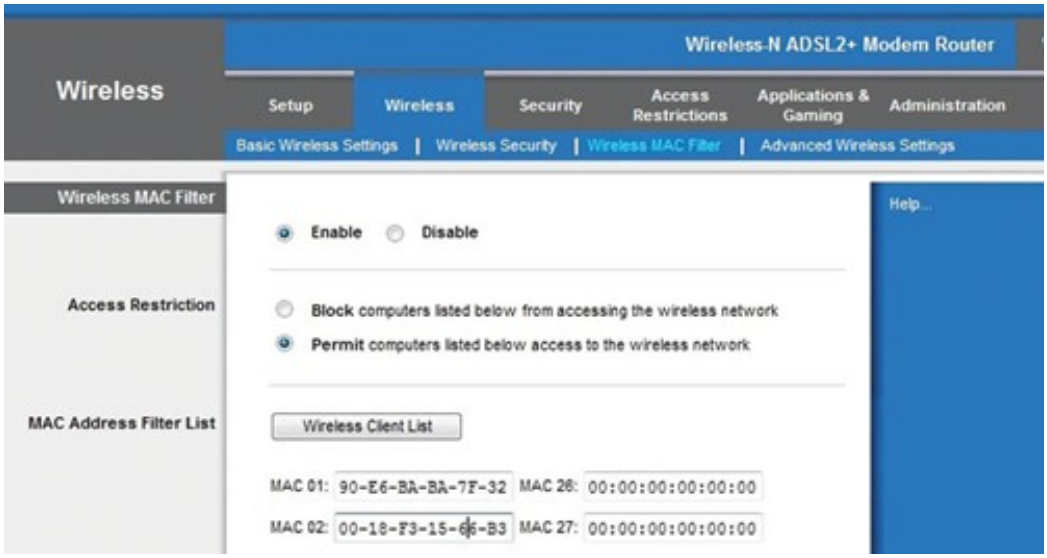
Bảo mật mạng Wi-Fi

Dựng "hàng rào" bảo mật cho mạng Wi-Fi không những giúp hạn chế người lạ chiếm dụng băng thông Internet mà còn giúp đảm bảo an toàn dữ liệu của bạn.

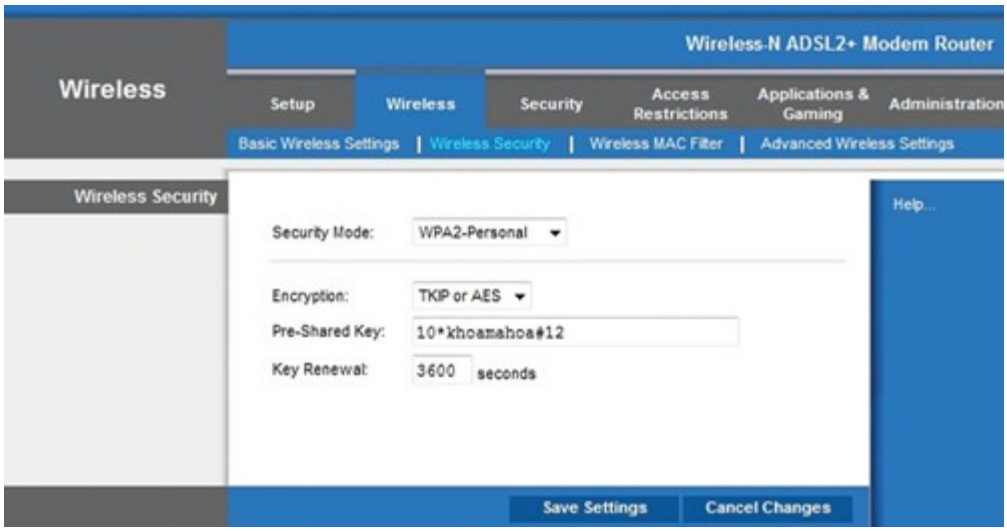


Trước tiên, bạn cần đăng nhập vào bộ định tuyến không dây (router) hay thiết bị truy cập không dây (Access Point - AP) - gọi tắt là thiết bị Wi-Fi. Với Router, bạn có thể nhận IP cấp phát từ thiết bị, nhưng với AP, thông thường bạn cần thiết lập địa chỉ IP trên máy tính cùng lớp địa chỉ IP của AP (xem tài liệu đi kèm AP để biết địa chỉ IP mặc định). Sau khi biết địa chỉ IP, tài khoản truy cập thiết bị (username, password), bạn hãy đăng nhập vào thiết bị Wi-Fi.

Thay đổi mật khẩu đăng nhập

Bước đầu tiên, bạn cần thay đổi ngay tài khoản đăng nhập mặc định, thường là admin. Vì nếu người khác biết tài khoản đăng nhập, họ có thể đăng nhập vào thiết bị Wi-Fi và tùy chỉnh các thông số mà bạn đã thiết lập. Chú ý nên đặt mật khẩu dài

và phức tạp gồm chữ hoa, thường, số, ký tự đặc biệt. Nếu thiết bị Wi-Fi của bạn hỗ trợ mạng Wi-Fi riêng biệt dành cho khách (guest), bạn cũng nên đặt mật khẩu truy cập Wi-Fi cho mạng Wi-Fi khách này, để khi khách truy cập, thiết bị Wi-Fi sẽ yêu cầu họ nhập mật khẩu truy cập.



Hình 1: Mã hóa WPA2.

Ẩn tên mạng (SSID)

Mỗi mạng Wi-Fi đều có một tên mạng (SSID) khác biệt nhau, một số thiết bị Wi-Fi hỗ trợ cùng lúc đến 4 SSID khác nhau. Bạn nên ẩn SSID nhằm tránh người lạ dò tìm và chú ý đến mạng Wi-Fi của bạn. Đây là phương cách bảo mật mạng Wi-Fi ở mức cơ bản nhất.

Bật chế độ mã hóa WPA2

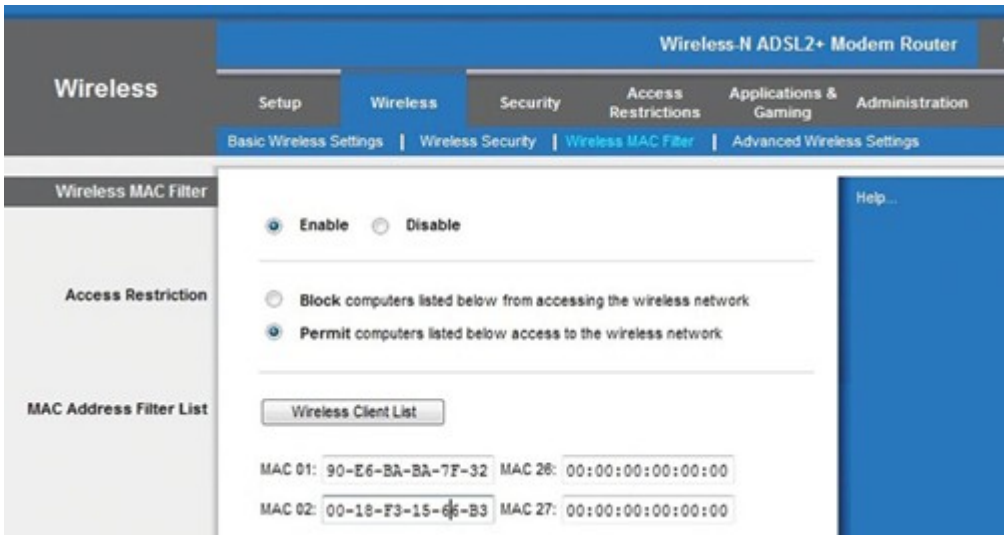
Nếu thiết bị Wi-Fi và các thiết bị truy cập Wi-Fi của bạn (máy tính xách tay, máy

tính bảng, điện thoại thông minh,…) đều hỗ trợ mã hóa WPA2, thì bạn nên bật chế độ mã hóa này lên (WPA2 Personal). WPA2 (Wi-Fi Protected Access 2) là chế độ mã hóa Wi-Fi mạnh nhất hiện nay. Nếu bạn sử dụng Wi-Fi trong doanh nghiệp, bạn nên chọn chế độ WPA2 Enterprise, kết hợp xác thực truy cập với máy chủ Radius.

Bật cơ chế lọc theo địa chỉ MAC

Mỗi thiết bị có thể truy cập mạng đều có địa chỉ MAC (Media Access Control) khác nhau. Mặc dù hiện nay có nhiều công cụ cho phép bạn thay đổi địa chỉ MAC, tuy nhiên nếu bạn kết hợp nhiều phương cách bảo mật Wi-Fi thì người lạ cũng khó lòng truy cập trái phép vào mạng Wi-Fi của bạn. Cơ chế lọc MAC trên thiết bị Wi-Fi giúp bạn dễ dàng kiểm soát các thiết bị truy cập mạng Wi-Fi. Bạn có thể gán các địa chỉ MAC vào danh sách được phép truy cập Wi-Fi hoặc không được phép truy cập mạng Wi-Fi.

Để biết địa chỉ MAC, trên máy tính xách tay chạy Windows 7, nhấn vào trình đơn *Start*, tại ô Search, nhập chữ *cmd* và nhấn *Enter*. Sau đó trên cửa sổ lệnh (màu đen) bạn nhập dòng lệnh *ipconfig /all*, nhấn *Enter*, bạn sẽ thấy địa chỉ MAC của máy tính. Nếu bạn dùng Mac OS X, mở *System Preferences*, nhấn *Network*, chọn *Wi-Fi* trong danh sách bên trái, nhấn *Advanced*, hãy chú ý dòng chữ tại ô “Airport ID” or “Wi-Fi ID”. Cách đơn giản hơn, đầu tiên bạn thiết lập thiết bị Wi-Fi không mã hóa (Open), sau đó cho các thiết bị truy cập vào mạng Wi-Fi, lúc này trên thiết bị Wi-Fi bạn sẽ nhìn thấy danh sách các thiết bị truy cập bao gồm địa chỉ IP, địa chỉ MAC.



Hình 2: Lọc truy cập theo địa chỉ MAC.

Giới hạn việc cấp phát địa chỉ IP động

Việc cấp phát địa chỉ IP động DHCP (Dynamic Host Configuration Protocol) từ thiết bị Wi-Fi giúp việc kết nối mạng Wi-Fi dễ dàng hơn. Tuy nhiên, để tăng cường khả năng bảo mật mạng Wi-Fi, bạn chỉ nên thiết lập sao cho lượng địa chỉ IP cấp phát tự động vừa đủ số thiết bị được phép truy cập mạng Wi-Fi.

Che giấu mạng với bên ngoài

Cuối cùng, bạn nên thiết lập chức năng chặn các yêu cầu từ bên ngoài (Block WAN Requests) nhằm che giấu mạng của bạn trước người dùng Internet khác, bên ngoài mạng của bạn. Vì nếu không thiết lập chức năng này, người dùng từ bên ngoài mạng có thể sử dụng các công cụ dò tìm địa chỉ IP công cộng (Public IP) trên thiết bị Wi-Fi của bạn, từ đó họ có thể tiến hành các cuộc tấn công xâm nhập.

Khi bạn đã áp dụng các phương thức bảo mật mạng Wi-Fi như hướng dẫn trên, bạn vẫn không nên chủ quan, lơ là trong việc phòng ngừa. Khoảng 2 tuần/lần bạn nên truy cập vào thiết bị Wi-Fi, kiểm tra xem có các bất thường trong các thiết lập Wi-Fi nào không. Mỗi 6 tháng/lần, bạn nên thay đổi mật khẩu truy cập Wi-Fi. Ngoài ra, hãy sử dụng thêm các công cụ, chẳng hạn NetStumbler (www.netstumbler.com), để kiểm tra mạng Wi-Fi.