



دولت جمهوری اسلامی افغانستان
ادارهٔ تعلیمات تخنیکي و مسلکي
معاونیت امور اکادمیک
ریاست نصاب و تربیه معلم

شبکه‌های بی سیم

رشته: کمپیوتر ساینس - دیپارتمنت: شبکه
صنف ۱۴ - سمستر اول

سال: ۱۳۹۹ هجری شمسی



شناسنامه کتاب

نام کتاب: شبکه‌های بی‌سیم

رشته: کامپیوتر ساینس

تدوین کننده: پوهنوال قربان علی فروغ

همکار تدوین کننده: داود فروتن

- کمیته نظارت: ندیمه سحر رئیس اداره تعلیمات تخنیک و مسلکی
- عبدالحمید اکبر معاون امور اکادمیک اداره تعلیمات تخنیک و مسلکی
- حبیب الله فلاح رئیس نصاب و تربیه معلم
- عبدالمتین شریفی آمر انکشاف نصاب تعلیمی، ریاست نصاب و تربیه معلم
- روح الله هوتک آمر طبع و نشر کتب درسی، ریاست نصاب و تربیه معلم
- احمد بشیر هیله‌من مسؤل انکشاف نصاب، پروژه انکشاف مهارت‌های افغانستان
- محمد زمان پویا کارشناس انکشاف نصاب، پروژه انکشاف مهارت‌های افغانستان
- علی خیبر یعقوبی سرپرست مدیریت عمومی تألیف کتب درسی، ریاست نصاب و تربیه معلم

- کمیته تصحیح: دوکتور فضل احمد امینی
- سحر احمدی
- محمد امان هوشمند مدیر عمومی بورد تصحیح کتب درسی و آثار علمی

دیزاین: صمد صبا و سید کاظم کاظمی

سال چاپ: ۱۳۹۹ هجری شمسی

تیراژ: ۱۰۰۰

چاپ: اول

وبسایت: www.tveta.gov.af

ایمیل: info@tveta.gov.af

حق چاپ برای اداره تعلیمات تخنیک و مسلکی محفوظ است.



سرود ملی

دا وطن افغانستان دی	دا عزت د هر افغان دی
کور د سولې کور د تورې	هر بچی یې قهرمان دی
دا وطن د ټولو کور دی	د بلوڅو، د ازبکو
د پښتون او هزاره وو	د ترکمنو، د تاجکو
ورسره عرب، ګوجر دي	پامیریان، نورستانیان
براهوي دي، قزلباش دي	هم ایماق، هم پشه یان
دا هیواد به تل ځلیري	لکه لمر پر شنه آسمان
په سینه کې د آسیا به	لکه زړه وی جاویدان
نوم د حق مودی رهبر	وایو الله اکبر وایو الله اکبر



پیام اداره تعلیمات تخنیکي و مسلکی

استادان نهایت گرامی و محصلان ارجمند!

تربیت نیروی بشری ماهر، متخصص و کارآمد از عوامل کلیدی و انکارناپذیر در توسعه اقتصادی و اجتماعی هر کشور محسوب می‌گردد و هر نوع سرمایه‌گذاری بزرگ در بخش‌های مختلف اقتصادی نیازمند به پلان‌گذاری و سرمایه‌گذاری در بخش نیروی بشری و توسعه منابع این نیرو می‌باشد. بر مبنای این اصل و بر اساس فرمان شماره ۱۱ مقام عالی ریاست جمهوری اسلامی افغانستان به تاریخ ۱۳۹۷/۲/۱ اداره تعلیمات تخنیکي و مسلکی از بدنه وزارت معارف مجزا و فصل جدیدی در بخش عرضه خدمات آموزشی در کشور گشوده شد. اداره تعلیمات تخنیکي و مسلکی به‌عنوان متولی و مجری آموزش‌های تخنیکي و مسلکی در کشور محسوب می‌شود که در چارچوب استراتژی ۵ ساله خویش دارای چهار اولویت مهم که عبارت‌اند از افزایش دسترسی عادلانه و مساویانه فراگیران آموزش‌های تخنیکي و مسلکی در سطح کشور، بهبود کیفیت در ارائه خدمات آموزشی، یادگیری مادام‌العمر و پیوسته و ارائه آموزش نظری و عملی مهارت‌ها به‌طور شفاف، کم‌هزینه و مؤثر که بتواند نیاز بازار کار و محصلان را در سطح محلی، ملی و بین‌المللی برآورده کند، می‌باشد. این اداره که فراگیرترین نظام تعلیمی کشور در بخش تعلیمات تخنیکي و مسلکی است، تلاش می‌کند تا در حیطه وظایف و صلاحیت خود زمینه دستیابی به هدف‌های تعیین‌شده را ممکن سازد و جهت رفع نیاز بازار کار، فعالیت‌های خویش را توسعه دهد.

نظام اجتماعی و طرز زندگی در افغانستان مطابق به احکام دین مقدس اسلام و رعایت تمامی قوانین مشروع و معقول انسانی عیار است. اداره تعلیمات تخنیکي و مسلکی جمهوری اسلامی افغانستان نیز با ایجاد زمینه‌های لازم برای تعلیم و تربیت جوانان و نوجوانان مستعد و علاقه‌مند به حرفه‌آموزی، ارتقای مهارت‌های شغلی در سطوح مختلف مهارتی، تربیت کادرهای مسلکی و حرفه‌ای و ظرفیت‌سازی تخصصی از طریق انگشاف و ایجاد مکاتب و انستیتوت‌های تخنیکي و مسلکی در سطح کشور با رویکرد ارزش‌های اسلامی و اخلاقی فعالیت می‌نماید.

فلذا جهت نیل به اهداف عالی این اداره که همانا تربیه افراد ماهر و توسعه نیروی بشری در کشور می‌باشد؛ داشتن نصاب تعلیمی بر وفق نیاز بازار کار امر حتمی و ضروری بوده و کتاب درسی یکی از ارکان مهم فرایند آموزش‌های تخنیکي و مسلکی محسوب می‌شود، پس باید همگام با تحولات و پیشرفت‌های علمی نوین و مطابق نیازمندی‌های جامعه و بازار کار تألیف و تدوین گردد و دارای چنان ظرافتی باشد که بتواند آموزه‌های دینی و اخلاقی را توأم با دست‌آورد‌های علوم جدید با روش‌های نوین به محصلان انتقال دهد. کتابی را که اکنون در اختیاردارید، بر اساس همین ویژگی‌ها تهیه و تدوین گردیده است.

بدین‌وسیله، صمیمانه آرزو مندیم که آموزگاران خوب، متعهد و دلسوز کشور با خلوص نیت، رسالت اسلامی و ملی خویش را ادا نموده و نوجوانان و جوانان کشور را به‌سوی قله‌های رفیع دانش و مهارت‌های مسلکی رهنمایی نمایند و از محصلان گرامی نیز می‌خواهیم که از این کتاب به‌درستی استفاده نموده، در حفظ و نگهداشت آن سعی بلیغ به خرج دهند. همچنان از مؤلفان، استادان، محصلان و اولیای محترم محصلان تقاضا می‌شود نظریات و پیشنهادات خود را در مورد این کتاب از نظر محتوا، ویرایش، چاپ، اشتباهات املائی، انشایی و تاپی عنوانی اداره تعلیمات تخنیکي و مسلکی کتباً ارسال نموده، امتنان بخشند.

در پایان لازم می‌دانیم در جنب امتنان از مؤلفان، تدوین‌کنندگان، مترجمان، مصححان و تدقیق‌کنندگان نصاب تعلیمات تخنیکي و مسلکی از تمامی نهادهای ملی و بین‌المللی که در تهیه، تدوین، طبع و توزیع کتب درسی زحمت‌کشیده و همکاری نموده‌اند، قدردانی و تشکر نمایم.

ندیمه سحر

رئیس اداره تعلیمات تخنیکي و مسلکی جمهوری اسلامی افغانستان

ط.....	مقدمه.....
۱.....	فصل اول: اساسات شبکه‌های بی‌سیم.....
۲.....	۱.۱ تاریخچه شبکه بی‌سیم.....
۳.....	۱.۲ معرفی شبکه‌های بی‌سیم.....
۴.....	۱.۳ نقش سازمان‌ها در شبکه‌های بی‌سیم.....
۵.....	۱.۳.۱ الف: سازمان‌های قانون‌ساز.....
۵.....	۱.۳.۲ ب: سازمان‌های استندردساز.....
۵.....	۱.۳.۳ ج: سازمان‌های هماهنگ‌کننده.....
۶.....	۱.۴ فایده‌های استفاده از شبکه‌های بی‌سیم.....
۶.....	۱.۵ مشکلات شبکه بی‌سیم.....
۷.....	۱.۵.۱ مشکلات مربوط به استفاده از امواج رادیویی.....
۸.....	۱.۶ سرعت واقعی شبکه‌های بی‌سیم.....
۱۰.....	۱.۷ روش کار شبکه بی‌سیم.....
۱۱.....	۱.۸ انواع شبکه‌های بی‌سیم.....
۱۱.....	۱.۸.۱ WPAN.....
۱۲.....	۱.۸.۲ WLAN.....
۱۲.....	۱.۸.۳ WWAN.....
۱۳.....	۱.۸.۴ WMAN.....
۱۴.....	۱.۸.۵ WGAN.....
۱۷.....	۱.۹ مقایسه شبکه‌های بی‌سیم با شبکه سیمی.....
۱۷.....	۱.۹.۱ نصب و پیاده‌سازی.....
۱۸.....	۱.۹.۱.۱ شبکه Ad hoc.....
۲۱.....	۱.۹.۲ مشکلات زیرساخت در شبکه سیمی نظر به شبکه بی‌سیم.....
۲۵.....	فصل دوم: تکنالوژی‌های بی‌سیم.....
۲۶.....	۲.۱ معرفی تکنالوژی Wi-Fi.....
۲۷.....	۲.۱.۱ تیوری فریکانس‌های رادیویی.....
۲۷.....	۲.۱.۱.۱ تعریف امواج الکترومقناطیسی.....
۳۱.....	۲.۱.۱.۲ موج.....

۳۱	طول موج	۲.۱.۱.۳
۳۳	فریکونسی	۲.۱.۱.۴
۳۳	دامنه موج	۲.۱.۱.۵
۳۵	ویژگی های مهم امواج رادیویی	۲.۱.۱.۶
۴۱	فرکانس آزاد و مجوز دار	۲.۲
۴۱	معرفی تکنالوژی بلوتوت	۲.۳
۴۲	معرفی تکنالوژی ZigBee	۲.۴
۴۳	معرفی تکنالوژی WiMax	۲.۵
۴۴	ویژگی های مهم تکنالوژی WiMax	۲.۵.۱
۴۵	قابلیت های فنی WiMax	۲.۵.۲
۴۵	مزایای WiMax	۲.۵.۳
۴۵	معرفی تکنالوژی ۳G	۲.۶
۴۷	معرفی تکنالوژی ۴G	۲.۷
۴۸	فرق ۴G با LTE	۲.۷.۱
۴۸	سرعت ۴G	۲.۷.۲
۴۸	مزیت های ۴G	۲.۷.۳
۴۸	انواع باند و طیف های ۴G	۲.۷.۴
۴۹	تکنالوژی Li-Fi	۲.۸
۵۳	فصل سوم: معرفی استندردهای شبکه بی سیم	
۵۴	معرفی استندردهای WLAN	۳.۱
۵۵	انواع استندرد IEEE ۸۰۲.۱۱	۳.۱.۱
۵۵	استندرد ۸۰۲.۱۱a	۳.۱.۱.۱
۵۵	استندرد ۸۰۲.۱۱b	۳.۱.۱.۲
۵۵	استندرد ۸۰۲.۱۱g	۳.۱.۲
۵۶	استندرد ۸۰۲.۱۱n	۳.۱.۲.۱
۵۶	استندرد ۸۰۲.۱۱ ac	۳.۱.۲.۲
۶۱	فصل چهارم: نحوه تنظیم اکسس پاینت و روترهای بی سیم	
۶۲	معرفی اکسس پاینت	۴.۱
۶۲	تنظیمات اکسس پاینت	۴.۲
۶۷	معرفی گزینه ها	۴.۳
۶۷	گزینه Status	۴.۳.۱

۶۸	تنظیمات WAN	۴.۴
۶۹	تنظیمات LAN	۴.۴.۱
۷۰	تنظیمات گزینه Wireless	۴.۴.۲
۷۰	نام شبکه بی سیم (Wireless Network Name)	۴.۴.۲.۱
۷۱	موقعیت فعالیت دستگاه (Region)	۴.۴.۲.۲
۷۲	انتخاب نوع استانداردها (Mode)	۴.۴.۲.۳
۷۲	عرض کانال (Channel Wide)	۴.۴.۲.۴
۷۲	کانال (Channel)	۴.۴.۲.۵
۷۳	حد اکثر ظرفیت ارسال (Max Tx Rate)	۴.۴.۲.۶
۷۴	فعالیت بی سیم و یا سیمی (Enable Wireless Router Radio)	۴.۴.۲.۷
۷۴	فعالیت پخش نام شبکه (Enable SSID Broadcast)	۴.۴.۲.۸
۷۴	فعال کردن خدمات Bridge (Enable WDS Bridging)	۴.۴.۲.۹
۷۶	تنظیمات پیشرفته بی سیم (Wireless Advanced)	۴.۴.۲.۱۰
۷۷	احصائیه دستگاه های متصل (Wireless Statistics)	۴.۴.۲.۱۱
۷۸	تنظیمات DHCP سرور (DHCP Settings)	۴.۴.۲.۱۲
۸۰	تنظیم ریزریو کردن IP (Address Reservation)	۴.۴.۲.۱۳
۸۰	تنظیمات مسیریابی ثابت (Static Routing)	۴.۴.۲.۱۴
۸۱	مشاهده جدول مسیریابی (System Routing Table)	۴.۴.۲.۱۵
۸۲	تنظیمات ناحیه دینامیکی (DDNS)	۴.۴.۲.۱۶
۸۳	تنظیمات زمان (Time Settings)	۴.۴.۲.۱۷
۸۹	فصل پنجم: معرفی و تنظیمات امنیتی شبکه های بی سیم	
۹۰	امنیت در شبکه های بیسیم	۵.۱
۹۱	پروتوکول امنیتی WEP:	۵.۱.۱
۹۱	پروتوکول امنیتی WPA/WPA۲:	۵.۱.۲
۹۵	تنظیمات امنیتی اکسس پاینت و روترهای بی سیم	۵.۲
۹۵	تنظیمات امنیتی شبکه بی سیم (Wireless Security)	۵.۲.۱
۹۶	تنظیمات فیلتر شدن آدرس MAC (MAC Filtering)	۵.۲.۲
۹۷	ارتقای لخت افزار (Firmware Upgrade)	۵.۲.۳
۹۸	تنظیمات پیش فرض (Factory Default)	۵.۲.۴
۱۰۰	تنظیمات backup و Restore	۵.۲.۵
۱۰۰	تنظیمات یوزرنیم و پاسورد سیستم	۵.۲.۶
۱۰۲	تنظیمات کنترل پهنای باند بر اساس محدوده آدرس IP	۵.۲.۷

۵.۲.۸	محدود کردن کامپیوترهای مشخص (Binding Settings)	۱۰۲
۵.۲.۹	تنظیمات کنترل دسترسی ها (Access Control Management)	۱۰۴
۵.۲.۱۰	تنظیمات زمان بندی استفاده اینترنت (Schedule Settings)	۱۰۴
فصل ششم: روش های حل مشکل در شبکه های بی سیم		
۶.۱	حل مشکل در شبکه های WLAN	۱۰۸
۶.۱.۱	اجرای دستورات تست و دریافت اطمینان از شبکه	۱۰۹
۶.۲	هشت راه حل مشکل برای وصل شدن به Wi-Fi در ویندوز	۱۱۵
۶.۲.۱	اجرای ابزار حل کننده مشکل (Network Troubleshooter)	۱۱۵
۶.۲.۲	Restart کردن اکسس پاینت	۱۱۶
۶.۲.۳	قطع ارتباط Wi-Fi و وصل کردن مجدد آن	۱۱۶
۶.۲.۴	اسکن کردن کامپیوتر برای ویروس	۱۱۷
۶.۲.۵	غیر فعال کردن آنتی ویروس	۱۱۷
۶.۲.۶	ریست کردن Reset TCP/IP Protocol & WINSOCK Catalog	۱۱۷
۶.۲.۷	حذف و نصب مجدد کارت شبکه	۱۱۸
۶.۲.۸	چک کردن سرویس های لازم برای شبکه اینترنت	۱۲۰
منابع و مأخذ		۱۲۴

شبکه های بی سیم با استفاده از امکانات و تجهیزات کمپیوتری سریعاً در حالت رشد و توسعه است. این شبکه ها نسبت به شبکه های سیمی دارای تجهیزات ساده بوده که نصب و اعیارسازی آن آسان و قابل حمل می باشد، به دلیل اینکه در شبکه های بی سیم انعطاف پذیری زیادی وجود دارد نسبت به شبکه های سیمی، به همین دلیل است که استفاده از آن روز به روز در حال افزایش است.

از ویژه گی های شبکه های بی سیم میتوان به قابلیت های چون در دسترس بودن آن بدون در نظر داشت یا محدودیت زمان و مکان، قابل حمل بودن آن، نصب و طراحی ساده و همچنان هزینه کمتر آن چونکه نیاز به کیبل کشی و وسیله نگهداری کیبل نمی باشد اشاره نمود.

هدف از شبکه های بی سیم در این کتاب اتصال دو یا چند کمپیوتر و ایجاد یک شبکه محلی بی سیم می باشد، که این شبکه برای ارسال و دریافت از امواج رادیویی استفاده می کند و خدمات لازم را انتقال می دهد.

محتویات این کتاب در قالب فصل های جداگانه ترتیب شده است، که در فصل اول اساسات شبکه بی سیم و انواع آن، فصل دوم تکنالوژی های بی سیم، فصل سوم استندرد های بی سیم، فصل چهارم نحوه اعیار سازی AP، فصل پنجم تنظیمات امنیتی در شبکه های بی سیم و در فصل ششم روی مشکلات معمول که در شبکه های بی سیم بوجود می آید و روش های حل این مشکلات بحث صورت گرفته است.

امید است این کتاب کمکی در جهت بالا بردن سطح آگاهی جامعه به خصوص محصلان در رابطه به شبکه های بی سیم باشد.



هدف کلی کتاب

آشنایی با اساسات شبکه های بی سیم، انواع شبکه های بی سیم، تکنالوژی های شبکه های بی سیم، استاندارد های شبکه بی سیم، نصب و اعیارسازی AP، مکانیزم های امنیتی شبکه های بی سیم، و خطایابی در شبکه های بی سیم.

فصل اول

اساسات شبکه‌های بی‌سیم



هدف کلی: با اساسات شبکه‌های بی‌سیم به‌صورت عموم آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. شبکه بی‌سیم را تعریف کنند.
۲. شبکه‌های بی‌سیم را تشریح کنند.
۳. فواید و اهمیت شبکه بی‌سیم را توضیح دهند.
۴. نواقص شبکه‌های بی‌سیم را توضیح دهند.
۵. انواع شبکه‌های WLAN، WMAN، WWAN و WGAN را تعریف و معرفی کرده بتوانند.
۶. تفاوت بین انواع شبکه‌های WLAN، WMAN، WWAN و WGAN را بیان کرده بتوانند.
۷. شبکه Ad Hoc را تنظیم و عیارسازی کرده بتوانند.

در این فصل در مورد نقش سازمان‌های استاندارد ساز، تاریخچه شبکه بی‌سیم، معرفی شبکه‌های بی‌سیم، اصطلاحات و مفاهیم شبکه بی‌سیم، فواید و نواقص این شبکه، انواع شبکه‌های بی‌سیم از لحاظ پوشش و در خاتمه تمرین فصل به صورت همه‌جانبه پرداخته شده است.

شبکه بی‌سیم با استفاده از امکانات و تجهیزات کمپیوتری، سریعاً در حال رشد و توسعه است. این شبکه دارای تجهیزات ساده بوده و نصب آن آسان و قابل انتقال است. در شبکه‌های کمپیوتری بی‌سیم، نیازی به کیبل کشی‌های طولیل در اتاق‌ها و هم‌چنان ضرورت به هزینه کردن برای خرید سخت‌افزارها و دستگاه‌های اضافی، نگهداری کیبل، جست‌وجوی کیبل شبکه و ... نیست.

اگر در یک اداره از شبکه بی‌سیم استفاده شود، در هر جا به صورت آنلاین با سایر کمپیوترها و دستگاه‌های دیگر ارتباط خواهیم داشت. با استفاده از شبکه‌های بی‌سیم می‌توان عملیات زیادی انجام داد که در شبکه‌های سیمی امکان انجام آن‌ها وجود ندارد؛ یعنی، تکنالوژی‌های شبکه سیمی، انعطاف پذیری و قابلیت‌های شبکه بی‌سیم را ندارد و سهولت‌های استفاده در آن محدود است. به همین دلیل است که استفاده کنندگان شبکه بی‌سیم روزبه‌روز در حال افزایش است. اگر شخصی از طریق شبکه‌های بی‌سیم وصل باشد، از نظر مکان محدودیتی برای او وجود ندارد و می‌تواند در کتاب‌خانه‌ها، هتل‌ها، میدان‌های هوایی، مراکز همایش و حتی کافی‌شاپ‌ها و سایر مکان‌های عمومی بدون هیچ محدودیتی و با سرعت خیلی بالا به شبکه بی‌سیم وصل شود و قابلیت استفاده از اینترنت را نیز داشته باشد. مهم‌ترین ویژگی شبکه‌های بی‌سیم، راحتی و سادگی آن و مهم‌تر از همه، قابلیت در دسترس بودن آن در تمام روزهای هفته است. شبکه بی‌سیم از لحاظ ساحت پوشش به انواع مختلف تقسیم می‌شود که عبارت اند از: WMAN، WLAN، WPAN و WGAN می‌باشد.

۱.۱ تاریخچه شبکه بی‌سیم

نورمن آبرامسون^۱، استاد دانشگاه هاوایی، اولین توسعه دهنده ارتباط شبکه بی‌سیم کمپیوتر در دنیا بود. او با استفاده از یک رادیوی ارزان قیمت، هفت کمپیوتر را در چهار جزیره مختلف به یک کمپیوتر مرکزی در جزیره اوهایو بدون استفاده از خط تیلیفون متصل کرد.

در سال ۱۹۹۷م. اشخاصی به اسم F.R Gfeller و Bapst در یک مقاله در ژورنال علمی IEEE، تئوری‌های را در مورد شبکه‌های بی‌سیم با استفاده از مادون قرمز^۲ (IR) ارائه کردند. مدت کوتاهی پس از آن، در سال ۱۹۸۰م. شخصی به اسم P.Ferrert در کنفرانس بین‌المللی مخابرات، کاربردهای تجربی و گزارش تئوری خود را برای گسترش طیف‌های رادیویی جهت ارتباطات بی‌سیم مطرح کرد.

^۱ Norman Abramson

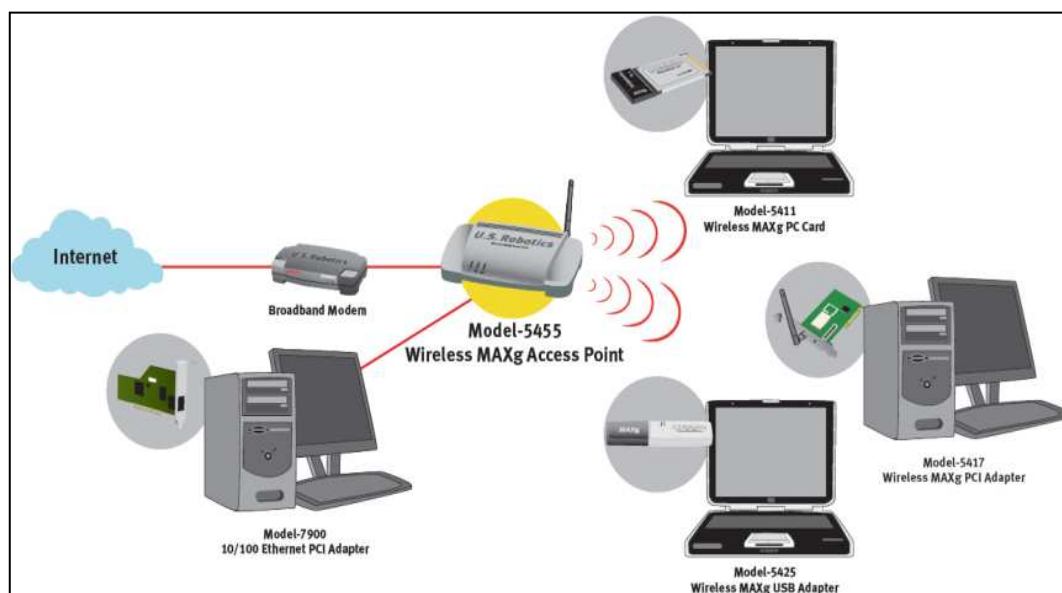
^۲ Infra-Red

در سال ۱۹۸۴ یک مقایسه بین مودم قرمز و CDMA جهت گسترش طیف شبکه‌های بی‌سیم در یک سمپوزیم شبکه‌های کامپیوتری توسط کاوه پهلوان مطرح شد که بعدها در مجله ارتباطات جامع IEEE منتشر شد. [2]

۱.۲ معرفی شبکه‌های بی‌سیم

هدف از شبکه بی‌سیم در این کتاب، اتصال دو یا چند کامپیوتر و ایجاد یک شبکه محلی بی‌سیم^۳ از طریق امواج رادیویی است. این شبکه جهت ارسال و دریافت اطلاعات، از امواج رادیویی استفاده می‌کند و سرویس‌های لازم را انتقال می‌دهد؛ لذا، واضح است که کامپیوترها در شبکه بی‌سیم توسط امواج رادیویی اطلاعات را انتقال داده و باعث اتصال پرینترها، انتقال فایل‌ها و دسترسی به منابع شبکه و اینترنت می‌شوند. تمام منابع شبکه توسط هر کامپیوتر موجود در شبکه به اشتراک گذاشته می‌شود و بدون قطع ارتباط، به هر اجزایی در شبکه بی‌سیم، شبکه محلی ایجاد می‌گردد.

برای ایجاد شبکه بی‌سیم به اجزاء اصلی مانند کارت شبکه بی‌سیم و دستگاه اکسس پاینت^۴ ضرورت است؛ درحالی‌که برای ایجاد شبکه سیمی حداقل یک دستگاه هاب^۵ و به مقدار کافی کیبل شبکه و کونکتورها ضرورت است. در شکل ۱-۱ شبکه محلی بی‌سیم نشان داده شده است.



شکل ۱-۱: نمونه از شبکه بی‌سیم [۳]

در شکل بالا دیده می‌شود که تعدادی از کامپیوترها توسط کارت شبکه بی‌سیم به اکسس پاینت وصل شده که به نام Transceiver نیز یاد می‌گردد. این کارت‌های شبکه به شکل بی‌سیم ارتباط کامپیوترها را به

^۳ Wireless LAN

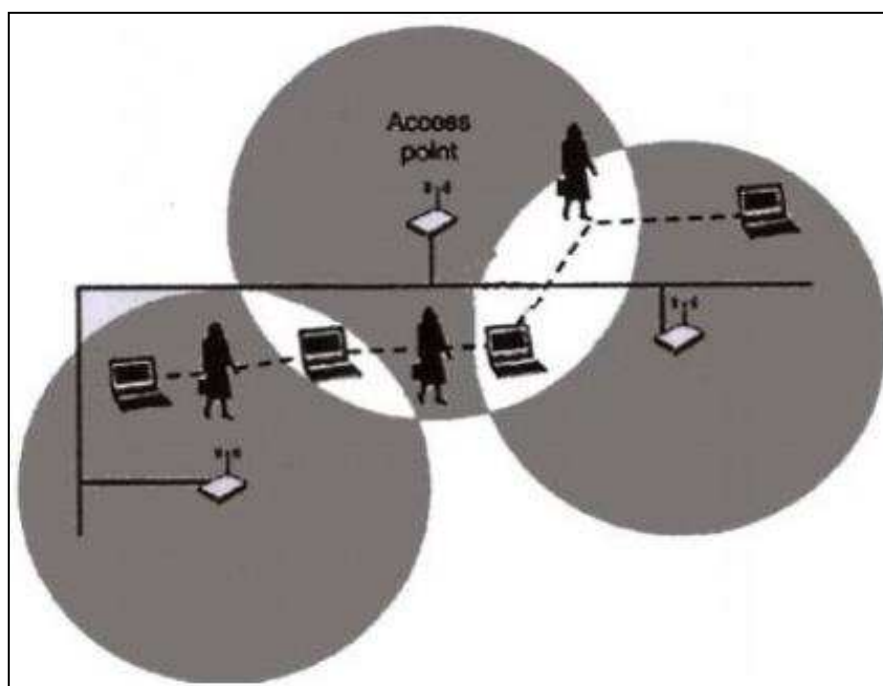
^۴ Access Point

^۵ Hub

شبکه برقرار می‌کند؛ به عبارت دیگر، این کارت‌ها قابلیت ایجاد امواج رادیویی را دارد؛ به همین دلیل، انتقال و دریافت اطلاعات به شکل امواج رادیویی صورت می‌گیرد.

کمپیوترها با استفاده از کارت شبکه بی‌سیم، می‌توانند با هر یک از دستگاه‌های شبکه بی‌سیم ارتباط برقرار کنند و توانایی ارسال و دریافت اطلاعات را در همه جا و حتی به شکل سیار^۶ دارند. در صورتی که چندین شبکه بی‌سیم به صورت پیوسته به یکدیگر وصل باشند، استفاده کننده قادر خواهد بود که بدون قطع شدن از شبکه، در هر جایی به صورت سیار از شبکه و منابع شبکه استفاده کند.

شکل ۱-۲ نشان می‌دهد که استفاده کننده به صورت سیار از چندین شبکه استفاده می‌کند. در این حالت وابستگی شبکه‌ها با استفاده از فضای پوشش^۷ تعیین و در نظر گرفته می‌شود.



شکل ۱-۲: خدمات شبکه بی‌سیم به صورت سیار^[۳]

مطابق شکل ۱-۲، استفاده کنندگان بدون هیچ محدودیتی در حال حرکت و تکاپو با شبکه ارتباط برقرار کرده و محدودیت تکنالوژی شبکه سیمی را ندارند.

۱.۳ نقش سازمان‌ها در شبکه‌های بی‌سیم

به صورت عموم سه کتگوری از سازمان‌ها برای راهنمایی و استندرد سازی شبکه‌های بی‌سیم وجود دارد. این سازمان‌ها باید به صورت هماهنگ و مشترک بین هم کار کنند؛ به عبارت دیگر، یک استندرد و یا یک

^۶Mobile

^۷RangeArea

تکنالوژی با هماهنگی و کار مشترک هر سه نوع سازمان به پیش برده می شود و زمینه ساخت یک تکنالوژی موفق را فراهم می کند. این سه کتگوری از سازمان ها عبارت اند از:

۱.۳.۱ الف: سازمان های قانون ساز

سازمان های که در بخش ایجاد اصول و قوانین برای شبکه های بی سیم فعالیت دارند؛ عبارت اند از: FCC و FCC.ETSI برگرفته شده از Federal Communications Commission و ETSI برگرفته شده از European Telecommunication Standards Institute است. این دو سازمان به عنوان سازمان های قانون ساز در عرصه صنعت و تکنالوژی های شبکه بی سیم مطرح هستند. سازمان FCC مجموعه قوانین را تهیه می کند و در ادامه، سازمان IEEE استانداردها را تعریف و توسعه می دهد. قابل یادآوری است که سازمان FCC در کشورهای آمریکایی و سازمان ETSI در کشورهای اروپایی فعالیت دارد؛ به عبارت دیگر، مجموعه قوانینی که در آمریکا و یا در اروپا ساخته می شود، از طریق این سازمان ها نظارت شده و به پیش برده می شود، به همین دلیل این کتگوری را به نام قانون سازی^۸ یاد می کنند. [۱]

۱.۳.۲ ب: سازمان های استاندارد ساز

سازمان های استاندارد ساز در جهت توسعه و ارائه استانداردها فعالیت دارند. یکی از سازمان های استاندارد ساز، سازمان IEEE است که برگرفته شده از Institute of Electrical and Electronics Engineers است؛ بنابراین، این کتگوری را به نام استاندارد سازی^۹ یاد می کنند. [۱]

۱.۳.۳ ج: سازمان های هماهنگ کننده

سازمان های هستند که جهت هماهنگی بین سازمان های قانون ساز و استاندارد ساز در عرصه تکنالوژی فعالیت می کنند. فعالیت این اتحادیه در راستای تست و ارزیابی هماهنگی بین استانداردها و ارائه سرتیفیکت لازم برای آن استاندارد است. به عنوان مثال اتحادیه Wi-Fi^{۱۰} یکی از این سازمان ها است که مسئولیت تست و ارزیابی تکنالوژی Wi-Fi را دارد. هر استاندارد بعد از تست مؤفقا نه و ارائه سرتیفیکت قادر به فعالیت است. اتحادیه Wi-Fi مسئولیت تست و ارزیابی تجهیزات را به عهده دارد. هدف از ارزیابی، استاندارد بودن از لحاظ تعامل با تکنالوژی های دیگر و مستدل بودن از لحاظ ساخت، کیفیت، کارایی و غیره است.

⁸ Regulation

⁹ Standardization

¹⁰ Wi-Fi Alliance

سه سازمان فوق‌الذکر ارائه خدمات برای شبکه‌های WLAN، معرفی و ایجاد قوانین، استانداردها و سازگاری تکنالوژی‌ها را به عهده دارند؛ بنابراین، این کتگوری را به نام سازگاری و هماهنگی^{۱۱} بین سازمان‌ها یاد می‌کنند.

۱.۴ فایده‌های استفاده از شبکه‌های بی‌سیم

شبکه‌های بی‌سیم دارای فواید زیادی است که در شبکه‌های سیمی وجود ندارد. مهم‌ترین و بارزترین فایده شبکه بی‌سیم، قابل حمل بودن^{۱۲} آن است. در حالت خاص اگر کامپیوتر لب‌تاپ را به شبکه بی‌سیم تنظیم کنیم؛ می‌توانیم هنگام حرکت در محیط کار یا دفتر، خانه و دیگر جای‌ها از شبکه و منابع شبکه استفاده کنیم. امروزه از شبکه بی‌سیم در تمام جای‌ها از قبیل ملی‌بس‌های شهری، هواپیماها، قطارها، کتاب‌خانه‌ها، شفاخانه‌ها، میدان‌های هوایی و دیگر جای‌ها به‌صورت قابل حمل و سیار استفاده شده و امکان دسترسی به منابع و ذخیره کردن اطلاعات در اینترنت وجود دارد.

۱.۵ مشکلات شبکه بی‌سیم

اگر شبکه‌های بی‌سیم بدون مشکل بودند، حتماً تا به حال جانشین شبکه‌های سیمی شده و آن‌ها را از دور رقابت خارج می‌کردند. بعضی مشکلات در شبکه بی‌سیم وجود دارد که هر روز در حال برطرف شدن است. امروزه دیده می‌شود که استفاده از شبکه‌های بی‌سیم هر روز در حال افزایش است و موارد استفاده آن بیش‌تر و جالب‌تر می‌گردد. شبکه بی‌سیم مانند هر تکنالوژی دیگر در برابر مزایا و فوایدی که دارد، بعضی مشکلات نیز دارد.

۱. مهم‌ترین مشکل استفاده از سیستم‌های بی‌سیم، سرعت انتقال اطلاعات در شبکه است. قسمی که می‌دانیم در شبکه‌های سیمی، سرعت ارسال اطلاعات ۱۰۰ Mbps است. از طرف دیگر بعضی تکنالوژی‌ها در شبکه‌های سیمی دارای سرعت ۱۰۰۰ Mbps نیز است که در بازار وجود دارد؛ اما به علت قیمت زیاد این نوع تجهیزات، از آن‌ها فقط در موارد خاصی استفاده می‌شود. برعکس، در بسیاری از شبکه‌های بی‌سیم استانداردهای رایج دارای سرعت ۱۰۸ Mbps است. از طرف دیگر اندازه این سرعت تابع شرایط مختلفی، چون امواج رادیویی مزاحم، تداخل امواج و وجود نقاط کور در شبکه محیط است. قدرت فرستنده‌های بی‌سیم، تعداد کاربران شبکه و عدم استفاده از پروتوکول‌های امنیتی از مشکلات دیگر در شبکه بی‌سیم است.

۲. مسأله دیگر، موضوع تأمین امنیت در شبکه‌های بی‌سیم است. این شبکه‌ها خیلی آسان‌تر نسبت به شبکه‌های سیمی می‌توانند مورد دست‌برد قرار گیرند. استانداردهای جدید، روش‌های کدگذاری جدیدی

Compatibility¹¹

Portability¹²

معرفی می کنند تا امنیت این شبکه ها را بالا ببرند؛ اما روش های کدگذاری سرعت انتقال اطلاعات را کاهش می دهد.

۳. در شبکه های بی سیم برای انتقال اطلاعات از امواج رادیویی استفاده می شود؛ بنابراین، شبکه بی سیم تمام مشکلات مربوط به امواج رادیویی و استفاده از آن را نیز دارد.

۱.۵.۱ مشکلات مربوط به استفاده از امواج رادیویی

۱. **وجود نویز در محیط:** تعریف کلی از نویز^{۱۳} در شبکه های کمپیوتری عبارت است از علاوه شدن دیتاهای فرعی بر دیتاهای اصلی؛ اما نویز در شبکه های بی سیم عبارت از هر موج رادیویی اضافی است که با امواج رادیویی اصلی (موردنظر) یکجا می شود. اضافه شدن امواج رادیویی اضافی، پیدا کردن موج اصلی (موردنظر) را دشوار و حتی ناممکن می سازد.

۲. **تداخل امواج رادیویی (Interferences):** یکی از مشکلات امواج رادیویی، تداخل امواج رادیویی^{۱۴} است. از آن جا که برخی از تجهیزات الکترونیکی از امواج رادیویی استفاده می کنند، تداخل این امواج می تواند عمل کرد این تجهیزات را مختل کند. تداخل یا همان Interferences عبارت از یک جا شدن فریکانس های رادیویی است که مزاحمت های ارتباطی را برای هم دیگر به وجود می آورد. این تداخل در اثر نزدیک شدن فریکانس های یک سان رادیویی به وجود می آید؛ به عنوان مثال، فریکانس تیلیفون های بی سیم و اجاق های مایکرو ویو با فریکانس مورد استفاده بعضی از تجهیزات شبکه های بی سیم یک سان است و این تیلیفون ها و اجاق ها می توانند تداخل امواج رادیویی ایجاد کنند. در نتیجه تداخل امواج رادیویی، سرعت انتقال اطلاعات کاهش می یابد. شکل زیر تداخل امواج رادیویی را در حالت ارتباط هم زمان^{۱۵} دستگاه ها نشان می دهد.



شکل ۱-۳: تداخل امواج در حالت ارتباط هم زمان بین دستگاه ها

۳. **تضعیف امواج رادیویی (Attenuation):** یکی از چالش های دیگر امواج رادیویی، تضعیف^{۱۶} امواج رادیویی است. امواج رادیویی در اثر عبور از موانع مختلف کم کم ضعیف گردیده و در نهایت قابل استفاده

¹³ Noise

¹⁴ Interferences

¹⁵ Simultaneous

¹⁶ Attenuation

نیست. میزان تضعیف امواج رادیویی ارتباط مستقیم به مقدار موانع و آلودگی هوای ناشی از گرد و خاک دارد. تضعیف امواج رادیویی، در هنگام انتقال در فضا رخ می‌دهد. تضعیف امواج رادیویی با خراب شدن شرایط جوی بیش‌تر می‌شود.

۴. **انعکاس امواج رادیویی (Reflection):** مسأله دیگر در انتشار امواج رادیویی، انعکاس این امواج در برخورد با اشیاء است. وقتی موج رادیویی به يك شیء شفاف و هموار که قابلیت جذب و نفوذ کردن را نداشته باشد، برخورد کند؛ امواج رادیویی برگشت کرده و تضعیف می‌شود. اگر موج چندین بار به اشیای زیادی برخورد کند، انرژی خود را از دست می‌دهد و به شدت تضعیف می‌شود؛ لذا، در چنین شرایطی قابل استفاده نیست.

۱.۶ سرعت واقعی شبکه‌های بی‌سیم

در این قسمت به صورت بسیار مختصر، به سرعت شبکه‌های بی‌سیم اشاره می‌کنیم. سرعت شبکه‌های بی‌سیم وابسته به نوع تکنالوژی به کار رفته در آن‌ها است. در باره انواع تکنالوژی‌های شبکه‌های بی‌سیم در ادامه بحث خواهیم کرد.

هر تکنالوژی شبکه بی‌سیم دارای یک سرعت نهایی^{۱۷} است که در آن سرعت، می‌تواند حد اکثر اطلاعات را انتقال دهند. سرعت انتقال اطلاعات به پهنای باند^{۱۸} یا توان عملیاتی^{۱۹} بستگی دارد؛ به عنوان مثال، استانداردهای Ethernet که تکنالوژی سیمی است، می‌تواند اطلاعات را روی کیبل^{۲۰} با سرعت ۱۰۰Mbps انتقال دهد؛ اما استاندارد IEEE ۸۰۲.۱۱a و IEEE ۸۰۲.۱۱g نوعی از استانداردهای شبکه بی‌سیم است که دارای سرعت ۱۱Mbps می‌باشد؛ یعنی، دارای سرعت نسبتاً خوبی است.

در ادامه با بعضی از اصطلاحات شبکه‌های بی‌سیم آشنا خواهیم شد. این اصطلاحات در خواندن این کتاب و هم‌چنان، جهت شبکه‌سازی و بخش‌های عملی ما را کمک می‌کند. ما باید با تخنیک‌ها، دانش و نحوه کار هریک از اجزای شبکه بی‌سیم و سخت‌افزارهای مورد نیاز و محیط پیاده سازی آن آشنا شویم؛ علاوه برآن، با تعدادی از تعاریف تخنیکی، نکات مهم هنگام خرید، تجهیزات شبکه بی‌سیم و سخت‌افزارهای استفاده شده در یک شبکه، آشنایی داشته باشیم.

در این قسمت اصطلاحاتی وجود دارد که در سرتاسر این کتاب از آن‌ها استفاده شده است. نگران این نباشیم که چگونه تمام اصطلاحات را به ذهن خود بسپاریم و یا آن‌ها را حفظ کنیم؛ چون تمام این اصطلاحات

^{۱۷}Maximum Speed

^{۱۸}Bandwidth

^{۱۹}Throughput

^{۲۰}Cable

به تکرار در این کتاب استفاده شده و خود به خود در ذهن ما حفظ می گردد. علاوه بر آن تا حد امکان، این اصطلاحات به صورت واضح در این بخش معرفی می گردد.

شبکه محلی (LAN): همان شبکه محلی Local Area Network است که در اساسات شبکه نیز خوانده شده است. شبکه محلی عبارت از شبکه کمپیوتری است که در یک موقعیت محدود قرار دارد و یک محیط کوچک جغرافیایی را احتوا می کند. معمولاً این نوع شبکه، محیط یا فضای یک خانه یا اداره را در بر می گیرد.

مُبدل شبکه: عبارت از دستگاهی است که جهت ارتباط یک کمپیوتر به شبکه استفاده می شود. این دستگاه به نام کارت شبکه یا کارت واسط شبکه (NIC^{۲۱}) نیز یاد می شود. مبدل شبکه به نام ادپترهای شبکه^{۲۲} نیز یاد می شود.

نقطه دسترسی (Access Point): نقطه دسترسی (AP) عبارت از دستگاهی است که تمام کمپیوترها از طریق آن به تمام بخش های شبکه وصل می گردند؛ به عبارت دیگر، این دستگاه به تمام کارت های شبکه بی سیم (NIC) امکان می دهد تا بتوانند با یک شبکه سیمی و بخش های دیگر شبکه ارتباط برقرار کنند. هر اکسس پاینت (AP) از طریق پورت Ethernet خود اجازه می دهد که اجزای شبکه بی سیم به شبکه سیمی نیز وصل گردد. اکسس پاینت یا AP به سادگی ارتباط شبکه بی سیم را به شبکه های سیمی برقرار می کند.

مسیریاب (Router): مسیریاب یک دستگاه سخت افزاری یا یک برنامه نرم افزاری است که به یک شبکه کمپیوتری اجازه می دهد تا به شبکه های دیگر وصل شود. با استفاده از یک مسیریاب^{۲۳} می توانید شبکه محلی LAN را به شبکه های بزرگ تر مثل اینترنت وصل کنید. معمولاً بعضی از Access Point ها دارای ویژگی مسیریابی نیز می باشند. این ویژگی ها را در هنگام خرید Access Point باید در نظر بگیریم. با استفاده از این نوع Access Point ها می توانیم از آن ها به عنوان مسیریاب نیز استفاده کنیم. از مسیریاب ها برای اتصال دو شبکه و یا ارتباط به شبکه های اینترنتی استفاده می شود.

راه بیرونی شبکه (Gateway): راه بیرونی شبکه یا Gateway را می توانیم به شکل سخت افزار یا نرم افزار داشته باشیم. این دستگاه به تمام اجزای داخلی یک شبکه اجازه می دهد تا به منابع بیرونی خود، یعنی شبکه های دیگر، سرورهای دیگر، اینترنت و غیره ارتباط برقرار کند. کمپیوترهای که بین هم شبکه سازی شده اند؛ توسط این دستگاه، راه بیرونی را به دست می آورند؛ به عبارت دیگر، توسط این دستگاه به سادگی

²¹Network Interface Card

²²Network Adaptor

²³Router

راه بیرونی شبکه محاسبه می‌گردد. نکته مهم این‌که، در یک شبکه محلی، Gateway به‌عنوان یک مسیر یاب عمل می‌کند و زمینه اشتراک تمام اجزای شبکه را به بیرون از شبکه فراهم می‌کند.

پروتوکول (Protocol): پروتوکول مجموعه قوانینی است که جهت هماهنگی، ایجاد ارتباطات، نگه‌داری ارتباطات، تنظیم و تعیین سرعت و غیره موارد مهم دیگر در شبکه استفاده می‌شود؛ به عبارت دیگر، پروتوکول عبارت از زبانی است که برای هماهنگی و هم‌زمانی بین واحدهای مختلف در سخت‌افزار و نرم‌افزار استفاده می‌شود؛ به عنوان مثال، جهت ارسال و دریافت اطلاعات در یک شبکه کامپیوتری به پروتوکول‌های ارسال نیاز است.

به عنوان مثال، پروتوکول TCP/IP یکی از پروتوکول‌های است که به هدف انتقال اطلاعات از یک شبکه به شبکه دیگر و یا از یک کامپیوتر به کامپیوتر دیگر استفاده می‌شود. این پروتوکول برگرفته شده از Transmission Control Protocol/Internet protocol است. توسط این پروتوکول با هماهنگی فرستنده و گیرنده، اطلاعات ارسال و دریافت می‌گردد. علاوه بر آن، از پروتوکول TCP/IP بر روی اینترنت، به خاطر دسترسی به شبکه‌های محلی به منظور استفاده از پرینترها، فایل‌های به اشتراک گذاشته شده و غیره استفاده می‌شود.

استندرد Ethernet: از این استندرد برای شبکه‌های سیمی و جهت شبکه سازی سیمی استفاده می‌گردد. این استندرد به صورت تکنالوژی سیم‌کشی بیان می‌شود. تعدادی از تجهیزات از قبیل مودم، برای اتصال به Access Point، از کیبل استفاده می‌کنند. یکی از حالت‌های استفاده از استندرد Ethernet، استفاده از کونکتور RJ45 است که برای اتصال کامپیوترها به دستگاه‌های شبکه استفاده می‌شود. نوع پورت‌ها و سرعت آن مطابق به استندردهای Ethernet عمل می‌کند. به صورت نمونه، استندرد Ethernet در شکل ۱-۴ نشان داده شده است.



شکل ۱-۴: نمونه از استندردهای Ethernet[۳]

۱.۷ روش کار شبکه بی‌سیم

کامپیوترها از طریق کارت شبکه بی‌سیم توسط امواج رادیویی معلومات را انتقال می‌دهند؛ اما امواج این تجهیزات، شبیه امواج رادیویی، حامل موج FM نیستند؛ بلکه، تجهیزات شبکه بی‌سیم، تنها سیگنال‌های را می‌فرستد که فقط می‌توانند تا ۳۰۰ متر، در صورت نبودن مانع، قابل استفاده باشند. این نوع عملیات معمولاً

فقط در محیط ۳۰۰ متری قابل اجرا است. شبکه‌های بی‌سیم مشابه به استانداردهای شبکه‌های سیمی، بسته‌های کوچک به نام بسته‌های Data یا Data Packet را انتقال می‌دهند.

هر کارت شبکه دارای یک پورت سریال منحصر به فرد است که به نام MAC²⁴ آدرس یاد می‌شود. آدرس MAC جهت ارسال اطلاعات مورد استفاده قرار می‌گیرد؛ به عبارت دیگر، جهت آدرس‌دهی دستگاه فرستنده و گیرنده به کار می‌روند. این آدرس در کارت شبکه بی‌سیم وجود دارد؛ لذا، بسته‌های Data که در آن، آدرس فرستنده و گیرنده وجود دارد، به همراه Data اصلی به کمک این آدرس فرستاده می‌شوند.

ارتباطات Wi-Fi از باند رادیویی 2.4 گیگاهرتز استفاده می‌کند. آن‌ها باند خود را با سایر وسایل الکترونیکی خانگی مانند تلفن‌های بی‌سیم و ماکرو ویوها به اشتراک می‌گذارند. شبکه بی‌سیم (Wi-Fi 5) یا 802.11a از باند پایین‌تر از 5GHz استفاده می‌کند.

۱.۸ انواع شبکه‌های بی‌سیم

۱.۸.۱ WPAN

نام این شبکه مخفف Wireless Personal Area Network است. این شبکه محیط کوچکی را پوشش می‌دهد و از استاندارد IEEE ۸۰۲.۱۵ با حمایت و پشتیبانی Bluetooth و Infra-Red استفاده می‌کند. این استاندارد به قطعات (Devices) اجازه برقراری ارتباط با یکدیگر را در محدوده کوچک فراهم می‌کند. بهترین نمونه برای این نوع شبکه، استفاده از تکنالوژی Bluetooth است. استفاده از IR محدود بوده و برای ارتباط مستقیم دستگاه‌ها در فاصله کوتاه‌تر استفاده می‌شود. این شبکه رابط بین PDA، کمپیوترهای شخصی، گوشی تلفن، MP۳ و غیره دستگاه‌های است که شبکه‌های شخصی و کوچک را تشکیل می‌دهد.

شکل ۱-۵ به صورت نمونه، شبکه WPAN را نشان می‌دهد. [۴]



شکل ۱-۵: نمونه شبکه WPAN [۱]

²⁴Media Access Control

۱.۸.۲ WLAN

اسم این شبکه برگرفته شده از Wireless Local Area Network است. این شبکه‌های بی‌سیم، امکان برقراری ارتباط و زمینه به‌اشتراک گذاری اطلاعات را بین تجهیزات مختلف در فاصله محدود (دفتر و یک تعمیر) فراهم می‌کند. این نوع شبکه بی‌سیم، بیش‌ترین استفاده را دارد که در دفاتر دولتی و بخش‌های خصوصی جهت ارتباطات کامپیوترها، دستگاه‌های بی‌سیم و غیره استفاده می‌شود. شبکه WLAN محدوده کوچکی را پوشش می‌دهد و از تکنالوژی Wi-Fi استفاده می‌کند. این نوع شبکه‌های بی‌سیم برای کاربران محلی در محیط‌های اداری، دانشگاهی، لابراتوارها، کتابخانه‌ها و غیره که ضرورت به استفاده از اینترنت دارند، مورد استفاده دارد. در این حالت اگر تعداد کاربران محدود باشد؛ می‌توان بدون استفاده از Access Point این ارتباط را برقرار کرد؛ در غیر این صورت، استفاده از Access Point ضروری است. هم‌چنان می‌توانیم با استفاده از آنتن‌های تقویت‌کننده، فاصله ارتباطی کاربران را با استفاده از استاندارد IEEE 802.11 طولانی‌تر بسازیم. [۴] شکل زیر شبکه WLAN را نشان می‌دهد.

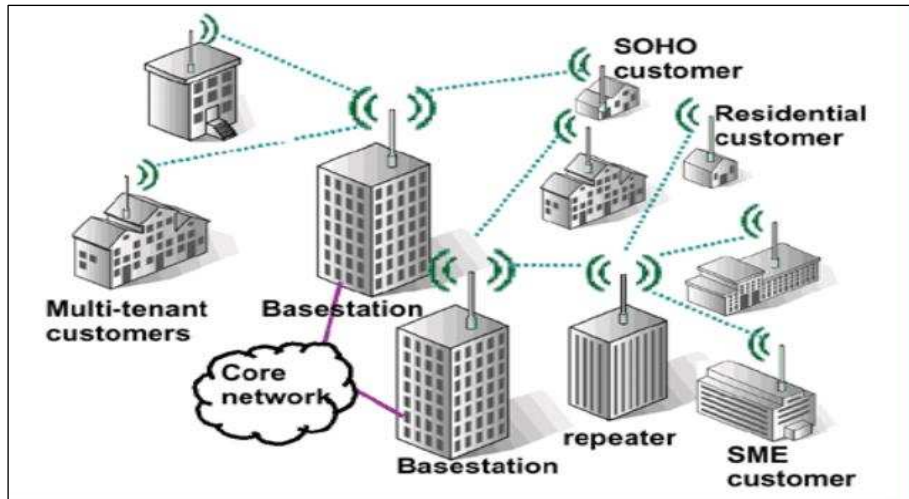
شکل ۱-۶ به صورت نمونه شبکه WLAN را نشان می‌دهد. [۴]



شکل ۱-۶: نمونه شبکه WLAN

۱.۸.۳ WWAN

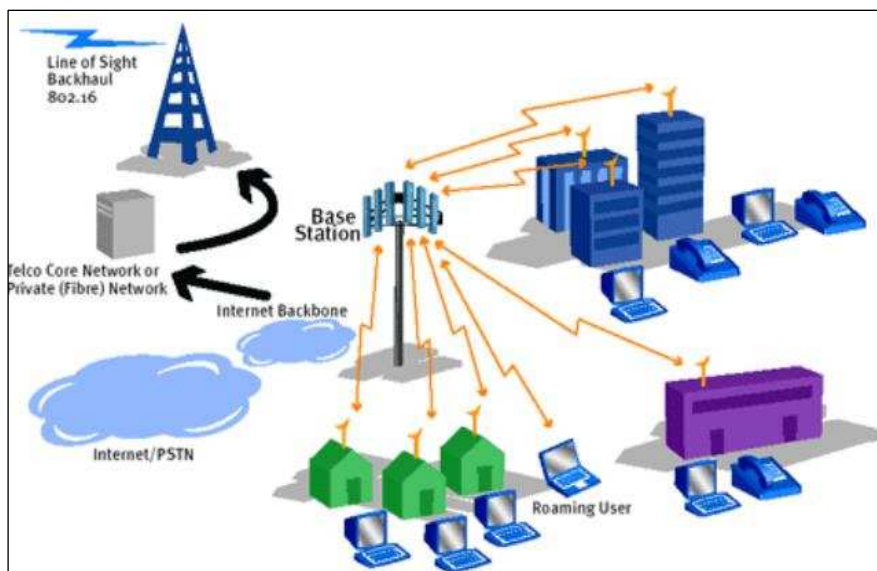
نام این نوع شبکه مخفف Wireless Wide Area Network است. این شبکه برای فاصله‌های طولانی مانند؛ شهرها و کشورها به کار می‌رود. این ارتباط از طریق آنتن‌های بی‌سیم یا ماهواره برقرار می‌گردد. شبکه‌های تلفنی بی‌سیم، نمونه‌های از شبکه‌های WWAN است که در سطح شهر و کشور فعالیت دارد. [۴] تکنالوژی‌های که در شبکه WWAN استفاده می‌شود، عبارت از 4G، 3G، UMTS، GPRS، GSM، WiMAX و غیره است. هر تکنالوژی فایده‌ها و نواقص خود را دارد که مقایسه آن در این جا و برای این کورس گنجایش ندارد. به صورت نمونه شکل ۱-۷ نمونه شبکه WWAN را نشان می‌دهد.



شکل ۱-۷: نمونه شبکه WWAN

۱.۸.۴ WMAN

نام این نوع شبکه برگرفته از Wireless Metropolitan Area Network است. با استفاده از شبکه WMAN بین چندین شبکه یا ساختمان در یک شهر ارتباط برقرار می‌شود. برای ارتباط پشتیبانی^{۲۵} آن از خطوط اجاره، فایبر نوری یا کیبل‌های مسی استفاده می‌گردد. برای استفاده از این شبکه، استاندارد IEEE 802.16 مطرح شده است. در ضمن، از تکنالوژی WiMAX برای اتصال مناطق وسیع (شهر) در این شبکه‌ها استفاده می‌شود. تکنالوژی‌هایی که در شبکه WWAN استفاده می‌شود، در شبکه WMAN نیز قابلیت استفاده دارد. شکل ۱-۸ به صورت نمونه، شبکه WMAN را نشان داده است. [۴]



شکل ۱-۸: نمونه شبکه WMAN

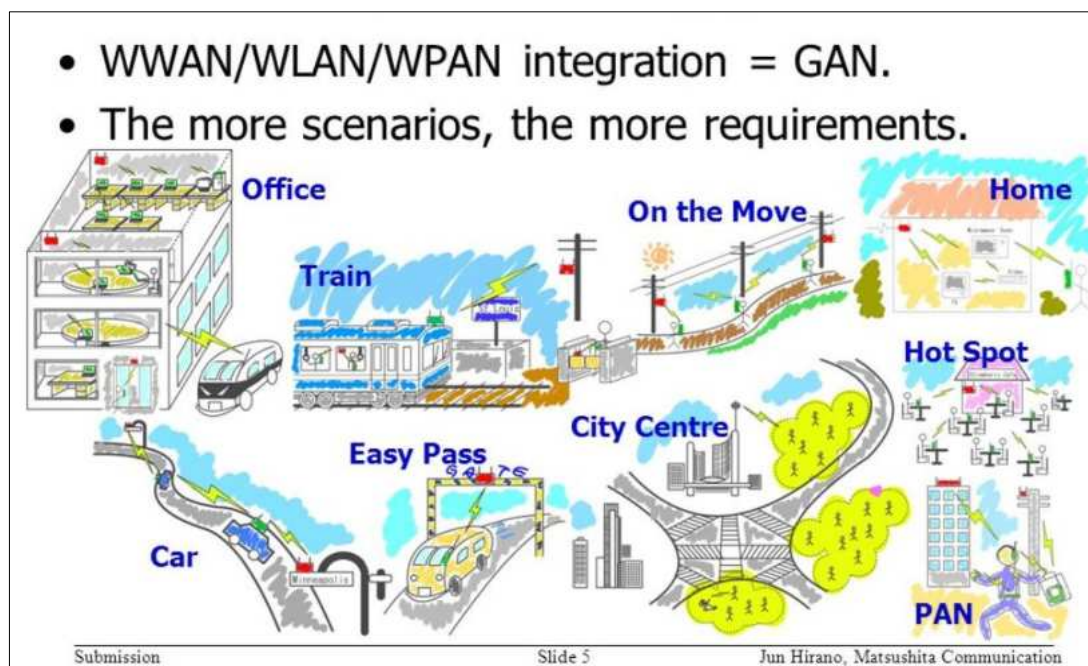
²⁵ Backup

۱.۸.۵ WGAN

نام این نوع شبکه از Wireless Global Area Network گرفته شده است. این شبکه، مرحله نهایی شبکه بزرگ جهانی (WGAN) می‌تواند باشد. این شبکه، مانند شبکه Cell Phone یا همان شبکه مخابراتی بی سیم که با وسعت جهانی فعالیت دارد، عمل کند. طرح پیش‌نهادی برای این شبکه IEEE 802.20 است. شبکه WGAN برای کاربران در کشورهای مختلف در اوقات مسافرت خدمات لازم را ارائه می‌کند؛ به عبارت دیگر، حالتی است که کاربران در همه وقت به شبکه متصل هستند. این نوع شبکه از لحاظ سرعت مانند شبکه‌های کیبلی^{۲۶}، دارای پهنای باند کافی برای استفاده از اینترنت می‌باشد؛ به عبارت دیگر، این شبکه به‌خاطر استفاده از سیستم‌های سیار در همه جا و در همه وقت، از سیستم‌های موبایل استفاده می‌کند. [۳]

این شبکه جهت خدمات شهری به‌صورت سیار، نظارت از ترافیک شهری، موقعیت‌یابی در همه وقت، ارتباطات دائمی از طریق وسایط ترانسپورتی و سیستم‌های هوشمند شهری استفاده مؤثر دارد.

شکل ۱-۹ به‌صورت نمونه، شبکه WGAN را نشان می‌دهد.

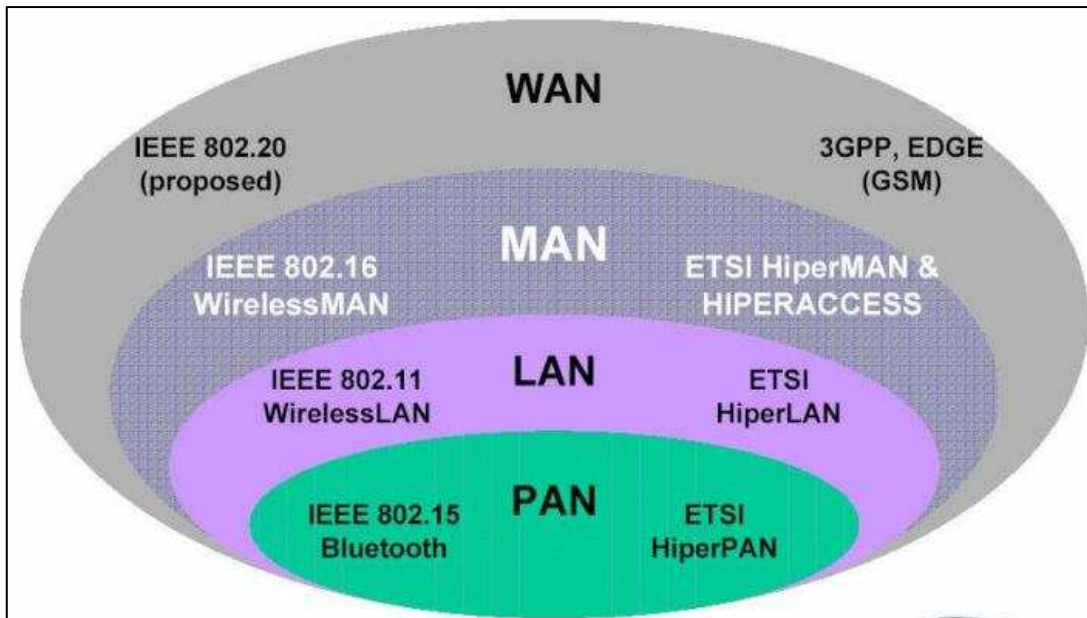


شکل ۱-۹: نمونه شبکه WGAN

جهت وضاحت بیشتر، تعدادی از اشکال از دیدگاه‌های مختلف و به‌صورت مفهومی در نظر گرفته شده است. شکل زیر ابعاد پوشش شبکه‌های یادشده را نشان می‌دهد.

شکل ۱-۱۰ انواع شبکه‌های مختلف را از لحاظ محیط و ابعاد پوشش نشان می‌دهد.

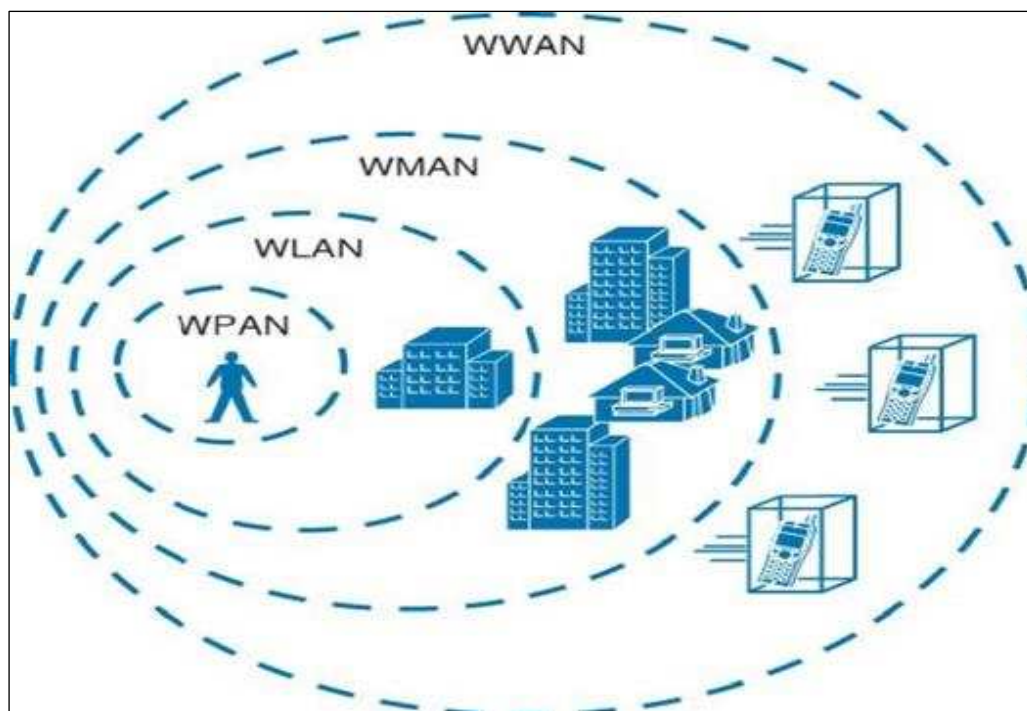
²⁶Cable Modem



شکل ۱-۱۰: انواع شبکه از لحاظ محیط و ابعاد پوشش [۵]

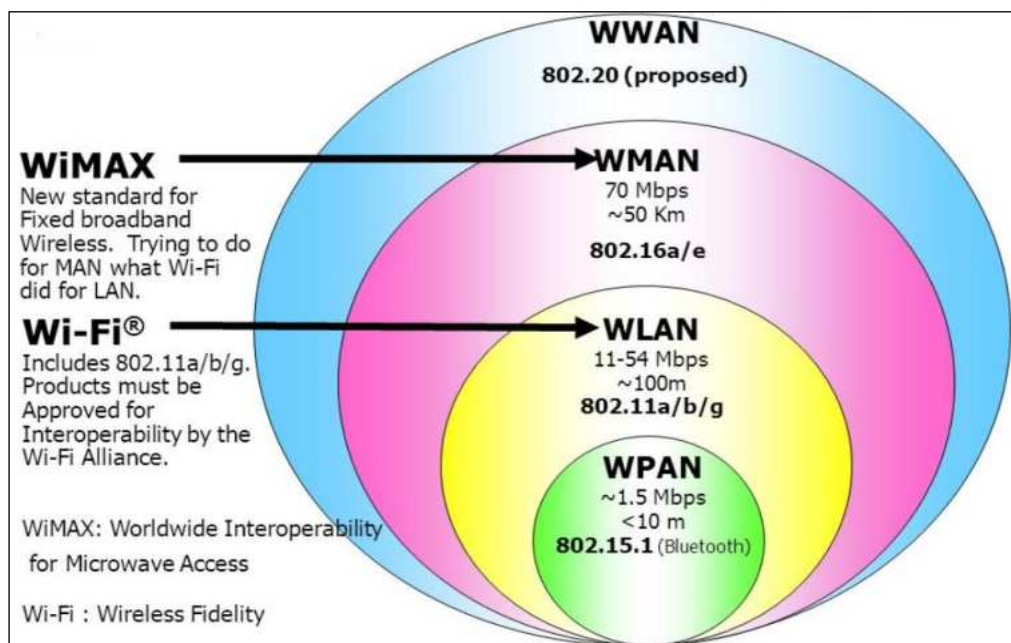
قسمی که یادآوری گردید، هر شبکه بی سیم از لحاظ اندازه و فضای پوشش متفاوت است. شبکه WPAN کوچکترین شبکه و شبکه WWAN بزرگترین نوع شبکه بی سیم است. جهت درک بیش تر مفهوم، شکل ذیل را در نظر بگیرید.

شکل ۱-۱۱ به صورت کلی تمام انواع شبکه های بی سیم شخصی، شبکه بی سیم محلی، شبکه بی سیم جهانی و شبکه بی سیم عمومی را نشان می دهد.



شکل ۱-۱۱: انواع شبکه بی سیم از لحاظ اندازه و محیط پوشش [۶]

مطابق شکل فوق دیده می‌شود که شبکه WPAN منحصر به فرد است. شبکه WLAN منحصر به یک تعمیر و یا یک سازمان است؛ شبکه WMAN منحصر به یک شهر و پوشش محیط یک شهر است و شبکه WWAN منحصر به ایجاد شبکه بین چندین کشور و ناحیه‌های بزرگ است. از لحاظ شناسایی و معرفی استانداردها و تکنالوژی‌های مورد استفاده در شبکه‌های WLAN، WPAN، WWAN شکل ذیل را مشاهده کنید. شکل ۱-۱۲ به جزئیات و تفاوت‌های انواع شبکه‌های بی‌سیم پرداخته است. در این شکل، انواع استانداردها، تکنالوژی‌ها و فاصله تحت پوشش مشخص شده است.



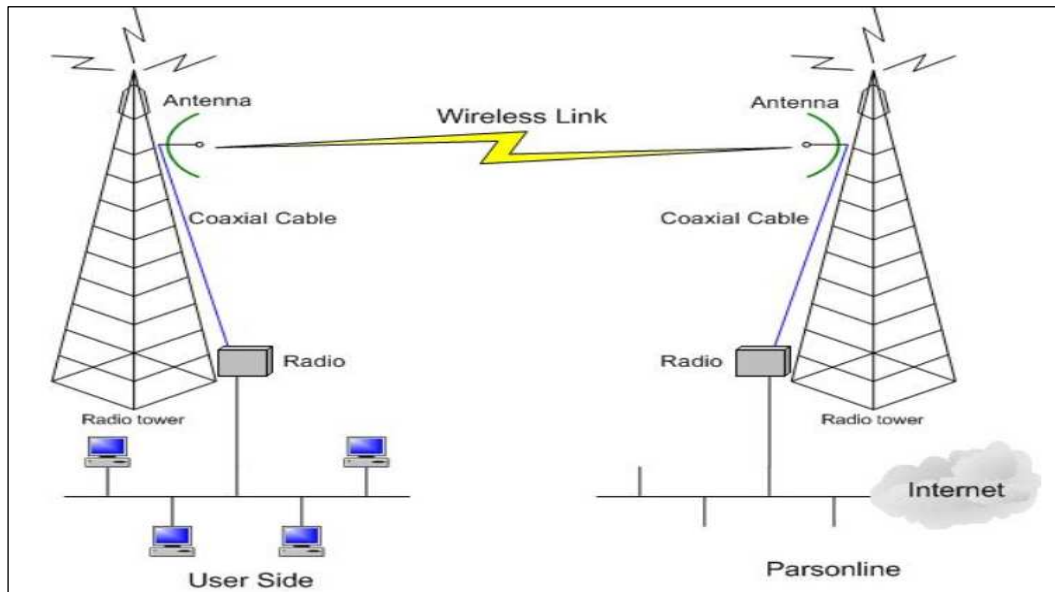
شکل ۱-۱۲: انواع شبکه‌های بی‌سیم از لحاظ تکنالوژی‌ها و استانداردها

در ارتباطات شبکه بی‌سیم، بعضی عوامل در کیفیت و پهنای باند تأثیر می‌گذارند که عبارت‌اند از:

۱. دید دو منطقه نسبت به هم و نبودن مانع بین دو آنتن در طول مسیر.
۲. امواج مزاحم^{۲۷} که از خطوط شبکه‌های بی‌سیم نزدیک یا ایستگاه‌های دیگر ایجاد می‌شود و در نهایت تأثیر مستقیم بالای امواج شبکه شما می‌گذارد.
۳. توانایی یا قدرت ارسال امواج در رادیوها (ساطع کننده‌ها) و آنتن‌ها و هم‌چنان قدرت ارسال و دریافت امواج.

²⁷Interferences

شکل زیر ارتباط دو آنتن بی سیم را به صورت دید مستقیم^{۲۸} با اجزاء و نیازمندی های یک آنتن نشان می دهد. قسمی که دیده می شود، هر آنتن با استفاده از فرستنده و گیرنده امواج و کابل Coaxial و غیره جزئیات آن نشان داده شده است. جهت وضاحت بیش تر شکل ۱-۱۳ را مشاهده کنید.



شکل ۱-۱۳: ارتباط دو آنتن با اجزاء و نیازمندی های آن [۵]

۱.۹ مقایسه شبکه های بی سیم با شبکه سیمی

قابلیت های زیادی را با مقایسه شبکه های بی سیم و سیمی می توانیم بررسی کنیم؛ اما به صورت مختصر به بعضی قابلیت های عمده و اساسی در این جا اشاره می کنیم:

۱. نصب و پیاده سازی؛
۲. هزینه؛
۳. قابلیت اطمینان؛
۴. کارایی؛
۵. امنیت.

۱.۹.۱ نصب و پیاده سازی

در شبکه های سیمی، به دلیل این که باید به هر شبکه LAN از بخش مربوطه خودش و از موقعیت سویچ مربوطه سیم کشی شود، به مسائلی هم چون کندن کاری دیوار، چینل کشی، دک کاری، نصب وال جک^{۲۹} و

²⁸Line of Site

²⁹Wall Jack

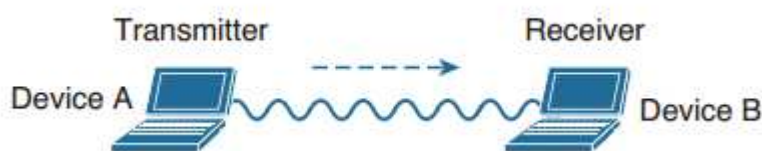
غیره ضرورت است؛ در ضمن، اگر محل فیزیکی سویچ شبکه و یا دستگاه‌های دیگر تغییر کند، باید سیم‌کشی دوباره انجام گیرد.

اما شبکه‌های بی‌سیم قابلیت ارسال و دریافت اطلاعات با استفاده از امواج را دارند. هم‌چنین این شبکه‌ها قابلیت حرکت و جابه‌جایی را دارا هستند؛ بنا براین، تغییرات در محل فیزیکی دستگاه‌های اصلی شبکه، به‌راحتی امکان‌پذیر است؛ لذا، جهت نصب و پیاده‌سازی آن، هزینه و زمان زیادی ضرورت نیست؛ به‌عبارت دیگر، به شکل سریع و با کم‌ترین هزینه امکان پذیر است. برای پیاده‌سازی شبکه‌های بی‌سیم از روش‌های ذیل استفاده می‌شود:

۱.۹.۱.۱ شبکه Ad hoc

این روش پیاده‌سازی جهت ارتباط مستقیم دستگاه‌های بی‌سیم به شکل همتا به همتا یا peer – to peer – است. در این روش تجهیزات را به شکل مستقیم به یک‌دیگر ارتباط داده و در نهایت سازگاری بین دستگاه‌های مختلف بی‌سیم ایجاد می‌شود.

شکل ۱-۱۴ نوعی از شبکه Ad Hoc را نشان می‌دهد.



شکل ۱-۱۴: شبکه Ad Hoc

تنظیم و نصب شبکه Ad Hoc

با استفاده از شبکه Ad Hoc می‌توانیم یک کامپیوتر را به‌صورت بی‌سیم به کامپیوترهای دیگر وصل کنیم؛ لذا، در این جا هدف از تنظیم و نصب شبکه Ad Hoc شریک ساختن منابع یک کامپیوتر به‌صورت بی‌سیم است. در صورتی که این کامپیوتر به اینترنت وصل باشد، می‌توانیم از خدمات اینترنتی این کامپیوتر نیز استفاده کنیم. قابل یادآوری است که خدمات و قابلیت‌های شبکه Ad Hoc در ویندوزهای قبلی به‌صورت پیش‌فرض موجود بود و با استفاده از گزینه ایجاد Connection به‌صورت بی‌سیم، این شبکه فعال می‌گردید؛ اما در ویندوز ۱۰ این قابلیت به‌صورت پیش‌فرض وجود ندارد و باید در محیط سیستم عامل ویندوز فعال گردد. جهت تنظیم و نصب شبکه Ad Hoc دستورها و تنظیمات ذیل را در نظر می‌گیریم.

مرحله اول: تست و چک کردن کارت شبکه

در ابتدا باید حالت مجازی بودن کامپیوتر خود را امتحان کنیم که آیا می‌توانیم ارتباط مجازی این کامپیوتر را با کامپیوترهای دیگر برقرار کنیم و یا خیر؟

برای این کار از دستور ذیل در محیط CMD استفاده می‌شود:

```
C:\> netsh Wlan show Wivers
```

اگر در ادامه، پیام زیر ظاهر گردیده؛ به این معنی است که Host قابلیت ایجاد کردن ارتباط مجازی را دارد.

Message: Hosted Network Supported: **Yes**

این پیام Yes تأیید کننده آن است که قابلیت‌های لازم برای ارتباطات مجازی در این کامپیوتر وجود دارد؛ و اگر به جای Yes، جواب No آمد؛ ضرورت به Update کردن کارت شبکه (NIC) داریم.

مرحله دوم: تنظیم و نصب شبکه Ad Hoc

جهت تنظیم و نصب شبکه Ad Hoc از دستور ذیل استفاده می‌کنیم

```
C:\> netsh wlan set Hostednetwork mode = allow ssid =
```

```
Connection-Name key = your-password
```

جهت وضاحت بیشتر به شکل ۱-۱۵ توجه کنید.

```
C:\Windows\System32>netsh wlan set hostednetwork mode=allow ssid=adhoc key=pass123456
The hosted network mode has been set to allow.
The SSID of the hosted network has been successfully changed.
The user key passphrase of the hosted network has been successfully changed.
```

شکل ۱-۱۵: شکل ایجاد شبکه Ad Hoc

مرحله سوم: فعال کردن شبکه Ad-Hoc

```
C:\> netsh wlan Start Hostednetwork
```

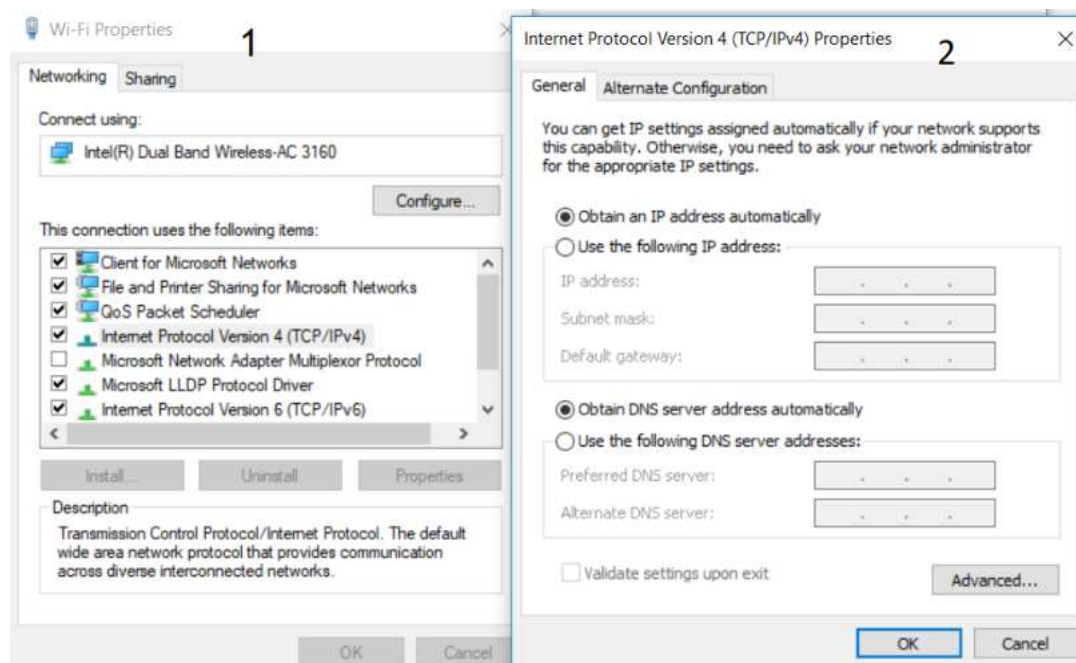
```
C:\Windows\System32>netsh wlan start hostednetwork
The hosted network started.
```

مرحله چهارم: دادن آدرس IP و Share کردن Connection

بعد از انجام دستور فوق، می‌توانیم به کنترل پنل کامپیوتر خود برویم تا connection شبکه خود را چک کنیم. روش چک کردن آن از طریق کنترل پنل به شرح زیر است:

Control panel → Network Sharing Center → Wi-Fi Connection →
Right click → Properties → Select TCP/IPV4 → properties → set IP
Address → OK → Select Tab Sharing → tick the allow other network
users to connect through this computer's internet connection

جهت وضاحت بیش‌تر به شکل ۱-۱۶ که به ترتیب با شماره ۱ و ۲ مشخص شده است، نگاه کنید.



شکل ۱-۱۶: تنظیم آدرس IP و شریک ساختن Connection شبکه

بعد از انجام مراحل فوق، اینترنت به صورت مشترک برای کار برانی که پاسورد و SSID (نام شبکه) را داشته باشند، قابل استفاده است.

جهت خاموش کردن Connection از دستور ذیل استفاده می‌کنیم:

C:\> netsh wlan **Stop** Hostednetwork

جهت حذف کردن Connection از دستور ذیل استفاده می‌کنیم:

C:\> netsh wlan **Delete**profile name= < SSID>

روش Infrastructure: در این روش، ارتباط تمامی تجهیزات با دستگاه مرکزی برقرار می‌شود؛ به همین دلیل، برقراری ارتباط شبکه‌های بی‌سیم از لحاظ زیرساخت^{۳۰} بسیار ساده است. هم‌چنان می‌توان گفت که نصب و پیاده سازی شبکه‌های سیمی یا تغییرات در آن بسیار مشکل‌تر، پرهزینه‌تر و زمان‌گیرتر نسبت به شبکه‌های بی‌سیم است. روشی که با زیرساخت، شبکه‌های بی‌سیم را می‌سازد، ضرورت به اکسس پاینت، مسیریاب‌های بی‌سیم، بریج بی‌سیم و غیره دارد. این روش بر شبکه‌های WLAN، WWAN، WMAN و WGAN قابل استفاده است. تنظیم و نصب این روش روی اکسس پاینت در فصل چهارم انجام خواهد شد و تمام جزئیات آن مانند تنظیم نام شبکه، تعیین آدرس‌های IP و غیره موارد دیگر مطابق ضرورت در همان فصل توضیح داده خواهد شد.

Infrastructure³⁰

۱.۹.۲ مشکلات زیرساخت در شبکه سیمی نظر به شبکه بی سیم

۱. هزینه: تجهیزات و سخت افزارهای لازم در شبکه های سیمی نسبت به شبکه های بی سیم به صورت چشم گیری بیش تر و پرهزینه تر است. این دستگاه ها و تجهیزات شامل هاب، سویچ، روتر، انواع کیبل ها، دک، Rack، Wall Jack، کونکتورها و غیره است که هزینه زیادی را بالای شبکه سیمی تحمیل می کند؛ اما در شبکه بی سیم، تجهیزات فوق یا ضرورت نیست یا این که تنها توسط یک دستگاه، زمینه نصب و پیاده سازی شبکه فراهم می شود؛ از سوی دیگر، می دانیم که در شبکه های سیمی در نظر گرفتن هزینه های نصب و تغییرات احتمالی محیطی و جابه جایی دستگاه های شبکه نیز هزینه قابل توجهی را طلب می کند. قابل ذکر است که با رشد روز افزون شبکه های بی سیم، قیمت و هزینه آن نیز در حال کاهش است.

۲. قابلیت اطمینان: تجهیزات و نوع ارتباط در شبکه سیمی نسبت به شبکه های بی سیم، بسیار قابل اعتمادتر است. از همین روست که سرمایه گذاری سازندگان دستگاه ها و تجهیزات شبکه سیمی، از حدود بیست سال گذشته در این عرصه بیش تر بوده است؛ البته، باید در موقع نصب و یا جابه جایی وسایل و تجهیزات شبکه، اتصال دستگاه ها و کیبل ها با دقت مدیریت و کنترل شود. برعکس، تجهیزات شبکه بی سیم مانند Broadband Router ها مشکلاتی در نوع اتصال دارند. مشکلاتی مانند قطع و وصل شدن های پیهم، تداخل امواج الکترومقناطیسی، تداخل با شبکه های بی سیم مجاور و نزدیک و غیره که البته روند رو به تکامل آن نسبت به گذشته مانند 802.11g است که باعث اطمینان بخشی بیش تر شده است.

۳. کارایی: شبکه های سیمی نسبت به شبکه های بی سیم، دارای کارایی بیش تری هستند. در ابتدا پهنای باند، ۱۰ Mbps سپس به پهنای باندهای بالاتر (100 Mbps, 1000Mbps) افزایش یافته است. در حال حاضر سویچ های با پهنای باند ۱ Gbps نیز ارائه شده اند. شبکه های بی سیم با استانداردهای ۸۰۲/۱۱b و ۸۰۲/۱۱a و ۸۰۲/۱۱g پهنای باند ۵۴ Mbps را به راحتی پوشش می دهند. امروزه در تکنالوژی های جدید، این روند با مقدار نسبتاً بالاتر ۱۰۸ Mbps نیز افزایش داده شده است. علاوه بر این کارایی، شبکه Wi-Fi نسبت به فاصله، حساس است؛ یعنی، حد اکثر کارایی با افزایش فاصله نسبت به Access Point پایین خواهد آمد. این پهنای باند برای به اشتراک گذاشتن انترنت یا فایل ها، کافی است؛ اما، برای برنامه های که نیاز به مبادله اطلاعات زیاد بین سرور و کلاینت به سرور (Client to Server) دارند، کافی نیست.

۴. **امنیت:** چون در شبکه‌های سیمی که به اینترنت هم متصل هستند، وجود فایروال از ضروریات و الزامات است و تجهیزاتی مانند هاب یا سویچ به‌تنهایی قادر به انجام وظایف فایروال نمی‌باشند؛ باید در چنین شبکه‌های، فایروال مجزا نصب شود. در تجهیزات شبکه‌های بی‌سیم مانند Broadband Router ها، فایروال به‌صورت نرم افزاری وجود داشته و تنها باید تنظیمات لازم صورت پذیرد؛ از سوی دیگر، به دلیل این که در شبکه‌های بی‌سیم از هوا به‌عنوان رسانه (Media) انتقال اطلاعات استفاده می‌شود، بدون پیاده سازی تکنیک‌های خاص مانند رمزنگاری، امنیت اطلاعات به‌طور کامل تأمین نمی‌شود. استفاده از رمزنگاری WEP باعث تأمین بیش‌تر امنیت در این تجهیزات گردیده است.



در این فصل به صورت مختصر راجع به نقش سازمان‌ها در شبکه‌های بی‌سیم بحث شد که در آن سه کتگوری از سازمان‌ها برای ایجاد قوانین، استانداردسازی و تأیید استانداردها معرفی گردید؛ البته، این سازمان‌ها به صورت هم‌آهنگ بین هم کار می‌کنند تا یک تکنالوژی مورد استفاده قرار گیرد.

در معرفی شبکه بی‌سیم توضیح داده شد که شبکه بی‌سیم جهت ارسال و دریافت اطلاعات از امواج رادیویی استفاده می‌کند و از این طریق، سرویس‌های لازم را انتقال می‌دهد. به صورت مختصر در بخش فواید و مزیت‌های شبکه بی‌سیم باید یادآور شویم که این شبکه نسبت به شبکه سیمی مزیت‌های زیادی دارد. مهم‌ترین و بارزترین فواید شبکه بی‌سیم قابل حمل بودن، هزینه کم، پیاده‌سازی سریع و غیره است.

در بخش مشکلات شبکه بی‌سیم یادآوری گردید که کاهش سرعت، مشکلات امنیتی، مشکلات در امواج رادیویی، نویز، تداخل در امواج رادیویی، تضعیف سیگنال، انعکاس، انکسار، جذب سیگنال و غیره موارد دیگر شامل مشکلات شبکه بی‌سیم است. هم‌چنان روش کار شبکه بی‌سیم توسط استانداردهای بی‌سیم مانند 802.11a و 802.11b، 802.11g و 802.11n تعیین می‌شود و این شبکه‌ها از امواج رادیویی استفاده می‌کنند. هر استاندارد فوق‌الذکر دارای سرعت، فاصله محدود، فریکانس‌ها و غیره مشخصات منحصر به فرد خود است که جزئیات آن در فصل‌های بعدی نیز تذکر داده خواهد شد.

در بخش دیگر راجع به انواع شبکه‌های بی‌سیم به صورت مفصل بحث گردید. به صورت عموم انواع شبکه‌های بی‌سیم عبارت‌اند از: WPAN، WLAN، WMAN، WWAN و WGAN. این تقسیم‌بندی بیش‌تر به لحاظ ساحت پوشش و یا فاصله تحت پوشش در نظر گرفته شده است.

هم‌چنان مقایسه‌ی بین شبکه سیمی با شبکه بی‌سیم صورت گرفت. این مقایسه از لحاظ نصب و پیاده‌سازی، هزینه، قابلیت اطمینان و کارایی صورت گرفته است. به صورت مختصر در این مقایسه واضح گردید که شبکه بی‌سیم از لحاظ نصب و پیاده‌سازی ساده و آسان و هم‌چنان از لحاظ هزینه ارزان است؛ اما، نسبت به شبکه سیمی هیچ‌گاه اطمینانی‌تر نیست و امنیت آن نیز نسبت به شبکه سیمی ضعیف است.



سوالات فصل اول

۱. شبکه بی سیم را تعریف کنید.
۲. فرق بین شبکه بی سیم و سیمی را در پنج سطر بنویسید.
۳. چهار فایده عمده و اصلی شبکه بی سیم را نام بگیرید.
۴. چهار نقص عمده و اصلی شبکه بی سیم را نام بگیرید.
۵. انواع شبکه های بی سیم را نام بگیرید.
۶. فرق شبکه WLAN و WMAN را بیان کنید.
۷. انواع تکنالوژی شبکه WPAN، WLAN و WMAN را به صورت جداگانه نام بگیرید.
۸. مهم ترین وسیله شبکه بی سیم در WLAN کدام است؟ نام گرفته و معلومات دهید.
۹. وظیفه اصلی دستگاه Access point را بنویسید.
۱۰. سازمان های را که در ایجاد، معرفی و سازگاری استانداردهای شبکه بی سیم نقش دارند، نام بگیرید.
۱۱. مسئولیت اتحادیه Wi-Fi را توضیح دهید.
۱۲. فرق بین مؤسسه FCC و ETSI چیست؟ توضیح دهید.
۱۳. روش های نصب و پیاده سازی شبکه های بی سیم را بیان کنید.
۱۴. روش Ad hoc کدام نوع از روش دیزاین است؟ توضیح بدهید.
۱۵. دستور ایجاد شبکه Ad Hoc را بنویسید.
۱۶. دستور فعال شدن (start) شبکه Ad Hoc را بنویسید.
۱۷. دستور غیر فعال شدن (Stop) شبکه Ad Hoc را بنویسید.
۱۸. دستور حذف شبکه Ad Hoc را بنویسید.
۱۹. به صورت عملی، کامپیوتر خود را با دو کامپیوتر دیگر به صورت بی سیم از طریق شبکه Ad Hoc وصل کنید.
۲۰. بعد از انجام سؤال ۱۹، یک فایل را از یک کامپیوتر به کامپیوتر دیگر از طریق شبکه Ad Hoc ارسال کنید.
۲۱. روش زیرساخت، دارای کدام مشکلات است؟ تنها مشکلات این روش را نام بگیرید.

فصل دوم

تکنالوژی های بی سیم



هدف کلی: محصلان با تکنالوژی های مهم و اساسی شبکه های بی سیم آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. انواع امواج الکترو مقناطیسی را نام بگیرند.
۲. امواج رادیو فریکونسی را توضیح بدهند.
۳. موارد استفاده امواج رادیویی را تشریح کرده بتوانند.
۴. ویژگی های امواج رادیویی را تحلیل کرده بتوانند.
۵. تکنالوژی Wi-Fi را معرفی کرده بتوانند.
۶. موارد استفاده تکنالوژی Wi-Fi، ۳G، ۴G و بلوتوث را توضیح کرده بتوانند.
۷. تفاوت های عمده و اساسی ۳G را با ۵G توضیح کرده بتوانند.
۸. ویژگی ها و قابلیت های WiMax را لیست کرده بتوانند.
۹. مزیت و نواقص تکنالوژی ZigBee را بیان کرده بتوانند.
۱۰. تکنالوژی Li-Fi معرفی کرده بتوانند.

در این فصل معرفی تکنالوژی‌های شبکه بی‌سیم، ویژگی‌های امواج رادیویی، امواج در شبکه بی‌سیم، طول امواج، انواع فریکانسی‌ها و بعضی محاسبات طول موج، فریکانسی، دامنه و هم‌چنان فریکانسی‌های موثر و غیره بحث گردیده است.

علاوه بر مطالب ذکر شده، انواع مختلف از تکنالوژی‌های بی‌سیم، مانند؛ تکنالوژی بلوتوت، تکنالوژی Wi-Fi، تکنالوژی WiMax، قابلیت‌ها و کاربردهای آن، تکنالوژی ZigBee و کاربردهای آن، معرفی و جزئیات کار و عمل کردن تکنالوژی ۳G، معرفی و جزئیات کار و عمل کرد ۴G بحث شده است. هم‌چنان تفاوت‌های اساسی بین ۴G و LTE و غیره موارد دیگر بحث گردیده است.

بحث مهم این فصل روی دو موضوع اساسی شبکه‌های بی‌سیم است. بحث اول در مورد تئوری و نظریه شبکه‌های بی‌سیم است. این تئوری از تعریف امواج رادیویی، امواج الکترومقنطاسی، انواع امواج الکترومقنطاسی است. البته امواج رادیویی که در شبکه‌های بی‌سیم برای مبادله اطلاعات استفاده می‌شود، نوعی از امواج الکترومقنطاسی است. چگونگی انتشار امواج الکترومقنطاسی و طی کردن فاصله‌های طولانی و غیره در این فصل بحث گردیده است.

بحث دومی این فصل، آشنایی تکنالوژی‌های مختلف شبکه‌های بی‌سیم است. در این بخش معرفی، قابلیت، مزیت، موارد استفاده، سرعت تخمینی، فاصله‌های قابل پیش بینی و موارد مهم دیگر بحث گردیده است.

۲.۱ معرفی تکنالوژی Wi-Fi

مطالب این فصل بیشتر روی تکنالوژی بی‌سیم متمرکز شده است که استانداردهای اتصال بین کامپیوترها می‌باشد و به نام تکنالوژی Wi-Fi^{۳۱} یاد می‌شود. تجهیزات به کار رفته در استاندارد Wi-Fi برای اشتراک گذاری فایل‌ها، اتصال به شبکه اینترنت و تجهیزات جانبی کامپیوتر، مانند پرنترهای بزرگ، کامره و اسکنر است. تجهیزات Wi-Fi نسبت به سایر تکنالوژی‌های شبکه بی‌سیم ارزان می‌باشد. هر کامپیوتر به خاطر اتصال به شبکه بی‌سیم، به کارت شبکه بی‌سیم که کم هزینه تر است، ضرورت دارد.

بنا براین ضرورت است که تکنالوژی‌های شبکه بی‌سیم و به صورت خاص تکنالوژی Wi-Fi و امواج رادیویی^{۳۲} را به صورت اساسی درک نمائیم. جهت درک عمیق از تکنالوژی‌های بی‌سیم ضرورت است که درباره تیوری امواج الکترومقنطاسی^{۳۳} و امواج رادیویی به صورت اساسی بحث نمائیم.

^{۳۱}Wi-Fi Alliance

^{۳۲}Radio Wave

^{۳۳}Electromagnetic Waves

۲.۱.۱ تیوری فریکانس‌های رادیویی

ارتباط شبکه بی‌سیم با استفاده از امواج رادیویی برقرار می‌گردد. این ارتباطات در اثر دو Media اصلی بهره‌گیری شده است. به عبارت دیگر نظریه فریکانس‌های رادیویی و ارتباطات از طریق امواج رادیویی، با استفاده از امواج صوتی و امواج الکترومقناطیسی تهداب گذاری شده است.

به عنوان مثال وقتی یک شخص با شخص دیگر صحبت می‌کند، امواج صوتی از طریق هوا انتقال می‌کند و توسط گوش یک شخص تفهیم صورت می‌گیرد. لذا امواج صوتی نوع بسیار قدیمی از ارتباطات شبکه بی‌سیم است. چون در این ارتباطات، انتقال اطلاعات از طریق هوا و بدون کدام سیم، صورت می‌گیرد. اما امواج الکترومقناطیسی نوع دیگر از ارتباطات بی‌سیم است که به شکل موثرتر مفهوم ارتباطات شبکه بی‌سیم را ارائه می‌کند. امواج الکترومقناطیسی به فریکانس‌های متفاوت تقسیم بندی شده و زمینه ارتباطات را فراهم می‌کند.

۲.۱.۱.۱ تعریف امواج الکترومقناطیسی

امواج الکترومقناطیسی عبارت از نوسان انرژی است که امروزه در شبکه‌های بی‌سیم مانند: WPAN، WLAN، WWAN، تلفن‌های بی‌سیم، ریموت کنترل^{۳۴}، رادیو، تلویزیون، بلوتوث، ماورای بنفس^{۳۵} و غیره استفاده چشم‌گیر دارد. علاوه بر آن تعدادی از امواج الکترومقناطیسی که با طول موج مختلف توزیع و پخش می‌شود، عبارت از اشعه گاما^{۳۶}، اشعه X^{۳۷}، نور قابل دید^{۳۸}، نور غیر قابل دید، امواج ماورای قرمز^{۳۹}، امواج ذره وی^{۴۰} و امواج رادیویی است. البته امواج رادیویی بیش‌ترین استفاده را در بخش شبکه‌های بی‌سیم WPAN، WLAN، WWAN، ارتباطات و نشرات سیستم‌های رادیو، تلویزیون، بلوتوث و غیره دارد. انواع امواج الکترومقناطیسی با تفاوت‌های طول موج، در شکل ۱-۲ نشان داده شده است. در این شکل از طرف چپ به راست، طول موج بزرگ‌تر می‌شود.

^{۳۴}Remote Control

^{۳۵}Ultraviolet

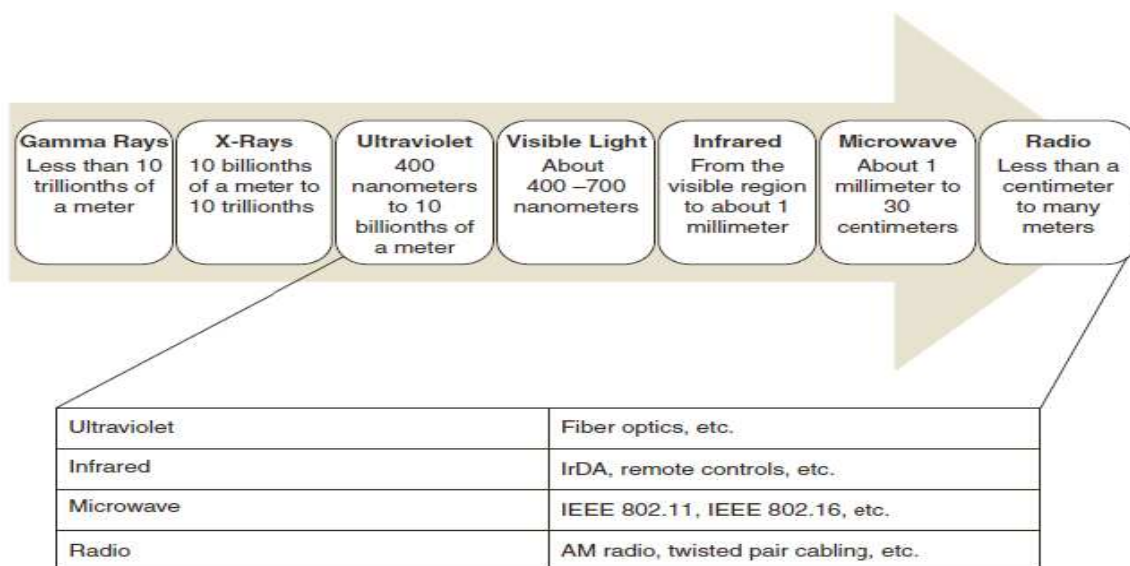
^{۳۶}Gama Ray

^{۳۷}X Ray

^{۳۸}Visible Light

^{۳۹}Infrared

^{۴۰}Microwave



شکل ۲- ۱: انواع امواج الکترومقناطیسی با طول موج‌های متفاوت [۱]

اگر به صورت عموم به امواج الکترومقناطیسی نظر اندازیم، دیده می‌شود که تمام امواج در دایره امواج الکترومقناطیسی وجود دارد. همه این امواج با طول موج‌های مختلف قادر به ارائه و معرفی استندهای مختلف و تکنالوژی‌های گوناگون در عرصه تجارت و طبابت شده است. امواج الکترومقناطیسی به صورت عموم شامل دو بخش یا ساحه می‌باشد که عبارت اند از: ۱- ساحه برقی،^{۴۱} ۲- ساحه مقناطیسی.^{۴۲}

در امواج الکترومقناطیسی ساحه برقی با ساحه مقناطیسی به شکلی باهم تاب خورده و پیچانده شده است که هر دو ساحه به دور هم پیچانده شده است. پیچانده شدن هر دو ساحه در اطراف هم دیگر تشکیل و ایجاد یک زاویه را می‌نماید. وقتی امواج توسط آنتن‌ها به یک جهت حرکت و یا انتشار می‌کند، بستگی به شیپ و جهت عیارسازی آنتن دارد. جهت وضاحت و شناخت بیش تر به این دو بخش اساسی یعنی ساحه برقی و ساحه مقناطیسی اشاره می‌کنیم.

ساحه مقناطیسی عبارت از قوه است که به واسطه حرکت چارچ‌های برقی به وجود می‌آید. لذا از اثر حرکت چارچ‌های برقی در اطراف خودش، ساحه مقناطیسی بوجود می‌آید. وقتی ساحه مقناطیسی از مرکز جذب توسعه پیدا کرد، فضا را متاثر ساخته و ساحه مقناطیسی را بیش تر می‌سازد. در نهایت تغییر ساحه مقناطیسی ساحه برقی را به وجود می‌آورد. (توسعه ساحه مقناطیسی)

پس واضح می‌شود که تغییر ساحه مقناطیسی می‌تواند ساحه برقی

را ایجاد کند و ساحه برقی، ساحه مقناطیسی را ایجاد کند.

^{۴۱} Electric Field

^{۴۲} Magnetic Field

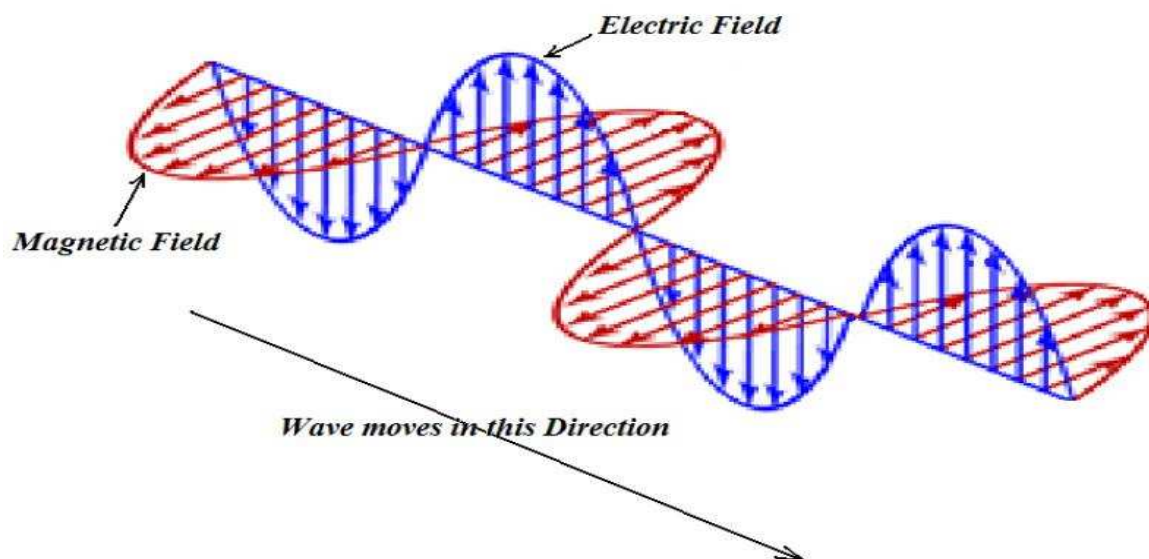
در باره این که آیا اول ساحه مقناطیسی به وجود آمده است یا ساحه برقی، لازم است بررسی بیش تر صورت گیرد. از تغییر کدام حالت، وضعیت تغییر می کند و ساحه جدید را به وجود می آورد. بنابر این جهت وضاحت مطلب می توانیم به مثال دیگری پردازیم.

پرسش تقدم تاخر ساحه مقناطیسی و ساحه برقی، به همان پرسش معروف می ماند که می گفتند: اول تخم مرغ بدنیا آمد یا خود مرغ؟ اگر بیش تر به اصل موضع پی ببریم دیده می شود که اول در اثر حرکت

به صورت واضح، در آغاز جریان برق AC در آنتن شبکه های بی سیم وجود دارد و از اثر حرکت جریان برق (حرکت الکترون ها) ساحه مقناطیسی بوجود می آید. با گسترش ساحه مقناطیسی، ساحه برقی معرفی می گردد و در اثر حرکت ساحه برقی؛ دوباره ساحه مقناطیسی به وجود می آید. بنا بر این در اثر همین امواج الکترومقناطیسی که شامل ساحه برقی و ساحه مقناطیسی است، ارتباطات شبکه بی سیم به وجود می آید و این ارتباطات زمینه تبادل اطلاعات را فراهم می کند. واضح است که تبادل اطلاعات از طریق این امواج اتفاق می افتد. بیش ترین امواج که در انتقال اطلاعات استفاده می شود، امواج رادیویی است.

الکترون ها و یا جریان برقی، ساحه مقناطیسی به وجود می آید و از اثر توسعه و گسترش ساحه مقناطیسی دوباره ساحه برقی به وجود می آید.

انواع از این امواج الکترومقناطیسی با طول موج مشخص و فریکانس های مشخص توسط سازمان IEEE استندرد سازی گردیده که مهم ترین آن عبارت از IEEE ۸۰۲.۱۱ است. شکل ۲-۲ دو ساحه مقناطیسی و ساحه برقی را در امواج الکترومقناطیسی نشان می دهد. مطابق این شکل دیده می شود که هر دو ساحه بالای یک دیگر یک زاویه را ساخته و در اثر تغییر محیط، محیط دیگر نیز پوشش داده می شود.



شکل ۲-۲: امواج الکترومقناطیسی با دو ساحه برقی و مقناطیسی [۶]

امواج الکترومقناطیسی استفاده زیاد دارد که امروز در بخش نشرات رادیو، تلویزیون، ارتباطات از طریق موبایل، بلوتوت، ریموت کنترلر و غیره استفاده دارد. این امواج از طریق یک فرستنده ارسال و توسط گیرنده‌ها دریافت می‌گردد. انواع امواج الکترومقناطیسی موارد استفاده در تکنالوژی‌های مختلف را فراهم می‌کند. هر تکنالوژی با فریکانس‌های متفاوت کار می‌کند که خود زمینه استفاده از فریکانس‌های متفاوت با طول موج متفاوت را به وجود می‌آورد. موارد استفاده امواج الکترومقناطیسی در شکل ۲-۳ نشان داده شده است.



شکل ۲-۳: موارد استفاده از امواج الکترومقناطیسی

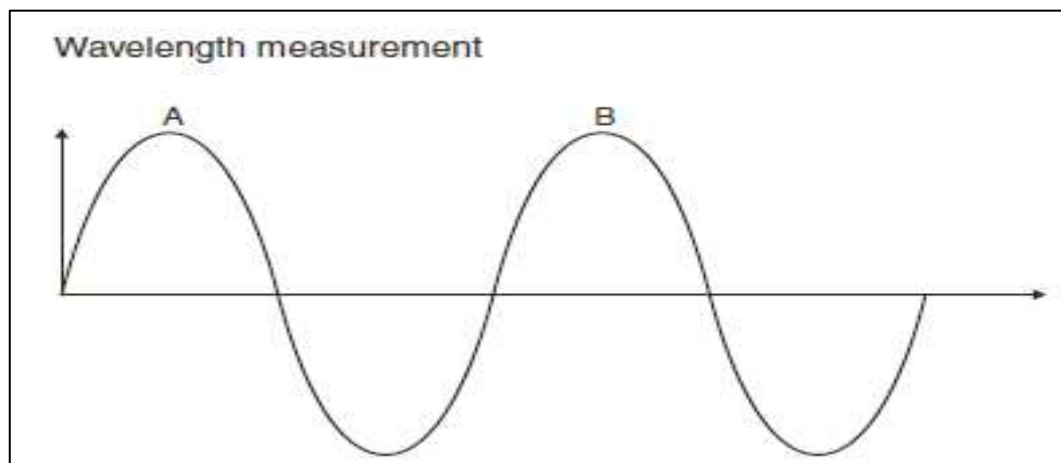
۲.۱.۱.۲ موج

اولین موضوع قابل بحث در امواج الکترومقناطیسی، موج^{۴۳} است. موج در یک محیط فیزیکی اتفاق می‌افتد و عبارت از یک حرکت از طریق مواد است. هم‌چنان موج هیچ‌گاه بدون حرکت مواد تعریف نمی‌شود. اما عبارت از حرکتی مانند نوسان از طریق مواد یا فضا است. قسمی که امواج در یک بحر اتفاق می‌افتد و باعث پستی و بلندی آب در بحر می‌شود.

امواج الکترومقناطیسی نیز عبارت از نوسانی است که از طریق فضا انتقال می‌کند. درحالی‌که بعضی اشخاص در اوایل مطالعه امواج الکترومقناطیسی فکر می‌کردند که مواد غیرقابل دید هستند که از طریق هوا به صورت امواج انتقال می‌کند.

۲.۱.۱.۳ طول موج

طول موج^{۴۴} برای امواج رادیویی عبارت از محاسبهٔ فاصله بین دو قله مجاور در یک موج است. به عنوان مثال دو قله باهم برابر و مجاور که به نام های نقطه اعظمی A و نقطه اعظمی B در یک موج است، به نام طول موج نامیده می‌شود. جهت وضاحت بیش‌تر شکل ۲-۴ را مشاهده نمایید.



شکل ۲-۴: طول موج [۴]

طول موج همیشه عبارت از بخش مهم و قابل سنجش در امواج است که هیچ‌گاه قابل چشم‌پوشی نمی‌باشد. علاوه بر آن طول موج سطح میزان نهایی دریافت اطلاعات توسط آنتن‌ها را نشان می‌دهد. هم‌چنان طول موج روش تعامل با محیط را در امواج رادیویی نیز تعیین می‌کند. به عنوان مثال امواج رادیویی در برابر اجسام مختلف و برخورد با اشیای مختلف، واکنش‌های متفاوت دارد. آن‌چه اثبات گردیده است، بعد از برخورد امواج رادیویی در برابر اجسامی که ذرات آن فشرده و متراکم باشد، طول موج زیادتر بزرگ می‌شود.

⁴³Wave

⁴⁴Wavelength

در صورتی که فشردگی ذرات اجسام در یک مواد کم تر باشد، بعد از برخورد طول موج زیاد تغییر نکرده و کم تر بزرگ می شود. به صورت عموم و در هر حالت طول امواج بعد از برخورد با اجسام، و به تناسب فشردگی ذرات در آن جسم، بزرگ تر می گردد. باید توجه داشته باشیم که بخش دیگر از امواج فریکونسی^{۴۵} است. فریکونسی همیشه با طول موج وابسته^{۴۶} است. هرگاه طول موج تغییر کند، به صورت حتمی فریکونسی نیز تغییر می کند و برعکس هرگاه فریکونسی تغییر کند، طول موج نیز تغییر می کند. به عبارت دیگر هرگاه طول موج داده شود، می توانیم فریکونسی را بدست آوریم و هرگاه فریکونسی داده شود، می توانیم با محاسبه فریکونسی، طول موج را به دست آوریم.

به عنوان مثال اگر سرعت نور ۲۹۹,۷۹۲,۴۵۸ متر بر ثانیه باشد و فریکونسی یک موج داده شده باشد، می توانیم طول موج را با استفاده از فرمول ذیل بدست بی آوریم.

$$W = 299,792,458 / f$$

در فرمول فوق W عبارت از طول موج (Wavelength)، f عبارت از فریکونسی (Frequency) و عدد ۲۹۹,۷۹۲,۴۵۸ عبارت از سرعت نور است که همیشه برابر به سرعت امواج الکترومقناطیسی گفته شده است. اگر به عنوان مثال فریکونسی (f) با ۲.۴GHz در نظر بگیریم، که مساوی به ۲,۴۵۰,۰۰۰,۰۰۰ هرتز می شود، طول موج را به شکل ذیل محاسبه کرده می توانیم.

$$W = 299,792,458 / 2,450,000,000$$

در نتیجه ۰.۱۲۳ متر و یا به صورت تقریبی مساوی به ۱۲.۳ سانتی متر طول موج به دست می آید. اگر جهت ایجاد فورمول بندی از حروف و علائم رسمی استفاده گردد، می توانیم به شکل ذیل ساده بسازیم.

اگر سمبول Greek Lambda را به شکل (λ)، سمبول سرعت نور را به C و سمبول فریکونسی را به f نشان دهیم. فورمول فوق الذکر به شکل ذیل خواهد بود. $F = C / \lambda$

فریکونسی را می توانیم به شکل ذیل به دست آوریم.

$$F = 299,792,458 / 0.123 \text{ cm}$$

بعد از محاسبه فوق فریکونسی ۲.۴۵GHz به دست می آید.

⁴⁵ Frequency

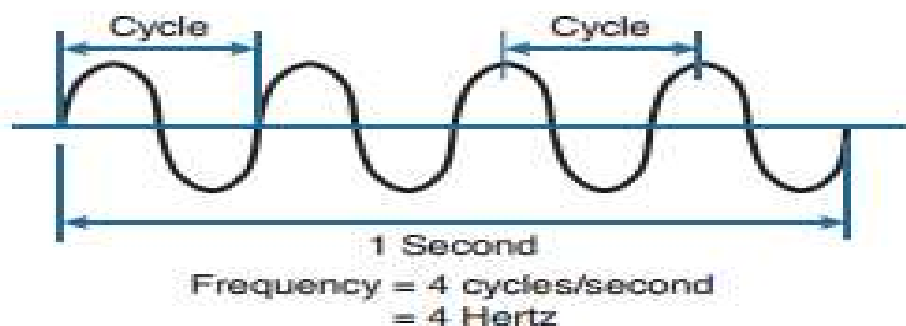
⁴⁶ Interrelated

۲.۱.۱.۴ فریکونسی

فریکونسی به تعداد دور از امواجی ارتباط می‌گیرد که در یک زمان داده شده اتفاق می‌افتد. معمولاً فریکونسی^{۴۷} به ثانیه محاسبه می‌شود. به عنوان مثال فریکونسی یک کیلوهرتز (۱ KHz) عبارت از ۱۰۰۰ دور از امواج در یک ثانیه است. تمام امواج الکترومقناطیسی شامل امواج رادیویی، به سرعت نور انتقال می‌کند. فریکونسی همیشه با طول موج در ارتباط بوده و در صورت تغییر فریکونسی طول موج نیز تغییر می‌کند. به عبارت دیگر آن گونه که در فرمول دیده شد، فریکونسی، طول موج و رسانه (Medium) که باعث انتقال اطلاعات می‌گردند، همیشه باهم دیگر وابستگی دارند. با تغییر رسانه و طول موج، حتماً فریکونسی نیز تغییر می‌کند.

به عنوان مثال: فریکونسی بالا دارای طول موج کوتاه‌تر و فریکونسی پائین دارای طول موج بزرگ‌تر می‌باشد.

شکل ۲-۵: تعداد دور در یک ثانیه و روش محاسبه فریکونسی را نشان می‌دهد.



شکل ۲-۵: تعداد دور در یک ثانیه (فریکونسی) [۶]

۲.۱.۱.۵ دامنه موج

فرض براین است که اگر امواج با فریکونسی پائین‌تر داشته باشیم، فاصله بیش‌تر طی می‌شود، به همین شکل اگر امواج با فریکونسی بالا منتشر گردد، فاصله طی شده، کم می‌شود. بنابراین ویژگی دیگر که عبارت از دامنه موج^{۴۸} است، نیز بر انتقال اطلاعات تاثیر دارد.

دامنه موج به عنوان یک بخش مهم در امواج قابل بحث است. وقتی که فاصله زیاد با استفاده از طول موج کوتاه، پوشش داده شود، تشخیص صدا و یا درک نوع سگنال مشکل می‌شود. هرگاه فاصله زیاد توسط طول موج بزرگ‌تر پوشش داده شود، تشخیص صدا و یا نوع سگنال مشکل نیست.

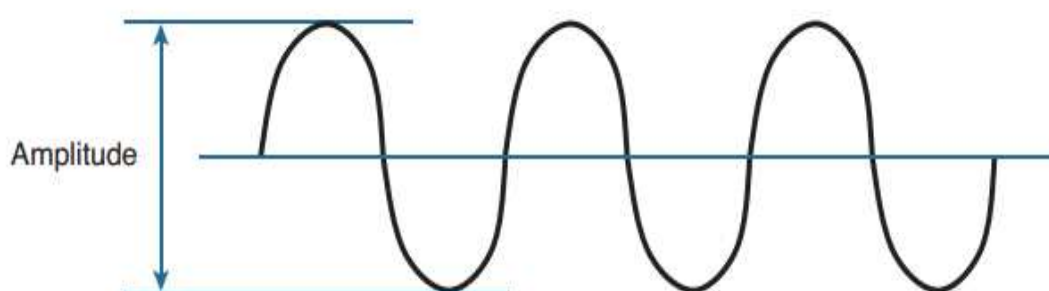
^{۴۷}Interrelated

^{۴۸}Amplitude

بنا بر این ویژگی دیگر امواج عبارت از دامنه است که اندازه طول موج را تعیین می‌کند تا در کدام فاصله تشخیص صدا و سگنال قابل فهم باشد. در امواج صوتی؛ وقتی صدا قابل تشخیص نباشد، دامنه را با روش مهندسی صدا (دست خود را در اطراف دهن قرار می‌دهند و بعد صدا می‌زنند) تا وقتی افزایش می‌دهند که صدا قابل شنیدن باشد. یا این که تقویه کننده صدا^{۴۹} را اضافه می‌کنند تا صدا را بلندتر کنند که بتواند فاصله بیش‌تر را طی کند. با اضافه کردن تقویه صدا؛ در اصل دامنه امواج صوتی را افزایش می‌دهند.

همان گونه که فریکونسی در فاصله امواج صوتی تاثیر دارد، به همان میزان امپلیتود یا دامنه در تشخیص (شنیدن) امواج صوتی در همان فاصله موثر است.

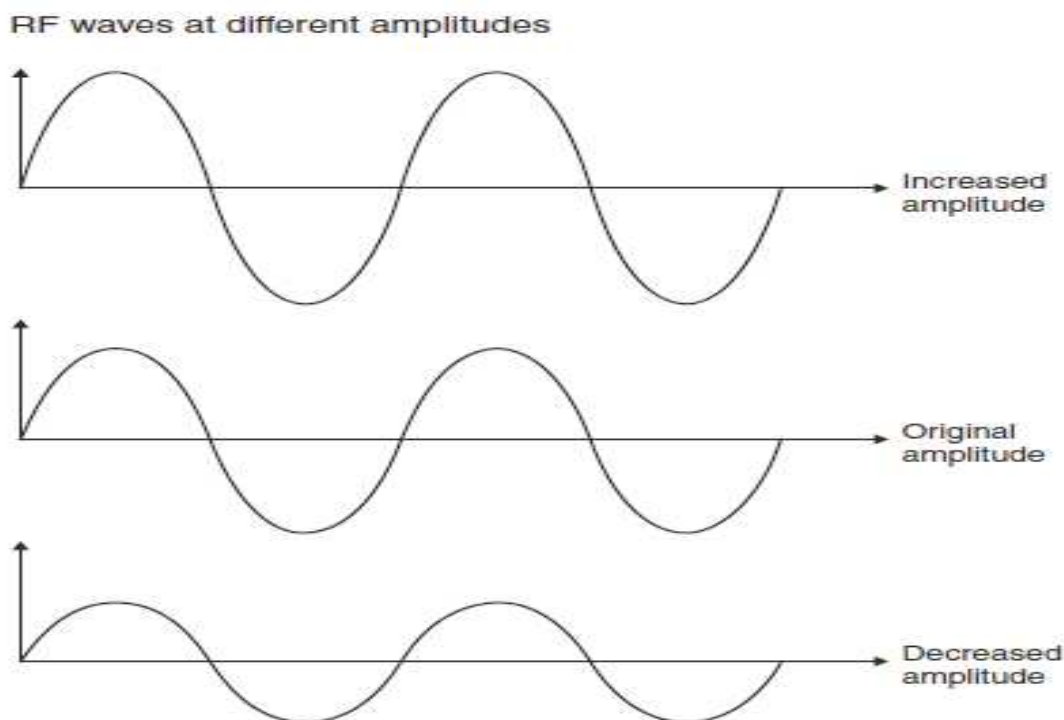
به صورت مختصر تشخیص و درک "امواج رادیویی با دامنه بالا نسبت به امواج رادیویی با دامنه پائین"، آسان است. هر قدر امواج با دامنه پائین منشر شود، به همان میزان درک و تشخیص امواج سخت‌تر می‌شود. با توضیحات فوق، گفته می‌توانیم که کیفیت ارتباطات با داشتن دامنه بزرگ‌تر به وجود می‌آید. جهت اثبات این ادعا به تیوری ریاضی مراجعه می‌کنیم که "انتشار امواج صدا تا ابد ادامه دارد، اما به دلیل کوچک شدن دامنه، صدا قابل تشخیص نمی‌باشد". به بیان دیگر با گذشت زمان، دامنه در امواج کاهش پیدا می‌کند و در اثر کاهش و کوچک شدن دامنه در امواج، سگنال و یا صدا در فاصله‌های دور قابل تشخیص نمی‌باشد. امواج رادیویی که جهت ارتباطات در شبکه بی سیم استفاده می‌شود، نیز حالت مشابه دارد. تنها امواجی قابل استفاده و موثر است که دارای دامنه بزرگ باشد. لذا در امواج رادیویی وقتی دامنه امواج، کاهش پیدا می‌کند، موثریت آن کم‌تر می‌شود. دامنه موج از بلندترین نقطه تا پائین‌ترین نقطه یک موج محاسبه می‌گردد. شکل ۲-۶ به صورت نمونه دامنه موج را نشان می‌دهد.



شکل ۲-۶: دامنه موج [۶]

شکل ۲-۷ امواج را با دامنه‌های متفاوت (حالت عادی، حالت افزایش یافته دامنه و حالت کاهش یافته دامنه) نشان داده است.

⁴⁹Amplifier



شکل ۲-۷: حالت‌های متفاوت امواج رادیویی فریکونسی با دامنه‌های متفاوت [۱]

۲.۱.۱.۶ ویژگی‌های مهم امواج رادیویی

امواج رادیویی، فریکونسی تنظیم یافته و حاوی معلوماتی است که به نام سگنال‌های رادیویی فریکونسی^{۵۰} یاد می‌شود. دانستن رفتار و ویژگی‌های^{۵۱} یک سگنال رادیو فریکونسی کمک می‌کند تا وضعیت و حالت‌های یک سگنال رادیویی را پیش‌بینی و قابل تشخیص بسازیم. این سگنال‌های رادیویی می‌تواند قوی یا ضعیف باشد. قدرت و ضعف امواج رادیویی یکی از ویژگی‌های اصلی امواج رادیویی است. هم‌چنان واکنش‌های امواج رادیویی در برابر مواد مختلف می‌تواند متفاوت باشد و در بعضی حالت‌ها می‌تواند باعث تداخل با هم‌دیگر شوند. رفتار و ویژگی‌های اصلی امواج رادیو فریکونسی عبارت‌اند از:

۱. نفع و دسترسی (Gain)
۲. از دست دادن (Loss)
۳. انعکاس (Reflection)
۴. انکسار (Refraction)
۵. تجزیه شدن (Diffraction)
۶. پراکنده شدن (Scattering)
۷. جذب شدن (Absorption)

^{۵۰}Radio Frequency Signal

^{۵۱}Radio Frequency Behavior

۸. اندازه موج بر اساس ولتاژ (VSWR)

۹. تقویه و تضعیف سگنال (Amplification and Attenuation)

۱۰. انتشار امواج (Wave Propagation)

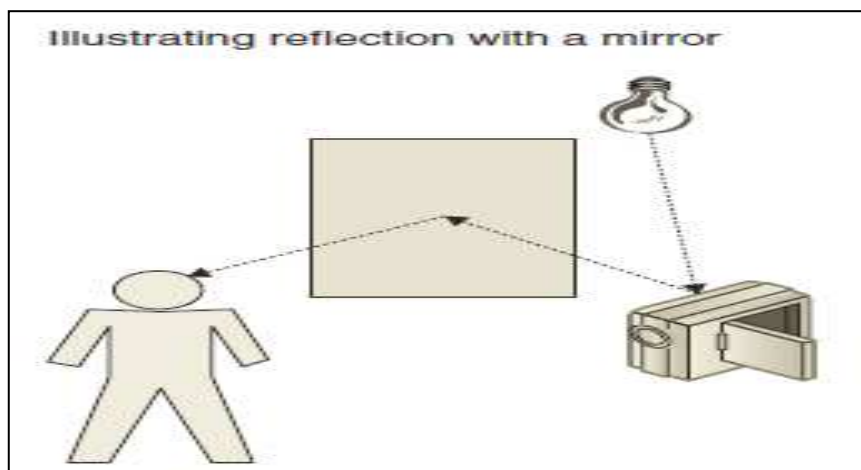
۱۱. تأخیر (Delay)

موارد فوق‌الذکر به صورت عموم از ویژگی‌های امواج رادیو فربکونسی است. هرکدام از گزینه‌های فوق‌الذکر نیازمند توضیحات است. اما جزئیات آن ضرورت به توضیحات بیش‌تر ندارد.

نفع و دست‌رسی (Gain): یکی از ویژگی‌های مهم و مثبت Gain است. در صورت داشتن Gain مناسب، استفاده و موثریت در شبکه‌های بی‌سیم بهتر و بیش‌تر می‌شود.

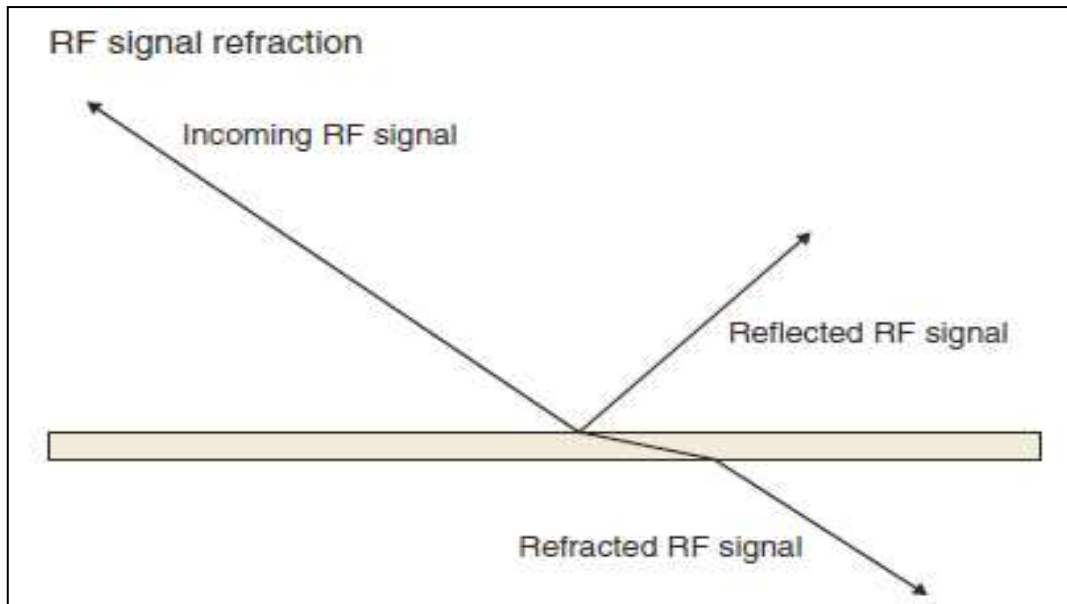
از دست دادن (Loss): در صورت از بین رفتن امواج رادیویی به دلیل فاصله طولانی و یا برخورد به کدام موانع، امواج رادیویی از بین رفته و قابل دریافت نمی‌باشد.

انعکاس (Reflection): انعکاس نوع دیگر از ویژگی‌های امواج رادیویی است که در اثر برخورد با اجسام شفاف و متراکم به وجود می‌آید. انعکاس در امواج نوری را در شکل ۲-۸ مشاهده کنید.



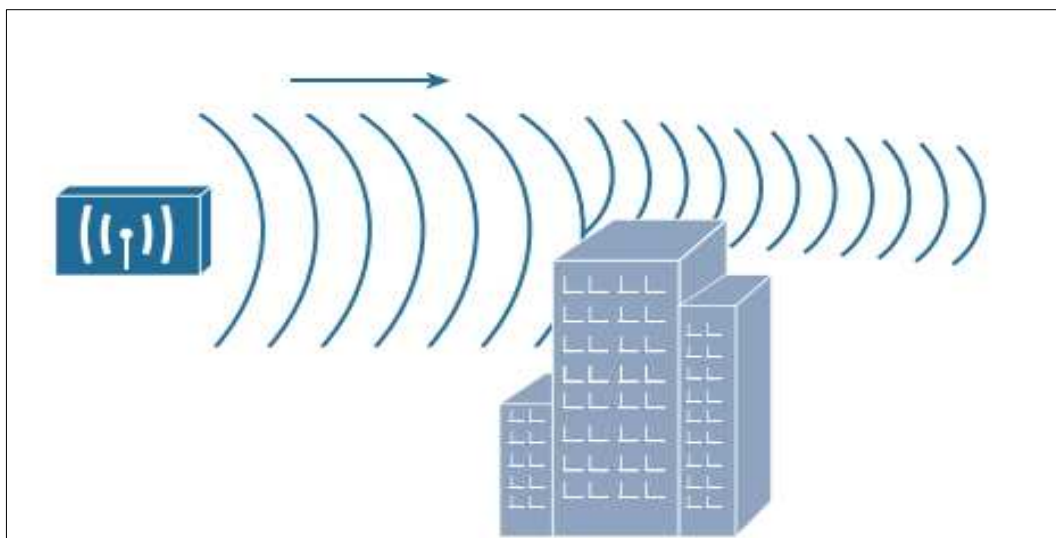
شکل ۲-۸: انعکاس در امواج نوری [۱]

انکسار (Refraction): در صورتی که تراکم مواد در اجسام مختلف، متفاوت باشد، در هنگام عبور امواج رادیویی از یک شی و برخورد با شی دیگر، انکسار رخ می‌دهد. شکل ۲-۹ انکسار سگنال رادیویی را نشان می‌دهد.



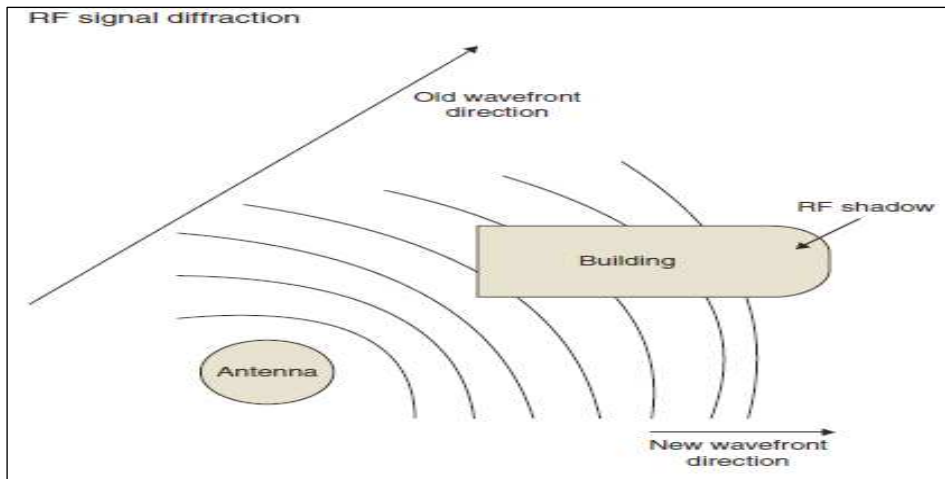
شکل ۲-۹: انکسار در امواج رادیویی [۴]

انحنای سگنال (Diffraction): زمانی که امواج رادیویی در اثر برخورد با یک جسم، برگشت داده شود و قسمی که به شکل سایه در اطراف شی منحنی ایجاد کند، به نام Diffraction یاد می‌شود. به عبارت دیگر این حالت در وقت برخورد سگنال رادیویی با تپه‌ها و ساختمان‌ها اتفاق می‌افتد و انحنای سگنال^{۵۲} را به وجود می‌آورد که به نام Diffraction یاد می‌شود. اشکال ۲-۱۰ انحنای سگنال را نشان می‌دهد.



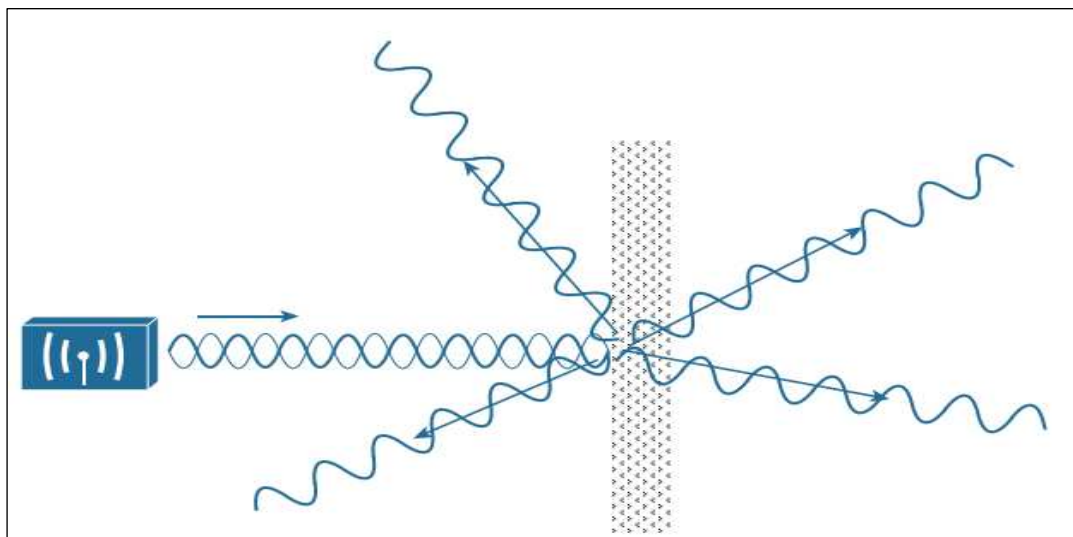
شکل ۲-۱۰: انحنای سگنال در امواج رادیویی [۶] (Diffraction)

⁵²Diffraction



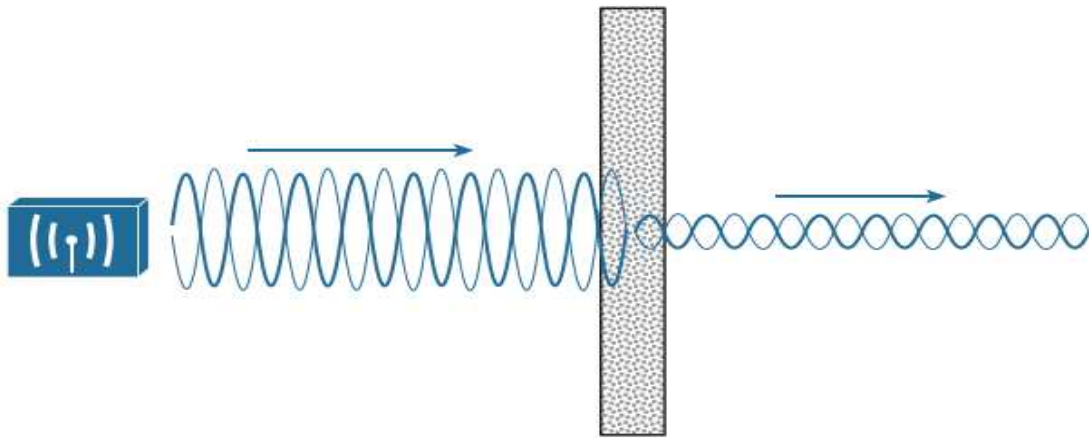
شکل ۲-۱۱: انحنای سگنال در امواج رادیویی [۱](Diffraction)

پراکنده شدن (Scattering): هرگاه یک موج رادیویی با اشیای محیط قسمی برخورد نماید که باعث پراکنده شدن آن گردد، به نام Scattering یاد می‌شود. به عبارت دیگر هرگاه از اثر برخورد یک موج رادیویی چندین انعکاس به وجود آید به نام پراکنده شدن موج یاد می‌شود. این حالت برای شبکه‌های بی‌سیم بدترین حالت بوده و قابل استفاده نمی‌باشد. این حالت در امواج رادیویی مشکلات جدی را در تشخیص سگنال رادیویی به وجود می‌آورد. جهت وضاحت بیش‌تر شکل ۲-۱۲ را مشاهده نمایید.



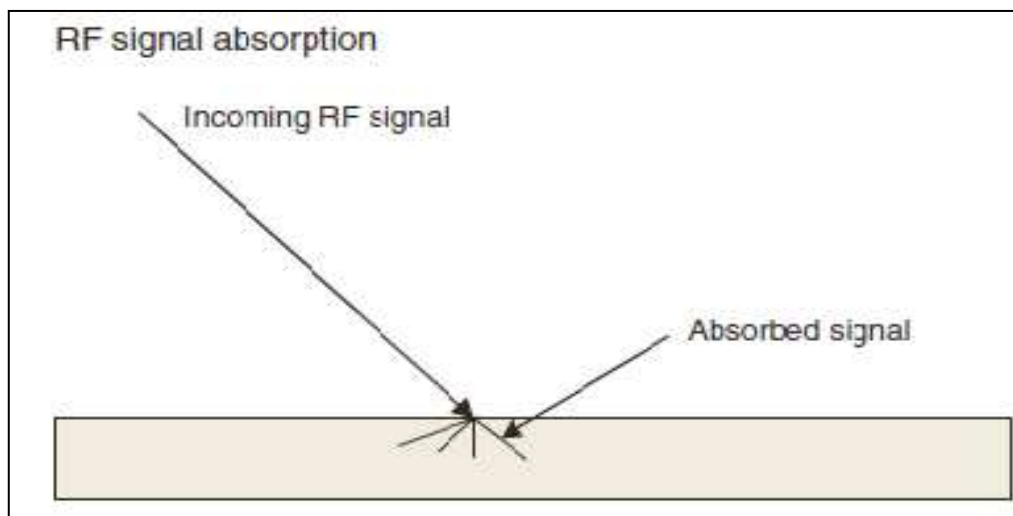
شکل ۲-۱۲: شکل پراکنده شدن موج رادیویی [۶](Scattering)

جذب شدن (Absorption): در صورتی که امواج رادیویی بعد از برخورد با اجسام، جذب گردد، به نام Absorption یاد می‌شود. این حالت در زمانی اتفاق می‌افتد که مواد در اجسام قابلیت جذب را داشته و قابلیت انعکاس و انکسار را نداشته باشد. شکل ۲-۱۳ جذب سگنال رادیویی را در یک مانع نشان می‌دهد.



شکل ۲-۱۳: جذب (Absorption) سگنال رادیویی توسط مانع [۶]

جهت وضاحت بیش‌تر شکل ۲-۱۴ را مشاهده کنید. شکل ذیل نیز Absorption را نشان می‌دهد.



شکل ۲-۱۴: شکل جذب امواج رادیویی توسط یک مانع [۴]

تقویه و تضعیف سگنال (Amplification and Attenuation): تقویه کردن امواج یکی از ویژگی‌های دیگر امواج رادیویی است. در صورت نیاز می‌توان توسط تقویه کننده‌ها، امواج را تقویه کنیم. هم‌چنان در صورت ضرورت می‌توان امواج رادیویی را تضعیف کنیم. این حالت زمانی ضرورت است که بخواهیم امواج را در فاصله مشخص کنترل کنیم تا نظر به بعضی محدودیت‌ها، امواج از فاصله مشخص بیش‌تر انتشار داده نشود.

انتشار امواج (Wave Propagation): انتشار امواج یکی از ویژگی‌های دیگر است که در محیط آزاد و هوا قابلیت انتشار را دارد.

تاخیر (Delay): تاخیر یا دیر رسیدن امواج به دلایل مختلف، یکی از ویژگی‌های امواج است که نظر به محیط، موانع، اجسام و ذرات مختلف، متفاوت خواهد بود.

ارتباطات رادیویی

انواع ارتباطات از طریق تکنالوژی‌های بی‌سیم بسیار گسترده است. به عبارت دیگر انواع مختلف از تکنالوژی‌های بی‌سیم وجود دارد که زمینه ارتباطات را به شکل بی‌سیم فراهم می‌کند. بیش‌ترین ارتباطات از طریق امواج رادیویی در شبکه بی‌سیم صورت می‌گیرد. هم‌چنان شیوه‌های مختلفی نیز در شبکه سازی بی‌سیم مورد استفاده قرار می‌گیرد که در ذیل به آن‌ها اشاره می‌کنیم:

۱. **فریکانس‌های رادیویی (Radio Frequency):** این فریکانس به فریکانس امواج رادیویی مشهور است. در این روش، بین فریکانس ۱۰ KHz تا سرعت چند گیگاهایت قرار می‌گیرد. آنتن‌های که این امواج را انتقال می‌دهند ممکن است به صورت تمام جهتی^{۵۳} و یا به جهت خاص^{۵۴} استفاده شود. آنتن‌های که به جهت خاص و در یک جهت قابلیت استفاده دارند، چون انتشار امواج بسیار زیاد است، امواج برای نقاط دورتر، ارسال می‌گردد. در این روش دیتا با سرعت ۱ تا ۱۱ میگاهایت در ثانیه انتقال می‌یابد، ارتباطات در این محدوده نیازی به مجوز ندارد و تجهیزات ارتباطی نیز به صورت گسترده فراهم می‌باشد.

۲. **امواج ذره‌یی (Microwave):** امواج ذره یا میکروویو شیوه دیگری از روش‌های ارتباطات در شبکه‌های بی‌سیم می‌باشد. امواج میکروویو تنها از یک جهت منتشر می‌شوند. سرعت انتقال این امواج متغیر بوده و از ۱ Mbps الی ۲ Mbps می‌باشد. یکی از مشکلات امواج میکروویو این است که شدیداً تحت تاثیر تغییرات در اتمسفر و نوسانات جوی؛ مانند: رعد و برق قرار دارد. این سیستم‌ها (امواج میکروویو) در دو نوع: ۱- ماهواره ۲- زمینی قابل استفاده می‌باشند. نوع زمینی آن از آنتن‌های بشقابی دوطرفه برای تقویت امواج استفاده می‌شود. برای استفاده از تجهیزات میکروویو نیاز به اخذ مجوز^{۵۵} است و به صورت دل‌خواه مانند تکنالوژی‌های Wi-Fi به صورت رایگان استفاده نمی‌شود. موضوع فریکانس‌های با مجوز^{۵۶} و فریکانس‌های بدون مجوز^{۵۷} در عنوان جداگانه بحث خواهد شد.

۳. **امواج مادون قرمز (Infrared):** این نوع از ارتباطات شبکه‌های بی‌سیم نوع دیگری از امواج رادیویی است. این امواج از طریق دایودهای نورگسیل (LED) یا لیزری (ILD) تولید می‌شوند. امواج مادون قرمز دارای فریکانس بالاست. لذا سرعت انتقال دیتا از ۱ الی ۱۳Mbps در ثانیه می‌باشد.

⁵³Omi Direction

⁵⁴Directional

⁵⁵Licenses

⁵⁶Licensed Frequency

⁵⁷Unlicensed Frequency

۲.۲ فرکانس آزاد و مجوز دار

فرکانس های 5GHZ و 2.4GHZ در تمام کشور ها از جمله فرکانس های آزاد است چون به صورت محلی استفاده می شود، نیاز به مجوز از طرف دولت ندارد اما سایر فرکانس ها در هر کشور جهت کنترل و جلوگیری از تداخل، نیاز به مجوز دارد و معمولاً وزارت مخابرات هر کشور مسئولیت آن را به عهده دارد. فرکانس های هم وجود دارد مثل فرکانس 900MHZ در بعضی کشور ها آزاد است در حالی که در کشور های دیگر نیاز به مجوز دارد. تمام شرکت های تامین کننده اینترنت، رسانه ها و شرکت های مخابراتی قبل از فعالیت باید محدوده فرکانسی خویش را با وزارت مخابرات تعیین کند. کسانی که در استفاده آن تخطی نماید از طرف نهاد مربوطه مجرم شناخته خواهد شد.

در تازه ترین رویداد ها کمیته ارتباطات فدرال امریکا فرکانس 6GHZ را برای نوع جدید wi-fi و اینترنت اشیا آزاد ساخته است.

۲.۳ معرفی تکنالوژی بلوتوت

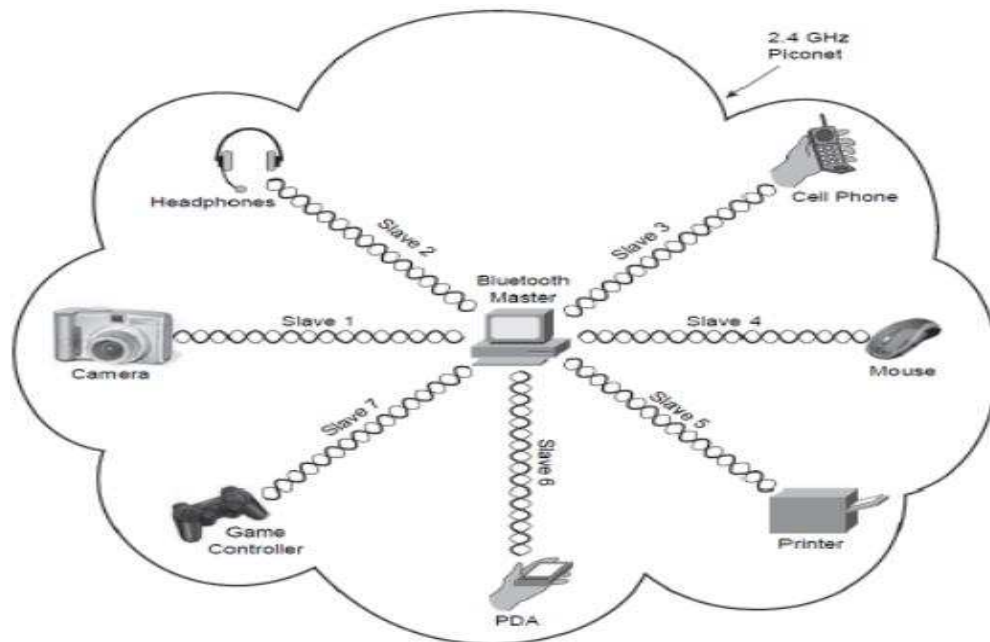
امروزه بلوتوت در همه تلفن ها، PDA ها، لپ تاپ ها، پرینترها و خیلی دستگاه های دیگر استفاده می شود. به دلیل این که بلوتوت از برق کم تر استفاده می کند و مصرف برق آن کم تر است، برای دستگاه های متحرک که با بطری کار می کنند، مناسب هستند.

از سال ۱۹۹۸ که گروه علاقه مندان بلوتوت تشکیل شده تا حال نسخه های مختلفی از این تکنالوژی طراحی و به کار گرفته شده است. در سال ۲۰۰۷ نسخه بلوتوت ۲.۱ وارد بازار شد که با EDR(Enhanced Data Rate) همراه بوده است. این نسخه یک ویژگی مهم داشت و آن هم سرعت هم گرایی (Quick Pairing) بین دو گره^{۵۸} بود. در این ویژگی دو دستگاه به شکل سریع هم دیگر را پیدا می کردند. این نسخه همچنین به صورت یک ویژگی دیگر به نام sniff subrating عمر بطری را تا ۵ دقیقه بیش تر افزایش می داد.

تکنالوژی بلوتوت ممکن است با LAN های ۸۰۲.۱۱ تداخل پیدا کند. دلیل تداخل پیدا کردن آن در این است که در محدوده فرکانسی 2.4GHz فعالیت می کند. اما چون برای فعالیت در مساحت تقریباً ۳۵ فوت طراحی شده، قدرت ارسالی خیلی پائینی دارد و هم چنان از طرف دیگر FHSS استفاده می کند، خیلی بعید است که تداخل به وجود آید.

بلوتوت به عنوان یک Piconet نیز در نظر گرفته می شود؛ زیرا به ۸ دستگاه به صورت هم زمان اجازه می دهد که باهم جوره شوند که در این صورت یک ماستر و هفت slave دارد. جزئیات بیش تر را در شکل ۲-۱۵ مشاهده نمایید.

^{۵۸} node



شکل ۲-۱۵: استفاده تکنالوژی بلوتوت به صورت هم‌زمان

۲.۴ معرفی تکنالوژی ZigBee

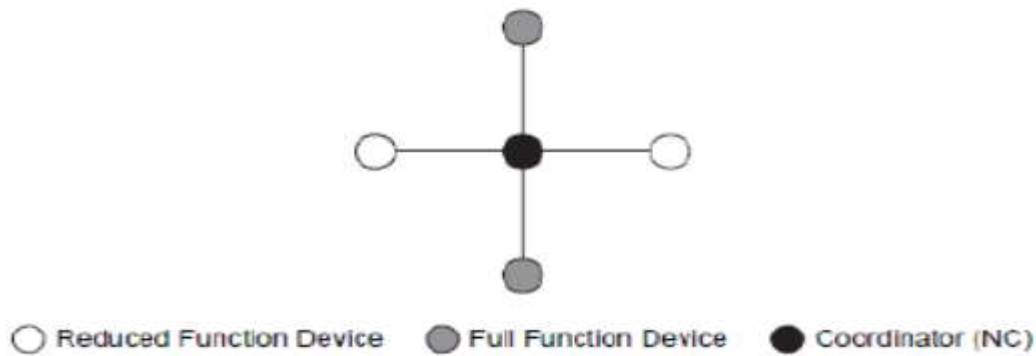
تکنالوژی ZigBee شامل Digital Radio های کوچک و هم‌چنان مصرف انرژی کم می‌شود. یکی از ویژگی‌های مثبت آن این است که با انرژی کمتر کار می‌کند که موارد استفاده و علاقمندان آن را افزایش داده است. این تکنالوژی براساس استاندارد IEEE 802.15.4 برای شبکه‌های WPAN طراحی شده است. این تکنالوژی برای Headphone های بلوتوت که با موبایل در ارتباط است، برای کنترل و سیستم‌های نظارت به کار می‌رود. این تکنالوژی در باندهای ISM که دارای استانداردها و فریکانس‌های بدون لایسنس است، فعالیت می‌کند. بیش‌ترین موارد استفاده این تکنالوژی در اتوماسیون‌های اداری، صنعتی، خانه‌های هوشمند و شهرهای هوشمند می‌باشد [۷].

شکل ۲-۱۶ یک توپولوژی نوع ستاره^{۵۹} را نمایش می‌دهد. در این شکل دستگاه مرکزی NC^{۶۰}، سایر دستگاه‌ها تمام وظیفه^{۶۱} و Reduced-Function می‌باشند.

⁵⁹ Star

⁶⁰Network Coordinator

⁶¹Full-Function



شکل ۲-۱۶: توپولوژی ستاره برای تکنالوژی ZigBee

یک دستگاه همه می تواند وظیفه ارسال، دریافت و یک تعداد کارهای دیگر را انجام دهد. اما یک دستگاه Reduced-function همه این قابلیت ها را ندارد و تنها می تواند کارهای چون گزارش گرمای یک سیستم به کنترلر را انجام دهد.

۲.۵ معرفی تکنالوژی WiMax

تکنالوژی WiMax^{۶۲} یک تکنالوژی مبتنی بر استاندارد است که می تواند به عنوان یک جایگزین برای سرویس های Broadband سیمی (ارتباطات cable یا DSL)، به راحتی دسترسی Last-mile را فراهم آورد.

یاد داشت: اصطلاح Last-mile برای ارتباطات و صنایع تکنولوژی، برای تعریف تکنالوژی ها و پروژه های مورد استفاده برای برقراری ارتباط بین مشترکین نهایی و شبکه های ارتباطی به کار می رود.

تکنالوژی WiMax در یک سلول معمولی با شعاع ۳ تا ۱۰ کیلومتر، با ظرفیت پهنای باند ۴۰ Mbps به ازای هر channel فراهم می کند. این پهنای باند کفایت تا صدها لینک تجاری با سرعت اتصال T۱ و هزاران مشتری عادی با سرعت اتصال DSL، به صورت همزمان پشتیبانی می کند.

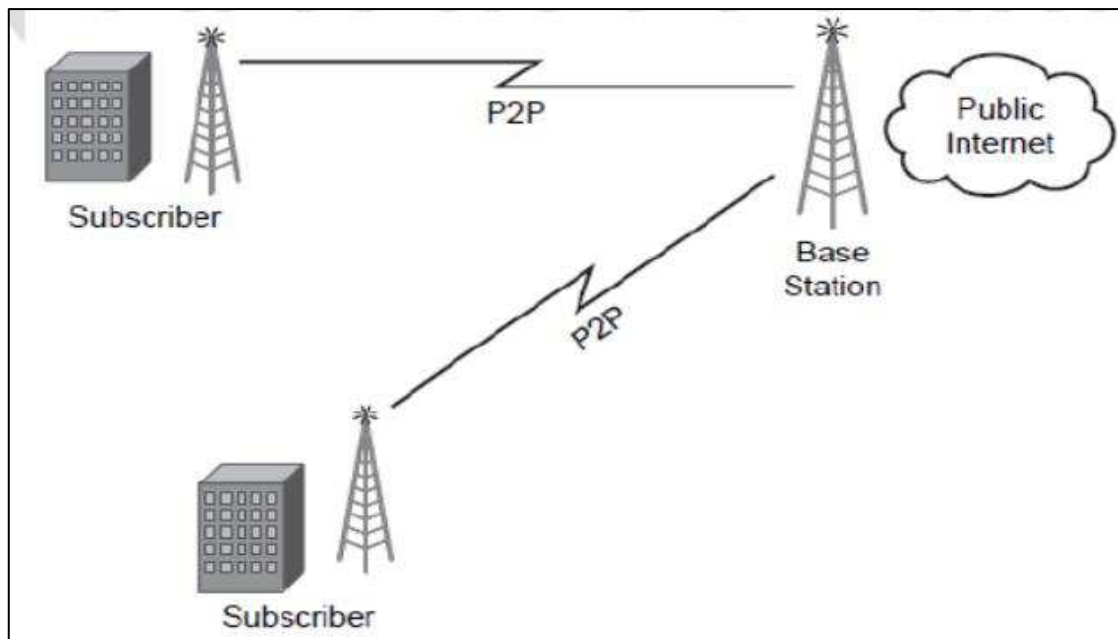
برخی از فراهم کنندگان سرویس (SP)، از این تکنالوژی به عنوان جایگزینی برای DSL یا Cable Modem استفاده می کنند. محدوده سیگنال در این سناریوی Non-LOS حدود ۳ تا ۴ مایل است و اندازه دیتا هم حدود ۳۰ Mbps است. اما گاهی کم تر در حدود ۱۵ Mbps نیز می شود.

اما حالت دید مستقیم (LOS WiMax^{۶۳}) که بیش تر مربوط شبکه T۱ قدیمی است، سرعت دیتا در حدود ۳۰ تا ۷۰ میگابایت در ثانیه و به صورت واقعی ۴۰ میگابایت در ثانیه است. این سناریو در واقع یک

^{۶۲}Worldwide Interoperability for Microwave Access

^{۶۳} Line of Site

توپولوژی نقطه به نقطه^{۶۴} است و سرویس‌های Backbone یا Backhaul را فراهم می‌کند. جزئیات را در شکل ۱۷-۲ مشاهده نمایید.



شکل ۱۷-۲: استفاده از تکنولوژی WiMax با سناریوی LOS

تکنولوژی WiMax در باند فرکانسی ۱۰ GHz تا ۶۶ GHz فعالیت می‌کند. لذا هیچ تداخلی با WLAN و تکنالوژی ۸۰۲.۱۱ ندارد.

۲.۵.۱ ویژگی‌های مهم تکنالوژی WiMax

ویژگی‌های اساسی WiMax قرار ذیل است:

۱. پوشش طولانی در شبکه ؛
۲. عدم نیاز LOS بین استفاده کننده‌گان، در صورت LOS فاصله قابل افزایش است ؛
۳. پهنای باند بالا (درحدود ۷۰ Mbps که تا ۱۰۰ Mbps نیز قابل افزایش است) ؛
۴. امکان پیاده سازی شبکه WiMAX در هر دو باند فرکانسی Licensed و Unlincense ؛
۵. تجهیزات گران قیمت در طراحی و پیاده سازی شبکه ؛
۶. امکان پیاده سازی شبکه با فریکانس‌های ۱۰-۶۶ GHZ و ۱۱-۲ GHZ ؛
۷. پهنای باند قابل تنظیم.

^{۶۴} Point-to-Point

۲.۵.۲ قابلیت‌های فنی WiMax

قابلیت‌های فنی WiMax قرار ذیل است:

۱. با محدوده فرکانسی بالاتر از ۱۰ GHZ ؛
۲. پهنای باند از ۲۰ GHz تا ۱۰۵ GHz ؛
۳. نرخ تبادل اطلاعات تا ۷۰ مگابایت در ثانیه ؛
۴. امکان تحت پوشش قراردادن منطقه وسیع به شعاع ۵۰ کیلومتر توسط هر ایستگاه ؛
۵. قابلیت سازگاری با سایر تکنولوژی‌های بی‌سیم مانند Wi-Fi ؛
۶. توانایی پشتیبانی از توپولوژی‌های تحت استاندارد IEEE مانند Token Ring و نیز توپولوژی‌های خارج از استاندارد مانند LLC.

۲.۵.۳ مزایای WiMax

۱. کیفیت سرویس بالاتر نسبت به سایر تکنولوژی‌ها ؛
۲. کارایی بالاتر با امکان تداخل کمتر ؛
۳. ساختار استاندارد IEEE ؛
۴. پشتیبانی از آنتن‌های هوشمند ؛
۵. حذف کیبل‌کشی‌های طولانی ؛
۶. صرفه جویی در هزینه‌های توسعه و نگهداری شبکه ؛
۷. قابلیت اتصال به خطوط کیبلی DSL و T۱/E۱ ؛
۸. امکان سرویس‌دهی به مشترکین ثابت و سیار ؛
۹. کمتر شدن قطعی‌های مکرر نسبت به سایر روش‌های اتصال به اینترنت.

۲.۶ معرفی تکنالوژی ۳G

نسل اول شبکه‌های تلفن همراه (۱G) انالوگ بود که حدود ۳۰ سال پیش به دنیا معرفی شد، این شبکه تنها مکالمات تلفنی مشترکان را منتقل می‌کرد. نسل دوم شبکه‌های تلفن همراه (۲G) که یک دهه بعد جای‌گزین نسل قبلی شد، دیجیتال بود که علاوه بر مکالمات تلفنی، امکان تبادل برخی اطلاعات ساده، نظیر پیامک و ایمیل را نیز داشت. در نسل سوم شبکه تلفن همراه (۳G) حدود سال‌های ۱۳۸۰ و ۱۳۸۱ به میدان آمدند. این تکنالوژی امکان وب‌گردی، گفت‌گوی تصویری و نیز پخش زنده محتوای چند رسانه را فراهم می‌کند. به عبارت دیگر نسل سوم شبکه تلفن همراه، روشی برای انتقال اطلاعات در تلفن‌های همراه و سیستم‌های بدون سیم می‌باشد. نسل جدید شبکه موبایل با رویکرد مولتی‌مدیا می‌باشد. تکنالوژی ۳G

برخلاف GSM که نسلی برای انتقال صدا و اطلاعات بود، با سرعت بالا برای انتقال چند رسانه^{۶۵} مساعد است.

وقتی صحبت از ۴G ویا ۳G می‌شود G مخفف Generation یا نسلی از تکنولوژی شبکه‌های بی‌سیم است، با گذشت زمان، در هر یک از این نسل‌ها سرعت دسترسی به اینترنت به صورت چشم‌گیری افزایش یافته است، اما سرویس ارائه شده در هر نسل با نسل قبلی سازگاری ندارد و برای استفاده از آن باید گوشی و ابزارهای خود را ارتقا دهیم و سرویس دهنده‌ها نیز باید سخت‌افزارهای جدیدی را نصب نمایند.

اولین کشوری که از شبکه ۳G به صورت گسترده و تجاری استفاده کرد، جاپان بود. در اولین روز اکتبر سال ۲۰۰۱ بزرگ‌ترین شرکت مخابراتی جاپان (ان تی تی) خدمات مخابراتی خود را به نسل سوم مجهز کرد. بالاخره از سال ۲۰۰۵ شبکه‌های نسل سوم ضریب نفوذ خود را افزایش دادند [۷].

در نسل سوم همه چیز در قالب اطلاعات رقمی (دجیتلی) منتقل می‌شود. امکانات از قبیل تلفن‌های تصویری بی‌سیم، با کیفیت مناسب به خوبی امکان پذیر است. حد اکثر سرعت در ۳G به ۴۲ مگابایت در ثانیه می‌رسد.

این افزایش سرعت به دلیل تکنولوژی نسل سوم موبایل است.

شبکه موبایل ۳G، جای‌گزین شبکه موبایل ۲G شده است. در ۲G گوشی‌های موبایل فقط توانایی‌های مانند مکالمه، ارسال پیام کوتاه و اندکی هم تبادل دیتا مانند MMS دارند. نسل سوم سرعت تبادل اطلاعات و فرمت‌های انتقال اطلاعات را توسعه داد و به عنوان مثال می‌توان، روی گوشی موبایل صفحات وب را بازدید کرد، ویدیو را دانلود کرد و به موسیقی گوش داد. روی شبکه‌های نسل سوم سرعت اینترنت هنوز کند است و نسبت به شبکه‌های بی‌سیم، صفحات وب و دیتا خیلی آهسته بارگذاری می‌شوند و نا امیدکننده هستند؛ ولی در مقایسه با استاندارد ۲G سریع‌تر است. در حال حاضر، سیستم مخابراتی بسیاری کشورها از نسل سوم پشتیبانی می‌کنند و می‌توانیم از اینترنت روی گوشی موبایل خویش استفاده کنیم. گوشی‌های تلفن همراه جدیدی که در بازار هست نیز بدون شک از نسل سوم پشتیبانی می‌کنند.

تکنالوژی نسل سوم یک تکنالوژی ارتباطی سیار است. با استفاده از تکنولوژی نسل سوم، می‌توانیم سرعتی ۲ مگابایت در ثانیه برای دسترسی به شبکه و خدمات اینترنت در حال سکون یا در حالت حرکت، سرعتی تا ۳۸۴ کیلوبایت در ثانیه و در موتور سرعتی حدود ۱۲۸ کیلوبایت در ثانیه داشته باشیم.

فناوری ۳G شرکت‌های مخابراتی را قادر می‌سازد تا به استفاده کنندگان خویش سرویس‌های وسیع و پیش‌رفته را همراه با افزایش ظرفیت و بهبود کارایی ارائه دهند. این خدمات می‌تواند شامل برقراری ارتباط صوتی بی‌سیم در مناطق وسیع و پهنای باند وسیع برای جابجایی اطلاعات در مناطق تحت پوشش با سرعتی

^{۶۵} Multimedia

حدود ۵ تا ۱۰ مگابایت در ثانیه باشد. همچنین ایجاد ارتباط تصویری و ویدیویی از دیگر مواردی است که روی این تکنولوژی در نظر گرفته شده است.

مهم‌ترین ویژگی‌های تکنولوژی ۳G

۱. افزایش ایمنی ارتباطی نسبت به نسل‌های قبلی؛
۲. افزایش پهنای باند دسترسی به اینترنت برای کاربران (نسل سوم تا ۲۱ مگابایت در ثانیه)؛
۳. افزایش کیفیت و خدمات قابل ارائه؛
۴. کاهش تاخیر ارتباط؛
۵. انتقال اطلاعات با کیفیت بهتر؛
۶. امکان تبدیل گوشی تلفن همراه با قابلیت انجام کلیه عملیات بانکی؛
۷. امکان توسعه آموزش مجازی در نقاط مختلف کشور بر اساس اینترنت؛
۸. امکان دریافت و مشاهده برنامه‌های تلویزیونی از طریق تلفن همراه با کیفیت فوق العاده؛
۹. امکان ارائه محتواهای صوتی و تصویری متنوع با کیفیت بالا.

خدمات ۳G

۱. اتصال به شبکه اینترنت با سرعت و قابلیت اطمینان بالا و در حین حرکت؛
۲. برقراری تماس تصویری؛
۳. دانلود ویدیو، امکان دریافت کلیپ‌های تصویری بر روی گوشی تلفن همراه؛
۴. امکان دریافت تصاویر تلویزیونی بر روی گوشی‌های تلفن همراه؛
۵. توانایی تبادل حجم انبوهی از اطلاعات؛
۶. دسترسی آسان‌تر به برنامه‌های کاربردی (app ها)؛
۷. شرکت در گیم‌های آنلاین.

۲.۷ معرفی تکنولوژی ۴G

تکنولوژی ۴G چهارمین و جدیدترین نسل از تکنولوژی‌های مخابراتی برای ارسال و دریافت اطلاعات از طریق شبکه‌های موبایل است. این تکنولوژی برحسب بعضی مشکلات نسل سوم و افزایش قابلیت‌های جدید عرضه گردیده است.

تکنولوژی ۴G بیش‌تر برای کسانی که موبایل‌های هوشمند، تبلت و لپ‌تاپ دارند، مناسب است. برای کسانی هنگامی که خارج از محدوده پوشش Wi-Fi هستند، با سرعت بالا برای استفاده از صفحات وب، استفاده از اپلیکیشن‌ها و کار با ایمیل، نهایت سهولت را فراهم می‌کند. مثلاً وقتی موتر در حال حرکت هستند، ۴G می‌تواند سرعتی یک‌سان یا حتی بالاتر نسبت به Wi-Fi یا در دفتر و منزل فراهم کند. در هتل‌ها و میدان‌های هوایی نیز ۴G اغلب سریع‌تر از Wi-Fi به‌صورت هم‌گانی مستقر و قابل استفاده است.

۲.۷.۱ فرق ۴G با LTE

تکنالوژی LTE برگرفته از Long Term Evolution یعنی با شعار تکامل بلند مدت نیز در دنیال تکنالوژی قدم گذاشته است. البته این تکنالوژی سریع‌ترین و باثبات‌ترین نوع از ۴G به حساب می‌آید. و به اعتقاد اکثر کارشناسان فنی و مسلکی؛ نزدیک‌ترین تکنالوژی به استانداردهای تعیین شده از طرف سازمان ملل است. LTE در ابتدا توسط Verizon به کار گرفته شد، که آن را در ۲۰۰ منطقه ارائه کرد. شرکت AT&T نیز استفاده آن را شروع و خدمات آن را عرضه کرده است. Sprint و T-Mobile نیز در حال چرخش به سمت استفاده از LTE هستند، که البته هنوز هیچ شهری را تحت پوشش آن قرار نداده اند.

۲.۷.۲ سرعت ۴G

ادعاها و البته تست‌های عمل کرد، بستگی به نوع دستگاه، موقعیت مکانی، و زمانی دارند. در بسیاری از تست‌ها، تلفن‌های ۴G، تبلت‌ها، و مودم‌های لپ‌تاپ‌ها، به‌طور کلی سرعتی از ۳ تا ۲۰ برابر سرعت دانلود دستگاه‌های ۳G را رقم زده‌اند. LTE پادشاه سرعت در بین تکنالوژی‌های ۴G است. دستگاه‌های LTE که تست شده‌اند، به‌طور میان‌گین سرعت دانلودی بین ۱۰ تا ۲۰ مگابایت در ثانیه را داشته‌اند، که به تکرار به بالای ۳۰ مگابایت در ثانیه هم رسیده است. سایر انواع ۴G، عموماً سرعت‌های دانلودی زیر ۱۰ مگابایت در ثانیه را در تست‌ها رقم زده‌اند. ولی تمام آن‌ها بهتر از ۳G بوده‌اند. سرعت دانلود با استفاده از ۳G، در تست‌ها بر روی تمام شبکه‌ها و تعداد زیادی از دستگاه‌ها، به‌طور میان‌گین زیر ۲ مگابایت در ثانیه بوده است.

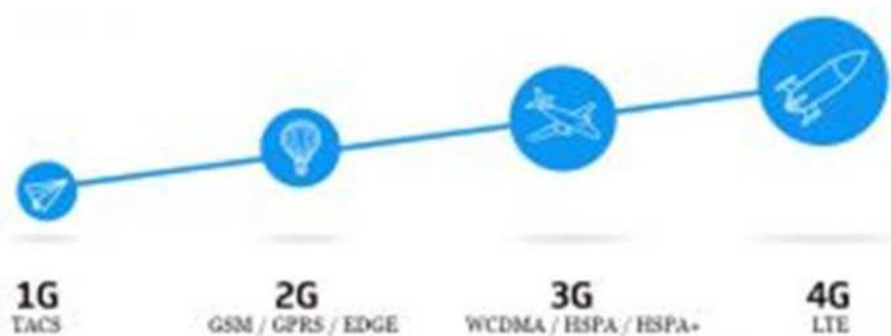
۲.۷.۳ مزیت‌های ۴G

- زمانی که شبکه‌های نسل چهارم، به شبکه‌های تلفن همراه امروزی متصل شدند و سرعت حداقلی ارتباط شما چیزی برابر با ۵۴ مگابایت در ثانیه شد.
- شما می‌توانید به راحتی نرم افزارهای مورد نظر خود را از اینترنت دانلود و نصب نمائید.
- شما می‌توانید سرویس آنلاین از قبیل تلویزیون‌های اینترنتی، اسکایپ، VOIP... استفاده نموده و از بهترین کیفیت صدا و تصویر مستفید شوید.
- این تکنالوژی به‌طور اوسط ۱۰۰ Mbps دیتا، برای کاربران موبایل همراه فراهم می‌کند.

۲.۷.۴ انواع باند و طیف‌های ۴G

باندهای متفاوتی در شبکه ۴G وجود دارد، که کمی پیچیده می‌شود. یکی از باندها ۲.۶GHz سریع‌ترین، به دنبال آن ۱GHz و ۸۰۰MHz هستند. در حالی که ۸۰۰MHz امکان ظرفیت‌های دیتا مشابه به اندازه باندهای سریع ۴G را ندارد. این باند برای طی مسافت‌های طولانی و همچنین نفوذ به دیوارها مناسب‌تر است و سیگنال بهتری را در محیط‌های بسته فراهم می‌کند.

لازم است بگویم 1G، 2G، 3G، 4G، 5G و ... همه نسل‌های مختلف تکنالوژی ارتباطات بی‌سیم هستند که با توجه به سرعت و ساحت پوشش فاصله دسته بندی شده اند.



مقایسه تکنالوژی‌های ارتباطی 1G، 2G، 3G و 4G [۷]

جدول زیر جهت فهم بیشتر و مقایسه دو تکنالوژی 3G و 4G در نظر گرفته شده است. قسمی که در این جدول ملاحظه می‌شود، از لحاظ سرعت، فریکونسی، پهنای باند، روش ارسال اطلاعات و تکنالوژی‌های قابل دسترس مقایسه گردیده است. در این جدول تفاوت‌های اساسی و مهم در سرعت، پهنای باند و روش ارسال اطلاعات دیده می‌شود. سرعت نسل سوم، حد اکثر 2 میگابایت در ثانیه؛ در حالی که سرعت نسل چهارم 100 میگابایت در ثانیه شناسایی گردیده است. حداکثر پهنای باند در نسل سوم، 20MHz و در نسل چهارم حد اکثر به بیش‌تر از 100MHz گفته شده است. روش ارسال اطلاعات در نسل سوم، ایجاد شرکت و هم‌چنان آدرس دهی هر بسته (بسته بندی) است. در حالی که نسل چهارم براساس بسته بندی صوتی براساس مطلق دیجیتال عمل می‌کند. جزئیات این تفاوت‌ها را در جدول زیر مشاهده نمایید.

Requirement	3G	4G
Speed	384Kbps to 2 Mbps	20 to 100 Mbps
Frequency Band	Dependent on Country	HFB (2-8 GHz)
Bandwidth	5-20 MHz	100 MHz or more
Switching Design Basis	Circuit & Packet	All Digital with packetized voice
Access Technologies	W-CDMA	OFDM & MC-CDMA

جدول مقایسه 3G با 4G [۷]

۲.۸ تکنالوژی Li-Fi

یک تکنالوژی نو ظهور بی‌سیم نوری است که در آن به جای امواج رادیویی از نور یا طیف مرئی برای انتقال اطلاعات استفاده می‌شود. برای اولین بار در فضاهای کاری آزمایش شده است و در آینده به عنوان جای‌گزین و پشتیبان شبکه بی‌سیم (Wi-Fi) برای ارتباطات داخلی مفید باشد زیرا می‌تواند نرخ انتقال دیتا با ظرفیت بالا را برای استفاده کننده فراهم کند. واژه Li-Fi مخفف light fidelity به معنی وفاداری جهت انتقال اطلاعات توسط نور است. این نام اولین بار از سوی پروفسور Harald Haas استاد دانشگاه

ادینبورگ اسکاتلند در سال ۲۰۱۱ مورد استفاده قرار گرفت. آقای هاس آینده را پیش‌بینی کرد که در آن میلیارد ها لامپ نقش پخش کننده اینترنت بیسیم را ایفا می‌کنند. Li-Fi انتقال داده ها را از طریق نور ارسال می‌کند و با ارسال اطلاعات از طریق یک چراغ لامپ LED انجام می‌شود.

یکی از مزایای اصلی لای فای این است که برخلاف وای فای تداخل الکترومغناطیسی ندارد چون اصلاً طیف‌شان باهم فرق دارد. به همین دلیل دچار تداخل نمی‌شود و به همین دلیل می‌تواند در اکثر جاها که تداخل امواج مسئله‌ی جدی است استفاده شود. در حالی که طیف امواج رادیویی در جهان به سرعت در حال پرشدن است، طیف امواج مرئی یا نور ۱۰ هزار بار بزرگ‌تر است و به این زودی‌ها به مشکل روبرو نخواهد شد. مزیت‌های دیگر عبارت است از سرعت معادل ۱۰۰ گیگابیت در ثانیه، امنیت بیشتر، مصرف انرژی کمتر و بازدهی بیشتر و عدم مضر بودن آن به بدن انسان می‌باشد.

در مورد معایب LiFi می‌توان گفت مهم‌ترین محدودیت این است که نور باید در جهت مناسب تابانیده شود و دستگاه نباید مسیر نور را از دست بدهد چون برای دسترسی به اینترنت هم باید نور باشد و هم آن نور باید مستقیم و در جهت درستی بتابد. مشکل بعدی این است که سانسورهای دریافت نور 66 در صورت که نور بیرونی زیاد باشد نمی‌توانند نور حامل اینترنت را به درستی حس کنند، مثلاً در نور زیاد آفتاب این مسئله می‌تواند مشکل ساز باشد.

موارد یاد شده مشکلات فعلی هستند شاید یک یا چند سال دیگر یک تعداد این مشکلات یا همه این مشکلات حل شود.



در این فصل تحت عنوان "تکنالوژی‌های شبکه بی‌سیم" به موضوعات بسیار مهم و اساسی شبکه‌های بی‌سیم پرداخته شد. وقتی خواسته باشیم که تکنالوژی‌های شبکه بی‌سیم را به دقت یاد بگیریم و یا تفاوت‌ها و مزیت‌ها را نسبت به هم‌دیگر آن شناسایی کنیم، بهتر است موضوعات اساسات بی‌سیم را بدانیم. به صورت عموم در این فصل دو بخش عمده توضیح گردید.

در ابتدا اساسات شبکه‌های بی‌سیم را به خوبی یاد گرفتیم و زمینه یادگیری تکنالوژی‌های شبکه بی‌سیم فراهم شد. عناوین مهم که در بخش اساسات شبکه بی‌سیم بحث گردید؛ بحث نظری امواج الکترومقنطسی، فریکانس‌های رادیویی، طول موج، فریکونسی، دامنه موج، ویژگی‌های مهم امواج رادیویی و بالاخره ارتباطات رادیویی است. قابل یادآوری است که بحث امواج الکترومقنطسی، ما و شما را برای یادگرفتن امواج رادیویی (تکنالوژی مورد استفاده شبکه بی‌سیم) آماده می‌کند. امواجی که باعث ارتباطات و انتقال اطلاعات در شبکه‌های کمپیوتری می‌شود؛ امواج رادیویی است. علاوه بر آن در امواج رادیویی موارد استفاده زیاد دارد که جزئیات آن در این فصل توضیح گردیده است. هم‌چنان جهت دانستن مزیت‌ها و مشکلات امواج رادیویی و ویژگی‌های مهم امواج رادیویی بحث گردید. یادگیری خصوصیات امواج رادیویی مهندسان و طراحان شبکه بی‌سیم را قادر می‌سازد تا از مشکلات احتمالی در شبکه جلوگیری کند. این ویژگی‌ها شامل: تضعیف سگنال، تقویه سگنال، انتشار سیگنال، نفع بردن از سگنال^{۶۷}، انعکاس، انکسار، طول موج، فریکونسی و غیره موارد دیگر است.

در بخش دوم این فصل، تکنالوژی‌های شبکه بی‌سیم مورد بحث قرار گرفت. این تکنالوژی‌ها شامل: تکنالوژی بلوتوت، تکنالوژی ZigBee، تکنالوژی WiMax، مزایای WiMax، تکنالوژی 3G، تکنالوژی 4G کارکردها و موارد استفاده هرکدام توضیح گردید. مقایسه تکنالوژی 4G با تکنالوژی جدید LTE نیز واضح گردید. از طرف دیگر مقایسه تکنالوژی‌های فوق در جدول به صورت واضح بیان گردید. تفاوت‌های عمده این تکنالوژی‌ها در پهنای باند، سرعت و فاصله است. به عنوان مثال سرعت 3G حد اکثر به 2Mbps و سرعت 4G حداکثر به 100Mbps می‌رسد. پهنای باند در 3G علاوه بر محدودیت تکنالوژی به کشورهای مختلف نیز بستگی دارد، درحالی‌که پهنای باند در 4G بیش‌تر از 100MHz می‌رسد. تاحالا بهترین تکنالوژی در فاصله‌های دور 4G شناسایی شده است. این تکنالوژی با باند 800MHz برای فاصله‌های دور نهایت موثر و قابل استفاده است.

^{۶۷}Gain



سوالات فصل دوم

۱. تکنالوژی‌های شبکه بی‌سیم را نام بگیرید.
۲. تفاوت عمده و اساسی تکنالوژی ۴G با ۳G را بیان کنید.
۳. ویژگی‌های امواج رادیویی را تنها نام بگیرید.
۴. انتشار امواج رادیویی چگونه اتفاق می‌افتد؟
۵. انعکاس در امواج رادیویی، در شبکه‌های بی‌سیم چه تاثیر منفی دارد؟
۶. رابطه طول موج و فریکونسی را بیان کنید.
۷. تاثیر دامنه، در امواج رادیویی چیست؟
۸. تغییرساحه مقناطیسی، ساحه برقی را ایجاد می‌کند؛ لذا تداوم امواج رادیویی چگونه اتفاق می‌افتد؟
۹. موارد استفاده تکنالوژی ZigBee را بیان کنید.
۱۰. مزایای تکنالوژی WiMax را بیان کنید.
۱۱. قابلیت‌های تخنیکی تکنالوژی WiMax را بیان کنید.

فصل سوم

معرفی استانداردهای شبکه بی سیم



هدف کلی: با استانداردهای رایج شبکه‌های بی سیم آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. استانداردهای Wi-Fi را معرفی کرده بتوانند.
۲. استاندارد IEEE ۸۰۲.۱۱a را توضیح داده بتوانند.
۳. استاندارد IEEE ۸۰۲.۱۱b را توضیح داده بتوانند.
۴. استاندارد IEEE ۸۰۲.۱۱g را توضیح داده بتوانند.
۵. استاندارد IEEE ۸۰۲.۱۱n را توضیح داده بتوانند.
۶. استاندارد IEEE ۸۰۲.۱۱ac را توضیح داده بتوانند.
۷. استانداردهای IEEE ۸۰۲.۱۱a، IEEE ۸۰۲.۱۱b، IEEE ۸۰۲.۱۱g، IEEE ۸۰۲.۱۱n و IEEE ۸۰۲.۱۱xn از لحاظ سرعت، فاصله، فریکونسی مورد استفاده و سازگاری مقایسه کرده بتوانند.
۸. قابلیت‌ها و عمل‌کردهای IEEE ۸۰۲.۱۱ac و IEEE ۸۰۲.۱۱ah را با استانداردهای دیگر را بدانند.

در این فصل در مورد تمام استانداردهای شبکه بی سیم بحث شده است. یادگیری و استفاده از استانداردهای مهم شبکه بی سیم، به ویژه استانداردهای شبکه WLAN یکی از اهداف این فصل است. در این فصل به صورت ویژه استانداردهای شبکه WLAN بسیار کوتاه و جامع معرفی شده است. بحث های مهم در مورد این استانداردها، شامل تفاوت های اساسی استانداردها، سرعت، فریکانس ها، سازگاری های هر استاندارد با استانداردهای دیگر و بقیه نکات مهم است. تفاوت های واقعی و عملی شبکه های بی سیم را با فهمیدن ویژگی ها و روش های عمل کرد آن ها می توانیم درک و شناسایی نماییم. نکته مهم دیگر این است که تمام استانداردهای فوق الذکر به صورت رایگان، یعنی بدون داشتن مجوز در شبکه های WLAN قابل استفاده است. این استانداردها در سخت افزارهای یک شبکه بی سیم قابل استفاده می باشند. به عنوان مثال یکی از سخت افزارهای شبکه بی سیم کارت های شبکه بی سیم (NIC) است که مطابق استانداردهای فوق الذکر امواج رادیویی را ایجاد، منتشر و دریافت می کنند.

شبکه بی سیم با استفاده از امواج رادیویی، زمینه ارتباطات و ایجاد شبکه های کمپیوتری را به صورت بی سیم فراهم می کند. این امواج با فریکانس های متفاوت و طول موج های متفاوت و هم چنان با امپلیتودهای متفاوت انتشار می کند. لذا تمام امواج رادیویی، دارای بعضی ویژگی های است که مطابق استانداردهای لازم در ارتباطات شبکه های بی سیم استفاده می شود. این ویژگی ها جهت تنظیم سرعت، فاصله، طول موج، فریکونسی و غیره مشخصات دیگر توسط سازمان های استاندارد ساز، استاندارد سازی شده است. یکی از سازمان های که در راستای استاندارد سازی نقش مهم و حیاتی دارد، انستیتوت انجمن مهندسان برق، تحت نام IEEE است. سازمان IEEE علاوه بر شبکه های بی سیم، در بخش شبکه های سیمی نیز استانداردهای لازم را ارائه کرده است. این سازمان در عرصه شبکه های بی سیم WLAN، استانداردهای IEEE 802.11 را ارائه کرده است. البته استانداردهای IEEE 802.11 در بخش WLAN، شامل استانداردهای فرعی IEEE 802.11a و IEEE 802.11b و IEEE 802.11g و IEEE 802.11n و IEEE 802.11xn و IEEE 802.11ac و چند استاندارد دیگر می باشند [۱].

۳.۱ معرفی استانداردهای WLAN

در این جا به صورت مختصر به معرفی استانداردهای شبکه بی سیم می پردازیم. هدف از این معرفی، استانداردهای تکنالوژی Wi-Fi است که در شبکه WLAN استفاده می شود. تاحال استانداردهای IEEE 802.11a، IEEE 802.11b، IEEE 802.11g و چند استاندارد دیگر هم راه با فواید و نواقص آن استفاده گردیده است. جهت معلومات جدید خوب است که همیشه به سایت www.WiFi.com مراجعه گردد تا آخرین تغییرات را در بخش شبکه های بی سیم و استانداردهای آن به دست آوریم.

موضوع مهمی که لازم است یادآور شویم، این که: 802.11b با استاندارد جدید که دارای سرعت بالا و خیلی گران قیمت با نام مخفف Wi-Fi5 با 802.11a کار نمی کند. لذا با 802.11b و 802.11g نیز کار کرده نمی تواند. در این جا استاندارد b با g دارای سرعت یک سان است و به هم سازگاری داشته و کار کرده

می‌توانند. اما هیچ‌گاه استاندارد a با b و g کار کرده نمی‌تواند. هدف از این استانداردها قابلیت و کارکرد اکسس پاینت (Access Point) است. در این جا دو نوع از Access Point ها را که تولید کمپنی‌های مختلف است در شکل مشاهده می‌نماییم. شکل ذیل نوعی از Access Point را نشان می‌دهد که تولید کمپنی Proxim-Orinoco است. البته این دستگاه علاوه بر قابلیت‌های access point، قابلیت‌های روتر را نیز دارد [6].

۳.۱.۱ انواع استاندارد ۸۰۲.۱۱ IEEE

استاندارد ۸۰۲.۱۱ IEEE اولین بار در سال ۱۹۹۰ توسط انستیتیوت IEEE معرفی گردید و اکنون تکنالوژی‌های متفاوتی از این استاندارد برای شبکه‌های بی‌سیم ارائه گردیده است.

استاندارد 802.11 برای روش‌های انتقال FHSS (frequency hopping spread spectrum) یا DSSS (direct sequence spread spectrum) با سرعت ۱Mbps تا ۲Mbps با فریکانس ۲.۴GHz قابل استفاده می‌باشد. استانداردهای ۸۰۲.۱۱ شامل استانداردهای ذیل است:

۳.۱.۱.۱ استاندارد ۸۰۲.۱۱a

استاندارد ۸۰۲.۱۱a یکی از استانداردهای است که با فریکانس بالا یعنی ۵GHz فعالیت می‌کند. این استاندارد برای انتقال اطلاعات از روش انتقال OFDM (orthogonal frequency division multiplexing) با سرعت 54Mbps کار می‌کند. آن گونه که قبلاً یادآوری شد، این استاندارد با استانداردهای دیگر مانند 802.11 b و استاندارد 802.11g سازگاری و هماهنگی لازم ندارد. استاندارد 802.11 a دارای حمایت بیش‌تر از 23 کانال^{۶۸} می‌باشد.

۳.۱.۱.۲ استاندارد ۸۰۲.۱۱b

این استاندارد با استفاده از فریکانس ۲.۴GHz دارای سرعت ۱۱Mbps است. این استاندارد به نام Wi-Fi با شعار ۸۰۲.۱۱ High Rate عرضه گردیده و با روش انتقال DSSS کار می‌کند. این استاندارد در شبکه‌های محلی WLAN کاربرد وسیع داشته و حد اقل به تعداد ۳ کانال را حمایت می‌کند و با استانداردهای ۸۰۲.۱۱g سازگاری دارد.

۳.۱.۲ استاندارد ۸۰۲.۱۱g

این استاندارد با فریکانس ۲.۴GHz فعالیت می‌کند. روش انتقال این استاندارد DSSS بوده سازگاری با استاندارد ۸۰۲.۱۱b دارد. سرعت انتقال اطلاعات در این استاندارد بالای ۵۴Mbps می‌رسد. هم‌چنان از لحاظ

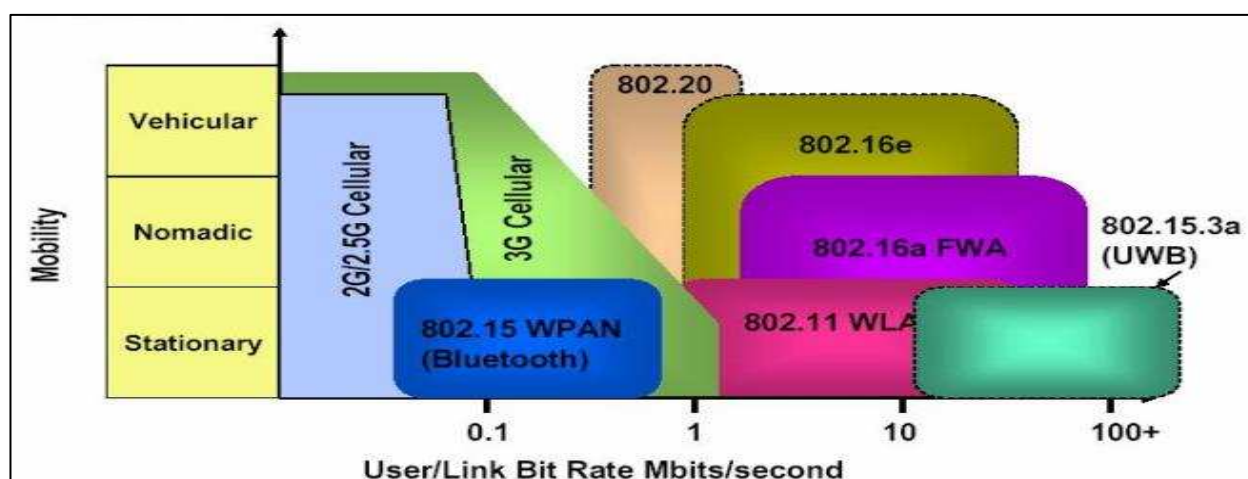
^{۶۸}Channels

کارایی به شکل بهتر و موثرتر عمل می کند؛ لذا در شبکه های محلی WLAN بیشترین استفاده را دارد. استاندارد ۸۰۲.۱۱g قابلیت حمایت و پشتیبانی ۳ کانال را دارد.

۳.۱.۲.۱ استاندارد ۸۰۲.۱۱n

استاندارد n ۸۰۲.۱۱ یکی از استانداردهای جدید است که در سال های اخیر ۲۰۰۹ میلادی در دنیای تکنالوژی مورد استفاده قرار گرفت. این استاندارد ادعای بیش تر از ۶۰۰Mbps سرعت را دارد و با فریکانس ۲.۴GHz و حد اقل با فاصله ۲۵۰ متر قابلیت کارایی دارد.

مطابق شکل ۱-۳ سرعت عمل کرد و برحسب ثانیه و قابلیت سیار بودن استانداردها و تکنالوژی های شبکه بی سیم را نشان می دهد.



شکل ۱-۳: استانداردها و تکنالوژی های شبکه بی سیم از لحاظ قابلیت های سرعت و سیار بودن

۳.۱.۲.۲ استاندارد ۸۰۲.۱۱ac

این استاندارد در سال ۲۰۱۳ یعنی شش سال پس از وای فای n به عنوان وای فای گیگابیتی معرفی شد این پروتکل روی باند ۵ گیگاهرتزی کار می کند و به همین دلیل برای انتقال سریع تر مناسب تر است. این استاندارد از تکنالوژی ارتباط بی سیم دو بانده استفاده می کند. به این ترتیب امکان پشتیبانی همزمان از ارتباطات روی هر دو باند فرکانسی ۲/۴ گیگاهرتز و ۵ گیگاهرتز برای کلاینت فراهم خواهد شد. این در حالی است که در روتر باید از آنتن های جداگانه استفاده کرد ۸۰۲.۱۱ac سازگاری با نسل های قدیمی یعنی ۸۰۲.۱۱b/g/n داشته و پهنای باندی تا ۱۳۰۰ مگابیت بر ثانیه در باند ۵ گیگاهرتز به علاوه پهنای باند ۴۵۰ مگابیت بر ثانیه در باند ۲/۴ گیگاهرتز پشتیبانی می کند.

در این استاندارد از تکنالوژی Multi-User MIMO - استفاده شده است. در این تکنالوژی به وسیله آنتن های هوشمند طیف ارسال و دریافت از چند آنتن به چند آنتن و چند مشترک باعث افزایش ظرفیت انتقال و کاهش تاخیر است.

علاوه بر استانداردهای فوق که یادآوری گردید، استانداردهای دیگر نیز در این سال‌های اخیر در صنعت و تکنالوژی شبکه بی‌سیم به‌میان آمده و معرفی شده است. استانداردهای مهم دیگر عبارت از: ۸۰۲.۱۱y، ۸۰۲.۱۱ad، ۸۰۲.۱۱af، ۸۰۲.۱۱ag، ۸۰۲.۱۱ah و بالاخره استانداردهای ۸۰۲.۱۱ax و استانداردهای ۸۰۲.۱۱ay است که در سال‌های اخیر به‌صنعت تکنالوژی و به‌خصوص به تکنالوژی‌های بی‌سیم اضافه گردیده است. جزئیات بیش‌تر در مورد استانداردهای ۸۰۲.۱۱ در جدول ذیل نشان داده شده است.

جدول ۳-۱: جدول تفاوت و مقایسه بین استانداردهای شبکه بی‌سیم [۱]

Standard	Bandwidth	Frequency	Range	Interoperability
IEEE 802.11a	Up to 54 Mbps	5 GHz band	150 ft (45.7 m)	Not interoperable with 802.11b, 802.11g, 802.11n
IEEE 802.11b	Up to 11 Mbps	2.4 GHz band	300 ft (91 m)	Interoperable with 802.11g
IEEE 802.11g	Up to 54 Mbps	2.4 GHz band	300 ft (91 m)	Interoperable with 802.11b
IEEE 802.11n (Pre - standard)	Up to 540 Mbps	2.4 GHz band	984 ft (250 m)	Interoperable with 802.11b, 802.11g

در جدول ۳-۲ بیش‌تر از استانداردهای مهم را مشاهده می‌نمایید. در این جدول از لحاظ تاریخ نشر استانداردها، فریکانس مورد استفاده در هر فریکانس، ظرفیت اطلاعات، حد اکثر سرعت انتقال و ارسال، فاصله قابل پوشش و ملاحظات و سازگاری‌های هر استاندارد نشان داده شده است.

جدول ۳-۲: جدول مقایسه استانداردهای شبکه بی‌سیم [۴]

Protocol	Release Date	RF Freq.	Through put	Data Rate (Max)	Max Range	Notes & Comments
802.11	1997	2.4 GHz	0.9 Mbps	2 Mbps	Undefined	Legacy
802.11a	1999	5 GHz	23 Mbps	54 Mbps	50m	▪Not compatible with b, g, n ▪Expensive
802.11b	1999	2.4 GHz	4.3 Mbps	11 Mbps	100m	First 2.4 GHz Technology
802.11g	2003	2.4 GHz	19 Mbps	54 Mbps	100m	Backward compatible with b Shares range with b
802.11n	2009*	2.4 & 5 GHz	74 Mbps	248 Mbps	250m	Newest Standard
802.11y	2008*	3.7 GHz	23 Mbps	54 Mbps	5000m	Newest Standard

در جدول ۳-۳ اکثر استانداردهای رایج را با جزئیات بیش‌تر، شامل روش انتقال اطلاعات، سال نشر، تعداد کانال‌های^{۶۹} قابل حمایت، سرعت و ظرفیت، فریکانس، فاصله پوشش به‌صورت تخمینی و غیره موارد دیگر را به وضاحت نشان می‌دهد. حتی بعضی استانداردهای که درحال حاضر روی آن در صنعت تکنالوژی کار ادامه دارد و قرار است در آینده‌ها ساخته شود، مانند: ۸۰۲.۱۱aZ برای سال‌های ۲۰۲۱ به صورت تخمینی نیز بیان شده است.

جدول ۳-۳: مقایسه استانداردهای جدید و پیش‌بینی‌های آینده در مورد شبکه بی‌سیم [۹]

Protocol [\[edit\]](#)

802.11 network PHY standards [hide]								
802.11 protocol	Release data ^[6]	Fre-quency	Band-width	Stream data rate ^[7]	Allowable MIMO streams	Modulation	Approximate range ^[citation needed]	
		(GHz)	(MHz)	(Mbit/s)			Indoor	Outdoor
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20 m (66 ft)	100 m (330 ft)
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35 m (115 ft)	120 m (390 ft)
		3.7 ^[A]						5,000 m (16,000 ft) ^[A]
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35 m (115 ft)	140 m (460 ft)
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	38 m (125 ft)	140 m (460 ft)
n	Oct 2009	2.4/5	20	Up to 288.8 ^[B]	4	MIMO-OFDM	70 m (230 ft)	250 m (820 ft) ^[B]
			40	Up to 600 ^[B]				
ac	Dec 2013	5	20	Up to 346.8 ^[B]	8		35 m (115 ft) ^[B]	
			40	Up to 800 ^[B]				
			80	Up to 1733.2 ^[B]				
			160	Up to 3466.8 ^[B]				
		0.054-0.79 ^[C]	6-8	Up to 568.9 ^[10]	4			
ad	Dec 2012	60	2,160	Up to 6,757 ^[11] (6.7 Gbit/s)	N/A	OFDM, single carrier, low-power single carrier	3.3 m (11 ft) ^[12]	
ah	Dec 2016	0.9	1-16	Up to 347 ^[13]	4	MIMO-OFDM		
aj	Est. Jul 2017	45/60						
ax	Est. Dec 2018	2.4/5		Up to 10.53 Gbit/s		MIMO-OFDM		
ay	Est. Nov 2019	60	8000	Up to 20,000 (20 Gbit/s) ^[14]	4	OFDM, single carrier,	10 m (33 ft)	100 m (328 ft)
az	Est. Mar 2021	60						
802.11 Standard rollups								
802.11-2007	Mar 2007	2.4, 5		Up to 54		DSSS, OFDM		
802.11-2012	Mar 2012	2.4, 5		Up to 150 ^[B]		DSSS, OFDM		
802.11-2016	Dec 2016	2.4, 5, 60		Up to 866.7 or 6,757 ^[B]		DSSS, OFDM		

A1

A2

IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5,000 m. As of 2009, it is only being licensed in the United States by the FCC.

B1

B2

B3

B4

B5

B6

Based on short guard interval; standard guard interval is ~10% slower. Rates vary widely based on distance, obstructions, and interference.

C1

IEEE 802.11af about using white space spectrum for WiFi based on the PHY layer of 802.11ac

⁶⁹Channels



در این فصل جهت یادگیری و استفاده موثر از شبکه‌های بی‌سیم، موضوعات استانداردهای شبکه بی‌سیم بحث گردید. علاوه بر توضیح استانداردهای شبکه بی‌سیم، مکانیزم و روش‌های استانداردسازی، سازمان‌های استاندارد ساز را نیز معرفی نمودیم.

موضوعات مهمی که در این فصل بیان گردید، معرفی استانداردهای شبکه بی‌سیم، انواع استانداردهای شبکه بی‌سیم شامل: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11y, IEEE 802.11ac می‌باشد. هر استاندارد دارای ویژگی‌های مهم و منحصر به فرد خود می‌باشد. همه استانداردهای فوق‌الذکر از لحاظ سرعت، باند، پهنای باند، فریکوانسی، فاصله و روش انتقال اطلاعات متفاوت است. بنا بر این، در این فصل تمام تفاوت‌ها و ویژگی‌های این استانداردها، به‌صورت جزئی بیان گردیده است. نکته مهم دیگر این است که هدف ما در این کتاب بیش‌تر استفاده از تکنالوژی‌های WLAN است. لذا استانداردهای مهم و قابل استفاده شبکه WLAN را بیان نمودیم. تفاوت‌های عمده و اساسی این استانداردها از لحاظ سرعت، سیار بودن، روش انتقال اطلاعات و فاصله قابل پوشش است. از طرف دیگر دانستیم که تمام این استانداردها از امواج رادیویی، جهت ارائه خدمات شبکه‌یی استفاده می‌کند. این امواج با فریکانس‌های مختلف، طول موج متفاوت، پهنای باند، دامنه و روش ارسال اطلاعات متفاوت زیر نظر سازمان IEEE استاندارد سازی شده است. استاندارد سازی شبکه WLAN، با شماره یازده (IEEE 802.11) نام‌گذاری شده است. هم‌چنان در این فصل فهمیدیم که شبکه Wi-Fi یکی از استانداردهای IEEE 802.11 است. در اخیر شماره یازده با زیر مجموعه‌های استاندارد 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac و غیره مسمی گردیده است. امروزه جدیدترین استانداردهای شبکه WLAN به‌نام 802.11ac است که از موثریت و توانایی‌های خوبی برخوردار است.



سوالات فصل سوم

۱. استانداردهای شبکه بی سیم را نام بگیرید.
۲. اهمیت استانداردها در شبکه‌های بی سیم چیست؟
۳. فرق بین استاندارد IEEE 802.11a با IEEE 802.11b در چیست؟
۴. فرق بین استاندارد IEEE 802.11g با IEEE 802.11b در چیست؟
۵. فرق استاندارد IEEE 802.11ac با استانداردهای دیگر در چیست؟
۶. شبکه Wi-Fi با استفاده از کدام استانداردها کار می کند؟
۷. شبکه بلوتوث با استفاده از کدام استانداردها کار می کند؟
۸. شبکه ad-hoc با استفاده از کدام استانداردها کار می کند؟
۹. شبکه WLAN با استفاده از کدام استانداردها کار می کند؟
۱۰. از لحاظ سرعت کدام یکی از استانداردها بهتر عمل می کند؟
۱۱. از لحاظ فاصله کدام استانداردها بهتر عمل می کند؟
۱۲. روش انتقال اطلاعات OFDM چگونه یک روش است؟
۱۳. روش انتقال اطلاعات DSSS چگونه یک روش است؟
۱۴. تفاوت دو روش انتقال اطلاعات OFDM و DSSS را بیان کنید.
۱۵. هدف از ناسازگاری بین دو استاندارد چیست؟ مفهوم را ارائه می کند؟

فصل چهارم

نحوه تنظیم اکسس پاینت و روترهای بی سیم



هدف کلی: با نحوه تنظیم و عیارسازی اکسس پاینت و روترهای بی سیم آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. با انواع اکسس پاینت‌ها آشنایی داشته باشند.
۲. آدرس IP اکسس پاینت شبکه خود را بدانند.
۳. از طریق کمپیوتر به شکل سیمی و بی سیم به اکسس پاینت وصل شده بتوانند.
۴. نام شبکه خود را تغییر داده بتوانند.
۵. انواع استانداردهای شبکه بی سیم را انتخاب و یا تغییر داده بتوانند.
۶. تنظیمات اکسس پاینت را از حالت پیش فرض به حالت دل خوا تغییر داده بتوانند.
۷. خدمات DHCP را فعال و غیر فعال بتوانند.
۸. تنظیمات LAN و WAN را با جزئیات آن انجام داده بتوانند.
۹. حداقل دو اکسس پاینت را بین هم به روش Bridging ارتباط داده بتوانند.
۱۰. در محیط روترهای بی سیم خدمات مسیریابی ثابت را فعال کرده بتوانند.
۱۱. تنظیمات DDNS را انجام داده بتوانند.
۱۲. تنظیمات ساحه پوشش اکسس پاینت را نظر به فاصله انجام داده بتوانند.

۴.۱ معرفی اکسس پاینت

اکسس پاینت یا نقطه دسترسی بی سیم، وسیله‌ای است که در شبکه کامپیوتری بی سیم، به دستگاه‌های مجهز به تکنالوژی اجازه می‌دهد تا به عضویت شبکه بی سیم درآمده و با سایر دستگاه‌ها و شبکه‌ها ارتباط برقرار کند. تکنالوژی‌های مورد استفاده بی سیم؛ مانند: Wi-Fi و بلوتوث، با پروتکل‌های مرتبط است که زمینه ارتباط دستگاه‌ها را به صورت بی سیم فراهم می‌کند. جهت اتصال اکسس پاینت به اینترنت و یا شبکه‌های جهانی، اکثراً این دستگاه را به روتر وصل می‌کنند. از طرف دیگر با این اتصال، ارتباط بین شبکه‌های بی سیم و سیمی برقرار می‌شود. این نوع دستگاه‌ها، امروزه از فرکانس‌های رادیویی، استانداردهای بی سیم جهت دریافت و ارسال دیتاها پشتیبانی می‌شود. جهت سازگاری و هم‌آهنگی، تمام این استانداردها توسط سازمان IEEE تعیین و تأیید شده‌اند. استانداردهای که اکسس پاینت‌ها و روترهای بی سیم استفاده می‌کنند از استاندارد ۸۰۲.۱۱ استفاده می‌کنند.

وظیفه اکسس پاینت را به زبان ساده می‌توان گفت که، مانند یک آنتن کار می‌کند و دستگاه‌های بی سیم باید برای برقراری ارتباط با سایر دستگاه‌ها و لوازم دیگر به آن وصل شوند.

اکسس پاینت بی سیم، به نام WAP^{۷۰} نیز یاد می‌شود. این دستگاه یکی از دستگاه‌های سخت‌افزاری است که امکانات اتصال دستگاه‌های Wi-Fi را به شبکه‌های سیمی فراهم می‌کند. اکسس پاینت‌ها معمولاً به صورت دستگاه مستقل، از طریق سوئیچ یا دستگاه‌های دیگر به روتر متصل می‌شوند؛ اما برخی از اکسس پاینت‌ها، دارای قابلیت‌های روتر یعنی مسیریابی را نیز دارند که به نام روترهای بی سیم یاد می‌شوند. اکسس پاینت‌ها، و سیله متفاوت با hotspot می‌باشند. زیرا hotspot محل فیزیکی محسوب می‌شود که در آن دسترسی Wi-Fi به یک شبکه محلی WLAN امکان پذیر است.

۴.۲ تنظیمات اکسس پاینت

برای تنظیمات اکسس پاینت، باید کامپیوتر خود را به اکسس پاینت وصل کنیم. روش وصل کردن یک کامپیوتر به اکسس پاینت جهت عیار سازی به دو حالت زیر صورت می‌گیرد.

حالت اول: از طریق ارتباط^{۷۱} بی سیم، کامپیوتر خود را به اکسس پاینت وصل کنیم و از طریق این کامپیوتر اکسس پاینت مورد نظر را عیار سازی نمائیم.

حالت دوم: توسط کیبل، کامپیوتر خود را به اکسس پاینت وصل می‌کنیم و از طریق این کامپیوتر، اکسس پاینت را عیار سازی نماییم.

^{۷۰}Wireless Access Point

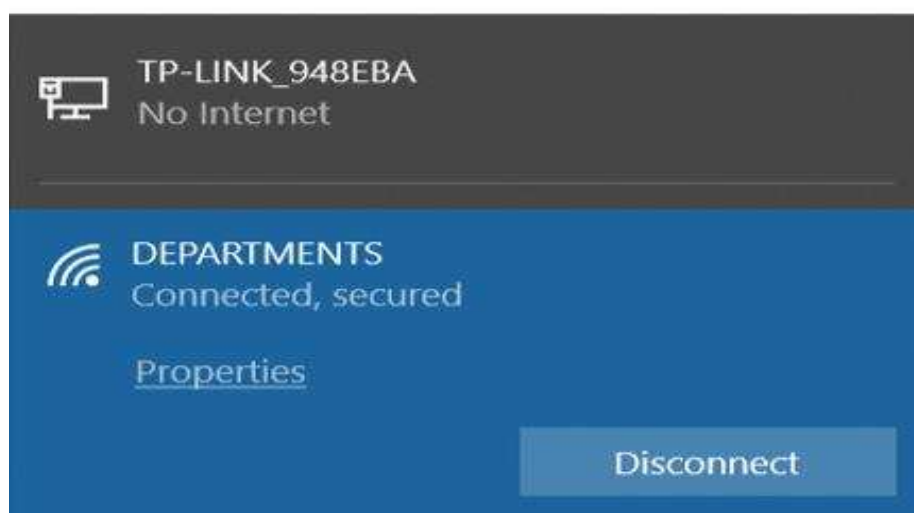
^{۷۱}Connection

اما در هردو حالت باید کارت شبکه بی سیم و یا سیم کامپیوتر خود را با آدرس IP تنظیم و ارتباط کامپیوتر به اکسس پاینت را امتحان کنیم. شکل ۴-۱ ارتباط بی سیم را به نام Wi-Fi در یک شبکه به نام DEPARTMENTS و ارتباط سیمی را به نام Ethernet در شبکه به نام TP-LINK-948EBA نشان می دهد. مطابق شکل زیر مشاهده می شود که هردو ارتباط فعال است.



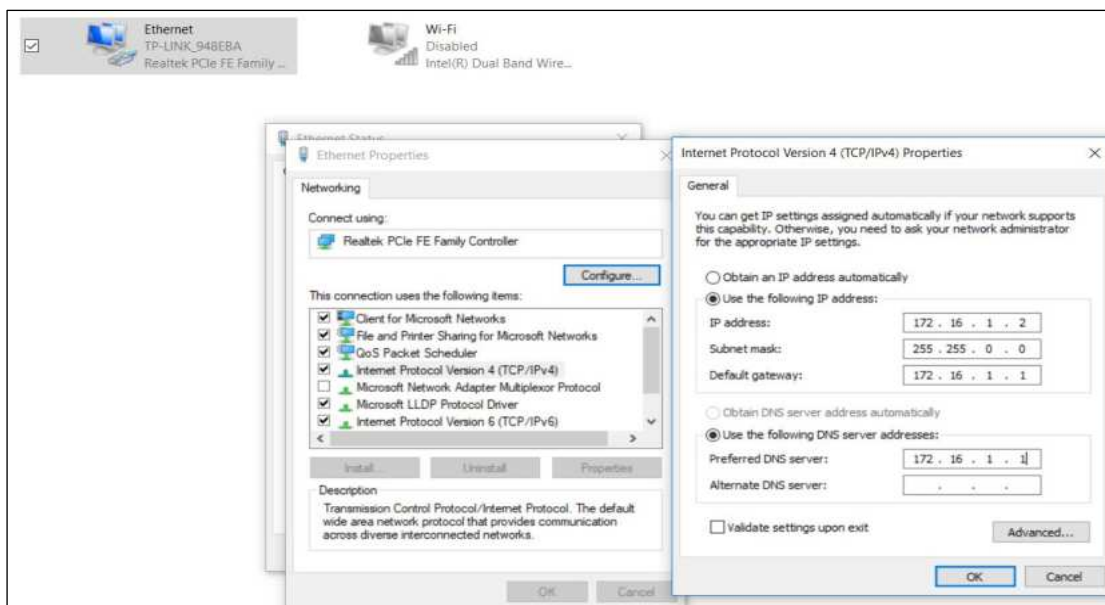
شکل ۴-۱: دو نوع ارتباط سیمی و بی سیم

حالا می خواهیم که از طریق کیبل، مطابق استانداردهای Ethernet به اکسس پاینت مورد نظر، جهت عیارسازی وصل شویم. گنکشن فعال از طریق Taskbar کامپیوتر مطابق شکل ۴-۲ قابل استفاده است. هم چنان در صورت نیاز می توانیم گنکشن های مورد نیاز را از این طریق تغییر بدهیم و گنکشن دیگر را انتخاب کنیم. شکل زیر را مشاهده نمایید.



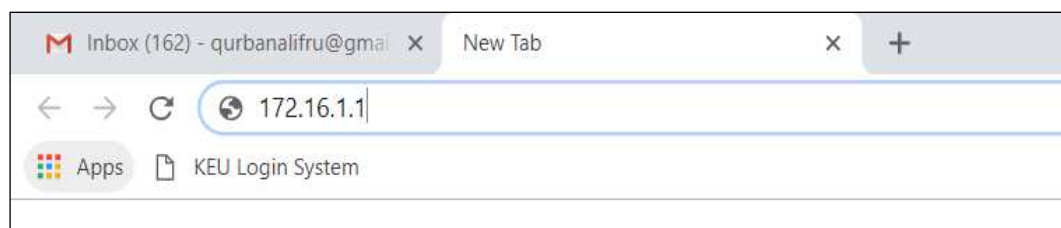
شکل ۴-۲: گنکشن های فعال در Taskbar کامپیوتر

جهت ارتباط و شناخت کامپیوتر توسط اکسس پاینت، باید از طریق تنظیمات TCP/IP به کامپیوتر خود آدرس IP بدهیم. این آدرس باید از یک کلاس و از یک زیر شبکه باشد. شکل ۴-۳ نشان می دهد که به گنکشن Ethernet آدرس IP داده شده است. این آدرس ارتباط منطقی بین کامپیوتر و اکسس پاینت را به وجود آورده است. در صورتی که تمام تنظیمات درست باشد، می توانیم محیط تنظیمات اکسس پاینت را از طریق Web Browser مشاهده کنیم و تنظیمات را مطابق ضرورت انجام دهیم. جزئیات آن را در شکل ۴-۳ مشاهده نمایید.



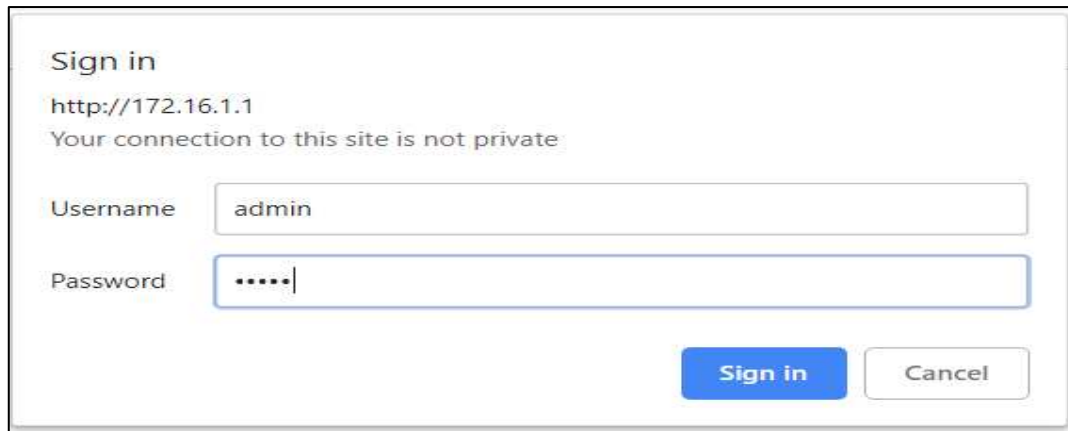
شکل ۴-۳: تنظیمات آدرس IP از طریق TCP/IP

در ادامه از طریق آدرس IP با استفاده از محیط Web Browser داخل اکسس پاینت می‌شویم. شکل ذیل مرحله داخل شدن به محیط تنظیمات اکسس پاینت را نشان می‌دهد. در این رهنمود آدرس IP اکسس پاینت را در Web Browser نوشته کرده و کلید Enter را فشار می‌دهیم. بعد از Enter کردن، دیده می‌شود که اکسس پاینت دارای یوزرنیم و پاسورد بوده و درخواست می‌نماید که افراد مجاز از طریق یوزرنیم و پاسورد داخل شود. ناگفته نماند که این آدرس، مربوط به شکل WLAN بوده و من حیث Gateway در کمپیوتر نیز معرفی می‌گردد. بنا بر این در روش اول با استفاده از آدرس IP اکسس پاینت، وارد اکسس پاینت می‌شویم. جزئیات را در شکل ۴-۴ مشاهده نمایید.



شکل ۴-۴: روش اول، وارد شدن به اکسس پاینت از طریق آدرس IP

با استفاده از آدرس IP و فشار دادن کلید انتر، محیط وارد نمودن یوزرنیم و پاسورد ظاهر می‌شود. این محیط برای تست کردن افراد مجاز و غیر مجاز است. در صورت درست بودن یوزرنیم و پاسورد، در مرحله بعدی وارد محیط تنظیمات اکسس پاینت می‌شویم. شکل ۴-۵ را مشاهده نمایید.



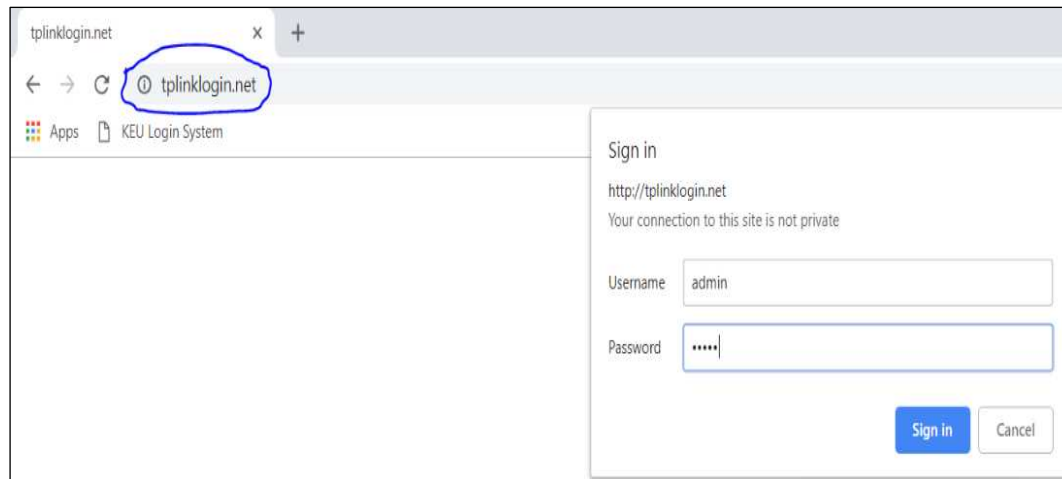
شکل ۴-۵: محیط وارد شدن با استفاده از آدرس IP

در روش دوم، می‌توانیم از طریق لینک مربوطه وارد اکسس پاینت شویم. در این روش لینک مربوطه وابسته به نوع اکسس پاینت است. لینک دسترسی به تنظیمات نوع TP-LINK، عبارت از <http://tplinklogin.net> است. جهت تنظیمات بخش مورد نیاز، در این‌جا از برند TP-LINK استفاده شده است.



شکل ۴-۶: اکسس پاینت از نوع TP-LINK

با استفاده از لینک مربوطه و فشار دادن کلید انتر، محیط لاگ‌ان به اکسس پاینت ظاهر می‌شود. جزئیات را در شکل ۴-۷ مشاهده نمایید.



شکل ۴-۷: روش دوم، وارد شدن به اکسس پاینت از طریق لینک مربوطه

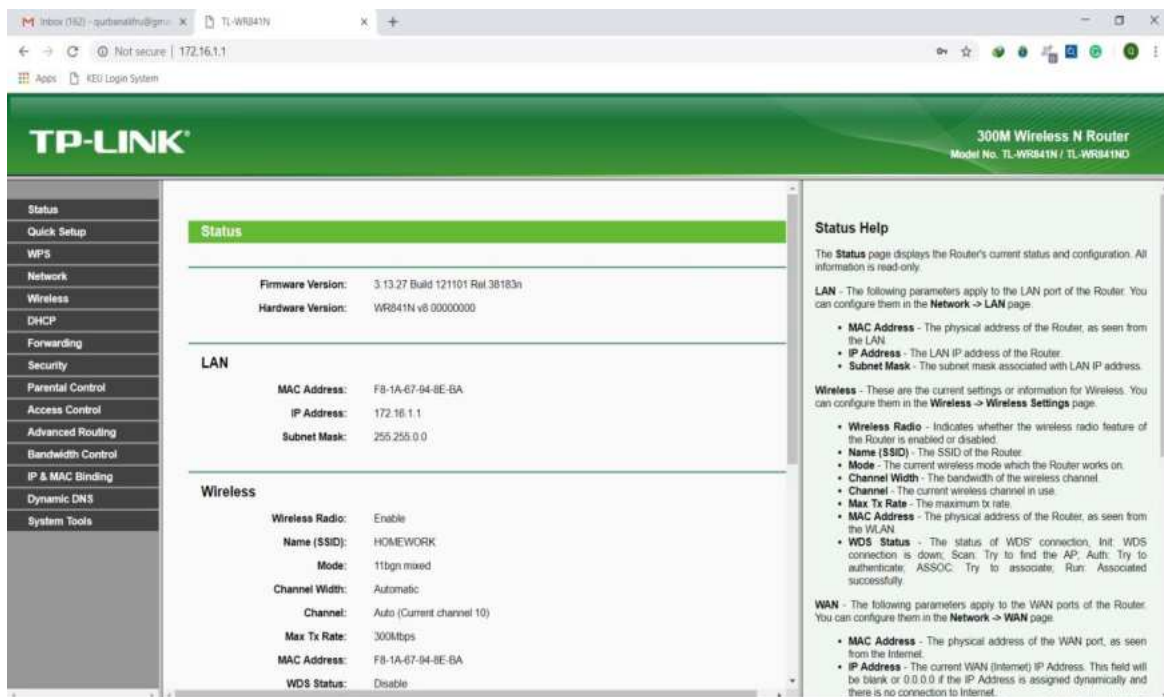
بعد از وارد نمودن موفقانه یوزرنیم و پاسورد اکسس پاینت، محیط تنظیمات آن به سادگی ظاهر و قابل استفاده می باشد. در شکل ذیل محیط تنظیمات اکسس پاینت از نوع TP-LINK نشان داده شده است. قسمی که دیده می شود این صفحه تنظیمات به صورت گرافیکی بوده و ضرورت به اجرا نمودن کدام دستور، کد کردن و غیره نمی باشد. محیط تنظیمات اکسس پاینت، یک صفحه گرافیکی است که به سادگی قابل عیار سازی است. در این صفحه از طرف چپ، گزینه های مختلف عیار سازی به صورت گرافیکی لیست گردیده است. در طرف چپ آن، رهنمایی هر گزینه به صورت جداگانه قابل مشاهده می باشد. هرگاه بالای یکی از گزینه های عیار سازی کلیک نمایید، تمام معلومات در مورد آن، در طرف چپ صفحه ظاهر می شود.

یادآوری مهم: دستگاهی که جهت عیار سازی در این کتاب در نظر گرفته شده است، نوع روتر بی سیم است. روترهای بی سیم علاوه بر این که قابلیت ها و عمل کردهای روتر (مسیریابی) را دارد، قابلیت های اکسس پاینت، سوئیچینگ و بریجینگ^{۲۲} را نیز دارد. در ادامه تمام تنظیمات و عیار سازی های که انجام می شود در محیط روترهای بی سیم انجام شده است. به عنوان مثال در این کتاب از روترهای بی سیم به نام WR۸۴۱N جهت تنظیمات استفاده شده است.

در شکل ذیل، نسخه Firmware، نسخه سخت افزار (WR۸۴۱N)، معرفی شبکه WLAN (آدرس IP ۱۷۲.۱۶.۱.۱، ماسک ۲۵۵.۲۵۵.۰.۰ و آدرس MAC آن ۸E-BE-۹۴-۶۷-۱A-F۸ و Wireless Radio) به وضاحت قابل رویت است. بنابراین اطلاعات مهم و ضروری در مورد اکسس پاینت و شبکه WLAN در این شبکه معرفی گردیده است.

همچنان مطابق شکل ۴-۸ مشاهده می گردد که این اکسس پاینت از نوع روتر بی سیم بوده و با فراهم شدن نقطه دسترسی، خدمات روتر از نوع (۳۰۰ M Wireless N Router) و مدل دستگاه را نیز نشان می دهد.

^{۲۲} Bridging



شکل ۴-۸: معرفی محیط عیار سازی اکسس پاینت از نوع TP-LINK

۴.۳ معرفی گزینه‌ها

یکی از گزینه‌ها مشاهده کردن آدرس IP و مشاهده کردن یوزرنیم و پاسورد است. هم‌چنان مشاهده کردن لینک برای ورود به اکسس پاینت است. در شکل ذیل آدرس IP، ۱۹۲.۱۶۸.۰.۱ برای ورود به اکسس پاینت از طریق شبکه LAN قابل مشاهده است. هم‌چنان لینک مربوطه جهت ورود به اکسس پاینت نیز در نظر گرفته شده است. روش دیگر ورود به اکسس پاینت لینک مربوطه آن، عبارت از <http://tplinklogin.net> است. شکل زیر روش ورود به اکسس پاینت و یوزرنیم و پاسوردهای پیش‌فرض اکسس پاینت را نشان می‌دهد.

Login data for the user interface

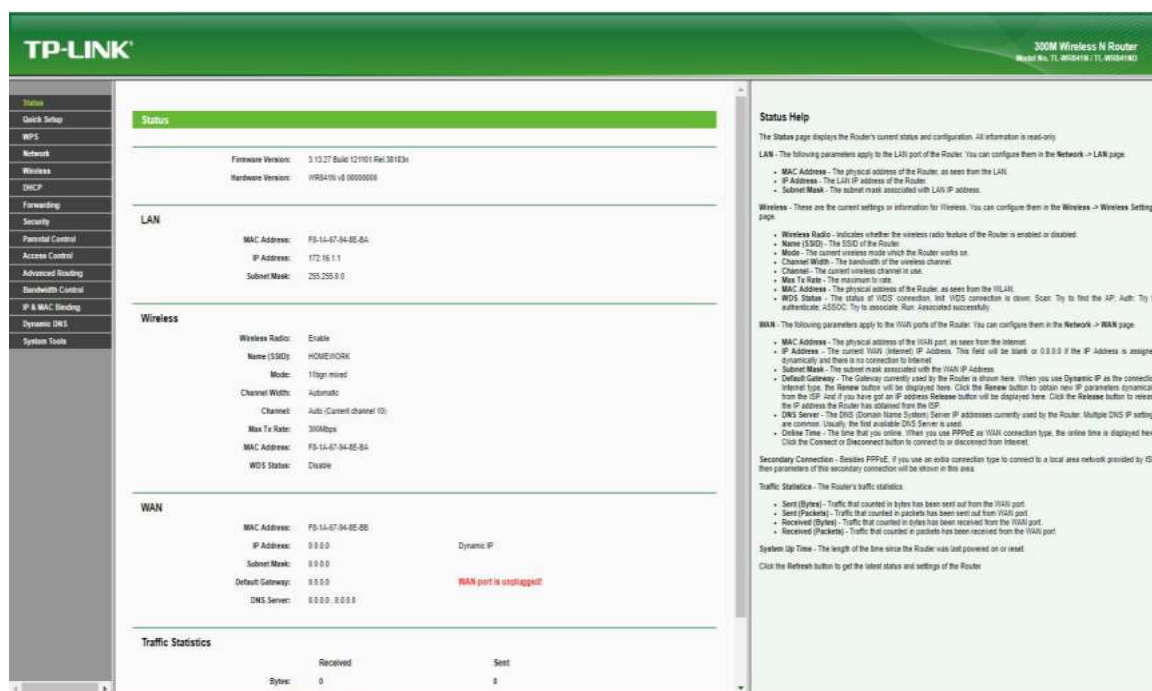
```
IP address:      192.168.0.1 (or http://tplinklogin.net)
Username:       admin
Password:      admin
```

شکل ۴-۹: روش ورود به اکسس پاینت با یوزرنیم و پاسورد پیش‌فرض

۴.۳.۱ گزینه Status

گزینه Status جهت مشاهده نمودن معلومات عمومی و نشان دادن وضعیت فعلی اکسس پاینت استفاده می‌شود. این گزینه به‌صورت عموم نسخه Firmware، نسخه سخت‌افزار، وضعیت و مشخصات شبکه LAN همراه با آدرس IP و MAC، وضعیت و مشخصات شبکه بی‌سیم، وضعیت و مشخصات شبکه WAN، آمار و

وضعیت فعلی ارسال و دریافت اطلاعات را نمایش می‌دهد. لذا این گزینه، تنها جهت دریافت معلومات و نمایش تنظیمات قبلی اکسس پاینت استفاده می‌شود. به عبارت دیگر گزینه‌های تنظیمات و عیارسازی در این جا قابل تطبیق نیست و تنها مشاهده وضعیت کلی اکسس پاینت است. علاوه برآن در سمت چپ آن، در مورد تمام گزینه‌های یاد شده، معلومات کافی ارائه نموده است. جهت معلومات بیش تر به شکل ۴-۹ با دقت توجه نمایید.



شکل ۴-۹: نمایش دادن وضعیت کلی دستگاه اکسس پاینت

۴.۴ تنظیمات WAN

حالا اگر خواسته باشیم عیار سازی اکسس پاینت انجام شود، باید از طریق گزینه‌های مربوطه اقدام شود. یکی از گزینه‌های که نیاز به عیار سازی دارد، گزینه WAN است که در شکل زیر نشان داده شده است. این گزینه، برای عیارسازی ارتباط شبکه داخلی (LAN) به شبکه بیرونی (WAN) است. از این طریق می‌توانیم شبکه داخلی خود را به شبکه بیرونی یعنی اینترنت وصل کنیم. در صورتی که اکسس پاینت شما به کدام مودیم، سویچ اصلی شبکه و یا روتر اصلی شبکه وصل باشد، ممکن به صورت خودکار عیار سازی این بخش انجام شود. در صورتی که این به صورت خود کار فعال نگردد، نیاز است که شما آدرس IP، ماسک و Gateway، DNS، اولی و دومی، نام اکسس پاینت و غیره را از این طریق عیار سازی نمایید. قسمی که در شکل دیده می‌شود، به صورت خودکار پیام داده است که در حال حاضر به شبکه WAN وصل نیست.

به عنوان مثال اگر اکسس پاینت شما به کدام دستگاه وصل گردیده باشد که آدرس IP آن ۱۹۲.۱۶۸.۱۰.۱ باشد؛ شما در گزینه IP Address می‌توانید IP، ۱۹۲.۱۶۸.۱۰.۲ را بدهید و در گزینه Default Gateway می‌توانید آدرس دستگاه متصل (۱۹۲.۱۶۸.۱۰.۱) را تنظیم کنید. در این صورت دیده می‌شود که Gateway برای اکسس پاینت شما دستگاه متصل (شبکه بیرونی) است. جزئیات آن را در شکل ۴-۱۰ مشاهده نمایید.

TP-LINK

Status
Quick Setup
WPS
Network
- WAN
- MAC Clone
- LAN
Wireless
DHCP
Forwarding
Security
Parental Control
Access Control
Advanced Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
System Tools

WAN

WAN Connection Type:

IP Address:
Subnet Mask:
Default Gateway:
 WAN port is unplugged!

MTU Size (in bytes): (The default is 1500, do not change unless necessary.)

☐ Use These DNS Servers
Primary DNS:
Secondary DNS: (Optional)
Host Name:
☐ Get IP with Unicast DHCP (it is usually not required.)

شکل ۴-۱۰: تنظیمات شبکه WAN

۴.۴.۱ تنظیمات LAN

با استفاده از تنظیمات LAN، می‌توانیم آدرس IP و ماسک برای اکسس‌پاینت خود را تنظیم کنیم. این آدرس مربوط به اجزای شبکه LAN می‌شود. از طریق این آدرس می‌توانیم به اکسس‌پاینت لاگ‌ان شویم و تنظیمات مورد نیاز خود را انجام دهیم. هم‌چنان این آدرس مربوط به تمام کمپیوترها، لپ‌تاپ‌ها، موبایل‌ها، PDAs و تمام دستگاه‌هایی می‌باشد که زیر پوشش این اکسس‌پاینت قرار دارد. در این شکل به عنوان مثال آدرس IP، ۱۷۲.۱۶.۱.۱ در نظر گرفته شده است. تمام اجزای متعلق به این شبکه LAN، از محدوده IP، ۱۷۲.۱۶.۱.۱ استفاده خواهند کرد. قسمی که در شکل ۴-۱۱ دیده می‌شود، آدرس MAC اکسس‌پاینت و ماسک مربوط به آن در آن مشاهده می‌گردد که در زمان ارتباطات داخلی بین اجزا و ارتباطات بیرونی (WAN) نهایت مهم و ضروری است.

شکل ۴-۱۱: تنظیمات شبکه LAN

۴.۴.۲ تنظیمات گزینه Wireless

بخشی بسیار مهم و اساسی در تنظیمات اکسس پاینت‌ها و روترهای بی‌سیم، گزینه Wireless Setting است. هم‌چنان این گزینه دارای چندین گزینه فرعی بسیار مهم و حیاتی می‌باشد. گزینه‌های فرعی آن شامل: نام اکسس پاینت (SSID)، ناحیه پوشش و موقعیت فعالیت دستگاه (Region)، نوع استانداردهای قابل استفاده در شبکه WLAN (Mode)، کانال^{۷۳}، فعالیت اکسس پاینت به صورت بی‌سیم و یا تنها سیمی^{۷۴}، نشر و پخش^{۷۵} نام شبکه (SSID) و فعالیت اکسس پاینت به صورت Bridge های بی‌سیم و غیره می‌باشد.

به دلیل این که این بخش دارای چندین گزینه فرعی است و هر گزینه فرعی در شبکه‌های بی‌سیم از اهمیت زیادی برخوردار می‌باشد، ضرورت است هر کدام به صورت جداگانه معرفی و توضیح داده شود. برای معلومات بیشتر به شکل ذیل با دقت توجه نمایید.

۴.۴.۲.۱ نام شبکه بی‌سیم (Wireless Network Name)

طوری که از مفهوم این عبارت فهمیده می‌شود، این گزینه برای تعیین نام شبکه بی‌سیم، یعنی WLAN استفاده می‌شود. هم‌چنان نام شبکه بی‌سیم WLAN، به نام SSID نیز یاد می‌شود. اصطلاح SSID برگرفته از Service Set Identifier است. به این مفهوم که تشخیص شبکه بی‌سیم از این طریق انجام می‌شود. هرگاه شما خواسته باشید که به یک شبکه بی‌سیم WLAN وصل شوید، اولین بار از طریق نام شبکه (SSID) آن می‌توانید ارتباط برقرار کنید. گزینه SSID تحت نام شبکه، از طریق Taskbar قابل شناسایی است. روش یافتن SSID را از طریق کامپیوترها، در شکل ۴-۱۲ مشاهده کرده می‌توانید. مطابق شکل ذیل نام یک

⁷³ Channel

⁷⁴ Enable Wireless Router Radio

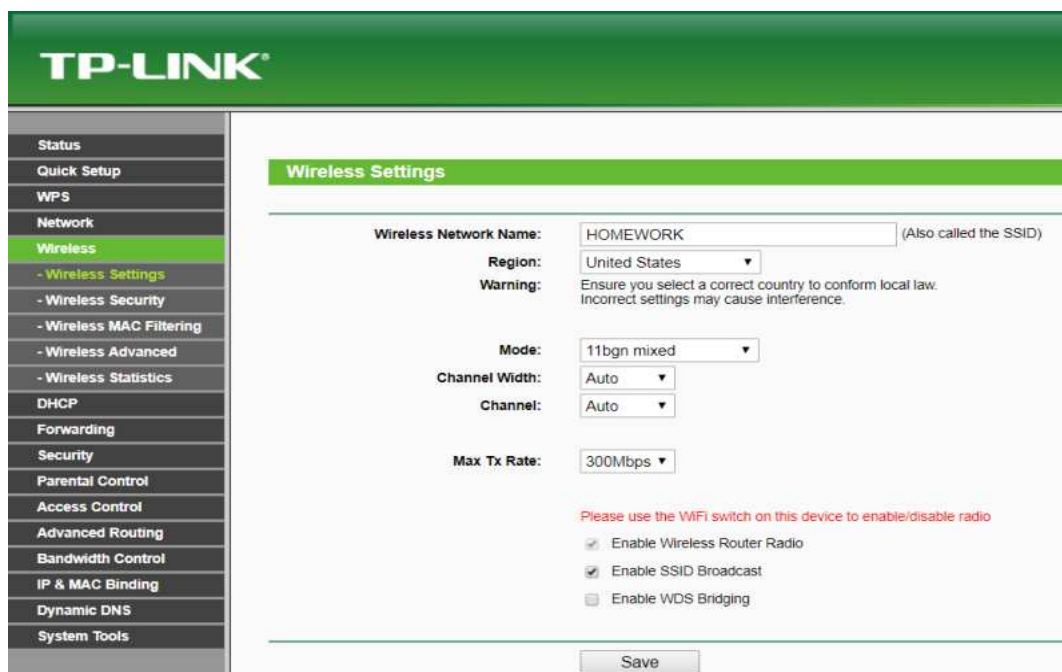
⁷⁵ Broadcast

شبکه (SSID) آن، به نام DEPARTMENTS گذاشته شده است و نام شبکه دومی آن TP-LINK_948EBA گذاشته شده است. لذا نام شبکه برای یافتن شبکه‌های بی‌سیم فعال، در محیط و همسایگی شما نهایت مهم است. از یک لحاظ ممکن تهدید امنیتی باشد و از دید دیگر برای یافتن شبکه‌های فعال به استفاده کننده‌ها کمک می‌کند.



شکل ۴-۱۲: نام شبکه (SSID) در شبکه WLAN

در شکل ۴-۱۳ به عنوان مثال، شبکه (SSID)، به نام HOMEWORK نام‌گذاری شده است. این نام در آینده‌ها برای یافتن این اکسس‌پاینت و استفاده از آن نهایت کمک می‌کند.



شکل ۴-۱۳: تنظیمات نام شبکه، استانداردها، کانال ارتباطی، نوع فعالیت SSID و فعالیت اکسس‌پاینت به صورت Bridge

۴.۴.۲.۲ موقعیت فعالیت دستگاه (Region)

این گزینه برای این است که اکسس‌پاینت شما در کدام کشور با کدام استانداردهای بی‌سیم و با کدام قوانین و محدودیت‌های امواج رادیویی فعالیت می‌کند. با استفاده از نام کشورها که از قبل در آن لست، اضافه گردیده

است، نام کشور خود را انتخاب کنید. نکته قابل یادآوری این است که نام تمام کشورهای دنیا در آن نیست و شما با توجه به استانداردهای مورد استفاده خود یکی از کشورها را انتخاب کنید.

۴.۴.۲.۳ انتخاب نوع استانداردها (Mode)

انواع استانداردهای بی سیم در فصل سوم این کتاب تشریح گردیده است. این استانداردها شامل ۸۰۲.۱۱a، ۸۰۲.۱۱b، ۸۰۲.۱۱g، ۸۰۲.۱۱n و غیره است که هر کدام به صورت جداگانه در فصل سوم کتاب معرفی شده است. از طرف دیگر می دانیم که هر استاندارد حاوی سرعت مشخص، پهنای باند مشخص، فاصله مشخص می باشد. بنا براین با استفاده از این گزینه می توانیم استاندارد سازگار را که ضرورت شبکه است با تمام اجزای شبکه WLAN، سرعت، فاصله، پهنای باند و موارد دیگر تعیین کنیم. در این گزینه حالت ترکیبی (Mixed) تمام این استانداردها نیز وجود دارد. با استفاده از این استانداردها باید سازگاری تمام اجزای شبکه WAN را در نظر بگیریم که جزئیات سازگاری استانداردها در فصل سوم بحث گردیده است.

در این جا به عنوان مثال حالت ترکیبی تمام این استانداردها به نام ۱۱bgn Mixed انتخاب گردیده است.

شکل ۴-۱۴ انتخاب استانداردهای بی سیم یعنی Mode را نشان می دهد.



شکل ۴-۱۴: تنظیم استانداردها (Mode) شبکه WLAN

۴.۴.۲.۴ عرض کانال (Channel Wide)

هدف از عرض کانال^{۷۶} پهنای پوشش امواج رادیویی است. در صورتی که شما خواسته باشید، اکسس پاینت را به اکسس پاینت به صورت Point-to-point وصل کنید، عرض کانال می تواند کوچک باشد. بهترین حالت برای اکسس پاینت های که در شبکه WLAN استفاده می شود، حالت خودکار^{۷۷} است. این گزینه در شکل بالا نشان داده شده است.

۴.۴.۲.۵ کانال (Channel)

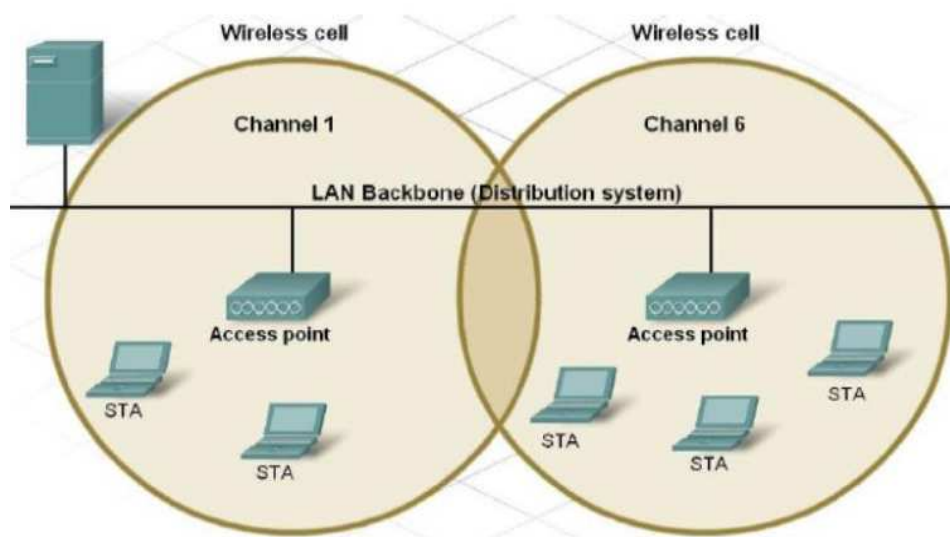
یکی از مفاهیم مهم در شبکه بیسیم، کانال است. انتخاب یک کانال درست به معنای افزایش قدرت شبکه بی سیم و افزایش سرعت ارتباط است. هم چنان هر کانال قادر به Conversaion های مختلف است. معمولاً اکسس پاینت ها بین ۱۱ تا ۱۳ کانال فعال دارند. اکسس پاینت ها بیش تر به صورت خودکار کانال های را که

⁷⁶Beam Width

⁷⁷Auto

کمترین ازدحام را داشته باشد، انتخاب می‌کنند. در صورتی که از طریق اکسس پاینت یکی از کانال‌ها انتخاب گردد، بیش‌تر اکسس پاینت‌ها را محدودتر می‌سازد. گزینه انتخاب کانال‌ها در شکل بالا نشان داده شده است.

هرگاه خواسته باشیم که اکسس پاینت A را با اکسس پاینت B وصل کنیم، این دو اکسس پاینت از طریق یک کانال مشابه وصل نمی‌گردد، بلکه به صورت خودکار یکی از کانال ۱ و دیگری از کانال ۲ استفاده خواهد کرد. از طرف دیگر هر کانال دارای ویژگی و مشخصات به خصوص خود می‌باشد، که از کدام فریکانس و طول موج استفاده می‌کند. به عبارت دیگر با تغییر کانال، فریکانس، طول موج، سرعت نیز تغییر می‌کند. شکل زیر استفاده از کانال در دو شبکه WLAN را نشان می‌دهد. در شکل ۴-۱۵ دیده می‌شود که دو اکسس پاینت در دو شبکه جداگانه، با دو کانال متفاوت (یکی با کانال ۱ و دیگر با کانال ۶) فعالیت می‌کند.



شکل ۴-۱۵ مفهوم و استفاده از کانال

۴.۴.۲.۶ حداکثر ظرفیت ارسال (Max Tx Rate)

این گزینه برای تعیین سرعت ارسال اکسس پاینت است. سرعت نهایی ارسال هر اکسس پاینت بستگی به استانداردها دارد که در فصل سوم بحث شده است. در این جا به عنوان مثال ۳۰۰ Mbps سرعت ارسال تعیین گردیده است. قابل یادآوری است که سرعت نهایی ارسال اطلاعات در این جا محدود گردیده و هر گونه سرعت دل خواه را نمی‌توانیم اضافه کنیم. در صورتی که می‌توانیم سرعت کم‌تر را انتخاب کنیم. شکل ۴-۱۶ گزینه انتخاب حداکثر ظرفیت ارسال اطلاعات را نشان می‌دهد.



شکل ۴-۱۶ تنظیم حداکثر ظرفیت ارسال اطلاعات، توسط اکسس پاینت

۴.۴.۲.۷ فعالیت بی سیم و یا سیمی (Enable Wireless Router Radio)

این گزینه برای فعالیت اکسس پاینت به صورت بی سیم یا سیمی است. از این طریق می توانیم خدمات بی سیم اکسس پاینت و یا روتر بی سیم را قطع کنیم. قسمی که در شکل نشان داده شده است، فعالیت شبکه بی سیم باید از این طریق فعال گردد. در صورتی که این گزینه انتخاب نگردد، اکسس پاینت، خدمات بی سیم نداشته و هیچ گاه نام شبکه (SSID) در لیست شبکه های بی سیم مشاهده نمی گردد. شکل ۴-۱۷ گزینه فعالیت بی سیم و سیمی را نشان می دهد.



شکل ۴-۱۷: تنظیم فعالیت اکسس پاینت و یا روتر به شکل بی سیم یا سیمی

۴.۴.۲.۸ فعالیت پخش نام شبکه (Enable SSID Broadcast)

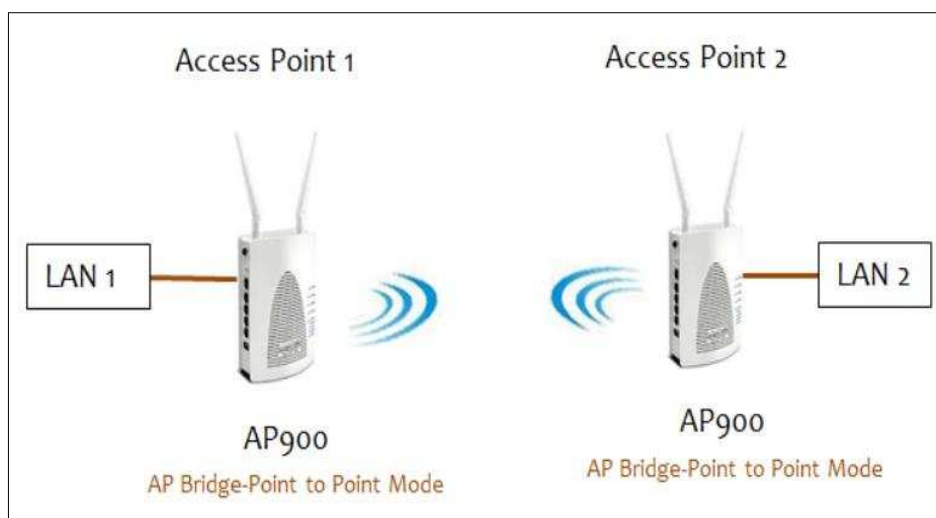
طوری که در بخش های گذشته تذکر داده شد که همیشه شبکه های بی سیم از طریق SSID آن قابل شناخت است. اگر شبکه بی سیم در محدوده پوشش آن Broadcast نگردد، شبکه بی سیم به صورت آشکار قابل تشخیص نخواهد بود. در بعضی حالت ها، به دلایل تامین امنیت بهتر و مخفی کردن نام شبکه، این گزینه را می توانیم غیر فعال بسازیم. در صورت غیر فعال کردن این گزینه، خدمات اکسس پاینت و پوشش آن به سادگی قابل شناخت نمی باشد. لذا ملاحظات امنیت در این مورد این است که، Broadcast کردن نام شبکه درست نیست و بهتر است که از دید عام مردم مخفی باشد. هم چنان برای شناسایی و یافتن خدمات شبکه بی سیم، می توانیم این گزینه را تایید (فعال) کنیم.

۴.۴.۲.۹ فعال کردن خدمات (Bridge) (Enable WDS Bridging)

این گزینه برای فعالیت اکسس پاینت به صورت پل^{۷۸} است. ایجاد کردن پل در شبکه های WLAN به معنی این است که دو شبکه LAN از طریق دو اکسس پاینت با هم دیگر وصل می گردد. در صورت نیاز به وصل کردن دو شبکه WLAN این گزینه فعال می گردد. در اثر فعال شدن این گزینه، هر اکسس پاینت حالت پل را انتخاب می کند و دو شبکه WLAN به صورت بی سیم، بین هم شبکه بی سیم را تشکیل می دهند. به عنوان مثال: اگر اکسس پاینت A با اکسس پاینت B به صورت بی سیم بین هم وصل گردد از طریق این گزینه امکان پذیر است. در این مورد، وقتی گزینه Enable WDS Bridging انتخاب گردد، بقیه تنظیمات آن نیز ظاهر می شود. تنظیمات پل به صورت بی سیم، دارای بعضی نیازمندی های دیگر از قبیل نام شبکه مقابل، آدرس

⁷⁸ Bridge

MAC اکسس پاینت مقابل و غیر می باشد. به عبارت دیگر مشخصات اکسس پاینت A به B و مشخصات اکسس پاینت B به A تنظیم می گردد. شکل ۴-۱۸ مفاهیم پل در شبکه های بی سیم را نشان داده است.



شکل ۴-۱۸: مفهوم Bridging در اکسس پاینت

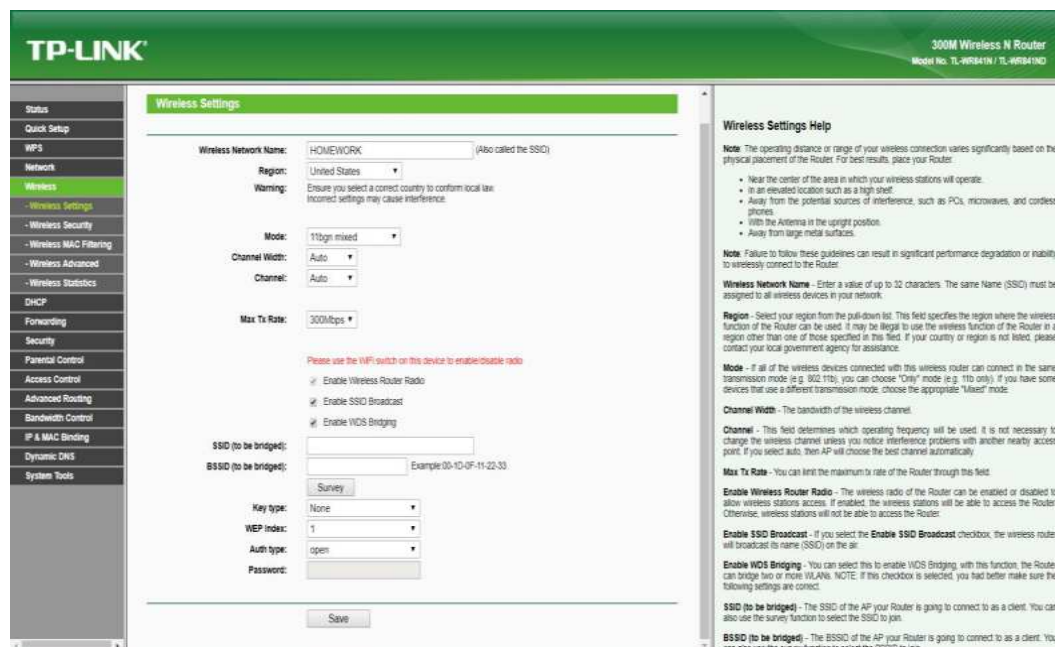
مشخصات ضروری برای تنظیم هردو اکسس پاینت عبارت از آدرس MAC، نام شبکه (SSID) و کانال ارتباطی است. هم چنان در صورت ضرورت بعضی تنظیمات امنیتی مانند پاسوردها، کلیدهای امنیتی و غیر نیز ممکن است. جهت وضاحت بیش تر به شکل ۴-۱۹ توجه نمایید.

شکل ۴-۱۹: تنظیمات Bridging در اکسس پاینت

مطابق شکل بالا تنظیم خدمات Bridging در اکسس پاینت ها، دیده می شود که با استفاده از گزینه Survey نیز می توانیم مشخصات اکسس پاینت های محدوده پوشش (شبکه نزدیک) را به دست آوریم و از این طریق گزینه های مورد نیاز را خانه پُری کنیم. بالاخره بعد از تأیید گزینه ذخیره^{۷۹} می توانیم از اکسس پاینت خود به صورت bridge استفاده کنیم.

^{۷۹}Save

شکل ذیل تمام تنظیمات یاد شده را نشان می‌دهد. از طرف دیگر دیده می‌شود که این تنظیمات به صورت گرافیکی و به اصطلاح و مفاهیم ساده در نظر گرفته شده است. قابل یادآوری است که در این جا اکسس پاینت از نوع کمپنی TP-LINK در نظر گرفته شده است. ممکن تمام گزینه‌ها از لحاظ ترتیب و جابه‌جایی با اکسس پاینت‌های دیگر متفاوت باشد، اما از لحاظ عمل کرد، تنوع گزینه‌ها، اصطلاحات و مفاهیم باهم یکسان می‌باشد. شکل ۴-۲۰ تنظیمات اساسی اکسس پاینت را نشان می‌دهد. به دقت توجه نمایید.



شکل ۴-۲۰: تنظیمات عمومی گزینه Wireless Setting در اکسس پاینت TP-LINK

۴.۴.۲.۱۰ تنظیمات پیش‌رفته بی‌سیم (Wireless Advanced)

این بخش در صورتی نیاز است که اکسس پاینت و شبکه بی‌سیم خویش را به صورت دل‌خواه و به شکل پیش‌رفته عیار سازی کنیم. از این طریق می‌توان محدودیت‌ها و سهولت‌های زیادی را در اکسس پاینت تطبیق و تنظیم نماییم. به عنوان مثال قدرت ارسال سیگنال‌های بی‌سیم به صورت عالی باشد یا ضعیف. در صورتی که خواسته باشیم فاصله‌های بیش‌تر توسط اکسس پاینت پوشش داده شود، سیگنال ضعیف در شبکه بی‌سیم خود نداشته باشیم، می‌توانیم قدرت ارسال را High انتخاب کنیم. هم‌چنان زمان‌بندی^{۸۰} ارسال و دریافت، تایید به طرف مقابل توسط میتود^{۸۱} RTS، آستانه^{۸۲} تکه سازی^{۸۳} و پارچه بسته‌های اطلاعاتی، فعال کردن^{۸۴} WMM جهت استفاده از اطلاعات چند رسانه‌ای توسط شبکه Wi-Fi و غیره تنظیمات از این طریق قابل پیاده سازی است. شکل ۴-۲۱ حالت پیش‌فرض تنظیمات را نشان می‌دهد. در صورتی که شرایط شبکه بی‌سیم بسیار متفاوت

⁸⁰ Interval

⁸¹ Ready To Send

⁸² Threshold

⁸³ Fragmentation

⁸⁴ Wi-Fi Multi Media

از شبکه‌های دیگر نباشد، از حالت پیش فرض استفاده گردد. جهت معلومات بیش تر شکل زیر را به دقت مشاهده نمایید.



شکل ۴-۲۱: تنظیمات پیشرفته اکسس پاینت

۴.۴.۲.۱۱ احصائیه دستگاه های متصل (Wireless Statistics)

در این بخش دستگاه‌های که در حال حاضر به اکسس پاینت به شکل بی سیم و سیمی متصل باشند، نشان داده می‌شود. این بخش برای دانستن تعداد دستگاه‌های فعال، حجم ارسال و دریافت اطلاعات از طرف هر کامپیوتر و یا دستگاه‌های دیگر، شناسایی افراد و دستگاه‌های غیر مجاز استفاده می‌شود. بنا بر این، این بخش جهت مطالعه وضعیت اکسس پاینت و شبکه WLAN نهایت موثر و مفید است. در صورتی که مشکلات سرعت و یا محدودیت‌های آدرس IP از طرف DHCP، قطع شدن بعضی کلاینت‌ها و غیره مشکلات دیگر مشاهده گردد، جهت مطالعه این مشکلات از این بخش به صورت همه جانبه استفاده می‌گردد. به صورت مختصر این بخش جهت نمایش و سروی دستگاه‌های متصل به صورت آنلاین نمایش داده می‌شود. شکل ۴-۲۲ نشان می‌دهد که در حال حاضر کدام دستگاه به این اکسس پاینت متصل نبوده و اکسس پاینت با دستگاه‌های دیگر در حال کدام ارسال و دریافت اطلاعات نمی‌باشد.



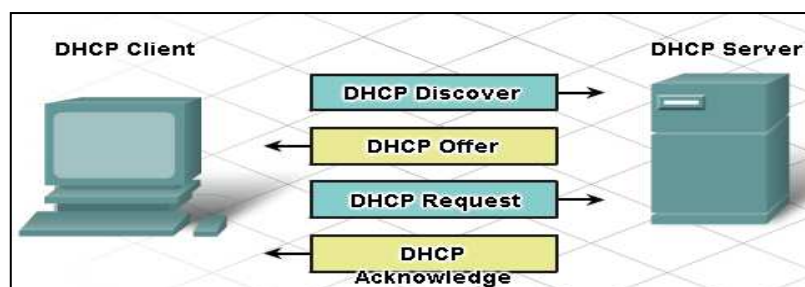
شکل ۴-۲۲: نمایش تعداد دستگاه‌های متصل به اکسس پاینت

یادآوری مهم: تنظیمات و عیارسازی‌های امنیتی در اکسس‌پاینت‌ها و روترهای بی‌سیم در فصل بعدی به صورت جداگانه بحث گردیده است. مطابق شکل فوق‌الذکر، مشاهده می‌گردد که تنظیمات امنیتی مانند: Wireless Security, Wireless MAC Filtering و غیره در محیط عیارسازی وجود دارد، اما در این فصل به آن پرداخته نشده است.

۴.۴.۲.۱۲ تنظیمات DHCP سرور (DHCP Settings)

پروتوکول DHCP یکی از پروتوکول‌های است که جهت فراهم کردن آدرس IP استفاده می‌شود. این پروتوکول با استفاده از یک لیست IP که از قبل ذخیره دارد، توزیع آن‌را به تمام کلاینت‌ها به عهده دارد. بنابر این، این پروتوکول منحصراً جهت فراهم کردن آدرس IP عمل می‌کند و تمام آدرس‌های IP که فعلاً توزیع نگردیده، در لیست خود نگهداری می‌کند. از این‌که بخش نظری پروتوکول DHCP و روش درخواست و دریافت IP، بحث‌های مفصل دارد، از طرف دیگر مربوط پلان و سرفصل این درس نمی‌شود، از توضیح بیش‌تر آن صرف نظر می‌گردد. اما جهت وضاحت بیش‌تر به یک شکل اکتفا می‌شود. در شکل ۴-۲۳ روش درخواست و دریافت آدرس IP با استفاده از پروتوکول DHCP نشان داده شده است. در این شکل دیده می‌شود که کلاینت از DHCP سرور درخواست IP نموده و سرور با استفاده از پروتوکول DHCP خدمات ارسال آدرس IP را انجام داده است.

جهت معلومات بیش‌تر به شکل زیر توجه نمایید.



شکل ۴ - ۲۳: روش فعالیت پروتوکول DHCP

آن‌چه از مفاهیم DHCP و شکل بالا یاد گرفتیم، حالا می‌خواهیم پروتوکول DHCP را در اکسس‌پاینت تنظیم و عیارسازی نماییم. قسمی که در شکل ذیل دیده می‌شود، در اکسس‌پاینت‌ها و یا روترهای بی‌سیم می‌توانیم خدمات DHCP را فعال و یا غیر فعال نماییم. فعال شدن آن با تائید گزینه Enable و غیر فعال شدن آن با تایید گزینه Disable انجام می‌شود. در ادامه انتخاب آدرس IP، اولین آدرس IP، آخرین آدرس IP، زمان تبدیل آدرس‌ها به حسب دقیقه، Gateway پیش‌فرض، ناحیه پیش‌فرض، DNS اولی و دومی به وضاحت در شکل دیده می‌شود.

تمام گزینه‌های فوق‌الذکر جهت انتخاب آدرس و تعیین فضای آدرس (آدرس اولی و آدرس آخری) و غیره در نظر گرفته شده است. به صورت مختصر بعضی گزینه‌های کلیدی آن در ذیل توضیح می‌شود:

Start IP Address: آدرس که در این گزینه نوشته شده است، اولین آدرسی است که توسط DHCP

مورد استفاده قرار می‌گیرد. به عنوان مثال آدرس ۱۷۲.۱۶.۱.۱ در این جا انتخاب گردیده است. این آدرس مربوط به شبکه WLAN می‌شود و آدرسی که به اولین کلاینت (کمپیوتر) توزیع می‌گردد، آدرس ۱۷۶.۱۶.۱.۲ خواهد بود و آدرس بعدی که به کمپیوتر بعدی توزیع می‌گردد، آدرس ۱۷۲.۱۶.۱.۳ خواهد بود و بالاخره تا تعداد کمپیوترها ختم گردد و یا تعداد آدرس‌های IP از این لست تمام شود.

End IP Adrees: آدرسی که در این گزینه نوشته می‌شود، آخرین آدرسی است که به یک کلاینت

تعلق می‌گیرد. به عبارت دیگر بعد از این آدرس کدام آدرسی دیگر به هیچ کلاینت ارسال نمی‌شود آدرس ۱۷۲.۱۶.۱.۲۲۰ آدرسی است که در این جا انتخاب گردیده است. به عبارت دیگر آخرین آدرسی که به آخرین کلاینت توزیع می‌گردد، آدرس ۱۷۲.۱۶.۱.۲۲۰ است و دیگر آدرسی بعد از این توزیع نخواهد شد.

هم‌چنان زمان نگه‌داری هر آدرس توسط هر کلاینت ۱۲۰ دقیقه انتخاب شده است. بعد از تکمیل ۱۲۰ دقیقه، آدرس‌های تمام کلاینت‌ها تغییر کرده و آدرس‌های جدید دریافت می‌کند. اما باید توجه داشته باشیم که فضای آدرس IP تغییر نمی‌کند، بلکه به عنوان مثال: آدرس کمپیوتر اولی به کمپیوتر دیگر و آدرس کمپیوتر دومی به کمپیوتر سومی یا چهارمی و یا به کدام کمپیوتر دیگر توزیع می‌گردد. علاوه بر این در صورت داشتن خدمات DNS و یا داشتن کدام DNS سرور می‌توانیم آدرس‌های DNS را نیز تنظیم کنیم.

از طرف دیگر اهمیت این پروتوکل در ارائه خدمات آن است که آدرس IP را به تمام کلاینت‌ها می‌فرستد و در صورت نیاز این پروتوکل را غیر فعال می‌سازد. در صورتی که تهدیدات امنیتی وجود داشته باشد و نه‌خواسته باشیم که به صورت خودکار آدرس‌های IP به کلاینت‌ها توزیع گردد، می‌توانیم خدمات DHCP را با گزینه Disable غیر فعال کنیم. با غیر فعال کردن خدمات DHCP، هکر و افراد مخرب به سادگی نمی‌توانند از اکسس پاینت استفاده کنند و یا به شبکه وصل شوند. شکل ۴-۲۴ را مشاهده کنید.

The image shows the DHCP Settings interface of a TP-LINK router. The left sidebar contains a menu with options: Status, Quick Setup, WPS, Network, Wireless, DHCP, - DHCP Settings, - DHCP Client List, - Address Reservation, Forwarding, Security, Parental Control, Access Control, and Advanced Routing. The main content area is titled 'DHCP Settings' and includes the following configuration options:

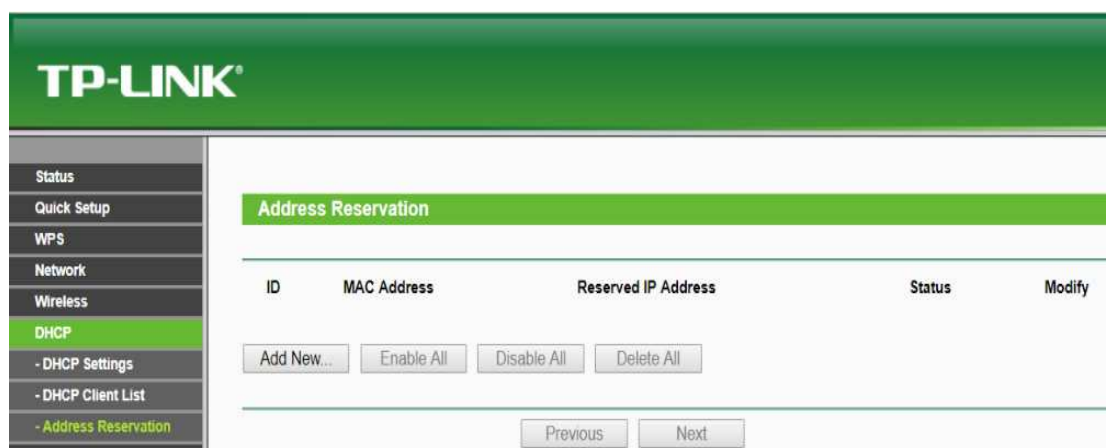
- DHCP Server:** Radio buttons for 'Disable' and 'Enable' (selected).
- Start IP Address:** Text box containing '172.16.1.1'.
- End IP Address:** Text box containing '172.16.1.220'.
- Address Lease Time:** Text box containing '120' with the unit 'minutes (1~2880 minutes, the default value is 120)'.
- Default Gateway:** Text box containing '172.16.1.1' with '(Optional)' next to it.
- Default Domain:** Text box with '(Optional)' next to it.
- Primary DNS:** Text box containing '0.0.0.0' with '(Optional)' next to it.
- Secondary DNS:** Text box containing '0.0.0.0' with '(Optional)' next to it.

A 'Save' button is located at the bottom of the settings area.

شکل ۴-۲۴: تنظیمات DHCP سرور در با استفاده از روتر بی‌سیم

۴.۴.۲.۱۳ تنظیم ریزریو کردن (Address Reservation) IP

یکی از گزینه‌های که در اکسس‌پاینت و روترهای بی‌سیم وجود دارد، تنظیم ریزریو کردن تعدادی از آدرس‌ها است. اکسس‌پاینت‌ها قابلیت تنظیم و عیارسازی ریزریو کردن آدرس‌های IP را دارند. با این تنظیمات می‌توانیم تعدادی از آدرس‌های را که به هر دلیل نمی‌خواهیم به کلاینت‌ها توزیع گردد، در این لست نگه‌داری می‌کنیم. هدف از این کاربرد در اکسس‌پاینت‌ها این است که شبکه WLAN شما ممکن به تعدادی از آدرس‌ها نیاز دارد که باید به صورت ثابت به بعضی از دستگاه‌ها توزیع گردد. معمولاً، پرنت‌های شبکه، اسکرها، کمره‌ها، سرورها و غیره ضرورت دارند که تا به صورت ثابت (دستی) آدرس IP خود را دریافت کنند و هیچ‌گاه نیاز نیست که با گذشت زمان آدرس‌های آن تغییر کند. بنا بر این آدرس‌های مورد نیاز شبکه خود را که به صورت ثابت باید توزیع گردد، شامل این لست می‌نماییم. این آدرس‌ها هیچ‌گاه به کسی توزیع نمی‌گردد. جهت انجام این کار از گزینه add new استفاده می‌کنیم و آدرس مورد نظر را ذخیره می‌نماییم. علاوه بر آن می‌توانیم این آدرس‌ها را از لست حذف، تغییر ویا فعال و غیر فعال بسازیم. تمام گزینه‌های قابل استفاده به وضاحت در شکل ۴-۲۵ نشان داده شده است.



شکل ۴-۲۵: تنظیمات ریزریو آدرس‌های IP توسط DHCP

۴.۴.۲.۱۴ تنظیمات مسیریابی ثابت (Static Routing)

یکی از بخش‌های بسیار مهم و قابل تنظیم، گزینه مسیریابی در روترهای بی‌سیم است. طوری که از گذشته بیاد داریم؛ مسیریابی به دو نوع است، که عبارت از مسیریابی ثابت^{۸۵} و مسیریابی دینامیک^{۸۶} می‌باشد. در این نوع روترها، تنها روش مسیریابی ثابت داریم که در شکل ذیل نشان داده شده است. مطابق شکل ذیل مسیریابی ثابت، با استفاده از گزینه Add New می‌توانیم گزینه‌های شبکه هدف^{۸۷}، ماسک^{۸۸} و Gateway را تنظیم و عیارسازی نماییم.

^{۸۵}Static Routing

^{۸۶}Dynamic Routing

^{۸۷}Destination Network

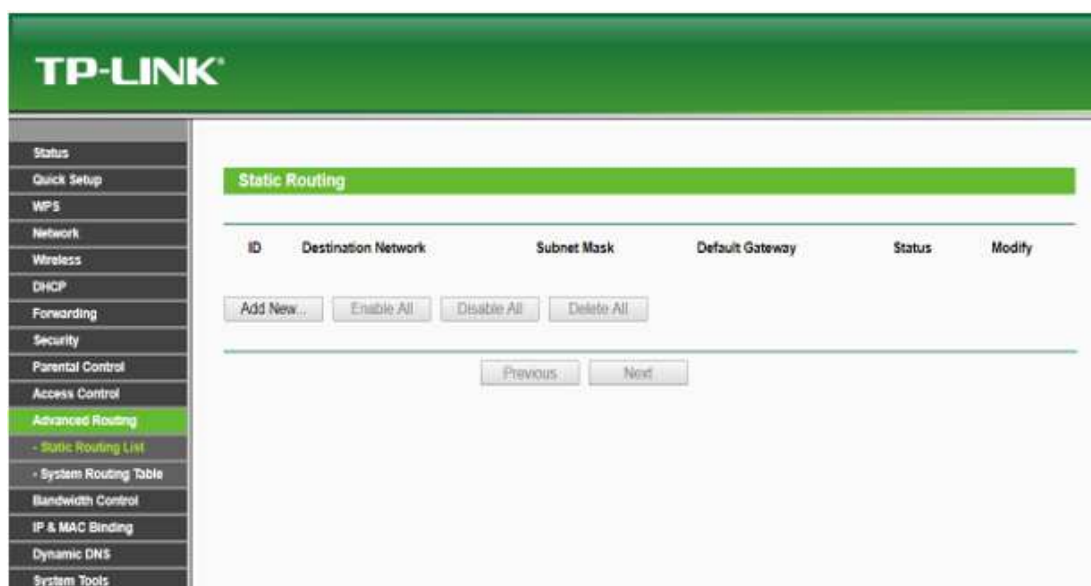
^{۸۸}Subnet Mask

شبکه هدف: در این بخش IP های اضافه می‌شود که تصمیم داریم اطلاعات را به آن شبکه و یا به آن هاست ارسال کنیم. به عبارت دیگر شبکه گیرنده و یا هاست گیرنده، به نام شبکه هدف است.

ماسک: هر IP که در بخش شبکه هدف قرار می‌گیرد، از خود ماسک مشخص دارد که تعداد بیت‌های شبکه و هاست را از هم‌دیگر جدا می‌کند. ماسک براساس کلاس‌های آدرس IP و یا جداسازی بخش شبکه و هاست تعریف می‌گردد.

Gateway: آدرس IP ای است که بین فرستنده و گیرنده قرار دارد و زمینه ارتباط و اتصال بین فرستنده و گیرنده را برقرار می‌کند.

وقتی که سه بخش فوق الذکر تکمیل گردد، جدول مسیریابی به صورت ثابت از این طریق فراهم می‌شود و روتر قادر به ارسال اطلاعات به شبکه‌های دیگر نیز می‌گردد. علاوه بر گزینه‌های یاد شده، گزینه‌های دیگر از قبیل Enable All, Disable All و Delete All را نیز داریم که می‌توانیم بالای این جدول اعمال نماییم. جزئیات تنظیمات مسیریابی ثابت در شکل ۴-۲۶ نشان داده شده است.



شکل ۴ - ۲۶: تنظیمات مسیریابی ثابت از طریق روتر بی‌سیم

۴.۴.۲.۱۵ مشاهده جدول مسیریابی (System Routing Table)

از این بخش صرف جهت دریافت معلومات و حصول اطمینان از صحت جدول مسیریابی استفاده می‌شود. قسمی که در شکل ۴-۲۷ ملاحظه می‌شود، دو شبکه هدف (آدرس IP) با ماسک‌های مربوطه، انترفیس‌های قابل استفاده و بدون تعیین کدام Gateway از آن استفاده شده است. مطابق معلوماتی که در ستون انترفیس مشاهده می‌شود، شبکه محلی LAN از طریق Gateway مربوطه به شبکه بیرونی WAN، از طریق این جدول مسیریابی وصل می‌گردد.

ID	Destination Network	Subnet Mask	Gateway	Interface
1	172.16.0.0	255.255.0.0	0.0.0.0	LAN & WLAN
2	209.0.0.0	255.0.0.0	0.0.0.0	LAN & WLAN

شکل ۴-۲۷: مشاهده کردن جدول مسیریابی ثابت

۴.۴.۲.۱۶ تنظیمات ناحیه دینامیکی (DDNS)

بخش دیگر تنظیمات در روترهای بی‌سیم، ناحیه دینامیکی است. با استفاده از این گزینه روتر می‌تواند تبدیل نام به آدرس و تبدیل آدرس به نام را به صورت خودکار انجام دهد. خدمات DDNS^{۸۹} در روترهای بی‌سیم، قابلیت دارد که برای استفاده از FTP سرور، سرور Web و یا بعضی سرورهای دیگر جهت تغییر آدرس به نام استفاده شود. هرگاه شما تعدادی از سرورهای خود را در داخل شبکه WLAN فعال نمایید، با استفاده از این قابلیت می‌توانید سرورهای خود را برای استفاده کنندگان بیرونی نیز قابل دسترس بسازید. البته شرایط این کار در این است که DDNS خود را در یکی از ISP ها راجستر نمایید. مطابق شکل ۴-۲۸ برای تنظیمات و تغییر احتمالی بعد از تنظیمات، ضرورت به یوزرنیم و پاسورد نیز می‌باشد. نام ناحیه^{۹۰} را می‌توانید به صورت دل‌خواه انتخاب کنید. در صورت ضرورت می‌توانید این خدمات را از طریق گزینه Enable DDNS فعال و غیر فعال کنید. در صورت تنظیمات موفقانه این سرویس و فعال کردن آن، برای استفاده مجدد باید از طریق یوزرنیم و پاسورد وارد DDNS شویم.

^{۸۹} Dynamic Domain Name System (DDNS)

^{۹۰} Domain Name

TP-LINK 300M Wireless N Router
Model No. TL-WR841N / TL-WR841ND

DDNS

Service Provider: No-IP (www.no-ip.com) [Go to register](#)

User Name:

Password:

Domain Name:

☐ Enable DDNS

Connection Status: DDNS not launching!

DDNS Help

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router. Before using this feature, you need to sign up with DDNS service providers such as [www.no-ip.com](#). The Dynamic DNS client service provider will give you a password or key.

Follow these instructions to set up DDNS:

If your selected dynamic DNS Service Provider is [www.no-ip.com](#):

1. Enter the **User Name** for your DDNS account.
2. Enter the **Password** for your DDNS account.
3. Enter the **Domain Name** you received from dynamic DNS service provider.
4. Click the **Login** button to login to the DDNS service.

Connection Status - The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

Notice: If you want to login again with another account after a successful login, please click the **Logout** button, then input your new username and password and click the **Login** button.

شکل ۴-۲۸: تنظیمات DDNS

۴.۴.۲.۱۷ تنظیمات زمان (Time Settings)

طوری که از عنوان این بخش معلوم می‌شود، تنظیم ساعت، تاریخ و کشور مربوطه از این طریق انجام می‌گیرد. تنظیم تاریخ و ساعت و موقعیت کشور همیشه در هماهنگی و سازگاری بین سیستم‌ها تاثیر دارد. لذا دقت در همه این بخش‌ها باعث کارایی سیستم و به‌خصوص در روترهای بی‌سیم می‌گردد. شکل ۴-۲۹ را مشاهده نمایید.

TP-LINK 300M Wireless N Router
Model No. TL-WR841N / TL-WR841ND

Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore

Date: 1/1/2012 (MM/DD/YY)

Time: 0:44:52 (HH:MM:SS)

NTP Server 1: 0.0.0.0 (Optional)

NTP Server 2: 0.0.0.0 (Optional)

☐ Enable Daylight Saving

Start: Mar 3rd Sun 2am

End: Nov 2nd Sun 3am

Daylight Saving Status: daylight saving is down.

Note: Click the "GET GMT" to update the time from the internet with the pre-defined servers or entering the customized server (IP Address or Domain Name) in the above frames.

Time Settings Help

This page allows you to set the time manually or to configure automatic time synchronization. The Router can automatically update the time from an NTP server via the Internet.

Time Zone - Select your local time zone from this pull-down list.

To set time manually:

1. Select your local time zone.
2. Enter the **Date** in Month/Day/Year format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

For automatic time synchronization:

1. Enter the address or domain of the **NTP Server 1** or **NTP Server 2**.
2. Click the **Get GMT** button to get GMT from the Internet.

To set up daylight saving:

1. Select the **Enable Daylight Saving** checkbox to enable daylight saving function.
2. Select the correct **Start time** and **End time** of daylight saving range.
3. Click **Save**.

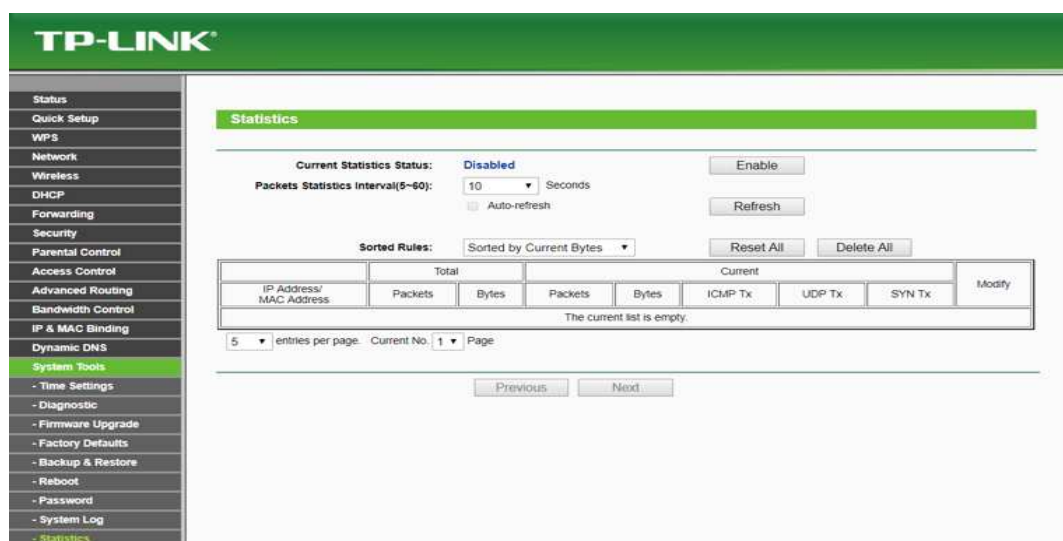
Note:

1. This setting will be used for some time-based functions such as firewall functions. These time dependent functions will not work if time is not set. Therefore, it is important to specify time settings as soon as you successfully login to the Router.
2. The time will be lost if the Router is turned off.
3. The Router will automatically obtain GMT from the Internet if it is configured accordingly.
4. In daylight saving configuration, start time and end time shall be within one year and start time shall be earlier than end time.
5. After you enable daylight saving function, it will take action in one minute.

شکل ۴-۲۹: تنظیمات تاریخ و کشور در روترهای بی‌سیم

مشاهده وضعیت استفاده کننده‌ها (Statistics)

این بخش به صورت بسیار همه جانبه وضعیت استفاده کننده‌ها و تعداد استفاده کننده را با تمام جزئیات آن نشان می‌دهد. شکل ۴-۳۰ را مشاهده نمایید.



شکل ۴-۳۰: مشاهده وضعیت فعلی روتر بی سیم از لحاظ ارسال بسته‌های اطلاعاتی

معلوم است که این بخش، آدرس‌های IP استفاده کننده‌ها، مجموع تعداد بسته‌های اطلاعاتی بر حسب بسته و بایت، وضعیت فعلی ارسال بسته‌ها و بایت‌ها، نوع بسته‌های فعلی و غیره را نمایش می‌دهد. مشاهده این بخش برای نگه‌داری و مدیریت شبکه و به خصوص در روترهای بی سیم نهایت مهم و موثر است. هم‌چنان این بخش می‌تواند برای پلان‌های مدیریتی شبکه، رفع نواقص، تهدیدات احتمالی، حملات جاری و غیره کمک کند. اگر دستگاهی یا کمپیوتری تشخیص گردد که بیش از حد معمول بسته‌های مبهم و نامعلوم می‌فرستد، معلوم است که نوع تهدید و حملات وجود دارد. اگر دستگاهی یا کمپیوتری که بیش از حد معمول اطلاعات می‌فرستد و تمام پهنای باند را مصروف نموده و از منابع استفاده بی مورد صورت می‌گیرد. در نهایت می‌توانیم برای بهبود وضعیت شبکه خود، پلان بهبودی ترتیب و اعمال نماییم.

در ادامه تعدادی از اکسس‌پاینت‌ها و روترهای بی سیم را که مربوط به شرکت‌های دیگر است، به صورت مختصر به معرفی می‌گیریم.

قابل یادآوری است که از لحاظ برند انواع مختلف اکسس‌پاینت‌ها و روترهای بی سیم در بازار وجود دارد، اما برحسب علاقمندی مشتریان، کارکرد بهتر، سادگی در تنظیمات و غیره موارد دیگر در این جا برند TP-LINK انتخاب گردیده و مطابق ضرورت به بخش‌های مهم عیارسازی آن پرداخته شده است. جهت یادآوری برندهای مهم اکسس‌پاینت‌ها و روترهای بی سیم قرار ذیل است.

- D – Link
- TP-LINK
- Linksys
- CISCO

- COM ۳
- ASUS
- SMC

نکته مهم این است که محیط تنظیمات از لحاظ ترتیب و جابه‌جایی گزینه‌ها در برندهای مختلف تفاوت‌های چشم‌گیر دیده می‌شود؛ اما از لحاظ روش، میتودهای مورد نیاز، عمل‌کرد و تعدد گزینه‌ها تفاوت‌های زیادی دیده نمی‌شود. در ادامه به‌صورت بسیار مختصر، از تمام برندهای فوق‌الذکر، تنها یک نوع دیگر از روترهای بی‌سیم به‌نام Linksys را معرفی می‌کنیم.

برند LinkSys مربوط به کمپنی سیسکو، علاوه بر ویژگی اکسس‌پاینت، ویژگی روترهای بی‌سیم را نیز دارد. این برند را در شکل ۴-۳۱ مشاهده نمایید.



شکل ۴-۳۱: اکسس پاینت و روتر بی‌سیم Linksys

محیط عیارسازی Linksys

طوری که قبلاً نیز یادآوری گردید، روترهای بی‌سیم از نوع Linksys نیز مشابه به TP-LINK بوده و دارای تمام گزینه‌های مورد ضرورت می‌باشد. اما جهت آشنایی و معرفی بیش‌تر محیط عیارسازی Linksys به شکل ذیل توجه نماید. در این شکل تمام بخش‌های مورد نیاز مانند: نسخه Firmware، نسخه سخت‌افزار، Basic Setup، DDNS، Wireless Settings، Security، Administration، Access Restrictions، Status، و غیره می‌باشد. به‌عبارت دیگر تمام گزینه‌های عیارسازی را در شکل ۴-۳۲ دیده می‌توانیم.

شکل ۴-۳۲: تنظیمات روترهای بی‌سیم از نوع Linksys

جهت معلومات بیش‌تر محیط عیارسازی Wireless Settings را در شکل ذیل در نظر بگیرید. طوری که در شکل ۴-۳۳ دیده می‌شود. در این بخش نیز به وضاحت دیده می‌شود که انتخاب استندردهای WLAN به نام Mode، نام شبکه به نام SSID، فریکونسی، عرض تشعشع، کانال‌های استندرد و در آخر فعال شدن و غیر فعال شدن SSID به وضاحت مشاهده می‌گردد که در تمام اکسس‌پاینت‌های دیگر نیز وجود دارد.

شکل ۴-۳۳: تنظیمات عمومی گزینه Wireless در اکسس‌پاینت Linksys

طوری که در شکل بالا دیده می‌شود، گزینه‌های تنظیمات با مقایسه نوع TP-LINK از لحاظ ترتیب متفاوت بوده است و از لحاظ نوع کارکرد و غیره باهم مشابه می‌باشد.

یادآوری مهم: تنظیمات و عیارسازی‌های امنیتی در اکسس‌پاینت‌ها و روترهای بی‌سیم در فصل بعدی به صورت جداگانه بحث گردیده است.



در این فصل بعد از معرفی مختصر اکسس پاینت، در مورد تنظیمات و قابلیت‌های اساسی آن به صورت همه جانبه پرداخته شد. در این فصل در ابتدا یاد گرفتیم که با استفاده از آدرس IP و یا لینک مربوطه، وارد اکسس پاینت می‌شویم. بعد از ورود به محیط تنظیمات، تمام گزینه‌های مهم و اساسی در اکسس پاینت همراه با قابلیت‌های روتر بی‌سیم از نوع TP-LINK را معرفی نمودیم. علاوه بر معرفی گزینه‌های قابل تنظیم، مثال‌های عملی تنظیمات روتر را یادآور شدیم. در این فصل تنظیمات نام شبکه، تنظیمات تغییر فریکانس‌ها و یا Mode، تنظیمات DHCP، تنظیمات کانال، تنظیمات DDNS، تنظیمات پیش‌رفته اکسس پاینت و غیره به صورت واقعی انجام شد. علاوه بر آن در اخیر به معرفی تنظیمات روتر بی‌سیم از نوع Linksys پرداخته شد. علاوه بر موارد فوق، تنظیمات مسیریابی ثابت و احصائی استفاده کننده‌ها و مشاهده وضعیت فعلی اکسس پاینت نیز معرفی گردید. چنانچه با تنظیمات دو نوع روترهای بی‌سیم آشنا شدیم، در نهایت نتیجه‌گیری این شد که تنظیمات اکسس پاینت‌ها و روترهای بی‌سیم شباهت‌های زیادی دارد. تنها گزینه‌های تنظیمات از لحاظ ترتیب و نام‌گذاری‌ها تفاوت‌های اندک دارد.



سوالات فصل چهارم

۱. اکسس پاینت را تعریف کنید.
۲. روش‌های لاگان شدن به اکسس پاینت را توضیح نمایید.
۳. گزینه‌های هم تنظیمات اکسس پاینت را لست کنید.
۴. هدف SSID در اکسس پاینت چیست؟
۵. اگر در مورد SSID، گزینه Disable انتخاب گردد، چی اتفاق می‌افتد.
۶. هدف از Mode در اکسس پاینت چیست؟
۷. کاربرد و موارد استفاده از Channel را بنویسید.
۸. قابلیت Bridgeing در اکسس پاینت کدام خدمات را فراهم می‌کند؟
۹. هدف از تنظیمات DHCP در اکسس پاینت چیست؟
۱۰. اگر در مورد DHCP، گزینه Disable انتخاب گردد، چی اتفاق می‌افتد.
۱۱. خدمات DDNS را توضیح بدهید.
۱۲. تنظیمات اکسس پاینت TP-LINK با اکسس پاینت Linksys چی فرق دارد؟
۱۳. خدمات Wi-Fi در اکسس پاینت چی وقت غیر فعال می‌گردد؟
۱۴. اکسس پاینت TP-LINK را طوری تنظیم کنید که به نام آن Practic-Group و تنها برای ۴۵ کامپیوتر آدرس IP توزیع کند.
۱۵. دو اکسس پاینت TP-LINK را از طریق قابلیت‌های Bridging با هم دیگر شان وصل کنید.

فصل پنجم

معرفی و تنظیمات امنیتی شبکه‌های بی‌سیم



هدف کلی: در مورد امنیت و تنظیمات امنیتی شبکه‌های بی‌سیم شناخت حاصل نمایند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. پروتوکول‌های امنیتی شبکه‌های بی‌سیم را معرفی کرده بتوانند.
۲. انواع حملات معمول در شبکه‌های بی‌سیم را نام گرفته بتوانند.
۳. عملکرد پروتوکول‌های WEP و WPA را توضیح داده بتوانند.
۴. تفاوت‌های اصلی WEP، WPA و WPA2 را بیان کرده بتوانند.
۵. روش MAC Filtering را معرفی کرده بتوانند.
۶. روش WEP و WPA را تطبیق کرده بتوانند.
۷. تنظیمات SSID و کنترل کردن دسترسی‌ها را انجام داده بتوانند.
۸. تنظیمات PSK را تطبیق کرده بتوانند.
۹. تنظیمات یوزرنیم و پاسورد سیستم را تطبیق کرده بتوانند.
۱۰. محدود سازی پهنای باند را تطبیق کرده بتوانند.

در این فصل روی موضوعات امنیتی در شبکه‌های بی‌سیم به صورت عموم بحث صورت گرفته است. علاوه بر معرفی پروتوکول‌های امنیتی و حملات احتمالی روی شبکه‌های بی‌سیم، تنظیمات امنیتی اکسس‌پاینت و روترهای بی‌سیم نیز انجام شده است. در بخش معرفی و آشنایی با پروتوکول‌های امنیتی؛ WPA، WEP و WPA2 نیز بحث شده است. جهت آشنایی با حملات در شبکه‌های بی‌سیم؛ چهار نوع حملات شناسایی گردیده است. هر حمله در عناوین جداگانه با مشخصات و جزئیات آن، همراه با روش راه حل‌های مناسب توضیح گردیده است.

بخش دیگر مهم این فصل تنظیمات امنیتی در شبکه‌های بی‌سیم است. تنظیمات امنیتی شامل، تغییرات تنظیمات پیش‌فرض، تنظیمات MAC Filtering، تنظیمات دسترسی به منابع، تنظیمات محدودیت‌های پهنای باند، تنظیمات امنیتی PSK، تنظیمات یوزرنیم و پاسورد سیستم یا محیط admin، تنظیمات بروز رسانی Firmware و غیره موارد دیگر است. هر کدام از بخش‌های فوق الذکر در تامین امنیت شبکه‌های بی‌سیم، اهمیت جداگانه دارد.

۵.۱ امنیت در شبکه‌های بی‌سیم

در ابتدا لازم است که تعریف مختصر از شبکه‌های بی‌سیم داشته باشیم. "شبکه بی‌سیم به افراد اجازه می‌دهد که به یک شبکه محلی یا اینترنت وصل شوند و بسته‌های اطلاعات را توسط امواج الکترومقناطیسی منتشر سازند". بنابر این ارسال و دریافت اطلاعات با استفاده از امواج، توسط فضا در محیط آزاد، بدون کیبل و لین فیزیکی صورت می‌گیرد. بنا بر این بحث امنیت شبکه‌های بی‌سیم به صورت جدی مطرح می‌شود، که آیا با نبود لین و خطوط فیزیکی ارسال و دریافت اطلاعات به صورت مطمئن صورت می‌گیرد یا خیر؟ از طرف دیگر برای کاربران مجاز در شبکه، باید دسترسی مطمئن به منابع شبکه فراهم شود، از هر جا و در هر زمان بدون کدام خطوط فیزیکی (به صورت بی‌سیم) از تمام خدمات شبکه مستفید شود.

نکته مهم دیگر؛ آیا ابزارهای امنیتی که از طرف مدیر شبکه طراحی و تطبیق می‌گردد، در نهایت پاسخ‌گوی نیازهای امنیتی است؟ یا این که کاربران نیز ملزم به رعایت بعضی نکات و محدودیت‌های امنیتی اند؟

به صورت عموم پروتوکول‌های امنیتی در شبکه‌های WLAN بر سه نوع ذیل است:

۱. Wired Equivalent privacy (WEP)

۲. WiFi Protected Access (WPA)

۳. WiFi Protected Access II (WPA2)

هر شبکه بی‌سیم از یکی از این پروتوکول‌ها جهت تامین امنیت اطلاعات در شبکه استفاده می‌کنند. برای این که متوجه باشیم کدام پروتوکول، امنیت بالاتری نسبت به پروتوکول دیگر دارد، لازم است در ابتدا پروتوکول‌ها را بشناسیم:

۵.۱.۱ پروتوکول امنیتی WEP

آنچه می‌توانیم از امنیت WEP بگوییم و نیازمند عملی شدن امنیت است، در عمل کرد و قابلیت‌های پروتوکول امنیتی WEP نیست. لذا پروتوکول WEP ضعیف‌ترین پروتوکول از نظر امنیت در شبکه‌های بی‌سیم است. پروتوکول WEP به هدف محرمانگی^{۹۱} به وجود آمد و معادل امنیت در سطح ارتباط سیمی بوده در سال ۱۹۹۷ در استانداردهای ۸۰۲.۱۱ شبکه Wi-Fi معرفی گردید. این پروتوکول امنیتی از روش رمزنگاری RC۴ استفاده می‌کند [۱۰]. چون مشکلات امنیتی در الگوریتم RC۴ نیز وجود دارد، یکی از مشکلات و ضعف الگوریتم WEP شده است. بررسی مشکلات الگوریتم RC۴ و آشنایی آن، در این کتاب نمی‌گنجد.

۵.۱.۲ پروتوکول امنیت WPA/WPA۲

این پروتوکول امنیتی شبکه‌های بی‌سیم از امنیت خوبی برخوردار است. پروتوکول WPA از لحاظ امنیتی بهبود یافته از WEP است. هم‌چنان پروتوکول WPA۲ از تکنالوژی امنیتی بالاتری نسبت به WPA استفاده می‌کند که خود نوع بهبود یافت و پیش‌رفته WPA است. به صورت معمول احتمال حملاتی که بالای WPA می‌رود، به چهار صورت ذیل انجام می‌پذیرد:

۱- هندشیک چهار طرفه (four-way handshake)

۲- بافر آور فلو (buffer over flow)

۳- برات فورس (brut force)

۴- شنود ترافیک (packet sniffer)

بهترین روش برای به دست آوردن پاسورد در این پروتوکول‌ها استفاده از روش بافر آور فلو می‌باشد؛ اما به دلیل این که به سختی می‌توان ابزارهای پیدا کرد که از روش بافر آور فلو پاسورد را بگیرند از روش‌های “هندشیک” و “برات فورس” به مراتب بیش‌تر استفاده می‌شود. از روش شنود ترافیک دقیقاً برعکس پروتوکول WEP بسیار کم‌تر استفاده می‌شود، چرا که در این پروتوکول پکت‌ها و ترافیک به صورت بسیار قوی (رمزنگاری) شده اند.

دست دادن چهار طرفه (four-way handshake): این روش بیش‌تر ارتباط بین اکسس پاینت و کلاینت را به قسم امن و مطمئن برقرار می‌کند. هرگاه اکسس پاینت با کلاینت احراز هویت^{۹۲} می‌کنند، در این جا بین این دو دستگاه کلیدهای احراز هویت مبادله می‌شود، در صورتی که کلید ضعیف باشد و یا روش نگهداری کلید درست نباشد، به جای کلاینت یک دستگاه مخرب جابه‌جا گردیده و عملیات هدفمند را در شبکه اعمال می‌کند.

^{۹۱} Privacy

^{۹۲} Authentification

بافر آور فلو (buffer over flow): این روش یک روش تضمینی است که تقریباً هر شبکه بی سیم را با هرگونه پیش گیری امنیتی می تواند مورد تهدید قرار دهد. این روش بافر کردن مودم، پسورد را به دست می آورد.

در این روش ابتدا هکر با استفاده از ارسال پکت های زیاد به سمت مودم هدف، باعث می شود بافر یا حافظه جانبی مودم را پر بسازد و به مرحله سرریز^{۹۳} برساند. مودم در عرض چند ثانیه در این حالت گیج می شود و هکر از همین زمان نهایت استفاده را می برد و از مودم درخواست می کند که پسورد خود را در اختیارش قرار دهد و از آن جایی که مودم در آن حالت نمی تواند تشخیص دهد که این دستور از طرف ادمین می باشد یا هکر، دستور را بدون کدام محدودیتی اجرا می کند و هکر پاسورد آن شبکه را به دست می آورد [۱۰].

برات فورس (brut force): این روش بر اساس حدس و گمان عمل می کند. به این منظور که شما در ابتدا رمز عبورهای تان را از بعضی کلمات ساده انتخاب کرده اید. هر وقت هکر خواسته باشد، تمام کلمات را در یک فایل پیش خود نگه داری می کند و به وسیله ابزارهای که در این زمینه هستند؛ هریک از کلمات را بر روی اکسس پاینت تست می کند. با این روش ممکن است پاسورد احتمالی شما در فایل باشد و اکسس پاینت شما مورد دست برد افراد دیگر قرار گیرد. تک آن رمزهای عبور احتمالی شما روی آن شبکه بی سیم تست می گردد.

اما موفقیت این روش به مراتب پایین تر از دو روش یاد شده است.

شنود ترافیک (Packet Sniffer): در این روش با استفاده از ابزارهای که وجود دارد، بسته های اطلاعاتی را مورد شنود قرار می دهند. در صورتی که الگوریتم رمزنگاری ضعیف باشد، این روش موفق خواهد بود. به عبارت دیگر، نوع حمله در این روش همانند حمله به پروتوکول WEP می باشد، ولی به دلیل این که در پروتوکول های WPA پکت ها به صورت رمز شده ارسال می شوند و چون هکر رمزنگاری قوی را می بیند به مراتب موفقیت خود را پایین تر احساس می کنند. اما اگر روش های لازم و مناسب را برای بهبود امنیت شبکه خود در نظر بگیریم و به صورت نکته به نکته شبکه خود را محدودتر کنیم، نفوذ هکرها سخت تر می شود. محدودیت های امنیتی قرار ذیل است:

- ۱- تغییر به پروتوکول امنیتی WPA۲؛
- ۲- انتخاب رمز عبوری امن برای شبکه های بی سیم؛
- ۳- تغییر پاسورد پیش فرض اکسس پاینت؛
- ۴- غیر فعال کردن WPS؛
- ۵- استفاده متداول از برنامه Who is on my WiFi؛
- ۶- فیلتر کردن اتصال از طریق MAC؛

⁹³ Over flow

۷- استفاده از shieleville؛

۸- SNIFF شبکه بی سیم به وسیله KISMET؛

تغییر به پروتوکول امنیتی WPA2: یکی از بهترین گزینه‌های انتخابی برای امنیت شبکه‌های بی سیم است. این پروتوکول نسبت به دیگر پروتوکول‌های امنیتی، امنیت بالاتری دارد. با داشتن این پروتوکول امنیتی، هکرها زمان لازم برای به دست آوردن پاسورد را ندارند [۱].

زمان ممکن برای به دست آوردن و نفوذ به این پروتوکول‌ها بین ۶ ساعت تا چند روز است. لذا به همین علت باعث می شود که نفوذگر از حمله بالای این پروتوکول اجتناب کند.

انتخاب رمز عبور امن برای شبکه بی سیم: قسمی که قبلاً اشاره شد، قابلیت حدس زدن و ساده بودن پاسورد می تواند سبب مشکلات امنیتی شود. اگر پاسورد شما امنیت لازم را نداشته باشد و به راحتی قابل حدس زدن باشد یک هکر به راحتی می تواند پاسورد شما را به دست آورد.

خیلی از افراد از قبیل شماره تلفن، تاریخ تولد، آدرس کوچه، نام شهر و غیره کلمات ساده را منحیث پاسورد شان استفاده می کنند. بنا بر این کلمات ساده قابل گمان بردن است و در یک فایل، هر کلمه به صورت یکی به یکی تست می گردد.

تغییر پاسورد پیش فرض اکسس پاینت: هر اکسس پاینت دارای یک پاسورد پیش فرض می باشد که بیش تر با یوزر و پاسورد admin می توانیم به اکسس پاینت وارد شویم. هم چنان هکرها نیز از یوزر و پاسورد پیش فرض آن کاملاً آگاهی دارند و با استفاده از آن به سادگی به اکسس پاینت شما وارد می شوند.

غیر فعال کردن WPS: این گزینه معمولاً برای امنیت شبکه‌های بی سیم است. اگر در همه سایت‌های اینترنتی هم جستجو کنید، فقط چیزهای مختلف در خصوص امن کردن از این ابزار می شنوید.

مثال: wifi protect setup

WPS مکانیزمی هست که به طور خودکار اطلاعات تبادلی میان دستگاه‌های Wi-Fi را رمزنگاری و امن می کند. این مکانیزم شامل تعریف رمز عبور، انتخاب پروتوکول رمزنگاری، اعتبار سنجی دستگاه‌های گیرنده و فرستنده اطلاعات و.... است.

در حقیقت تمامی کارهای که باید یک کاربر به طور دستی برای امنیت شبکه بی سیم انجام دهد، با زدن یک کلید انجام می گیرد. توجه کنید که تمامی دستگاه‌های درون شبکه شما باید از WPS پشتیبانی کند. به دلیل این که خودکار است و هر استفاده کننده را اجازه تنظیمات امنیتی نمی دهد، باید غیر فعال گردد.

استفاده متداول از برنامه Who is on my WiFi: این برنامه این امکان را به شما می دهد که در هر لحظه بدانید که کی ها و چند نفر به شبکه بی سیم شما متصل هستند. هم چنان به راحتی لست و نام کسانی را که از اکسس پاینت شما استفاده می کنند، مشاهده کرده می توانید.

فیلتر کردن اتصال از طریق MAC : در اکسس پاینت قابلیت دیگری وجود دارد که شما می‌توانید از طریق آدرس MAC، تمام افراد غیر مجاز را محدود بسازید. این تنظیمات به دوشکل صورت می‌گیرد. اول، هرکمیپوتری قابل اعتماد است، آدرس MAC آن در لیست استفاده کنندگان مجاز اضافه می‌شود. دوم، هرکمیپوتری که قابل اعتماد نیست، آدرس MAC آن در لیست استفاده کنندگان غیر مجاز اضافه می‌شود. در این روش هرکس به هرصورتی که بتواند پاسورد شبکه را به‌دست آورد، قادر نخواهد بود که به‌شبکه متصل شود.

تقسیم بندی بالا از دید امنیتی کلی و عمومی بوده است و بیش‌تر بررسی بخش نظری و چالش‌های امنیتی پروتوکول‌های امنیتی را مرور کردیم. اما از دید دیگر نیز تقسیم بندی امنیتی شبکه‌های بی‌سیم وجود دارد. از دید دیگر به لحاظ عملی، تنظیمات امنیتی شبکه بی‌سیم را بخش‌های مختلف تقسیم بندی می‌کنند. این تقسیم بندی مهم‌تر از تقسیم بندی قبلی است.

به‌صورت عموم چهار روش امنیتی در شبکه‌های بی‌سیم جهت تامین امنیت و تنظیمات امنیتی شبکه بی‌سیم مورد استفاده قرار می‌گیرد.

۱. WEP: این اصطلاح برگرفته شده از Wired Equivalent Protocol/Privacy است. در این روش از شنود استفاده کنندگان که در شبکه مجوز ندارند، جلوگیری به‌عمل می‌آید. این روش امنیتی بیش‌تر در شبکه‌های کوچک قابلیت استفاده دارد و برای آن مناسب‌تر است. زیرا در این روش نیاز به تنظیمات دستی کلید (Key) مربوطه در هر Client می‌باشد. روش رمزنگاری WEP براساس الگوریتم RC۴ به‌وسیله الگوریتم RSA کار می‌کند. دلیل که الگوریتم RC4 در تولید کلید ضعف دارد، لذا روش WEP، یک روش رمزنگاری موفق نمی‌باشد.

۲. WPA/WPA۲: این اصطلاح برگرفته شده از Wi-Fi Protected Access است. این روش الگوریتم رمزنگاری WPA نیز براساس الگوریتم RC۴ کار می‌کند. لذا روش پیش‌رفته‌تر آن، الگوریتم رمزنگاری WPA۲ است که به‌وسیله AES کار می‌کند. این روش از امنیت و کارایی خوبی برخوردار است. [۱۰]

۳. SSID: این اصطلاح برگرفته شده از Service Set Identifier است. هر شبکه WLAN دارای یک نام و مشخصه می‌باشد. لذا هر شبکه محلی دارای یک شناسه (Identifier) منحصر به فرد می‌باشد که برای شناسایی شبکه WLAN استفاده می‌شود. این شناسه‌ها در Access Point تنظیم می‌گردد و مطابق آن تمام Clients ها خود را تنظیم می‌کنند. هر کاربر برای دسترسی به شبکه مورد نظر خود باید تنظیمات SSID مربوطه را انجام دهد.

۴. MAC Filtering: هدف از MAC همان آدرس فیزیکی است که به‌نام Media Access Control یاد می‌شود. در این روش لستی از آدرس‌های MAC مورد نظر را در یک Access Point ذخیره می‌نمایند و تمام Client هایی که آدرس MAC شان ذخیره شده باشند، اجازه استفاده از شبکه را دارند. به‌عبارت دیگر آدرس MAC هر کمیپوتر که در Access Point ذخیره نباشد، توانایی استفاده از شبکه و منابع شبکه مانند اینترنت را ندارند. در این روش همیشه آدرس‌های کمیپوتر با لستی از آدرس‌های

MAC در داخل Access Point مقایسه می‌گردد و مطابق آن لست در خواست‌ها اجرا می‌گردد. این روش امنیتی برای شبکه‌های کوچک مناسب بوده و برای شبکه‌های بزرگ استفاده ندارد. زیرا در شبکه‌های بزرگ امکان ورود این آدرس‌ها از لحاظ زیادی به Access Point ها بسیار مشکل می‌باشد. در ادامه، مواردی که از لحاظ امنیتی اهمیت بیش‌تر دارند و از طرف دیگر قابل عیارسازی اند، مطابق به مفردات درسی این کتاب به آن پرداخته می‌شود.

۵.۲ تنظیمات امنیتی اکسس پاینت و روترهای بی‌سیم

تنظیمات امنیتی در اکسس پاینت ها و روترهای بی‌سیم، بخش‌های مختلف داشته که در ادامه به نکات مهم آن پرداخته می‌شود.

۵.۲.۱ تنظیمات امنیتی شبکه بی‌سیم (Wireless Security)

در محیط تنظیمات امنیتی دو گزینه مهم و اساسی وجود دارد. گزینه اول این که شبکه WLAN از لحاظ امنیتی کدام مشکل نداشته و تنظیمات امنیتی را غیر فعال (Disable Security) می‌کنیم. گزینه دوم این که WLAN در امنیت کامل نبوده و ضرورت به فعال شدن تنظیمات امنیتی است. تنظیمات امنیتی شامل تعدادی از الگوریتم‌های امنیتی است که در عنوان قبلی به آن پرداخته شده است. اگر شما از الگوریتم‌های امنیتی (WPA/WPA2 (Recommended استفاده می‌کنید، ضرورت به وارد کردن یک پاسورد PSK^{۹۴} نیز دارید. الگوریتم PSK از خود یک کلید (پاسورد) مشترک برای تمام استفاده کننده‌های WLAN فراهم می‌کند. همه افرادی که این پاسورد به دسترس شان قرار می‌گیرد، از آن به صورت مشترک استفاده می‌کنند. برای استفاده این الگوریتم زمان ضرورت است که هر استفاده کننده از طریق کمپیوتر، موبایل و تبلت خود به اکسس پاینت وصل شوند. در زمان وصل شدن به اکسس پاینت این پاسورد توسط اکسس پاینت خواسته می‌شود. در صورتی که پاسورد درست و دقیق باشد، این فرد مجاز شناخته می‌شود. به عنوان مثال در شکل ذیل این پاسورد "accesspoint۱۰" معرفی شده است. البته الگوریتم که امنیت این پاسورد را تامین می‌کند، به نام الگوریتم AES معرفی شده است.

گزینه دیگر، اگر از الگوریتم WPA/WPA2-Enterprise استفاده شود، در این صورت ضرورت به Radios سرورها دارید. به عبارت دیگر سرورهای جداگانه ضرورت است که مسئولیت احراز هویت^{۹۵} افراد مجاز و غیر مجاز را به عهده گیرد. این سرورها را به نام Radios Server ها یاد می‌کنند. این حالت پیچیدگی، تنظیمات و هزینه زیادی ضرورت دارد. در صورتی که اهمیت شبکه‌های WAN زیاد باشد و ملاحظات امنیتی شدیداً قوی باشد، نیاز به امنیت بیش‌تر دارید و بهتر است از این گزینه استفاده شود.

^{۹۴}Pre Shared Key

^{۹۵}Autintication

در روش Radios سرورها، علاوه بر اکسس پاینت، سرور جداگانه تمام یوزرنیمها و پاسوردها را در خود ذخیره نموده و احراز هویت از طریق این سرور انجام می‌شود. بنا بر این مسئله تنظیمات را پیچیده تر می‌سازد. به جزئیات این‌ها در شکل ۵-۱ توجه نمایید.

شکل ۵-۱: تنظیمات امنیتی PSK در اکسس پاینت

۵.۲.۲ تنظیمات فیلتر شدن آدرس MAC (MAC Filtering)

فلتر کردن آدرس‌های MAC یکی از گزینه‌های قوی و معتبر در تامین امنیت شبکه‌های WLAN است. در روش فلتر کردن آدرس MAC، اکسس پاینت‌ها و روترهای بی‌سیم براساس آدرس MAC استفاده کنندگان تصمیم می‌گیرند. این تصمیم بستگی به نوع پالسی و سیاست مدیر شبکه دارد. ممکن است لستی از MAC آدرس‌ها را اجازه دهد که از شبکه استفاده کند و یا ممکن است این لست را اجازه ندهد تا از منابع و خدمات شبکه استفاده کند. در این روش آدرس‌های MAC هر کامپیوتر، لپ‌تاپ، تبلت، موبایل و غیره در یک لست ثبت می‌شود. این لست جهت احراز هویت استفاده کنندگان توسط اکسس پاینت استفاده می‌شود.

طوری که در شکل ۵-۲ دیده می‌شود، دو نوع سیاست کلی برای این روش وجود دارد.

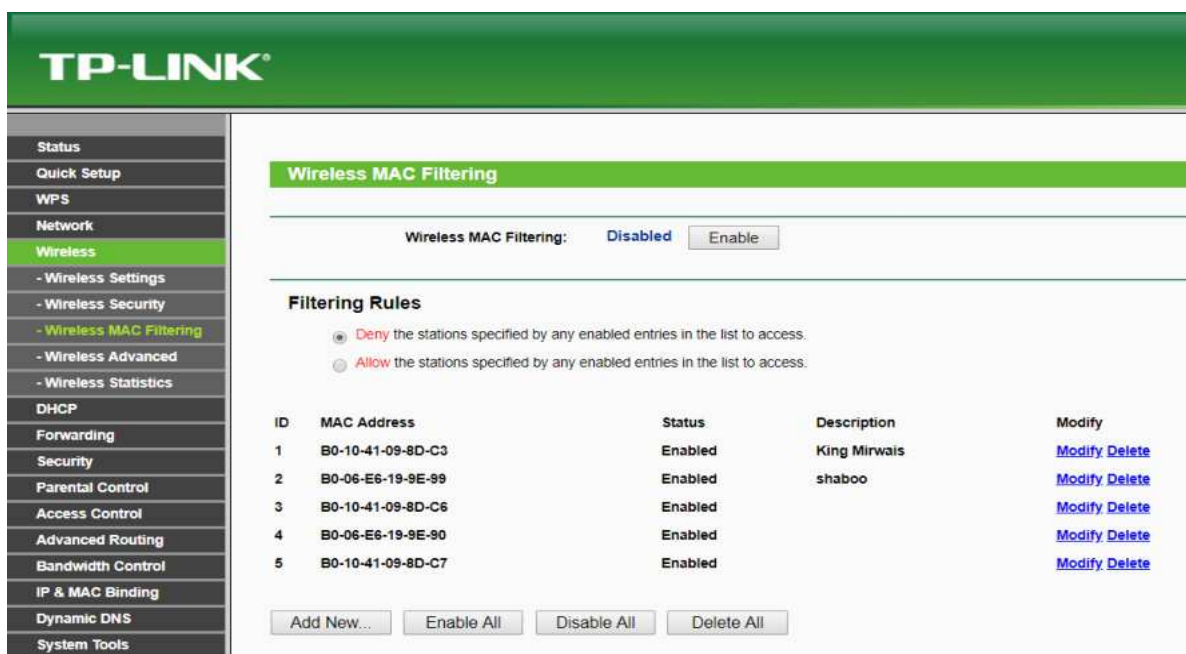
سیاست اول: لست آدرس‌های MAC که در اکسس پاینت موجود است، جهت استفاده از منابع و خدمات شبکه ممنوع (Deny) است.

سیاست دوم: لست آدرس‌های MAC که در اکسس پاینت موجود است، جهت استفاده از منابع و خدمات شبکه اجازه (Allow) است.

در ادامه دیده می‌شود که تعدادی از آدرس‌های MAC در لیست ذخیره شده است. این لیست فعلاً به دلیل انتخاب گزینه اولی، برای استفاده مجاز نیست. در صورتی که خواسته باشیم این لیست را ادامه بدهیم از گزینه Add New می‌توانیم استفاده کنیم. علاوه بر آن مطابق ضرورت از گزینه‌های Enable All، Disable All، Delete All نیز می‌توانیم استفاده کنیم. به عبارت دیگر تمام لیست را می‌توانیم با انتخاب یک گزینه فعال، غیر فعال و حذف کنیم.

هم‌چنان مطابق شکل ذیل، می‌توانیم فعالیت فلتر کردن MAC را فعال و یا مطلقاً غیر فعال کنیم.

یادآوری: تنظیمات فلتر شدن MAC، قوی‌ترین، نهایی‌ترین، موثرترین و کاربردی‌ترین گزینه برای تامین امنیت شبکه WLAN است. جزئیات این موضوع را در شکل ۵-۲ ملاحظه نمایید.



شکل ۵-۲: تنظیمات فلتر کردن آدرس MAC

۵.۲.۳ ارتقای لخت‌افزار (Firmware Upgrade)

ارتقای^{۹۶} لخت‌افزار یا Firmware یکی از گزینه‌های است که در اکسس‌پاینت‌ها و روترهای بی‌سیم وجود دارد. با استفاده از این گزینه، Firmware قابل ارتقا است. اما باید متوجه باشیم که از کدام منبع ارتقای لخت‌افزار را انجام می‌دهیم. طوری که در شکل زیر دیده می‌شود، دو گزینه (محلی و آنلاین) برای ارتقای لخت‌افزار در نظر گرفته شده است.

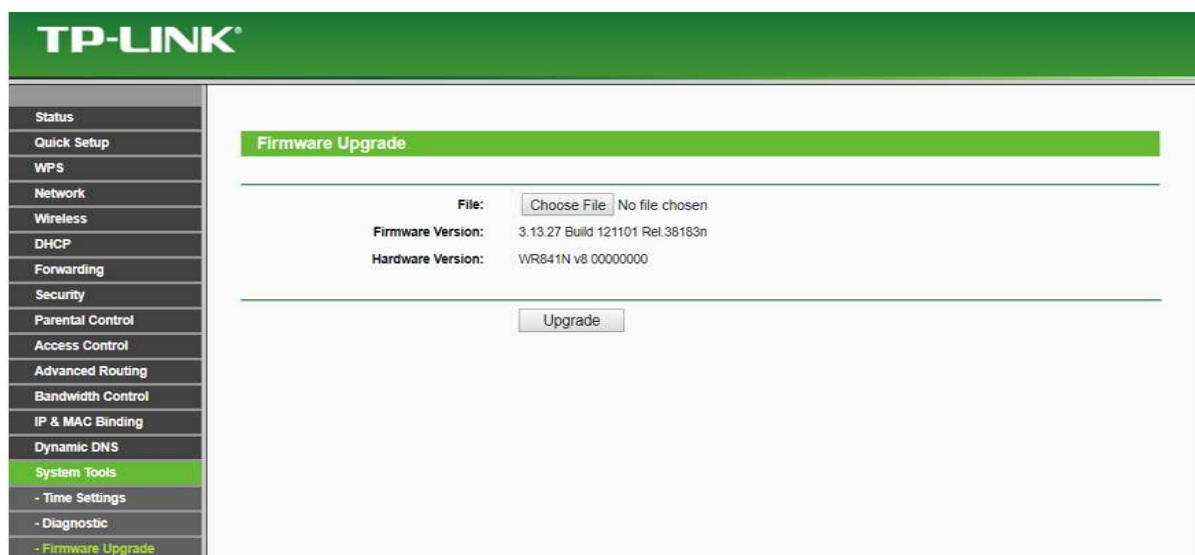
در روش محلی^{۹۷}؛ فایل ارتقا قبل از این مرحله باید در کامپیوتر شما ذخیره شده باشد. هم‌چنان این فایل باید از منابع معتبر و با اطمینان کافی دریافت شده باشد. هیچ‌گاه فایل آلوده، مخرب، نفوذگری و غیر نباشد.

^{۹۶} Upgrade

^{۹۷} Choose File

همیشه کوشش شود که از وبسایت‌های معتبر و از کمپنی‌های معتبر، توسط کمپیوتر دانلود گردد. در ادامه از کمپیوتر خود به صورت محلی روی اکسس‌پاینت و یا روتر بی‌سیم، بارگزاری^{۹۸} شود.

در روش آنلاین^{۹۹}؛ در همین لحظه به‌صورت آنلاین باید از طریق اینترنت و از وبسایت‌های معتبر باید ارتقای لخت‌افزار صورت گیرد. در این روش قبل از ارتقای لخت‌افزار، باید منابع ارتقا تست و شناسایی گردد. اعتبار و اطمینان وبسایت آن با دقت تمام و سرتفکت آن کمپنی شناسایی شود. هیچ‌گاه فایل آلوده، مخرب، نفوذگر و غیره نباشد. همیشه کوشش شود که از وبسایت‌های معتبر و از کمپنی‌های معتبر توسط کمپیوتر دانلود گردد. علاوه بر آن در وقت ارتقا، نهایت به اتصال^{۱۰۰} اینترنت خود توجه داشته باشیم و از اتصال اینترنت مطمئن استفاده کنیم. هم‌چنان نباید جریان دانلود و گرفتن فایل ارتقا قطع و یا به‌سکتگی مواجه شود. در صورت قطع شدن اتصال اینترنت، باید مراحل انجام ارتقا از اول شروع گردد. شکل ۵-۳ دو روش ارتقای لخت‌افزار را نشان می‌دهد.



شکل ۵-۳: ارتقای لخت‌افزار در روترهای بی‌سیم

۵.۲.۴ تنظیمات پیش فرض (Factory Default)

در اکسس‌پاینت‌ها و روترهای بی‌سیم گاهی نیاز است که به تنظیمات اولیه^{۱۰۱} (تنظیمات کمپنی) خود برگردانده شود. این گزینه در بسیار حالت‌ها ضرورت است که تنظیمات اکسس‌پاینت و روترهای بی‌سیم از بین برده شود و به تنظیمات اولیه برگردانده شود. در وقتی که پاسوردهای اکسس‌پاینت فراموش گردد و به دلایل مختلف گاهی عمل کرد درست نداشته باشد، ضرورت می‌شود که به تنظیمات اولیه آن برگردانده شود.

^{۹۸}Upload

^{۹۹} Online

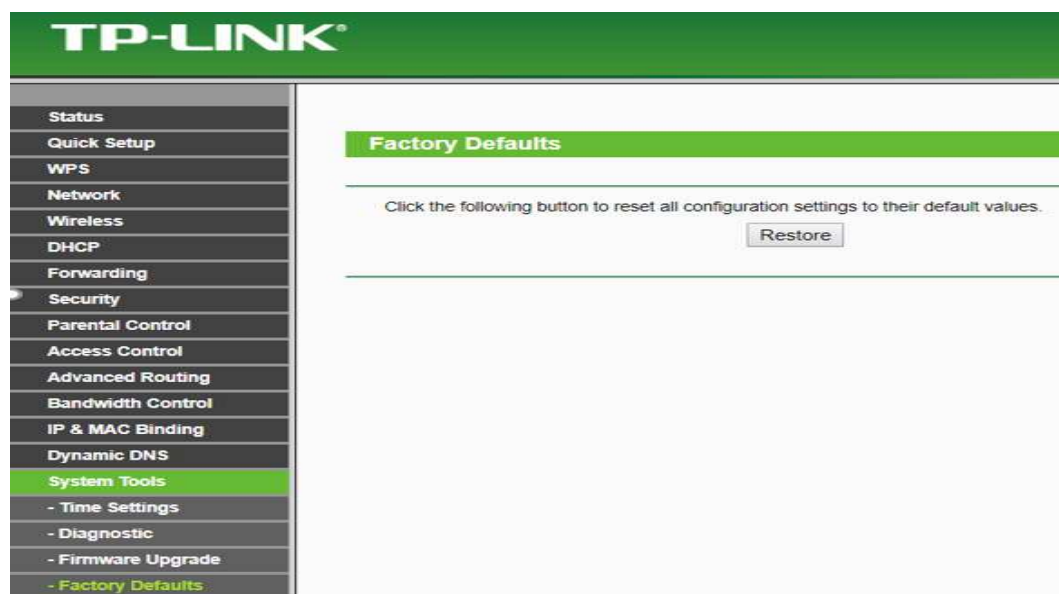
^{۱۰۰}Connections

^{۱۰۱}Default Factory Settings

نکته مهم این است که برگرداندن به تنظیمات اولیه، به دو حالت ممکن است. حالت اول از طریق تنظیمات اکسس پاینت، مطابق شکل زیر و حالت دوم از طریق دکمه Reset از بیرون دستگاه انجام می شود. در حالت دوم باید دکمه Reset را تا وقتی فشار داده نگه داریم که تمام چراغ های روتر بی سیم، روشن گردد. بعد از روشن شدن تمام چراغ های روتر، روتر بی سیم، به حالت تنظیمات اولیه یعنی کمپنی خود قرار خواهد گرفت. وقتی یک اکسس پاینت و یا روتر بی سیم به حالت اولیه خود قرار گیرد، به معنی این است که تنظیمات قبلی شما حذف گردیده است و تنظیمات اولیه کمپنی فعال گردیده است.

تنظیمات پیش فرض چیست؟

هر اکسس پاینت و روتر بی سیم از خود تنظیمات پیش فرض دارد. این تنظیمات عبارت از تنظیماتی است که به صورت پیش فرض بار اول در کمپنی انجام می گیرد و بعد از بسته بندی با همان تنظیمات کمپنی به بازار و مارکیت های فروش، عرضه می شود. به عنوان مثال تنظیمات اولیه در یک اکسس پاینت عبارت از: آدرس IP، یوزرنیم، پاسورد، نام شبکه (SSID) و غیره موارد دیگر است. هر کدام از این موارد در تمام اکسس پاینت های یک برند، یکسان و مشابه می باشد. در برند TP-LINK آدرس IP پیش فرض ۱۹۲.۱۶۸.۱.۱ و یوزرنیم و پاسورد پیش فرض admin و نام شبکه (SSID) آن TP-LINK است. از این جهت به لحاظ امنیتی هیچگاه نباید یک روتر بی سیم و یا اکسس پاینت به صورت تنظیمات اولیه آن مورد استفاده قرار گیرد. بلکه در اولین فرصت باید تنظیمات اولیه آن تغییر داده شود و بعد مورد استفاده قرار گیرد. دلیل در این است که تنظیمات کمپنی برای همه اکسس پاینت ها یکسان است و همه افراد تخریکی و مسلکی به شمول هرکرا از این تنظیمات اطلاع کامل دارد. لذا افراد عادی نیز می تواند از این تنظیمات سوء استفاده نماید. شکل ۴-۵ نشان می دهد که جهت حذف تنظیمات خود از گزینه Restore استفاده نماییم. به عبارت دیگر با استفاده از گزینه Restore می توانیم اکسس پاینت را به تنظیمات کمپنی ببریم.

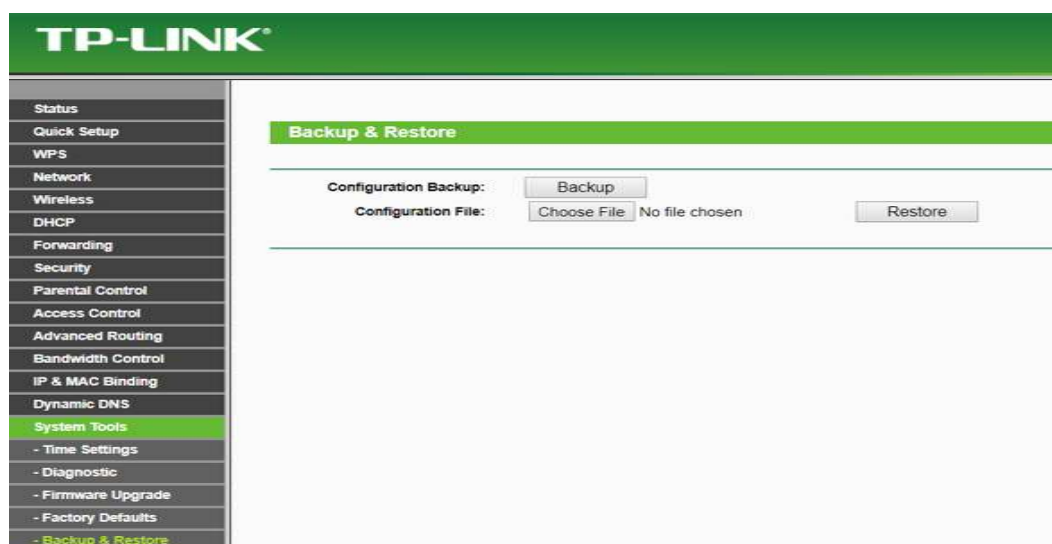


شکل ۴-۵: تنظیمات پیش فرض از طریق گزینه Restore

۵.۲.۵ تنظیمات Restore و backup

گزینه backup: در صورتی که مدیر شبکه خواسته باشد که از تمام تنظیمات روتر بی‌سیم و یا اکسس‌پاینت، کاپی احتیاطی پیش خود نگهداری نماید، از گزینه backup استفاده می‌کند. تنظیمات Backup به‌هدف کاپی گرفتن فایل تنظیمات است که در صورت ضرورت از آن استفاده دوباره استفاده می‌گردد. جهت درک مطلب به شکل زیر توجه نمایید.

گزینه Restore: این گزینه جهت استفاده از فایل backup استفاده می‌شود. به‌بیان دیگر؛ وقتی خواسته باشیم که فایل backup را روی اکسس‌پاینت و یا روتر بی‌سیم اجرا کنیم؛ از گزینه Restore استفاده می‌کنیم. توصیه مدیریتی و امنیتی شبکه این است که همیشه از تنظیمات خود backup داشته باشیم و در صورت ضرورت آن‌را دوباره Restore نماییم. شکل ۵-۵ به‌وضاحت نشان می‌دهد که با استفاده از گزینه Backup فایل تنظیمات دانلود و به‌کمپیوتر ما ذخیره می‌شود. اما گزینه Restore زمانی استفاده می‌گردد که فایل را در کمپیوتر و یا سرورهای داخلی خود داشته باشیم و آن‌را روی روتر خود دوباره اجرا کنیم.



شکل ۵-۵: تنظیمات کاپی گرفتن فایل عیارسازی و استفاده دوباره آن (Backup and Restore)

۵.۲.۶ تنظیمات یوزرنیم و پاسورد سیستم

یکی از مسایل مهم امنیتی در روترهای بی‌سیم، تعریف یوزرنیم و پاسورد جدید برای سیستم است. این یوزرنیم و پاسورد توسط مدیر شبکه^{۱۰۲} در وقت ورود به سیستم (محیط عیارسازی) مورد استفاده قرار می‌گیرد. بنا بر این، این یوزرنیم و پاسورد به‌صورت کل برای تمام بخش‌های شبکه مهم و اساسی است. در صورت افشا شدن این لایه امنیتی، تقریباً تمام امکانات و خدمات شبکه، مورد دستبرد افراد مخرب قرار خواهند گرفت. به

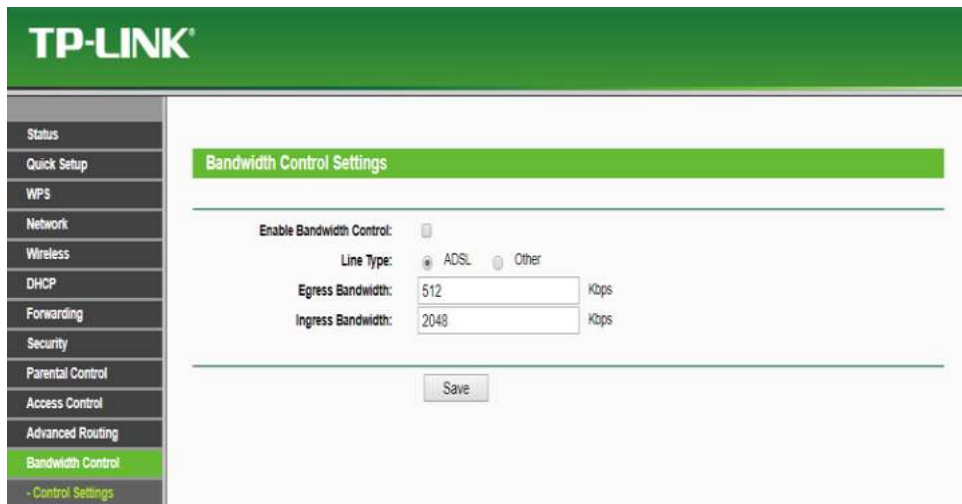
عبارت دیگر، وقتی یوزرنیم و پاسورد روتر شبکه به دسترس افراد غیر مجاز قرار گیرد، تقریباً تمام منابع در اختیار شان است.

نکته مهم: در عنوان قبلی در مورد Restore کردن به هدف Reset کردن روتر توضیح داده شد. اگر روتر بی سیم و یا اکسس پاینت Reset گردد، تمام تنظیمات به شمول یوزرنیم و پاسورد سیستم، به حالت اولی (تنظیمات کمپنی) قرار می گیرد. از طرف دیگر می دانیم که یوزرنیم و پاسورد اکسس پاینت ها به صورت پیش فرض، admin است و هر کسی از آن اطلاع دارد و می تواند به نفع شخصی خود سوء استفاده نماید. شکل ۵-۶ جزئیات این تنظیمات را نشان می دهد.

شکل ۵-۶: تنظیمات یوزرنیم و پاسورد سیستم

تنظیمات کنترل کردن پهنای باند (Bandwidth Control Settings)

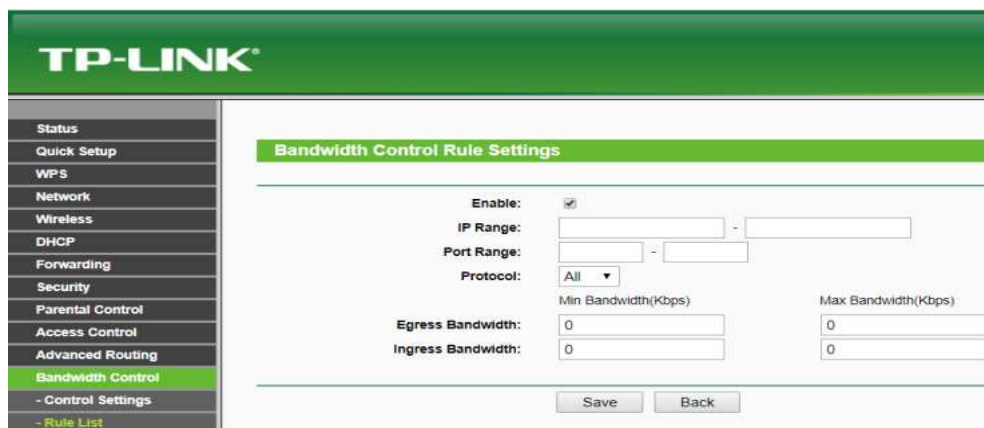
با استفاده از تنظیم پهنای باند می توانیم به صورت عمومی اطلاعات ورودی و خروجی روی اکسس پاینت و یا روتر بی سیم را کنترل کنیم. این گزینه برای محدود سازی استفاده از اینترنت و یا منابع دیگر شبکه می تواند موثر باشد. به عنوان مثال: چندین شبکه WLAN داریم که در نهایت همه این ها از طریق یک اتصال عمومی به اینترنت وصل است. حالا ضرورت است که پهنای باند کلی را بالای هر کدام تقسیم کنیم تا تمام شبکه های WLAN از دسترسی به اینترنت مستفید گردد. مطابق شکل زیر دو محدودیت را می توانیم اضافه کنیم. مقدار معلوماتی که از طریق این روتر خارج می شود، به نام Egress و مقدار معلوماتی که به روتر وارد می شود به نام Ingress یاد می شود. هر دو گزینه را می توان بر حسب کیلو بایت بر ثانیه محدود و یا کنترل کنیم. در شکل ۵-۷ این مقدار به ترتیب ۵۱۲ کیلو بایت بر ثانیه و ۲۰۴۸ کیلو بایت بر ثانیه در نظر گرفته شده است.



شکل ۵-۷: تنظیمات کنترل کردن پهنای باند روی روتر بی سیم

۵.۲.۷ تنظیمات کنترل پهنای باند بر اساس محدوده آدرس IP

این تنظیمات براساس محدوده آدرس IP، پورت و پروتوکول انجام می شود. قسمی که در شکل دیده می شود، با استفاده از اضافه کردن محدوده از آدرس های IP می توانیم، پهنای باند را کنترل کنیم. به عبارت دیگر می توانیم به تعدادی از کامپیوترهای که ضرورت کم تر به اینترنت دارند و یا به تعداد پروتوکول هایی که ضرورت به استفاده آن در شبکه نیست، بهتر است که حق استفاده از اینترنت را محدود بسازیم. انعطاف پذیری این تنظیمات در این است که با استفاده از Min Bandwidth و Max Bandwidth می تواند حداقل و حد اکثر استفاده از پهنای باند را محدود بسازیم. جزئیات بیش تر را در شکل ۵-۸ مشاهده نمایید.

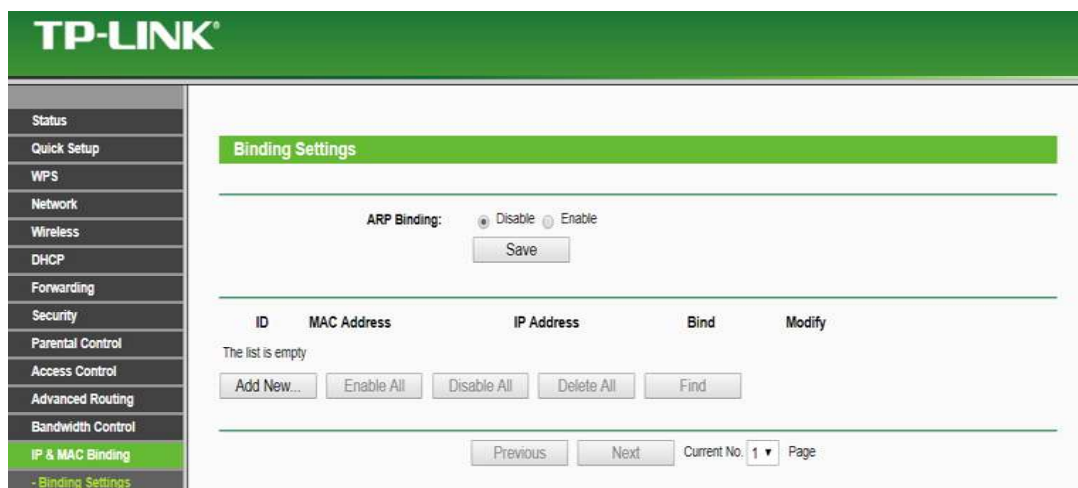


شکل ۵-۸: تنظیمات محدودسازی پهنای باند براساس آدرس IP و پروتوکول

۵.۲.۸ محدود کردن کامپیوترهای مشخص (Binding Settings)

محدود کردن دسترسی بعضی کامپیوترهای، یکی از گزینه های دیگر در روترهای بی سیم است. با استفاده از این گزینه می توانیم تعدادی از آدرس های IP همراه با آدرس MAC آنرا شامل لست بسازیم. در این صورت این کامپیوتر در محدوده کنترل شده قرار گرفته و نمی تواند از شبکه LAN استفاده کند. ممکن بعضی کامپیوترها به لحاظ امنیتی از دسترسی به LAN محروم گردد. مطابق شکل ذیل می توانیم این گزینه را برای

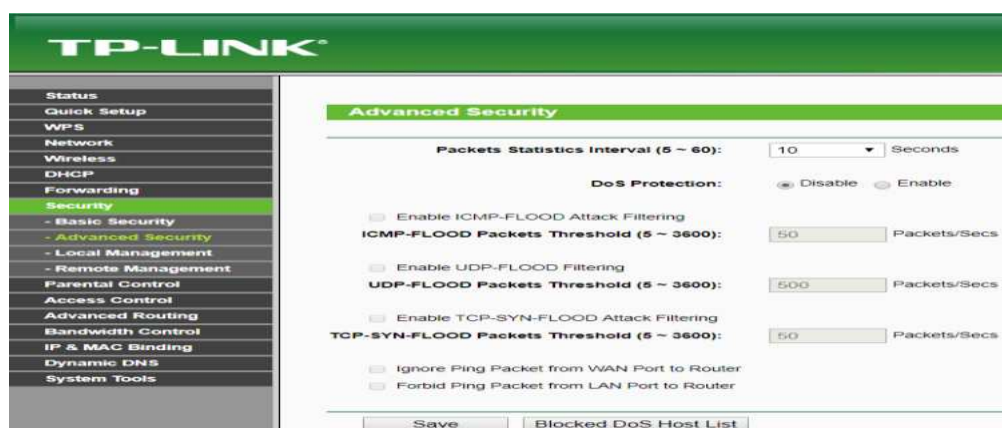
تعدادی از کمپیوترها فعال و یا در صورت ضرورت غیر فعال کنیم. جهت معلومات بیشتر به شکل ۵-۹ توجه نمایید.



شکل ۵-۹: محدود کردن کمپیوترهای مشخص از شبکه LAN

تنظیمات پیشرفته امنیتی (Advanced Security)

در این بخش از تنظیمات امنیتی باید با دقت بیشتر توجه داشته باشیم. با استفاده از این تنظیمات می‌توانیم از حملات و تهدیدات احتمالی که بالای کارایی شبکه تاثیر منفی می‌گذارد، باید جلوگیری کنیم. این حملات و تهدیدات احتمالی، حملات DoS، ICMP-Flood Attack، UDP-Flood، TCP-SYN-Flood، انجام بیش از حد دستور ping و غیره موارد دیگر را در بر می‌گیرد. طوری که در شکل زیر دیده می‌شود، تعداد بسته‌ها^{۱۰۳} برحسب ثانیه قابل تنظیم است. به اطمینان گفته می‌توانیم که تنظیمات این بخش امنیتی بالای کارایی شبکه و عمل کرد روتر بی‌سیم نهایت موثر واقع می‌شود. از طرف دیگر از حملات و تهدیدات احتمالی پیش‌گیری می‌نماید. جزئیات این را در شکل ۵-۱۰ ببینید.

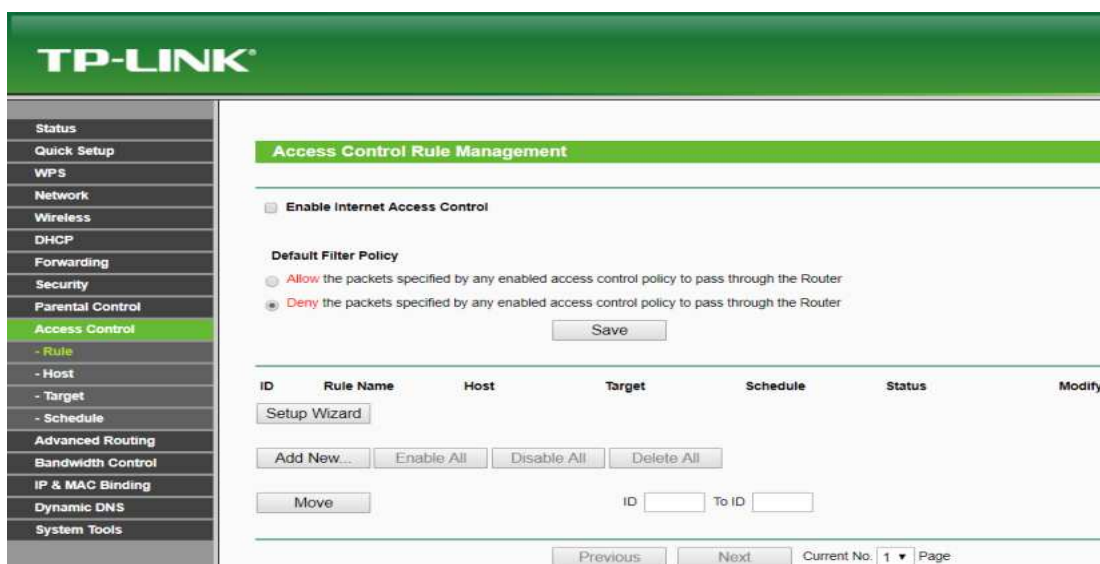


شکل ۵-۱۰: تنظیمات پیشرفته امنیتی

¹⁰³Packets

۵.۲.۹ تنظیمات کنترل دسترسی‌ها (Access Control Management)

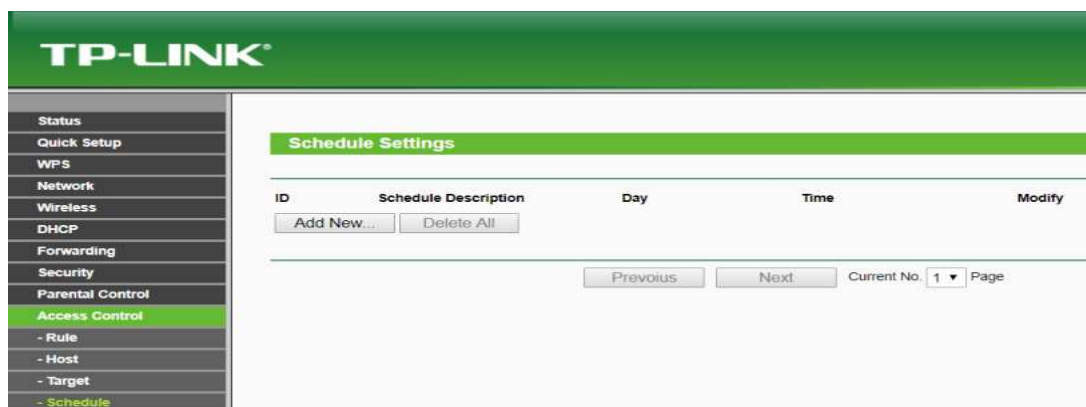
اولین امکانات این بخش فعال کردن کنترل دسترسی به اینترنت است. لذا با استفاده از کنترل دسترسی می‌توانیم نوع بسته‌های مشخص شده را اجازه و یا منع نماییم. خوبی دیگر این گزینه در این است که می‌توانیم هاست‌های مشخص را در زمان مشخص با تعیین نوع بسته‌ها و دیتا محدود سازیم و یا اجازه دسترسی به منابع شبکه را فراهم سازیم. بنا بر این مطابق ضرورت و تنظیم زمان، دسترسی هاست‌ها را با توجه به نوع دیتاهای مشخص، کنترل کنیم. شکل ۵-۱۱ را مشاهده نمایید.



شکل ۵-۱۱: تنظیمات دسترسی به اینترنت براساس فلتر کردن نوع بسته‌ها

۵.۲.۱۰ تنظیمات زمان‌بندی استفاده اینترنت (Schedule Settings)

در این روش با استفاده از محدود کردن روز و ساعت می‌توانیم دسترسی به اینترنت را محدود سازیم. این روش در نهایت کاربرد و موارد استفاده زیاد دارد. مطابق شکل ۵-۱۲ با استفاده از این روش می‌توانیم تقسیم اوقات استفاده از اینترنت را بر اساس ساعت برای کارمندان اداره، محصلان و بخش‌های دیگر یک سازمان تنظیم و عملی بسازیم.



شکل ۵-۱۲: تنظیمات دسترسی به اینترنت براساس تقسیم بندی روز و ساعت



در این فصل موضوعات مهم امنیتی در شبکه‌های بی‌سیم و به‌صورت خاص در شبکه WLAN به‌صورت جامع بحث گردید. آنچه در این فصل گفته شد؛ معرفی پروتوکول‌های امنیتی و حملات احتمالی روی شبکه‌های بی‌سیم، تنظیمات امنیتی اکسس‌پاینت و روترهای بی‌سیم، استفاده موثر از لحاظ کارایی، کنترل کردن پهنای باند و غیره بحث گردید. بخش مهم دیگر این فصل معرفی و آشنایی پروتوکول‌های امنیتی؛ WEP، WPA و WPA2 و هم‌چنان حملات احتمالی نیز توضیح گردید. به‌صورت عموم، چهار نوع حملات اساسی در شبکه‌های بی‌سیم معرفی گردید.

قسمی که به‌یاد داریم؛ تنظیمات امنیتی در شبکه‌های بی‌سیم و به‌صورت خاص در اکسس‌پاینت‌ها و روترهای بی‌سیم هدف اصلی این فصل دانسته شده است. بالاخره در این فصل به تنظیمات امنیتی اکسس‌پاینت و روترهای بی‌سیم آشنا شدیم. این تنظیمات عبارت از: تغییرات تنظیمات پیش‌فرض، تنظیمات MAC Filtering، تنظیمات دسترسی به منابع، تنظیمات محدودیت‌های پهنای باند، تنظیمات امنیتی PSK، تنظیمات یوزرنیم و پاسورد سیستم یا محیط admin، تنظیمات بروز رسانی Firmware و غیره موارد دیگر است که به آنها آشنا شدیم.



سوالات و فعالیتهای فصل پنجم

۱. بخش‌های مهم امنیت در شبکه WLAN را نام بگیرید.
۲. تفاوت الگوریتم‌های امنیتی WEP و WPA در چیست؟
۳. احراز هویت در شبکه بی‌سیم چگونه اتفاق می‌افتد؟
۴. هدف از استفاده SSID در شبکه WLAN در چیست؟
۵. چرا باید از تنظیمات پیش‌فرض اکسس‌پاینت استفاده نشود.

فعالیت‌ها

۱. فلوجارت میتودهای RTS و CTS را ترسیم کنید.
۲. نام شبکه (SSID) در شبکه WLAN چگونه غیر فعال می‌گردد؟
۳. لطف نموده حل اقل سه اکسس‌پاینت را بین هم به‌صورت Bridge وصل سازید.
۴. روش MAC Filtering را در یک اکسس‌پاینت تطبیق نمایید.
۵. با استفاده از کدام گزینه می‌توانید اکسس‌پاینت را Reset نمایید.
۶. در یک روتر بی‌سیم، backup فایل تنظیمات را انجام دهید.
۷. حد اقل دو کلاس آدرس IP را به نوبت بالای DHCP سرور تطبیق نمایید.
۸. پاسورد پیش‌فرض روتر بی‌سیم را تغییر دهید.

فصل ششم

روش‌های حل مشکل در شبکه‌های بی‌سیم



هدف کلی: با روش‌های حل مشکلات شبکه‌های بی‌سیم آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. مشکلات در شبکه‌های بی‌سیم را تشخیص داده بتوانند.
۲. مشکلات در شبکه Wi-Fi را حل کرده بتوانند.
۳. مشکلات در سرور DHCP را تشخیص و برطرف کرده بتوانند.
۴. مشکلات در کارت شبکه (NIC) را تشخیص داده بتوانند.
۵. از درست کارکردن کارت شبکه و پروتوکول TCP/IP اطمینان حاصل کرده بتوانند.
۶. در صورتی که نام شبکه مخفی گردیده باشد، اقدام به راه حل آن کرده بتوانند.
۷. آدرس‌های IP معتبر و نا معتبر را تشخیص داده بتوانند.
۸. حذف و تجدید آدرس IP را مطابق دستورالعمل‌ها، انجام داده بتوانند.

در این فصل مشکلات عمده و اساسی در شبکه‌های بی‌سیم و به‌خصوص مشکلات در شبکه‌های WLAN را معرفی خواهیم کرد. هم‌چنان علاوه بر موضوعات نظری حل مشکل، به‌موضوعات عملی و تطبیقی آن نیز اشاره خواهد شد. هم‌چنان کوشش شده است که ابزارهای حل مشکل نیز معرفی گردد.

مشکلاتی که در این فصل به آن اشاره خواهد شد، TCP/IP Stak، مشکلات کارت شبکه، عدم سرویس دهی سرور DHCP، مخفی بودن SSID، فراموش شدن یوزر نیم و پاسورد اکسس‌پاینت و یا روترهای بی‌سیم و غیره خواهد بود. کوشش می‌گردد که بعد از شناسایی مشکلات، راه حل مناسب و قابل اجرا نیز پیشنهاد گردد. هم‌چنان بخش مهم این فصل، ارائه و معرفی دستورالعمل‌های حل مشکل، معرفی ابزارهای حل مشکل در موارد مختلف است. کوشش می‌شود که استفاده و تنظیمات مناسب Wi-Fi، ضرورت‌های حل مشکل، تنظیمات، ریست، حذف و یا تنظیم مجدد آن به روش ساده و کوتاه معرفی گردد.

هم‌چنان برای شناسایی مشکلات در شبکه Wi-Fi به صورت جداگانه بحث خواهد شد. در این فصل راه حل‌های شبکه Wi-Fi به‌صورت جداگانه بیان خواهد شد.

۶.۱ حل مشکل در شبکه‌های WLAN

برای حل مشکل^{۱۰۴} در شبکه‌های WLAN باید معلومات جانبی شبکه را نیز داشته باشیم. هدف این است که محصلان عزیز باید مباحث ابتدایی شبکه را از گذشته به‌یاد داشته باشند. در غیر آن روش‌های حل مشکل به‌سادگی قابل تطبیق نمی‌باشد.

مباحث حل مشکل همیشه بر اساس یک میتود قابل حل نمی‌باشد و هیچ‌گاه تشخیص مشکل به‌یک‌بارگی قابل انجام نمی‌باشد. هدف این است که تشخیص مشکل، ضرورت به‌تطبیق میتودهای مختلف دارد تا به‌صورت مطمئن قضاوت شود که کدام جای شبکه، احتمالاً در گیر بعضی مشکلات است.

هم‌چنان باید توجه داشته باشیم که تمام مباحث حل مشکل، همیشه تسلسل منطقی نداشته است؛ که مانند بخش‌های نظری این کتاب، عناوین را دنبال هم بحث کنیم. بلکه براساس فرضیه‌ها و سناریوهای مشکل می‌توانیم روش حل مشکل را گام به‌گام تطبیق کنیم. هم‌چنان انجام روش‌های حل مشکل باید به صورت یکایک با تسلسل درست انجام گیرد.

استفاده از Wi-Fi کمپیوتر

جهت استفاده از Wi-Fi باید نکات ذیل را در نظر بگیریم.

- مطمئن باشیم که کلید Wi-Fi بر روی لب تاپ روشن باشد. جهت اطمینان باید چراغ Wi-Fi روشن باشد.
- مطمئن باشیم که کمپیوتر در حالت airplane mode نباشد.

¹⁰⁴Troubleshooting

- در صورت امکان، از نزدیک اکسس پاینت و یا روتر بی سیم را استفاده کنید.
- اگر نام شبکه (SSID) را در لیست نمی بینید، شاید روتر و یا اکسس پاینت برای شما تنظیم نشده باشد. ممکن نام شبکه را از دید شما مخفی کرده باشد. در این حالت باید به صورت دستی متصل شوید.

۶.۱.۱ اجرای دستورات تست و دریافت اطمینان از شبکه

بعضی ابزارهای موثر برای حل مشکل وجود دارد. این ابزارها در مرحله اول مشکلات را شناسایی و در مرحله دوم مشکل را رفع می نماید. یکی از این ابزارها به نام حل کننده مشکل^{۱۰۵} در ویندوز است. با استفاده از این ابزار مشکلات شبکه شناسایی و بعد برای حل آن تلاش می کنند. در صورتی که مشکلات سخت افزاری باشد و یا مشکلات جدی تری که با این ابزارها قابل اصلاح نباشد، پیام دیگر صادر می شود. در این صورت اجرای بعضی دستورات جهت تست و اطمینان از حل مشکل لازم است. این دستورات قرار ذیل می باشد:

- TCP/IP stack را ریست کنید.

C:\Windows\system۳۲>netsh Winsock reset

- پروتوکول TCP/IP را تست کنید.

با استفاده از پروگرام CMD از طریق Start Menu می توانید دستور ذیل را اجرا کنید.

C:\> Ping ۱۲۷.۰.۰.۱

کنکشن شبکه بی سیم خود را غیر فعال^{۱۰۶} و دوباره فعال^{۱۰۷} کنید.

با استفاده از تنظیمات کنکشن های شبکه، می توانید کنکشن های مورد نظر خود را انتخاب، بعد از آن غیر فعال و دوباره فعال کنید.



شکل ۶-۱ غیر فعال کردن کنکشن شبکه

¹⁰⁵Network Troubleshooter

¹⁰⁶ Disable

¹⁰⁷Enable

- آدرس IP اولی را حذف کنید.

به هدف حذف آدرس IP دستور ذیل را چندین بار تکرار کنید.

C:\> ipconfig/release

- آدرس IP جدید را تقاضا کنید.

C:\> ipconfig/renew

در صورتی که کمپیوتر شما گاهی به شبکه WLAN وصل نمی گردد، ممکن است از اثر مشکلات متفاوت باشد.

۱. ممکن است کمپیوتر شما بعضی مشکلات داشته باشد.
۲. ممکن است دستگاه اکسس پاینت و یا روتر بی سیم مشکلات داشته باشد.
۳. ممکن است، محیط و یا فاصله بین شما و اکسس پاینت مساعد نبوده، تداخل امواج، تضعیف امواج و غیره مشکلات محیطی باعث گردیده باشد.

اول: اگر مشکلات در کمپیوتر باشد، دستورات عملی و ابزارهای حل مشکل را در کمپیوتر اجرا کنید. یکی از ابزارهای مورد استفاده پروگرام CMD است. روی پروگرام CMD دستورات ذیل را به ترتیب مطابق لست اجرا کنید. بعد از آن ببینید که مشکل حل شده است یا خیر!

- عبارت netsh winsock reset را تایپ و Enter کنید؛

که پروتوکول TCP/IP را ریست می کند.

- عبارت netsh int ip reset را تایپ و Enter کنید؛

که آدرس IP را ریست می کند.

- عبارت ipconfig/release را تایپ و Enter کنید؛

که آدرس قبلی را حذف می کند

- عبارت ipconfig/renew را تایپ و Enter کنید.

که آدرس قبلی را دوباره تقاضا و دریافت می کند.

- عبارت ipconfig/flushdns را تایپ و Enter کنید.

در صورتی که پروتوکول DNS و نام و آدرس آن تغییر کرده باشد، توسط این دستور تازه، update و هم آهنگ به کمپیوترتان می شود.

دوم: اگر مشکل در اکسس پاینت و یا روتر بی سیم باشد، باید مدیر شبکه مشکلات اکسس پاینت را حل نماید.

معمولی ترین مشکلات و اشتباهاتی که در اکسس پاینت اتفاق می افتد، از اثر درست عمل نکردن سرور DHCP است. در این صورت باید مشکلات از طریق روتر بی سیم و یا اکسس پاینت حل شود.

الف: مشکلات در سرور DHCP

مشکلات در سرور DHCP گاهی به اثر محدود بودن آدرس IP اتفاق می افتد.

راه حل:

در این صورت باید تعداد آدرس های IP ، حسب ضرورت استفاده کنندگان و کاربران افزایش داده شود. این عملیه توسط مدیر شبکه در تنظیمات DHCP انجام می شود. در فصل پنجم در مورد محدوده آدرس IP در بخش تنظیمات DHCP به صورت همه جانبه بحث شده است که مطابق آن می توان از طریق اولین و آخرین IP این مشکل را حل کرد.

قابل یادآوری است که در این حالت سرور DHCP به کمپیوترها آدرس IP توزیع نمی کند و کمپیوتر به صورت محلی از خودش آدرس IP تقاضا می کند. آدرسی که از طرف سیستم عامل کمپیوتر به خودش تقدیم می گردد، از محدوده ۱۶۹.۲۵۴.۰.۰ است. این آدرس به نام آدرس لینک محلی^{۱۰۸} یاد می شود. هر وقتی کمپیوتر از این محدوده که شامل کلاس B است، آدرس دریافت نماید، به این معنی است که خدمات DHCP توقف کرده و آدرس IP را به صورت خود کار به هاست ها ارسال نمی کند.

در صورتی که تعداد آدرس های IP در سرور DHCP، کافی است و سرویس ارسال و ارائه آدرس IP به خوبی اتفاق نمی افتد، در این صورت مشکل از عمل کرد ضعیف اکسس پاینت است. اکسس پاینت و یا روتر بی سیم، می تواند به دلایل زیر فعالیت ضعیف داشته باشد:

ضعف در ساخت و قطعات سخت افزاری و نرم افزاری آن، چون سیستم عامل ضعیف، حافظه ضعیف، قدرت پروسس ضعیف، عدم میتودهای مدیر ترافیک، نداشتن پالیسی برای اولویت های شبکه و غیره خواهد بود.

هر یک از مشکلات می تواند ضعف عمل کرد را به وجود آورد. این ضعف عمل کرد تنها مشکلات اتصال و ارتباط به کمپیوترها و یا کاربران را به وجود نمی آورد، بلکه در بخش های مختلف و در ارائه سرویس های مختلف مشکلات جدی را به وجود می آورد. اما معلوم است که این مشکلات در اثر بار ترافیکی بیش تر، بیش تر خواهد شد. بنا بر این یکی از عمل کردهای ضعیف می تواند عدم توانایی ارسال آدرس IP به هاست ها باشد.

برای شناسایی مشکلات باز هم بهتر است که آدرس IP کمپیوتر تست گردد؛ در این حالت باز هم آدرس IP لینک محلی دریافت خواهد شد. آدرس از طرف سیستم عامل کمپیوتر به خودش ارسال و از محدوده

¹⁰⁸Link-Local Address

۱۶۹.۲۵۴.۰.۰ انتخاب می‌گردد. در صورت مشاهده کردن آدرس بالا مطمئن می‌شویم که سرور DHCP خدمات IP را انجام نمی‌دهد و کمپیوتر مجبور می‌شود که توسط خودش آدرس محلی از لینک خود را انتخاب کند.

راه حل:

در صورت عمل کرد ضعیف اکسس پاینت اگر مشکلات زیرساخت^{۱۰۹} باشد، راه حلی مناسب دیده نمی‌شود. تنها راه حل دائمی این است که برندهای قوی، Update با تجهیزات و قطعات توانمند خریداری شود. اما در راه حل‌های کوتاه مدت بهتر است که با گذشت چند ساعت و یا مطابق ضرورت (قطع شدن اتصال)، اکسس پاینت و یا روتر بی‌سیم را Restart کنیم. با هر بار Restart شدن، برای چند لحظه عمل کرد آن بهتر خواهد شد.

روش Restart نمودن یک اکسس پاینت و یا روتر بی‌سیم می‌تواند به انواع متفاوت ذیل انجام گیرد:

- سیم برق روتر را از دو شاخه بکشید.
 - دکمه Restart را فشار داده نگه‌دارید تا دستگاه Restart شود.
- برخی از اکسس پاینت‌ها و یا روترها از خود بطری پشتیبان دارند، بنا بر این وقتی آن‌ها را از برق می‌کشید چراغ‌ها روشن می‌مانند، در این دستگاه‌ها باید بطری را نیز بکشید.
- اگر به این صورت مشکلات به شکل اساسی حل نگردید می‌توانید روتر یا اکسس پاینت را ریست^{۱۱۰} نمایید. موضوع ریست کردن اکسس پاینت‌ها در فصل پنجم برای عیارسازی پیش‌فرض به صورت همه جانبه توضیح داده شده است. اما به دلیل حل مشکل از طریق ریست نمودن روتر بی‌سیم به نکات ذیل توجه نمایید.
- دکمه reset را حد اقل ۳۰ ثانیه یا بیش‌تر فشار داده نگه‌دارید. این دکمه را تا وقتی فشار داده نگه‌دارید که چراغ‌های مودم شروع به چشمک زدن خواهد کرد و صبر کنید تا چشمک زدن‌شان متوقف شود.
 - چند دقیقه صبر کنید تا اکسس پاینت و یا روتر کاملاً شروع شود و به حالت عادی به کار آغاز کند.
 - از طریق کمپیوتر خود دوباره برای اتصال به شبکه از طریق Taskbar تلاش کنید.
- در ادامه برای اطمینان اتصال کمپیوترتان به اکسس پاینت، بهتر است Default Gateway را تست (Ping) کنید. آدرس Default Gateway در کمپیوترتان از طریق تنظیمات TCP/IP قابل شناسایی است. لذا Gateway کمپیوتر خود را پیدا نموده و آن را امتحان نمایید.

^{۱۰۹}Infrastructure

^{۱۱۰}Reset

البته آدرس اکسس پاینت برای کمپیوتر شما Gateway است. اگر آدرس IP اکسس پاینت شما ۱۹۲.۱۶۸.۱.۱ باشد، می‌توانید از طریق پروگرام CMD آن را Ping کنید. به عنوان مثال: C:\> Ping ۱۹۲.۱۶۸.۱.۱

در صورتی که نتایج ذیل ظاهر شود، مطمئن می‌شویم که به اکسس پاینت به صورت صد در صد وصل می‌باشیم. پیام‌های ذیل نشان می‌دهد که تمام بسته‌های اطلاعاتی که به آدرس اکسس پاینت ارسال گردیده، به صورت موفقانه به آن رسیده است.

Reply from 192.168.1.1: bytes=32 time=5ms TTL=64

Reply from 192.168.1.1: bytes=32 time=5ms TTL=64

Reply from 192.168.1.1: bytes=32 time=5ms TTL=64

Reply from 192.168.1.1: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.1.1: Packets: Sent=4, Received=4, Lost=0 (0% loss), Approximate round trip time in milli-seconds: Minimum=4ms, Maximum=5ms, Average=4ms

اگر دستور ping موفقانه انجام شد و پیام بالا نیز دریافت شد؛ اما مشکلات اتصال و دسترسی کمپیوتر شما به اینترنت حل نگردید، لذا مشکل در کمپیوتر، اکسس پاینت و یا روتر بی‌سیم نیست، ممکن است اشکال از بخش دیگر شبکه و یا در ISP باشد.

چک نمودن کارت شبکه (Network Adapter)

بعضی اوقات مشکلات در کارت شبکه نیز به وجود می‌آید. اگر با انجام تمام فعالیت‌های بالا، مطمئن می‌شویم که اکسس پاینت و روتر درست عمل می‌کند و یا با تست کردن بعضی کمپیوترهای دیگر اطمینان حاصل می‌کنیم که تنها یک کمپیوتر به صورت درست عمل کرده نمی‌تواند و این کمپیوتر به شبکه و اینترنت متصل نمی‌شود و کماکان مشکلات اتصال به شبکه و اینترنت حل نه گردیده؛ این احتمال وجود دارد که مشکل مربوط به کارت شبکه یا اداپتور شبکه شما باشد.

راه حل:

سعی کنیم از طریق حل کننده مشکل کارت شبکه^{۱۱۱} این معضل را شناسایی و حل کنیم. با استفاده از این ابزار می‌توانیم کارت شبکه و درایور مربوطه به آن را بروز رسانی کنیم. درایورهای قدیمی یا ناقص می‌تواند سبب ایجاد مشکلات زیادی شود. با این روش اگر درایور جدید در اختیار دارید، نصب نموده بعداً بروز رسانی کنید. مراحل انجام این کار را در ذیل مشاهده نمایید.

^{۱۱۱}Networkadaptor troubleshooter

Start Menu → Control panel → Search Troubleshooter

بعد از یافتن ابزار Troubleshooter مراحل ذیل را انجام دهید.

Troubleshooting → View all → Network Adapter

بعد از انجام آن می‌توانید درایور قدیمی خود را به شکل زیر بروز رسانی کنید.

My PC → Right click → Manage → Device Manager → fine the Network Adapter → Right click on network adapter → Choose Properties → Update Driver → Search automatically for updated driver software

اگر ویندوز نتوانست نسخه جدیدی برای درایور شما پیدا کند، از وبسایت کمپنی سازنده کمپیوتر خود آخرین ورژن را دانلود نمایید. اگر کمپیوتر شما به اینترنت وصل نمی‌شود؛ توسط کمپیوتری دیگر، دانلود و با استفاده از حافظه USB به کمپیوتر خود نصب کنید. البته برای دانلود درایور مناسب باید نام کمپنی سازنده و نام یا مدل کمپیوتر خود را بدانید.

مشکل مخفی بودن نام شبکه بی سیم

در صورتی که شما نمی‌توانید از طریق نام شبکه (SSID) به Wi-Fi شبکه خود وصل شوید، ممکن است نام شبکه برای شما قابل مشاهده نباشد.

• اگر نام شبکه خود را نمی‌بینید، از طریق admin وارد تنظیمات اکسس پاینت شوید.

در این صورت ممکن است نام شبکه برای انتشار و Broadcast کردن فعال نشده باشد. لذا بعد از وارد شدن تمام تنظیمات و به خصوص نام شبکه را چک کنید.

راه حل:

- کمپیوتر خود را از طریق کیبل Ethernet به روتر بی سیم و یا اکسس پاینت وصل کنید.
- یکی از Browser های خود را باز و از طریق آدرس IP اکسس پاینت وارد سیستم شوید. کوشش کنید که آدرس پیش فرض را برای روتر خود پیدا کنید. مثال: ۱۹۲.۱۶۸.۱.۱ و یا ۱۹۲.۱۶۸.۲۴۹.۱ در اکسس پاینت برند TP-LINK است.
- از طریق یوزرنیم و پاسورد خود (پیش فرض admin) وارد شوید.
- با استفاده از گزینه Wireless SSID، چک باکس Enable SSID Broadcast تایید کنید.
- با تایید این گزینه خدمات پخش و نشر نام شبکه فعال می‌گردد. این خدمات در آینده‌ها از طریق تمام کمپیوترها قابل دریافت است و در Taskbar کمپیوتر به صورت خود کار ظاهر می‌گردد.
- یکی از محدودیت‌های دیگر محدود کردن آدرس MAC توسط روش فلتر کردن MAC است که در روترهای بی سیم تطبیق می‌شود.
- از طریق گزینه MAC Filtering نیز می‌توانید اطمینان حاصل کنید.

- اگر MAC کمپیوتر شما شامل این لست کمپیوترهای مجاز نباشد، باید MAC کمپیوتر خود را در این لست شامل کنید.
- جهت یافتن آدرس MAC کمپیوتر خود و هم‌چنان اضافه کردن به لست MAC، دستور زیر را اجرا کنید.

CMD → C:\> ipconfig/ all

- در ادامه آدرس MAC ظاهر می‌شود، آن را یادداشت و به لست MAC های مجاز اضافه کنید.
- بعد از اطمینان همه موارد فوق حالا از طریق پروگرام CMD می‌توانید امتحان کنید که کمپیوتر شما آدرس IP خود را دریافت کرده است یا خیر ؟

مثال:

CMD → C:\> ipconfig/renew

CMD → C:\> ipconfig/ all

- آدرس IP کمپیوتر خود را مشاهده کرده می‌توانید.

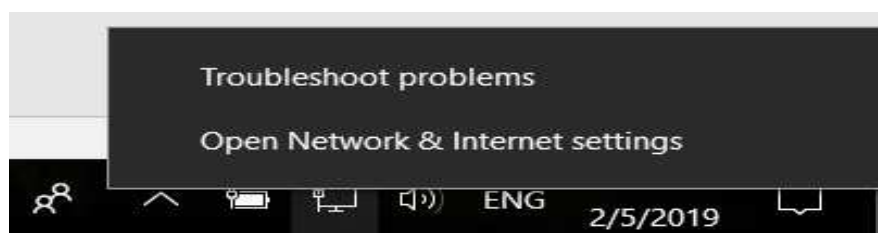
۶.۲ هشت راه حل مشکل برای وصل شدن به Wi-Fi در ویندوز

راه حل‌های ذیل به‌صورت همه جانبه و کلی، جهت راهنمایی‌ها و استفاده سریع از ابزارها بیان شده است. این راه حل‌ها قرار ذیل است:

۶.۲.۱ اجرای ابزار حل‌کننده مشکل (Network Troubleshooter)

اولین قدم برای حل مشکل عدم اتصال به اینترنت اجرای ابزار Network Troubleshooter می‌باشد. برای این کار از روش زیر اقدام کنید.

- در کمپیوتر خود برروی علامت Wi-Fi در گوشه سمت راست پایین صفحه، راست کلیک کنید. سپس Troubleshoot Problems را انتخاب کنید.



در ادامه مسیر را دنبال کنید تا به‌صورت خود کار، مشکل را بررسی و در صورت امکان آن را حل کند.

۶.۲.۲ Restart کردن اکسس پاینت

در صورتی که مرحله اول مشکل عدم اتصال به اینترنت را حل نکرد، این مرحله را نیز انجام دهید.

- اکسس پاینت را Restart کنید (برای ۳۰ ثانیه از برق قطع کنید)
- کامپیوتر خود را Restart کنید و اکسس پاینت را دوباره به برق وصل کنید.

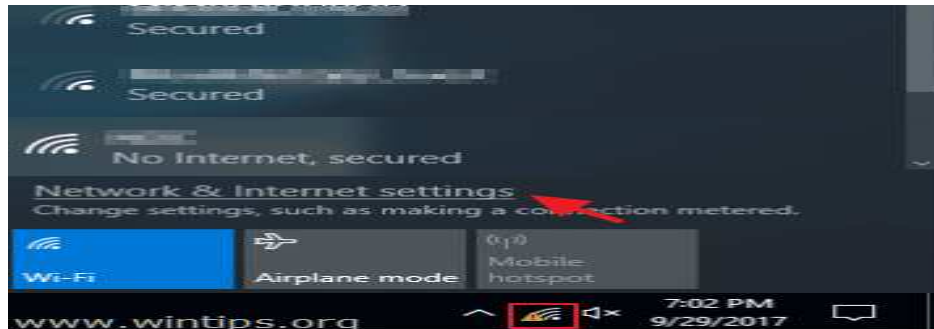
یادداشت: در بسیاری موارد؛ با انجام فعالیت‌های بالا مشکل حل می‌شود.

۶.۲.۳ قطع ارتباط Wi-Fi و وصل کردن مجدد آن

در کامپیوتر ارتباط خود را از Wi-Fi قطع کنید و دوباره وصل شوید. برای این کار شبکه را از لیست Wi-Fi های شناخته شده حذف کنید. برای انجام این کار فعالیت زیر را انجام دهید.

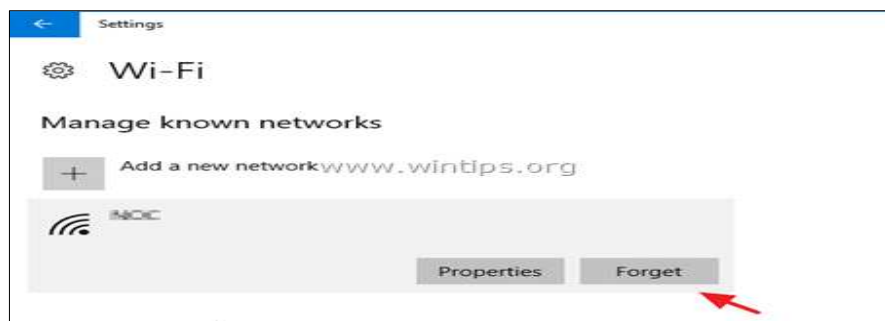
- بر روی علامت Wi-Fi کلیک کرده و در گزینه‌های موجود **Network settings** را انتخاب کنید.

شکل ۶-۲ را مشاهده نمایید.



شکل ۶-۲: تنظیمات شبکه بی سیم (Network Settings)

- از منوی سمت چپ **Wi-Fi** را انتخاب کنید و وارد **Manage known networks** شوید.
- شبکه که به آن متصل هستید را انتخاب و دکمه **Forget** را بزنید.



شکل ۶-۳: حذف شبکه از لیست Wi-Fi

۶.۲.۴ اسکن کردن کامپیوتر برای ویروس

گاهی اوقات بعضی بدافزارها موجب مشکلات برای دسترسی به اینترنت می‌شوند. بنابراین بهتر است که کامپیوتر خود را اسکن کنید.

۶.۲.۵ غیر فعال کردن آنتی ویروس

گاهی اوقات ممکن است پروگرام آنتی ویروس باعث قطع اینترنت شود. آنتی ویروس‌هایی مانند Avast می‌توانند جهت تأمین امنیت؛ ارتباط اینترنت شما را زیر نظر بگیرد و در صورت نیاز قطع کند.

راه حل: یا آنتی ویروس غیر فعال گردد و یا پروگرام‌ها را Update کنید تا آنتی ویروس از لحاظ تهدیدات مطمئن شود.

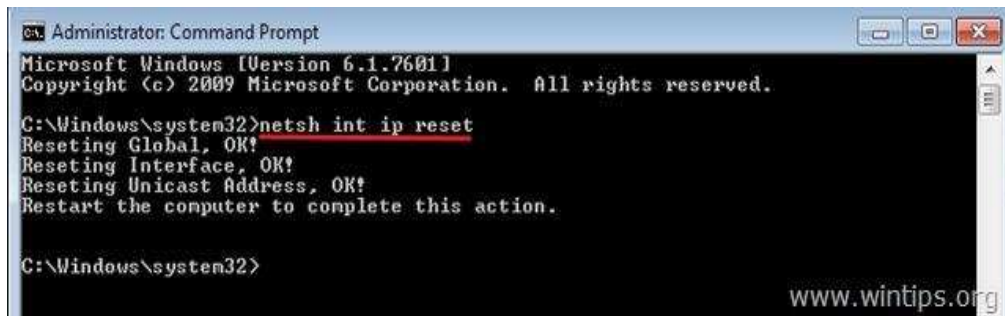
۶.۲.۶ ریست کردن TCP/IP Protocol & WINSOCK Catalog

حالت دیگر این است که شما همیشه به Wi-Fi وصل هستید، اما خدمات اینترنت فعال نیست. این کار باعث مشکلات و خرابی تنظیمات TCP/IP می‌شود. برای Reset کردن این تنظیمات به پروگرام CMD administrator Run as اقدام کنید.

در محیط CMD دستورات زیر را اجرا کنید.

```
C:\> netsh int ip reset
```

اجرای این دستور را در شکل ۶-۴ مشاهده نمایید.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

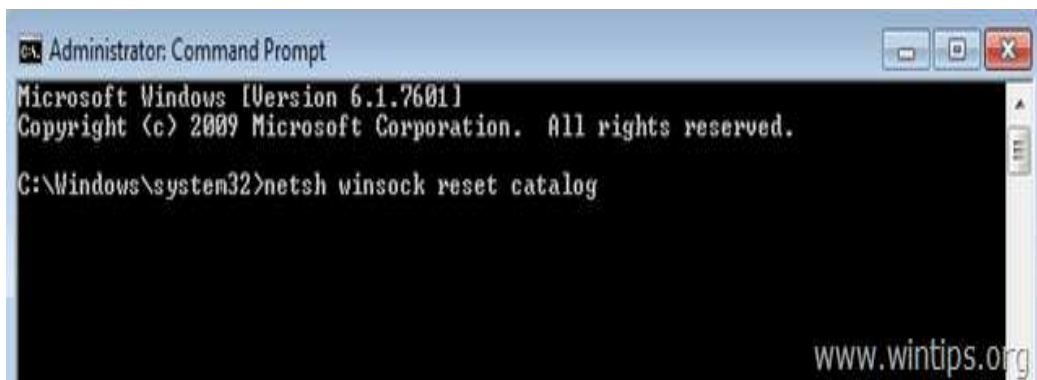
C:\Windows\system32>netsh int ip reset
Resetting Global, OK!
Resetting Interface, OK!
Resetting Unicast Address, OK!
Restart the computer to complete this action.

C:\Windows\system32>
```

شکل ۶-۴: ریست کردن پروتوکول TCP/IP

کامپیوتر را Restart و اتصال اینترنت خود را چک کنید. در صورتی که هنوز مشکل وجود دارد به CMD برگردید و دستور زیر را اجرا کنید.

C:\> netshwinsock reset catalog



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh winsock reset catalog
```

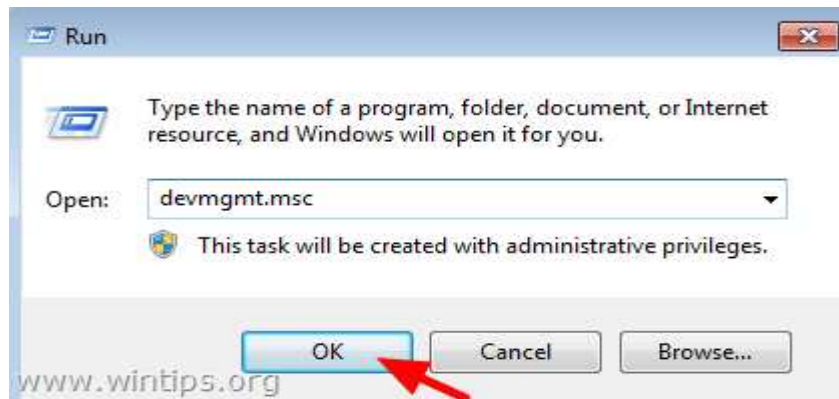
شکل ۶-۵: ریست کردن TCP/IP با دستور catalog

بعد از Restart دوباره؛ اینترنت را چک کنید. اگر مشکل از این لحاظ باشد، حل گردیده است.

۶.۲.۷ حذف و نصب مجدد کارت شبکه

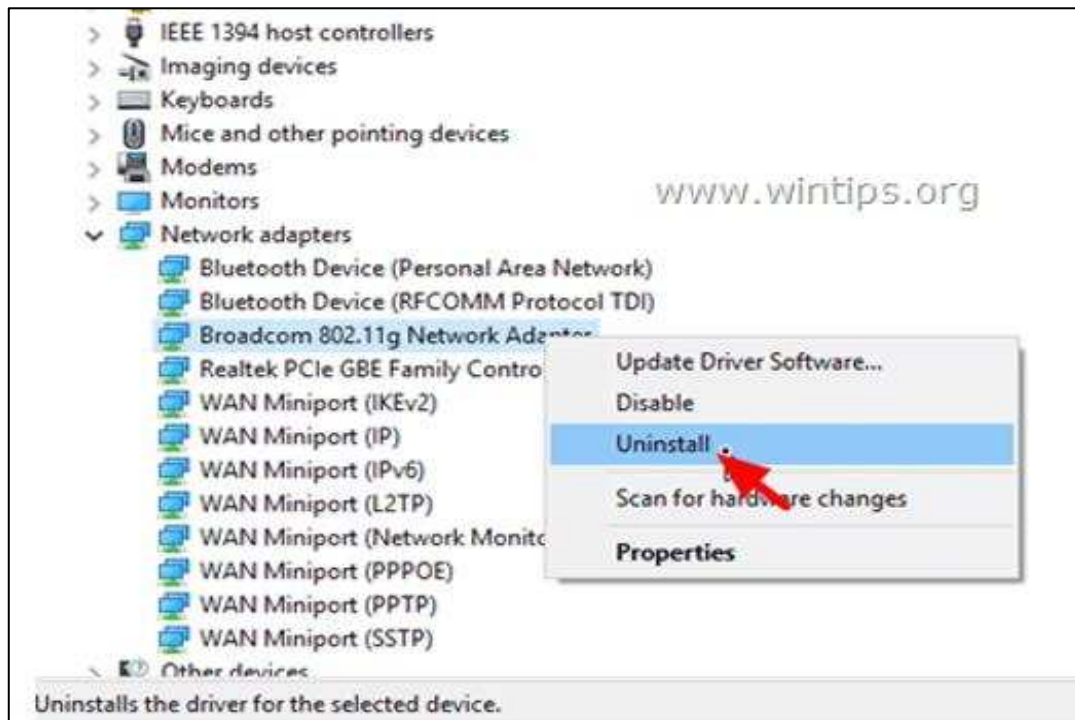
یکی از مشکلات احتمالی درست کار نکردن کارت شبکه است. بهتر است قبل از انجام آن، فایل نصب درایور کارت شبکه را دانلود کنید. به دلیل این که ارتباط کامپیوتر شما از اینترنت قطع می گردد.

با استفاده از اجرای دستور devmgmt.msc توسط پروگرام Run می توانید به Device Manager وارد شوید. شکل ۶-۶ را مشاهده کنید.



شکل ۶-۶: دستور Device Manager از طریق Run

بعد از آن در صفحه Device Manager، کارت شبکه بی سیم (802.11 bgn) را پیدا کنید و مطابق شکل ۶-۷ آن را حذف^{۱۱۲} کنید.



شکل ۶-۷: حذف کردن درایور کارت شبکه بی سیم

بعد از حذف درایور کارت شبکه، درایور دالود شده را نصب کنید و کامپیوتر را Restart کنید.

^{۱۱۲} Uninstall

۶.۲.۸ چک کردن سرویس‌های لازم برای شبکه اینترنت

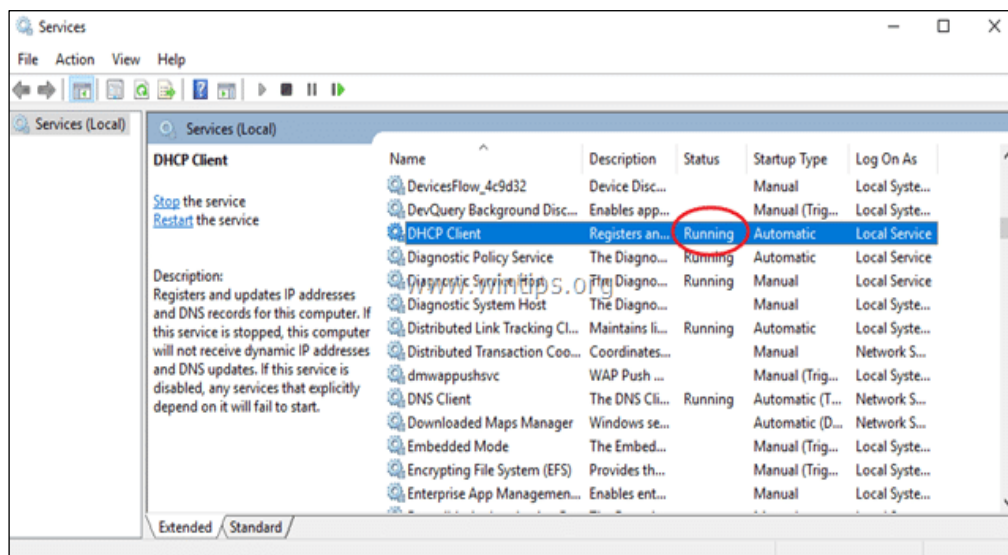
در صورتی که تمام روش‌های بالا جواب نداد؛ آخرین روش این است که سرویس‌های^{۱۱۳} زیر فعال باشند.

1. COM+ Event System (for WZC issues)
2. Diagnostic Policy Service
3. DHCP Client
4. DNS Client
5. Network Connections
6. Network Location Awareness
7. Remote Procedure Call (RPC)
8. Server
9. TCP/IP Netbios helper
10. WLAN AutoConfig
11. Workstation

برای چک کردن آن‌ها اقدامات زیر را انجام دهید!

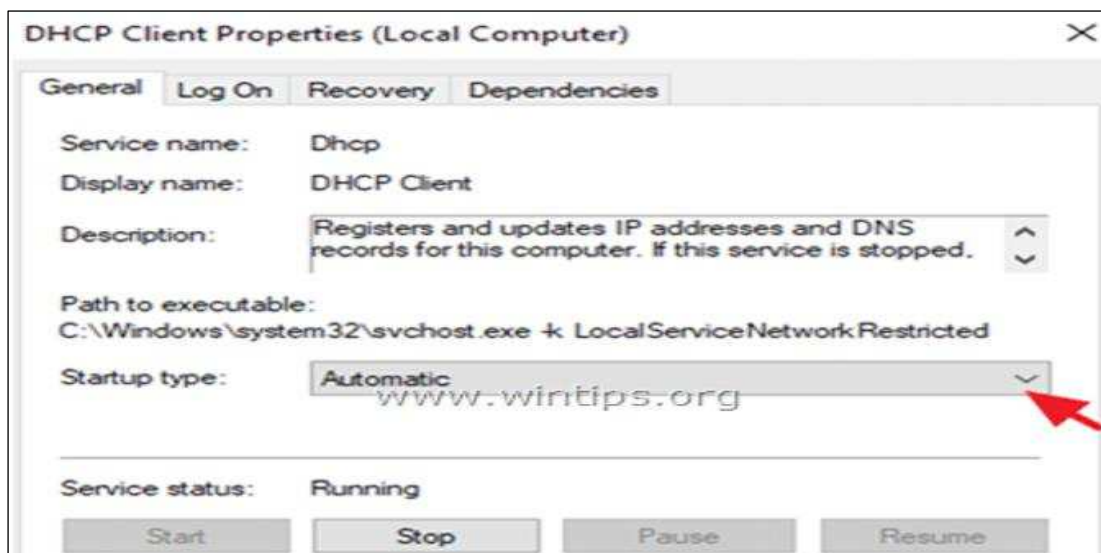
از طریق پروگرام Run دستور Services.msc را تطبیق کنید.

مطابق شکل ۶-۸ لیست تمام سرویس‌ها ظاهر می‌شود. اکنون تمام سرویس‌های بالا را چک و بررسی کنید که فعال است یا خیر؟



شکل ۶-۸: یافتن سرویس DHCP از طریق سرویس ویندوز

در صورتی که فعال نیستند بر روی آن‌ها کلیک کرده و مطابق تصویر زیر آن‌ها را فعال کنید.



شکل ۶-۹. فعال و یا غیر فعال کردن خدمات DHCP سرور



در این فصل مباحث حل مشکل در شبکه‌های بی‌سیم و به‌صورت خاص در مورد شبکه WLAN بیان گردید. علاوه بر موضوعات نظری حل مشکل، به موضوعات عملی و تطبیقی، شناسایی مشکلات احتمالی، روش‌های حل مشکل، معرفی ابزارهای حل مشکل، دستورالعمل‌های حل مشکل و غیره اشاره گردید. قابل یادآوری است که برای حل هر مشکل، راه حل مناسب با ابزارها و دستورالعمل‌های مرتبط به آن نیز بیان گردید.

مشکلاتی که در این فصل به آن اشاره شد، عبارت از مشکلات در TCP/IP Stak، مشکلات در کارت شبکه، مشکلات در سرور DHCP، مشکلات در مخفی بودن SSID، مشکلات در یوزر نیم و پاسورد اکسس‌پاینت و یا روترهای بی‌سیم و غیره بود. بعد از ارائه و شناسایی مشکلات به صورت جداگانه برای هر کدام آن، راه حل مناسب و قابل اجرا نیز پیش‌نهاد شد. بخش دیگر که در این فصل بیان گردید، ارائه دستورالعمل‌های حل مشکل، معرفی ابزارهای حل مشکل در موارد مختلف است. استفاده از Wi-Fi و تنظیمات مناسب Wi-Fi یکی از ضرورت‌های حل مشکل است که به این صورت می‌توانیم تنظیمات Wi-Fi را ریست، حذف و یا تنظیم مجدد کنیم. گاهی اوقات عمل‌کرد ضعیف سرویس‌های سیستم عامل نیز باعث می‌شود که شبکه بی‌سیم درست کار کرده نتواند. بنا بر این شناسایی مشکلات و راه حل‌های مناسب آن، نیز در این فصل بیان گردیده است.

هم‌چنان برای شناسایی مشکلات در شبکه Wi-Fi بحث‌های جداگانه‌یی در نظر گرفته شد که در نهایت، جهت راه حل‌های شبکه Wi-Fi به‌صورت جداگانه هشت راه حل مرحله‌یی بیان گردید. این راه‌ها هر کدام مشکلات احتمالی را برطرف خواهند کرد. در صورتی که در مرحله اول، مشکل حل نگردد؛ با استفاده از مرحله دوم و یا مرحله سوم و بالاخره در یکی از مراحل تا مرحله هشتم، مشکل برطرف خواهد شد.



۱. مشکلات عمده و اساسی در شبکه‌های بی‌سیم را نام بگیرید.
۲. آدرس Gateway را در شبکه خود بدست آورید.
۳. آدرس Gateway خود را تست کنید.
۴. دستور حذف آدرس IP را بنویسید.
۵. دستور حل مشکل در TCP/IP Stack را بنویسید.
۶. نام شبکه خود را به‌دست آورید.
۷. اگر نام شبکه مخفی باشد، چگونه مشکل را حل کرده می‌توانید.
۸. حداقل پنج راه حل برای حل مشکلات Wi-Fi لست کنید.
۹. عمده‌ترین مشکلات در اکسس‌پاینت‌ها کدام است؟
۱۰. اگر مشکل در سرور DHCP مربوط به اکسس‌پاینت باشد، راه حل چیست؟
۱۱. اگر مشکل فراموش شدن یوزرنیم یا پاسورد اکسس‌پاینت باشد، راه حل چیست؟
۱۲. اگر کامپیوتر شما آدرس ۱۶۹.۲۵۴.۱۰.۱۲۴ گرفته باشد، مشکل و راه حل چیست؟
۱۳. موارد استفاده و کاربرد دستور ipconfig/flushdns چیست؟

- [1] D. Coleman و D. A. Westcott D, Certified Wireless Network Administrator (CWNA), Indian simultaneously in Canada: Wiley, 2010.
- [2] K. j. Kim و N. Joukov, Mobile and Wireless Technologies 2017, Singapore: Springer , 2018.
- [3] M. Hakimi Kia, Wireless Networks, Hardward and software , 1389.
- [4] T. Carpenter و J. Barrettt, Certified Wireless Network Administrator (CWNA), New York: McGraw-Hill, 2008.
- [5] M. Neezad, Wireless Sensor Networking, 1394.
- [6] D. Hucaby, CCNA Wireless 200-355, IN 46240 USA: Cisco Press, 2015.
- [7] .Z.Jun و A. Jamlipour, Wireless Sensor Networks: A Networking Perspective,JOHN WILEY&SONS, 2009.
- [8] K. NIT, "4G,"International Journal of Electronics and Communication Engineering,pp. 67-73, 1 Number 2013.
- [9] "www.wikipedia.org," 2017. [درون خطی].
- [10] P. Venkataram, Wireless and Mobile Network Security, Moujpur, Delhi 110 053: Tata McGraw , 2012.