



در شماره گذشته آموزش نتورک پلاس با استانداردهای بیسیم و سایر مباحث مرتبط با شبکه‌های بیسیم، روش‌های دسترسی و IEEE 802.11 Frames آشنا شدیم. در شماره فوق این مبحث را ادامه می‌دهیم.

برای مطالعه بخش چهارم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

نوآوری های 802.11

درست است که برخی از سرویس‌های لایه فیزیکی عملکرد متفاوتی دارند، اما همه استانداردهای 802.11 از سیگنالینگ نیمه دویپلکس استفاده می‌کنند. به عبارت دیگر، یک گره بی‌سیم با استفاده از یکی از تکنیک‌های موجود در استاندارد 802.11 می‌تواند فرآیند انتقال یا دریافت را مدیریت کرده، اما نمی‌تواند هر دو کار را همزمان انجام دهد، مگر اینکه گره بیش از یک گیرنده/فرستنده را نصب کرده باشد. برخی از نقاط دسترسی بی‌سیم می‌توانند با استفاده از فرکانس‌های مختلف، سیگنال تمام دویپلکس را شبیه‌سازی کنند. با این وجود، انتقال برای هر آنتن هنوز به شکل نیمه دویپلکس خواهد بود. علیرغم این محدودیت فیزیکی، 802.11n همراه با نوآوری‌هایی معرفی شد که نشان داد استانداردهای 802.11 در آینده این پتانسیل را دارند تا سریع‌تر و قابل اعتمادتر باشند. از جمله این نوآوری‌ها به موارد زیر می‌توان اشاره کرد:

مایمو- MIMO (چند ورودی- چند خروجی) اولین بار همراه با استاندارد 802.11n و آنتن‌های چندگانه اکسس پوینت و دستگاه کلاینتی که فرآیند پردازش داده‌های وارد و خارج شوند را به شکل همزمان مدیریت می‌کرد، ارائه شد. شکل زیر روتر دو بانده SOHO که از استانداردهای 802.11n/802.11ac پشتیبانی کرده و سه آنتنه است را نشان می‌دهد.



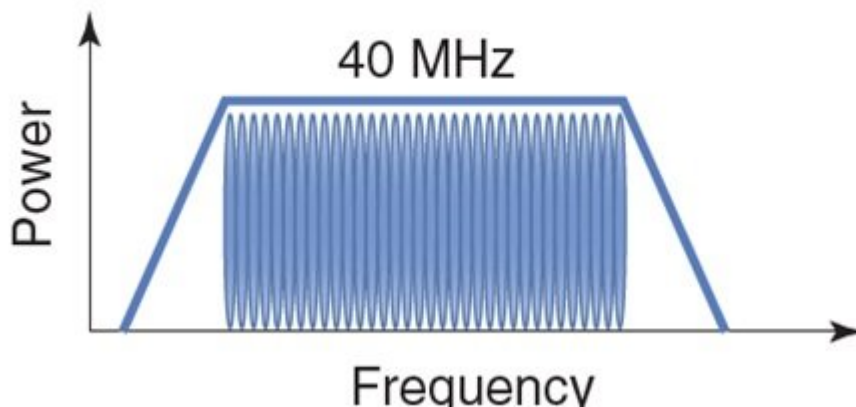
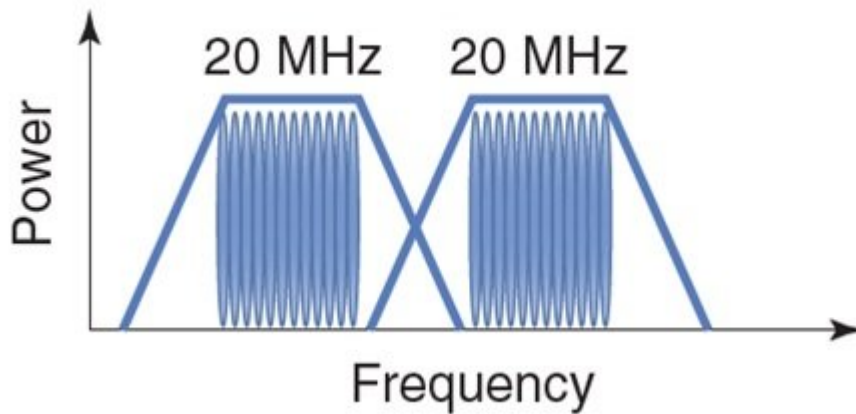
درست است برخی از دستگاه‌های چندآنته بر مبنای استاندارد 802.11g ارائه شده‌اند، اما این آنتن‌ها به شیوه خودشان پردازش جریان داده‌ها را مدیریت می‌کنند. اما در نقطه مقابل، دستگاه‌های 802.11n/ac به‌طور همزمان داده‌ها را از طریق دو یا چند آنتن پردازش می‌کنند. همان‌گونه که قبلاً یاد گرفتید، سیگنال‌های بیسیم در چند مسیر انتشار پیدا می‌کنند. بنابراین، انتظار نمی‌رود چند سیگنال بتوانند در یک زمان از طریق گیرنده‌ای دریافت شوند. MIMO سعی می‌کند با رویکرد تنظیم فاز یا دامنه سیگنال‌های هر آنتن از مزایای این تکنیک به بهترین شکل استفاده کند. این انتقال از دو طریق دو راهکار زیر بهبود پیدا می‌کند.

کیفیت سیگنال و محدوده - تنوع فضایی آنتن‌های مختلف باعث کاهش نویز در انتقال شده و فاصله موثر انتقال سیگنال‌ها را به شکل قابل توجهی افزایش می‌دهند. هر آنتن شکلی تقریباً متفاوت از یک سیگنال دریافت کرده و در نتیجه نقاط قوت و مثبت هر سیگنال با یکدیگر جمع می‌شوند.

ظرفیت سیگنال - تسهیم‌سازی فضایی جریان داده جدیدی را میان هر یک از آنتن‌های اضافی می‌افزاید. در نتیجه حجم و میزان داده‌های ارسالی و دریافتی افزایش پیدا می‌کند. این رویکرد با افزایش هر جفت آنتن افزایش پیدا می‌کند.

• MU-MIMO (چند کاربره- چند ورودی چند خروجی) - بر مبنای رویکرد MIMO، یک فناوری جدیدتر به نام MU-MIMO همراه با محصولات 802.11ac Wave 2 به بازار عرضه شده که به چندین آنتن اجازه می‌دهد به‌طور همزمان به چند کلاینت سرویس‌دهی کنند. این ویژگی تراکم را کاهش می‌دهد و از این طریق به انتقال سریع‌تر اطلاعات کمک می‌کند. یک اکسس پوینت MU-MIMO تنها زمانی از حداکثر ظرفیت خود می‌تواند استفاده کند که دستگاه‌های کلاینت از فناوری MU-MIMO پشتیبانی کنند.

• پیوند کانال (Channel bonding) - در استاندارد 802.11n، دو کانال مجاور 20 مگاهرتزی می‌توانند برای ایجاد یک کانال 40 مگاهرتزی، به صورت یکپارچه یا پیوندی ترکیب شوند، همان‌گونه که در شکل زیر نشان داده شده است.



اتصال دو کانال 20 مگاهرتزی پهنای باند موجود در یک کانال 20 مگاهرتزی را دو برابر می‌کند. به همین دلیل است که به‌طور معمول مقدار کمی از پهنای باند موجود به عنوان بافر و برای مقابله با مشکل تداخل در بالا و پایین کانال‌های 20 مگاهرتز به جای انتقال داده‌ها تخصیص داده می‌شود. از آنجایی که باند 5 گیگاهرتز کانال‌های بیشتری داشته و کمتر شلوغ است (حداقل برای NW)، گزینه بهتری در مقایسه با باند 2.4 گیگاهرتزی برای پیوند کانال‌ها است. همین مسئله باعث شد تا روند توسعه استاندارد 802.11ac با هدف بهبود کارایی نسبت به استاندارد 802.11n با جدیت دنبال شود. استاندارد جدیدتر 802.11ac با پشتیبانی از کانال‌های 20، 40 و 80 مگاهرتزی تکنیک پیوند کانال را بهبود بخشید که نتیجه آن پدید آمدن کانال‌های 160 مگاهرتزی است.

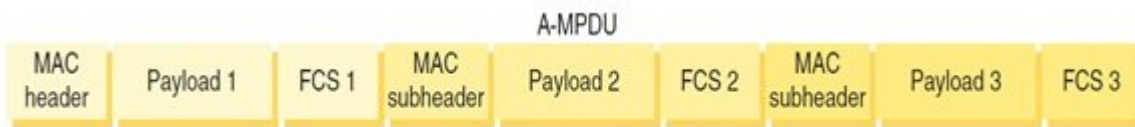
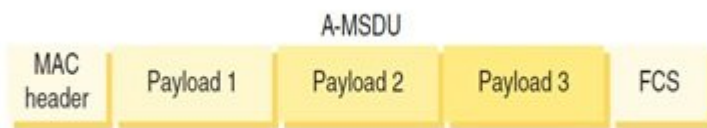
• جمع فریم: با اتکا بر استاندارد 802.11n، شبکه‌ها می‌توانند از یکی از دو تکنیک A-MPDU سرنام Unit Data Protocol Pro یا A-MSDU سرنام Unit Data Service Data Aggregated Mac برای ترکیب فریم‌های چندگانه داده‌ای به منظور ساخت فریم بزرگ‌تر استفاده کنند.

استاندارد 802.11ac از تکنیک A-MPDU به شکل پیش‌فرض برای همه انتقال‌ها استفاده می‌کند. هر دو روش با هدف ترکیب چند فریم با یکدیگر به منظور کاهش سرباره‌ها استفاده می‌شوند. هر فریم بزرگی تنها یک کپی از اطلاعات آدرسی در اختیار دارد که درون فریم‌های کوچک‌تر قرار دارند. به‌تناسب، فیلدها فضای تجمیع کمتری را اشغال می‌کنند. علاوه بر این، جایگزینی چهار فریم کوچک با یک فریم بزرگ مشکل کنترل خطا را بهتر و دسترسی به مدیا را ساده‌تر می‌کند، زیرا تعداد پیام‌های مبادله شده کلاینت برای برقراری ارتباط به یک چهارم کاهش پیدا می‌کند. حداکثر اندازه فریم برای هر دو استاندارد 802.11n و 802.11ac در جدول زیر نشان داده شده است. این اعداد را با حداکثر فریم 4095 بایت استانداردهای 802.11b/a/g مقایسه کنید.

حداکثر اندازه فریم استفاده شده در رویکرد تجمیع فریم		
استاندارد وای فای	A-MSDU	A-MPDU
802.11n	bytes 7935	bytes 65,535

802.11ac	bytes 11,454	bytes 4,692,480
----------	--------------	-----------------

شکل زیر نشان می‌دهد که دو رویکرد A-MSDU و A-MPDU چگونه به کم شدن سرپاره‌ها کمک می‌کند.



مزیت رویکرد A-MSDU بیشتر از رویکرد A-MPDU است که اطلاعات فریم بیشتری را با سایر فریم‌ها در یک زمان انتقال می‌دهد. ضعف بالقوه استفاده از فریم‌های بزرگ، افزایش احتمال خطا در هنگام انتقال بلوک‌های بزرگ‌تر داده‌ای است. بنابراین، مزیت A-MPDU این است که برخی از داده‌های بررسی خطا را حفظ کرده و در نتیجه قابلیت اطمینان بیشتری را ارائه می‌کند.

توجه داشته باشید که همه تکنیک‌های ذکر شده در این مطلب ممکن است در پیاده‌سازی استانداردهای 802.11n و 802.11ac استفاده نشوند. علاوه بر این، دستیابی به حداکثر توان عملیاتی به دو فاکتور تعداد و نوع استراتژی‌های استفاده شده بستگی دارد. به‌کارگیری باند 2.4 گیگاهرتز (برای 802.11n) یا باند 5 گیگاهرتز در یک شبکه نیز عامل تعیین‌کننده‌ای هستند. با توجه به این عوامل، توان عملیاتی واقعی پردازش در شبکه‌های 802.11n بین 65 مگابیت تا 500 مگابیت در ثانیه متغیر است، در حالیکه توان عملیاتی واقعی شبکه‌های 802.11ac موج دوم در زمان نوشتن این مطلب تا 891 مگابیت بر ثانیه برای هر کلاینت در فاصله کوتاه است. همان‌گونه که قبلاً ذکر شد، 802.11n و 802.11ac با هر سه نسخه پیشین 802.11 سازگاری دارند. با این حال، در محیط‌های ترکیبی، بعضی از تکنیک‌های استاندارد جدید برای بهبود کارایی تأثیر چندانی نخواهند داشت. برای اطمینان از این موضوع که شبکه محلی 802.11n از نرخ انتقال داده سریعی برخوردار خواهد بود، این استاندارد برای استفاده در دستگاه‌های سازگار با استاندارد 802.11n بهینه‌سازی شده است. استاندارد 802.11ac رفته رفته در حال فراگیر شدن بوده و با دستگاه‌های مبتنی بر استانداردهای 802.11ac و 802.11n قابل استفاده است.

امنیت شبکه‌های وای‌فای

همان‌گونه که ممکن است حدس زده باشید، اکثر سازمان‌ها یک یا چند استاندارد 802.11 را در شبکه‌های محلی بیسیم خود استفاده می‌کنند. به‌طور پیش‌فرض، 802.11 هیچ‌گونه استاندارد امنیتی ارائه نمی‌کند. در نتیجه کلاینت‌ها با دانستن SSID که بیشتر اکسس‌پوینت‌ها بر مبنای رویکرد پخش (broadcast) آن‌را انتشار می‌دهند قادر هستند به شبکه دسترسی داشته باشند. مدیران شبکه ممکن است برای افزایش امنیت مانع از انتشار SSID ها شوند تا شناسایی آن سخت‌تر شود، با این حال، این رویکرد امنیت واقعی را به ارمغان نخواهد آورد. برای حل این مشکل دو راه راهکار احراز هویت و رمزگذاری برای حفظ امنیت شبکه‌های بیسیم ارائه شده است. با توجه به این‌که در شماره‌های آینده مبحث تأمین امنیت روی شبکه‌ها را به شکل مفصل بررسی خواهیم کرد، در نتیجه در این‌جا رویکردها و راهکارهای پیشنهاد شده در ارتباط با دو مکانیزم فوق و همچنین سایر تهدیداتی که پیرامون شبکه‌های وای‌فای قرار دارند را بررسی نکرده و در مقاله‌های آتی به سراغ این مبحث خواهیم رفت.

اشکال‌زدایی شبکه‌های وای‌فای

در شماره‌های قبلی آموزش **نورک‌پلاس** با ابزارهایی که برای آزمایش کابل‌های فیبر نوری و مسی در شبکه‌های اینترنت استفاده می‌شوند آشنا شدید. تست‌هایی که برای بررسی قطعی یا عملکرد کابل استفاده می‌شوند به شما درباره گره‌ها، ارتباطات بی‌سیم یا اکسس‌پوینت‌هایی که روی یک شبکه قرار دارند اطلاعاتی نمی‌دهند. برای این منظور شما به ابزارهایی که روی پروتکل‌های بی‌سیم و کارت‌های شبکه متمرکز هستند نیاز دارید. همان‌گونه که در ابتدای مبحث شبکه‌های بی‌سیم به آن اشاره داشتیم، شما می‌توانید با نگاه کردن به خصلت‌ها و ویژگی‌های مرتبط با شبکه‌های بی‌سیم روی ایستگاه کاری خودتان اطلاعاتی درباره محیط بیسیم به دست آورید. با این حال، این رویکرد تنها اطلاعات مختصری درباره محیط بیسیم ارائه کرده و تنها برای یک ایستگاه کاری سودمند است. برای آن‌که

تصویر کاملی از محیط بیسیم به دست آورید، باید از ابزارهای پیشرفته شبکه‌های بیسیم استفاده کنید.

ابزارهایی ویژه شبکه‌های بیسیم

بسیاری از برنامه‌های کاربردی می‌توانند سیگنال‌های بی‌سیم را در یک محدوده جغرافیایی خاص اسکن کنند و تمام نقاط دسترسی و گره‌های بی‌سیم که در یک محدوده قرار گرفته‌اند را شناسایی کنند. این رویکرد برای تعیین این‌که آیا یک اکسس پوینت به درستی کار می‌کند یا به درستی در مکانی قرار گرفته مفید است. به این ترتیب تمام گره‌هایی که اکسس پوینت به آن‌ها خدمت‌رسانی می‌کند قادر هستند روی کانل‌های مناسب در یک باند فرکانسی درست به شبکه متصل شوند. در این مقاله با دو ابزار کاربردی که اطلاعات مفیدی درباره شبکه‌ها در اختیارتان قرار می‌دهند آشنا خواهید شد. برای اطلاع بیشتر درباره نرم‌افزارهایی که برای ارزیابی عملکرد شبکه‌ها استفاده می‌شوند به مقاله [10 ابزار رایگان تحلیلی و نظارتی بر شبکه‌های کامپیوتری](#) مراجعه کنید.

- ابزارهای تحلیل‌گر طیف‌سنجی - دستگاهی است که می‌تواند کیفیت یک سیگنال بی‌سیم را ارزیابی کند. به‌طور مثال، طیف‌سنجی و تحلیل طیف فرکانسی کمک می‌کند تا مکان‌هایی که بیشتر تداخل دارند را پیدا کنیم.
- ابزار تحلیل‌گر وای‌فای، نرم‌افزاری است که می‌تواند در دسترس بودن شبکه وای‌فای را ارزیابی کرده و کمک می‌کند تا تنظیمات مربوط به سیگنال‌های وای‌فای را به شکل بهتری تنظیم کرده و تهدیدات امنیتی پیرامون شبکه‌های وای‌فای را شناسایی کنید. شناسایی کانال‌های بی‌سیم که نزدیکی شما در حال استفاده هستند، به شما کمک می‌کند تنظیمات کانال‌های بی‌سیم را به درستی پیکربندی کنید.
- ابزارهای نرم‌افزاری که می‌توانند در ارزیابی شبکه‌های بی‌سیم استفاده شوند، اغلب به صورت رایگان در دسترس هستند و ممکن است از سوی تولیدکنندگان اکسس‌پوینت‌ها ارائه شده باشد. در ادامه با فهرستی از قابلیت‌های خاص و مشترک ابزارهای تست شبکه‌های بی‌سیم آشنا خواهید شد.
- شناسایی گره‌ها، اکسس‌پوینت‌های در حال انتقال و کانال‌هایی که ارتباط را برقرار کرده‌اند.
- اندازه‌گیری قدرت سیگنال و تعیین محدوده یک اکسس‌پوینت
- نشان دادن ضعیف شدن، از دست رفتن یا وجود نویز روی سیگنال
- تفسیر اطلاعات قدرت سیگنال برای ارزیابی موقعیت مکانی اکسس‌پوینت
- حصول اطمینان از برقراری ارتباط مناسب و اتصال مجدد زمانی که در حال حرکت میان اکسس‌پوینت‌ها هستید
- ضبط و تفسیر ترافیک مبادله شده بین اکسس‌پوینت‌ها و گره‌ها
- اندازه‌گیری میزان مصرف و ارزیابی خطای انتقال داده‌ها
- تجزیه و تحلیل ویژگی‌های هر کانال در یک باند فرکانس برای نشان دادن مطلوب‌ترین کانال‌ها

اجتناب از بروز مشکلات

ممکن است تجربه ناخوشایندی از عدم دسترسی به شبکه را تجربه کرده باشید، حتا زمانی که مطمئن بوده‌اید که نام کاربری و گذرواژه را به درستی وارد کرده‌اید. شاید متوجه شوید که کلید Caps Lock در زمان تایپ گذرواژه‌ها روشن بوده و کاراکترهای بزرگ و کوچک به اشتباه وارد شده‌اند یا ممکن است قصد اتصال به سرور اشتباهی را داشته‌اید. در هر شبکه‌ای، بیشتر متغیرها باید به شکل دقیق روی کلاینت‌ها، سرورها و دستگاه‌های ارتباطی تنظیم شده باشند تا ارتباط برقرار شود. شبکه‌های بی‌سیم چند متغیر بیشتر نسبت به شبکه‌های سیمی دارند. در ادامه با برخی از اشتباهات رایج پیرامون شبکه‌های بی‌سیم آشنا می‌شوید.

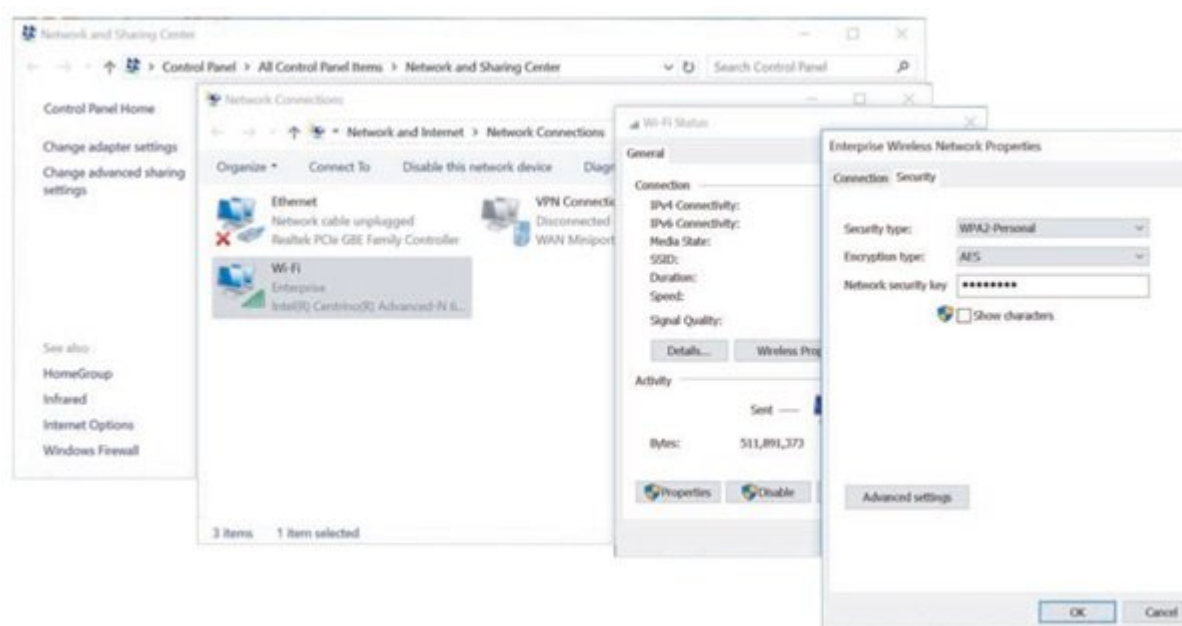
SSID اشتباه

کلاینت بی‌سیم ممکن است مجبور شود SSID صحیح را انتخاب کند. همان‌گونه که آموخته‌اید، شما می‌توانید کلاینت‌ها

را ملزم کنید تا برای دسترسی به هر اکسس پوینت جست و جوی را انجام دهد (یا کلاینتها ممکن است به شکلی پیکربندی شده باشند که به شکل پیش فرض این کار را انجام دهند). با این حال، اگر اکسس پوینت SSID را به شکل پخش منتشر نکند یا اگر ایستگاه کاری به شکلی پیکربندی نشده باشد تا جست و جوی برای اکسس پوینتها انجام دهد، شما باید SSID را به شکل دستی وارد کنید. دقت کنید که SSIDها حساس به حروف هستند. یعنی CLASS_1 برابر Class_1 نیست.

عدم هماهنگی پارامترهای امنیتی

دستگاه کلاینت بیسیم باید به شکلی پیکربندی شده باشد تا از رمزگذاری یکسان با اکسس پوینت استفاده کند. اغلب اوقات این کار به شکل خودکار بین اکسس پوینت و کلاینت انجام می شود. برای پیکربندی دستی نوع مکانیزم امنیتی روی سرویس گیرنده ای مبتنی بر ویندوز 10، Network and Sharing Center را باز کنید، روی Change adapter settings کلیک کرده، روی ارتباط فعال کلیک راست کرده، گزینه Status، را کلیک کرده و سپس کادر مربوط به ویژگی های ارتباط را باز کنید. برای تغییر نوع مکانیزم امنیتی، نوع رمزنگاری یا کلید امنیتی، روی زبانه Security کلیک کنید. شکل زیر این فرآیند را نشان می دهد.



- عبارت عبوری اشتباه - به طور مشابه، شما باید از کلید امنیتی یا عبارت عبوری که منطبق با اکسس پوینت است استفاده کنید. اگر این گونه نباشد، دستگاه کلاینت و اکسس پوینت نمی توانند احراز و تایید را به درستی انجام دهند.
- هم پوشانی کانالها یا فرکانسهای ناسازگار - شما یاد گرفتید که اکسس پوینت کانال و فرکانسی را منتشر می کند تا کلاینتها با آن ارتباط برقرار کنند. کلاینتها پس از آن، به طور خودکار کانال و فرکانس صحیح را می شناسند. با این حال، اگر کلاینت را ملزوم کنید فقط از یک کانال یا فرکانسی متفاوت از آن چیزی که اکسس پوینت ارائه کرده استفاده کند، ارتباط شکست خورده و با مشکل روبرو می شود. به طور مشابه، به کارگیری کانالها یا فرکانسهایی که در فرکانس طیفی بسیار نزدیک به یکدیگر قرار دارند نیز باعث می شود تا مشکل تداخل رخ دهد.
- استانداردهای ناسازگار (802.11n / ac / g / a / b) - اگر اکسس پوینت شما به گونه ای تنظیم شده که برای برقراری ارتباط تنها از استاندارد 802.11ac استفاده می کند، حتی زمانی که دفترچه راهنما اعلام می دارد که اکسس پوینت از 802.11n و 802.11ac استفاده می کند، کلاینتها نیز باید از استاندارد 802.11ac استفاده کنند. برخی از دستگاهها می توانند استاندارد صحیح 802.11 را شناسایی کرده و خود را با آن تطبیق دهند. با این حال، اگر آنها پیکربندی شده اند تا فقط از یک استاندارد خاص استفاده کنند، ممکن است هیچ گاه موفق نشوند از طریق به کارگیری یک استاندارد متفاوت اکسس پوینت را پیدا کنند.
- قرار دادن نادرست آنتن- در دنیای شبکه ها، عوامل مختلفی می توانند باعث بروز خطاها (داده ای) یا کاهش عملکرد

شوند. مطمئن شوید که محدوده جغرافیایی توصیه شده برای اکسس پوینت را به دقت بررسی کرده‌اید، آنتن‌ها به شکل درستی نصب شده‌اند و کلاینت‌ها در فاصله درستی قرار دارند. اگر یک کلاینت بیش از حد از یک اکسس پوینت دور باشد خطاهای داده‌ای بیشتری را تجربه خواهد کرد. به‌طور مثال، شما می‌توانید از آنتن‌های پرقدرتی به جای آنتن‌های استاندارد روتر خود استفاده کنید تا شعاع بیشتری را روتر پوشش دهد.

• تداخل - اگر خطا در برقراری ارتباطات بی‌سیم متناوب بوده و تشخیص آن‌ها دشوار است، ممکن است علت بروز مشکل تداخل باشد. منابع تولید کننده تداخل الکترومغناطیس همچون چراغ‌های فلورسنت، ماشین‌آلات سنگین، تلفن‌های بی‌سیم و مایکروویو در مسیر انتقال اطلاعات را بررسی کنید.

• اتصالات سیمی و بی‌سیم همزمان - یک ایستگاه کاری برای انتقال از طریق یک اتصال سیمی یا بی‌سیم طراحی شده است، اما نمی‌تواند در یک زمان هر دو تکنیک را پشتیبانی کند. هنگام حل مشکلات مربوط به اتصال، بررسی کنید که کامپیوتر در تلاش برای برقراری ارتباط با کدامیک از این دو اتصال است. شما می‌توانید این مشکل را با غیر فعال کردن آداپتور وای‌فای یا با جدا کردن کابل اترنت حل کنید.

• مشکلات مرتبط با به‌روزرسانی میان‌افراز- به‌روز رسانی کارت شبکه یا میان‌افزار اکسس پوینت می‌تواند آسیب‌پذیری‌ها را وصله کرده و عملکرد را بهبود بخشد. اما در برخی موارد ممکن است باعث بروز مشکلاتی شوند، در نتیجه ابتدا بهتر است قبل از ارتقا به ارزیابی این مسئله بپردازید.

• نوع آنتن اشتباه - برخی فکر می‌کنند آنتن‌های چند جهته تقریباً همیشه بهترین انتخاب در هنگام تنظیم پوشش وای‌فای بوده و سعی می‌کنند اکسس پوینت را در مرکز ناحیه‌ای قرار دهند که همه جا را تحت پوشش قرار دهد با این تصور که سیگنال‌ها در همه جهات ارسال خواهند شد. با این حال، در بسیاری از موارد، نصب آنتن‌های یک جهته به جای چند جهته، امکان دسترسی به سیگنال‌ها را افزایش داده و سیگنال‌ها را به مکان درستی هدایت می‌کنند. به‌طور مثال، فرض کنید یک شرکت آنتن چند جهته را در نزدیکی یک سقف 30 فوتی کارخانه‌ای نصب می‌کند. از آنجایی که سیگنال آنتن در همه جهات پخش می‌شود، توان سیگنال‌ها به شکل کروی پخش شده و در نتیجه بهترین سیگنال فقط در دسترس کارگرانی است که روی سقف راه می‌روند که بدیهی است این حالت قابل قبول نیست! برای حل این مشکل سیگنال باید به طبقه پایین هدایت شود. در نتیجه یک آنتن را می‌توان در بالا و پایین قرار داد تا پوششی گنبدی شکل را ایجاد کنند تا دسترسی به سیگنال‌ها به درستی انجام شود.

برای اطلاع درباره سایر مشکلات مرتبط با شبکه‌های وای‌فای به مقاله [مشکلات شبکه را خودتان حل کنید](#) مراجعه کنید.

در شماره آینده آموزش **نتورک پلاس** به سراغ مبحث مجازی‌سازی و محاسبات ابری خواهیم رفت.

تاریخ انتشار:
02 اردیبهشت 1398

نشانی منبع:

<https://www.shabakeh-mag.com/networking-technology/14983/%D8%A2%D9%85%D9%88%D8%B2-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3%D8%8C-%D8%B9%DB%8C%D8%A8%E2%80%8C%E2%80%8C%D8%A7%D8%A8-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A8%DB%8C%D8%B3%DB%8C%D9%85-%D8%A8%D8%AE%D8%B4-41>