Làm thế nào

9 điều cần làm sau khi thiết lập mạng Wi-Fi

Sau khi thiết lập hay nâng cấp hệ thống mạng Wi-Fi, bạn cần kiểm tra lại những yếu tố sau trước khi cho phép mọi người kết nối.

Sau khi hoàn tất quá trình lắp đặt hệ thống mạng Wi-Fi, ai cũng nóng lòng muốn bật lên ngay và kêu gọi mọi người cùng nhau kết nối và truy cập Internet. Tuy nhiên, chuyên gia an ninh mạng khuyên rằng, không bao giờ thừa nếu bạn bỏ ra vài phút để kiểm tra lại kỹ càng hơn trước khi cho phép mọi người kết nối. Các vấn đề cần lưu tâm ở đây là bảo mật và hiệu năng của hệ thống mạng không dây. Bài viết sau đây sẽ đề cập kỹ hơn với 9 lưu ý cần thiết.

1. Kiểm tra lại các điểm truy cập riêng lẻ

Nếu hệ thống mạng không dây mới của bạn có nhiều thiết bị truy cập không dây (access point) riêng lẻ thì đây là điều đầu tiên cần làm. Bạn cần xem từng thiết bị xem có hoạt động hay không, các đèn báo có sáng hay chớp đúng như trong sách hướng dẫn đi kèm hay không. Nếu một trong những access point bị hỏng thì bạn cần thay ngay để không làm ảnh hưởng đến toàn hệ thống mạng. Bạn cần nhớ rằng, access point là điểm truy cập không dây, hoạt động tương tự các bộ chuyển mạch mạng (switch). Bạn có thể gắn access point vào bất kỳ nút mạng (đầu mạng) nào.

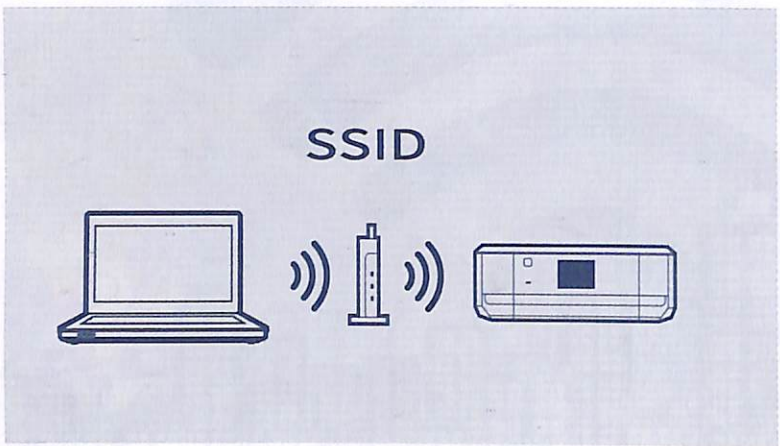
Cần bố trí các thiết bị phát Wi-Fi ở vị trí phù hợp.

Cũng trong bước này, bạn cần kiểm tra lại dây cáp nối có được gắn chắc chắn chưa, các thông số thiết lập đã chính xác để access point có thể truy cập và phát tín hiệu hay không. Rất nhiều trường hợp vì thiết lập sai một thông số bên trong thiết bị access point mà dẫn đến tín hiệu phát không tốt, thậm chí người dùng không kết nối được với mạng Wi-Fi. Với tác vụ chẩn đoán các thiết lập có chính xác hay chưa thì bạn nên kiểm tra xem nhà sản xuất thiết bị access point có bổ sung tiện ích cài đặt nhanh hay không. Thông thường, trên các tiện ích Quick Setup có chức năng chẩn đoán (diagnose) và hướng dẫn khắc phục lỗi thiết lập sai.

Cũng trong bước này, bạn nên xem lại vị trí đặt của các access point sao cho hợp lý để sóng phát ra được rộng và có độ phủ cao hơn. Nên tránh các vị trí góc hẹp, bị che bởi tường gạch, tấm kim loại hay gỗ.

2. Kiểm tra lại thông số VLAN cho từng SSID

Nếu hệ thống mạng của bạn được thiết lập với nhiều mạng LAN ảo (virtual LANs) và SSID thì rất có



Kiểm tra kỹ thông số VLAN cho từng SSID.

thể bạn sẽ thiết lập sai các thông số liên quan trên router, switch hay access point. Ví dụ, mặc dù bạn chỉ định mỗi SSID với một VLAN đơn, nhưng rất có thể thông số VLAN Tagging bị khai báo sai. Điều này vô tình khiến hệ thống tự động trỏ một VLAN riêng (private VLAN) đến với một VLAN công khai (guest VLAN). Bên cạnh đó, khi bạn chạy thử mỗi access point thì cần kiểm tra thật kỹ thông số này để chắc chắn rằng chúng được vận hành hoàn hảo, vì sẽ rất tốn thời gian để sửa, thiết lập lại đúng cho các VLAN bị cấu hình sai.

Bạn cần biết, VLAN là một mạng ảo địa phương hoặc mạng LAN ảo, được sử dụng để phân chia lĩnh vực phát sóng của một thiết bị mạng.

Sau khi cài đặt cho từng access point, bạn nên thử kết nối với mỗi SSID (tên mạng Wi-Fi) để chắc chắn rằng các thiết bị đầu cuối được cấp một địa chỉ IP của một VLAN cụ thể. Để chắc chắn thiết lập định tuyến Inter-VLAN không vô tình kích hoạt hay các quy tắc liên quan đến tường lửa bị cấu hình sai, bạn cần cho phép người dùng truy cập có thể "ping" qua lại giữa các thiết bị hoạt động trên cùng một VLAN và giữa các thiết bị sử dụng với các mạng VLAN khác.

3. Dò lại một lần nữa thiết lập của SSID

Để truyền tín hiệu từ access point đến các thiết bị cần sử dụng, bạn cần cho phép thiết bị phát (ở đây là access point) truyền sóng với SSID tương ứng. Nói dễ hiểu, ví dụ access point A với thiết lập SSID là Wi-Fi_A sẽ truyền tín hiệu đến người dùng thiết bị cuối (máy tính bảng, điện thoại…) khi các thiết bị này kết nối với SSID này.

Nếu bạn đang sử dụng công cụ điều khiển mạng không dây để quản lý tất cả các access point, SSID và những thiết lập khác thì bước này sẽ trở nên đơn giản hơn. Một lưu ý nhỏ ở đây là mặc định, tên mạng Wi-Fi (SSID) thường được hiện công khai để bất kỳ ai cũng có thể dò ra được, vì vậy việc ẩn và thay đổi SSID là bước tiếp theo trong bảo mật mạng Wi-Fi. Để thực hiện, bạn vào mục *Wireless > Basic Wireless Settings*, thay đổi tên SSID trong phần Network Name, sau đó chọn Disable trong mục SSID Broadcast. Tuy nhiên, việc này sẽ khiến cho việc kết nối Wi-Fi của bạn khó khăn hơn vì phải nhập thủ công từ SSID cho đến mật khẩu.

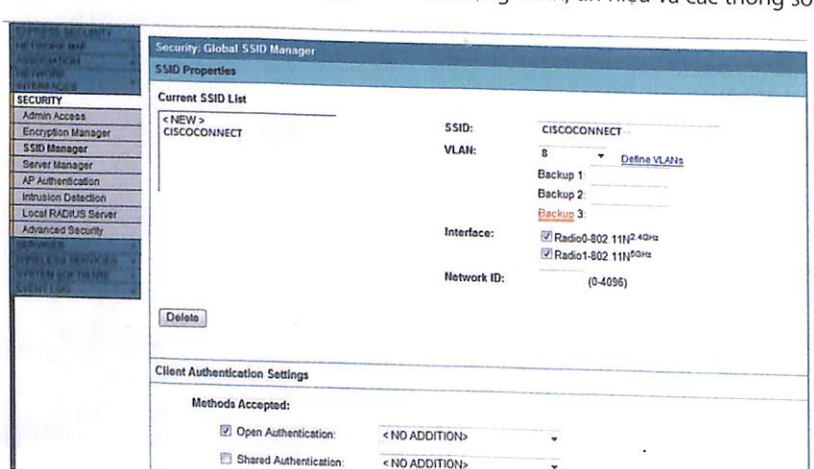
Việc chọn tên mạng Wi-Fi cũng là một lưu ý, mặc dù tên SSID cho phép tối đa 32 ký tự và chấp nhận cả dấu chấm, dấu cách… Nhưng bạn nên chọn tên SSID sao cho đơn giản và mang nét đặc trưng cho dễ quản lý nếu hệ thống mạng có nhiều SSID.

4. Kiểm tra vùng phủ sóng không dây

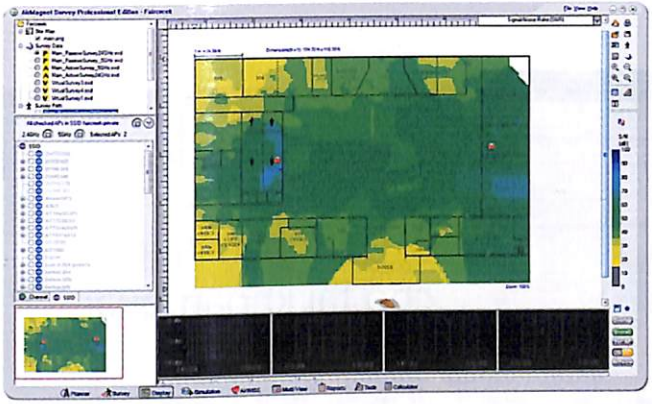
Một lần nữa, bạn cần kiểm tra xem sóng Wi-Fi có được phủ rộng khắp hay không, mặc dù hiện nay công nghệ trên các thiết bị phát và ăng-ten tích hợp giúp sóng "len lỏi" đến mọi ngóc ngách.

Ngoài cách thủ công là bạn mang điện thoại hay laptop chạy đến khắp nơi trong nhà và kiểm tra xem mạng Wi-Fi "sóng sánh" thế nào, thì có cách khác tiện lợi hơn là sử dụng công cụ đo và phân tích mức phủ sóng.

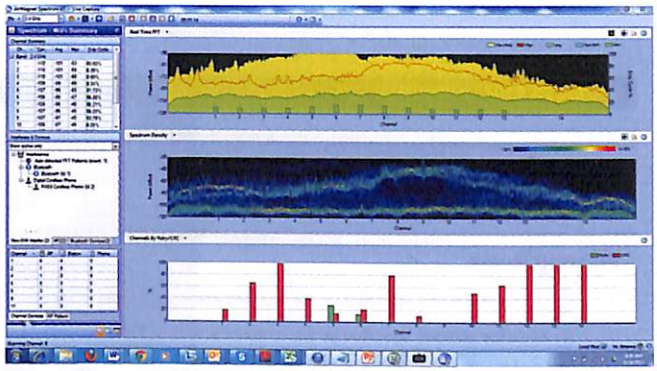
Bạn có thể dùng đến các công cụ như AirMagnet, Ekahau hay TamoGraph để xem mức sóng phát ra (được đo bằng giá trị dBm) của hệ thống mạng không dây. Các công cụ này còn sơ đồ hóa dữ liệu thu được giúp cho bạn dễ hình dung hơn. Những tiện ích này còn thống kê được độ nhiễu và mức độ SNR hay thậm chí các tên mạng SSID bị ẩn. Các công cụ khảo sát bằng bản đồ cho phép bạn hình dung được mức sử dụng kênh, tín hiệu và các thông số



Xem lại các thiết lập liên quan đến SSID (tên mạng và những tùy chọn liên quan đến tên mạng Wi-Fi).



Bản đồ mức sóng không dây được đo bằng công cụ AirMagnet Survey.



Công cụ phân tích mức sử dụng kênh Wi-Fi AirMagnet Spectrum XT với biểu đồ thống kê trực quan về tín hiệu sóng Wi-Fi, độ nhiễu, tần số, kênh...

khác trên bản đồ nhiệt. Biết rõ về hệ thống mạng sẽ cực kỳ hữu ích, nhất là đối với các mạng lớn.

5. Kiểm tra lại băng tần của mạng Wi-Fi

Hầu hết các access point mới đều có tính năng tự động chọn kênh giúp thiết lập kênh tốt nhất khi thiết bị khởi động. Bên cạnh đó, một số mẫu access point còn có thêm tính năng chọn kênh động để dò sóng Wi-Fi liên tục hay định kỳ nhằm chuyển sang kênh có tín hiệu tốt nhất. Nhưng mức độ cảm biến và chính xác nói chung thay đổi tùy theo loại access point, do đó bạn nên luôn kiểm tra lại những lần tự động dò kênh bằng cách thủ công ngay sau đó và sau này cũng phải kiểm tra định kỳ. Tuy nhiên, để có thể phân tích các kênh chính xác, trước hết bạn cần phải tìm hiểu về các băng tần và kênh của mạng không dây.

Công nghệ ngày nay hiện có hai băng tần vô tuyến RF (radio frequency) dành để sử dụng mạng Wi-Fi là 2,4GHz và 5GHz. Cả hai băng tần này dùng phổ sóng vô tuyến không cần đăng ký, nghĩa là thiết bị Wi-Fi không truy cập độc quyền vào các làn sóng trong không gian nhưng phải chia sẻ với các thiết bị không dây khác, gồm điện thoại không dây, camera an ninh không dây, lò vi sóng, thiết bị Bluetooth và Zigbee, hệ thống radar cùng những chủng loại thiết bị khác. Thiết bị Wi-Fi dùng các chuẩn cũ hơn như 802.11b và 802.11g chỉ sử dụng băng tần 2,4GHz, trong khi thiết bị dùng chuẩn mới hơn là 802.11n và 802.11ac có thể sử dụng cả hai loại băng tần 2,4GHz và 5GHz.

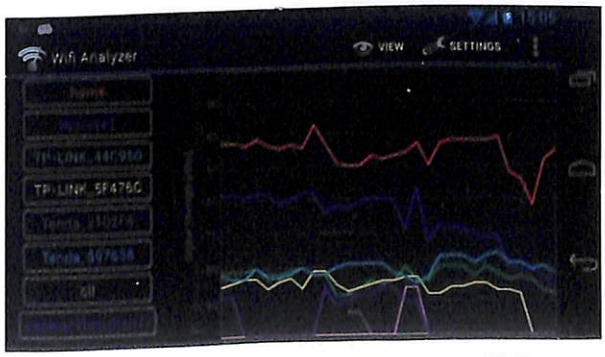
Bạn sẽ thấy rằng băng tần 2,4GHz khá chật chội và có thiết kế kênh trùng lắp nên làm hạn chế số kênh khả dụng. Dù băng tần này thật sự không đủ rộng cho các mạng Wi-Fi nhưng việc nó phải chia sẻ với nhiều công nghệ không dây không cần đăng ký sử dụng cũng làm cho băng tần càng kém hiệu quả hơn. Trong khi đó, băng tần 5GHz rộng hơn nhiều nên ít bị nghẽn, dù vậy có vài quy định về cách sử dụng có thể làm hạn chế số kênh khả dụng trong băng tần này.

6. Kiểm tra mức sử dụng kênh

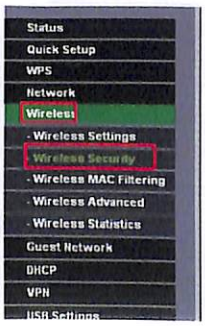
Hiện có nhiều tiện ích giúp phân tích phổ RF như AirMagnet Spectrum XT hay Wi-Spy để bạn đo mức sử dụng kênh Wi-Fi. Những công cụ này còn cho biết mức độ tín hiệu và nhiễu, ngay cả từ các thiết bị không dùng Wi-Fi. Thường thì các công cụ phát hiện Wi-Fi và thậm chí các phần mềm phân tích chuyên nghiệp tự chúng không thể đọc được tín hiệu không-Wi-Fi. Tuy nhiên, hầu hết các phần mềm phân tích và công cụ khảo sát chuyên nghiệp đều có tích hợp trình phân tích phổ RF.

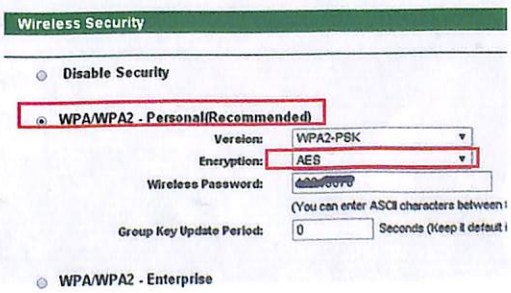
7. Đảm bảo bảo mật cho mạng không dây

Bạn cần biết, hiện tại mã hóa mạng không dây WPA2 bảo mật hơn WPA,WEP; WPA2 dùng khóa mã hóa động có thể thay đổi theo thời gian định trước (mặc định là 3.600 giây). Do đó, bạn cần đặt mức bảo mật cho mạng Wi-Fi lên mức WPA2-Personal ở mục *Wireless > Wireless Security > Security Mode*. Với doanh nghiệp có máy chủ xác thực Radius thì bạn nên chọn WPA2-Enterprise, tiếp theo bạn chọn mã hóa AES, và đặt khóa mã hóa từ

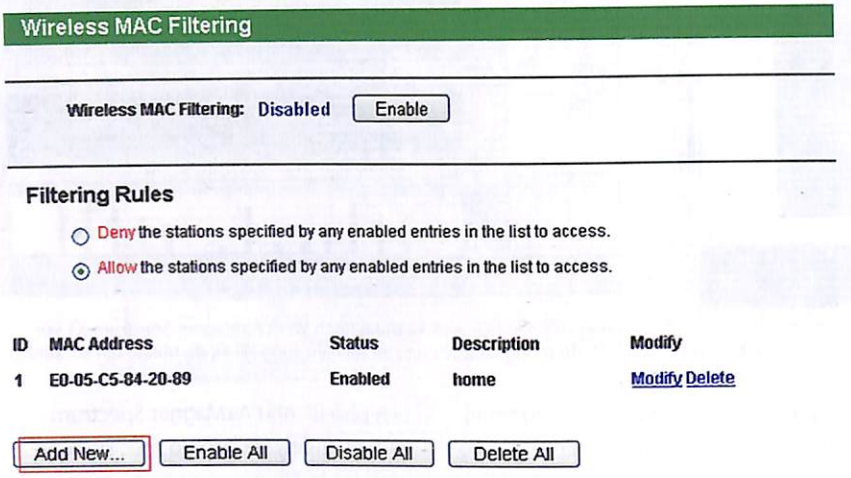


Ứng dụng Wifi Analyzer giúp phân tích băng tần mạng Wi-Fi.





Thiết lập bảo mật ở chuẩn WPA2 giúp cho mạng Wi-Fi được an toàn và khó bị hacker tấn công hơn.



Công cụ đo tốc độ truy cập Speedtest.net.

8-63 ký tự phức tạp.

Nếu cần mức bảo mật cao hơn, bạn có thể bật chế độ kiểm soát truy cập thông qua địa chỉ MAC (Media Access Control). Địa chỉ MAC là dãy số và ký tự duy nhất trên mỗi thiết bị mạng, do đó việc lọc địa chỉ MAC sẽ giúp bạn xác định cụ thể máy tính nào được phép/không được phép truy cập mạng Wi-Fi. Để thiết lập, vào mục *Wireless* > *Wireless MAC Filter* > chọn *Enable*, chọn *Permit*. Nếu các máy tính đã truy cập vào mạng Wi-Fi, bạn có thể nhấn ngay nút *Wireless Client List* để ghi nhận các địa chỉ MAC, nếu không bạn phải nhập thủ công từng địa chỉ MAC các máy tính mà bạn cho phép truy cập.

Bảo mật mạng không dây không dừng ở việc đặt mật khẩu bảo vệ truy cập hay lọc địa chỉ MAC, bạn cũng cần bảo vệ các thiết bị phát khỏi bị xâm nhập và phá hoại. Vì chỉ cần tìm ra được vị trí access point thì hacker có thể xóa sạch mọi thiết lập của hệ thống mạng chỉ sau vài giây Reset đưa thiết bị về trạng thái mặc định lúc xuất xưởng (*Restore factory defaults*).

8. Kiểm tra tốc độ truy cập

Để xem tốc độ truy cập thực tế của mạng không dây vừa tạo, bạn nên sử dụng một công cụ đo khách quan thay vì kiểm tra bằng cảm quan thông qua việc truy cập web. Có một công cụ nền web khá hữu ích là *Speedtest.net* của Ookla để bạn lựa chọn. Speedtest có thể đo tốc độ upload, download cũng như giới hạn băng thông của mạng Wi-Fi.

Bạn cũng nên đo tốc độ truy cập nội bộ thông qua một công cụ đo hiệu năng mạng không dây. Chẳng hạn như *NetStress* của Nuts About Net, *LAN Speed Test* của TotuSoft.

9. Đảm bảo an toàn cho tài khoản quản trị

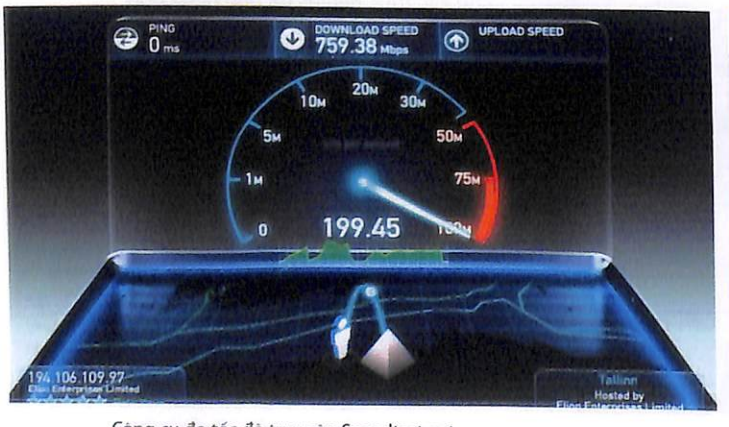
Việc đầu tiên là bạn cần đổi mật khẩu quản trị cho mạng Wi-Fi ngay trong lần đầu truy cập. Đây là điều cần thiết vì những mật khẩu mặc định của từng hãng sản xuất và dòng sản phẩm được giới hacker thuộc lòng. Bạn cũng nên đặt mật khẩu càng khó đoán càng tốt. Tham khảo cách đặt mật khẩu mạnh tại *www.pcworld.com.vn/T1233742*.

Một số dòng access point có phép bạn thiết lập chế độ truy cập giao diện quản trị với nhiều địa chỉ khác nhau. Điều này giúp cho việc bảo mật được tốt hơn, nhưng bạn cần lưu lại các địa chỉ và thông tin đăng nhập để không phải "mò mẫm" khi lỡ quên sau đó.

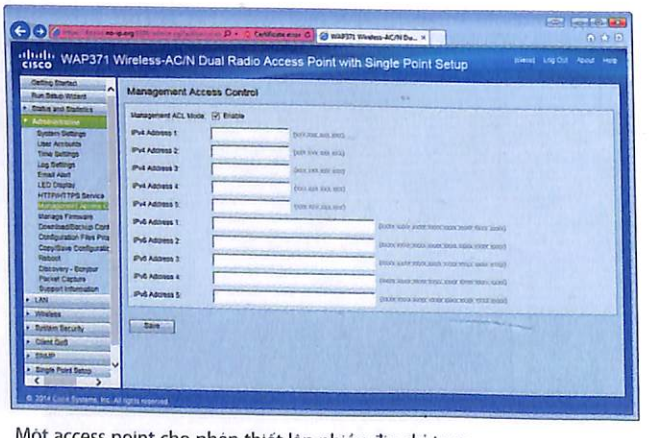
Một mẹo nhỏ với người dùng iOS là bạn nên lưu lại thông tin đăng nhập vào giao diện quản trị vào ứng dụng Notes trên iPhone/iPad (dùng iOS 9 trở lên). Sau đó kích hoạt chức năng bảo vệ bằng mật khẩu. Như vậy, hệ thống mạng của bạn trở nên an toàn hơn với "hai lớp bảo vệ".

Một access point cho phép thiết lập nhiều địa chỉ truy cập giao diện quản lý mạng Wi-Fi.

HUY HOÀNG



Công cụ đo tốc độ truy cập Speedtest.net.



Một access point cho phép thiết lập nhiều địa chỉ truy cập giao diện quản lý mạng Wi-Fi.