گام به گام تا رسیدن به یک شبکه ایده‌ال

چگونه روتر بی‌سیم خود را تنظیم و بهینه سازی کنیم (بخش دوم)

تنظیمات پایه و اولیه روی اغلب روترها در خود کارخانه انجام می‌شود تا کارها تا حد ممکن ساده گردد. اما حتی اگر شما همه چیز را به راحتی متصل کرده باشید و شبکه شما کار هم بکند به این معنا نیست که عملکرد و امنیت شبکه شما به همان خوبی است که باید باشد. اگر می‌خواهید بهترین عملکرد ممکن را از شبکه وای‌فای خانگی خود دریافت کنید این مراحل ساده تنظیمات روتر را دنبال کنید.

بخش اول این مقاله را می توانید در اینجا بخوانید.

قلب شبکه خانگی شما را روتر آن تشکیل می‌دهد، بنابراین برای در اختیار داشتن یک شبکه خانگی ایده‌ال اول باید به این قطعه سخت افزاری رسیدگی کنیم. در بخش اول این مقاله به نحوه انتخاب روتر، اتصال آن به اینترنت، دسترسی به کنسول مدیریتی برای سفارشی سازی تنظیمات و مدیریت آدرس‌های ای‌پی با سرور DHCP پرداختیم.

کار با آی‌پی‌های ثابت

حالا که با استفاده از سرور DHCP تعدادی آدرس آی‌پی در اختیار دارید، باید به طور دستی آنها را به دستگاه‌هایی که به آدرس ثابت نیاز دارند اختصاص دهید. کاری که شما باید انجام دهید این است که برای آداپتور شبکه دستگاه مورد نظر خود یک IP address ، Subnet Mask، Gateway address و یک DNS server address واحد در نظر بگیرید. بر اساس مثالی که ما برای تعیین مجموعه آی‌پی در سرور DHCP در نظر گرفتیم، شما باید از آدرس‌هایی بین 192.168.0.52 تا 192.168.0.254 برای IP address و 255.255.255.0 برای Subnet Mask استفاده کنید. آدرس‌های Gateway و DNS نیز با آدرس ای‌پی روتر یکسان است که در مثال ما 192.168.0.1 است.

فهرست آدرس‌های ای‌پی ثابتی که انتخاب می‌کنید را یادداشت کنید تا در آینده به اشتباه دوباره از آنها استفاده نکنید. فرآیند تنظیم آدرس‌های ای‌پی ثابت به یک آداپتور شبکه به دستگاهی که استفاده می‌کنید بستگی دارد، بنابراین برای پیدا کردن روش انجام آن به راهنمای آن مراجعه کنید.

فعال سازی وای‌فای شما

حالا که پیکربندی شبکه شما انجام شده، وقت آن رسیده است تا به تنظیمات شبکه بی‌سیم خود بپردازید. انجام کار بسیار راحت است. وقتی این کار را انجام می‌دهید مطمئن شوید که یکی از کامپیوترهای شما از طریق کابل اترنت به شبکه متصل شده باشد. اگر شما بخواهید پیکربندی وای‌فای را به صورت بی‌سیم انجام دهید، هر زمان که یک تغییر را اعمال می‌کنید اتصال به کنسول مدیریتی را از دست خواهید داد.

حالا مراحل زیر را دنبال کنید:

- به کنسول مدیریتی روتر رفته و بخشی با عنوان Wireless Setup را پیدا کنید. این نام ممکن است بر اساس نوع روتری که شما استفاده می‌کنید متفاوت باشد، اما نام هر بخش کاملا گویای وظیفه‌ای که انجام می‌دهد است
- به احتمال زیاد شبکه بی‌سیم شما به طور پیش فرض فعال است. اما اگر اینطور نیست آن را روشن کنید. اگر از یک روتر دو بانده استفاده می‌کنید، باید تنظیمات مربوط به هر دو شبکه 2.4 و 5 گیگاهرتز را مشاهده کنید و هر کدام را به طور جداگانه پیکربندی کنید
- سپس مطمئن شوید که Channel روی Auto تنظیم شده باشد و بخش Mode را در وضعیت پیش فرض خود رها کنید. در آینده اگر احساس کردید که شبکه بی‌سیم شما کند کار می‌کند یا اتصال شما دائما قطع می‌شود می‌توانید این تنظیمات را تغییر دهید
- حالا نوبت SSID است. SSID بیانگر نام شبکه بی‌سیم شما است. شما می‌توانید برای شبکه خود هر نامی که مایل هستید را انتخاب کنید و فراموش نکنید که به هیچ وجه نباید آن را در حالت پیش فرض رها کنید.
- مرحله نهایی تنظیم نوع کدگذاری است که شبکه وای‌فای شما استفاده خواهد کرد. چند انتخاب در اختیار شما است، اما بهتر است از WPA2 استفاده کنید
- احتمالا برای WPA2 نیز چند گزینه برای انتخاب وجود دارد، اما بهتر است [WPA2-PSK [AES را انتخاب کنید. در حال حاضر این بالاترین سطح امنیت برای یک شبکه بی‌سیم است. بعضی از روترها هنوز هم WEP را ارائه می‌کنند. به هیچ وجه از آن استفاده نکنید زیرا در مقابل حملات سایبری بسیار آسیب پذیر است
- بعد از این که نوع کدگذاری خود را WPA2 انتخاب کردید، باید یک گذرواژه یا Passphrase نیز انتخاب کنید. این گذرواژه باید بین 8 تا 63 کاراکتر باشد و از حروف (بزرگ و کوچک)، اعداد و کاراکترهای ویژه تشکیل شده باشد. هر چه گذرواژه شما طولانی‌تر و پیچیده‌تر باشد امنیت آن نیز بیشتر خواهد بود. گذرواژه‌هایی مثل hy*#Pnj125!ou که به طور تصادفی ایجاد می‌شوند از همه بهتر هستند.

بعد از اعمال این تنظیمات حالا وقت آن رسیده تا تغییرات را ذخیره کرده و اتصال خود را آزمایش کنید. دستگاه‌های بی‌سیم شما حالا باید بتوانند به شبکه و اینترنت دسترسی داشته باشند.

واژه‌ای به نام امنیت

خیلی از روترها از قابلیتی به نام Wi-Fi Protected Setup یا WPS استفاده می‌کنند که یک استاندارد امنیتی شبکه برای امن نگه داشتن آسان یک شبکه خانگی از طریق فشردن یک دکمه است. اما باید آن را غیرفعال کنید. محققان

دریافته‌اند که WPS می‌تواند در مقابل حملات مخرب آسیب پذیر باشد. ریسک استفاده از WPS تنها به این دلیل که کار ما را راحت می‌کند قابل توجیه نیست.

یکی از موارد دیگری که شما برای افزایش سطح امنیت می‌توانید به آن رسیدگی کنید مخفی کردن نام شبکه (SSID) از دید دیگران است. با انجام این کار نام شبکه شما در فهرست شبکه‌های جستجو شده توسط دستگاه‌های بی‌سیم (چه افراد غریبه یا خودی) قرار نمی‌گیرد و برای اتصال به شبکه شما باید SSID را به طور دستی در دستگاه خود وارد کنید. هر چند این روش سطح امنیت واقعی شبکه شما را بالا نمی‌برد، اما می‌تواند شبکه شما را از دید کاربران غریبه پنهان کند.

بر اساس مدل روتری که استفاده می‌کنید، در صفحه تنظیمات بی‌سیم ممکن است گزینه‌ای برای فعال کردن شبکه مهمان وجود داشته باشد. شبکه مهمان یا Guest Network به کسانی که به خانه شما سر می‌زنند اجازه می‌دهد تا بدون امکان دسترسی به سایر دستگاه‌های موجود در شبکه شما تنها از اینترنت آن استفاده کنند. ما به شما توصیه می‌کنیم برای افزایش سطح امنیت شبکه خود حتما از این گزینه استفاده کنید. شبکه مهمان برای هر دو باند 2.4 و 5 گیگاهرتز موجود است و پیکربندی آن به همان شیوه معمول شبکه بی‌سیم انجام می‌شود، اما فراموش نکنید که برای آن حتما از یک گذرواژه متفاوت استفاده کنید.

داده‌های خود را به اشتراک بگذارید

یکی از مهمترین جنبه‌های استفاده از یک شبکه خانگی توانایی به اشتراک گذاری منابع در آن است. روش‌های گوناگونی برای انجام این کار وجود دارد. استفاده از یک سرور بهترین راهکار برای این کار است، اما همه کاربران خانگی آن را در اختیار ندارند. دستگاه‌های Network Attached Storage یا NAS راهکاری ساده اما گران‌تر برای به اشتراک گذاری منابع هستند. خیلی از روترهای پیشرفته به عنوان یک راه حل جایگزین از پورت‌های USB داخلی استفاده می‌کنند که می‌توان از آنها برای به اشتراک گذاری هارد درایو یا چاپگر با کاربران شبکه استفاده کرد.

منبع:

pcmag

تاریخ انتشار:
25 مهر 1396

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/10165/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%B1%D9%88%D8%AA%D8%B1-%D8%A8%DB%8C%E2%80%8E%D8%B3%DB%8C%D9%85-%D8%AE%D9%88%D8%AF-%D8%B1%D8%A7-%D8%AA%D9%86%D8%B8%DB%8C%D9%85-%D9%88-%D8%A8%D9%87%DB%8C%D9%86%D9%87-%D8%B3%D8%A7%D8%B2%DB%8C-%DA%A9%D9%86%DB%8C%D9%85-%D8%A8%D8%AE%D8%B4-%D8%AF%D9%88%D9%85