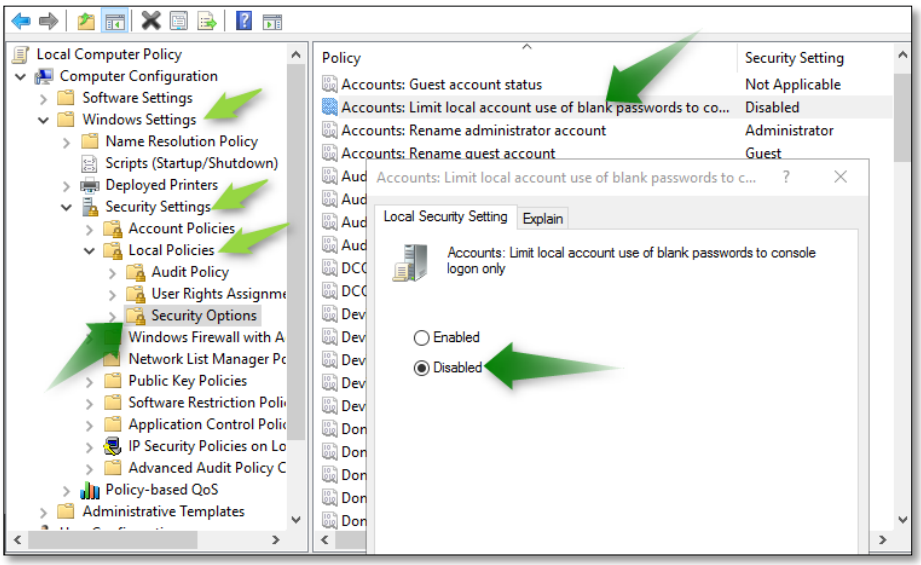


Hình 3.33 Xử lý sự cố máy in mạng

+ **Cho phép tài khoản không có password có thể truy cập trong Group Policy**

Mở Group Policy bằng cách vào Run gõ lệnh: **gpedit.msc**

+ Tiếp tục trỏ đến **Computer Configuration / Windows Settings / Security Settings / Local Policies / Security Options** rồi click đôi vào dòng **Accounts: Limit local account use of blank passwords to console login only** chọn **Disable** rồi **OK**

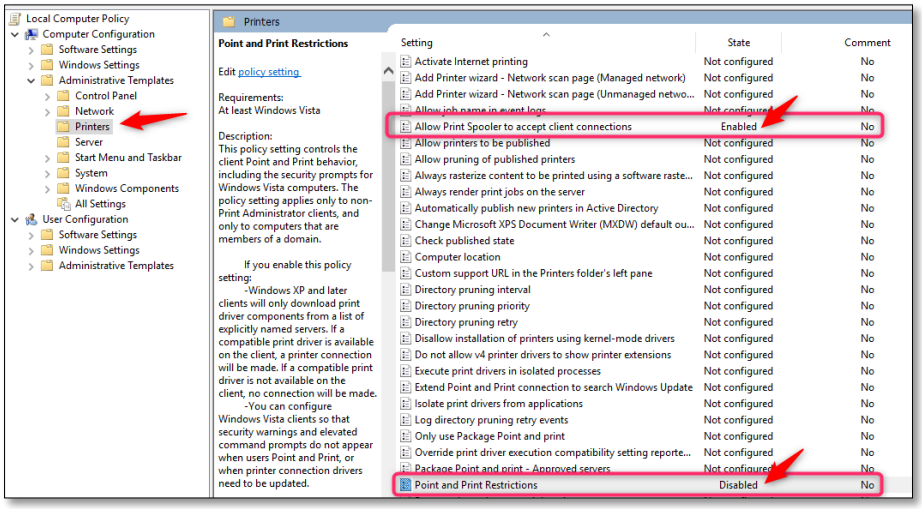


Hình 3.34 Xử lý sự cố máy in mạng

Sau khi đã chỉnh xong trong Policy thì vào Run gõ tiếp lệnh: **gpupdate /force** đợi chạy xong thì kiểm tra có thể vào share trên máy khác được chưa, nếu còn hỏi User và pass thì bạn chỉ cần nhập tên user là đã có thể vào được. Nếu vẫn chưa được thì khởi động lại máy là bạn đã có thể truy cập vào tài nguyên đã share của máy khác.

Tiếp tục chỉnh trên máy chủ máy in như sau.

- Vào Group Policy bằng cách vào Run nhập **gpedit.msc** rồi Enter. Tìm đến nhánh Computer Configuration > Administrative Templates > Printers. Chọn dòng Allow Print Spooler to accept client connections rồi chọn Enable. Tiếp tục chọn dòng Point and Print Restrictions chọn Disable



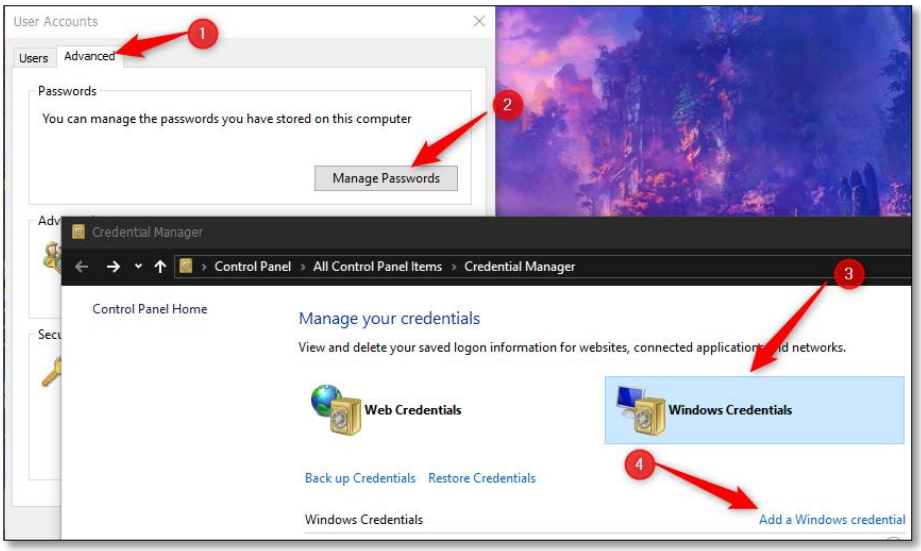
Hình 3.35 Xử lý sự cố máy in mạng

- Đa số lỗi không share được máy in xảy ra do trùng tên user trên máy chủ và máy con mà password khác nhau. Nên bạn tạo một user mới với tên và mật khẩu là: **mayin** để khỏi bị lỗi. Rồi chạy file reg sau để ẩn user mayin này khỏi màn hình đăng nhập Windows.
- File reg bạn soạn thảo có nội dung như sau:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList]
"mayin"=dword:00000000 ; Change ChangeMe to the user name you want to hide.
```

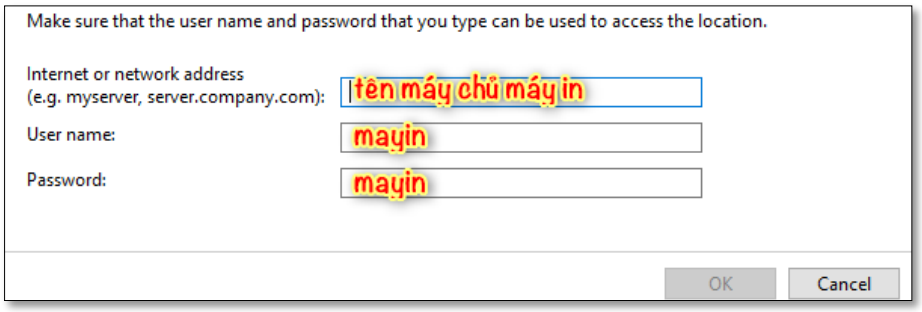
Chỉnh trên máy con

- Vào Run nhập: control userpasswords2 rồi Enter sẽ ra cửa sổ sau, chọn như hình (Trên Windows 7 thì chọn theo thứ tự: Add a local printer -> Create a new port)



Hình 3.36 Xử lý sự cố máy in mạng

- Tiếp tục nhập như hình

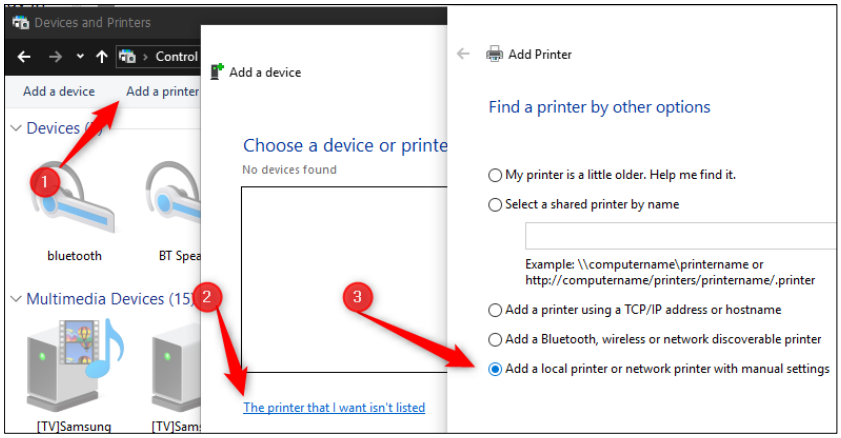


Hình 3.37 Xử lý sự cố máy in mạng

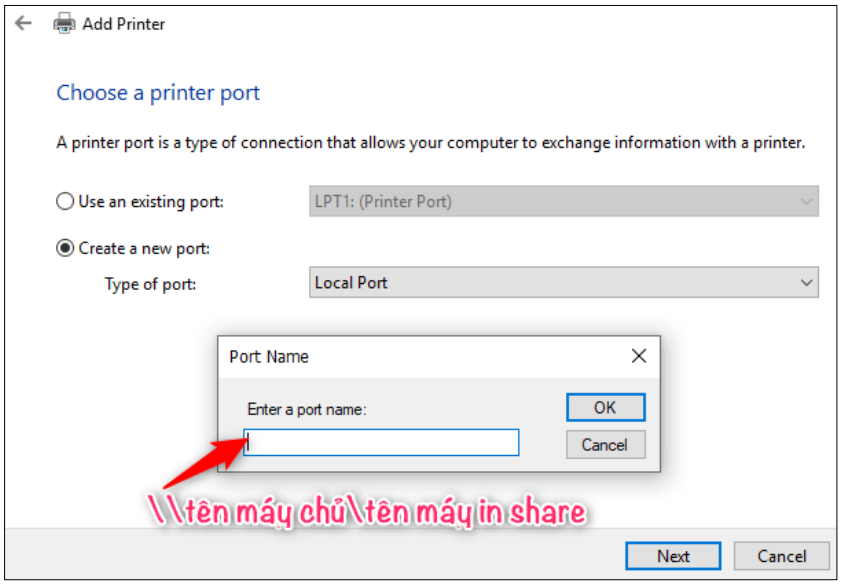
- Xong vào Run gõ **\\tên máy tính của máy chủ máy in** Enter
- Nếu vào được sẽ hiện ra tên máy tên máy in trong cửa sổ mới. Kích đôi vào tên máy in để kết nối. Nếu ở bước nhập tên máy chủ vào Run mà báo lỗi thì thử thay bằng địa chỉ IP của máy chủ, nếu vào được thì vào lại **control userpasswords2** làm như ở trên nhưng thay vì nhập tên máy chủ bạn thay bằng địa chỉ IP máy chủ.
- Lưu ý: Nếu dùng địa chỉ IP máy chủ thì trên máy chủ bạn phải đặt IP tĩnh cho máy chủ, để mỗi lần khởi động lại khỏi bị nhảy IP khác sẽ không kết nối được máy in.

Nếu khi kích đôi vào tên máy in để kết nối mà báo lỗi thì làm như sau:

Mở Control Panel chọn Devices and Printers rồi chọn như hình (trên Win 7 có thể khác)

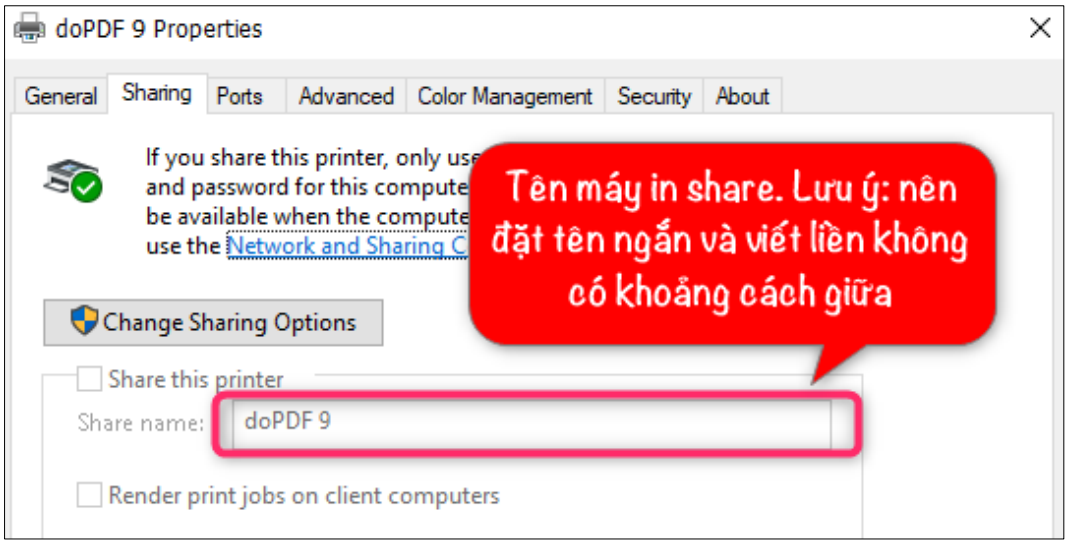


Hình 3.38 Xử lý sự cố máy in mạng



Hình 3.39 Xử lý sự cố máy in mạng

- Xem tên máy in share bằng cách trên máy chủ kích phải vào máy in



Hình 3.40 Xử lý sự cố máy in mạng

Câu hỏi ôn tập

- Xác định các sự cố kết nối mạng, sửa chữa các sự cố đó?
- Cài đặt và quản lý máy in, khắc phục các sự cố của máy in khi dùng chung trên mạng LAN.

BÀI 4. MẠNG INTERNET DÙNG CHUNG

Giới thiệu:

Internet là một hệ thống thông tin toàn cầu có thể được truy nhập công cộng gồm các mạng máy tính được liên kết với nhau. Hệ thống này truyền thông tin theo kiểu nối chuyển gói dữ liệu (packet switching) dựa trên một giao thức liên mạng đã được chuẩn hóa (giao thức IP). Hệ thống này bao gồm hàng ngàn mạng máy tính nhỏ hơn của các doanh nghiệp, của các viện nghiên cứu và các trường đại học, của người dùng cá nhân và các chính phủ trên toàn cầu.

1. Mục tiêu:

- Trình bày được các nguyên tắc của nhà cung cấp dịch vụ Internet
- Kiểm tra, khắc phục các sự cố kết nối Internet băng thông rộng.

2. Nội dung bài học

2.1 Các nguyên tắc của nhà cung cấp dịch vụ Internet.

Nhà cung cấp dịch vụ Internet hay **Nhà cung cấp dịch vụ nối mạng** (tiếng Anh: *Internet Service Provider*, viết tắt: **ISP**) chuyên cung cấp các giải pháp kết nối mạng toàn cầu (Internet) cho các đơn vị tổ chức hay các cá nhân người dùng. Các ISP phải thuê đường và cổng của một IAP. Các ISP có quyền kinh doanh thông qua các hợp đồng cung cấp dịch vụ Internet cho các tổ chức và các cá nhân.

Các loại ISP dùng riêng được quyền cung cấp đầy đủ các dịch vụ Internet. Điều khác nhau duy nhất giữa ISP và ISP riêng là không cung cấp dịch vụ Internet với mục đích kinh doanh. Người dùng chỉ cần thoả thuận với một ISP hay ISP riêng nào đó về các dịch vụ được sử dụng và thủ tục thanh toán được gọi là thuê bao Internet.

Một số ISP ở Việt Nam là VNPT, FPT, Viettel, CMC, VDC, Netnam.

Việc thực hiện hợp tác kinh doanh với tổ chức, doanh nghiệp cung cấp dịch vụ nội dung thông tin trên mạng viễn thông di động theo nguyên tắc quy định tại Khoản 1 Điều 29 Nghị định 72/2013/NĐ-CP về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng, cụ thể như sau:

- Thông qua thương lượng trên cơ sở bảo đảm công bằng, hợp lý, phù hợp với quyền, lợi ích của các bên tham gia;
- Sử dụng hiệu quả tài nguyên viễn thông và cơ sở hạ tầng viễn thông;
- Bảo đảm hoạt động an toàn, thống nhất của các mạng viễn thông;
- Bảo đảm quyền, lợi ích hợp pháp của người sử dụng dịch vụ viễn thông và tổ chức, cá nhân có liên quan;
- Cung cấp kết nối cho các tổ chức, doanh nghiệp cung cấp dịch vụ nội dung thông tin trên mạng viễn thông di động tại bất kỳ điểm nào khả thi về mặt kỹ thuật trên mạng viễn thông và thực hiện kết nối kịp thời, hợp lý, công khai, minh bạch;
- Không phân biệt đối xử về kết nối, giá cước, thanh toán, tiêu chuẩn, quy chuẩn kỹ thuật viễn thông, chất lượng mạng và dịch vụ viễn thông.

2.2 Sự cố trong dùng chung kết nối cáp quang.

Cách nhận biết báo đèn converter quang bị lỗi khi nào và cách khắc phục

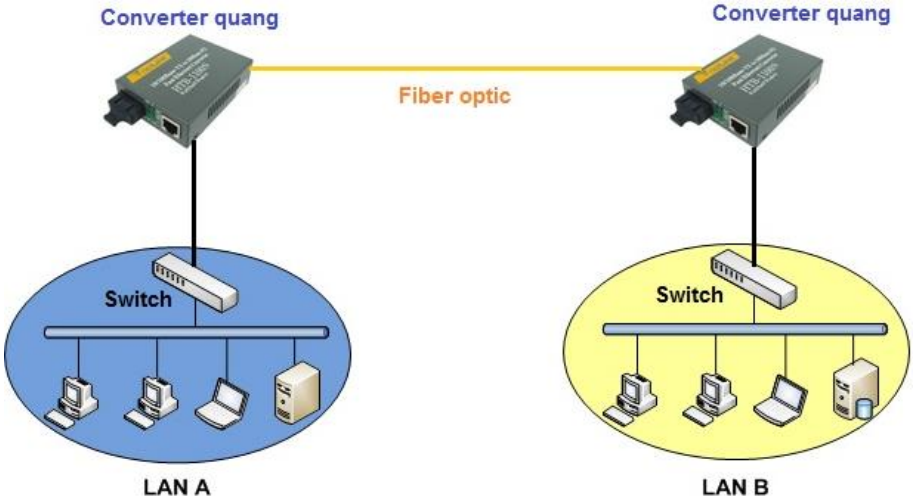
- Nắm bắt được nguyên lý hoạt động Converter quang điện có 6 đèn LED thông báo trạng thái,Những người thi công cáp quang lành nghề biết cách xem đèn trên Converter

quang điện,khi xử lý sự cố hay bảo trì hệ thống cáp quang họ không phải mất thời gian vào những sự cố đơn giản.Và có thể nắm bắt được hệ thống mạng đang làm việc ra sao và giúp ta khắc phục nhanh hệ thống mạng khi sự cố xảy ra.

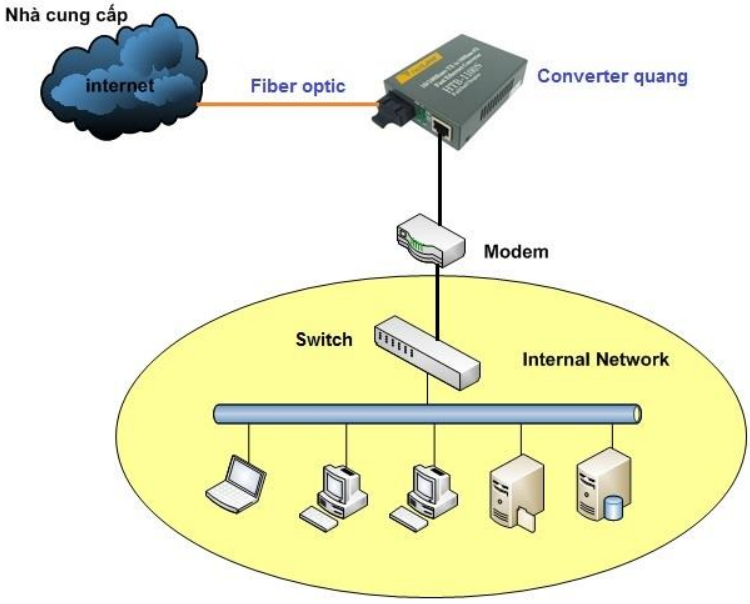
Kí hiệu trên Converter quang

- Đèn trên Converter quang được chia thành 2 hàng dọc FX và TX, 3 hàng ngang là ngõ vào, tín hiệu truyền nhận, ngõ ra. Khi hoạt động bình thường cả 6 đèn sẽ sáng với Converter quang điện 10/100, 2 đèn giữa Link/Act sáng nhấp nháy liên tục(Nháy càng nhanh tính hiệu mạng càng mạnh).
- Các kí hiệu được viết trên đèn:
  + PWR: đèn nguồn
  + Link/Activity: dữ liệu mạng truyền nhận
  + FX: Thông báo kết nối mạng cáp quang
  + TX: Thông báo mạng internet kết nối (Ethernet)
  + FDX: chế độ Full Duplex (Converter quang 2 cổng)

Hệ thống mạng Lan và internet sử dụng converter quang



Hình 4.1 Hệ thống mạng LAN sử dụng một đôi Converter quang điện

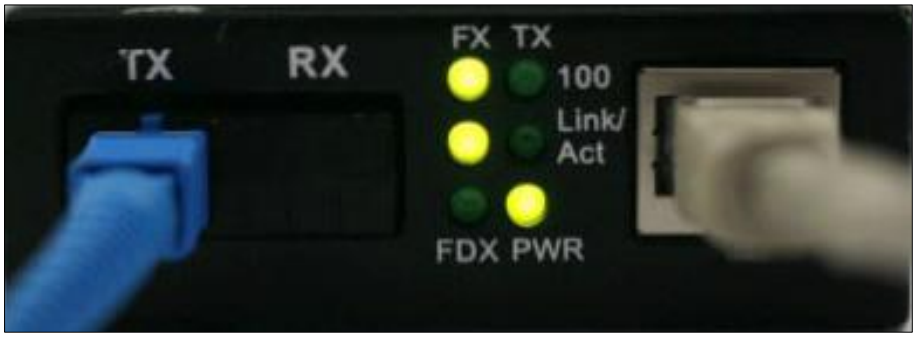


Hình 4.2 Hệ thống mạng Internet sử dụng Converter quang điện

Trạng thái trên converter quang điện 10/100M Trường hợp mất tín hiệu quang, 2 đèn Link/Act của hàng FX bị tắt: kiểm tra Dây nhảy quang nối từ Converter quang điện vào hộp phối quang (ODF quang) xem có bị đứt không. Tiếp đến ta kiểm tra đường cáp quang nối từ ODF quang điểm bên này sang ODF đầu bên kia có thể kiểm tra bằng cách dùng đèn Laser hoặc nguồn sáng mạnh soi ở một đầu để kiểm tra thông quang (Với hệ thống mạng Internet sử dụng Converter quang điện đoạn cáp quang này do nhà cung cấp dịch vụ quản lý, ta gọi cho nhân viên nhà mạng đến khắc phục đường truyền)

Hình 4.3 Converter quang - Bộ chuyển đổi quang điện 10/100 Mbps mất tín hiệu quang

Trường hợp mất kết nối LAN từ Switch đến Converter quang điện, đèn hàng TX và đèn FDX sẽ bị mất: Thử dùng cổng khác trên Switch mạng. Kiểm tra dây cáp mạng nối từ Bộ chuyển đổi quang điện vào Switch (với hệ thống mạng Internet sử dụng Converter quang điện ta kiểm tra dây cáp từ Media converter vào Modem và từ Modem vào Switch) được kết nối đúng chưa, Cáp mạng phải được cắm chắc chắn tại tất cả các kết nối. Nếu cáp được cắm tốt mà vẫn chưa có mạng ta dùng cáp mạng khác thay thế.



Hình 4.4 Bộ chuyển đổi quang điện 10/100Mbps mất tín hiệu LAN

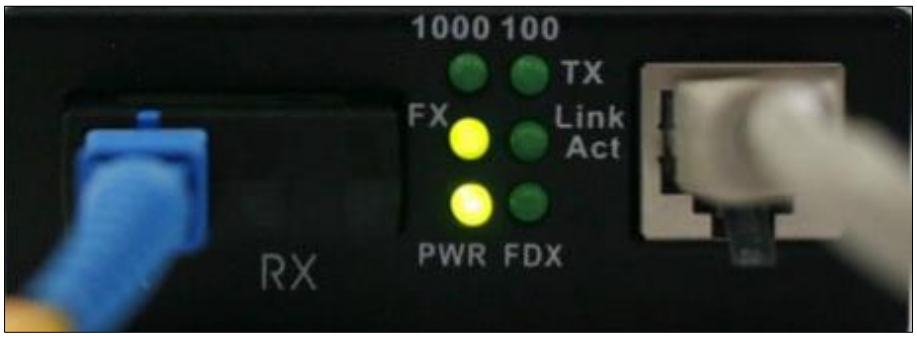
Trong trường hợp sáng đủ 6 đèn mà kết nối vẫn down: có nhiều trường hợp Bộ chuyển đổi quang điện, Modem, Switch bị treo ta cần khởi động lại. Trường hợp ta không tìm ra ngay điểm xảy ra sự cố ta chia mạng thành các đoạn nhỏ để dễ dàng xử lý.

Hình 4.5 Bộ chuyển đổi quang điện 10/100Mbps mất tín hiệu LAN

Trạng thái trên Converter quang điện 1GB Khi mất tín hiệu quang, đèn FX sẽ tắt, Converter quang điện sẽ còn 4 đèn sáng.

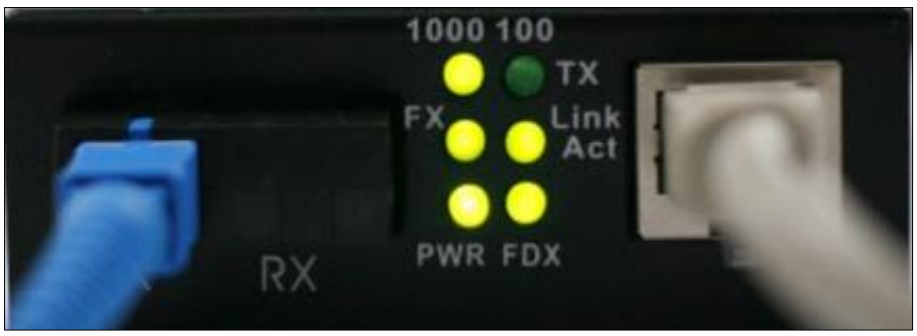
Hình 4.6 Converter quang – Bộ chuyển đổi quang điện 1G khi mất tín hiệu quang

Khi mất kết nối LAN từ Switch đến Converter quang điện 2 đèn hàng TX sẽ mất, lúc này chỉ còn FX và đèn nguồn trên Converter quang sáng



Hình 4.7 Bộ chuyển đổi quang điện 1GB mất kết nối LAN

Khi Converter quang điện sáng đủ 5 đèn mà kết nối vẫn bị mất: ta nên kiểm tra xem thiết bị như Switch hoặc Bộ chuyển đổi quang điện có bị treo không và khởi động lại, kết hợp với việc phân đoạn mạng thành những đoạn nhỏ để tìm điểm xảy ra sự cố giúp ta khắc phục nhanh hơn.



Hình 4.8 Converter quang điện 1G sáng đèn nhưng mất kết nối

- **Cách khắc phục FTTH có tín hiệu nhưng không sử dụng được dịch vụ**

Hiện nay hầu hết mọi người đều có nhu cầu sử dụng dịch vụ kết nối Internet tốc độ cao. Trong đó việc lựa chọn sử dụng dịch vụ truy nhập Internet trên cáp quang FTTH đang có xu hướng tăng nhanh.

Đầu tiên các bạn kiểm tra đèn trên bộ Media Converter để phân đoạn lỗi:

Hình 4.9 Kiểm tra đèn trên bộ Media Converter

- **Sáng đủ 6 đèn:** Kết nối tốt
- **Đèn FX, FX Link/ACT không sáng**: lỗi kết nối quang từ Converter đến phía nhà mạng, gọi nhân viên kiểm tra mạng ngoại vi.
- **Đèn TX không sáng**: lỗi dây kết nối từ cổng WAN modem-Converter, kiểm tra, cắm lại dây.
- **Không đèn nào sáng**: không có nguồn cho Converter, kiểm tra, cắm lại nguồn Converter.

Trường hợp đèn Converter sáng đủ, nhưng không kết nối được Internet, chia thành các Trường hợp sau:

- **Trường hợp *1***: *Lỗi tại modem:* 6 đèn Converter sáng, đèn WAN không sáng, đèn LAN kết nối từ máy tính – modem sáng

+ Các bạn kiểm tra cáp kết nối theo đúng mô hình: máy tính -> cổng LAN modem, cổng WAN modem -> Converter. Đảm bảo 6 đèn Media converter sáng đủ, đèn LAN cổng nối vào máy tính sáng, đảm bảo máy tính truy cập được vào modem ở địa chỉ "192.168.1.1".

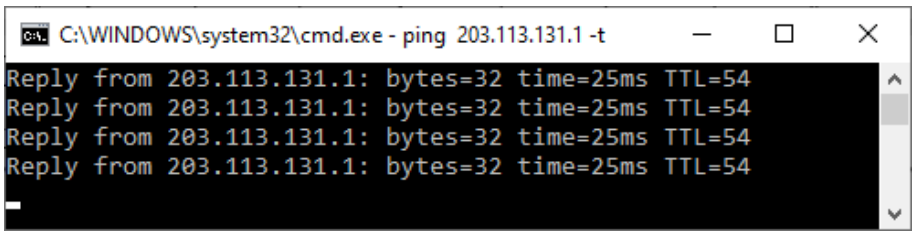
+ Bạn truy cập modem và kiểm tra cấu hình PPPoE có bị mất không:

+ Nếu mất cấu hình: Bạn cấu hình lại modem (Các thông số cần chú ý Conection type: PPPoE, Username, Password) –> khởi động lại modem–>vào modem kiểm tra lại một lần nữa cấu hình có bị mất không. Nếu bị mất –> modem không nhận cấu hình –> Nhân viên Viettel kiểm tra thiết bị modem.

+ Nếu không mất cấu hình: Bạn "reset factory default" cho modem –> cấu hình lại PPPoE –> khởi động lại modem, tắt bật lại Media Converter, đợi 1.5 -2 phút.

- **Trường hợp 2**: Lỗi từ phía máy tính bạn: 6 đèn Converter sáng, đèn WAN modem sáng, đèn LAN modem kết nối tới máy tính sáng nhưng máy tính không vào được Internet.

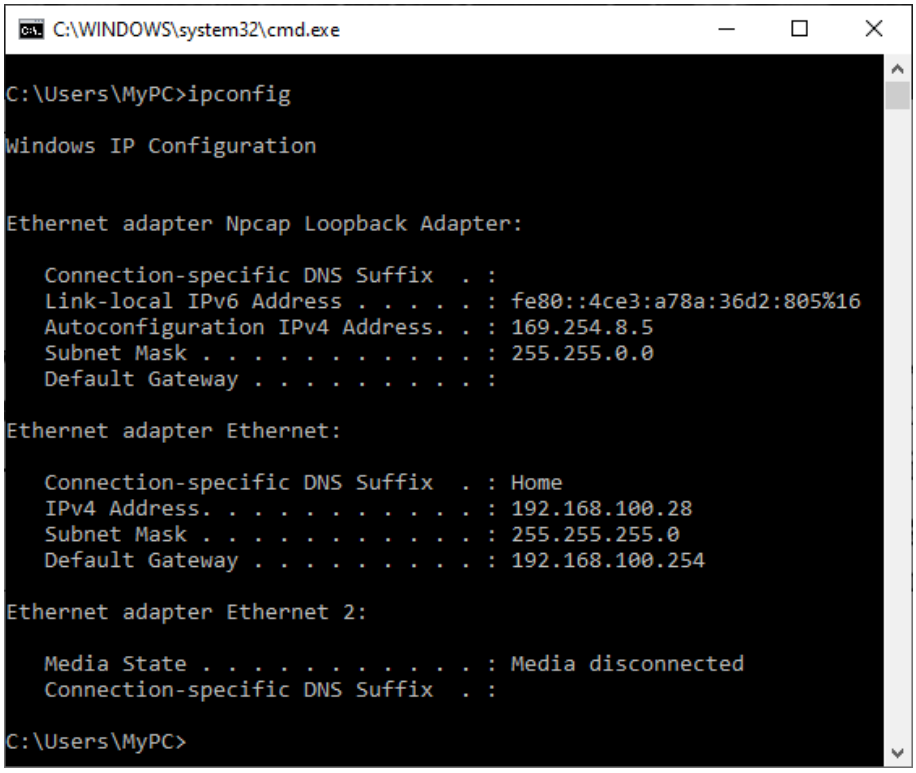
+ Bạn kiểm tra lại DNS, proxy sử dụng lệnh "ping –t 203.113.131.1" tới DNS của nhà mạng. Nếu nhận được trả lời như hình dưới tức là máy tính kết nối tốt đến Internet.



Hình 4.10 sử dụng lệnh ping để kiểm tra kết nối

+ Nếu kết quả trả lời không giống như hình 4.10 thì báo ngay cho nhân viên nhà mạng kiểm tra trực tiếp.

- Sử dụng lệnh ipconfig để kiểm tra IP



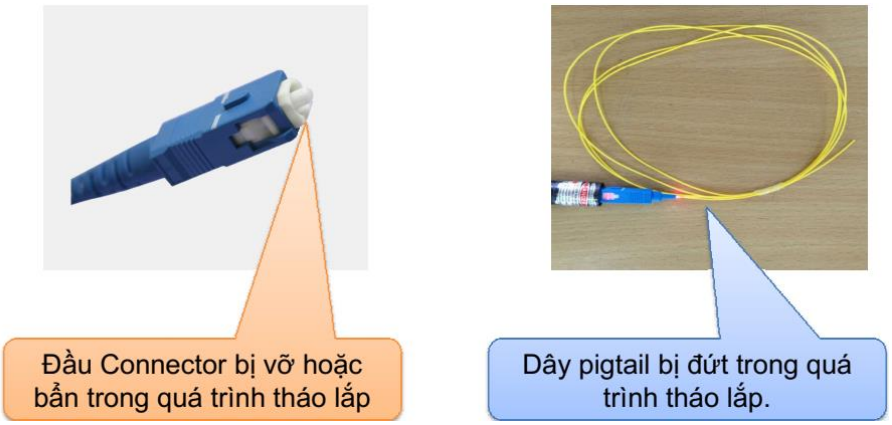
Hình 4.11 sử dụng lệnh ipconfig để kiểm tra

+ Nếu Ipv4 Address: 169.254…. và default gateway không có, tức là máy tính không nhận được DHCP từ modem –> khởi động lại modem và kiểm tra lại lệnh Ipconfig. Nếu không được cứ bình tĩnh đặt IP tĩnh cho các máy tính trùng với dãi IP 192.168.100.254 của modem.

+ **Chú ý**: Hầu hết KH sử dụng FTTH đều có sử dụng qua mạng nội bộ có các thiết bị trung gian.

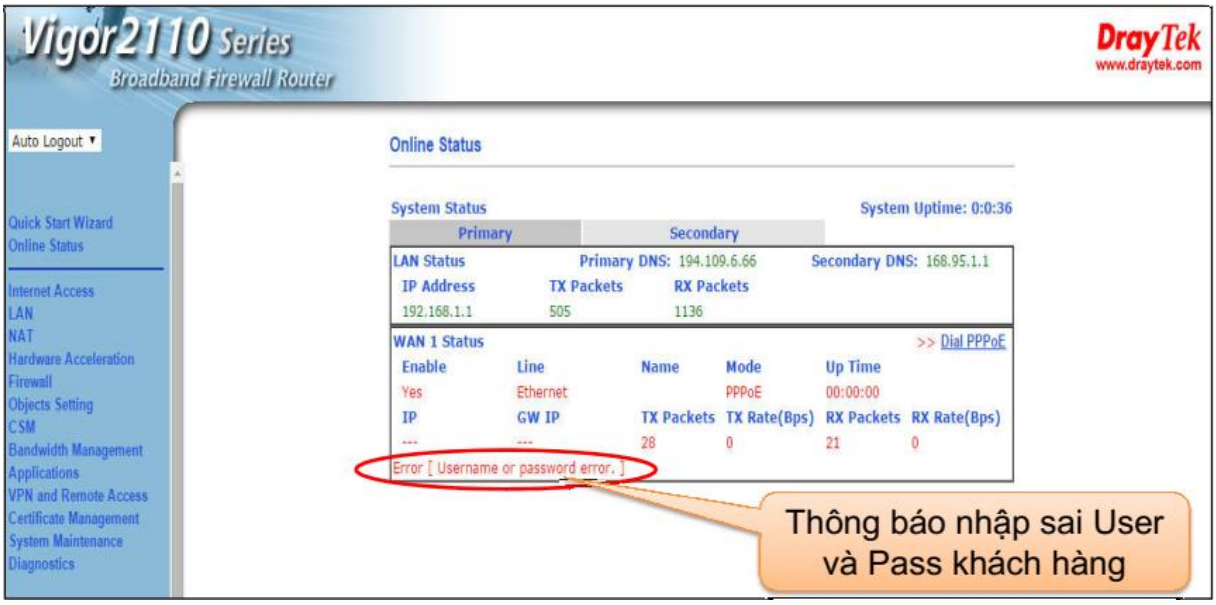
Sự cố Connector

- Đèn WAN trên Modem không sáng cho dù đã đổi vị trí cắm. Kiểm tra lại đầu connector hoặc dây Pigtail có bị hỏng hoặc đứt bằng bút thử Laser.



Hình 4.12 Sự cố Connector

Sai User và Pass khách hàng



Hình 4.13 Sai User và Pass

+ Kiểm tra lại Username & Password xem nhập đã đúng chưa (tắt các bộ gõ tiếng Việt).

+ Nếu vẫn không được báo nhà cung cấp dịch vụ ISP .

2.3 Sự cố về băng rộng dùng chung

Internet chập chờn: Do lỗi thi công đấu nối:

- **Thuê bao AON.**

+ Khoảng cách cáp từ đài đến thuê bao lớn dẫn đến có nhiều mối hàn, mối nối dẫn đến suy hao hàn nối lớn.

+ Các thao tác kỹ thuật xếp sợi vào khay có bán kính uốn cong nhỏ, gây suy hao mỗi khi có lực tác động lên cáp.

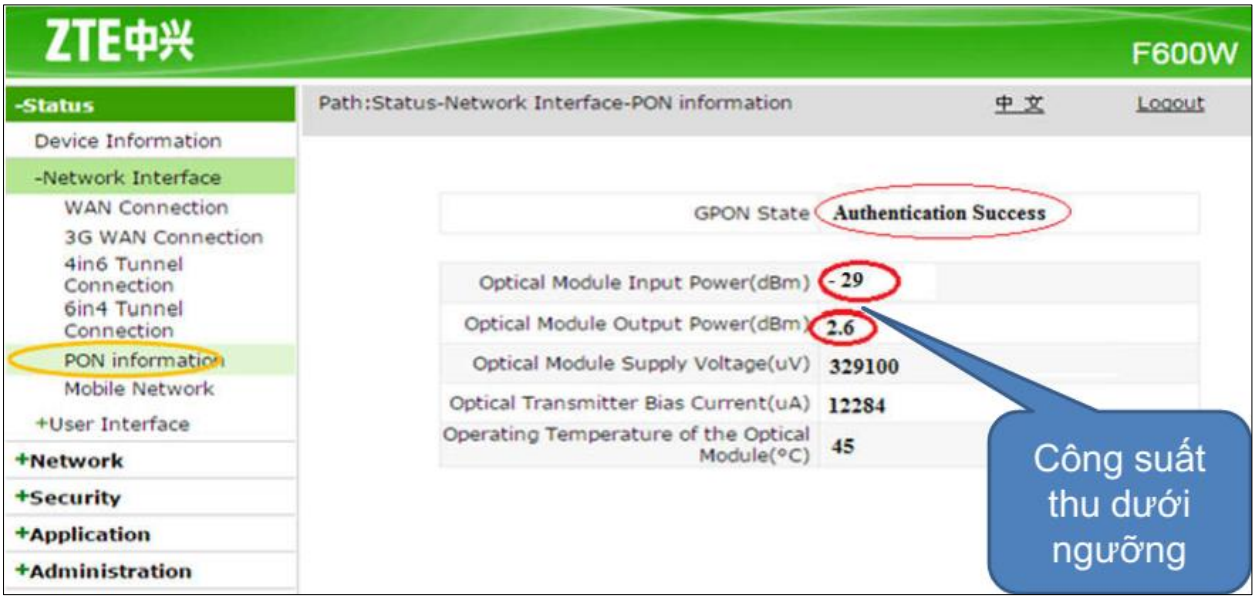
+ Sử dụng máy đo OTDR đo ở chế độ Real Time để phát hiện và xử lý.

- **Thuê bao GPON.**

+ Khoảng cách cáp từ đài đến thuê bao lớn dẫn đến có nhiều mối hàn, mối nối dẫn đến suy hao hàn nối lớn.

+ Thi công dây thuê bao không đúng qui trình dẫn đến bị rút sợi tại đầu Fastconnector. Gây suy hao lớn khi có tác động của gió lên dây dẫn.

+ Dùng máy đo công suất để đo và xử lý.



Hình 4.13 Internet chập chờn

Internet chậm: Do lỗi máy tính:

- **Máy bị Virus.**

+ Trong quá trình sử dụng, máy bị nhiễm Virut làm cho tốc độ truy cập Internet chậm.

+ Sử dụng Virut bản quyền để quét và xử lý.

+ Trường hợp không thể quét xử lý hết, nên cài lại hệ điều hành máy tính.

- **Máy tính quá nhiều rác.**

+ Máy tính sử dụng lâu ngày sinh ra lượng rác nhất định, điều này làm chiếm hết dung lượng bộ nhớ đệm, gây ra làm chậm khả năng xử lý của máy tính.

+ Sử dụng các phần mềm dọn rác máy tính để quét và dọn dẹp máy.

+ Do sử dụng một số phần mềm ẩn danh: UltraSurf hoặc Hotspot Shield.

+ Một số người thường sử dụng các phần mềm ẩn danh hoặc Fix IP để truy cập các trang Facebook. Tuy nhiên, nó lại gây cản trở cho việc truy cập các trang Web.

2.4 Kỹ thuật băng rộng

Băng thông rộng (tiếng Anh: Broadband) đề cập đến các công nghệ truyền tải dung lượng cao khác nhau được sử dụng để truyền dữ liệu, giọng nói và video qua khoảng cách xa và với tốc độ cao.

Các phương tiện truyền dẫn phổ biến bao gồm cáp đồng trục, cáp quang và sóng vô tuyến.

Cách thức hoạt động của Băng thông rộng

- Ngày nay, thảo luận về **băng thông rộng** thường tập trung vào việc sử dụng nó để cung cấp truy cập internet tốc độ cao.

- Trong lịch sử, Internet băng thông rộng được xem là nhanh hơn kết nối internet quay số truyền thống. Tuy nhiên, hiện nay các định nghĩa được yêu cầu rõ ràng hơn.

- Chẳng hạn, Uỷ ban Truyền thông Liên bang của Mỹ (FCC) đã ra phán quyết vào năm 2015 rằng, để được coi là internet băng thông rộng, dịch vụ phải cung cấp tốc độ tải xuống và tải lên ít nhất tương ứng làn lượt là 25 megabit và 3 megabit.

- Tuy nhiên, nói chung, hai đặc điểm để xác định băng thông rộng là tốc độ cao và có sẵn ở mọi thời điểm. Cả hai đặc điểm này phục vụ để phân biệt băng thông rộng với các kết nối quay số cũ. Kết nối Internet quay số chậm hơn, và chỉ khả dụngg khi người dùng yêu cầu cụ thể.
- Do những lợi thế rõ ràng của nó so với các dịch vụ quay số, truy cập Internet băng thông rộng được cả người dùng cuối và chính phủ ưa thích.
- Mặc dù có sức hấp dẫn rộng rãi, việc truy cập vào băng thông mà băng thông rộng cung cấp chỉ tập trung cao chỉ ở một số quốc gia.

Ví dụ về Băng thông rộng

- Một khái niệm mới nổi của công nghệ truyền dẫn **băng thông rộng** là việc sử dụng các mạng vệ tinh tiên tiến để cung cấp truy cập Internet mà không cần đầu tư qui mô lớn vào cơ sở hạ tầng trên mặt đất.
- Một ví dụ đáng chú ý của phương pháp mới nổi này là dự án Starlink hiện đang được theo đuổi bởi công ty phát triển và thăm dò không gian tư nhân, SpaceX.
- Thông qua dự án này, Elon Musk, người sáng lập SpaceX đặt mục tiêu ra mắt một loạt 12.000 vệ tinh chưa từng có được thiết kế để hoạt động song song, cung cấp truy cập Internet vệ tinh tốc độ cao cho người dùng trên toàn thế giới.
- Tính đến tháng 11 năm 2019, khoảng 120 vệ tinh đã được SpaceX triển khai theo chương trình mới này. Tuy nhiên, công ty ước tính rằng về lâu dài, dự án có thể đòi hỏi phải phóng tới 42.000 vệ tinh.
- Nếu thành công, mục tiêu đã nêu của dự án là cung cấp dịch vụ Internet băng rộng chi phí thấp cho người dùng trên toàn thế giới, có khả năng vượt qua các nhà cung cấp viễn thông mặt đất.

Câu hỏi ôn tập

- Trình bày các nguyên tắc của nhà cung cấp dịch vụ Internet
- Kiểm tra và khắc phục các sự cố kết nối Internet băng thông rộng.

BÀI 5. BẢO MẬT, BẢO TRÌ

Giới thiệu:

Bảo mật thông tin là bảo vệ thông tin dữ liệu cá nhân, tổ chức nhằm tránh khỏi sự "đánh cắp, ăn cắp" bởi những kẻ xấu hoặc tin tặc. An ninh thông tin cũng như sự bảo mật an toàn thông tin nói chung. Việc bảo mật tốt những dữ liệu và thông tin sẽ tránh những rủi ro không đáng có cho chính cá nhân và doanh nghiệp của bạn.

Bảo trì là hoạt động chăm sóc kĩ thuật, điều chỉnh, sửa chữa hoặc thay thế một hoặc nhiều chi tiết hay cụm chi tiết máy nhằm duy trì hoặc khôi phục các thông số hoạt động, bảo đảm máy móc thiết bị hoạt động với năng suất, tốc độ, tải trọng đã xác định trước.

1. Mục tiêu:

- Phát hiện được các sự cố về tường lửa và vấn đề cần bảo mật trên hệ thống mạng.
- Kiểm tra và quét các loại virus máy tính xâm nhập vào mạng
- Sao lưu và phục hồi dữ liệu thường xuyên, có định kỳ
- Nâng cấp mở rộng hệ thống mạng đang sử dụng

2. Nội dung bài học

2.1 Sự cố về bức tường lửa

Windows có một số tính năng bảo mật để giữ cho máy tính và dữ liệu của bạn an toàn, chống lại các chương trình độc hại và tin tặc. Một trong những tính năng này là Windows Firewall, nó giúp chặn truy cập trái phép và các ứng dụng có khả năng gây hại vào máy tính của bạn.

Tuy nhiên, trong quá trình sử dụng, bạn có thể gặp một số vấn đề về Firewall (tường lửa), ví dụ không thể kích hoạt tính năng này hoặc lỗi 80070424, lỗi dịch vụ 5 (0x5). Đôi khi các ứng dụng hoặc tính năng như hỗ trợ từ xa (Remote Assitant) không hoạt động hoặc bạn không thể quyền truy cập vào tệp chia sẻ và máy in dùng chung vì chúng bị chặn bởi Windows Firewall.

Nếu bạn gặp phải bất kỳ vấn đề nào trong số những vấn đề hoặc các vấn đề tương tự, bạn có thể sử dụng "**Windows Firewall Troubleshooter**" - công cụ tự động quét và khắc phục sự cố thường gặp. Bạn cũng có thể khôi phục cài đặt tưởng lửa về chế độ mặc định và tự chặn ứng dụng thông qua Windows Firewall.

Trong giáo trình này hướng dẫn các bạn các bước đơn giản để khắc phục và giải quyết các sự cố với Windows Firewall.

Để khắc phục sự cố Windows Firewall, thực hiện các bước sau:

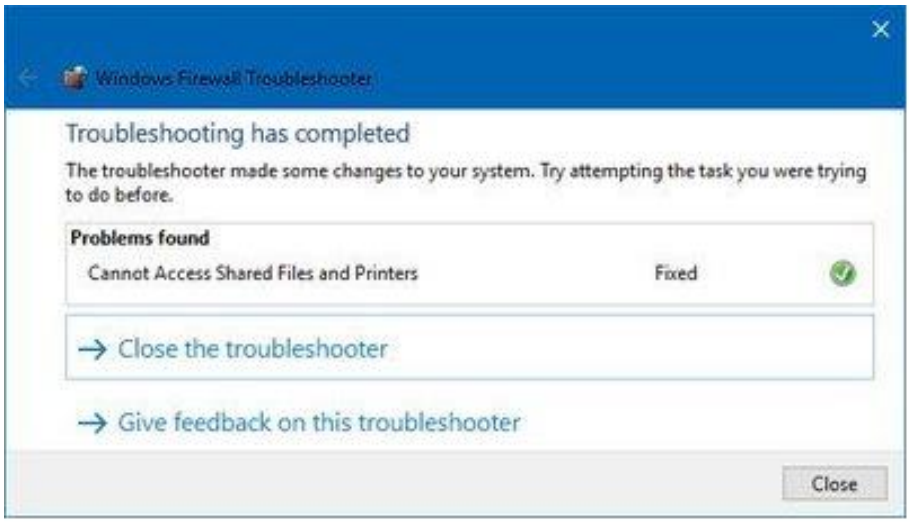
- Tải Windows Firewall Troubleshooter từ Microsoft.
- Bấm đúp vào tệp **WindowsFirewall.diagcab.**
- Nhấp vào **Next.**

Hình 5.1 Sự cố về bức tường lửa

- Tùy thuộc vào kết quả khắc phục sự cố, nhấp vào tuỳ chọn để khắc phục sự cố.

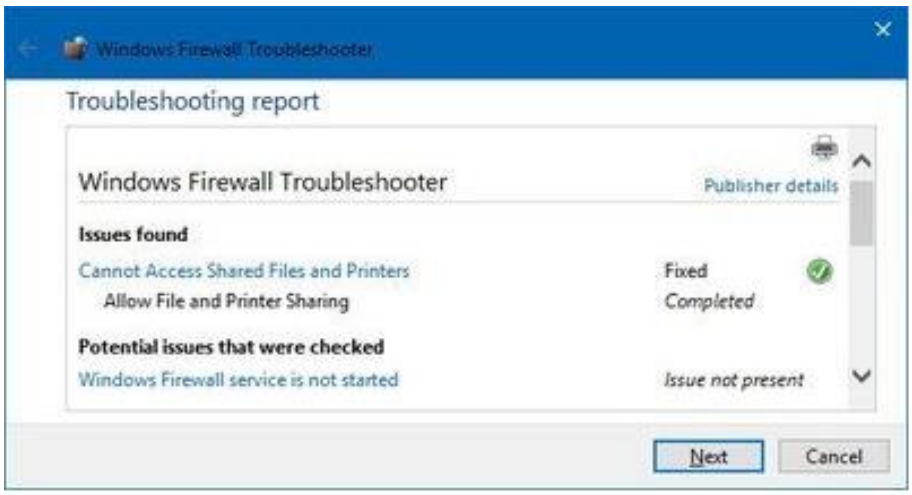
Hình 5.2 Sự cố về bức tường lửa

- Nếu vấn đề đã được giải quyết nhấp vào "**Close the troubleshooter"** để đóng trình khắc phục sự cố.



Hình 5.3 Sự cố về bức tường lửa

+ Nếu vẫn chưa khắc phục được sự cố, hãy click vào liên kết "**View detailed information**" để xem báo cáo tất cả các vấn đề trình khắc phục sự cố đã cố gắng khắc phục như quyền truy cập vào tệp chia sẻ và máy in dùng chung, các vấn đề với Remote Assitant, không thể khởi động Windows Firewall hoặc các dịch vụ có liên quan khác như dịch vụ BFE.



Hình 5.4 Sự cố về bức tường lửa

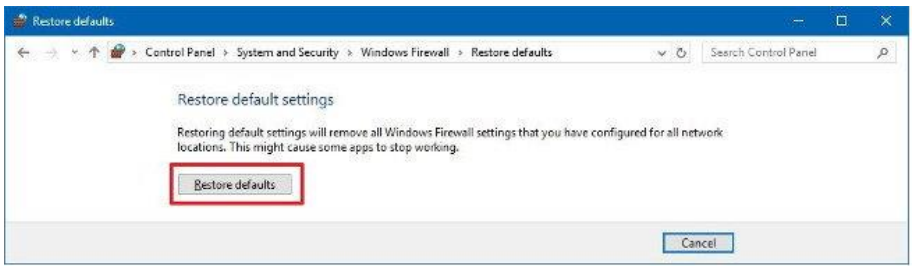
+ Sau đó, bạn có thể sử dụng thông tin này để tiếp tục nghiên cứu và tìm kiếm cách khắc phục trên công cụ tìm kiếm hoặc yêu cầu trợ giúp trong diễn đàn Windows Central.

Cách thiết lập lại cài đặt Windows Firewall

- Ngoài ra, nếu trình khắc phục sự cố không tìm thấy bất kỳ vấn đề gì, ví dụ vấn đề do một cài đặt cụ thể đã được định cấu hình trước trên thiết bị của bạn. Trong trường hợp này, bạn có thể thử gỡ bỏ cấu hình hiện tại và khôi phục cài đặt Windows Firewall mặc định.
- **Chú ý**: Sau khi khôi phục cài đặt mặc định, bạn có thể phải cấu hình lại các ứng dụng yêu cầu sự cho phép thông qua tường lửa.
- Để thiết lập lại Windows Firewall về cài đặt mặc định, thực hiện theo các bước sau:
  + Mở **Control Panel.**
  + Click vào **System and Security.**
  + Chọn **Windows Firewall.**

Hình 5.5 Sự cố về bức tường lửa

  + Trên thanh bên trái, nhấp vào liên kết "**Restore defaults**".
  + Chọn "**Restore defaults**".



Hình 5.6 Sự cố về bức tường lửa

  + Cuối cùng chọn "**Yes**" để xác nhận.
- Sau khi bạn đã hoàn tất các bước trên, các cài đặt mặc định đã được khôi phục và

khắc phục tất cả các vấn đề về cấu hình trên thiết bị của bạn.

Tất cả các máy tính Windows đều có các tính năng bảo vệ hệ điều hành khỏi hacker, vi rút và các loại phần mềm độc hại khác. Ngoài ra còn có các biện pháp bảo vệ "tại chỗ" để ngăn ngừa các tai nạn do người dùng tự gây ra, chẳng hạn như vô tình cài đặt các phần mềm không mong muốn hoặc thay đổi cài đặt hệ thống quan trọng. Hầu hết các tính năng này đã tồn tại dưới nhiều hình thức trong nhiều năm. Một trong số chúng là Windows Firewall (tường lửa windows), luôn là một phần của Windows và có trong XP, 7, 8, 8,1 và gần đây nhất là Windows 10.

Nó được kích hoạt theo mặc định. Nhiệm vụ của nó là bảo vệ máy tính, dữ liệu của bạn và thậm chí là nhận dạng của bạn.

Nhưng chính xác tường lửa là gì và tại sao nó lại cần thiết. Để hiểu điều này, hãy xem xét ví dụ thực tế. Trong lĩnh vực vật lý, tường lửa là một bức tường được thiết kế đặc biệt để chặn hoặc ngăn chặn sự lây lan của ngọn lửa hiện có hoặc đang tiếp cận đến. Khi một ngọn lửa đến gần, bức tường vẫn đứng vững trên mặt đất và bảo vệ những gì phía sau nó.

Windows Firewall cũng thực hiện chức năng tương tự, chỉ khác ở đây là dữ liệu (hoặc cụ thể hơn là các gói dữ liệu). Một trong những công việc của nó là xem xét những gì đang cố gắng xâm nhập vào máy tính từ các trang web và email, sau đó quyết định xem dữ liệu đó có nguy hiểm hay không. Nếu dữ liệu an toàn, nó sẽ cho phép dữ liệu vượt quá. Nếu cảm thấy dữ liệu có thể đe dọa đến sự ổn định của máy tính thì thông tin trên đó sẽ bị từ chối. Đó là lớp phòng thủ, giống như một bức tường lửa vật lý.

Tuy nhiên, đây là một lời giải thích rất đơn giản về một chủ đề rất kỹ thuật. Nếu bạn muốn tìm hiểu sâu hơn thì xem bài viết Tường lửa (Firewall) là gì? Những kiến thức tổng quan về Firewall.

Cách truy cập tường lửa

Tường lửa Windows cung cấp một số cài đặt mà bạn có thể định cấu hình.

Bạn có thể cấu hình cách tường lửa thực hiện và những dữ liệu, ứng dụng tường lửa chặn và cho qua. Bạn có thể tự chặn một chương trình theo mặc định được thông qua chẳng hạn như Microsoft Tips hoặc Get Office. Khi chặn các chương trình này, về bản chất có nghĩa là vô hiệu hóa chúng. Nếu bạn không thích những nhắc nhở khi mua Microsoft Office hoặc nếu những mẹo này đang làm phiền, bạn có thể làm cho chúng "biến mất".

Bạn cũng có thể chọn để các ứng dụng chuyển dữ liệu qua máy tính của bạn mà theo mặc định nó không được thông qua. Điều này thường xảy ra với các ứng dụng của bên thứ ba mà bạn cài đặt như iTunes vì Windows yêu cầu sự cho phép của bạn để cài đặt và thông qua. Tuy nhiên, các tính năng cũng có thể liên quan đến Windows như tùy chọn sử dụng Hyper-V để tạo các máy ảo hoặc Remote Desktop để truy cập vào máy tính của bạn từ xa.

Bạn cũng có tùy chọn để tắt tường lửa hoàn toàn khi muốn sử dụng bộ phần mềm bảo mật của bên thứ ba, như các chương trình chống virus do McAfee hoặc Norton cung cấp. Đây thường là dịch vụ thử nghiệm miễn phí trên máy tính cá nhân mới và người dùng thường đăng ký. Bạn cũng có thể vô hiệu hóa tường lửa Windows nếu bạn đã cài đặt một phần mềm miễn phí.

Lưu ý: Điều quan trọng là phải duy trì một tường lửa duy nhất, vì vậy đừng tắt tường lửa Windows trừ khi bạn có một ứng dụng khác thay thế và không chạy nhiều tường lửa cùng một lúc.

Khi bạn đã sẵn sàng thay đổi tường lửa Windows, hãy truy cập các tùy chọn tường lửa:

- Nhấp vào khu vực tìm kiếm của thanh **Taskbar**.
- Gõ **Windows Firewall.**
- Trong kết quả, **click Windows Firewall Control Panel** .
- Từ khu vực tường lửa của Windows, bạn có thể thực hiện một số thao tác. Tùy chọn để tường lửa của Windows ở chế độ On hoặc Off.
- Tường lửa sẽ chặn một số phần mềm độc hại mà bạn không biết. Bạn có thể bấm để xác minh và sau đó sử dụng mũi tên quay lại để trở về màn hình tường lửa chính. Bạn cũng có thể khôi phục lại mặc định nếu bạn đã thay đổi chúng bằng tùy chọn **Restore Defaults** ở khung bên trái.

Cách cho phép ứng dụng thông qua tường lửa Windows

Windows Firewall cho phép ứng dụng thông qua dựa trên việc xác nhận bạn kết nối với mạng riêng tư (private network) hay mạng công cộng (public network) hoặc cả hai. Nếu bạn chỉ chọn **Private** thì bạn chỉ có thể sử dụng ứng dụng hoặc tính năng khi kết nối với mạng riêng tư, chẳng hạn như mạng ở nhà hoặc văn phòng. Nếu bạn chọn **Public**, bạn có thể truy cập ứng dụng khi kết nối với mạng công cộng, chẳng hạn như mạng trong quán cà phê hoặc khách sạn. Như bạn thấy ở đây, bạn cũng có thể chọn cả hai.

Để cho phép một ứng dụng thông qua Windows Firewall:

- Mở **Windows Firewall**. Bạn có thể tìm kiếm nó từ thanh **Taskbar** như hướng dẫn ở trên.
- Chọn **Allow an App or Feature Through Windows Firewall** (Cho phép ứng dụng hoặc tính năng thông qua tường lửa Windows)
- Nhấp **Change Settings** và gõ một mật khẩu quản trị viên nếu được yêu cầu.
- Xác định ứng dụng cho phép thông qua tường lửa. Nó sẽ không có dấu tích bên cạnh.
- Tích vào (các) hộp để cho phép truy cập từ mạng riêng tư hay mạng công cộng bằng hai tùy chọn **Private** và **Public**. Đầu tiên bạn nên chọn Private trước sau đó chọn Public sau nếu không nhận được kết quả mong muốn.
- Cuối cùng chọn **OK.**

Cách chặn ứng dụng thông qua tường lửa Windows 10

Tường lửa của Windows cho phép một số ứng dụng Windows 10 và các tính năng truyền dữ liệu đi vào và đi ra khỏi máy tính mà không cần bất kỳ tác động của người dùng nào. Các ứng dụng bao gồm Microsoft Edge và Microsoft Photos, các tính năng cần thiết như Core Networking (mạng lõi) và Windows Defender Security Center. Các ứng dụng khác của Microsoft như Cortana có thể yêu cầu sự cho phép của bạn khi sử dụng lần đầu tiên. Tuy nhiên trong tương lai có thể Cortana không cần sự cho phép của bạn vẫn được mặc định kích hoạt. Điều đó có nghĩa là các ứng dụng và tính năng khác có thể được kích hoạt dù bạn có muốn hay không. Ví dụ, Remote Assistance (hỗ trợ từ xa) được bật theo mặc định. Chương trình này cho phép một kỹ thuật viên truy cập vào máy tính của bạn từ xa để

giúp bạn giải quyết vấn đề nếu bạn cấp quyền truy cập. Mặc dù ứng dụng này bị khóa và khá an toàn, nhưng một số người dùng coi đây là lỗ hổng bảo mật mở. Nếu muốn đóng tùy chọn này, bạn có thể chặn quyền truy cập.

Ngoài ra bạn cần xem xét các ứng dụng của bên thứ. Điều quan trọng là cần chặn (hoặc có thể gỡ cài đặt) các ứng dụng không mong nếu bạn không sử dụng chúng. Bạn có thể kiểm tra các mục liên quan như chia sẻ tệp, chia sẻ nhạc, chỉnh sửa ảnh, v.v... và chặn những mục không cho phép truy cập. Và khi sử dụng ứng dụng này, bạn sẽ được nhắc cho phép ứng dụng thông qua tường lửa. Điều này sẽ giúp bạn sử dụng các ứng dụng khi cần thiết và cũng ngăn bạn vô tình gỡ cài đặt ứng dụng mà hệ thống cần để hoạt động đúng cách.

Để chặn một chương trình trên máy tính Windows 10:

Thực hiện các bước từ 1-3 giống phần cho phép ứng dụng thông qua tường lửa

Xác định ứng dụng chặn thông qua tường lửa. Nó sẽ có dấu tích bên cạnh.

Tích vào (các) hộp để không cho phép truy cập từ mạng riêng tư hay mạng công cộng bằng hai tùy chọn **Private** và **Public**. Chọn cả hai

Sau đó chọn **OK.**

Khi bạn đã hoàn tất, các ứng dụng bạn đã chọn sẽ bị chặn dựa trên các loại mạng mà bạn đã chọn.

Tường lửa của bên thứ ba miễn phí

Nếu bạn muốn sử dụng tường lửa từ nhà cung cấp bên thứ ba, bạn hoàn toàn có thể sử dụng chúng. Hãy nhớ rằng, tường lửa của Windows bảo vệ máy tính của bạn khá tốt nên bạn không cần phải khám phá các tùy chọn khác nếu bạn không muốn. Đó là sự lựa chọn của bạn và nếu bạn muốn thử nó, đây là một vài lựa chọn miễn phí:

- **ZoneAlarm Free Firewall** - ZoneAlarm đã có khoảng một thời gian rất dài và là một tên đáng tin cậy. Nó bảo vệ máy tính của bạn ở nhiều cấp độ từ ẩn cổng mở đến cập nhật bảo mật thời gian thực. Thật dễ dàng để tải xuống và cài đặt nó.
- **TinyWall** - Sử dụng đơn giản hiệu quả và không xâm nhập, tường lửa này là một lựa chọn tốt cho những người dùng chỉ có một chút kinh nghiệm.
- **Comodo Firewall** - Tường lửa này đi kèm với một bộ bảo mật đầy đủ và tốt nhất cho người dùng chuyên nghiệp. Nó bao gồm các cập nhật tự động nhưng không có nhiều trợ giúp được cài sẵn.

Bất kể bạn quyết định làm gì hoặc không làm với Windows Firewall, hãy nhớ rằng bạn cần bật tường lửa để bảo vệ máy tính khỏi phần mềm độc hại, vi rút và các mối đe dọa khác. Bạn cũng nên thường xuyên kiểm tra nó, có lẽ một tháng một lần. Chú ý đến bất kỳ thông báo nào bạn thấy về tường lửa và giải quyết ngay lập tức. Chúng xuất hiện trong khu vực thông báo của thanh Taskbar ở phía bên phải.

2.2 Virus

Virus máy tính là gì? Cách phòng chống virus máy tính

Khi sử dụng máy tính chúng ta thường nghe tới virus máy tính, vậy virus máy tính là gì? virus máy tính có hại hay không? Cách thức mà virus máy tính lây lan từ máy này qua máy khác? Cách phòng chống virus máy tính?

Virus máy tính là gì?

- Trong khoa học máy tính, **virus máy tính** (thường được người sử dụng gọi tắt là virus hay vi-rút) là những đoạn mã chương trình được thiết kế để thực hiện tối thiểu là hai việc:

+ **Tự xen vào hoạt động hiện hành của máy tính** một cách hợp lệ, để thực hiện tự nhân bản và những công việc theo chủ ý của người lập trình. Sau khi kết thúc thực thi mã virus thì điều khiển được trả cho trình đang thực thi mà máy không bị "treo", trừ trường hợp virus cố ý treo máy.

+ **Tự sao chép chính nó**, tức tự nhân bản, một cách hợp lệ lây nhiễm vào những tập tin (file) hay các vùng xác định (boot, FAT sector) ở các thiết bị lưu trữ như đĩa cứng, đĩa mềm, thiết bị nhớ flash (phổ biến là USB),… thậm chí cả EPROM chính của máy.

Virus máy tính có gây hại không?

- Về cơ bản, virus máy tính là phần mềm do con người tạo ra chính vì vậy chúng thường có một mục đích nhất định và thường là các mục đích gây hại. Bạn có thể coi virus máy tính là một bệnh dịch và luôn có khả năng lây nhiễm cho máy tính của bạn.
- Kể từ khi xuất hiện cho tới nay, virus máy tính đã có rất nhiều loại khác nhau và trong số đó có những virus gây ra những hậu quả rất lớn, thiệt hại lên tới hàng trăm triệu USD. Chính vì vậy người sử dụng máy tính cần phải tìm ra các phương pháp để có thể tiêu diệt chúng tránh làm ảnh hưởng tới các dữ liệu có trên máy tính hoặc thông tin cá nhân của bạn. Các giải pháp người dùng nên lựa chọn đó là sử dụng **phần mềm diệt virus** để bảo vệ, ngăn chặn và loại bỏ virus.

Cách thức lây lan của Virus máy tính?

- Virus có rất nhiều cách lây lan và phá hoại khác nhau tùy thuộc vào mục đích của người đã tạo ra nó. Thông thường virus sẽ tấn công thông qua các kết nối ngoại vi trên máy tính của bạn như **mạng nội bộ, thông qua email, các file bạn download về từ internet, các Website độc hại, các web phim cấp 3, và đặc biệt là USB**. Một số loại virus tinh vi hơn, chúng xâm nhập bằng cách lợi dụng lỗ hổng từ hệ điều hành hoặc các phần mềm bạn sử dụng.

Làm sao để bảo vệ máy tính khỏi virus?

- Có một số cách để bảo vệ máy tính khỏi virus độc hại mà bạn có thể áp dụng
- Cài đặt các phần mềm diệt virus
- Đóng băng ổ đĩa (dùng Deep Freeze)
- Sao lưu dữ liệu (Ghost cả ổ cứng, hoặc các ổ chứa dữ liệu quan trọng)
- Hạn chế việc sao chép không cần thiết và không chạy các chương trình tải từ Internet hoặc sao chép từ máy khác khi chưa đủ tin cậy.
- Không mở những tệp gửi kèm trong thư điện tử nếu có nghi ngờ về nguồn gốc hay nội dung thư.
- Không truy cập vào các trang web có nội dung không lành mạnh.
- Thường xuyên cập nhật các bản sửa lỗi cho các phần mềm chạy trên máy tính của mình, kể cả hệ điều hành.
- Định kì sao lưu dữ liệu để có thể khôi phục khi bị virus phá hoại.
- Định kì quét và diệt virus bằng các phần mềm diệt virus

2.3 Những vấn đề về bảo mật vô tuyến

Mạng không dây là một hệ thống các thiết bị được gom nhóm lại với nhau. Chúng có khả năng giao thiết thông qua sóng vô tuyến. Vậy ưu nhược điểm của chúng là gì. Và hệ thống bảo mật mạng không dây ra làm sao?

- **Bảo mật mạng không dây**

Hình 5.7 bảo mật vô tuyến

Ưu nhược điểm của mạng không dây

- Ưu điểm của mạng không dây
  + Chi phí lắp đặt giảm đáng kể so với mạng có dây
  + Công nghệ mạng không dây được tích hợp cho tất cả các thiết bị dị dông jcungx như máy tính xách tay. Đảm bảo tất cả mọi tiết bị đều có tính năng kết nối mạng không dây
  + Mạng không dây tạo được sự thoải mái trong việc truyền tải dữ liệu mà không có sự ràng buộc về khoảng cách và không gian giữa các thiết bị. Chỉ cần di chuyển ở bất kì nơi nào trong phạm vi phủ sóng
  + Mạng không dây sử dụng sóng hồng ngoại và sóng radio để truyền dữ liệu giữa các thiết bị. Sóng radio truyền tín hiệu đi xa hơn, lâu và rộng hơn, băng thông cao hơn. Vì vậy sóng radio được sử dụng rộng rãi hơn tia hồng ngoại.
- Nhược điểm của mạng không dây
  + Tốc độ mạng không dây phụ thuộc vào băng thông, và tốc độ này thường thấp hơn mạng có dây.
  + Rất khó quản lý thông tin và có khả năng đánh rơi dữ liệu trên đường truyền.

Khả năng bảo mật mạng không dây

- Mạng không dây dùng trong gia đình, các doanh nghiệp, cơ quan chính phủ,… luôn có khả năng bị hacker dễ dàng xâm nhập vào đường truyền để đánh cắp thông tin. Và từ đó, có thể sẽ gây ra những hậu quả nghiêm trọng. Thế nhưng, người dùng vẫn chưa để ý đến vấn đề bảo mật mạng không dây. Một vấn đề đáng được quan tâm ngày nay.

Hình 5.8 bảo mật vô tuyến

Các lỗ hổng trong việc bảo mật mạng không dây

- *Hạn chế khả năng quản trị*: Mạng không dây cho phép tất cả mọi người kết nối vào hệ thống trong phạm vi phủ sóng. Chỉ cần nằm trong bán kính phủ sóng của mạng không dây thì bất kì ai cũng có thể kết nối và khai thác tài nguyên của hệ thống đó. Vì vậy, đây là cơ hội tốt cho các hacker xâm nhập vào hệ thống.
- *Khả năng mã hoá dữ liệu*: Mặc dù dữ liệu đã được mã hoá trước khi được truyền qua hệ thống mạng không dây. Tuy nhiên, các hacker có thể sử dụng thiết bị wifi đã được thay đổi để chặn dữ liệu, gây nên những khó khăn cho hệ thống.
- *Xác thực quyền người dùng*: Hầu hết các kết nối mạng không dây đều mặc định ở chế độ mở hoàn toàn. Nghĩa là khôn gcung cấp đầy đủ quyền quản trị cho người quản lý. Cũng như không có khả năng xác thực quyền người dùng, hay phân quyền cho các kết nối xuất phát từ hệ thống
- *Khả năng phát hiện và phòng chống tấn công*: Các hình thức tấn công của hacker ngày càng đa dạng. Đây là trở ngại cho hầu hết các tổ chức và khó khăn khi tìm cách phòng chống.
- Chính vì hệ thống **bảo mật mạng không dây** không được an toàn. Nên nhà cung cấp đã cho một số chuẩn và đưa ra một số dịch vụ nhằm khắc phục những vấn đề trên. Dịch vụ thuê đường truyền riêng trong nước là một trong những giải pháp khắc phục hiệu quả nhất. Phù hợp cho các tổ chức, doanh nghiệp yêu cầu hệ thống băng thông và bảo mật cao.

2.4 Ghi tài liệu

Hồ sơ tài liệu lưu trữ có ý nghĩa vô cùng quan trọng với từng đơn vị, cơ quan, tổ chức, doanh nghiệp. Chính vì vậy, việc bảo mật hồ sơ tài liệu trong kỷ nguyên internet hiện nay là vấn đề cần trọng mà mỗi đơn vị đều luôn lưu tâm. Vậy cách bảo mật hồ sơ tài liệu nào an toàn hiện nay?

Phương thức quản lý hồ sơ tài liệu thường áp dụng

Thông thường các đơn vị, doanh nghiệp thường quản lý hồ sơ, tài liệu và bảo mật chúng theo phương pháp truyền thống. Việc quản lý tài liệu thường được thực hiện theo cách ghi nhận lại trên giấy tờ, sổ sách theo dõi… sau đó lưu lại trong thư viện hoặc kho lưu trữ, đánh dấu mã số và ghi chép thông tin vào các kẹp file hồ sơ để có thể tìm kiếm lại khi cần.

Tuy nhiên theo thời gian khối lượng các tài liệu, hồ sơ, công văn, giấy tờ tăng lên rất nhiều. Ban đầu chúng ta lưu thành các tủ tài liệu, sau đó việc lưu trữ thông tin trên máy tính cũng trở nên quá tải làm chúng ta mất phương hướng trong việc quản lý thông tin, tìm kiếm, tra cứu hồ sơ tài liệu.

Những năm qua, công tác quản lý công văn, tài liệu tại các đơn vị theo cách quản lý truyền thống đã bộc lộ nhiều hạn chế. Qua thời gian, tài liệu dễ bị hỏng, việc tra cứu tài liệu mất nhiều thời gian làm giảm hiệu quả công việc.

Chính vì thế, nhu cầu số hóa tài liệu là giải pháp hữu hiệu trong việc phát triển của các đơn vị, doanh nghiệp.

Bảo mật hồ sơ tài liệu trong kỷ nguyên internet

Thay vì phải tốn nhiều thời gian, công sức, chi phí cho việc quản lý tài liệu theo cách truyền thống thì hiện nay, nhiều doanh nghiệp, cơ quan, tổ chức đã tiến hành áp dụng công nghệ thông tin với các phần mềm quản lý hồ sơ tài liệu chuyên nghiệp phục vụ cho ngành văn thư lưu trữ và quản lý tài liệu.

Bảo mật hồ sơ tài liệu trong kỷ nguyên internet bằng phần mềm quản lý tài liệu hiện đại

Thời đại Internet lên ngôi thì việc ứng dụng công nghệ thông tin vào cải cách hành chính là điều tất yếu giúp các doanh nghiệp tiết kiệm thờ gian, chi phí để phát triển mạnh mẽ hơn.

Hiện nay, có rất nhiều phần mềm quản lý tài liệu được xây dựng nhằm bảo mật thông tin hồ sơ, tài liệu và tối giản các thủ tục quản lý cho mỗi doanh nghiệp ứng dụng. Một trong số các phần mềm được doanh nghiệp trong nước sử dụng nhất hiện nay là phần mềm văn phòng điện tử Cloudoffice.

Đây là hệ thống phần mềm bao gồm phần mềm quản lý văn bản, hồ sơ tài liệu và điều hành quản trị công việc toàn diện và chuyên nghiệp. Phần mềm được thiết kế một cách khoa học với đầy đủ chức năng trao đổi thông tin, điều hành tác nghiệp và quản lý văn bản, điều hành công việc trực tuyến trên mạng máy tính. Có khả năng theo dõi xử lý văn bản và điều hành công việc từ xa thông qua Internet.

Với phần mềm quản lý hồ sơ, tài liệu Cloudoffice người quản lý có thể phân loại hồ sơ tài liệu theo các chủ đề, nhóm lĩnh vực quản lý khác nhau, định nghĩa các thuộc tính cho từng chủ đề tài liệu giúp quản lý tài liệu đa dạng và linh hoạt theo từng thời điểm. Điều này sẽ giúp người đùng dễ dàng quản lý và tìm kiếm khi cần.

Bên cạnh đó, phần mềm còn cho phép phép lưu trữ các hồ sơ, tài liệu dùng chung cho cả đơn vị hoặc nhóm người dùng. Các tài liệu được lưu trữ có thể là các phần mềm, biểu

mẫu, ấn chỉ, tài liệu về hình ảnh, âm thanh, video… Không những thế, phần mềm còn cho phép quản lý các hồ sơ sự kiện. Các sự kiện có thể được quản lý thành 1 hồ sơ theo dõi diễn tiến từ lúc bắt đầu cho tới khi kết thúc sự kiện. Chức năng này áp dụng hiệu quả trong trường hợp quản lý hồ sơ khiếu nại tố cáo, hồ sơ vi phạm, hồ sơ triển khai dự án, triển khai hợp đồng. Chúng ta dễ dàng tìm kiếm lại hồ sơ của sự kiện nào đó để theo dõi hoặc tiếp tục cập nhận các nội dung, vấn đề mới của sự kiện.

Khả năng quản lý các loại tài liêu đặt thù và theo dõi đánh dấu kết quả thực hiện cũng được nhà thiết kế tích hợp trong phần mềm. Đặc biệt, phần mềm còn có chức năng cảnh báo các tài liệu sắp hết hạn áp dụng đối với một số tài liệu có hạn quản lý hoặc theo dõi như hợp đồng, dự án…

Với chức năng phân quyền trong phần mềm văn phòng điện tử, người quản trị hệ thống được phép tạo lập các thành viên mới, đổi quyền truy cập của các thành viên, phân các quyền truy cập các chức năng của phần mềm. Do đó, việc bảo mật thông tin luôn được đảm bảo an toàn tuyệt đối.

Nhờ những ưu điểm tích cực chức năng tiện ích, phần mềm quản lý văn bản, tài liệu Cloudoffice được xem là giải pháp hữu hiệu cho việc quản lý và bảo mật hồ sơ, tài liệu. Phần mềm đã và đang được rất nhiều đơn vị cơ quan, tổ chức, doanh nghiệp lựa chọn áp dụng và đem lại nhiều lợi ích thiết thực. Phần mềm góp phần giảm thiểu rất nhiều thời gian làm việc cho đội ngũ nhân viên, tiết kiệm nhiều không gian lưu trữ văn bản do toàn bộ hồ sơ, tài liệu được scan lại và sắp xếp lưu trữ theo cách quản lý rất khoa học trên các máy tính chuyên dụng, an toàn và bảo mật.

2.5 Sao lưu thông tin

Bảo vệ dữ liệu là việc vô cùng thiết yếu, bởi dữ liệu là tài sản quan trọng nhất của người dùng trên máy tính. Có thể nói nhu cầu sử dụng máy tính và mạng đều xuất phát từ dữ liệu.

Thông thường khi quyết định lựa chọn một phương pháp bảo vệ máy tính thì dữ liệu giữ vai trò tiên quyết. Hệ điều hành và các ứng dụng có thể cài đặt lại, nhưng dữ liệu người được tạo bởi người dùng là duy nhất, nếu bị mất sẽ không có gì thay thế được, thậm chí còn có thể gây ra những thiệt hại vô cùng lớn cho cá nhân, tổ chức. Có rất nhiều nguyên nhân khách quan, chủ quan làm mất dữ liệu như lỗi hệ thống, virus hoặc tự tay xóa nhầm.

Ngoài ra một số dữ liệu rất bí mật, quan trọng chúng ta không muốn mất nó mà còn không muốn người khác xem nếu không được cho phép.

Trong giáo trình này sẽ cùng bạn đọc tìm hiểu một số biện pháp bảo vệ dữ liệu trên máy tính, tùy thuộc vào mức độ quan trọng và điều kiện riêng mà bạn có thể lựa chọn phương pháp phù hợp cho dữ liệu của mình.

Backup dữ liệu kịp thời và thường xuyên

- Bước quan trọng nhất trong việc bảo vệ dữ liệu khỏi bị thất lạc là thực hiện backup thường xuyên. Chúng ta cần thực hiện backup theo chu kỳ bao lâu? Điều này phụ thuộc vào lượng dữ liệu sẽ bị mất nếu hệ thống bị đánh sập hoàn toàn. Chúng ta có thể thực hiện backup hàng tuần, hàng ngày, hay hàng giờ.

- **Một số lỗi backup thường gặp**

+ Chúng ta có thể sử dụng tiện ích backup được tích hợp trong hệ điều hành Windows (ntbackup.exe) để thực hiện những tiến trình backup cơ bản, ngoài ra, có thể

sử dụng Wizard Mode để đơn giản hóa tiến trình tạo và khôi phục các file backup, hay có thể cấu hình thủ công các cài đặt backup và lên lịch thực hiện tác vụ backup để tự động hóa tác vụ này.

+ Ngoài công cụ trên, có rất nhiều công cụ backup nhóm ba khác với nhiều tùy chọn nâng cao hơn. Cho dù chúng ta lựa chọn công cụ nào, thì việc lưu trữ một bản copy dự phòng của file backup là rất quan trọng để đề phòng trường hợp những băng/đĩa chứa file backup bị phá hủy cùng với dữ liệu gốc. Hiện nay có một phương pháp rất hiệu quả mà chúng ta có thể sử dụng để lưu trữ dự phòng bản backup đó là backup trực tuyến.

- **Áp dụng bảo mật chia sẻ và bảo mật cấp độ file**

+ Để bảo mật dữ liệu, thao tác đầu tiên là cài đặt giấy phép cho file và thư mục. Nếu đang chia sẻ dữ liệu qua mạng, chúng ta có thể cài đặt các giấy phép chia sẻ để kiểm soát những tài khoản người dùng nào có thể hay không thể truy cập vào những file này qua mạng. Với Windows 2000 và Windows XP, chúng ta thực hiện cài đặt giấy phép bằng cách click vào nút Permissions trên tab Sharing của cửa sổ thuộc tính Properties của thư mục hay file.

+ Tuy nhiên, những giấy phép cấp độ chia sẻ sẽ không có hiệu lực với người dùng đang sử dụng máy tính lưu trữ dữ liệu chia sẻ. Nếu máy tính được nhiều người sử dụng thì chúng ta phải sử dụng các giấy phép cấp độ file (còn được gọi là giấy phép NTFS vì chúng chỉ xuất hiện trên những thư mục và file được lưu trữ trên phân vùng được định dạng NTFS). Những giấy phép cấp độ file, được cài đặt trong tab Security của hộp thoại thuộc tính Properties, bảo mật hơn so với các giấy phép cấp độ chia sẻ.

+ Trong cả hai trường hợp, chúng ta có thể cài đặt giấy phép cho tài khoản người dùng hay nhóm, và có thể cho phép hay từ chối nhiều cấp độ truy cập khác nhau từ read-only (chỉ đọc) tới toàn quyền truy cập.

- **Đặt mật khẩu bảo vệ tài liệu**

+ Một số ứng dụng, như Microsoft Office và Adobe Acrobat, cho phép chúng ta cài đặt mật khẩu trên nhiều tài liệu khác nhau. Để mở những tài liệu này chúng ta sẽ phải nhập vào mật khẩu đã cài đặt cho chúng. Trong Microsoft Word 2003, để đặt mật khẩu cho tài liệu, vào menu Tools | Options rồi click vào tab Security. Chúng ta có thể cài đặt mật khẩu mở file này và đặt mật khẩu chống chỉnh sửa. Ngoài ra chúng ta có thể cài đặt kiểu mã hóa được sử dụng.

+ Cách khóa thư mục bằng mật khẩu với lệnh file *.BAT

+ Một số phần mềm nén như WinZip hay PKZip cũng hỗ trợ cả tính năng mã hóa file nén.

- **Sử dụng mã hóa EFS**

+ Các hệ điều hành Windows từ Windows 2000 đến Windows 10 đều được hỗ trợ tính năng mã hóa Encrypting File System (EFS – mã hóa file hệ thống). Chúng ta có thể sử dụng phương pháp mã hóa tích hợp nền tảng giấy phép này để bảo vệ các file và thư mục riêng biệt được lưu trữ trên phân vùng định dạng NTFS. Thao tác mã hóa file và thư mục rất đơn giản, chỉ cần click vào nút Advanced trên tab General của trang thuộc tính Properties. Lưu ý rằng chúng ta không thể sử dụng kết hợp mã hóa EFS và nén NTFS.

- **Cách mã hóa file, thư mục bằng EFS trên Windows 10**

+ EFS sử dụng kết hợp mã hóa đối xứng và bất đối xứng cho cả bảo mật và thực thi. Để mã hóa file với EFS, người dùng phải có một giấy phép EFS, có thể được tạo bởi Windows Certification Authority, hay một giấy phép tự phân nếu không có Certificate Authority nào trên mạng. Các file EFS có thể được mở bởi tài khoản người dùng đã mã hóa chúng, hay bởi một tác nhân khôi phục chuyên dụng. Với Windows XP hay Windows 2003 chúng ta còn có thể chỉ định những tài khoản người dùng khác được phân quyền để truy cập vào những file được mã hóa bằng EFS.

+ Lưu ý rằng EFS được sử dụng để bảo vệ dữ liệu trên ổ đĩa. Nếu gửi một file được mã hóa EFS qua mạng và ai đó sử dụng một Sniffer (trình phân tích dữ liệu) để đánh cắp thì họ có thể đọc dữ liệu trong file này.

- **Sử dụng công cụ mã hóa ổ đĩa**

+ Trong một số phiên bản của Windows Vista, Windows 7, Windows Server 2008 và Windows Server 2008 R2 tích hợp một công cụ mã hóa ổ đĩa khá mạnh có tên BitLocker. Mặc định, công cụ này sử dụng bộ mã hóa AES (Advanced Encryption Standard) vận hành theo chế độ CBC (Cipher-Block Chaining).

- **BitLocker và EFS khác nhau như thế nào?**

+ Ngoài ra chúng ta có thể sử dụng nhiều công cụ mã hóa ổ đĩa nhóm ba khác cho phép mã hóa toàn bộ ổ đĩa. Khi mã hóa toàn bộ ổ đĩa, người dùng sẽ không thể truy cập vào dữ liệu trong đó. Dữ liệu sẽ được mã hóa tự động khi được ghi vào ổ đĩa này, và sẽ tự động được giải mã trước khi được tải vào bộ nhớ. Một số công cụ có thể tạo những vùng lưu trữ vô hình bên trong một phân vùng, sau đó hoạt động như ổ đĩa ẩn bên trong một ổ đĩa. Những người dùng khác chỉ có thể thấy dữ liệu trong ổ đĩa ngoài.

+ Những công cụ mã hóa ổ đĩa có thể được sử dụng để mã hóa ổ đĩa di động. Một số cho phép tạo một mật khẩu chủ cùng với những mật khẩu phụ với quyền thấp hơn để cấp cho những người dùng khác, như Whole Disk Encryption, Drive Crypt, …

- **Tận dụng Public Key Infrastructure**

+ Một Public Key Infrastructure (PKI) là một hệ thống quản lý những cặp Private Key và Public Key, và các giấy phép số. Do các Key và giấy phép được phát hành bởi một công cụ nhóm ba đáng tin cậy nên bảo mật nền tảng giấy phép mà hệ thống này cung cấp khá mạnh.

+ Chúng ta có thể bảo mật dữ liệu muốn chia sẻ với người khác bằng cách mã hóa dữ liệu này với một Public Key và người được chia sẻ. Tất cả người dùng trong mạng sẽ thấy dữ liệu này, tuy nhiên duy nhất người dùng có Private Key tương ứng với Public Key mới có thể giải mã.

- **Ẩn dữ liệu với kiểu mã hóa Steganography**

+ Steganography là một kiểu mã hóa tạo email ẩn trong đó chỉ có người gửi và người nhận mới biết đến sự tồn tại của email này.

+ Chúng ta có thể sử dụng một ứng dụng Steganography để ẩn dữ liệu bên trong dữ liệu khác. Ví dụ, chúng ta có thể ẩn một email văn bản trong một file ảnh .JPG hay một file nhạc MP3, …

+ Steganography không thực hiện mã hóa email, do đó nó thường được sử dụng

với các phần mềm mã hóa. Trước tiên dữ liệu sẽ được mã hóa, sau đó ẩn nó bên trong file khác bằng một phần mềm Steganography.

+ Một số công cụ mã hóa kiểu Steganography yêu cầu sự hoán đổi của một Key bí mật, trong khi đó số khác lại sử dụng Key mật mã Private và Public. Một ví dụ điển hình của phần mềm Steganography là StegoMagic. Đây là một phần mềm miễn phí giúp mã hóa email và ẩn chúng trong các file .TXT, .WAV, hay .BMP.

- **Bảo vệ dữ liệu gửi đi bằng cách bảo mật IP**

+ Dữ liệu của chúng ta có thể bị tin tặc đánh cắp khi đang truyền qua mạng bằng một phần mềm Sniffer. Để bảo vệ dữ liệu khi đang truyền qua mạng chúng ta có thể sử dụng Internet Protocol Security (IPSec), tuy nhiên cả hệ thống gửi và hệ thống nhận phải hỗ trợ IPSec. Kể từ hệ điều hành Windows 2000, Windows đã được tích hợp khả năng hỗ trợ cho IPSec. Các ứng dụng không phải nhận biết IPSec vì nó vận hành tại mô hình mạng cấp độ thấp.

+ Encapsulating Security Payload (ESP) là giao thức được IPSec sử dụng để mã hóa dữ liệu. IPSec có thể vận hành theo chế độ đường hầm để cung cấp khả năng bảo vệ tại cổng nối, hay trong chế độ truyền để cung cấp khả năng bảo vệ khi dữ liệu đang được truyền. Để sử dụng IPSec trong Windows, chúng ta phải tạo một chính sách IPSec, lựa chọn phương thức thẩm định quyền và những bộ lọc IP sẽ sử dụng. Để cấu hình những cài đặt của IPSec, mở cửa sổ thuộc tính Properties của giao thức TCP/IP trên tab Options của Advanced TCP/IP Settings.

- **Bảo mật dữ liệu truyền qua mạng Wifi**

+ Dữ liệu mà chúng ta gửi qua mạng Wifi dễ bị tác động hơn so với khi gửi qua mạng Ethernet. Tin tặc không cần phải truy cập vật lý tới mạng hay các thiết bị trên đó, bất cứ người dùng nào sử dụng laptop đã được kích hoạt Wifi và một ăng ten thu phát sóng mạnh có thể đánh cắp dữ liệu hay đột nhập vào mạng và truy cập vào dữ liệu được lưu trữ trên mạng đó nếu điểm truy cập Wifi không được cấu hình bảo mật.

+ Bảo mật WiFi từ những bước cơ bản

+ Chúng ta chỉ nên gửi và lưu trữ dữ liệu những mạng Wifi đã được mã hóa. Để mã hóa mạng Wifi, tốt nhất nên sử dụng WPA/WPA2 kết hợp với AES thay vì Wired Equivalent Protocol (WEP).

- **Sử dụng Rights Management để duy trì kiểm soát**

+ Nếu cần gửi dữ liệu cho những người dùng khác nhưng chúng ta lại lo lắng về việc bảo vệ dữ liệu này khi không còn nằm trên hệ thống của chúng ta nữa thì chúng ta có thể sử dụng Windows Rights Management Services (RMS) để kiểm soát hành vi của người nhận đối với dữ liệu họ nhận được. Ví dụ, chúng ta có thể phân quyền để người nhận có thể đọc tài liệu Word nhận được nhưng không thể hiệu chỉnh, copy hay lưu tài liệu này. Ngoài ra chúng ta có thể chặn người nhận chuyển tiếp email mà chúng ta gửi đi, hay cài đặt thời hạn sử dụng cho email hay tài liệu để người nhận không thể truy cập sau thời hạn đó.

+ Để sử dụng RMS, chúng ta cần cấu hình Windows Server 2003 như một máy chủ RMS. Người dùng cần sử dụng Internet Explorer hay cài đặt phần mềm máy trạm để truy cập vào các tài liệu được RMS bảo vệ. Những người dùng được phân quyền cần

phải tải một giấy phép từ máy chủ RMS.

- Hy vọng một số giải pháp trên đây có thể giúp cho máy tính cũng như dữ liệu của bạn an toàn hơn trong thời đại an ninh mạng đang bị đe dọa này.

2.6 Nâng cấp mạng

Chúng ta đã biết bảo mật WEP rất dễ bị crack, công nghệ bảo mật này chỉ bảo vệ được mạng không dây của bạn trước những người dùng thông thường. Còn ngoài ra, đối với các hacker, kể cả các hacker mới vào nghề cũng có thể download các công cụ miễn phí và thực hiện theo một hướng dẫn nào đó để crack khóa WEP của bạn. Sau khi phá được khóa, hacker có thể kết nối đến mạng Wi-Fi và truy nhập vào các tài nguyên chia sẻ chung trên mạng của bạn. Ngoài ra các hacker còn có thể giải mã lưu lượng thời gian thực trên mạng.

Chính vì lý do đó mà chúng ta cần sử dụng một công nghệ an toàn nhất để bảo vệ cho mạng không dây của mình: hiện tại đó chính là Wi-Fi Protected Access 2 (WPA2), đây là công nghệ sử dụng mã hóa AES/CCMP.

Có hai dạng thức của công nghệ WPA và WPA2: Personal hoặc Pre-shared Key (PSK) cho người dùng gia đình và Enterprise cho doanh nghiệp.

Chế độ Personal rất dễ trong cài đặt và sử dụng. Bạn có thể tạo một khóa mã hóa (giống như một mật khẩu) trên router không dây hoặc điểm truy cập. Sau đó nhập vào khóa này trên các máy tính và các thiết bị để kết nối với mạng Wi-Fi.

Chế độ Enterprise phức tạp hơn nhiều và yêu cầu một máy chủ ngoài, máy chủ này được gọi là RADIUS server, để kích hoạt nhận thực 802.1X. Tuy nhiên chế độ này thích hợp với việc sử dụng trong các doanh nghiệp. Bạn có thể tạo các username và password cho người dùng để sử dụng khi kết nối. Các khóa mã hóa thực không được lưu trên máy tính và thiết bị do đó sẽ bảo vệ cho mạng của bạn tốt hơn nếu chúng có bị mất hoặc bị đánh cắp.

Khi sử dụng chế độ Enterprise, bạn có thể thu hồi sự truy cập của người dùng khi họ không làm tại công ty của bạn nữa. Nếu sử dụng chế độ Personal, bạn sẽ phải thay đổi khóa mã hóa (trên tất cả các điểm truy cập và tất cả máy tính) mỗi khi một máy hoặc một thiết bị bị mất hay bị đánh cắp và khi có nhân viên nào đó rời công ty.

Kiểm tra các phương pháp bảo mật hiện hành

Nếu bạn không chắc chắn về phương pháp bảo mật mà mình đang sử dụng, hãy kiểm tra nhanh trong Windows bằng cách vào danh sách các mạng không dây có sẵn.

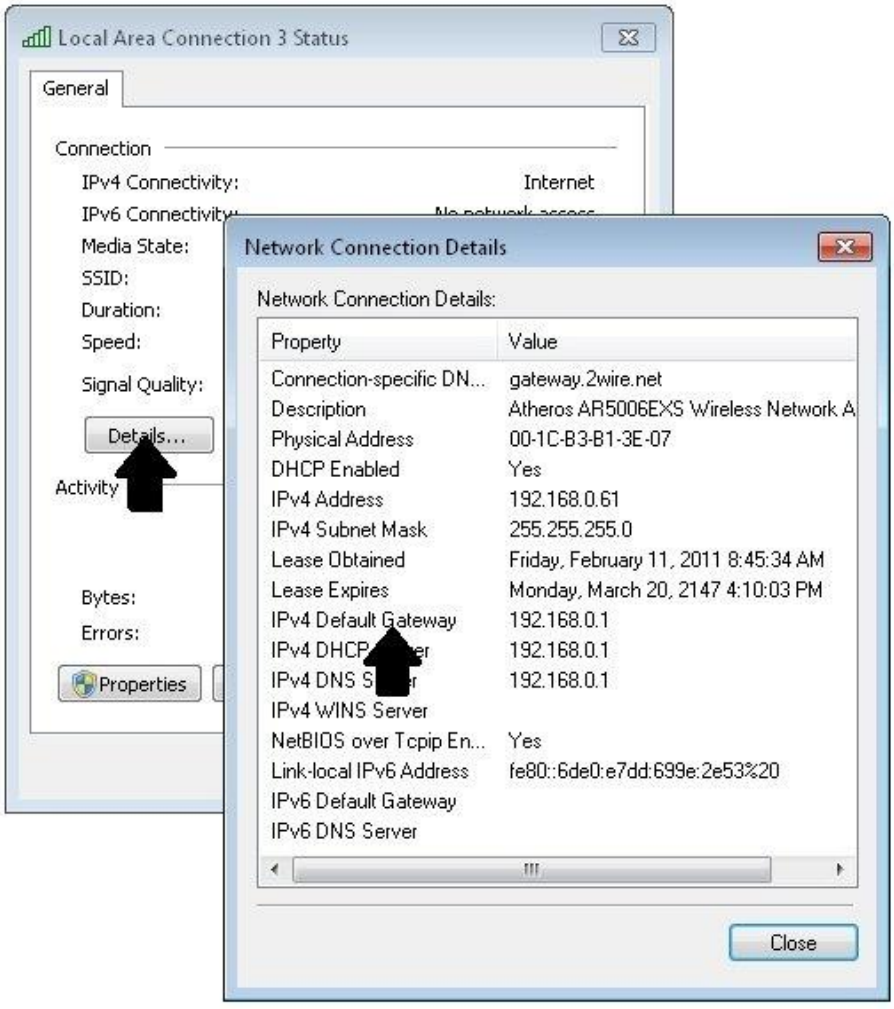
Trong Windows XP (tối thiểu ở đây là Service Pack 2), các mạng sử dụng một số kiểu bảo mật này sẽ có thông báo được bảo mật. Nếu đang sử dụng WPA hoặc WPA2, thông báo sẽ được hiển thị trong dấu ngoặc đơn, còn lại sẽ là trường hợp sử dụng WEP. Trong Windows Vista và Windows 7, bạn chỉ cần di chuột qua mạng nằm trong danh sách là có thể xem được các thông tin chi tiết, các thông tin này gồm có kiểu bảo mật.

Thẩm định tương thích WPA2

Hầu hết các sản phẩm Wi-Fi được sản xuất từ sau năm 2005 đều hỗ trợ WPA2. Nếu có một router không dây, các điểm truy cập, máy tính hay các thiết bị Wi-Fi khác được sản xuất trước 2005, bạn cần kiểm tra xem thiết bị của mình có hỗ trợ WPA2 hay không.

Để kiểm tra xem router không dây hoặc điểm truy cập có hỗ trợ WPA2 hay không, bạn hãy nhập địa chỉ IP của nó vào trình duyệt web, đăng nhập vào panel điều khiển và kiểm tra các thiết lập không dây.

***Lưu ý**: Nếu không biết địa chỉ IP của router là gì, hãy triệu gọi hộp thoại **Wireless Network Connection Status** trong Windows, kích nút **Details,** sau đó tham khảo phần **Default Gateway**. Xem hình.*



Hình 5.9 nâng cấp bảo mật mạng

***Lưu ý**: Nếu không nhớ mật khẩu, hãy tham khảo hướng sử dụng hay tìm kiếm trên Google để lấy mật khẩu mặc định. Nếu đã thay đổi mật khẩu mặc định, bạn có thể thiết lập lại mật khẩu mặc định nhà máy bằng cách giữ nút reset nhỏ ở phía sau router hay điểm truy cập không dây của mình.*

Nếu không thấy WPA2 trong các thiết lập bảo mật không dây của router hay điểm truy cập không dây, bạn có thể cần đến sự hỗ trợ từ các nâng cấp phần mềm bổ sung của nhà máy. Trong panel điều khiển, tìm các thông tin về hệ thống và trạng thái để kiểm tra xem phiên bản được cài đặt của phần mềm. Sau đó vào phần hỗ trợ trong website của nhà sản xuất và kiểm tra các desktop có sẵn cho model của bạn. Nếu có phát hành phần mềm mới nào cho thiết bị, hãy download nó và upload thông qua trang phần mềm trên panel điều khiển.

Nếu bạn có một số máy tính Windows, hãy cài đặt Service Pack 3, đây là phiên bản hỗ trợ WPA2. Kích **Start, right-click My Computer**, chọn **Properties**. Nếu đã cài đặt Service Pack 3, bạn sẽ thấy dòng chữ **"Windows XP Service Pack 3"**. Còn trong trường hợp không thấy, bạn hãy download và cài đặt bằng cách sử dụng Windows Updates.

Nếu đang sử dụng một adapter không dây cũ, adapter này có thể không hỗ trợ WPA2 nếu Windows hỗ trợ nó. Để kiểm tra sự hỗ trợ của nó trong Windows XP, mở hộp thoại **Wireless Network Connection Properties,** chọn tab **Wireless Networks**, kích **Add**. Bảo đảm **WPA2** có trong menu sổ xuống trong phần **Network Authentication**.

Nếu không thấy WPA2, bạn có thể tìm sự hỗ trợ từ các nâng cấp driver bởi nhà sản xuất. Kiểm tra phiên bản của driver đã được cài đặt: Mở hộp thoại **Wireless Network Connection Properties** trong Windows, kích nút **Configure**, chọn tab **Driver**. Sau đó vào phần hỗ trợ của website nhà sản xuất và kiểm tra các download tương ứng với model thiết bị của bạn.

Nếu có phiên bản driver mới hơn, hãy download và nâng cấp bằng cách thực hiện theo hướng dẫn của nhà sản xuất hay thông qua tab **Driver**.

Sử dụng WPA2-Personal (PSK)

Để kích hoạt bảo mật WPA2-Personal, bạn cần nhập địa chỉ IP của router không dây hay điểm truy cập vào trình duyệt web, đăng nhập vào panel điều khiển và sau đó tìm các thiết lập bảo mật không dây.

Nếu không biết địa chỉ IP của router hoặc không nhớ mật khẩu, bạn hãy tham khảo các lưu ý trong phần trước.

Khi tìm thấy phần các thiết lập bảo mật không dây, chọn bảo mật **WPA2** và mã hóa **AES**. Tiếp đó nhập vào 8 đến 63 ký tự làm **Pre-Shared Key** hoặc **Passphrase.** Cần biết rằng mật khẩu càng dài và càng phức tạp thì bảo mật của bạn càng an toàn. Thêm vào đó cũng nên sử dụng cả các ký tự in hoa và in thường cũng như các chữ số trong mật khẩu. Ghi mật khẩu ra giấy và cất giữ ở một nơi an toàn. Cuối cùng không được quên lưu lại các thay đổi mà bạn vừa thực hiện.

Lúc này bạn phải nhập vào cùng một mật khẩu trên các máy tính hoặc thiết bị được trang bị Wi-Fi. Trong Windows, bạn sẽ được nhắc nhở để nhập vào thông tin này khi kết nối. Tuy nhiên nếu đã từng sử dụng WEP hoặc WPA, Windows có thể không kết nối cho tới khi bạn sửa các thiết lập bảo mật đã lưu:

Trong Windows XP, kích đúp vào biểu tượng mạng không dây ở góc trên bên dưới, kích **Change the order of preferred networks**. Sau đó kích tên mạng và thay đổi Network Authentication thành **WPA2-PSK**, Data Encryption thành **AES** và nhập mật khẩu vào hai lần trong trường **Network Key**. Xem thể hiện trong hình.

Trong Windows Vista và Windows 7, triệu gọi danh sách các mạng không dây có sẵn, kích phải vào một mạng nào đó và chọn **Properties**. Sau đó thay đổi Security Type thành **WPA2-Personal**, Encryption Type thành **AES**, nhập vào mật khẩu làm **Network Security Key**.

Sử dụng WPA2-Enterprise

Trước khi có thể sử dụng WPA2-Enterprise, bạn phải chọn và cài đặt một máy chủ RADIUS server. Nếu đã có một Windows Server, bạn sẽ có thể sử dụng IAS hoặc NPS server. Các máy chủ RADIUS khác gồm có FreeRADIUS, Elektron và ClearBox. Lưu ý rằng một số điểm truy cập lớp doanh nghiệp (chẳng hạn như ZyXEL ZyAIR G-2000 Plus v2 sẽ có tích hợp các máy chủ RADIUS). Nếu không có kinh phí hoặc chưa có nhiều kinh

nghiệm trong việc điều hành một máy chủ riêng, bạn có thể sử dụng thông qua dịch vụ hosting, chẳng hạn như AuthenticateMyWiFi.

Câu hỏi ôn tập

- Kiểm tra và cho biết các sự cố về tường lửa, vấn đề cần bảo mật trên hệ thống mạng là gì?.
- Cài đặt 1 chương trình diệt virus và quét các loại virus máy tính xâm nhập vào mạng LAN.
- Trình bày phương pháp sao lưu, phục hồi dữ liệu thường xuyên, có định kỳ?
- Hãy nâng cấp mở rộng hệ thống mạng LAN đang sử dụng thành mạng MAN

Tài liệu cần tham khảo:

[1] Thiết kế & các giải pháp cho mạng không dây – NXB GTVT Tác giả: Nguyễn Nam Thuận – Năm 2004

[2] Giải Pháp Bảo Trì Mạng Nội Bộ - NXB Thống kê - Tổng hợp và biên dịch VN-GUIDE – Năm 2002

[3] Trang web http://quantrimang.com và các diễn đàn kỹ thuật công nghệ.

[4] Tài liệu bài giảng của VNPT về dịch vụ FiberVNN.