تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بین‌المللی

آموزش رایگان دوره نتورک‌پلاس (Network+) استانداردهای وای‌فای 802.11، روش دسترسی CSMA/CA (بخش 40)

در شماره گذشته آموزش نتورک‌پلاس با ارتباط حوزه نزدیک، مادون قرمز، سامانه بازشناسی با امواج رادیویی، یواس‌بی بی‌سیم ، استانداردهای WLAN 802.11، بلوتوث و ANT+ آشنا شدیم. در این شماره مبحث استانداردهای بیسیم و سایر مباحث مرتبط با شبکه های بیسیم را ادامه خواهیم داد.

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

در شماره گذشته به شکل مختصر اطلاعاتی در ارتباط با استانداردهای وای‌فای 802.11 به دست آوردیم. اکنون قصد داریم کمی بیشتر در مورد این استانداردها اطلاع کسب کنیم.

- 802.11b، انجمن IEEE در سال 1999 استاندارد 802.11b را منتشر کرد که باند 2.4 گیگاهرتز را به کانال‌های 22 مگاهرتزی تقسیم کرد. این استاندارد در مقایسه با سایر فناوری‌های WLAN 802.11 کمترین هزینه را برای مدیران شبکه‌ها به همراه داشت، با این حال، بیشتر مدیران شبکه تصمیم گرفتند استاندارد 802.11b را با یک استاندارد سریع‌تر، همچون استاندارد 802.11n جایگزین کنند.
- 802.11a، با وجود این‌که کارگروه استاندارد 802.11a کار خود را خیلی قبل‌تر از کارگروه 802.11b آغاز کرد، اما استاندارد 802.11a پس از استاندارد 802.11b منتشر شد. توان عملیاتی بالاتر 802.11a نسبت به 802.11b در زمان استفاده از فرکانس‌های بالاتر، روش منحصر به فرد آن برای مدولاسیون داده‌ها و پهنای باند بیشتر در دسترس از مهم‌ترین ویژگی‌های این استاندارد به شمار می‌روند. باند کاری این استاندارد روی فرکانس 5 گیگاهرتز (5 GHz U-NII) بوده و دارای 8 کانال ارسال و دریافت است. شاید مهم‌ترین ویژگی این استاندارد پشتیبانی از باند 5 گیگاهرتز باشد که تراکم کمتری نسبت به باند 2.4 گیگاهرتز دارد. همین مسئله باعث می‌شود تا سیگنال‌های 802.11a کمتر در معرض تداخل قرار گیرند. با این‌حال، سیگنال‌های فرکانس بالاتر برای انتقال به انرژی بیشتری نیاز دارند و در فواصل کوتاه‌تری نسبت به سیگناهای فرکانس پایین‌تر حرکت می‌کنند. در نتیجه، شبکه‌های 802.11a به تراکم بیشتر اکسس‌پوینت‌ها نیاز دارند تا همان فاصله‌ای که شبکه‌های 802.11b پوشش می‌دهند را پشتیبانی کنند. نقاط دسترسی اضافی، جزء ماهیت ذاتی تجهیزات 802.11a هستند که این استاندارد را گران‌تر از802.11b یا 802.11g قرار داده است. همین مسئله باعث می‌شود تا استاندارد 802.11a به ندرت استفاده شود.
- 802.11g، انجمن IEEE استاندارد جدید شبکه‌های محلی بی‌سیم موسوم به 802.11g را به عنوان جایگزین مقرون به صرفه استاندارد 802.11b منتشر کرده، استانداردی که به لحاظ تئوری توان عملیاتی آن افزایش پیدا کرده و از تکنیک‌های مختلف مدولاسیون داده‌ها بهره می‌برد. علاوه بر این، 802.11g از مزیت سازگاری با شبکه‌های 802.11b برخوردار است. این سازگاری مزیت مهمی در زمان خوش بود، زیرا به مدیران شبکه

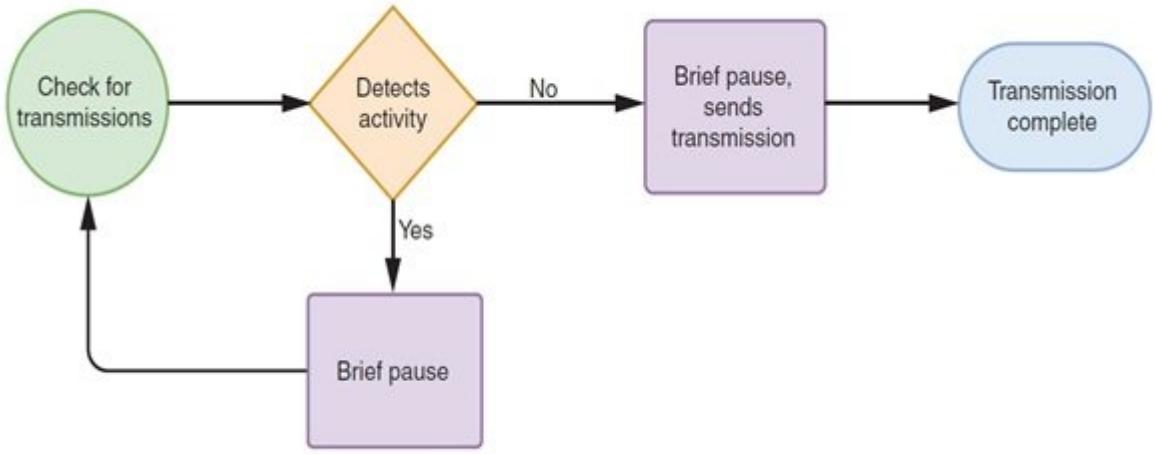
اجازه می‌داد اکسس‌پوینت‌های بی‌سیم خود را ارتقا دهند، در حالی که بازهم به کامپیوترهای قدیمی اجازه دسترسی بی‌سیم را ارائه می‌دادند.

- 802.11n، در سال 2009 میلادی انجمنIEEE استاندارد 802.11n را تصویب کرد. هرچند این استاندارد از سال‌ها قبل در حال توسعه بود، اما تولیدکنندگان تجهیزات شبکه از اواسط سال 2007، عرضه محصولات سازگار با استاندارد 802.11n را آغاز کردند. هدف اولیه استاندارد IEEE's 802.11n ایجاد یک استاندارد بی‌سیمی بود که بهره‌وری به مراتب بالاتر و موثرتری نسبت به استانداردهای قبلی ارائه کند. استانداردی که در عمل موفق شد یک چنین کاری را انجام دهد. 802.11n حداکثر توان عملیاتی 600 مگابیت در ثانیه را دارد که در عمل یک زیرساخت واقعی برای سیگنال‌های ویدیویی و تلفنی را ارائه کرد. IEEE در زمان انتشار این استاندارد تاکید کرد که استاندارد 802.11n با استانداردهای b ،802.11a و g سازگاری دارد. این سازگاری از آن جهت امکان‌پذیر است است که 802.11n از هر دو باند فرکانسی 2.4 گیگاهرتز و 5.0 گیگاهرتز استفاده می‌کند.
- 802.11ac به‌طور رسمی اوایل سال 2014 میلادی تصویب شد. 802.11ac در باند 5 گیگاهرتز عمل می‌کند. استانداردی که با افزایش پهنای باند و دامنه مفید منطبق با معیارهای تعیین شده پیشرفت قابل توجهی نسبت به اسلاف خود داشت. 802.11ac اولین استاندارد وای‌فایی است که به قابلیت‌های گیگابیت اترنت نزدیک‌تر شده است و از کلاینت‌های بی‌سیم بیشتری در یک زمان پشتیبانی به عمل می‌آورد. در حقیقت، عملکرد اکسس‌پوینت‌های 802.11ac به جای آن‌که شبیه به یک هاب باشند بیشتر شبیه به یک سوییچ هستند که در یک زمان می‌توانند انتقال‌های چندگانه در یک طیف فرکانسی یکسان را مدیریت کند. این استاندارد جدید در سه موج به کار گرفته شده است که دستگاه‌های Wave 1 و Wave 2 در زمان نگارش این مطلب در دسترس قرار دارند.
- لازم به توضیح است که استانداردهای 802.11ax و 802.11y نیز در زمان نگارش این مقاله از سوی انجمن IEEE به تصویب رسیده‌اند.

صرفنظر از استانداردهای مختلفی که برای شبکه‌های 802.11 ارائه شده است، هر یک از این استانداردها قابلیت‌ها و نوآوری‌های جالب توجهی را ارائه کرده‌اند. توجه داشته باشید که همه شبکه‌های 802.11 از روش دسترسی یکسانی پیروی می‌کنند، با این حال، برخی از نوآوری‌های به کار رفته در این استانداردها همان‌گونه که در ادامه مشاهده خواهید کرد، راه را برای دستیابی به عملکرد بهتر در استانداردهای بعدی هموار کردند.

روش دسترسی

در شماره‌های گذشته یاد گرفتید که لایه پیوند داده و به ویژه زیرلایه مک مسئولیت اضافه کردن آدرس‌های فیزیکی به یک فریم داده‌ای و اداره کردن دسترسی چند گره به یک رسانه واحد را عهده‌دار هستند. شبیه به Ethernet 802.3، در استاندارد 802.11 آدرس‌های فیزیکی 48 بیتی به یک فریم اضافه می‌شوند تا منبع و مقصد آن‌را شناسایی کنند. به‌کارگیری یک طرح آدرس‌دهی فیزیکی یکسان، به شبکه‌های 802.11 اجازه می دهد با سایر شبکه‌های IEEE 802 از جمله شبکه‌های اترنت (802.3)، ترکیب شوند. با این حال، شبکه‌های 802.11 از یک روش دسترسی متفاوت نسبت به شبکه‌های اترنت استفاده می‌کنند. دستگاه‌های بی‌سیم برای انتقال و دریافت به‌طور همزمان طراحی نشده‌اند و بنابراین نمی‌توانند مانع بروز مشکل تصادم شوند. در اینجا، استانداردهای 802.11، از رویکرد دسترسی چندگانه با قابلیت شنود سیگنال حامل/پیشگیری از تصادم (CSMA / CA) سرنام Carrier Sense Multiple Access/Collision Avoidance برای دسترسی به یک رسانه مشترک همان‌گونه که در شکل زیر نشان داده شده است استفاده می‌کنند.



در مقایسه با رویکرد دسترسی چندگانه با قابلیت شنود سیگنال حامل/تشخیص تصادم (CSMA / CD) سرنام Carrier Sense Multiple Access with Collision Detection رویکرد CSMA/CA احتمال بالقوه بروز تصادم را کاهش می‌دهد، اما نمی‌تواند وقوع یک تصادم را تشخیص دهد و بنابراین نمی‌تواند مانع به وجود آمدن تصادم‌هایی شود که رخ می‌دهند. عملکرد CSMA/CA که در شکل بالا مشاهده می‌کنید به شرح زیر است:

مرحله اول: با استفاده از رویکرد CSMA / CA، یک گره در شبکه 802.11 قبل از فرستادن داده‌ها، وضعیت انتقال بیسیم در دسترس را بررسی می‌کند. (دایره سبز در شکل)

• اگر گره مبدا هیچ فعالیت انتقال در شبکه را شناسایی نکند، مدت زمان اندکی صبر کرده(یک بازه زمانی تصادفی) و سپس اقدام به ارسال داده می‌کند.

• اگر مبدا فعالیتی را تشخیص دهد، قبل از آن‌که به بازبینی دومرتبه کانال بپردازد، مدت زمان کوتاهی را به انتظار می‌نشیند.

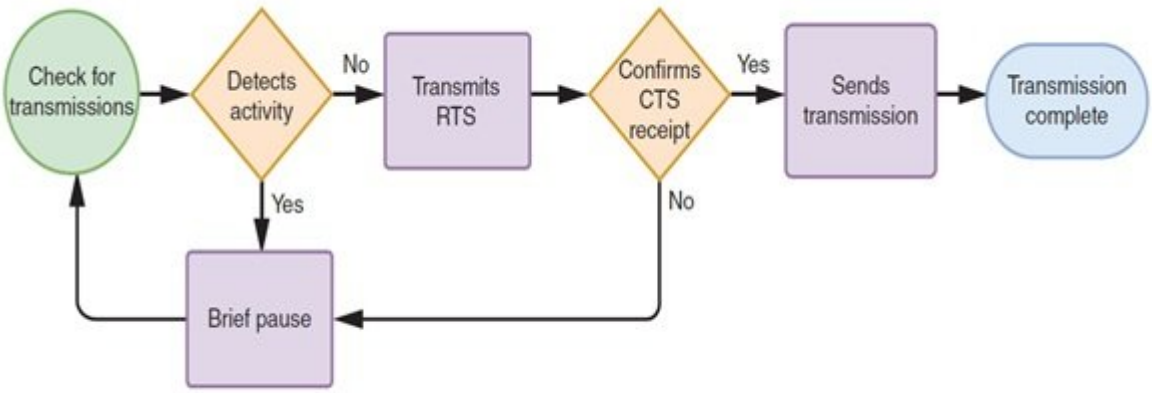
مرحله 2: گره مقصد دریافت انتقال را دریافت کرده و پس از تایید دقت آن یک بسته ACK (تأیید) را برای مبدا ارسال می‌کند.

• اگر مبدا این تایید را تصدیق کرد، فرض می‌کند که انتقال به درستی انجام شده است.

• تداخل یا انتقال‌های دیگر در شبکه می‌توانند فرآیند تبادل را مختل کنند. اگر پس از ارسال یک پیام، گره مبدا قادر به دریافت پیام تصدیق از گره مقصد نباشد، فرض می‌کند که انتقال به درستی انجام نشده و فرایند CSMA / CA را دوباره آغاز می‌کند.

استفاده از بسته‌های ACK برای تأیید هر انتقال به این معنی است که شبکه‌های 802.11 نیاز به سرباره بیشتری نسبت به شبکه‌های 802.3 دارند. یک شبکه بی‌سیم به لحاظ تئوری حداکثر توان عملیاتی 10 مگابیت در ثانیه را ارائه می‌کند که نشان می‌دهد نرخ انتقال داده‌ها در هر ثانیه نسبت به شبکه‌های اترنت سیمی با همان حداکثر توان عملیاتی به لحاظ تئوری کمتر است. گره‌هایی که در یک شبکه بی‌سیم به شدت دور از هم هستند، یک چالش خاص را به وجود می‌آورند که اجازه نمی‌دهند تکنیک هم‌دستی مانع بروز مشکل تصادم شود. این مسئله "مشکل پنهان گره" نام گرفته است، جایی که یک گره در منطقه قابل پوشش در رویت سایر گره‌ها قرار ندارد. یک راه حصول اطمینان از این‌که بسته‌ها توسط سایر مکانیزم‌های انتقال بلوکه نمی‌شوند، ذخیره کردن رسانه برای استفاده از یک گره است. به عبارت ساده‌تر به تمام گره‌ها هشدار داده می‌شود که در محدوده فرستنده، گیرنده یا هر دو، در خلال تبادل اطلاعات، هیچ‌گونه ارسالی انجام ندهند. در 802.11، این راهکار را می‌توان از طریق پروتکل اختیاری RTS / CTS سرنام (Request to Send / Clear to Send) پیاده‌سازی کرد. شکل زیر رویکرد CSMA / CA در هنگام استفاده از پروتکل RTS / CTS را نشان می‌دهد. این تکنیک مشکل پایانه پنهان که عمدتا در شبکه‌های بی‌سیم رخ می‌دهد را

حل کرد.



هنگام استفاده از پروتکل RTS / CTS گره مبدا یک سیگنال RTS را برای اکسس پیونت ارسال می‌کند تا فرصت انحصاری انتقال در اختیارش قرار دهد. اکسس‌پوینت موافقت خود را با یک سیگنال CTS نشان می‌دهد، در این حالت اکسس پوینت به‌طور موقت ارتباط با تمام گره‌ها در محدوده خود را به حالت تعلیق درآورده و صبر می‌کند تا گره مبدا فرآیند انتقال را تکمیل کند. هنگامی که از پروتکل RTS / CTS استفاده می‌شود، بهره‌وری شبکه کاهش پیدا می‌کند. با این حال، هنگام انتقال بسته‌های بزرگ این رویکرد ارزشمند است.

Association

فرض کنید لپ‌تاپ خود را به یک کافی‌نت محلی می‌برید، آن‌را روشن می‌کنید و لپ‌تاپ شما پیغامی نشان می‌دهد که به شبکه بی‌سیم کافه‌نت متصل شده و به اینترنت دسترسی دارید. این فرآیند به ظاهر ساده association نامیده می‌شود که شامل تبادل بسته‌ها میان اکسس پوینت کافی‌نت و کامپیوتر شما است. Association یکی دیگر از عملکردهای زیرلایه مک است که درون استاندارد 802.11 تعریف شده است. مادامی که یک گره بی سیم فعال و پروتکل‌های بی‌سیم آن در حال اجرا است، گره در فواصل زمانی معین محیط پیرامون خود را برای دریافت نشانه‌هایی از اکسس پوینت رصد می‌کند که به این عمل پویش می‌گویند. یک گره می‌تواند یکی از دو حالت پویش انفعالی یا فعال را اجرا کند.

• پویش فعال – کلاینت بی‌سیم ابتکار عمل را به شرح زیر به دست می‌گیرد:

○○ کامپیوتر فریم مخصوصی به نام پروب (probe) را در همه کانال‌های موجود در محدوده فرکانس خود انتقال می‌دهد.

○○ اکسس پوینتی که فریم پروب را شناسایی می‌کند، پاسخی را ارسال می‌کند که این پاسخ حاوی تمام اطلاعاتی است که یک کامپیوتر برای برقراری ارتباط با اکسس پوینت به آن نیاز دارد. کد وضعیت و شناسه گره یا شناسه ایستگاه برای آن کامپیوتر از جمله این موارد است.

○○ در این مرحله کامپیوتر می‌تواند درخواست برقراری ارتباط با اکسس پوینت را قبول کند. آخرین مرحله در برقراری ارتباط با اکسس پوینت حداقل برای اولین بار رضایت کاربر است.

○○ دو گره شروع ارتباط را روی کانال فرکانس مشخص شده توسط (اکسس پوینت) AP آغاز می‌کنند.

• پویش انفعالی – اکسس پوینت به شرح زیر کار خود را آغاز می‌کند:

○○ یک کامپیوتر مجهز به آداپتور بی‌سیم به تمام کانال‌ها در محدوده فرکانس کاری خود به منظور دریافت سیگنال ویژه‌ای که اکسس پوینت ارسال می‌کند گوش می‌دهد. سیگنال ویژه‌ای که beacon frame نام دارد. به عبارت ساده‌تر اکسس پوینت به‌طور متناوب با ارسال فریم Beaconing از ایستگاه‌هایی که در نظر دارند به شبکه متصل

شوند دعوت به عمل می‌آورد و بر همین اساس فریم Beacon را ارسال می‌کند. beacon frame حاوی اطلاعاتی است که یک گره بی‌سیم برای برقراری ارتباط با اکسس پوینت به آن نیاز دارد. از جمله این اطلاعات می‌توان به سرعت انتقال شبکه و SSID (شناسه سرویس) و رشته‌ای منحصر به فرد برای شناسایی اکسس پوینت اشاره کرد.

○○ کامپیوتر با تاییده کاربر می‌تواند ارتباط با اکسس پوینت را آغاز کند.

○○ دو گره در یک کانال فرکانسی به اجماع می‌رسند و ارتباط برقرار می‌کنند

هنگام پیکربندی یک شبکه بی‌سیم محلی، بیشتر مدیران شبکه یک SSID منحصر به فرد را برای اکسس‌پوینت استفاده می‌کنند و تمایلی ندارند از SSID پیش‌فرض ارائه شده از سوی سازنده دستگاه استفاده کنند. SSID پیش‌فرض اغلب شامل نام سازنده و در برخی مدل‌ها شماره مدل اکسس پوینت است که ممکن است هکرها را اغوا کند از آسیب‌پذیری‌های احتمالی یک مدل خاص برای حمله به شبکه استفاده کنند. تغییر SSID امنیت بهتر و مدیریت ساده‌تر شبکه را به همراه خواهد داشت. پیشنهاد می‌کنم به توصیه‌های زیر دقت کنید تا شبکه ایمنی را پیاده‌سازی کنید.

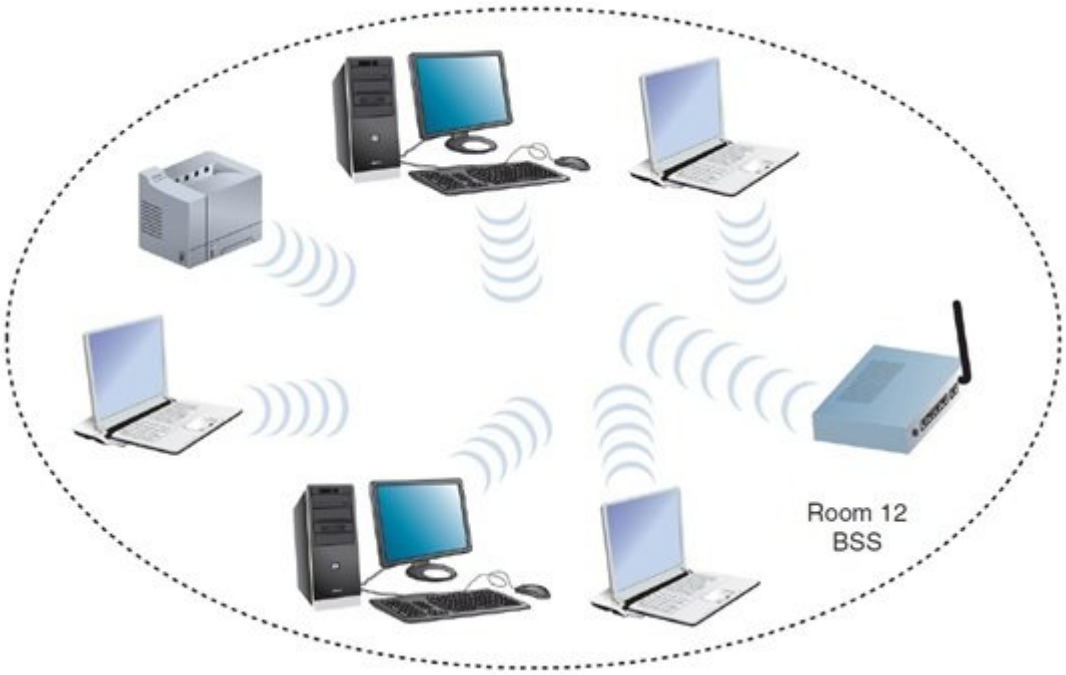
• ماهیت شبکه را در زمان تعیین SSID پنهان کنید تا اطلاعات کمی در اختیار هکرها قرار دهید. به‌طور مثال، ایده خوبی نیست که SSID اکسس‌پوینت بخش حسابداری را "Acctg" نام‌گذاری کنید.

• سعی کنید اشتباهات کارمندان برای استفاده از SSID را با تعیین یک SSID که به خاطرآوری آن ساده باشد، اما نرمال و عادی نباشد کاهش دهید. این‌کار امنیت دستگاه‌های کلاینت را افزایش می‌دهد.

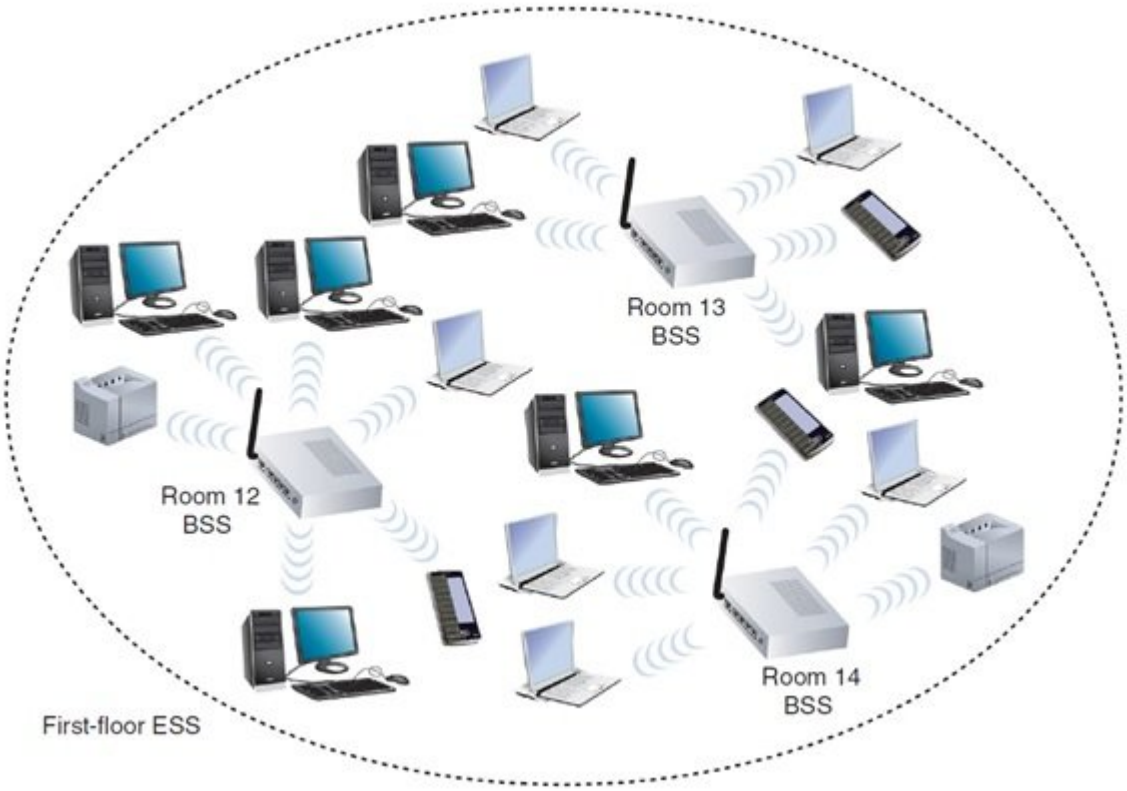
بد نیست به ترمینولوژی ارائه شده از سوی IEEE در ارتباط با SSIDها نگاهی داشته باشید. از مهم‌ترین ترمینولوژی‌های ارائه شده از سوی IEEE برای پیکربندی SSID به موارد زیر می‌توان اشاره کرد:

• مجموعه سرویس‌های پایه (BSS) سرنام basic service set- گروهی از گره‌هایی که به یک اکسس پوینت متصل می‌شوند. شناسه این گروه از گره‌ها با عنوان BSSID سرنام basic service set identifier شناخته می‌شود. توجه داشته باشید که این موضوع تنها هب تجهیزاتی که اکسس پوینت متصل شده‌اند و نه محدوده‌ای که اکسس‌پوینت پوشش می‌دهد اشاره دارد.

• مجموعه خدمات گسترش یافته (ESS) سرنام ***(extended service set*** —) – به گروهی از اکسس‌پوینت‌ها که به شبکه محلی یکسانی متصل شده‌اند، اطلاق می‌شود. مجموعه سرویس‌های پایه (BSS) که متعلق به مجموعه سرویس‌های گسترده یافته یکسان هستند یک شناسه ویژه را به اشتراک قرار می‌دهند که ESSID سرنام **extended service set identifier** نامیده می‌شود. در یک ESS، یک کلاینت می‌تواند با هر یک از اکسس‌پوینت‌های که از ESSID یکسانی دارند ارتباط برقرار کند. در عمل، بسیاری از متخصصان شبکه بین واژگان SSID و ESSID... تفاوتی قائل نمی‌شوند. آن‌ها به سادگی هر اکسس‌پوینت درون یک گروه یا شبکه محلی را با SSID یکسانی پیکربندی می‌کنند که کار درستی نیست. شکل زیر شبکه‌ای تنها با یک BSS را نشان می‌دهد.



شکل زیر شبکه‌ای را نشان می‌دهد که متشکل از چندین BSS بوده که یک ESS را تشکیل می‌دهند.



IEEE 802.11 Frames

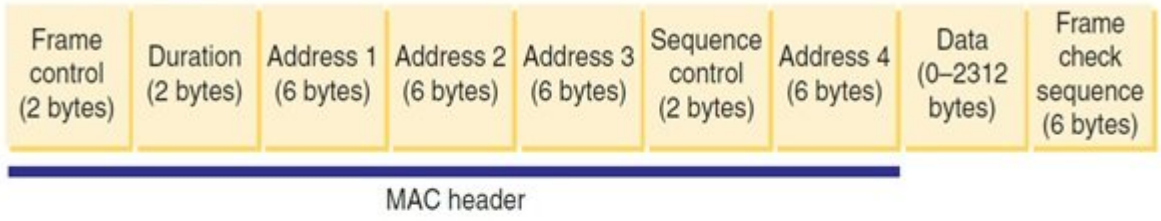
شما درباره انواع مختلف سربارهای مورد نیاز برای مدیریت دسترسی به شبکه‌های بی‌سیم 802.11، همچون ACK ها، پروب‌ها و beaconها مطالبی را فراگرفتید. برای هر یک از این مباحث، استاندارد 802.11 یک نوع فریم خاص در زیر لایه MAC مشخص کرده است. این فریم‌های چندگانه به سه گروه تقسیم می‌شوند:

• فریم‌های مدیریتی - در ارتباط و همکاری مجدد نقش دارند. پروب و beacon frame از جمله فریم‌های مدیریتی هستند.

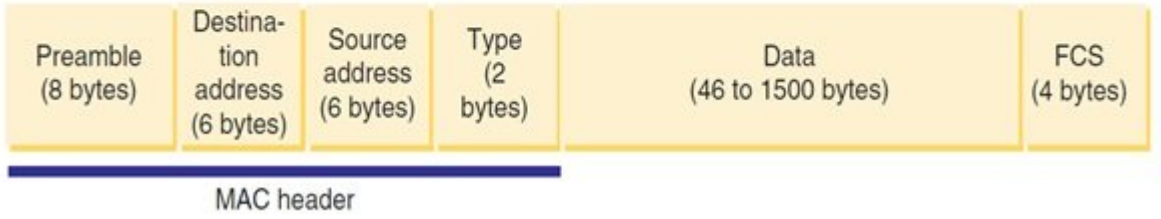
• فریم‌های کنترلی – در نحوه دسترسی به مدیا و تحویل داده‌ها نقش دارند از جمله این فریم‌ها می‌توان به ACK و RTS / CTS اشاره کرد.

• فریم داده‌ای – مسئولیت انتقال داده‌ها میان گره‌ها بر عهده این فریم‌ها است. یک فریم داده‌ای 802.11 در شکل زیر نشان داده شده است.

802.11 data frame:



802.3 (Ethernet) frame:



همان‌گونه که در شکل بالا مشاهده می‌کنید، فریم داده‌ای حجم قابل توجهی از سربار را حمل می‌کند.

نکته: با توجه به اینکه مبحث فریم‌های شبکه بیسیم 802.11 از جمله مباحث مهم دنیای شبکه است و ممکن است در آزمون **نتورک‌پلاس** سوالاتی در ارتباط با آن مطرح شود، پیشنهاد می‌کنم برای مطالعه هرچه دقیق‌تر این مبحث به مطلب **Understanding the 802.11 Wireless LAN MAC frame format** مراجعه کنید.

در شماره آینده آموزش **نتورک‌پلاس** مبحث استانداردهای بی‌سیم را ادامه خواهیم داد.

تاریخ انتشار:
31 فروردین 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/14965/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%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-network-%D8%A7%D8%B3%D8%AA%D8%A7%D9%86%D8%AF%D8%A7%D8%B1%D8%AF%D9%87%D8%A7%DB%8C-%D9%88%D8%A7%DB%8C%E2%80%8C%D9%81%D8%A7%DB%8C-80211%D8%8C-%D8%B1%D9%88%D8%B4