Bảo mật mạng Wi-Fi

Bảo mật mạng Wi-Fi giúp ngăn chặn người lạ mặt truy cập trái phép vào hệ thống mạng nội bộ.

Bảo mật mạng Wi-Fi có thể xem như việc gắn ổ khóa vào cửa, cách trao chìa khóa vào nhà đúng người. Do đó, sau khi thiết lập một mạng Wi-Fi mặc định trên modem/router Wi-Fi (ID: A1005_127), access point, thì bước quan trọng tiếp theo là thiết lập bảo mật cho mạng Wi-Fi sao cho an toàn nhất. Để minh họa bài viết, chúng tôi dùng modem/router ADSL của CISCO: LINKSYS WAG120N. Đây là một trong những thiết bị có đầy đủ các chế độ mã hóa mạnh nhất và các thiết lập bảo mật mạng Wi-Fi cho cả người dùng cá nhân, gia đình lẫn doanh nghiệp.

Trước tiên, bạn cần thay đổi tài khoản đăng nhập mặc định (username và password: admin) của LINKSYS WAG120N vì nếu tin tặc biết tài khoản đăng nhập mặc định, họ có thể truy cập vào thiết bị dễ dàng và thay đổi các thông số thiết lập trên đó. Bạn vào mục **Administration.Management,** nhấn chọn ô Modem Router User Name để đổi tên, chọn ô **Modem Router Password** để đổi mật khẩu và nhập lại mật khẩu đăng nhập lần nữa vào ô **Re-Enter to Confirm,** sau đó nhấn **Save Settings** để lưu các thiết lập.

Từ lúc này, để truy cập vào LINKSYS WAG120N, bạn cần đăng nhập với tài khoản mới thay đổi ở trên. Tiếp theo, bạn cần ẩn và thay đổi tên mạng Wi-Fi mặc định (SSID) - mặc định SSID sẽ được modem/router Wi-Fi phát quảng bá và bất kỳ ai cũng có thể "nhìn thấy", nên việc ẩn và thay đổi SSID là bước cần thiết trong bảo mật mạng Wi-Fi (Bạn chỉ nên ẩn tên mạng Wi-Fi nếu chỉ muốn cho một vài người trong gia đình/công ty sử dụng, còn trong trường hợp bạn thường xuyên có khách cần sử dụng Wi-Fi thì chỉ cần đổi tên mạng Wi-Fi mặc định là đủ).

Vào mục **Wireless.Basic Wireless Settings**, chuyển mục **Wireless Configuration** từ **Wi-Fi Protected Setup** sang **Manual**, sau đó thay đổi tên SSID trong phần **Network Name (SSID)**, chọn **Disable** trong mục **SSID Broadcast** rồi nhấn **Save Settings** . Lúc này, các thiết bị máy khách kết nối không dây (client): máy tính xách tay (MTXT), card mạng không dây, điện thoại di động, netbook... sẽ không thể phát hiện ra tên mạng của bạn. Để client truy cập mạng Wi-Fi, bạn cần cung cấp SSID và nhập thủ công trên mỗi máy.

Tiếp theo là phần khá quan trọng trong thiết lập bảo mật mạng Wi-Fi. Hiện nay, hầu hết các modem/router Wi-Fi đều hỗ trợ chế độ bảo mật WPA2/WPA/WEP, trong đó

WPA2 là chế độ bảo mật cao nhất, sau đó là WPA và cuối cùng là WEP - WPA/WPA2 dùng khóa mã hóa động (thay đổi theo thời gian định trước - mặc định là 3600 giây). Lời khuyên là bạn nên dùng mức bảo mật cao nhất mà thiết bị hỗ trợ để đảm bảo an toàn dữ liệu truyền qua mạng Wi-Fi. Trên LINKSYS WAG120N, vào mục **Wireless.Wireless Security**, chọn Security Mode là **WPA2-Personal** (thiết lập được đề nghị cho người dùng cá nhân, gia đình. Với doanh nghiệp có máy chủ xác thực Radius, nên chọn WPA2-Enterprise), tiếp theo chọn mã hóa **TKIP or AES**, và đặt khóa từ 8-63 ký tự trong ô **Pre-Shared** Key (bạn sẽ cung cấp khóa này cho những ai được phép truy cập vào mạng Wi-Fi của mình), nhấn Save **Settings** để lưu các thiết lập.

Để tăng cường thêm khả năng bảo mật cho mạng Wi-Fi, bạn có thể thiết lập lọc truy cập mạng Wi-Fi theo địa chỉ MAC (Media Access Control). Địa chỉ MAC là dãy số và ký tự duy nhất trên mỗi thiết bị mạng, tham khảo thêm bài viết (ID: A0911_120).

Tiêu điểm:

Những việc cần làm để bảo mật mạng Wi-Fi

- Thay đổi tài khoản đăng nhập mặc định của modem/router, access point.
- Ẩn và thay đổi tên mạng Wi-Fi mặc định (SSID).
- Thiết lập mã hóa mạng Wi-Fi.
- Thiết lập tính năng lọc truy cập mạng Wi-Fi theo địa chỉ MAC.

Việc lọc địa chỉ MAC giúp bạn xác định cụ thể máy tính nào được phép/không được phép truy cập mạng Wi-Fi. Vào mục **Wireless.Wireless MAC Filter**, chọn **Enable**, chọn **Permit**. Nếu các client đã truy cập vào mạng Wi-Fi, bạn có thể nhấn ngay nút **Wireless Client List** để ghi nhận các địa chỉ MAC, còn không thì bạn nhập thủ công từng địa chỉ MAC các client mà bạn cho phép truy cập. Sau đó nhấn **Save Settings** để lưu các thiết lập.

Ngoài ra, LINKSYS còn đem đến cho người dùng tính năng hỗ trợ thiết lập nhanh kết nối bảo mật mạng Wi-Fi rất hữu ích: **Wi-Fi Protected Setup**. Nếu client hỗ trợ **Wi-Fi Protected Setup**, trên modem/router LINKSYS WAG120N, vào phần Wireless.Basic Wireless Settings, chọn **Wi-Fi Protected Setup** rồi nhấn Save Settings, sau

đó thực hiện thiết lập nhanh kết nối bảo mật mạng Wi-Fi trên client:

Nếu client có nút **Wi-Fi Protected Setup**, nhấn nút này; sau đó trên WAG120N nhấn vào biểu tượng trong mục 1 phần Wireless.Basic **Wireless Settings** hoặc nhấn nút ở mặt trước modem/router.

- Nếu client có số PIN **Wi-Fi Protected Setup** thì nhập số PIN này vào mục 2 và nhấn nút **Register** trong phần **Basic Wireless Settings** của WAG120N.
- Nếu client yêu cầu số PIN của modem/router, hãy nhập dãy số ở mục 3 trên WAG120N vào client.

Việc bảo mật mạng Wi-Fi giúp ngăn chặn người lạ mặt truy

cập trái phép vào hệ thống mạng nội bộ. Với tất cả các sản phẩm modem/router Wi-Fi, access point của CISCO như LINKSYS WRT610N, LINKSYS WRT320N, LINKSYS WAP610N, LINKSYS WRT160NL, LINKSYS WRT160N, LINKSYS WRT120N, LINKSYS WAG160N... bạn đều có thể thực hiện các thiết lập bảo mật Wi-Fi tương tự như trên.

Một số kinh nghiệm bảo mật và "giữ gìn" mạng Wi-Fi

Chắc hẳn các bạn đều biết rằng Wi-Fi là một mạng không dây hoạt động nhờ vào sóng vô tuyến. Chính điều đó khiến cho hệ thống mạng Wi-Fi dễ dàng gặp phải các mối nguy hại từ phía bên ngoài.

Nếu bạn đang có ý định lắp đặt Wi-Fi cho gia đình thì mười quy tắc sau đây sẽ đảm bảo cho bạn một hệ thống Wi-Fi “sạch” và hoạt động một cách trơn tru. Còn nếu hiện tại bạn đang vận hành một hệ thống Wi-Fi tại nhà thì cũng không nên bỏ qua bài viết này vì nó sẽ đóng vai trò "giúp đỡ". Hãy kiểm tra xem mình đã làm đủ các yêu cầu cần thiết để có một mạng không dây hoàn hảo hay chưa nhé!

Tắt modem hoặc rút điện khi ngừng sử dụng mạng Wi-Fi

Đây là một thao tác đơn giản và rất hiệu quả nhưng đôi khi nhiều người lại quên thực hiện. Có nhiều lý do khiến bạn nên làm việc này. Thứ nhất, nó sẽ kéo dài tuổi thọ cho Router và đồng thời không phí phạm điện năng một cách vô ích. Thứ hai, nếu không tắt Router khi không sử dụng, nhiều khả năng bạn sẽ dễ dàng trở thành con mồi cho các tay hacker. Máy tính sẽ dễ dàng bị tấn công trong khi bạn không có mặt ở đó.

Nếu sử dụng hệ điều hành Windows XP, bạn hãy nhấn vào biểu tượng mạng không dây trên khay hệ thống rồi chọn **Disable**. Còn nếu bạn dùng Windows Vista hay Windows 7, để ngắt kết nối khỏi mạng Wi-fi, hãy click vào biểu tượng mạng trên khay hệ thống, sau đó phải chuột lên kết nối hiện tại và chọn **Disconnect.**

Cài đặt các phần mềm bảo mật cần thiết

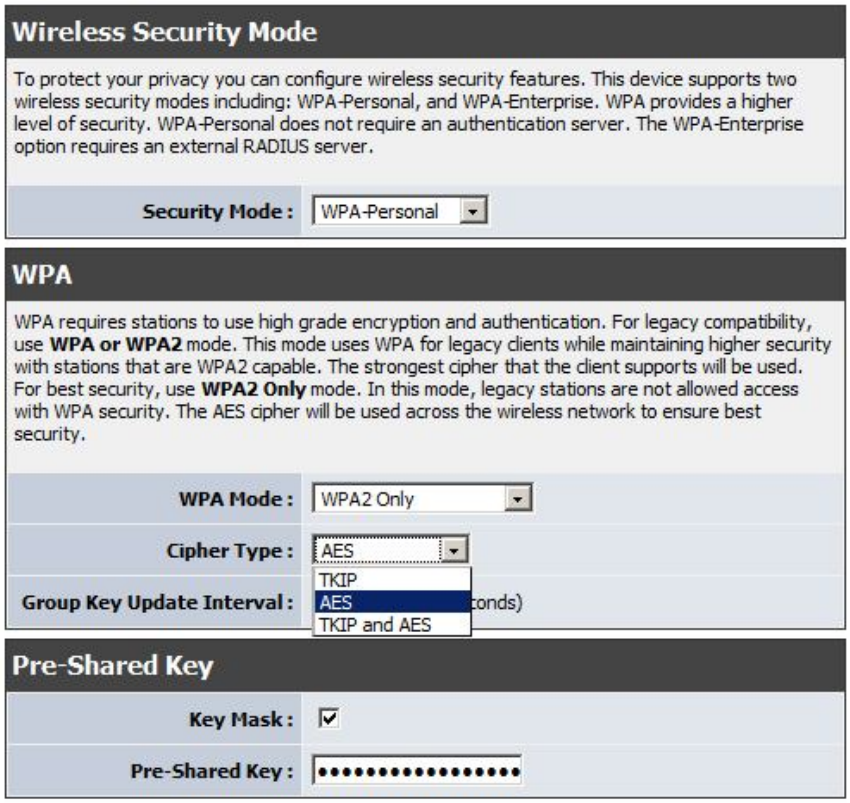
Có lẽ nhiều người sẽ cho rằng điều này khá thừa thãi khi bảo mật là vấn đề vô cùng quan trọng trong việc thiết lập và sử dụng mạng Internet không dây. Tuy nhiên, trên thực tế, vẫn có nhiều người dùng bỏ qua thao tác hết sức đơn giản này. Mạng Wi-Fi là một môi trường "mở", bởi vậy, việc bảo mật là hết sức cần thiết. Hãy luôn ghi nhớ điều đó.

Ngày nay, các phần mềm miễn phí dùng làm tường lửa, chống virus, trojan có chất lượng rất tốt và không hề kém cạnh so với sản phẩm đến từ các thương hiệu nổi tiếng như Norton, Kasperksy... Có thể kể ra một số cái tên tiêu biểu về khả năng bảo mật cũng như cách sử dụng dễ dàng như: *Panda Cloud Antivirus*, *AVG 9 Antivirus Free Edition*, *Comodo Internet Security Suite.*

Sử dụng mã hóa WPA2

Đặt password là điều hiển nhiên nếu bạn dùng mạng Wi-Fi tại gia, nhưng điều cần lưu ý đó là bạn nên sử dụng mã hóa WPA2. Cách thức mã hóa này sẽ đảm bảo an toàn cho dữ liệu khá cao. Bạn nên biết rằng, đối với những hacker cao tay thì việc ”bắt” dữ liệu

trong quá trình truyền tải là điều hoàn toàn có thể. Chính vì vậy, việc mã hóa dữ liệu là điều hết sức cần thiết. Với công nghệ mã hóa WPA2, bạn sẽ an tâm hơn trong quá trình sử dụng internet của mình.



Thêm vào đó, chỉ những người sở hữu password mới có thể kết nối với mạng của bạn. Còn lại những người

khác sẽ không thể kết nối và truy cập các file mà bạn chia sẻ - hoặc sử dụng kết nối internet cho các mục đích không hợp lệ. Lưu ý là tùy vào hãng sản xuất mà cách đặt password WAP2 khác nhau. Hãy truy cập vào website chính thức của hãng hoặc nhờ người bán tư vấn là những biện pháp hiệu quả nhất.

Không nên lạm dụng tính năng SSID

Các hệ thống Wi-Fi có tham số để phân biệt và được gọi là định danh mạng SSID (Service Set Identifier). Để kết nối vào một mạng Wi-Fi, máy tính phải tìm thấy thông tin về định danh mạng này.

Mặc định SSID của một hệ thống Wi-Fi được cấu hình cho phép bất kỳ máy tính nào cũng có thể tìm

thấy thông tin này. Để tăng tính bảo mật cho mạng Wi-Fi, người sử dụng có thể che giấu SSID bằng việc bỏ chọn yếu tố này.

Tuy nhiên, biện pháp này không phải là an toàn tuyệt đối. Bởi chỉ với một số công cụ, những kẻ tấn công (hacker) có thể dễ dàng dò ra SSID đã được ẩn đi này. Hơn nữa, việc che giấu SSID cũng gây khó khăn cho người sử dụng bình thường khi họ phải tự nhập tham số nếu muốn kết nối vào mạng Wi-Fi.

Từ bỏ sử dụng SSID và đầu tư vào các công cụ bảo mật khác là một kế hoạch khả thi mà bạn nên cân nhắc tới. Hiệu quả từ việc sử dụng SSID là không cao, đồng thời nó còn gây ra những khó khăn trong quá trình sử dụng Wi-Fi của bạn.

Bảo mật tuyệt đối các thông tin cá nhân

Các hình thức mua bán và thanh toán trên mạng ngày càng phổ biến. Nếu bạn thường xuyên sử dụng các dịch vụ giao dịch trên mạng thì việc phải cung cấp các thông tin cá nhân là điều hiển nhiển. Do vậy, điều đó sẽ hết sức nguy hiểm nếu bạn không có các biện pháp bảo vệ cần thiết.

Một lời khuyên nhỏ dựa trên kinh nghiệm của người viết là tuyệt đối không để trình duyệt lưu trữ các thông tin nhạy cảm của bản thân, đồng thời sử dụng các chương trình quản lý password như: Password Manager, Roboform Password Manager… Thêm vào đó, nên xóa hết lịch sử hoặc bộ nhớ tạm mỗi khi lướt web xong bằng mạng Wi-Fi.

Tắt bỏ chức năng chia sẻ file và máy in của Windows

File sharing là một chức năng cho phép những người dùng Windows chia sẻ file qua mạng LAN hoặc không dây. File sharing được hỗ trợ bởi giao thức riêng của Microsoft, gọi là NetBIOS. Mặc dù chức năng chia sẻ này tỏ ra rất tiện lợi cho người sử dụng, nhưng nó cũng gây ra nhiều nguy hiểm về mặt bảo mật thông tin.

Có những trường hợp người sử dụng thậm chí chia sẻ toàn bộ đĩa cứng chứa nhiều thông tin quan trọng mà không hề đặt mật khẩu, hoặc đặt mật khẩu rất đơn giản khiến kẻ tấn công có thể truy nhập dữ liệu một cách dễ dàng.

Một nguy hiểm tiềm tàng nữa nằm ở chỗ, mặc dù NetBIOS vốn chỉ được thiết kế để hoạt động trong mạng cục bộ (LAN) nhưng lại có thể hoạt động trên nền TCP/IP vốn là giao thức cho phép truy nhập trên diện rộng. Điều này dẫn tới nguy cơ lớn cho những cá nhân truy nhập Internet: họ có thể vô tình phơi mình ra trước các cuộc tấn công nhằm vào dịch vụ NetBIOS.

Tắt bỏ chức năng này nếu không thực sự cần dùng đến là một biện pháp bảo mật mà bạn nên áp dụng. Có rất nhiều cách chia sẻ file vừa dễ dàng vừa bảo đảm an toàn cho bạn.

Sử dụng bộ lọc địa chỉ MAC

Lọc địa chỉ MAC (MAC Filtering) là một trong những biện pháp hạn chế nạn truy cập Wi-Fi bất hợp pháp khá phổ biến. Với mỗi máy tính, ứng với một card mạng có một địa chỉ MAC tương ứng (do nhà sản xuất thiết lập). Hầu hết các Router Wi-Fi đều cung cấp tính năng chỉ cho phép những máy tính có địa chỉ MAC nằm trong danh sách được thiết lập mới được phép truy cập. Bởi vậy, sử dụng phương pháp này là cách tương đối hiệu quả trong việc hạn chế

được phần lớn những cuộc truy cập bất hợp pháp vào mạng Wi-Fi của bạn.

Tắt tính năng cấp phát IP tự động (DHCP)

Để truy cập được vào mạng, máy tính sử cần phải có thêm địa chỉ IP, bất kể là không dây hay có dây.

Thông thường các hệ thống Wi-Fi cũng được cấu hình mặc định cấp phát địa chỉ IP động cho các máy tính (chức năng DHCP). Để tăng mức độ an ninh, chúng ta nên tắt chức năng DHCP trên hệ thống Wi-Fi.

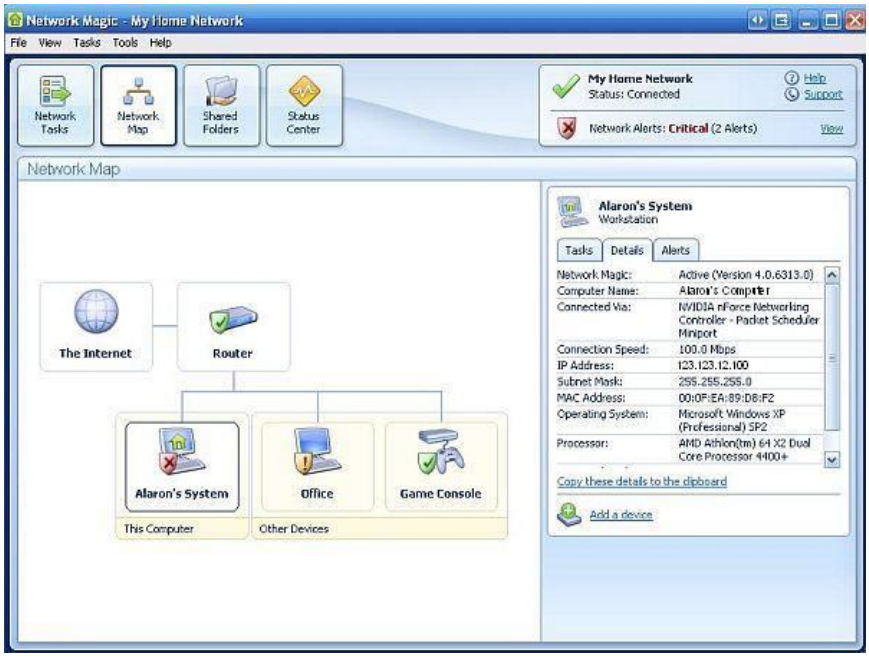
Tuy nhiên, kể cả khi đã bỏ chức năng DHCP, hacker vẫn có thể dò ra dải địa chỉ IP bằng các công cụ khác. Ngoài ra, việc bỏ tính năng DHCP cũng làm giảm tính tiện lợi vốn có của Wi-Fi. Do đó, có thể triển khai biện pháp trung gian là cho phép DHCP nhưng hạn chế, chỉ cấp IP cho các máy tính theo danh sách có sẵn (danh sách địa chỉ MAC).

Cả hai cách này không dễ thực hiện đối với người dùng phổ thông và khá rắc rối đối với những người mới sử dụng mạng Wi-Fi tại nhà. Chính vì vậy, bạn

cần hỏi người cung cấp mạng hoặc phân phối Router để có được những thông tin cần thiết hoặc yêu cầu họ cấu hình bảo mật cho mình.

Tạo mạng riêng ảo VPN kết hợp cùng việc theo dõi các thiết bị kết nối

Đối với những tay hacker chuyên nghiệp, họ đều có thể qua hết mọi cạm bẫy tự động mà bạn đã sắp đặt và đang "nhăm nhe" phá hoại hệ thống không dây mà bạn đã dày công xây dựng. Nếu các biện pháp tự động cũng không ăn thua thì lời khuyên dành cho bạn là thử sử dụng những phần mềm kiểm tra các thiết bị kết nào mạng của mình.



Để ngăn các cuộc xâm nhập lạ mặt, hãy tải về và cài đặt phiên bản miễn phí của Network Magic. Theo đó, chương trình sẽ vẽ ra một bản đồ tất cả các thiết bị đang hiện diện trên mạng bao gồm máy tính, máy chủ, máy in và các thiết bị khác. Nhờ vậy bạn có thể dễ dàng xác định thiết bị nào đang kết nối trong mạng và dễ dàng phát hiện ra kẻ lạ mặt.

10 mẹo bảo mật Wi-Fi

cho các nhân viên

Bảo mật Wi-Fi là một chủ đề rất phổ biến ngày nay, "phương pháp tốt nhất" hiện vẫn đang được tranh luận một cách mạnh mẽ trên nhiều forum. Chúng tôi nhận thức ra điều này từ việc theo dõi rất nhiều bài được post trên các forum và phát hiện ra có rất nhiều quan điểm đưa ra yêu cầu kết nối một cách an toàn với các mạng Wi-Fi hoàn toàn xa lạ.

Với quan điểm đó, chúng tôi muốn xem xét đến các mối quan tâm về bảo mật Wi-Fi từ quan điểm của nhân viên làm việc di động. Vì những người đi lại thường xuyên như vậy thường gặp các mạng Wi-Fi hoàn toàn xa lạ nên cần có một giải pháp cung cấp một số lợi ích cho những người trong hoàn cảnh này. Ở đây chúng tôi đưa ra 10 mẹo bảo mật mà các nhân viên trên đường nên biết để tránh các vấn đề về mất an toàn bảo mật với các mạng Wi-Fi không rõ tung tích.

1. Tắt adapter Wi-Fi client khi không sử dụng Internet

Lý do cho việc thực hiện này rất nhiều. Trước hết nó có thể tiết kiệm pin cho laptop của bạn – đây thực sự là một vấn đề với các nhân viên trên đường. Thứ hai, nó là cách đơn giản nhất để ngăn chặn các tấn công sử lợi dụng cấu hình của Windows được thiết lập một cách mặc định cho phép các kết nối ad hoc nặc danh.

2. Thẩm định rằng SSID tương ứng thực sự với mạng Wi-Fi của nhà cung cấp

Việc thẩm định SSID sẽ giúp bạn ngăn chặn được việc kết giao với một mạng xấu mang tên Evil twin. Evil twin được bắt chước sau tấn công xâm nhập của kẻ thứ ba bên ngoài, nơi

hacker thiết lập một thiết bị để đóng giả một mạng Wi-Fi tin cậy. Người dùng rất dễ sử dụng mạng giả mạo này và như vậy là cho phép kẻ tấn công có được các byte lưu lượng được gửi hoặc nhận.

3. Cài đặt phần mềm tường lửa trên máy tính của bạn

Microsoft Windows XP và Vista đều được kết hợp với một phần mềm tường lửa bên trong, tuy nhiên trong cả hai trường hợp đều thật sự chưa thích hợp. Thực sự có rất nhiều các ứng dụng phần mềm tường lửa miễn phí rất tốt cho phép bạn bảo vệ mình khi đi trên đường. Chúng tôi sử dụng Online-Armor, một ứng dụng mới đã có nhiều nhận xét đánh giá rất tốt về nó.

4. Vô hiệu hóa tính năng chia sẻ file và máy in của Windows

Mặc định, tính năng chia sẻ file và máy in của Windows được vô hiệu hóa, tuy nhiên nhiều người dùng kích hoạt tính năng này để chia sẻ các file và máy in trong công việc hoặc mạng ở nhà. Việc kích hoạt tính năng này khi di chuyển bên ngoài lại là một vấn đề. Nó có thể cho phép kẻ lạ mặt trong mạng Wi-Fi nào đó truy cập không thẩm định vào các file của bạn. Trong trường hợp này bạn nên tham về cách vô hiệu hóa tính năng chia sẻ file và máy in trong Windows trên QuanTriMang.com.

5. Tránh các phiên giao dịch trực tuyến nhạy cảm khi sử dụng mạng Wi-Fi mở

Đây là một việc hiển nhiên nhưng chúng tôi cảm thấy nó thực sự rất quan trọng cần phải đề cập đến.

6. Luôn cập nhật hệ điều hành của laptop

Cùng với hệ điều hành, bạn phải cập nhật luôn cả các phần mềm chống virus, tường lửa, trình duyệt web và cả các ứng dụng Wi-Fi client. Chỉ bằng cách như vậy bạn mới loại trừ được nhiều vấn đề gây ra bởi các lỗ hổng của ứng dụng.

7. Bảo vệ các thông tin cá nhân cũng như thẻ tín dụng, thẻ ngân hàng

Việc cho phép trình duyệt web nhớ các thông tin cá nhân là một cách cho các hacker có thể sử dụng để lấy về các thông tin nhạy cảm của bạn nếu laptop bị mất hoặc bị đánh cắp.

8. Sử dụng các kỹ thuật lướt Web an toàn và nặc danh

Điều này rất quan trọng nếu

một dịch vụ VPN không có sẵn hoặc VPN không được thiết lập đúng. Có nhiều dịch vụ Web khác nhau cung cấp các giải pháp SSL VPN bằng cách tạo một đường hầm được mã hóa từ laptop đến máy chủ an toàn của họ. Cách làm này đã loại trừ được toàn bộ các vấn đề nguy hiểm có thể. Một trong số các dịch vụ ưu việt đó phải kể đến là Megaproxy và TOR. Chúng tôi sử dụng một phương pháp khác nhẹ hơn dựa trên công nghệ USB flash drive. IronKey là một USB flash drive an toàn với FireFox và công nghệ TOR được cài đặt từ trước. Nếu truy cập Internet có sẵn thì thiết bị sẽ tự động cấu hình một đường hầm SSL đến các máy chủ IronKey an toàn.

9. Nếu được cần thiết hãy sử dụng công nghệ VPN

Vấn đề với các mẹo trước là nó áp dụng chỉ cho các ứng dụng nền tảng Web. Vậy thì các ứng dụng email như Outlook thì sao? Đây cũng là nơi VPN đang phát triển mạnh vai trò của

nó. Hầu hết các nhân viên trên đường đang làm nhiệm vụ đều sử dụng phương pháp này một cách chưa thực sự thấu đáo. Đường hầm VPN cho phép nhân viên có thể kết nối từ xa với mạng gia đình hoặc mạng công ty. Sau đó tất cả các ứng dụng doanh nghiệp thông thường, việc chia sẻ file và truy cập Internet đều được quản lý bởi mạng của công ty. Có nhiều phần cứng và ứng dụng VPN phần mềm để bạn có thể lựa chọn. Trong trường hợp này thì lựa chọn của chúng tôi đưa ra là OpenVPN.

10. Sử dụng các ứng dụng truy cập từ xa cho vấn đề bảo mật

Không có bất kỳ một lưu lượng dữ liệu nhạy cảm nào được truyền tải trên các mạng đáng ngờ đến laptop của bạn là một giải pháp duy nhất. Điều này có thể thực hiện bằng cách sử dụng một dịch vụ như LogMeIn, dịch vụ này sẽ cho phép các

nhân viên có thể điều khiển từ xa máy tính tại nhà hoặc văn phòng thông qua một đường hầm SSL. Việc lướt Web, email và các ứng dụng khác đều chỉ được thực hiện trên máy tính điều khiển xa. Chính vì vậy không có dữ liệu nào được truyền tải đến máy tính của người đang đi trên đường.

Kết luận

Những nhân viên làm việc trên đường phải thật sự thận trọng và sáng tạo. Bên cạnh các công việc thông thường, họ cần phải duy trì sự liên lạc một cách liên tục khi xa gia đình và văn phòng. Với các mẹo đơn giản này chúng tôi mong có thể giúp bảo vệ được máy tính của họ và các thông tin trên đó không gặp phải vấn đề gì trong bảo mật dù ở bất kỳ nơi đâu.

Hướng dẫn sử dụng, bảo mật mạng Wifi

Mạng không dây là một trong những phát minh lớn của thế kỷ 21. Thay vì phải sử dụng dây cáp để kết nối máy tính và các thiết bị với nhau, giờ đây, bạn đã có thể sử dụng sóng radio để kết nối. Công nghệ này đã được biết đến rộng rãi với cái tên 'Wifi'. Một khi được thiết lập chính xác, Wifi sẽ không gặp bất kì vấn đề nào cả. Tuy nhiên, để cấu hình chuẩn ở lần đầu tiên, bạn sẽ gặp rất nhiều khó khăn.

Kết nối Wifi rất dễ gặp một số vấn đề khó hiểu. Bên cạnh đó, cũng giống như những loại giao tiếp được gửi qua sóng radio, nó yêu cầu

người dùng phải tập trung nhiều vào phần cài đặt bảo mật nhằm tránh bị chặn dữ liệu bởi kẻ xấu.

Đó chính là lý do tại sao chúng tôi viết bài này. Bài viết sẽ cung cấp tất cả những gì bạn cần để mạng Wifi có thể chạy mượt và bảo mật nhưng không bao gồm thông tin hoặc ý tưởng để lướt web an toàn bằng mạng không dây khi truy cập ở điểm công cộng.

Bắt đầu bằng việc kiểm tra

Cho dù thiết lập một mạng không dây mới hoặc khi cần phải giúp một mạng hoạt động tốt, trước tiên bạn nên kiểm tra toàn bộ mạng, tất cả mọi thứ cấu thành nên mạng Wifi.

Trong điều kiện tốt nhất, mạng Wifi cần phải được cấu hình càng chạy nhanh và bảo mật càng tốt. Tuy nhiên, điều này rất khó thực hiện đối với những thiết bị cũ. Ví dụ, các thiết bị mới có thể hỗ trợ chuẩn Wifi mới nhất, nhưng những thiết bị được sản xuất nhiều năm trước đó thì có thể không.

Vậy nên, bằng cách kiểm tra tất cả các thiết bị đang kết nối (hoặc

sắp kết nối) với mạng Wifi để xem nó hỗ trợ chuẩn Wifi nào, người dùng có thể thiết lập cấu hình tốt nhất cho router.

Có 3 phần thông tin quan trọng cần ghi lại về mỗi thiết bị, có thể là một chiếc laptop, smartphone, game console, Internet radio, camera bảo mật không dây hoặc bất kì thiết bị nào sử dụng Wifi.

Trước tiên, chuẩn Wifi thiết bị hỗ trợ; tiếp theo, loại mã hóa nó có thể sử dụng; cuối cùng, địa chỉ **Media Access Control (MAC)** của thiết bị. Bạn có thể cần tham khảo hướng dẫn đi kèm để tìm ra 2 phần thông tin đầu tiên, hoặc tìm kiếm chúng trên mạng. Tuy nhiên, thông tin thứ 3 bạn có thể tìm thấy ngay trên thiết bị (chúng tôi sẽ hướng dẫn cách thực hiện sau).

Khám phá chuẩn Wifi

Wifi là thuật ngữ bao trùm cho 3 chuẩn giao tiếp không dây dù khác nhưng lại có liên quan tới nhau: **802.11b**,**802.11g** và **802.11n**. Vẫn còn một chuẩn thứ 4 – **802.11a** – nhưng ngày nay nó ít được nhắc đến hơn.

Những chuẩn này nhìn qua thì không có ý nghĩa gì cả, nhưng chúng lại là đại diện cho dữ liệu kỹ thuật được cung cấp bởi Viện kỹ nghệ Điện và Điện Tử (Institute of Electrical and Electronics Engineers – IEEE). Những dữ liệu này rất dài, miêu tả chi tiết về cách tương tác của các thiết bị không dây.

Chuẩn Wifi	802.11b		802.11a		
Phổ biến	✓✓✓	Sử dụng rộng rãi, nhiều nơi sử dụng	✓	Công nghệ mới	✓✓
Tốc độ	11 Mbps	Lên tới 11 Mbps (chú ý: dịch vụ cable modem chỉ lên được 4 - 5 Mbps)	54 Mbps	Lên tới 54 Mbps (gấp 5 lần 802.11b)	54 Mbps
Chi phí	$	Không đắt	$ $ $	Đắt hơn đôi chút	$ $
Tần số	2.4 GHz	Đông hơn ở băng thông 2.4 GHz. Một số xung đột có thể xảy ra với các thiết bị 2.4 GHz khác như điện thoại không dây, lò vi sóng,...	5 GHz	Không đông ở băng thông 5GHz có thể tồn tại cùng với 2.4 GHz mà không bị giao thoa	2.4 GHz
Phạm vi	100-150	Phạm vi phủ sóng tốt	25-75	Phủ sóng ngắn hơn so với 802.11b & 802.11g	100-150
Truy cập công cộng	✓		✗		✓
Tương thích	OK 802.11b	Được sử dụng rộng rãi	OK 802.11a	Không tương thích với 802.11b	OK 802.11b 802.11g

Dẫu vậy, rất dễ để "chắt lọc" từ những thông tin chi tiết này. Ví

dụ, **802.11n** là chuẩn mới và nhanh nhất hiện nay, có thể cung cấp phạm vi phủ sóng tốt nhất.

802.11b là chuẩn cũ và chậm nhất, với phạm vi phủ sóng ngắn nhất trong khi **802.11g** có vẻ như là sự kết hợp giữa 2 chuẩn trên. Một điều may mắn khác là những chuẩn Wifi mới vẫn tương thích với những chuẩn cũ. Vậy nên nếu bạn có chiếc máy tính xách tay có chuẩn Wifi **801.11n** cùng một chiếc router chỉ hỗ trợ **802.11g**, cả 2 thiết bị vẫn có thể kết nối với nhau ở tốc độ và phạm vi **802.11g**.

Trừ phi phát hiện ra có vấn đề liên quan đến tốc độ trên mạng không dây, bạn sẽ không phải lo lắng gì khi triển khai sử dụng thiết bị mới, hoạt động nhanh với một chiếc router cũ, chạy chậm.

Nếu router là mẫu mới hơn **802.11n**, nó cần được thiết lập chính xác để khai thác hết khả năng hoạt động.

Một mạng Wifi chỉ hoạt động ở tốc độ thấp nhất của thiết bị đang kết nối. Điều này có nghĩa là nếu một chiếc máy laptop **802.11b** cũ kết nối với chiếc router **802.11n** và chủ động sử dụng kết nối wifi,

thì kết nối Wifi của tất cả các thiết bị Wifi khác sẽ phải chậm lại để thích nghi với laptop.

Dẫu vậy, điều này không hẳn lúc nào cũng đúng trong thực tế. Theo lý thuyết, một số router cao cấp có thể duy trì nhiều tốc độ khác nhau trong cùng lúc – nhưng trong hầu hết các trường hợp, mạng sẽ bị chậm lại về tốc độ của thiết bị chậm nhất.

Xác định tốc độ của router

Bằng cách tìm hiểu chuẩn Wifi được hỗ trợ bởi những thiết bị Wifi, người dùng có thể xác định tốc độ phù hợp với mạng không dây – nó sẽ chạy ở tốc độ của thiết bị chậm nhất đang kết nối.

Bước tiếp theo là xem những gì có thể thay đổi trong cấu hình của router không dây nhằm tăng tốc độ. Một điều quan trọng cần nhớ là những lựa chọn xuất hiện trong cấu hình phụ thuộc rất nhiều vào mẫu và nhà sản xuất router. Dẫu vậy, chúng tôi sẽ cố gắng giải thích chi tiết nhất có thể.

Bắt đầu bằng việc đăng nhập vào trang cấu hình của router. Cách dễ

nhất để thực hiện điều này là mở một trình duyệt web và điền địa chỉ IP, ví như **192.168.2.1**, vào thanh **Address** hoặc **Location** ở trên cùng. Tuy nhiên, bạn sẽ cần phải tham khảo bản hướng dẫn để có được thông tin chính xác hơn.

Tiếp đến, tìm lựa chọn có tên **Wifi** hoặc **Wireless** và kích vào nó. Trong bảng cài đặt này sẽ có những lựa chọn để bạn chọn loại hình hoặc chế độ mạng không dây.

Ví dụ, ở router thử nghiệm có rất nhiều lựa chọn: **802.11b-only, 802.11g-only, both 802.11b and g (802.11b/g)**, cùng với 2 lựa chọn tốc độ cao khác.

Nếu tất cả các thiết bị Wifi của bạn hỗ trợ chuẩn **802.11g**, hãy chọn mạng **802.11g-only** để đảm bảo có tốc độ Wifi đầy đủ cho tất cả các thiết bị bằng cách ngăn chặn không cho kết nối tất cả những thiết bị có chuẩn**802.11b**.

Mặt khác, nếu bạn có chiếc router mới **802.11n** có dán nhãn “dual-band”, có một lựa chọn khác để nhận được tốc độ Wifi tốt nhất.

Router dual-band có thể hoạt động cùng lúc 2 mạng không dây khác nhau – một dành cho thiết bị **802.11b/g** và một cho thiết bị **802.11n**. Điều này có nghĩa là những máy hỗ trợ chuẩn **802.11n** có thể kết nối tới router này và không bị chậm khi có thiết bị **802.11b** hoặc **802.11g** kết nối. Điều này sẽ giúp người dùng có được kết hợp hoàn hảo của tốc độ cùng sự linh hoạt cao.

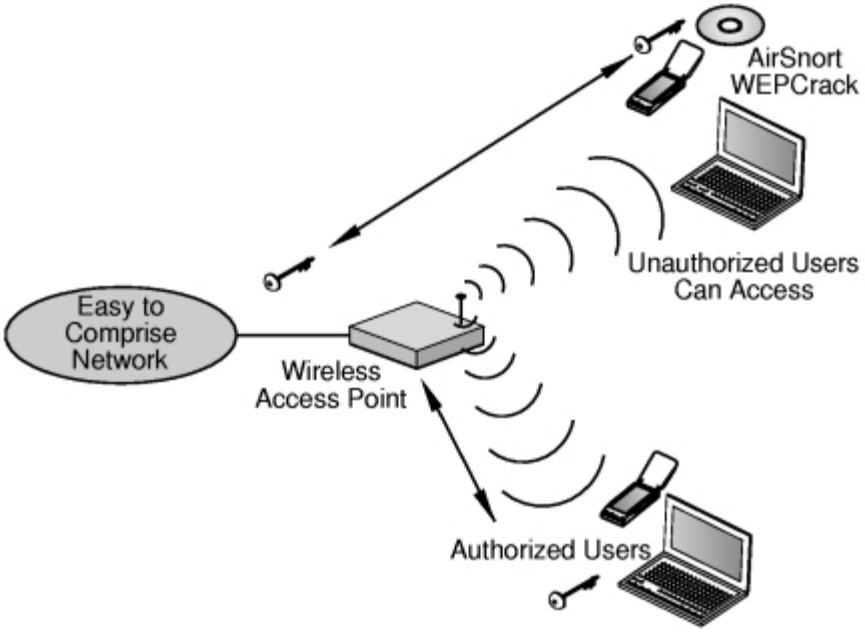
Dẫu vậy, một vấn đề khác lại nảy sinh. Router dual-band chỉ hoạt động khi chạy mạng **802.11n** ở khu vực có tần số vô tuyến 5GHz thay vì tần số thông dụng 2.4GHz.

Vấn đề nằm ở chỗ không phải tất cả các thiết bị **802.11n** đều có thể hoạt động với tần số cao, vậy nên hãy kiểm tra thiết bị của mình (qua hướng dẫn sử dụng hoặc qua trang web của nhà sản xuất) trước khi kích hoạt lựa chọn này hoặc bỏ tiền ra để nâng cấp router.

Kích hoạt mã hóa

Điều tiếp theo cần kiểm tra là loại hình mã hóa mạng không dây mà router hỗ trợ. Có 2 lựa chọn – **Wired Equivalent Privacy**

(WEP) và **Wifi Protected Access (WPA)** – và cả 2 đều ngăn chặn những thiết bị kết nối với mạng không dây mà không có mật khẩu cần thiết.



WEP là chuẩn cũ và được hỗ trợ rộng rãi nhất, nhưng giờ đây nó cũng được coi là mạng kém bảo mật bởi một mạng Wifi được bảo vệ bởi mã hóa WEP hoàn toàn có thể bị phá trong vòng vài phút. Sự thật là bạn không nên sử dụng chuẩn WEP một chút nào, nhưng nó lại là lựa chọn duy nhất đối với những thiết bị Wifi đời cũ.

Nếu hiện giờ bạn vẫn đang sở hữu thiết bị Wifi chỉ hỗ trợ chuẩn

WEP, chúng tôi khuyên bạn nên thay thế chúng bằng những thiết bị tương đương nhưng hỗ trợ chuẩn WPA hoặc dừng hẳn không sử dụng chúng nữa.

Hiển nhiên, đây không phải lựa chọn hoàn hảo khi máy tính vẫn còn chạy tốt. Tuy nhiên, Wifi tích hợp sẵn có thể cập nhật được bằng cách sử dụng chiếc USB Wifi adapter mới có hỗ trợ WPA. Dù không phải lựa chọn hoàn hảo, nhưng nó lại giúp cải thiện bảo mật cho thiết bị của bạn.

Mặt khác, nếu router của bạn chỉ hỗ trợ chuẩn WEP, lời khuyên của chúng tôi là thay thế chúng ngay lập tức.

Với chuẩn Wifi, bạn cần phải tham khảo hướng dẫn phù hợp hoặc qua trang web của nhà sản xuất để xem chuẩn mã hóa nào thiết bị của mình hỗ trợ. Nếu chúng đều hỗ trợ WPA, việc tiếp theo là kiểm tra mã hóa WPA đã được kích hoạt hay chưa.

Tìm kiếm trên trang cấu hình router để thấy cài đặt bảo mật hoặc mã hóa Wifi rồi chọn **WPA-TKIP** hoặc nhẹ nhàng hơn là **WPA2-**

PSK.

Nếu cần thiết, hãy tạo mật khẩu mới (nên chọn mật khẩu kết hợp giữa số, ký tự và chấm câu để khiến nó khó bị hack hơn). Bên cạnh đó, hãy nhớ rằng tất cả các thiết bị kết nối tới mạng sẽ cần phải nhập đúng mật khẩu vừa tạo.

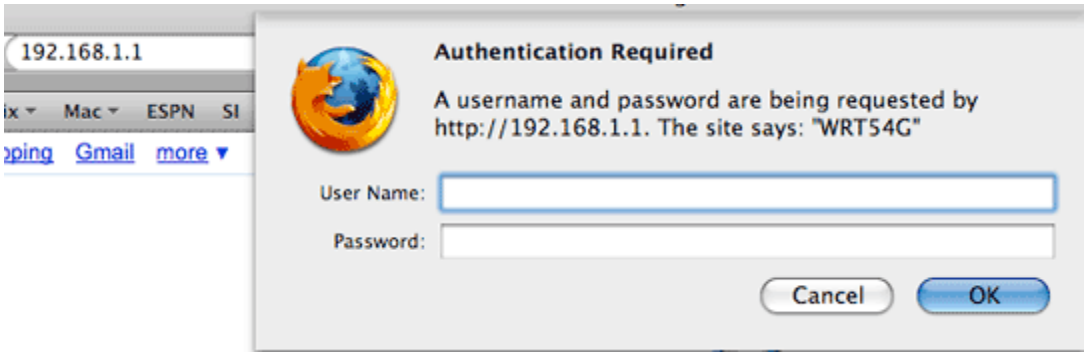
NHỮNG BƯỚC CƠ BẢN ĐỂ BẢO MẬT MẠNG WIFI

Bước đầu tiên để bảo vệ bất kì mạng không dây là thay đổi Password ngầm định của Router .

I. Bước đầu tiên

Bước đầu tiên để bảo vệ bất kì mạng không dây là thay đổi Password ngầm định của Router . Hầu hết những nhà sản xuất đều thiết lập Password ngầm định theo một số từ khoá sau như "admin" , "password" , và địa chỉ IP của Router hầu hết là "192.168.x.1" , ở đây x là 0,1 hoặc 15 .

Bước tiếp theo là kiểm tra cập nhật Firmware cho Router của bạn nếu như Model đó quá cũ . Nhiều Router không hỗ trợ những thiết lập an ninh tiên tiến như WPA , chúng ta sẽ nói sau .



II. Những câu chuyện hoang đường

Đôi khi bạn nhận được một số lời khuyên về bảo mật mạng không dây tồi từ một số người bán Router và đôi khi đó lại là những lời khuyên không có một chút ích lợi gì cả hoặc thậm trí còn gây khó khăn cho người sử dụng . Dưới đây là một số lời khuyên kiểu như vậy

Ẩn SSID

SSID (Service Set Identifier) là mã nhận dạng (thông thường là tên đơn giản) của Router không dây . Nếu thiết bị Wireless nhận ra nhiều SSID từ nhiều trạm AP (Access Point) , thông thường nó sẽ hỏi người dùng muốn kết nối tới SSID nào .

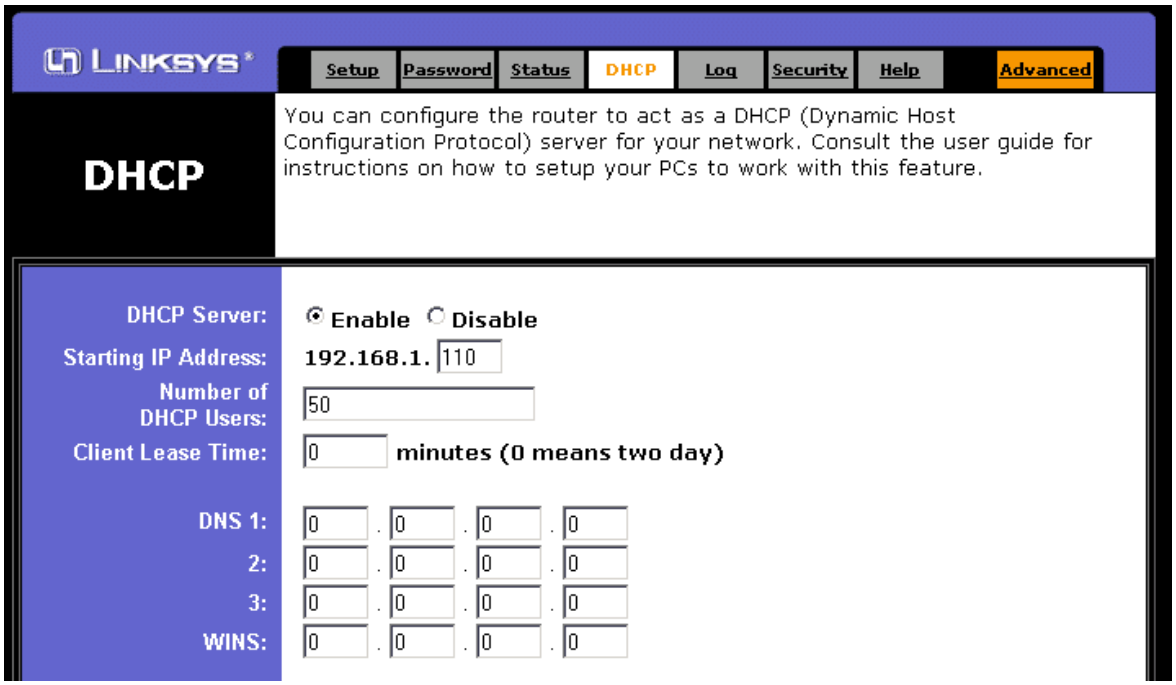
Việc ẩn SSID chính là ngăn chặn Phần mềm truy cập Wireless hiển thị mạng của bạn để lựa chọn phần kết nối , nhưng nó lại không phải là biện pháp an ninh mang tính thực tế . Bất kì lúc nào người dùng kết nối tới Router , SSID được truyền theo kiểu một đoạn văn bản được mã hoá và thông tin SSID đều có thể bị ai đó thấy được mạng trong Mode thụ động .

Thay đổi SSID

Đôi khi phương pháp này cũng được cho là một hình thức bảo vệ , nhưng thực tế lại hoàn toàn khác . Nó không ngăn chặn việc nhận dạng ra Router và vẫn bị Hack bất kì lúc nào .

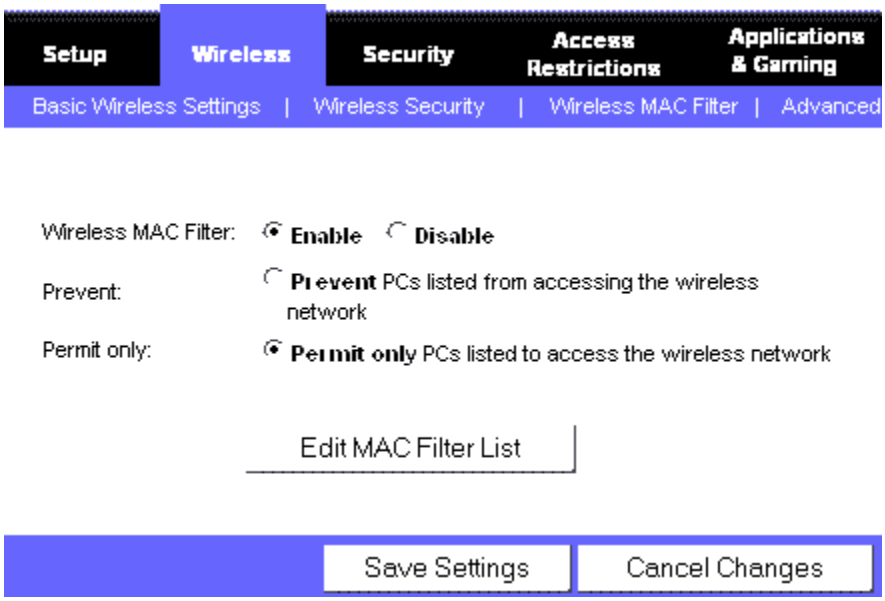
Disable DHCP

Việc tắt DHCP và dùng địa chỉ tĩnh không chống lại được những kẻ khác cố tính chõ mũi vào công việc của bạn . Những Hacker có thể gán những địa chỉ IP và theo phương pháp hỏi đáp để tìm ra những địa chỉ IP của bạn .



Sử dụng bộ lọc địa chỉ MAC

Theo lí thuyết có vẻ như rất hoàn hảo . Mọi Card mạng đều có địa chỉ MAC duy nhất , và Router không dây có thể được đặt cấu hình để chặn tất cả những Card mạng có địa chỉ MAC khác . Tuy nhiên vấn đề ở đây chính là bộ lọc địa chỉ MAC mà địa chỉ này dễ dàng bị làm giả mạo và không khó khăn gì để nhận dạng bằng một phần mềm theo dõi thích hợp . Bên cạnh đó nếu trong ngôi nhà của bạn lại có nhiều thiết bị truy cập tới Router như Console , điện thoại và thiết bị gia dụng thì việc phát hiện ra những địa chỉ MAC này càng trở nên dễ dàng .



Tất cả những biện pháp an ninh trên là không thực tế , với việc sử dụng bộ lọc địa chỉ MAC là mức độ bảo mật thấp nhất . Để ngăn chặn những kẻ xâm nhập mạng tốt nhất bạn nên dùng phương pháp mã hoá (Encryption) .

III. Những phương pháp mã hóa - Encryption

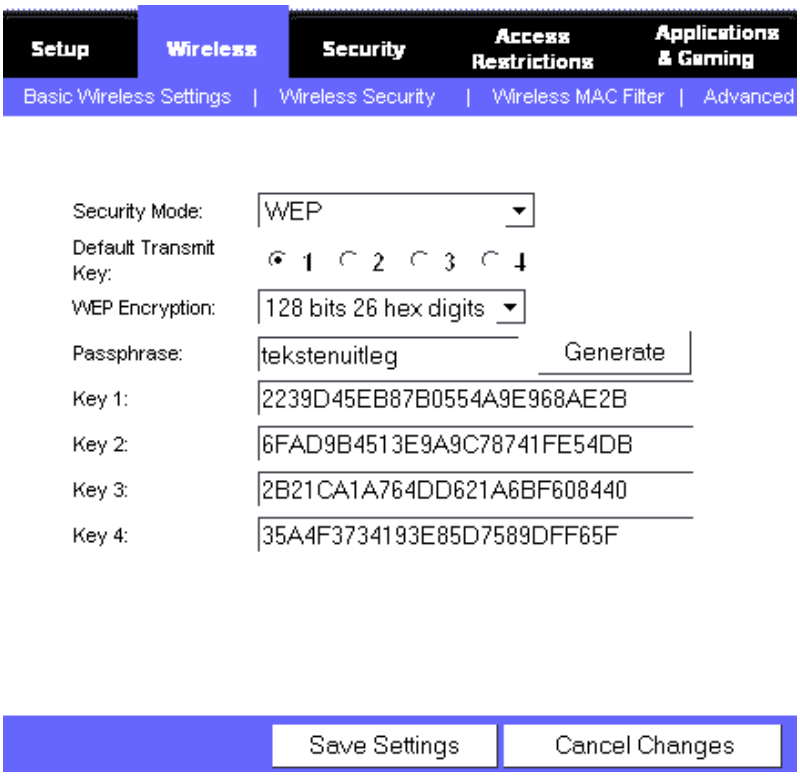
WEP (Wired Equivalent Privacy) và **WPA** (Wi-Fi Protected Access) là hai chuẩn mã hoá được dùng rộng rãi hiện nay trong những thiết bị không dây . Trong hai chuẩn trên WPA là mạnh hơn cả và có thể dùng trong mọi tình huống mà tại đó đã sẵn sàng .

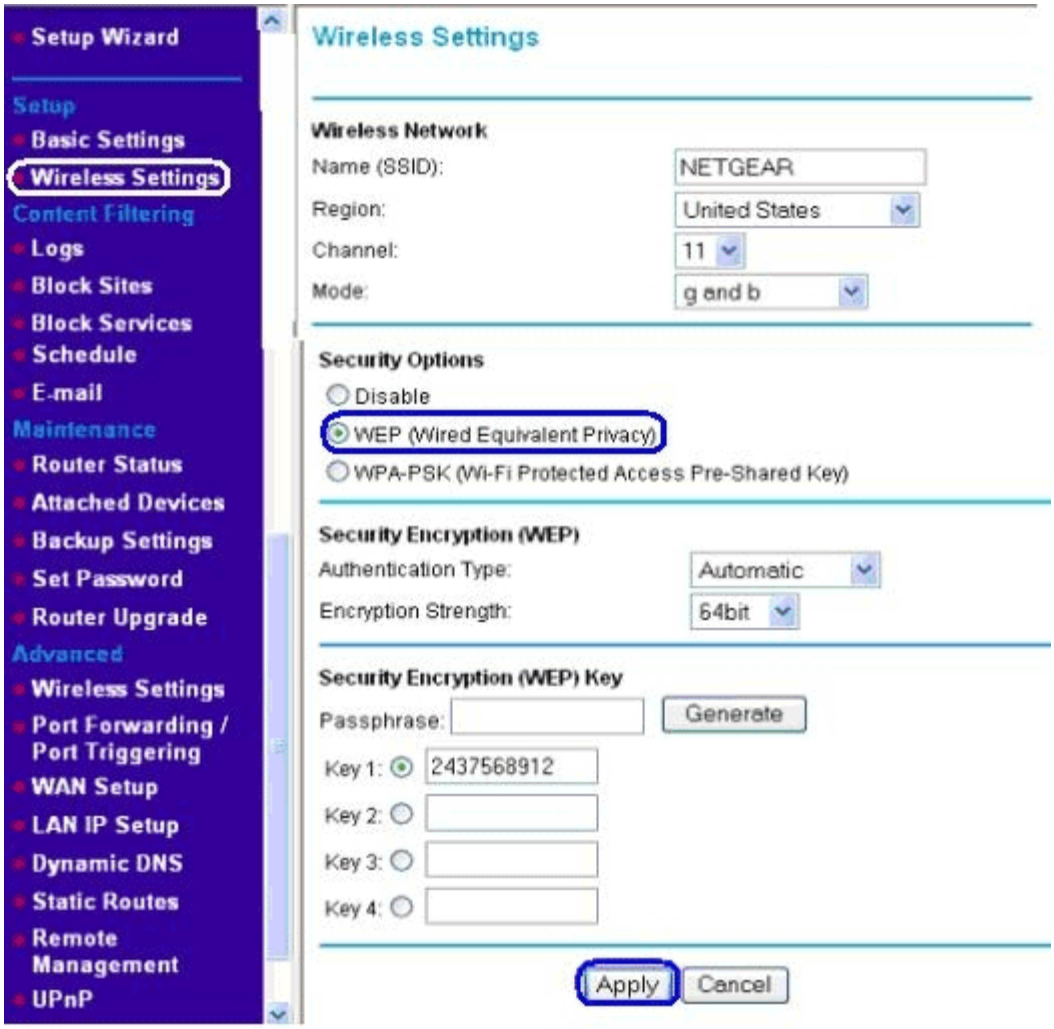
WEP : cũ kĩ , đã bị loại bỏ , nhưng tốt hơn là không có gì

WEP là giao thức an ninh Wireless đầu tiên . Ban đầu WEP dùng khoá mã 40-bit , nhưng về sau mở rộng lên tới 104-bit . Tuy nhiên về sau những nhà nghiên cứu đã thành công khi bẻ khóa WEP 104-bit trong hai phút bằng máy tính Pentium-M loại cũ .

Thật không may mắn khi mà những thiết bị sử dụng WEP vẫn còn chiếm tới 25% trên thị trường và dữ liệu bị đánh cắp lớn nhất trong lịch sử nước Mỹ chính là trong trường hợp mã hoá WEP .

Bây giờ mã hoá WEP 104-bit có thể bị bẻ gẫy một cách dễ dàng , vì thế chuẩn này sẽ không còn tồn tại được lâu nữa do độ an toàn kém .





Mặc dù yếu như vậy , lỗi như vậy nhưng WEP vẫn còn dùng tốt hơn là trong Router của bạn không đặt gì cả , và ít nhất cũng ngăn chặn người hàng xóm lướt Web trên mạng của bạn .

Có một số chuẩn mã hoá dựa trên WEP khác được đề cập như WEP2 . WEP2 là sự cố gắng tồn tại trong thời gian ngắn với cải tiến những chuẩn ban đầu bằng kết hợp cả từ khoá 128-bit với giá trị Vector 128-bit . WEP2 lại không cải thiện bất kì những gì mà yếu kém của WEP nhưng nó làm cho những Hacker khó khăn hơn khi bẻ khoá và tất nhiên WEP2 tốt hơn chuẩn WEP ban đầu .

Một số nhà sản xuất khác đã phát triển công nghệ riêng của mình sửa những lỗi của WEP . Những kiểu này yêu cầu kết hợp WEP với những Adapter riêng và hiệu quả đem lại cũng rất to lớn . Tuy nhiên giải pháp này chỉ sử dụng khi mà không còn có giải pháp nào tốt hơn .

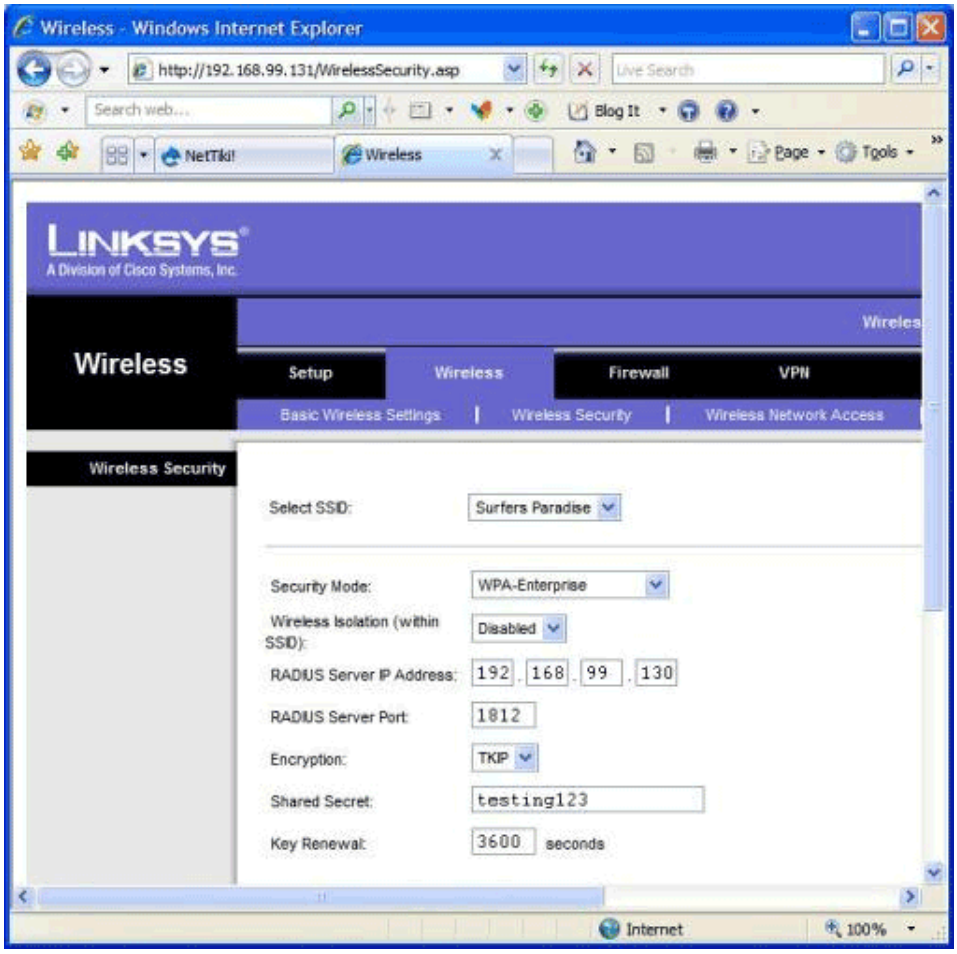
WPA và WPA2

WPA được phát triển để bù lại những lỗi trong WEP và nó là giao thức bảo mật tốt hơn . Không như WEP , WPA dùng Vector 48-bit và từ khoá mã 128-bit . Quan trọng hơn cả WPA dùng giao thức TKIP (Temporary Key Integrity Protocol) .

WEP sử dụng lại cùng từ khoá để mã hoá tất cả gói dữ liệu được truyền trên mạng , trong khi đó TKIP của WPA thay đổi khoá mã mọi thời điểm khi gói dữ liệu được truyền đi . Điều đó lại kết hợp với sử dụng từ khoá dài hơn khiến cho những Hacker không thể có kịp thời gian để xâm nhập được vào gói truyền dữ liệu .

Chuẩn WPA2 được cập nhật từ năm 2004 với những tính năng của WPA được hỗ trợ từ phía chính phủ Mỹ và sử dụng giao thức mã hoá gọi là AES (Advanced Encryption Standard) . Bây giờ AES cũng được dùng với WPA phụ thuộc vào Firmware trong Router .

Không như WPA , WPA2 lại không tương thích ngược ; những Router cũ hơn có khả năng mã hoá WPA với TKIP không thể dùng được WPA2 . WPA2 lại tương thích cả AES và TKIP . Nếu có khả năng bạn nên thay thế WPA bằng WPA2 .



Có hai mức độ an ninh bên trong WPA và WPA2 đó là WPA Personal (hoặc WPA-PSK) và WPA Enterprise .

WPA-Personal dùng khóa xác nhận được chia xẻ trước giữa tất cả các hệ thống trong mạng . Điều đó có nghĩa là mạng này ẩn chứa việc dễ bị xâm nhập bằng cuộc tấn công "dựa trên từ điển" nếu Password sử dụng không đủ mạnh . Những mạng tại gia đình không quá lo lắng về điều này nếu bạn không làm lộ bí mật của từ khoá .

WPA Enterprise được dùng cho những máy chủ RADIUS (Remote Authentication Dial User Service) riêng biệt . Trong trường hợp này những thiết bị muốn truy cập tới Access Point (AP) phải có những yêu cầu kiểm tra chứng nhận riêng biệt . AP chuyển yêu cầu và bất kì thông tin kết hợp tới máy chủ RADIUS . Máy chủ RADIUS kiểm tra chứng nhận này tại dữ liệu lưu trữ trong đó và nó có thể cho phép người dùng truy cập hoặc từ chối hoặc phản hồi lại những thông tin khác như Password thứ hai hoặc nguồn tương đương .

Những máy chủ RADIUS thông thường dành riêng cho khai thác trong môi trường xí nghiệp , tại đó chúng cung cấp thêm hai mức độ bảo vệ và tăng mức độ điều khiển tài nguyên trên hệ thống mạng cho mỗi người sử dụng . Như vậy nó nằm ngoài phạm vi sử dụng máy tính tại gia đình .

Tóm lại nếu như bạn đã hiểu một cách đầy đủ những thuật ngữ trên thì muốn cấu hình chế độ bảo mật hãy dùng giao thức WPA kết hợp với từ khoá mạnh . WPA2 dựa trên AES an toàn hơn WPA dựa trên TKIP và cả hai giải pháp này an toàn hơn hẳn so với WEP .

IV. Bảo mật cho mạng Media của bạn

Hiện nay mạng không dây là đặc tính chung của nhiều kiểu thiết bị dân dụng . Tất cả những Console thế hệ hiện tại đều hỗ trợ kết nối không dây và tính năng này có trong mọi thiết bị như máy tính xách tay , thiết bị cầm tay hoặc những thiết bị kết nối Internet kiểu bảng . Mạng không dây có mặt khắp mọi nơi nhưng có sự khác nhau trong các thiết bị mạng và cùng kiểu thiết bị sẽ chia xẻ mạng được tốt hơn . Rất khó để tìm ra cùng chuẩn mã hoá trong tất cả các thiết bị .

Bảng dưới đây trợ giúp phần nào cho bạn để có thể đồng bộ thiết lập chế độ an toàn giữa những thiết bị phần cứng khác nhau

Thiết bị	WEP	WPA-PSK	WPA2-PSK
PlayStation Portable	Có	Có	Không
Nintendo DS	Có	Không	Không
PlayStation 3	Có	Có	Có
Wii	Có	Có	Có
Xbox 360 WiFi adapter	Có	Có	Không
iPhone	Có	Có	Có
Nokia N800/N810	Có	Có	Có
Asus Eee PC	Có	Có	Có*

* Phần cứng Eee PC hỗ trợ WPA2 , nhưng hệ điều hành Asus Linux cài đặt không sử dụng được khả năng này

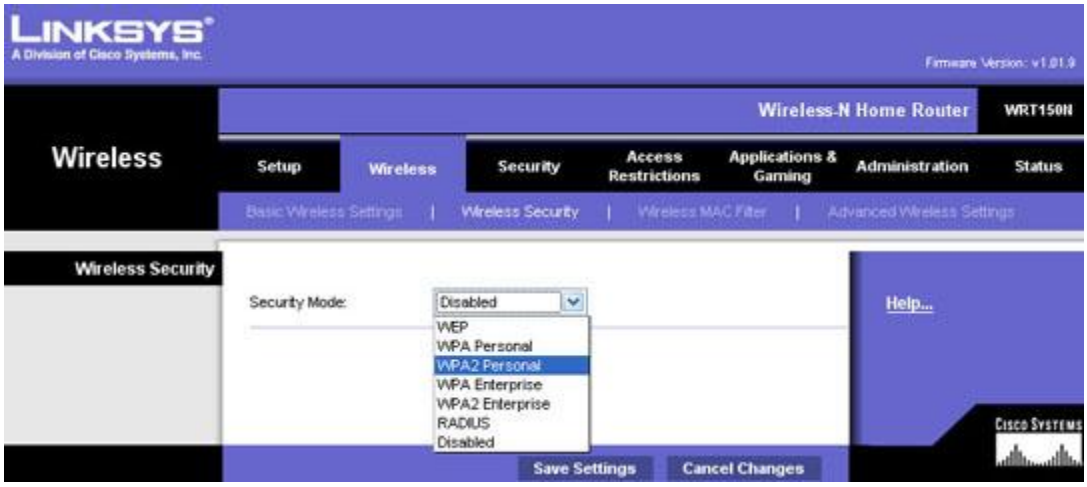
Bảng trên liệt kê hầu hết những thiết bị có khả năng sử dụng Wi-Fi . Tin tốt là tất cả trong số những thiết bị trên đều hỗ trợ một số kiểu mã hoá . Tin không tốt ở đây là sự lựa chọn giữa TKIP và EAS rất phức tạp . Ví dụ , Nintendo Wii hỗ trợ AES cho cả WPA và WPA2 , nhưng lại không hỗ trợ TKIP cho WPA2 . Do đó nếu bạn muốn khả năng tương thích cao nhất trong những thiết bị của bạn thì chọn Router thiết lập đầu tiên là WPA2 (AES) hoặc thứ hai là WPA (TKIP) .

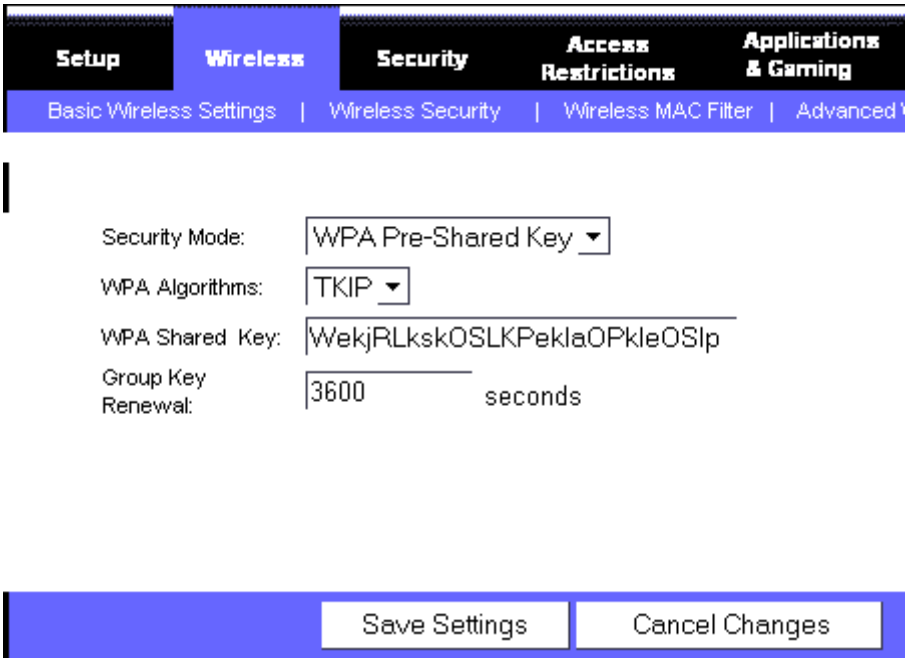
Thật không may mắn khi Nintendo DS lại vô cùng đơn độc vì nó chỉ hỗ trợ WEP . Vì thế nếu có kế hoạch sử dụng mạng không dây có cả Nintendo DS thì bạn đang mắc kẹt với những vấn đề vềv giao thức bảo mật cũ . Nintendo DS thực sự không cần thiết để được bảo vệ tối đa vì những Hacker chẳng làm gì với nó cả thậm trí cả khi họ đã xâm nhập vào đó .

Ngoài Nintendo DS thì thực hiện với WPA rất dễ dàng . Tất cả những thiết bị khác đã được liệt kê trên đều hỗ trợ WPA và hiện tại cũng dễ dàng mua Router cũng hỗ trợ WPA . Tuy nhiên với WPA2 điều này sẽ hơi khác một chút , chuẩn mã hoá mới nhất này không tương thích ngược với hầu hết WPA thông dụng hiện nay . WPA2 an toàn hơn WPA , nhưng dù sao WPA cũng là chuẩn an toàn có thể chấp nhận được và vẫn là giải pháp chung nhất .

Cho phép chuẩn an ninh của mạng không dây

Thực tế kích hoạt chế độ chuẩn an ninh rất đơn giản . Dưới đây là hình ảnh của Router Linksys WRT150 (802.11n Draft 2.0) và quá trình này cũng tương tư như trong những các thiết bị khác .





Chúng ta đang loại bỏ WEP vì thế bạn thực sự không cần dùng tới nó và chỉ tập trung vào những lựa chọn trong WPA .

WPA Personal (hoặc WPA – PSK) và WPA2 Personal được cấu hình gần như tương tự nhau , chọn phương pháp mã hoá (TKIP hoặc AES) và vào từ khoá mã hoá . Bạn có thể không cần thay đổi thời gian thay đổi từ khoá ngầm định (3600 giây) nhưng nếu muốn bạn có thể làm điều đó . Từ những thông tin này bạn sẽ đặt cấu hình cho Card mạng không dây trong máy tính của mình phù hợp là được .

Kết luận

Thực tế rất dễ dàng để bảo mật mạng không dây . Bạn không cần mất thời gian để cấu hình địa chỉ MAC bằng tay hoặc Disable DHCP khi mà chỉ cần cho phép chuẩn mã hoá phù hợp là được rất nhanh chóng , dễ dàng và hiệu quả tốt nhất .

WPA2 (AES) là phương pháp mã hoá tốt nhất hiện nay , tiếp theo là WPA2 (TKIP) , WPA (AES) , WPA (TKIP) và WEP .

Bất kì Router nào hiện tại cũng có WPA là cũng quá đủ để bảo vệ và chỉ dùng WEP khi mà phải dùng đến mà không còn biện pháp nào khác còn hơn là truyền dữ liệu mà không bảo vệ gì cả .

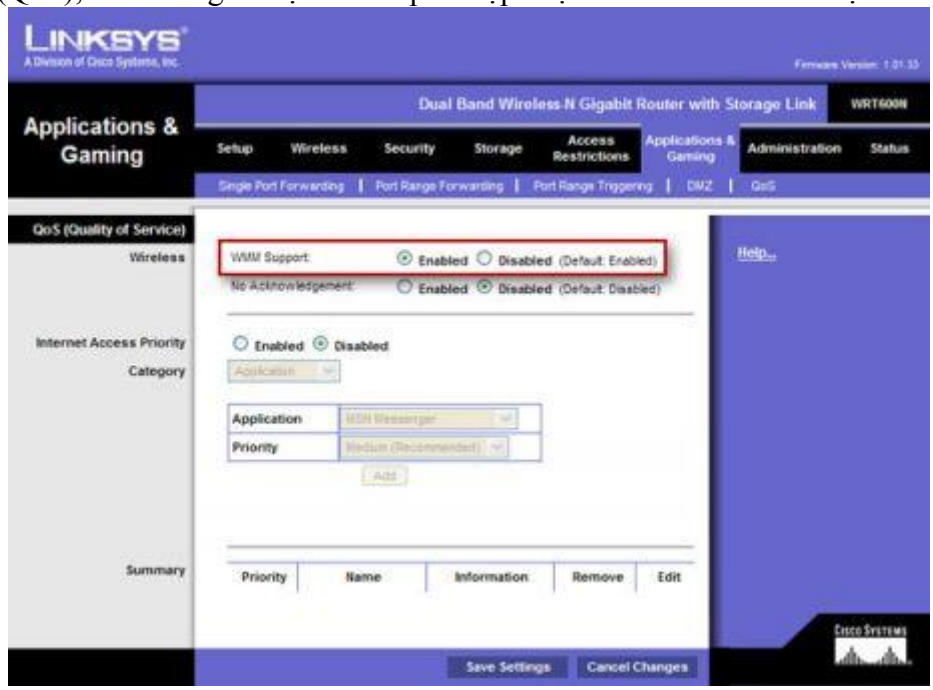
(sưu tầm)

Cách nâng cao tính năng và bảo mật cho mạng WIFI

Bạn hoàn toàn thỏa mãn với hệ thống mạng không dây Wi-Fi tại nhà hay tại văn phòng. Điều này cho thấy hai mặt tốt và xấu. Mặt tốt là xin chúc mừng bạn hệ thống mạng hoạt động khá tốt nhưng mặt xấu là gần như chắc chắn việc kiểm tra tính bảo mật và tăng tốc độ thực thi ít được quan tâm. Các bước sau đây sẽ giúp cho hệ thống mạng không dây hoạt động mạnh mẽ hơn và dữ liệu của bạn an toàn hơn.

1. Tối ưu hóa Wi-Fi cho các dịch vụ VoIP, Video và chơi game

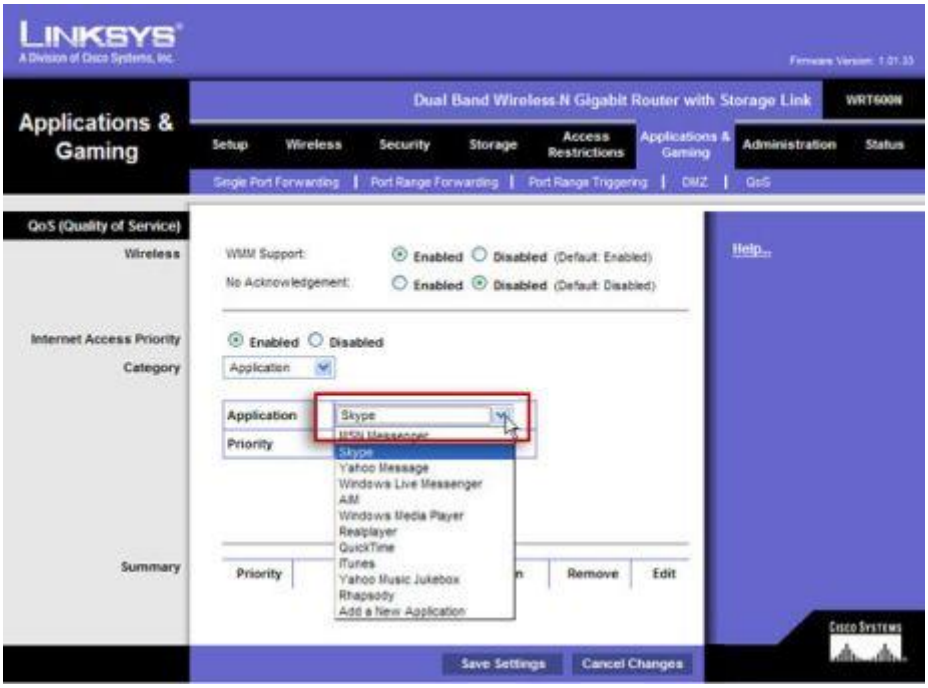
Nếu trong lúc bạn đang chơi Second Life hoặc dùng iTune để tải nhạc thì có cảm giác như mạng bị chập chờn,bạn khoan hãy nghĩ đến chuyện mua một router mới. Hầu hết các router được sản xuất trong khoảng 2 năm trở lại đây đều có tính năng quản lý chất lượng dịch vụ (QoS), nếu không có bạn có thể phải cập nhật firmware để kích hoạt nó.



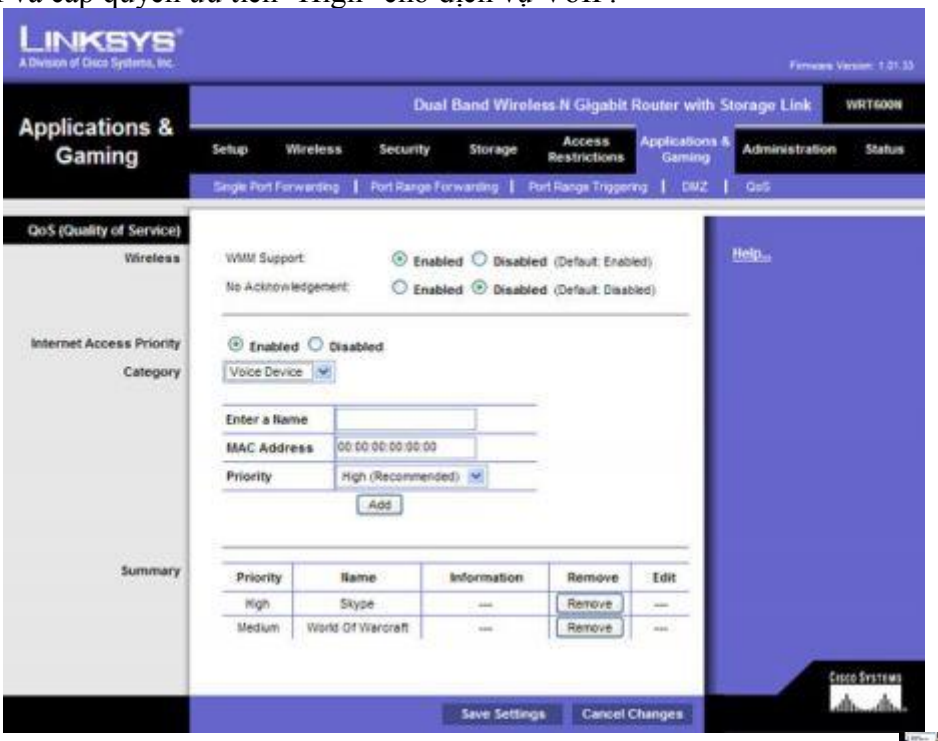
Ví dụ chương trình cấu hình của router Linksys ở hình trên, bạn vào tab QoS có trong phần "Application & Gaming". Kiểm tra chắc chắn rằng phần "WMM Support" đã được chọn (như hình)

Bật chế độ tùy chọn "Internet Access Priority" dành cho các ứng dụng voice và media. Đầu tiên chọn ứng dụng tương ứng từ danh sách sổ xuống (drop-down list)

2. Ưu tiên hóa những gói dữ liệu



Sau đó chọn "High", "Medium", "Normal" hay "Low" tùy theo độ ưu tiên bạn muốn gán cho gói dữ liệu, sau đó nhấn nút "Add". Bạn có thể ưu tiên cho hoạt động hội thoại trên mạng bằng cách cấp quyền ưu tiên "Low" cho các dịch vụ download khác như BitTorrent hay IDM và cấp quyền ưu tiên "High" cho dịch vụ VoIP.



Quote

wifiexpert

Xem hồ sơ

Gởi nhắn tin tới wifiexpert

Tìm bài gởi bởi wifiexpert

#2
01-03-2009, 08:59 PM

wifiexpert
Junior Member

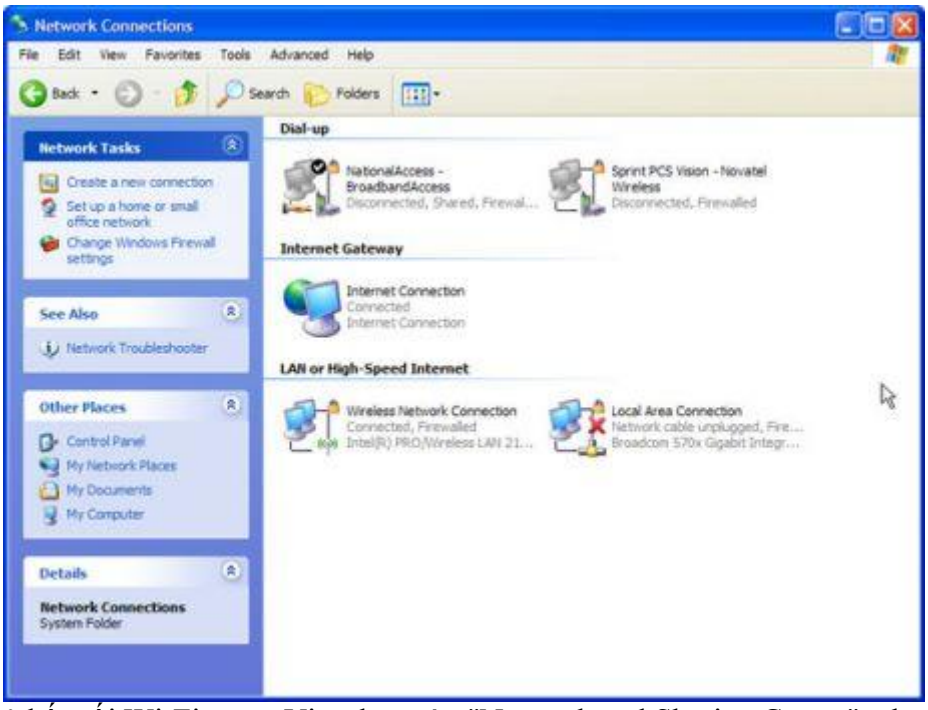
Tham gia ngày: Nov 2008
Bài gởi: 13

---

3. Tắt Wi-Fi khi không dùng đến

Điều này sẽ ngăn chặn việc bạn vô tình kết nối vào các điểm truy cập độc hại và nó cũng giúp kéo dài thời gian sử dụng pin cho laptop. Một vài sản phẩm máy tính xách tay có nút trên thân máy dùng để làm việc này, nếu không thì bạn có thể tắt Wi-Fi bằng cách nhấn phải lên biểu tượng kết nối không dây ở System tray và chọn "Disable"

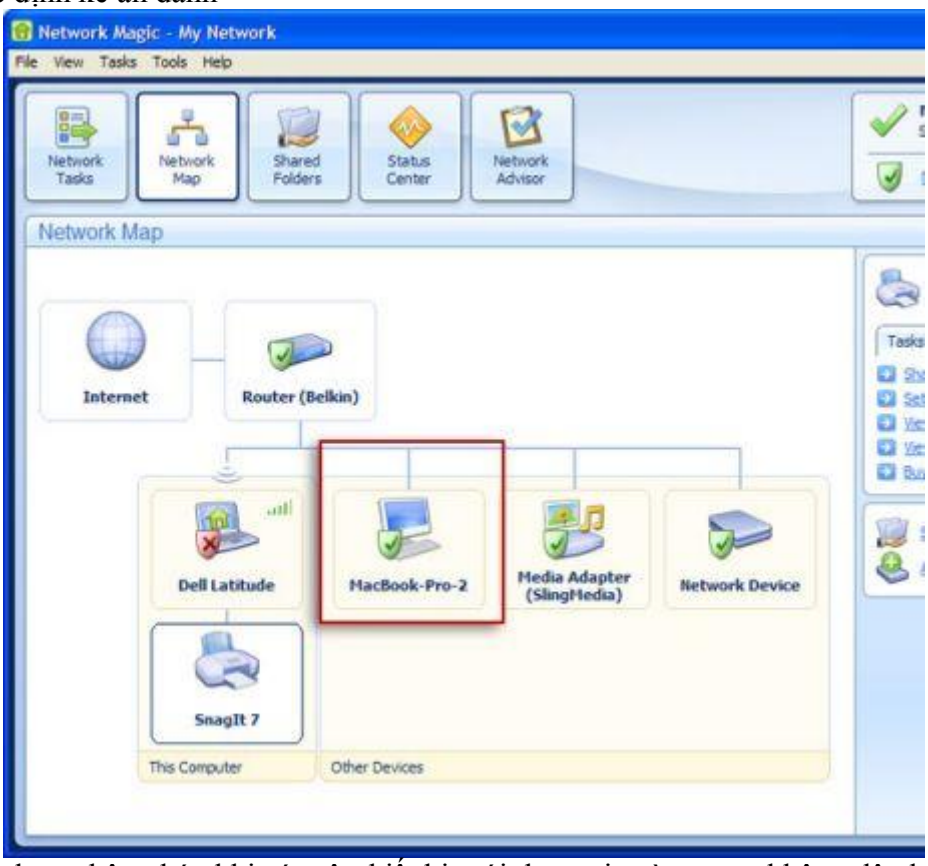
Để bật lại kết nối Wi-Fi, bạn chỉ cần vào Control Panel và nhấp đúp chuột lên biểu tượng kết nối



Để tắt/mở kết nối Wi-Fi trong Vista bạn vào "Network and Sharing Center", chọn "View Status" phía dưới phần "Connections" và chọn Disable/Enable. Nếu bạn sử dụng card Wi-Fi của một hãng thứ ba thì bạn cần sử dụng phần mềm đi kèm để thực hiện việc tắt/mở

4. Theo dõi những người không mời mà đến trên mạng Wi-Fi của bạn

Những người lạ mắt có thể đang ẩn mình trên hệ thống Wi-Fi của bạn. Đừng làm ra vẻ rằng bạn đang được bảo vệ bởi vì bạn có mã hóa. Các cơ chế mã hóa đặc biệt là WEP có thể bị bẽ gảy và thậm chí việc lọc địa chỉ MAC address cũng có thể bị qua mặt. Để ngăn các cuộc xâm nhập lạ mặt hãy tải về và cài đặt phiên bản miễn phí của phần mềm Network Magic. Chương trình sẽ vẽ ra một bản đồ tất cả các thiết bị đang hiện diện trên mạng bao gồm máy tính, máy chủ, máy in và các thiết bị khác. Nhờ vậy bạn có thể dễ dàng xác định kẻ ẩn danh



Để nhận được thông báo khi có một thiết bị mới tham gia vào mạng không dây bạn chọn "Options" từ trình đơn "Tools", nhấn vào tab "Notifications" và đánh dấu chọn mục "A new device joins the network".

Việc cuối cùng là bạn nhấn vào tab "Security" và đánh dấu chọn "Automatically track new devices as Intruders" để theo dõi từng cử chỉ hành động của kẻ xâm nhập. Điều này rất hữu hiệu trong trường hợp việc xâm nhập xảy ra trong lúc bạn rời khỏi bàn làm việc.

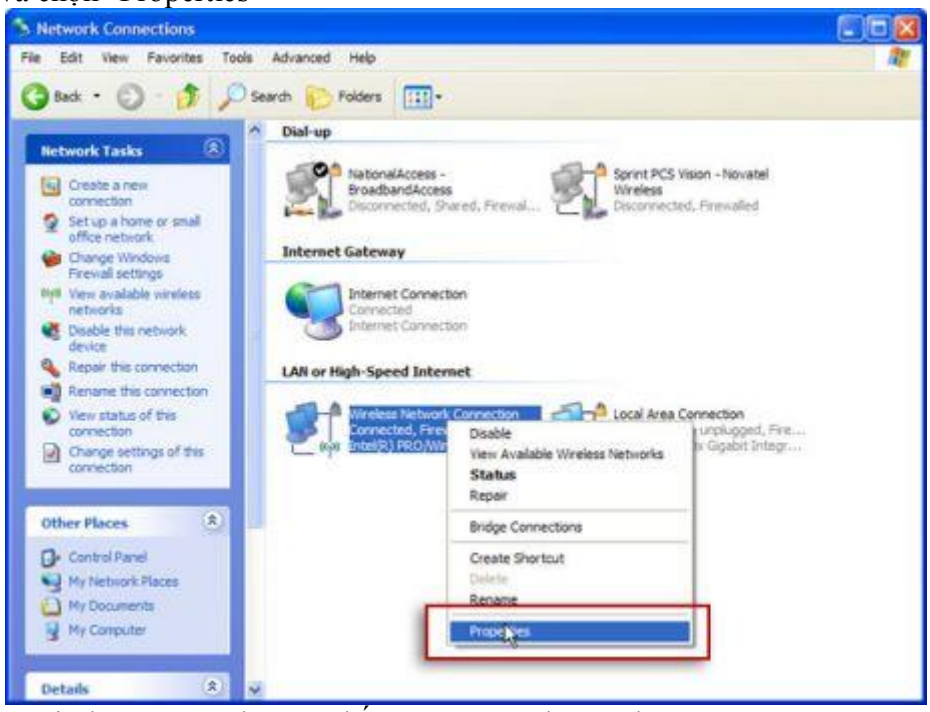
5. Một điểm kết nối không dây an toàn

Các điểm kết nối không dây công cộng là món mồi béo bở cho các hacker bởi vì nó được mở cho mọi người tham gia nên thiếu hòan toàn việc mã hóa dữ liệu khi truyền. Trừ phi bạn sử dụng một phần mềm tạo mạng riêng ảo (VPN) nếu không thì bất cứ ai cũng có thể thấy được tất cả dữ liệu của bạn bao gồm mật khẩu và email. Nếu bạn chưa có một phần mềm VPN cho riêng mình thì hãy sử dụng bản miễn phí là Hotspot Shield của hãng AnchorFree.

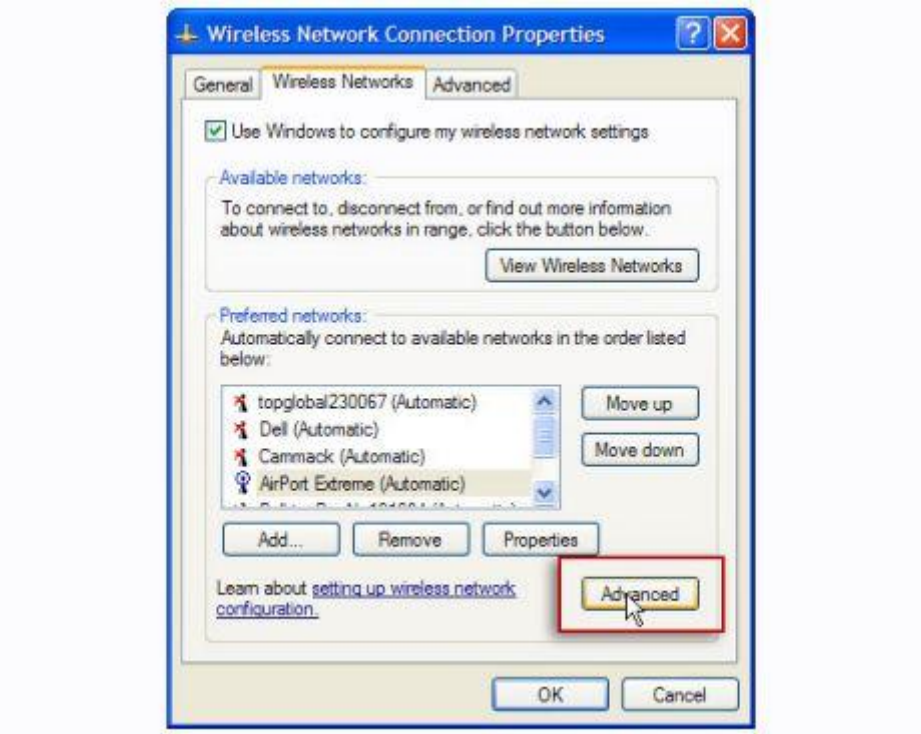
6. Vô hiệu hóa Peer-to-Peer (Ad-Hoc) Wi-Fi

Một trong những mối nguy hiểm bảo mật là xuất phát từ các mạng độc hại (malicious networks) gọi là "ad-hoc" được bắt nguồn từ máy tính khác. Ví dụ, hacker có thể ngồi tại phi trường và bắt đầu phát tán một SSID co tên là "T-Mobile" hay "Free Wi-Fi". Lúc đó thiết bị Wi-Fi của bạn có thể tự động thiết lập kết nối hoặc bạn vô tình nhấn vào do vậy bạn đã mở cửa cho hacker truy xuất vào máy tính của mình. Trên thực tế rất hiếm khi bạn cần kết nối với một máy tính khác bằng kết nối Wi-Fi do vậy hãy vô hiệu hóa chức năng này.

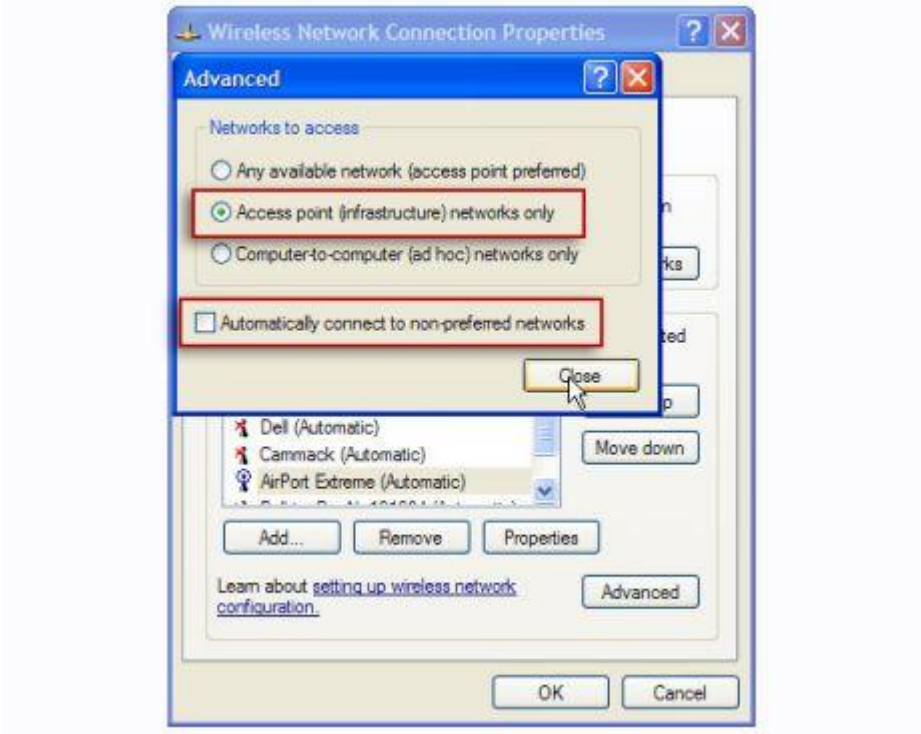
Mở cửa sổ "Network Connections" trong Control Panel, nhấn phải chuột vào biểu tượng wireless và chọn "Properties"



Chọn tab "Wireless Networks" và nhấn vào nút "Advanced"



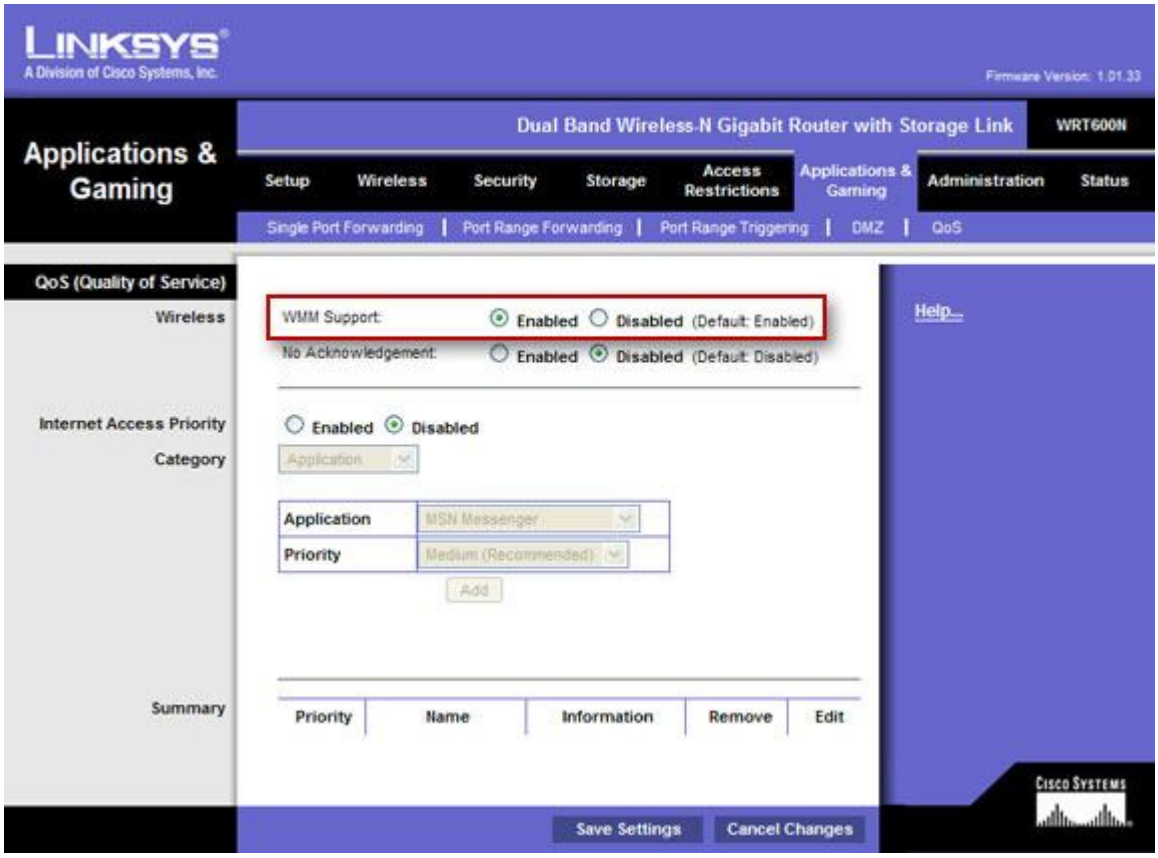
Chọn "Access point (infrastructure) networks only". Chắc chắn rằng mục "Automatically connect to non-preferred networks" không được đánh dấu.



Cải thiện khả năng bảo mật hệ thống mạng Wifi

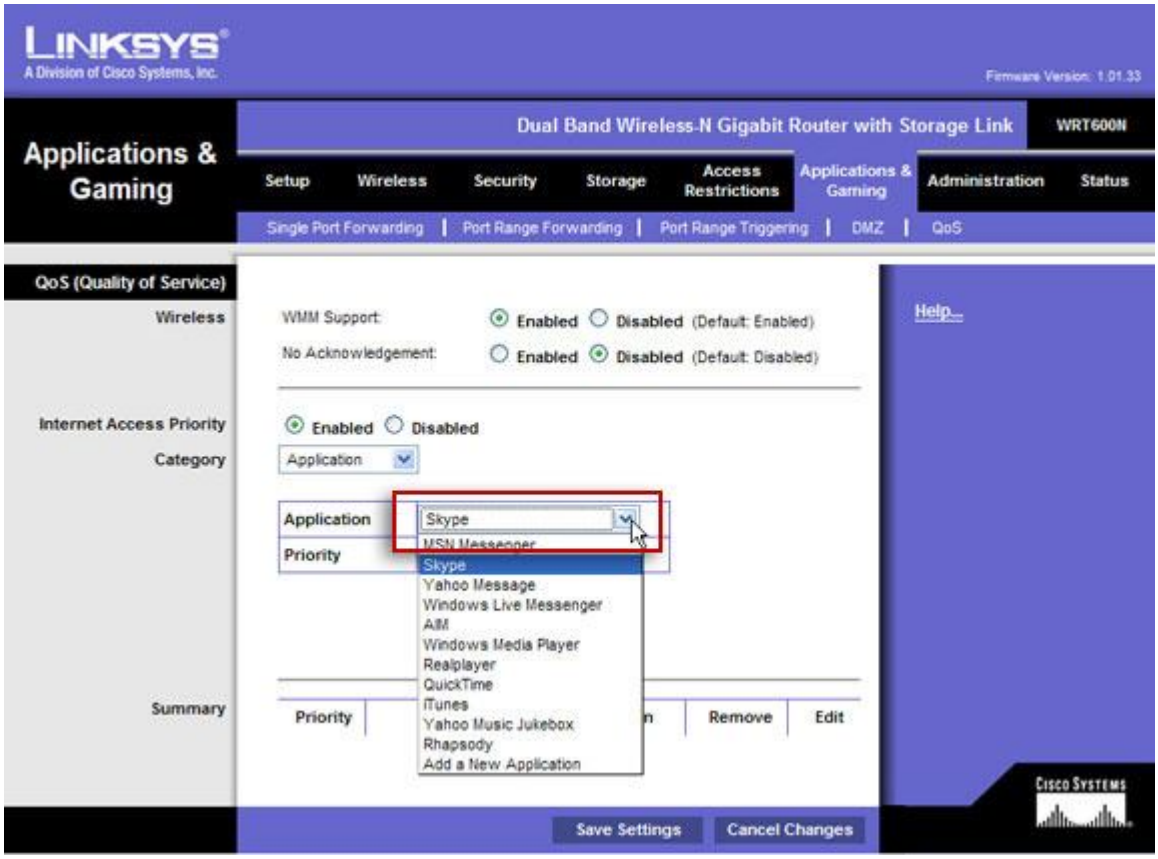
Quản Trị Mạng - Có thể bạn đã quá quen với việc sử dụng mạng Wifi ở nhà cũng như công sở, văn phòng làm việc, nhưng ít ai ngờ rằng chính trong môi trường quen thuộc này lại ẩn chứa những điều bất ngờ. Trong bất kỳ hoàn cảnh nào thì những ưu điểm và nhược điểm luôn tồn tại song song với nhau, và hệ thống mạng wifi chúng ta đang đề cập đến cũng không phải là ngoại lệ. Trong bài viết dưới đây, chúng tôi sẽ giới thiệu và trình bày một số thao tác cơ bản để người sử dụng cải thiện cũng như nâng cao hiệu suất và độ bảo mật của hệ thống mạng Wifi họ đang sử dụng.

Tối ưu hóa hiệu suất của Wifi dành cho VoIP, video và game:



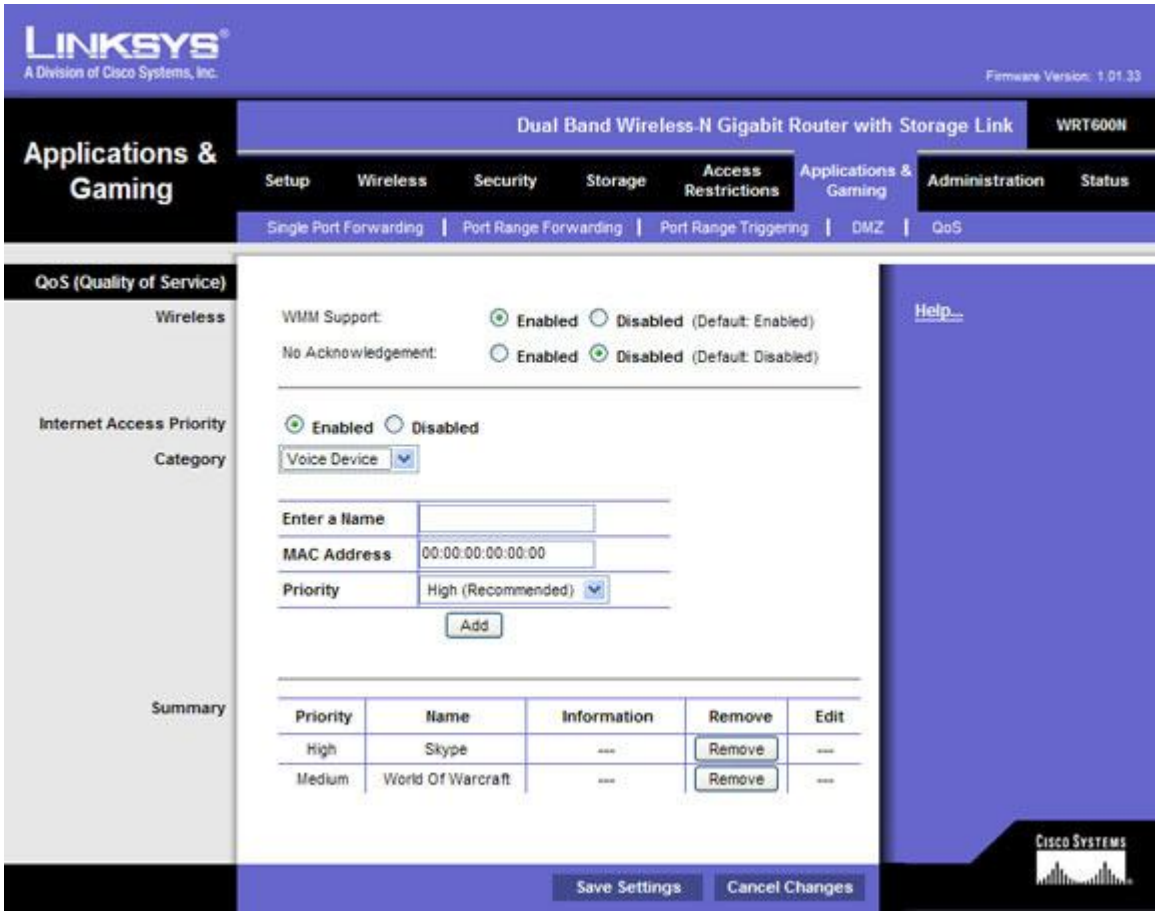
Nếu cuộc hội thoại Skype hoặc trò chơi Second Life của bạn bị gián đoạn giữa chừng, quá trình truyền tải ca nhạc qua iTunes cũng gặp vấn đề tương tự như vậy khi ai đó trong nhà bắt đầu chơi World of Warcraft... đây chính là thời điểm thích hợp để bạn nghĩ đến việc mua mới 1 thiết bị router. Hầu hết các dòng thiết bị router trong vòng 20 năm trở lại đây đều có tính năng Quality of service – QoS, mặc dù người sử dụng sẽ phải tiến hành nâng cấp firmware để kích hoạt. Ví dụ như phần cấu hình QoS dành cho router Linksys thường nằm ở mục Applications & Gaming (nhưng trước tiên phải kích hoạt tính năng WMM Support – như ảnh minh họa)

Chọn ứng dụng QoS tương ứng:



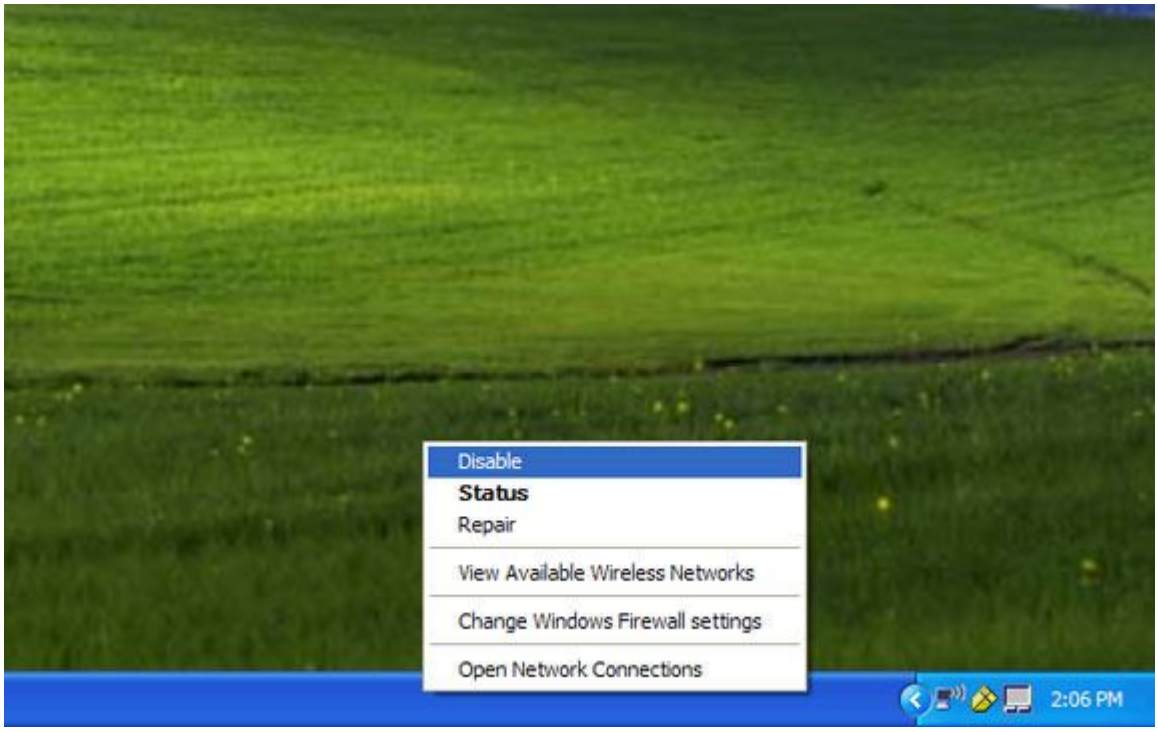
Để tiếp tục, chúng ta cần bật tính năng hỗ trợ Internet Access Priority dành cho những chương trình yêu cầu nhiều dữ liệu voice và media. Như ví dụ tại đây, các bạn chọn lần lượt từng ứng dụng trong danh sách.

Ưu tiên các gói dữ liệu khác nhau:



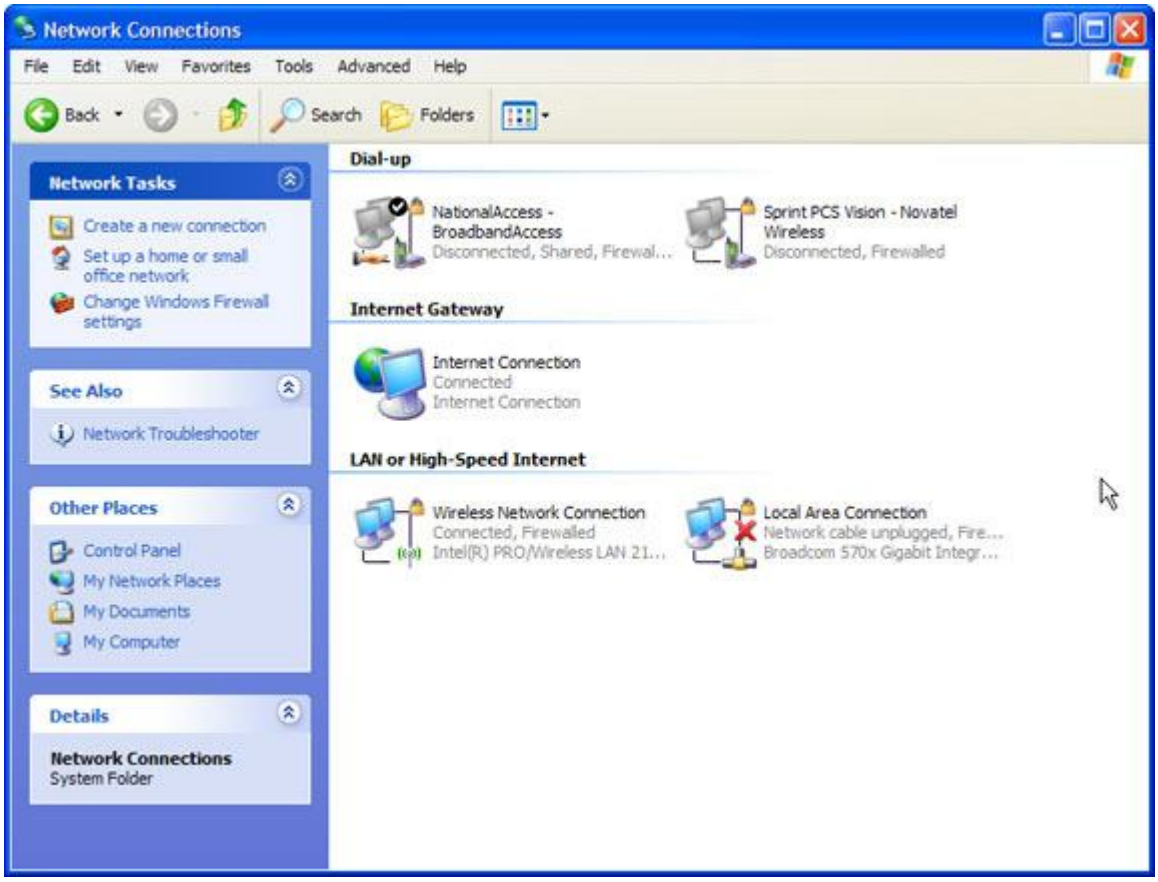
Khi chuyển sang bước này, chúng ta có thể chọn các mức độ ưu tiên – Priority tương ứng dành cho chương trình, với các mức độ High, Medium, Normal, hoặc Low, sau đó nhấn nút Add bên dưới. Ví dụ, các bạn có thể thiết lập chế độ Low đối với những chương trình, dịch vụ download như BitTorrent, High dành cho VoIP... để đảm bảo chất lượng. Bên cạnh đó, các bạn cần lưu ý rằng Linksys còn hỗ trợ người dùng cụ thể hơn nữa đối với các thiết bị VoIP, ví dụ như điện thoại khi kết nối trực tiếp tới hệ thống mạng. Tuy nhiên, không phải tất cả các thiết bị router đều có được tính năng này, nhưng tối thiểu nhất vẫn là QoS hoặc WMM, hệ thống sẽ tự động quản lý và phân chia lượng dữ liệu sao cho phù hợp, tuy nhiên tính năng trên lại chưa được kích hoạt ở chế độ mặc định (như đã đề cập ở trên).

Tắt Wifi khi không sử dụng:



Về mặt kỹ thuật, đây cũng là 1 cách tiết kiệm năng lượng của máy laptop, đó là tắt chức năng của card mạng Wifi khi không dùng đến. Đồng thời, quá trình này cũng giúp bạn tránh khỏi những vùng phát sóng vô tình có chứa các loại mã độc, bên cạnh đó còn giúp người sử dụng kéo dài tuổi thọ của pin laptop. Rất nhiều mẫu laptop hiện nay có nút bấm bật hoặc tắt Wifi, hoặc trong Windows XP thì chúng ta chỉ cần nhấn chuột phải vào biểu tượng Wifi dưới khay hệ thống và chọn Disable.

Bật Wifi trong Windows XP:



Việc tắt Wifi như trên sẽ tạm thời xóa bỏ biểu tượng của chương trình khỏi khay hệ thống, để khôi phục lại trong hệ điều hành Windows XP, các bạn hãy mở Network Connections trong Control Panel, sau đó kích đúp vào biểu tượng Wifi.

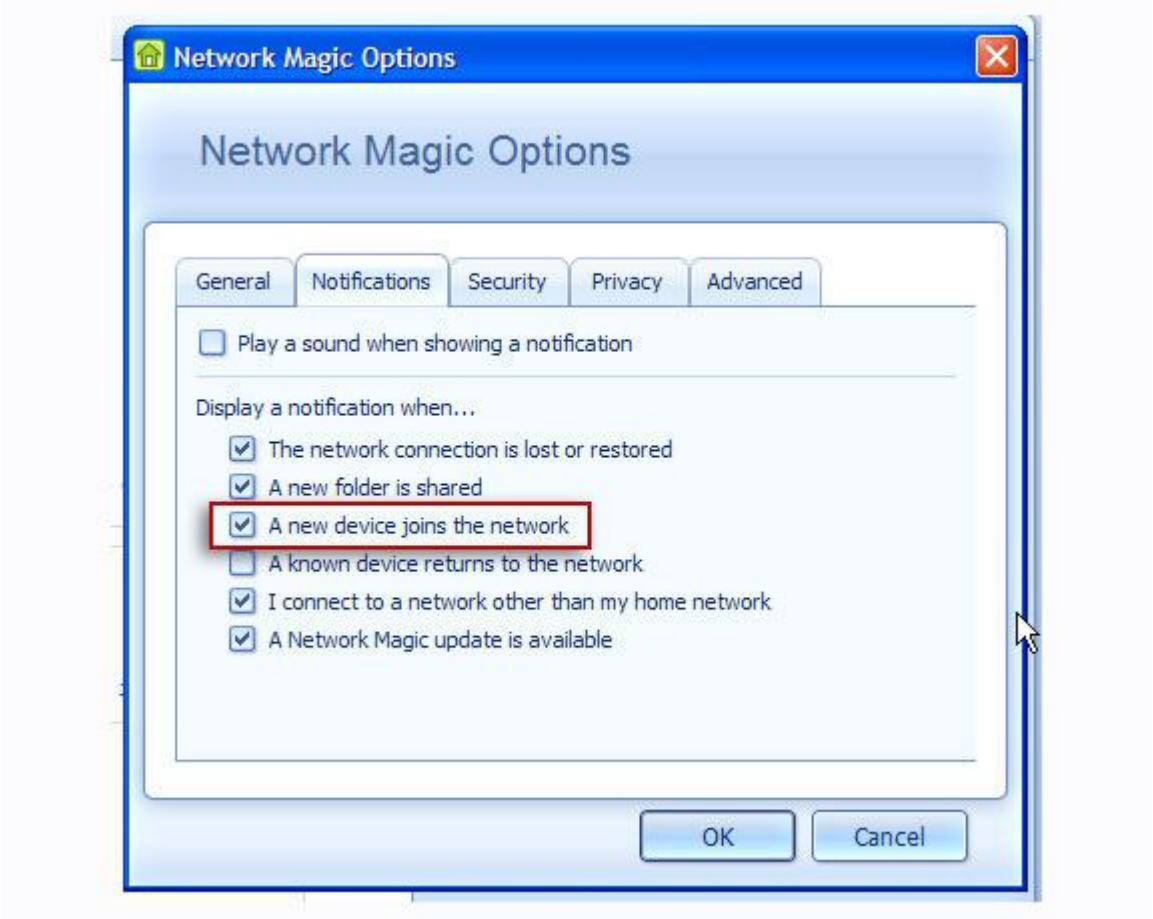
Bật và tắt Wifi trong Windows Vista:

Để thực hiện việc trên trong Windows Vista, chúng ta chỉ việc mở Network and Sharing Center trong Control Panel và chọn View status ở bên dưới Connections.

Theo dõi những hiện tượng bất thường trong hệ thống mạng của bạn:

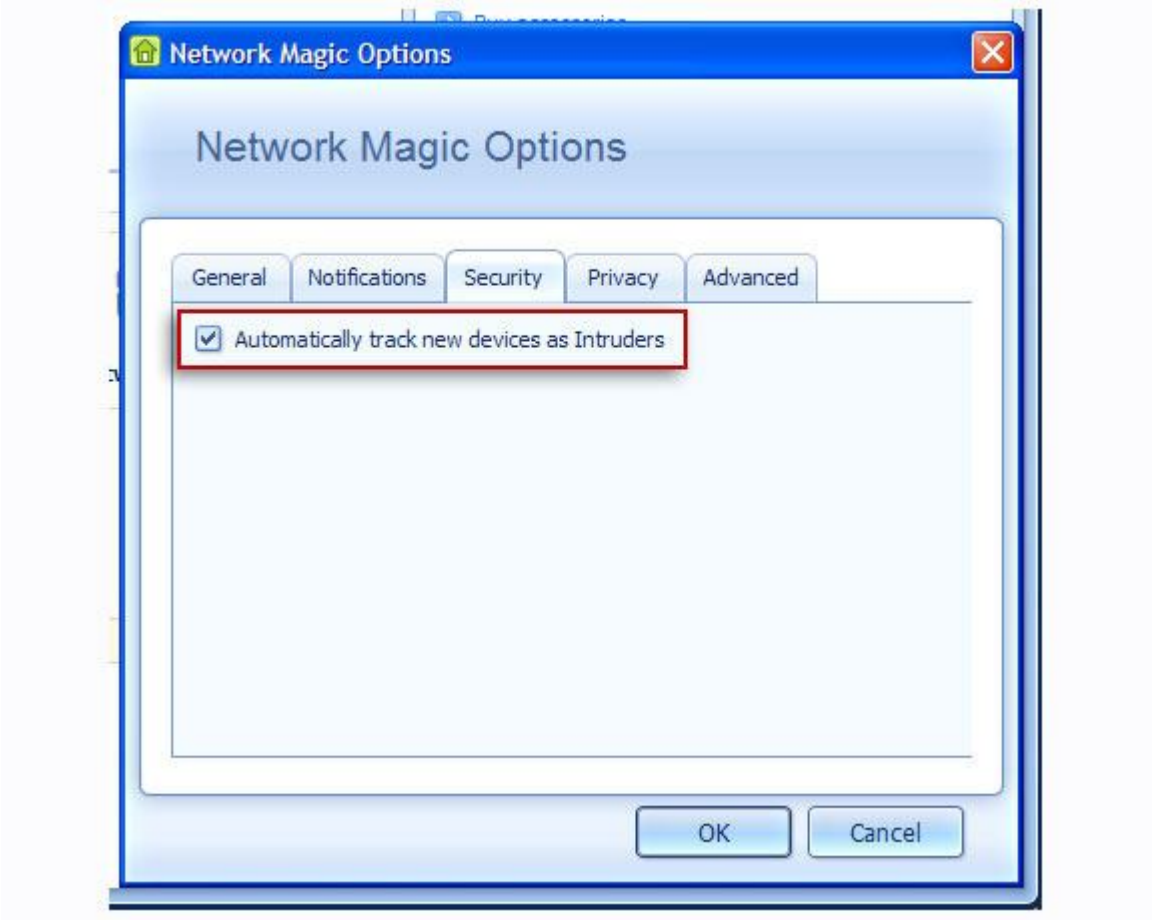
Khi sử dụng hoặc quản lý mạng Wifi ở nhà hoặc công sở, liệu bạn có phát hiện được những ai đang xâm nhập vào hệ thống hay không? Trên thực tế, có rất nhiều người sử dụng nghĩ rằng mạng Wifi của họ hoàn toàn bảo mật, các biện pháp mã hóa dữ liệu họ dùng rất đảm bảo... Nhưng về mặt kỹ thuật, các cơ chế bảo mật, đặc biệt là WEP có thể dễ dàng bị đột nhập, thậm chí các luồng dữ liệu cấp phát qua địa chỉ MAC cũng có thể bị giả mạo. Để khắc phục, các bạn hãy download và sử dụng phiên bản miễn phí của ứng dụng Network Magic Essentials – chương trình này sẽ hiển thị bản đồ hiển thị tương ứng của tất cả các thành phần máy tính, server, máy in hoặc các thiết bị ngoại vi đang kết nối tới hệ thống mạng của người sử dụng.

Nhận thông báo mỗi khi có thiết bị kết nối:



Nhưng trên thực tế, không phải lúc nào các bạn cũng luôn bật Network Magic ở chế độ hoạt động, nhưng thay vào đó, chúng ta có thể thiết lập chế độ hiển thị thông báo dưới dạng pop – up khi có 1 thiết bị mới bất kỳ kết nối vào hệ thống mạng, do đó có thể dễ dàng phát hiện và đề phòng trước sự xâm nhập của kẻ lạ. Để thực hiện, các bạn chọn mục Options từ menu Tools, sau đó chọn thẻ Notifications và đánh dấu vào ô A new device joins the network.

"Theo dõi" những kẻ xâm nhập – Intruder:

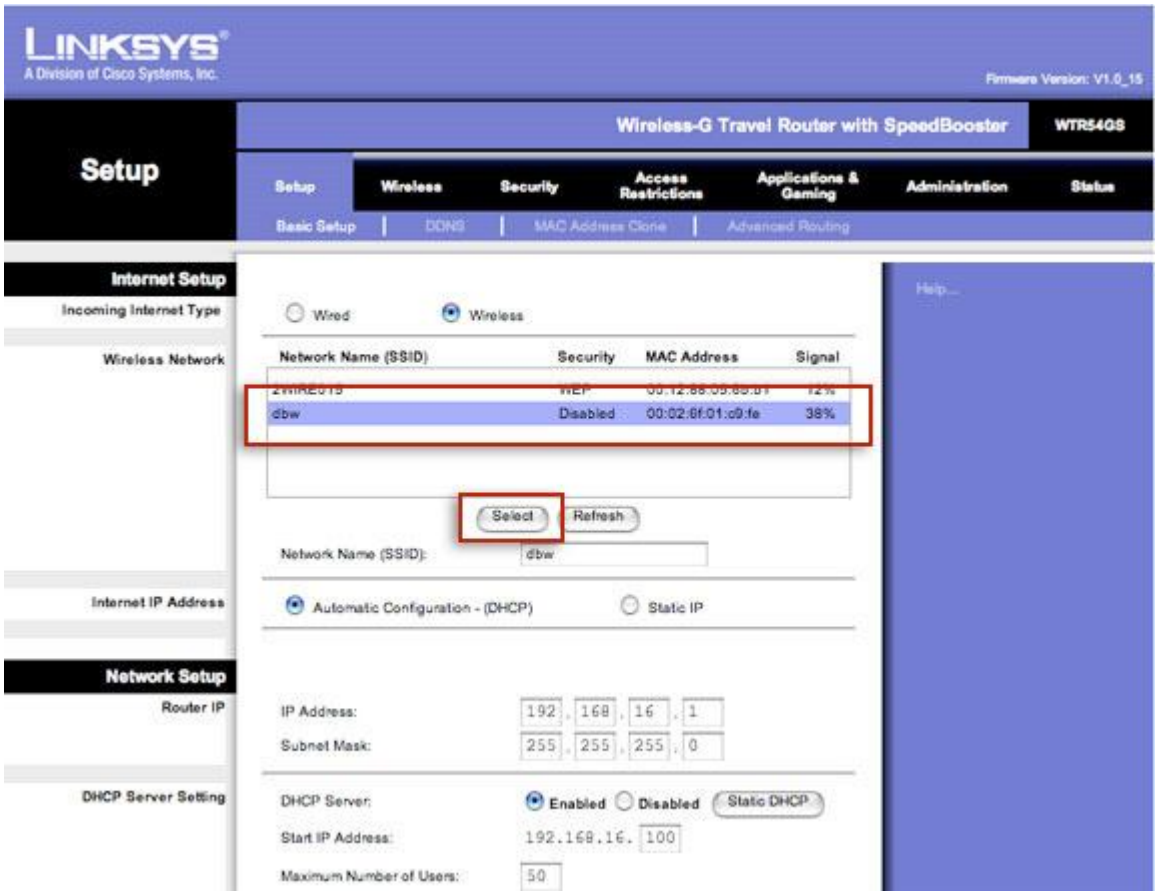


Cuối cùng, chọn thẻ Security và đánh dấu vào ô Automatically track new devices as Intruders, do vậy người dùng có thể giám sát mọi hoạt động của những thành phần được cho là Intruder – kẻ xâm nhập.

Chia sẻ Hotspot:

Hiện nay, dòng sản phẩm router Linksys Wireless-G Travel có 1 tính năng khá độc đáo: cho phép người sử dụng chia sẻ kết nối Wifi qua mạng kết nối có dây đã được mã hóa. Do vậy, trên thực tế chúng ta có thể áp dụng cách này để chia sẻ 1 đường kết nối băng thông rộng có trả phí.

Sử dụng Wifi để chia sẻ Wifi:

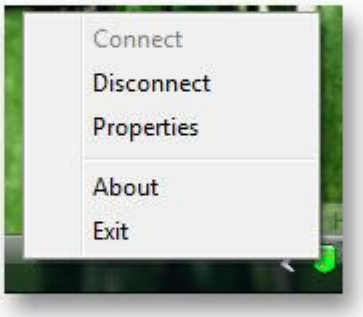


Để chia sẻ Wifi, các bạn chỉ cần bật router, kết nối qua Wifi, mở phần thiết lập – Configuration bằng trình duyệt, tại đây chọn phần Hotspot chúng ta muốn kết nối từ trong danh sách (ví dụ như T-Mobile) và nhấn nút Select. Sau đó mở 1 cửa sổ mới trên trình duyệt và đăng nhập vào Hotspot đó, thực hiện bất cứ thao tác thiết lập cần thiết, và từ bây giờ trở đi, các máy tính khác có thể kết nối tới Linksys Travel Router cũng sẽ tự động kết nối qua Hotspot này có tính phí này, nhưng họ lại không cần phải trả thêm bất kỳ khoản chi phí nào.

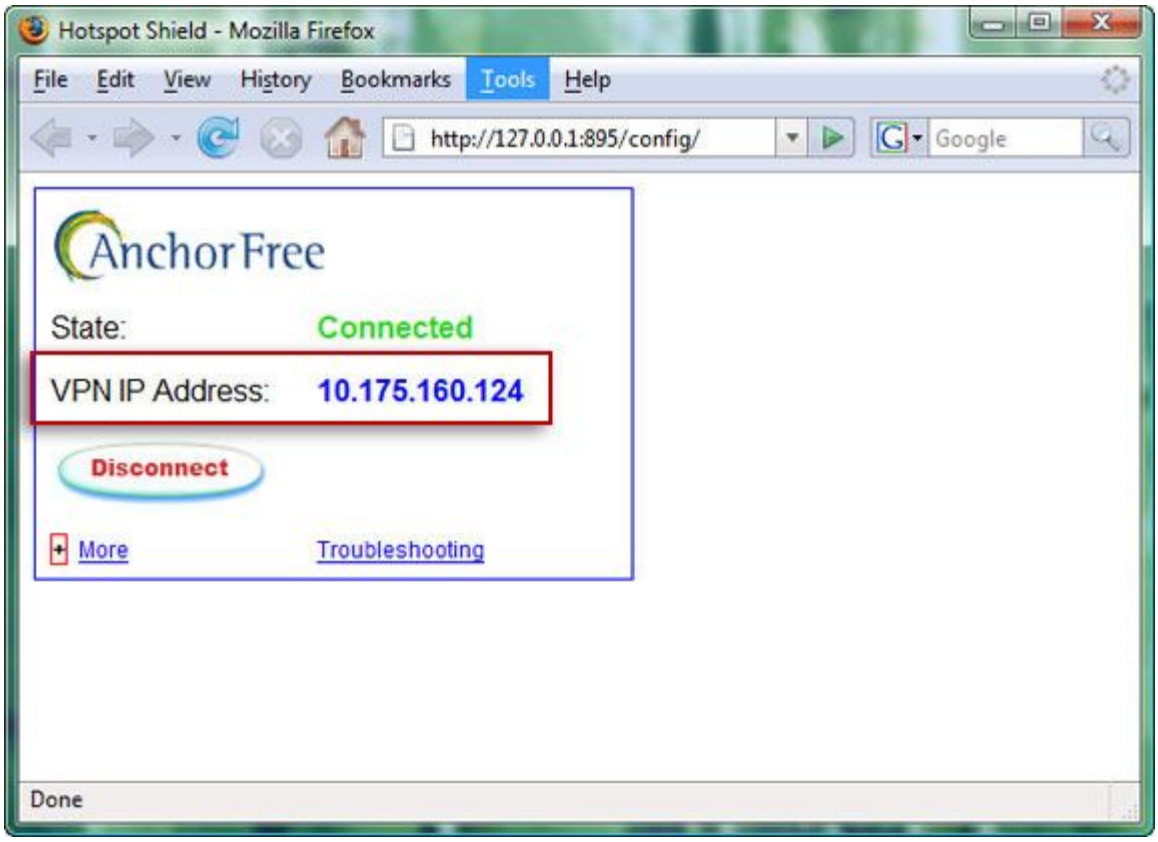
Bảo đảm an toàn cho kết nối Hotspot:

Trên thực tế, những điểm thu phát sóng công cộng – Public hotspot chính là mục tiêu hấp dẫn của những kẻ hacker, bên cạnh đó một số hệ thống mạng hoàn toàn không được trang bị bất cứ hình thức bảo mật nào là để phục vụ cho toàn bộ khách hàng ở khu vực đó. Trừ khi người quản lý sử dụng 1 phần mềm VPN thì bất cứ ai cũng có thể thấy được toàn bộ lưu lượng Internet qua wireless, bao gồm các chuỗi mật khẩu và tin nhắn email. Nếu không sử dụng chức năng VPN nào, các bạn hãy tham khảo và dùng chương trình Hotspot Shield - hoàn toàn miễn phí của hãng phần mềm AnchorFree. Tất cả những gì cần làm là download và cài đặt, trình duyệt của bạn sẽ hiển thị màn hình như trên, nhấn nút Run Hotspot Shield và chức năng bảo vệ của chương trình sẽ bắt đầu.

Tắt VPN của Hotspot Shield:

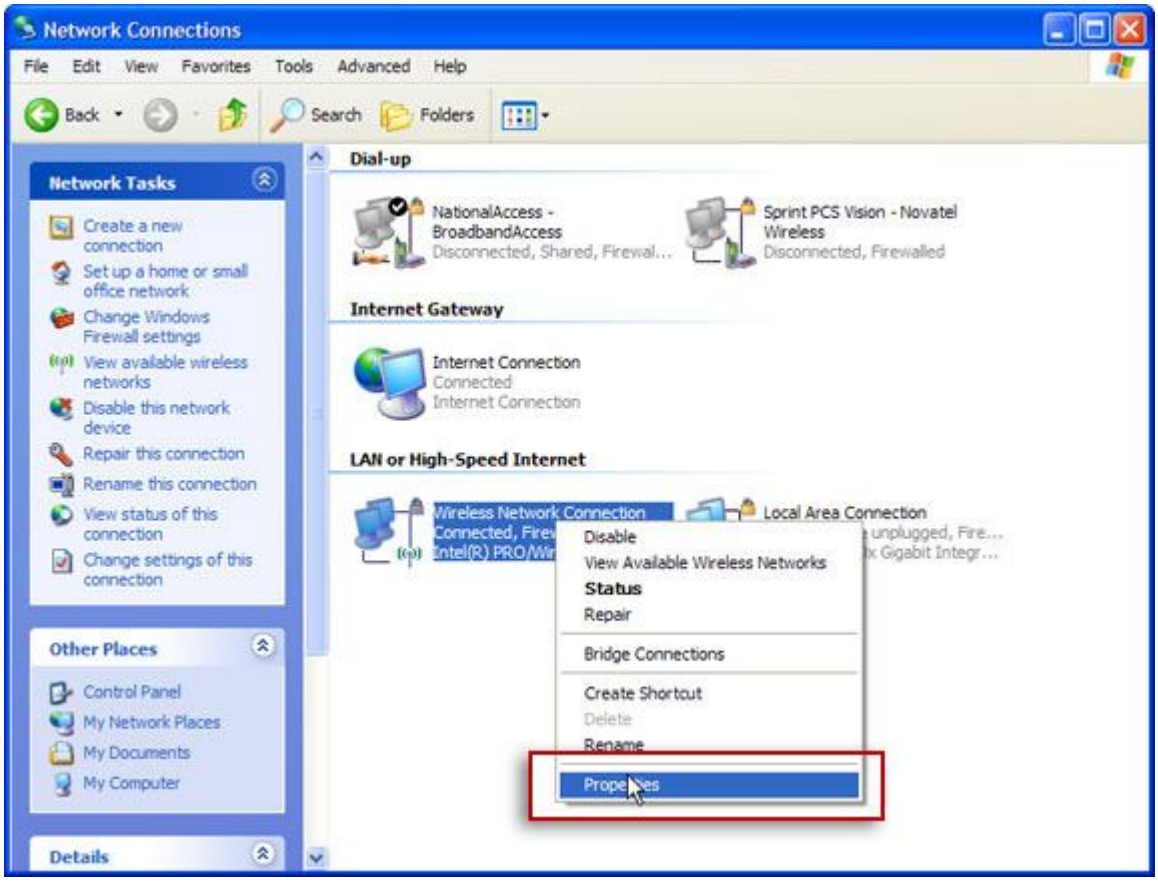


Nếu không muốn sử dụng Hotspot Shield, các bạn chỉ cần nhấn chuột phải vào biểu tượng chương trình ở dưới khay hệ thống và chọn Disconnect, màu của biểu tượng sẽ chyển từ xanh thành đỏ. Để kích hoạt trở lại, chúng ta nhấn chuột phải và chọn Connect.

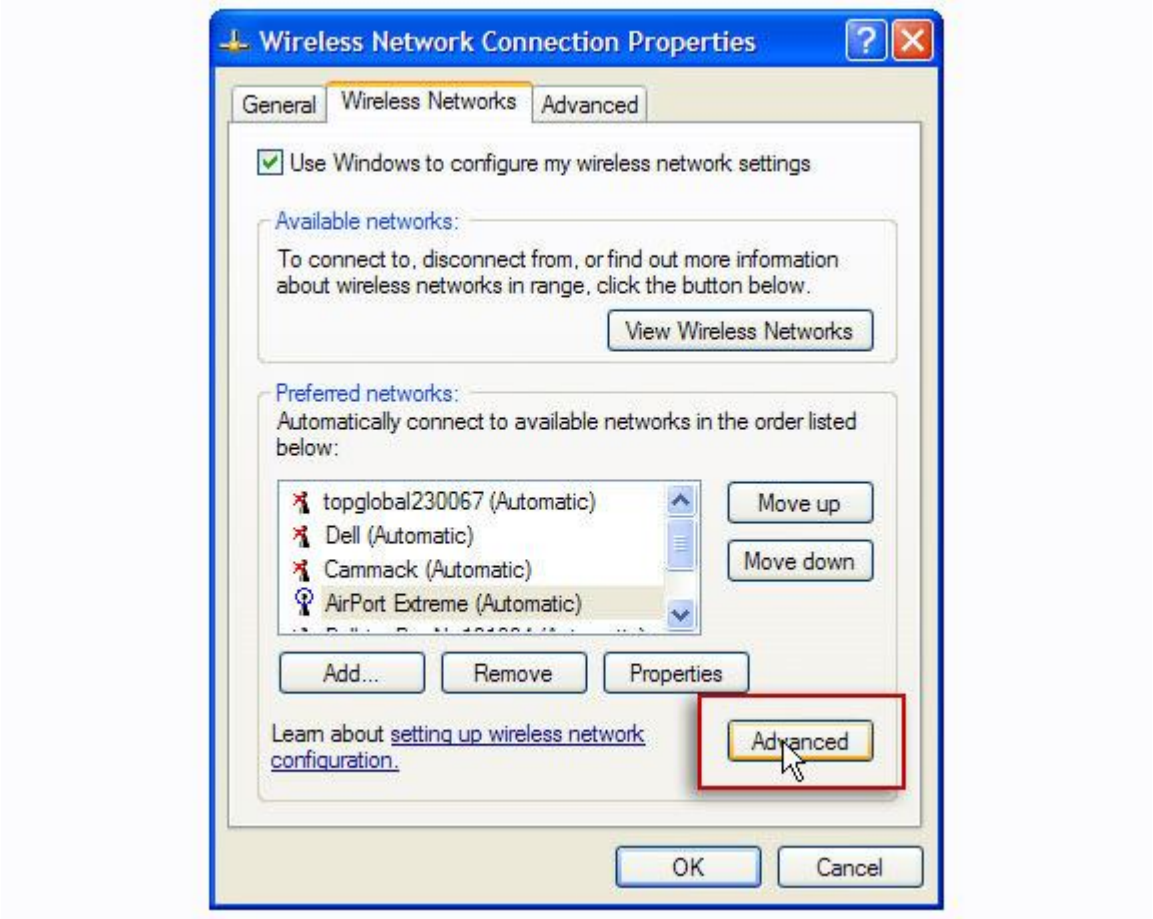


Bên cạnh đó, trong quá trình kết nối, để biết được địa chỉ IP hiện tại của hệ thống, các bạn chọn phần Properties trong menu hiển thị. Vì Hotspot Shield là 1 ứng dụng miễn phí, nên chúng ta sẽ nhìn thấy 1 đoạn banner quảng cáo ở phía top trên trình duyệt.

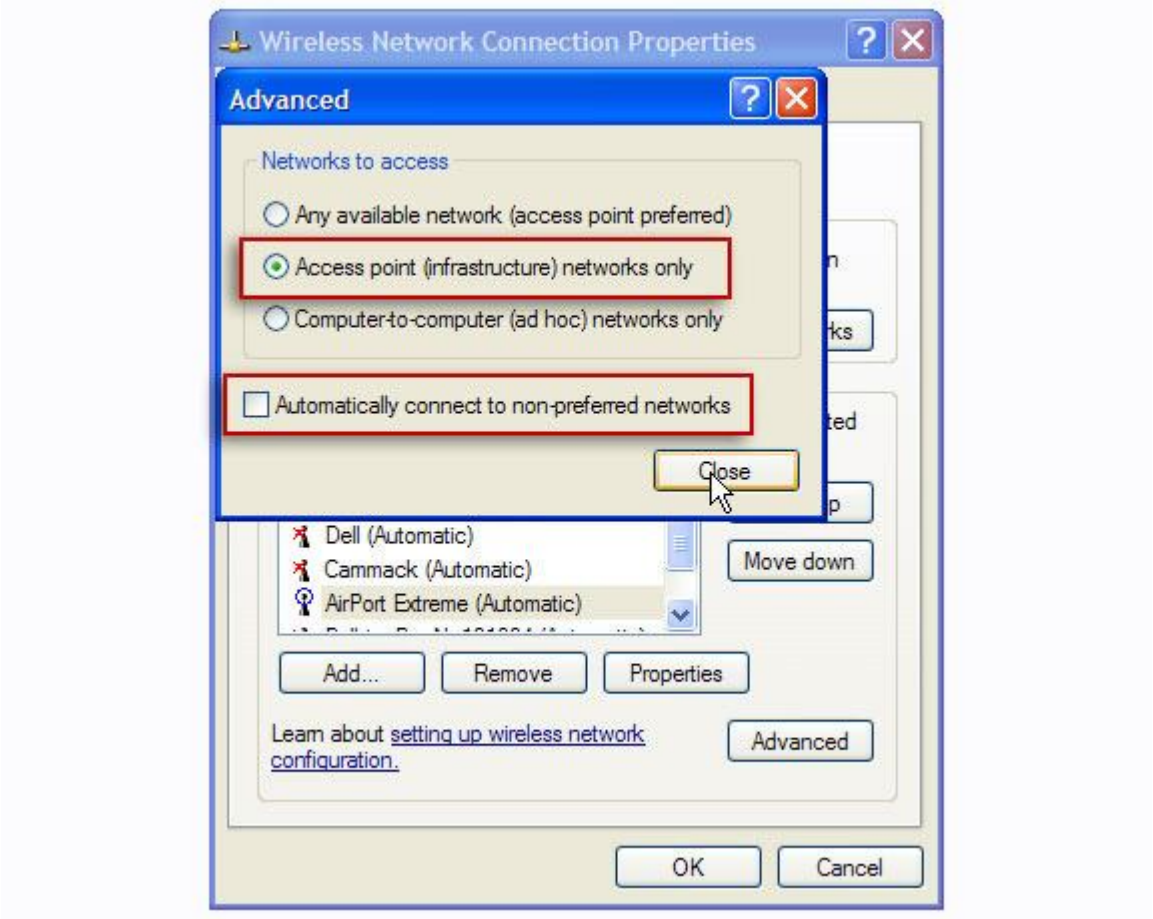
Tắt chức năng Peer – to – Peer (Ad – Hoc) qua Wi-Fi:



Một trong những nguyên nhân chủ yếu và phổ biến nhất để kẻ xấu xâm nhập và phát tán mã độc qua các kết nối Wifi công cộng là mạng Wifi ad – hoc, bắt nguồn từ 1 máy tính bất kỳ trong hệ thống. Ví dụ, 1 kẻ tin tặc ngồi trong phạm vi của 1 sân bay và bắt đầu kết nối vào SSID có tên là T-Mobile hoặc Free Wi-Fi. Nhiều người sử dụng khác có thể vô tình hoặc tự động kết nối vào đúng SSID đó, và các loại chương trình độc hại sẽ xâm nhập vào máy tính của họ. Để tắt bỏ tính năng này trong Windows XP, các bạn hãy mở phần Network Connections từ Control Panel, nhấn chuột phải vào phần kết nối Wifi và chọn Properties.



Chọn tiếp thẻ Wireless Networks và nhấn nút Advanced.



Cuối cùng, chọn phần Access point (infrastructure) networks only, và các bạn cũng đừng quên bỏ dấu check tại ô Automatically connect to non-preferred networks. Còn trong Windows Vista hoặc 7 thì chúng ta không cần phải làm như vậy vì có cơ chế tùy chọn hệ thống mạng ad-hoc ngay tại bước đầu tiên.

Chúc các bạn thành công!

T.Anh (theo PC World)